

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ

Математико-механический факультет

ИЗБРАННЫЕ ГЛАВЫ
дискретного гармонического анализа
и геометрического моделирования

Под редакцией проф. В. Н. Малозёмова

Санкт-Петербург
2009 г.

АННОТАЦИЯ

Избранные главы дискретного гармонического анализа и геометрического моделирования. Под ред. проф. В. Н. Малозёмова. 2009. 584 с.

Дискретный гармонический анализ (Discrete Harmonic Analysis, DHA) — относительно молодое направление в прикладной математике, ориентированное на цифровую обработку сигналов. В DHA используются, в основном, дискретное преобразование Фурье, дискретные вейвлетные преобразования и циклические свёртки.

Геометрическое моделирование (Computer Aided Geometric Design, CAGD) связано с построением кривых и поверхностей по ограниченной информации. К популярным средствам CAGD относятся кривые и поверхности Безье и поверхности Кунса.

Для совершенствования базовых знаний в области DHA & CAGD и для дальнейшего развития этих направлений на математико-механическом факультете СПбГУ в 2004 году был организован семинар. Основные итоги работы семинара за 2004–2008 годы подводятся в этой книге.

Для студентов старших курсов и аспирантов математических специальностей и специалистов в области цифровой обработки сигналов и геометрического моделирования.

*Тот, кто знает Учение,
уступает тому, кто находит
в нём удовольствие.
Конфуций*

Содержание

Предисловие	9
Основные обозначения	11

2004

<i>В. Н. Малозёмов, О. В. Просеков</i> ПЕРЕСТАНОВКИ И КРОНЕКЕРОВО ПРОИЗВЕДЕНИЕ МАТРИЦ	12
<i>В. Н. Малозёмов, О. В. Просеков</i> ФАКТОРИЗАЦИЯ КУЛИ-ТЮЮКИ МАТРИЦЫ ФУРЬЕ	20
<i>В. Н. Малозёмов, О. В. Просеков</i> ФАКТОРИЗАЦИЯ ГУДА МАТРИЦЫ ФУРЬЕ	30
<i>В. Н. Малозёмов</i> ПАРАМЕТРИЧЕСКОЕ КОДИРОВАНИЕ ИНДЕКСОВ	35
<i>В. Н. Малозёмов</i> О СПЕКТРЕ ФУРЬЕ ФУНКЦИЙ УОЛША	41
<i>В. Н. Малозёмов</i> РЯДЫ ФУРЬЕ И ДПФ	48
<i>В. Н. Малозёмов, С. В. Рыбин</i> РЕКУРРЕНТНЫЙ ВАРИАНТ МЕТОДА НАИМЕНЬШИХ КВАДРАТОВ	50
<i>М. И. Григорьев, В. Н. Малозёмов, А. Н. Сергеев</i> ПОЛИНОМЫ БЕРНШТЕЙНА И СОСТАВНЫЕ КРИВЫЕ БЕЗЬЕ	53

2005

<i>В. Н. Малозёмов, Н. А. Селянинова</i> ПРЯМАЯ ЛИФТИНГОВАЯ СХЕМА	64
<i>В. Н. Малозёмов, А. Б. Певный</i> ПРОГРАММИРОВАНИЕ И МАТЕМАТИКА	74

<i>В. Н. Малозёмов, С. В. Рыбин</i> ЧАСТОТНЫЙ КОНВЕРТЕР	91
<i>В. Н. Малозёмов</i> ПОДСЧЁТ КОЛИЧЕСТВА АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ ПРИ ВЫЧИСЛЕНИИ БПФ	94
<i>В. Н. Малозёмов, О. В. Просеков</i> БЫСТРОЕ ВЫЧИСЛЕНИЕ ЦИКЛИЧЕСКИХ СВЁРТОК МАЛЫХ ПОРЯДКОВ	100
<i>О. В. Просеков</i> БЫСТРОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ МАЛЫХ ПОРЯДКОВ . .	112

2006

<i>В. Н. Малозёмов, А. Н. Сабает</i> ТЕОРЕМА ОБ ОТСЧЁТАХ В ДИСКРЕТНОМ ПЕРИОДИЧЕСКОМ СЛУЧАЕ	141
<i>В. Н. Малозёмов, А. Б. Певный</i> ЖЁСТКИЕ ФРЕЙМЫ	147
<i>В. Н. Малозёмов, Н. А. Селянинова</i> ДВОЙСТВЕННАЯ ЛИФТИНГОВАЯ СХЕМА	156
<i>А. Б. Певный</i> ФРЕЙМЫ В КОНЕЧНОМЕРНЫХ ПРОСТРАНСТВАХ И ЗАДАЧА МИНИМИЗАЦИИ ФРЕЙМОВОГО ПОТЕНЦИАЛА	166
<i>В. А. Жёлудев, В. Н. Малозёмов, А. Б. Певный</i> БАНКИ ФИЛЬТРОВ И ФРЕЙМЫ	173
<i>В. Н. Малозёмов, О. В. Просеков</i> ФАКТОРИЗАЦИЯ МАТРИЦ РЕВЕРСНЫХ ПЕРЕСТАНОВОК . . .	187
<i>В. Н. Малозёмов</i> РАЗБИЕНИЕ КРИВЫХ БЕЗЪЕ	195
<i>В. Н. Малозёмов</i> ВАРИАЦИИ КРИВЫХ БЕЗЪЕ	202
<i>Г. Н. Малолеткин</i> ВЫЧИСЛЕНИЕ ДПФ ЛЮБОЙ ДЛИНЫ	208
<i>В. Н. Малозёмов, О. В. Просеков</i> ПАРАМЕТРИЧЕСКИЙ ВАРИАНТ МЕТОДА ПРОСТЫХ МНОЖИТЕЛЕЙ	212
<i>В. Н. Малозёмов, О. В. Просеков</i> ОБЩИЙ ПОДХОД К ВЫЧИСЛЕНИЮ ДПФ	218

<i>В. Н. Малозёмов, О. В. Просеков</i>	
ПАРАМЕТРИЧЕСКАЯ ФАКТОРИЗАЦИЯ МАТРИЦЫ ФУРЬЕ . . .	224
<i>О. В. Просеков</i>	
ПАРАМЕТРИЧЕСКИЙ ВАРИАНТ МНОГОМЕРНОГО БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ	233
<i>В. Н. Малозёмов</i>	
РАЗДЕЛЁННЫЕ РАЗНОСТИ С КРАТНЫМИ УЗЛАМИ	241
<i>Н. В. Чашников</i>	
БИЛИНЕЙНЫЕ ПОВЕРХНОСТИ КУНСА И ПОВЕРХНОСТИ БЕЗЬЕ	248
<i>В. Н. Малозёмов</i>	
ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ПОЛЯРНЫХ ФОРМ	258
<i>И. В. Агафонова</i>	
ФАКТОРИЗАЦИЯ БОЛЬШИХ ЦЕЛЫХ ЧИСЕЛ И КРИПТОГРАФИЯ	265
<i>М. И. Григорьев, В. Н. Малозёмов, А. Н. Сергеев</i>	
МОЖНО ЛИ ПОСТРОИТЬ ОКРУЖНОСТЬ С ПОМОЩЬЮ КРИВЫХ БЕЗЬЕ?	281

2007

<i>В. Н. Малозёмов, А. Б. Певный</i>	
ФРЕЙМ МЕРСЕДЕС-БЕНЦ В n -МЕРНОМ ПРОСТРАНСТВЕ	288
<i>В. Н. Малозёмов, Н. В. Чашников</i>	
БИКУБИЧЕСКИЕ ПОВЕРХНОСТИ КУНСА	295
<i>Н. В. Чашников</i>	
СОСТАВНЫЕ ПАРАМЕТРИЧЕСКИЕ ПОВЕРХНОСТИ КУНСА . .	303
<i>М. И. Григорьев</i>	
ПОСТРОЕНИЕ СФЕРЫ С ПОМОЩЬЮ ПРОЕКТИВНЫХ ПОВЕРХНОСТЕЙ БЕЗЬЕ	309
<i>В. Н. Малозёмов, А. Б. Певный</i>	
СИСТЕМЫ МЕРСЕДЕС-БЕНЦ И ЖЁСТКИЕ ФРЕЙМЫ	315
<i>И. А. Капелюхин, В. Н. Малозёмов, А. Н. Сергеев</i>	
ПОВЕРХНОСТИ БЕЗЬЕ НА ТРЕУГОЛЬНИКЕ. ПЕРЕПАРАМЕТРИЗАЦИЯ	321
<i>М. И. Григорьев, В. Н. Малозёмов</i>	
ПОЛЕ ЗАМКНУТЫХ КРИВЫХ БЕЗЬЕ	328

<i>М. Н. Истомина</i>	
ВОССТАНОВЛЕНИЕ СИГНАЛА В СЛУЧАЕ УТРАТЫ ОДНОГО ФРЕЙМОВОГО КОЭФФИЦИЕНТА	334
<i>А. Б. Певный</i>	
МАКСИМАЛЬНАЯ ИЗБЫТОЧНОСТЬ ГАРМОНИЧЕСКИХ ФРЕЙМОВ	337
<i>В. Н. Малозёмов, А. Н. Сергеев, Н. В. Чашников</i>	
ПОВЕРХНОСТИ КУНСА НА ТРЕУГОЛЬНИКЕ	341
<i>В. Н. Малозёмов, А. Б. Певный</i>	
ЧЕТВЁРТОЕ ОПРЕДЕЛЕНИЕ ЖЁСТКОГО ФРЕЙМА	347
<i>М. И. Григорьев</i>	
МОДЕЛИРОВАНИЕ ПОВЕРХНОСТЕЙ ВРАЩЕНИЯ	352
<i>В. Н. Малозёмов, Н. А. Соловьёва</i>	
ДВОЙСТВЕННЫЕ ФРЕЙМЫ	357
<i>В. Н. Малозёмов, О. В. Просеков</i>	
КРОНЕКЕРОВО УМНОЖЕНИЕ МАТРИЦ И КОММУТАТИВНОСТЬ	361
<i>Н. В. Чашников</i>	
ПОВЕРХНОСТЬ ВРАЩЕНИЯ КАК ПОВЕРХНОСТЬ КУНСА	364
<i>В. Н. Малозёмов, Д. А. Хорохонов, Н. В. Чашников</i>	
ДИСКРЕТНЫЕ ПЕРИОДИЧЕСКИЕ СПЛАЙНЫ С ВЕКТОРНЫМИ КОЭФФИЦИЕНТАМИ И ГЕОМЕТРИЧЕСКОЕ МОДЕЛИРОВАНИЕ	371
<i>М. И. Григорьев</i>	
ОБОБЩЁННЫЕ ПОВЕРХНОСТИ ВРАЩЕНИЯ	382
<i>В. Н. Малозёмов, А. Б. Певный</i>	
РАВНОУГОЛЬНЫЕ СИСТЕМЫ ВЕКТОРОВ И ЖЁСТКИЕ ФРЕЙМЫ	389
<i>А. Н. Сабеев</i>	
ПРИМЕНЕНИЕ СХЕМЫ КЛЕНШОУ ДЛЯ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ С ТРЁХ- И ПЯТИДИАГОНАЛЬНЫМИ ЦИКЛИЧЕСКИМИ МАТРИЦАМИ	397
<i>А. М. Дурагин, Н. А. Соловьёва</i>	
ВЕЩЕСТВЕННЫЕ ГАРМОНИЧЕСКИЕ ФРЕЙМЫ	406
<i>Н. В. Чашников</i>	
СМЕШИВАЮЩИЕ ФУНКЦИИ	411
<i>А. М. Дурагин, А. Б. Певный</i>	
ФРЕЙМЫ ГРАССМАНА	423

<i>И. В. Агафонова</i> КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ	428
----------------------------------------------------------------------------------------------	-----

2008

<i>В. Н. Малозёмов, О. В. Просеков, А. Н. Сабеев</i> ДИСКРЕТНЫЕ ФУНКЦИИ ВИЛЕНКИНА-КРЕСТЕНСОНА	452
<i>В. Н. Малозёмов, Н. А. Соловьёва</i> ОБ УНИТАРНЫХ МАТРИЦАХ И СИНГУЛЯРНЫХ РАЗЛОЖЕНИЯХ	460
<i>В. Н. Малозёмов, А. Б. Певный</i> СИСТЕМ МЕРСЕДЕС-БЕНЦ ПРИ $m > n + 1$ НЕ СУЩЕСТВУЕТ	464
<i>Н. А. Соловьёва</i> О ЖЁСТКИХ ФРЕЙМАХ СПЕЦИАЛЬНОГО ВИДА	466
<i>Н. В. Чашников</i> СОСТАВНЫЕ И ОБОБЩЁННЫЕ ПОВЕРХНОСТИ КУНСА	468
<i>В. В. Максименко, А. Б. Певный</i> СУЩЕСТВОВАНИЕ РАВНОУГОЛЬНЫХ ЖЁСТКИХ ФРЕЙМОВ	477
<i>А. М. Дурагин</i> МАКСИМАЛЬНАЯ ИЗБЫТОЧНОСТЬ ВЕЩЕСТВЕННЫХ ГАРМОНИЧЕСКИХ ФРЕЙМОВ	484
<i>М. И. Григорьев</i> ПОЛИНОМЫ БЕРНШТЕЙНА ОТ ДВУХ ПЕРЕМЕННЫХ	492
<i>М. И. Григорьев, А. Н. Сергеев</i> ПОЛЯРНАЯ ФОРМА ПОЛИНОМОВ ОТ ДВУХ ПЕРЕМЕННЫХ	500
<i>Н. А. Соловьёва</i> ОБОБЩЁННЫЕ ГАРМОНИЧЕСКИЕ ФРЕЙМЫ	507
<i>М. И. Григорьев, В. Н. Малозёмов, А. Н. Сергеев</i> ОСНОВНАЯ ЛЕММА ТЕОРИИ ПОЛЯРНЫХ ФОРМ ПОЛИНОМОВ ОТ ДВУХ ПЕРЕМЕННЫХ	516
<i>В. Н. Малозёмов, С. М. Машарский</i> АНСАМБЛИ ДИСКРЕТНЫХ ПЕРИОДИЧЕСКИХ СИГНАЛОВ	522
<i>Н. В. Чашников</i> ПОСТРОЕНИЕ ЗАМКНУТЫХ КРИВЫХ С ПОМОЩЬЮ ДИСКРЕТНЫХ ПЕРИОДИЧЕСКИХ СПЛАЙНОВ	529

<i>М. И. Григорьев, В. Н. Малозёмов</i> ПОСТРОЕНИЕ КРИВЫХ С ПОМОЩЬЮ ОБОБЩЁННЫХ ПОЛИНОМОВ БЕРНШТЕЙНА	534
<i>М. Н. Истомина, А. Б. Певный</i> МЕТОД ПОПЕРЕМЕННОГО ПРОЕКТИРОВАНИЯ ДЛЯ ПОСТРОЕНИЯ РАВНОУГОЛЬНЫХ ЖЁСТКИХ ФРЕЙМОВ	542
<i>А. Н. Сабеев</i> ЗАМЕЧАНИЕ О СИСТЕМАХ МЕРСЕДЕС-БЕНЦ	551
<i>М. И. Григорьев</i> ПОВЕРХНОСТИ БЕЗЬЕ НА ЧЕТЫРЁХУГОЛЬНИКЕ И ГЛАДКИЕ СОСТАВНЫЕ ПОВЕРХНОСТИ	553
<i>Н. В. Чашников</i> ПОВЕРХНОСТИ КУНСА НА ТРЕУГОЛЬНИКЕ С ГРАНИЧНЫМИ УСЛОВИЯМИ ПЕРВОГО ПОРЯДКА	564
<i>В. Н. Малозёмов</i> НЕСКОЛЬКО ЗАМЕЧАНИЙ О ЖЁСТКИХ ФРЕЙМАХ	575
Список участников семинара	582
Предметный указатель	583

Предисловие

В данной книге подводятся итоги работы семинара по дискретному гармоническому анализу и геометрическому моделированию при математикомеханическом факультете СПбГУ за 2004–2008 годы. Семинар был организован в январе 2004 года, сразу после опубликования книги:

Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Части 1-3. СПб., НИИММ СПбГУ, 2003. 288 с.

Перед участниками семинара ставилась задача дальнейшего развития дискретного гармонического анализа (Discrete Harmonic Analysis, DHA). Вскоре проблематику семинара пришлось расширить, включив в неё геометрическое моделирование (Computer Aided Geometric Design, CAGD). Вопросы визуализации в наше время игнорировать нельзя. Семинар стал называться «DHA & CAGD».

С первого взгляда, объединение двух указанных направлений выглядит искусственным, однако, как выяснилось, дискретные периодические сплайны с векторными коэффициентами являются адекватным математическим аппаратом при моделировании замкнутых кривых и поверхностей. Так в CAGD вошло дискретное преобразование Фурье.

В работе семинара «DHA & CAGD» принимали участие студенты старших курсов и аспиранты, у которых я был научным руководителем. Со временем к нам присоединилась группа из Сыктывкарского университета, руководимая проф. А. Б. Певным. Список участников семинара приведён в конце книги.

С самого начала было принято принципиальное решение — вести сайт семинара. Его создал и в течение пяти лет поддерживал О. В. Просеков (в 2004 году — аспирант первого курса, ныне — кандидат физ.-мат. наук). Адрес сайта: <http://dha.spb.ru>. На сайте много полезной информации, но наибольшую ценность имеет раздел «Избранные доклады». Из докладов этого раздела и составлена книга.

Доклады приведены в хронологическом порядке. По ним можно проследить, как формируется «язык семинара», как аспиранты становятся кандидатами наук. Содержание каждого доклада относительно независимо, что облегчает чтение.

Жанр данной книги определить непросто. Естественно, авторы докладов стремились получить новые результаты. Но для этого требовалось навести порядок в базовых знаниях, представить их в виде, удобном для непосредственного применения. Например, чтобы заниматься быстрым преобразованием Фурье, нужно разобраться в кронекеровом умножении матриц и свойствах специальных матриц перестановок. Добиться успеха в теории кривых и поверхностей Безье невозможно без углубления в свойства полиномов в форме Бернштейна от одной и двух переменных. Вопросам совершенствования

базовых знаний на семинаре уделялось большое внимание, что нашло отражение в соответствующих докладах. В этом плане книга является учебным изданием. Вместе с тем, книга содержит и новые результаты. Они касаются параметрических вариантов быстрого преобразования Фурье, вейвлетных разложений дискретных периодических сигналов, равноугольных жёстких фреймов (в частности, фреймов Мерседес-Бенц в n -мерном пространстве), составных поверхностей Безье и Кунса. В предметном указателе более подробно представлены объекты исследований. Так что книга имеет и научный характер. Можно сказать, что данная книга относится к жанру учебно-научной литературы.

Основной труд по подготовке этого издания взял на себя М. И. Григорьев, который как участник семинара тоже прошёл путь от аспиранта первого курса до кандидата физ.-мат. наук.

Надеюсь, что книга будет интересна широкому кругу читателей, и прежде всего студентам, выбирающим тему научного исследования.

Июнь 2009 г.

В. Н. Малозёмов

Основные обозначения

\mathbb{Z} , \mathbb{R} , \mathbb{C} — множества целых, вещественных и комплексных чисел соответственно;

$k : j = \{k, k+1, \dots, j\}$ — множество целых чисел от k до j включительно ($k, j \in \mathbb{Z}$);

$[\alpha]$ — целая часть числа $\alpha \in \mathbb{R}$, определяемая неравенствами

$$[\alpha] \leq \alpha < [\alpha] + 1;$$

$\langle k \rangle_n = k - [k/n]n$ — вычет целого числа k по модулю натурального n ;

$\omega_n = \exp(2\pi i/n)$ — корень n -й степени из единицы;

\mathbb{C}_N — пространство сигналов (комплекснозначных N -периодических функций целочисленного аргумента $x = x(j)$, $j \in \mathbb{Z}$);

$\delta_N = \delta_N(j)$ — единичный N -периодический импульс, равный единице, когда j делится на N , и равный нулю в противном случае;

$\langle x, y \rangle = \sum_{j=0}^{N-1} x(j) \overline{y(j)}$ — скалярное произведение сигналов x и y ;

$\|x\| = \sqrt{\langle x, x \rangle}$ — норма сигнала x ;

$u = x * y$ — циклическая свёртка сигналов x и y (сигнал с отсчётами

$$u(k) = \sum_{j=0}^{N-1} x(j) y(k-j), \quad k \in \mathbb{Z};$$

\mathcal{F}_N — дискретное преобразование Фурье порядка N , сопоставляющее сигналу x его спектр $X = \mathcal{F}_N(x)$ с компонентами

$$X(k) = \sum_{j=0}^{N-1} x(j) \omega_N^{-kj}, \quad k \in \mathbb{Z};$$

\mathcal{F}_N^{-1} — обратное преобразование Фурье, действующее по формуле

$$x(j) = \frac{1}{N} \sum_{k=0}^{N-1} X(k) \omega_N^{kj}, \quad j \in \mathbb{Z};$$

I_n — единичная матрица порядка n .

ПЕРЕСТАНОВКИ И КРОНЕКЕРОВО ПРОИЗВЕДЕНИЕ МАТРИЦ

В. Н. Малозёмов

О. В. Просеков

31 марта 2004 г.

Доклад представляет собой вариации на темы первой половины обзорной статьи [1].

Будут использоваться следующие обозначения:

$A_n = A_n[0 : n - 1, 0 : n - 1]$ — квадратная матрица порядка n , индексы строк и столбцов которой изменяются от 0 до $n - 1$;

$I_n = I_n[0 : n - 1, 0 : n - 1]$ — единичная матрица порядка n .

1°. Пусть m, n — натуральные числа. Введём квадратную матрицу $L_{mn}^{(n)}$ порядка mn с элементами

$$L_{mn}^{(n)}[i + jm, i' + j'n] = \begin{cases} 1, & \text{если } i' = i \text{ и } j' = j, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Здесь $i, i' \in 0 : m - 1, j, j' \in 0 : n - 1$. При $m = 2, n = 3$ имеем

$$L_6^{(3)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Нетрудно проверить, что

$$L_n^{(n)} = I_n, \quad L_m^{(1)} = I_m. \quad (1)$$

Умножение матрицы $L_{mn}^{(n)}$ на вектор $x \in \mathbb{C}^{mn}$ порождает вектор $X = L_{mn}^{(n)} x$ с компонентами

$$X(i + jm) = x(i + jn), \quad i \in 0 : m - 1, \quad j \in 0 : n - 1. \quad (2)$$

Действительно,

$$X(i + j m) = \sum_{i'=0}^{m-1} \sum_{j'=0}^{n-1} L_{mn}^{(n)}[i + j m, i' n + j'] \times x(i' n + j') = x(i n + j).$$

В каждой строке и каждом столбце матрицы $L_{mn}^{(n)}$ лишь один элемент отличен от нуля (равен единице). Такие матрицы называются *матрицами перестановок*. Для $L_{mn}^{(n)}$ как матрицы перестановок справедлива формула $(L_{mn}^{(n)})^{-1} = (L_{mn}^{(n)})^T$. Можно получить более точный результат.

ЛЕММА 1. $(L_{mn}^{(n)})^{-1} = L_{mn}^{(m)}$.

Доказательство. Достаточно проверить, что $L_{mn}^{(n)} L_{mn}^{(m)} = I_{mn}$. Имеем

$$\begin{aligned} (L_{mn}^{(n)} L_{mn}^{(m)})[i + j m, i' + j' m] &= \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} L_{mn}^{(n)}[i + j m, i_1 n + j_1] \times \\ &\times L_{mn}^{(m)}[i_1 n + j_1, i' + j' m] = L_{mn}^{(m)}[j + i n, j' m + i']. \end{aligned}$$

Последнее выражение равно единице только при $j' = j, i' = i$. □

ЛЕММА 2. Пусть $N = r m n$. Тогда

$$L_N^{(mn)} = L_N^{(m)} L_N^{(n)}. \quad (3)$$

Доказательство. Положим $X = L_N^{(mn)} x$. Согласно (2)

$$X(i + j r) = x(i m n + j), \quad i \in 0 : r - 1, \quad j \in 0 : m n - 1.$$

Представим индекс j в виде $j = k n + l, l \in 0 : n - 1, k \in 0 : m - 1$. Получим

$$X(k n r + l r + i) = x(i m n + k n + l).$$

Вектор $Y = L_N^{(n)} x$ имеет координаты

$$Y(p + l m r) = x(p n + l), \quad l \in 0 : n - 1, \quad p \in 0 : m r - 1.$$

Вычислим координаты вектора $Z = L_N^{(m)} Y$:

$$\begin{aligned} Z(k n r + l r + i) &= Y((l r + i) m + k) = Y(l r m + (i m + k)) = \\ &= x((i m + k) n + l) = x(i m n + k n + l) = X(k n r + l r + i). \end{aligned}$$

Значит, $Z = X$, т. е. $(L_N^{(m)} L_N^{(n)}) x = L_N^{(mn)} x$. Отсюда очевидным образом следует (3). □

З а м е ч а н и я.

1) Согласно (3), $L_N^{(nm)} = L_N^{(n)} L_N^{(m)}$, так что

$$L_N^{(m)} L_N^{(n)} = L_N^{(n)} L_N^{(m)}.$$

2) В условиях леммы 2 справедлива формула

$$L_N^{(rm)} L_N^{(nr)} = L_N^{(r)}. \quad (4)$$

Действительно, $L_N^{(rm)} L_N^{(nr)} = (L_N^{(rm)} L_N^{(n)}) L_N^{(r)} = L_N^{(r)}$.

2°. Кронекеровым произведением матриц A_m и B_n называется матрица $D_{mn} = A_m \otimes B_n$ с элементами

$$D_{mn}[i n + j, i' n + j'] = A_m[i, i'] B_n[j, j'], \quad i, i' \in 0 : m - 1, \quad j, j' \in 0 : n - 1.$$

Более наглядно

$$D_{mn} = \begin{bmatrix} A_m[0, 0] B_n & A_m[0, 1] B_n & \dots & A_m[0, m-1] B_n \\ A_m[1, 0] B_n & A_m[1, 1] B_n & \dots & A_m[1, m-1] B_n \\ \dots & \dots & \dots & \dots \\ A_m[m-1, 0] B_n & A_m[m-1, 1] B_n & \dots & A_m[m-1, m-1] B_n \end{bmatrix}.$$

Операция кронекерова умножения ассоциативна, т. е.

$$(A_m \otimes B_n) \otimes C_p = A_m \otimes (B_n \otimes C_p).$$

Проверим это. При $i \in 0 : m - 1$, $j \in 0 : n - 1$, $k \in 0 : p - 1$ имеем

$$\begin{aligned} & \left((A_m \otimes B_n) \otimes C_p \right) [i n p + j p + k, i' n p + j' p + k'] = \\ & = \left((A_m \otimes B_n) \otimes C_p \right) [(i n + j) p + k, (i' n + j') p + k'] = \\ & = (A_m \otimes B_n) [i n + j, i' n + j'] C_p[k, k'] = A_m[i, i'] B_n[j, j'] C_p[k, k']. \end{aligned}$$

Вместе с тем,

$$\begin{aligned} & \left(A_m \otimes (B_n \otimes C_p) \right) [i n p + j p + k, i' n p + j' p + k'] = \\ & = \left(A_m \otimes (B_n \otimes C_p) \right) [i n p + (j p + k), i' n p + (j' p + k')] = \\ & = A_m[i, i'] (B_n \otimes C_p) [j p + k, j' p + k'] = A_m[i, i'] B_n[j, j'] C_p[k, k']. \end{aligned}$$

Ассоциативность установлена.

Коммутативность заменяется следующим свойством.

ТЕОРЕМА 1. $B_n \otimes A_m = L_{mn}^{(n)}(A_m \otimes B_n)L_{mn}^{(m)}.$

Доказательство. В силу леммы 1 достаточно проверить, что

$$L_{mn}^{(m)}(B_n \otimes A_m) = (A_m \otimes B_n)L_{mn}^{(m)}. \quad (5)$$

Сравним элементы с индексами $(j + i n, j' m + i')$, $i, i' \in 0 : m - 1$, $j, j' \in 0 : n - 1$. Имеем

$$\begin{aligned} \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} L_{mn}^{(m)}[j + i n, j_1 m + i_1] \times (B_n \otimes A_m)[j_1 m + i_1, j' m + i'] = \\ = (B_n \otimes A_m)[j m + i, j' m + i'] = B_n[j, j'] A_m[i, i']. \end{aligned}$$

Вместе с тем,

$$\begin{aligned} \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} (A_m \otimes B_n)[j + i n, j_1 + i_1 n] \times L_{mn}^{(m)}[j_1 + i_1 n, j' m + i'] = \\ = (A_m \otimes B_n)[i n + j, i' n + j'] = A_m[i, i'] B_n[j, j']. \end{aligned}$$

Равенство (5), равносильное утверждение теоремы, установлено. \square

3°. В лемме 2 указана факторизация матрицы перестановок $L_{mn}^{(n)}$, связанная с разложением на множители верхнего индекса. Существует факторизация, связанная с разложением на множители нижнего индекса.

ЛЕММА 3. Пусть $N = r m n$. Тогда

$$L_N^{(n)} = (L_{rn}^{(n)} \otimes I_m)(I_r \otimes L_{mn}^{(n)}). \quad (6)$$

Доказательство. Вектор $X = L_N^{(n)} x$ имеет компоненты

$$X(i + j r m) = x(i n + j), \quad i \in 0 : r m - 1, \quad j \in 0 : n - 1.$$

Положив $i = k m + l$, $l \in 0 : m - 1$, $k \in 0 : r - 1$, получим

$$X(j r m + k m + l) = x(k m n + l n + j).$$

Введём вектор $Y = (I_r \otimes L_{mn}^{(n)}) x$. Для него

$$Y(k m n + j m + l) = \sum_{k'=0}^{r-1} \sum_{j'=0}^{n-1} \sum_{l'=0}^{m-1} (I_r \otimes L_{mn}^{(n)})[k m n + j m + l, k' m n + l' n + j'] \times$$

$$\begin{aligned} \times x(k' mn + l' n + j') &= \sum_{k'=0}^{r-1} \sum_{j'=0}^{n-1} \sum_{l'=0}^{m-1} I_r[k, k'] \times L_{mn}^{(n)}[l + j m, l' n + j'] \times \\ &\times x(k' mn + l' n + j') = x(k mn + l n + j). \end{aligned}$$

Вычислим компоненты вектора $Z = (L_{rn}^{(n)} \otimes I_m) Y$:

$$\begin{aligned} Z(j rm + k m + l) &= \\ &= \sum_{k'=0}^{r-1} \sum_{j'=0}^{n-1} \sum_{l'=0}^{m-1} (L_{rn}^{(n)} \otimes I_m)[(j r + k) m + l, (k' n + j') m + l'] \times Y((k' n + j') m + l') = \\ &= \sum_{k'=0}^{r-1} \sum_{j'=0}^{n-1} \sum_{l'=0}^{m-1} L_{rn}^{(n)}[k + j r, k' n + j'] \times I_m[l, l'] \times Y((k' n + j') m + l') = \\ &= Y((k n + j) m + l) = x(k mn + l n + j) = X(j rm + k m + l). \end{aligned}$$

Значит, $Z = X$, т. е. $(L_{rn}^{(n)} \otimes I_m)(I_r \otimes L_{mn}^{(n)}) x = L_N^{(n)} x$. Отсюда очевидным образом следует (6). \square

4°. Между кронекеровым и обычным произведениями матриц имеется глубокая связь.

ТЕОРЕМА 2. *Справедлива формула*

$$(A_m \otimes B_n)(G_m \otimes H_n) = (A_m G_m) \otimes (B_n H_n).$$

Доказательство. Сравним элементы с индексами $(i n + j, i' n + j')$, $i, i' \in 0 : m - 1$, $j, j' \in 0 : n - 1$. Запишем

$$\begin{aligned} &((A_m \otimes B_n)(G_m \otimes H_n))[i n + j, i' n + j'] = \\ &= \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} (A_m \otimes B_n)[i n + j, i_1 n + j_1] \times (G_m \otimes H_n)[i_1 n + j_1, i' n + j'] = \\ &= \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} A_m[i, i_1] \times B_n[j, j_1] \times G_m[i_1, i'] \times H_n[j_1, j'] = \\ &= \sum_{i_1=0}^{m-1} A_m[i, i_1] \times G_m[i_1, i'] \sum_{j_1=0}^{n-1} B_n[j, j_1] \times H_n[j_1, j'] = \\ &= (A_m G_m)[i, i'] (B_n H_n)[j, j']. \end{aligned}$$

Остаётся учесть, что

$$((A_m G_m) \otimes (B_n H_n))[i n + j, i' n + j'] = (A_m G_m)[i, i'] (B_n H_n)[j, j'].$$

Теорема доказана. \square

Теорема 2 допускает естественные обобщения.

ЛЕММА 4. *Для пар квадратных матриц $A_{\nu,m}$, $B_{\nu,n}$, $\nu = 1, \dots, s$, порядков m и n соответственно справедлива формула*

$$\prod_{\nu=1}^s (A_{\nu,m} \otimes B_{\nu,n}) = \left(\prod_{\nu=1}^s A_{\nu,m} \right) \otimes \left(\prod_{\nu=1}^s B_{\nu,n} \right).$$

Доказательство. При $s = 2$ утверждение леммы следует из теоремы 2. Сделаем индукционный переход от s к $s + 1$. Согласно индукционному предположению и теореме 2 имеем

$$\begin{aligned} \prod_{\nu=1}^{s+1} (A_{\nu,m} \otimes B_{\nu,n}) &= \left(\left(\prod_{\nu=1}^s A_{\nu,m} \right) \otimes \left(\prod_{\nu=1}^s B_{\nu,n} \right) \right) (A_{s+1,m} \otimes B_{s+1,n}) = \\ &= \left(\prod_{\nu=1}^{s+1} A_{\nu,m} \right) \otimes \left(\prod_{\nu=1}^{s+1} B_{\nu,n} \right). \end{aligned}$$

Лемма доказана. □

ТЕОРЕМА 3. *Справедлива формула*

$$\begin{aligned} \prod_{\nu=1}^s (A_{\nu,n_1} \otimes B_{\nu,n_2} \otimes \dots \otimes G_{\nu,n_p}) &= \\ &= \left(\prod_{\nu=1}^s A_{\nu,n_1} \right) \otimes \left(\prod_{\nu=1}^s B_{\nu,n_2} \right) \otimes \dots \otimes \left(\prod_{\nu=1}^s G_{\nu,n_p} \right). \end{aligned} \tag{7}$$

Доказательство. При $p = 2$ теорема 3 соответствует лемме 4. Сделаем индукционный переход от p к $p + 1$. В силу леммы 4 и индукционного предположения имеем

$$\begin{aligned} \prod_{\nu=1}^s (A_{\nu,n_1} \otimes B_{\nu,n_2} \otimes \dots \otimes G_{\nu,n_p} \otimes H_{\nu,n_{p+1}}) &= \\ &= \left(\prod_{\nu=1}^s (A_{\nu,n_1} \otimes B_{\nu,n_2} \otimes \dots \otimes G_{\nu,n_p}) \right) \otimes \left(\prod_{\nu=1}^s H_{\nu,n_{p+1}} \right) = \\ &= \left(\prod_{\nu=1}^s A_{\nu,n_1} \right) \otimes \left(\prod_{\nu=1}^s B_{\nu,n_2} \right) \otimes \dots \otimes \left(\prod_{\nu=1}^s G_{\nu,n_p} \right) \otimes \left(\prod_{\nu=1}^s H_{\nu,n_{p+1}} \right). \end{aligned}$$

Теорема доказана. □

5°. Рассмотрим некоторые приложения предыдущих результатов. Пусть $N = n_1 n_2 \dots n_s$. Обозначим $\Delta_1 = 1$; $\Delta_\nu = n_1 n_2 \dots n_{\nu-1}$, $\nu = 2, \dots, s+1$; $N_\nu = N/\Delta_{\nu+1}$. Очевидно, что $N_0 = N$, $N_s = 1$ и $N_\nu = n_{\nu+1} \dots n_s$ при $\nu = 1, \dots, s-1$.

ТЕОРЕМА 4. *Справедлива формула*

$$A_{n_1} \otimes A_{n_2} \otimes \dots \otimes A_{n_s} = \prod_{\nu=1}^s (I_{\Delta_\nu} \otimes A_{n_\nu} \otimes I_{N_\nu}). \quad (8)$$

Более того, сомножители в правой части (8) можно переставлять в любом порядке.

Доказательство. Воспользуемся соотношением (7). Приняв во внимание, что $I_m \otimes I_n = I_{mn}$, запишем

$$\begin{aligned} A_{n_1} \otimes A_{n_2} \otimes \dots \otimes A_{n_s} &= \underbrace{(A_{n_1} I_{n_1} \dots I_{n_1})}_{(s-1) \text{ раз}} \otimes \underbrace{(I_{n_2} A_{n_2} I_{n_2} \dots I_{n_2})}_{(s-2) \text{ раза}} \otimes \dots \otimes \\ &\otimes \underbrace{(I_{n_s} \dots I_{n_s} A_{n_s})}_{(s-1) \text{ раз}} = (A_{n_1} \otimes I_{N_1})(I_{n_1} \otimes A_{n_2} \otimes I_{N_2}) \dots (I_{\Delta_s} \otimes A_{n_s}). \end{aligned} \quad (9)$$

Формулы (8) и (9) равносильны, поскольку $I_{\Delta_1} = I_{N_s} = I_1 = (1)$ и $I_{n_1} = I_{\Delta_2}$.

Возможность переставлять сомножители в правой части (8) следует из того, что матрицу A_{n_ν} можно получить, заменив в произведении $\underbrace{I_{n_\nu} I_{n_\nu} \dots I_{n_\nu}}_{s \text{ раз}}$ любой сомножитель на A_{n_ν} . Теорема доказана. \square

Теорема 4 служит основой для вывода других вариантов факторизации кронекерова произведения матриц.

ТЕОРЕМА 5. *Справедлива формула*

$$A_{n_1} \otimes A_{n_2} \otimes \dots \otimes A_{n_s} = \prod_{\nu=1}^s (I_{\Delta_\nu} \otimes L_{N_{\nu-1}}^{(n_\nu)})(I_{N/n_\nu} \otimes A_{n_\nu})(I_{\Delta_\nu} \otimes L_{N_{\nu-1}}^{(N_\nu)}). \quad (10)$$

Доказательство. В силу теоремы 1 и леммы 4 имеем

$$\begin{aligned} I_{\Delta_\nu} \otimes (A_{n_\nu} \otimes I_{N_\nu}) &= (I_{\Delta_\nu} I_{\Delta_\nu} I_{\Delta_\nu}) \otimes \left(L_{N_{\nu-1}}^{(n_\nu)} (I_{N_\nu} \otimes A_{n_\nu}) L_{N_{\nu-1}}^{(N_\nu)} \right) = \\ &= (I_{\Delta_\nu} \otimes L_{N_{\nu-1}}^{(n_\nu)})(I_{N/n_\nu} \otimes A_{n_\nu})(I_{\Delta_\nu} \otimes L_{N_{\nu-1}}^{(N_\nu)}). \end{aligned}$$

Подставляя это в правую часть (8), приходим к (10). \square

Отметим, что согласно (1)

$$\begin{aligned} I_{\Delta_s} \otimes L_{N_{s-1}}^{(n_s)} &= I_{\Delta_s} \otimes L_{n_s}^{(n_s)} = I_N, \\ I_{\Delta_s} \otimes L_{N_{s-1}}^{(N_s)} &= I_{\Delta_s} \otimes L_{n_s}^{(1)} = I_N. \end{aligned}$$

ТЕОРЕМА 6. *Справедливо разложение*

$$A_{n_1} \otimes A_{n_2} \otimes \cdots \otimes A_{n_s} = \prod_{\nu=1}^s L_N^{(n_\nu)} (I_{N/n_\nu} \otimes A_{n_\nu}).$$

Доказательство. По теореме 1

$$(I_{\Delta_\nu} \otimes A_{n_\nu}) \otimes I_{N_\nu} = L_N^{(\Delta_{\nu+1})} (I_{N/n_\nu} \otimes A_{n_\nu}) L_N^{(N_\nu)}. \quad (11)$$

Теперь два соседних сомножителя из правой части (8) приводятся к виду

$$L_N^{(\Delta_\nu)} (I_{N/n_{\nu-1}} \otimes A_{n_{\nu-1}}) (L_N^{(N_{\nu-1})} L_N^{(\Delta_{\nu+1})}) (I_{N/n_\nu} \otimes A_{n_\nu}) L_N^{(N_\nu)}.$$

Поскольку $N_{\nu-1} \Delta_{\nu+1} = n_\nu N$, то согласно (4) $L_N^{(N_{\nu-1})} L_N^{(\Delta_{\nu+1})} = L_N^{(n_\nu)}$. Заключение теоремы становится очевидным, если учесть, что в правой части (11) при $\nu = 1$ и $\nu = s$ соответственно $L_N^{(\Delta_2)} = L_N^{(n_1)}$ и $L_N^{(N_s)} = L_N^{(1)} = I_N$. \square

ТЕОРЕМА 7. *Справедливо разложение*

$$A_{n_1} \otimes A_{n_2} \otimes \cdots \otimes A_{n_s} = \prod_{\nu=1}^s (A_{n_\nu} \otimes I_{N/n_\nu}) L_N^{(n_\nu)}.$$

Доказательство аналогично предыдущему. Вместо (11) используется формула

$$I_{\Delta_\nu} \otimes (A_{n_\nu} \otimes I_{N_\nu}) = L_N^{(\Delta_\nu)} (A_{n_\nu} \otimes I_{N/n_\nu}) L_N^{(N_{\nu-1})}.$$

ЛИТЕРАТУРА

1. Johnson J., Johnson R. W., Rodriguez D., Tolimieri R. *A methodology for designing, modifying and implementing Fourier transform algorithms on various architectures* // Circuits, Systems and Signal Processing. 1990. V. 9. No. 4. P. 449–500.
2. Воеводин В. В., Кузнецов Ю. А. *Матрицы и вычисления*. М.: Наука, 1984. С. 80–82.

ФАКТОРИЗАЦИЯ КУЛИ-ТЬЮКИ МАТРИЦЫ ФУРЬЕ

В. Н. Малозёмов О. В. Просеков

14 апреля 2004 г.

Доклад представляет собой вариации на темы второй половины обзорной статьи [1].

Будут использоваться следующие обозначения:

$A_n = A_n[0 : n - 1, 0 : n - 1]$ — квадратная матрица порядка n , индексы строк и столбцов которой изменяются от 0 до $n - 1$;

$I_n = I_n[0 : n - 1, 0 : n - 1]$ — единичная матрица порядка n .

1°. Рассмотрим вопрос о факторизации матрицы Фурье F_N с элементами

$$F_N[k, l] = \omega_N^{kl}, \quad k, l \in 0 : N - 1,$$

где $\omega_N = \exp(2\pi i/N)$ — корень N -й степени из единицы. Нам потребуются две специальные матрицы — матрица перестановок $L_{mn}^{(n)}$ и диагональная матрица вращений $T_{mn}^{(m)}$. Они определяются так:

$$L_{mn}^{(n)}[i + j m, i' n + j'] = \begin{cases} 1, & \text{если } i' = i \text{ и } j' = j, \\ 0 & \text{в остальных случаях;} \end{cases}$$
$$T_{mn}^{(m)}[i + j m, i' + j' m] = \begin{cases} \omega_{mn}^{ij}, & \text{если } i' = i \text{ и } j' = j, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Здесь $i, i' \in 0 : m - 1$, $j, j' \in 0 : n - 1$. Из определений следует, что

$$L_n^{(n)} = I_n, \quad L_m^{(1)} = I_m, \quad T_n^{(1)} = I_n. \quad (1)$$

Нетрудно проверить, что

$$(L_{mn}^{(n)})^{-1} = (L_{mn}^{(n)})^T = L_{mn}^{(m)}. \quad (2)$$

ЛЕММА 1. *Справедливо равенство*

$$T_{mn}^{(m)} L_{mn}^{(n)} = L_{mn}^{(n)} T_{mn}^{(m)}. \quad (3)$$

Доказательство. Сравним элементы с индексами $(i + j m, i' n + j')$. Имеем

$$\begin{aligned} \left(T_{mn}^{(m)} L_{mn}^{(n)} \right) [i + j m, i' n + j'] &= \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} T_{mn}^{(m)} [i + j m, i_1 + j_1 m] \times \\ &\times L_{mn}^{(n)} [i_1 + j_1 m, i' n + j'] = \omega_{mn}^{ij} L_{mn}^{(n)} [i + j m, i' n + j'] = \\ &= \begin{cases} \omega_{mn}^{ij}, & \text{если } i' = i \text{ и } j' = j, \\ 0 & \text{в остальных случаях.} \end{cases} \end{aligned}$$

Вместе с тем,

$$\begin{aligned} \left(L_{mn}^{(n)} T_{mn}^{(m)} \right) [i + j m, i' n + j'] &= \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} L_{mn}^{(n)} [i + j m, i_1 n + j_1] \times \\ &\times T_{mn}^{(m)} [i_1 n + j_1, i' n + j'] = \omega_{mn}^{i'j'} L_{mn}^{(n)} [i + j m, i' n + j'] = \\ &= \begin{cases} \omega_{mn}^{ij}, & \text{если } i' = i \text{ и } j' = j, \\ 0 & \text{в остальных случаях.} \end{cases} \end{aligned}$$

Лемма доказана. \square

2°. Матрицу Фурье порядка $N = mn$ можно разложить на множители (факторизовать).

ЛЕММА 2. *Справедлива формула*

$$F_{mn} = (F_m \otimes I_n) T_{mn}^{(n)} (I_m \otimes F_n) L_{mn}^{(m)}. \quad (4)$$

Знак \otimes обозначает кронекерово умножение матриц [2].

Доказательство. В силу (2) достаточно проверить равенство

$$F_{mn} L_{mn}^{(n)} = (F_m \otimes I_n) T_{mn}^{(n)} (I_m \otimes F_n).$$

Сравним элементы с индексами $(i n + j, i' n + j')$. Имеем

$$\begin{aligned} \left(F_{mn} L_{mn}^{(n)} \right) [i n + j, i' n + j'] &= \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} F_{mn} [i n + j, i_1 + j_1 m] \times \\ &\times L_{mn}^{(n)} [i_1 + j_1 m, i' n + j'] = F_{mn} [i n + j, i' + j' m] = \omega_{mn}^{(in+j)(i'+j'm)} = \omega_m^{ii'} \omega_{mn}^{ji'} \omega_n^{jj'}. \end{aligned}$$

Вместе с тем,

$$\begin{aligned} & \left((F_m \otimes I_n) T_{mn}^{(n)} (I_m \otimes F_n) \right) [i \ n + j, i' \ n + j'] = \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} (F_m \otimes I_n) [i \ n + j, i_1 \ n + j_1] \times \\ & \times T_{mn}^{(n)} [i_1 \ n + j_1, i_1 \ n + j_1] \times (I_m \otimes F_n) [i_1 \ n + j_1, i' \ n + j'] = \sum_{i_1=0}^{m-1} \sum_{j_1=0}^{n-1} F_m [i, i_1] \times I_n [j, j_1] \times \\ & \times \omega_{mn}^{i_1 j_1} \times I_m [i_1, i'] \times F_n [j_1, j'] = F_m [i, i'] \omega_{mn}^{j i'} F_n [j, j'] = \omega_m^{i i'} \omega_{mn}^{j i'} \omega_n^{j j'} . \end{aligned}$$

Лемма доказана. \square

Разложение (4) представляет собой наиболее совершенную форму результата, полученного Кули и Тьюки [3].

Лемма 2 допускает обобщение на тот случай, когда порядок N матрицы Фурье является произведением s натуральных чисел, отличных от единицы, т. е. $N = n_1 n_2 \dots n_s$. Обозначим $\Delta_1 = 1$, $\Delta_\nu = n_1 n_2 \dots n_{\nu-1}$ при $\nu = 2, \dots, s+1$; $N_\nu = N/\Delta_{\nu+1}$. Очевидно, что $N_0 = N$, $N_s = 1$ и $N_\nu = n_{\nu+1} \dots n_s$ при $\nu = 1, \dots, s-1$.

ТЕОРЕМА 1. Пусть $N = n_1 n_2 \dots n_s$. Тогда

$$F_N = \left(\prod_{\nu=1}^s \left(I_{\Delta_\nu} \otimes F_{n_\nu} \otimes I_{N_\nu} \right) \left(I_{\Delta_\nu} \otimes T_{N_{\nu-1}}^{(N_\nu)} \right) \right) R_N^T, \quad (5)$$

где

$$R_N = \prod_{\nu=1}^{s-1} \left(I_{\Delta_\nu} \otimes L_{N_{\nu-1}}^{(N_\nu)} \right).$$

Доказательство. При $s = 2$ имеем $N = n_1 n_2$, $N_1 = n_2$, $N_2 = 1$, так что согласно (1) и (2)

$$\begin{aligned} & \left(I_{\Delta_1} \otimes F_{n_1} \otimes I_{N_1} \right) \left(I_{\Delta_1} \otimes T_{N_0}^{(N_1)} \right) = (F_{n_1} \otimes I_{n_2}) T_N^{(n_2)}, \\ & \left(I_{\Delta_2} \otimes F_{n_2} \otimes I_{N_2} \right) \left(I_{\Delta_2} \otimes T_{N_1}^{(N_2)} \right) = I_{n_1} \otimes F_{n_2}, \\ & R_N = I_{\Delta_1} \otimes L_{N_0}^{(N_1)} = L_N^{(n_2)}, \quad R_N^T = L_N^{(n_1)}. \end{aligned}$$

Формула (5) принимает вид

$$F_{n_1 n_2} = (F_{n_1} \otimes I_{n_2}) T_{n_1 n_2}^{(n_2)} (I_{n_1} \otimes F_{n_2}) L_{n_1 n_2}^{(n_1)}.$$

Это соответствует (4) при $m = n_1$, $n = n_2$.

Сделаем индукционный переход от s к $s + 1$. Пусть $N = n_1 \dots n_s n_{s+1}$. На основании (4) запишем

$$F_{n_1(n_2 \dots n_{s+1})} = (F_{n_1} \otimes I_{n_2 \dots n_{s+1}}) T_N^{(n_2 \dots n_{s+1})} (I_{n_1} \otimes F_{n_2 \dots n_{s+1}}) L_N^{(n_1)}.$$

Здесь

$$(F_{n_1} \otimes I_{n_2 \dots n_{s+1}}) T_N^{(n_2 \dots n_{s+1})} = \left(I_{\Delta_1} \otimes F_{n_1} \otimes I_{N_1} \right) \left(I_{\Delta_1} \otimes T_{N_0}^{(N_1)} \right)$$

и в силу индукционного предположения

$$\begin{aligned} I_{n_1} \otimes F_{n_2 \dots n_{s+1}} &= I_{n_1} \otimes \left[\left(\prod_{\nu=2}^{s+1} \left(I_{n_2 \dots n_{\nu-1}} \otimes F_{n_\nu} \otimes I_{n_{\nu+1} \dots n_{s+1}} \right) \times \right. \right. \\ &\quad \left. \left. \times \left(I_{n_2 \dots n_{\nu-1}} \otimes T_{n_\nu \dots n_{s+1}}^{(n_{\nu+1} \dots n_{s+1})} \right) \right) R_{n_2 \dots n_{s+1}}^T \right] = \\ &= \left(\prod_{\nu=2}^{s+1} \left(I_{\Delta_\nu} \otimes F_{n_\nu} \otimes I_{N_\nu} \right) \left(I_{\Delta_\nu} \otimes T_{N_{\nu-1}}^{(N_\nu)} \right) \right) \left(I_{n_1} \otimes R_{n_2 \dots n_{s+1}}^T \right). \end{aligned}$$

Остаётся проверить, что

$$(I_{n_1} \otimes R_{n_2 \dots n_{s+1}}^T) L_N^{(n_1)} = R_{n_1 n_2 \dots n_{s+1}}^T$$

или, после транспонирования¹,

$$L_N^{(N_1)} (I_{n_1} \otimes R_{n_2 \dots n_{s+1}}) = R_{n_1 n_2 \dots n_{s+1}}. \quad (6)$$

Имеем

$$I_{n_1} \otimes R_{n_2 \dots n_{s+1}} = I_{n_1} \otimes \left(\prod_{\nu=2}^s \left(I_{n_2 \dots n_{\nu-1}} \otimes L_{n_\nu \dots n_{s+1}}^{(n_{\nu+1} \dots n_{s+1})} \right) \right) = \prod_{\nu=2}^s \left(I_{\Delta_\nu} \otimes L_{N_{\nu-1}}^{(N_\nu)} \right).$$

К этому нужно добавить, что $L_N^{(N_1)} = I_{\Delta_1} \otimes L_{N_0}^{(N_1)}$. Формула (6), а с ней и теорема, доказаны. \square

3°. Установим, что при $N = n^s$ матрица R_N^T из правой части (5) совпадает с матрицей реверсных перестановок Rev_{n^s} . Напомним определение последней.

Любое число $i \in 0 : n^s - 1$ посредством последовательного деления на n можно единственным образом представить в виде

$$i = i_{s-1} n^{s-1} + i_{s-2} n^{s-2} + \dots + i_0, \quad (7)$$

¹ $(AB)^T = B^T A^T$ и $(A \otimes B)^T = (A^T \otimes B^T)$

где $i_\nu \in 0 : n-1$ при всех $\nu \in 0 : s-1$. Вместо (7) используется более компактная запись $i = (i_{s-1}, i_{s-2}, \dots, i_0)_n$, правая часть которой называется n -ичным кодом числа i . Число с перевёрнутым n -ичным кодом обозначается $\text{rev}_s(i)$. Таким образом, $\text{rev}_s(i) = (i_0, i_1, \dots, i_{s-1})_n$. Матрица реверсных перестановок Rev_{n^s} определяется так:

$$\text{Rev}_{n^s}[i, j] = \begin{cases} 1, & \text{если } j = \text{rev}_s(i), \\ 0 & \text{в остальных случаях.} \end{cases}$$

Здесь $i, j \in 0 : n^s - 1$. При $s = 1$ имеем $\text{Rev}_n = I_n$. Действие матрицы Rev_{n^s} на вектор x приводит к вектору $X = \text{Rev}_{n^s} x$ с компонентами $X(i) = x(\text{rev}_s(i))$, $i \in 0 : n^s - 1$.

ЛЕММА 3. *Справедливо рекуррентное соотношение*

$$\text{Rev}_{n^s} = (I_n \otimes \text{Rev}_{n^{s-1}}) L_{n^s}^{(n)}, \quad s = 2, 3, \dots \quad (8)$$

Доказательство. Обозначим $X = \text{Rev}_{n^s} x$. Тогда

$$X(i + j n^{s-1}) = x(\text{rev}_s(i + j n^{s-1})), \quad i \in 0 : n^{s-1} - 1, \quad j \in 0 : n - 1.$$

Для числа $i + j n^{s-1} = j n^{s-1} + i_{s-2} n^{s-2} + \dots + i_0$ имеем

$$\text{rev}_s(i + j n^{s-1}) = i_0 n^{s-1} + \dots + i_{s-2} n + j = n \text{rev}_{s-1}(i) + j.$$

Значит,

$$X(i + j n^{s-1}) = x(n \text{rev}_{s-1}(i) + j), \quad i \in 0 : n^{s-1} - 1, \quad j \in 0 : n - 1. \quad (9)$$

Обозначим $Y = L_{n^s}^{(n)} x$. Для этого вектора

$$Y(i + j n^{s-1}) = x(i n + j).$$

Найдём компоненты вектора $Z = (I_n \otimes \text{Rev}_{n^{s-1}}) Y$:

$$\begin{aligned} Z(i + j n^{s-1}) &= \sum_{i'=0}^{n^{s-1}-1} \sum_{j'=0}^{n-1} (I_n \otimes \text{Rev}_{n^{s-1}})[i + j n^{s-1}, i' + j' n^{s-1}] \times Y(i' + j' n^{s-1}) = \\ &= \sum_{i'=0}^{n^{s-1}-1} \sum_{j'=0}^{n-1} I_n[j, j'] \times \text{Rev}_{n^{s-1}}[i, i'] \times Y(i' + j' n^{s-1}) = \\ &= Y(\text{rev}_{s-1}(i) + j n^{s-1}) = x(n \text{rev}_{s-1}(i) + j). \end{aligned}$$

Учитывая (9), получаем $Z = X$. Лемма доказана. \square

Из (8) при $s = 2$ следует, что

$$\text{Rev}_{n^2} = L_{n^2}^{(n)}. \quad (10)$$

ЛЕММА 4. *Справедливо разложение*

$$\text{Rev}_{n^s} = \prod_{\nu=1}^{s-1} \left(I_{\Delta_{s-\nu}} \otimes L_{\Delta_{\nu+2}}^{(n)} \right), \quad (11)$$

где $\Delta_\nu = n^{\nu-1}$.

Доказательство. При $s = 2$ формула (11) совпадает с (10). Сделаем индукционный переход от s к $s + 1$. Согласно индукционному предположению (11) и соотношению (8) имеем

$$\begin{aligned} \text{Rev}_{n^{s+1}} &= \left(I_n \otimes \prod_{\nu=1}^{s-1} \left(I_{\Delta_{s-\nu}} \otimes L_{\Delta_{\nu+2}}^{(n)} \right) \right) L_{n^{s+1}}^{(n)} = \\ &= \left(\prod_{\nu=1}^{s-1} \left(I_{\Delta_{s+1-\nu}} \otimes L_{\Delta_{\nu+2}}^{(n)} \right) \right) \left(I_{\Delta_1} \otimes L_{\Delta_{s+2}}^{(n)} \right) = \prod_{\nu=1}^s \left(I_{\Delta_{s+1-\nu}} \otimes L_{\Delta_{\nu+2}}^{(n)} \right). \end{aligned}$$

Лемма доказана. \square

Вернёмся к матрице R_N и отметим, что

$$R_N^T = \prod_{\nu=1}^{s-1} \left(I_{\Delta_{s-\nu}} \otimes L_{N_{s-\nu-1}}^{(n_{s-\nu})} \right). \quad (12)$$

При $N = n^s$ имеем $N_{s-\nu-1} = n^{\nu+1} = \Delta_{\nu+2}$, поэтому правые части формул (11) и (12) совпадают. Значит, $R_N^T = \text{Rev}_{n^s}$.

При $N = n^s$ формула (5) принимает вид

$$F_{n^s} = \left(\prod_{\nu=1}^s \left(I_{\Delta_\nu} \otimes F_n \otimes I_{N_\nu} \right) \left(I_{\Delta_\nu} \otimes T_{N_{\nu-1}}^{(N_\nu)} \right) \right) \text{Rev}_{n^s}, \quad (13)$$

где $\Delta_\nu = n^{\nu-1}$, $N_\nu = N/n^\nu$.

4°. Фундаментальное разложение (13) порождает другие варианты факторизации матрицы Фурье порядка $N = n^s$.

ТЕОРЕМА 2. *Справедлива формула*

$$F_{n^s} = \left(\prod_{\nu=1}^s \left[\left(F_n \otimes I_{N/n} \right) \left(T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu} \right) L_N^{(n)} \right] \right) \text{Rev}_{n^s}. \quad (14)$$

Доказательство. Воспользуемся свойствами операции кронекерова умножения матриц [2]. Запишем

$$I_{\Delta_\nu} \otimes (F_n \otimes I_{N_\nu}) = L_N^{(\Delta_\nu)} (F_n \otimes I_{N/n}) L_N^{(N_{\nu-1})}.$$

Поскольку $L_N^{(N_{\nu-1})} L_N^{(\Delta_\nu)} = I_N$, то

$$\begin{aligned} (I_{\Delta_\nu} \otimes F_n \otimes I_{N_\nu}) (I_{\Delta_\nu} \otimes T_{N_{\nu-1}}^{(N_\nu)}) &= L_N^{(\Delta_\nu)} (F_n \otimes I_{N/n}) L_N^{(N_{\nu-1})} L_N^{(\Delta_\nu)} \times \\ &\times (T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu}) L_N^{(N_{\nu-1})} = L_N^{(\Delta_\nu)} (F_n \otimes I_{N/n}) (T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu}) L_N^{(N_{\nu-1})}. \end{aligned}$$

Обозначим $H_N^{(\nu)} = (F_n \otimes I_{N/n}) (T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu})$. Тогда последнее выражение примет вид $L_N^{(\Delta_\nu)} H_N^{(\nu)} L_N^{(N_{\nu-1})}$.

Преобразуем произведение двух соседних сомножителей в правой части (13). Принимая во внимание, что $L_N^{(N_{\nu-1})} L_N^{(\Delta_{\nu+1})} = L_N^{(n)}$, получаем

$$L_N^{(\Delta_\nu)} H_N^{(\nu)} L_N^{(N_{\nu-1})} L_N^{(\Delta_{\nu+1})} H_N^{(\nu+1)} L_N^{(N_\nu)} = L_N^{(\Delta_\nu)} H_N^{(\nu)} L_N^{(n)} H_N^{(\nu+1)} L_N^{(N_\nu)}.$$

Остаётся учесть, что $L_N^{(\Delta_1)} = L_N^{(1)} = I_N$ и $L_N^{(N_{s-1})} = L_N^{(n)}$. □

С помощью равенства $F_n \otimes I_{N/n} = L_N^{(n)} (I_{N/n} \otimes F_n) L_N^{(N/n)}$ разложение (14) приводится к такому виду:

$$F_{n^s} = \left(\prod_{\nu=1}^s \left[L_N^{(n)} (I_{N/n} \otimes F_n) G_N^{(\nu)} \right] \right) \text{Rev}_{n^s},$$

где $G_N^{(\nu)} = L_N^{(N/n)} (T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu}) L_N^{(n)}$.

Обозначим через $[\alpha]$ целую часть числа α .

ЛЕММА 5. При всех $\nu \in 1 : s$ матрица $G_N^{(\nu)}$ является диагональной. Для её диагональных элементов справедлива формула

$$G_N^{(\nu)}[i + j n, i + j n] = \omega_{N_{\nu-1}}^{i[j/\Delta_\nu]}, \quad i \in 0 : n-1, \quad j \in 0 : n^{s-1} - 1. \quad (15)$$

Доказательство. Воспользуемся тем, что $T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu}$ — диагональная матрица. Получим

$$\begin{aligned} G_N^{(\nu)}[i + j n, i' + j' n] &= \sum_{i_1=0}^{n-1} \sum_{j_1=0}^{N/n-1} L_N^{(N/n)}[i + j n, i_1 N/n + j_1] \times \\ &\times (T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu})[i_1 N/n + j_1, i_1 N/n + j_1] \times L_N^{(n)}[i_1 N/n + j_1, j' n + i'] = \end{aligned}$$

$$\begin{aligned}
&= \left(T_{N_{\nu-1}}^{(N_{\nu})} \otimes I_{\Delta_{\nu}} \right) [i N/n + j, i N/n + j] \times L_N^{(n)} [j + i N/n, j' n + i'] = \\
&= \begin{cases} \left(T_{N_{\nu-1}}^{(N_{\nu})} \otimes I_{\Delta_{\nu}} \right) [i N/n + j, i N/n + j], & \text{если } i' = i \text{ и } j' = j, \\ 0 & \text{в остальных случаях.} \end{cases}
\end{aligned}$$

При $\nu = 1$ имеем

$$G_N^{(1)} [i + j n, i + j n] = T_N^{(N/n)} [i N/n + j, i N/n + j] = \omega_N^{ij},$$

что соответствует (15). Нетрудно понять, что $G_N^{(s)} = I_N$. Это также находится в согласии с (15), поскольку $\lfloor j/\Delta_s \rfloor = 0$ при $j \in 0 : \Delta_s - 1$.

Пусть $\nu \in 2 : s - 1$. Представим индекс $j \in 0 : n^{s-1} - 1$ в виде $j = k_{\nu} \Delta_{\nu} + l_{\nu}$, где $l_{\nu} \in 0 : \Delta_{\nu} - 1$, $k_{\nu} \in 0 : N_{\nu} - 1$. Так как $N_{\nu} \Delta_{\nu} = N/n$, то

$$\begin{aligned}
G_N^{(\nu)} [i + j n, i + j n] &= \left(T_{N_{\nu-1}}^{(N_{\nu})} \otimes I_{\Delta_{\nu}} \right) [(i N_{\nu} + k_{\nu}) \Delta_{\nu} + l_{\nu}, (i N_{\nu} + k_{\nu}) \Delta_{\nu} + l_{\nu}] = \\
&= T_{N_{\nu-1}}^{(N_{\nu})} [i N_{\nu} + k_{\nu}, i N_{\nu} + k_{\nu}] I_{\Delta_{\nu}} [l_{\nu}, l_{\nu}] = \omega_{N_{\nu-1}}^{i k_{\nu}}.
\end{aligned}$$

Остаётся учесть, что $k_{\nu} = \lfloor j/\Delta_{\nu} \rfloor$. Лемма доказана. \square

5°. Вернёмся к формуле Кули-Тьюки (4) и рассмотрим другой вариант её обобщения на случай нескольких сомножителей, отличный от указанного в теореме 1.

ТЕОРЕМА 3. Пусть $N = n_1 n_2 \dots n_s$. Тогда

$$F_N = \prod_{\nu=1}^s \left(F_{n_{\nu}} \otimes I_{N/n_{\nu}} \right) \left(T_{N_{\nu-1}}^{(N_{\nu})} \otimes I_{\Delta_{\nu}} \right) \left(L_{N_{\nu-1}}^{(n_{\nu})} \otimes I_{\Delta_{\nu}} \right). \quad (16)$$

Доказательство. При $s = 2$ имеем $N = n_1 n_2$, $N_1 = n_2$, $N_2 = 1$, так что согласно (1)

$$\begin{aligned}
&\left(F_{n_1} \otimes I_{N/n_1} \right) \left(T_{N_0}^{(N_1)} \otimes I_{\Delta_1} \right) \left(L_{N_0}^{(n_1)} \otimes I_{\Delta_1} \right) = (F_{n_1} \otimes I_{n_2}) T_N^{(n_2)} L_N^{(n_1)}, \\
&\left(F_{n_2} \otimes I_{N/n_2} \right) \left(T_{N_1}^{(N_2)} \otimes I_{\Delta_2} \right) \left(L_{N_1}^{(n_2)} \otimes I_{\Delta_2} \right) = F_{n_2} \otimes I_{n_1} = L_N^{(n_2)} (I_{n_1} \otimes F_{n_2}) L_N^{(n_1)}.
\end{aligned}$$

Формула (16) принимает вид

$$\begin{aligned}
F_{n_1 n_2} &= (F_{n_1} \otimes I_{n_2}) T_{n_1 n_2}^{(n_2)} (L_{n_1 n_2}^{(n_1)} L_{n_1 n_2}^{(n_2)}) (I_{n_1} \otimes F_{n_2}) L_{n_1 n_2}^{(n_1)} = \\
&= (F_{n_1} \otimes I_{n_2}) T_{n_1 n_2}^{(n_2)} (I_{n_1} \otimes F_{n_2}) L_{n_1 n_2}^{(n_1)}.
\end{aligned}$$

Это соответствует (4) при $m = n_1$, $n = n_2$.

Сделаем индукционный переход от s к $s + 1$. Пусть $N = n_1 \dots n_s n_{s+1}$. На основании (4) запишем

$$\begin{aligned} F_{n_1(n_2 \dots n_{s+1})} &= (F_{n_1} \otimes I_{N/n_1}) T_N^{(N_1)} (I_{n_1} \otimes F_{n_2 \dots n_{s+1}}) L_N^{(n_1)} = \\ &= (F_{n_1} \otimes I_{N/n_1}) T_N^{(N_1)} L_N^{(n_1)} (F_{n_2 \dots n_{s+1}} \otimes I_{n_1}). \end{aligned}$$

Здесь

$$(F_{n_1} \otimes I_{N/n_1}) T_N^{(N_1)} L_N^{(n_1)} = (F_{n_1} \otimes I_{N/n_1}) (T_{N_0}^{(N_1)} \otimes I_{\Delta_1}) (L_{N_0}^{(n_1)} \otimes I_{\Delta_1})$$

и в силу индукционного предположения

$$\begin{aligned} F_{n_2 \dots n_{s+1}} \otimes I_{n_1} &= \left(\prod_{\nu=2}^{s+1} (F_{n_\nu} \otimes I_{(n_2 \dots n_{s+1})/n_\nu}) (T_{n_\nu \dots n_{s+1}}^{(n_{\nu+1} \dots n_{s+1})} \otimes I_{n_2 \dots n_{\nu-1}}) \times \right. \\ &\times \left. (L_{n_\nu \dots n_{s+1}}^{(n_\nu)} \otimes I_{n_2 \dots n_{\nu-1}}) \right) \otimes I_{n_1} = \prod_{\nu=2}^{s+1} (F_{n_\nu} \otimes I_{N/n_\nu}) (T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu}) (L_{N_{\nu-1}}^{(n_\nu)} \otimes I_{\Delta_\nu}). \end{aligned}$$

Значит,

$$F_{n_1 n_2 \dots n_{s+1}} = \prod_{\nu=1}^{s+1} (F_{n_\nu} \otimes I_{N/n_\nu}) (T_{N_{\nu-1}}^{(N_\nu)} \otimes I_{\Delta_\nu}) (L_{N_{\nu-1}}^{(n_\nu)} \otimes I_{\Delta_\nu}).$$

Теорема доказана. \square

6°. Сделаем два заключительных замечания.

- 1) При $N = n^s$ множество матриц перестановок $\{L_N^{(n^k)}\}_{k=0}^{s-1}$ образует циклическую группу по умножению. Это связано со свойством [2]

$$L_{rmn}^{(m)} L_{rmn}^{(n)} = L_{rmn}^{(mn)}. \quad (17)$$

Согласно (17), $L_{n^s}^{(n^k)} L_{n^s}^{(n)} = L_{n^s}^{(n^{k+1})}$ при $k \in 1 : s - 1$. К тому же в силу (1) $L_{n^s}^{(1)} = I_{n^s}$ и $L_{n^s}^{(n^s)} = I_{n^s}$.

- 2) Матрица реверсных перестановок Rev_{n^s} симметрична. Действительно,

$$(\text{Rev}_{n^s})^T[i, j] = \text{Rev}_{n^s}[j, i] = \begin{cases} 1, & \text{если } i = \text{rev}_s(j), \\ 0 & \text{в остальных случаях.} \end{cases}$$

Поскольку $\text{rev}_s(\text{rev}_s(j)) = j$, то условие $i = \text{rev}_s(j)$ равносильно условию $j = \text{rev}_s(i)$. Поэтому

$$(\text{Rev}_{n^s})^T[i, j] = \begin{cases} 1, & \text{если } j = \text{rev}_s(i), \\ 0 & \text{в остальных случаях} \end{cases} = \text{Rev}_{n^s}[i, j].$$

Для симметричной матрицы перестановок Rev_{n^s} справедливо равенство

$$\text{Rev}_{n^s} \text{Rev}_{n^s} = I_{n^s}.$$

ЛИТЕРАТУРА

1. Johnson J., Johnson R. W., Rodriguez D., Tolimieri R. *A methodology for designing, modifying and implementing Fourier transform algorithms on various architectures* // Circuits, Systems and Signal Processing. 1990. V. 9. No. 4. P. 449–500.
2. Малозёмов В. Н., Просеков О. В. *Перестановки и кронекерово произведение матриц* // Семинар «DHA & CAGD». Избранные доклады. 31 марта 2004 г. (<http://www.dha.spb.ru/rep04.shtml#0331>).
3. Cooley J. W., Tukey J. W. *An algorithm for the machine calculation of complex Fourier series* // Math. Comput. 1965. V. 19. No. 90. P. 297–301.
4. Temperton C. *Self-sorting mixed-radix Fast Fourier Transform* // J. Comput. Phys. 1983. V. 52. No. 1. P. 1–23.
5. Белый А. А., Бовбель Е. И., Микулович В. И. *Алгоритмы быстрого преобразования Фурье и их свойства* // Зарубежная радиоэлектроника. 1979. № 2. С. 3–29.

ФАКТОРИЗАЦИЯ ГУДА МАТРИЦЫ ФУРЬЕ

В. Н. Малозёмов О. В. Просеков

5 мая 2004 г.

Доклад примыкает к двум предыдущим докладам тех же авторов. Излагается на современном уровне метод простых множителей Гуда.

С современных позиций рассматривается вопрос о факторизации матрицы Фурье, порядок которой равен произведению попарно взаимно простых чисел [1]. Используется обозначение

$$\langle k \rangle_n = k - \lfloor k/n \rfloor n, \quad k \in \mathbb{Z}.$$

1°. Пусть m, n — взаимно простые натуральные числа. Введём две квадратные матрицы порядка mn :

$$Q_{mn}^{(n)}[k, k_1 n + k_2] = \begin{cases} 1, & \text{если } k_1 = \langle k \rangle_m \text{ и } k_2 = \langle k \rangle_n, \\ 0 & \text{в остальных случаях;} \end{cases}$$

$$P_{mn}^{(n)}[l, l_1 n + l_2] = \begin{cases} 1, & \text{если } l = \langle l_1 n + l_2 m \rangle_{mn}, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Здесь $k, l \in 0 : mn - 1$, $k_1, l_1 \in 0 : m - 1$, $k_2, l_2 \in 0 : n - 1$. Матрица $Q_{mn}^{(n)}$ заполняется по строкам, а матрица $P_{mn}^{(n)}$ — по столбцам. Например, при $m = 2$, $n = 3$ имеем

$$Q_6^{(3)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad P_6^{(3)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

Данные для построения этих матриц приведены в таблицах 1 и 2 соответственно.

k	$k_1 = \langle k \rangle_2$	$k_2 = \langle k \rangle_3$	$3k_1 + k_2$
0	0	0	0
1	1	1	4
2	0	2	2
3	1	0	3
4	0	1	1
5	1	2	5

Таблица 1

l_1	l_2	$3l_1 + l_2$	$l = \langle 3l_1 + 2l_2 \rangle_6$
0	0	0	0
0	1	1	2
0	2	2	4
1	0	3	3
1	1	4	5
1	2	5	1

Таблица 2

Отметим, что

$$Q_n^{(n)} = P_n^{(n)} = I_n, \quad Q_m^{(1)} = P_m^{(1)} = I_m. \quad (1)$$

ЛЕММА. При взаимно простых m и n матрицы $Q_{mn}^{(n)}$ и $P_{mn}^{(n)}$ являются матрицами перестановок.

Доказательство. Сначала разберёмся с $Q_{mn}^{(n)}$. По построению в каждой строке этой матрицы лишь один элемент отличен от нуля (равен единице). Остаётся проверить, что если для индексов строк $k, k' \in 0 : mn - 1$ выполняется равенство

$$\langle k \rangle_m n + \langle k \rangle_n = \langle k' \rangle_m n + \langle k' \rangle_n, \quad (2)$$

то $k = k'$. Из (2) следует, что

$$\langle k - k' \rangle_m = \langle \langle k \rangle_m - \langle k' \rangle_m \rangle_m = 0, \quad \langle k - k' \rangle_n = \langle \langle k \rangle_n - \langle k' \rangle_n \rangle_n = 0,$$

т. е. $k - k'$ делится как на m , так и на n . По условию m и n взаимно просты, поэтому $k - k'$ делится на произведение mn . Поскольку к тому же $|k - k'| \leq mn - 1$, то необходимо $k = k'$.

Обратимся к матрице $P_{mn}^{(n)}$. По построению в каждом столбце этой матрицы лишь один элемент отличен от нуля (равен единице). Остаётся показать, что если для индексов столбцов $l_1 n + l_2$ и $l'_1 n + l'_2$ с $l_1, l'_1 \in 0 : m - 1$, $l_2, l'_2 \in 0 : n - 1$ выполняется равенство

$$\langle l_1 n + l_2 \rangle_{mn} = \langle l'_1 n + l'_2 \rangle_{mn}, \quad (3)$$

то $l_1 = l'_1$ и $l_2 = l'_2$. Из (3) следует, что

$$(l_1 - l'_1) n + (l_2 - l'_2) m = q mn \quad (4)$$

при некотором целом q . Взяв вычеты по модулю m , получим $\langle (l_1 - l'_1) n \rangle_m = 0$. По условию n и m взаимно просты, поэтому $l_1 - l'_1$ делится на m . Поскольку к тому же $|l_1 - l'_1| \leq m - 1$, то необходимо $l_1 = l'_1$. Аналогично с помощью (4) и вычетов по модулю n устанавливается, что $l_2 = l'_2$. Лемма доказана. \square

СЛЕДСТВИЕ. *Справедливы равенства*

$$(Q_{mn}^{(n)})^{-1} = (Q_{mn}^{(n)})^T, \quad (P_{mn}^{(n)})^{-1} = (P_{mn}^{(n)})^T. \quad (5)$$

2°. По-прежнему считаем, что m и n взаимно простые числа. Введём матрицу Фурье F_N с элементами

$$F_N[k, l] = \omega_N^{kl}, \quad k, l \in 0 : N - 1,$$

где $\omega_N = \exp(2\pi i/N)$.

ТЕОРЕМА 1. *При $N = mn$ имеет место разложение*

$$F_N = Q_{mn}^{(n)}(F_m \otimes F_n)(P_{mn}^{(n)})^T. \quad (6)$$

Символ \otimes обозначает кронекерово умножение матриц [2].

Доказательство. В силу (5) достаточно проверить, что

$$F_N P_{mn}^{(n)} = Q_{mn}^{(n)}(F_m \otimes F_n). \quad (7)$$

Сравним элементы с индексами $(k, l_1 n + l_2)$, $k \in 0 : N - 1$, $l_1 \in 0 : m - 1$, $l_2 \in 0 : n - 1$, матриц, стоящих в левой и правой частях равенства (7). Запишем

$$\begin{aligned} (F_N P_{mn}^{(n)})[k, l_1 n + l_2] &= \sum_{l=0}^{N-1} F_N[k, l] \times P_{mn}^{(n)}[l, l_1 n + l_2] = \\ &= F_{mn}[k, \langle l_1 n + l_2 m \rangle_{mn}] = \omega_m^{kl_1} \omega_n^{kl_2}. \end{aligned}$$

Вместе с тем,

$$\begin{aligned} (Q_{mn}^{(n)}(F_m \otimes F_n))[k, l_1 n + l_2] &= \sum_{k_1=0}^{m-1} \sum_{k_2=0}^{n-1} Q_{mn}^{(n)}[k, k_1 n + k_2] \times \\ &\times (F_m \otimes F_n)[k_1 n + k_2, l_1 n + l_2] = (F_m \otimes F_n)[\langle k \rangle_m n + \langle k \rangle_n, l_1 n + l_2] = \\ &= F_m[\langle k \rangle_m, l_1] F_n[\langle k \rangle_n, l_2] = \omega_m^{kl_1} \omega_n^{kl_2}. \end{aligned}$$

Равенство (7), а с ним и теорема, доказаны. \square

В силу симметричности матрицы Фурье формулу (6) можно переписать в эквивалентном виде

$$F_N = P_{mn}^{(n)}(F_m \otimes F_n)(Q_{mn}^{(n)})^T.$$

3°. Теорема 1 допускает обобщение на случай, когда порядок N матрицы Фурье является произведением нескольких попарно взаимно простых чисел, т. е. $N = n_1 n_2 \dots n_s$, $\text{НОД}(n_k, n_j) = 1$ при $k \neq j$.

Обозначим $\Delta_1 = 1$, $\Delta_\nu = n_1 n_2 \dots n_{\nu-1}$ при $\nu = 2, \dots, s+1$; $N_\nu = N/\Delta_{\nu+1}$. Очевидно, что $N_0 = N$, $N_s = 1$ и $N_\nu = n_{\nu+1} \dots n_s$ при $\nu = 1, \dots, s-1$.

ТЕОРЕМА 2. Пусть N равно произведению попарно взаимно простых чисел n_1, n_2, \dots, n_s , отличных от единицы. Тогда

$$F_N = Q_N (F_{n_1} \otimes F_{n_2} \otimes \dots \otimes F_{n_s}) P_N^T, \quad (8)$$

где

$$Q_N = \prod_{\nu=1}^{s-1} (I_{\Delta_\nu} \otimes Q_{N_{\nu-1}}^{(N_\nu)}), \quad P_N = \prod_{\nu=1}^{s-1} (I_{\Delta_\nu} \otimes P_{N_{\nu-1}}^{(N_\nu)}).$$

Доказательство. При $s = 2$, когда $N = n_1 n_2$, $N_1 = n_2$, формула (8) соответствует (6) при $m = n_1$, $n = n_2$. Сделаем индукционный переход от s к $s+1$.

Возьмём $N = n_1 \dots n_s n_{s+1}$ с попарно взаимно простыми сомножителями n_ν . Взаимно простыми будут n_1 и произведение $n_2 \dots n_{s+1}$. Согласно (6), индукционному предположению и свойствам кронекерова умножения имеем

$$\begin{aligned} F_{n_1(n_2 \dots n_{s+1})} &= Q_N^{(N_1)} (F_{n_1} \otimes F_{n_2 \dots n_{s+1}}) (P_N^{(N_1)})^T = \\ &= Q_N^{(N_1)} \left\{ F_{n_1} \otimes \left[\left(\prod_{\nu=2}^s (I_{n_2 \dots n_{\nu-1}} \otimes Q_{n_\nu \dots n_{s+1}}^{(n_{\nu+1} \dots n_{s+1})}) \right) (F_{n_2} \otimes \dots \otimes F_{n_{s+1}}) \right] \right. \\ &\quad \times \left. \left(\prod_{\nu=2}^s (I_{n_2 \dots n_{\nu-1}} \otimes P_{n_\nu \dots n_{s+1}}^{(n_{\nu+1} \dots n_{s+1})}) \right)^T \right\} (P_N^{(N_1)})^T = \\ &= Q_N^{(N_1)} \left(\prod_{\nu=2}^s (I_{\Delta_\nu} \otimes Q_{N_{\nu-1}}^{(N_\nu)}) \right) (F_{n_1} \otimes F_{n_2} \otimes \dots \otimes F_{n_{s+1}}) \times \\ &\quad \times \left(\prod_{\nu=2}^s (I_{\Delta_\nu} \otimes P_{N_{\nu-1}}^{(N_\nu)}) \right)^T (P_N^{(N_1)})^T. \end{aligned}$$

Остаётся учесть, что

$$Q_N^{(N_1)} = I_{\Delta_1} \otimes Q_{N_0}^{(N_1)}, \quad P_N^{(N_1)} = I_{\Delta_1} \otimes P_{N_0}^{(N_1)}.$$

Теорема доказана. □

По поводу различных вариантов факторизации кронекерова произведения $F_{n_1} \otimes F_{n_2} \otimes \dots \otimes F_{n_s}$ см. [2]

ЛИТЕРАТУРА

1. Гуд И. Дж. *О взаимоотношении между двумя быстрыми преобразованиями Фурье* / В кн.: Макклеллан Дж. Х., Рейдер Ч. М. *Применение теории чисел в цифровой обработке сигналов*. М.: Радио и связь, 1983. С. 136–147.
2. Малозёмов В. Н., Просеков О. В. *Перестановки и кронекерово произведение матриц* // Семинар «DHA & CAGD». Избранные доклады. 31 марта 2004 г. (<http://www.dha.spb.ru/rep04.shtml#0331>).

ПАРАМЕТРИЧЕСКОЕ КОДИРОВАНИЕ ИНДЕКСОВ

В. Н. Малозёмов

19 мая 2004 г.

В параметрическом множестве кодов индексов рассматриваются пары сопряжённых кодов. В частности, сопряжёнными являются руританский и китайский коды. Вводится понятие самосопряжённых кодов и устанавливается критерий их существования.

1°. Пусть $N = n_1 n_2 \dots n_s$, где n_α — попарно взаимно простые натуральные числа, отличные от единицы. Обозначим $N_\alpha = N/n_\alpha$. При каждом $\alpha \in 1 : s$ возьмём натуральное число $p_\alpha \in 1 : n_\alpha - 1$, взаимно простое с n_α .

ПРЕДЛОЖЕНИЕ 1. *Формула*

$$j = \left\langle \sum_{\alpha=1}^s j_\alpha p_\alpha N_\alpha \right\rangle_N \quad (1)$$

устанавливает взаимно однозначное соответствие между наборами коэффициентов (j_1, j_2, \dots, j_s) с $j_\alpha \in 0 : n_\alpha - 1$ и числами $j \in 0 : N - 1$.

Доказательство. Поскольку мощности множества векторов (j_1, j_2, \dots, j_s) с $j_\alpha \in 0 : n_\alpha - 1$ и множества чисел $j \in 0 : N - 1$ равны, то достаточно проверить, что разные векторы (j_1, j_2, \dots, j_s) порождают разные j . Допустив, что $(j_1, j_2, \dots, j_s) \rightarrow j$, $(j'_1, j'_2, \dots, j'_s) \rightarrow j$, получим

$$\sum_{\alpha=1}^s (j_\alpha - j'_\alpha) p_\alpha N_\alpha = r N$$

при некотором целом r . Отсюда следует, что при всех $\alpha \in 1 : s$

$$\langle (j_\alpha - j'_\alpha) p_\alpha N_\alpha \rangle_{n_\alpha} = 0.$$

Поскольку произведение $p_\alpha N_\alpha$ взаимно просто с n_α , то $j_\alpha - j'_\alpha$ делится на n_α , а так как $|j_\alpha - j'_\alpha| \leq n_\alpha - 1$, то необходимо $j_\alpha = j'_\alpha$ при всех $\alpha \in 1 : s$.

Теперь ясно, что разные наборы коэффициентов (j_1, j_2, \dots, j_s) порождают разные j . Предложение доказано. \square

2°. Перепишем (1) в виде

$$\sum_{\alpha=1}^s j_{\alpha} p_{\alpha} N_{\alpha} = r N + j.$$

Как следствие, получаем $\langle j_{\alpha} p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = \langle j \rangle_{n_{\alpha}}$ при всех $\alpha \in 1 : s$. Отсюда можно вывести явную формулу для j_{α} . Действительно, по условию числа $p_{\alpha} N_{\alpha}$ и n_{α} взаимно просты. Это гарантирует, что уравнение $\langle x p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = 1$ имеет на множестве $1 : n_{\alpha} - 1$ единственное решение $x = q_{\alpha}$ [1]. Более того, q_{α} взаимно просто с n_{α} .

Покажем, что

$$j_{\alpha} = \langle j q_{\alpha} \rangle_{n_{\alpha}}, \quad \alpha \in 1 : s. \quad (2)$$

Для этого достаточно проверить, что правая часть (2) удовлетворяет уравнению $\langle x p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = \langle j \rangle_{n_{\alpha}}$. Имеем

$$\langle \langle j q_{\alpha} \rangle_{n_{\alpha}} p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = \langle j \langle q_{\alpha} p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} \rangle_{n_{\alpha}} = \langle j \rangle_{n_{\alpha}}.$$

Формула (2) установлена.

Формулу (1) можно воспринимать как разложение индекса $j \in 0 : N - 1$ по базису $\{p_{\alpha} N_{\alpha}\}_{\alpha=1}^s$, в котором коэффициенты j_{α} вычисляются по формуле (2).

Обозначим $p = (p_1, p_2, \dots, p_s)$ и запишем (1) в компактном виде

$$j = (j_1, j_2, \dots, j_s)_p. \quad (3)$$

Правую часть (3) будем называть *p-кодом индекса j*.

3°. Как отмечалось, q_{α} взаимно просто с n_{α} при всех $\alpha \in 1 : s$. Это даёт возможность записать представление

$$j = (j_1^*, j_2^*, \dots, j_s^*)_q, \quad (4)$$

где $q = (q_1, q_2, \dots, q_s)$. Для вычисления коэффициента j_{α}^* нужно решить уравнение $\langle x q_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = 1$. Очевидно, что единственным на множестве $1 : n_{\alpha} - 1$ решением этого уравнения является $x = p_{\alpha}$. Отсюда следует, что

$$j_{\alpha}^* = \langle j p_{\alpha} \rangle_{n_{\alpha}}, \quad \alpha \in 1 : s.$$

Коды (3), (4) индекса $j \in 0 : N - 1$ назовём *сопряжёнными*. Если $p = q$, то эти коды совпадают. В таком случае код $j = (j_1, j_2, \dots, j_s)_p$ с $j_{\alpha} = \langle j p_{\alpha} \rangle_{n_{\alpha}}$ при $\alpha \in 1 : s$ назовём *самосопряжённым*.

4°. При $p_1 = p_2 = \dots = p_s = 1$, т. е. при $p = (1, 1, \dots, 1)$, p -код индекса j называется *руританским* [2]. Вернёмся к подробной записи формулы (3) для руританского кода:

$$j = \left\langle \sum_{\alpha=1}^s j_{\alpha} N_{\alpha} \right\rangle_N. \quad (5)$$

Здесь $j_{\alpha} = \langle j q_{\alpha} \rangle_{n_{\alpha}}$, причём q_{α} — единственное на множестве $1 : n_{\alpha} - 1$ решение уравнения $\langle x N_{\alpha} \rangle_{n_{\alpha}} = 1$.

Сопряжённый к руританскому код называется *китайским*. Он порождает представление

$$j = \left\langle \sum_{\alpha=1}^s j_{\alpha}^* q_{\alpha} N_{\alpha} \right\rangle_N \quad (6)$$

с $j_{\alpha}^* = \langle j \rangle_{n_{\alpha}}$.

ПРИМЕР 1. Пусть $s = 2$, $n_1 = 4$, $n_2 = 25$, так что $N = 100$, $N_1 = 25$, $N_2 = 4$. Вычислим $q_1 \in 1 : 3$ и $q_2 \in 1 : 24$. Для этого нужно решить уравнения $\langle 25 x \rangle_4 = 1$ и $\langle 4 x \rangle_{25} = 1$. Очевидно, что $q_1 = 1$, $q_2 = 19$. Согласно (5) любое число $j \in 0 : 99$ допускает руританское представление

$$j = \langle 25 j_1 + 4 j_2 \rangle_{100},$$

где $j_1 = \langle j \rangle_4$, $j_2 = \langle 19 j \rangle_{25}$. (Проверьте это на $j = 13$.)

Китайское представление числа $j \in 0 : 99$ определяется формулой (6):

$$j = \langle 25 j_1^* + 76 j_2^* \rangle_{100},$$

где $j_1^* = \langle j \rangle_4$, $j_2^* = \langle j \rangle_{25}$. (Проверьте это на $j = 31$.)

5°. Обратимся к самосопряжённым кодам. Напомним, что взаимно простые с n_{α} числа p_{α} , q_{α} принадлежат множеству $1 : n_{\alpha} - 1$ и связаны соотношением $\langle q_{\alpha} p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = 1$. Выполнение условия $p_{\alpha} = q_{\alpha}$ можно обеспечить, решив уравнение

$$\langle x^2 N_{\alpha} \rangle_{n_{\alpha}} = 1. \quad (7)$$

Обозначим через b_{α} единственное на множестве $1 : n_{\alpha} - 1$ решение уравнения $\langle x N_{\alpha} \rangle_{n_{\alpha}} = 1$.

ПРЕДЛОЖЕНИЕ 2. Уравнение (7) равносильно уравнению

$$\langle x^2 \rangle_{n_{\alpha}} = b_{\alpha}. \quad (8)$$

Доказательство. Пусть $\langle x_0^2 N_\alpha \rangle_{n_\alpha} = 1$. Тогда

$$\langle x_0^2 \rangle_{n_\alpha} = \langle x_0^2 \langle b_\alpha N_\alpha \rangle_{n_\alpha} \rangle_{n_\alpha} = \langle \langle x_0^2 N_\alpha \rangle_{n_\alpha} b_\alpha \rangle_{n_\alpha} = \langle b_\alpha \rangle_{n_\alpha} = b_\alpha.$$

Наоборот, если $\langle x_0^2 \rangle_{n_\alpha} = b_\alpha$, то

$$\langle x_0^2 N_\alpha \rangle_{n_\alpha} = \langle \langle x_0^2 \rangle_{n_\alpha} N_\alpha \rangle_{n_\alpha} = \langle b_\alpha N_\alpha \rangle_{n_\alpha} = 1.$$

Предложение доказано. \square

В случае, когда уравнение (8) имеет решение, говорят, что b_α является *квадратичным вычетом по модулю n_α* [3]. Уравнение (8) не всегда имеет решение. Например, не существует целых x , удовлетворяющих уравнению $\langle x^2 \rangle_5 = 2$. В то же время уравнение $\langle x^2 \rangle_5 = 4$ имеет на множестве $1 : 4$ два решения $x = 2$ и $x = 3$.

Предположим, что уравнение (8) имеет решение $x = p_\alpha$ на множестве $1 : n_\alpha$ при всех $\alpha \in 1 : s$. Обозначим $p = (p_1, p_2, \dots, p_s)$. Тогда p -код числа $j \in 0 : N-1$ является самосопряжённым, т. е. $j = (j_1, j_2, \dots, j_s)_p$, где $j_\alpha = \langle j p_\alpha \rangle_{n_\alpha}$.

ПРИМЕР 2. Сохраним данные примера 1: $n_1 = 4$, $n_2 = 25$. Покажем, что в этом случае существует четыре самосопряжённых кода.

Решив уравнения $\langle 25x \rangle_4 = 1$, $\langle 4x \rangle_{25} = 1$, найдём $b_1 = 1$, $b_2 = 19$. Перейдём к уравнениям

$$\langle x^2 \rangle_4 = 1, \quad \langle x^2 \rangle_{25} = 19.$$

Первое из них имеет два решения $p_1 = 1$ и $p_1 = 3$. Столько же решений имеет и второе уравнение: $p_2 = 12$, $p_2 = 13$. Комбинируя значения p_1 и p_2 , получаем четыре самосопряжённых кода для чисел $j \in 0 : 99$:

1) $p_1 = 1$, $p_2 = 12$;

$$j = \langle 25j_1 + 48j_2 \rangle_{100}, \quad j_1 = \langle j \rangle_4, \quad j_2 = \langle 12j \rangle_{25}.$$

2) $p_1 = 1$, $p_2 = 13$;

$$j = \langle 25j_1 + 52j_2 \rangle_{100}, \quad j_1 = \langle j \rangle_4, \quad j_2 = \langle 13j \rangle_{25}.$$

3) $p_1 = 3$, $p_2 = 12$;

$$j = \langle 75j_1 + 48j_2 \rangle_{100}, \quad j_1 = \langle 3j \rangle_4, \quad j_2 = \langle 12j \rangle_{25}.$$

4) $p_1 = 3$, $p_2 = 13$;

$$j = \langle 75j_1 + 52j_2 \rangle_{100}, \quad j_1 = \langle 3j \rangle_4, \quad j_2 = \langle 13j \rangle_{25}.$$

6°. Отметим одно замечательное свойство китайского кода (6).

ПРЕДЛОЖЕНИЕ 3. Пусть числа $k, j \in 0 : N - 1$ имеют китайские коды

$$k = (k_1^*, k_2^*, \dots, k_s^*)_q, \quad j = (j_1^*, j_2^*, \dots, j_s^*)_q,$$

где $k_\alpha^* = \langle k \rangle_{n_\alpha}$, $j_\alpha^* = \langle j \rangle_{n_\alpha}$. Тогда

$$\langle k + j \rangle_N = (\langle k_1^* + j_1^* \rangle_{n_1}, \dots, \langle k_s^* + j_s^* \rangle_{n_s})_q,$$

$$\langle k j \rangle_N = (\langle k_1^* j_1^* \rangle_{n_1}, \dots, \langle k_s^* j_s^* \rangle_{n_s})_q.$$

Доказательство. Запишем

$$(\langle k + j \rangle_N)_\alpha^* = \langle \langle k + j \rangle_N \rangle_{n_\alpha} = \langle k + j \rangle_{n_\alpha} = \langle \langle k \rangle_{n_\alpha} + \langle j \rangle_{n_\alpha} \rangle_{n_\alpha} = \langle k_\alpha^* + j_\alpha^* \rangle_{n_\alpha}.$$

Аналогично

$$(\langle k j \rangle_N)_\alpha^* = \langle \langle k j \rangle_N \rangle_{n_\alpha} = \langle k j \rangle_{n_\alpha} = \langle \langle k \rangle_{n_\alpha} \langle j \rangle_{n_\alpha} \rangle_{n_\alpha} = \langle k_\alpha^* j_\alpha^* \rangle_{n_\alpha}.$$

Предложение доказано. \square

7°. Сопряжённые коды применяются в методе простых множителей быстрого вычисления дискретного преобразования Фурье [2]. Точнее, используется следующее свойство комплексного числа $\omega_N = \exp(2\pi i/N)$, являющегося корнем N -й степени из единицы.

ПРЕДЛОЖЕНИЕ 4. Пусть $k, j \in 0 : N - 1$, причём известны p -код числа j и сопряжённый код числа k :

$$j = (j_1, j_2, \dots, j_s)_p, \quad k = (k_1^*, k_2^*, \dots, k_s^*)_q,$$

где $j_\alpha = \langle j q_\alpha \rangle_{n_\alpha}$, $k_\alpha^* = \langle k p_\alpha \rangle_{n_\alpha}$. Тогда

$$\omega_N^{kj} = \prod_{\alpha=1}^s \omega_{n_\alpha}^{k_\alpha^* j_\alpha}. \quad (9)$$

Доказательство. Поскольку $\langle q_\alpha p_\alpha N_\alpha \rangle_{n_\alpha} = 1$, то

$$\begin{aligned} \omega_N^{kj} &= \omega_N^{\left(\sum_{\alpha=1}^s k_\alpha^* q_\alpha N_\alpha\right) \left(\sum_{\alpha=1}^s j_\alpha p_\alpha N_\alpha\right)} = \omega_N^{\sum_{\alpha=1}^s k_\alpha^* j_\alpha q_\alpha p_\alpha N_\alpha^2} = \\ &= \prod_{\alpha=1}^s \omega_{n_\alpha}^{k_\alpha^* j_\alpha \langle q_\alpha p_\alpha N_\alpha \rangle_{n_\alpha}} = \prod_{\alpha=1}^s \omega_{n_\alpha}^{k_\alpha^* j_\alpha}. \end{aligned}$$

Предложение доказано. \square

СЛЕДСТВИЕ. В случае самосопряжённых кодов

$$k = (k_1, k_2, \dots, k_s)_p, \quad j = (j_1, j_2, \dots, j_s)_p$$

с $k_\alpha = \langle k p_\alpha \rangle_{n_\alpha}$, $j_\alpha = \langle j p_\alpha \rangle_{n_\alpha}$ формула (9) принимает вид

$$\omega_N^{kj} = \prod_{\alpha=1}^s \omega_{n_\alpha}^{k_\alpha j_\alpha}.$$

8°. Вопросы кодирования индексов рассматривались также в работах [4, 5].

ЛИТЕРАТУРА

1. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. СПб.: НИИММ, 2003. Часть первая. Предварительные сведения.
2. Гуд И. Дж. *О взаимоотношении между двумя быстрыми преобразованиями Фурье*. В кн.: Макклеллан Дж. Х., Рейдер Ч. М. *Применение теории чисел в цифровой обработке сигналов*. М.: Радио и связь, 1983.
3. Виноградов И. М. *Основы теории чисел*. Изд. седьмое. М.: Наука, 1965. Глава пятая.
4. Burrus C. S. *Index mappings for multidimensional formulation of the DFT and convolution* // IEEE Trans. Acoust., Speech, Signal Processing. 1977. Vol. ASSP-25. No. 3. P. 239–242.
5. Свердлик М. Б. *Матричная интерпретация алгоритма БПФ для взаимно простых сомножителей* // Радиотехника и электроника. 1983. № 10. С. 1931–1938.

О СПЕКТРЕ ФУРЬЕ ФУНКЦИЙ УОЛША

В. Н. Малозёмов

23 июня 2004 г.

Выводятся явные формулы для спектра Фурье функций Радемахера. Устанавливаются некоторые общие соотношения для спектра Фурье функций Уолша.

1°. Пусть $N = 2^s$. Для чисел $k, j \in 0 : N - 1$ с двоичными кодами $k = (k_{s-1}, k_{s-2}, \dots, k_0)_2$, $j = (j_{s-1}, j_{s-2}, \dots, j_0)_2$ положим

$$\{k, j\}_s = \sum_{\alpha=0}^{s-1} k_{\alpha} j_{\alpha}.$$

Дискретные функции Уолша v_k определяются формулой

$$v_k(j) = (-1)^{\{k, j\}_s}, \quad k, j \in 0 : N - 1.$$

Спектром Фурье функции v_k называется функция V_k со значениями

$$V_k(j) = \sum_{l=0}^{N-1} v_k(l) \omega_N^{-lj}, \quad j \in 0 : N - 1,$$

где $\omega_N = \exp(2\pi i/N)$. Займёмся вычислением спектров V_k .

2°. Очевидно, что $v_0(j) \equiv 1$; $v_1(j) = (-1)^{j_0} = (-1)^j$, $j \in 0 : N - 1$. Спектры Фурье этих функций вычисляются легко:

$$\begin{aligned} V_0(j) &= \sum_{l=0}^{N-1} \omega_N^{-lj} = N \delta_N(j), \\ V_1(j) &= \sum_{l=0}^{N-1} (-1)^l \omega_N^{-lj} = \sum_{l=0}^{N-1} \omega_2^l \omega_N^{-lj} = \sum_{l=0}^{N-1} \omega_N^{-l(j-N/2)} = N \delta_N(j - N/2). \end{aligned}$$

Отметим, что $V_1(j) = V_0(j - N/2)$.

Обозначим $N_{\nu} = N/2^{\nu}$, $\Delta_{\nu} = 2^{\nu-1}$ и введём функции Радемахера r_{ν} :

$$r_{\nu}(j) = v_{N_{\nu}}(j), \quad \nu \in 1 : s.$$

ТЕОРЕМА 1. Для спектра Фурье R_ν функции Радемахера r_ν справедливо представление

$$R_\nu(j) = \begin{cases} 2^\nu \left(1 - i \operatorname{ctg} \frac{(2p+1)\pi}{N_{\nu-1}} \right) & \text{при } j = (2p+1)\Delta_\nu, p \in 0 : N_\nu - 1; \\ 0 & \text{при остальных } j \in 0 : N - 1. \end{cases} \quad (1)$$

Доказательство. Воспользуемся тем, что

$$r_\nu(j) = (-1)^{j_{s-\nu}} = (-1)^{\lfloor j/N_\nu \rfloor}, \quad j \in 0 : N - 1.$$

Запишем

$$R_\nu(j) = \sum_{l=0}^{N-1} (-1)^{\lfloor l/N_\nu \rfloor} \omega_N^{-lj}.$$

Положим $l = k N_\nu + q$, $q \in 0 : N_\nu - 1$, $k \in 0 : \Delta_{\nu+1} - 1$. Тогда $\lfloor l/N_\nu \rfloor = k$ и

$$\begin{aligned} R_\nu(j) &= \sum_{k=0}^{\Delta_{\nu+1}-1} (-1)^k \sum_{q=0}^{N_\nu-1} \omega_N^{-(k N_\nu + q)j} = \sum_{k=0}^{\Delta_{\nu+1}-1} (-1)^k \omega_{\Delta_{\nu+1}}^{-kj} \sum_{q=0}^{N_\nu-1} \omega_N^{-qj} = \\ &= \sum_{k=0}^{\Delta_{\nu+1}-1} \omega_{\Delta_{\nu+1}}^{-k(j-\Delta_\nu)} \sum_{q=0}^{N_\nu-1} \omega_N^{-qj} = 2^\nu \delta_{\Delta_{\nu+1}}(j - \Delta_\nu) \sum_{q=0}^{N_\nu-1} \omega_N^{-qj}. \end{aligned}$$

Ясно, что функция $R_\nu(j)$ отлична от нуля только при $j = \Delta_\nu + p \Delta_{\nu+1} = (2p+1)\Delta_\nu$, $p \in 0 : N_\nu - 1$. При указанных j имеем

$$\begin{aligned} R_\nu(j) &= 2^\nu \sum_{q=0}^{N_\nu-1} \omega_N^{-q(2p+1)\Delta_\nu} = 2^\nu \sum_{q=0}^{N_\nu-1} \omega_{N_{\nu-1}}^{-q(2p+1)} = \\ &= 2^\nu \frac{1 - \omega_{N_{\nu-1}}^{-N_\nu(2p+1)}}{1 - \omega_{N_{\nu-1}}^{-(2p+1)}} = 2^\nu \left(1 - i \operatorname{ctg} \frac{(2p+1)\pi}{N_{\nu-1}} \right). \end{aligned}$$

Теорема доказана. □

Формулу (1) можно переписать в виде

$$V_{N_\nu}(j) = \begin{cases} 2^\nu \left(1 - i \operatorname{ctg} \frac{\pi j}{N} \right) & \text{при } j = (2p+1)\Delta_\nu, p \in 0 : N_\nu - 1; \\ 0 & \text{при остальных } j \in 0 : N - 1. \end{cases} \quad (2)$$

Отсюда, в частности, следует, что спектр $V_{N_\nu}(j)$ имеет ровно N_ν ненулевых компонент.

3°. Вычислим V_2 и V_3 . Поскольку $V_2 = V_{N_{s-1}}$, то $V_2(j)$ имеет только два ненулевых значения при $j = N/4$ и $j = 3N/4$. При этом согласно (2)

$$\begin{aligned} V_2(N/4) &= N_1 \left(1 - i \operatorname{ctg} \frac{\pi}{4} \right) = N_1 (1 - i), \\ V_2(3N/4) &= N_1 \left(1 - i \operatorname{ctg} \frac{3\pi}{4} \right) = N_1 (1 + i). \end{aligned}$$

Функция Уолша $v_3(j)$ допускает представление

$$v_3(j) = (-1)^{j_1+j_0} = (-1)^{\lfloor j/2 \rfloor + j}, \quad j \in 0 : N-1,$$

так что

$$V_3(j) = \sum_{l=0}^{N-1} (-1)^{\lfloor l/2 \rfloor + l} \omega_N^{-lj}.$$

Положим $l = 2k + q$, $q \in 0 : 1$, $k \in 0 : N_1 - 1$. Тогда $\lfloor l/2 \rfloor + l = 3k + q$ и

$$\begin{aligned} V_3(j) &= \sum_{q=0}^1 (-1)^q \sum_{k=0}^{N_1-1} (-1)^k \omega_N^{-(2k+q)j} = \sum_{q=0}^1 (-1)^q \omega_N^{-qj} \sum_{k=0}^{N_1-1} (-1)^k \omega_N^{-kj} = \\ &= N_1 (1 - \omega_N^{-j}) \delta_{N_1}(j - N_2). \end{aligned}$$

Ясно, что функция $V_3(j)$ отлична от нуля только при $j = N_2 = N/4$ и $j = N_2 + N_1 = 3N/4$. При этом

$$\begin{aligned} V_3(N/4) &= N_1 (1 - \omega_4^{-1}) = N_1 (1 + i), \\ V_3(3N/4) &= N_1 (1 - \omega_4^{-3}) = N_1 (1 - i). \end{aligned}$$

Отметим, что $V_3(j) = V_2(j - N_1)$. Имеется в виду, что как функции Уолша $v_k(j)$, так и их спектры $V_k(j)$ продолжены с периодом N на все $j \in \mathbb{Z}$.

4°. Как известно,

$$v_k(j) v_{k'}(j) = v_{k \oplus k'}(j), \quad j \in 0 : N-1, \quad (3)$$

где символ \oplus обозначает поразрядное сложение двоичных кодов по модулю два. Поскольку $2k + 1 = 2k \oplus 1$, то

$$v_{2k+1}(j) = v_{2k}(j) v_1(j), \quad j \in 0 : N-1. \quad (4)$$

ТЕОРЕМА 2. *Справедлива формула*

$$V_{2k+1}(j) = V_{2k}(j - N_1), \quad j \in \mathbb{Z}.$$

Доказательство. Воспользуемся соотношением

$$\mathcal{F}_N(xy) = N^{-1}(X * Y).$$

Согласно (4), $V_{2k+1} = N^{-1}(V_{2k} * V_1)$. Так как $V_1(j) = N \delta_N(j - N_1)$, то

$$V_{2k+1}(j) = \frac{1}{N} \sum_{l=0}^{N-1} V_{2k}(l) V_1(j-l) = \sum_{l=0}^{N-1} V_{2k}(l) \delta_N((j - N_1) - l) = V_{2k}(j - N_1).$$

Теорема доказана. \square

5°. Функции Уолша с основным периодом $0 : N_1 - 1$ будем обозначать $v_k^{(1)}$. Таким образом,

$$v_k^{(1)}(j) = (-1)^{\{k,j\}_{s-1}}, \quad k, j \in 0 : N_1 - 1.$$

Выведем рекуррентное соотношение, связывающее спектры V_k и $V_k^{(1)}$.

ЛЕММА. При $k, j \in 0 : N_1 - 1$ справедливы формулы

$$\begin{aligned} v_k(j) &= v_k^{(1)}(j), & v_k(N_1 + j) &= v_k^{(1)}(j), \\ v_{N_1+k}(j) &= v_k^{(1)}(j), & v_{N_1+k}(N_1 + j) &= -v_k^{(1)}(j). \end{aligned} \quad (5)$$

Для доказательства нужно вспомнить, что числа $v_k(0), v_k(1), \dots, v_k(N-1)$ образуют строку матрицы Адамара A_s с индексом k и воспользоваться рекуррентным соотношением [1, с. 54]

$$A_s = \begin{bmatrix} A_{s-1} & A_{s-1} \\ A_{s-1} & -A_{s-1} \end{bmatrix}.$$

ТЕОРЕМА 3. При $k, p \in 0 : N_1 - 1$ справедливы формулы

$$V_k(2p) = 2 V_k^{(1)}(p), \quad V_k(2p+1) = 0, \quad (6)$$

$$V_{N_1+k}(2p) = 0, \quad V_{N_1+k}(2p+1) = \frac{1}{N_1} \sum_{j=0}^{N_1-1} V_k^{(1)}(j) h(p-j), \quad (7)$$

где

$$h(j) = 2 \left(1 - i \operatorname{ctg} \frac{\pi(2j+1)}{N} \right).$$

Доказательство. При $k \in 0 : N_1 - 1$ согласно (5) имеем

$$\begin{aligned} V_k(j) &= \sum_{l=0}^{N_1-1} v_k(l) \omega_N^{-lj} + \sum_{l=N_1}^{N-1} v_k(l) \omega_N^{-lj} = \sum_{l=0}^{N_1-1} v_k^{(1)}(l) \omega_N^{-lj} + \\ &+ \sum_{l=0}^{N_1-1} v_k^{(1)}(l) \omega_N^{-(N_1+l)j} = (1 + (-1)^j) \sum_{l=0}^{N_1-1} v_k^{(1)}(l) \omega_N^{-lj}. \end{aligned}$$

Отсюда непосредственно следует (6).

Теперь рассмотрим функции Уолша v_{N_1+k} при $k \in 0 : N_1 - 1$. Так как $N_1 + k = N_1 \oplus k$, то согласно (3)

$$V_{N_1+k} = N^{-1}(V_k * V_{N_1}). \quad (8)$$

При этом в силу (2)

$$V_{N_1}(j) = \begin{cases} 2 \left(1 - i \operatorname{ctg} \frac{\pi j}{N}\right) & \text{при нечётных } j, \\ 0 & \text{при чётных } j. \end{cases}$$

Распишем формулу (8) подробнее:

$$V_{N_1+k}(2p) = \frac{1}{N} \sum_{l=0}^{N_1-1} V_k(2l+1) V_{N_1}(2(p-l)-1) + \frac{1}{N} \sum_{l=0}^{N_1-1} V_k(2l) V_{N_1}(2(p-l)). \quad (9)$$

Обе суммы в правой части этого соотношения равны нулю. Первая — за счёт $V_k(2l+1)$, вторая — за счёт $V_{N_1}(2(p-l))$. Таким образом, $V_{N_1+k}(2p) = 0$ при $p \in 0 : N_1 - 1$. Далее, аналогично (9) с использованием (6) получаем

$$V_{N_1+k}(2p+1) = \frac{1}{N_1} \sum_{l=0}^{N_1-1} V_k^{(1)}(l) V_{N_1}(2(p-l)+1).$$

Остаётся учесть, что $V_{N_1}(2j+1) = h(j)$. Формула (7), а вместе с ней и теорема доказаны. \square

6°. Приведём ещё один результат общего характера.

ТЕОРЕМА 4. Пусть $N \geq 8$ и $k \in 0 : N_2 - 1$. Тогда

$$V_{3N_2+k}(j) = i^j V_{N_1+k}(j), \quad j \in 0 : N - 1.$$

Доказательство. Зафиксируем $k = (k_{s-3}, \dots, k_0)_2$ и запишем

$$\begin{aligned} 3N_2 + k &= N_1 + N_2 + k = (1, 1, k_{s-3}, \dots, k_0)_2, \\ N_1 + k &= (1, 0, k_{s-3}, \dots, k_0)_2. \end{aligned}$$

Покажем, что

$$v_{3N_2+k}(j) = v_{N_1+k}(\langle j + N_2 \rangle_N), \quad j \in 0 : N-1. \quad (10)$$

Возьмём $j = (j_{s-1}, j_{s-2}, \dots, j_0)_2$. Если $j_{s-2} = 0$, т. е. $j = (j_{s-1}, 0, j_{s-3}, \dots, j_0)_2$, то $\langle j + N_2 \rangle_N = (j_{s-1}, 1, j_{s-3}, \dots, j_0)_2$. Получаем

$$\{3N_2 + k, j\}_s = \{N_1 + k, \langle j + N_2 \rangle_N\}_s = j_{s-1} + \sum_{\alpha=0}^{s-3} k_\alpha j_\alpha.$$

Это гарантирует справедливость (10).

Пусть $j_{s-2} = 1$, т. е. $j = (j_{s-1}, 1, j_{s-3}, \dots, j_0)_2$. Тогда

$$\langle j + N_2 \rangle_N = (\langle j_{s-1} + 1 \rangle_2, 0, j_{s-3}, \dots, j_0)_2.$$

Имеем

$$\begin{aligned} \{3N_2 + k, j\}_s &= j_{s-1} + 1 + \sum_{\alpha=0}^{s-3} k_\alpha j_\alpha, \\ \{N_1 + k, \langle j + N_2 \rangle_N\}_s &= \langle j_{s-1} + 1 \rangle_2 + \sum_{\alpha=0}^{s-3} k_\alpha j_\alpha. \end{aligned}$$

Поскольку

$$(-1)^{\langle j_{s-1} + 1 \rangle_2} = (-1)^{j_{s-1} + 1},$$

то и в этом случае выполняется равенство (10).

Обратимся к спектрам Фурье. В силу N -периодичности функций Уолша и (10) получим

$$\begin{aligned} V_{3N_2+k}(j) &= \sum_{l=0}^{N-1} v_{N_1+k}(l + N_2) \omega_N^{-lj} = \sum_{l=0}^{N-1} v_{N_1+k}(l) \omega_N^{-(l-N_2)j} = \\ &= \omega_4^j V_{N_1+k}(j) = i^j V_{N_1+k}(j). \end{aligned}$$

Теорема доказана. \square

Дальнейшие сведения о спектре Фурье функций Уолша имеются в [2, 3, 4].

ЛИТЕРАТУРА

1. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Часть вторая. СПб.: НИИММ, 2003. 100 с.
2. Львович А. А., Кузьмин Б. Д. Аналитическое выражение для спектров функций Уолша // Радиотехника. 1980. Т. 35. № 1. С. 33–39.
3. Зеленков А. В. Быстрое преобразование спектра сигнала из базиса Уолша в базис дискретных экспоненциальных функций // Радиотехника и электроника. 1977. Т. 27. № 3. С. 552–565.
4. Пойда В. Н. *Спектральный анализ в дискретных ортогональных базисах*. Минск: Наука и техника, 1978. 136 с.

РЯДЫ ФУРЬЕ И ДПФ

В. Н. Малозёмов

7 декабря 2004 г.

Рассмотрим непрерывную 1-периодическую функцию $f(x)$. Предположим, что она разлагается в ряд Фурье

$$f(x) = \sum_{p=-\infty}^{\infty} a_p \exp(2\pi i p x). \quad (1)$$

Здесь

$$a_p = \int_0^1 f(x) \exp(-2\pi i p x) dx. \quad (2)$$

Будем считать, что

$$\sum_{p=-\infty}^{\infty} |a_p| < \infty. \quad (3)$$

На отрезке $[0, 1]$ введём сетку $x_j = j/N$, $j \in 0 : N - 1$. В узлах x_j имеем

$$f_j := f(x_j) = \sum_{p=-\infty}^{\infty} a_p \omega_N^{pj}, \quad \omega_N = \exp(2\pi i/N).$$

Представив p в виде $p = sN + k$, $k \in 0 : N - 1$, $s \in \mathbb{Z}$, преобразуем последнюю формулу:

$$f_j = \sum_{k=0}^{N-1} \sum_{s=-\infty}^{\infty} a_{k+sN} \omega_N^{(k+sN)j} = \sum_{k=0}^{N-1} \omega_N^{kj} \sum_{s=-\infty}^{\infty} a_{k+sN}.$$

Обозначим

$$A_k^{(N)} = \sum_{s=-\infty}^{\infty} a_{k+sN}. \quad (4)$$

Тогда

$$f_j = \sum_{k=0}^{N-1} A_k^{(N)} \omega_N^{kj}, \quad j \in 0 : N - 1. \quad (5)$$

Из (5) следует, что

$$A_k^{(N)} = \frac{1}{N} \sum_{j=0}^{N-1} f_j \omega_N^{-kj} = \frac{1}{N} \sum_{j=0}^{N-1} f(x_j) \exp(-2\pi i k x_j). \quad (6)$$

Правая часть (6) является квадратурной суммой для интеграла из правой части (2) при $p = k$. Значит, $A_k^{(N)} \rightarrow a_k$ при $N \rightarrow \infty$ и всех $k \in \mathbb{Z}$. Приближённое равенство $A_k^{(N)} \approx a_k$ тем более точно, чем более гладкой будет функция $f(x)$. Этот факт находится в полном согласии с формулами (4) и (3).

Введём индексное множество $I_N = \{k \in \mathbb{Z} \mid -N/2 < k \leq N/2\}$. Очевидно, что $I_N = -n+1 : n$ при $N = 2n$ и $I_N = -n+1 : n-1$ при $N = 2n-1$. В обоих случаях $|I_N| = N$. Поскольку последовательность $\{A_k^{(N)}\}$ N -периодична, то равенство (5) можно переписать в виде

$$f(x_j) = \sum_{k \in I_N} A_k^{(N)} \exp(2\pi i k x_j), \quad (7)$$

где в силу (6)

$$A_k^{(N)} = \frac{1}{N} \sum_{j=0}^{N-1} f_j \omega_N^{-kj}.$$

Рассмотрим тригонометрический полином

$$T_N(x) = \sum_{k \in I_N} A_k^{(N)} \exp(2\pi i k x).$$

Согласно (7), $T_N(x_j) = f(x_j)$, т. е. $T_N(x)$ интерполирует $f(x)$ в узлах x_j . Анализ приближённой формулы

$$f(x) \approx T_N(x), \quad x \in [0, 1], \quad (8)$$

связан с разложением (1). Поскольку

$$\max_{x \in [0, 1]} |f(x) - T_N(x)| \leq \sum_{k \in I_N} |A_k^{(N)} - a_k| + \sum_{k \notin I_N} |a_k|,$$

то точность формулы (8) зависит от того, насколько точны соотношения $A_k^{(N)} \approx a_k$ при $k \in I_N$ и $a_k \approx 0$ при $k \notin I_N$.

При выборе N нужно учитывать скорость изменения функции $f(x)$. Вычисление коэффициентов $A_k^{(N)}$ основано на использовании быстрого преобразования Фурье.

Доклад является вариацией на тему из [1, с. 166–170].

ЛИТЕРАТУРА

1. Бахвалов Н. С., Жидков Н. П., Кобельков Г. М. *Численные методы*. М.: Наука, 1987. 600 с.

РЕКУРРЕНТНЫЙ ВАРИАНТ МЕТОДА НАИМЕНЬШИХ КВАДРАТОВ

В. Н. Малозёмов С. В. Рыбин

7 декабря 2004 г.

1°. Пусть A_i — $(r_i \times n)$ -матрицы, $i = 1, \dots, m$. Обозначим

$$g_i(x) = b_i - A_i x$$

и рассмотрим при фиксированном $\lambda \in (0, 1]$ последовательность экстремальных задач

$$Q_k(x) := \sum_{i=1}^k \lambda^{k-i} \|g_i(x)\|^2 \rightarrow \min, \quad k = 1, \dots, m. \quad (1)$$

При $\lambda = 1$ и $k = m$ имеем стандартную блочную задачу о наименьших квадратах.

Приведем квадратичную функцию $Q_k(x)$ к каноническому виду. Запишем

$$\begin{aligned} Q_k(x) &= \sum_{i=1}^k \lambda^{k-i} \langle b_i - A_i x, b_i - A_i x \rangle = \\ &= \sum_{i=1}^k \lambda^{k-i} \|b_i\|^2 - 2 \left\langle \sum_{i=1}^k \lambda^{k-i} A_i^T b_i, x \right\rangle + \left\langle \left(\sum_{i=1}^k \lambda^{k-i} A_i^T A_i \right) x, x \right\rangle. \end{aligned}$$

Обозначим

$$H_k = \sum_{i=1}^k \lambda^{k-i} A_i^T A_i.$$

Тогда

$$Q_k(x) = \langle H_k x, x \rangle - 2 \left\langle \sum_{i=1}^k \lambda^{k-i} A_i^T b_i, x \right\rangle + \sum_{i=1}^k \lambda^{k-i} \|b_i\|^2.$$

Отметим, что

$$H_k = \lambda H_{k-1} + A_k^T A_k, \quad k = 1, \dots, m; \quad H_0 = \mathbf{0}. \quad (2)$$

В силу определения матрица H_k симметрична и неотрицательно определена. Если она имеет обратную, то решением задачи (1) при фиксированном k является вектор

$$\Psi_k = H_k^{-1} \left(\sum_{i=1}^k \lambda^{k-i} A_i^T b_i \right). \quad (3)$$

ТЕОРЕМА. *Предположим, что матрица $A_1^T A_1$ положительно определена. Тогда векторы Ψ_k могут быть вычислены рекуррентно:*

$$\begin{aligned} \Psi_k &= \Psi_{k-1} + H_k^{-1} A_k^T (b_k - A_k \Psi_{k-1}), \quad k = 1, \dots, m; \\ \Psi_0 &\text{ — произвольный вектор.} \end{aligned} \quad (4)$$

Доказательство. Так как матрица $A_1^T A_1$ положительно определена, то все матрицы H_1, \dots, H_m также положительно определены и, в частности, обратимы.

При $k = 1$ формула (4) проверяется непосредственно:

$$H_1 = A_1^T A_1, \quad \Psi_1 = H_1^{-1} A_1^T b_1 = \Psi_0 + H_1^{-1} A_1^T (b_1 - A_1 \Psi_0).$$

Пусть $k \geq 2$. Согласно (3)

$$\lambda H_{k-1} \Psi_{k-1} = \sum_{i=1}^{k-1} \lambda^{k-i} A_i^T b_i = H_k \Psi_k - A_k^T b_k.$$

Учитывая (2), получаем

$$\begin{aligned} H_k \Psi_k &= \lambda H_{k-1} \Psi_{k-1} + A_k^T b_k = (H_k - A_k^T A_k) \Psi_{k-1} + A_k^T b_k = \\ &= H_k \Psi_{k-1} + A_k^T (b_k - A_k \Psi_{k-1}). \end{aligned}$$

Остается обе части последнего равенства умножить на H_k^{-1} . □

2°. Матрицы H_k пересчитываются по формуле (2). Выведем формулу для пересчета H_k^{-1} .

ЛЕММА (Шерман-Моррисон-Вудбери). *Пусть*

$$D = H + A^T A,$$

где A — $(r \times n)$ -матрица. Если матрица H симметрична и положительно определена, то

$$D^{-1} = H^{-1} - H^{-1} A^T P^{-1} A H^{-1}, \quad (5)$$

где $P = I_r + A H^{-1} A^T$, I_r — единичная $(r \times r)$ -матрица.

Доказательство. Ясно, что матрицы D и P положительно определены и потому имеют обратные. Покажем, что

$$(H + A^T A)(H^{-1} - H^{-1} A^T P^{-1} A H^{-1}) = I_n.$$

Преобразуем левую часть:

$$\begin{aligned} I_n + A^T A H^{-1} - A^T P^{-1} A H^{-1} - A^T (A H^{-1} A^T) P^{-1} A H^{-1} = \\ = I_n + A^T A H^{-1} - A^T P^{-1} A H^{-1} - A^T (P - I_r) P^{-1} A H^{-1} = I_n. \end{aligned}$$

Лемма доказана. □

Из (2) и (5) следует, что

$$H_k^{-1} = \lambda^{-1} H_{k-1}^{-1} - \lambda^{-2} H_{k-1}^{-1} A_k^T P_k^{-1} A_k H_{k-1}^{-1}, \quad (6)$$

где $P_k = I_{r_k} + \lambda^{-1} A_k H_{k-1}^{-1} A_k^T$.

При $r_k = 1$ матрица A_k становится вектором-строкой. В этом случае формула (6) принимает более простой вид:

$$H_k^{-1} = \lambda^{-1} H_{k-1}^{-1} - \lambda^{-2} \alpha_k^{-1} (H_{k-1}^{-1} A_k^T) (H_{k-1}^{-1} A_k^T)^T,$$

где $\alpha_k = 1 + \lambda^{-1} \langle A_k, H_{k-1}^{-1} A_k^T \rangle$.

3°. Указанная теорема вместе с леммой используются в алгоритме последовательной регрессии при адаптивной обработке сигналов [1, с.139-145]. По поводу леммы Шермана-Моррисона-Вудбери см.[2]

ЛИТЕРАТУРА

1. Уидроу Б., Стирнз С. *Адаптивная обработка сигналов*. М.: Радио и связь, 1989. 440с.
2. Малозёмов В. Н., Монако М. Ф., Петров А. В. *Формулы Фробениуса, Шермана-Моррисона и близкие вопросы* // Журн. вычисл. мат. и матем. физики. 2002. Т. 42. No. 10. С. 1459–1465.

ПОЛИНОМЫ БЕРНШТЕЙНА И СОСТАВНЫЕ КРИВЫЕ БЕЗЬЕ

М. И. Григорьев В. Н. Малозёмов А. Н. Сергеев

14 декабря 2004 г.

1°. При натуральном n алгебраический полином

$$B(x) = \sum_{k=0}^n y_k C_n^k x^k (1-x)^{n-k} \quad (1)$$

называется *полиномом в форме Бернштейна* или просто *полиномом Бернштейна* [1]. Очевидно, что

$$B(0) = y_0, \quad B(1) = y_n. \quad (2)$$

Базисные полиномы $p_{nk}(x) = C_n^k x^k (1-x)^{n-k}$ обладают следующими свойствами:

$$p_{nk}(x) > 0 \quad \text{при } x \in (0, 1) \text{ и всех } k = 0, 1, \dots, n; \quad (3)$$

$$\sum_{k=0}^n p_{nk}(x) \equiv 1. \quad (4)$$

ЛЕММА 1. При всех вещественных x справедливо равенство

$$\frac{1}{n} \sum_{k=1}^n k p_{nk}(x) = x. \quad (5)$$

Доказательство. Равенство (5) достаточно проверить при $x \in (0, 1)$. Имеем

$$(\ln p_{nk}(x))' = \frac{k}{x} - \frac{n-k}{1-x} = \frac{n}{x(1-x)} \left(\frac{k}{n} - x \right).$$

Вместе с тем, $(\ln p_{nk}(x))' = p'_{nk}(x)/p_{nk}(x)$. Значит,

$$p'_{nk}(x) = \frac{n}{x(1-x)} \left(\frac{k}{n} - x \right) p_{nk}(x).$$

Теперь продифференцируем тождество (4). Получим

$$\frac{n}{x(1-x)} \sum_{k=0}^n \left(\frac{k}{n} - x \right) p_{nk}(x) \equiv 0.$$

Отсюда и из (4) следует (5). \square

Обозначим $y_k^{(0)} = y_k$, $k \in 0 : n$.

ТЕОРЕМА 1. *Справедлива формула*

$$B(x) = \sum_{k=0}^{n-1} y_k^{(1)} p_{n-1,k}(x), \quad (6)$$

где $y_k^{(1)} = (1-x)y_k^{(0)} + xy_{k+1}^{(0)}$.

Доказательство. Имеем

$$\begin{aligned} \sum_{k=0}^{n-1} y_k^{(1)} C_{n-1}^k x^k (1-x)^{n-1-k} &= \sum_{k=0}^{n-1} y_k^{(0)} C_{n-1}^k x^k (1-x)^{n-k} + \\ &+ \sum_{k=1}^n y_k^{(0)} C_{n-1}^{k-1} x^k (1-x)^{n-k} = y_0^{(0)} (1-x)^n + y_n^{(0)} x^n + \\ &+ \sum_{k=1}^{n-1} y_k^{(0)} (C_{n-1}^k + C_{n-1}^{k-1}) x^k (1-x)^{n-k} = \sum_{k=0}^n y_k C_n^k x^k (1-x)^{n-k}. \end{aligned}$$

Мы воспользовались тем, что $C_{n-1}^k + C_{n-1}^{k-1} = C_n^k$ при $k \in 1 : n-1$. \square

Преобразование (6) можно продолжить:

$$B(x) = \sum_{k=0}^{n-2} y_k^{(2)} p_{n-2,k}(x),$$

где $y_k^{(2)} = (1-x)y_k^{(1)} + xy_{k+1}^{(1)}$, и т. д. В результате получим

$$B(x) = \sum_{k=0}^1 y_k^{(n-1)} p_{1k}(x) = (1-x)y_0^{(n-1)} + xy_1^{(n-1)} =: y_0^{(n)}.$$

Таким образом, выведено рекуррентное соотношение

$$\begin{aligned} y_k^{(i)} &= (1-x)y_k^{(i-1)} + xy_{k+1}^{(i-1)}, \quad i = 1, \dots, n, \quad k = 0, 1, \dots, n-i; \\ y_k^{(0)} &= y_k, \quad k = 0, 1, \dots, n, \end{aligned} \quad (7)$$

которое позволяет вычислить значение $B(x) = y_0^{(n)}$ в фиксированной точке $x \in (0, 1)$.

2°. Перепишем формулу (1) в виде

$$B(x) = \sum_{k=0}^n p_{nk}(x) y_k.$$

С учетом свойств (3) и (4) коэффициентов $p_{nk}(x)$ заключаем, что число $B(x)$ при фиксированном $x \in (0, 1)$ есть выпуклая комбинация чисел y_0, y_1, \dots, y_n . Рекуррентное соотношение (7) представляет собой быстрый способ вычисления этой выпуклой комбинации.

Введём векторный полином Бернштейна

$$\mathcal{B}(x) = \sum_{k=0}^n p_{nk}(x) Y_k, \quad (8)$$

где $Y_k = (y_{k1}, \dots, y_{ks})$. Согласно (2)

$$\mathcal{B}(0) = Y_0, \quad \mathcal{B}(1) = Y_n.$$

Рекуррентное соотношение

$$\begin{aligned} Y_k^{(i)} &= (1-x) Y_k^{(i-1)} + x Y_{k+1}^{(i-1)}, \quad i = 1, \dots, n, \quad k = 0, 1, \dots, n-i; \\ Y_k^{(0)} &= Y_k, \quad k = 0, 1, \dots, n, \end{aligned} \quad (9)$$

позволяет вычислить вектор $\mathcal{B}(x) = Y_0^{(n)}$ при фиксированном $x \in (0, 1)$ как выпуклую комбинацию векторов Y_0, Y_1, \dots, Y_n . Когда параметр x пробегает весь отрезок $[0, 1]$, вектор $\mathcal{B}(x)$ описывает кривую в пространстве \mathbb{R}^s , соединяющую точки Y_0 и Y_n . Такая кривая называется *кривой Безье* [2]. По существу, кривая Безье определяется соотношением (9).

Рассмотрим частный случай: $s = 2$, $Y_k = (k/n, y_k)$, $k \in 0 : n$. На основании (8) и (5) получим $\mathcal{B}(x) = (x, B(x))$, $x \in [0, 1]$. Схема (9) позволяет построить график полинома Бернштейна (рис. 1). Отметим, что абсцисса точки $Y_k^{(i)}$ в данном случае равна $\frac{ix + k}{n}$.

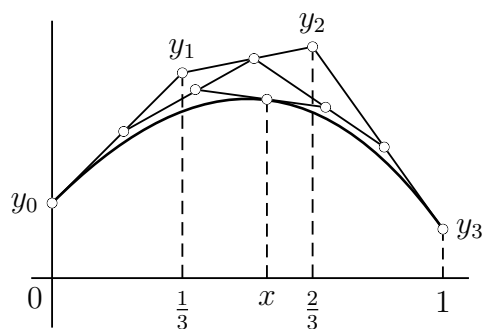


Рис. 1. График полинома Бернштейна при $n = 3$

Точки $Y_k = (y_{k1}, y_{k2})$, $k \in 0 : n$, порождают произвольную кривую Безье на плоскости (рис. 2), а точки $Y_k = (y_{k1}, y_{k2}, y_{k3})$, $k \in 0 : n$, — пространственную кривую Безье.

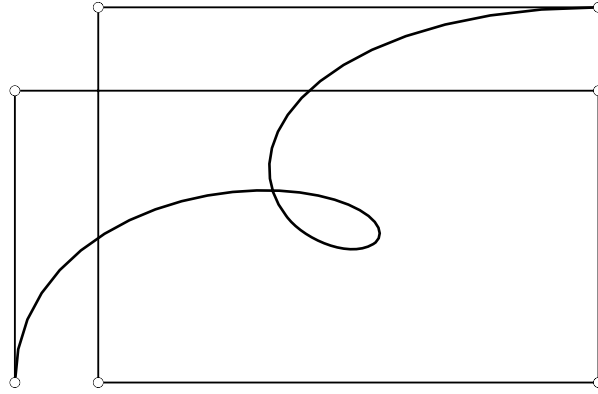


Рис. 2. Кривая Безье на плоскости

3°. Рассмотрим простейший вариант задачи о построении гладких составных кривых Безье. Предварительно установим еще одно свойство полиномов Бернштейна.

ЛЕММА 2. *Полином Бернштейна (1) допускает представление*

$$B(x) = \sum_{i=0}^n (\Delta^i y_0) C_n^i x^i, \quad (10)$$

где $\Delta^i y_0 = \sum_{k=0}^i (-1)^{i-k} C_i^k y_k$ — нисходящая конечная разность i -го порядка.

Доказательство. Имеем

$$\begin{aligned} B(x) &= \sum_{k=0}^n y_k C_n^k \sum_{i=0}^{n-k} C_{n-k}^i (-1)^{n-k-i} x^{n-i} = \\ &= \sum_{i=0}^n \sum_{k=0}^{n-i} y_k C_n^k C_{n-k}^i (-1)^{n-k-i} x^{n-i}. \end{aligned}$$

Поскольку $C_n^k C_{n-k}^i = C_n^i C_{n-i}^k$, то

$$B(x) = \sum_{i=0}^n C_n^i \left(\sum_{k=0}^{n-i} (-1)^{n-i-k} C_{n-i}^k y_k \right) x^{n-i} =$$

$$= \sum_{i=0}^n C_n^{m-i} (\Delta^{n-i} y_0) x^{n-i} = \sum_{i=0}^n C_n^i (\Delta^i y_0) x^i.$$

Лемма доказана. \square

Полином (1) соответствует отрезку $[0, 1]$. Запишем полином Бернштейна степени m , соответствующий отрезку $[-1, 0]$:

$$\begin{aligned} Q(x) &= \sum_{k=0}^m y_{-m+k} C_m^k (1+x)^k (-x)^{m-k} = \\ &= \sum_{k=0}^m (-1)^k y_{-k} C_m^k x^k (1+x)^{m-k}. \end{aligned} \quad (11)$$

ЛЕММА 3. Полином $Q(x)$ допускает представление

$$Q(x) = \sum_{i=0}^m (\nabla^i y_0) C_m^i x^i, \quad (12)$$

где $\nabla^i y_0 = \sum_{k=0}^i (-1)^k C_i^k y_{-k}$ — восходящая конечная разность i -го порядка.

Доказательство. Имеем

$$\begin{aligned} Q(x) &= \sum_{k=0}^m (-1)^k y_{-k} C_m^k \sum_{i=0}^{m-k} C_{m-k}^i x^{m-i} = \\ &= \sum_{i=0}^m \sum_{k=0}^{m-i} (-1)^k y_{-k} C_m^k C_{m-k}^i x^{m-i} = \\ &= \sum_{i=0}^m C_m^i \left(\sum_{k=0}^{m-i} (-1)^k C_{m-i}^k y_{-k} \right) x^{m-i} = \\ &= \sum_{i=0}^m C_m^{m-i} (\nabla^{m-i} y_0) x^{m-i} = \sum_{i=0}^m C_m^i (\nabla^i y_0) x^i. \end{aligned}$$

Лемма доказана. \square

По поводу вычисления конечных разностей $\Delta^i y_0$ и $\nabla^i y_0$ см. [3, с. 55-64].

Введём составную функцию

$$S(x) = \begin{cases} Q(x) & \text{при } x \in [-1, 0], \\ B(x) & \text{при } x \in [0, 1]. \end{cases}$$

ТЕОРЕМА 2. Функция $S(x)$ будет r раз непрерывно дифференцируемой на отрезке $[-1, 1]$ тогда и только тогда, когда выполняется условие

$$C_m^i \nabla^i y_0 = C_n^i \Delta^i y_0 \quad \text{при } i = 1, \dots, r. \quad (13)$$

При $m = n$ условие (13) принимает вид

$$\nabla^i y_0 = \Delta^i y_0 \quad \text{при } i = 1, \dots, r.$$

Доказательство непосредственно следует из (10) и (12). \square

Графиком $S(x)$ является кривая, сшитая из двух кривых Безье (рис. 3).

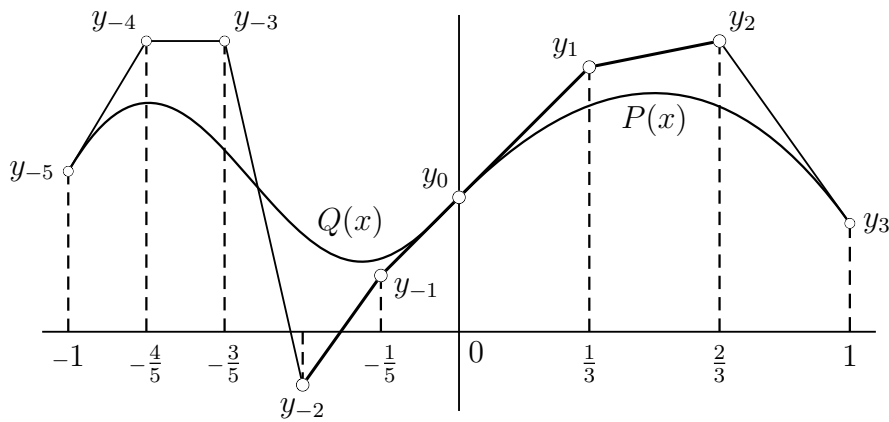


Рис. 3. Составная кривая Безье при $r = 2$

4°. Допустим, что построен график полинома $Q(x)$ на отрезке $[-1, 0]$ по узлам $(-k/m, y_{-k})$, $k \in 0 : m$. Для того, чтобы продолжить его на отрезок $[0, 1]$ с сохранением гладкости до r -го порядка включительно, нужно обеспечить выполнение условия (13). Перепишем это условие в виде

$$\Delta^i y_0 = (C_m^i / C_n^i) \nabla^i y_0, \quad i = 1, \dots, r.$$

Величины $\nabla^i y_0$, $i \in 1 : r$, известны. Вычислив $\Delta^i y_0$, $i \in 1 : r$, найдем y_1, \dots, y_r по формуле

$$y_k = \sum_{i=0}^k C_k^i \Delta^i y_0, \quad k = 1, \dots, r.$$

Набор узлов $(k/n, y_k)$, $k \in 0 : r$, обеспечивает выполнение условия (13). Остальные узлы $(k/n, y_k)$, $k \in r+1 : n$, — произвольны. По схеме (7) строим график $B(x)$ на $[0, 1]$ как продолжение графика $Q(x)$ на $[-1, 0]$.

5°. Представим себе такую ситуацию: график $B(x)$ на $[0, 1]$ уже построен, но он нас не устраивает. Мы хотели бы увеличить степень полинома $B(x)$, чтобы усложнить поведение кривой Безье (сделать ее более гибкой). Разумеется, с сохранением гладкости составной кривой $S(x)$ на отрезке $[-1, 1]$.

Основой для решения этой задачи является следующее свойство полиномов Бернштейна.

ТЕОРЕМА 3. *Полином (1) можно представить в виде*

$$B(x) = \sum_{k=0}^{n+1} \hat{y}_k C_{n+1}^k x^k (1-x)^{n+1-k}, \quad (14)$$

где $\hat{y}_0 = y_0$, $\hat{y}_{n+1} = y_n$ и

$$\hat{y}_k = \left(1 - \frac{k}{n+1}\right) y_k + \frac{k}{n+1} y_{k-1}, \quad k \in 1 : n.$$

Доказательство. Распишем подробно правую часть формулы (14):

$$\begin{aligned} & y_0 (1-x)^{n+1} + y_n x^{n+1} + \sum_{k=1}^n \left(1 - \frac{k}{n+1}\right) y_k C_{n+1}^k x^k (1-x)^{n+1-k} + \\ & + \sum_{k=0}^{n-1} \frac{k+1}{n+1} y_k C_{n+1}^{k+1} x^{k+1} (1-x)^{n-k}. \end{aligned} \quad (15)$$

Отметим, что

$$\left(1 - \frac{k}{n+1}\right) C_{n+1}^k = C_n^k, \quad \frac{k+1}{n+1} C_{n+1}^{k+1} = C_n^k.$$

Подставляя это в (15), получаем выражение

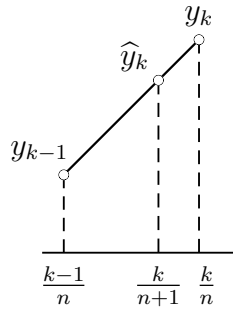
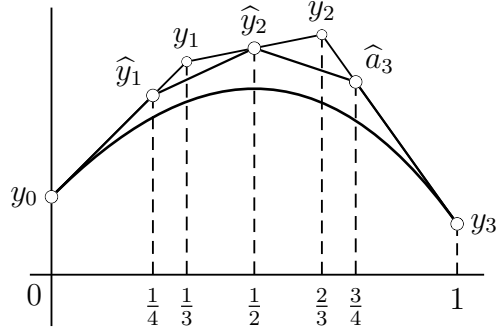
$$\begin{aligned} & y_0 [(1-x)^{n+1} + x(1-x)^n] + y_n [x^{n+1} + x^n(1-x)] + \\ & + \sum_{k=1}^{n-1} y_k C_n^k [x^k (1-x)^{n+1-k} + x^{k+1} (1-x)^{n-k}]. \end{aligned}$$

Остается учесть, что при $k \in 0 : n$

$$x^k (1-x)^{n+1-k} + x^{k+1} (1-x)^{n-k} = x^k (1-x)^{n-k}.$$

Теорема доказана. □

Дадим геометрическую интерпретацию теоремы 3. Обозначим через Γ_n непрерывную ломаную с узлами $(k/n, y_k)$, $k \in 0 : n$. Она называется *характеристическим многоугольником* для $B(x)$. Наряду с Γ_n рассмотрим непрерывную ломаную Γ_{n+1} с узлами $(k/(n+1), \hat{y}_k)$, $k \in 0 : n+1$. Нетрудно проверить, что узлы $(k/(n+1), \hat{y}_k)$ лежат на Γ_n (как показано на рис. 4). Данное наблюдение дает простой способ построения Γ_{n+1} по Γ_n (рис. 5). Теорема 3 утверждает, что как Γ_n , так и Γ_{n+1} являются характеристическими многоугольниками для $B(x)$.

Рис. 4. Звено ломаной Γ_n Рис. 5. Переход от ломаной Γ_3 к Γ_4

Если составная кривая $S(x)$ была r раз непрерывно дифференцируемой, то по теореме 2 выполняется условие

$$C_m^i \nabla^i y_0 = C_{n+1}^i \Delta^i \hat{y}_0, \quad i \in 1 : r.$$

Закрепим узлы $(k/(n+1), \hat{y}_k)$, $k \in 0 : r$. Остальными узлами $(k/(n+1), \hat{y}_k)$, $k \in r+1 : n+1$, при построении составной кривой Безье можно управлять. Очевидно, что количество степеней свободы у составной кривой Безье увеличилось на единицу.

От ломаной Γ_{n+1} можно перейти к ломаной Γ_{n+2} и т.д., приобретая каждый раз лишнюю степень свободы.

6°. Построение составной кривой Безье в пространстве \mathbb{R}^s производится по аналогичной схеме. В частности, выполнение векторного условия

$$C_m^i \nabla^i Y_0 = C_n^i \Delta^i Y_0 \quad \text{при } i = 1, \dots, r$$

гарантирует непрерывную дифференцируемость составной кривой Безье до r -го порядка включительно.

7°. Обратимся к вопросу о вычислении производной полинома Бернштейна (1).

ЛЕММА 4. При $n \geq 2$ справедлива формула

$$B'(x) = \sum_{k=0}^{n-1} u_k^{(1)} p_{n-1,k}(x), \quad (16)$$

где $u_k^{(1)} = n(y_{k+1} - y_k)$.

Доказательство. Имеем

$$p'_{n0}(x) = -n p_{n-1,0}(x), \quad p'_{nn}(x) = n p_{n-1,n-1}(x). \quad (17)$$

Далее при $k \in 1 : n-1$

$$p'_{nk}(x) = k C_n^k x^{k-1} (1-x)^{n-k} - (n-k) C_n^{n-k} x^k (1-x)^{n-1-k}.$$

Поскольку $k C_n^k = n C_{n-1}^{k-1}$, $(n-k) C_n^{n-k} = n C_{n-1}^k$, то

$$p'_{nk}(x) = n (p_{n-1,k-1}(x) - p_{n-1,k}(x)). \quad (18)$$

На основании (17), (18) получаем

$$\begin{aligned} B'(x) &= \sum_{k=0}^n y_k p'_{nk}(x) = y_0 p'_{n0}(x) + y_n p'_{nn}(x) + \\ &+ n \sum_{k=1}^{n-1} y_k (p_{n-1,k-1}(x) - p_{n-1,k}(x)) = n \sum_{k=1}^n y_k p_{n-1,k-1}(x) - \\ &- n \sum_{k=0}^{n-1} y_k p_{n-1,k}(x) = n \sum_{k=0}^{n-1} (y_{k+1} - y_k) p_{n-1,k}(x), \end{aligned}$$

что равносильно (16). □

Из (16), в частности, следует, что

$$B'(0) = n(y_1 - y_0), \quad B'(1) = n(y_n - y_{n-1}).$$

Это значит, что график полинома $B(x)$ в точках $x = 0$ и $x = 1$ касается характеристического многоугольника (см. рис. 1).

ТЕОРЕМА 4. При $n \geq 2$ и $x \in (0, 1)$ справедливо равенство

$$B'(x) = n(y_1^{(n-1)} - y_0^{(n-1)}),$$

где $y_0^{(n-1)}$ и $y_1^{(n-1)}$ вычисляются по схеме (7).

Доказательство. Формулу (16) сопоставим с (6). Правую часть (16) можно преобразовать так же, как правую часть (6). В результате получим

$$B'(x) = \sum_{k=0}^{n-2} u_k^{(2)} p_{n-2,k}(x),$$

где

$$\begin{aligned} u_k^{(2)} &= (1-x) u_k^{(1)} + x u_{k+1}^{(1)} = (1-x) \left[n (y_{k+1}^{(0)} - y_k^{(0)}) \right] + \\ &+ x \left[n (y_{k+2}^{(0)} - y_{k+1}^{(0)}) \right] = n \left[(1-x) y_{k+1}^{(0)} + x y_{k+2}^{(0)} \right] - \\ &- n \left[(1-x) y_k^{(0)} + x y_{k+1}^{(0)} \right] = n (y_{k+1}^{(1)} - y_k^{(1)}). \end{aligned}$$

Аналогично

$$B'(x) = \sum_{k=0}^{n-3} u_k^{(3)} p_{n-3,k}(x),$$

где $u_k^{(3)} = n (y_{k+1}^{(2)} - y_k^{(2)})$, и т. д. Наконец,

$$\begin{aligned} B'(x) &= \sum_{k=0}^1 u_k^{(n-1)} p_{1k}(x) = (1-x) u_0^{(n-1)} + x u_1^{(n-1)} = \\ &= (1-x) \left[n (y_1^{(n-2)} - y_0^{(n-2)}) \right] + x \left[n (y_2^{(n-2)} - y_1^{(n-2)}) \right] = \\ &= n (y_1^{(n-1)} - y_0^{(n-1)}). \end{aligned}$$

Теорема доказана. \square

Теорема 4 показывает, что можно одновременно вычислить значения $B(x)$ и $B'(x)$ в точке $x \in (0, 1)$. Для этого по схеме (7) нужно найти $y_0^{(n-1)}$ и $y_1^{(n-1)}$, после чего положить

$$B(x) = (1-x) y_0^{(n-1)} + x y_1^{(n-1)}, \quad B'(x) = n (y_1^{(n-1)} - y_0^{(n-1)}). \quad (19)$$

Дадим геометрическую интерпретацию равенств (19). Вернемся к векторной схеме (9) при $Y_k = (k/n, y_k)$, $k \in 0 : n$. Как отмечалось в п. 2°, точки $Y_0^{(n-1)}$ и $Y_1^{(n-1)}$ имеют координаты $(\frac{(n-1)x}{n}, y_0^{(n-1)})$ и $(\frac{(n-1)x+1}{n}, y_1^{(n-1)})$ соответственно. Равенства (19) гарантируют, что в точке x график полинома Бернштейна касается отрезка, соединяющего точки $Y_0^{(n-1)}$ и $Y_1^{(n-1)}$ (см. рис. 1).

8°. Дополнительная информация о полиномах Бернштейна и кривых Безье имеется на сайте [4].

ЛИТЕРАТУРА

1. Виденский В. С. *Многочлены Бернштейна*. Л.: ЛГПИ им. А. И. Герцена, 1990. 64 с.
2. Безье П. *Геометрические методы*. В кн.: Математика и САПР. 2. М.: Мир, 1989. С. 96–257.
3. Мысовских И. П. *Лекции по численным методам*. Изд. второе. СПб.: Изд-во СПбГУ, 1998. 472 с.
4. *On-Line Geometric Modeling Notes*.
<http://graphics.cs.ucdavis.edu/CAGDNotes/>.

ПРЯМАЯ ЛИФТИНГОВАЯ СХЕМА

В. Н. Малозёмов

Н. А. Селянинова

26 апреля 2005 г.

Доклад представляет собой усовершенствованный вариант первой части статьи [1]. Описано полное лифтинговое преобразование сигнала, основанное на дискретной периодической сплайн-интерполяции. Выведены формулы точного восстановления сигнала (обращения).

Используются следующие обозначения:

\mathbb{C}_N — пространство сигналов (комплекснозначных N -периодических функций целочисленного аргумента),

$\omega_N = \exp(2\pi i/N)$ — корень N -й степени из единицы,

\mathcal{F}_N — дискретное преобразование Фурье порядка N (сопоставляющее сигналу x сигнал $X = \mathcal{F}_N(x)$ с компонентами

$$X(k) = \sum_{j=0}^{N-1} x(j) \omega_N^{-kj}, \quad k \in \mathbb{Z}.$$

1. Предварительные сведения

1.1. Пусть сигнал x принадлежит пространству \mathbb{C}_N , где $N = 2m$. Обозначим

$$e(j) = x(2j), \quad d(j) = x(2j+1), \quad j \in 0 : m-1.$$

ПРЕДЛОЖЕНИЕ 1. Спектры $X = \mathcal{F}_N(x)$, $E = \mathcal{F}_m(e)$, $D = \mathcal{F}_m(d)$ связаны соотношением

$$X(k) = E(k) + \omega_N^{-k} D(k), \quad k \in \mathbb{Z}. \quad (1.1)$$

Доказательство. При $k \in \mathbb{Z}$ имеем

$$\frac{1}{2} [X(k) + X(k+m)] = \frac{1}{2} \sum_{j=0}^{2m-1} x(j) \omega_N^{-kj} (1 + (-1)^j) =$$

$$\begin{aligned}
&= \sum_{l=0}^{m-1} x(2l) \omega_m^{-kl} = \sum_{l=0}^{m-1} e(l) \omega_m^{-kl} = E(k), \\
\frac{1}{2} [X(k) - X(k+m)] &= \frac{1}{2} \sum_{j=0}^{2m-1} x(j) \omega_N^{-kj} (1 - (-1)^j) = \\
&= \sum_{l=0}^{m-1} x(2l+1) \omega_N^{-k(2l+1)} = \omega_N^{-k} \sum_{l=0}^{m-1} d(l) \omega_m^{-kl} = \omega_N^{-k} D(k).
\end{aligned}$$

Сложив эти равенства, придем к (1.1). \square

1.2. Напомним (см. [2]), что при $N = nm$ и натуральном r B -сплайн $Q_r \in \mathbb{C}_N$ определяется формулой

$$Q_r(j) = \frac{1}{N} \sum_{k=0}^{N-1} u^r(k) \omega_N^{kj}, \quad (1.2)$$

где

$$u(k) = \begin{cases} n^2 & \text{при } k = 0, \\ \left[\sin \frac{\pi k}{m} \left(\sin \frac{\pi k}{N} \right)^{-1} \right]^2 & \text{при } k = 1, \dots, N-1. \end{cases} \quad (1.3)$$

Сплайном порядка r называется линейная комбинация с комплексными коэффициентами сдвигов B -сплайна:

$$S(j) = \sum_{p=0}^{m-1} c(p) Q_r(j - pn).$$

Рассмотрим задачу сплайн-интерполяции

$$S(ln) = z(l), \quad l \in 0 : m-1. \quad (1.4)$$

ПРЕДЛОЖЕНИЕ 2. Задача (1.4) имеет единственное решение. Для дискретного преобразования Фурье $C = \mathcal{F}_m(c)$ коэффициентов интерполяционного сплайна справедлива формула

$$C(k) = Z(k)/T_r(k), \quad k \in 0 : m-1,$$

где $Z = \mathcal{F}_m(z)$ и

$$T_r(k) = \sum_{p=0}^{m-1} Q_r(pn) \omega_m^{-kp}.$$

1.3. В дальнейшем нас будет интересовать случай $n = 2$.

ПРЕДЛОЖЕНИЕ 3. Коэффициенты $T_r(k)$ при $n = 2$ допускают представление

$$T_r(k) = \frac{1}{2} \left[\left(2 \cos \frac{\pi k}{N} \right)^{2r} + \left(2 \sin \frac{\pi k}{N} \right)^{2r} \right], \quad k \in 0 : m - 1. \quad (1.5)$$

Доказательство. Формула (1.5) при $n = 2$ (при $N = 2m$) принимает вид

$$u(k) = \left(2 \cos \frac{\pi k}{N} \right)^2, \quad k \in 0 : N - 1.$$

В силу (1.2)

$$[\mathcal{F}_N(Q_r)](k) = u^r(k) = \left(2 \cos \frac{\pi k}{N} \right)^{2r}, \quad k \in 0 : N - 1. \quad (1.6)$$

Вместе с тем,

$$\begin{aligned} [\mathcal{F}_N(Q_r)](k) + [\mathcal{F}_N(Q_r)](k+m) &= \sum_{j=0}^{2m-1} Q_r(j) \omega_N^{-kj} (1 + (-1)^j) = \\ &= 2 \sum_{p=0}^{m-1} Q_r(2p) \omega_m^{-kp} = 2 T_r(k). \end{aligned}$$

Отсюда и из (1.6) следует (1.5). \square

1.4. Пусть S - интерполяционный сплайн при $N = 2m$. Он определяется условием

$$S(2l) = z(l), \quad l \in 0 : m - 1.$$

Вычислим значения $\sigma(l) = S(2l+1)$, $l \in 0 : m - 1$. Для этого достаточно найти $\mathcal{F}_m(\sigma)$.

ПРЕДЛОЖЕНИЕ 4. Справедлива формула

$$[\mathcal{F}_m(\sigma)](k) = \omega_N^k U_1(k) Z(k), \quad k \in 0 : m - 1, \quad (1.7)$$

где $Z = \mathcal{F}_m(z)$ и

$$U_1(k) = \frac{\left(\cos \frac{\pi k}{N} \right)^{2r} - \left(\sin \frac{\pi k}{N} \right)^{2r}}{\left(\cos \frac{\pi k}{N} \right)^{2r} + \left(\sin \frac{\pi k}{N} \right)^{2r}}.$$

Доказательство. По определению сплайна при $N = 2m$ имеем

$$S(2l+1) = \sum_{p=0}^{m-1} c(p) Q_r(2(l-p)+1).$$

Обозначим $h(p) = Q_r(2p+1)$. Тогда последнее равенство можно переписать в виде $\sigma = c * h$. По теореме о свёртке

$$\mathcal{F}_m(\sigma) = \mathcal{F}_m(c) \mathcal{F}_m(h). \quad (1.8)$$

Найдём $\mathcal{F}_m(h)$. Поскольку

$$\begin{aligned} [\mathcal{F}_N(Q_r)](k) - [\mathcal{F}_N(Q_r)](k+m) &= \sum_{j=0}^{2m-1} Q_r(j) \omega_N^{-kj} (1 - (-1)^j) = \\ &= 2 \sum_{p=0}^{m-1} Q_r(2p+1) \omega_N^{-k(2p+1)} = 2 \omega_N^{-k} \sum_{p=0}^{m-1} h(p) \omega_m^{-kp} = 2 \omega_N^{-k} [\mathcal{F}_m(h)](k), \end{aligned}$$

то

$$\begin{aligned} [\mathcal{F}_m(h)](k) &= \frac{1}{2} \omega_N^k [u^r(k) - u^r(k+m)] = \\ &= \frac{1}{2} \omega_N^k \left[(2 \cos \frac{\pi k}{N})^{2r} - (2 \sin \frac{\pi k}{N})^{2r} \right]. \end{aligned} \quad (1.9)$$

Теперь (1.7) следует из (1.8), предложения 2, (1.5) и (1.9). \square

Отметим, что N -периодический сигнал U_1 удовлетворяет условию $U_1(k+m) = -U_1(k)$. Это гарантирует, в частности, что сигнал $\omega_N^k U_1(k)$ является m -периодическим.

2. Лифтинговое преобразование сигнала

2.1. Пусть $z \in \mathbb{C}_N$, где $N = 2m$. Имея в виду дальнейшее развитие событий, введём обозначения $N_0 = N$, $N_1 = m$, $e_0 = z$. Лифтинговое преобразование сигнала z осуществляется в три этапа.

Split. Расщепим сигнал e_0 на два сигнала

$$\tilde{e}_1(l) = e_0(2l), \quad \tilde{d}_1(l) = e_0(2l+1), \quad l \in 0 : N_1 - 1.$$

Обозначим $\tilde{E}_1 = \mathcal{F}_{N_1}(e_1)$, $\tilde{D}_1 = \mathcal{F}_{N_1}(d_1)$.

Predict. Предскажем значения $\tilde{d}_1(l)$ с помощью интерполяционного сплайна $S_1(j)$, определяемого условием

$$S_1(2l) = \tilde{e}_1(l), \quad l \in 0 : N_1 - 1.$$

Положим $\sigma_1(l) = S_1(2l+1)$, $l \in 0 : N_1 - 1$. Разность

$$d_1(l) = \tilde{d}_1(l) - \sigma_1(l), \quad l \in 0 : N_1 - 1,$$

вообще говоря, мала. Для спектра $D_1 = \mathcal{F}_{N_1}(d_1)$ этой разности согласно (1.7) справедлива формула

$$D_1(k) = \tilde{D}_1(k) - \omega_{N_0}^k U_1(k) \tilde{E}_1(k), \quad k \in 0 : N_1 - 1. \quad (2.1)$$

Lifting. Обновим сигнал \tilde{e}_1 . Для этого введём сигнал e_1 , спектр которого $E_1 = \mathcal{F}_{N_1}(e_1)$ определим так:

$$E_1(k) = \tilde{E}_1(k) + \beta_1(k) \omega_{N_0}^{-k} D_1(k), \quad k \in 0 : N_1 - 1. \quad (2.2)$$

Здесь β_1 — произвольный N_0 -периодический сигнал, удовлетворяющий условию

$$\beta_1(k + N_1) = -\beta_1(k), \quad k \in 0 : N_1 - 1.$$

Ясно, что правая часть (2.2) является N_1 -периодическим сигналом.

2.2. Пара (D_1, E_1) называется *лифтинговым преобразованием сигнала z в спектральной форме*. Спектр E_1 содержит основную информацию о спектре $E_0 = \mathcal{F}_{N_0}(e_0)$ сигнала z , а спектр D_1 — детали.

Выразим D_1, E_1 через E_0 . Для этого введём два вспомогательных сигнала

$$\tilde{g}_1(k) = \omega_{N_0}^k (1 - U_1(k)), \quad \tilde{h}_1(k) = 1 + \beta_1(k) (1 - U_1(k)), \quad k \in 0 : N_0 - 1.$$

ПРЕДЛОЖЕНИЕ 5. При $k \in 0 : N_1 - 1$ справедливы равенства

$$\begin{aligned} D_1(k) &= \frac{1}{2} [\tilde{g}_1(k) E_0(k) + \tilde{g}_1(k + N_1) E_0(k + N_1)], \\ E_1(k) &= \frac{1}{2} [\tilde{h}_1(k) E_0(k) + \tilde{h}_1(k + N_1) E_0(k + N_1)]. \end{aligned} \quad (2.3)$$

Доказательство. Из предложения 1, в частности, следует, что

$$E_0(k) = \tilde{E}_1(k) + \omega_{N_0}^{-k} \tilde{D}_1(k), \quad k \in 0 : N_1 - 1.$$

Заменяя k на $k + N_1$, запишем

$$E_0(k + N_1) = \tilde{E}_1(k) - \omega_{N_0}^{-k} \tilde{D}_1(k), \quad k \in 0 : N_1 - 1.$$

Сложим и вычтем данные равенства. При $k \in 0 : N_1 - 1$ получим

$$\begin{aligned} \tilde{E}_1(k) &= \frac{1}{2} [E_0(k) + E_0(k + N_1)], \\ \tilde{D}_1(k) &= \frac{1}{2} \omega_{N_0}^k [E_0(k) - E_0(k + N_1)]. \end{aligned} \quad (2.4)$$

Остаётся подставить (2.4) в (2.1) и (2.2):

$$\begin{aligned} D_1(k) &= \frac{1}{2} \omega_{N_0}^k \left\{ [E_0(k) - E_0(k + N_1)] - U_1(k) [E_0(k) + E_0(k + N_1)] \right\} = \\ &= \frac{1}{2} [\tilde{g}_1(k) E_0(k) + \tilde{g}_1(k + N_1) E_0(k + N_1)] ; \\ E_1(k) &= \frac{1}{2} \left\{ [E_0(k) + E_0(k + N_1)] + \beta_1(k) [(1 - U_1(k)) E_0(k) - \right. \\ &\left. - (1 + U_1(k)) E_0(k + N_1)] \right\} = \frac{1}{2} [\tilde{h}_1(k) E_0(k) + \tilde{h}_1(k + N_1) E_0(k + N_1)] . \end{aligned}$$

Предложение доказано. \square

2.3. Обратная задача восстановления спектра E_0 исходного сигнала z по паре (D_1, E_1) решается легко. Введём ещё два вспомогательных сигнала

$$h_1(k) = 1 + U_1(k) , \quad g_1(k) = \omega_{N_0}^{-k} (1 - \beta_1(k) h_1(k)) , \quad k \in 0 : N_0 - 1 .$$

ПРЕДЛОЖЕНИЕ 6. *Справедлива формула обращения*

$$E_0(k) = h_1(k) E_1(k) + g_1(k) D_1(k) , \quad k \in 0 : N_0 - 1 . \quad (2.5)$$

Доказательство. Согласно (2.2) и (2.1)

$$\begin{aligned} \tilde{E}_1(k) &= E_1(k) - \beta_1(k) \omega_{N_0}^{-k} D_1(k) , \\ \tilde{D}_1(k) &= D_1(k) + \omega_{N_0}^k U_1(k) \tilde{E}_1(k) = \\ &= D_1(k) + \omega_{N_0}^k U_1(k) E_1(k) - \beta_1(k) U_1(k) D_1(k) = \\ &= (1 - \beta_1(k) U_1(k)) D_1(k) + \omega_{N_0}^k U_1(k) E_1(k) . \end{aligned}$$

На основании предложения 1 заключаем, что при $k \in 0 : N_0 - 1$

$$\begin{aligned} E_0(k) &= \tilde{E}_1(k) + \omega_{N_0}^{-k} \tilde{D}_1(k) = E_1(k) - \beta_1(k) \omega_{N_0}^{-k} D_1(k) + \\ &+ \omega_{N_0}^{-k} (1 - \beta_1(k) U_1(k)) D_1(k) + U_1(k) E_1(k) = \\ &= h_1(k) E_1(k) + g_1(k) D_1(k) . \end{aligned}$$

Предложение доказано. \square

С вычислительной точки зрения формулу (2.5) лучше записать так: при $k \in 0 : N_1 - 1$

$$\begin{aligned} E_0(k) &= h_1(k) E_1(k) + g_1(k) D_1(k) , \\ E_0(k + N_1) &= h_1(k + N_1) E_1(k) + g_1(k + N_1) D_1(k) . \end{aligned} \quad (2.6)$$

3. Многоуровневое лифтинговое преобразование

3.1. Теперь будем считать, что $N = 2^s$. Обозначим $N_\nu = N/2^\nu$, $\nu = 0, 1, \dots, s$. Это обозначение согласовано с обозначениями N_0, N_1 из предыдущего раздела. Отметим также, что $N_s = 1$.

В разделе 2 было описано лифтинговое преобразование $E_0 \rightarrow (D_1, E_1)$. Это преобразование можно продолжить:

$$E_1 \rightarrow (D_2, E_2), \quad E_2 \rightarrow (D_3, E_3), \quad \dots, \quad E_{s-1} \rightarrow (D_s, E_s).$$

Выведем соответствующие формулы. Положим при $k \in 0 : N_{\nu-1} - 1$

$$U_\nu(k) = \frac{\left(\cos \frac{\pi k}{N_{\nu-1}}\right)^{2r} - \left(\sin \frac{\pi k}{N_{\nu-1}}\right)^{2r}}{\left(\cos \frac{\pi k}{N_{\nu-1}}\right)^{2r} + \left(\sin \frac{\pi k}{N_{\nu-1}}\right)^{2r}},$$

$$\tilde{g}_\nu(k) = \omega_{N_{\nu-1}}^k (1 - U_\nu(k)), \quad \tilde{h}_\nu(k) = 1 + \beta_\nu(k)(1 - U_\nu(k)).$$

Здесь $\beta_\nu(k)$ — произвольная $N_{\nu-1}$ -периодическая функция, удовлетворяющая условию

$$\beta_\nu(k + N_\nu) = -\beta_\nu(k), \quad k \in 0 : N_\nu - 1.$$

Аналогично предложению 5 доказывается следующее утверждение: *при $k \in 0 : N_\nu - 1$ справедливы равенства*

$$\begin{aligned} D_\nu(k) &= \frac{1}{2} [\tilde{g}_\nu(k) E_{\nu-1}(k) + \tilde{g}_\nu(k + N_\nu) E_{\nu-1}(k + N_\nu)], \\ E_\nu(k) &= \frac{1}{2} [\tilde{h}_\nu(k) E_{\nu-1}(k) + \tilde{h}_\nu(k + N_\nu) E_{\nu-1}(k + N_\nu)]. \end{aligned}$$

Набор спектров $(D_1, D_2, \dots, D_s, E_s)$ называется *полным лифтинговым преобразованием сигнала z* . Отметим, что D_s, E_s — это числа.

3.2. По полному лифтинговому преобразованию $(D_1, D_2, \dots, D_s, E_s)$ легко восстановить спектр E_0 исходного сигнала z . Для этого введём два вспомогательных сигнала

$$h_\nu(k) = 1 + U_\nu(k), \quad g_\nu(k) = \omega_{N_{\nu-1}}^{-k} (1 - \beta_\nu(k) h_\nu(k)), \quad k \in 0 : N_{\nu-1} - 1.$$

Согласно (2.6) имеем

$$\begin{aligned} E_{\nu-1}(k) &= h_\nu(k) E_\nu(k) + g_\nu(k) D_\nu(k), \\ E_{\nu-1}(k + N_\nu) &= h_\nu(k + N_\nu) E_\nu(k) + g_\nu(k + N_\nu) D_\nu(k), \\ k &\in 0 : N_\nu - 1, \quad \nu = s, s-1, \dots, 1. \end{aligned} \tag{3.1}$$

При $\nu = 1$ получим $E_0 = \mathcal{F}_N(z)$.

4. Лифтинговые разложения сигнала

4.1. Перепишем (3.1) в виде

$$E_{\nu-1} = h_\nu E_\nu + g_\nu D_\nu, \quad \nu = s, s-1, \dots, 1. \quad (4.1)$$

ПРЕДЛОЖЕНИЕ 7. При любом $t \in 1 : s$ справедлива формула

$$E_0 = h_1 h_2 \dots h_t E_t + \sum_{\nu=1}^t h_1 h_2 \dots h_{\nu-1} g_\nu D_\nu. \quad (4.2)$$

Доказательство. При $t = 1$ соотношение (4.2) совпадает с (2.5). Индукционный переход легко осуществить, опираясь на (4.1). \square

Введём обозначения $H_\nu = h_1 h_2 \dots h_\nu$, $G_\nu = h_1 h_2 \dots h_{\nu-1} g_\nu$,

$$\phi_\nu = \mathcal{F}_N^{-1}(H_\nu), \quad \psi_\nu = \mathcal{F}_N^{-1}(G_\nu).$$

ПРЕДЛОЖЕНИЕ 8. Пусть $N = 2^s$ и $t \in 1 : s$. Для любого сигнала $z \in \mathbb{C}_N$ справедливо разложение

$$z(j) = \sum_{k=0}^{N_t-1} e_t(k) \phi_t(j - 2^t k) + \sum_{\nu=1}^t \sum_{k=0}^{N_\nu-1} d_\nu(k) \psi_\nu(j - 2^\nu k), \quad j \in \mathbb{Z}, \quad (4.3)$$

где $e_t = \mathcal{F}_{N_t}^{-1}(E_t)$, $d_\nu = \mathcal{F}_{N_\nu}^{-1}(D_\nu)$.

Доказательство. Применим к (4.2) обратное преобразование Фурье порядка N . Получим

$$z = \mathcal{F}_N^{-1}(H_t E_t) + \sum_{\nu=1}^t \mathcal{F}_N^{-1}(G_\nu D_\nu). \quad (4.4)$$

Отметим, что

$$\begin{aligned} [\mathcal{F}_N^{-1}(G_\nu D_\nu)](j) &= \frac{1}{N} \sum_{l=0}^{N-1} G_\nu(l) D_\nu(l) \omega_N^{lj} = \\ &= \frac{1}{N} \sum_{l=0}^{N-1} G_\nu(l) \omega_N^{lj} \sum_{k=0}^{N_\nu-1} d_\nu(k) \omega_{N_\nu}^{-lk} = \\ &= \sum_{k=0}^{N_\nu-1} d_\nu(k) \left\{ \frac{1}{N} \sum_{l=0}^{N-1} G_\nu(l) \omega_N^{l(j-2^\nu k)} \right\} = \sum_{k=0}^{N_\nu-1} d_\nu(k) \psi_\nu(j - 2^\nu k). \end{aligned} \quad (4.5)$$

Аналогично показывается, что

$$[\mathcal{F}_N^{-1}(H_t E_t)](j) = \sum_{k=0}^{N_t-1} e_t(k) \phi_t(j - 2^t k). \quad (4.6)$$

Подставив (4.5), (4.6) в (4.4), придём к (4.3). \square

Формула (4.3) называется *лифтинговым разложением сигнала* z .

Правая часть (4.3) при каждом $t \in 1 : s$ содержит ровно N слагаемых (по размерности пространства \mathbb{C}_N). Поскольку разложение (4.3) справедливо для любого сигнала $z \in \mathbb{C}_N$, то система сигналов

$$\left\{ \left\{ \phi_t(j - 2^t k) \right\}_{k=0}^{N_t-1} ; \left\{ \psi_\nu(j - 2^\nu k) \right\}_{k=0}^{N_\nu-1}, \quad \nu = 1, \dots, t \right\}$$

необходимо является базисом в \mathbb{C}_N .

4.2. При $t = s$ формула (4.3) называется *полным лифтинговым разложением сигнала* z . Первая сумма в правой части такого разложения вырождается до одного слагаемого $e_s(0) \phi_s(j)$.

ПРЕДЛОЖЕНИЕ 9. *Имеет место тождество $\phi_s(j) \equiv 1$.*

Доказательство. Достаточно проверить, что $H_s = N\delta_N$.

Напомним, что

$$h_\nu(k) = 1 + U_\nu(k) = \frac{2 \left(\cos \frac{\pi k}{2N_\nu} \right)^{2r}}{\left(\cos \frac{\pi k}{2N_\nu} \right)^{2r} + \left(\sin \frac{\pi k}{2N_\nu} \right)^{2r}}$$

и

$$H_s(k) = \prod_{\nu=1}^s h_\nu(k).$$

Ясно, что $H_s(0) = N$. Нужно показать, что $H_s(k) = 0$ при $k \in 1 : N - 1$.

Возьмём $k \in 1 : N - 1$ и представим его в виде

$$k = (k_{s-1}, \dots, k_{s-p+1}, 1, 0, \dots, 0)_2 = (2n+1)N_p$$

при некотором $p \in 1 : s$. Так как

$$\cos \frac{\pi k}{2N_p} = \cos \frac{\pi}{2} (2n+1) = 0,$$

то $h_p(k) = 0$. Значит, и $H_s(k) = 0$. Предложение доказано. \square

На основании предложений 8 и 9 заключаем, что полное лифтинговое разложение сигнала $z \in \mathbb{C}_N$ имеет вид

$$z(j) = e_s(0) + \sum_{\nu=1}^s \sum_{k=0}^{N_\nu-1} d_\nu(k) \psi_\nu(j - 2^\nu k), \quad j \in \mathbb{Z}.$$

ЛИТЕРАТУРА

1. Жёлудев В. А., Певный А. Б. *Биортогональные вейвлетные схемы, основанные на интерполяции дискретными сплайнами* // Журн. выч. мат. и матем. физ. 2001. Т. 41. № 4. С. 537–548.
2. Малозёмов В. Н., Певный А. Б. *Дискретные периодические сплайны и их вычислительные применения* // Журн. выч. мат. и матем. физ. 1998. Т. 38. № 8. С. 1235–1246.

ПРОГРАММИРОВАНИЕ И МАТЕМАТИКА

В. Н. Малозёмов А. Б. Певный

17 мая 2005 г.

Введение

При разработке численного метода решения некоторой задачи нужно иметь в виду, что метод будет реализован в форме алгоритма, а затем программы. Конечным звеном этой цепочки является *программа*, и именно программа характеризует качество цепочки в целом.

Обычно существует несколько способов решения поставленной задачи. Каждый способ реализуется своей программой. Как конечный продукт, программа может быть примитивной или изящной, красивой. К сожалению, понятие «красивая программа» не формализуется. К необходимым условиям для составления такой программы следует отнести стремление к минимизации количества операций и используемой памяти. Этого можно достичь с помощью математических приёмов. В определённом смысле, *хорошая программа основана на хорошей математике*. Приведём три характерных примера.

Пример 1. Вычислить сумму

$$S_n = \sum_{k=1}^n \frac{(-1)^{k(k-1)/2}}{k!!},$$

где $k!!$ (двойной факториал) — это произведение натуральных чисел, не превосходящих k и имеющих одинаковую с k чётность, т. е.

$$(2m)!! = 2 \cdot 4 \cdot \dots \cdot (2m), \quad (2m+1)!! = 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2m+1).$$

Обозначим $b_k = k(k-1)/2$, $c_k = k!!$, $a_k = (-1)^{b_k}/c_k$. Тогда $S_n = \sum_{k=1}^n a_k$. В принципе, можно независимо вычислить все a_k и, сложив их, получить S_n . Программа, реализующая такой способ, будет примитивной. Чтобы написать красивую программу, будем действовать иначе.

Отметим, что $b_k - b_{k-2} = 2k - 3$. Это приводит к рекуррентному соотношению для последовательности $\{b_k\}$:

$$b_k = b_{k-2} + (2k - 3), \quad k = 2, 3, \dots; \quad b_0 = b_1 = 0.$$

Менее тривиальным является рекуррентное соотношение для $\{c_k\}$:

$$c_k = k c_{k-2}, \quad k = 2, 3, \dots; \quad c_0 = c_1 = 1.$$

Теперь имеем

$$a_k = \frac{(-1)^{b_k}}{c_k} = \frac{(-1)^{b_{k-2}+(2k-3)}}{k c_{k-2}} = -\frac{1}{k} a_{k-2},$$

так что

$$a_k = -a_{k-2}/k, \quad k = 2, 3, \dots; \quad a_0 = a_1 = 1.$$

Это соотношение положим в основу программы:

```

a := 1; a1 := 1; s := 1;
for k := 2 to n do begin
  a2 := a1; a1 := a;
  a := -a2/k; s := s + a
end

```

После работы программы $s = S_n$. В ячейке a находится текущее значение a_k , в ячейках $a1, a2$ — значения a_{k-1}, a_{k-2} . Табл. 1 дает представление об изменении содержимого ячеек $a, a1, a2$ в цикле по k .

Таблица 1

k	a	$a1$	$a2$
1	a_1	a_0	—
2	a_2	a_1	a_0
3	a_3	a_2	a_1
...
n	a_n	a_{n-1}	a_{n-2}

Пример 2. Вычислить значение производной n -го порядка функции $f(x) = \sin(x)/x$ в точке $x \neq 0$.

В отличие от предыдущего примера у нас нет явной формулы для $f^{(n)}(x)$. Однако без этого можно обойтись. Последовательно дифференцируя, получаем

$$\begin{aligned}
 x f(x) &= \sin(x), & f(x) + x f'(x) &= [\sin(x)]', \\
 2f'(x) + x f''(x) &= [\sin(x)]'', & 3f''(x) + x f'''(x) &= [\sin(x)]''', \dots, \\
 n f^{(n-1)}(x) + x f^{(n)}(x) &= [\sin(x)]^{(n)}.
 \end{aligned}$$

Приходим к рекуррентному соотношению по номеру производной:

$$\begin{aligned}
 f^{(k)}(x) &= ([\sin(x)]^{(k)} - k f^{(k-1)}(x)) / x, & k &= 1, 2, \dots, n; \\
 f^{(0)}(x) &= \sin(x)/x.
 \end{aligned}$$

В свою очередь величина $p_k = [\sin(x)]^{(k)}$ удовлетворяет рекуррентному соотношению

$$p_k = -p_{k-2}, \quad k = 1, 2, \dots, n; \quad p_{-1} = -\cos(x), \quad p_0 = \sin(x).$$

Указанные соображения приводят к следующей эффективной программе:

```

p := sin(x); p1 := -cos(x); fn := p/x;
for k := 1 to n do begin
    p2 := p1; p1 := p; p := -p2;
    fn := (p - k * fn)/x
end

```

После работы программы $fn = f^{(n)}(x)$.

Пример 3. Заданы n вещественных чисел $a[1], a[2], \dots, a[n]$. Вычислить

$$p_n = \max_{1 \leq i \leq j \leq n} \sum_{l=i}^j a[l]$$

при дополнительном условии: каждое $a[l]$ можно вызывать только один раз.

Если не обращать внимания на дополнительное условие, то задача решается просто. Действительно, обозначим

$$s_{ij} = \sum_{l=i}^j a[l].$$

Вычислив последовательно суммы

$$\begin{array}{cccccc}
 s_{11}, & s_{12}, & s_{13}, & \dots & s_{1,n-1}, & s_{1n}, \\
 & s_{22}, & s_{23}, & \dots & s_{2,n-1}, & s_{2n}, \\
 & & \dots & \dots & \dots & \dots \\
 & & & & s_{n-1,n-1}, & s_{n-1,n}, \\
 & & & & & s_{nn}
 \end{array}$$

и найдя среди них наибольшую, получим p_n . Дополнительное условие существенно усложняет задачу. Более того, не совсем понятно, как подступиться к её решению. На помощь приходят рекуррентные мотивы.

Положим

$$p_k = \max_{1 \leq i \leq j \leq k} s_{ij}, \quad q_k = \max_{1 \leq i \leq k} s_{ik}.$$

Очевидно, что

$$p_k = \max\{p_{k-1}, q_k\}, \quad k = 2, 3, \dots, n; \quad p_1 = a[1]. \quad (1.1)$$

Поскольку

[illegible]

TO

$$q_k = a[k] + \max\{0, q_{k-1}\}, \quad k = 2, 3, \dots, n; \quad q_1 = a[1]. \quad (1.2)$$

Система рекуррентных соотношений (1.1), (1.2) позволяет записать редкую по красоте программу:

```

p := a[1]; q := p;
for k := 2 to n do begin
  if q < 0 then q := 0;
  q := a[k] + q;
  if p < q then p := q;
end

```

После работы программы $p = p_n$. Видно, что каждое $a[k]$ вызывается только один раз!

Во всех трёх примерах для составления продвинутой программы использовались рекуррентные соотношения. Такие соотношения не всегда лежат на поверхности, и для их обнаружения требуется определённый опыт. Вместе с тем, в области рекуррентных вычислений существуют вполне регулярные приёмы, которые применяются при решении существенно разных по содержанию задач. Одним из таких приёмов является схема Кленшоу. Эта замечательная схема, предложенная 50 лет назад, не относится однако к числу широко известных.

2. Схеми Кленшоу

2.1. Рассмотрим алгебраический полином вида

$$P(x) = \frac{1}{2}a[0] + \sum_{k=1}^n a[k]T_k(x),$$

где $T_k(x)$ — полиномы Чебышёва, определяемые рекуррентным соотношением

$$T_k(x) = 2xT_{k-1}(x) - T_{k-2}(x), \quad k = 2, 3, \dots; \quad T_0(x) \equiv 1, \quad T_1(x) = x. \quad (2.1)$$

Поставим задачу: вычислить значение $P(x)$ в фиксированной точке x .

Примитивную программу, решающую эту задачу, можно записать сразу.

```

p := 0.5 * a[0] + x * a[1];
t := x; t1 := 1; c := 2 * x;
for k := 2 to n do begin
    t2 := t1; t1 := t;
    t := c * t1 - t2;
    p := p + t * a[k]
end

```

После работы программы $p = P(x)$. В программе используется $2n + 1$ умножений и $2n - 1$ сложений.

Кленшоу в работе [1] предложил другой метод решения, который приводит к программе с $n + 2$ умножениями и $2n + 1$ сложениями. Идея Кленшоу заключается в следующем.

Введём рекуррентную последовательность $\{b_k\}$, исходя из условий

$$a[k] = b_k - 2xb_{k+1} + b_{k+2}, \quad k = n, n-1, \dots, 0; \quad b_{n+2} = b_{n+1} = 0. \quad (2.2)$$

Такую последовательность построить можно:

$$b_{n+1} = 0, \quad b_n = a[n]; \quad b_k = a[k] + 2xb_{k+1} - b_{k+2}, \quad k = n-1, n-2, \dots, 0. \quad (2.3)$$

Обозначим $\tilde{P}(x) = P(x) + \frac{1}{2}a[0]$, $t_k = T_k(x)$ и запишем

$$\begin{aligned}
\tilde{P}(x) &= \sum_{k=0}^n a[k]t_k = \sum_{k=0}^n (b_k - 2xb_{k+1} + b_{k+2})t_k = \\
&= \sum_{k=0}^n b_k t_k - 2x \sum_{k=1}^{n+1} b_k t_{k-1} + \sum_{k=2}^{n+2} b_k t_{k-2} = \\
&= b_0 t_0 + b_1 t_1 - 2xb_1 t_0 + \sum_{k=2}^n b_k (t_k - 2xt_{k-1} + t_{k-2}).
\end{aligned}$$

Согласно (2.1) последняя сумма равна нулю, поэтому

$$\tilde{P}(x) = b_0 t_0 + b_1 (t_1 - 2xt_0) = b_0 - xb_1.$$

Теперь имеем

$$P(x) = \tilde{P}(x) - \frac{1}{2}a[0] = b_0 - xb_1 - \frac{1}{2}(b_0 - 2xb_1 + b_2) = \frac{1}{2}(b_0 - b_2).$$

Мы пришли к замечательной формуле

$$P(x) = \frac{1}{2}(b_0 - b_2).$$

Она показывает, что в основу вычисления значения $P(x)$ можно положить рекуррентное соотношение (2.3). Приведём соответствующую программу:

```

b := a[n]; b1 := 0; c := 2 * x;
for k := n - 1 downto 0 do begin
    b2 := b1; b1 := b;
    b := a[k] + c * b1 - b2
end;
p := 0.5 * (b - b2)

```

После работы программы $p = P(x)$. В ячейке b находится текущее значение b_k , в ячейках $b1, b2$ — значения b_{k+1}, b_{k+2} . Как и было обещано, в программе используется $n + 2$ умножения и $2n + 1$ сложения.

Приём Кленшоу заметно уменьшает количество умножений. Суть этого приёма составляет разложение (2.2) коэффициентов $a[k]$, в котором правая часть соответствует однородной форме рекуррентного соотношения (2.1).

2.2. Встанем на более общую точку зрения. Она поможет нам выявить дополнительные возможности схемы Кленшоу.

Пусть имеется скалярный динамический процесс

$$v_k = c_k v_{k-1} + d_k v_{k-2}, \quad k = 1, 2, \dots, n, \quad (2.4)$$

с заданными начальными значениями v_0, v_{-1} . Определим стоимость траектории линейной функцией

$$P = \sum_{k=1}^n a_k v_k.$$

Требуется вычислить P как функцию начальных значений v_0, v_{-1} .

Воспользуемся идеей Кленшоу. Введём числовую последовательность $\{b_k\}$, исходя из условий

$$a_k = b_k - c_{k+1}b_{k+1} - d_{k+2}b_{k+2}, \quad k = n, n-1, \dots, 1; \quad b_{n+2} = b_{n+1} = 0. \quad (2.5)$$

Такую последовательность построить можно:

$$\begin{aligned} b_n &= a_n, \quad b_{n-1} = a_{n-1} + c_n b_n, \\ b_k &= a_k + c_{k+1} b_{k+1} + d_{k+2} b_{k+2}, \quad k = n-2, n-3, \dots, 1. \end{aligned} \quad (2.6)$$

На основании (2.5) запишем

$$\begin{aligned} P &= \sum_{k=1}^n (b_k - c_{k+1} b_{k+1} - d_{k+2} b_{k+2}) v_k = \\ &= \sum_{k=1}^n b_k v_k - \sum_{k=2}^{n+1} b_k c_k v_{k-1} - \sum_{k=3}^{n+2} b_k d_k v_{k-2} = \\ &= b_1 v_1 + b_2 v_2 - b_2 c_2 v_1 + \sum_{k=3}^n b_k (v_k - c_k v_{k-1} - d_k v_{k-2}). \end{aligned}$$

В силу (2.4) последняя сумма равна нулю. Значит,

$$\begin{aligned} P &= b_1 v_1 + b_2 (v_2 - c_2 v_1) = b_1 v_1 + b_2 d_2 v_0 = \\ &= b_1 (c_1 v_0 + d_1 v_{-1}) + b_2 d_2 v_0 = (b_1 c_1 + b_2 d_2) v_0 + b_1 d_1 v_{-1}. \end{aligned}$$

Если положить $a_0 = 0$ и расширить рекуррентное соотношение (2.6) до $k = 0$, то получим

$$P = b_0 v_0 + b_1 d_1 v_{-1}.$$

Приведём на псевдоязыке программу вычисления P как функции параметров v_0, v_{-1} :

```

a0 := 0; b1 := a_n;
b := a_{n-1} + c_n * b1;
for k := n - 2 downto 0 do begin
    b2 := b1; b1 := b;
    b := a_k + c_{k+1} * b1 + d_{k+2} * b2
end;
p := b * v_0 + b1 * d_1 * v_{-1}

```

Видим, что изменение начальных значений v_0, v_{-1} повлияет только на последнюю строку программы.

Коэффициенты a_k, c_k, d_k могут быть заданы явно в виде простой формулы или, в свою очередь, удовлетворять некоторым рекуррентным соотношениям. Это следует учитывать при составлении окончательного варианта программы.

3. Алгоритм Гёрцеля

Заметка Кленшоу [1] была опубликована в 1955 году. В 1958 году Гёрцель предложил быстрый алгоритм вычисления одной компоненты дискретного преобразования Фурье [2]. В этом разделе мы покажем, что алгоритм Гёрцеля является одной из реализаций схемы Кленшоу.

Напомним, что дискретное преобразование Фурье определяется формулой

$$X_k = \sum_{j=0}^{n-1} x_j \omega_n^{-kj}, \quad k = 0, 1, \dots, n-1. \quad (3.1)$$

Здесь $\omega_n = \exp(2\pi i/n)$, так что

$$\omega_n^{-kj} = \cos\left(\frac{2\pi kj}{n}\right) - i \sin\left(\frac{2\pi kj}{n}\right).$$

Рассмотрим задачу вычисления X_k при фиксированном k по заданным x_0, x_1, \dots, x_{n-1} (вообще говоря, комплексным).

Обозначим $\varphi = 2\pi k/n$, $c_j = \cos(j\varphi)$, $s_j = \sin(j\varphi)$. Тогда формулу (3.1) можно переписать так:

$$X_k = x_0 + \sum_{j=1}^{n-1} x_j c_j - i \sum_{j=1}^{n-1} x_j s_j. \quad (3.2)$$

Для одновременного вычисления сумм

$$A_k = \sum_{j=1}^{n-1} x_j c_j, \quad B_k = \sum_{j=1}^{n-1} x_j s_j$$

воспользуемся идеей Кленшоу. Для этого заметим, что при $j = 1, 2, \dots$

$$\begin{aligned} c_j + c_{j-2} &= 2 \cos(\varphi) c_{j-1}, & s_j + s_{j-2} &= 2 \cos(\varphi) s_{j-1}, \\ c_0 &= 1, \quad c_{-1} = \cos(\varphi); & s_0 &= 0, \quad s_{-1} = -\sin(\varphi). \end{aligned}$$

Таким образом, последовательности $\{c_j\}$ и $\{s_j\}$ удовлетворяют одному и тому же рекуррентному соотношению

$$v_j = 2 \cos(\varphi) v_{j-1} - v_{j-2}, \quad (3.3)$$

но разным начальным условиями. Формула (3.3) соответствует (2.4) при $c_j = 2 \cos(\varphi)$, $d_j = -1$. Для вычисления суммы

$$P = \sum_{j=1}^{n-1} x_j v_j$$

введём последовательность $\{b_j\}$, исходя из условий

$$x_j = b_j - 2 \cos(\varphi) b_{j+1} + b_{j+2}, \quad j = n-1, n-2, \dots, 1; \quad b_{n+1} = b_n = 0.$$

Здесь

$$\begin{aligned} b_n &= 0, \quad b_{n-1} = x_{n-1}, \\ b_j &= x_j + 2 \cos(\varphi) b_{j+1} - b_{j+2}, \quad j = n-2, n-3, \dots, 1. \end{aligned} \quad (3.4)$$

Тогда, как показано в п. 2.2,

$$P = (b_1 c_1 + b_2 d_2) v_0 + b_1 d_1 v_{-1} = (2 \cos(\varphi) b_1 - b_2) v_0 - b_1 v_{-1}.$$

В частности,

$$A_k = (2 \cos(\varphi) b_1 - b_2) - b_1 \cos(\varphi) = b_1 \cos(\varphi) - b_2, \quad B_k = b_1 \sin(\varphi).$$

Вспоминая (3.2), приходим к окончательному представлению

$$X_k = x_0 + A_k - i B_k = x_0 - b_2 + b_1 (\cos(\varphi) - i \sin(\varphi)). \quad (3.5)$$

Вычисление X_k по формуле (3.5) называется *алгоритмом Гёрцеля*. Мы получили этот алгоритм с помощью схемы Кленшоу.

Основным элементом алгоритма Гёрцеля является вычисление коэффициентов b_1, b_2 по формуле (3.4). Запишем программу вычисления указанных коэффициентов:

```

b := xn-1; b1 := 0;
a := 2 * cos(2 * π * k / n);
for j := n - 2 downto 1 do begin
    b2 := b1; b1 := b;
    b := xj + a * b1 - b2
end

```

После работы программы $b = b_1$, $b1 = b_2$. В программе используется $n - 2$ умножения на вещественное число a , $2(n - 2)$ сложения и лишь один раз вычисляется тригонометрическая функция!

4. Решение системы линейных уравнений с трёхдиагональной матрицей

Рассмотрим систему линейных уравнений

$$\begin{aligned} q_k x_{k-1} + p_k x_k + x_{k+1} &= f_k, \quad k = 1, 2, \dots, n, \\ x_0 &= c, \quad x_{n+1} = d. \end{aligned} \quad (4.1)$$

В отличие от (2.4) соотношения (4.1) являются неоднородными, а вместо начальных условий заданы краевые условия. Тем не менее, для решения системы (4.1) попытаемся применить схему Кленшоу. Введём «стоимость траектории»

$$P = \sum_{k=1}^{n+1} a_k x_k,$$

где $a_1 = a_2 = \dots = a_n = 0$, $a_{n+1} = 1$. Собственно, величина P нам известна, $P = d$. Приём Кленшоу побуждает нас ввести специальное представление для известных коэффициентов a_k .

Построим последовательность $\{b_k\}$, исходя из условий

$$a_k = q_{k+1}b_{k+1} + p_k b_k + b_{k-1}, \quad k = n+1, n, \dots, 1; \quad b_{n+2} = b_{n+1} = 0. \quad (4.2)$$

Такую последовательность построить можно:

$$b_n = 1, \quad b_{n-1} = -p_n; \quad b_{k-1} = -p_k b_k - q_{k+1} b_{k+1}, \quad k = n-1, n-2, \dots, 1.$$

Согласно (4.2) и (4.1)

$$\begin{aligned} P &= \sum_{k=1}^{n+1} (q_{k+1}b_{k+1} + p_k b_k + b_{k-1})x_k = \\ &= \sum_{k=2}^{n+2} b_k q_k x_{k-1} + \sum_{k=1}^{n+1} b_k p_k x_k + \sum_{k=0}^n b_k x_{k+1} = \\ &= b_1 p_1 x_1 + b_0 x_1 + b_1 x_2 + \sum_{k=2}^n b_k f_k. \end{aligned}$$

Поскольку $p_1 x_1 + x_2 = f_1 - q_1 x_0$, то

$$P = b_0 x_1 + b_1 (f_1 - q_1 x_0) + \sum_{k=2}^n b_k f_k = b_0 x_1 - b_1 q_1 x_0 + \sum_{k=1}^n b_k f_k.$$

Значит,

$$b_0 x_1 = d + b_1 q_1 c - \sum_{k=1}^n b_k f_k. \quad (4.3)$$

Эта формула является следствием (4.1). В частности, если $b_0 = 0$, а правая часть (4.3) отлична от нуля, то система (4.1) не имеет решения.

Предположим, что $b_0 \neq 0$. Тогда

$$x_1 = \left(d + b_1 q_1 c - \sum_{k=1}^n b_k f_k \right) / b_0.$$

На основании (4.1) по известным x_0, x_1 последовательно найдём x_2, x_3, \dots, x_n .

Запишем программу, реализующую описанный метод решения системы (4.1):

```

b := -pn; b1 := 1; s := fn;
for k := n - 1 downto 1 do begin
    s := s + b * fk;
    b2 := b1; b1 := b;
    b := -b1 * pk - b2 * qk+1
end;
x[0] := c; x[1] := (d + c * b1 * q1 - s) / b;
for k := 1 to n - 1 do
    x[k + 1] := fk - pk * x[k] - qk * x[k - 1];
x[n + 1] := d

```

После работы программы в массиве $x[0..n + 1]$ будет находиться решение системы (4.1).

В окончательный вариант программы нужно включить проверку условия $b_0 \neq 0$ в виде $|b_0| > eps$, где eps — малое положительное число.

Другой подход к решению системы (4.1) предложен в [3].

5. Свёртывание конечной цепной дроби

Рассмотрим последовательность цепных дробей

$$R_0(x) \equiv b_0, \quad R_1(x) = b_0 + \frac{a_1 x}{b_1}, \quad R_2(x) = b_0 + \frac{a_1 x}{b_1 + \frac{a_2 x}{b_2}}, \dots,$$

$$R_n(x) = b_0 + \frac{a_1 x}{b_1 + \frac{a_2 x}{b_2 + \dots + \frac{a_n x}{b_n}}}.$$

Каждую такую дробь можно представить в виде отношения алгебраических полиномов

$$R_k(x) = \frac{P_k(x)}{Q_k(x)}.$$

Например,

$$R_0(x) = \frac{b_0}{1}, \quad R_1(x) = \frac{b_0 b_1 + a_1 x}{b_1}, \quad R_2(x) = \frac{b_0 (b_1 b_2 + a_2 x) + b_2 a_1 x}{b_1 b_2 + a_2 x}.$$

Поставим задачу: вычислить коэффициенты полиномов $P_n(x)$ и $Q_n(x)$.

Как известно [4, 5], последовательности $\{P_k(x)\}$ и $\{Q_k(x)\}$ удовлетворяют рекуррентным соотношениям: при $k = 1, 2, \dots, n$

$$\begin{aligned} P_k(x) &= b_k P_{k-1}(x) + a_k x P_{k-2}(x), \\ Q_k(x) &= b_k Q_{k-1}(x) + a_k x Q_{k-2}(x), \\ P_0(x) &\equiv b_0, \quad Q_0(x) \equiv 1, \quad P_{-1}(x) \equiv 1, \quad Q_{-1}(x) \equiv 0. \end{aligned}$$

Проследим за степенями полиномов $P_k(x)$ и $Q_k(x)$ (табл. 2).

Таблица 2

k	0	1	2	3	4	5	...	n
степень P_k	0	1	1	2	2	3	...	$\lfloor (n+1)/2 \rfloor$
степень Q_k	0	0	1	1	2	2	...	$\lfloor n/2 \rfloor$

В программе коэффициенты полиномов P_k , Q_k будут размещены в массивах $p, q[0..\lfloor (n+1)/2 \rfloor]$.

Отметим, что полиномы P_k , Q_k удовлетворяют одному и тому же рекуррентному соотношению

$$v_k = b_k v_{k-1} + a_k x v_{k-2}, \quad k = 1, 2, \dots, n,$$

при разных начальных значениях v_0, v_{-1} . Выразим v_n через v_0 и v_{-1} . Для этого воспользуемся схемой Кленшоу.

Имеем

$$v_n = \sum_{k=0}^n c_k v_k,$$

где $c_0 = c_1 = \dots = c_{n-1} = 0$, $c_n = 1$. Представим c_k в виде

$$c_k = g_k - b_{k+1} g_{k+1} - a_{k+2} x g_{k+2}, \quad k = n, n-1, \dots, 0; \quad g_{n+2} = g_{n+1} = 0.$$

Последовательность $\{g_k\}$ построить можно:

$$g_n = 1, \quad g_{n-1} = b_n; \quad g_k = b_{k+1} g_{k+1} + a_{k+2} x g_{k+2}, \quad k = n-2, n-3, \dots, 0. \quad (5.1)$$

Здесь $g_k = g_k(x)$ — алгебраический полином. Теперь запишем

$$\begin{aligned} v_n &= \sum_{k=0}^n (g_k - b_{k+1} g_{k+1} - a_{k+2} x g_{k+2}) v_k = \\ &= \sum_{k=0}^n g_k v_k - \sum_{k=1}^{n+1} g_k b_k v_{k-1} - \sum_{k=2}^{n+2} g_k a_k x v_{k-2} = \end{aligned}$$

$$= g_0 v_0 + g_1 v_1 - g_1 b_1 v_0 = g_0 v_0 + g_1 a_1 x v_{-1}.$$

Если положить $v_0 = b_0$, $v_{-1} = 1$, то получим

$$P_n(x) = b_0 g_0(x) + a_1 x g_1(x). \quad (5.2)$$

Если положить $v_0 = 1$, $v_{-1} = 0$, то получим $Q_n(x) = g_0(x)$. Правая часть (5.2) соответствует правой части (5.1) при $k = -1$. Перепишем (5.1) в виде

$$g_n = 1, \quad g_{n-1} = b_n; \quad g_{k-1} = b_k g_k + a_{k+1} x g_{k+1}, \quad k = n-1, n-2, \dots, 0. \quad (5.3)$$

Тогда $P_n(x) = g_{-1}(x)$, $Q_n(x) = g_0(x)$. Таким образом, задача вычисления коэффициентов полиномов P_n , Q_n сведена к задаче вычисления коэффициентов полиномов g_{-1}, g_0 по формуле (5.3).

Отметим, что степень полинома g_k не превосходит $r_k = \lfloor (n-k)/2 \rfloor$. Очевидно, что

$$r_{k-1} = r_{k+1} + 1, \quad k = n-1, n-2, \dots, 0; \quad r_n = r_{n-1} = 0.$$

В табл. 3 приведены значения r_k .

Таблица 3

k	n	$n-1$	$n-2$	$n-3$	\dots	0	-1
r_k	0	0	1	1	\dots	$\lfloor n/2 \rfloor$	$\lfloor (n+1)/2 \rfloor$

Пусть

$$g_k(x) = \sum_{j=0}^{r_k} \xi_{kj} x^j.$$

Из (5.3) выведем рекуррентное соотношение для коэффициентов ξ_{kj} . Имеем

$$\sum_{j=0}^{r_{k-1}} \xi_{k-1,j} x^j = b_k \sum_{j=0}^{r_k} \xi_{kj} x^j + a_{k+1} \sum_{j=1}^{r_{k-1}} \xi_{k+1,j-1} x^j.$$

Отсюда следует, что при $k = n-1, n-2, \dots, 0$

$$\begin{aligned} \xi_{k-1,0} &= b_k \xi_{k0}; \quad \xi_{k-1,j} = b_k \xi_{kj} + a_{k+1} \xi_{k+1,j-1}, \quad j = 1, 2, \dots, r_k; \\ \xi_{k-1,r_{k-1}} &= a_{k+1} \xi_{k+1,r_{k-1}-1}, \quad \text{если } r_k < r_{k-1}. \end{aligned} \quad (5.4)$$

При $r_k < r_{k-1}$ можно положить $\xi_{k,r_{k-1}} = 0$ и использовать рекуррентное соотношение для $\xi_{k-1,j}$ при $j = 1, 2, \dots, r_{k-1}$. К (5.4) нужно добавить начальные условия $\xi_{n0} = 1$, $\xi_{n-1,0} = b_n$.

Матрица коэффициентов $\{\xi_{kj}\}$ заполняется строка за строкой снизу вверх, как показано в табл. 4 при $n = 4$, $r_{-1} = 2$.

Таблица 4

$k \backslash j$	0	1	2
-1	$\xi_{-1,0}$	$\xi_{-1,1}$	$\xi_{-1,2}$
0	ξ_{00}	ξ_{01}	ξ_{02}
1	ξ_{10}	ξ_{11}	0
$p_{\text{нов}}$	2	ξ_{20}	ξ_{21}
p	3	ξ_{30}	0
q	4	ξ_{40}	

Для формирования строк будут использоваться два массива $p, q[0.. \lfloor \frac{n+1}{2} \rfloor]$.

Приведём соответствующую программу:

```

 $p[0] := b_n; q[0] := 1;$ 
 $r := 0; r1 := 0;$ 
for  $k := n - 1$  downto 0 do begin
   $r2 := r1; r1 := r; r := r2 + 1;$ 
  if  $r1 < r$  then  $p[r] := 0;$ 
   $u := b_k; v := a_{k+1};$ 
  for  $j := r$  downto 1 do begin
     $d := p[j];$ 
     $p[j] := u * d + v * q[j - 1];$ 
     $q[j] := d$ 
  end;
   $d := p[0]; p[0] := u * d; q[0] := d$ 
end

```

После работы программы $r = \lfloor (n + 1)/2 \rfloor$ и

$$P_n(x) = \sum_{j=0}^r p[j]x^j, \quad Q_n(x) = \sum_{j=0}^r q[j]x^j.$$

6. Заключительные замечания

Мы рассмотрели схему Кленшоу применительно к линейным рекуррентным соотношениям 2-го порядка. Нетрудно понять, как она будет выглядеть в случае линейных рекуррентных соотношений 3-го, 4-го и более высоких порядков.

Наряду со схемой Кленшоу существуют и другие регулярные приёмы, используемые при составлении эффектных программ. Эти приёмы основаны на

идеях из различных разделов дискретной математики, таких как комбинаторика, теория графов, динамическое программирование и пр. [6, 7, 8].

В заключение приведём 12 задач, допускающих красивые решения. Много других задач подобного рода имеются в [9, 10].

Задачи

1. Для объема k -мерного шара радиуса r справедлива формула

$$v_k = \frac{(2r)^k}{k!!} \left(\frac{\pi}{2}\right)^{\lfloor k/2 \rfloor}, \quad k = 1, 2, \dots$$

Вычислить v_n .

2. Вычислить значение производной n -го порядка функции

$$f(x) = \exp(-x^2/2)$$

в точке x .

3. Вычислить интеграл

$$c_n = \int_0^\varphi \sin^n x \, dx$$

при фиксированном φ и $n \geq 1$.

4. Алгебраический полином

$$P(x) = (1 + x + x^2 + \dots + x^n)^r$$

представить в виде

$$P(x) = \sum_{k=0}^{rn} a_k x^k.$$

Коэффициенты a_0, a_1, \dots, a_{rn} записать в массив $a[0..rn]$.

5. Рассмотрим алгебраический полином в форме Бернштейна

$$B(x) = \sum_{k=0}^n y[k] C_n^k x^k (1-x)^{n-k}. \quad (6.1)$$

Вычислить $B(x)$ в точке x .

6. Полином (6.1) представить в виде

$$B(x) = \sum_{k=0}^n b_k x^k.$$

Коэффициенты b_0, b_1, \dots, b_n записать в исходный массив $y[0..n]$. (Такие преобразования называются *преобразованиями на месте*.)

7. Алгебраический полином

$$B(x) = \sum_{k=0}^n y[k] x^k$$

представить в форме Бернштейна (6.1).

8. Полиномы Бернулли $Q_k(x)$ определяются с помощью рекуррентного соотношения

$$Q'_k(x) = kQ_{k-1}(x), \int_0^1 Q_k(x) dx = 0, k = 1, 2, \dots; \quad Q_0(x) \equiv 1.$$

Вычислить коэффициенты полинома $Q_n(x)$.

9. Рекуррентное соотношение

$$P_k(x) = \frac{d}{dx} [x(1-x)P_{k-1}(x)], \quad k = 1, 2, \dots; \quad P_0(x) \equiv 1$$

определяет так называемые *логистические полиномы*. Вычислить коэффициенты $P_n(x)$.

10. Числа Стирлинга первого рода вводятся как коэффициенты разложения

$$x(x-1)\dots(x-n+1) = \sum_{k=1}^n (-1)^{n-k} a_{nk} x^k.$$

Вычислить $a_{n1}, a_{n2}, \dots, a_{nn}$.

11. Числа Стирлинга второго рода вводятся как коэффициенты разложения

$$x^n = \sum_{k=1}^n b_{nk} x(x-1)\dots(x-n+1).$$

Вычислить $b_{n1}, b_{n2}, \dots, b_{nn}$.

12. Вычислить сумму

$$S = \sum_{j=1}^n (j^3 + 3j^2 + 2j) a[j],$$

используя только сложения (в количестве $4n - 1$ операций).

ЛИТЕРАТУРА

1. *Clenshaw C.* A note on the summation of Chebyshev series // Math. Tabl. Aids. Comput. 1955. V. 9. P. 118–120.
2. *Goertzel G.* An algorithm for the evaluation of finite trigonometric series // Amer. Math. Monthly. 1958. V. 65. P. 34–35.
3. *Mikloško J.* The numerical computation of three-term recurrence relations and the tridiagonal system of linear equations by the method of shooting // Журн. вычисл. мат. и матем. физ. 1974. Т. 14. № 6. С. 1371–1377.
4. *Хинчин А.Я.* Цепные дроби. Изд. 4-е. М.: Наука, 1978. 112 с.
5. *Скоробогатько В.Я.* Теория ветвящихся цепных дробей и ее применение в вычислительной математике. М.: Наука, 1983. 312 с.
6. *Романовский И.В.* Дискретный анализ. Изд. 3-е. СПб: Невский диалект, 2004. 320 с.
7. *Кормен Т., Лейзерсон Ч., Ривест Р.* Алгоритмы: построение и анализ. Пер. с англ.. М.: МЦНМО, 2002. 960 с.
8. *Кнут Д.Э.* Искусство программирования. Т. 2. Пер. с англ. Изд. 3-е. М.-СПб-Киев: Вильямс, 2000. 828 с.
9. *Малозёмов В.Н., Певный А.Б.* Рекуррентные вычисления. Л.: Изд-во ЛГУ, 1976. 56 с.
10. *Воронин А.В., Кузнецов В.А., Корзун Д.Ж.* Командные чемпионаты по программированию: организация, задачи и решения. Петрозаводск: Изд-во ПетрГУ, 2001. 268 с.

ЧАСТОТНЫЙ КОНВЕРТЕР

В. Н. Малозёмов С. В. Рыбин

24 мая 2005 г.

1°. Пусть N_1, N_2 – натуральные числа, отличные от единицы, причём $N_1 \neq N_2$. Обозначим $n = \min\{N_1, N_2\}$, $N = N_1 N_2$.

Возьмем сигнал $x \in \mathbb{C}_{N_1}$ со спектром $X = \mathcal{F}_{N_1}(x)$ и преобразуем его в сигнал $y \in \mathbb{C}_{N_2}$, спектр которого $Y = \mathcal{F}_{N_2}(y)$ определяется формулой

$$Y(k) = \begin{cases} X(k) & \text{при } k \in 0 : n-1, \\ 0 & \text{при } k \in n : N_2-1. \end{cases}$$

Сигнал y можно записать в явном виде

$$y(j) = \frac{1}{N_2} \sum_{k=0}^{n-1} X(k) \omega_{N_2}^{kj}, \quad j \in \mathbb{Z}. \quad (1)$$

Оператор $\mathcal{K} : \mathbb{C}_{N_1} \rightarrow \mathbb{C}_{N_2}$, сопоставляющий сигналу $x \in \mathbb{C}_{N_1}$ сигнал $y \in \mathbb{C}_{N_2}$ вида (1), называется *частотным конвертером*. Покажем, как реализовать оператор \mathcal{K} во временной области.

2°. Реализация состоит из трех этапов.

1) **Растяжение.** Растянем сигнал $x \in \mathbb{C}_{N_1}$ до сигнала $\hat{x} \in \mathbb{C}_N$ по правилу

$$\hat{x}(j) = \begin{cases} x(j/N_2), & \text{если } j \text{ делится на } N_2, \\ 0 & \text{при остальных } j \in \mathbb{Z}. \end{cases}$$

2) **Фильтрация.** Отфильтруем сигнал \hat{x} с помощью фильтра \mathcal{L} , импульсная характеристика h которого имеет спектр $H = \mathcal{F}_N(h)$ вида

$$H(k) = \begin{cases} N_1 & \text{при } k \in 0 : n-1, \\ 0 & \text{при } k \in n : N-1. \end{cases}$$

Получим сигнал $\hat{y} = \mathcal{L}(\hat{x}) = h * \hat{x}$.

3) **Прореживание.** Выделим сигнал $y(j) = \hat{y}(jN_1)$, принадлежащий пространству \mathbb{C}_{N_2} .

Проверим, что сигнал y допускает представление (1).

3°. Обозначим $\hat{X} = \mathcal{F}_N(\hat{x})$. Согласно определению ДПФ

$$\hat{X}(k) = \sum_{l=0}^{N_1-1} x(l) \omega_N^{-klN_2} = \sum_{l=0}^{N_1-1} x(l) \omega_{N_1}^{-kl} = X(k), \quad k \in \mathbb{Z}.$$

По теореме о циклической свертке $\hat{Y} := \mathcal{F}_N(\hat{y}) = H\hat{X}$, так что

$$\hat{Y}(k) = \begin{cases} N_1 X(k) & \text{при } k \in 0 : n-1, \\ 0 & \text{при } k \in n : N-1. \end{cases} \quad (2)$$

Теперь выясним, как связаны спектры сигнала \hat{y} и прореженного сигнала $y(j) = \hat{y}(jN_1)$. Запишем

$$\begin{aligned} Y(k) &= \sum_{j=0}^{N_2-1} y(j) \omega_{N_2}^{-kj} = \sum_{j=0}^{N_2-1} \hat{y}(jN_1) \omega_{N_2N_1}^{-kjN_1} = \\ &= \sum_{j'=0}^{N-1} \hat{y}(j') \omega_N^{-kj'} \delta_{N_1}(j') = \sum_{j=0}^{N-1} \hat{y}(j) \omega_N^{-kj} \left\{ \frac{1}{N_1} \sum_{p=0}^{N_1-1} \omega_{N_1N_2}^{-pjN_2} \right\} = \\ &= \frac{1}{N_1} \sum_{p=0}^{N_1-1} \sum_{j=0}^{N-1} \hat{y}(j) \omega_N^{-j(k+pN_2)} = \frac{1}{N_1} \sum_{p=0}^{N_1-1} \hat{Y}(k + pN_2). \end{aligned}$$

Согласно (2) в последней сумме при $k \in 0 : N_2 - 1$ отлично от нуля лишь одно слагаемое, соответствующее $p = 0$. Значит,

$$Y(k) = \frac{1}{N_1} \hat{Y}(k) = \begin{cases} X(k) & \text{при } k \in 0 : n-1, \\ 0 & \text{при } k \in n : N_2-1. \end{cases}$$

Представление (1) следует из формулы обращения для ДПФ.

4°. Обратимся к фильтру \mathcal{L} с импульсной характеристикой

$$h(j) = \sum_{k=0}^{N-1} H(k) \omega_N^{kj} = \frac{1}{N_2} \sum_{k=0}^{n-1} \omega_N^{kj}.$$

Обозначим $m = \max\{N_1, N_2\}$, так что $N = mn$. Очевидно, что $h(0) = n/N_2$ и

$$h(j) = \frac{1 - \omega_N^{nj}}{N_2(1 - \omega_N^j)} = \frac{1 - \omega_m^j}{N_2(1 - \omega_N^j)}, \quad j \in 1 : N-1. \quad (3)$$

Упростим формулу (3). Поскольку

$$1 - \omega_m^j = (1 - \cos(2\pi j/m)) - i \sin(2\pi j/m) =$$

$$= -2i \sin(\pi j/m) [\cos(\pi j/m) + i \sin(\pi j/m)] = -2i \sin(\pi j/m) \omega_{2m}^j$$

и аналогично

$$1 - \omega_N^j = -2i \sin(\pi j/N) \omega_{2N}^j,$$

то при $j \in 1 : N - 1$

$$N_2 h(j) = \frac{\sin(\pi j/m) \omega_{2m}^j}{\sin(\pi j/N) \omega_{2N}^j} = \frac{\sin(\pi j/m)}{\sin(\pi j/N)} \omega_{2N}^{(n-1)j}.$$

Окончательно получаем

$$h(j) = \begin{cases} n/N_2 & \text{при } j = 0, \\ \frac{\sin(\pi j/m)}{N_2 \sin(\pi j/N)} \omega_{2N}^{(n-1)j} & \text{при } j \in 1 : N - 1. \end{cases}$$

ЛИТЕРАТУРА

1. Куприянов М.С., Матюшкин Б.Д. *Цифровая обработка сигналов*. СПб.: Политехника, 2002. Часть 2, глава 6.
2. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа* СПб.: НИИММ, 2003. Часть 1.

ПОДСЧЁТ КОЛИЧЕСТВА АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ ПРИ ВЫЧИСЛЕНИИ БПФ

В. Н. Малозёмов

20 сентября 2005 г.

1°. Рассмотрим сначала случай $N = pq$. Пусть $x \in \mathbb{C}_N$. Положим

$$x_r(s) = x(r + ps), \quad s \in 0 : q - 1, \quad r \in 0 : p - 1.$$

Имеем

$$\begin{aligned} X(k) &= \sum_{j=0}^{N-1} x(j) \omega_N^{-kj} = \sum_{r=0}^{p-1} \sum_{s=0}^{q-1} x(r + ps) \omega_N^{-k(r+ps)} = \\ &= \sum_{r=0}^{p-1} \omega_N^{-kr} \sum_{s=0}^{q-1} x_r(s) \omega_q^{-ks}. \end{aligned}$$

Обозначим

$$X_r(k) = \sum_{s=0}^{q-1} x_r(s) \omega_q^{-ks}.$$

Тогда

$$X(k) = \sum_{r=0}^{p-1} \omega_N^{-kr} X_r(k).$$

Представим индекс k в виде $k = \alpha + \beta q$. В силу q -периодичности спектров X_r получим

$$\begin{aligned} X(\alpha + \beta q) &= \sum_{r=0}^{p-1} \omega_N^{-(\alpha + \beta q)r} X_r(\alpha + \beta q) = \sum_{r=0}^{p-1} \left(\omega_N^{-\alpha r} X_r(\alpha) \right) \omega_p^{-\beta r}, \\ &\quad \alpha \in 0 : q - 1, \quad \beta \in 0 : p - 1. \end{aligned}$$

Приходим к следующей схеме вычисления спектра X сигнала $x \in \mathbb{C}_N$.

- 1) Сигнал $x(j)$ разбить на p серий $x_r(s) = x(r+ps)$, $s \in 0 : q-1$, $r \in 0 : p-1$:

$$\begin{array}{ccccccc} x(0), & x(p), & x(2p), & \dots, & x((q-1)p), \\ x(1), & x(p+1), & x(2p+1), & \dots, & x((q-1)p+1), \\ \dots & \dots & \dots & \dots & \dots \\ x(p-1), & x(2p-1), & x(3p-1), & \dots, & x(qp-1). \end{array}$$

- 2) Вычислить спектры X_r каждой серии (длины q):

$$\begin{array}{ccccccc} X_0(0), & X_0(1), & \dots, & X_0(q-1), \\ X_1(0), & X_1(1), & \dots, & X_1(q-1), \\ \dots & \dots & \dots & \dots \\ X_{p-1}(0), & X_{p-1}(1), & \dots, & X_{p-1}(q-1). \end{array}$$

- 3) Преобразовать сформированную матрицу (по столбцам):

$$\tilde{X}_r(\alpha) = (\omega_N^{-\alpha})^r X_r(\alpha), \quad r \in 0 : p-1, \quad \alpha \in 0 : q-1.$$

- 4) Вычислить спектры q новых столбцов (каждый длины p):

$$\begin{array}{ccccccc} X(0), & X(1), & \dots, & X(q-1), \\ X(q), & X(q+1), & \dots, & X(2q-1), \\ \dots & \dots & \dots & \dots \\ X((p-1)q), & X((p-1)q+1), & \dots, & X(pq-1). \end{array}$$

- 5) Для получения спектра X сшить строки последней матрицы.

2°. Сколько умножений в таком алгоритме?

Для вычисления ДПФ длины p необходимо произвести $(p-1)^2$ умножений (учесть, что $\omega_p^{-\beta r} = 1$ при $\beta = 0$ и при $r = 0$). Значит, пункт 4 требует $q(p-1)^2$ умножений. По аналогичной причине пункт 3 требует $(q-1)(p-1)$ умножений. На пункты 3 и 4 приходится $q(p-1)^2 + (q-1)(p-1) = (pq-1)(p-1)$ умножений.

Обозначим через $\psi(N)$ количество комплексных умножений, необходимых для вычисления ДПФ длины N . Согласно описанию алгоритма получаем рекуррентное соотношение

$$\psi(pq) = p\psi(q) + (pq-1)(p-1). \quad (1)$$

3°. Пусть теперь $N = n_1 n_2 \dots n_s$. Положим $p = n_1$, $q = n_2 n_3 \dots n_s$. Согласно (1)

$$\psi(n_1 n_2 \dots n_s) = (N - 1)(n_1 - 1) + n_1 \psi(n_2 n_3 \dots n_s).$$

В свою очередь

$$\psi(n_2 n_3 \dots n_s) = (n_2 n_3 \dots n_s - 1)(n_2 - 1) + n_2 \psi(n_3 \dots n_s).$$

Значит,

$$\psi(N) = (N - 1)(n_1 - 1) + (N - n_1)(n_2 - 1) + n_1 n_2 \psi(n_3 \dots n_s).$$

Сделаем ещё один шаг:

$$\begin{aligned} \psi(n_3 \dots n_s) &= (n_3 \dots n_s - 1)(n_3 - 1) + n_3 \psi(n_4 \dots n_s); \\ \psi(N) &= (N - 1)(n_1 - 1) + (N - n_1)(n_2 - 1) + (N - n_1 n_2)(n_3 - 1) + \\ &\quad + n_1 n_2 n_3 \psi(n_4 \dots n_s). \end{aligned}$$

Окончательно

$$\begin{aligned} \psi(N) &= (N - 1)(n_1 - 1) + \sum_{k=2}^{s-2} (N - n_1 n_2 \dots n_{k-1})(n_k - 1) + \\ &\quad + n_1 n_2 \dots n_{s-2} \psi(n_{s-1} n_s). \end{aligned}$$

Поскольку $\psi(n_{s-1} n_s) = (n_{s-1} n_s - 1)(n_{s-1} - 1) + n_{s-1} (n_s - 1)^2$, то

$$\psi(N) = (N - 1)(n_1 - 1) + \sum_{k=2}^s (N - n_1 n_2 \dots n_{k-1})(n_k - 1).$$

Эту формулу можно переписать в виде

$$\psi(N) = \sum_{k=1}^s (N - n_0 n_1 n_2 \dots n_{k-1})(n_k - 1), \quad (2)$$

где положено $n_0 = 1$.

При $N = 2^s$ из (2) следует, что

$$\psi(N) = \sum_{k=1}^s (N - 2^{k-1}) = Ns - N + 1 = N \log_2 N - N + 1. \quad (3)$$

4°. Разумеется, величина $\psi(N)$ является оценкой сверху количества комплексных умножений при фиксированном правиле их подсчёта. При $N = 2^s$ оценку (3) можно улучшить. Для этого отметим, что при $p = 2$ в пункте 4 алгоритма вообще не производится умножений. Рекуррентное соотношение (1) уточняется:

$$\psi(2q) = 2\psi(q) + q - 1. \quad (4)$$

Согласно (4) получаем

$$\begin{aligned} \psi(2^s) &= 2^{s-1} - 1 + 2\psi(2^{s-1}) = 2^{s-1} - 1 + 2[2^{s-2} - 1 + 2\psi(2^{s-2})] = \\ &= 2 \cdot 2^{s-1} - (1 + 2) + 2^2\psi(2^{s-2}). \end{aligned}$$

По той же причине $\psi(2^{s-2}) = 2^{s-3} - 1 + 2\psi(2^{s-3})$, так что

$$\psi(2^s) = 3 \cdot 2^{s-1} - (1 + 2 + 2^2) + 2^3\psi(2^{s-3}).$$

Окончательно при $N = 2^s$

$$\begin{aligned} \psi(N) &= (s-1)2^{s-1} - (1 + 2 + \dots + 2^{s-2}) + 2^{s-1}\psi(2) = \\ &= (s-1)2^{s-1} - (2^{s-1} - 1) = s2^{s-1} - 2^s + 1 = \\ &= \frac{1}{2}N \log_2 N - N + 1. \end{aligned} \quad (5)$$

Мы воспользовались тем, что $\psi(2) = 0$.

В [1] указаны более грубые, чем (2) и (5), оценки для $\psi(N)$.

5°. Подсчитаем количество сложений в описанном алгоритме. Для вычисления одного ДПФ длины p необходимо произвести $p(p-1)$ сложений. Значит, пункт 4 требует $qp(p-1)$ сложений. Обозначив через $\eta(N)$ количество комплексных сложений, необходимых для вычисления ДПФ длины N , придём к рекуррентному соотношению

$$\eta(pq) = p\eta(q) + qp(p-1).$$

При $N = n_1n_2 \dots n_s$ последовательно получаем

$$\begin{aligned} \eta(N) &= N(n_1 - 1) + n_1\eta(n_2n_3 \dots n_s) = N(n_1 - 1) + n_1[n_2n_3 \dots n_s(n_2 - 1) + \\ &+ n_2\eta(n_3 \dots n_s)] = N(n_1 - 1) + N(n_2 - 1) + n_1n_2\eta(n_3 \dots n_s). \end{aligned}$$

Окончательно

$$\eta(N) = \sum_{k=1}^{s-1} N(n_k - 1) + n_1n_2 \dots n_{s-1}\eta(n_s).$$

Поскольку $\eta(n_s) = n_s(n_s - 1)$, то

$$\eta(N) = N \sum_{k=1}^s (n_k - 1). \quad (6)$$

При $N = 2^s$ из (6) следует формула

$$\eta(N) = Ns = N \log_2 N. \quad (7)$$

6°. Строго говоря, алгоритм п. 1° приводит к таким рекуррентным соотношениям:

$$\begin{aligned} \psi(pq) &= p\psi(q) + q\psi(p) + (p-1)(q-1), \\ \eta(pq) &= p\eta(q) + q\eta(p). \end{aligned} \quad (8)$$

Нас интересует случай $p = 4$. Напомним алгоритм БПФ при $N = 4$ [2]:

$$\begin{aligned} s(1) &= x(0) + x(2), \quad s(3) = x(1) + x(3), \quad s(5) = s(1) + s(3), \\ s(2) &= x(0) - x(2), \quad s(4) = x(1) - x(3), \quad s(6) = s(1) - s(3), \\ m(1) &= i s(4), \\ s(7) &= s(2) - m(1), \quad s(8) = s(2) + m(1), \\ X(0) &= s(5), \quad X(1) = s(7), \quad X(2) = s(6), \quad X(3) = s(8). \end{aligned}$$

Умножение на i мы не будем считать арифметической операцией, поскольку это умножение сводится к пересылке вещественной части на место мнимой, а мнимой (после изменения знака) — на место вещественной. Таким образом,

$$\psi(4) = 0, \quad \eta(4) = 8. \quad (9)$$

Согласно (8) и (9)

$$\begin{aligned} \psi(4q) &= 4\psi(q) + 3q - 3, \\ \eta(4q) &= 4\eta(q) + 8q. \end{aligned} \quad (10)$$

При $N = 4^t$ последовательно получаем

$$\begin{aligned} \psi(4^t) &= 3 \cdot 4^{t-1} - 3 + 4 [3 \cdot 4^{t-2} - 3 + 4\psi(4^{t-2})] = \\ &= 2(3 \cdot 4^{t-1}) - 3(1 + 4) + 4^2 [3 \cdot 4^{t-3} - 3 + 4\psi(4^{t-3})] = \\ &= 3(3 \cdot 4^{t-1}) - 3(1 + 4 + 4^2) + 4^3 \psi(4^{t-3}) = \dots = \\ &= (t-1)(3 \cdot 4^{t-1}) - 3(1 + 4 + 4^2 + \dots + 4^{t-2}) + 4^{t-1} \psi(4) = \\ &= (3t-3)4^{t-1} - (4^{t-1} - 1) = 3t4^{t-1} - 4^t + 1. \end{aligned}$$

Поскольку $N = 4^t = 2^{2t}$, то $2t = \log_2 N$. Приходим к формуле

$$\psi(N) = \frac{3}{8} N \log_2 N - N + 1. \quad (11)$$

Сравнение (5) и (11) показывает, что при $N = 4^t = 2^{2t}$ последовательное применение алгоритма БПФ с основанием $p = 4$ более эффективно по количеству комплексных умножений, чем последовательное применение алгоритма БПФ с основанием $p = 2$.

Обратимся к подсчёту количества комплексных сложений. Согласно (10) имеем

$$\begin{aligned}\eta(4^t) &= 8 \cdot 4^{t-1} + 4 [8 \cdot 4^{t-2} + 4 \eta(4^{t-2})] = \\ &= 2(2 \cdot 4^t) + 4^2 [8 \cdot 4^{t-3} + 4 \eta(4^{t-3})] = 3(2 \cdot 4^t) + 4^3 \eta(4^{t-3}) = \\ &= \dots = (t-1)(2 \cdot 4^t) + 4^{t-1} \eta(4) = 2t \cdot 4^t,\end{aligned}$$

т. е. при $N = 4^t$

$$\eta(N) = N \log_2 N. \quad (12)$$

Сравнивая (7) и (12), заключаем, что при $N = 4^t = 2^{2t}$ количество комплексных сложений одинаково как при последовательном применении алгоритма БПФ с основанием $p = 2$, так и при последовательном применении алгоритма БПФ с основанием $p = 4$.

ЛИТЕРАТУРА

1. Henrici P. *Fast Fourier methods in computational complex analysis* // SIAM Rev. 1979. V. 21. N. 4. P. 481–527.
2. Малозёмов В. Н., Просеков О. В. *О быстром преобразовании Фурье малых порядков* // Вестник СПбГУ. Сер. 1. 2003. Вып. 1 (№ 1). С. 36–45.

БЫСТРОЕ ВЫЧИСЛЕНИЕ ЦИКЛИЧЕСКИХ СВЁРТОК МАЛЫХ ПОРЯДКОВ

В. Н. Малозёмов

О. В. Просеков

18 октября 2005 г.

Напомним, что циклической свёрткой сигналов x, h из \mathbb{C}_N называется сигнал $u = x * h$ с отсчётами

$$\begin{aligned} u_j &= \sum_{k=0}^{N-1} x_k h_{j-k} = \\ &= \sum_{k=0}^j x_k h_{j-k} + \sum_{k=j+1}^{N-1} x_k h_{N+j-k}, \quad j \in 0 : N-1. \end{aligned} \tag{1}$$

Если ввести правоциркулянтную матрицу

$$H_N = \begin{bmatrix} h_0 & h_{N-1} & h_{N-2} & \dots & h_1 \\ h_1 & h_0 & h_{N-1} & \dots & h_2 \\ \dots & \dots & \dots & \dots & \dots \\ h_{N-1} & h_{N-2} & h_{N-3} & \dots & h_0 \end{bmatrix},$$

то формулу (1) можно переписать так:

$$u = H_N x.$$

Рассмотрим вопрос о быстром вычислении циклической свёртки при $N = 2, 3, 4, 5$ на основе факторизации матрицы H_N . Нам потребуется одно элементарное свойство матриц: в предположении, что D — квадратная матрица и определено произведение CGA , справедливо равенство

$$\begin{bmatrix} D & 0 \\ 0 & CGA \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & G \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & A \end{bmatrix}.$$

1°. Начнём с $N = 2$. Имеем

$$\begin{aligned} u_0 &= h_0 x_0 + h_1 x_1, \\ u_1 &= h_1 x_0 + h_0 x_1. \end{aligned}$$

Поскольку

$$\begin{aligned} u_0 + u_1 &= (h_0 + h_1)(x_0 + x_1), \\ u_0 - u_1 &= (h_0 - h_1)(x_0 - x_1), \end{aligned}$$

то

$$\begin{aligned} u_0 &= \frac{1}{2}[(h_0 + h_1)(x_0 + x_1) + (h_0 - h_1)(x_0 - x_1)], \\ u_1 &= \frac{1}{2}[(h_0 + h_1)(x_0 + x_1) - (h_0 - h_1)(x_0 - x_1)]. \end{aligned}$$

Последнюю формулу можно переписать в виде

$$\begin{aligned} \begin{bmatrix} u_0 \\ u_1 \end{bmatrix} &= \frac{1}{2} \begin{bmatrix} h_0 + h_1 & h_0 - h_1 \\ h_0 + h_1 & -(h_0 - h_1) \end{bmatrix} \begin{bmatrix} x_0 + x_1 \\ x_0 - x_1 \end{bmatrix} = \\ &= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} h_0 + h_1 & 0 \\ 0 & h_0 - h_1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}. \end{aligned} \quad (2)$$

По существу, получена факторизация матрицы H_2 :

$$\begin{bmatrix} h_0 & h_1 \\ h_1 & h_0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} h_0 + h_1 & 0 \\ 0 & h_0 - h_1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (3)$$

или, в компактной записи,

$$H_2 = C_2 G_2 A_2,$$

где $A_2 = C_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ и G_2 — диагональная матрица с диагональными элементами

$$\begin{bmatrix} g_0 \\ g_1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \end{bmatrix}.$$

Элементы матриц A_2 , C_2 , G_2 являются константами. Вычисления по формуле (2) требуют 2 умножения и 4 сложения.

2°. Попутно разберёмся с факторизацией матрицы $\begin{bmatrix} h_0 & h_2 \\ h_1 & h_0 \end{bmatrix}$. Пусть

$$\begin{aligned} v_0 &= h_0 x_0 + h_2 x_1, \\ v_1 &= h_1 x_0 + h_0 x_1. \end{aligned}$$

Поскольку

$$\begin{aligned} v_0 &= (h_2 - h_0) x_1 + h_0 (x_0 + x_1), \\ v_1 &= (h_1 - h_0) x_0 + h_0 (x_0 + x_1), \end{aligned}$$

то

$$\begin{aligned} \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} &= \begin{bmatrix} h_2 - h_0 & 0 & h_0 \\ 0 & h_1 - h_0 & h_0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_0 \\ x_0 + x_1 \end{bmatrix} = \\ &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} h_2 - h_0 \\ h_1 - h_0 \\ h_0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix}. \end{aligned}$$

Отсюда следует, что

$$\begin{bmatrix} h_0 & h_2 \\ h_1 & h_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} h_2 - h_0 \\ h_1 - h_0 \\ h_0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (4)$$

3°. Обратимся к случаю $N = 4$. Запишем

$$H_4 = \begin{bmatrix} h_0 & h_3 & h_2 & h_1 \\ h_1 & h_0 & h_3 & h_2 \\ h_2 & h_1 & h_0 & h_3 \\ h_3 & h_2 & h_1 & h_0 \end{bmatrix} = \begin{bmatrix} H_2^{(0)} & H_2^{(1)} \\ H_2^{(1)} & H_2^{(0)} \end{bmatrix}.$$

Видно, что матрица H_4 является блочным вариантом матрицы H_2 . Согласно (3) получаем

$$\begin{aligned} \begin{bmatrix} h_0 & h_3 & h_2 & h_1 \\ h_1 & h_0 & h_3 & h_2 \\ h_2 & h_1 & h_0 & h_3 \\ h_3 & h_2 & h_1 & h_0 \end{bmatrix} &= \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \times \\ &\times \frac{1}{2} \begin{bmatrix} h_0 + h_2 & h_3 + h_1 & 0 & 0 \\ h_1 + h_3 & h_0 + h_2 & 0 & 0 \\ 0 & 0 & h_0 - h_2 & h_3 - h_1 \\ 0 & 0 & h_1 - h_3 & h_0 - h_2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}. \quad (5) \end{aligned}$$

Для факторизации диагональных блоков воспользуемся формулами (3) и (4):

$$\begin{bmatrix} h_0 + h_2 & h_3 + h_1 \\ h_1 + h_3 & h_0 + h_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2} \text{diag} \begin{bmatrix} (h_0 + h_2) + (h_1 + h_3) \\ (h_0 + h_2) - (h_1 + h_3) \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (6)$$

$$\begin{bmatrix} h_0 - h_2 & h_3 - h_1 \\ h_1 - h_3 & h_0 - h_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \times \\ \times \text{diag} \begin{bmatrix} -(h_1 - h_3) - (h_0 - h_2) \\ (h_1 - h_3) - (h_0 - h_2) \\ h_0 - h_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \quad (7)$$

Подставив (6), (7) в (5), придём к разложению

$$\begin{bmatrix} h_0 & h_3 & h_2 & h_1 \\ h_1 & h_0 & h_3 & h_2 \\ h_2 & h_1 & h_0 & h_3 \\ h_3 & h_2 & h_1 & h_0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \times \\ \times \text{diag} \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \\ g_4 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}, \quad (8)$$

где

$$\begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \\ g_4 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & -2 & -2 \\ 0 & 0 & -2 & 2 \\ 0 & 0 & 2 & 0 \end{bmatrix} \begin{bmatrix} h_0 + h_2 \\ h_1 + h_3 \\ h_0 - h_2 \\ h_1 - h_3 \end{bmatrix} = \frac{1}{4} \text{diag} \begin{bmatrix} 1 \\ 1 \\ -2 \\ -2 \\ 2 \end{bmatrix} \times \\ \times \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \end{bmatrix}.$$

Из (8) следует, что вычисление четырёхточечной свёртки требует 5 умножений и 15 сложений.

4°. Пусть $N = 3$. Приведём матрицу H_3 к блочно-диагональному виду. Имеем

$$\begin{bmatrix} h_0 & h_2 & h_1 \\ h_1 & h_0 & h_2 \\ h_2 & h_1 & h_0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{bmatrix} = \begin{bmatrix} h_0 + h_1 + h_2 & h_0 + h_1 - 2h_2 & h_0 - 2h_1 + h_2 \\ h_0 + h_1 + h_2 & -2h_0 + h_1 + h_2 & h_0 + h_1 - 2h_2 \\ h_0 + h_1 + h_2 & h_0 - 2h_1 + h_2 & -2h_0 + h_1 + h_2 \end{bmatrix}.$$

Далее

$$\begin{aligned} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{bmatrix} \begin{bmatrix} h_0 & h_2 & h_1 \\ h_1 & h_0 & h_2 \\ h_2 & h_1 & h_0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{bmatrix} = \\ = 3 \begin{bmatrix} h_0 + h_1 + h_2 & 0 & 0 \\ 0 & 2h_0 - h_1 - h_2 & -h_0 - h_1 + 2h_2 \\ 0 & -h_0 + 2h_1 - h_2 & 2h_0 - h_1 - h_2 \end{bmatrix}. \end{aligned}$$

Согласно (4)

$$\begin{bmatrix} 2h_0 - h_1 - h_2 & -h_0 - h_1 + 2h_2 \\ -h_0 + 2h_1 - h_2 & 2h_0 - h_1 - h_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} -3h_0 + 3h_2 \\ -3h_0 + 3h_1 \\ 2h_0 - h_1 - h_2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

С учётом равенств

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{bmatrix}^{-1} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix}, \quad (9)$$

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

получаем

$$\begin{aligned} \begin{bmatrix} h_0 & h_2 & h_1 \\ h_1 & h_0 & h_2 \\ h_2 & h_1 & h_0 \end{bmatrix} &= \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \times \\ &\times \text{diag} \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad (10) \end{aligned}$$

где

$$\begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \end{bmatrix} = \frac{1}{3} \begin{bmatrix} h_0 + h_1 + h_2 \\ -3h_0 + 3h_2 \\ -3h_0 + 3h_1 \\ 2h_0 - h_1 - h_2 \end{bmatrix} = \frac{1}{3} \text{diag} \begin{bmatrix} 1 \\ -3 \\ -3 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \\ 2 & -1 & -1 \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ h_2 \end{bmatrix} =$$

$$= \frac{1}{3} \text{diag} \begin{bmatrix} 1 \\ -3 \\ -3 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ h_2 \end{bmatrix}.$$

На основании (10) заключаем, что вычисление трёхточечной свёртки требует 4 умножения и 11 сложений.

Отметим, что обобщение формулы (9) на матрицы n -го порядка имеет вид

$$\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1-n & 1 & \dots & 1 \\ 1 & 1 & 1-n & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1-n \end{bmatrix}^{-1} = \frac{1}{n} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & -1 & 0 & \dots & 0 \\ 1 & 0 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & -1 \end{bmatrix}. \quad (11)$$

5°. Рассмотрим случай $N = 5$. Обозначим $s = h_0 + h_1 + h_2 + h_3 + h_4$. Тогда

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -4 & 1 & 1 & 1 \\ 1 & 1 & -4 & 1 & 1 \\ 1 & 1 & 1 & -4 & 1 \\ 1 & 1 & 1 & 1 & -4 \end{bmatrix} \begin{bmatrix} h_0 & h_4 & h_3 & h_2 & h_1 \\ h_1 & h_0 & h_4 & h_3 & h_2 \\ h_2 & h_1 & h_0 & h_4 & h_3 \\ h_3 & h_2 & h_1 & h_0 & h_4 \\ h_4 & h_3 & h_2 & h_1 & h_0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -4 & 1 & 1 & 1 \\ 1 & 1 & -4 & 1 & 1 \\ 1 & 1 & 1 & -4 & 1 \\ 1 & 1 & 1 & 1 & -4 \end{bmatrix} =$$

$$= 5 \begin{bmatrix} s & 0 & 0 & 0 & 0 \\ 0 & & & & \\ 0 & & B & & \\ 0 & & & & \\ 0 & & & & \end{bmatrix}, \quad (12)$$

где

$$B = \begin{bmatrix} 5h_0 - s & 5h_4 - s & 5h_3 - s & 5h_2 - s \\ 5h_1 - s & 5h_0 - s & 5h_4 - s & 5h_3 - s \\ 5h_2 - s & 5h_1 - s & 5h_0 - s & 5h_4 - s \\ 5h_3 - s & 5h_2 - s & 5h_1 - s & 5h_0 - s \end{bmatrix} = - \begin{bmatrix} H_2^{(0)} & H_2^{(2)} \\ H_2^{(1)} & H_2^{(0)} \end{bmatrix}. \quad (13)$$

Воспользуемся блочным вариантом формулы (4):

$$\begin{bmatrix} H_2^{(0)} & H_2^{(2)} \\ H_2^{(1)} & H_2^{(0)} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \times$$

$$\times \text{diag} \begin{bmatrix} -5(h_2 - h_4) - 5(h_0 - h_3) \\ 5(h_1 - h_4) - 5(h_0 - h_3) \\ 5(h_0 - h_3) \\ -5(h_1 - h_4) - 5(h_0 - h_2) \\ 5(h_1 - h_3) - 5(h_0 - h_2) \\ 5(h_0 - h_2) \\ 5(h_0 - h_4) \\ 5(h_0 - h_1) \\ s - 5h_0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}. \quad (14)$$

Объединяя формулы (12)–(14) и учитывая (11) при $n = 5$, приходим к разложению

$$H_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \times$$

$$\times \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \\ g_4 \\ g_5 \\ g_6 \\ g_7 \\ g_8 \\ g_9 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \times$$

$$\times \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix}, \quad (15)$$

где

$$\begin{aligned}
 \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \\ g_4 \\ g_5 \\ g_6 \\ g_7 \\ g_8 \\ g_9 \end{bmatrix} &= -\frac{1}{5} \begin{bmatrix} -s \\ -5(h_2 - h_4) - 5(h_0 - h_3) \\ 5(h_1 - h_4) - 5(h_0 - h_3) \\ 5(h_0 - h_3) \\ -5(h_1 - h_4) - 5(h_0 - h_2) \\ 5(h_1 - h_3) - 5(h_0 - h_2) \\ 5(h_0 - h_2) \\ 5(h_0 - h_4) \\ 5(h_0 - h_1) \\ s - 5h_0 \end{bmatrix} = \\
 &= \frac{1}{5} \text{diag} \begin{bmatrix} 1 \\ 5 \\ 5 \\ -5 \\ 5 \\ 5 \\ -5 \\ -5 \\ -5 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 0 & -1 & 1 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 1 & -1 & 0 & -1 \\ 1 & -1 & -1 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 & 0 \\ 4 & -1 & -1 & -1 & -1 \end{bmatrix} \begin{bmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \end{bmatrix}.
 \end{aligned}$$

Для полноты картины факторизуем матрицу, стоящую после диагональной:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 0 & -1 & 1 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 1 & -1 & 0 & -1 \\ 1 & -1 & -1 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 \\ 1 & -1 & 0 & 0 & 0 \\ 4 & -1 & -1 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 1 \\ 0 & 1 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 & 1 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix} =$$

$$\begin{aligned}
&= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \times \\
&\times \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix}.
\end{aligned}$$

С учётом равенств

$$\begin{aligned}
&\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} = \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \\
&\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix},
\end{aligned}$$

$$\begin{aligned}
& \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \end{bmatrix} = \\
& = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}
\end{aligned}$$

формулу (15) можно переписать так:

$$\begin{aligned}
H_5 &= \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \times \\
& \times \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ g_3 \\ g_4 \\ g_5 \\ g_6 \\ g_7 \\ g_8 \\ g_9 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \times \\
& \times \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}. \quad (16)
\end{aligned}$$

Формула (16) показывает, что пятиточечную свёртку можно вычислить, используя 10 умножений и 31 сложение.

6°. В докладе представлен матричный подход к построению быстрых алгоритмов циклических свёрток. Другой (полиномиальный) подход описан в [1] и в [2, с. 105–111].

Доклад примыкает к работе авторов [3].

ЛИТЕРАТУРА

1. Агарвал Р. К., Кули Дж. У. *Новые алгоритмы для цифровой свёртки*. В кн.: Макклелан Дж. Х., Рейдер Ч. М. *Применение теории чисел в цифровой обработке сигналов*. М.: Радио и связь, 1983. С. 91–117.
2. Блейхут Р. *Быстрые алгоритмы цифровой обработки сигналов*. М.: Мир, 1989. 448 с.
3. Малозёмов В. Н., Просеков О. В. *О быстром преобразовании Фурье малых порядков* // Вестник СПбГУ. Сер. 1. 2003. Вып. 1 (№ 1). С. 36–45.

БЫСТРОЕ ПРЕОБРАЗОВАНИЕ ФУРЬЕ МАЛЫХ ПОРЯДКОВ

О. В. Просеков

6 декабря 2005 г.

Быстрое преобразование Фурье связано с разложением матрицы Фурье на сомножители специальной структуры. Такая факторизация определяется далеко не единственным образом. В [1] были рассмотрены порядки 2, 3, 4, 5, 6. В данной работе продолжается развитие идей, изложенных в [1]. Благодаря полному учёту симметрии в матрице Фурье удалось улучшить факторизации, указанные выше, и получить новые для порядков 7, 8, 9, 10, 11, 12 и 16.

1°. Дискретное преобразование Фурье сигнала $x \in \mathbb{C}_N$, определяемое формулой

$$X(k) = \sum_{j=0}^{N-1} x(j) \omega_N^{-kj}, \quad k \in 0 : N-1, \quad (1)$$

где $\omega_N = \exp(2\pi i/N)$, можно записать в виде умножения матрицы на вектор

$$X = \bar{F}_N x.$$

Здесь F_N — матрица Фурье, $F_N[k, j] = \omega_N^{kj}$, $k, j \in 0 : N-1$. Быстрое преобразование Фурье (БПФ) основано на приведении формулы (1) к виду [2, с. 429]

$$X = CBAx. \quad (2)$$

Здесь B — диагональная матрица, ответственная за умножения, A и C — матрицы, элементы которых равны 0, 1 или -1 . Матрицы A и C называются соответственно матрицей предсложений и матрицей постсложений.

Факторизация (2) имеет целью минимизировать число умножений. Чтобы минимизировать число сложений, нужно факторизовать матрицы A и C , т. е. перейти к разложению

$$X = C_1 C_2 \dots C_m B A_n A_{n-1} \dots A_1 x, \quad (3)$$

в котором сомножители C_k и A_l обладают следующими свойствами: их элементы по-прежнему равны 0, 1 или -1 , но в каждой строке этих сомножителей содержится, по возможности, не более двух отличных от нуля элементов.

Разложение (3) не единственно, поэтому можно ставить дополнительные условия. Например, можно потребовать, чтобы матрицы C_k и A_l были, в основном, симметричными, строки и столбцы линейно независимы, чтобы значение -1 стояло, по возможности, на диагоналях и т. д. Такие дополнительные условия трудно формализовать. В начале мы приведём вывод «совершенных» разложений матрицы Фурье вида (3) при $N = 3, 4, 5, 6$. При этом будут использоваться только элементарные средства.

2°. Введём обозначения

$$a_k = \sum_{j=0}^{N-1} x_j \cos\left(\frac{2\pi k}{N} j\right), \quad b_k = -i \sum_{j=1}^{N-1} x_j \sin\left(\frac{2\pi k}{N} j\right). \quad (4)$$

Поскольку $a_{N-k} = a_k$ и $b_{N-k} = -b_k$, то формула (1) принимает следующий вид

$$X_k = a_k + b_k, \quad X_{N-k} = a_k - b_k, \quad k = 0, 1, \dots, \lfloor N/2 \rfloor.$$

Отметим, что $b_0 = 0$, и при нечётном N формулы (4) можно переписать так:

$$\begin{aligned} a_0 &= x_0 + \sum_{j=1}^{\lfloor N/2 \rfloor} (x_j + x_{N-j}), \\ a_k &= x_0 + \sum_{j=1}^{\lfloor N/2 \rfloor} (x_j + x_{N-j}) \cos\left(\frac{2\pi k}{N} j\right), \quad k = 1, \dots, \lfloor N/2 \rfloor, \\ b_k &= -i \sum_{j=1}^{\lfloor N/2 \rfloor} (x_j - x_{N-j}) \sin\left(\frac{2\pi k}{N} j\right), \quad k = 1, \dots, \lfloor N/2 \rfloor. \end{aligned}$$

При чётном N , $b_{N/2} = 0$ и формулы (4) принимают вид

$$\begin{aligned} a_0 &= x_0 + x_{N/2} + \sum_{j=1}^{N/2-1} (x_j + x_{N-j}), \\ a_k &= x_0 + (-1)^k x_{N/2} + \sum_{j=1}^{N/2-1} (x_j + x_{N-j}) \cos\left(\frac{2\pi k}{N} j\right), \quad k = 1, \dots, N/2 - 1, \\ a_{N/2} &= x_0 + (-1)^{N/2} x_{N/2} + \sum_{j=1}^{N/2-1} (-1)^j (x_j + x_{N-j}), \end{aligned}$$

$$b_k = -i \sum_{j=1}^{N/2-1} (x_j - x_{N-j}) \sin\left(\frac{2\pi k}{N} j\right), \quad k = 1, \dots, N/2 - 1.$$

По существу, получена факторизация матрицы Фурье

$$F_N = A \begin{bmatrix} C & 0 \\ 0 & S \end{bmatrix} A, \quad (5)$$

где C, S — квадратные матрицы с элементами

$$C[k, j] = \cos\left(k j \frac{2\pi}{N}\right), \quad S[l, p] = i \sin\left(l p \frac{2\pi}{N}\right).$$

Здесь $k, j \in 0 : \lfloor N/2 \rfloor$ и $l, p \in 1 : \lfloor N/2 \rfloor$ при нечётном N ; $k, j \in 0 : N/2$ и $l, p \in 1 : N/2 - 1$ при чётном N .

В формуле (5) A — квадратная матрица порядка N следующего вида:

$$A = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 1 \\ 0 & 0 & 1 & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & 1 & \dots & 0 \\ 0 & \dots & 1 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 1 & \dots & -1 & 0 \\ 0 & 1 & 0 & \dots & 0 & -1 \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 1 \\ 0 & 0 & 1 & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & \dots & 0 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 1 & \dots & -1 & 0 \\ 0 & 1 & 0 & \dots & 0 & -1 \end{bmatrix}.$$

(при нечётном N) (при чётном N)

Нам потребуется одно элементарное свойство матриц: в предположении, что D — квадратная матрица и определено произведение CBA , справедливо равенство

$$\begin{bmatrix} D & 0 \\ 0 & CBA \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & C \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & B \end{bmatrix} \begin{bmatrix} I & 0 \\ 0 & A \end{bmatrix}.$$

Случай, когда $N = 2$ тривиален и не нуждается в упрощении:

$$F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

3°. Обратимся к случаю $N = 3$. Положим $\theta = 2\pi/3$. Согласно (5) имеем

$$F_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 1 & \cos \theta & 0 \\ 0 & 0 & i \sin \theta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix}. \quad (6)$$

Факторизуем верхний блок средней матрицы в правой части (6). Для этого приведём его к диагональному виду:

$$\begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & \cos \theta \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \cos \theta - 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Отсюда следует, что

$$\begin{bmatrix} 1 & 1 \\ 1 & \cos \theta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} \cos \theta - 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}. \quad (7)$$

Подставив (7) в (6), приходим к окончательной формуле

$$F_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} \cos \theta - 1 \\ 1 \\ i \sin \theta \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix}. \quad (8)$$

Разложение (8) можно представить в виде $F_3 = A_1 A_2 B A_2 A_1 x$, где A_1, A_2 — симметричные матрицы.

4°. Аналогичным образом можно разобратся со случаем $N = 6$. Положим $\theta = \pi/3$. Согласно (5) имеем

$$F_6 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix} \times$$

$$\times \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & \cos \theta & -\cos \theta & -1 & 0 & 0 \\ 1 & -\cos \theta & -\cos \theta & 1 & 0 & 0 \\ 1 & -1 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -i \sin \theta & i \sin \theta \\ 0 & 0 & 0 & 0 & i \sin \theta & i \sin \theta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}. \quad (9)$$

Факторизуем верхний блок средней матрицы в правой части (9):

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \cos \theta & -\cos \theta & -1 \\ 1 & -\cos \theta & -\cos \theta & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & -\cos \theta & 0 & 1 \\ 1 & 0 & -\cos \theta & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{bmatrix}.$$

Первую матрицу правой части приведём к диагональному виду:

$$\begin{aligned} & \begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & -\cos \theta & 0 & 1 \\ 1 & 0 & -\cos \theta & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = \\ & = \begin{bmatrix} -\cos \theta - 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -\cos \theta - 1 \end{bmatrix}. \end{aligned}$$

Отсюда следует, что

$$\begin{aligned} & \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & -\cos \theta & 0 & 1 \\ 1 & 0 & -\cos \theta & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} = \\ & = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} -\cos \theta - 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -\cos \theta - 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}. \quad (10) \end{aligned}$$

Разберёмся с нижним блоком средней матрицы в правой части (9):

$$\begin{bmatrix} -i \sin \theta & i \sin \theta \\ i \sin \theta & i \sin \theta \end{bmatrix} = \begin{bmatrix} i \sin \theta & 0 \\ 0 & i \sin \theta \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}. \quad (11)$$

Объединив (9)–(11), придём к окончательной формуле

$$\begin{aligned} F_6 &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} -\cos \theta - 1 \\ 1 \\ 1 \\ -\cos \theta - 1 \\ i \sin \theta \\ i \sin \theta \end{bmatrix} \times \\ & \times \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}. \quad (12) \end{aligned}$$

Разложение (12) можно представить в виде $F_6 = A_1 A_3 B A_3 A_2 A_1$, где A_1 , A_2 , A_3 — симметричные матрицы.

5°. Перейдём к случаю $N = 4$. Согласно (5) имеем

$$F_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}. \quad (13)$$

Факторизуем верхний блок средней матрицы в правой части (13):

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Отсюда следует, что

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & -1 \end{bmatrix}. \quad (14)$$

Подставив (14) в (13), получим

$$F_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} 1 \\ 1 \\ 1 \\ i \end{bmatrix} \times$$

$$\times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}. \quad (15)$$

Формулу (15) можно упростить, если перемножить первые две и последние две матрицы в правой её части. Придём к окончательной формуле

$$F_4 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \text{diag} \begin{bmatrix} 1 \\ 1 \\ 1 \\ i \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}. \quad (16)$$

Разложение (16) можно представить в виде $X = A_1 B A_2 A_1 x$, где A_1, A_2 — симметричные матрицы.

6°. Рассмотрим случай $N = 5$. Обозначим $\theta = 2\pi/5$. Согласно (5) имеем

$$F_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{bmatrix} \times$$

$$\times \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & \cos \theta & \cos 2\theta & 0 & 0 \\ 1 & \cos 2\theta & \cos \theta & 0 & 0 \\ 0 & 0 & 0 & -i \sin \theta & i \sin 2\theta \\ 0 & 0 & 0 & i \sin 2\theta & i \sin \theta \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{bmatrix}. \quad (17)$$

Средняя матрица в правой части (17) имеет блочно-диагональную структуру. Для факторизации этих блоков нам потребуются следующее предложение.

ПРЕДЛОЖЕНИЕ. *Справедливы формулы*

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} a+b & 0 \\ 0 & a-b \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (18)$$

$$\begin{bmatrix} c & a \\ a & b \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c-a & 0 & 0 \\ 0 & b-a & 0 \\ 0 & 0 & a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}. \quad (19)$$

Доказательство. Начнём с формулы (18). Пусть

$$u_0 = ax_0 + bx_1,$$

$$u_1 = bx_0 + ax_1.$$

Поскольку

$$u_0 + u_1 = (a+b)(x_0 + x_1),$$

$$u_0 - u_1 = (a-b)(x_0 - x_1),$$

то

$$u_0 = \frac{1}{2}[(a+b)(x_0 + x_1) + (a-b)(x_0 - x_1)],$$

$$u_1 = \frac{1}{2}[(a+b)(x_0 + x_1) - (a-b)(x_0 - x_1)].$$

Последнюю формулу можно переписать в виде

$$\begin{bmatrix} u_0 \\ u_1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} a+b & a-b \\ a+b & -(a-b) \end{bmatrix} \begin{bmatrix} x_0 + x_1 \\ x_0 - x_1 \end{bmatrix} =$$

$$= \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} a+b & 0 \\ 0 & a-b \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix},$$

что равносильно (18).

Установим формулу (19). Пусть

$$\begin{aligned}v_0 &= c x_0 + a x_1, \\v_1 &= a x_0 + b x_1.\end{aligned}$$

Поскольку

$$\begin{aligned}v_0 &= (c - a) x_0 + a (x_0 + x_1), \\v_1 &= (b - a) x_1 + a (x_0 + x_1),\end{aligned}$$

то

$$\begin{aligned}\begin{bmatrix} v_0 \\ v_1 \end{bmatrix} &= \begin{bmatrix} c - a & 0 & a \\ 0 & b - a & a \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_0 + x_1 \end{bmatrix} = \\ &= \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} c - a \\ b - a \\ a \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \end{bmatrix},\end{aligned}$$

что равносильно (19). Предложение доказано. \square

Факторизуем верхний блок средней матрицы в правой части (17):

$$\begin{aligned}&\begin{bmatrix} 1 & 1 & 1 \\ 1 & \cos \theta & \cos 2\theta \\ 1 & \cos 2\theta & \cos \theta \end{bmatrix} = \\ &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 \\ 1 & \frac{1}{2}(\cos \theta + \cos 2\theta) & 0 \\ 0 & 0 & \frac{1}{2}(\cos \theta - \cos 2\theta) \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix}.\end{aligned}$$

Далее, воспользовавшись формулой (7), получим

$$\begin{aligned}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \cos \theta & \cos 2\theta \\ 1 & \cos 2\theta & \cos \theta \end{bmatrix} &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \\ &\times \text{diag} \begin{bmatrix} \frac{1}{2}(\cos \theta + \cos 2\theta) - 1 \\ 1 \\ \frac{1}{2}(\cos \theta - \cos 2\theta) \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix}. \quad (20)\end{aligned}$$

Согласно формуле (19)

$$\begin{bmatrix} -i \sin \theta & i \sin 2\theta \\ i \sin 2\theta & i \sin \theta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} i(\sin \theta + \sin 2\theta) \\ -i(\sin \theta - \sin 2\theta) \\ -i \sin 2\theta \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}. \quad (21)$$

На основании (17), (20) и (21) приходим к окончательной формуле

$$\begin{aligned} F_5 = & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \times \\ & \times \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \text{diag} \begin{bmatrix} \frac{1}{2}(\cos \theta + \cos 2\theta) - 1 \\ 1 \\ \frac{1}{2}(\cos \theta - \cos 2\theta) \\ i(\sin \theta + \sin 2\theta) \\ -i(\sin \theta - \sin 2\theta) \\ -i \sin 2\theta \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \times \\ & \times \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{bmatrix}. \quad (22) \end{aligned}$$

Разложение (22) можно представить в виде $F_5 = A_1 A_2 A_3^T B A_3 A_2 A_1$, где A_1, A_2 — симметричные матрицы.

7°. Таким же образом можно получить факторизации матриц Фурье для других малых порядков. В приложении приведены факторизации матрицы Фурье порядков от 2 до 12 и 16. В таблице 1 указаны характеристики соответствующих алгоритмов БПФ.

В заключение отметим, что практическую ценность представляет использование алгоритмов БПФ малых порядков в составе алгоритмов БПФ при $N = n_1 n_2 \cdots n_s$. В этом случае разложение матрицы Фурье содержит множитель $I_{\Delta_\nu} \otimes F_{n_\nu} \otimes I_{N_\nu}$ [3, 4]. Данный множитель позволяет использовать векторные и параллельные операции, что особенно актуально (в связи с развитием современных технологий) для реализации БПФ.

Рассмотрим пример. Пусть требуется вычислить вектор $X = (I_2 \otimes F_2 \otimes I_2) x$.

Порядок алгоритма БПФ	Число множителей в факторизации	Порядок диагональной матрицы	Число умножений	Число сложений
2	1	2	0	2
3	5	3	2	6
4	3	4	0	8
5	7	6	5	17
6	6	6	4	18
7	7	9	8	36
8	6	8	2	26
9	7	12	10	42
10	8	12	10	44
11	9	21	20	84
12	7	12	8	48
16	9	18	10	74

Таблица 1. Характеристики алгоритмов БПФ

По определению кронекерова умножения [5]

$$I_2 \otimes F_2 \otimes I_2 = \begin{bmatrix} I_2 & I_2 & 0_2 & 0_2 \\ I_2 & -I_2 & 0_2 & 0_2 \\ 0_2 & 0_2 & I_2 & I_2 \\ 0_2 & 0_2 & I_2 & -I_2 \end{bmatrix}.$$

Тогда

$$\begin{bmatrix} X_0 \\ X_1 \end{bmatrix} = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} + \begin{bmatrix} x_2 \\ x_3 \end{bmatrix}, \quad \begin{bmatrix} X_4 \\ X_5 \end{bmatrix} = \begin{bmatrix} x_4 \\ x_5 \end{bmatrix} + \begin{bmatrix} x_2 \\ x_3 \end{bmatrix} \quad \text{— параллельно-векторная сумма;}$$

$$\begin{bmatrix} X_2 \\ X_3 \end{bmatrix} = \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} - \begin{bmatrix} x_2 \\ x_3 \end{bmatrix}, \quad \begin{bmatrix} X_6 \\ X_7 \end{bmatrix} = \begin{bmatrix} x_4 \\ x_5 \end{bmatrix} - \begin{bmatrix} x_2 \\ x_3 \end{bmatrix} \quad \text{— параллельно-векторная разность.}$$

Таким образом, операции сложения и вычитания двух чисел заменяются на параллельные операции сложения и вычитания векторов.

ЛИТЕРАТУРА

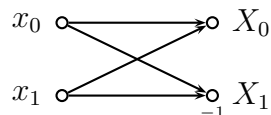
1. Малозёмов В. Н., Просеков О. В. *О быстром преобразовании Фурье малых порядков* // Вестник СПбГУ. Сер. 1. 2003. Вып. 1 (№ 1). С. 36–45.

2. Блейхут Р. *Быстрые алгоритмы цифровой обработки сигналов*. М.: Мир, 1989. 448 с.
3. Малозёмов В. Н., Просеков О. В. *Факторизация Кули-Тьюки матрицы Фурье* // Семинар «DHA & CAGD». Избранные доклады. 14 апреля 2004 г. (<http://dha.spb.ru/rep04.shtml#0414>).
4. Малозёмов В. Н., Просеков О. В. *Факторизация Гуда матрицы Фурье* // Семинар «DHA & CAGD». Избранные доклады. 5 мая 2004 г. (<http://dha.spb.ru/rep04.shtml#0505>).
5. Малозёмов В. Н., Просеков О. В. *Перестановки и кронекерово произведение матриц* // Семинар «DHA & CAGD». Избранные доклады. 31 марта 2004 г. (<http://dha.spb.ru/rep04.shtml#0331>).

Приложение. Алгоритмы БПФ порядков 2–12, 16

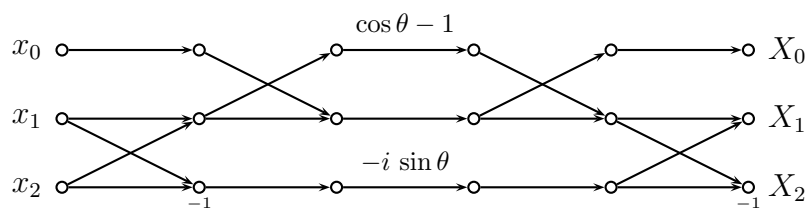
Ниже приведены факторизации матриц Фурье порядков 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 и 16. Соответствующие алгоритмы БПФ представлены в виде графических схем. Также указано число нетривиальных арифметических операций в алгоритмах (умножения на ± 1 и $\pm i$ не учитываются).

Алгоритм БПФ порядка 2: 0 умножений, 2 сложения.



$$F_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Алгоритм БПФ порядка 3: 2 умножения, 6 сложений.

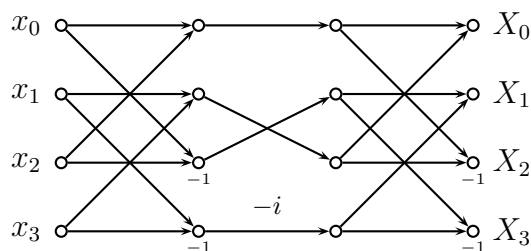


$$F_3 = A_1 A_2 M A_2 A_1,$$

где A_1, A_2 — симметричные матрицы. $\theta = 2\pi/3$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} \cos \theta - 1 \\ 1 \\ i \sin \theta \end{bmatrix}.$$

Алгоритм БПФ порядка 4: 0 умножений, 8 сложений.

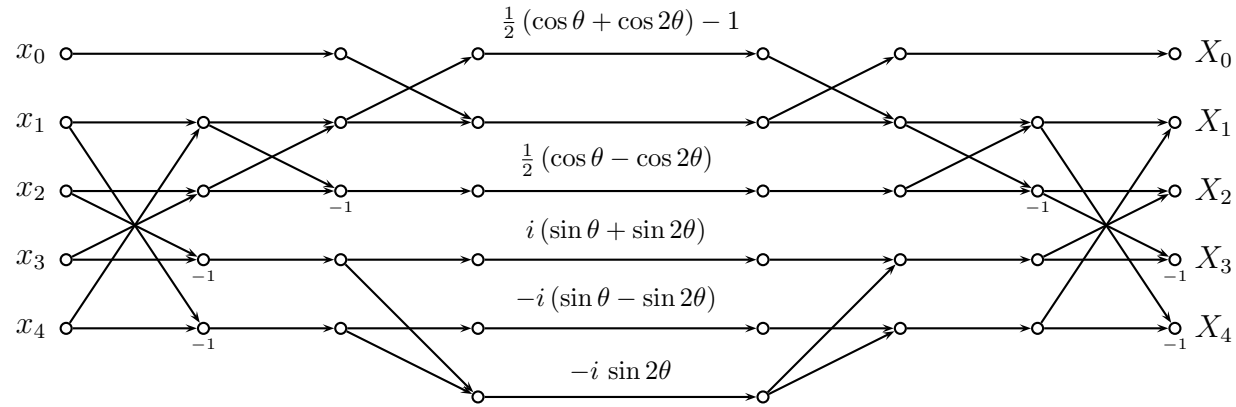


$$F_4 = A_1 M A_2 A_1,$$

где A_1, A_2 — симметричные матрицы.

$$A_1 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} 1 \\ 1 \\ 1 \\ i \end{bmatrix}.$$

Алгоритм БПФ порядка 5: 5 умножений, 17 сложений.

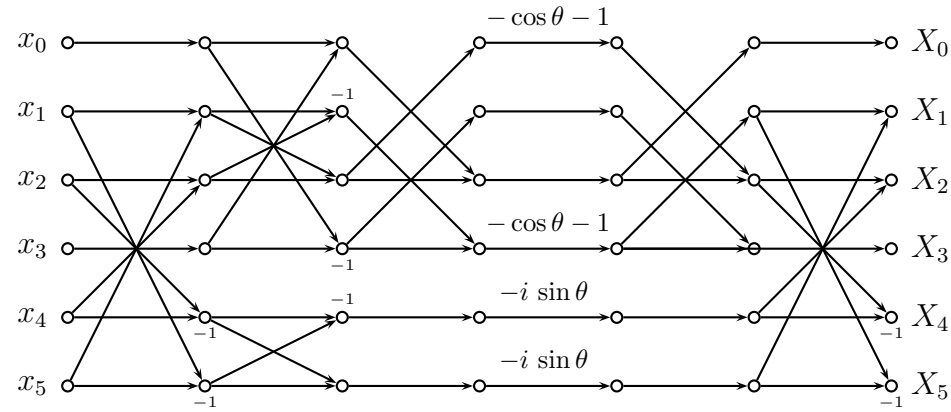


$$F_5 = A_1 A_2 A_3^T M A_3 A_2 A_1,$$

где A_1, A_2 — симметричные матрицы. $\theta = 2\pi/5$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 1 & 0 & 0 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} \frac{1}{2}(\cos \theta + \cos 2\theta) - 1 \\ 1 \\ \frac{1}{2}(\cos \theta - \cos 2\theta) \\ -i(\sin \theta + \sin 2\theta) \\ i(\sin \theta - \sin 2\theta) \\ i \sin 2\theta \end{bmatrix}.$$

Алгоритм БПФ порядка 6: 4 умножения, 18 сложений.

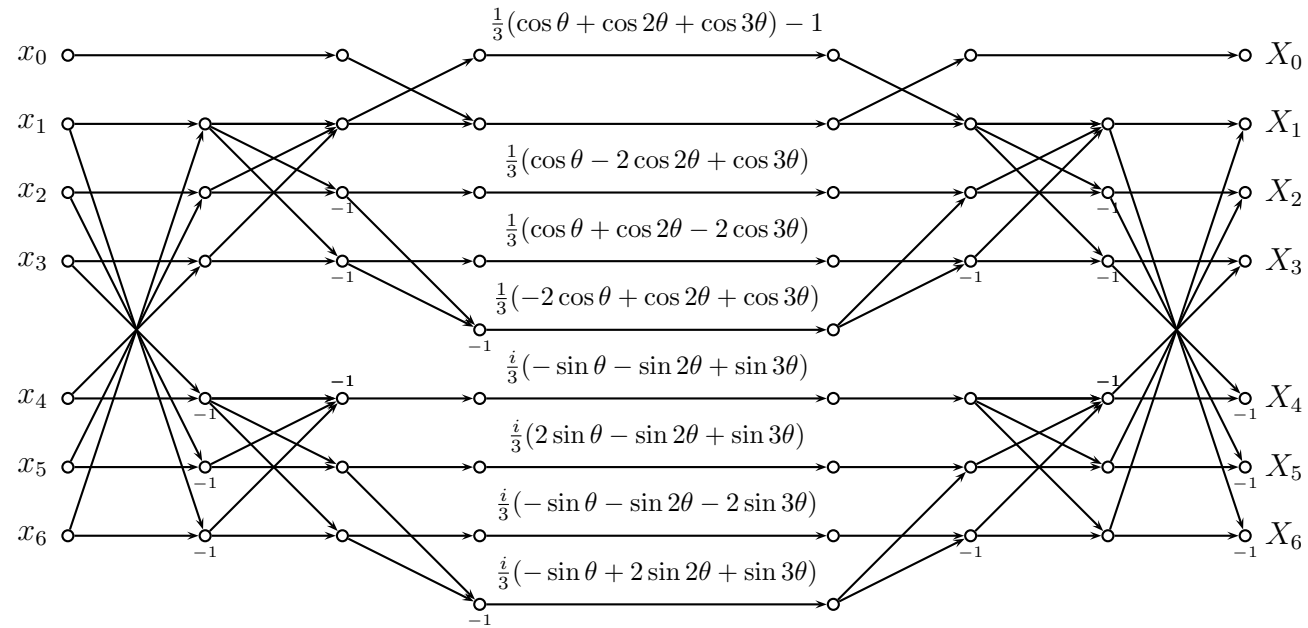


$$F_6 = A_1 A_3 M A_3 A_2 A_1,$$

где A_1, A_2, A_3 — симметричные матрицы. $\theta = \pi/3$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} -\cos \theta - 1 \\ 1 \\ 1 \\ -\cos \theta - 1 \\ i \sin \theta \\ i \sin \theta \end{bmatrix}.$$

Алгоритм БПФ порядка 7: 8 умножений, 36 сложений.



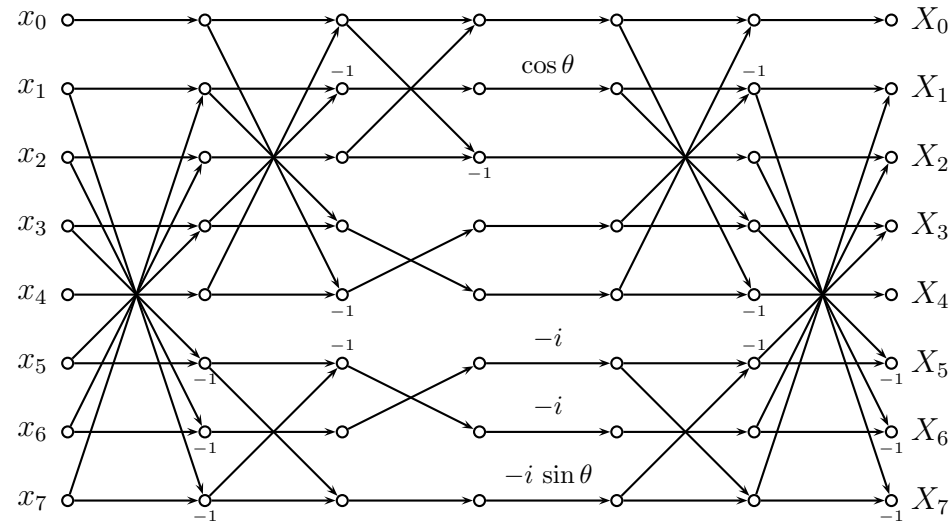
$$F_7 = A_1 A_2 A_3^T M A_3 A_2 A_1,$$

где A_1, A_2 — симметричные матрицы. $\theta = 2\pi/7$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} \frac{1}{3}(\cos \theta + \cos 2\theta + \cos 3\theta) - 1 \\ 1 \\ \frac{1}{3}(\cos \theta - 2\cos 2\theta + \cos 3\theta) \\ \frac{1}{3}(\cos \theta + \cos 2\theta - 2\cos 3\theta) \\ \frac{1}{3}(-2\cos \theta + \cos 2\theta + \cos 3\theta) \\ \frac{i}{3}(\sin \theta + \sin 2\theta - \sin 3\theta) \\ \frac{i}{3}(-2\sin \theta + \sin 2\theta - \sin 3\theta) \\ \frac{i}{3}(\sin \theta + \sin 2\theta + 2\sin 3\theta) \\ \frac{i}{3}(\sin \theta - 2\sin 2\theta - \sin 3\theta) \end{bmatrix}.$$

Алгоритм БПФ порядка 8: 2 умножения, 26 сложений.

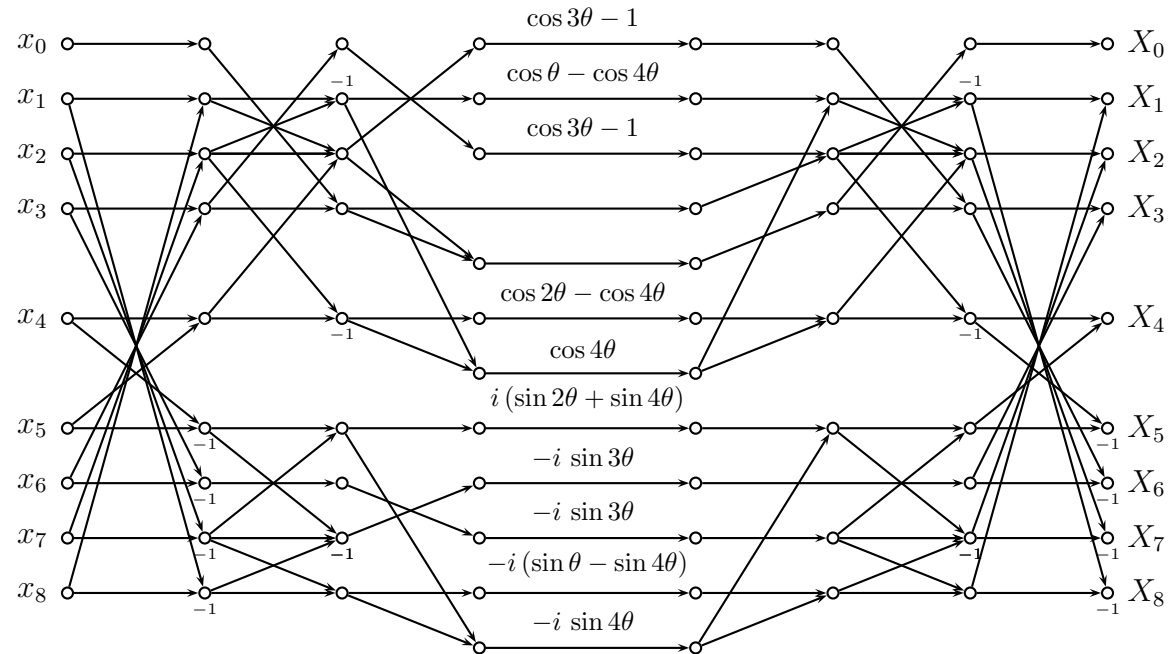


$$F_8 = A_1 A_2 M A_3 A_2 A_1,$$

где A_1, A_2, A_3 — симметричные матрицы. $\theta = \pi/4$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \quad A_3 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} 1 \\ \cos \theta \\ 1 \\ 1 \\ 1 \\ i \\ i \\ i \sin \theta \end{bmatrix}.$$

Алгоритм БПФ порядка 9: 10 умножений, 42 сложения.



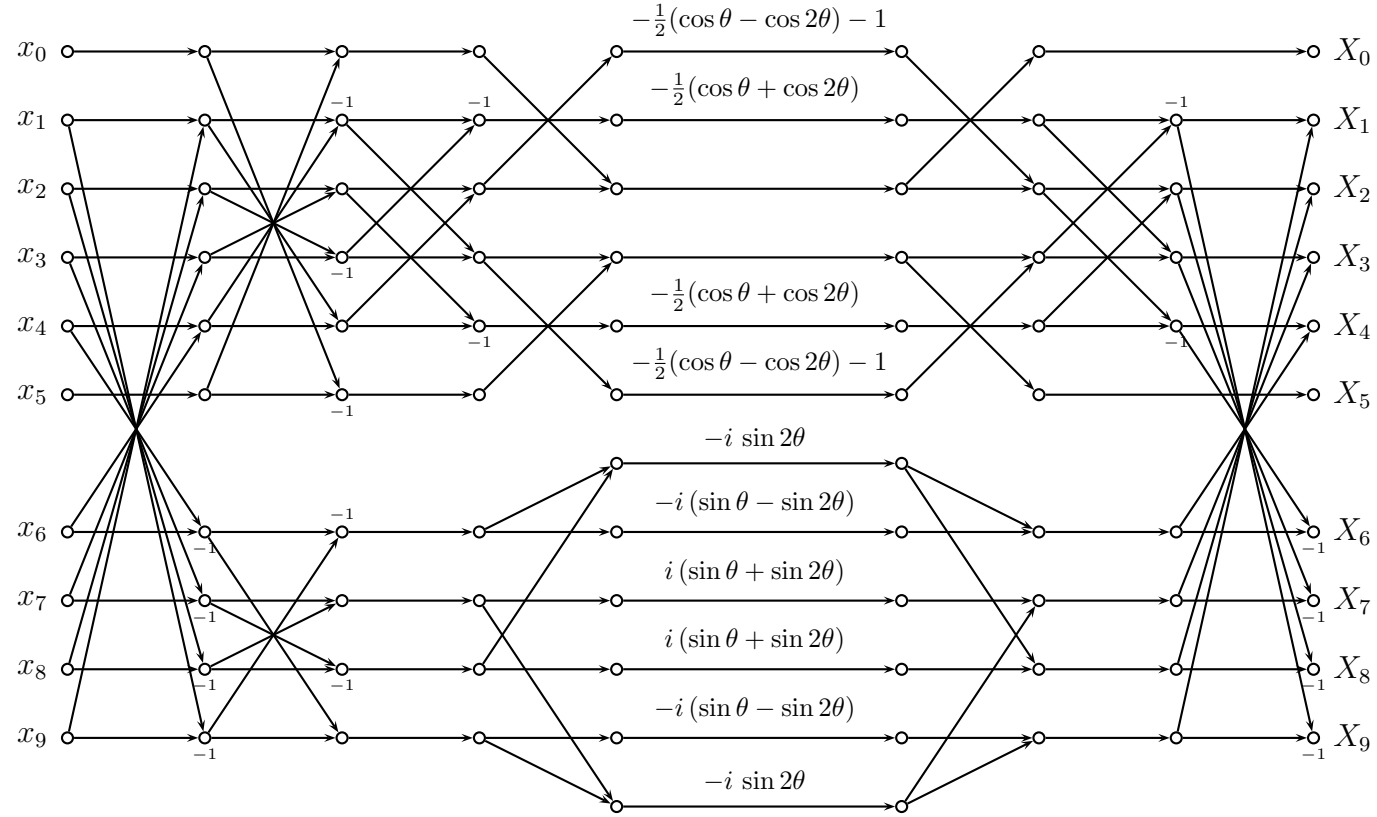
$$F_9 = A_1 A_2 A_4 M A_3 A_2 A_1,$$

где A_1, A_2 — симметричные матрицы. $\theta = 2\pi/9$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} \cos 3\theta - 1 \\ \cos \theta - \cos 4\theta \\ \cos 3\theta - 1 \\ 1 \\ 1 \\ \cos 2\theta - \cos 4\theta \\ \cos 4\theta \\ -i(\sin 2\theta + \sin 4\theta) \\ i \sin 3\theta \\ i \sin 3\theta \\ i(\sin \theta - \sin 4\theta) \\ i \sin 4\theta \end{bmatrix}, \quad A_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Алгоритм БПФ порядка 10: 10 умножений, 44 сложения.



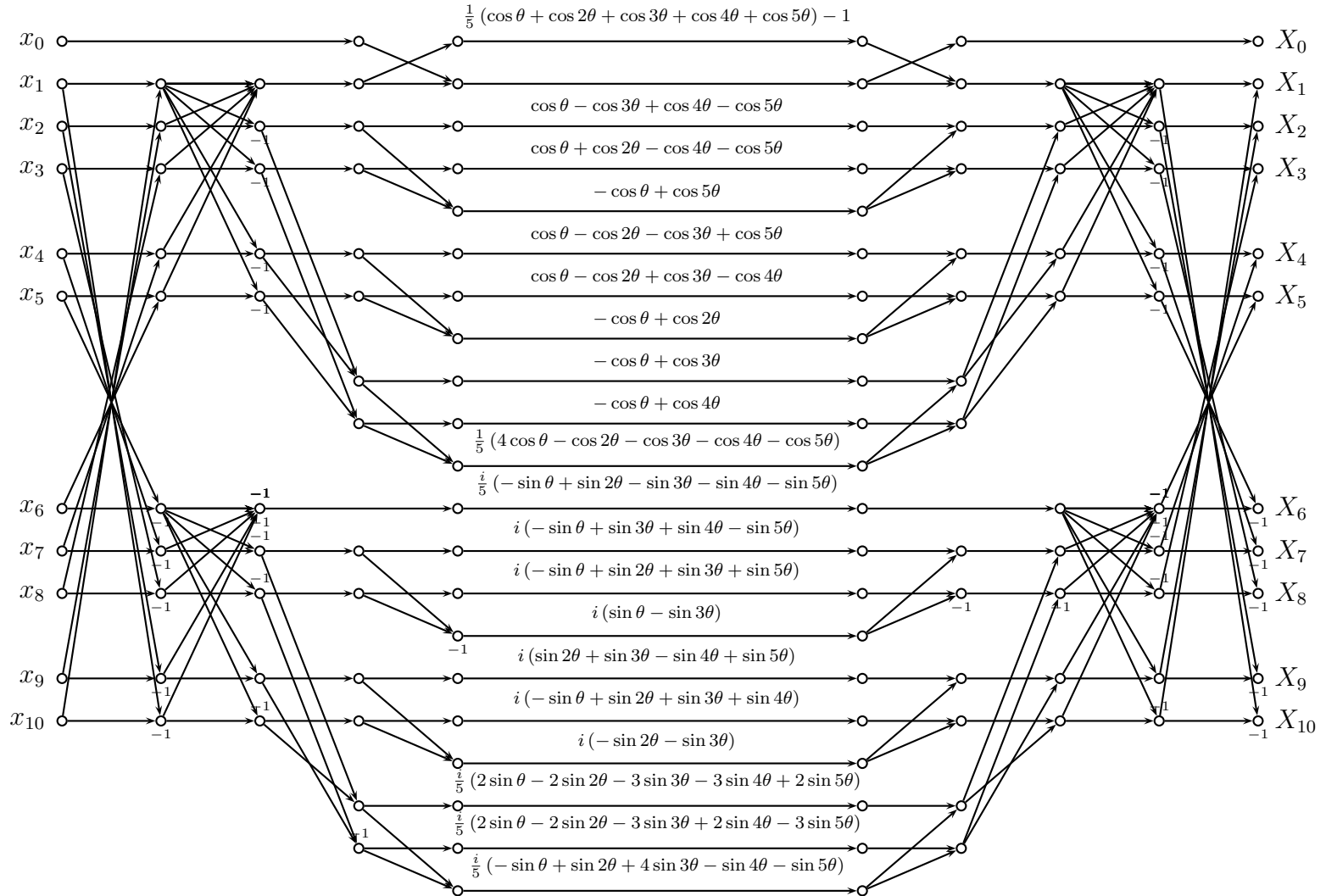
$$F_{10} = A_1 A_3 A_4^T M A_4 A_3 A_2 A_1,$$

где A_1, A_2, A_3 — симметричные матрицы. $\theta = \pi/5$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} -\frac{1}{2}(\cos \theta - \cos 2\theta) - 1 \\ -\frac{1}{2}(\cos \theta + \cos 2\theta) \\ 1 \\ 1 \\ -\frac{1}{2}(\cos \theta + \cos 2\theta) \\ -\frac{1}{2}(\cos \theta - \cos 2\theta) - 1 \\ i \sin 2\theta \\ i(\sin \theta - \sin 2\theta) \\ -i(\sin \theta + \sin 2\theta) \\ -i(\sin \theta + \sin 2\theta) \\ i(\sin \theta - \sin 2\theta) \\ i \sin 2\theta \end{bmatrix}.$$

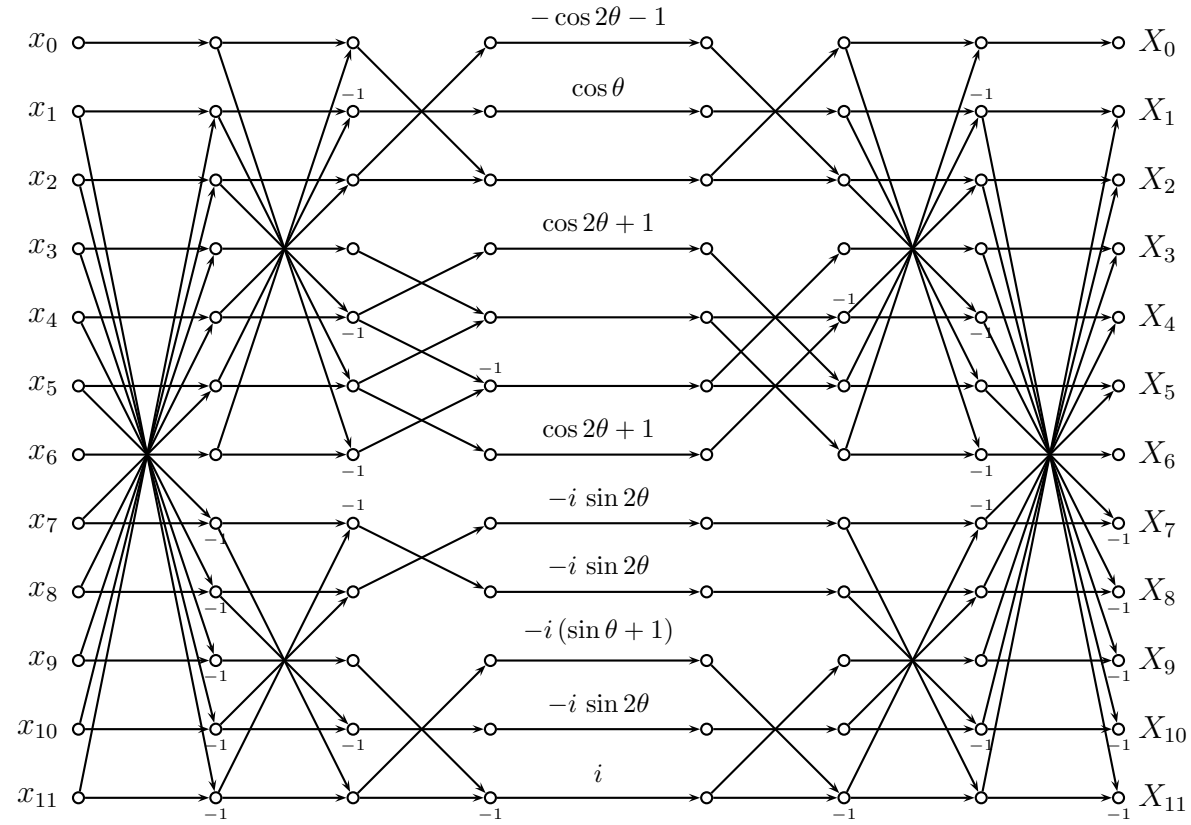
Алгоритм БПФ порядка 11: 20 умножений, 84 сложения.



[illegible]

$$A_4 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \quad M = \text{diag} \begin{bmatrix} \frac{1}{5} (\cos \theta + \cos 2\theta + \cos 3\theta + \cos 4\theta + \cos 5\theta) - 1 \\ 1 \\ \cos \theta - \cos 3\theta + \cos 4\theta - \cos 5\theta \\ \cos \theta + \cos 2\theta - \cos 4\theta - \cos 5\theta \\ -\cos \theta + \cos 5\theta \\ \cos \theta - \cos 2\theta - \cos 3\theta + \cos 5\theta \\ \cos \theta - \cos 2\theta + \cos 3\theta - \cos 4\theta \\ -\cos \theta + \cos 2\theta \\ -\cos \theta + \cos 3\theta \\ -\cos \theta + \cos 4\theta \\ \frac{1}{5} (4 \cos \theta - \cos 2\theta - \cos 3\theta - \cos 4\theta - \cos 5\theta) \\ \frac{i}{5} (-\sin \theta + \sin 2\theta - \sin 3\theta - \sin 4\theta - \sin 5\theta) \\ -i (-\sin \theta + \sin 3\theta + \sin 4\theta - \sin 5\theta) \\ -i (-\sin \theta + \sin 2\theta + \sin 3\theta + \sin 5\theta) \\ -i (\sin \theta - \sin 3\theta) \\ -i (\sin 2\theta + \sin 3\theta - \sin 4\theta + \sin 5\theta) \\ -i (-\sin \theta + \sin 2\theta + \sin 3\theta + \sin 4\theta) \\ -i (-\sin 2\theta - \sin 3\theta) \\ -\frac{i}{5} (2 \sin \theta - 2 \sin 2\theta - 3 \sin 3\theta - 3 \sin 4\theta + 2 \sin 5\theta) \\ -\frac{i}{5} (2 \sin \theta - 2 \sin 2\theta - 3 \sin 3\theta + 2 \sin 4\theta - 3 \sin 5\theta) \\ -\frac{i}{5} (-\sin \theta + \sin 2\theta + 4 \sin 3\theta - \sin 4\theta - \sin 5\theta) \end{bmatrix}.$$

Алгоритм БПФ порядка 12: 8 умножений, 48 сложений.

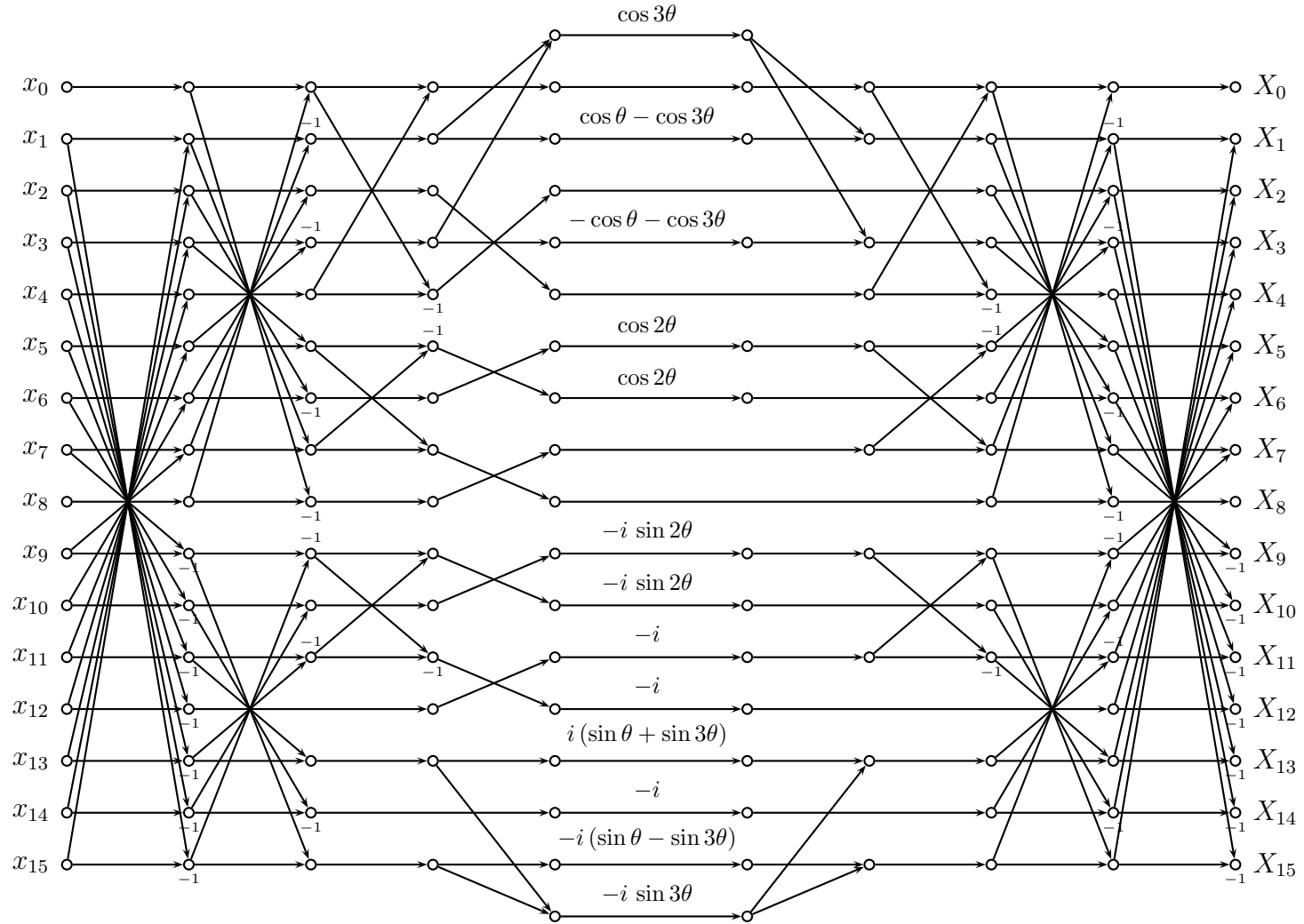


$$F_{12} = A_1 A_2 A_4 M A_3 A_2 A_1 x,$$

где A_1, A_2, A_3, A_4 — симметричные матрицы. $\theta = \pi/6$

$$\begin{aligned}
 A_1 = & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix} & A_2 = & \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \\
A_3 = & \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}, & M = \text{diag} & \begin{bmatrix} -\cos 2\theta - 1 \\ \cos \theta \\ 1 \\ \cos 2\theta + 1 \\ 1 \\ 1 \\ \cos 2\theta + 1 \\ i \sin 2\theta \\ i \sin 2\theta \\ i(\sin \theta + 1) \\ i \sin 2\theta \\ -i \end{bmatrix}, & A_4 = & \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}.
 \end{aligned}$$

Алгоритм БПФ порядка 16: 10 умножений, 74 сложения.



$$F_{16} = A_1 A_2 A_3 A_5 M A_4 A_3 A_2 A_1,$$

где A_1, A_2, A_3 — симметричные матрицы. $\theta = \pi/8$

$$A_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

[illegible]

ТЕОРЕМА ОБ ОТСЧЁТАХ В ДИСКРЕТНОМ ПЕРИОДИЧЕСКОМ СЛУЧАЕ

В. Н. Малозёмов А. Н. Сабаев

7 февраля 2006 г.

1°. Пусть $N = mn$, где $n \geq 2$, и μ, ν — целые числа, удовлетворяющие условиям

$$0 \leq \mu < \nu \leq N - 1, \quad \nu - \mu + 1 = N - m. \quad (1)$$

Введём функцию

$$h_m(j) = \frac{1}{m} \sum_{k=\mu-m}^{\mu-1} \omega_N^{kj}, \quad j \in \mathbb{Z}. \quad (2)$$

ТЕОРЕМА 1. Если спектр Фурье X сигнала $x \in \mathbb{C}_N$ равен нулю на множестве $\mu : \nu$, то

$$x(j) = \frac{1}{N} \sum_{l=0}^{m-1} x(ln) h_m(j - ln), \quad j \in \mathbb{Z}. \quad (3)$$

Доказательство. Имеем

$$\begin{aligned} x(j) &= \frac{1}{N} \sum_{k=0}^{N-1} X(k + \nu + 1) \omega_N^{(k+\nu+1)j} = \\ &= \frac{1}{N} \omega_N^{(\nu+1)j} \sum_{k=0}^{m-1} X(k + \nu + 1) \omega_N^{kj}. \end{aligned} \quad (4)$$

Мы воспользовались тем, что при изменении k от m до $N - 1$ индекс $k + \nu + 1$ изменяется в силу (1) от $N + \mu$ до $N + \nu$. Далее

$$n \omega_m^{-(\nu+1)l} x(ln) = \frac{1}{m} \sum_{k=0}^{m-1} X(k + \nu + 1) \omega_m^{kl}, \quad l \in 0 : m - 1.$$

Отсюда следует, что

$$X(k + \nu + 1) = n \sum_{l=0}^{m-1} x(ln) \omega_m^{-l(k+\nu+1)}, \quad k \in 0 : m - 1.$$

Подставляя это в (4) и меняя порядок суммирования, получаем

$$x(j) = \sum_{l=0}^{m-1} x(ln) \left[\frac{1}{m} \sum_{k=0}^{m-1} \omega_N^{(k+\nu+1)(j-ln)} \right].$$

Отметим, что в силу (1)

$$\frac{1}{m} \sum_{k=0}^{m-1} \omega_N^{(k+\nu+1)j} = \frac{1}{m} \sum_{k=\nu+1-N}^{m+\nu-N} \omega_N^{kj} = \frac{1}{m} \sum_{k=\mu-m}^{\mu-1} \omega_N^{kj} = h_m(j),$$

поэтому

$$x(j) = \sum_{l=0}^{m-1} x(ln) h_m(j - ln).$$

Теорема доказана. □

Нетрудно проверить, что ядро $h_m(j)$ обладает свойством

$$h_m(ln) = \delta_m(l), \quad l \in \mathbb{Z}. \quad (5)$$

Действительно,

$$h_m(ln) = \frac{1}{m} \sum_{k=0}^{m-1} \omega_m^{(k+\nu+1)l} = \omega_m^{(\nu+1)l} \delta_m(l) = \delta_m(l).$$

2°. Рассмотрим частный случай $\nu = N - \mu$. В силу (1), $m = 2\mu - 1$. Формула (2) принимает вид

$$h_m(j) = \frac{1}{m} \sum_{k=-\mu+1}^{\mu-1} \omega_N^{kj}. \quad (6)$$

ТЕОРЕМА 2. Ядро (6) допускает представление

$$h_m(j) = \begin{cases} 1 & \text{при } j = 0, \\ \frac{\sin(\pi j/n)}{m \sin(\pi j/N)} & \text{при } j \in 1 : N - 1. \end{cases} \quad (7)$$

Доказательство. При $j = 0$ равенство (7) очевидно.

Пусть $j \in 1 : N - 1$. Тогда

$$\sum_{k=-\mu+1}^{\mu-1} \omega_N^{kj} = \frac{\omega_N^{(-\mu+1)j} - \omega_N^{\mu j}}{1 - \omega_N^j} = \omega_N^{(-\mu+1)j} \frac{1 - \omega_N^j}{1 - \omega_N^j}.$$

Поскольку

$$\begin{aligned} 1 - \omega_n^j &= (1 - \cos(2\pi j/n)) - i \sin(2\pi j/n) = \\ &= -2i \sin(\pi j/n) [\cos(\pi j/n) + i \sin(\pi j/n)] = \\ &= -2i \sin(\pi j/n) \omega_{2n}^j \end{aligned}$$

и, аналогично

$$1 - \omega_N^j = -2i \sin(\pi j/N) \omega_{2N}^j,$$

то при $j \in 1 : N - 1$

$$\frac{1 - \omega_n^j}{1 - \omega_N^j} = \frac{\sin(\pi j/n)}{\sin(\pi j/N)} \omega_{2N}^{(m-1)j}. \quad (8)$$

Остаётся учесть, что

$$\omega_{2N}^{(m-1)j} = \omega_{2N}^{2(\mu-1)j} = \omega_N^{(\mu-1)j}.$$

Теорема доказана. \square

3°. Рассмотрим ещё один частный случай $\nu = N - \mu - 1$. В силу (1), $m = 2\mu$. Формула (2) принимает вид

$$\begin{aligned} h_m(j) &= \frac{1}{m} \sum_{k=-\mu}^{\mu-1} \omega_N^{kj} = \frac{1}{m} \left[\omega_N^{-\mu j} + \sum_{k=-\mu+1}^{\mu-1} \omega_N^{kj} \right] = \\ &= \frac{1}{m} \left[\cos \frac{\pi j}{n} + \sum_{k=-\mu+1}^{\mu-1} \omega_N^{kj} \right] - \frac{i}{m} \sin \frac{\pi j}{n}. \end{aligned}$$

Обозначим

$$\tilde{h}_m(j) = \frac{1}{m} \left[\cos \frac{\pi j}{n} + \sum_{k=-\mu+1}^{\mu-1} \omega_m^{kj} \right].$$

Тогда

$$h_m(j) = \tilde{h}_m(j) - \frac{i}{m} \sin \frac{\pi j}{n}. \quad (9)$$

ТЕОРЕМА 3. Ядро $\tilde{h}_m(j)$ допускает представление

$$\tilde{h}_m(j) = \begin{cases} 1 & \text{при } j = 0, \\ \frac{1}{m} \sin \frac{\pi j}{n} \operatorname{ctg} \frac{\pi j}{N} & \text{при } j \in 1 : N - 1. \end{cases} \quad (10)$$

Доказательство. При $j = 0$ равенство (10) очевидно.

Пусть $j \in 1 : N - 1$. Имеем

$$\sum_{k=-\mu+1}^{\mu-1} \omega_N^{kj} = \frac{\omega_N^{(-\mu+1)j} - \omega_N^{\mu j}}{1 - \omega_N^j} = \omega_N^{-\mu j} \frac{\omega_N^j - \omega_n^j}{1 - \omega_N^j} = -\omega_{2n}^{-j} + \omega_{2n}^{-j} \frac{1 - \omega_n^j}{1 - \omega_N^j}.$$

Воспользуемся формулой (8). Получим

$$\begin{aligned} \sum_{k=-\mu+1}^{\mu-1} \omega_N^{kj} &= -\omega_{2n}^{-j} + \omega_{2n}^{-j} \frac{\sin(\pi j/n)}{\sin(\pi j/N)} = \\ &= -\cos \frac{\pi j}{n} + i \sin \frac{\pi j}{n} + \left(\cos \frac{\pi j}{N} - i \sin \frac{\pi j}{N} \right) \frac{\sin(\pi j/n)}{\sin(\pi j/N)} = \\ &= -\cos \frac{\pi j}{n} + \cos \frac{\pi j}{N} \frac{\sin(\pi j/n)}{\sin(\pi j/N)}. \end{aligned}$$

Мнимая часть оказалась равной нулю. Последнюю формулу перепишем в виде

$$\cos \frac{\pi j}{n} + \sum_{k=-\mu+1}^{\mu-1} \omega_N^{kj} = \sin \frac{\pi j}{n} \operatorname{ctg} \frac{\pi j}{N}.$$

Поделив на m , придем к соотношению

$$\tilde{h}_m(j) = \frac{1}{m} \sin \frac{\pi j}{n} \operatorname{ctg} \frac{\pi j}{N}.$$

Теорема доказана. □

Из (9) и (5) (а также из (10)) следует равенство

$$\tilde{h}_m(ln) = \delta_m(l), \quad l \in \mathbb{Z}. \quad (11)$$

4°. Теорема об отсчётах при $\nu = N - \mu$ (при $m = 2\mu - 1$) связана с интерполяционной задачей

$$\begin{aligned} x(ln) &= z(l), & l \in 0 : m - 1; \\ X(k) &= 0, & k \in \mu : N - \mu. \end{aligned} \quad (12)$$

где $z(l)$ — произвольные числа (вообще говоря, комплексные).

ТЕОРЕМА 4. *Единственным решением задачи (12) является сигнал*

$$x(j) = \sum_{l=0}^{m-1} z(l) h_m(j - ln).$$

Ядро h_m определяется формулами (6), (7).

Доказательство. Условия (12) представляют собой систему из N линейных уравнений с N неизвестными $x(0), x(1), \dots, x(N-1)$. Рассмотрим однородную систему

$$\begin{aligned} x(ln) &= 0, & l &\in 0 : m-1, \\ X(k) &= 0, & k &\in \mu : N-\mu. \end{aligned}$$

Согласно теореме об отсчётах она имеет только нулевое решение. Значит система (12) однозначно разрешима при любых $z(l)$. Теорема доказана. \square

Важно отметить, что при вещественных $z(l)$ интерполяционный сигнал $x(j)$ также вещественный.

5°. Обратимся к случаю $\nu = N - \mu - 1$, когда $m = 2\mu$.

ТЕОРЕМА 5. *Сигнал*

$$x(j) = \sum_{l=0}^{m-1} z(l) \tilde{h}_m(j - ln),$$

где ядро \tilde{h}_m определяется формулой (10), удовлетворяет интерполяционным условиям

$$x(ln) = z(l), \quad l \in 0 : m-1.$$

Доказательство. Согласно (11)

$$x(ln) = \sum_{l'=0}^{m-1} z(l') \tilde{h}_m((l-l')n) = \sum_{l'=0}^{m-1} z(l') \delta_m(l-l') = z(l).$$

Теорема доказана. \square

И здесь вещественные значения $z(l)$ порождают вещественный интерполяционный сигнал $x(j)$.

6°. Задачи интерполяции в пространстве \mathbb{C}_N (и, в частности, задачи оптимальной интерполяции) рассматривались в работах [1, 2, 3].

ЛИТЕРАТУРА

1. Бер М. Г., Малозёмов В. Н. *Об интерполяции дискретных периодических данных* // Проблемы передачи информации. 1992. Т. 28. № 4. С. 60–68.
2. Малозёмов В. Н., Певный А. Б. *Дискретные периодические сплайны и их вычислительные применения* // Журн. вычисл. мат. и матем. физ. 1998. Т. 38. № 8. С. 1235–1246.
3. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Части 1–3. СПб.: НИИММ, 2003. 288 с.

ЖЁСТКИЕ ФРЕЙМЫ

В. Н. Малозёмов

А. Б. Певный

21 февраля 2006 г.

Доклад представляет собой вариации на темы из [1, с. 99–100] и [2]. Основное внимание уделяется примерам жёстких фреймов.

1°. Жёстким фреймом в \mathbb{C}_N называется набор сигналов $\{\psi_1, \dots, \psi_M\}$, $M \geq N$, такой, что при некотором $A > 0$ (константа фрейма) любой сигнал $x \in \mathbb{C}_N$ допускает представление

$$x = \frac{1}{A} \sum_{k=1}^M \langle x, \psi_k \rangle \psi_k. \quad (1)$$

Если все сигналы ψ_k нормированы, то константа A называется также *коэффициентом избыточности*.

Приведём три примера.

ПРИМЕР 1. Пусть $\{u_0, u_1, \dots, u_{N-1}\}$ — ортонормированный базис в \mathbb{C}_N . Повторим этот базис m раз и умножим каждый элемент полученной последовательности на произвольное комплексное число, по модулю равное единице. Другими словами, при $p = sN + k$ положим

$$\psi_p(j) = \alpha_{sk} u_k(j), \quad k \in 0 : N-1, \quad s \in 0 : m-1,$$

где $|\alpha_{sk}| = 1$. Система сигналов $\{\psi_p\}_{p=0}^{mN-1}$ образует жёсткий фрейм с коэффициентом избыточности m . Действительно,

$$\sum_{p=0}^{mN-1} \langle x, \psi_p \rangle \psi_p = \sum_{s=0}^{m-1} \sum_{k=0}^{N-1} \overline{\alpha_{sk}} \langle x, u_k \rangle \alpha_{sk} u_k = mx.$$

В частности, жёстким фреймом в \mathbb{C}_N с коэффициентом избыточности 2 является следующая система, состоящая из $2N$ сигналов:

$$\psi_k = \delta_N(\cdot - k), \quad k \in 0 : N-1; \quad \psi_{N+k} = -\delta_N(\cdot - k), \quad k \in 0 : N-1.$$

ПРИМЕР 2. Рассмотрим сигналы

$$\psi_k(j) = \omega_{mN}^{kj}, \quad j \in 0 : N-1, \quad k \in 0 : mN-1.$$

Считаем, что все ψ_k принадлежат \mathbb{C}_N . Имеем при $j \in 0 : N-1$

$$\begin{aligned} \sum_{k=0}^{mN-1} \langle x, \psi_k \rangle \psi_k(j) &= \sum_{k=0}^{mN-1} \left(\sum_{l=0}^{N-1} x(l) \omega_{mN}^{-kl} \right) \omega_{mN}^{kj} = \\ &= \sum_{l=0}^{N-1} x(l) \sum_{k=0}^{mN-1} \omega_{mN}^{k(j-l)} = mN \sum_{l=0}^{N-1} x(l) \delta_{mN}(j-l) = mNx(j). \end{aligned}$$

Значит, $\{\psi_k\}_{k=0}^{mN-1}$ — фрейм в \mathbb{C}_N с константой mN .

ПРИМЕР 3. Обозначим через ψ_k векторы на плоскости, направленные из начала координат в вершины правильного n -угольника, $n \geq 3$. В формульном виде

$$\psi_k = \left(\sin \frac{2\pi k}{n}, \cos \frac{2\pi k}{n} \right), \quad k \in 0 : n-1.$$

Будем считать ψ_k заданными на основном периоде нормированными сигналами из \mathbb{C}_2 . Покажем, что $\{\psi_k\}_{k=0}^{n-1}$ — фрейм в \mathbb{C}_2 с коэффициентом избыточности $\frac{n}{2}$.

Имеем $\langle x, \psi_k \rangle = x(0) \sin \frac{2\pi k}{n} + x(1) \cos \frac{2\pi k}{n}$. Поскольку

$$\begin{aligned} &\sum_{k=0}^{n-1} \left[x(0) \sin \frac{2\pi k}{n} + x(1) \cos \frac{2\pi k}{n} \right] \sin \frac{2\pi k}{n} = \\ &= \frac{1}{2} x(0) \sum_{k=0}^{n-1} (1 - \cos \frac{4\pi k}{n}) + \frac{1}{2} x(1) \sum_{k=0}^{n-1} \sin \frac{4\pi k}{n}, \\ &\sum_{k=0}^{n-1} \left[x(0) \sin \frac{2\pi k}{n} + x(1) \cos \frac{2\pi k}{n} \right] \cos \frac{2\pi k}{n} = \\ &= \frac{1}{2} x(0) \sum_{k=0}^{n-1} \sin \frac{4\pi k}{n} + \frac{1}{2} x(1) \sum_{k=0}^{n-1} (1 - \cos \frac{4\pi k}{n}) \end{aligned}$$

и при $n \geq 3$

$$\sum_{k=0}^{n-1} \omega_n^{2k} = n\delta_n(2) = 0,$$

то

$$\sum_{k=0}^{n-1} \langle x, \psi_k \rangle \psi_k = \frac{n}{2} x.$$

Утверждение доказано.

2°. Существует эквивалентное определение жёсткого фрейма.

ПРЕДЛОЖЕНИЕ 1. Набор сигналов $\{\psi_k\}_{k=1}^M$ является жёстким фреймом в \mathbb{C}_N с константой A тогда и только тогда, когда для любого сигнала $x \in \mathbb{C}_N$ справедливо равенство

$$\sum_{k=1}^M |\langle x, \psi_k \rangle|^2 = A \|x\|^2. \quad (2)$$

Доказательство. Равенство (2) следует из (1), если последнее умножить скалярно на x . Проверим, что (1) следует из (2).

Воспользуемся формулами

$$\begin{aligned} |x(j) + y(j)|^2 &= |x(j)|^2 + |y(j)|^2 + 2\operatorname{Re}[x(j)\overline{y(j)}], \\ |x(j) + iy(j)|^2 &= |x(j)|^2 + |y(j)|^2 + 2\operatorname{Im}[x(j)\overline{y(j)}]. \end{aligned}$$

С их помощью легко устанавливается так называемое «тождество поляризации»: при любых $x, y \in \mathbb{C}_N$

$$\langle x, y \rangle = \frac{1}{4} [\|x + y\|^2 - \|x - y\|^2 + i\|x + iy\|^2 - i\|x - iy\|^2]. \quad (3)$$

На основании (2) и (3) получаем

$$\begin{aligned} x(j) &= \langle x, \delta_N(j - \cdot) \rangle = \frac{1}{4} [\|x + \delta_N(j - \cdot)\|^2 - \|x - \delta_N(j - \cdot)\|^2 + \\ &+ i\|x + i\delta_N(j - \cdot)\|^2 - i\|x - i\delta_N(j - \cdot)\|^2] = \frac{1}{4A} \sum_{k=1}^M [|\langle x, \psi_k \rangle + \overline{\psi_k(j)}|^2 - \\ &- |\langle x, \psi_k \rangle - \overline{\psi_k(j)}|^2 + i|\langle x, \psi_k \rangle + i\overline{\psi_k(j)}|^2 - i|\langle x, \psi_k \rangle - i\overline{\psi_k(j)}|^2] = \\ &= \frac{1}{A} \sum_{k=1}^M \langle x, \psi_k \rangle \psi_k(j). \end{aligned}$$

Предложение доказано. \square

ПРЕДЛОЖЕНИЕ 2. Если $\{\psi_k\}_{k=1}^M$ — жёсткий фрейм с константой $A = 1$ и если $\|\psi_k\| = 1$ при всех k , то система $\{\psi_k\}_{k=1}^M$ образует ортонормированный базис в \mathbb{C}_N . В частности, необходимо $M = N$.

Доказательство. В силу (1) пространство \mathbb{C}_N является линейной оболочкой сигналов ψ_1, \dots, ψ_M . Остаётся проверить попарную ортогональность этих сигналов. Согласно (2)

$$\|\psi_k\|^2 = \sum_{k'=1}^M |\langle \psi_k, \psi_{k'} \rangle|^2 = \|\psi_k\|^4 + \sum_{k' \neq k} |\langle \psi_k, \psi_{k'} \rangle|^2.$$

Поскольку $\|\psi_k\| = 1$, то $\langle \psi_k, \psi_{k'} \rangle = 0$ при $k \neq k'$.

Предложение доказано. \square

3°. В пространстве \mathbb{C}_N при чётном N , $N = 2N_1$, рассмотрим $m > 2$ фильтров анализа $\tilde{g}_0, \tilde{g}_1, \dots, \tilde{g}_{m-1}$ и столько же фильтров синтеза g_0, g_1, \dots, g_{m-1} . Фильтры анализа, действуя на сигнал $x \in \mathbb{C}_N$, выдают m сигналов d_0, d_1, \dots, d_{m-1} из \mathbb{C}_{N_1} , таких, что их ДПФ $D_i = \mathcal{F}_{N_1}(d_i)$ связаны с ДПФ $X = \mathcal{F}_N(x)$ сигнала x формулой

$$D_i(k) = \frac{1}{2} [\overline{\tilde{g}_i(k)} X(k) + \overline{\tilde{g}_i(k + N_1)} X(k + N_1)], \quad (4)$$

$$k \in 0 : N_1 - 1, \quad i = 0, 1, \dots, m - 1.$$

Спектры D_i имеют период N_1 . Сигналы d_i определяются с помощью обратного ДПФ

$$d_i = \mathcal{F}_{N_1}^{-1}(D_i), \quad i \in 0 : m - 1.$$

Такое определение d_i равносильно следующему: $d_i(k) = y_i(2k)$, $k \in 0 : N_1 - 1$, где $y_i = \mathcal{F}_N^{-1}(\overline{\tilde{g}_i} X)$.

Фильтры синтеза g_0, g_1, \dots, g_{m-1} реконструируют спектр сигнала x по формуле

$$\hat{X}(k) = \sum_{i=0}^{m-1} g_i(k) D_i(k), \quad k \in 0 : N - 1. \quad (5)$$

Сигнал $\hat{x} = \mathcal{F}_N^{-1}(\hat{X})$ принимается за восстановленный x . Если $\hat{x} = x$, то набор $\{\tilde{g}_i, g_i \mid i \in 0 : m - 1\}$ называется *банком фильтров совершенной реконструкции*.

Выведем условие совершенной реконструкции. Перепишем формулу (5) в виде: при $k \in 0 : N_1 - 1$

$$\begin{aligned} \hat{X}(k) &= \sum_{i=0}^{m-1} g_i(k) D_i(k), \\ \hat{X}(k + N_1) &= \sum_{i=0}^{m-1} g_i(k + N_1) D_i(k). \end{aligned} \quad (6)$$

Матрицы преобразований (4) и (6) обозначим $\tilde{P}(k)$ и $P(k)$ соответственно, так что

$$\tilde{P}(k) = \frac{1}{2} \begin{bmatrix} \overline{\tilde{g}_0(k)} & \overline{\tilde{g}_0(k + N_1)} \\ \overline{\tilde{g}_1(k)} & \overline{\tilde{g}_1(k + N_1)} \\ \dots & \dots \\ \overline{\tilde{g}_{m-1}(k)} & \overline{\tilde{g}_{m-1}(k + N_1)} \end{bmatrix},$$

$$P(k) = \begin{bmatrix} g_0(k) & g_1(k) & \dots & g_{m-1}(k) \\ g_0(k + N_1) & g_1(k + N_1) & \dots & g_{m-1}(k + N_1) \end{bmatrix}.$$

Равенство $\widehat{X} = X$, равносильное $\widehat{x} = x$, выполняется тогда и только тогда, когда

$$P(k)\tilde{P}(k) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad k \in 0 : N_1 - 1. \quad (7)$$

4°. Введём сигналы

$$\psi_i = \mathcal{F}_N^{-1}(g_i), \quad i \in 0 : m - 1.$$

ПРЕДЛОЖЕНИЕ 3. *Справедливо разложение*

$$\widehat{x}(j) = \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} d_i(k) \psi_i(j - 2k), \quad j \in \mathbb{Z}. \quad (8)$$

Доказательство. Обозначим $x_i = \mathcal{F}_N^{-1}(g_i D_i)$. Тогда

$$\widehat{x} = x_0 + x_1 + \cdots + x_{m-1}.$$

По определению \mathcal{F}_N^{-1} имеем

$$x_i(j) = \frac{1}{N} \sum_{l=0}^{N-1} g_i(l) D_i(l) \omega_N^{lj}.$$

Поскольку $D_i(l) = \sum_{k=0}^{N_1-1} d_i(k) \omega_{N_1}^{-lk}$ и $\omega_{N_1}^{-lk} = \omega_N^{-2lk}$, то

$$x_i(j) = \sum_{k=0}^{N_1-1} d_i(k) \left\{ \frac{1}{N} \sum_{l=0}^{N-1} g_i(l) \omega_N^{l(j-2k)} \right\} = \sum_{k=0}^{N_1-1} d_i(k) \psi_i(j - 2k).$$

Суммируя по i от 0 до $m - 1$, приходим к (8). □

Разложение (8) будет фреймовым, если

$$d_i(k) = \langle x, \psi_i(\cdot - 2k) \rangle, \quad i \in 0 : m - 1, \quad k \in 0 : N_1 - 1. \quad (9)$$

Выясним, когда выполняется это условие. Так как

$$[\mathcal{F}_N(\psi_i(\cdot - 2k))](l) = \sum_{j=0}^{N-1} \psi_i(j - 2k) \omega_N^{-l(j-2k)-2lk} = \omega_{N_1}^{-lk} g_i(l),$$

то по обобщённому равенству Парсеваля

$$\langle x, \psi_i(\cdot - 2k) \rangle = \frac{1}{N} \sum_{l=0}^{N-1} X(l) \overline{g_i(l)} \omega_{N_1}^{lk}.$$

Вместе с тем, согласно (4)

$$\begin{aligned} d_i(k) &= \frac{1}{2N_1} \sum_{l=0}^{N_1-1} [\overline{\tilde{g}_i(l)}X(l) + \overline{\tilde{g}_i(l+N_1)}X(l+N_1)]\omega_{N_1}^{lk} = \\ &= \frac{1}{N} \sum_{l=0}^{N-1} \overline{\tilde{g}_i(l)}X(l)\omega_{N_1}^{lk}. \end{aligned}$$

Для справедливости равенства (9) при всех $x \in \mathbb{C}_N$ или, что эквивалентно, равенства

$$\frac{1}{N} \sum_{l=0}^{N-1} [\overline{\tilde{g}_i(l)} - \overline{g_i(l)}]X(l)\omega_{N_1}^{kl} = 0, \quad i \in 0 : m-1, \quad k \in 0 : N_1-1,$$

при всех $X \in \mathbb{C}_N$ необходимо и достаточно, чтобы

$$g_i = \tilde{g}_i, \quad i \in 0 : m-1, \quad (10)$$

т. е. чтобы фильтры синтеза совпадали с фильтрами анализа.

Приходим к следующему заключению.

ПРЕДЛОЖЕНИЕ 4. При выполнении условия (10) и условия совершенной реконструкции (7) любой сигнал $x \in \mathbb{C}_N$ можно представить в виде

$$x = \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} \langle x, \psi_i(\cdot - 2k) \rangle \psi_i(\cdot - 2k). \quad (11)$$

Таким образом, система сигналов $\{\psi_i(j-2k)\}$ является жёстким фреймом с константой $A = 1$.

Напомним, что $m > 2$. В силу предложения 2 хотя бы одна из норм $\|\psi_i\|$ отлична от единицы.

5°. Рассмотрим важный частный случай.

По-прежнему считаем, что N чётно, $N = 2N_1$. Пусть $m = 3$. Фильтры, соответствующие трём каналам, традиционно обозначаются h, g_1, g_2 . Условия (7) и (10) в данном случае примут вид

$$|h(k)|^2 + |g_1(k)|^2 + |g_2(k)|^2 = 2, \quad k \in 0 : N-1, \quad (12)$$

$$h(k)\overline{h(k+N_1)} + g_1(k)\overline{g_1(k+N_1)} + g_2(k)\overline{g_2(k+N_1)} = 0, \quad k \in 0 : N_1-1. \quad (13)$$

Построим фильтры h, g_1, g_2 , удовлетворяющие соотношениям (12), (13).

Возьмём нечётное число r и положим

$$\begin{aligned} c &= \left(\cos \frac{\pi k}{N} \right)^{2r}, \quad s = \left(\sin \frac{\pi k}{N} \right)^{2r}, \\ h(k) &= \frac{\sqrt{2}c}{c+s}, \quad g_1(k) = \frac{\sqrt{2}s}{c+s}. \end{aligned} \quad (14)$$

Функция h является аналогом известного фильтра Баттерворта [3].

Фильтр g_2 в силу (12) должен удовлетворять условию

$$|g_2(k)|^2 = 2 - \frac{2c^2+2s^2}{(c+s)^2} = \frac{4}{(c+s)^2} \left(\frac{1}{2} \sin \frac{2\pi k}{N} \right)^{2r}.$$

В качестве g_2 возьмём

$$g_2(k) = \frac{2}{c+s} \left(\frac{1}{2} \sin \frac{2\pi k}{N} \right)^r. \quad (15)$$

Отметим, что $g_2 \in \mathbb{C}_N$ и $g_2(k + N_1) = -g_2(k)$ при всех k в силу нечётности r .

Фильтры (14), (15) удовлетворяют соотношению (12) по построению. Непосредственно проверяется и выполнение соотношения (13):

$$\frac{2cs}{(c+s)^2} + \frac{2sc}{(c+s)^2} - \left(2 - \frac{2c^2+2s^2}{(c+s)^2} \right) = 0.$$

Обозначим $\varphi = \mathcal{F}_N^{-1}(h)$, $\psi = \mathcal{F}_N^{-1}(g_1)$, $\eta = \mathcal{F}_N^{-1}(g_2)$. В силу предложения 4 любой сигнал $x \in \mathbb{C}_N$ допускает представление

$$\begin{aligned} x &= \sum_{k=0}^{N_1-1} \langle x, \varphi(\cdot - 2k) \rangle \varphi(\cdot - 2k) + \sum_{k=0}^{N_1-1} \langle x, \psi(\cdot - 2k) \rangle \psi(\cdot - 2k) + \\ &\quad + \sum_{k=0}^{N_1-1} \langle x, \eta(\cdot - 2k) \rangle \eta(\cdot - 2k). \end{aligned} \quad (16)$$

Поскольку фильтры h и g_1 вещественные и чётные, то такими же будут сигналы φ и ψ . Фильтр g_2 — вещественный и нечётный. Это обеспечивает чётность и чистую мнимость сигнала η . Обозначим $\theta = \operatorname{Im} \eta$, так что $\eta = i\theta$. Сигнал θ является вещественным и нечётным. Нечётность проверяется так:

$$\theta(-j) = \operatorname{Im} \eta(-j) = \operatorname{Im} \overline{\eta(j)} = -\theta(j).$$

На рис. 1 слева изображены фильтры h , g_1 , g_2 вида (14), (15), справа — соответствующие вейвлеты φ , ψ , θ при $r = 3$, $N = 128$.

Отметим, что

$$\langle x, \eta(\cdot - 2k) \rangle \eta(\cdot - 2k) = \langle x, \theta(\cdot - 2k) \rangle \theta(\cdot - 2k),$$

поэтому последнюю сумму в правой части разложения (16) можно заменить суммой

$$\sum_{k=0}^{N_1-1} \langle x, \theta(\cdot - 2k) \rangle \theta(\cdot - 2k).$$

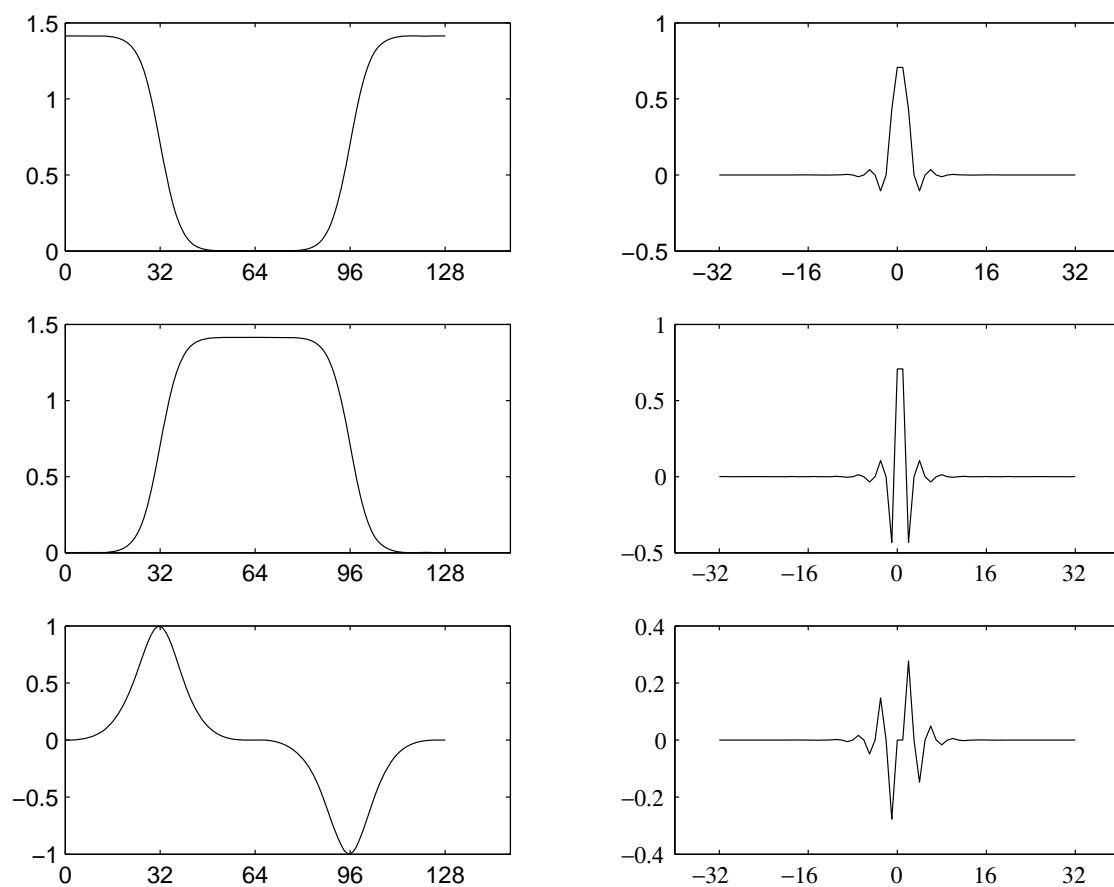


Рис. 1. Фильтры h , g_1 , g_2 (слева) и соответствующие вейвлеты φ , ψ , θ (справа) при $r = 3$, $N = 128$.

6°. Из (12) следует, что

$$\|h\|^2 + \|g_1\|^2 + \|g_2\|^2 = 2N.$$

В силу равенства Парсеваля

$$\|\varphi\|^2 + \|\psi\|^2 + \|\theta\|^2 = 2.$$

В примере, изображённом на рисунке, $\|\varphi\|^2 = \|\psi\|^2 = 0.898$, $\|\theta\|^2 = 0.204$. Обращает на себя внимание малость нормы θ по сравнению с нормами φ и ψ .

ЛИТЕРАТУРА

1. Добеши И. *Десять лекций по вейвлетам*. Пер. с англ. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.
2. Жёлудев В. А., Певный А. Б. *Дискретные периодические фреймы* // Вестник Сыктывкарского Университета. 2006. Вып. 6. С. 87–94.
3. Жёлудев В. А., Певный А. Б. *Вейвлетное преобразование Баттерворта и его реализация с помощью рекурсивных фильтров* // Журн. вычисл. мат. и матем. физ. 2002. Т. 42. № 4. С. 607–618.

ДВОЙСТВЕННАЯ ЛИФТИНГОВАЯ СХЕМА

В. Н. Малозёмов Н. А. Селянинова

14 марта 2006 г.

Прямая лифтинговая схема, основанная на дискретной сплайн-интерполяции по чётным индексам, рассматривалась в [1, 2]. В данном докладе изучается двойственная лифтинговая схема, в которой используется дискретная сплайн-интерполяция по нечётным индексам. Ярким и неожиданным фактом, связывающим эти схемы, является *биортогональность базисов* прямого и двойственного лифтингового разложения.

В идейном плане мы следуем работе [2].

Сохраняются обозначения из предыдущего доклада [1].

1. Предварительные сведения

1.1. Рассмотрим пространство \mathbb{C}_N при $N = 2N_1$. Возьмём сигнал $x \in \mathbb{C}_N$ и разобьём его на две части

$$e(j) = x(2j), \quad d(j) = x(2j + 1).$$

Легко проверяется, что спектры Фурье $X = \mathcal{F}_N(x)$, $E = \mathcal{F}_{N_1}(e)$, $D = \mathcal{F}_{N_1}(d)$ сигналов x , e , d связаны соотношениями: при $k \in 0 : N_1 - 1$

$$\begin{aligned} X(k) &= E(k) + \omega_N^{-k} D(k), \\ X(k + N_1) &= E(k) - \omega_N^{-k} D(k). \end{aligned} \tag{1.1}$$

Формулы (1.1) допускают обращение: при $k \in 0 : N_1 - 1$

$$\begin{aligned} E(k) &= \frac{1}{2} [X(k) + X(k + N_1)], \\ D(k) &= \frac{1}{2} [X(k) - X(k + N_1)] \omega_N^k. \end{aligned} \tag{1.2}$$

1.2. Нам потребуются дискретные периодические сплайны вида

$$S(j) = \sum_{p=0}^{N_1-1} c(p) Q_r(j - 2p - 1), \quad (1.3)$$

где

$$Q_r(j) = \frac{1}{N} \sum_{k=0}^{N-1} \left(2 \cos \frac{\pi k}{N}\right)^{2r} \omega_N^{kj}.$$

Аналогично [3, 4] показывается, что единственным решением интерполяционной задачи

$$S(2l + 1) = d(l), \quad l \in 0 : N_1 - 1,$$

является сплайн S_1 с вектором коэффициентов $c = (c_0, c_1, \dots, c_{N_1-1})$, дискретное преобразование Фурье которого $C = \mathcal{F}_{N_1}(c)$ определяется формулой

$$C(k) = D(k)/T_r(k), \quad k \in 0 : N_1 - 1, \quad (1.4)$$

где

$$T_r(k) = \frac{1}{2} \left[\left(2 \cos \frac{\pi k}{N}\right)^{2r} + \left(2 \sin \frac{\pi k}{N}\right)^{2r} \right].$$

Обозначим $\sigma_1(l) = S_1(2l)$ и найдём $\mathcal{F}_{N_1}(\sigma_1)$. Имеем

$$\sigma_1(l) = \sum_{p=0}^{N_1-1} c(p) Q_r(2l - p - 1)$$

или $\sigma_1 = c * h_r$, где $h_r(l) = Q_r(2l - 1)$. По теореме о свёртке

$$\mathcal{F}_{N_1}(\sigma_1) = \mathcal{F}_{N_1}(c) \mathcal{F}_{N_1}(h_r). \quad (1.5)$$

Вычислим $\mathcal{F}_{N_1}(h_r)$. Поскольку

$$\begin{aligned} [\mathcal{F}_N(Q_r)](k) - [\mathcal{F}_N(Q_r)](k + N_1) &= \sum_{j=0}^{N-1} Q_r(j) \omega_N^{-kj} [1 - (-1)^j] = \\ &= 2 \sum_{l=0}^{N_1-1} Q_r(2l + 1) \omega_N^{-k(2l+1)} = 2 \sum_{l=1}^{N_1} Q_r(2l - 1) \omega_N^{-k(2l-1)} = \\ &= 2 \omega_N^k \sum_{l=0}^{N_1-1} h_r(l) \omega_N^{-kl} = 2 \omega_N^k [\mathcal{F}_{N_1}(h_r)](k), \end{aligned}$$

то

$$[\mathcal{F}_{N_1}(h_r)](k) = \frac{1}{2} \omega_N^{-k} \left[\left(2 \cos \frac{\pi k}{N}\right)^{2r} - \left(2 \sin \frac{\pi k}{N}\right)^{2r} \right].$$

Обозначим

$$U_1(k) = \frac{\left(\cos \frac{\pi k}{N}\right)^{2r} - \left(\sin \frac{\pi k}{N}\right)^{2r}}{\left(\cos \frac{\pi k}{N}\right)^{2r} + \left(\sin \frac{\pi k}{N}\right)^{2r}}.$$

На основании (1.4) и (1.5) получаем

$$[\mathcal{F}_{N_1}(\sigma_1)](k) = \omega_N^{-k} U_1(k) D(k), \quad k \in 0 : N_1 - 1. \quad (1.6)$$

1.3. Напомним определение прямого лифтингового преобразования [1, 2]. Считаем, что $N = 2^s$. Обозначим $N_\nu = N/2^\nu$,

$$U_\nu(k) = \frac{\left(\cos \frac{\pi k}{N_{\nu-1}}\right)^{2r} - \left(\sin \frac{\pi k}{N_{\nu-1}}\right)^{2r}}{\left(\cos \frac{\pi k}{N_{\nu-1}}\right)^{2r} + \left(\sin \frac{\pi k}{N_{\nu-1}}\right)^{2r}}, \quad k \in 0 : N_{\nu-1} - 1, \quad \nu \in 1 : s. \quad (1.7)$$

При каждом $\nu \in 1 : s$ введём два вспомогательных сигнала

$$\tilde{g}_\nu(k) = \omega_{N_{\nu-1}}^k (1 - U_\nu(k)), \quad \tilde{h}_\nu(k) = 1 + \beta_\nu(k)(1 - U_\nu(k)), \quad k \in 0 : N_{\nu-1} - 1. \quad (1.8)$$

Здесь $\beta_\nu(k)$ — произвольная $N_{\nu-1}$ -периодическая функция, удовлетворяющая условию

$$\beta_\nu(k + N_\nu) = -\beta_\nu(k), \quad k \in 0 : N_\nu - 1.$$

Проведём вычисления по следующим рекуррентным формулам:

$$\begin{aligned} E_0 &= \mathcal{F}_N(x); \\ D_\nu(k) &= \frac{1}{2} [\tilde{g}_\nu(k) E_{\nu-1}(k) + \tilde{g}_\nu(k + N_\nu) E_{\nu-1}(k + N_\nu)], \\ E_\nu(k) &= \frac{1}{2} [\tilde{h}_\nu(k) E_{\nu-1}(k) + \tilde{h}_\nu(k + N_\nu) E_{\nu-1}(k + N_\nu)], \\ k &\in 0 : N_\nu - 1, \quad \nu = 1, \dots, s. \end{aligned}$$

Набор спектров $(D_1, D_2, \dots, D_s, E_s)$ называется *прямым лифтинговым преобразованием* сигнала x .

Для обращения прямого лифтингового преобразования введём при каждом $\nu \in 1 : s$ ещё два вспомогательных сигнала

$$h_\nu(k) = 1 + U_\nu(k), \quad g_\nu(k) = \omega_{N_{\nu-1}}^{-k} (1 - \beta_\nu(k)(1 + U_\nu(k))), \quad k \in 0 : N_{\nu-1} - 1. \quad (1.9)$$

Допустим, что известен набор спектров $(D_1, D_2, \dots, D_s, E_s)$. Проведём вычисления по формулам

$$\begin{aligned} E_{\nu-1}(k) &= h_\nu(k) E_\nu(k) + g_\nu(k) D_\nu(k), \\ E_{\nu-1}(k + N_\nu) &= h_\nu(k + N_\nu) E_\nu(k) + g_\nu(k + N_\nu) D_\nu(k), \\ k &\in 0 : N_\nu - 1, \quad \nu = s, s-1, \dots, 1. \end{aligned}$$

При $\nu = 1$ получим спектр E_0 , равный $\mathcal{F}_N(x)$.

1.4. Введём дальнейшие обозначения

$$H_\nu = h_1 h_2 \cdots h_\nu, \quad G_\nu = h_1 \cdots h_{\nu-1} g_\nu, \\ \varphi_\nu = \mathcal{F}_N^{-1}(H_\nu), \quad \psi_\nu = \mathcal{F}_N^{-1}(G_\nu).$$

Как показано в [1, 2], при каждом $t \in 1 : s$ система сигналов

$$\left\{ \left\{ \varphi_t(j - 2^t k) \right\}_{k=0}^{N_t-1}; \left\{ \psi_\nu(j - 2^\nu k) \right\}_{k=0}^{N_\nu-1}, \nu = 1, \dots, t \right\} \quad (1.10)$$

образует базис в \mathbb{C}_N . Более того, для любого сигнала $x \in \mathbb{C}_N$ справедливо прямое лифтинговое разложение

$$x(j) = \sum_{k=0}^{N_t-1} e_t(k) \varphi_t(j - 2^t k) + \sum_{\nu=1}^t \sum_{k=0}^{N_\nu-1} d_\nu(k) \psi_\nu(j - 2^\nu k), \quad j \in \mathbb{Z},$$

где $e_t = \mathcal{F}_{N_t}^{-1}(E_t)$, $d_\nu = \mathcal{F}_{N_\nu}^{-1}(D_\nu)$.

2. Двойственное лифтинговое преобразование

2.1. Сначала рассмотрим случай $N = 2N_1$. Возьмём сигнал $x \in \mathbb{C}_N$. Двойственное лифтинговое преобразование сигнала x осуществляется в три этапа.

Split. Переобозначим $e_0 := x$ и расщепим e_0 на два сигнала

$$\tilde{e}_1(l) = e_0(2l), \quad \tilde{d}_1(l) = e_0(2l+1), \quad l \in 0 : N_1 - 1.$$

Вычислим $\tilde{E}_1 = \mathcal{F}_{N_1}(\tilde{e}_1)$, $\tilde{D}_1 = \mathcal{F}_{N_1}(\tilde{d}_1)$.

Predict. Предскажем значения $\tilde{e}_1(l)$ с помощью интерполяционного сплайна $S_1(j)$ вида (1.3), определяемого условием

$$S_1(2l+1) = \tilde{d}_1(l), \quad l \in 0 : N_1 - 1.$$

Положим $\sigma_1(l) = S_1(2l)$, $l \in 0 : N_1 - 1$. Полусумма

$$e_1(l) = \frac{1}{2} [\tilde{e}_1(l) + \sigma_1(l)],$$

вообще говоря, мало отличается от $\tilde{e}_1(l)$, $l \in 0 : N_1 - 1$. Согласно (1.6)

$$[\mathcal{F}_{N_1}(\sigma_1)](k) = \omega_N^{-k} U_1(k) \tilde{D}_1(k),$$

так что

$$E_1(k) := \mathcal{F}_{N_1}(e_1) = \frac{1}{2} [\tilde{E}_1(k) + \omega_N^{-k} U_1(k) \tilde{D}_1(k)], \quad k \in 0 : N_1 - 1. \quad (2.1)$$

Lifting. Обновим сигнал \tilde{d}_1 . Для этого введём сигнал d_1 , спектр которого $D_1 = \mathcal{F}_{N_1}(d_1)$ определим так:

$$D_1(k) = \tilde{D}_1(k) - 2\alpha_1(k)\omega_N^k E_1(k), \quad k \in 0 : N_1 - 1. \quad (2.2)$$

Здесь α_1 — произвольный N -периодический сигнал, удовлетворяющий условию

$$\alpha_1(k + N_1) = -\alpha_1(k), \quad k \in 0 : N_1 - 1.$$

Ясно, что правая часть (2.2) является N_1 -периодическим сигналом.

Пара (D_1, E_1) называется *двойственным лифтинговым преобразованием сигнала x в спектральной форме*.

2.2. Теперь будем считать, что $N=2^s$. Обозначим $N_\nu = N/2^\nu$. В предыдущем пункте было описано двойственное лифтинговое преобразование $E_0 \rightarrow (D_1, E_1)$. Это преобразование можно продолжить:

$$E_1 \rightarrow (D_2, E_2), \quad E_2 \rightarrow (D_3, E_3), \dots, \quad E_{s-1} \rightarrow (D_s, E_s).$$

Выведем соответствующие формулы. Положим

$$\tilde{p}_\nu(k) = \frac{1}{2}(1+U_\nu(k)), \quad \tilde{q}_\nu(k) = \omega_{N_{\nu-1}}^k(1-\alpha_\nu(k)(1+U_\nu(k))), \quad k \in 0 : N_{\nu-1}-1. \quad (2.3)$$

Здесь $U_\nu(k)$ то же, что и в (1.7), а $\alpha_\nu(k)$ — произвольная $N_{\nu-1}$ -периодическая функция, удовлетворяющая условию

$$\alpha_\nu(k + N_\nu) = -\alpha_\nu(k), \quad k \in 0 : N_\nu - 1.$$

ПРЕДЛОЖЕНИЕ 1. *Справедливы рекуррентные соотношения*

$$\begin{aligned} E_0 &= \mathcal{F}_N(x); \\ E_\nu(k) &= \frac{1}{2} [\tilde{p}_\nu(k)E_{\nu-1}(k) + \tilde{p}_\nu(k + N_\nu)E_{\nu-1}(k + N_\nu)], \\ D_\nu(k) &= \frac{1}{2} [\tilde{q}_\nu(k)E_{\nu-1}(k) + \tilde{q}_\nu(k + N_\nu)E_{\nu-1}(k + N_\nu)], \\ k &\in 0 : N_\nu - 1, \quad \nu = 1, \dots, s. \end{aligned} \quad (2.4)$$

Доказательство проводится так же, как в случае прямой лифтинговой схемы (со ссылкой на формулы (1.2), (2.1) и (2.2)).

Набор спектров $(D_1, D_2, \dots, D_s, E_s)$ называется *полным двойственным лифтинговым преобразованием сигнала x* .

2.3. Для восстановления спектра E_0 исходного сигнала x по $(D_1, D_2, \dots, D_s, E_s)$ введём при каждом $\nu \in 1 : s$ два вспомогательных сигнала

$$p_\nu(k) = 2(1 + \alpha_\nu(k)(1 - U_\nu(k))), \quad q_\nu(k) = \omega_{N_{\nu-1}}^{-k}(1 - U_\nu(k)), \quad k \in 0 : N_{\nu-1} - 1. \quad (2.5)$$

ПРЕДЛОЖЕНИЕ 2. Формулы (2.4) допускают обращение

$$\begin{aligned} E_{\nu-1}(k) &= p_\nu(k)E_\nu(k) + q_\nu(k)D_\nu(k), \\ E_{\nu-1}(k + N_\nu) &= p_\nu(k + N_\nu)E_\nu(k) + q_\nu(k + N_\nu)D_\nu(k), \\ k &\in 0 : N_\nu - 1, \quad \nu = s, s-1, \dots, 1. \end{aligned} \quad (2.6)$$

При $\nu = 1$ получаем $E_0 = \mathcal{F}_N(x)$.

Доказательство опирается на тождества

$$\begin{aligned} p_\nu(k)\tilde{p}_\nu(k) + q_\nu(k)\tilde{q}_\nu(k) &\equiv 2, \\ p_\nu(k)\tilde{p}_\nu(k + N_\nu) + q_\nu(k)\tilde{q}_\nu(k + N_\nu) &\equiv 0. \end{aligned} \quad (2.7)$$

Справедливость равенств (2.6) проверяется справа налево. При этом используются формулы (2.4) и (2.7). \square

ПРЕДЛОЖЕНИЕ 3. Пусть $\nu \in 1 : s$ и $\alpha_\nu = \bar{\beta}_\nu$. Тогда при $k \in 0 : N_{\nu-1} - 1$

$$\begin{aligned} \tilde{p}_\nu(k) &= \frac{1}{2}h_\nu(k), \quad \tilde{q}_\nu(k) = \overline{g_\nu(k)}, \\ \overline{p_\nu(k)} &= 2\tilde{h}_\nu(k), \quad \overline{q_\nu(k)} = \tilde{g}_\nu(k). \end{aligned} \quad (2.8)$$

Доказательство следует из определений (1.8), (1.9), (2.3) и (2.5).

3. Двойственные лифтинговые разложения сигнала

3.1. Введём обозначения

$$\begin{aligned} \tilde{H}_\nu &= \tilde{h}_1\tilde{h}_2 \cdots \tilde{h}_\nu, \quad \tilde{G}_\nu = \tilde{h}_1 \cdots \tilde{h}_{\nu-1}\tilde{g}_\nu, \\ \tilde{\varphi}_\nu &= \mathcal{F}_N^{-1}(\tilde{H}_\nu), \quad \tilde{\psi}_\nu = \mathcal{F}_N^{-1}(\tilde{G}_\nu). \end{aligned}$$

ПРЕДЛОЖЕНИЕ 4. Пусть $N = 2^s$, $t \in 1 : s$, $\alpha_\nu = \bar{\beta}_\nu$ при $\nu \in 1 : t$. Для любого сигнала $x \in \mathbb{C}_N$ справедливо разложение

$$x(j) = 2^t \sum_{k=0}^{N_t-1} e_t(k) \tilde{\varphi}_t(j - 2^t k) + \sum_{\nu=1}^t 2^{\nu-1} \sum_{k=0}^{N_\nu-1} d_\nu(k) \tilde{\psi}_\nu(j - 2^\nu k), \quad j \in \mathbb{Z}, \quad (3.1)$$

где $e_t = \mathcal{F}_{N_t}^{-1}(E_t)$, $d_\nu = \mathcal{F}_{N_\nu}^{-1}(D_\nu)$. Спектры E_t, D_ν вычисляются рекуррентно по формулам (2.4).

Доказательство. Перепишем (2.6) в виде

$$E_{\nu-1} = p_{\nu} E_{\nu} + q_{\nu} D_{\nu}, \quad \nu = 1, \dots, s.$$

По индукции проверяется, что

$$E_0 = p_1 p_2 \cdots p_t E_t + \sum_{\nu=1}^t p_1 \cdots p_{\nu-1} q_{\nu} D_{\nu}.$$

Перепишем последнее равенство в терминах \tilde{h}_{ν} , \tilde{g}_{ν} . Согласно (2.8)

$$E_0 = 2^t \tilde{h}_1 \tilde{h}_2 \cdots \tilde{h}_t E_t + \sum_{\nu=1}^t 2^{\nu-1} \tilde{h}_1 \cdots \tilde{h}_{\nu-1} \tilde{g}_{\nu} D_{\nu}.$$

Применив обратное ДПФ, получим

$$x = 2^t \mathcal{F}_N^{-1}(\tilde{H}_t E_t) + \sum_{\nu=1}^t 2^{\nu-1} \mathcal{F}_N^{-1}(\tilde{G}_{\nu} D_{\nu}). \quad (3.2)$$

Отметим, что

$$\begin{aligned} [\mathcal{F}_N^{-1}(\tilde{G}_{\nu} D_{\nu})](j) &= \frac{1}{N} \sum_{l=0}^{N-1} \tilde{G}_{\nu}(l) D_{\nu}(l) \omega_N^{lj} = \\ &= \frac{1}{N} \sum_{l=0}^{N-1} \tilde{G}_{\nu}(l) \omega_N^{lj} \sum_{k=0}^{N_{\nu}-1} d_{\nu}(k) \omega_{N_{\nu}}^{-lk} = \\ &= \sum_{k=0}^{N_{\nu}-1} d_{\nu}(k) \left\{ \frac{1}{N} \sum_{l=0}^{N-1} \tilde{G}_{\nu}(l) \omega_N^{l(j-2^{\nu}k)} \right\} = \sum_{k=0}^{N_{\nu}-1} d_{\nu}(k) \tilde{\psi}_{\nu}(j - 2^{\nu}k). \end{aligned} \quad (3.3)$$

Аналогично показывается, что

$$[\mathcal{F}_N^{-1}(\tilde{H}_t E_t)](j) = \sum_{k=0}^{N_t-1} e_t(k) \tilde{\varphi}_t(j - 2^t k). \quad (3.4)$$

Подставляя (3.3) и (3.4) в (3.2), приходим к (3.1). \square

Формула (3.1) называется *двойственным лифтинговым разложением сигнала x* .

3.2. Правая часть (3.1) при каждом $t \in 1 : s$ содержит ровно N слагаемых (по размерности пространства \mathbb{C}_N). Поскольку разложение (3.1) справедливо для любого сигнала $x \in \mathbb{C}_N$, то система сигналов

$$\left\{ \left\{ \tilde{\varphi}_t(j - 2^t k) \right\}_{k=0}^{N_t-1} ; \left\{ \tilde{\psi}_\nu(j - 2^\nu k) \right\}_{k=0}^{N_\nu-1}, \nu = 1, \dots, t \right\} \quad (3.5)$$

необходимо является базисом в \mathbb{C}_N .

4. Биортогональность прямого и двойственного базисов

Оказывается, что базис (3.5) двойственного лифтингового разложения биортогонален базису (1.10) прямого лифтингового разложения при каждом $t \in 1 : s$. Точнее, справедливо следующее утверждение.

ПРЕДЛОЖЕНИЕ 5. При любом $\nu \in 1 : s$ и любых целых l, m выполняются равенства

$$\begin{aligned} \langle \varphi_\nu(\cdot - 2^\nu l), \tilde{\varphi}_\nu(\cdot - 2^\nu m) \rangle &= \delta_{N_\nu}(m - l), \\ \langle \varphi_\nu(\cdot - 2^\nu l), \tilde{\psi}_\nu(\cdot - 2^\nu m) \rangle &= 0, \\ \langle \psi_\nu(\cdot - 2^\nu l), \tilde{\psi}_\nu(\cdot - 2^\nu m) \rangle &= \delta_{N_\nu}(m - l), \\ \langle \psi_\nu(\cdot - 2^\nu l), \tilde{\varphi}_\nu(\cdot - 2^\nu m) \rangle &= 0. \end{aligned} \quad (4.1)$$

Доказательство. Введём обозначение $\lambda_{lm} = \langle \varphi_\nu(\cdot - 2^\nu l), \tilde{\varphi}_\nu(\cdot - 2^\nu m) \rangle$. Поскольку

$$\begin{aligned} [\mathcal{F}_N(\varphi_\nu(\cdot - 2^\nu l))](k) &= \omega_{N_\nu}^{-lk} H_\nu(k), \\ [\mathcal{F}_N(\tilde{\varphi}_\nu(\cdot - 2^\nu m))](k) &= \omega_{N_\nu}^{-mk} \tilde{H}_\nu(k), \end{aligned}$$

то по обобщённому равенству Парсеваля

$$\begin{aligned} \lambda_{lm} &= \frac{1}{N} \sum_{k=0}^{N-1} \omega_{N_\nu}^{(m-l)k} H_\nu(k) \overline{\tilde{H}_\nu(k)} = \\ &= \frac{1}{N} \sum_{k=0}^{N-1} \omega_{N_\nu}^{(m-l)k} h_1(k) \tilde{h}_1(k) \cdots h_\nu(k) \tilde{h}_\nu(k). \end{aligned}$$

Отметим, что

$$h_\mu(k) \tilde{h}_\mu(k) = 1 + U_\mu(k) + \beta_\mu(k)(1 - U_\mu^2(k)).$$

Обозначим $\zeta_\mu(k) = U_\mu(k) + \beta_\mu(k)(1 - U_\mu^2(k))$. Очевидно, что ζ_μ — $N_{\mu-1}$ -периодический сигнал, обладающий свойством

$$\zeta_\mu(k + N_\mu) = -\zeta_\mu(k), \quad k \in 0 : N_\mu - 1.$$

В принятых обозначениях

$$\lambda_{lm} = \frac{1}{N} \sum_{k=0}^{N-1} \omega_{N_\nu}^{(m-l)k} (1 + \zeta_1(k)) \cdots (1 + \zeta_\nu(k)).$$

Выражение $(1 + \zeta_2(k)) \cdots (1 + \zeta_\nu(k))$ имеет период N_1 , поэтому

$$\begin{aligned} \lambda_{lm} &= \frac{1}{N} \sum_{k=0}^{N_1-1} \omega_{N_\nu}^{(m-l)k} [1 + \zeta_1(k) + 1 + \zeta_1(k + N_1)] (1 + \zeta_2(k)) \cdots (1 + \zeta_\nu(k)) = \\ &= \frac{1}{N_1} \sum_{k=0}^{N_1-1} \omega_{N_\nu}^{(m-l)k} (1 + \zeta_2(k)) \cdots (1 + \zeta_\nu(k)). \end{aligned}$$

Повторив этот приём ν раз, получим

$$\lambda_{lm} = \frac{1}{N_\nu} \sum_{k=0}^{N_\nu-1} \omega_{N_\nu}^{(m-l)k} = \delta_{N_\nu}(m - l).$$

Остальные соотношения в (4.1) проверяются аналогично. При доказательстве третьего соотношения используется равенство

$$g_\nu(k) \tilde{g}_\nu(k) = 1 - \zeta_\nu(k).$$

Вывод второго и четвёртого соотношений основан на формулах

$$\begin{aligned} h_\nu(k) \tilde{g}_\nu(k) &= \omega_{N_{\nu-1}}^k (1 - U_\nu^2(k)), \\ g_\nu(k) \tilde{h}_\nu(k) &= \omega_{N_{\nu-1}}^{-k} [1 - \beta_\nu(k)(1 + U_\nu(k))] [1 + \beta_\nu(k)(1 - U_\nu(k))], \end{aligned}$$

в силу которых

$$\begin{aligned} h_\nu(k + N_\nu) \tilde{g}_\nu(k + N_\nu) &= -h_\nu(k) \tilde{g}_\nu(k), \\ g_\nu(k + N_\nu) \tilde{h}_\nu(k + N_\nu) &= -g_\nu(k) \tilde{h}_\nu(k). \end{aligned}$$

Предложение доказано. □

ЛИТЕРАТУРА

1. Малозёмов В. Н., Селянинова Н. А. *Прямая лифтинговая схема* // Семинар «DHA & CAGD». Избранные доклады. 26 апреля 2005 г. (<http://dha.spb.ru/rep05.shtml#0426>).
2. Жёлудев В. А., Певный А. Б. *Биортогональные вейвлетные схемы, основанные на интерполяции дискретными сплайнами* // Журн. вычисл. мат. и матем. физ. 2001. Т. 41. № 4. С. 537–548.
3. Малозёмов В. Н., Певный А. Б. *Дискретные периодические сплайны и их вычислительные применения* // Журн. вычисл. мат. и матем. физ. 1998. Т. 38. № 8. С. 1235–1246.
4. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Части 1–3. СПб.: НИИММ, 2003. 288 с.

ФРЕЙМЫ В КОНЕЧНОМЕРНЫХ ПРОСТРАНСТВАХ И ЗАДАЧА МИНИМИЗАЦИИ ФРЕЙМОВОГО ПОТЕНЦИАЛА

А. Б. Певный

28 марта 2006 г.

Излагаются основы теории фреймов в конечномерных пространствах. Приводится подробное решение задачи минимизации фреймового потенциала, основанное на идеях статьи [1].

1°. Система векторов $\{\varphi_i\}_{i=1}^M$ в пространстве \mathbb{C}^N при $M \geq N$ называется *фреймом*, если существуют положительные числа A, B , такие, что

$$A \|x\|^2 \leq \sum_{i=1}^M |\langle x, \varphi_i \rangle|^2 \leq B \|x\|^2, \quad x \in \mathbb{C}^N. \quad (1)$$

Числа A, B называются *границами фрейма*.

Введём вектор-столбцы $\varphi_i = (\varphi_{i1}, \dots, \varphi_{iN})^T$ и матрицу Φ с элементами $\Phi_{ik} = \overline{\varphi}_{ik}$, $i \in 1 : M$, $k \in 1 : N$. Матрица $S = \Phi^* \Phi$ называется *матрицей фрейма*. (Знак $*$ обозначает эрмитово сопряжение — транспонирование плюс комплексное сопряжение.) По определению

$$S_{kl} = \sum_{i=1}^M \Phi_{ki}^* \Phi_{il} = \sum_{i=1}^M \varphi_{ik} \overline{\varphi}_{il}, \quad k, l \in 1 : N. \quad (2)$$

Поскольку

$$(\Phi x)_i = \sum_{k=1}^N \Phi_{ik} x_k = \sum_{k=1}^N x_k \overline{\varphi}_{ik} = \langle x, \varphi_i \rangle, \quad (3)$$

то

$$\sum_{i=1}^M |\langle x, \varphi_i \rangle|^2 = \|\Phi x\|^2 = \langle S x, x \rangle. \quad (4)$$

Согласно (1) эрмитова матрица S положительно определена. Точными границами фрейма являются наименьшее λ_1 и наибольшее λ_N собственные числа матрицы S , т. е. $A = \lambda_1$, $B = \lambda_N$.

2°. По коэффициентам $c_i = \langle x, \varphi_i \rangle$, $i \in 1 : M$, можно восстановить вектор x . Действительно, матрица Φ^* состоит из столбцов $\varphi_1, \dots, \varphi_M$, поэтому

$$\Phi^* y = \sum_{i=1}^M y_i \varphi_i, \quad y \in \mathbb{C}^M. \quad (5)$$

Подставив в (5) $y = \Phi x$, на основании (3) получим

$$Sx = \Phi^* \Phi x = \sum_{i=1}^M (\Phi x)_i \varphi_i = \sum_{i=1}^M \langle x, \varphi_i \rangle \varphi_i. \quad (6)$$

Матрица S имеет обратную S^{-1} , которая также является эрмитовой. Согласно (6)

$$x = S(S^{-1}x) = \sum_{i=1}^M \langle S^{-1}x, \varphi_i \rangle \varphi_i = \sum_{i=1}^M \langle x, S^{-1}\varphi_i \rangle \varphi_i.$$

Обозначим $\widehat{\varphi}_i = S^{-1}\varphi_i$. Тогда

$$x = \sum_{i=1}^M \langle x, \widehat{\varphi}_i \rangle \varphi_i, \quad x \in \mathbb{C}^N. \quad (7)$$

ПРЕДЛОЖЕНИЕ 1. Векторы $\{\widehat{\varphi}_i\}_{i=1}^M$ образуют фрейм с матрицей фрейма $\widehat{S} = S^{-1}$.

Доказательство. Воспользуемся формулой (4). Запишем

$$\begin{aligned} \sum_{i=1}^M |\langle x, \widehat{\varphi}_i \rangle|^2 &= \sum_{i=1}^M |\langle S^{-1}x, \varphi_i \rangle|^2 = \|\Phi S^{-1}x\|^2 = \\ &= \langle \Phi S^{-1}x, \Phi S^{-1}x \rangle = \langle S^{-1}x, x \rangle. \end{aligned} \quad (8)$$

У эрмитовой матрицы S^{-1} наименьшее и наибольшее собственные числа равны соответственно $1/\lambda_N$ и $1/\lambda_1$. Поэтому система $\{\widehat{\varphi}_i\}_{i=1}^M$ является фреймом с точными границами $\widehat{A} = 1/\lambda_N$, $\widehat{B} = 1/\lambda_1$.

Из (8) следует, что $S^{-1} = \widehat{S}$. Вычисление \widehat{S} можно провести и непосредственно. Так как $(\widehat{\Phi})^* = S^{-1}\Phi^*$, то

$$\widehat{S} := (\widehat{\Phi})^* \widehat{\Phi} = S^{-1} \Phi^* \Phi S^{-1} = S^{-1}.$$

Предложение доказано. □

Фрейм $\{\widehat{\varphi}_i\}_{i=1}^M$ называется *каноническим двойственным фреймом*. У фрейма $\{\widehat{\varphi}_i\}_{i=1}^M$ в свою очередь есть канонический двойственный фрейм, совпадающий с исходным фреймом $\{\varphi_i\}_{i=1}^M$. Отсюда, в частности, следует, что наряду с (7) справедливо разложение

$$x = \sum_{i=1}^M \langle x, \varphi_i \rangle \widehat{\varphi}_i, \quad x \in \mathbb{C}^N. \quad (9)$$

3°. Согласно (3) формулу (9) можно переписать так:

$$x = \sum_{i=1}^M (\Phi x)_i \widehat{\varphi}_i = (\widehat{\Phi})^* \Phi x, \quad x \in \mathbb{C}^N.$$

Это значит, что $(\widehat{\Phi})^* \Phi = I_N$. Кроме $(\widehat{\Phi})^*$, могут существовать и другие матрицы $(\widetilde{\Phi})^*$ со столбцами $\widetilde{\varphi}_1, \dots, \widetilde{\varphi}_M$, такие, что

$$(\widetilde{\Phi})^* \Phi = I_N. \quad (10)$$

Если при этом матрица $\widetilde{S} = (\widetilde{\Phi})^* \widetilde{\Phi}$ положительно определена, то система $\{\widetilde{\varphi}_i\}_{i=1}^M$ называется *двойственным фреймом* по отношению к $\{\varphi_i\}_{i=1}^M$.

Из (10) следует, что для любого двойственного фрейма $\{\widetilde{\varphi}_i\}_{i=1}^M$ справедливо разложение

$$x = (\widetilde{\Phi})^* \Phi x = \sum_{i=1}^M \langle x, \varphi_i \rangle \widetilde{\varphi}_i, \quad x \in \mathbb{C}^N. \quad (11)$$

Эрмитово сопряжение обеих частей (10) приводит к формуле $\Phi^* \widetilde{\Phi} = I_N$ и к разложению

$$x = \Phi^* \widetilde{\Phi} x = \sum_{i=1}^M \langle x, \widetilde{\varphi}_i \rangle \varphi_i, \quad x \in \mathbb{C}^N. \quad (12)$$

Итак, двойственный фрейм определяется матрицей $\widetilde{\Phi}$. Чтобы найти все двойственные фреймы, нужно найти все матрицы $\widetilde{\Phi}$, удовлетворяющие соотношению (10), и такие, что матрица $\widetilde{S} = (\widetilde{\Phi})^* \widetilde{\Phi}$ является положительно определённой.

Избыточные разложения (11) и (12) привлекли внимание многих исследователей, занимающихся цифровой обработкой сигналов. Фреймовые разложения более устойчивы к потерям при передаче коэффициентов. Они могут служить инструментом для исправления ошибок, допущенных при передаче по каналам связи.

4°. Рассмотрим произвольные векторы $\varphi_i \in \mathbb{C}^N$, $i \in 1 : M$, $M \geq N$, не предполагая, что они образуют фрейм. Как и в п. 1°, введём матрицу Φ с элементами $\Phi_{ik} = \bar{\varphi}_{ik}$, $i \in 1 : M$, $k \in 1 : N$, и матрицу $S = \Phi^* \Phi$. Поскольку S — неотрицательно определённая эрмитова матрица, то все её собственные числа $\lambda_1, \dots, \lambda_N$ вещественны и неотрицательны.

Известно, что сумма собственных чисел λ_k равна сумме диагональных элементов матрицы S . Последняя называется *следом* матрицы S и обозначается $\text{tr}(S)$. В силу (2)

$$\sum_{k=1}^N \lambda_k = \text{tr}(S) = \sum_{k=1}^N S_{kk} = \sum_{k=1}^N \sum_{i=1}^M |\varphi_{ik}|^2 = \sum_{i=1}^M \|\varphi_i\|^2. \quad (13)$$

Выражение

$$P(\Phi) = P(\varphi_1, \dots, \varphi_M) = \sum_{i,j=1}^M |\langle \varphi_i, \varphi_j \rangle|^2$$

называется *фреймовым потенциалом*.

ПРЕДЛОЖЕНИЕ 2. *Справедливо равенство*

$$P(\Phi) = \text{tr}(S^2). \quad (14)$$

Доказательство. Имеем

$$P(\Phi) = \sum_{i,j=1}^M \langle \varphi_i, \varphi_j \rangle \langle \varphi_j, \varphi_i \rangle = \sum_{i,j=1}^M \sum_{k=1}^N \varphi_{ik} \bar{\varphi}_{jk} \sum_{l=1}^N \varphi_{jl} \bar{\varphi}_{il}. \quad (15)$$

Далее, поскольку S — эрмитова матрица, то

$$S_{lk} = \bar{S}_{kl}, \quad (S^2)_{kk} = \sum_{l=1}^N S_{kl} \bar{S}_{kl}.$$

Отсюда в силу (2) следует, что

$$\text{tr}(S^2) = \sum_{k,l=1}^N S_{kl} \bar{S}_{kl} = \sum_{k,l=1}^N \sum_{i=1}^M \varphi_{ik} \bar{\varphi}_{il} \sum_{j=1}^M \bar{\varphi}_{jk} \varphi_{jl}. \quad (16)$$

Сравнивая (15) и (16), приходим к (14). Предложение доказано. \square

ПРЕДЛОЖЕНИЕ 3. Для любого набора векторов $\varphi_1, \dots, \varphi_M$ из \mathbb{C}^N справедливо неравенство

$$P(\Phi) \geq \frac{1}{N} \left(\sum_{i=1}^M \|\varphi_i\|^2 \right)^2. \quad (17)$$

Доказательство. Собственными числами матрицы S^2 являются $\lambda_1^2, \dots, \lambda_N^2$, так что

$$\text{tr}(S^2) = \sum_{k=1}^N \lambda_k^2. \quad (18)$$

Воспользуемся неравенством между средним арифметическим и средним квадратичным:

$$\frac{1}{N} \sum_{k=1}^N \lambda_k \leq \left(\frac{1}{N} \sum_{k=1}^N \lambda_k^2 \right)^{1/2}. \quad (19)$$

На основании (14), (18) и (19) получим

$$P(\Phi) \geq \frac{1}{N} \left(\sum_{k=1}^N \lambda_k \right)^2.$$

Остаётся воспользоваться формулой (13). Предложение доказано. \square

5°. Равенство в (17) достигается тогда и только тогда, когда неравенство (19) выполняется как равенство, что возможно лишь при $\lambda_1 = \dots = \lambda_N =: \lambda$. В этом случае $S = \lambda I_N$ и согласно (4)

$$\sum_{i=1}^M |\langle x, \varphi_i \rangle|^2 = \lambda \|x\|^2, \quad x \in \mathbb{C}^N. \quad (20)$$

Выполнение условия (20) означает, что система $\{\varphi_i\}_{i=1}^M$ является *жестким фреймом* (с константой λ). Таким образом, неравенство (17) обращается в равенство на жестких фреймах и только на них.

6°. Приведём конструкцию, позволяющую получать жесткие фреймы с константой $\lambda > 0$ в неограниченном количестве. Возьмём ортогональную $(M \times M)$ -матрицу F со столбцами F_1, \dots, F_M , у которых $\|F_k\|^2 = \lambda$ при всех $k \in 1 : M$. Из первых N столбцов составим $(M \times N)$ -матрицу Φ . Рассмотрим сопряжённую матрицу Φ^* размера $N \times M$ и её столбцы обозначим $\varphi_1, \dots, \varphi_M$.

Система $\{\varphi_i\}_{i=1}^M$ образует жёсткий фрейм с константой λ , поскольку

$$\begin{aligned} (\Phi^* \Phi)_{ik} &= \sum_{l=1}^M \Phi_{il}^* \Phi_{lk} = \sum_{l=1}^M \Phi_{lk} \bar{\Phi}_{li} = \\ &= \langle F_k, F_i \rangle = \begin{cases} \lambda & \text{при } k = i, \\ 0 & \text{при } k \neq i. \end{cases} \end{aligned}$$

Указанная конструкция имеет общий характер. Пусть $S = \Phi^* \Phi$ — матрица жёсткого фрейма с константой $\lambda > 0$. Покажем, что с помощью добавления $M - N$ столбцов от матрицы Φ можно перейти к ортогональной $(M \times M)$ -матрице F , у которой квадрат нормы каждого столбца равен λ .

По условию $\Phi^* \Phi = \lambda I_N$, так что столбцы матрицы Φ ортогональны и квадрат нормы каждого из них равен λ . Эти столбцы можно дополнить $M - N$ столбцами до ортогонального базиса в \mathbb{C}^M , причём так, чтобы квадрат нормы новых столбцов также равнялся λ . Расширенная матрица и будет требуемой матрицей F .

7°. Обозначим через Ω множество наборов $\{\varphi_1, \dots, \varphi_M\}$ векторов из \mathbb{C}^N , таких, что

$$\sum_{i=1}^M \|\varphi_i\|^2 = b.$$

Здесь $b > 0$ — фиксированное число. Рассмотрим экстремальную задачу

$$P(\varphi_1, \dots, \varphi_M) \rightarrow \min_{\{\varphi_1, \dots, \varphi_M\} \in \Omega}. \quad (21)$$

ПРЕДЛОЖЕНИЕ 4. Минимальное значение потенциала P на множестве Ω равно b^2/N . Множество решений задачи (21) совпадает с множеством жёстких фреймов с константой b/N .

Доказательство. Пусть $\{\varphi_1^0, \dots, \varphi_M^0\}$ — жёсткий фрейм с константой b/N . Тогда матрица фрейма имеет вид $S = \frac{b}{N} I_N$. Согласно (13)

$$\sum_{i=1}^M \|\varphi_i^0\|^2 = \text{tr}(S) = b,$$

т. е. $\{\varphi_1^0, \dots, \varphi_M^0\} \in \Omega$. При этом в силу (14)

$$P(\varphi_1^0, \dots, \varphi_M^0) = \text{tr}(S^2) = \frac{b^2}{N}.$$

В то же время, на основании (17) для любого набора $\{\varphi_1, \dots, \varphi_M\}$ из Ω справедливо неравенство

$$P(\varphi_1, \dots, \varphi_M) \geq \frac{b^2}{N}.$$

Значит, минимальное значение потенциала в задаче (21) равно b^2/N и достигается на указанных выше жёстких фреймах. Покажем, что только на них.

Пусть $\{\varphi_1, \dots, \varphi_M\} \in \Omega$ и $P(\varphi_1, \dots, \varphi_M) = b^2/N$. Как обычно, собственные числа матрицы $S = \Phi^* \Phi$ обозначим $\lambda_1, \dots, \lambda_N$. Согласно (14), (18), (19) и (13) имеем

$$\frac{b^2}{N} = P(\varphi_1, \dots, \varphi_M) = \sum_{k=1}^N \lambda_k^2 \geq \frac{1}{N} \left(\sum_{k=1}^N \lambda_k \right)^2 = \frac{1}{N} \left(\sum_{i=1}^M \|\varphi_i\|^2 \right)^2 = \frac{b^2}{N}. \quad (22)$$

Отсюда следует, что $\lambda_1 = \dots = \lambda_N =: \lambda$, $S = \lambda I_N$ и в силу (20)

$$\sum_{i=1}^M |\langle x, \varphi_i \rangle|^2 = \lambda \|x\|^2, \quad x \in \mathbb{C}^N.$$

Соотношения (22) приводят также к равенству $N\lambda^2 = b^2/N$. Ввиду неотрицательности λ получаем $\lambda = b/N$. Таким образом, набор $\{\varphi_1, \dots, \varphi_M\}$ является жёстким фреймом с константой b/N .

Предложение доказано. □

ЛИТЕРАТУРА

1. Casazza P. G. *Custom building finite frames* // Contemporary Math. 2004. V. 345. P. 61–86.

БАНКИ ФИЛЬТРОВ И ФРЕЙМЫ

В. А. Жёлудев В. Н. Малозёмов А. Б. Певный

30 марта 2006 г.

Предлагается общий метод построения фреймов в пространстве дискретных периодических сигналов чётной размерности $N = 2N_1$, состоящих из mN_1 сигналов при $m > 2$. Метод основан на использовании банков фильтров совершенной реконструкции. В качестве приложения при $m = 3$ на базе фильтров Баттерворта построено новое семейство вещественных фреймов. Найдены точные границы таких фреймов.

1. ВВЕДЕНИЕ

В докладе будут использоваться следующие обозначения:

\mathbb{C}_N — пространство сигналов (комплекснозначных N -периодических функций целочисленного аргумента $x = x(j)$, $j \in \mathbb{Z}$),

$\langle x, y \rangle = \sum_{j=0}^{N-1} x(j) \overline{y(j)}$ — скалярное произведение сигналов x и y ,

$\omega_N = \exp(2\pi i/N)$ — корень N -й степени из единицы,

\mathcal{F}_N — дискретное преобразование Фурье (ДПФ) порядка N , сопоставляющее сигналу x сигнал $X = \mathcal{F}_N(x)$ с компонентами

$$X(k) = \sum_{j=0}^{N-1} x(j) \omega_N^{-kj}, \quad k \in \mathbb{Z}.$$

Система сигналов $\varphi_1, \varphi_2, \dots, \varphi_M$, $M \geq N$, называется *фреймом*, если существуют положительные числа A, B такие, что для всех $x \in \mathbb{C}_N$

$$A \|x\|^2 \leq \sum_{i=1}^M |\langle x, \varphi_i \rangle|^2 \leq B \|x\|^2.$$

Константы A, B называются *границами фрейма*. Начальные сведения о фреймах имеются в [1, 2].

Иницилирующими для нас были работы [3, 4], где строились фреймы в пространстве $\ell^2(\mathbb{Z})$. Но для дискретного гармонического анализа представляет интерес и N -периодический случай. При построении фреймов в \mathbb{C}_N может быть использован эффективный аппарат дискретного преобразования Фурье [5].

Одним из важных источников, приводящих к фреймам, являются банки фильтров совершенной реконструкции. О них пойдёт речь в разд. 2. Особенность периодического случая состоит в том, что фильтры задаются своими частотными характеристиками. На основе результатов разд. 2 в разд. 3 строятся пары двойственных фреймов. В разд. 4 как частный случай строится семейство вещественных фреймов Баттерворта, которые могут найти применение в цифровой обработке сигналов. Для таких фреймов найдены точные границы.

2. БАНКИ ФИЛЬТРОВ

2.1. Следуя основополагающей статье [3], рассмотрим банк из m фильтров анализа и m фильтров синтеза, где $m > 2$. Но в отличие от [3], будем предполагать, что все сигналы и фильтры являются N -периодическими. Считаем также, что N – чётное число, $N = 2N_1$.

Начнём с m фильтров анализа $\tilde{g}_0, \tilde{g}_1, \dots, \tilde{g}_{m-1}$ из \mathbb{C}_N , которые, действуя на сигнал $x \in \mathbb{C}_N$, выдают m сигналов d_0, d_1, \dots, d_{m-1} из \mathbb{C}_{N_1} , таких, что их ДПФ $D_i = \mathcal{F}_{N_1}(d_i)$ связаны с ДПФ $X = \mathcal{F}_N(x)$ сигнала x формулой

$$D_i(k) = \frac{1}{2} \left[\overline{\tilde{g}_i(k)} X(k) + \overline{\tilde{g}_i(k + N_1)} X(k + N_1) \right], \quad (2.1)$$

$$k \in 0 : N_1 - 1, \quad i = 0, 1, \dots, m - 1.$$

Спектры D_i имеют период N_1 . Сигналы d_i определяются с помощью обратного ДПФ,

$$d_i = \mathcal{F}_{N_1}^{-1}(D_i), \quad i = 0, 1, \dots, m - 1. \quad (2.2)$$

Такое определение $\{d_i\}$ равносильно следующему: $d_i(k) = y_i(2k)$, $k \in 0 : N_1 - 1$, где $y_i = \mathcal{F}_N^{-1}(\overline{\tilde{g}_i} X)$.

Фильтры синтеза g_0, g_1, \dots, g_{m-1} из \mathbb{C}_N реконструируют спектр сигнала x по формуле

$$\hat{X}(k) = \sum_{i=0}^{m-1} g_i(k) D_i(k), \quad k \in 0 : N - 1. \quad (2.3)$$

Сигнал $\hat{x} = \mathcal{F}_N^{-1}(\hat{X})$ принимается за восстановленный сигнал x . Если $\hat{x} = x$, то набор $\{\tilde{g}_i, g_i \mid i \in 0 : m-1\}$ называется *банком фильтров совершенной реконструкции*.

2.2. Выведем условие совершенной реконструкции. Запишем формулу (2.3) в виде: при $k \in 0 : N_1 - 1$

$$\begin{aligned}\hat{X}(k) &= \sum_{i=0}^{m-1} g_i(k) D_i(k), \\ \hat{X}(k + N_1) &= \sum_{i=0}^{m-1} g_i(k + N_1) D_i(k).\end{aligned}\tag{2.4}$$

Матрицы преобразований (2.1) и (2.4) обозначим $\tilde{P}(k)$ и $P(k)$ соответственно, так что

$$\begin{aligned}\tilde{P}(k) &= \frac{1}{2} \begin{bmatrix} \overline{\tilde{g}_0(k)} & \overline{\tilde{g}_0(k + N_1)} \\ \overline{\tilde{g}_1(k)} & \overline{\tilde{g}_1(k + N_1)} \\ \vdots & \vdots \\ \overline{\tilde{g}_{m-1}(k)} & \overline{\tilde{g}_{m-1}(k + N_1)} \end{bmatrix}, \\ P(k) &= \begin{bmatrix} g_0(k) & g_1(k) & \cdots & g_{m-1}(k) \\ g_0(k + N_1) & g_1(k + N_1) & \cdots & g_{m-1}(k + N_1) \end{bmatrix}.\end{aligned}$$

Равенство $\hat{X} = X$, равносильное $\hat{x} = x$, выполняется тогда и только тогда, когда

$$P(k) \tilde{P}(k) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad k \in 0 : N_1 - 1.\tag{2.5}$$

3. РАЗЛОЖЕНИЕ СИГНАЛОВ ПО ФРЕЙМУ

3.1. Введём сигналы

$$\psi_i = \mathcal{F}_N^{-1}(g_i), \quad \tilde{\psi}_i = \mathcal{F}_N^{-1}(\tilde{g}_i), \quad i \in 0 : m-1.$$

ПРЕДЛОЖЕНИЕ 1. *Справедливо разложение*

$$\hat{x}(j) = \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} d_i(k) \psi_i(j - 2k), \quad j \in \mathbb{Z},\tag{3.1}$$

где коэффициенты $d_i(k)$ определяются формулой (2.2).

Доказательство. Обозначим $x_i = \mathcal{F}_N^{-1}(g_i D_i)$. Тогда

$$\widehat{x} = x_0 + x_1 + \cdots + x_{m-1}.$$

По определению \mathcal{F}_N^{-1} имеем

$$x_i(j) = \frac{1}{N} \sum_{l=0}^{N-1} g_i(l) D_i(l) \omega_N^{lj}.$$

Поскольку $D_i(l) = \sum_{k=0}^{N_1-1} d_i(k) \omega_{N_1}^{-lk}$ и $\omega_{N_1}^{-lk} = \omega_N^{-2lk}$, то

$$x_i(j) = \sum_{k=0}^{N_1-1} d_i(k) \left\{ \frac{1}{N} \sum_{l=0}^{N-1} g_i(l) \omega_N^{l(j-2k)} \right\} = \sum_{k=0}^{N_1-1} d_i(k) \psi_i(j-2k).$$

Суммируя по i от 0 до $m-1$, придём к (3.1). \square

ПРЕДЛОЖЕНИЕ 2. *Справедливы равенства*

$$d_i(k) = \langle x, \widetilde{\psi}_i(\cdot - 2k) \rangle, \quad i \in 0 : m-1, \quad k \in N_1-1. \quad (3.2)$$

Доказательство. Имеем

$$\begin{aligned} \left[\mathcal{F}_N(\widetilde{\psi}_i(\cdot - 2k)) \right](l) &= \sum_{j=0}^{N-1} \widetilde{\psi}_i(j-2k) \omega_N^{-2(j-2k)-2lk} = \\ &= \omega_N^{-2lk} \sum_{j=0}^{N-1} \widetilde{\psi}_i(j) \omega_N^{-lj} = \omega_{N_1}^{-lk} \widetilde{g}_i(l). \end{aligned}$$

По обобщённому равенству Парсеваля

$$\langle x, \widetilde{\psi}_i(\cdot - 2k) \rangle = \frac{1}{N} \sum_{l=0}^{N-1} X(l) \overline{\widetilde{g}_i(l)} \omega_{N_1}^{lk}. \quad (3.3)$$

Вместе с тем, по определению d_i равны $\mathcal{F}_{N_1}^{-1}(D_i)$, где D_i задаются формулой (2.1), так что

$$\begin{aligned} d_i(k) &= \frac{1}{2N_1} \sum_{l=0}^{N_1-1} \left[\overline{\widetilde{g}_i(l)} X(l) + \overline{\widetilde{g}_i(l+N_1)} X(l+N_1) \right] \omega_{N_1}^{kl} = \\ &= \frac{1}{N} \sum_{l=0}^{N-1} \overline{\widetilde{g}_i(l)} X(l) \omega_{N_1}^{kl}. \end{aligned} \quad (3.4)$$

Из (3.3) и (3.4) следует (3.2). \square

На основании предложений 1 и 2 приходим, в частности, к такому заключению: *при выполнении условия совершенной реконструкции (2.5) любой сигнал $x \in \mathbb{C}_N$ допускает представление*

$$x = \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} \langle x, \tilde{\psi}_i(j-2k) \rangle \psi_i(j-2k). \quad (3.5)$$

3.2. Теперь можно ввести пару двойственных фреймов.

ПРЕДЛОЖЕНИЕ 3. Пусть выполнено условие совершенной реконструкции (2.5). Системы сигналов

$$\{\psi_i(j-2k) \mid k \in 0 : N_1-1, i \in 0 : m-1\}, \quad (3.6)$$

$$\{\tilde{\psi}_i(j-2k) \mid k \in 0 : N_1-1, i \in 0 : m-1\} \quad (3.7)$$

являются фреймами в \mathbb{C}_N . Наряду с разложением (3.5) имеет место разложение

$$x = \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} \langle x, \psi_i(\cdot-2k) \rangle \tilde{\psi}_i(\cdot-2k), \quad x \in \mathbb{C}_N. \quad (3.8)$$

Фреймы (3.6) и (3.7) называются *двойственными*.

Доказательство. Разберёмся сначала с системой (3.7). Обозначим

$$\tilde{S}(x) = \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} |\langle x, \tilde{\psi}_i(\cdot-2k) \rangle|^2.$$

В силу (3.2) и равенства Парсеваля

$$\tilde{S}(x) = \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} |d_i(k)|^2 = \frac{1}{N_1} \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} |D_i(k)|^2.$$

Введём вектор-столбец $D(k) = (D_0(k), D_1(k), \dots, D_{m-1}(k))^T$. Согласно определению матрицы $\tilde{P}(k)$

$$D(k) = \tilde{P}(k) X_k, \quad k \in 0 : N_1-1,$$

где $X_k = (X(k), X(k+N_1))^T$. При этом

$$\|D(k)\|^2 = \langle \tilde{P}(k) X_k, \tilde{P}(k) X_k \rangle = \langle (\tilde{P}(k))^* \tilde{P}(k) X_k, X_k \rangle.$$

Звёздочка означает эрмитово сопряжение.

Из условия совершенной реконструкции (2.5) следует, что $\text{rank } \tilde{P}(k) = 2$ при всех k . Значит, квадратная матрица второго порядка $\tilde{H}(k) = (\tilde{P}(k))^* \tilde{P}(k)$ является эрмитовой и положительно определённой. Пусть $0 < \tilde{\lambda}_1(k) \leq \tilde{\lambda}_2(k)$ её собственные числа. Тогда для величины

$$\tilde{S}(x) = \frac{1}{N_1} \sum_{k=0}^{N_1-1} \|D(k)\|^2 = \frac{1}{N_1} \sum_{k=0}^{N_1-1} \langle \tilde{H}(k) X_k, X_k \rangle$$

справедливы оценки

$$\frac{2}{N} \sum_{k=0}^{N_1-1} \tilde{\lambda}_1(k) \|X_k\|^2 \leq \tilde{S}(x) \leq \frac{2}{N} \sum_{k=0}^{N_1-1} \tilde{\lambda}_2(k) \|X_k\|^2.$$

Положим

$$\tilde{A} = 2 \min_{k \in 0:N_1-1} \tilde{\lambda}_1(k), \quad \tilde{B} = 2 \max_{k \in 0:N_1-1} \tilde{\lambda}_2(k)$$

и учтём, что $\frac{1}{N} \sum_{k=0}^{N_1-1} \|X_k\|^2 = \frac{1}{N} \|X\|^2 = \|x\|^2$. Придём к неравенствам

$$\tilde{A} \|x\|^2 \leq \tilde{S}(x) \leq \tilde{B} \|x\|^2.$$

Значит, система (3.7) является фреймом в \mathbb{C}_N с границами \tilde{A}, \tilde{B} .

Утверждение о фреймовости системы (3.6) проверяется аналогично, только нужно поменять местами фильтры анализа и фильтры синтеза.

Итак, пусть теперь $\{g_i\}_{i=0}^{m-1}$ — фильтры анализа, а $\{\tilde{g}_i\}_{i=0}^{m-1}$ — фильтры синтеза. Тогда формула декомпозиции примет вид

$$D(k) = Q(k) X_k, \quad k \in 0 : N_1 - 1,$$

а формула реконструкции запишется так:

$$(\hat{X}(k), \hat{X}(k + N_1))^T = \tilde{Q}(k) D(k), \quad k \in 0 : N_1 - 1.$$

Здесь

$$Q(k) = \frac{1}{2} \begin{bmatrix} \overline{g_0(k)} & \overline{g_0(k + N_1)} \\ \overline{g_1(k)} & \overline{g_1(k + N_1)} \\ \vdots & \vdots \\ \overline{g_{m-1}(k)} & \overline{g_{m-1}(k + N_1)} \end{bmatrix},$$

$$\tilde{Q}(k) = \begin{bmatrix} \tilde{g}_0(k) & \tilde{g}_1(k) & \cdots & \tilde{g}_{m-1}(k) \\ \tilde{g}_0(k + N_1) & \tilde{g}_1(k + N_1) & \cdots & \tilde{g}_{m-1}(k + N_1) \end{bmatrix}.$$

Очевидно, что $Q(k) = \frac{1}{2}(P(k))^*$, $\tilde{Q}(k) = 2(\tilde{P}(k))^*$. Согласно (2.5)

$$\tilde{Q}(k) Q(k) = (\tilde{P}(k))^* (P(k))^* = [P(k) \tilde{P}(k)]^* = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

т. е. для нового банка фильтров также выполнено условие совершенной реконструкции. Отсюда следует справедливость формулы (3.8).

Аналогично предыдущему величина

$$S(x) = \sum_{i=0}^{m-1} \sum_{k=0}^{N_1-1} |\langle x, \psi_i(\cdot - 2k) \rangle|^2$$

преобразуется к виду

$$S(x) = \frac{1}{N_1} \sum_{k=0}^{N_1-1} \langle H(k) X_k, X_k \rangle,$$

где $H(k) = (Q(k))^* Q(k)$ — эрмитова положительно определённая матрица второго порядка. Пусть $0 < \lambda_1(k) \leq \lambda_2(k)$ её собственные числа. Положив

$$A = 2 \min_{k \in 0:N_1-1} \lambda_1(k), \quad B = 2 \max_{k \in 0:N_1-1} \lambda_2(k),$$

придём к неравенствам

$$A \|x\|^2 \leq S(x) \leq B \|x\|^2.$$

Значит, система (3.6) является фреймом в \mathbb{C}_N с границами A, B .

Предложение доказано. \square

4. ФРЕЙМЫ БАТТЕРВОРТА

4.1. Рассмотрим частный случай теории, полезный для цифровой обработки сигналов. По-прежнему считаем, что N — чётное число, $N = 2N_1$.

Пусть $m = 3$. Фильтры анализа будем традиционно обозначать $\tilde{h}(k)$, $\tilde{g}_1(k)$, $\tilde{g}_2(k)$, а фильтры синтеза — $h(k)$, $g_1(k)$, $g_2(k)$. Условия совершенной реконструкции (2.5) перепишутся в виде

$$h(k) \tilde{h}(k) + g_1(k) \tilde{g}_1(k) + g_2(k) \tilde{g}_2(k) = 2, \quad k \in 0 : N - 1, \quad (4.1)$$

$$h(k) \overline{\tilde{h}(k + N_1)} + g_1(k) \overline{\tilde{g}_1(k + N_1)} + g_2(k) \overline{\tilde{g}_2(k + N_1)} = 0, \quad k \in 0 : N - 1. \quad (4.2)$$

С точки зрения цифровой обработки сигналов желательны фильтры, которые являются дробно-рациональными функциями от ω_N^k . Дробно-рациональные фильтры, удовлетворяющие условиям (4.1) и (4.2), можно построить на основе фильтров Баттерворта.

4.2. Возьмём натуральное число $r \geq 2$ и положим

$$c = \left(\cos \frac{k\pi}{N} \right)^{2r}, \quad s = \left(\sin \frac{k\pi}{N} \right)^{2r},$$

$$h(k) = \tilde{h}(k) = \frac{\sqrt{2}c}{c+s}, \quad g_1(k) = \tilde{g}_1(k) = \frac{\sqrt{2}s}{c+s}.$$

Функция $h(k)$ представляет собой аналог фильтра Баттерворта [6]. Фильтры $g_2(k)$, $\tilde{g}_2(k)$ в силу (4.1) должны удовлетворять соотношению

$$g_2(k) \overline{\tilde{g}_2(k)} = 2 - \frac{2c^2 + 2s^2}{(c+s)^2} = \frac{4cs}{(c+s)^2} = \frac{4}{(c+s)^2} \left(\frac{1}{2} \sin \frac{2k\pi}{N} \right)^{2r}. \quad (4.3)$$

Получили задачу факторизации: разбить правую часть (4.3) на два множителя $g_2(k)$, $\tilde{g}_2(k)$ так, чтобы выполнялось условие (4.2).

Выберем два чётных числа p, q , в сумме равных $2r$, $p + q = 2r$. Положим

$$g_2(k) = \omega_N^k \frac{2}{c+s} \left(\frac{1}{2} \sin \frac{2k\pi}{N} \right)^p, \quad \tilde{g}_2(k) = \omega_N^k \frac{2}{c+s} \left(\frac{1}{2} \sin \frac{2k\pi}{N} \right)^q. \quad (4.4)$$

В этом случае соотношение (4.3) (а значит, и (4.1)) выполняется. Отметим, что в силу чётности q

$$\overline{\tilde{g}_2(k + N_1)} = -\omega_N^{-k} \frac{2}{c+s} \left(\frac{1}{2} \sin \frac{2k\pi}{N} \right)^q.$$

Теперь легко проверить, что и соотношение (4.2) выполняется.

При чётном r выделяется вариант $p = q = r$, когда $g_2(k) = \tilde{g}_2(k)$. Поскольку по условию $h(k) = \tilde{h}(k)$ и $g_1(k) = \tilde{g}_1(k)$, то получаем, что фильтры синтеза полностью совпадают с фильтрами анализа. Это приводит к жёсткому фрейму [7].

4.3. Построенные фильтры являются дробно-рациональными функциями от $z = \omega_N^k$, так как

$$4 \cos^2 \frac{k\pi}{N} = z + 2 + z^{-1}, \quad 4 \sin^2 \frac{k\pi}{N} = -z + 2 - z^{-1}.$$

В случае дробно-рациональных фильтров декомпозицию и реконструкцию сигнала $x \in \mathbb{C}_N$ можно осуществить за $O(N)$ операций. Подробнее об этом в [6].

4.4. Очевидно, что сигналы h и g_1 вещественные и чётные. Поэтому вейлеты $\varphi = \mathcal{F}_N^{-1}(h)$ и $\psi = \mathcal{F}_N^{-1}(g_1)$ чётные и вещественные (рис. 1).

Сигналы (4.4) являются чётными. Например, для g_2 в силу чётности p имеем

$$g_2(-k) = \omega_N^{-k} \frac{2}{c+s} \left(\frac{1}{2} \sin \frac{2k\pi}{N} \right)^p = \overline{g_2(k)}.$$

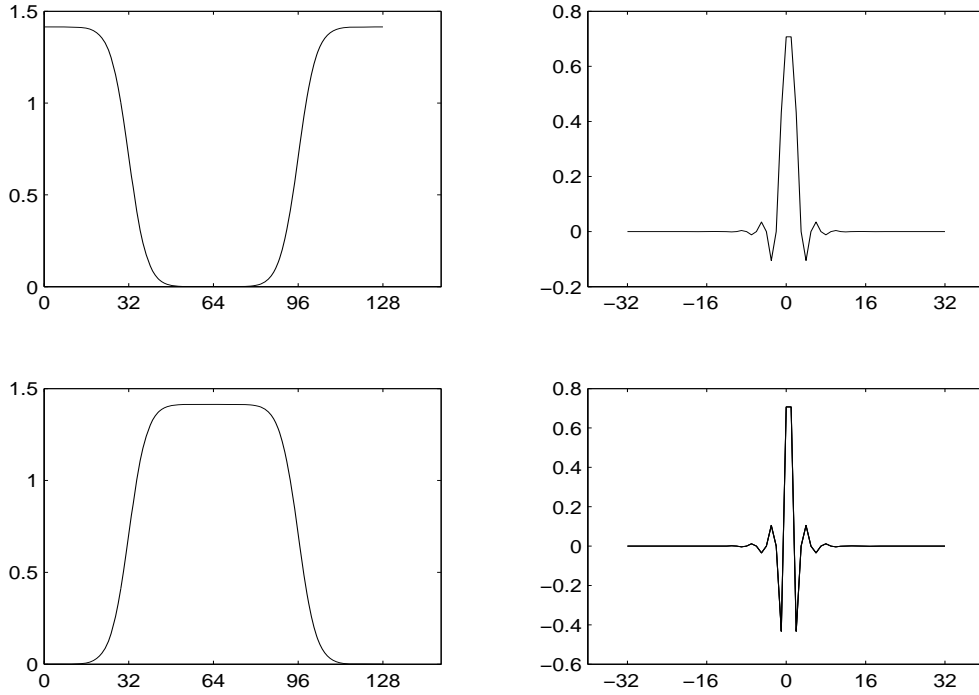


Рис. 1. Фильтры h , g_1 (слева) и соответствующие им вейвлеты φ , ψ (справа) при $r = 3$, $N = 128$.

Как следствие, вейвлеты $\theta = \mathcal{F}_N^{-1}(g_2)$ и $\tilde{\theta} = \mathcal{F}_N^{-1}(\tilde{g}_2)$ будут вещественными.

Рассмотрим вопрос о симметричности вейвлетов $\theta(j)$ и $\tilde{\theta}(j)$. Фильтр

$$\hat{g}_p(k) = \frac{2}{c+s} \left(\frac{1}{2} \sin \frac{2k\pi}{N} \right)^p$$

при чётном p вещественный и чётный. Поэтому соответствующий вейвлет $\theta_p = \mathcal{F}_N^{-1}(\hat{g}_p)$ — чётный и вещественный.

Наличие множителя ω_N^k приводит к сдвигу на одну позицию. Для вейвлетов $\theta(j)$ и $\tilde{\theta}(j)$ имеем

$$\theta(j) = \theta_p(j+1), \quad \tilde{\theta}(j) = \theta_q(j+1).$$

Эти вейвлеты вещественны и имеют ось симметрии $j = -1$.

На рис. 2 приведены графики фильтра \hat{g}_p и соответствующего вейвлета θ_p при $r = 3$, $p = 4$ и $N = 128$.

Отметим, что фильтр $\hat{g}_p(k)$ при чётном p имеет период N_1 .

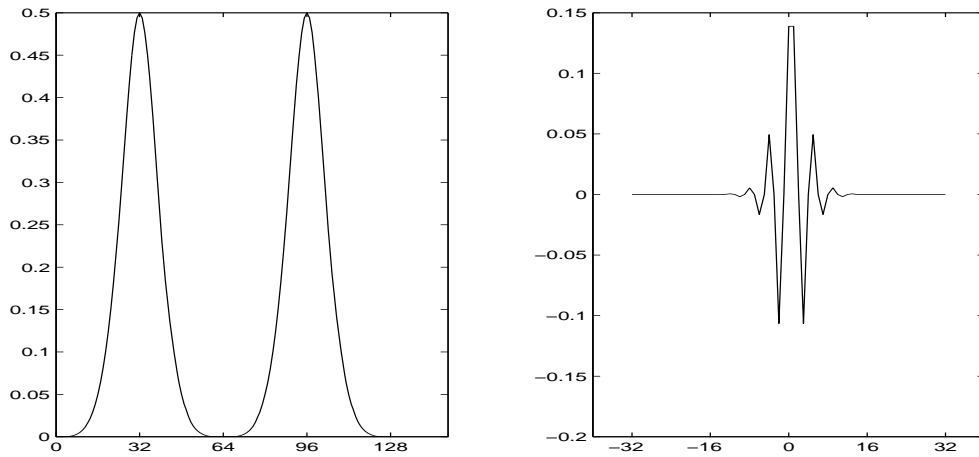


Рис. 2. Фильтр \hat{g}_p (слева) и вейвлет θ_p (справа) при $r = 3$, $p = 4$ и $N = 128$.

4.5. Согласно (3.5) для любого сигнала $x \in \mathbb{C}_N$ справедливо разложение

$$x = \sum_{k=0}^{N_1-1} \langle x, \varphi(\cdot - 2k) \rangle \varphi(\cdot - 2k) + \sum_{k=0}^{N_1-1} \langle x, \psi(\cdot - 2k) \rangle \psi(\cdot - 2k) + \sum_{k=0}^{N_1-1} \langle x, \tilde{\theta}(\cdot - 2k) \rangle \theta(\cdot - 2k),$$

а также аналогичное разложение, в котором θ и $\tilde{\theta}$ меняются местами.

По аналогии с вейвлетным преобразованием сигналов фреймовое преобразование может быть распространено на более грубые уровни разрешения. Это достигается путём итеративного применения описанного выше преобразования к низкочастотному блоку коэффициентов, начиная с $d_0(k) = \langle x, \varphi(\cdot - 2k) \rangle$, $k \in 0 : N_1 - 1$. В результате придём к многоуровневому разложению сигнала.

4.6. При каждом выборе чётных натуральных чисел p, q , $p + q = 2r$, получаются исходный фрейм $\{\varphi, \psi, \theta\}$ и двойственный фрейм $\{\varphi, \psi, \tilde{\theta}\}$. Можно точно вычислить границы этих фреймов. Пусть для определённости $p \geq q$. Тогда $p \geq r \geq q$. Дополнительно будем предполагать, что $N_2 = N/4$ — целое число.

ПРЕДЛОЖЕНИЕ 4. *Величины*

$$A = 2^{2r-2p}, \quad B = 1 \quad \text{и} \quad \tilde{A} = 1, \quad \tilde{B} = 2^{2r-2q} \quad (4.5)$$

являются границами фреймов $\{\varphi, \psi, \theta\}$ и $\{\varphi, \psi, \tilde{\theta}\}$ соответственно.

Доказательство. Для фрейма $\{\varphi, \psi, \theta\}$ имеем

$$H(k) = \frac{1}{4} \begin{bmatrix} h(k) & g_1(k) & g_2(k) \\ h(k+N_1) & g_1(k+N_1) & g_2(k+N_1) \end{bmatrix} \begin{bmatrix} \overline{h(k)} & \overline{h(k+N_1)} \\ \overline{g_1(k)} & \overline{g_1(k+N_1)} \\ \overline{g_2(k)} & \overline{g_2(k+N_1)} \end{bmatrix} =$$

$$= \begin{bmatrix} a(k) & b(k) \\ b(k) & a(k) \end{bmatrix},$$

где

$$a(k) = \frac{1}{4} \left[|h(k)|^2 + |g_1(k)|^2 + |g_2(k)|^2 \right] = \frac{c^2 + s^2 + 2\left(\frac{1}{2} \sin \frac{2k\pi}{N}\right)^{2p}}{2(c+s)^2},$$

$$b(k) = \frac{1}{4} \left[h(k) \overline{h(k+N_1)} + g_1(k) \overline{g_1(k+N_1)} + g_2(k) \overline{g_2(k+N_1)} \right] =$$

$$= \frac{cs - \left(\frac{1}{2} \sin \frac{2k\pi}{N}\right)^{2p}}{(c+s)^2}.$$

Поскольку $cs = \left(\cos \frac{k\pi}{N} \sin \frac{k\pi}{N}\right)^{2r} = \left(\frac{1}{2} \sin \frac{2k\pi}{N}\right)^{2r}$, то

$$b(k) = \frac{\left(\frac{1}{4} \sin^2 \frac{2k\pi}{N}\right)^r - \left(\frac{1}{4} \sin^2 \frac{2k\pi}{N}\right)^p}{\left(\left(\cos^2 \frac{k\pi}{N}\right)^r + \left(\sin^2 \frac{k\pi}{N}\right)^r\right)^2}. \quad (4.6)$$

По условию $p \geq r$, так что $b(k) \geq 0$. Очевидно, что $a(k) > 0$.

Собственными числами матрицы $H(k)$ являются

$$\lambda_1(k) = a(k) - b(k), \quad \lambda_2(k) = a(k) + b(k).$$

Принимая во внимание тождество $a(k) + b(k) \equiv \frac{1}{2}$, получаем

$$B := 2 \max_{k \in 0:N_1-1} \lambda_2(k) = 1.$$

Далее,

$$\lambda_1(k) = (a(k) + b(k)) - 2b(k) = \frac{1}{2} - 2b(k). \quad (4.7)$$

Значит, минимизация $\lambda_1(k)$ сводится к максимизации N_1 -периодической функции $b(k)$ при $p \geq r$. Покажем, что

$$\max_{k \in 0:N_1-1} b(k) = \frac{1}{4}(1 - 2^{2r-2p}). \quad (4.8)$$

При $p = r$ это очевидно (см. (4.6)). Будем считать, что $p > r$.

Рассмотрим функцию $u(t) = t^r - t^p$. Её производная $u'(t) = t^{r-1}(r - pt^{p-r})$ имеет единственный положительный корень $t_0 = (r/p)^{1/(p-r)}$ и положительна на $(0, t_0)$. Нас интересует $u(t)$ на отрезке $[0, \frac{1}{4}]$. Проверим, что $\frac{1}{4} < t_0$. Отсюда будет следовать, что $u(t)$ на $[0, \frac{1}{4}]$ строго возрастает.

Неравенство $t_0 > \frac{1}{4}$ равносильно следующему

$$r \left(\frac{1}{4}\right)^r > p \left(\frac{1}{4}\right)^p. \quad (4.9)$$

Функция $\xi(t) = t \left(\frac{1}{4}\right)^t$ имеет производную $\xi'(t) = \xi(t) \left(\frac{1}{t} - \ln 4\right)$, которая отрицательна при $t \geq 1$. Это гарантирует справедливость неравенства (4.9). Установлено, в частности, что $u(t)$ достигает максимального значения на $[0, \frac{1}{4}]$ в единственной точке $t = \frac{1}{4}$.

Согласно (4.6) числитель дроби $b(k)$ равен $u\left(\frac{1}{4} \sin^2 \frac{2k\pi}{N}\right)$. По доказанному он достигает наибольшего значения на $0 : N_1 - 1$ только при $k = N_2 = N_1/2$. Как мы сейчас выясним, на этом же индексе достигается наименьшее значение знаменателя дроби $b(k)$. Отсюда будет следовать, что $k = N_2$ — единственный индекс из $0 : N_1 - 1$, на котором достигается максимум самой дроби $b(k)$.

Рассмотрим функцию $v(t) = ((1-t)^r + t^r)^2$. Её производная

$$v'(t) = 2r((1-t)^r + t^r)(-(1-t)^{r-1} + t^{r-1})$$

обращается в ноль при $t = \frac{1}{2}$, отрицательна на $[0, \frac{1}{2})$ и положительна на $(\frac{1}{2}, 1]$. Значит, $v(t)$ достигает наименьшего значения на $[0, 1]$ в единственной точке $t = \frac{1}{2}$. Знаменатель дроби $b(k)$ равен $v\left(\sin^2 \frac{2k\pi}{N}\right)$. Он достигает наименьшего значения на $0 : N_1 - 1$ только при $k = N_2$.

Доказано, что максимум дроби $b(k)$ на $0 : N_1 - 1$ достигается на единственном индексе $k = N_2$. При этом

$$b(N_2) = \frac{2^{-2r} - 2^{-2p}}{2^{-2r+2}} = \frac{1}{4}(1 - 2^{2r-2p}).$$

Соотношение (4.8) установлено.

На основании (4.7) и (4.8) получаем

$$A = 2 \min_{k \in 0:N_1-1} \lambda_1(k) = 1 - 4 \max_{k \in 0:N_1-1} b(k) = 2^{2r-2p}.$$

Границы фрейма $\{\varphi, \psi, \theta\}$ вычислены.

Обратимся к двойственному фрейму $\{\varphi, \psi, \tilde{\theta}\}$. Вычисление его границ проводится по той же схеме с заменой p на q . Отличие заключается в том, что вместо неравенства $p \geq r$ выполняется неравенство $q \leq r$.

Собственными числами матрицы $\tilde{H}(k)$ являются

$$\tilde{\lambda}_1(k) = \tilde{a}(k) + \tilde{b}(k), \quad \tilde{\lambda}_2(k) = \tilde{a}(k) - \tilde{b}(k),$$

где

$$\tilde{a}(k) = \frac{c^2 + s^2 + 2\left(\frac{1}{2} \sin \frac{2k\pi}{N}\right)^{2q}}{2(c+s)^2},$$

$$\tilde{b}(k) = \frac{cs - \left(\frac{1}{2} \sin \frac{2k\pi}{N}\right)^{2q}}{(c+s)^2} = -\frac{\left(\frac{1}{2} \sin^2 \frac{2k\pi}{N}\right)^{2q} - \left(\frac{1}{2} \sin^2 \frac{2k\pi}{N}\right)^{2r}}{\left(\left(\cos^2 \frac{k\pi}{N}\right)^r + \left(\sin^2 \frac{k\pi}{N}\right)^r\right)^2}.$$

Очевидно, что $b(k) \leq 0$. Поскольку $\tilde{a}(k) + \tilde{b}(k) \equiv \frac{1}{2}$, то

$$\tilde{A} = 2 \min_{k \in 0:N_1-1} \tilde{\lambda}_2(k) = 1.$$

Далее,

$$\tilde{\lambda}_2(k) = (\tilde{a}(k) + \tilde{b}(k)) - 2\tilde{b}(k) = \frac{1}{2} + 2(-\tilde{b}(k)).$$

Аналогично (4.8)

$$\max_{k \in 0:N_1-1} \{-b(k)\} = \frac{1}{4}(2^{2r-2q} - 1).$$

Поэтому

$$\tilde{B} = 2 \max_{k \in 0:N_1-1} \tilde{\lambda}_2(k) = 1 + 4 \max_{k \in 0:N_1-1} \{-b(k)\} = 2^{2r-2q}.$$

Предложение доказано. \square

Отметим, что согласно (4.5) и равенству $p + q = 2r$ границы двойственных фреймов Баттерворта связаны соотношениями

$$\tilde{A} = 1/B, \quad \tilde{B} = 1/A.$$

ЛИТЕРАТУРА

1. Добеши И. *Десять лекций по вейвлетам*. Пер. с англ. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.
2. Новиков И. Я., Стечкин С. Б. *Основы теории всплесков* // Успехи матем. наук. 1998. Т. 53. Вып. 6 (324). С. 53–128.
3. Cvetković Z., Vetterli M. *Oversampled filter banks* // IEEE Trans. Sign. Proc. 1998. V. 46. No. 5. P. 1245–1255.
4. Averbuch A. Z., Zheludev V. A., Cohen T. *Interpolatory frames in signal spaces* // IEEE Trans. Sign. Proc. 2006. V. 54. No. 6. P. 2126–2139.
5. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Части 1–3. СПб.: НИИММ, 2003. 288 с.

6. Жёлудев В. А., Певный А. Б. *Вейвлетное преобразование Баттерворта и его реализация с помощью рекурсивных фильтров* // Журн. выч. мат. и матем. физ. 2002. Т. 42. № 4. С. 607–618.
7. Жёлудев В. А., Певный А. Б. *Дискретные периодические фреймы* // Вестн. Сыктывкарского ун-та. Сер. 1. 2006. Вып. 6. С. 87–94.

ФАКТОРИЗАЦИЯ МАТРИЦ РЕВЕРСНЫХ ПЕРЕСТАНОВОК

В. Н. Малозёмов

О. В. Просеков

2 мая 2006 г.

1. ФОРМУЛИРОВКА РЕЗУЛЬТАТА

Пусть s и n_1, n_2, \dots, n_s — натуральные числа, отличные от единицы. Введём обозначения

$$N = n_1 n_2 \cdots n_s; \quad N_\nu = n_{\nu+1} \cdots n_s \quad \text{при } \nu \in 0 : s-1; \quad N_s = 1; \\ \Delta_1 = 1; \quad \Delta_\nu = n_1 n_2 \cdots n_{\nu-1} \quad \text{при } \nu \in 2 : s+1.$$

Очевидно, что $N_0 = N$ и $\Delta_{\nu+1} N_\nu = N$ при всех $\nu \in 0 : s$.

Любое число $i \in 0 : N-1$ с помощью последовательного деления можно единственным образом представить в виде

$$i = i_s(n_{s-1}n_{s-2} \cdots n_1) + i_{s-1}(n_{s-2} \cdots n_1) + \cdots + \\ + i_2 n_1 + i_1 = \sum_{\nu=1}^s i_\nu \Delta_\nu, \quad (1.1)$$

где $i_\nu \in 0 : n_\nu - 1$. Будем использовать компактную запись формулы (1.1):

$$i = (i_s, i_{s-1}, \dots, i_1)_{n_s, n_{s-1}, \dots, n_1}. \quad (1.2)$$

Правая часть (1.2) называется *смешанным кодом числа i* .

Числу i сопоставим число с ревертированным кодом

$$\text{rev}_{n_1, n_2, \dots, n_s}((i_s, i_{s-1}, \dots, i_1)_{n_s, n_{s-1}, \dots, n_1}) = (i_1, i_2, \dots, i_s)_{n_1, n_2, \dots, n_s} = \\ = i_1(n_2 n_3 \cdots n_s) + i_2(n_3 \cdots n_s) + \cdots + i_{s-1} n_s + i_s = \sum_{\nu=1}^s i_\nu N_\nu.$$

Ясно, что $\text{rev}_{n_1, n_2, \dots, n_s}(i) \in 0 : N-1$. Поскольку

$$\text{rev}_{n_1, n_2, \dots, n_s}(\text{rev}_{n_s, n_{s-1}, \dots, n_1}(j)) = j, \quad j \in 0 : N-1, \quad (1.3)$$

то преобразование $\text{rev}_{n_1, n_2, \dots, n_s}$ является перестановкой множества $\{0, 1, \dots, N-1\}$.

Матрица реверсных перестановок определяется так:

$$\text{Rev}_{n_1, n_2, \dots, n_s}[i, j] = \begin{cases} 1, & \text{если } j = \text{rev}_{n_1, n_2, \dots, n_s}(i), \\ 0 & \text{в остальных случаях.} \end{cases}$$

Индексы строк и столбцов матрицы $\text{Rev}_{n_1, n_2, \dots, n_s}$ изменяются от 0 до $N-1$.

Основным результатом данной статьи является следующая

ТЕОРЕМА. *Справедливы разложения*

$$\text{Rev}_{n_1, n_2, \dots, n_s} = \prod_{\nu=1}^{s-1} (I_{\Delta_\nu} \otimes \text{Rev}_{n_\nu, N_\nu}), \quad (1.4)$$

$$\text{Rev}_{n_1, n_2, \dots, n_s} = \prod_{\nu=2}^s (I_{N_\nu} \otimes \text{Rev}_{\Delta_\nu, n_\nu}), \quad (1.5)$$

$$\text{Rev}_{n_1, n_2, \dots, n_s} = \prod_{\nu=1}^{s-1} (\text{Rev}_{n_{s-\nu}, N_{s-\nu}} \otimes I_{\Delta_{s-\nu}}), \quad (1.6)$$

$$\text{Rev}_{n_1, n_2, \dots, n_s} = \prod_{\nu=2}^s (\text{Rev}_{\Delta_{s-\nu+2}, n_{s-\nu+2}} \otimes I_{N_{s-\nu+2}}). \quad (1.7)$$

Здесь $I_n = I_n[0 : n-1, 0 : n-1]$ — единичная матрица n -го порядка и \otimes — знак кронекерова умножения матриц.

В правой части формул (1.4)–(1.7) присутствуют матрицы Rev , зависящие только от двух параметров.

Матрицы реверсных перестановок используются в теории быстрых ортогональных преобразований [1, 2, 3, 4].

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

2.1. Сначала разберёмся с матрицами реверсных перестановок, зависящими от двух параметров. Согласно определению

$$\text{rev}_{n_1, n_2}(i_2 n_1 + i_1) = i_1 n_2 + i_2,$$

где $i_\nu \in 0 : n_\nu - 1$. Соответственно

$$Rev_{n_1, n_2}[i_2 n_1 + i_1, j_1 n_2 + j_2] = \begin{cases} 1 & \text{при } j_1 = i_1, j_2 = i_2, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Вектор $X = Rev_{n_1, n_2} x$ имеет следующие компоненты:

$$X = \left(x(0), x(n_2), \dots, x((n_1 - 1)n_2), x(1), x(n_2 + 1), \dots, x((n_1 - 1)n_2 + 1), \right. \\ \left. \dots, x(n_2 - 1), x(2n_2 - 1), \dots, x(n_1 n_2 - 1) \right).$$

Действие матрицы Rev_{n_1, n_2} можно пояснить на неформальном уровне. Для этого одномерный массив x представим в виде таблицы

$$\begin{array}{ccccccc} x(0), & & x(1), & & \dots, & & x(n_2 - 1), \\ x(n_2), & & x(n_2 + 1), & & \dots, & & x(2n_2 - 1), \\ \dots & & \dots & & \dots & & \dots \\ x((n_1 - 1)n_2), & x((n_1 - 1)n_2 + 1), & \dots, & & x(n_1 n_2 - 1). \end{array}$$

Вектор $X = Rev_{n_1, n_2} x$ получится, если столбцы этой таблицы поочерёдно записать в одномерный массив.

2.2. Обратимся к общей матрице реверсных перестановок.

ЛЕММА 1. *Справедливо равенство*

$$(Rev_{n_1, n_2, \dots, n_s})^T = Rev_{n_s, n_{s-1}, \dots, n_1}. \quad (2.1)$$

Доказательство. Поскольку $Rev_{n_1, n_2, \dots, n_s}$ — матрица перестановок, то

$$Rev_{n_1, n_2, \dots, n_s} (Rev_{n_1, n_2, \dots, n_s})^T = I_N. \quad (2.2)$$

Покажем, что

$$Rev_{n_s, n_{s-1}, \dots, n_1} Rev_{n_1, n_2, \dots, n_s} = I_N. \quad (2.3)$$

Отсюда и из (2.2) будет следовать (2.1).

Запишем выражение для элемента с индексами (i, j) матрицы из левой части (2.3):

$$\sum_{k=0}^{N-1} Rev_{n_s, n_{s-1}, \dots, n_1}[i, k] \times Rev_{n_1, n_2, \dots, n_s}[k, j] = Rev_{n_1, n_2, \dots, n_s}[\text{rev}_{n_s, n_{s-1}, \dots, n_1}(i), j].$$

Это выражение равно единице при $j = \text{rev}_{n_1, n_2, \dots, n_s}(\text{rev}_{n_s, n_{s-1}, \dots, n_1}(i))$ или, в силу (1.3), при $j = i$; в остальных случаях оно равно нулю. Данное наблюдение соответствует (2.3). Лемма доказана. \square

2.3. Возьмём, число $i = (i_\nu, i_{\nu-1}, \dots, i_1)_{n_\nu, n_{\nu-1}, \dots, n_1} = j n_1 + i_1$, где $j = (i_\nu, i_{\nu-1}, \dots, i_2)_{n_\nu, n_{\nu-1}, \dots, n_2}$.

ЛЕММА 2. Пусть $i = j n_1 + i_1$. Тогда

$$\text{rev}_{n_1, n_2, \dots, n_\nu}(i) = i_1 (n_2 n_3 \cdots n_\nu) + \text{rev}_{n_2, \dots, n_\nu}(j). \quad (2.4)$$

Доказательство. Имеем

$$\begin{aligned} & i_1 (n_2 n_3 \cdots n_\nu) + \text{rev}_{n_2, \dots, n_\nu}((i_\nu, i_{\nu-1}, \dots, i_2)_{n_\nu, n_{\nu-1}, \dots, n_2}) = \\ & = i_1 (n_2 n_3 \cdots n_\nu) + (i_2, i_3, \dots, i_\nu)_{n_2, n_3, \dots, n_\nu} = (i_1, i_2, \dots, i_\nu)_{n_1, n_2, \dots, n_\nu} = \\ & = \text{rev}_{n_1, n_2, \dots, n_\nu}(i), \end{aligned}$$

что равносильно (2.4). \square

2.4. Напомним определение и некоторые свойства кронекерова умножения квадратных матриц [5, с. 80–82].

Кронекеровым произведением матриц $A_m = A_m[0 : m - 1, 0 : m - 1]$ и $B_n = B_n[0 : n - 1, 0 : n - 1]$ называется матрица $D_{mn} = A_m \otimes B_n$ с элементами

$$D_{mn}[i n + j, i' n + j'] = A_m[i, i'] B_n[j, j'], \quad i, i' \in 0 : m - 1, \quad j, j' \in 0 : n - 1.$$

Операция кронекерова умножения ассоциативна.

Покажем, что

$$\text{Rev}_{m,n}(A_m \otimes B_n) = (B_n \otimes A_m) \text{Rev}_{m,n}. \quad (2.5)$$

Сравним элементы с индексами $(i_2 m + i_1, i'_1 n + i'_2)$, где $i_1, i'_1 \in 0 : m - 1$, $i_2, i'_2 \in 0 : n - 1$. Запишем

$$\begin{aligned} & \left(\text{Rev}_{m,n}(A_m \otimes B_n) \right) [i_2 m + i_1, i'_1 n + i'_2] = \\ & = \sum_{k_1=0}^{m-1} \sum_{k_2=0}^{n-1} \text{Rev}_{m,n}[i_2 m + i_1, k_1 n + k_2] \times (A_m \otimes B_n)[k_1 n + k_2, i'_1 n + i'_2] = \\ & = (A_m \otimes B_n)[i_1 n + i_2, i'_1 n + i'_2] = A_m[i_1, i'_1] B_n[i_2, i'_2]. \end{aligned}$$

Вместе с тем,

$$\begin{aligned} & \left((B_n \otimes A_m) \text{Rev}_{m,n} \right) [i_2 m + i_1, i'_1 n + i'_2] = \\ & = \sum_{k_1=0}^{m-1} \sum_{k_2=0}^{n-1} (B_n \otimes A_m)[i_2 m + i_1, k_2 m + k_1] \times \text{Rev}_{m,n}[k_2 m + k_1, i'_1 n + i'_2] = \\ & = (B_n \otimes A_m)[i_2 m + i_1, i'_2 m + i'_1] = B_n[i_2, i'_2] A_m[i_1, i'_1]. \end{aligned}$$

Равенство (2.5) установлено.

Умножим обе части (2.5) слева на $Rev_{n,m}$. Согласно (2.3) получим

$$A_m \otimes B_n = Rev_{n,m}(B_n \otimes A_m)Rev_{m,n}. \quad (2.6)$$

Нам потребуются ещё два свойства кронекерова умножения:

$$(A_m \otimes B_n)^T = A_m^T \otimes B_n^T;$$

для пар квадратных матриц $A_m^{(\nu)}, B_n^{(\nu)}$, $\nu \in 1 : s$, порядков m и n соответственно справедлива формула

$$\prod_{\nu=1}^s (A_m^{(\nu)} \otimes B_n^{(\nu)}) = \left(\prod_{\nu=1}^s A_m^{(\nu)} \right) \otimes \left(\prod_{\nu=1}^s B_n^{(\nu)} \right).$$

В частности, если все $A_m^{(\nu)}$ равны I_m , то

$$\prod_{\nu=1}^s (I_m \otimes B_n^{(\nu)}) = I_m \otimes \left(\prod_{\nu=1}^s B_n^{(\nu)} \right). \quad (2.7)$$

3. РЕКУРРЕНТНЫЕ СООТНОШЕНИЯ

ЛЕММА 3. При $\nu = 3, 4, \dots, s$ справедливо рекуррентное соотношение

$$Rev_{n_1, n_2, \dots, n_\nu} = Rev_{n_1, n_2 \dots n_\nu} (I_{n_1} \otimes Rev_{n_2, \dots, n_\nu}). \quad (3.1)$$

Доказательство. Обозначим $N^{(\nu)} = n_1 n_2 \dots n_\nu$, $N_1^{(\nu)} = n_2 \dots n_\nu$. Возьмём произвольный вектор x с множеством индексов $0 : N^{(\nu)} - 1$ и покажем, что

$$Rev_{n_1, n_2, \dots, n_\nu} x = Rev_{n_1, n_2 \dots n_\nu} (I_{n_1} \otimes Rev_{n_2, \dots, n_\nu}) x. \quad (3.2)$$

Отсюда будет следовать (3.1).

Сравним компоненты векторов $X = Rev_{n_1, n_2, \dots, n_\nu} x$ и $Z = Rev_{n_1, N_1^{(\nu)}} Y$, где $Y = (I_{n_1} \otimes Rev_{n_2, \dots, n_\nu}) x$. Как и в п. 2.3 зафиксируем индекс $i = (i_\nu, i_{\nu-1}, \dots, i_1)_{n_\nu, n_{\nu-1}, \dots, n_1} = j n_1 + i_1$. Имеем

$$\begin{aligned} X(i) &= x(\text{rev}_{n_1, n_2, \dots, n_\nu}(i)), \\ Z(i) &= Z(j n_1 + i_1) = Y(i_1 N_1^{(\nu)} + j). \end{aligned}$$

В силу (2.4)

$$\begin{aligned} Y(i_1 N_1^{(\nu)} + j) &= \sum_{i'_1=0}^{n_1-1} \sum_{j'=0}^{N_1^{(\nu)}-1} (I_{n_1} \otimes Rev_{n_2, \dots, n_\nu}) [i_1 N_1^{(\nu)} + j, i'_1 N_1^{(\nu)} + j'] \times \\ &\times x(i'_1 N_1^{(\nu)} + j') = \sum_{i'_1=0}^{n_1-1} \sum_{j'=0}^{N_1^{(\nu)}-1} I_{n_1} [i_1, i'_1] \times Rev_{n_2, \dots, n_\nu} [j, j'] \times x(i'_1 N_1^{(\nu)} + j') = \end{aligned}$$

ЛИТЕРАТУРА

1. Власенко В. А., Лаппа Ю. М., Ярославский Л. П. *Методы синтеза быстрых алгоритмов свёртки и спектрального анализа сигналов*. М.: Наука, 1990. 180 с.
2. Johnson J., Johnson R. W., Rodriguez D., Tolimieri R. *A methodology for designing, modifying and implementing Fourier transform algorithms on various architectures* // Circuits, Systems and Signal Processing. 1990. V. 9. No. 4. P. 449–500.
3. Малозёмов В. Н., Машарский С. М. *Обобщенные вейвлетные базисы, связанные с дискретным преобразованием Виленкина-Крестенсона* // Алгебра и анализ. 2001. Т. 13. Вып. 1. С. 111–157.
4. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Части 1–3. СПб.: НИИММ, 2003. 320 с.
5. Воеводин В. В., Кузнецов Ю. А. *Матрицы и вычисления*. М.: Наука, 1984. 320 с.

РАЗБИЕНИЕ КРИВЫХ БЕЗЬЕ

В. Н. Малозёмов

3 июня 2006 г.

Данный доклад является добавлением к [1]. Здесь дается новое обоснование процедуры разбиения кривых Безье, которая называется «subdivision» [2, с. 68-70]. Кроме того, рассматривается вопрос об экстраполяции кривых Безье.

1°. Возьмём произвольные вещественные числа y_0, y_1, \dots, y_n и построим треугольный массив полиномов в форме Бернштейна

$$B_{ik}(x) = \sum_{\alpha=0}^i y_{k+\alpha} p_{i\alpha}(x), \quad i \in 0:n, \quad k \in 0:n-i,$$

где $p_{i\alpha}(x) = C_i^\alpha x^\alpha (1-x)^{i-\alpha}$, $i \in 1:n$, $\alpha \in 0:i$; $p_{00}(x) \equiv 1$ (рис. 1).

$$\begin{array}{cccccc} B_{00} & B_{01} & \dots & B_{0,n-1} & B_{0,n} & \\ B_{10} & B_{11} & \dots & B_{1,n-1} & & \\ \dots & \dots & \dots & \dots & \dots & \dots \\ B_{n-1,0} & B_{n-1,1} & & & & \\ B_{n0} & & & & & \end{array}$$

Рис. 1

Ясно, что $B_{0k}(x) \equiv y_k$ при $k \in 0:n$ и $B_{n0}(x) = \sum_{\alpha=0}^n y_\alpha p_{n\alpha}(x) =: B_n(x)$.

Введём полюсы $Y_k = (k/n, y_k)$, $k \in 0:n$, и при фиксированном x сформируем треугольный массив $\{Y_k^{(i)}\}$ по классической схеме последовательных линейных интерполяций:

$$\begin{aligned} Y_k^{(i)} &= (1-x)Y_k^{(i-1)} + xY_{k+1}^{(i-1)}, \quad i \in 1:n, \quad k \in 0:n-i; \\ Y_k^{(0)} &= Y_k, \quad k \in 0:n. \end{aligned} \tag{1}$$

ПРЕДЛОЖЕНИЕ 1. *Справедлива формула*

$$Y_k^{(i)} = \left(\frac{ix+k}{n}, B_{ik}(x) \right), \quad i \in 0:n, \quad k \in 0:n-i. \quad (2)$$

Доказательство. При $i = 0$ утверждение тривиально. При $i = 1$ согласно (1) имеем: по первой координате

$$(1-x)\frac{k}{n} + x\frac{k+1}{n} = \frac{x+k}{n};$$

по второй координате

$$(1-x)y_k + xy_{k+1} = y_k p_{10}(x) + y_{k+1} p_{11}(x) = B_{1k}(x).$$

Таким образом, при $i = 1$ равенство (2) выполняется.

Сделаем индукционный переход от $i-1$ к i , $i \geq 2$. Легко разобраться с первой координатой. Согласно индукционному предположению

$$(1-x)\frac{(i-1)x+k}{n} + x\frac{(i-1)x+k+1}{n} = \frac{ix+k}{n}.$$

Переходя ко второй координате, отметим, что базисные полиномы Бернштейна $p_{i\alpha}(x)$ удовлетворяют рекуррентным соотношениям

$$\begin{aligned} p_{i\alpha} &= (1-x)p_{i-1,\alpha} + xp_{i-1,\alpha-1}, \quad i \in 2:n, \quad \alpha \in 1:i-1; \\ p_{i0} &= (1-x)p_{i-1,0}, \quad p_{ii} = xp_{i-1,i-1}, \quad i \in 1:n; \\ p_{00} &\equiv 1. \end{aligned}$$

Поэтому

$$\begin{aligned} &(1-x)B_{i-1,k}(x) + xB_{i-1,k+1}(x) = \\ &= (1-x) \sum_{\alpha=0}^{i-1} y_{k+\alpha} p_{i-1,\alpha} + x \sum_{\alpha=0}^{i-1} y_{k+1+\alpha} p_{i-1,\alpha} = \\ &= (1-x)y_k p_{i-1,0} + \sum_{\alpha=1}^{i-1} y_{k+\alpha} [(1-x)p_{i-1,\alpha} + xp_{i-1,\alpha-1}] + \\ &\quad + xy_{k+i} p_{i-1,i-1} = \sum_{\alpha=0}^i y_{k+\alpha} p_{i\alpha} = B_{ik}(x). \end{aligned}$$

Предложение доказано. □

При $i = n$ из (2) следует, что $Y_0^{(n)} = (x, B_n(x))$. Это значит, что $Y_0^{(n)}$ есть точка графика полинома в форме Бернштейна $B_n(x)$.

Схема (1) позволяет построить график полинома $B_n(x)$ на отрезке $[0, 1]$. Он представляет собой простейший вариант кривой Безье. На рис. 2 показано построение точки $(c, B_n(c))$ при $n = 3$ и приведён вид всей кривой Безье.

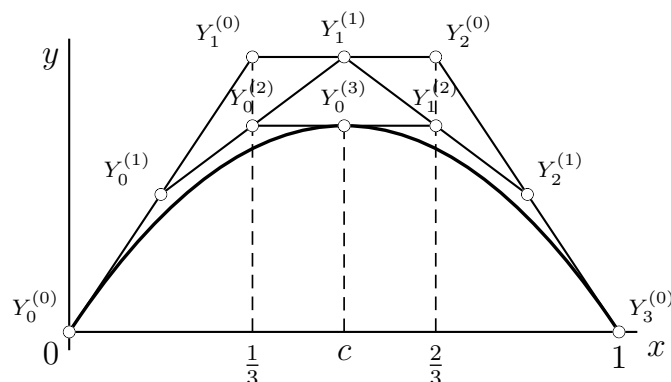


Рис. 2

Непрерывная ломаная, соединяющая полюсы $Y_0^{(0)}$, $Y_1^{(0)}$, $Y_2^{(0)}$, $Y_3^{(0)}$, называется характеристическим многоугольником данной кривой Безье. Напомним [1], что кривая Безье проходит через точки $Y_0^{(0)}$ и $Y_3^{(0)}$ и касается отрезка $[Y_0^{(0)}, Y_1^{(0)}]$ при $x = 0$, отрезка $[Y_2^{(0)}, Y_3^{(0)}]$ при $x = 1$ и отрезка $[Y_0^{(2)}, Y_1^{(2)}]$ при $x = c$.

Мы хотим доказать одно общее свойство кривых Безье, которое на рис. 2 соответствует тому, что непрерывная ломаная, соединяющая полюсы $Y_0^{(0)}$, $Y_0^{(1)}$, $Y_0^{(2)}$, $Y_0^{(3)}$, является характеристическим многоугольником дуги кривой Безье над отрезком $[0, c]$.

2°. Зафиксируем $c \in (0, 1)$ и обозначим $y_k^{(i)} = B_{ik}(c)$.

ПРЕДЛОЖЕНИЕ 2. *Справедливо тождество*

$$\sum_{i=0}^n y_0^{(i)} p_{ni}(x) = B_n(cx). \quad (3)$$

Доказательство. Имеем

$$\sum_{i=0}^n \left(\sum_{\alpha=0}^i y_{\alpha} p_{i\alpha}(c) \right) p_{ni}(x) = \sum_{\alpha=0}^n y_{\alpha} \sum_{i=\alpha}^n p_{i\alpha}(c) p_{ni}(x).$$

Нужно проверить, что

$$\sum_{i=\alpha}^n p_{i\alpha}(c) p_{ni}(x) = p_{n\alpha}(cx).$$

Запишем

$$\begin{aligned}
 & \sum_{i=\alpha}^n C_i^\alpha c^\alpha (1-c)^{i-\alpha} C_n^i x^i (1-x)^{n-i} = \\
 & = (cx)^\alpha \sum_{i=\alpha}^n C_i^\alpha C_n^i (x-cx)^{i-\alpha} (1-x)^{n-\alpha-(i-\alpha)} = \\
 & = (cx)^\alpha \sum_{i=0}^{n-\alpha} C_{i+\alpha}^\alpha C_n^{i+\alpha} (x-cx)^i (1-x)^{n-\alpha-i}.
 \end{aligned}$$

Поскольку $C_{i+\alpha}^\alpha C_n^{i+\alpha} = C_n^\alpha C_{n-\alpha}^i$, то последнее выражение преобразуется к виду

$$C_n^\alpha (cx)^\alpha (1-cx)^{n-\alpha} = p_{n\alpha}(cx).$$

Предложение доказано. \square

Обозначим $u = cx$. Тогда в силу (3)

$$\sum_{i=0}^n y_0^{(i)} p_{ni}\left(\frac{u}{c}\right) = B_n(u), \quad u \in [0, c]. \quad (4)$$

Зафиксируем $u \in (0, c)$, положим $x = u/c$ и рассмотрим полюсы

$$Z_i := Y_0^{(i)} = \left(\frac{ic}{n}, y_0^{(i)}\right), \quad i \in 0 : n. \quad (5)$$

Воспользуемся схемой (1) для полюсов $\{Z_k\}$ (мы поменяли индекс i на k) и параметра x :

$$\begin{aligned}
 Z_k^{(i)} &= (1-x)Z_k^{(i-1)} + xZ_{k+1}^{(i-1)}, \quad i \in 1 : n, \quad k \in 0 : n-i; \\
 Z_k^{(0)} &= Z_k, \quad k \in 0 : n.
 \end{aligned} \quad (6)$$

Получим $Z_0^{(n)} = (u, B_n(u))$. Действительно, по второй координате это равенство следует из (2) и (4), а по первой координате проверяется так же, как в предложении 1.

Схема (6) позволяет построить дугу кривой Безье над отрезком $[0, c]$ по полюсам $Y_0^{(0)}, Y_0^{(1)}, \dots, Y_0^{(n)}$ вида (5).

3°. Аналогичный результат можно получить и для отрезка $[c, 1]$.

ПРЕДЛОЖЕНИЕ 3. *Справедливо тождество*

$$\sum_{i=0}^n y_i^{(n-i)} p_{ni}(x) = B_n(x + c(1-x)). \quad (7)$$

Доказательство. Имеем

$$\begin{aligned} \sum_{i=0}^n \left(\sum_{\alpha=0}^{n-i} y_{i+\alpha} p_{n-i,\alpha}(c) \right) p_{ni}(x) &= \sum_{i=0}^n \left(\sum_{k=i}^n y_k p_{n-i,k-i}(c) \right) p_{ni}(x) = \\ &= \sum_{k=0}^n y_k \sum_{i=0}^k p_{n-i,k-i}(c) p_{ni}(x). \end{aligned}$$

Нужно проверить, что

$$\sum_{i=0}^k p_{n-i,k-i}(c) p_{ni}(x) = p_{nk}(x + c(1-x)).$$

Запишем

$$\begin{aligned} \sum_{i=0}^k C_{n-i}^{k-i} c^{k-i} (1-c)^{n-k} C_n^i x^i (1-x)^{n-i} &= \\ = [(1-c)(1-x)]^{n-k} \sum_{i=0}^k C_{n-i}^{k-i} C_n^i (c(1-x))^{k-i} x^i. \end{aligned}$$

Поскольку $C_{n-i}^{k-i} C_n^i = C_n^k C_k^i$, то последнее выражение преобразуется к виду

$$\begin{aligned} [(1-c)(1-x)]^{n-k} C_n^k (x + c(1-x))^k &= \\ = C_n^k (x + c(1-x))^k (1 - (x + c(1-x)))^{n-k} &= p_{nk}(x + c(1-x)). \end{aligned}$$

Предложение доказано. □

Обозначим $u = x + c(1-x) = c + x(1-c)$. Тогда в силу (7)

$$\sum_{i=0}^n y_i^{(n-i)} p_{ni}\left(\frac{u-c}{1-c}\right) = B_n(u), \quad u \in [c, 1]. \quad (8)$$

Зафиксируем $u \in (c, 1)$, положим $x = (u - c)/(1 - c)$ и рассмотрим полюсы

$$W_i := Y_i^{(n-i)} = \left(\frac{(n-i)c+i}{n}, y_i^{(n-i)} \right), \quad i \in 0 : n. \quad (9)$$

Воспользуемся схемой (1) для полюсов $\{W_k\}$ (мы снова поменяли индекс i на k) и параметра x :

$$\begin{aligned} W_k^{(i)} &= (1-x)W_k^{(i-1)} + xW_{k+1}^{(i-1)}, \quad i \in 1 : n, \quad k \in 0 : n-i; \\ W_k^{(0)} &= W_k, \quad k \in 0 : n. \end{aligned} \quad (10)$$

Получим $W_0^{(n)} = (u, B_n(u))$. Действительно, по второй координате это равенство следует из (2) и (8). Что касается первой координаты, то так же, как в предложении 1, доказывается, что у вектора $W_k^{(i)}$ она равна $c + \frac{ix+k}{n}(1-c)$. В частности, у полюса $W_0^{(k)}$ она равна u .

Схема (10) позволяет построить дугу кривой Безье над отрезком $[c, 1]$ по полюсам $Y_0^{(n)}, Y_1^{(n-1)}, \dots, Y_n^{(0)}$ вида (9).

4°. Перепишем соотношение (1) по второй координате при $x = c$:

$$\begin{aligned} y_k^{(i)} &= (1-c)y_k^{(i-1)} + cy_{k+1}^{(i-1)}, \quad i \in 1:n, \quad k \in 0:n-i; \\ y_k^{(0)} &= y_k, \quad k \in 0:n. \end{aligned} \quad (11)$$

Согласно (2), $y_k^{(i)} = B_{ik}(c)$. По формуле (11) строка за строкой вычисляется треугольный массив $\{y_k^{(i)}\}$ (рис. 3):

$$\begin{array}{cccccc} y_0^{(0)} & y_1^{(0)} & \dots & y_{n-1}^{(0)} & y_n^{(0)} & \\ y_0^{(1)} & y_1^{(1)} & \dots & y_{n-1}^{(1)} & & \\ \dots & \dots & \dots & \dots & \dots & \dots \\ y_0^{(n-1)} & y_1^{(n-1)} & & & & \\ y_0^{(n)} & & & & & \end{array}$$

Рис. 3

Базовой здесь является первая строка $y_0^{(0)}, y_1^{(0)}, \dots, y_n^{(0)}$. По ней формируется первый столбец $y_0^{(0)}, y_0^{(1)}, \dots, y_0^{(n)}$ и полюсы (5), а также наклонная строка $y_0^{(n)}, y_1^{(n-1)}, \dots, y_n^{(0)}$ и полюсы (9).

Полюсы (5) порождают дугу кривой Безье над отрезком $[0, c]$, а полюсы (9) — дугу той же кривой над отрезком $[c, 1]$.

Отметим, что формула (11) допускает обращение

$$y_{k+1}^{(i-1)} = y_k^{(i-1)} + \frac{1}{c}(y_k^{(i)} - y_k^{(i-1)}), \quad i = n, n-1, \dots, 1, \quad k = 0, 1, \dots, n-i.$$

По данным первого столбца $y_0^{(0)}, y_0^{(1)}, \dots, y_0^{(n)}$, которые теперь можно считать произвольными, вычисляются элементы как первой строки $y_0^{(0)}, y_1^{(0)}, \dots, y_n^{(0)}$, так и наклонной строки $y_0^{(n)}, y_1^{(n-1)}, \dots, y_n^{(0)}$. Полюсы $Z_k = (kc/n, y_0^{(k)})$, $k \in 0:n$, определяют дугу кривой Безье над $[0, c]$, а полюсы $W_k = \left(\frac{(n-k)c+k}{n}, y_k^{(n-k)}\right)$, $k \in 0:n$, вычисленные по данным первого столбца, позволяют естественным образом построить продолжение кривой Безье над $[c, 1]$ (экстраполировать её).

ЛИТЕРАТУРА

1. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Полиномы Бернштейна и составные кривые Безье*. // Семинар «DHA & CAGD». Избранные доклады. 14 декабря 2004 г. (<http://dha.spb.ru/rep04.shtml#1214>).
2. Farin G. *Curves and surfaces for CAGD*. 5th ed. San Diego: Academic Press, 2002. xvii+499 pp.

ВАРИАЦИИ КРИВЫХ БЕЗЬЕ

В. Н. Малозёмов

25 июля 2006 г.

1°. Пусть заданы упорядоченные вектор-строки

$$Y_k = (y_{k1}, \dots, y_{ks}), \quad k = 0, 1, \dots, n,$$

которые мы будем называть *полюсами*. Зафиксируем $x \in [0, 1]$ и проведём вычисления по рекуррентной формуле (*схема де Кастельжю*):

$$\begin{aligned} Y_k^{(i)} &= (1-x)Y_k^{(i-1)} + xY_{k+1}^{(i-1)}, \quad i \in 1:n, \quad k \in 0:n-i; \\ Y_k^{(0)} &= Y_k, \quad k \in 0:n. \end{aligned} \quad (1)$$

Вектор-строку $Y_k^{(i)}$ можно выразить через исходные полюсы Y_k, \dots, Y_{k+i} .

ПРЕДЛОЖЕНИЕ 1 (см. [1]). *Справедливо равенство*

$$Y_k^{(i)} = \sum_{\alpha=0}^i p_{i\alpha}(x) Y_{k+\alpha}, \quad (2)$$

где $p_{i\alpha}(x) = C_i^\alpha x^\alpha (1-x)^{i-\alpha}$.

Нас интересует вектор $Y_0^{(n)}$ как функция от x , $Y_0^{(n)} = Y_0^{(n)}(x)$. Из (1) следует, что $Y_0^{(n)}(0) = Y_0$, $Y_0^{(n)}(1) = Y_n$. Формула (2) при $i = n$ принимает вид

$$Y_0^{(n)}(x) = \sum_{\alpha=0}^n p_{n\alpha}(x) Y_\alpha. \quad (3)$$

Когда x пробегает отрезок $[0, 1]$, точка $Y_0^{(n)}(x)$ описывает кривую в пространстве \mathbb{R}^s , соединяющую Y_0 и Y_n . Эта кривая называется *кривой Безье*.

Обратим внимание на точки $x_1 < x_2 < \dots < x_m$ из интервала $(0, 1)$. Обозначим $B_i = Y_0^{(n)}(x_i)$. Согласно (3)

$$B_i = \sum_{\alpha=0}^n p_{n\alpha}(x_i) Y_\alpha, \quad i \in 1:m. \quad (4)$$

Мы хотим, чтобы кривая Безье проходила не через точки B_i , а через близкие точки \widehat{B}_i . Для этого нужно заменить полюсы Y_k на новые полюсы \widehat{Y}_k , что сводится к решению системы векторных уравнений

$$\widehat{B}_i = \sum_{\alpha=0}^n p_{n\alpha}(x_i) \widehat{Y}_\alpha, \quad i \in 1:m. \quad (5)$$

Желая сохранить начало и конец кривой Безье, полагаем

$$\widehat{Y}_0 = Y_0, \quad \widehat{Y}_n = Y_n. \quad (6)$$

Вычтем (4) из (5). С учётом (6) получим

$$\sum_{\alpha=1}^{n-1} p_{n\alpha}(x_i) (\widehat{Y}_\alpha - Y_\alpha) = \widehat{B}_i - B_i, \quad i \in 1:m. \quad (7)$$

Обозначим $Z_\alpha = \widehat{Y}_\alpha - Y_\alpha$, $R_i = \widehat{B}_i - B_i$ и перепишем (7) в виде

$$\sum_{\alpha=1}^{n-1} p_{n\alpha}(x_i) Z_\alpha = R_i, \quad i \in 1:m. \quad (8)$$

Считаем, что $m < n - 1$. Тогда в системе (8) неизвестных Z_α больше, чем уравнений. Мы заинтересованы в том, чтобы евклидова норма векторов Z_α была мала. Поставим экстремальную задачу: *минимизировать* $\sum_{\alpha=1}^{n-1} \|Z_\alpha\|^2$ *при ограничениях* (8). При $m = 1$ и $s = 1$ решение задачи указано в [2, с. 112–114]. Мы дадим решение в общем случае.

2°. Введём матрицы

$$A = \begin{bmatrix} p_{n1}(x_1) & \dots & p_{n,n-1}(x_1) \\ \dots & \dots & \dots \\ p_{n1}(x_m) & \dots & p_{n,n-1}(x_m) \end{bmatrix}, \quad Z = \begin{bmatrix} Z_1 \\ \vdots \\ Z_{n-1} \end{bmatrix}, \quad R = \begin{bmatrix} R_1 \\ \vdots \\ R_m \end{bmatrix}.$$

С их помощью интересующую нас экстремальную задачу можно записать так:

$$\|Z\|^2 := \sum_{\alpha=1}^{n-1} \left(\sum_{\beta=1}^s |z_{\alpha\beta}|^2 \right) \rightarrow \min, \quad AZ = R. \quad (9)$$

Нашей ближайшей целью является проверка линейной независимости строк матрицы A .

3°. Напомним, что система непрерывных на отрезке $[a, b]$ функций $u_0(x), u_1(x), \dots, u_n(x)$ называется *чебышёвской*, если любой обобщённый полином

$$P(x) = \sum_{i=0}^n c_i u_i(x),$$

у которого не все коэффициенты равны нулю (нетривиальный полином), имеет на $[a, b]$ не более n нулей.

ПРЕДЛОЖЕНИЕ 2. Система функций $p_{n0}(x), p_{n1}(x), \dots, p_{nn}(x)$ является чебышёвской на $[0, 1]$.

Доказательство. Составим нетривиальную линейную комбинацию

$$B(x) = \sum_{i=0}^n y_i p_{ni}(x).$$

Воспользуемся формулой [3]

$$B(x) = \sum_{k=0}^n C_n^k (\Delta^k y)_0 x^k, \quad (10)$$

где $(\Delta^k y)_0 = \sum_{\alpha=0}^k (-1)^{k-\alpha} C_k^\alpha y_\alpha$ — конечная разность k -го порядка. Как известно [4, с. 60]

$$y_i = \sum_{\alpha=0}^i C_i^\alpha (\Delta^\alpha y)_0, \quad i \in 0 : n.$$

По условию не все y_i равны нулю, а тогда не все $(\Delta^k y)_0$ равны нулю. Получили, что алгебраический полином (10) нетривиальный, откуда следует, что он имеет на $[0, 1]$ не более n нулей. Предложение доказано. \square

ПРЕДЛОЖЕНИЕ 3. Система функций $p_{n1}(x), \dots, p_{n,n-1}(x)$ является чебышёвской на интервале $(0, 1)$.

Доказательство. Составим нетривиальную линейную комбинацию

$$\begin{aligned} G(x) &= \sum_{i=1}^{n-1} y_i p_{ni}(x) = \sum_{i=1}^{n-1} y_i C_n^i x^i (1-x)^{n-i} = \\ &= x(1-x) \sum_{k=0}^{n-2} y_{k+1} C_n^{k+1} x^k (1-x)^{n-2-k}. \end{aligned}$$

Так как

$$C_n^{k+1} = C_{n-2}^k \frac{(n-1)n}{(k+1)(n-k-1)},$$

то

$$G(x) = (n-1)nx(1-x) \sum_{k=0}^{n-2} \frac{y_{k+1}}{(k+1)(n-k-1)} p_{n-2,k}(x).$$

В силу предложения 2 полином

$$\widehat{G}(x) = \sum_{k=0}^{n-2} \frac{y_{k+1}}{(k+1)(n-k-1)} p_{n-2,k}(x)$$

имеет на $[0, 1]$ не более $n-2$ нулей, а тогда $G(x)$ имеет не более $n-2$ нулей на интервале $(0, 1)$. Предложение доказано. \square

Введём вектор-строку

$$U(x) = (p_{n1}(x), \dots, p_{n,n-1}(x)).$$

ПРЕДЛОЖЕНИЕ 4. Для произвольных точек $x_1 < x_2 < \dots < x_{n-1}$ из интервала $(0, 1)$ векторы $U(x_1), U(x_2), \dots, U(x_{n-1})$ линейно независимы.

Доказательство. Рассмотрим квадратную матрицу

$$\begin{bmatrix} p_{n1}(x_1) & \dots & p_{n,n-1}(x_1) \\ \dots & \dots & \dots \\ p_{n1}(x_{n-1}) & \dots & p_{n,n-1}(x_{n-1}) \end{bmatrix}.$$

Требуется установить линейную независимость её строк. Для этого достаточно проверить, что столбцы линейно независимы.

Пусть

$$\sum_{i=1}^{n-1} y_i p_{ni}(x_k) = 0, \quad k \in 1 : n-1.$$

Это значит, что точки x_k являются нулями полинома

$$G(x) = \sum_{i=1}^{n-1} y_i p_{ni}(x).$$

Данные нули лежат в интервале $(0, 1)$ и их количество равно $n-1$. В силу предложения 3 такое возможно только тогда, когда все y_i равны нулю. Предложение доказано. \square

4°. Вернёмся к задаче (9). Согласно предложению 4 строки матрицы A при $m < n - 1$ линейно независимы. В этом случае матрица AA^T симметрична и положительно определена и у неё существует обратная матрица $(AA^T)^{-1}$, которая также симметрична и положительно определена.

ПРЕДЛОЖЕНИЕ 5. *Единственным решением задачи (9) является матрица*

$$\hat{Z} = A^T(AA^T)^{-1}R.$$

Доказательство. Очевидно, что матрица \hat{Z} удовлетворяет ограничению задачи (9). Любую другую матрицу Z , удовлетворяющую этому ограничению, можно представить в виде $Z = \hat{Z} + H$, где $AH = \mathbb{O}$.

Запишем

$$\begin{aligned} \|Z\|^2 &= \|\hat{Z} + H\|^2 = \sum_{\alpha=1}^{n-1} \sum_{\beta=1}^s |\hat{z}_{\alpha\beta} + h_{\alpha\beta}|^2 = \\ &= \|\hat{Z}\|^2 + \|H\|^2 + 2 \sum_{\alpha=1}^{n-1} \sum_{\beta=1}^s \hat{z}_{\alpha\beta} h_{\alpha\beta}. \end{aligned} \quad (11)$$

Последняя двойная сумма есть сумма диагональных элементов матрицы \hat{Z}^TH . Она обозначается $\text{tr}(\hat{Z}^TH)$. Поскольку

$$\hat{Z}^TH = R^T(AA^T)^{-1}(AH) = \mathbb{O},$$

то $\text{tr}(\hat{Z}^TH) = 0$. Формула (11) принимает вид

$$\|\hat{Z} + H\|^2 = \|\hat{Z}\|^2 + \|H\|^2.$$

Отсюда следует и оптимальность матрицы \hat{Z} и её единственность.

Предложение доказано. \square

5°. Обозначим через \hat{Z}_α строку матрицы \hat{Z} с индексом α . Тогда решение системы векторных уравнений (5), наиболее близкое к полюсам $\{Y_\alpha\}$, допускает представление

$$\hat{Y}_\alpha = Y_\alpha + \hat{Z}_\alpha, \quad \alpha \in 1 : n - 1.$$

ЛИТЕРАТУРА

1. Малозёмов В. Н. *Разбиение кривых Безье* // Семинар «DHA & CAGD». Избранные доклады. 3 июня 2006 г.
(<http://dha.spb.ru/refs06.shtml#0603>).
2. Farin G. *Curves and Surfaces for CAGD*. 5th ed. San Diego: Academic Press, 2002. xvii+499pp.
3. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Полиномы Бернштейна и составные кривые Безье*. // Семинар «DHA & CAGD». Избранные доклады. 14 декабря 2004 г. (<http://dha.spb.ru/refs04.shtml#1214>).
4. Мысовских И. П. *Лекции по методам вычислений*. СПб.: Изд-во СПбГУ, 1998. 472 с.

ВЫЧИСЛЕНИЕ ДПФ ЛЮБОЙ ДЛИНЫ*

Г. Н. Малолеткин

25 июля 2006 г.

Алгоритм Кули-Тьюки непосредственно применяется к вычислению ДПФ длины, равной степени двойки. Оказывается, что ДПФ любой длины N сводится к ДПФ длины $M = 2^m \geq 2N - 1$.

1°. Дискретное преобразование Фурье (ДПФ) сигнала $x \in \mathbb{C}_N$, определяемое формулой

$$X(k) = \sum_{j=0}^{N-1} x(j) \omega_N^{-kj}, \quad k \in 0 : N - 1,$$

можно записать в виде умножения матрицы на вектор

$$X = \bar{F}_N x,$$

где $\bar{F}_N[k, j] = \omega_N^{-kj}$, $k, j \in 0 : N - 1$.

Введём диагональную матрицу D_N ,

$$D_N = \text{diag} (1, \omega_{2N}^{-1}, \omega_{2N}^{-4}, \dots, \omega_{2N}^{-(N-1)^2}),$$

и симметричную тёплицеву матрицу G_N ,

$$G_N[k, j] = \omega_{2N}^{(k-j)^2}, \quad k, j \in 0 : N - 1.$$

ПРЕДЛОЖЕНИЕ. *Справедливо равенство*

$$\bar{F}_N = D_N G_N D_N. \quad (1)$$

Доказательство. Имеем

$$\bar{F}_N[k, j] = \omega_N^{-kj} = \omega_{2N}^{-k^2} \omega_{2N}^{(k-j)^2} \omega_{2N}^{-j^2}.$$

* Доклад прочитан 25 апреля 1987 г. на семинаре по цифровой обработке сигналов, предшествовавшем данному семинару

Вместе с тем,

$$\begin{aligned}
 (D_N G_N D_N)[k, j] &= \sum_{l=0}^{N-1} D_N[k, l] \sum_{l'=0}^{N-1} G_N[l, l'] D_N[l', j] = \\
 &= \sum_{l=0}^{N-1} D_N[k, l] G_N[l, j] \omega_{2N}^{-j^2} = \omega_{2N}^{-k^2} G_N[k, j] \omega_{2N}^{-j^2} = \\
 &= \omega_{2N}^{-k^2} \omega_{2N}^{(k-j)^2} \omega_{2N}^{-j^2}.
 \end{aligned}$$

Предложение доказано. \square

2°. Обозначим $a_k = \omega_{2N}^{k^2}$. Тогда матрицу G_N можно представить так:

$$G_N = \begin{bmatrix} a_0 & a_1 & \dots & a_{N-2} & a_{N-1} \\ a_1 & a_0 & \dots & a_{N-3} & a_{N-2} \\ \dots & \dots & \dots & \dots & \dots \\ a_{N-1} & a_{N-2} & \dots & a_1 & a_0 \end{bmatrix}.$$

Вложим G_N в правоциркулянтную матрицу \widehat{G}_M порядка $M = 2^m \geq 2N - 1$. Строку с индексом 0 матрицы \widehat{G}_M определим следующим образом

$$(a_0 \ a_1 \ \dots \ a_{N-1} \ 0 \ \dots \ 0 \ a_{N-1} \ a_{N-2} \ \dots \ a_1). \quad (2)$$

Нулей поставлено столько, чтобы длина строки равнялась M . Из строки (2) с помощью циклических сдвигов вправо формируется квадратная матрица \widehat{G}_M . Например, если

$$G_3 = \begin{bmatrix} a_0 & a_1 & a_2 \\ a_1 & a_0 & a_1 \\ a_2 & a_1 & a_0 \end{bmatrix},$$

то

$$\widehat{G}_8 = \begin{bmatrix} a_0 & a_1 & a_2 & 0 & 0 & 0 & a_2 & a_1 \\ a_1 & a_0 & a_1 & a_2 & 0 & 0 & 0 & a_2 \\ a_2 & a_1 & a_0 & a_1 & a_2 & 0 & 0 & 0 \\ 0 & a_2 & a_1 & a_0 & a_1 & a_2 & 0 & 0 \\ 0 & 0 & a_2 & a_1 & a_0 & a_1 & a_2 & 0 \\ 0 & 0 & 0 & a_2 & a_1 & a_0 & a_1 & a_2 \\ a_2 & 0 & 0 & 0 & a_2 & a_1 & a_0 & a_1 \\ a_1 & a_2 & 0 & 0 & 0 & a_2 & a_1 & a_0 \end{bmatrix},$$

По построению матрица \widehat{G}_M правоциркулянтная и симметричная, при этом подматрица $\widehat{G}_M[0 : N - 1, 0 : N - 1]$ совпадает с G_N , т. е.

$$G_N = [I_N \ 0] \widehat{G}_M \begin{bmatrix} I_N \\ 0 \end{bmatrix}. \quad (3)$$

3°. Согласно (1) и (3)

$$\bar{F}_N x = [D_N \ 0] \hat{G}_M \begin{bmatrix} D_N x \\ 0 \end{bmatrix}. \quad (4)$$

Обозначим $z = D_N x$, $\hat{z} = \begin{bmatrix} z \\ 0 \end{bmatrix}$, и пусть \hat{h} — сигнал из \mathbb{C}_M , который на основном периоде имеет вид (2). Поскольку $\hat{h}(-j) = \hat{h}(j)$, то

$$(\hat{G}_M \hat{z})(j) = \sum_{k=0}^{M-1} \hat{z}(k) \hat{h}(j-k), \quad j \in 0 : M-1. \quad (5)$$

В правой части (5) стоит циклическая свёртка $\hat{z} * \hat{h}$. По теореме о свёртке

$$\hat{z} * \hat{h} = \mathcal{F}_M^{-1}(\mathcal{F}_M(\hat{z}) \cdot \mathcal{F}_M(\hat{h})). \quad (6)$$

Спектр $\hat{H} = \mathcal{F}_M(\hat{h})$ не зависит от x . Его компоненты можно вычислить заранее по формуле

$$\begin{aligned} \hat{H}(k) &= 1 + \sum_{j=0}^{N-1} \omega_{2N}^{j^2} \omega_M^{-kj} + \sum_{j=0}^{N-1} \omega_{2N}^{j^2} \omega_M^{-k(M-j)} = \\ &= 1 + 2 \sum_{j=0}^{N-1} \omega_{2N}^{j^2} \cos\left(\frac{2\pi k}{M} j\right), \quad k \in 0 : M-1. \end{aligned} \quad (7)$$

На основании (4), (5) и (6) приходим к следующей схеме вычисления спектра $X = \bar{F}_N x$.

- 1) Формируем вектор z с компонентами $z(j) = \omega_{2N}^{-j^2} x(j)$, $j \in 0 : N-1$, и дополняем его нулями до M -мерного вектора \hat{z} .
- 2) Вычисляем $\hat{Z} = \mathcal{F}_M(\hat{z})$.
- 3) Покомпонентно умножаем \hat{Z} на \hat{H} вида (7). Получаем вектор $\hat{Y} = \hat{Z} \hat{H}$.
- 4) Вычисляем $\hat{X} = \mathcal{F}_M^{-1}(\hat{Y})$.
- 5) Находим компоненты спектра $X = \bar{F}_N x$ по формуле

$$X(k) = \omega_{2N}^{-k^2} \hat{X}(k), \quad k \in 0 : N-1.$$

Самыми плохими для этой схемы являются N вида $N = 2^s + 1$. Для них

$$2N-1 = 2^{s+1} + 1, \quad M = 2^{s+2} = 4(N-1).$$

ЛИТЕРАТУРА

1. Блейхут Р. *Быстрые алгоритмы цифровой обработки сигналов*. М.: Мир, 1989. С. 147–149.
2. Нуссбаумер Г. *Быстрое преобразование Фурье и алгоритмы вычисления свёрток*. М.: Радио и связь, 1985. С. 103–104.

ПАРАМЕТРИЧЕСКИЙ ВАРИАНТ МЕТОДА ПРОСТЫХ МНОЖИТЕЛЕЙ

В. Н. Малозёмов О. В. Просеков

5 сентября 2006 г.

1. ФОРМУЛИРОВКА РЕЗУЛЬТАТОВ

1.1. Пусть n_1, n_2, \dots, n_s — попарно взаимно простые натуральные числа, отличные от единицы. Введём обозначения

$$\begin{aligned} N &= n_1 n_2 \cdots n_s; \\ N_\nu &= n_{\nu+1} n_{\nu+2} \cdots n_s \quad \text{при } \nu \in 0 : s-1, \quad N_s = 1; \\ \Delta_1 &= 1; \quad \Delta_\nu = n_1 n_2 \cdots n_{\nu-1} \quad \text{при } \nu \in 2 : s+1, \\ B_\nu &= N/n_\nu \quad \text{при } \nu \in 1 : s. \end{aligned}$$

Очевидно, что $\Delta_\nu N_\nu = B_\nu$, $\nu \in 1 : s$.

При каждом $\nu \in 1 : s$ зафиксируем число $p_\nu \in 1 : n_\nu - 1$, взаимно простое с n_ν . Вектор $p = (p_1, p_2, \dots, p_s)$ назовём *вектором параметров*.

Поскольку $p_\nu B_\nu$ взаимно просто с n_ν , то уравнение $\langle x p_\nu B_\nu \rangle_{n_\nu} = 1$ имеет единственное на множестве $1 : n_\nu - 1$ решение. Обозначим его q_ν . Вектор $q = (q_1, q_2, \dots, q_s)$ назовём *сопряжённым вектором параметров*.

1.2. Введём перестановку $\text{perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}$, сопоставляющую числу $j \in 0 : N - 1$ с разложением $j = \sum_{\nu=1}^s j_\nu \Delta_\nu$, $j_\nu \in 0 : n_\nu - 1$, число

$$k = \left\langle \sum_{\nu=1}^s j_\nu p_\nu B_\nu \right\rangle_N.$$

Эта перестановка определена и при $s = 1$. Запись $k = \text{perm}_{n_1}^{(p_1)}(j)$ означает, что $k = \langle j p_1 \rangle_{n_1}$. Такая перестановка называется *эйлеровой*.

Матрицу перестановок $\text{Perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}[0 : N - 1, 0 : N - 1]$ определим обычным способом:

$$\text{Perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}[j, k] = \begin{cases} 1, & \text{если } k = \text{perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}(j), \\ 0 & \text{в остальных случаях.} \end{cases}$$

Матрицы $\text{Perm}_{n_\nu}^{(p_\nu)}$, $\nu \in 1 : s$, назовём *матрицами эйлеровых перестановок*. При $p_1 = p_2 = \dots = p_s = 1$ получим *матрицу руританских перестановок* $\text{Perm}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)}$.

1.3. Сформулируем основные результаты доклада.

ТЕОРЕМА 1. *Справедливо разложение*

$$\text{Perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} = \left(\text{Perm}_{n_s}^{(p_s)} \otimes \text{Perm}_{n_{s-1}}^{(p_{s-1})} \otimes \dots \otimes \text{Perm}_{n_1}^{(p_1)} \right) \prod_{\nu=2}^s (I_{N_\nu} \otimes \text{Perm}_{\Delta_\nu, n_\nu}^{(1, 1)}).$$

ТЕОРЕМА 2. *При любом векторе параметров $p = (p_1, p_2, \dots, p_s)$ матрица Фурье F_N допускает представление*

$$F_N = \left(\text{Perm}_{n_1, n_2, \dots, n_s}^{(q_1, q_2, \dots, q_s)} \right)^T (F_{n_s} \otimes F_{n_{s-1}} \otimes \dots \otimes F_{n_1}) \text{Perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}, \quad (1)$$

где $q = (q_1, q_2, \dots, q_s)$ — сопряжённый вектор параметров.

В разделе 2 приводится доказательство теоремы 1, в разделе 3 — доказательство теоремы 2. Раздел 4 посвящён детальному обсуждению полученных результатов.

2. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1

2.1. Начнём с двух предварительных утверждений.

ЛЕММА 1. *При $\nu \in 2 : s$ имеет место рекуррентное соотношение*

$$\text{perm}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}(j + j_\nu \Delta_\nu) = \langle n_\nu \text{perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})}(j) + \Delta_\nu \text{perm}_{n_\nu}^{(p_\nu)}(j_\nu) \rangle_{\Delta_{\nu+1}},$$

где $j \in 0 : \Delta_\nu - 1$, $j_\nu \in 0 : n_\nu - 1$.

Доказательство. Пусть $j = j_1 + j_2 \Delta_2 + \dots + j_{\nu-1} \Delta_{\nu-1}$. Пользуясь формулой $\langle k n \rangle_{mn} = n \langle k \rangle_m$, получаем

$$\begin{aligned} \text{perm}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}(j + j_\nu \Delta_\nu) &= \left\langle \sum_{\alpha=1}^{\nu} j_\alpha p_\alpha \frac{\Delta_{\nu+1}}{n_\alpha} \right\rangle_{\Delta_{\nu+1}} = \\ &= \left\langle n_\nu \sum_{\alpha=1}^{\nu-1} j_\alpha p_\alpha \frac{\Delta_\nu}{n_\alpha} + j_\nu p_\nu \Delta_\nu \right\rangle_{\Delta_\nu n_\nu} = \left\langle n_\nu \left\langle \sum_{\alpha=1}^{\nu-1} j_\alpha p_\alpha \frac{\Delta_\nu}{n_\alpha} \right\rangle_{\Delta_\nu} + \Delta_\nu \langle j_\nu p_\nu \rangle_{n_\nu} \right\rangle_{\Delta_\nu n_\nu} = \\ &= \langle n_\nu \text{perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})}(j) + \Delta_\nu \text{perm}_{n_\nu}^{(p_\nu)}(j_\nu) \rangle_{\Delta_{\nu+1}}. \end{aligned}$$

Лемма доказана. \square

ЛЕММА 2. Для параметрических матриц перестановок при $\nu \in 2 : s$ справедливо рекуррентное соотношение

$$\text{Perm}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)} = (\text{Perm}_{n_\nu}^{(p_\nu)} \otimes \text{Perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})}) \text{Perm}_{\Delta_\nu, n_\nu}^{(1,1)}. \quad (2)$$

Доказательство. Возьмём произвольный $\Delta_{\nu+1}$ -мерный вектор x и обозначим $X = \text{Perm}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)} x$. Тогда при $j \in 0 : \Delta_\nu - 1$, $j_\nu \in 0 : n_\nu - 1$ в силу леммы 1

$$\begin{aligned} X(j + j_\nu \Delta_\nu) &= x(\text{perm}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}(j + j_\nu \Delta_\nu)) = \\ &= x(\langle n_\nu \text{perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})}(j) + \Delta_\nu \text{perm}_{n_\nu}^{(p_\nu)}(j_\nu) \rangle_{\Delta_{\nu+1}}). \end{aligned} \quad (3)$$

Далее, поскольку $\text{perm}_{n_1, n_2}^{(p_1, p_2)}(j_1 + j_2 n_1) = \langle j_1 p_1 n_2 + j_2 p_2 n_1 \rangle_{n_1 n_2}$, то для вектора $Y = \text{Perm}_{\Delta_\nu, n_\nu}^{(1,1)} x$ имеем

$$Y(j + j_\nu \Delta_\nu) = x(\langle j n_\nu + j_\nu \Delta_\nu \rangle_{\Delta_\nu n_\nu}).$$

Найдём компоненты вектора $Z = (\text{Perm}_{n_\nu}^{(p_\nu)} \otimes \text{Perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})}) Y$. Запишем

$$\begin{aligned} Z(j + j_\nu \Delta_\nu) &= \sum_{j'_\nu=0}^{n_\nu-1} \sum_{j'=0}^{\Delta_\nu-1} (\text{Perm}_{n_\nu}^{(p_\nu)} \otimes \text{Perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})}) [j'_\nu \Delta_\nu + j, j'_\nu \Delta_\nu + j'] \times \\ &\times Y(j'_\nu \Delta_\nu + j') = \sum_{j'_\nu=0}^{n_\nu-1} \sum_{j'=0}^{\Delta_\nu-1} \text{Perm}_{n_\nu}^{(p_\nu)} [j'_\nu, j'_\nu] \times \text{Perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})} [j, j'] \times \\ &\times Y(j' + j'_\nu \Delta_\nu) = Y(\text{perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})}(j) + \Delta_\nu \text{perm}_{n_\nu}^{(p_\nu)}(j_\nu)) = \\ &= x(\langle n_\nu \text{perm}_{n_1, n_2, \dots, n_{\nu-1}}^{(p_1, p_2, \dots, p_{\nu-1})}(j) + \Delta_\nu \text{perm}_{n_\nu}^{(p_\nu)}(j_\nu) \rangle_{\Delta_{\nu+1}}). \end{aligned} \quad (4)$$

Сравнивая (3) и (4), приходим к равенству $Z = X$. Отсюда очевидным образом следует (2). Лемма доказана. \square

2.2. Обратимся к доказательству теоремы 1. При $s = 2$ её заключение совпадает с (2) при $\nu = 2$. Сделаем индукционный переход от s к $s + 1$.

Согласно (2), индукционному предположению и связи кронекерова умножения с обычным умножением матриц [1] имеем

$$\begin{aligned} \text{Perm}_{n_1, \dots, n_s, n_{s+1}}^{(p_1, \dots, p_s, p_{s+1})} &= (\text{Perm}_{n_{s+1}}^{(p_{s+1})} \otimes \text{Perm}_{n_1, \dots, n_s}^{(p_1, \dots, p_s)}) \text{Perm}_{\Delta_{s+1}, n_{s+1}}^{(1,1)} = \\ &= \left\{ [\text{Perm}_{n_{s+1}}^{(p_{s+1})} \underbrace{I_{n_{s+1}} \dots I_{n_{s+1}}}_{(s-1) \text{ раз}}] \otimes [(\text{Perm}_{n_s}^{(p_s)} \otimes \text{Perm}_{n_{s-1}}^{(p_{s-1})} \otimes \dots \otimes \text{Perm}_{n_1}^{(p_1)})] \right\} \times \end{aligned}$$

$$\begin{aligned}
& \times \prod_{\nu=2}^s \left(I_{n_{\nu+1} \dots n_s} \otimes \text{Perm}_{\Delta_\nu, n_\nu}^{(1,1)} \right) \Big] \Big\} (I_1 \otimes \text{Perm}_{\Delta_{s+1}, n_{s+1}}^{(1,1)}) = \\
& = \left(\text{Perm}_{n_{s+1}}^{(p_{s+1})} \otimes \text{Perm}_{n_s}^{(p_s)} \otimes \dots \otimes \text{Perm}_{n_1}^{(p_1)} \right) \prod_{\nu=2}^{s+1} \left(I_{n_{\nu+1} \dots n_{s+1}} \otimes \text{Perm}_{\Delta_\nu, n_\nu}^{(1,1)} \right).
\end{aligned}$$

Теорема доказана. \square

3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2

Проверим равенство, эквивалентное (1):

$$\text{Perm}_{n_1, n_2, \dots, n_s}^{(q_1, q_2, \dots, q_s)} F_N \left(\text{Perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} \right)^T = F_{n_s} \otimes F_{n_{s-1}} \otimes \dots \otimes F_{n_1}. \quad (5)$$

В силу определения кронекерова умножения матриц

$$\begin{aligned}
& \left(F_{n_s} \otimes F_{n_{s-1}} \otimes \dots \otimes F_{n_1} \right) \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, \sum_{\nu=1}^s j_\nu \Delta_\nu \right] = \\
& = \prod_{\nu=1}^s F_{n_\nu} [k_\nu, j_\nu] = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu}.
\end{aligned} \quad (6)$$

Вместе с тем,

$$\begin{aligned}
& \left(\text{Perm}_{n_1, n_2, \dots, n_s}^{(q_1, q_2, \dots, q_s)} F_N \left(\text{Perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} \right)^T \right) \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, \sum_{\nu=1}^s j_\nu \Delta_\nu \right] = \\
& = \sum_{l=0}^{N-1} \sum_{l'=0}^{N-1} \text{Perm}_{n_1, n_2, \dots, n_s}^{(q_1, q_2, \dots, q_s)} \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, l \right] \times F_N[l, l'] \times \text{Perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} \left[\sum_{\nu=1}^s j_\nu \Delta_\nu, l' \right] = \\
& = F_N \left[\text{perm}_{n_1, n_2, \dots, n_s}^{(q_1, q_2, \dots, q_s)} \left(\sum_{\nu=1}^s k_\nu \Delta_\nu \right), \text{perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} \left(\sum_{\nu=1}^s j_\nu \Delta_\nu \right) \right] = \\
& = \omega_N^{\left(\sum_{\nu=1}^s k_\nu q_\nu B_\nu \right) \left(\sum_{\nu=1}^s j_\nu p_\nu B_\nu \right)} = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu \langle q_\nu p_\nu B_\nu \rangle_{n_\nu}} = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu}. \quad (7)
\end{aligned}$$

Мы воспользовались формулой $\langle q_\nu p_\nu B_\nu \rangle_{n_\nu} = 1$, $\nu \in 1 : s$, справедливой в силу определения q_ν .

Сравнивая (6) и (7), приходим к (5). Теорема доказана. \square

4. ОБСУЖДЕНИЕ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

4.1. Очевидно, что $\text{Perm}_{n_\nu}^{(1)} = I_{n_\nu}$. Из теоремы 1 при $p_1 = p_2 = \dots = p_s = 1$ следует разложение матрицы руританских перестановок:

$$\text{Perm}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)} = \prod_{\nu=2}^s (I_{N_\nu} \otimes \text{Perm}_{\Delta_\nu, n_\nu}^{(1,1)}).$$

Более того, само заключение теоремы 1 можно переписать в виде

$$\text{Perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} = (\text{Perm}_{n_s}^{(p_s)} \otimes \text{Perm}_{n_{s-1}}^{(p_{s-1})} \otimes \dots \otimes \text{Perm}_{n_1}^{(p_1)}) \text{Perm}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)}.$$

4.2. Теорема 2 при $p_1 = p_2 = \dots = p_s = 1$ по существу установлена Гудом [2, 3]. Отметим, что компоненты вектора параметров $q = (q_1, q_2, \dots, q_s)$, сопряжённого с $p = (1, 1, \dots, 1)$, определяются из условия $\langle q_\nu B_\nu \rangle_{n_\nu} = 1$, $\nu \in 1 : s$. Матрица перестановок с таким q называется *матрицей китайских перестановок*.

Идея использования вектора параметров $p = (p_1, p_2, \dots, p_s)$ при факторизации матрицы Фурье принадлежит М. Б. Свердлику [4].

В связи с теоремой 2 вызывают интерес *самосопряжённые векторы параметров* p , такие, что сопряжённый вектор параметров q совпадает с p . В этом случае в разложении (1) присутствует только одна матрица перестановок.

Обозначим через b_ν единственное на множестве $1 : n_\nu - 1$ решение уравнения $\langle x B_\nu \rangle_{n_\nu} = 1$. Самосопряжённый вектор параметров существует тогда и только тогда, когда при всех $\nu \in 1 : s$ число b_ν является квадратичным вычетом по модулю n_ν [5].

Пусть p_ν — решение уравнения $\langle x^2 \rangle_{n_\nu} = b_\nu$. В этом случае вектор параметров $p = (p_1, p_2, \dots, p_s)$ будет самосопряжённым. Например, при $s = 2$, $n_1 = 4$, $n_2 = 25$ существует четыре самосопряжённых вектора параметров: $p = (1, 12)$, $p = (1, 13)$, $p = (3, 12)$ и $p = (3, 13)$. Подробности см. в [5].

Ещё один пример: при $s = 3$, $n_1 = 2$, $n_2 = 3$, $n_3 = 5$ самосопряжённым будет руританский вектор параметров $p = (1, 1, 1)$.

Теорема 2 вместе с теоремой 1 дают наиболее глубокую параметрическую факторизацию матрицы Фурье F_N при $N = n_1 n_2 \dots n_s$ с попарно взаимно простыми сомножителями n_ν .

4.3. В заключение укажем явный вид перестановки, обратной к перестановке $\text{perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}$. Пусть $k \in 0 : N - 1$. Тогда

$$(\text{perm}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)})^{-1}(k) = \sum_{\nu=1}^s \langle k q_\nu \rangle_{n_\nu} \Delta_\nu,$$

где q_ν — компоненты сопряжённого с $p = (p_1, p_2, \dots, p_s)$ вектора параметров.

Нужно проверить, что

$$\left\langle \sum_{\nu=1}^s \langle k q_\nu \rangle_{n_\nu} p_\nu B_\nu \right\rangle_N = k. \quad (8)$$

Обозначим левую часть равенства (8) через k' . Запишем

$$\sum_{\nu=1}^s \langle k q_\nu \rangle_{n_\nu} p_\nu B_\nu = t N + k'.$$

Взяв вычеты по модулю n_μ , получим

$$\langle \langle k q_\mu \rangle_{n_\mu} p_\mu B_\mu \rangle_{n_\mu} = \langle k' \rangle_{n_\mu},$$

или

$$\langle k \langle q_\mu p_\mu B_\mu \rangle_{n_\mu} \rangle_{n_\mu} = \langle k' \rangle_{n_\mu},$$

или $\langle k \rangle_{n_\mu} = \langle k' \rangle_{n_\mu}$. Значит, разность $k - k'$ делится на n_μ при всех $\mu \in 1 : s$. В силу попарной взаимной простоты n_μ разность $k - k'$ делится на произведение $n_1 n_2 \cdots n_s = N$. Поскольку к тому же $|k - k'| \leq N - 1$, то необходимо $k = k'$. Утверждение доказано.

ЛИТЕРАТУРА

1. Малозёмов В. Н., Просеков О. В. *Перестановки и кронекерово произведение матриц* // Семинар «DHA & CAGD». Избранные доклады. 31 марта 2004 г. (<http://dha.spb.ru/rep04.shtml#0331>).
2. Гуд И. Дж. *О взаимоотношении между двумя быстрыми преобразованиями Фурье* / В кн.: Макклеллан Дж. Х., Рейдер Ч. М. *Применение теории чисел в цифровой обработке сигналов*. М.: Радио и связь, 1983. С. 136–147.
3. Малозёмов В. Н., Просеков О. В. *Факторизация Гуда матрицы Фурье* // Семинар «DHA & CAGD». Избранные доклады. 5 мая 2004 г. (<http://dha.spb.ru/rep04.shtml#0505>).
4. Свердлик М. Б. *Матричная интерпретация алгоритма БПФ для взаимно простых сомножителей* // Радиотехника и электроника. 1983. № 10. С. 1931–1938.
5. Малозёмов В. Н. *Параметрическое кодирование индексов* // Семинар «DHA & CAGD». Избранные доклады. 19 мая 2004 г. (<http://dha.spb.ru/rep04.shtml#0519>).

ОБЩИЙ ПОДХОД К ВЫЧИСЛЕНИЮ ДПФ

В. Н. Малозёмов

О. В. Просеков

12 сентября 2006 г.

В докладе представлен усовершенствованный вариант общего подхода к вычислению ДПФ, предложенного М. Б. Свердликом [1].

1°. Пусть s и n_1, n_2, \dots, n_s — произвольные натуральные числа, отличные от единицы, и $N = n_1 n_2 \dots n_s$. Предположим, что при всех $\nu \in 1 : s$ найдутся числа p_ν, q_ν из $1 : N-1$, взаимно простые с n_ν , и натуральные D_ν, G_ν такие, что любые $k, j \in 0 : N-1$ допускают представления

$$\begin{aligned} j &= \left\langle \sum_{\nu=1}^s j_\nu p_\nu D_\nu \right\rangle_N, & j_\nu &\in 0 : n_\nu - 1, \\ k &= \left\langle \sum_{\mu=1}^s k_\mu q_\mu G_\mu \right\rangle_N, & k_\mu &\in 0 : n_\mu - 1. \end{aligned} \quad (1)$$

Поскольку множества коэффициентов (j_1, j_2, \dots, j_s) и (k_1, k_2, \dots, k_s) имеют ту же мощность, что и множество $0 : N-1$, то разложения (1) единственны.

Отметим (рис. 1), что

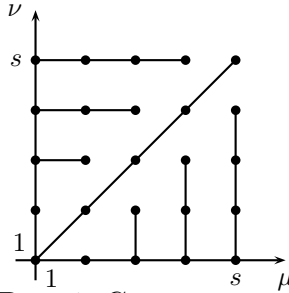


Рис. 1. Суммирование по квадрату

$$\begin{aligned} \left(\sum_{\mu=1}^s k_\mu q_\mu G_\mu \right) \left(\sum_{\nu=1}^s j_\nu p_\nu D_\nu \right) &= \sum_{\nu=1}^s k_\nu j_\nu q_\nu p_\nu G_\nu D_\nu + \\ &+ \sum_{\mu=2}^s \sum_{\nu=1}^{\mu-1} k_\mu j_\nu q_\mu p_\nu G_\mu D_\nu + \sum_{\nu=2}^s \sum_{\mu=1}^{\nu-1} k_\mu j_\nu q_\mu p_\nu G_\mu D_\nu = \\ &= A + L + H. \end{aligned}$$

Поэтому

$$\omega_N^{kj} = \omega_N^A \omega_N^L \omega_N^H. \quad (2)$$

Сокращение количества арифметических операций при вычислении ДПФ возможно в трёх случаях:

- (C1) $\langle L \rangle_N = \langle H \rangle_N = 0$,
- (C2) $\langle L \rangle_N = 0$,
- (C3) $\langle H \rangle_N = 0$.

2°. Условие (C1) выполняется, когда

$$\langle G_\mu D_\nu \rangle_N = 0 \quad \text{при } \mu \neq \nu. \quad (3)$$

Обозначим $B_\nu = N/n_\nu$. Самый простой способ обеспечить (3) — положить $G_\mu = B_\mu$, $D_\nu = B_\nu$. В этом случае $G_\mu D_\nu = N(N/(n_\nu n_\mu))$. Формула (2) принимает вид

$$\omega_N^{kj} = \omega_N^A = \prod_{\nu=1}^s \omega_N^{k_\nu j_\nu q_\nu p_\nu B_\nu^2} = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu \langle q_\nu p_\nu B_\nu \rangle_{n_\nu}}.$$

Если $\langle q_\nu p_\nu B_\nu \rangle_{n_\nu} = 1$ при всех $\nu \in 1 : s$, то получаем дальнейшее упрощение

$$\omega_N^{kj} = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu}. \quad (4)$$

Перепишем формулы (1) при выбранных G_μ , D_ν :

$$j = \left\langle \sum_{\nu=1}^s j_\nu p_\nu B_\nu \right\rangle_N, \quad j_\nu \in 0 : n_\nu - 1, \quad (5)$$

$$k = \left\langle \sum_{\mu=1}^s k_\mu q_\mu B_\mu \right\rangle_N, \quad k_\mu \in 0 : n_\mu - 1. \quad (6)$$

Взаимно однозначное соответствие между элементами множества $0 : N - 1$ и наборами коэффициентов (j_1, j_2, \dots, j_s) и (k_1, k_2, \dots, k_s) можно гарантировать лишь тогда, когда числа n_1, n_2, \dots, n_s попарно взаимно просты. Действительно, пусть, например, наряду с (5) имеется разложение

$$j = \left\langle \sum_{\nu=1}^s j'_\nu p_\nu B_\nu \right\rangle_N, \quad j'_\nu \in 0 : n_\nu - 1. \quad (7)$$

Покажем, что при сделанном предположении $j'_\nu = j_\nu$ при всех $\nu \in 1 : s$. Согласно (5) и (7)

$$\sum_{\nu=1}^s (j'_\nu - j_\nu) p_\nu B_\nu = t N.$$

Взяв вычеты по модулю n_μ , получим $\langle (j'_\mu - j_\mu) p_\mu B_\mu \rangle_{n_\mu} = 0$. Поскольку произведение $p_\mu B_\mu$ взаимно просто с n_μ , то $(j'_\mu - j_\mu)$ делится на n_μ . К равенству $j'_\mu = j_\mu$ мы приходим на том основании, что $|j'_\mu - j_\mu| \leq n_\mu - 1$.

Формулы (5), (6) и (4) порождают параметрический вариант метода простых множителей для вычисления ДПФ [2].

3°. Условие (C2) выполняется, когда

$$\langle G_\mu D_\nu \rangle_N = 0 \quad \text{при } \mu \in 2 : s, \nu \in 1 : \mu - 1. \quad (8)$$

Обозначим

$$\begin{aligned} \Delta_1 &= 1; \quad \Delta_\nu = n_1 n_2 \cdots n_{\nu-1} \quad \text{при } \nu \in 2 : s+1, \\ N_\nu &= n_{\nu+1} n_{\nu+2} \cdots n_s \quad \text{при } \nu \in 0 : s-1, \quad N_s = 1. \end{aligned}$$

Для обеспечения (8) положим

$$G_\mu = \Delta_\mu, \quad D_\nu = N_\nu. \quad (9)$$

В этом случае $G_\mu D_\nu = n_1 \cdots n_{\mu-1} n_{\nu+1} \cdots n_s = N(n_{\nu+1} \cdots n_{\mu-1})$. В частности, $G_\mu D_{\mu-1} = N$.

Согласно (9), $G_\nu D_\nu = N/n_\nu$, так что

$$\omega_N^A = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu q_\nu p_\nu}.$$

Если $\langle p_\nu q_\nu \rangle_{n_\nu} = 1$ при всех $\nu \in 1 : s$, то приходим к дальнейшему упрощению

$$\omega_N^A = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu}. \quad (10)$$

Условие (C2) гарантирует равенство $\omega_N^L = 1$. В то же время

$$\omega_N^H = \prod_{\nu=2}^s \omega_N^{j_\nu p_\nu N_\nu \sum_{\mu=1}^{\nu-1} k_\mu q_\mu \Delta_\mu}. \quad (11)$$

Обозначим

$$u_1 = 0, \quad u_\nu = j_\nu p_\nu \sum_{\mu=1}^{\nu-1} k_\mu q_\mu \Delta_\mu \quad \text{при } \nu = 2 : s.$$

Объединив (2), (10) и (11), получим формулу

$$\omega_N^{kj} = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu} \omega_{\Delta_{\nu+1}}^{u_\nu}. \quad (12)$$

Перепишем (1) при $D_\nu = N_\nu$ и $G_\mu = \Delta_\mu$:

$$j = \left\langle \sum_{\nu=1}^s j_\nu p_\nu N_\nu \right\rangle_N, \quad j_\nu \in 0 : n_\nu - 1, \quad (13)$$

$$k = \left\langle \sum_{\mu=1}^s k_{\mu} q_{\mu} \Delta_{\mu} \right\rangle_N, \quad k_{\mu} \in 0 : n_{\mu} - 1. \quad (14)$$

Покажем, что любые $j, k \in 0 : N - 1$ допускают такое представление.

Если наряду с (14) справедливо равенство

$$k = \left\langle \sum_{\mu=1}^s k'_{\mu} q_{\mu} \Delta_{\mu} \right\rangle_N, \quad k'_{\mu} \in 0 : n_{\mu} - 1,$$

то

$$(k'_1 - k_1) q_1 + \sum_{\mu=2}^s (k'_{\mu} - k_{\mu}) q_{\mu} \Delta_{\mu} = t N.$$

Взяв вычеты по модулю n_1 , запишем $\langle (k'_1 - k_1) q_1 \rangle_{n_1} = 0$. Отсюда и из взаимной простоты q_1 и n_1 следует, что $k'_1 = k_1$. Пусть $k'_{\mu} = k_{\mu}$ при $\mu \in 1 : \alpha - 1$. Тогда

$$(k'_{\alpha} - k_{\alpha}) q_{\alpha} \Delta_{\alpha} + \sum_{\mu=\alpha+1}^s (k'_{\mu} - k_{\mu}) q_{\mu} \Delta_{\mu} = t N.$$

Поделим эти равенства на Δ_{α} , а затем возьмём вычеты по модулю n_{α} . Получим $\langle (k'_{\alpha} - k_{\alpha}) q_{\alpha} \rangle_{n_{\alpha}} = 0$. По той же причине, что и раньше, $k'_{\alpha} = k_{\alpha}$.

Аналогично, допустив, что наряду с (13) справедливо равенство

$$j = \left\langle \sum_{\nu=1}^s j'_{\nu} p_{\nu} N_{\nu} \right\rangle_N, \quad j'_{\nu} \in 0 : n_{\nu} - 1,$$

последовательно установим, что $j'_s = j_s, j'_{s-1} = j_{s-1}, \dots, j'_1 = j_1$.

Формулы (13), (14) и (12) порождают параметрический вариант быстрого преобразования Фурье с прореживание по времени [1].

4°. Последнее условие (СЗ) выполняется, когда

$$\langle G_{\mu} D_{\nu} \rangle_N = 0 \quad \text{при } \nu \in 2 : s, \mu \in 1 : \nu - 1.$$

Это обеспечивается следующим выбором

$$D_{\nu} = \Delta_{\nu}, \quad G_{\mu} = N_{\mu},$$

поскольку $D_{\nu} G_{\mu} = n_1 \cdots n_{\nu-1} n_{\mu+1} \cdots n_s = N(n_{\mu+1} \cdots n_{\nu-1})$. В частности, $D_{\nu} G_{\nu-1} = N$.

Условие (СЗ) гарантирует равенство $\omega_N^H = 1$. В то же время

$$\omega_N^L = \prod_{\mu=2}^s \omega_N^{k_{\mu} q_{\mu} N_{\mu} \sum_{\nu=1}^{\mu-1} j_{\nu} p_{\nu} \Delta_{\nu}}.$$

Обозначим

$$v_1 = 0, \quad v_\mu = k_\mu q_\mu \sum_{\nu=1}^{\mu-1} j_\nu p_\nu \Delta_\nu \quad \text{при } \mu = 2 : s.$$

Если потребовать дополнительно, чтобы $\langle p_\nu q_\nu \rangle_{n_\nu} = 1$ при всех $\nu \in 1 : s$, то так же, как в предыдущем пункте, получим

$$\omega_N^{kj} = \prod_{\mu=1}^s \omega_{n_\mu}^{k_\mu j_\mu} \omega_{\Delta_{\mu+1}}^{v_\mu}. \quad (15)$$

Перепишем (1) при $D_\nu = \Delta_\nu$ и $G_\mu = N_\mu$:

$$j = \left\langle \sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu \right\rangle_N, \quad j_\nu \in 0 : n_\nu - 1, \quad (16)$$

$$k = \left\langle \sum_{\mu=1}^s k_\mu q_\mu N_\mu \right\rangle_N, \quad k_\mu \in 0 : n_\mu - 1. \quad (17)$$

Формулы (16), (17) и (15) порождают параметрический вариант быстрого преобразования Фурье с прореживание по частоте [1].

5°. Рассмотрим обобщённую реверсную перестановку π множества $0 : N-1$, сопоставляющую числу $l = \sum_{\nu=1}^s l_\nu \Delta_\nu$, где $l_\nu \in 0 : n_\nu - 1$, число

$$k = \left\langle \sum_{\nu=1}^s l_\nu p_\nu N_\nu \right\rangle_N.$$

Здесь, как и раньше, p_ν принадлежит $1 : N-1$ и взаимно просто с n_ν . Найдём обратную перестановку π^{-1} .

Имеем

$$\sum_{\nu=1}^{s-1} l_\nu p_\nu N_\nu + l_s p_s = t N + k.$$

Взяв вычеты по модулю n_s , получим $\langle l_s p_s \rangle_{n_s} = \langle k \rangle_{n_s}$. Пусть q_ν принадлежат $1 : n_\nu - 1$ и удовлетворяют условию $\langle q_\nu p_\nu \rangle_{n_\nu} = 1$, $\nu \in 1 : s$. Тогда, в частности, $l_s = \langle k q_s \rangle_{n_s}$.

Предположим, что уже вычислены $l_s, l_{s-1}, \dots, l_{\alpha+1}$. Обозначим

$$r_\alpha = k - \sum_{\nu=\alpha+1}^s l_\nu p_\nu N_\nu \quad (18)$$

и запишем

$$\sum_{\nu=1}^{\alpha-1} l_{\nu} p_{\nu} N_{\nu} + l_{\alpha} p_{\alpha} N_{\alpha} = t N + r_{\alpha}.$$

Поделим это равенство на N_{α} , после чего возьмём вычеты по модулю n_{α} . Придём к формуле

$$\langle l_{\alpha} p_{\alpha} \rangle_{n_{\alpha}} = \langle r_{\alpha} / N_{\alpha} \rangle_{n_{\alpha}}.$$

Отсюда следует, что

$$l_{\alpha} = \langle (q_{\alpha} r_{\alpha}) / N_{\alpha} \rangle_{n_{\alpha}}, \quad \alpha = s-1, s-2, \dots, 1. \quad (19)$$

Если учесть, что $r_s = k$ и $N_s = 1$, то (19) справедливо и при $\alpha = s$.

Таким образом,

$$\pi^{-1}(k) = \sum_{\nu=1}^s l_{\nu} \Delta_{\nu},$$

где l_{ν} последовательно вычисляется по формуле (19).

ЛИТЕРАТУРА

1. Свердлик М. Б. *Матричная интерпретация и вычислительная эффективность алгоритмов БПФ* // Радиотехника и электроника. 1984. № 2. С. 265–274.
2. Малозёмов В. Н., Просеков О. В. *Параметрический вариант метода простых множителей* // Семинар «DHA & CAGD». Избранные доклады. 5 сентября 2006 г. (<http://dha.spb.ru/rep06.shtml#0905>).

ПАРАМЕТРИЧЕСКАЯ ФАКТОРИЗАЦИЯ МАТРИЦЫ ФУРЬЕ

В. Н. Малозёмов

О. В. Просеков

19 сентября 2006 г.

Этот доклад примыкает к [1]. Используются те же обозначения.

1°. Пусть $N = n_1 n_2 \cdots n_s$ и p_ν при $\nu \in 1 : s$ — фиксированные натуральные числа, взаимно простые с n_ν . Вектор $p = (p_1, p_2, \dots, p_s)$ называется вектором параметров.

Введём перестановки $\text{mix}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}$ и $\text{rev}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}$, сопоставляющие числу $j \in 0 : N - 1$ с разложением

$$j = \sum_{\nu=1}^s j_\nu \Delta_\nu, \quad j_\nu \in 0 : n_\nu - 1,$$

числа

$$\begin{aligned} \text{mix}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}(j) &= \left\langle \sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu \right\rangle_N, \\ \text{rev}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}(j) &= \left\langle \sum_{\nu=1}^s j_\nu p_\nu N_\nu \right\rangle_N. \end{aligned}$$

Эти перестановки содержательны и при $s = 1$:

$$\text{mix}_{n_1}^{(p_1)}(j_1) = \text{rev}_{n_1}^{(p_1)}(j_1) = \langle j_1 p_1 \rangle_{n_1}, \quad j_1 \in 0 : n_1 - 1.$$

При $s = 2$ имеем

$$\text{mix}_{n_1, n_2}^{(p_1, p_2)}(j_1 + j_2 n_1) = \langle j_1 p_1 + j_2 p_2 n_1 \rangle_{n_1 n_2}, \quad (1)$$

$$\text{rev}_{n_1, n_2}^{(p_1, p_2)}(j_1 + j_2 n_1) = \langle j_1 p_1 n_2 + j_2 p_2 \rangle_{n_1 n_2}. \quad (2)$$

Формально

$$\text{mix}_{n_1, 1}^{(p_1, 1)}(j_1) = \langle j_1 p_1 \rangle_{n_1} = \text{mix}_{n_1}^{(p_1)}(j_1), \quad j_1 \in 0 : n_1 - 1,$$

$$\text{rev}_{1, n_2}^{(1, p_2)}(j_2) = \langle j_2 p_2 \rangle_{n_2} = \text{rev}_{n_2}^{(p_2)}(j_2), \quad j_2 \in 0 : n_2 - 1.$$

Обозначим $N_\mu^{(\nu)} = n_{\mu+1} n_{\mu+2} \cdots n_\nu$.

ЛЕММА 1. При $\nu = 2, \dots, s$ справедливы рекуррентные соотношения

$$\text{mix}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}(i_1 + i n_1) = \langle i_1 p_1 + n_1 \text{mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)}(i) \rangle_{\Delta_{\nu+1}}, \quad (3)$$

$$\text{rev}_{n_1, \dots, n_{\nu-1}, n_\nu}^{(p_1, \dots, p_{\nu-1}, p_\nu)}(j + j_\nu \Delta_\nu) = \langle n_\nu \text{rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}(j) + j_\nu p_\nu \rangle_{\Delta_{\nu+1}}. \quad (4)$$

Здесь $i_1 \in 0 : n_1 - 1$, $j_\nu \in 0 : n_\nu - 1$, $i \in 0 : N_1^{(\nu)} - 1$, $j \in 0 : \Delta_\nu - 1$.

Доказательство. Пусть $i = i_2 + i_3 n_2 + i_4 n_2 n_3 + \dots + i_\nu (n_2 n_3 \dots n_{\nu-1})$. Тогда

$$\text{mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)}(i) = \left\langle \sum_{\alpha=2}^{\nu} i_\alpha p_\alpha (n_2 n_3 \dots n_{\alpha-1}) \right\rangle_{n_2 n_3 \dots n_\nu}.$$

Воспользуемся формулой $\langle k n \rangle_{mn} = n \langle k \rangle_m$. Получим

$$\begin{aligned} \text{mix}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}(i_1 + i n_1) &= \left\langle i_1 p_1 + n_1 \sum_{\alpha=2}^{\nu} i_\alpha p_\alpha (n_2 n_3 \dots n_{\alpha-1}) \right\rangle_{n_1 (n_2 \dots n_\nu)} = \\ &= \left\langle i_1 p_1 + n_1 \left\langle \sum_{\alpha=2}^{\nu} i_\alpha p_\alpha (n_2 n_3 \dots n_{\alpha-1}) \right\rangle_{n_2 \dots n_\nu} \right\rangle_{n_1 (n_2 \dots n_\nu)} = \\ &= \langle i_1 p_1 + n_1 \text{mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)}(i) \rangle_{\Delta_{\nu+1}}. \end{aligned}$$

Соотношение (3) установлено.

Аналогично проверяется соотношение (4). Пусть $j = j_1 \Delta_1 + j_2 \Delta_2 + \dots + j_{\nu-1} \Delta_{\nu-1}$. Тогда

$$\begin{aligned} \text{rev}_{n_1, \dots, n_{\nu-1}, n_\nu}^{(p_1, \dots, p_{\nu-1}, p_\nu)}(j + j_\nu \Delta_\nu) &= \left\langle \sum_{\alpha=1}^{\nu-1} j_\alpha p_\alpha N_\alpha^{(\nu)} + j_\nu p_\nu \right\rangle_{n_\nu \Delta_\nu} = \\ &= \left\langle n_\nu \left\langle \sum_{\alpha=1}^{\nu-1} j_\alpha p_\alpha N_\alpha^{(\nu-1)} \right\rangle_{\Delta_\nu} + j_\nu p_\nu \right\rangle_{n_\nu \Delta_\nu} = \\ &= \langle n_\nu \text{rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}(j) + j_\nu p_\nu \rangle_{\Delta_{\nu+1}}. \end{aligned}$$

Лемма доказана. □

2°. Введём матрицы перестановок Mix и Rev :

$$\begin{aligned} \text{Mix}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}[j, k] &= \begin{cases} 1, & \text{если } k = \text{mix}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}(j), \\ 0 & \text{в остальных случаях;} \end{cases} \\ \text{Rev}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}[j, k] &= \begin{cases} 1, & \text{если } k = \text{rev}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}(j), \\ 0 & \text{в остальных случаях.} \end{cases} \end{aligned}$$

ЛЕММА 2. При $\nu = 2, \dots, s$ справедливы рекуррентные соотношения

$$\text{Mix}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)} = (\text{Mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)} \otimes I_{n_1}) \text{Mix}_{n_1, n_2 \dots n_\nu}^{(p_1, 1)}, \quad (5)$$

$$\text{Rev}_{n_1, \dots, n_{\nu-1}, n_\nu}^{(p_1, \dots, p_{\nu-1}, p_\nu)} = (I_{n_\nu} \otimes \text{Rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}) \text{Rev}_{\Delta_\nu, n_\nu}^{(1, p_\nu)}. \quad (6)$$

Доказательство. Возьмём произвольный $\Delta_{\nu+1}$ -мерный вектор x и обозначим $X = \text{Mix}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)} x$. В силу (3)

$$\begin{aligned} X(i_1 + i n_1) &= x(\text{mix}_{n_1, n_2, \dots, n_\nu}^{(p_1, p_2, \dots, p_\nu)}(i_1 + i n_1)) = \\ &= x(\langle i_1 p_1 + n_1 \text{mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)}(i) \rangle_{\Delta_{\nu+1}}). \end{aligned} \quad (7)$$

Далее, согласно (1) для вектора $Y = \text{Mix}_{n_1, n_2 \dots n_\nu}^{(p_1, 1)} x$ имеем

$$Y(i_1 + i n_1) = x(\langle i_1 p_1 + i n_1 \rangle_{\Delta_{\nu+1}}).$$

Найдём компоненты вектора $Z = (\text{Mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)} \otimes I_{n_1}) Y$. Запишем

$$\begin{aligned} Z(i_1 + i n_1) &= \sum_{i'_1=0}^{n_1-1} \sum_{i'=0}^{N_1^{(\nu)}-1} (\text{Mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)} \otimes I_{n_1}) [i_1 + i n_1, i'_1 + i' n_1] \times Y(i'_1 + i' n_1) = \\ &= \sum_{i'_1=0}^{n_1-1} \sum_{i'=0}^{N_1^{(\nu)}-1} \text{Mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)} [i, i'] \times I_{n_1} [i_1, i'_1] \times Y(i'_1 + i' n_1) = \\ &= Y(i_1 + n_1 \text{mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)}(i)) = x(\langle i_1 p_1 + n_1 \text{mix}_{n_2, \dots, n_\nu}^{(p_2, \dots, p_\nu)}(i) \rangle_{\Delta_{\nu+1}}). \end{aligned} \quad (8)$$

Сравнивая (7) и (8), приходим к равенству $Z = X$. Отсюда следует (5).

Проверим соотношение (6). Обозначим $X = \text{Rev}_{n_1, \dots, n_{\nu-1}, n_\nu}^{(p_1, \dots, p_{\nu-1}, p_\nu)} x$. В силу (4)

$$\begin{aligned} X(j + j_\nu \Delta_\nu) &= x(\text{rev}_{n_1, \dots, n_{\nu-1}, n_\nu}^{(p_1, \dots, p_{\nu-1}, p_\nu)}(j + j_\nu \Delta_\nu)) = \\ &= x(\langle n_\nu \text{rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}(j) + j_\nu p_\nu \rangle_{\Delta_{\nu+1}}). \end{aligned} \quad (9)$$

В то же время согласно (2) для вектора $Y = \text{Rev}_{\Delta_\nu, n_\nu}^{(1, p_\nu)} x$ имеем

$$Y(j + j_\nu \Delta_\nu) = x(\langle j n_\nu + j_\nu p_\nu \rangle_{\Delta_{\nu+1}}).$$

Найдём компоненты вектора $Z = (I_{n_\nu} \otimes \text{Rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}) Y$. Запишем

$$Z(j + j_\nu \Delta_\nu) = \sum_{j'_\nu=0}^{n_\nu-1} \sum_{j'=0}^{\Delta_\nu-1} (I_{n_\nu} \otimes \text{Rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}) [j + j_\nu \Delta_\nu, j' + j'_\nu \Delta_\nu] \times$$

$$\begin{aligned}
\times Y(j' + j'_\nu \Delta_\nu) &= \sum_{j'_\nu=0}^{n_\nu-1} \sum_{j'=0}^{\Delta_\nu-1} I_{n_\nu}[j_\nu, j'_\nu] \times \text{Rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}[j, j'] \times \\
&\times Y(j' + j'_\nu \Delta_\nu) = Y(\text{rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}(j) + j_\nu \Delta_\nu) = \\
&= x(\langle n_\nu \text{rev}_{n_1, \dots, n_{\nu-1}}^{(p_1, \dots, p_{\nu-1})}(j) + j_\nu p_\nu \rangle_{\Delta_{\nu+1}}). \quad (10)
\end{aligned}$$

Сравнивая (9) и (10), приходим к равенству $Z = X$. Отсюда следует (6).

Лемма доказана. \square

ТЕОРЕМА 1. При $s \geq 2$ справедливы разложения

$$\text{Mix}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} = \prod_{\nu=0}^{s-1} (\text{Mix}_{n_{s-\nu}, N_{s-\nu}}^{(p_{s-\nu}, 1)} \otimes I_{\Delta_{s-\nu}}), \quad (11)$$

$$\text{Rev}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} = \prod_{\nu=1}^s (I_{N_\nu} \otimes \text{Rev}_{\Delta_\nu, n_\nu}^{(1, p_\nu)}). \quad (12)$$

Доказательство. Отметим, что согласно замечанию из п. 1°

$$\text{Mix}_{n_s, N_s}^{(p_s, 1)} = \text{Mix}_{n_s, 1}^{(p_s, 1)} = \text{Mix}_{n_s}^{(p_s)}, \quad (13)$$

$$\text{Rev}_{\Delta_1, n_1}^{(1, p_1)} = \text{Rev}_{1, n_1}^{(1, p_1)} = \text{Rev}_{n_1}^{(p_1)}. \quad (14)$$

При $s = 2$ формула (11) принимает вид

$$\text{Mix}_{n_1, n_2}^{(p_1, p_2)} = (\text{Mix}_{n_2, N_2}^{(p_2, 1)} \otimes I_{\Delta_2}) \text{Mix}_{n_1, N_1}^{(p_1, 1)}.$$

Её справедливость следует из (5) и (13). Сделаем индукционный переход от s к $s + 1$. На основании леммы 2 и индукционного предположения имеем

$$\begin{aligned}
\text{Mix}_{n_1, n_2, \dots, n_{s+1}}^{(p_1, p_2, \dots, p_{s+1})} &= (\text{Mix}_{n_2, \dots, n_{s+1}}^{(p_2, \dots, p_{s+1})} \otimes I_{n_1}) \text{Mix}_{n_1, n_2 \dots n_{s+1}}^{(p_1, 1)} = \\
&= \left(\prod_{\nu=0}^{s-1} (\text{Mix}_{n_{s+1-\nu}, n_{s+2-\nu} \dots n_{s+1}}^{(p_{s+1-\nu}, 1)} \otimes I_{n_2 \dots n_{s-\nu}}) \otimes \underbrace{I_{n_1} I_{n_1} \dots I_{n_1}}_{s \text{ раз}} \right) \text{Mix}_{n_1, n_2 \dots n_{s+1}}^{(p_1, 1)} = \\
&= \left(\prod_{\nu=0}^{s-1} (\text{Mix}_{n_{s+1-\nu}, n_{s+2-\nu} \dots n_{s+1}}^{(p_{s+1-\nu}, 1)} \otimes I_{n_1 n_2 \dots n_{s-\nu}}) \right) (\text{Mix}_{n_1, n_2 \dots n_{s+1}}^{(p_1, 1)} \otimes I_{\Delta_1}) = \\
&= \prod_{\nu=0}^s (\text{Mix}_{n_{s+1-\nu}, n_{s+2-\nu} \dots n_{s+1}}^{(p_{s+1-\nu}, 1)} \otimes I_{\Delta_{s+1-\nu}}).
\end{aligned}$$

Формула (11) установлена.

Обратимся к формуле (12). При $s = 2$ она принимает вид

$$Rev_{n_1, n_2}^{(p_1, p_2)} = (I_{N_1} \otimes Rev_{\Delta_1, n_1}^{(1, p_1)}) Rev_{\Delta_2, n_2}^{(1, p_2)}.$$

Справедливость этого равенства следует из (6) и (14). Сделаем индукционный переход от s к $s + 1$. На основании леммы 2 и индукционного предположения имеем

$$\begin{aligned} Rev_{n_1, \dots, n_s, n_{s+1}}^{(p_1, \dots, p_s, p_{s+1})} &= (I_{n_{s+1}} \otimes Rev_{n_1, \dots, n_s}^{(p_1, \dots, p_s)}) Rev_{\Delta_{s+1}, n_{s+1}}^{(1, p_{s+1})} = \\ &= \left(\underbrace{I_{n_{s+1}} I_{n_{s+1}} \cdots I_{n_{s+1}}}_{s \text{ раз}} \otimes \prod_{\nu=1}^s (I_{n_{\nu+1} \cdots n_s} \otimes Rev_{\Delta_{\nu}, n_{\nu}}^{(1, p_{\nu})}) \right) (I_1 \otimes Rev_{\Delta_{s+1}, n_{s+1}}^{(1, p_{s+1})}) = \\ &= \prod_{\nu=1}^{s+1} (I_{n_{\nu+1} \cdots n_{s+1}} \otimes Rev_{\Delta_{\nu}, n_{\nu}}^{(1, p_{\nu})}). \end{aligned}$$

Теорема доказана. \square

3°. Рассмотрим вопрос о параметрической факторизации матрицы Фурье F_N с элементами $F_N[k, j] = \omega_N^{kj}$, $k, j \in 0 : N - 1$. Для этого нам потребуется диагональная матрица вращений $Twid$:

$$Twid_{n_1, \dots, n_{\nu}}^{(p_1, \dots, p_{\nu})} \left[\sum_{\alpha=1}^{\nu} j_{\alpha} \Delta_{\alpha}, \sum_{\alpha=1}^{\nu} j'_{\alpha} \Delta_{\alpha} \right] = \begin{cases} \omega_{\Delta_{\nu+1}}^{j_{\nu} p_{\nu} \sum_{\alpha=1}^{\nu-1} j_{\alpha} p_{\alpha} \Delta_{\alpha}}, & \text{если } j'_{\alpha} = j_{\alpha}, \alpha \in 1 : \nu; \\ 0 & \text{в остальных случаях.} \end{cases}$$

Здесь $j_{\alpha}, j'_{\alpha} \in 0 : n_{\alpha} - 1$, $\alpha \in 1 : \nu$; $\nu \in 2 : s$. По определению $Twid_{n_1}^{(p_1)} = I_{n_1}$.

ЛЕММА 3. При $s = 2$ и $\langle q_1 p_1 \rangle_{n_1} = \langle q_2 p_2 \rangle_{n_2} = 1$ справедливо разложение

$$F_{n_1 n_2} = (Mix_{n_1, n_2}^{(q_1, q_2)})^T (F_{n_2} \otimes I_{n_1}) Twid_{n_1, n_2}^{(q_1, p_2)} (I_{n_2} \otimes F_{n_1}) Rev_{n_1, n_2}^{(p_1, p_2)}. \quad (15)$$

Доказательство. Достаточно проверить равенство матриц

$$Mix_{n_1, n_2}^{(q_1, q_2)} F_{n_1 n_2} (Rev_{n_1, n_2}^{(p_1, p_2)})^T = (F_{n_2} \otimes I_{n_1}) Twid_{n_1, n_2}^{(q_1, p_2)} (I_{n_2} \otimes F_{n_1}).$$

Сравним элементы с индексами $(k_1 + k_2 n_1, j_1 + j_2 n_1)$. Согласно (1), (2) имеем

$$\begin{aligned} & \left(Mix_{n_1, n_2}^{(q_1, q_2)} F_{n_1 n_2} (Rev_{n_1, n_2}^{(p_1, p_2)})^T \right) [k_1 + k_2 n_1, j_1 + j_2 n_1] = \\ &= \sum_{l=0}^{n_1 n_2 - 1} \sum_{l'=0}^{n_1 n_2 - 1} Mix_{n_1, n_2}^{(q_1, q_2)} [k_1 + k_2 n_1, l] \times F_{n_1 n_2} [l, l'] \times Rev_{n_1, n_2}^{(p_1, p_2)} [j_1 + j_2 n_1, l'] = \\ &= F_{n_1 n_2} [\text{mix}_{n_1, n_2}^{(q_1, q_2)}(k_1 + k_2 n_1), \text{rev}_{n_1, n_2}^{(p_1, p_2)}(j_1 + j_2 n_1)] = \omega_{n_1 n_2}^{(k_1 q_1 + k_2 q_2 n_1)(j_1 p_1 n_2 + j_2 p_2)} = \\ &= \omega_{n_1}^{k_1 j_1 q_1 p_1} \omega_{n_1 n_2}^{k_1 j_2 q_1 p_2} \omega_{n_2}^{k_2 j_2 q_2 p_2} = \omega_{n_1}^{k_1 j_1} \omega_{n_1 n_2}^{k_1 j_2 q_1 p_2} \omega_{n_2}^{k_2 j_2}. \end{aligned}$$

Вместе с тем,

$$\begin{aligned}
& \left((F_{n_2} \otimes I_{n_1}) \text{Twid}_{n_1, n_2}^{(q_1, p_2)} (I_{n_2} \otimes F_{n_1}) \right) [k_1 + k_2 n_1, j_1 + j_2 n_1] = \\
& = \sum_{l_1=0}^{n_1-1} \sum_{l_2=0}^{n_2-1} (F_{n_2} \otimes I_{n_1}) [k_1 + k_2 n_1, l_1 + l_2 n_1] \times \text{Twid}_{n_1, n_2}^{(q_1, p_2)} [l_1 + l_2 n_1, l_1 + l_2 n_1] \times \\
& \times (I_{n_2} \otimes F_{n_1}) [l_1 + l_2 n_1, j_1 + j_2 n_1] = \sum_{l_1=0}^{n_1-1} \sum_{l_2=0}^{n_2-1} F_{n_2} [k_2, l_2] \times I_{n_1} [k_1, l_1] \times \omega_{n_1 n_2}^{l_2 p_2 l_1 q_1} \times \\
& \times I_{n_2} [l_2, j_2] \times F_{n_1} [l_1, j_1] = \omega_{n_2}^{k_2 j_2} \omega_{n_1 n_2}^{j_2 p_2 k_1 q_1} \omega_{n_1}^{k_1 j_1}.
\end{aligned}$$

Лемма доказана. \square

Транспонируем матрицы, стоящие в левой и правой частях (15), и поменяем местами p_1 и q_1 , p_2 и q_2 . Придём к другому разложению матрицы Фурье:

$$F_{n_1 n_2} = (\text{Rev}_{n_1, n_2}^{(q_1, q_2)})^T (I_{n_2} \otimes F_{n_1}) \text{Twid}_{n_1, n_2}^{(p_1, q_2)} (F_{n_2} \otimes I_{n_1}) \text{Mix}_{n_1, n_2}^{(p_1, p_2)}. \quad (16)$$

ТЕОРЕМА 2. При $N = n_1 n_2 \cdots n_s$ и любом векторе параметров $p = (p_1, p_2, \dots, p_s)$ матрица Фурье F_N допускает представление

$$F_N = (\text{Rev}_{n_1, \dots, n_s}^{(q_1, \dots, q_s)})^T \left(\prod_{\nu=1}^s (I_{N_\nu} \otimes \text{Twid}_{n_1, \dots, n_{\nu-1}, n_\nu}^{(p_1, \dots, p_{\nu-1}, q_\nu)}) (I_{N_\nu} \otimes F_{n_\nu} \otimes I_{\Delta_\nu}) \right) \text{Mix}_{n_1, \dots, n_s}^{(p_1, \dots, p_s)}, \quad (17)$$

где $q = (q_1, q_2, \dots, q_s)$ — сопряжённый вектор параметров, компоненты которого удовлетворяет условию $\langle q_\nu p_\nu \rangle_{n_\nu} = 1$, $\nu \in 1 : s$.

Доказательство. При $s = 2$ формула (17) совпадает с (16). Сделаем индукционный переход от s к $s + 1$.

Обозначим

$$\begin{aligned}
L_s &= \text{Rev}_{n_1, \dots, n_s}^{(q_1, \dots, q_s)} F_N (\text{Mix}_{n_1, \dots, n_s}^{(p_1, \dots, p_s)})^T, \\
G_s &= \prod_{\nu=1}^s (I_{N_\nu} \otimes \text{Twid}_{n_1, \dots, n_{\nu-1}, n_\nu}^{(p_1, \dots, p_{\nu-1}, q_\nu)}) (I_{N_\nu} \otimes F_{n_\nu} \otimes I_{\Delta_\nu}).
\end{aligned}$$

По индукционному предположению $L_s = G_s$. Нужно проверить, что $L_{s+1} = G_{s+1}$.

Выясним, что даёт равенство $L_s = G_s$. Имеем

$$\begin{aligned}
& L_s \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, \sum_{\nu=1}^s j_\nu \Delta_\nu \right] = \\
& = \sum_{l=0}^{N-1} \sum_{l'=0}^{N-1} \text{Rev}_{n_1, \dots, n_s}^{(q_1, \dots, q_s)} \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, l \right] \times F_N [l, l'] \times \text{Mix}_{n_1, \dots, n_s}^{(p_1, \dots, p_s)} \left[\sum_{\nu=1}^s j_\nu \Delta_\nu, l' \right] =
\end{aligned}$$

$$\begin{aligned}
&= F_N \left[\text{rev}_{n_1, \dots, n_s}^{(q_1, \dots, q_s)} \left(\sum_{\nu=1}^s k_\nu \Delta_\nu \right), \text{mix}_{n_1, \dots, n_s}^{(p_1, \dots, p_s)} \left(\sum_{\nu=1}^s j_\nu \Delta_\nu \right) \right] = \\
&= \omega_N^{\left(\sum_{\nu=1}^s k_\nu q_\nu N_\nu \right) \left(\sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu \right)}.
\end{aligned}$$

Значит,

$$G_s \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, \sum_{\nu=1}^s j_\nu \Delta_\nu \right] = \omega_N^{\left(\sum_{\nu=1}^s k_\nu q_\nu N_\nu \right) \left(\sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu \right)}.$$

Ясно, что

$$\begin{aligned}
L_{s+1} \left[\sum_{\nu=1}^{s+1} k_\nu \Delta_\nu, \sum_{\nu=1}^{s+1} j_\nu \Delta_\nu \right] &= \omega_{n_1 \dots n_s n_{s+1}}^{\left(\sum_{\nu=1}^{s+1} k_\nu q_\nu (n_{\nu+1} \dots n_{s+1}) \right) \left(\sum_{\nu=1}^{s+1} j_\nu p_\nu \Delta_\nu \right)} = \\
&= \omega_{n_1 \dots n_s n_{s+1}}^{\left(n_{s+1} \sum_{\nu=1}^s k_\nu q_\nu (n_{\nu+1} \dots n_s) + k_{s+1} q_{s+1} \right) \left(\sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu + j_{s+1} p_{s+1} (n_1 \dots n_s) \right)} = \\
&= \omega_{n_1 \dots n_s}^{\left(\sum_{\nu=1}^s k_\nu q_\nu N_\nu \right) \left(\sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu \right)} \omega_{n_1 \dots n_s n_{s+1}}^{k_{s+1} q_{s+1} \sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu} \omega_{n_{s+1}}^{k_{s+1} j_{s+1} q_{s+1} p_{s+1}} = \\
&= G_s \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, \sum_{\nu=1}^s j_\nu \Delta_\nu \right] \omega_{n_1 \dots n_s n_{s+1}}^{k_{s+1} q_{s+1} \sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu} F_{n_{s+1}}[k_{s+1}, j_{s+1}].
\end{aligned}$$

(Мы воспользовались равенством $\langle q_{s+1} p_{s+1} \rangle_{n_{s+1}} = 1$.) Требуется установить, что то же значение имеет элемент $G_{s+1} \left[\sum_{\nu=1}^{s+1} k_\nu \Delta_\nu, \sum_{\nu=1}^{s+1} j_\nu \Delta_\nu \right]$.

Преобразуем выражение для G_{s+1} . Запишем

$$\begin{aligned}
G_{s+1} &= \left(\prod_{\nu=1}^s \left(I_{n_{s+1}} \otimes (I_{n_{\nu+1} \dots n_s} \otimes \text{Twid}_{n_1, \dots, n_{\nu-1}, n_\nu}^{(p_1, \dots, p_{\nu-1}, q_\nu)}) \right) \right) \times \\
&\times \left(I_{n_{s+1}} \otimes (I_{n_{\nu+1} \dots n_s} \otimes F_{n_\nu} \otimes I_{\Delta_\nu}) \right) \text{Twid}_{n_1, \dots, n_s, n_{s+1}}^{(p_1, \dots, p_s, q_{s+1})} (F_{n_{s+1}} \otimes I_{\Delta_{s+1}}) = \\
&= (I_{n_{s+1}} \otimes G_s) \text{Twid}_{n_1, \dots, n_s, n_{s+1}}^{(p_1, \dots, p_s, q_{s+1})} (F_{n_{s+1}} \otimes I_{\Delta_{s+1}}).
\end{aligned}$$

Вычислим

$$\begin{aligned}
&G_{s+1} \left[\sum_{\nu=1}^{s+1} k_\nu \Delta_\nu, \sum_{\nu=1}^{s+1} j_\nu \Delta_\nu \right] = \\
&= \sum_{k'_1=0}^{n_1-1} \dots \sum_{k'_s=0}^{n_s-1} \sum_{k'_{s+1}=0}^{n_{s+1}-1} (I_{n_{s+1}} \otimes G_s) \left[\sum_{\nu=1}^s k_\nu \Delta_\nu + k_{s+1} \Delta_{s+1}, \sum_{\nu=1}^s k'_\nu \Delta_\nu + k'_{s+1} \Delta_{s+1} \right] \times \\
&\times \text{Twid}_{n_1, \dots, n_s, n_{s+1}}^{(p_1, \dots, p_s, q_{s+1})} \left[\sum_{\nu=1}^s k'_\nu \Delta_\nu + k'_{s+1} \Delta_{s+1}, \sum_{\nu=1}^s k'_\nu \Delta_\nu + k'_{s+1} \Delta_{s+1} \right] \times \\
&\times (F_{n_{s+1}} \otimes I_{\Delta_{s+1}}) \left[\sum_{\nu=1}^s k'_\nu \Delta_\nu + k'_{s+1} \Delta_{s+1}, \sum_{\nu=1}^s j_\nu \Delta_\nu + j_{s+1} \Delta_{s+1} \right] =
\end{aligned}$$

$$\begin{aligned}
&= \sum_{k'_1=0}^{n_1-1} \cdots \sum_{k'_s=0}^{n_s-1} \sum_{k'_{s+1}=0}^{n_{s+1}-1} I_{n_{s+1}}[k_{s+1}, k'_{s+1}] \times G_s \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, \sum_{\nu=1}^s k'_\nu \Delta_\nu \right] \times \\
&\times \text{Twid}_{n_1, \dots, n_s, n_{s+1}}^{(p_1, \dots, p_s, q_{s+1})} \left[\sum_{\nu=1}^s k'_\nu \Delta_\nu + k'_{s+1} \Delta_{s+1}, \sum_{\nu=1}^s k'_\nu \Delta_\nu + k'_{s+1} \Delta_{s+1} \right] \times \\
&\times F_{n_{s+1}}[k'_{s+1}, j_{s+1}] \times I_{\Delta_{s+1}} \left[\sum_{\nu=1}^s k'_\nu \Delta_\nu, \sum_{\nu=1}^s j_\nu \Delta_\nu \right] = \\
&= G_s \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, \sum_{\nu=1}^s j_\nu \Delta_\nu \right] \times \\
&\times \text{Twid}_{n_1, \dots, n_s, n_{s+1}}^{(p_1, \dots, p_s, q_{s+1})} \left[\sum_{\nu=1}^s j_\nu \Delta_\nu + k_{s+1} \Delta_{s+1}, \sum_{\nu=1}^s j_\nu \Delta_\nu + k_{s+1} \Delta_{s+1} \right] \times \\
&\times F_{n_{s+1}}[k_{s+1}, j_{s+1}].
\end{aligned}$$

Остаётся учесть, что

$$\begin{aligned}
&\text{Twid}_{n_1, \dots, n_s, n_{s+1}}^{(p_1, \dots, p_s, q_{s+1})} \left[\sum_{\nu=1}^s j_\nu \Delta_\nu + k_{s+1} \Delta_{s+1}, \sum_{\nu=1}^s j_\nu \Delta_\nu + k_{s+1} \Delta_{s+1} \right] = \\
&= \omega_{n_1 \dots n_s n_{s+1}}^{k_{s+1} q_{s+1} \sum_{\nu=1}^s j_\nu p_\nu \Delta_\nu}.
\end{aligned}$$

Теорема доказана. \square

Транспонируем матрицы, стоящие в левой и правой частях (17), и поменяем местами параметры p_ν и q_ν при всех $\nu \in 1 : s$. Придём к другому представлению матрицы Фурье:

$$\begin{aligned}
F_N &= (\text{Mix}_{n_1, \dots, n_s}^{(q_1, \dots, q_s)})^T \left(\prod_{\nu=0}^{s-1} (I_{N_{s-\nu}} \otimes F_{n_{s-\nu}} \otimes I_{\Delta_{s-\nu}}) \times \right. \\
&\times \left. (I_{N_{s-\nu}} \otimes \text{Twid}_{n_1, \dots, n_{s-\nu-1}, n_{s-\nu}}^{(q_1, \dots, q_{s-\nu-1}, p_{s-\nu})}) \right) \text{Rev}_{n_1, \dots, n_s}^{(p_1, \dots, p_s)}.
\end{aligned}$$

Теорема 2 вместе с теоремой 1 дают наиболее глубокое параметрическое разложение матрицы Фурье F_N при $N = n_1 n_2 \cdots n_s$.

4°. В заключение установим связь между матрицами параметрических перестановок Rev и Mix .

ТЕОРЕМА 3. *Справедливо равенство*

$$\text{Rev}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} = \text{Rev}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)} \text{Mix}_{n_s, n_{s-1}, \dots, n_1}^{(p_s, p_{s-1}, \dots, p_1)}.$$

Доказательство. Возьмём произвольный N -мерный вектор x . Для векторов $X = \text{Rev}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)} x$, $Y = \text{Mix}_{n_s, n_{s-1}, \dots, n_1}^{(p_s, p_{s-1}, \dots, p_1)} x$, $Z = \text{Rev}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)} Y$ имеем соответственно

$$\begin{aligned}
X(j) &= x(\text{rev}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}(j)), \\
Y(j) &= x(\text{mix}_{n_s, n_{s-1}, \dots, n_1}^{(p_s, p_{s-1}, \dots, p_1)}(j)), \\
Z(j) &= Y(\text{rev}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)}(j)) = \\
&= x(\text{mix}_{n_s, n_{s-1}, \dots, n_1}^{(p_s, p_{s-1}, \dots, p_1)}(\text{rev}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)}(j))).
\end{aligned}$$

Покажем, что

$$\text{rev}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}(j) = \text{mix}_{n_s, n_{s-1}, \dots, n_1}^{(p_s, p_{s-1}, \dots, p_1)}(\text{rev}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)}(j)). \quad (18)$$

Отсюда будет следовать равенство $X = Z$, эквивалентное требуемому.

Пусть $j = \sum_{\nu=1}^s j_\nu \Delta_\nu$. Тогда

$$\text{rev}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)}(j) = \sum_{\nu=1}^s j_\nu N_\nu = \sum_{\nu=1}^s j_{s-\nu+1} N_{s-\nu+1}.$$

Переобозначим $n'_\nu = n_{s-\nu+1}$, $p'_\nu = p_{s-\nu+1}$. В этом случае

$$\begin{aligned}
\Delta'_\nu &:= n'_1 n'_2 \cdots n'_{\nu-1} = n_s n_{s-1} \cdots n_{s-\nu+2} = N_{s-\nu+1}, \\
\text{rev}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)}(j) &= \sum_{\nu=1}^s j_{s-\nu+1} \Delta'_\nu, \\
\text{mix}_{n_s, n_{s-1}, \dots, n_1}^{(p_s, p_{s-1}, \dots, p_1)}(\text{rev}_{n_1, n_2, \dots, n_s}^{(1, 1, \dots, 1)}(j)) &= \text{mix}_{n'_1, n'_2, \dots, n'_s}^{(p'_1, p'_2, \dots, p'_s)}\left(\sum_{\nu=1}^s j_{s-\nu+1} \Delta'_\nu\right) = \\
&= \left\langle \sum_{\nu=1}^s j_{s-\nu+1} p'_\nu \Delta'_\nu \right\rangle_N = \left\langle \sum_{\nu=1}^s j_{s-\nu+1} p_{s-\nu+1} N_{s-\nu+1} \right\rangle_N = \\
&= \left\langle \sum_{\nu=1}^s j_\nu p_\nu N_\nu \right\rangle_N = \text{rev}_{n_1, n_2, \dots, n_s}^{(p_1, p_2, \dots, p_s)}(j).
\end{aligned}$$

Формула (18), а с ней и теорема, доказаны. \square

ЛИТЕРАТУРА

1. Малозёмов В. Н., Просеков О. В. *Общий подход к вычислению ДПФ* // Семинар «DHA & CAGD». Избранные доклады. 12 сентября 2006 г. (<http://dha.spb.ru/rep06.shtml#0912>).

ПАРАМЕТРИЧЕСКИЙ ВАРИАНТ МНОГОМЕРНОГО БЫСТРОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ

О. В. Просеков

26 сентября 2006 г.

1°. Пусть m_1, m_2, \dots, m_t — натуральные числа, отличные от единицы. Введём обозначения

$$\begin{aligned} m &= (m_1, m_2, \dots, m_t); \\ M &= m_1 m_2 \cdots m_t; \\ M_\mu &= m_{\mu+1} m_{\mu+2} \cdots m_t \quad \text{при } \mu \in 0 : t-1, \quad M_t = 1; \\ \Lambda_1 &= 1; \quad \Lambda_\mu = m_1 m_2 \cdots m_{\mu-1} \quad \text{при } \mu \in 2 : t+1. \end{aligned}$$

Многомерное дискретное преобразование Фурье сигнала $x_m \in C_{m_1} \times C_{m_2} \times \cdots \times C_{m_t}$, определяется формулой

$$X_m(k_1, k_2, \dots, k_t) = \sum_{j_t=0}^{m_t-1} \cdots \sum_{j_2=0}^{m_2-1} \sum_{j_1=0}^{m_1-1} x_m(j_1, j_2, \dots, j_t) \omega_{m_1}^{-k_1 j_1} \omega_{m_2}^{-k_2 j_2} \cdots \omega_{m_t}^{-k_t j_t},$$

где $k_\mu \in 0 : m_\mu - 1$, $\mu \in 1 : t$.

ПРЕДЛОЖЕНИЕ. Пусть $x(j_1 + j_2 \Lambda_1 + \cdots + j_t \Lambda_t) = x_m(j_1, j_2, \dots, j_t)$ и

$$X = (\bar{F}_{m_t} \otimes \cdots \otimes \bar{F}_{m_2} \otimes \bar{F}_{m_1}) x,$$

где $\bar{F}_{m_\mu}[k, j] = \omega_{m_\mu}^{-kj}$, $k, j \in 0 : m_\mu - 1$, $\mu \in 1 : t$. Тогда

$$X_m(k_1, k_2, \dots, k_t) = X(k_1 + k_2 \Lambda_1 + \cdots + k_t \Lambda_t).$$

Доказательство. В силу известного свойства кронекерова умножения матриц [1] имеем

$$(\bar{F}_{m_t} \otimes \cdots \otimes \bar{F}_{m_2} \otimes \bar{F}_{m_1}) \left[\sum_{\mu=1}^t k_\mu \Lambda_\mu, \sum_{\mu=1}^t j_\mu \Lambda_\mu \right] = \prod_{\mu=1}^t \bar{F}_{m_\mu}[k_\mu, j_\mu] = \prod_{\mu=1}^t \omega_{m_\mu}^{-k_\mu j_\mu}.$$

Поэтому

$$\begin{aligned}
& X\left(\sum_{\mu=1}^t k_{\mu} \Lambda_{\mu}\right) = \\
& = \sum_{j_t=0}^{m_t-1} \cdots \sum_{j_2=0}^{m_2-1} \sum_{j_1=0}^{m_1-1} \left(\bar{F}_{m_t} \otimes \cdots \otimes \bar{F}_{m_2} \otimes \bar{F}_{m_1}\right) \left[\sum_{\mu=1}^t k_{\mu} \Lambda_{\mu}, \sum_{\mu=1}^t j_{\mu} \Lambda_{\mu}\right] \times \\
& \quad \times x\left(\sum_{\mu=1}^t j_{\mu} \Lambda_{\mu}\right) = \sum_{j_t=0}^{m_t-1} \cdots \sum_{j_2=0}^{m_2-1} \sum_{j_1=0}^{m_1-1} x\left(\sum_{\mu=1}^t j_{\mu} \Lambda_{\mu}\right) \prod_{\mu=1}^t \omega_{m_{\nu}}^{-k_{\mu} j_{\mu}} = \\
& = \sum_{j_t=0}^{m_t-1} \cdots \sum_{j_2=0}^{m_2-1} \sum_{j_1=0}^{m_1-1} x_m(j_1, j_2, \dots, j_t) \prod_{\mu=1}^t \omega_{m_{\nu}}^{-k_{\mu} j_{\mu}} = X_m(k_1, k_2, \dots, k_t).
\end{aligned}$$

Предложение доказано. \square

2°. Рассмотрим один из вариантов факторизации матрицы $F_{m_t} \otimes \cdots \otimes F_{m_2} \otimes F_{m_1}$. Введём матрицу $n = \{n_{\nu, \mu}\}$ ($\nu \in 1 : s$, $\mu \in 1 : t$), такую, что $m_{\mu} = n_{1, \mu} \times \cdots \times n_{s, \mu}$. Считаем $n_{\nu, \mu} \geq 1$. Пусть

$$\begin{aligned}
N_{\nu, \mu} &= n_{\nu+1, \mu} n_{\nu+2, \mu} \cdots n_{s, \mu} \quad \text{при } \nu \in 0 : s-1, \quad N_{s, \mu} = 1; \\
\Delta_{1, \mu} &= 1; \quad \Delta_{\nu, \mu} = n_{1, \mu} n_{2, \mu} \cdots n_{\nu-1, \mu} \quad \text{при } \nu \in 2 : s+1.
\end{aligned}$$

Выберем матрицу параметров $p = \{p_{\nu, \mu}\}$ ($\nu \in 1 : s$, $\mu \in 1 : t$), такую, что каждое $p_{\nu, \mu}$ взаимно просто с $n_{\nu, \mu}$. Тогда матрицы Фурье $F_{m_{\mu}}$ допускают параметрическое представление [2]

$$\begin{aligned}
F_{m_{\mu}} &= \left(\text{Rev}_{n_{1, \mu}, \dots, n_{s, \mu}}^{(q_{1, \mu}, \dots, q_{s, \mu})}\right)^T \left(\prod_{\nu=1}^s (I_{N_{\nu, \mu}} \otimes \text{Twid}_{n_{1, \mu}, \dots, n_{\nu-1, \mu}, n_{\nu, \mu}}^{(p_{1, \mu}, \dots, p_{\nu-1, \mu}, q_{\nu, \mu})}) \times \right. \\
& \quad \left. \times (I_{N_{\nu, \mu}} \otimes F_{n_{\nu, \mu}} \otimes I_{\Delta_{\nu, \mu}})\right) \text{Mix}_{n_{1, \mu}, \dots, n_{s, \mu}}^{(p_{1, \mu}, \dots, p_{s, \mu})}. \quad (1)
\end{aligned}$$

В этой формуле $q = \{q_{\nu, \mu}\}$ — матрица сопряжённых параметров; при $n_{\nu, \mu} > 1$ соответствующее $q_{\nu, \mu}$ определяется соотношением $\langle q_{\nu, \mu} p_{\nu, \mu} \rangle_{n_{\nu, \mu}} = 1$, при $n_{\nu, \mu} = 1$ соответствующее $q_{\nu, \mu}$ равно нулю. Матрица $\text{Twid}_{n_{1, \mu}, \dots, n_{\nu-1, \mu}, n_{\nu, \mu}}^{(p_{1, \mu}, \dots, p_{\nu-1, \mu}, p_{\nu, \mu})}$ — диагональная параметрическая матрица вращений с элементами

$$\text{Twid}_{n_{1, \mu}, \dots, n_{\nu-1, \mu}, n_{\nu, \mu}}^{(p_{1, \mu}, \dots, p_{\nu-1, \mu}, p_{\nu, \mu})} \left[\sum_{\alpha=1}^{\nu} j_{\alpha} \Delta_{\alpha, \mu}, \sum_{\alpha=1}^{\nu} j_{\alpha} \Delta_{\alpha, \mu} \right] = \omega_{\Delta_{\nu+1, \mu}}^{j_{\nu} p_{\nu} \sum_{\alpha=1}^{\nu-1} j_{\alpha} p_{\alpha, \mu} \Delta_{\alpha, \mu}}. \quad (2)$$

Здесь $\nu \in 2 : s$, $\mu \in 1 : t$ и $j_{\alpha} \in 0 : n_{\alpha, \mu} - 1$. Напомним, что $\text{Twid}_{n_{1, \mu}}^{(p_{1, \mu})} = I_{n_{1, \mu}}$.

Матрицы $Mix_{n_{1,\mu}, \dots, n_{s,\mu}}^{(p_{1,\mu}, \dots, p_{s,\mu})}$ и $Rev_{n_{1,\mu}, \dots, n_{s,\mu}}^{(q_{1,\mu}, \dots, q_{s,\mu})}$ допускают разложения [2]

$$Mix_{n_{1,\mu}, \dots, n_{s,\mu}}^{(p_{1,\mu}, \dots, p_{s,\mu})} = \prod_{\nu=0}^{s-1} (Mix_{n_{s-\nu,\mu}, N_{s-\nu,\mu}}^{(p_{s-\nu,\mu}, 1)} \otimes I_{\Delta_{s-\nu,\mu}}), \quad (3)$$

$$Rev_{n_{1,\mu}, \dots, n_{s,\mu}}^{(q_{1,\mu}, \dots, q_{s,\mu})} = \prod_{\nu=1}^s (I_{N_{\nu,\mu}} \otimes Rev_{\Delta_{\nu,\mu}, n_{\nu,\mu}}^{(1, q_{\nu,\mu})}). \quad (4)$$

Если $n_{\nu,\mu} = 1$, то $Mix_{1, N_{s-\nu,\mu}}^{(p_{s-\nu,\mu}, 1)} = I_{N_{s-\nu,\mu}}$ и $Rev_{\Delta_{\nu,\mu}, 1}^{(1, 0)} = I_{\Delta_{\nu,\mu}}$.

Справедлива следующая

ТЕОРЕМА 1. При любой матрице параметров $p = \{p_{\nu,\mu}\}$ матрица $F_{m_t} \otimes \dots \otimes F_{m_2} \otimes F_{m_1}$ допускает представление

$$F_{m_t} \otimes \dots \otimes F_{m_2} \otimes F_{m_1} = (R_m^{(q)})^T \left(\prod_{\nu=1}^s T_m^{(\nu)} \prod_{\mu=1}^t (I_{M_\mu N_{\nu,\mu}} \otimes F_{n_{\nu,\mu}} \otimes I_{\Lambda_\mu \Delta_{\nu,\mu}}) \right) S_m^{(p)}, \quad (5)$$

где $q = \{q_{\nu,\mu}\}$ — матрица сопряжённых параметров; $S_m^{(p)}$ и $R_m^{(q)}$ — матрицы перестановок вида

$$S_m^{(p)} = \prod_{\nu=0}^{s-1} \prod_{\mu=1}^t (I_{M_\mu} \otimes Mix_{n_{s-\nu,\mu}, N_{s-\nu,\mu}}^{(p_{s-\nu,\mu}, 1)} \otimes I_{\Delta_{s-\nu,\mu} \Lambda_\mu}), \quad (6)$$

$$R_m^{(q)} = \prod_{\nu=1}^s \prod_{\mu=1}^t (I_{M_\mu N_{\nu,\mu}} \otimes Rev_{\Delta_{\nu,\mu}, n_{\nu,\mu}}^{(1, q_{\nu,\mu})} \otimes I_{\Lambda_\mu}); \quad (7)$$

$T_m^{(\nu)}$ — диагональная матрица с элементами

$$T_m^{(\nu)} \left[\sum_{\mu=1}^t \sum_{\alpha=1}^s j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_\mu, \sum_{\mu=1}^t \sum_{\alpha=1}^s j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_\mu \right] = \prod_{\mu=1}^t \omega_{\Delta_{\nu+1,\mu}}^{j_{\nu,\mu} q_{\nu,\mu} \sum_{\alpha=1}^{\nu-1} j_{\alpha,\mu} p_{\alpha,\mu} \Delta_{\alpha,\mu}}, \quad (8)$$

где $\nu \in 2 : s$, $\mu \in 1 : t$ и $j_\alpha \in 0 : n_{\alpha,\mu} - 1$.

Доказательство. Нам понадобятся следующие свойства кронекерова умножения матриц [3]:

$$A_{m_t}^{(t)} \otimes \dots \otimes A_{m_2}^{(2)} \otimes A_{m_1}^{(1)} = \prod_{\mu=1}^t (I_{M_\mu} \otimes A_{m_\mu}^{(\mu)} \otimes I_{\Lambda_\mu}), \quad (9)$$

$$\begin{aligned} & \prod_{\nu=1}^s (A_{m_1}^{(\nu)} \otimes B_{m_2}^{(\nu)} \otimes \dots \otimes G_{m_t}^{(\nu)}) = \\ & = \left(\prod_{\nu=1}^s A_{m_1}^{(\nu)} \right) \otimes \left(\prod_{\nu=1}^s B_{m_2}^{(\nu)} \right) \otimes \dots \otimes \left(\prod_{\nu=1}^s G_{m_t}^{(\nu)} \right). \end{aligned} \quad (10)$$

Сомножители в правой части (9) можно переставлять в любом порядке.

Выведем формулу (5), опираясь на приведённые свойства кронекерова умножения. На этом пути мы получим формулы (6), (7) и (8).

Введём обозначения

$$\begin{aligned} S_{m_\mu}^{(\mu)} &= \text{Mix}_{n_{1,\mu}, \dots, n_{s,\mu}}^{(p_{1,\mu}, \dots, p_{s,\mu})}, & R_{m_\mu}^{(\mu)} &= \text{Rev}_{n_{1,\mu}, \dots, n_{s,\mu}}^{(q_{1,\mu}, \dots, q_{s,\mu})}, \\ T_{m_\mu}^{(\nu)} &= I_{N_{\nu,\mu}} \otimes \text{Twid}_{n_{1,\mu}, \dots, n_{\nu-1,\mu}, n_{\nu,\mu}}^{(p_{1,\mu}, \dots, p_{\nu-1,\mu}, q_{\nu,\mu})}, & D_{m_\mu}^{(\nu)} &= I_{N_{\nu,\mu}} \otimes F_{n_{\nu,\mu}} \otimes I_{\Delta_{\nu,\mu}}. \\ H_{m_\mu}^{(\mu)} &= \prod_{\nu=1}^s T_{m_\mu}^{(\nu)} D_{m_\mu}^{(\nu)}. \end{aligned}$$

В этих обозначениях формула (1) примет следующий вид

$$F_{m_\mu} = (R_{m_\mu}^{(\mu)})^T H_{m_\mu}^{(\mu)} S_{m_\mu}^{(\mu)}.$$

Тогда

$$\begin{aligned} &F_{m_t} \otimes \dots \otimes F_{m_2} \otimes F_{m_1} = \\ &= \left((R_{m_t}^{(t)})^T H_{m_t}^{(t)} S_{m_t}^{(t)} \right) \otimes \dots \otimes \left((R_{m_2}^{(2)})^T H_{m_2}^{(2)} S_{m_2}^{(2)} \right) \otimes \left((R_{m_1}^{(1)})^T H_{m_1}^{(1)} S_{m_1}^{(1)} \right) = \\ &= \left(R_{m_t}^{(t)} \otimes \dots \otimes R_{m_2}^{(2)} \otimes R_{m_1}^{(1)} \right)^T \left(H_{m_t}^{(t)} \otimes \dots \otimes H_{m_2}^{(2)} \otimes H_{m_1}^{(1)} \right) \times \\ &\quad \times \left(S_{m_t}^{(t)} \otimes \dots \otimes S_{m_2}^{(2)} \otimes S_{m_1}^{(1)} \right). \end{aligned} \quad (11)$$

Здесь мы использовали свойство (10). Разберёмся с матрицами перестановок в формуле (11). Учитывая разложения (3), (4) и пользуясь (9), получаем

$$\begin{aligned} S_{m_t}^{(t)} \otimes \dots \otimes S_{m_2}^{(2)} \otimes S_{m_1}^{(1)} &= \prod_{\mu=1}^t (I_{M_\mu} \otimes \text{Mix}_{n_{1,\mu}, \dots, n_{s,\mu}}^{(p_{1,\mu}, \dots, p_{s,\mu})} \otimes I_{\Lambda_\mu}) = \\ &= \prod_{\nu=0}^{s-1} \prod_{\mu=1}^t (I_{M_\mu} \otimes \text{Mix}_{n_{s-\nu,\mu}, N_{s-\nu,\mu}}^{(p_{s-\nu,\mu}, 1)} \otimes I_{\Delta_{s-\nu,\mu} \Lambda_\mu}) = S_m^{(p)}, \\ R_{m_t}^{(t)} \otimes \dots \otimes R_{m_2}^{(2)} \otimes R_{m_1}^{(1)} &= \prod_{\mu=1}^t (I_{M_\mu} \otimes \text{Rev}_{n_{1,\mu}, \dots, n_{s,\mu}}^{(q_{1,\mu}, \dots, q_{s,\mu})} \otimes I_{\Lambda_\mu}) = \\ &= \prod_{\nu=1}^s \prod_{\mu=1}^t (I_{M_\mu N_{\nu,\mu}} \otimes \text{Rev}_{\Delta_{\nu,\mu}, n_{\nu,\mu}}^{(1, q_{\nu,\mu})} \otimes I_{\Lambda_\mu}) = R_m^{(q)}. \end{aligned}$$

Формулы (6) и (7) установлены.

В силу определения матрицы $H_{m_\mu}^{(\mu)}$ и свойства (10) приходим к следующему соотношению

$$H_{m_t}^{(t)} \otimes \dots \otimes H_{m_2}^{(2)} \otimes H_{m_1}^{(1)} = \prod_{\nu=1}^s (T_{m_t}^{(\nu)} \otimes \dots \otimes T_{m_2}^{(\nu)} \otimes T_{m_1}^{(\nu)}) \times \\ \times (D_{m_t}^{(\nu)} \otimes \dots \otimes D_{m_2}^{(\nu)} \otimes D_{m_1}^{(\nu)}). \quad (12)$$

Разберёмся с диагональной матрицей $T_{m_t}^{(\nu)} \otimes \dots \otimes T_{m_2}^{(\nu)} \otimes T_{m_1}^{(\nu)}$. Имеем

$$T_{m_t}^{(\nu)} \otimes \dots \otimes T_{m_2}^{(\nu)} \otimes T_{m_1}^{(\nu)} = (I_{N_{\nu,t}} \otimes \text{Twid}_{n_{1,t}, \dots, n_{\nu-1,t}, t, q_{\nu,t}}^{(p_{1,t}, \dots, p_{\nu-1,t}, q_{\nu,t})}) \otimes \dots \otimes \\ \otimes (I_{N_{\nu,2}} \otimes \text{Twid}_{n_{1,2}, \dots, n_{\nu-1,2}, 2, q_{\nu,2}}^{(p_{1,2}, \dots, p_{\nu-1,2}, q_{\nu,2})}) \otimes (I_{N_{\nu,1}} \otimes \text{Twid}_{n_{1,1}, \dots, n_{\nu-1,1}, 1, q_{\nu,1}}^{(p_{1,1}, \dots, p_{\nu-1,1}, q_{\nu,1})}).$$

По определению параметрической матрицы вращений (2) получим

$$(I_{N_{\nu,\mu}} \otimes \text{Twid}_{n_{1,\mu}, \dots, n_{\nu-1,\mu}, \mu, q_{\nu,\mu}}^{(p_{1,\mu}, \dots, p_{\nu-1,\mu}, q_{\nu,\mu})}) \left[\sum_{\alpha=1}^s j_{\alpha} \Delta_{\alpha,\mu}, \sum_{\alpha=1}^s j_{\alpha} \Delta_{\alpha,\mu} \right] = \omega_{\Delta_{\nu+1,\mu}}^{j_{\nu} q_{\nu,\mu} \sum_{\alpha=1}^{\nu-1} j_{\alpha} p_{\alpha,\mu} \Delta_{\alpha,\mu}}.$$

Следовательно,

$$T_{m_t}^{(\nu)} \otimes \dots \otimes T_{m_2}^{(\nu)} \otimes T_{m_1}^{(\nu)} \left[\sum_{\mu=1}^t \sum_{\alpha=1}^s j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_{\mu}, \sum_{\mu=1}^t \sum_{\alpha=1}^s j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_{\mu} \right] = \\ = \prod_{\mu=1}^t \omega_{\Delta_{\nu+1,\mu}}^{j_{\nu,\mu} q_{\nu,\mu} \sum_{\alpha=1}^{\nu-1} j_{\alpha,\mu} p_{\alpha,\mu} \Delta_{\alpha,\mu}} = T_m^{(\nu)} \left[\sum_{\mu=1}^t \sum_{\alpha=1}^s j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_{\mu}, \sum_{\mu=1}^t \sum_{\alpha=1}^s j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_{\mu} \right].$$

Формула (8) установлена.

Пусть $D_m^{(\nu)} = D_{m_t}^{(\nu)} \otimes \dots \otimes D_{m_2}^{(\nu)} \otimes D_{m_1}^{(\nu)}$. По свойству (9)

$$D_m^{(\nu)} = \prod_{\mu=1}^t (I_{M_{\mu}} \otimes D_{m_{\mu}}^{(\nu)} \otimes I_{\Lambda_{\mu}}) = \prod_{\mu=1}^t (I_{M_{\mu} N_{\nu,\mu}} \otimes F_{n_{\nu,\mu}} \otimes I_{\Lambda_{\mu} \Delta_{\nu,\mu}}). \quad (13)$$

Подставив формулы (12) и (13) в (11), получим (5).

Теорема доказана. \square

З а м е ч а н и е. Матрицы $R_m^{(q)}$ и $S_m^{(p)}$ могут быть представлены в явном виде:

$$S_m^{(p)} \left[\sum_{\mu=1}^t j_{\mu} \Lambda_{\mu}, \sum_{\mu=1}^t k_{\mu} \Lambda_{\mu} \right] = (S_{m_t}^{(t)} \otimes \dots \otimes S_{m_2}^{(2)} \otimes S_{m_1}^{(1)}) \left[\sum_{\mu=1}^t j_{\mu} \Lambda_{\mu}, \sum_{\mu=1}^t k_{\mu} \Lambda_{\mu} \right] = \\ = \prod_{\mu=1}^t \text{Mix}_{n_{1,\mu}, \dots, n_{s,\mu}}^{(p_{1,\mu}, \dots, p_{s,\mu})} [j_{\mu}, k_{\mu}] = \begin{cases} 1, & \text{если } k_{\mu} = \text{mix}_{n_{1,\mu}, \dots, n_{s,\mu}}^{(p_{1,\mu}, \dots, p_{s,\mu})}(j_{\mu}), \\ 0 & \text{в остальных случаях,} \end{cases} \\ R_m^{(q)} \left[\sum_{\mu=1}^t j_{\mu} \Lambda_{\mu}, \sum_{\mu=1}^t k_{\mu} \Lambda_{\mu} \right] = (R_{m_t}^{(t)} \otimes \dots \otimes R_{m_2}^{(2)} \otimes R_{m_1}^{(1)}) \left[\sum_{\mu=1}^t j_{\mu} \Lambda_{\mu}, \sum_{\mu=1}^t k_{\mu} \Lambda_{\mu} \right] = \\ = \prod_{\mu=1}^t \text{Rev}_{n_{1,\mu}, \dots, n_{s,\mu}}^{(q_{1,\mu}, \dots, q_{s,\mu})} [j_{\mu}, k_{\mu}] = \begin{cases} 1, & \text{если } k_{\mu} = \text{rev}_{n_{1,\mu}, \dots, n_{s,\mu}}^{(q_{1,\mu}, \dots, q_{s,\mu})}(j_{\mu}), \\ 0 & \text{в остальных случаях.} \end{cases}$$

Поскольку $\text{Twid}_{n_{1,\mu}}^{(p_{1,\mu})} = I_{n_{1,\mu}}$, то $T_m^{(1)} = I_M$.

3°. Рассмотрим пример. Пусть $m = (24, 6, 2)$ и

$$n = \begin{bmatrix} 2 & 1 & 1 \\ 3 & 2 & 1 \\ 4 & 3 & 2 \end{bmatrix}, \quad p = \begin{bmatrix} 3 & 1 & 1 \\ 2 & 3 & 1 \\ 3 & 2 & 3 \end{bmatrix}, \quad q = \begin{bmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 3 & 2 & 1 \end{bmatrix}.$$

По формуле (5) получим

$$\begin{aligned} F_{24} \otimes F_6 \otimes F_2 &= (R_m^{(q)})^T \left(T_m^{(1)} (I_{144} \otimes F_2 \otimes I_1) (I_{12} \otimes F_1 \otimes I_{24}) (I_2 \otimes F_1 \otimes I_{144}) \times \right. \\ &\quad \times T_m^{(2)} (I_{48} \otimes F_3 \otimes I_2) (I_6 \otimes F_2 \otimes I_{24}) (I_2 \otimes F_1 \otimes I_{144}) \times \\ &\quad \times T_m^{(3)} (I_{12} \otimes F_4 \otimes I_6) (I_2 \otimes F_3 \otimes I_{48}) (I_1 \otimes F_2 \otimes I_{144}) \left. \right) S_m^{(p)} = \\ &= (R_m^{(q)})^T \left((I_{144} \otimes F_2) T_m^{(2)} (I_{48} \otimes F_3 \otimes I_2) (I_6 \otimes F_2 \otimes I_{24}) \times \right. \\ &\quad \times T_m^{(3)} (I_{12} \otimes F_4 \otimes I_6) (I_2 \otimes F_3 \otimes I_{48}) (F_2 \otimes I_{144}) \left. \right) S_m^{(p)}. \end{aligned}$$

Матрица $S_m^{(p)}$ определяется формулой (6):

$$\begin{aligned} S_m^{(p)} &= (I_{12} \otimes \text{Mix}_{4,1}^{(3,1)} \otimes I_6) (I_2 \otimes \text{Mix}_{3,1}^{(2,1)} \otimes I_{48}) (I_1 \otimes \text{Mix}_{2,1}^{(3,1)} \otimes I_{144}) \times \\ &\quad \times (I_{12} \otimes \text{Mix}_{3,4}^{(2,1)} \otimes I_2) (I_2 \otimes \text{Mix}_{2,3}^{(3,1)} \otimes I_{24}) (I_1 \otimes \text{Mix}_{1,2}^{(1,1)} \otimes I_{144}) \times \\ &\quad \times (I_{12} \otimes \text{Mix}_{2,12}^{(3,1)} \otimes I_1) (I_2 \otimes \text{Mix}_{1,6}^{(1,1)} \otimes I_{24}) (I_1 \otimes \text{Mix}_{1,2}^{(1,1)} \otimes I_{144}) = \\ &= (I_{12} \otimes \text{Mix}_{4,1}^{(3,1)} \otimes I_6) (I_2 \otimes \text{Mix}_{3,1}^{(2,1)} \otimes I_{48}) \times \\ &\quad \times (I_{12} \otimes \text{Mix}_{3,4}^{(2,1)} \otimes I_2) (I_2 \otimes \text{Mix}_{2,3}^{(3,1)} \otimes I_{24}) (I_{12} \otimes \text{Mix}_{2,12}^{(3,1)}). \end{aligned}$$

Матрица $R_m^{(q)}$ определяется формулой (7):

$$\begin{aligned} R_m^{(q)} &= (I_{144} \otimes \text{Rev}_{1,2}^{(1,1)} \otimes I_1) (I_{12} \otimes \text{Rev}_{1,1}^{(1,0)} \otimes I_{24}) (I_2 \otimes \text{Rev}_{1,1}^{(1,0)} \otimes I_{144}) \times \\ &\quad \times (I_{48} \otimes \text{Rev}_{2,3}^{(1,2)} \otimes I_1) (I_6 \otimes \text{Rev}_{1,2}^{(1,1)} \otimes I_{24}) (I_2 \otimes \text{Rev}_{1,1}^{(1,0)} \otimes I_{144}) \times \\ &\quad \times (I_{12} \otimes \text{Rev}_{6,4}^{(1,3)} \otimes I_1) (I_2 \otimes \text{Rev}_{2,3}^{(1,2)} \otimes I_{24}) (I_1 \otimes \text{Rev}_{1,2}^{(1,1)} \otimes I_{144}) = \\ &= (I_{48} \otimes \text{Rev}_{2,3}^{(1,2)}) (I_{12} \otimes \text{Rev}_{6,4}^{(1,3)}) (I_2 \otimes \text{Rev}_{2,3}^{(1,2)} \otimes I_{24}). \end{aligned}$$

Матрицы вращений $T_m^{(2)}$ и $T_m^{(3)}$ получаются следующие:

$$\begin{aligned} T_m^{(2)} \left[\sum_{\mu=1}^3 \sum_{\alpha=1}^3 j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_{\mu}, \sum_{\mu=1}^3 \sum_{\alpha=1}^3 j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_{\mu} \right] &= \prod_{\mu=1}^3 \omega_{\Delta_{3,\mu}}^{j_{2,\mu} q_{2,\mu} j_{1,\mu} p_{1,\mu} \Delta_{1,\mu}} = \\ &= \omega_6^{6 j_{2,1} j_{1,1}} \omega_2^{j_{2,2} j_{1,2}} \omega_1^{0 j_{2,3} j_{1,3}} = 1, \end{aligned}$$

$$\begin{aligned}
T_m^{(3)} \left[\sum_{\mu=1}^3 \sum_{\alpha=1}^3 j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_{\mu}, \sum_{\mu=1}^3 \sum_{\alpha=1}^3 j_{\alpha,\mu} \Delta_{\alpha,\mu} \Lambda_{\mu} \right] &= \prod_{\mu=1}^3 \omega_{\Delta_{4,\mu}}^{j_{3,\mu} q_{3,\mu} \sum_{\alpha=1}^2 j_{\alpha,\mu} p_{\alpha,\mu} \Delta_{\alpha,\mu}} = \\
&= \omega_{24}^{3 j_{3,1} (3 j_{1,1} + 4 j_{2,1})} \omega_6^{2 j_{3,2} (j_{1,2} + 3 j_{2,2})} \omega_2^{j_{3,3} (j_{1,3} + j_{2,3})} = \\
&= \omega_8^{j_{3,1} (3 j_{1,1} + 4 j_{2,1})} \omega_6^{6 j_{3,2} j_{2,2}} \omega_2^{j_{3,3}} = \omega_8^{3 j_{3,1} j_{1,1}} (-1)^{j_{3,1} j_{2,1} + j_{3,3}}.
\end{aligned}$$

В матрице $T_m^{(2)}$ все диагональные элементы тривиальные (равны 1), т. е. $T_m^{(2)} = I_{288}$. В матрице $T_m^{(3)}$ среди диагональных элементов 156 равны 1, 24 равны -1 , 36 равны i и оставшиеся 72 — нетривиальные.

4°. Подсчитаем количество арифметических операций, необходимых для вычисления многомерного ДПФ. Обозначим через $\psi(N)$ количество комплексных умножений, необходимых для вычисления ДПФ длины N , а через $\eta(N)$ — количество комплексных сложений. В построчно-столбцовом подходе вычисления многомерного ДПФ [4, с. 259], когда к μ -й размерности применяется соответствующий одномерный алгоритм БПФ M/m_μ раз, нам потребуется следующее количество арифметических операций:

$$\begin{aligned}
\psi(M) &= \sum_{\mu=1}^t \psi(m_\mu) M/m_\mu = \\
&= \sum_{\mu=1}^t M/m_\mu \sum_{\nu=1}^s (N_{\nu,\mu} (\Delta_{\nu,\mu} - 1) (n_{\nu,\mu} - 1) + N_{\nu,\mu} \psi(n_{\nu,\mu}) \Delta_{\nu,\mu}), \\
\eta(M) &= \sum_{\mu=1}^t \eta(m_\mu) M/m_\mu = \sum_{\mu=1}^t M/m_\mu \sum_{\nu=1}^s N_{\nu,\mu} \eta(n_{\nu,\mu}) \Delta_{\nu,\mu}.
\end{aligned}$$

В теореме 1 диагональная матрица $T_m^{(\nu)}$ зависит от матриц параметров p и q . Обозначим через $\varphi_\nu(n, p, q)$ число комплексных нетривиальных элементов в матрице $T_m^{(\nu)}$. Понятно, что $\varphi_\nu(n, p, q) < M$.

В предложенном методе вычисления многомерного ДПФ, в формуле (5), потребуется следующее количество арифметических операций:

$$\begin{aligned}
\psi(M) &= \sum_{\nu=1}^s \sum_{\mu=1}^t M_\mu N_{\nu,\mu} \psi(n_{\nu,\mu}) \Delta_{\nu,\mu} \Lambda_\mu + \sum_{\nu=2}^s \varphi_\nu(n, p, q), \\
\eta(M) &= \sum_{\nu=1}^s \sum_{\mu=1}^t M_\mu N_{\nu,\mu} \eta(n_{\nu,\mu}) \Delta_{\nu,\mu} \Lambda_\mu.
\end{aligned}$$

Если в приведённом в п. 3 примере использовать алгоритмы БПФ малых порядков с $\psi(2) = 0$, $\eta(2) = 2$, $\psi(3) = 2$, $\eta(3) = 6$ и $\psi(4) = 0$, $\eta(4) = 8$ [5], то

получим такой результат:

$$\begin{aligned}\psi(288) &= 144 \cdot 0 + 48 \cdot 2 \cdot 2 + 6 \cdot 0 \cdot 2 + 12 \cdot 0 \cdot 6 + 2 \cdot 2 \cdot 48 + 0 \cdot 144 + 72 = \\ &= 384 + 72 = 456,\end{aligned}$$

$$\eta(288) = 144 \cdot 2 + 48 \cdot 6 \cdot 2 + 6 \cdot 2 \cdot 2 + 12 \cdot 8 \cdot 6 + 2 \cdot 6 \cdot 48 + 2 \cdot 144 = 2328.$$

В непараметрическом случае (все $p_\nu = q_\nu = 1$) число умножений будет равно

$$\psi(288) = 384 + 96 + 180 = 660.$$

Для построчно-столбцевого метода вычисления многомерного ДПФ число умножений будет равно

$$\psi(288) = 12 \cdot 39 + 48 \cdot 12 + 144 \cdot 0 = 1044.$$

В заключение отметим, что результат, представленный в теореме 1, может быть использован в методе простых множителей [6]. Результат теоремы в непараметрическом случае для $M = 2^t$ был получен в [7].

ЛИТЕРАТУРА

1. Малозёмов В. Н., Просеков О. В. *Факторизация матриц реверсных перестановок* // Семинар «DHA & CAGD». Избранные доклады. 2 мая 2006 г. (<http://dha.spb.ru/rep06.shtml#0502>).
2. Малозёмов В. Н., Просеков О. В. *Параметрическая факторизация матрицы Фурье* // Семинар «DHA & CAGD». Избранные доклады. 19 сентября 2006 г. (<http://dha.spb.ru/rep06.shtml#0919>).
3. Малозёмов В. Н., Просеков О. В. *Перестановки и кронекерово произведение матриц* // Семинар «DHA & CAGD». Избранные доклады. 31 марта 2004 г. (<http://dha.spb.ru/rep04.shtml#0331>).
4. Блейхут Р. *Быстрые алгоритмы цифровой обработки сигналов*. М.: Мир, 1989. 448 с.
5. Просеков О. В. *Быстрое преобразование Фурье малых порядков* // Семинар «DHA & CAGD». Избранные доклады. 6 декабря 2005 г. (<http://dha.spb.ru/rep05.shtml#1206>).
6. Малозёмов В. Н., Просеков О. В. *Параметрический вариант метода простых множителей* // Семинар «DHA & CAGD». Избранные доклады. 5 сентября 2006 г. (<http://dha.spb.ru/rep06.shtml#0905>).
7. Власенко В. А., Лаппа Ю. М. *Матричный подход к построению быстрых алгоритмов многомерного ДПФ* // Изв. вузов. Радиоэлектроника. 1986. Т. 29. № 1. С. 86–89.

РАЗДЕЛЁННЫЕ РАЗНОСТИ С КРАТНЫМИ УЗЛАМИ

В. Н. Малозёмов

10 октября 2006 г.

Разделённые разности с кратными узлами активно используются в геометрическом моделировании. Теорию таких разностей можно строить либо с помощью предельного перехода от разделённых разностей с простыми узлами [1, с. 173-181], либо на основе эрмитовой интерполяции [2, с. 65-77]. Мы выбираем второй вариант.

1°. Обозначим через \mathcal{P}_n множество алгебраических полиномов степени не выше n . Рассмотрим задачу эрмитовой интерполяции: найти полином $P_n \in \mathcal{P}_n$, удовлетворяющий условиям

$$P_n^{(s)}(x_k) = f^{(s)}(x_k), \quad k \in 1 : m, \quad s \in 0 : r_k - 1. \quad (1)$$

Здесь x_1, \dots, x_m – попарно различные точки на вещественной прямой и $\sum_{k=1}^m r_k = n + 1$. Предполагается, что все производные функции f из правой части (1) существуют.

ПРЕДЛОЖЕНИЕ 1. *Задача (1) имеет решение и это решение единственно.*

Доказательство. Условия (1) – это система линейных уравнений $(n + 1)$ -го порядка относительно коэффициентов полинома $P_n(x)$. Предложение будет доказано, если мы установим, что однородная система имеет только нулевое решение.

Рассмотрим однородную систему

$$P_n^{(s)}(x_k) = 0, \quad k \in 1 : m, \quad s \in 0 : r_k - 1, \quad (2)$$

и возьмём любое её решение, порождающее полином $\hat{P}_n(x)$. Согласно (2) полином $\hat{P}_n(x)$ имеет $n + 1$ корней с учётом их кратности. Поскольку $\hat{P}_n \in \mathcal{P}_n$, то необходимо $\hat{P}_n(x) \equiv 0$. Но тогда все коэффициенты $\hat{P}_n(x)$ равны нулю, т. е. система (2) имеет только нулевое решение. \square

Старший коэффициент (при x^n) интерполяционного полинома $P_n(x)$ называется *разделённой разностью n -го порядка функции f* и обозначается

$$f[x_1^{\langle r_1 \rangle}, \dots, x_m^{\langle r_m \rangle}].$$

Из определения (и единственности интерполяционного полинома) следует, что разделённая разность линейна по f и симметрична по узлам. Последнее означает, что

$$f[x_1^{\langle r_1 \rangle}, \dots, x_i^{\langle r_i \rangle}, \dots, x_j^{\langle r_j \rangle}, \dots, x_m^{\langle r_m \rangle}] = f[x_1^{\langle r_1 \rangle}, \dots, x_j^{\langle r_j \rangle}, \dots, x_i^{\langle r_i \rangle}, \dots, x_m^{\langle r_m \rangle}].$$

В дальнейшем вместо $x_k^{(1)}$ будем писать x_k . Запись $x_k^{(0)}$ нужно понимать так, что узел x_k отсутствует.

2°. Рассмотрим частные случаи.

1) $m = 1, r_1 = 1$ [$n = 0$]. Имеем $P_0(x) \equiv f(x_1)$. По определению

$$f[x_1] = f(x_1).$$

2) $m = 1, r_1 = n + 1$. Задача (1) принимает вид

$$P_n^{(s)}(x_1) = f^{(s)}(x_1), \quad s \in 0 : n.$$

Её решением является полином Тейлора

$$P_n(x) = \sum_{s=0}^n \frac{f^{(s)}(x_1)}{s!} (x - x_1)^s.$$

По определению

$$f[x_1^{\langle n+1 \rangle}] = \frac{f^{(n)}(x_1)}{n!}.$$

3) $m = 2, r_1 = r_2 = 1$ [$n = 1$]. Запишем интерполяционный полином

$$P_1(x) = \frac{x_2 - x}{x_2 - x_1} f(x_1) + \frac{x - x_1}{x_2 - x_1} f(x_2).$$

По определению

$$f[x_1, x_2] = \frac{f(x_2) - f(x_1)}{x_2 - x_1}.$$

4) $f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$. В этом случае интерполяционный полином $P_n(x)$ совпадает с $f(x)$, так что

$$f[x_1^{\langle r_1 \rangle}, \dots, x_m^{\langle r_m \rangle}] = a_0.$$

5) $f \in \mathcal{P}_{n-1}$. По определению разделённой разности

$$f[x_1^{\langle r_1 \rangle}, \dots, x_m^{\langle r_m \rangle}] = 0.$$

3°. Обозначим через P_{n-1} и Q_{n-1} интерполяционные полиномы степени не выше $n - 1$, построенные по узлам $x_1^{(r_1)}, \dots, x_{m-1}^{(r_{m-1})}, x_m^{(r_m-1)}$ и $x_1^{(r_1-1)}, x_2^{(r_2)}, \dots, x_m^{(r_m)}$ соответственно.

ПРЕДЛОЖЕНИЕ 2. При $m \geq 2$ справедливо тождество

$$P_n(x) = \frac{x_m - x}{x_m - x_1} P_{n-1}(x) + \frac{x - x_1}{x_m - x_1} Q_{n-1}(x). \quad (3)$$

Доказательство. Достаточно проверить, что полином $\tilde{P}_n(x)$, стоящий в правой части (3), удовлетворяет условиям (1).

Начнём с соотношения

$$\tilde{P}_n^{(s)}(x_1) = f^{(s)}(x_1), \quad s \in 0 : r_1 - 1. \quad (4)$$

Ясно, что $\tilde{P}_n(x_1) = P_{n-1}(x_1) = f(x_1)$. При $r_1 > 1$ имеем по определению

$$\begin{aligned} P_{n-1}^{(s)}(x_1) &= f^{(s)}(x_1), & s \in 0 : r_1 - 1; \\ Q_{n-1}^{(s)}(x_1) &= f^{(s)}(x_1), & s \in 0 : r_1 - 2. \end{aligned} \quad (5)$$

Воспользуемся формулой Лейбница для производной s -го порядка от произведения двух функций, согласно которой при $s \in 1 : r_1 - 1$

$$\begin{aligned} \tilde{P}_n^{(s)}(x) &= \frac{x_m - x}{x_m - x_1} P_{n-1}^{(s)}(x) - \frac{s}{x_m - x_1} P_{n-1}^{(s-1)}(x) + \\ &+ \frac{x - x_1}{x_m - x_1} Q_{n-1}^{(s)}(x) + \frac{s}{x_m - x_1} Q_{n-1}^{(s-1)}(x). \end{aligned} \quad (6)$$

При $x = x_1$ в силу (5) получим

$$\tilde{P}_n^{(s)}(x_1) = P_{n-1}^{(s)}(x_1) = f^{(s)}(x_1), \quad s \in 1 : r_1 - 1.$$

Равенства (4) установлены.

При $k \in 2 : m - 1$ проверка соотношений

$$\tilde{P}_n^{(s)}(x_k) = f^{(s)}(x_k), \quad s \in 0 : r_k - 1, \quad (7)$$

упрощается, поскольку в этом случае

$$P_{n-1}^{(s)}(x_k) = Q_{n-1}^{(s)}(x_k) = f^{(s)}(x_k), \quad s \in 0 : r_k - 1. \quad (8)$$

Согласно определению $\tilde{P}_n(x)$ и (8) при $s = 0$ имеем $\tilde{P}_n(x_k) = f(x_k)$. При $s \in 1 : r_k - 1$ соотношения (7) следуют из (6) и (8).

Остаётся проверить равенства

$$\tilde{P}_n^{(s)}(x_m) = f^{(s)}(x_m), \quad s \in 0 : r_m - 1. \quad (9)$$

При $s = 0$ имеем $\tilde{P}_n(x_m) = Q_{n-1}(x_m) = f(x_m)$. Если $r_m > 1$, то по определению

$$\begin{aligned} P_{n-1}^{(s)}(x_m) &= f^{(s)}(x_m), & s \in 0 : r_m - 2; \\ Q_{n-1}^{(s)}(x_m) &= f^{(s)}(x_m), & s \in 0 : r_m - 1. \end{aligned}$$

Учитывая это и формулу (6), приходим к (9) при $s \in 1 : r_m - 1$.

Предложение доказано. \square

СЛЕДСТВИЕ. При $m \geq 2$ для разделённых разностей справедливо рекуррентное соотношение

$$\begin{aligned} f[x_1^{(r_1)}, \dots, x_m^{(r_m)}] &= \frac{1}{x_m - x_1} \left\{ f[x_1^{(r_1-1)}, x_2^{(r_2)}, \dots, x_m^{(r_m)}] - \right. \\ &\quad \left. - f[x_1^{(r_1)}, \dots, x_{m-1}^{(r_{m-1})}, x_m^{(r_m-1)}] \right\}. \end{aligned} \quad (10)$$

4°. Переобозначим узлы $\underbrace{x_1, \dots, x_1}_{r_1 \text{ раз}}, \dots, \underbrace{x_m, \dots, x_m}_{r_m \text{ раз}}$ следующим образом:

$\xi_1, \xi_2, \dots, \xi_{n+1}$. Тогда формулу (10) при $\xi_{n+1} \neq \xi_1$ (при $m \geq 2$) можно переписать так:

$$f[\xi_1, \xi_2, \dots, \xi_{n+1}] = \frac{f[\xi_2, \dots, \xi_{n+1}] - f[\xi_1, \dots, \xi_n]}{\xi_{n+1} - \xi_1}. \quad (11)$$

Или так

$$f[\xi_2, \dots, \xi_{n+1}] = f[\xi_1, \dots, \xi_n] + (\xi_{n+1} - \xi_1) f[\xi_1, \xi_2, \dots, \xi_{n+1}]. \quad (12)$$

Последняя формула верна и при $\xi_{n+1} = \xi_1$ (при $m = 1$), поскольку в этом случае

$$f[\xi_2, \dots, \xi_{n+1}] = f[\xi_1, \dots, \xi_n] = \frac{f^{(n-1)}(x_1)}{(n-1)!}.$$

ПРЕДЛОЖЕНИЕ 3. Для разделённых разностей справедлив аналог формулы Лейбница:

$$(fg)[\xi_i, \dots, \xi_{i+k}] = \sum_{l=0}^k f[\xi_i, \dots, \xi_{i+l}] g[\xi_{i+l}, \dots, \xi_{i+k}]. \quad (13)$$

Доказательство. При $k = 0$ утверждение очевидно. Сделаем индукционный переход от k к $k + 1$.

При $\xi_{i+k+1} = \xi_i$, когда $\xi_i = \xi_{i+1} = \dots = \xi_{i+k+1}$, согласно классической формуле Лейбница имеем

$$\begin{aligned} (fg)[\xi_i, \dots, \xi_{i+k+1}] &= \frac{(fg)^{(k+1)}(\xi_i)}{(k+1)!} = \frac{1}{(k+1)!} \sum_{l=0}^{k+1} C_{k+1}^l f^{(l)}(\xi_i) g^{(k+1-l)}(\xi_i) = \\ &= \sum_{l=0}^{k+1} \frac{f^{(l)}(\xi_i)}{l!} \frac{g^{(k+1-l)}(\xi_i)}{(k+1-l)!} = \sum_{l=0}^{k+1} f[\xi_i, \dots, \xi_{i+l}] g[\xi_{i+l}, \dots, \xi_{i+k+1}]. \end{aligned}$$

Пусть $\xi_{i+k+1} \neq \xi_i$. Воспользуемся (11) и индукционным предположением. Запишем

$$\begin{aligned} (fg)[\xi_i, \dots, \xi_{i+k+1}] &= \frac{(fg)[\xi_{i+1}, \dots, \xi_{i+k+1}] - (fg)[\xi_i, \dots, \xi_{i+k}]}{\xi_{i+k+1} - \xi_i} = \\ &= (\xi_{i+k+1} - \xi_i)^{-1} \left\{ \sum_{l=1}^{k+1} f[\xi_{i+1}, \dots, \xi_{i+l}] g[\xi_{i+l}, \dots, \xi_{i+k+1}] - \right. \\ &\quad \left. - \sum_{l=0}^k f[\xi_i, \dots, \xi_{i+l}] g[\xi_{i+l}, \dots, \xi_{i+k}] \right\}. \end{aligned} \quad (14)$$

В силу (12)

$$\begin{aligned} f[\xi_{i+1}, \dots, \xi_{i+l}] &= f[\xi_i, \dots, \xi_{i+l-1}] + (\xi_{i+l} - \xi_i) f[\xi_i, \dots, \xi_{i+l}], \\ g[\xi_{i+l}, \dots, \xi_{i+k}] &= g[\xi_{i+l+1}, \dots, \xi_{i+k+1}] - (\xi_{i+k+1} - \xi_{i+l}) g[\xi_{i+l}, \dots, \xi_{i+k+1}]. \end{aligned}$$

Подставляя это в (14), получаем

$$\begin{aligned} (fg)[\xi_i, \dots, \xi_{i+k+1}] &= (\xi_{i+k+1} - \xi_i)^{-1} \left\{ \sum_{l=1}^{k+1} f[\xi_i, \dots, \xi_{i+l-1}] g[\xi_{i+l}, \dots, \xi_{i+k+1}] + \right. \\ &\quad + \sum_{l=1}^{k+1} (\xi_{i+l} - \xi_i) f[\xi_i, \dots, \xi_{i+l}] g[\xi_{i+l}, \dots, \xi_{i+k+1}] + \\ &\quad + \sum_{l=0}^k (\xi_{i+k+1} - \xi_{i+l}) f[\xi_i, \dots, \xi_{i+l}] g[\xi_{i+l}, \dots, \xi_{i+k+1}] - \\ &\quad \left. - \sum_{l=0}^k f[\xi_i, \dots, \xi_{i+l}] g[\xi_{i+l+1}, \dots, \xi_{i+k+1}] \right\}. \end{aligned}$$

В фигурных скобках первая и последняя суммы взаимно уничтожаются. Приходим к равенству

$$\begin{aligned} (fg)[\xi_i, \dots, \xi_{i+k+1}] &= f[\xi_i, \dots, \xi_{i+k+1}]g[\xi_{i+k+1}] + \\ &+ f[\xi_i]g[\xi_i, \dots, \xi_{i+k+1}] + \sum_{l=1}^k f[\xi_i, \dots, \xi_{i+l}]g[\xi_{i+l}, \dots, \xi_{i+k+1}] = \\ &= \sum_{l=0}^{k+1} f[\xi_i, \dots, \xi_{i+l}]g[\xi_{i+l}, \dots, \xi_{i+k+1}]. \end{aligned}$$

Предложение доказано. \square

5°. Формула (13) имеет много приложений. Рассмотрим одно из них.

ПРЕДЛОЖЕНИЕ 4. При натуральном r и $k \in 0 : r$ справедливо тождество

$$(\xi - x)^r [\xi_i, \dots, \xi_{i+k}] = \sum_{\alpha_0 + \dots + \alpha_k = r-k} \prod_{s=0}^k (\xi_{i+s} - x)^{\alpha_s}. \quad (15)$$

Суммирование ведётся по всем целым неотрицательным индексам α_s , таким, что $\alpha_0 + \alpha_1 + \dots + \alpha_k = r - k$.

Доказательство. При $r = 1$ утверждение очевидно (как для $k = 0$, так и для $k = 1$). Сделаем индукционный переход от r к $r + 1$.

Требуется установить, что при $k \in 0 : r + 1$

$$(\xi - x)^{r+1} [\xi_i, \dots, \xi_{i+k}] = \sum_{\alpha_0 + \dots + \alpha_k = r+1-k} \prod_{s=0}^k (\xi_{i+s} - x)^{\alpha_s}. \quad (16)$$

При $k = r + 1$ формула (16) верна (она принимает вид $1 = 1$). Верна она и при $k = 0$. Пусть $k \in 1 : r$. На основании (13) и индукционного предположения запишем

$$\begin{aligned} ((\xi - x)^r (\xi - x)) [\xi_i, \dots, \xi_{i+k}] &= \sum_{l=0}^k (\xi - x)^r [\xi_i, \dots, \xi_{i+l}] (\xi - x) [\xi_{i+l}, \dots, \xi_{i+k}] = \\ &= (\xi - x)^r [\xi_i, \dots, \xi_{i+k-1}] + (\xi - x)^r [\xi_i, \dots, \xi_{i+k}] (\xi_{i+k} - x) = \\ &= \sum_{\alpha_0 + \dots + \alpha_{k-1} = r-k+1} \prod_{s=0}^{k-1} (\xi_{i+s} - x)^{\alpha_s} + \\ &+ \sum_{\alpha_0 + \dots + \alpha_k = r-k} \left(\prod_{s=0}^{k-1} (\xi_{i+s} - x)^{\alpha_s} \right) (\xi_{i+k} - x)^{\alpha_k+1} = \end{aligned}$$

$$= \sum_{\alpha_0 + \dots + \alpha_k = r+1-k} \prod_{s=0}^k (\xi_{i+s} - x)^{\alpha_s}.$$

Последняя сумма составлена из двух сумм, соответствующих $\alpha_k = 0$ и $\alpha_k \geq 1$.

Предложение доказано. \square

Формула (15), в частности, показывает, что разделённая разность k -го порядка по ξ от полинома r -й степени $(\xi - x)^r$ является полиномом $(r - k)$ -й степени от x .

ЛИТЕРАТУРА

1. Березин И. С., Жидков Н. П. *Методы вычислений*. Том 1. Изд. второе. М.: Физматгиз, 1962. 464 с.
2. Мысовских И. П. *Лекции по методам вычислений*. Изд. второе. СПб.: Изд-во СПбГУ, 1998. 472 с.

БИЛИНЕЙНЫЕ ПОВЕРХНОСТИ КУНСА И ПОВЕРХНОСТИ БЕЗЬЕ

Н. В. Чашников

18 ноября 2006 г.

1°. Пусть $D = [0, 1]^2$, $\Gamma = \partial D$. Ставится задача: *построить по вектор-функции $b: \Gamma \rightarrow \mathbb{R}^3$ возможно более простую вектор-функцию $c: D \rightarrow \mathbb{R}^3$, удовлетворяющую условию*

$$c|_{\Gamma} \equiv b. \quad (1)$$

Рассмотрим геометрическую интерпретацию этой задачи. Вектор-функция $c(u, v)$ задаёт поверхность в пространстве \mathbb{R}^3 , состоящую из точек $c(u, v)$ при $u, v \in [0, 1]$. Вектор-функция $b(u, v)$ задаёт 4 кривые,

$$\begin{aligned} &\{b(u, 0) \mid u \in [0, 1]\}, \quad \{b(u, 1) \mid u \in [0, 1]\}, \\ &\{b(0, v) \mid v \in [0, 1]\}, \quad \{b(1, v) \mid v \in [0, 1]\}, \end{aligned}$$

пересекающихся в точках $b(0, 0)$, $b(0, 1)$, $b(1, 0)$, $b(1, 1)$. Условие (1) в таком случае означает, что кривые, задаваемые вектор-функцией b , являются граничными кривыми для поверхности, задаваемой вектор-функцией c .

Определим вектор-функцию $c: D \rightarrow \mathbb{R}^3$ следующим образом:

$$c(u, v) = c_1(u, v) + c_2(u, v) - c_3(u, v), \quad (2)$$

где

$$\begin{aligned} c_1(u, v) &= (1 - u)b(0, v) + u b(1, v), \\ c_2(u, v) &= (1 - v)b(u, 0) + v b(u, 1), \\ c_3(u, v) &= (1 - u)(1 - v)b(0, 0) + (1 - u)v b(0, 1) + \\ &\quad + u(1 - v)b(1, 0) + uv b(1, 1). \end{aligned}$$

ПРЕДЛОЖЕНИЕ 1. Вектор-функция $c(u, v)$ вида (2) удовлетворяет условию (1).

Доказательство. Требуется показать, что для любой пары $(u, v) \in \Gamma$ выполнено $c(u, v) = b(u, v)$. Так как $(u, v) \in \Gamma$, то либо $u = 0$, либо $u = 1$, либо $v = 0$, либо $v = 1$. Если $u = 0$, то

$$\begin{aligned} c(u, v) &= c(0, v) = b(0, v) + (1 - v)b(0, 0) + vb(0, 1) - (1 - v)b(0, 0) - vb(0, 1) = \\ &= b(0, v) = b(u, v), \end{aligned}$$

остальные случаи рассматриваются аналогично. \square

Поверхность, задаваемая вектор-функцией вида (2), называется *билинейной поверхностью Кунса*.

ПРИМЕР. Пусть граничные кривые определены следующим образом (см. рис. 1):

$$\begin{aligned} b(u, 0) &= (u, 0, 0), & b(u, 1) &= (u, 1, u(1 - u)), \\ b(0, v) &= (0, v, 0), & b(1, v) &= (1, v, v(1 - v)). \end{aligned}$$

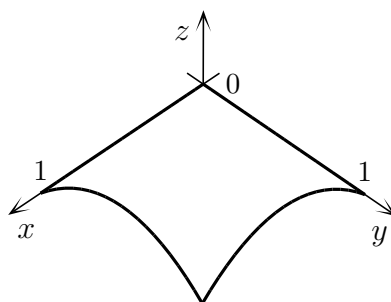


Рис. 1. Граничные кривые.

Вектор-функция c_1 задаёт *линейчатую поверхность*, образованную множеством отрезков с концами $b(0, v)$ и $b(1, v)$ (см. рис. 2), вектор-функция c_2 — линейчатую поверхность, образованную множеством отрезков с концами $b(u, 0)$ и $b(u, 1)$ (см. рис. 3), а вектор-функция c_3 — линейчатую поверхность, образованную множеством отрезков с концами, лежащими на отрезках от $b(0, 0)$ к $b(0, 1)$ и от $b(1, 0)$ к $b(1, 1)$ (см. рис. 4). Поверхность Кунса изображена на рис. 5.

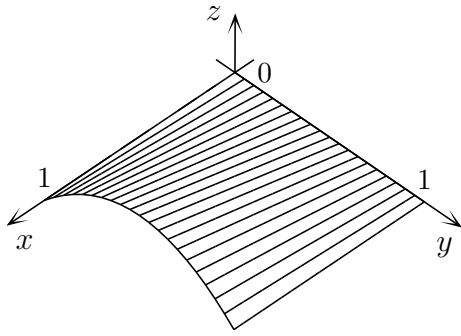
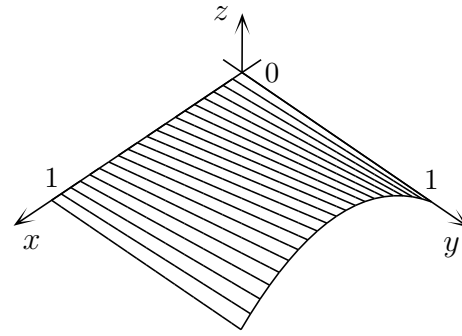
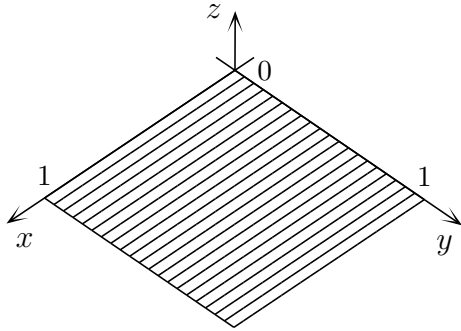
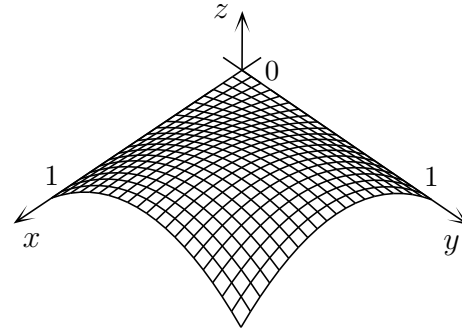
Рис. 2. $c_1(u, v)$.Рис. 3. $c_2(u, v)$.Рис. 4. $c_3(u, v)$.

Рис. 5. Поверхность Кунса.

2°. Мы определили поверхность Кунса в случае, когда областью изменения параметров u и v является квадрат $D = [0, 1]^2$. Аналогичную поверхность можно построить, если заменить D на прямоугольник $E = [u_0, u_1] \times [v_0, v_1]$ с границей $S = \partial E$. Здесь u_0, u_1, v_0 и v_1 — произвольные вещественные числа, для которых выполнены неравенства $u_0 < u_1, v_0 < v_1$. Нетрудно видеть, что в таком случае формула для поверхности Кунса, удовлетворяющая условию $c|_S = b$, будет выглядеть следующим образом:

$$c(u, v) = c_1(u, v) + c_2(u, v) - c_3(u, v), \quad (3)$$

где

$$\begin{aligned} c_1(u, v) &= \frac{u_1 - u}{u_1 - u_0} b(u_0, v) + \frac{u - u_0}{u_1 - u_0} b(u_1, v), \\ c_2(u, v) &= \frac{v_1 - v}{v_1 - v_0} b(u, v_0) + \frac{v - v_0}{v_1 - v_0} b(u, v_1), \\ c_3(u, v) &= \frac{u_1 - u}{u_1 - u_0} \frac{v_1 - v}{v_1 - v_0} b(u_0, v_0) + \frac{u_1 - u}{u_1 - u_0} \frac{v - v_0}{v_1 - v_0} b(u_0, v_1) + \\ &+ \frac{u - u_0}{u_1 - u_0} \frac{v_1 - v}{v_1 - v_0} b(u_1, v_0) + \frac{u - u_0}{u_1 - u_0} \frac{v - v_0}{v_1 - v_0} b(u_1, v_1). \end{aligned}$$

Пусть $E' = [u'_0, u'_1] \times [v'_0, v'_1] \subset E$, $S' = \partial E'$.

ПРЕДЛОЖЕНИЕ 2. Пусть вектор-функция $c(u, v)$ построена по формуле (3) для некоторой функции b , а вектор-функция $e: E' \rightarrow \mathbb{R}^3$ построена по той же формуле, но для граничной функции $d = c|_{S'}$. Тогда $e \equiv c|_{E'}$.

Доказательство. Рассмотрим сначала случай $E = [0, 1]^2$, $E' = [0, u_1] \times [0, 1]$. По формуле (3) для $(u, v) \in E'$ имеем:

$$\begin{aligned} e(u, v) = & \frac{u_1 - u}{u_1} c(0, v) + \frac{u}{u_1} c(u_1, v) + (1 - v) c(u, 0) + v c(u, 1) - \\ & - \frac{u_1 - u}{u_1} (1 - v) c(0, 0) - \frac{u_1 - u}{u_1} v c(0, 1) - \\ & - \frac{u}{u_1} (1 - v) c(u_1, 0) - \frac{u}{u_1} v c(u_1, 1). \end{aligned}$$

Подставим значение $c(u_1, v)$ из формулы (2). Учитывая, что $c|_{\Gamma} \equiv b$, получаем:

$$\begin{aligned} e(u, v) = & \frac{u_1 - u}{u_1} b(0, v) + \frac{u}{u_1} \left[(1 - u_1) b(0, v) + u_1 b(1, v) + (1 - v) b(u_1, 0) + \right. \\ & + v b(u_1, 1) - (1 - u_1)(1 - v) b(0, 0) - (1 - u_1) v b(0, 1) - \\ & - u_1 (1 - v) b(1, 0) - u_1 v b(1, 1) \left. \right] + (1 - v) b(u, 0) + v b(u, 1) - \\ & - \frac{u_1 - u}{u_1} (1 - v) b(0, 0) - \frac{u_1 - u}{u_1} v b(0, 1) - \\ & - \frac{u}{u_1} (1 - v) b(u_1, 0) - \frac{u}{u_1} v b(u_1, 1). \end{aligned}$$

После раскрытия скобок придём к формуле

$$\begin{aligned} e(u, v) = & (1 - u) b(0, v) + u b(1, v) - (1 - u)(1 - v) b(0, 0) - (1 - u) v b(0, 1) - \\ & - u (1 - v) b(1, 0) - u v b(0, 0) + (1 - v) b(u, 0) + v b(u, 1) = \\ = & c(u, v). \end{aligned}$$

Итак, для случая $E = [0, 1]^2$, $E' = [0, u_1] \times [0, 1]$ утверждение доказано. При помощи замены переменных $(u, v) \mapsto (1 - u, v)$ получим, что оно выполнено для случая $E = [0, 1]^2$, $E' = [1 - u_1, 1] \times [0, 1]$. Используя перестановку переменных $(u, v) \mapsto (v, u)$, установим, что утверждение выполнено для случаев $E = [0, 1]^2$, $E' = [0, 1] \times [0, v_1]$ и $E = [0, 1]^2$, $E' = [0, 1] \times [v_0, 1]$. Наконец, при помощи линейной замены переменных получим, что утверждение верно для случаев, когда $E = [u_0, u_1] \times [v_0, v_1]$, а $E' = [u'_0, u_1] \times [v_0, v_1]$, либо $E' = [u_0, u'_1] \times [v_0, v_1]$, либо $E' = [u_0, u_1] \times [v'_0, v_1]$, либо $E' = [u_0, u_1] \times [v_0, v'_1]$.

Рассмотрим теперь общий случай: $E = [u_0, u_1] \times [v_0, v_1]$, $E' = [u'_0, u'_1] \times [v'_0, v'_1]$. Пусть вектор-функция $c: E \rightarrow \mathbb{R}^3$ построена по формуле (3) для некоторой

границной функции $b: \partial E \rightarrow \mathbb{R}^3$. Пусть $E_1 = [u_0, u'_1] \times [v_0, v_1]$. Построим вектор-функцию e_1 по формуле (3) для граничной функции $c|_{\partial E_1}$. Доказано, что $e_1 \equiv c|_{E_1}$. Пусть $E_2 = [u'_0, u'_1] \times [v_0, v_1]$. Построим вектор-функцию e_2 по формуле (3) для граничной функции $e_1|_{\partial E_2}$. Утверждение для множеств E_1, E_2 уже доказано, поэтому $e_2 \equiv e_1|_{E_2} \equiv c|_{E_2}$. Далее рассмотрим множество $E_3 = [u'_0, u'_1] \times [v_0, v'_1]$ и построим вектор-функцию e_3 по формуле (3) для граничной функции $e_2|_{\partial E_3}$. Тогда будет выполнено $e_3 \equiv e_2|_{E_3} \equiv c|_{E_3}$. И наконец, рассмотрим множество $[u'_0, u'_1] \times [v'_0, v'_1] = E'$ и построим вектор-функцию $e(u, v)$ по формуле (3) для граничной функции $e_3|_{\partial E'} \equiv c|_{\partial E'} \equiv d$. Тогда будет выполнено $e \equiv e_3|_{E'} \equiv c|_{E'}$, что и требовалось доказать. \square

З а м е ч а н и е. Доказанное предложение имеет наглядную геометрическую интерпретацию. Пусть для некоторых граничных кривых построена поверхность Кунса. Возьмём прямоугольную область параметров, являющуюся подмножеством исходной, и рассмотрим кривые на поверхности Кунса, соответствующие значениям параметров на границе этой области. По этим кривым можно построить новую поверхность Кунса. По доказанному предложению, эта поверхность будет являться подмножеством исходной поверхности Кунса.

3°. Существует бесконечное множество поверхностей, проходящих через заданные граничные кривые. Поверхность Кунса выделяется из этого множества тем, что она обладает свойством *минимизации искривления*.

Пусть заданы граничные кривые $b: \Gamma \rightarrow \mathbb{R}^3$, причём

$$b(0, v), b(1, v), b(u, 0), b(u, 1) \in C^1([0, 1]). \quad (4)$$

Обозначим

$$\Phi = \left\{ a: D \rightarrow \mathbb{R}^3 \mid a \in C^1(D), a_{uv}, a_{vu} \in C(D), a|_{\Gamma} \equiv b \right\}.$$

Заметим, что если $a_{uv}, a_{vu} \in C(D)$, то $a_{uv} \equiv a_{vu}$. Положим

$$G(a) = \iint_D \|a_{uv}(u, v)\|^2 du dv, \quad a \in \Phi,$$

и рассмотрим задачу минимизации функционала G на множестве Φ :

$$G(a) \longrightarrow \min, \quad a \in \Phi. \quad (5)$$

Будем решать эту задачу отдельно для каждой координаты.

Пусть $a(u, v) = (x(u, v), y(u, v), z(u, v))$, $b(u, v) = (x^0(u, v), y^0(u, v), z^0(u, v))$. Обозначим

$$\Omega = \left\{ x: D \rightarrow \mathbb{R} \mid x \in C^1(D), x_{uv}, x_{vu} \in C(D), x|_{\Gamma} \equiv x^0 \right\},$$

$$F(x) = \iint_D [x_{uv}(u, v)]^2 du dv, \quad x \in \Omega.$$

Тогда $G(a) = F(x) + F(y) + F(z)$, а условие $a \in \Phi$ разбивается на условие $x \in \Omega$ и аналогичные независимые условия для y и z , поэтому достаточно решить задачу вида

$$F(x) \longrightarrow \min, \quad x \in \Omega, \quad (6)$$

для каждой координаты в отдельности.

Введём множество допустимых вариаций

$$\Omega_0 = \left\{ h: D \rightarrow \mathbb{R} \mid h \in C^1(D), h_{uv}, h_{vu} \in C(D), h|_{\Gamma} \equiv 0 \right\}.$$

Тогда $x + \alpha h \in \Omega$ для всех $x \in \Omega$, $h \in \Omega_0$, $\alpha \in \mathbb{R}$, при этом

$$F(x + \alpha h) = F(x) + 2\alpha l(x, h) + \alpha^2 d(h),$$

где

$$l(x, h) = \iint_D x_{uv} h_{uv} du dv, \quad d(h) = \iint_D h_{uv}^2 du dv.$$

Заметим, что $d(h) \geq 0 \quad \forall h \in \Omega_0$.

ЛЕММА 1. *Функция $x_* \in \Omega$ является решением задачи (6) тогда и только тогда, когда*

$$l(x_*, h) = 0 \quad \forall h \in \Omega_0.$$

Доказательство. Необходимость.

Пусть $x_* \in \Omega$ — решение (6). Тогда для $\forall \alpha \in \mathbb{R}, \alpha > 0, h \in \Omega_0$ выполнено

$$0 \leq \frac{1}{\alpha} (F(x_* + \alpha h) - F(x_*)) = 2l(x_*, h) + \alpha d(h)$$

Устремив α к нулю, получим $l(x_*, h) \geq 0$. Но $-h \in \Omega_0$, поэтому аналогичным образом получаем $l(x_*, -h) \geq 0$, значит $l(x_*, h) = -l(x_*, -h) \leq 0$, то есть $l(x_*, h) = 0$.

Достаточность. Пусть $l(x_*, h) = 0 \quad \forall h \in \Omega_0$. Тогда для $\forall x \in \Omega$ будем иметь $h = x - x_* \in \Omega_0$, поэтому

$$F(x) = F(x_* + h) = F(x_*) + 2l(x_*, h) + d(h) = F(x_*) + d(h) \geq F(x_*).$$

Лемма доказана. □

Определим функцию $c^x: D \rightarrow \mathbb{R}$ по формуле, аналогичной (2):

$$\begin{aligned} c^x(u, v) = & (1-u)x^0(0, v) + ux^0(1, v) + (1-v)x^0(u, 0) + vx^0(u, 1) - \\ & - (1-u)(1-v)x^0(0, 0) - (1-u)v x^0(0, 1) - \\ & - u(1-v)x^0(1, 0) - uv x^0(1, 1). \end{aligned} \quad (7)$$

Ясно, что $c^x|_\Gamma \equiv x^0$. Кроме того, из (4) следует, что

$$x^0(0, v), x^0(1, v), x^0(u, 0), x^0(u, 1) \in C^1([0, 1]),$$

поэтому

$$c_{uv}^x, c_{vu}^x \in C(D).$$

ЛЕММА 2.

$$\iint_D c_{uv}^x h_{uv} du dv = 0 \quad \forall h \in \Omega_0.$$

Доказательство. Из (7) видно, что $c_{uv}^x(u, v) = f(u) + g(v)$, где f, g — некоторые функции класса $C([0, 1])$. Поэтому

$$\begin{aligned} \iint_D c_{uv}^x h_{uv} du dv &= \iint_D (f(u) + g(v)) h_{uv}(u, v) du dv = \\ &= \int_0^1 f(u) \left(\int_0^1 h_{uv}(u, v) dv \right) du + \int_0^1 g(v) \left(\int_0^1 h_{uv}(u, v) du \right) dv = \\ &= \int_0^1 f(u) (h_u(u, 1) - h_u(u, 0)) du + \int_0^1 g(v) (h_v(1, v) - h_v(0, v)) dv = \\ &= 0, \end{aligned}$$

так как $h(u, 1) \equiv 0$, $h(u, 0) \equiv 0$, $h(1, v) \equiv 0$ и $h(0, v) \equiv 0$. □

ЛЕММА 3. Пусть $f \in C^1(D)$ и $f_{uv}(u, v) \equiv 0$. Тогда

$$f(u, v) = f(u, 0) + f(0, v) - f(0, 0) \quad \forall u, v \in [0, 1].$$

Доказательство. Используя формулу Ньютона-Лейбница, получаем

$$f_u(u, v) - f_u(u, 0) = \int_0^v f_{uv}(u, w) dw = 0.$$

Поэтому

$$f(u, v) - f(0, v) = \int_0^u f_u(t, v) dt = \int_0^u f_u(t, 0) dt = f(u, 0) - f(0, 0),$$

что и требовалось. □

ЛЕММА 4. Пусть $x \in \Omega$ и

$$\iint_D x_{uv} h_{uv} du dv = 0 \quad \forall h \in \Omega_0.$$

Тогда $x \equiv c^x$.

Доказательство. Обозначим $h = x - c^x$. Так как $(x - c^x)|_\Gamma \equiv 0$, то $h \in \Omega_0$.

Используя лемму 2, получаем

$$\begin{aligned} \iint_D h_{uv}^2 du dv &= \iint_D (x_{uv} - c_{uv}^x) h_{uv} du dv = \\ &= \iint_D x_{uv} h_{uv} du dv - \iint_D c_{uv}^x h_{uv} du dv = 0. \end{aligned}$$

Значит, $h_{uv} \equiv 0$. По лемме 3

$$h(u, v) = h(u, 0) + h(0, v) - h(0, 0) \quad \forall u, v \in [0, 1].$$

Условие $h \in \Omega_0$ приводит к тождеству $h \equiv 0$, которое равносильно требуемому. \square

ПРЕДЛОЖЕНИЕ 3. Пусть дана вектор-функция $b: \Gamma \rightarrow \mathbb{R}^3$, удовлетворяющая условиям (4). Тогда единственным решением задачи (5) является вектор-функция $c(u, v)$, построенная по формуле (2).

Доказательство. Из лемм 1, 2 и 4 следует, что единственным решением задачи (6) является функция вида (7). Решая задачу (6) для трёх координатных функций, получаем по формуле (7) функции c^x , c^y и c^z . Таким образом, единственным решением задачи (5) будет вектор-функция

$$c(u, v) = (c^x(u, v), c^y(u, v), c^z(u, v)).$$

Но, как нетрудно видеть, эта вектор-функция совпадает с вектор-функцией, получаемой по формуле (2). \square

4°. Перейдём теперь к связи поверхностей Кунса с поверхностями Безье. Начнём с необходимых определений.

Базисным полиномом Бернштейна называется полином

$$p_{nk}(x) = C_n^k x^k (1 - x)^{n-k},$$

где $k = 0, 1, \dots, n$.

Кривой Безье, построенной по полюсам $Y_0, \dots, Y_n \in \mathbb{R}^3$, называется кривая, определяемая вектор-функцией

$$B(x) = \sum_{k=0}^n p_{nk}(x) Y_k, \quad x \in [0, 1].$$

Поверхностью Безье, построенной по полюсам $\{Z_{ij}\} \subset \mathbb{R}^3$ ($i = 0, \dots, m$, $j = 0, \dots, n$), называется поверхность, задаваемая вектор-функцией

$$C(u, v) = \sum_{i=0}^m \sum_{j=0}^n p_{mi}(u) p_{nj}(v) Z_{ij}, \quad u \in [0, 1], v \in [0, 1].$$

Нам также потребуются следующие свойства базисных полиномов Бернштейна:

$$\sum_{k=0}^n p_{nk}(x) = 1 \quad \forall x \in \mathbb{R}, \quad (8)$$

$$\sum_{k=0}^n \frac{k}{n} p_{nk}(x) = x \quad \forall x \in \mathbb{R}. \quad (9)$$

Рассмотрим задачу построения билинейной поверхности Кунса в случае, когда граничные кривые являются кривыми Безье, причём противоположные кривые имеют одинаковое количество полюсов. Пусть вектор-функция $b: \Gamma \rightarrow \mathbb{R}^3$ задаёт граничные кривые, причём кривой $b(u, 0)$ соответствуют полюса $\{Y_{i0}\}_{i=0}^m$, кривой $b(u, 1)$ — полюса $\{Y_{in}\}_{i=0}^m$, кривой $b(0, v)$ — полюса $\{Y_{0j}\}_{j=0}^n$, а кривой $b(1, v)$ — полюса $\{Y_{mj}\}_{j=0}^n$. Обозначим через $c(u, v)$ вектор-функцию (2), определяющую поверхность Кунса.

ПРЕДЛОЖЕНИЕ 4. Билинейная поверхность Кунса, задаваемая вектор-функцией $c(u, v)$, совпадает с поверхностью Безье, построенной по полюсам $\{Z_{ij} \mid i \in 0 : m, j \in 0 : n\}$, где

$$Z_{ij} = \left(1 - \frac{i}{m}\right) Y_{0j} + \frac{i}{m} Y_{mj} + \left(1 - \frac{j}{n}\right) Y_{i0} + \frac{j}{n} Y_{in} - \\ - \left(1 - \frac{i}{m}\right) \left(1 - \frac{j}{n}\right) Y_{00} - \left(1 - \frac{i}{m}\right) \frac{j}{n} Y_{0n} - \frac{i}{m} \left(1 - \frac{j}{n}\right) Y_{m0} - \frac{i}{m} \frac{j}{n} Y_{mn}.$$

Доказательство. Пусть $C: D \rightarrow \mathbb{R}^3$ — поверхность Безье, построенная по полюсам $\{Z_{ij}\}$:

$$C(u, v) = \sum_{i=0}^m \sum_{j=0}^n p_{mi}(u) p_{nj}(v) Z_{ij} = \\ = \left(\sum_{i=0}^m \left(1 - \frac{i}{m}\right) p_{mi}(u) \right) \left(\sum_{j=0}^n p_{nj}(v) Y_{0j} \right) + \left(\sum_{i=0}^m \frac{i}{m} p_{mi}(u) \right) \left(\sum_{j=0}^n p_{nj}(v) Y_{mj} \right) +$$

$$\begin{aligned}
& + \left(\sum_{j=0}^n \left(1 - \frac{j}{n} \right) p_{nj}(v) \right) \left(\sum_{i=0}^m p_{mi}(u) Y_{i0} \right) + \left(\sum_{j=0}^n \frac{j}{n} p_{nj}(v) \right) \left(\sum_{i=0}^m p_{mi}(u) Y_{in} \right) - \\
& - \left(\sum_{i=0}^m \left(1 - \frac{i}{m} \right) p_{mi}(u) \right) \left(\sum_{j=0}^n \left(1 - \frac{j}{n} \right) p_{nj}(v) \right) Y_{00} - \\
& - \left(\sum_{i=0}^m \left(1 - \frac{i}{m} \right) p_{mi}(u) \right) \left(\sum_{j=0}^n \frac{j}{n} p_{nj}(v) \right) Y_{0n} - \\
& - \left(\sum_{i=0}^m \frac{i}{m} p_{mi}(u) \right) \left(\sum_{j=0}^n \left(1 - \frac{j}{n} \right) p_{nj}(v) \right) Y_{m0} - \\
& - \left(\sum_{i=0}^m \frac{i}{m} p_{mi}(u) \right) \left(\sum_{j=0}^n \frac{j}{n} p_{nj}(v) \right) Y_{mn}.
\end{aligned}$$

Рассмотрим первое слагаемое в правой части этого равенства. Используя (8) и (9), получаем

$$\sum_{i=0}^m \left(1 - \frac{i}{m} \right) p_{mi}(u) = \sum_{i=0}^m p_{mi}(u) - \sum_{i=0}^m \frac{i}{m} p_{mi}(u) = 1 - u,$$

а так как $\{Y_{0j}\}$ являются полюсами для кривой Безье $b(0, v)$, то

$$\sum_{j=0}^n p_{nj}(v) Y_{0j} = b(0, v),$$

то есть первое слагаемое равно $(1 - u) b(0, v)$. Аналогичным образом преобразуются остальные слагаемые. Если учесть, что

$$Y_{00} = b(0, 0), \quad Y_{0n} = b(0, 1), \quad Y_{m0} = b(1, 0), \quad Y_{mn} = b(1, 1),$$

то окончательно получим

$$\begin{aligned}
C(u, v) &= (1 - u) b(0, v) + u b(1, v) + (1 - v) b(u, 0) + v b(u, 1) - \\
&- (1 - u)(1 - v) b(0, 0) - (1 - u) v b(0, 1) - u(1 - v) b(1, 0) - u v b(1, 1) = c(u, v),
\end{aligned}$$

что и требовалось. \square

ЛИТЕРАТУРА

1. G. Farin. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.

ОСНОВНЫЕ ПОНЯТИЯ ТЕОРИИ ПОЛЯРНЫХ ФОРМ

В. Н. Малозёмов

2 декабря 2006 г.

1°. Напомним [1, 2], что *полярной формой* алгебраического полинома от одной переменной вида

$$P(x) = \sum_{k=0}^n C_n^k a_k x^k \quad (1)$$

называется выражение

$$p(x_1, \dots, x_n) = \sum_{k=0}^n a_k \sigma_k(x_1, \dots, x_n), \quad (2)$$

где $\sigma_k(x_1, \dots, x_n)$ — основные симметрические полиномы от n переменных:

$$\begin{aligned} \sigma_0(x_1, \dots, x_n) &\equiv 1, \\ \sigma_k(x_1, \dots, x_n) &= \sum_{I_k \subset N} \prod_{i \in I_k} x_i, \quad k = 1, \dots, n. \end{aligned} \quad (3)$$

Суммирование в правой части (3) ведётся по всем подмножествам I_k множества $N = \{1, \dots, n\}$, содержащим ровно k элементов. В частности,

$$\begin{aligned} \sigma_1(x_1, \dots, x_n) &= x_1 + x_2 + \dots + x_n, \\ \sigma_n(x_1, \dots, x_n) &= x_1 x_2 \dots x_n. \end{aligned}$$

Очевидно, что полярная форма (2) является симметричной функцией своих аргументов. С порождающим полиномом (1) её связывает соотношение

$$p(x, \dots, x) = P(x). \quad (4)$$

Значение полярной формы при конкретных значениях аргументов x_1, \dots, x_n называется *полюсом* полинома $P(x)$.

2°. Покажем, как эффективно вычислять полюсы.

Зафиксируем x_1, \dots, x_n и построим треугольный массив $\{a_k^{(i)}\}$, $k \in 0 : n-i$, $i \in 0 : n$, по правилу

$$\begin{aligned} a_k^{(i)} &= a_k^{(i-1)} + x_{n-i+1} a_{k+1}^{(i-1)}, & k \in 0 : n-i, & i \in 1 : n; \\ a_k^{(0)} &= a_k, & k \in 0 : n. \end{aligned}$$

ПРЕДЛОЖЕНИЕ 1. *Справедливо равенство*

$$p(x_1, \dots, x_n) = a_0^{(n)}. \quad (5)$$

Доказательство. При $n = 1$ утверждение очевидно. Пусть $n \geq 2$. Из определения основных симметрических полиномов следует, что они удовлетворяют рекуррентному соотношению

$$\sigma_k(x_1, \dots, x_n) = \sigma_k(x_1, \dots, x_{n-1}) + x_n \sigma_{k-1}(x_1, \dots, x_{n-1}), \quad k \in 1 : n-1. \quad (6)$$

Согласно (6)

$$\begin{aligned} p(x_1, \dots, x_n) &= a_0 + \sum_{k=1}^{n-1} a_k [\sigma_k(x_1, \dots, x_{n-1}) + x_n \sigma_{k-1}(x_1, \dots, x_{n-1})] + \\ &+ a_n x_1 \cdots x_n = \sum_{k=0}^{n-1} a_k \sigma_k(x_1, \dots, x_{n-1}) + x_n \sum_{k=0}^{n-1} a_{k+1} \sigma_k(x_1, \dots, x_{n-1}) = \\ &= \sum_{k=0}^{n-1} (a_k^{(0)} + x_n a_{k+1}^{(0)}) \sigma_k(x_1, \dots, x_{n-1}) = \sum_{k=0}^{n-1} a_k^{(1)} \sigma_k(x_1, \dots, x_{n-1}). \end{aligned}$$

Продолжив аналогично, получим

$$p(x_1, \dots, x_n) = \sum_{k=0}^1 a_k^{(n-1)} \sigma_k(x_1) = a_0^{(n-1)} + x_1 a_1^{(n-1)} = a_0^{(n)}.$$

Предложение доказано. \square

3°. Важнейшим свойством полярной формы является её мультиаффинность.

ПРЕДЛОЖЕНИЕ 2. *При любом $j \in 1 : n$*

$$\begin{aligned} p(x_1, \dots, \alpha x'_j + \beta x''_j, \dots, x_n) &= \alpha p(x_1, \dots, x'_j, \dots, x_n) + \\ &+ \beta p(x_1, \dots, x''_j, \dots, x_n), \end{aligned} \quad (7)$$

если $\alpha + \beta = 1$.

Доказательство. При $n = 1$ имеем $p(x_1) = a_0 + a_1 x_1$. Взяв $\alpha + \beta = 1$, получим

$$p(\alpha x'_1 + \beta x''_1) = (\alpha + \beta) a_0 + a_1 (\alpha x'_1 + \beta x''_1) = \alpha p(x'_1) + \beta p(x''_1),$$

что соответствует (7).

Пусть $n \geq 2$. В силу симметричности полярной формы достаточно рассмотреть случай $j = n$. Если же учесть формулу (2), то дело сводится к проверке соотношения

$$\begin{aligned} \sigma_k(x_1, \dots, x_{n-1}, \alpha x'_n + \beta x''_n) &= \alpha \sigma_k(x_1, \dots, x_{n-1}, x'_n) + \\ &+ \beta \sigma_k(x_1, \dots, x_{n-1}, x''_n), \quad k \in 0 : n, \quad \alpha + \beta = 1. \end{aligned} \quad (8)$$

При $k = 0$ и $k = n$ равенство (8) очевидно. При $k \in 1 : n - 1$ воспользуемся формулой (6), согласно которой

$$\begin{aligned} \sigma_k(x_1, \dots, x_{n-1}, \alpha x'_n + \beta x''_n) &= (\alpha + \beta) \sigma_k(x_1, \dots, x_{n-1}) + \\ &+ (\alpha x'_n + \beta x''_n) \sigma_{k-1}(x_1, \dots, x_{n-1}) = \alpha \sigma_k(x_1, \dots, x_{n-1}, x'_n) + \\ &+ \beta \sigma_k(x_1, \dots, x_{n-1}, x''_n). \end{aligned}$$

Предложение доказано. □

4°. Зафиксируем $2n$ точек на вещественной оси

$$x_1 \leq x_2 \leq \dots \leq x_n < x_{n+1} \leq \dots \leq x_{2n} \quad (9)$$

и введём $n + 1$ полюс полинома $P(x)$ вида (1):

$$p_{i,i+1,\dots,i+n-1} = p(x_i, x_{i+1}, \dots, x_{i+n-1}), \quad i = 1, \dots, n + 1. \quad (10)$$

Такая система полюсов называется *примитивной* [1, с. 143]. Покажем, как по полюсам (10) восстановить значение $P(x)$ в любой точке $x = x_*$.

Вычисления проводятся по следующей схеме:

$$\begin{array}{ccccccc} p_{1,2,\dots,n} & & & & & & \\ & p_{2,\dots,n,*} & & & & & \\ p_{2,3,\dots,n+1} & & p_{3,\dots,*,*} & & & & \\ & p_{3,\dots,*,n+1} & & \ddots & & & \\ p_{3,4,\dots,n+2} & & & & p_{n,*,\dots,*} & & \\ \dots & & & & & p_{*,*,\dots,*} & \\ & p_{n-1,\dots,2n-2} & & & p_{*,\dots,*,n+1} & & \\ & & p_{n,*,\dots,2n-2} & & \ddots & & \\ p_{n,\dots,2n-1} & & & p_{*,*,\dots,2n-2} & & & \\ & p_{*,n+1,\dots,2n-1} & & & & & \\ p_{n+1,\dots,2n} & & & & & & \end{array}$$

В первом столбце стоят исходные данные. Элементы второго столбца вычисляются по формуле

$$p_{i+1,\dots,n,*,n+1,\dots,n+i-1} = [(x_{n+i} - x_*)p_{i,i+1,\dots,n+i-1} + (x_* - x_i)p_{i+1,\dots,n+i-1,n+i}]/(x_{n+i} - x_i), \quad i = 1, \dots, n. \quad (11)$$

Справедливость (11) следует из симметричности и мультиаффинности полярной формы. Действительно,

$$\begin{aligned} & \frac{(x_{n+i} - x_*)p(x_{i+1}, \dots, x_{n+i-1}, x_i) + (x_* - x_i)p(x_{i+1}, \dots, x_{n+i-1}, x_{n+i})}{x_{n+i} - x_i} = \\ & = p\left(x_{i+1}, \dots, x_{n+i-1}, \frac{(x_{n+i} - x_*)x_i + (x_* - x_i)x_{n+i}}{x_{n+i} - x_i}\right) = \\ & = p(x_{i+1}, \dots, x_{n+i-1}, x_*) = p(x_{i+1}, \dots, x_n, x_*, x_{n+1}, \dots, x_{n+i-1}). \end{aligned}$$

Формула (11) определяет *процедуру включения узла*.

Остальные столбцы треугольной таблицы заполняются аналогично. Элементы $(k+1)$ -го столбца вычисляются так:

$$\begin{aligned} p_{i+k,\dots,n,\underbrace{*,\dots,*}_{k \text{ раз}},n+1,\dots,n+i-1} &= [(x_{n+i} - x_*)p_{i+k-1,\dots,n,\underbrace{*,\dots,*}_{(k-1) \text{ раз}},n+1,\dots,n+i-1} + \\ &+ (x_* - x_{i+k-1})p_{i+k,\dots,n,\underbrace{*,\dots,*}_{(k-1) \text{ раз}},n+1,\dots,n+i}]/(x_{n+i} - x_{i+k-1}), \\ & i = 1, \dots, n - k + 1; \quad k = 1, 2, \dots, n. \end{aligned}$$

Поскольку $x_n < x_{n+1}$, то все вычисления по указанным формулам выполнимы. В результате согласно (4) получим $p_{*,*,\dots,*} = P(x_*)$.

5°. Зафиксируем числа y_1, y_2, \dots, y_{n+1} и рассмотрим задачу *интерполирования по полюсам*: найти полином $P(x)$ вида (1), такой, что

$$p(x_i, x_{i+1}, \dots, x_{i+n-1}) = y_i, \quad i = 1, 2, \dots, n+1. \quad (12)$$

ПРЕДЛОЖЕНИЕ 3. При выполнении условия (9) интерполяционная задача (12) имеет решение при любых правых частях и это решение единственно.

Доказательство. Напомним, что

$$p(x_1, \dots, x_n) = \sum_{k=0}^n a_k \sigma_k(x_1, \dots, x_n).$$

Это значит, что (12) есть система линейных уравнений относительно коэффициентов $\{a_k\}$ полинома $P(x)$.

Рассмотрим однородную систему

$$p(x_i, x_{i+1}, \dots, x_{i+n-1}) = 0, \quad i = 1, \dots, n+1, \quad (13)$$

и покажем, что она имеет только нулевое решение. Отсюда будет следовать требуемое заключение.

Возьмём любое решение системы (13). Соответствующий полином вида (1) обозначим $P_0(x)$. По условию его примитивные полюсы $p_0(x_i, \dots, x_{i+n-1})$ при $i \in 1 : n+1$ равны нулю. Применяв процедуру включения узла получим, что $P_0(x) \equiv 0$. Но тогда и все коэффициенты полинома $P_0(x)$ равны нулю.

Предложение доказано. \square

6°. Условие (9), очевидно, выполняется при

$$x_1 = \dots = x_n = 0, \quad x_{n+1} = \dots = x_{2n} = 1. \quad (14)$$

ПРЕДЛОЖЕНИЕ 4. В случае (14) единственным решением интерполяционной задачи (12) является полином

$$P(x) = \sum_{i=0}^n y_{i+1} C_n^i x^i (1-x)^{n-i}.$$

Доказательство. В данном случае

$$\begin{aligned} \sigma_k(x_i, \dots, x_n, x_{n+1}, \dots, x_{n+i-1}) &= \sigma_k(0, \dots, 0, \underbrace{1, \dots, 1}_{(i-1) \text{ раз}}) = \\ &= \begin{cases} C_{i-1}^k & \text{при } k \in 0 : i-1, \\ 0 & \text{при } k \in i : n, \end{cases} \end{aligned}$$

поэтому система уравнений (12) примет вид

$$\sum_{k=0}^{i-1} C_{i-1}^k a_k = y_i, \quad i \in 1 : n+1. \quad (15)$$

Как известно [3, с. 60], ей удовлетворяют числа

$$a_k = (\Delta^k y)_1 = \sum_{i=0}^k (-1)^{k-i} C_k^i y_{i+1}, \quad k \in 0 : n$$

(к этому факту мы ещё вернёмся). Для интерполяционного по полюсам полинома получаем формулу

$$\begin{aligned} P(x) &= \sum_{k=0}^n C_n^k (\Delta^k y)_1 x^k = \sum_{k=0}^n C_n^k x^k \sum_{i=0}^k (-1)^{k-i} C_k^i y_{i+1} = \\ &= \sum_{i=0}^n y_{i+1} \sum_{k=i}^n (-1)^{k-i} C_n^k C_k^i x^k. \end{aligned}$$

Остаётся проверить, что

$$\sum_{k=i}^n (-1)^{k-i} C_n^k C_k^i x^k = C_n^i x^i (1-x)^{n-i}, \quad i \in 0 : n. \quad (16)$$

Но это очевидно, поскольку $C_n^k C_k^i = C_n^i C_{n-i}^{k-i}$.

Вернёмся к системе уравнений (15) и покажем, что

$$\sum_{k=0}^i C_i^k (\Delta^k y)_1 = y_{i+1}, \quad i \in 0 : n. \quad (17)$$

При $i = 0$ равенство (17) тривиально. Пусть $i \in 1 : n$. Имеем

$$\begin{aligned} \sum_{k=0}^i C_i^k (\Delta^k y)_1 &= \sum_{k=0}^{i-1} C_i^k \sum_{l=0}^k (-1)^{k-l} C_k^l y_{l+1} + \sum_{l=0}^i (-1)^{i-l} C_i^l y_{l+1} = \\ &= \sum_{l=0}^{i-1} y_{l+1} \sum_{k=l}^{i-1} (-1)^{k-l} C_i^k C_k^l + \sum_{l=0}^{i-1} (-1)^{i-l} C_i^l y_{l+1} + y_{i+1} = \\ &= y_{i+1} + \sum_{l=0}^{i-1} y_{l+1} \left\{ \sum_{k=l}^i (-1)^{k-l} C_i^k C_k^l \right\}. \end{aligned}$$

Выражение в фигурных скобках при $l \in 0 : i - 1$ равно нулю. Это следует из (16) при $x = 1$. Равенство (17), а с ним и предложение, доказаны. \square

По существу установлено, что при выполнении условия (14) интерполяционным по полюсам полиномом является полином в форме Бернштейна, коэффициентами которого служат сами полюсы y_1, y_2, \dots, y_{n+1} .

ЛИТЕРАТУРА

1. Кастельжо П. *Теория полюсов* / В кн.: Математика и САПР. Том 1. Пер. с фр. М.: Мир, 1988. С. 130–200.
2. Малозёмов В. Н., Сергеев А. Н. *Аналитические основы теории полярных форм* // Алгебра и анализ. 1998. Т. 10. Вып. 6. С. 156–185.
3. Мысовских И. П. *Лекции по методам вычислений*. Изд. 2-е. СПб.: Изд-во СПбГУ, 1998. 472 с.

ФАКТОРИЗАЦИЯ БОЛЬШИХ ЦЕЛЫХ ЧИСЕЛ И КРИПТОГРАФИЯ

И. В. Агафонова

12 декабря 2006 г.

1. Односторонние функции

В криптографии «с открытым ключом» (асимметрические криптосистемы) центральными являются понятия:

- односторонняя функция (однонаправленная);
- односторонняя функция с секретом.

Функция $f: X \rightarrow Y$ **односторонняя**, если существует эффективный алгоритм для её вычисления при любом X , но не существует эффективного алгоритма для вычисления обратной к ней функции. (Под эффективным алгоритмом понимается полиномиальный, в отличие от экспоненциального.) Функция называется **односторонней с секретом** (потайным ходом, лазейкой, *trap-door*), если при наличии некоторой дополнительной информации (ключа) возможно её эффективное обращение. Односторонними (на современном уровне наших знаний) являются функции:

- 1) Умножение целых чисел

$$f(x, y) = x y$$

- 2) Возведение заданного числа в степень по данному модулю

$$f_{n,a}(m) = \langle a^m \rangle_n$$

(Эта запись означает вычет a^m по модулю n)

- 3) Возведение числа в заданную степень по данному модулю

$$f_{n,m}(a) = \langle a^m \rangle_n$$

Нахождение функций, обратных к данным, приводит к задачам:

- 1) Факторизация целого числа: $f = xy$, найти x и y , зная f .
- 2) Дискретное логарифмирование: пусть $f = \langle a^m \rangle_n$, найти m , зная n , f , a .
Для простого n дискретный логарифм называется также **индексом**.
- 3) Извлечение корня по модулю: пусть $f = \langle a^m \rangle_n$, найти a , зная n , f , m .

З а м е ч а н и е (об извлечении корня по модулю). Для последней задачи точно известно, что существует эффективный алгоритм, находящий корень по модулю или устанавливающий, что такого корня нет. (См. [1]). Сам эффективный алгоритм не построен. Выяснено, что для его построения достаточно знать разложение n на простые множители. Таким образом, используемых односторонних функций, собственно, две, и современные криптосистемы почти все основаны на проблеме факторизации целых чисел или на проблеме дискретного логарифма в конечной абелевой группе. Задачи эти в настоящее время одинаково трудны.

2. RSA — самая известная криптосистема с открытым ключом

На первой из этих односторонних функций основана предложенная в 1978 г. и выдержавшая испытание временем криптосистема RSA (Rivest, Shamir, Adleman [2]).

Вот её краткое описание.

Представим себе сеть абонентов, где каждые два должны иметь возможность обмениваться секретной информацией.

Каждый из абонентов сети

- (1) выбирает 2 различных простых числа p и q ;
- (2) находит $n = pq$ и функцию Эйлера $\varphi(n) = (p-1)(q-1)$;
- (3) выбирает целое число e такое, что $e < \varphi(n)$ и $\text{НОД}(e, \varphi(n)) = 1$;
- (4) числа n и e помещает в открытый справочник (это **открытый ключ**).

Теперь любой абонент сети может послать данному абоненту секретное сообщение с помощью открытого ключа: сообщение представляется в виде целого числа $a < n$ (длинное сообщение разбивают на блоки) и шифруется по формуле $b = f(a) = \langle a^e \rangle_n$. Прочсть его можно, зная целое d такое, что

$\langle e d \rangle_{\varphi(n)} = 1$ (обратный вычет)¹. Обозначения e и d являются традиционными и происходят от *encode* и *decode*. При известном d декодирование производится по формуле $a = \langle b^d \rangle_n$.

Обоснование этой формулы:

Покажем, что для любого целого a от 0 до $n-1$ выполнится соотношение

$$\left\langle (\langle a^e \rangle_n)^d \right\rangle_n = a.$$

Действительно,

$$\left\langle (\langle a^e \rangle_n)^d \right\rangle_n = \langle a^{ed} \rangle_n.$$

Так как e и d взаимно обратны по модулю $\varphi(n)$, то $ed = 1 + k\varphi(n)$ для некоторого натурального k , поэтому

$$\langle a^{ed} \rangle_n = \langle a^{1+k\varphi(n)} \rangle_n = \langle a \rangle_n \cdot \langle a^{\varphi(n)} \rangle_n^k = \langle a \rangle_n = a.$$

Использована теорема Эйлера $\langle a^{\varphi(n)} \rangle_n = 1$.

Закодированный с помощью RSA текст защищён от несанкционированного прочтения настолько, насколько затруднено разложение на множители числа n .

В связи с этим развиваются алгоритмы разложения целых чисел на множители. В известном конкурсном списке RSA [3] приводятся большие числа, за факторизацию которых объявлены премии. Выпишем здесь для наглядности два из этих чисел:

- число RSA-640 (640 двоичных, 193 десятичных цифры, уже факторизовано):

310741824049004372135075003588856793003734602284272754572016194882
32064405180815045563468296a232867824379162728380334154710731085019
19548529007337724822783525742386454014691736602477652346609;

- число RSA-704 (704 двоичных, 212 десятичных цифр, не факторизовано, премия \$30000):

740375634795617128280467960974295731425931888892312890849362326389
727650340282662768919964196251178439958943305021275853701189680982
867331732731089309005525051168770632990723963807867100860969625379
34650563796359.

¹Значение d можно определить, зная p и q : находим $\varphi(n) = (p-1)(q-1)$ и затем вычисляем d по расширенному алгоритму Евклида.

3. Выбор темы — алгоритм квадратичного решета

В то время, когда был изобретён RSA, числа более чем с 80 десятичными знаками не поддавались разложению. Все известные алгоритмы либо работали слишком медленно, либо требовали чисел специального вида. Это делало относительно безопасными даже маленькие, 256-битовые ключи. Первым серьёзным прорывом было квадратичное решето, quadratic sieve (QS). Это относительно простой алгоритм факторизации, предложенный Carl Pomerance в 1981 г., который может разлагать на множители числа до 110 десятичных разрядов или около того и для таких чисел остается лучшим. Для чисел ещё больших применяется метод решета числового поля, general number field sieve (GNFS). Однако метод решета числового поля даже для базового описания требует сложных многосторонних разъяснений и обоснований. В то же время основные идеи обоих методов решета совпадают.

4. Основные идеи

4.1. Метод Ферма: факторизация, использующая разность квадратов

Известный из алгебры метод Ферма состоит в вычислении квадратов по модулю n для целых x , чуть больших \sqrt{n} , в надежде встретить полный квадрат y^2 . Метод быстро работает, если $n = pq$ и числа p, q близки друг другу. (Вот почему в RSA не выбирают близких чисел p, q .)

Суть метода. Пусть надо разложить на множители число n . Если удастся найти два числа x и y такие, что $x^2 - y^2 = n$, то $(x + y)(x - y) = n$.

Числа $(x + y)$ и $(x - y)$ являются множителями n , возможно, тривиальными (когда одно из этих чисел 1, а другое n .)

Эти два числа x и y , дающие $x^2 - y^2 = n$, найдутся, если найдётся такое целое x , что $x^2 - n$ является квадратом. Тогда $x^2 - (x^2 - n)$ — разность квадратов, равная n .

Поиск начинают с $x = \lfloor \sqrt{n} \rfloor + 1$, наименьшего возможного числа, при котором разность $x^2 - n$ положительна. Увеличивают x на 1 и вычисляют $x^2 - n$, пока $x^2 - n$ не окажется точным квадратом. Если это произошло, пытаются разложить n как $(x - \sqrt{x^2 - n})(x + \sqrt{x^2 - n})$. Если это разложение тривиально, продолжают увеличивать x .

В качестве примера продемонстрируем разложение на множители числа $n = 364729$. Найдём $\lfloor \sqrt{n} \rfloor + 1 = 604$. Вычисляем

$$604^2 - 364729 = 87 \quad \text{— не точный квадрат.}$$

Продолжаем:

$$605^2 - 364729 = 1296 = 36^2 \quad \text{— точный квадрат.}$$

Тогда

$$364729 = 605^2 - 36^2 = (605 + 36)(605 - 36) = 641 \cdot 569.$$

Разумеется, для очень больших n нет оснований считать, что искомым полный квадрат найдётся случайно возле \sqrt{n} .

Ключевым для дальнейшего продвижения явилось наблюдение, что если мы возьмём несколько значений $x^2 - n$, ни одно из которых само не является квадратом, и перемножим их, то мы можем получить квадрат — скажем, y^2 . Пусть X — произведение $X = \prod x_i$ таких x_i , для которых $\prod (x_i^2 - n) = y^2$. Тогда $X^2 - y^2$ кратно n . Следовательно, $(X - y)(X + y)$ — факторизация *некоторого кратного* n ; другими словами, по крайней мере одна из скобок делится на какой-то множитель n . Вычисляя НОД каждой скобки и n по алгоритму Евклида, мы можем выявить этот множитель. Он опять может быть тривиальным; в таком случае нам не повезло и надо попытаться снова с другим квадратом.

Уточним понятие «везения». Мы проверяем для найденных целых X и $y = \sqrt{X^2 - n}$ условие нетривиальности

$$1 < \text{НОД}(n, X \pm y) < n,$$

которое можно записать также $\langle X \pm y \rangle_n \neq 0$ или $\langle X \rangle_n \neq \langle \pm y \rangle_n$.

При выполнении этого условия получаем, что $\text{НОД}(n, X + y)$ — множитель n и $\text{НОД}(n, X - y)$ — множитель n .

Это условие выполняется с вероятностью 0.5, если $n = pq$, и с ещё большей вероятностью для других n . Это следует из теории квадратичных вычетов.

Подробнее об этом.

Вычет a (целое число от 0 до $n - 1$, или, что является более предпочтительным для излагаемого алгоритма, от $-n/2$ до $n/2$), называют квадратичным вычетом по модулю n , если a и n взаимно просты и существует такое x , что $\langle x^2 \rangle_n = a$. В противном случае a — квадратичный невычет. Пусть a — квадратичный вычет по модулю $n = pq$, p и q — различные простые числа. Известно, что в этом случае

- $\langle a \rangle_p$ — квадратичный вычет по модулю p ;
- $\langle a \rangle_q$ — квадратичный вычет по модулю q ;
- $\langle a \rangle_p$ имеет два корня по модулю p , x и $-x$, в интервале от $-n/2$ до $n/2$ (или x и $p - x$ в интервале от 0 до $n - 1$);

- $\langle a \rangle_q$ имеет два корня по модулю q , y и $-y$ (или y и $p - y$);
- любая комбинация корня по модулю p и корня по модулю q позволяет найти один корень по модулю n .

Возможных комбинаций четыре. Вероятность получить нетривиальные множители в этом случае 0.5.

Осталось выяснить, как из данного списка значений $x^2 - n$ выделить такие $x_i^2 - n$, произведение которых — квадрат.

4.2. Нахождение подмножества из списка целых, произведение которых — квадрат

Пусть дан набор целых чисел и необходимо выявить такое его подмножество, чтобы произведение чисел этого подмножества было точным квадратом, если это возможно.

Например, дан набор $\{10, 24, 35, 52, 54, 78\}$, произведение $24 \times 52 \times 78$ равно $97344 = 312^2$. Грубая попытка перебрать все подмножества слишком трудоёмка. Мы используем другой подход, основанный на разложении чисел на простые множители.

Вначале разложим каждое число набора (считаем, что это легко):

$$\begin{aligned} 10 &= 2 \times 5, \\ 24 &= 2^3 \times 3, \\ 35 &= 5 \times 7, \\ 52 &= 2^2 \times 13, \\ 54 &= 2 \times 3^3, \\ 78 &= 2 \times 3 \times 13. \end{aligned}$$

Перемножая два каких-то числа, мы просто складываем показатели степеней используемых простых чисел. Произведение будет квадратом, если и только если все степени простых чисел, его составляющие, будут чётными. Запишем каждое выше полученное разложение в виде вектора показателей, где k -я компонента показывает степень k -го простого числа:

$$\begin{aligned} (1 \ 0 \ 1 \ 0 \ 0 \ 0), \\ (3 \ 1 \ 0 \ 0 \ 0 \ 0), \\ (0 \ 0 \ 1 \ 1 \ 0 \ 0), \\ (2 \ 0 \ 0 \ 0 \ 0 \ 1), \\ (1 \ 3 \ 0 \ 0 \ 0 \ 0), \\ (1 \ 1 \ 0 \ 0 \ 0 \ 1). \end{aligned}$$

Умножая числа, мы просто складываем векторы. Так как нас интересует только чётность, берём все компоненты по модулю 2:

$$\begin{aligned} & (1 \ 0 \ 1 \ 0 \ 0 \ 0), \\ & (1 \ 1 \ 0 \ 0 \ 0 \ 0), \\ & (0 \ 0 \ 1 \ 1 \ 0 \ 0), \\ & (0 \ 0 \ 0 \ 0 \ 0 \ 1), \\ & (1 \ 1 \ 0 \ 0 \ 0 \ 0), \\ & (1 \ 1 \ 0 \ 0 \ 0 \ 1). \end{aligned}$$

Нам нужно получить нетривиальную линейную комбинацию по модулю 2 (с коэффициентами 0 и 1), дающую нулевой вектор $(0 \ 0 \ 0 \ 0 \ 0 \ 0)$.

Это можно перефразировать как матричное уравнение $Ax = \mathbf{0}$ (умножение и сложение по правилам для вычетов по модулю 2), где неизвестным является вектор коэффициентов линейной комбинации, а матрица A состоит из векторов показателей, записанных по столбцам:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Вектор $x = (0 \ 1 \ 0 \ 1 \ 0 \ 1)$, как видим, является нетривиальным решением уравнения $Ax = \mathbf{0}$ и соответствует приведённому выше произведению $24 \times 52 \times 78$.

Обсудим способ получения нетривиальных решений.

То, что матричное уравнение $Ax = \mathbf{0}$ дано над полем вычетов по модулю 2, упрощает алгоритм гауссова исключения неизвестных. В частности, из элементарных преобразований требуется только прибавление к строке другой строки по модулю 2 (булевская операция \oplus).

Опишем простой алгоритм на псевдоязыке. Матрицу A будем приводить к виду, позволяющему сразу выписать общее решение системы. Массивы $A[1..m, 1..n]$ и $used[1..m]$ (последний заведён для пометок строк) отнесём к булевскому типу, но сохраним для их элементов обозначения 1 и 0 вместо **true** и **false**. Также используем для логических операций и отношений знаки \wedge , \neg , \neq , \oplus вместо **and**, **not**, $<>$ и **xor**.

Выполним действия:

```

for r := 1 to m do used[r] := 0;
for k := 1 to n do
for r := 1 to m do
if (A[r,k]  $\wedge$   $\neg$ used[r]) then begin
  for i := 1 to m do if (A[i,k]  $\wedge$  r  $\neq$  i then
    for j := 1 to n do A[i,j] := A[i,j]  $\oplus$  A[r,j];
  used[r] := 1;
end;

```

Когда описанный алгоритм отработает, каждая строка матрицы, кроме полностью нулевых, будет начинаться с *ведущей единицы* (элемента строки, равного 1 и стоящего в столбце с наименьшим номером), и при этом позиции всех ведущих единиц будут различны.

Например, матрица

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

примет вид

$$\begin{pmatrix} 0 & \boxed{1} & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \boxed{1} & 0 & 1 & 1 \\ \boxed{1} & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \boxed{1} & 1 & 0 \end{pmatrix}.$$

Ведущие единицы выделены.

Результат будет более наглядным, если отсортировать строки по возрастанию позиций ведущих единиц, а последними поместить нулевые строки, не получившие пометку *used*. Тогда матрица примет *ступенчатый вид*:

$$\begin{pmatrix} \boxed{1} & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & \boxed{1} & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & \boxed{1} & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & \boxed{1} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

то есть такой, что для всех $i > 1$ ведущая единица в i -й строке находится хотя бы на одну позицию правее, чем в $(i - 1)$ -й.

Число ведущих единиц равно рангу матрицы A . Система уравнений заведомо имеет нетривиальные решения, если этот ранг меньше числа столб-

цов (в частности, если число строк m меньше числа столбцов n)².

Пусть нетривиальные решения имеются. Нам достаточно найти одно из них.

В соответствии с наличием или отсутствием ведущих единиц в соответствующих столбцах переменные разделились на *базисные* и *свободные* [5].

Теперь мы берём любой столбец, отвечающий свободной переменной, и эту переменную полагаем равной 1. Остальные свободные переменные можем брать как 0, так и 1. Итоговая матрица в строках с ведущими единицами уже содержит выражения базисных переменных через свободные, так что и их мы найдём.

В последнем примере нарочно взят один нулевой столбец, чтобы показать, что эта экзотическая ситуация ничего не меняет в алгоритме. Напротив, мы можем сразу взять значение $x_3 = 1$, остальные свободные переменные положить равными 0, тогда и все базисные переменные будут равны 0. Решение $(0 \ 0 \ 1 \ 0 \ 0 \ 0 \ 0)$ сообщает, что третье число из набора, давшего линейную систему, является полным квадратом.

Есть и ещё решения; например, при значениях базисных переменных $x_3 = 1$, $x_6 = 1$, $x_7 = 0$ из первой строки находим $x_1 = x_6 = 1$, из второй $x_2 = x_7 = 0$, из третьей $x_4 = x_6 \oplus x_7 = 1$, из четвёртой $x_5 = x_6 = 1$. Решение $(1 \ 0 \ 1 \ 1 \ 1 \ 1 \ 0)$ означает, что произведение 1-го, 3-го, 4-го, 5-го и 6-го чисел набора — полный квадрат.

Применим этот метод к приводившейся выше системе уравнений, построенной для набора $\{10, 24, 35, 52, 54, 78\}$. Метод преобразует матрицу

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

к виду

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

²В случае, когда ранг матрицы A равен числу столбцов, нетривиальных решений не будет. На практике это означает, что исследуемых целых чисел набрано недостаточно.

Двигаясь по строчкам сверху вниз, выписываем общее решение

$$x_1 = 0, \quad x_2 = x_5 \oplus x_6, \quad x_3 = 0, \quad x_4 = x_6.$$

Нетривиальных решений три: при $x_5 = 0, x_6 = 1$ уже известное нам $(0 \ 1 \ 0 \ 1 \ 0 \ 1)$; при $x_5 = 1, x_6 = 0$ решение $(0 \ 1 \ 0 \ 0 \ 1 \ 0)$, соответствующее произведению $24 \times 56 = 1296 = 36^2$; при $x_5 = 1, x_6 = 1$ решение $(0 \ 0 \ 0 \ 1 \ 1 \ 1)$, соответствующее произведению $52 \times 54 \times 78 = 219024 = 468^2$.

Осталась проблема: если среди наших чисел есть число с очень большими множителями, то в матрице будет очень много строк, и наш метод станет неэффективным. Во избежание этого мы требуем, чтобы входные числа были *B-гладкими*, что означает, что их простые множители не превышают некоторого целого B . Если говорят просто о гладких числах, значит, имеют в виду, что B весьма мало в сравнении с n .

Нам предстоит применять этот метод для чисел вида $x^2 - n$ при $x = \lfloor \sqrt{n} \rfloor + 1, \lfloor \sqrt{n} \rfloor + 2, \dots$. Что делать, если в разложении этих чисел присутствуют большие простые множители?

Мы просто отбросим числа с большими множителями! Теоретические исследования показывают, что имеется достаточно большое количество значений в последовательности $x^2 - n$, которые являются гладкими.

Например, рассмотрим число $n = 112093$. Здесь $\sqrt{n} \approx 334.8$.

Начнём с $x = \lfloor \sqrt{n} \rfloor + 1 = 335$ и будем увеличивать x до $M = 350$. Зададим предварительно границу гладкости $B = 29$. Выбор чисел M и B определяется следующими соображениями:

- чем меньше значения M и B , тем быстрее работает алгоритм;
- значения M и B должны быть достаточно велики, чтобы описанная выше однородная система линейных уравнений по модулю 2 имела нетривиальное решение.

Таким образом, по ходу решения мы сможем откорректировать выбранные значения как в сторону увеличения, так и в сторону уменьшения.

Мы получили значения:

x	335	336	337	338	339	340	341	342	343	344
$x^2 - n$	132	803	1476	2151	2828	3507	4188	4871	5556	6243

x	345	346	347	348	349	350	...	374	375
$x^2 - n$	6932	7623	8316	9011	9708	10407	...	27783	28352

Ни одно из значений вида $x^2 - n$ не квадрат; однако, если мы разложим каждое значение по степеням простых чисел, мы увидим, что четыре из них не имеют множителей больше 11:

$$\begin{aligned} 132 &= 2^2 \times 3 \times 11, \\ 7623 &= 3^2 \times 7 \times 11^2, \\ 8316 &= 2^2 \times 3^3 \times 7 \times 11, \\ 27783 &= 3^4 \times 7^3. \end{aligned}$$

(Позже покажем, как эти четыре числа найти, не раскладывая весь список на множители.)

Соответствующая система уравнений $Ax = \mathbf{0}$ имеет матрицу

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

Решением её по модулю 2 будет вектор $(x_3 \ x_3 + x_4 \ x_3 \ x_4)$.

При $x_3 = 1, x_4 = 0$ это решение нетривиально: $(1 \ 1 \ 1 \ 0)$. Это значит, что точным квадратом будет произведение первых трёх чисел:

$$2^2 \cdot 3 \cdot 11 \cdot 3^2 \cdot 7 \cdot 11^2 \cdot 2^2 \cdot 3^3 \cdot 7 \cdot 11 = 2^4 \cdot 3^6 \cdot 7^2 \cdot 11^4 = (2^2 \cdot 3^3 \cdot 7 \cdot 11^2)^2 = 91476^2.$$

В обозначениях предыдущего пункта $X = \prod x_i = 335 \cdot 346 \cdot 347$, $y = 91476$. Здесь $X - y = 40220770 - 91476 = 40129294$. Находим

$$\text{НОД}(X - y, n) = \text{НОД}(40129294, 112093) = 112093.$$

К сожалению, найденный делитель числа $n = 112093$ тривиален.

Заметим, что и $\text{НОД}(X + y, n) = \text{НОД}(40312246, 112093) = 1$ — тривиальный делитель.

Возьмем тогда другое решение системы $Ax = \mathbf{0}$, а именно решение $(0 \ 1 \ 0 \ 1)$, получающееся при $x_3 = 0, x_4 = 1$. Оно означает, что точным квадратом будет произведение второго и четвертого чисел:

$$3^2 \cdot 7 \cdot 11^2 \cdot 3^4 \cdot 7^3 = 3^6 \cdot 7^4 \cdot 11^2 = (3^3 \cdot 7^2 \cdot 11)^2 = 14553^2.$$

Имеем $X = \prod x_i = 346 \cdot 374 = 129404$, $y = 14553$. Находим

$$\text{НОД}(X - y, n) = \text{НОД}(114851, 112093) = 197.$$

Найден нетривиальный делитель 197 числа $n = 112093$.

Теперь число n можно разложить на множители: $112093 = 569 \cdot 197$.

4.3. Факторные базы

Имеется ряд методов, основанных на изложенном выше принципе, в том числе и методы решета. Они пользуются следующей терминологией.

Набор небольших простых чисел, к которому обычно добавляют и -1 , образует так называемую **факторную базу** $\{-1, p_1, p_2, \dots, p_h\}$, где p_i — небольшие простые числа, ограниченные некоторым B , $p_i \leq B$.

Добавление -1 вызвано тем, что в этих методах экономнее работать не с наименьшими положительными, а с **наименьшими по абсолютной величине** вычетами по модулю n , но в нашем упрощённом изложении мы этого не требуем. Мы работали в нашем примере с факторной базой $\{2, 3, 7, 11\}$, хотя первоначально планировалась граница $B = 29$. (Оказалось, что и базы $\{2, 3, 7, 11\}$ достаточно для решения системы).

Обращает на себя внимание отсутствие в факторной базе малого простого числа 5. Действительно, в факторную базу включают только такие простые p_i , для которых $\left(\frac{n}{p_i}\right) = 1$ (символ Лежандра; его равенство 1 означает, что n — квадратичный вычет по модулю p_i). Если это не так, то среди чисел вида $x^2 - n$ не найдётся ни одного, делящегося на p_i , и это число не имеет смысла включать в базу.

Символ Лежандра для простого нечётного p вычисляется по формуле $\left(\frac{n}{p}\right) = \left\langle n^{\frac{p-1}{2}} \right\rangle_p$, вычисление несложно. Число n оказалось квадратичным невычетом по модулю 5, а также по модулям 13, 17, 19, 23, 29, 37, ..., так что если бы границы $B = 11$ оказалось недостаточно, пришлось бы расширять базу, включая в неё простые числа 31, 41, 43 и так далее.

4.4. Просеивание

Пора вернуться к узкому месту предыдущих выкладок: как из набора чисел вида $x^2 - n$ выделить гладкие числа, не раскладывая каждое на множители.

Основная идея: вместо того, чтобы перебирать эти числа и проверять, делятся ли их квадраты по модулю n на простые числа из базы, перебирают по очереди простые числа из базы и сразу для всех чисел вида $x^2 - n$ проверяют, делятся ли они на очередное p и его степени.

Метод основан на решете Эратосфена, откуда и получил своё название. Решетом служат простые числа факторной базы и дополнительно их небольшие степени, и при просеивании мы числа не вычёркиваем, а **делим на эти простые**. Те числа, что перейдут в 1, будут B -гладкими.

Продemonстрируем этот метод на нашем наборе чисел:

132	803	1476	2151	2828	3507	4188	4871	5556
6243	6932	7623	8316	9011	9708	10407	11108	11811
12516	13223	13932	14643	15356	16071	16788	17507	18228
18951	19676	20403	21132	21863	22596	23331	24068	24807
25548	26291	27036	27783	28532				

Начинаем с 2. Первое просеивание:

66	803	738	2151	1414	3507	2094	4871	2778
6243	3466	7623	4158	9011	4854	10407	5554	11811
6258	13223	6966	14643	7678	16071	8394	17507	9114
18951	9838	20403	10566	21863	11298	23331	12034	24807
12774	26291	13518	27783	14266				

Заметим, что в исходной таблице чётные числа шли через одно. Это, конечно, не случайность. Школьная алгебра показывает, что для любого целого d выполняется равенство

$$(x + kd)^2 - n = (x^2 - n) + d(2kx + dk^2),$$

так что если число из нашего набора делится на d , то и все числа, отстоящие от него на расстояние, кратное d , делятся на d .

Есть изменённые числа (в таблице они выделены). Снова прогоняем через 2:

33	803	369	2151	707	3507	1047	4871	1389
6243	1733	7623	2079	9011	2427	10407	2777	11811
3129	13233	3483	14643	3839	16071	4197	17507	4557
18951	4919	20403	5283	21863	5649	23331	6017	24807
6387	26291	6759	27783	7133				

При следующем прогоне через делитель 2 изменений уже не будет (в данном маленьком примере это видно до прогона), так что дальше делим уже на 3 — следующее простое число факторной базы:

11	803	123	717	707	1169	349	4871	463
2081	1733	2541	693	9011	809	3469	2777	3937
1043	13223	1161	4881	3839	5357	1399	17507	1519
6317	4919	6801	1761	21863	1883	7777	6017	8269
2129	26291	2253	9261	7133				

Нас уже не удивляет, что если число делится на 3, то и каждое третье после него делится на 3. Не должно удивлять нас и то, что таких цепочек две, одна начинается с 1-й клетки, другая с 3-й. Наличие двух цепочек вытекает из того, что квадратичное сравнение по модулю p имеет ровно два решения (если вообще имеет решение). Разумеется, это наблюдение, сильно сокращающее расчёты, используется при просеивании: находят первые два числа, делящиеся на p , и идут от них «с периодом p ». Для малых простых можно обойтись без специального алгоритма, просто тестировать первые p чисел, чтобы определить, какие из них делятся на p , а потом идти по цепочке. Для больших простых такой трудоёмкой процедуры следует избегать. Существует эффективный алгоритм для нахождения этих двух решений (Shanks-Tonelli algorithm [5]).

Повторяем деление на 3 ещё 3 раза и получаем:

11	803	41	239	707	1169	349	4871	463
2081	1733	847	77	9011	809	3469	2777	3937
1043	13223	43	1627	3839	5357	1399	17507	1519
6317	4919	2267	587	21863	1883	7777	6017	8269
2129	26291	751	343	7133				

При следующем прогоне через делитель 3 изменений не будет. Далее делим на 7 — следующее число факторной базы:

11	803	41	239	101	167	349	4871	463
2081	1733	121	11	9011	809	3469	2777	3937
149	1889	43	1627	3839	5357	1399	2501	217
6317	4919	2267	587	21863	269	1111	6017	8269
2129	26291	751	49	1019				

Попутно приятно обратить внимание на две цепочки делителя 7, с 4-й и с 5-й клетки.

Ещё два прогона через 7 приводят к первой единице:

11	803	41	239	101	167	349	4871	463
2081	1733	121	11	9011	809	3469	2777	3937
149	1889	43	1627	3839	5357	1399	2501	31
6317	4919	2267	587	21863	269	1111	6017	8269
2129	26291	751	1	1019				

При следующем прогоне через 7 изменений не будет. Делим на 11. Это понадобится проделать дважды, после чего получим числа:

1	73	41	239	101	167	349	4871	463
2081	1733	1	1	9011	809	3469	2777	3937
149	1889	43	1627	349	487	1399	2501	31
6317	4919	2267	587	21863	269	101	547	8269
2129	26291	751	1	1019				

Появились новые единицы, и эта таблица для нас последняя.

Там, где теперь стоят 1, в исходной таблице находились 11-гладкие числа.

Их список мы уже приводили: 132, 7623, 8316, 27783. Разложение их на множители получено параллельно с просеиванием.

5. Заключительные замечания

Мы изложили базовую реализацию метода квадратичного решета, она имеет много версий. Рекорд метода — разложение RSA-129.

Метод имеет субэкспоненциальную эмпирическую сложность, то есть наихудшее время его работы представимо в форме $e^{o(N)}$, где $N = \log n$ (число двоичных разрядов в записи n), оценка времени выполнения $O(e^{(C+o(1))\sqrt{N \log N}})$ с константой $C = 9/8$.

Метод решета в числовом поле имеет лучшую оценку $O(e^{(C+o(1))\sqrt[3]{n} \cdot \sqrt[3]{\log^2 N}})$.

Для более детального ознакомления с методами факторизации и их местом в современной криптологии можно рекомендовать книги [1, 6, 7, 8, 9].

Список литературы

1. Брассар Ж. *Современная криптология*. М.: ПОЛИМЕД, 1999.
2. Rivest R. L., Shamir A., Adleman L. M. *A method for obtaining digital signatures and public-key cryptosystems* // Communications of the ACM. 1978. V. 21, P. 120–126.
3. *The RSA Challenge Numbers* // RSA Laboratories. (<http://www.rsasecurity.com/rsalabs/node.asp?id=2093>).
4. Стренг Г. *Линейная алгебра и её применения*. М.: Мир, 1980.
5. Shanks D. *Five number-theoretic algorithms* // Proceedings of the Second Manitoba Conference on Numerical Mathematics (Winnipeg), Utilitas Math. 1973. P. 51–70. Congressus Numerantium, No. VII.
6. Смарт Н. *Криптография*. М.: Техносфера, 2005.

7. Тилборг ван Х. К. А. *Основы криптологии: профессиональное руководство и интерактивный учебник*. М.: Мир, 2006.
8. Земор Ж. *Курс криптографии*. М.-Ижевск: НИЦ «Регулярная и космическая динамика»; Институт космических исследований, 2006.
9. Василенко О. Н. *Теоретико-числовые алгоритмы в криптографии*. М.: МЦНМО, 2003.

МОЖНО ЛИ ПОСТРОИТЬ ОКРУЖНОСТЬ С ПОМОЩЬЮ КРИВЫХ БЕЗЬЕ?

М. И. Григорьев В. Н. Малозёмов А. Н. Сергеев

19 декабря 2006 г.

Доклад основан на материале из [1, Chapter 12].

1°. Зафиксируем три точки на плоскости $P_0(x_0, y_0)$, $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, не лежащие на одной прямой, и три положительных числа w_0 , w_1 , w_2 . По ним можно построить дробно-рациональную кривую Безье второго порядка

$$\mathfrak{R}(u) = \frac{w_0(1-u)^2 P_0 + 2w_1(1-u)u P_1 + w_2 u^2 P_2}{w_0(1-u)^2 + 2w_1(1-u)u + w_2 u^2}, \quad u \in [0, 1]. \quad (1)$$

Геометрические соображения, приводящие к кривой (1), и метод вычисления $\mathfrak{R}(u)$ при фиксированном u описаны в [1, с. 209-215].

Введём обозначения $w = w_0(1-u)^2 + 2w_1(1-u)u + w_2 u^2$,

$$\lambda_0 = \frac{w_0(1-u)^2}{w}, \quad \lambda_1 = \frac{2w_1(1-u)u}{w}, \quad \lambda_2 = \frac{w_2 u^2}{w}.$$

Тогда (1) можно переписать в виде

$$\mathfrak{R}(u) = \lambda_0 P_0 + \lambda_1 P_1 + \lambda_2 P_2, \quad (2)$$

где коэффициенты λ_i удовлетворяют условиям: они неотрицательны и в сумме равны единице. Это значит, что точка $\mathfrak{R}(u)$ при фиксированном $u \in [0, 1]$ является выпуклой комбинацией точек P_0 , P_1 , P_2 . Вся кривая $\mathfrak{R} = \{\mathfrak{R}(u) \mid u \in [0, 1]\}$ лежит в треугольнике с вершинами P_0 , P_1 , P_2 . В частности, $\mathfrak{R}(0) = P_0$, $\mathfrak{R}(1) = P_2$.

Зафиксируем $u \in (0, 1)$. В этом случае все коэффициенты λ_i положительны. В силу определения λ_i

$$\frac{\lambda_0}{\lambda_1} = \frac{w_0}{2w_1} \frac{1-u}{u}, \quad \frac{\lambda_1}{\lambda_2} = \frac{2w_1}{w_2} \frac{1-u}{u},$$

так что

$$\frac{2w_1}{w_0} \frac{\lambda_0}{\lambda_1} = \frac{w_2}{2w_1} \frac{\lambda_1}{\lambda_2}.$$

Обозначив $\mu = w_1^2/(w_0w_2)$, получим

$$4\mu\lambda_0\lambda_2 = \lambda_1^2. \quad (3)$$

Таким образом, барицентрические координаты точек кривой $\mathfrak{R}(u)$ при $u \in (0, 1)$ удовлетворяют соотношению (3). Соотношение (3) выполняется и при граничных значениях параметра $u = 0$, $u = 1$.

Если ввести множество \mathfrak{B} точек P вида

$$P = \lambda_0 P_0 + \lambda_1 P_1 + \lambda_2 P_2,$$

где коэффициенты λ_i неотрицательны, в сумме равны единице и удовлетворяют соотношению (3), то по существу доказано, что $\mathfrak{R} \subset \mathfrak{B}$. Проверим обратное включение $\mathfrak{B} \subset \mathfrak{R}$.

Возьмём точку $P \in \mathfrak{B}$ с барицентрическими координатами $\lambda_0, \lambda_1, \lambda_2$. Нужно найти $u \in [0, 1]$, такое, что $P = \mathfrak{R}(u)$. Если $\lambda_0 = 0$, то, согласно (3), $\lambda_1 = 0$. В этом случае $\lambda_2 = 1$ и $P = P_2 = \mathfrak{R}(1)$. При $\lambda_2 = 0$ будет $\lambda_1 = 0$, $\lambda_0 = 1$, $P = P_0 = \mathfrak{R}(0)$. В дальнейшем считаем, что все коэффициенты λ_i положительны. Обозначим

$$f(u) = \frac{w_2 u^2}{w_0(1-u)^2 + 2w_1(1-u)u + w_2 u^2} = \frac{w_2 u^2}{w}$$

и покажем, что уравнение $f(u) = \lambda_2$ имеет единственное на $(0, 1)$ решение. Ясно, что $f(0) = 0$, $f(1) = 1$, поэтому достаточно проверить, что $f'(u) > 0$ на $(0, 1)$. Запишем

$$f'(u) = w_2 u \frac{2w - uw'}{w^2}. \quad (4)$$

Поскольку $w' = 2[(w_1 - w_0)(1 - u) + (w_2 - w_1)u]$, то

$$\begin{aligned} 2w - uw' &= 2[w_0(1-u)^2 + 2w_1(1-u)u + w_2 u^2 - \\ &\quad - (w_1 - w_0)(1-u)u - (w_2 - w_1)u^2] = \\ &= 2[w_0(1-u)^2 + (w_1 + w_0)(1-u)u + w_1 u^2]. \end{aligned}$$

Отсюда и из (4) следует, что $f'(u) > 0$ при $u \in (0, 1)$. Значит, существует единственное $u \in (0, 1)$, такое, что $\lambda_2 = w_2 u^2/w$. Покажем, что при этом $\lambda_1 = 2w_1(1-u)u/w$, $\lambda_0 = w_0(1-u)^2/w$. Тем самым будет установлено требуемое включение $\mathfrak{B} \subset \mathfrak{R}$.

Согласно (3), λ_1 (при фиксированном λ_2) является положительным корнем уравнения

$$\varphi(\lambda) := \lambda^2 - 4\mu\lambda_2((1 - \lambda_2) - \lambda) = 0. \quad (5)$$

Производная $\varphi'(\lambda) = 2\lambda + 4\mu\lambda_2$ равна нулю при отрицательном $\lambda = -2\mu\lambda_2$, поэтому квадратное уравнение (5) имеет *единственный* положительный корень. Проверим, что $\lambda = 2w_1(1 - u)u/w$ удовлетворяет (5). Действительно,

$$4\mu\lambda_2 \left(1 - \lambda_2 - \frac{2w_1(1 - u)u}{w} \right) = 4 \frac{w_1^2}{w_0w_2} \frac{w_2u^2}{w} \frac{w_0(1 - u)^2}{w} = \left(\frac{2w_1(1 - u)u}{w} \right)^2.$$

Значит, $\lambda_1 = 2w_1(1 - u)u/w$. Остаётся отметить, что

$$\lambda_0 = 1 - \lambda_1 - \lambda_2 = w_0(1 - u)^2/w.$$

Включение $\mathfrak{B} \subset \mathfrak{R}$, а с ним и равенство $\mathfrak{R} = \mathfrak{B}$, установлены.

Полученный результат можно сформулировать так.

ПРЕДЛОЖЕНИЕ 1. *Дробно-рациональная кривая Безье второго порядка (1) в барицентрических (относительно точек P_0, P_1, P_2) координатах определяется уравнением (3) с $\mu = w_1^2/(w_0w_2)$.*

2°. Зафиксируем $r > 0$ и рассмотрим точки $P_0(r, 0)$, $P_1(r, r)$, $P_2(0, r)$. Обозначим через \mathcal{C} четверть окружности, построенную так, как показано на рис. 1.

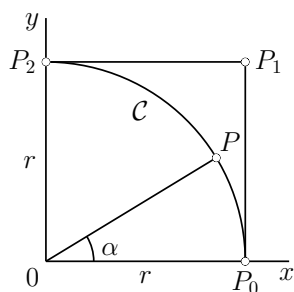


Рис. 1

Выясним, существуют ли веса w_0, w_1, w_2 , при которых соответствующая дробно-рациональная кривая Безье (1) совпадает с \mathcal{C} .

Возьмём точку $P \in \mathcal{C}$ с координатами $x = r \cos \alpha$, $y = r \sin \alpha$, $\alpha \in [0, \frac{\pi}{2}]$. Найдём её барицентрические координаты относительно P_0, P_1, P_2 . Имеем

$$P = \lambda_0 \begin{pmatrix} r \\ 0 \end{pmatrix} + \lambda_1 \begin{pmatrix} r \\ r \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ r \end{pmatrix},$$

так что

$$\lambda_0 + \lambda_1 = \cos \alpha,$$

$$\lambda_1 + \lambda_2 = \sin \alpha,$$

$$\lambda_0 + \lambda_1 + \lambda_2 = 1.$$

Отсюда следует, что

$$\lambda_0 = 1 - \sin \alpha, \quad \lambda_2 = 1 - \cos \alpha, \quad \lambda_1 = \sin \alpha + \cos \alpha - 1,$$

причём все λ_i неотрицательны. Далее

$$\lambda_1^2 = 2(1 - \sin \alpha - \cos \alpha + \sin \alpha \cos \alpha) = 2(1 - \sin \alpha)(1 - \cos \alpha) = 2\lambda_0\lambda_2.$$

Значит, кривая \mathcal{C} в барицентрических координатах определяется уравнением $\lambda_1^2 = 2\lambda_0\lambda_2$. Согласно предложению 1, \mathcal{C} является дробно-рациональной кривой Безье второго порядка с параметром $\mu = \frac{1}{2}$. Поскольку $\mu = w_1^2/(w_0w_2)$, то взяв, например, $w_0 = w_2 = 1$, $w_1 = \sqrt{2}/2$, получим кривую \mathfrak{R} , совпадающую с \mathcal{C} .

Как известно, кривая $\mathfrak{R}(u)$ вида (1) строится с помощью обычной кривой Безье в \mathbb{R}^3 , порождённой точками $\hat{P}_i(w_ix_i, w_iy_i, w_i)$, $i \in 0 : 2$. Поэтому на вопрос, поставленный в заголовке доклада, следует дать такой ответ: можно, если использовать кривые Безье в \mathbb{R}^3 .

3°. Вернёмся к кривой $\mathfrak{R}(u)$ вида (1).

ПРЕДЛОЖЕНИЕ 2. *Кривая*

$$\tilde{\mathfrak{R}}(t) = \frac{(1-t)^2P_0 + 2\tilde{w}_1(1-t)tP_1 + t^2P_2}{(1-t)^2 + 2\tilde{w}_1(1-t)t + t^2}, \quad t \in [0, 1], \quad (6)$$

с $\tilde{w}_1 = \sqrt{\mu}$ обладает тем свойством, что

$$\{\mathfrak{R}(u) \mid u \in [0, 1]\} = \{\tilde{\mathfrak{R}}(t) \mid t \in [0, 1]\}. \quad (7)$$

Доказательство. Обозначим множества, стоящие в левой и правой частях равенства (7), через \mathfrak{R} и $\tilde{\mathfrak{R}}$ соответственно. Проверим, что $\mathfrak{R} \subset \tilde{\mathfrak{R}}$ и $\tilde{\mathfrak{R}} \subset \mathfrak{R}$.

Воспользуемся отображением

$$u = \frac{t}{\rho(1-t) + t} \quad (8)$$

отрезка $[0, 1]$ на себя при $\rho = \sqrt{w_2/w_0}$ с обратным отображением

$$t = \frac{\rho u}{(1-u) + \rho u}. \quad (9)$$

Зафиксируем $u \in [0, 1]$ и представим его в виде (8). Подставив (8) в (1), получим

$$\begin{aligned} \mathfrak{R}(u) &= \frac{w_0\rho^2(1-t)^2P_0 + 2w_1\rho(1-t)tP_1 + w_2t^2P_2}{w_0\rho^2(1-t)^2 + 2w_1\rho(1-t)t + w_2t^2} = \\ &= \frac{w_2(1-t)^2P_0 + 2w_1\sqrt{w_2/w_0}(1-t)tP_1 + w_2t^2P_2}{w_2(1-t)^2 + 2w_1\sqrt{w_2/w_0}(1-t)t + w_2t^2}. \end{aligned}$$

После деления числителя и знаменателя на w_2 придём к равенству $\mathfrak{R}(u) = \tilde{\mathfrak{R}}(t)$, которое гарантирует, что $\mathfrak{R} \subset \tilde{\mathfrak{R}}$.

Для проверки обратного включения зафиксируем $t \in [0, 1]$ и представим его в виде (9). Подставив (9) в (6), получим

$$\tilde{\mathfrak{R}}(t) = \frac{(1-u)^2 P_0 + 2\tilde{w}_1 \rho (1-u) u P_1 + \rho^2 u^2 P_2}{(1-u)^2 + 2\tilde{w}_1 \rho (1-u) u + \rho^2 u^2}. \quad (10)$$

Отметим, что $\tilde{w}_1 \rho = w_1/w_0$. После умножения числителя и знаменателя дроби (10) на w_0 придём к равенству $\tilde{\mathfrak{R}}(t) = \mathfrak{R}(u)$, которое гарантирует, что $\tilde{\mathfrak{R}} \subset \mathfrak{R}$. Предложение доказано. \square

Говорят, что дробно-рациональная кривая Безье (6) имеет *стандартную форму*. Согласно предложению 2 любая дробно-рациональная кривая Безье второго порядка может быть приведена к стандартной форме.

4°. Дадим классификацию дробно-рациональных кривых Безье второго порядка в зависимости от значений параметра μ .

Рассмотрим на плоскости три точки P_0, P_1, P_2 , не лежащие на одной прямой. Систему декартовых координат введём так, как показано на рис. 2.

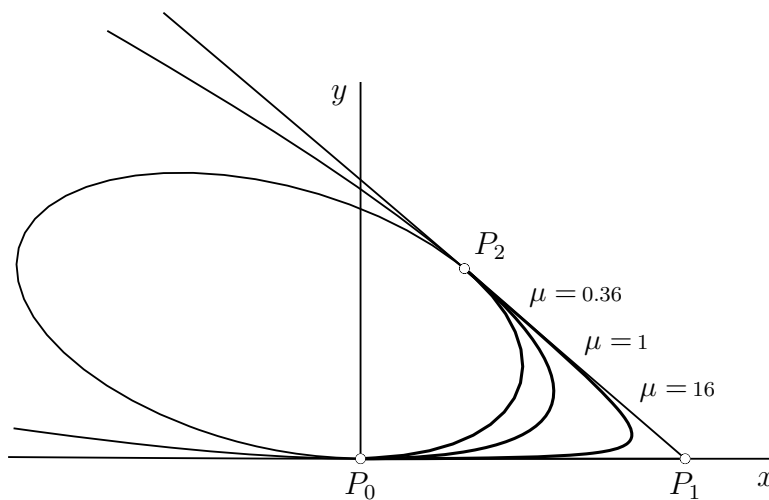


Рис. 2

В этом случае $P_0 = P_0(0, 0)$, $P_1 = P_1(x_1, 0)$, $P_2 = P_2(x_2, y_2)$, где $x_1 > 0$, $y_2 > 0$. При фиксированном $\mu > 0$ по точкам P_0, P_1, P_2 построим кривую $\tilde{\mathfrak{R}}(t)$ вида (6). Возьмём на ней точку $P(x, y)$ с барицентрическими координатами $\lambda_0, \lambda_1, \lambda_2$. Имеем

$$\begin{pmatrix} x \\ y \end{pmatrix} = \lambda_0 \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \lambda_1 \begin{pmatrix} x_1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Приходим к системе соотношений

$$\begin{aligned}\lambda_0 + \lambda_1 + \lambda_2 &= 1, \\ \lambda_1 x_1 + \lambda_2 x_2 &= x, \\ \lambda_2 y_2 &= y.\end{aligned}$$

Отсюда следует, что

$$\begin{aligned}\lambda_2 &= \frac{y}{y_2}, \quad \lambda_1 = \frac{xy_2 - yx_2}{x_1 y_2}, \\ \lambda_0 &= \frac{-xy_2 - y(x_1 - x_2) + x_1 y_2}{x_1 y_2}.\end{aligned}$$

Подставив это в (3) и умножив обе части равенства на $(x_1 y_2)^2$, получим

$$4\mu y x_1 [-xy_2 - y(x_1 - x_2) + x_1 y_2] - (xy_2 - yx_2)^2 = 0.$$

Данное уравнение преобразуется к виду

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_1x + 2a_2y + a = 0, \quad (11)$$

где

$$\begin{aligned}a_{11} &= -y_2^2, \quad a_{22} = -4\mu x_1(x_1 - x_2) - x_2^2, \\ a_{12} &= -2\mu x_1 y_2 + x_2 y_2, \\ a_1 &= 0, \quad a_2 = 2\mu x_1^2 y_2, \quad a = 0.\end{aligned}$$

Инвариантами уравнения (11) являются два определителя

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_1 \\ a_{12} & a_{22} & a_2 \\ a_1 & a_2 & a \end{vmatrix}, \quad \delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{vmatrix}$$

и число $\varepsilon = a_{11} + a_{22}$. Вычислим их. Имеем

$$\Delta = \begin{vmatrix} -y_2^2 & -2\mu x_1 y_2 + x_2 y_2 & 0 \\ -2\mu x_1 y_2 + x_2 y_2 & -4\mu x_1(x_1 - x_2) - x_2^2 & 2\mu x_1^2 y_2 \\ 0 & 2\mu x_1^2 y_2 & 0 \end{vmatrix} = 4\mu^2 x_1^4 y_2^4,$$

$$\begin{aligned}\delta &= y_2^2 [4\mu x_1(x_1 - x_2) - x_2^2] - (-2\mu x_1 y_2 + x_2 y_2)^2 = \\ &= 4\mu x_1(x_1 - x_2)y_2^2 - 4\mu^2 x_1^2 y_2^2 + 4\mu x_1 x_2 y_2^2 = 4\mu x_1^2 y_2^2 (1 - \mu),\end{aligned}$$

$$\begin{aligned}\varepsilon &= -[y_2^2 + (x_2^2 - 4\mu x_1 x_2 + 4\mu x_1^2)] = \\ &= -[y_2^2 + (x_2 - 2\mu x_1)^2 + 4\mu x_1^2(1 - \mu)].\end{aligned}$$

Отметим, что $\Delta > 0$. При $\mu < 1$ выполняются неравенства $\delta > 0$ и $\varepsilon < 0$.

На основании результатов о классификации кривых второго порядка [2] приходим к следующему заключению.

ПРЕДЛОЖЕНИЕ 3. *Дробно-рациональная кривая Безье второго порядка является дугой параболы при $\mu = 1$, гиперболы при $\mu > 1$ и эллипса при $\mu \in (0, 1)$.*

На рис. 2 представлены все три случая.

ЛИТЕРАТУРА

1. Farin G. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.
2. Привалов И. И. *Аналитическая геометрия*. 35-е изд. Лань, 2005.

ФРЕЙМ МЕРСЕДЕС-БЕНЦ В n -МЕРНОМ ПРОСТРАНСТВЕ

В. Н. Малозёмов А. Б. Певный

16 января 2007 г.

В докладе представлен усовершенствованный вариант результатов из [1, 2].

1°. Напомним [3, с. 99–100], что жёстким фреймом в \mathbb{R}^n называется семейство из $m \geq n$ векторов $\{\varphi_1, \varphi_2, \dots, \varphi_m\}$, такое, что для любого $x \in \mathbb{R}^n$ выполняется равенство

$$\sum_{j=1}^m |\langle x, \varphi_j \rangle|^2 = A \|x\|^2, \quad (1)$$

где $A > 0$ — некоторая константа (константа фрейма). Нас интересует случай $m = n + 1$.

В \mathbb{R}^2 жёсткий фрейм образуют векторы

$$b_1^2 = (0, 1), \quad b_2^2 = \left(-\frac{\sqrt{3}}{2}, -\frac{1}{2}\right), \quad b_3^2 = \left(\frac{\sqrt{3}}{2}, -\frac{1}{2}\right) \quad (2)$$

(верхний индекс указывает на размерность вектора). Для них

$$\sum_{j=1}^3 |\langle x, b_j^2 \rangle|^2 = \frac{3}{2} \|x\|^2.$$

Отметим также, что

$$\sum_{j=1}^3 b_j^2 = \mathbb{O}; \quad \langle b_j^2, b_k^2 \rangle = -\frac{1}{2} \quad \text{при } k \neq j.$$

В [4] жёсткий фрейм (2) назван *фреймом Мерседес-Бенц*. Покажем, что аналогичные фреймы существуют в \mathbb{R}^n при любом $n \geq 2$.

2°. Начнём со вспомогательного утверждения.

ЛЕММА. При $n \geq 2$ в пространстве \mathbb{R}^n можно построить систему из $n + 1$ единичных векторов $\{b_1^n, b_2^n, \dots, b_{n+1}^n\}$ со свойством

$$\langle b_j^n, b_k^n \rangle = -\frac{1}{n} \quad \text{при } k \neq j. \quad (3)$$

Доказательство проведём индукцией по n . При $n = 2$ система (2) обладает требуемым свойством. Сделаем индукционный переход от $n - 1$ к n .

Допустим, что система $\{b_j^{n-1}\}_{j=1}^n$ уже построена. Согласно индукционному предположению

$$\|b_j^{n-1}\| = 1; \quad \langle b_j^{n-1}, b_k^{n-1} \rangle = -\frac{1}{n-1} \quad \text{при } k \neq j. \quad (4)$$

Переходя к построению системы $\{b_j^n\}_{j=1}^{n+1}$, полагаем $b_{n+1}^n = (0, \dots, 0, 1)$. Векторы b_j^n при $j \in 1 : n$ будем искать в виде

$$b_j^n = c_n (b_j^{n-1}, -h_n).$$

Константу c_n выберем из условия нормировки

$$1 = \|b_j^n\|^2 = c_n^2 (1 + h_n^2).$$

Отсюда

$$c_n = \frac{1}{\sqrt{1 + h_n^2}}. \quad (5)$$

За счёт h_n нужно обеспечить выполнение условий (3).

Имеем

$$\langle b_j^n, b_k^n \rangle = \begin{cases} c_n^2 (\langle b_j^{n-1}, b_k^{n-1} \rangle + h_n^2) & \text{при } j, k \in 1 : n, k \neq j; \\ -c_n h_n & \text{при } j \in 1 : n, k = n + 1. \end{cases}$$

На основании (4) приходим к уравнениям

$$c_n^2 \left(h_n^2 - \frac{1}{n-1} \right) = -\frac{1}{n}, \quad c_n h_n = \frac{1}{n}. \quad (6)$$

Из второго уравнения и (5) следует, что $h_n = \frac{1}{\sqrt{n^2-1}}$. При этом $c_n = \frac{\sqrt{n^2-1}}{n}$. Первое равенство в (6) выполняется автоматически!

Лемма доказана. \square

Сумма построенных векторов $b_1^n, b_2^n, \dots, b_{n+1}^n$ равна нулю. Действительно, согласно (3)

$$\begin{aligned} \left\| \sum_{j=1}^{n+1} b_j^n \right\|^2 &= \sum_{j,k} \langle b_j^n, b_k^n \rangle = (n+1) + \sum_{k \neq j} \langle b_j^n, b_k^n \rangle = \\ &= (n+1) - \frac{1}{n} \left[(n+1)^2 - (n+1) \right] = 0. \end{aligned}$$

Более принципиальным является следующее свойство.

ТЕОРЕМА 1. Система векторов $\{b_j^n\}_{j=1}^{n+1}$ образует жёсткий фрейм в \mathbb{R}^n с константой $A = 1 + \frac{1}{n}$.

Доказательство. Рассмотрим первые n векторов b_1^n, \dots, b_n^n . Их матрица Грама G_n с элементами $\langle b_j^n, b_k^n \rangle$ имеет вид

$$G_n = \begin{bmatrix} 1 & -\frac{1}{n} & -\frac{1}{n} & \dots & -\frac{1}{n} \\ -\frac{1}{n} & 1 & -\frac{1}{n} & \dots & -\frac{1}{n} \\ \dots & \dots & \dots & \dots & \dots \\ -\frac{1}{n} & -\frac{1}{n} & -\frac{1}{n} & \dots & 1 \end{bmatrix}.$$

Диагональное преобладание гарантирует невырожденность G_n . Более того, как нетрудно проверить,

$$G_n^{-1} = \frac{n}{n+1} \begin{bmatrix} 2 & 1 & 1 & \dots & 1 \\ 1 & 2 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 2 \end{bmatrix}.$$

Значит, векторы b_1^n, \dots, b_n^n линейно независимы.

Возьмём вектор $x \in \mathbb{R}^n$ и разложим его по базису $\{b_j^n\}_{j=1}^n$:

$$x = \sum_{j=1}^n x_j b_j^n.$$

Для квадрата нормы получим формулу

$$\|x\|^2 = \sum_{j,k} x_j x_k \langle b_j^n, b_k^n \rangle = \sum_{j,k} G_n[j, k] x_j x_k. \quad (7)$$

Вместе с тем,

$$\begin{aligned} \sum_{i=1}^{n+1} |\langle x, b_i^n \rangle|^2 &= \sum_{i=1}^n \left| \sum_{j=1}^n x_j \langle b_j^n, b_i^n \rangle \right|^2 + \\ &+ \left| \sum_{j=1}^n x_j \langle b_j^n, b_{n+1}^n \rangle \right|^2 =: S_1 + S_2. \end{aligned} \quad (8)$$

Преобразуем S_1 и S_2 . Запишем

$$\begin{aligned} S_1 &= \sum_{i=1}^n \sum_{j=1}^n x_j \langle b_j^n, b_i^n \rangle \sum_{k=1}^n x_k \langle b_k^n, b_i^n \rangle = \\ &= \sum_{j,k} x_j x_k \sum_{i=1}^n \langle b_j^n, b_i^n \rangle \langle b_k^n, b_i^n \rangle. \end{aligned}$$

Последнюю сумму (по i) обозначим через d_{jk} . Ясно, что

$$d_{jk} = \begin{cases} 1 + \frac{n-1}{n^2} & \text{при } k = j, \\ -\frac{2}{n} + \frac{n-2}{n^2} & \text{при } k \neq j, \end{cases}$$

или $d_{jk} = (1 + \frac{1}{n}) G_n[j, k] - \frac{1}{n^2}$. Далее

$$S_2 = \frac{1}{n^2} \left| \sum_{j=1}^n x_j \right|^2 = \frac{1}{n^2} \sum_{j,k} x_j x_k.$$

Теперь сложим S_1 и S_2 :

$$S_1 + S_2 = (1 + \frac{1}{n}) \sum_{j,k} G_n[j, k] x_j x_k.$$

Вспоминая формулы (7) и (8), приходим к равенству

$$\sum_{i=1}^{n+1} |\langle x, b_i^n \rangle|^2 = (1 + \frac{1}{n}) \|x\|^2.$$

Теорема доказана. □

Фрейм $\{b_j^n\}_{j=1}^{n+1}$ назовём *фреймом Мерседес-Бенц*.

3°. Систему $\Phi = \{\varphi_1, \varphi_2, \dots, \varphi_{n+1}\}$ единичных n -мерных векторов будем называть *системой Мерседес-Бенц*, если выполняется условие

$$\langle \varphi_j, \varphi_k \rangle = -\frac{1}{n} \quad \text{при } k \neq j. \quad (9)$$

Лемма показывает, что системы Мерседес-Бенц существуют. Более того, любая такая система является жёстким фреймом с константой $A = 1 + \frac{1}{n}$. Это следует из доказательства теоремы 1, в котором использовались только нормированность векторов b_j^n и условие (3).

ТЕОРЕМА 2. Системы Мерседес-Бенц и только они доставляют максимум функционалу

$$S(Z) = \sum_{k \neq j} \|\zeta_j - \zeta_k\|$$

среди всех систем $Z = \{\zeta_1, \zeta_2, \dots, \zeta_{n+1}\}$ единичных n -мерных векторов.

Доказательство. Возьмём систему Мерседес-Бенц $\Phi = \{\varphi_1, \varphi_2, \dots, \varphi_{n+1}\}$ и обозначим $s_{jk} = \|\varphi_j - \varphi_k\|$. Согласно (9) при $k \neq j$ имеем

$$s_{jk}^2 = 2 - 2 \langle \varphi_j, \varphi_k \rangle = 2 \left(1 + \frac{1}{n}\right).$$

Количество s_{jk} при $k \neq j$ равно $(n+1)^2 - (n+1) = n(n+1)$, поэтому

$$S(\Phi) = n(n+1) \sqrt{2 \left(1 + \frac{1}{n}\right)} = (n+1) \sqrt{2n(n+1)}.$$

Отметим, что правая часть последнего равенства одинакова для всех систем Мерседес-Бенц.

Теперь нужно показать, что

$$S(Z) < (n+1) \sqrt{2n(n+1)}$$

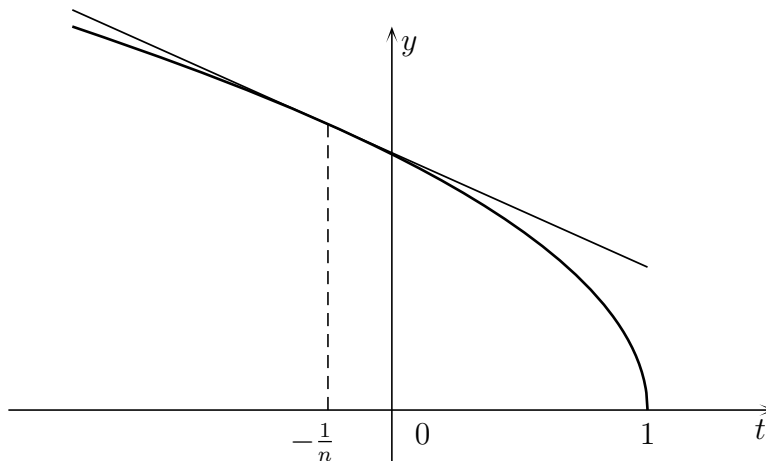
для любой системы $Z = \{\zeta_1, \zeta_2, \dots, \zeta_{n+1}\}$ единичных n -мерных векторов, у которой хотя бы одно скалярное произведение $\langle \zeta_j, \zeta_k \rangle$ при $k \neq j$ отлично от $-\frac{1}{n}$.

Воспользуемся идеей из [5]. Запишем

$$\|\zeta_j - \zeta_k\| = \sqrt{2} y(\langle \zeta_j, \zeta_k \rangle),$$

где $y(t) = \sqrt{1-t}$. Поскольку $y''(t) < 0$ при $t < 1$, то функция $y(t)$ строго вогнута на $(-\infty, 1]$. Проведём касательную в точке $t_0 = -\frac{1}{n}$ (см. рис.):

$$h(t) = y\left(-\frac{1}{n}\right) + y'\left(-\frac{1}{n}\right) \left(t + \frac{1}{n}\right).$$



Тогда $y(t) < h(t)$ при всех $t \leq 1$, $t \neq -\frac{1}{n}$. Как следствие при $k \neq j$ получаем

$$\|\zeta_j - \zeta_k\| \leq \sqrt{2} h(\langle \zeta_j, \zeta_k \rangle),$$

причём хотя бы один раз неравенство выполняется как строгое. Складывая, приходим к строгому неравенству

$$S(Z) < \sqrt{2} \sum_{k \neq j} h(\langle \zeta_j, \zeta_k \rangle).$$

Далее

$$h(t) = \sqrt{\frac{n+1}{n}} - \frac{1}{2} \sqrt{\frac{n}{n+1}} \left(t + \frac{1}{n}\right) = \frac{2n+1}{2\sqrt{n(n+1)}} - \frac{\sqrt{n}}{2\sqrt{n+1}} t,$$

поэтому

$$S(Z) < \frac{\sqrt{2}}{2} \left\{ (2n+1) \sqrt{n(n+1)} - \frac{\sqrt{n}}{\sqrt{n+1}} \sum_{k \neq j} \langle \zeta_j, \zeta_k \rangle \right\}. \quad (10)$$

Остаётся учесть, что

$$\begin{aligned} \sum_{k \neq j} \langle \zeta_j, \zeta_k \rangle &= \sum_{j=1}^{n+1} \sum_{k=1}^{n+1} \langle \zeta_j, \zeta_k \rangle - \sum_{j=1}^{n+1} \langle \zeta_j, \zeta_j \rangle = \\ &= \left\| \sum_{j=1}^{n+1} \zeta_j \right\|^2 - (n+1). \end{aligned}$$

Подставив это в (10), окончательно получим

$$\begin{aligned} S(Z) &< \frac{\sqrt{2}}{2} \left\{ (2n+2) \sqrt{n(n+1)} - \frac{\sqrt{n}}{\sqrt{n+1}} \left\| \sum_{j=1}^{n+1} \zeta_j \right\|^2 \right\} \leq \\ &\leq (n+1) \sqrt{2n(n+1)}. \end{aligned}$$

Теорема доказана. □

ЛИТЕРАТУРА

1. Певный А. Б., Истомина М. Н. *Фрейм Мерседес-Бенц в n -мерном пространстве* // Вестник СыктГУ. Сер. 1. Вып. 6. 2006. С. 219–222.
2. Истомина М. Н., Певный А. Б. *О расположении точек на сфере и фрейме Мерседес-Бенц* // Матем. просвещение. Сер. 3. Вып. 11. 2007. С. 105–112.
3. Добеши И. *Десять лекций по вейвлетам*. Пер. с англ. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.
4. Casazza P., Kovačević J. *Equal-norm tight frames with erasures* // Advances in Comp. Math. (Special issue on frames). 2002. P. 387–430.
5. Андреев Н. Н., Юдин В. А. *Экстремальные расположения точек на сфере* // Матем. просвещение. Сер. 3. Вып. 1. 1997. С. 115–121.

БИКУБИЧЕСКИЕ ПОВЕРХНОСТИ КУНСА

В. Н. Малозёмов

Н. В. Чашников

23 января 2007 г.

1°. Пусть заданы непрерывно дифференцируемые на отрезке $[0, 1]$ функции

$$\begin{aligned} f_1(v), f_2(v), f_3(v), f_4(v), \\ g_1(u), g_2(u), g_3(u), g_4(u). \end{aligned}$$

Обозначим $D = [0, 1]^2$. Ставится задача: *построить возможно более простую функцию $a : D \rightarrow \mathbb{R}$, удовлетворяющую граничным условиям*

$$\begin{aligned} a(0, v) \equiv f_1(v), \quad a_u(0, v) \equiv f_2(v), \quad a_u(1, v) \equiv f_3(v), \quad a(1, v) \equiv f_4(v), \\ a(u, 0) \equiv g_1(u), \quad a_v(u, 0) \equiv g_2(u), \quad a_v(u, 1) \equiv g_3(u), \quad a(u, 1) \equiv g_4(u). \end{aligned} \quad (1)$$

Введём на $C^1[0, 1]$ линейные (однородные и аддитивные) функционалы

$$L_1(f) = f(0), \quad L_2(f) = f'(0), \quad L_3(f) = f'(1), \quad L_4(f) = f(1).$$

Функционалы L_i можно применять и к непрерывно дифференцируемым функциям двух переменных, заданным на D , если фиксировать один из аргументов. Пусть $a \in C^1(D)$. Тогда $a(\cdot, v)$ есть функция первого аргумента при фиксированном втором, $a(u, \cdot)$ — функция второго аргумента при фиксированном первом и

$$\begin{aligned} L_1(a(\cdot, v)) &= a(0, v), & L_1(a(u, \cdot)) &= a(u, 0), \\ L_2(a(\cdot, v)) &= a_u(0, v), & L_2(a(u, \cdot)) &= a_v(u, 0), \\ L_3(a(\cdot, v)) &= a_u(1, v), & L_3(a(u, \cdot)) &= a_v(u, 1), \\ L_4(a(\cdot, v)) &= a(1, v), & L_4(a(u, \cdot)) &= a(u, 1). \end{aligned}$$

С использованием функционалов L_i граничные условия (1) можно переписать в виде

$$\begin{aligned} L_i(a(\cdot, v)) &= f_i(v), & v &\in [0, 1], \quad i \in 1 : 4; \\ L_j(a(u, \cdot)) &= g_j(u), & u &\in [0, 1], \quad j \in 1 : 4. \end{aligned} \quad (2)$$

2°. Граничные функции f_i, g_j должны удовлетворять естественным условиям согласования в вершинах квадрата D :

$$\begin{aligned} f_1(0) &= g_1(0), & f_1(1) &= g_4(0), & f_4(1) &= g_4(1), & f_4(0) &= g_1(1), \\ f'_1(0) &= g_2(0), & f'_1(1) &= g_3(0), & f'_4(1) &= g_3(1), & f'_4(0) &= g_2(1), \\ f_2(0) &= g'_1(0), & f_2(1) &= g'_4(0), & f_3(1) &= g'_4(1), & f_3(0) &= g'_1(1). \end{aligned}$$

Функция $a \in C^1(D)$, которую мы построим, будет иметь непрерывные на D смешанные производные a_{uv} и a_{vu} , которые, как известно, должны быть равны между собой [1, с. 456]. В частности, $a_{uv} = a_{vu}$ в вершинах квадрата D . Это приводит к дополнительным условиям согласования

$$f'_2(0) = g'_2(0), \quad f'_2(1) = g'_3(0), \quad f'_3(1) = g'_3(1), \quad f'_3(0) = g'_2(1).$$

Замечательно, что все 16 условий согласования можно записать единообразно:

$$L_i(f_j) = L_j(g_i), \quad i, j \in 1 : 4. \quad (3)$$

Формула (3) допускает матричное представление

$$\begin{bmatrix} f_1(0) & f_2(0) & f_3(0) & f_4(0) \\ f'_1(0) & f'_2(0) & f'_3(0) & f'_4(0) \\ f'_1(1) & f'_2(1) & f'_3(1) & f'_4(1) \\ f_1(1) & f_2(1) & f_3(1) & f_4(1) \end{bmatrix} = \begin{bmatrix} g_1(0) & g'_1(0) & g'_1(1) & g_1(1) \\ g_2(0) & g'_2(0) & g'_2(1) & g_2(1) \\ g_3(0) & g'_3(0) & g'_3(1) & g_3(1) \\ g_4(0) & g'_4(0) & g'_4(1) & g_4(1) \end{bmatrix}. \quad (4)$$

3°. Введём кубические полиномы Эрмита H_1, H_2, H_3, H_4 , исходя из интерполяционных условий

$$\begin{aligned} H_1(0) &= 1, & H'_1(0) &= 0, & H'_1(1) &= 0, & H_1(1) &= 0; \\ H_2(0) &= 0, & H'_2(0) &= 1, & H'_2(1) &= 0, & H_2(1) &= 0; \\ H_3(0) &= 0, & H'_3(0) &= 0, & H'_3(1) &= 1, & H_3(1) &= 0; \\ H_4(0) &= 0, & H'_4(0) &= 0, & H'_4(1) &= 0, & H_4(1) &= 1. \end{aligned} \quad (5)$$

Нетрудно проверить, что

$$\begin{aligned} H_1(x) &= 2x^3 - 3x^2 + 1, \\ H_2(x) &= x^3 - 2x^2 + x, \\ H_3(x) &= x^3 - x^2, \\ H_4(x) &= -2x^3 + 3x^2. \end{aligned}$$

Графики этих полиномов представлены на рис. 1.

Отметим, что условия (5) можно записать в компактном виде

$$L_i(H_j) = \delta_{ij}, \quad i, j \in 1 : 4, \quad (6)$$

где δ_{ij} — символ Кронекера.

В качестве H_j могут быть взяты любые другие непрерывно дифференцируемые функции, удовлетворяющие условиям (6).

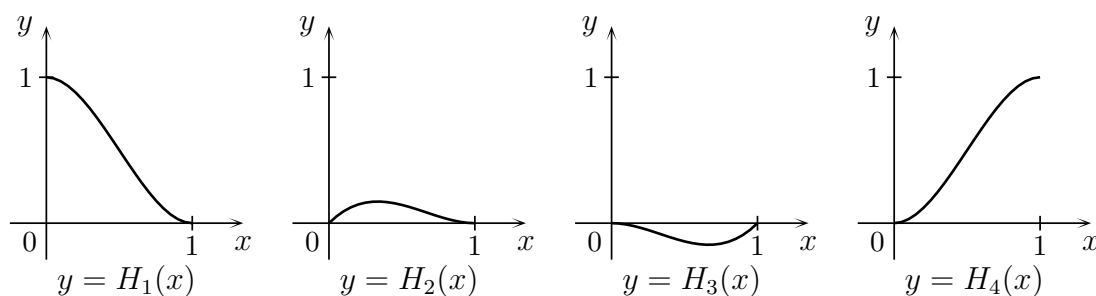


Рис. 1. Графики кубических полиномов Эрмита.

4°. Положим

$$a(u, v) = \sum_{i=1}^4 f_i(v) H_i(u) + \sum_{j=1}^4 g_j(u) H_j(v) - \sum_{i=1}^4 \sum_{j=1}^4 L_i(g_j) H_i(u) H_j(v). \quad (7)$$

Очевидно, что $a \in C^1(D)$ и существуют непрерывные на D смешанные производные a_{uv} и a_{vu} .

ПРЕДЛОЖЕНИЕ 1. При выполнении условий согласования (3) функция $a(u, v)$ вида (7) удовлетворяет граничным условиям (2).

Доказательство. Согласно линейности функционалов L_k и формуле (6) при $k \in 1 : 4$ имеем

$$\begin{aligned} L_k(a(\cdot, v)) &= \sum_{i=1}^4 f_i(v) L_k(H_i) + \sum_{j=1}^4 L_k(g_j) H_j(v) - \\ &- \sum_{i=1}^4 \sum_{j=1}^4 L_i(g_j) H_j(v) L_k(H_i) = f_k(v). \end{aligned}$$

Аналогично с учётом (3) получаем

$$\begin{aligned} L_k(a(u, \cdot)) &= \sum_{i=1}^4 L_k(f_i) H_i(u) + \sum_{j=1}^4 g_j(u) L_k(H_j) - \\ &- \sum_{i=1}^4 \sum_{j=1}^4 L_j(f_i) H_i(u) L_k(H_j) = g_k(u). \end{aligned}$$

Предложение доказано. □

График функции $a(u, v)$ вида (7) на множестве D называется *бикубической поверхностью Кунса*.

ПРИМЕР 1. Пусть

$$f_1(v) \equiv 0, \quad f_4(v) \equiv 0, \quad g_1(u) \equiv 0, \quad g_4(u) \equiv 0.$$

Функции $f_2(v)$ и $f_3(v)$ будут многочленами, кратными $v(1-v)$, а функции $g_2(u)$ и $g_3(u)$ — многочленами, кратными $u(1-u)$. В этом случае 12 из 16 условий согласования (4), в которых участвуют внешние строки и столбцы матрицы, будут выполнены. Остаётся обеспечить равенства

$$f'_2(0) = g'_2(0), \quad f'_2(1) = g'_3(0), \quad f'_3(0) = g'_2(1), \quad f'_3(1) = g'_3(1). \quad (8)$$

Положим

$$\begin{aligned} f_2(v) &= a v(1-v), & f_3(v) &= b v(1-v)(5v-1), \\ g_2(u) &= c u(1-u), & g_3(u) &= d u(1-u)(5u-1). \end{aligned}$$

Условия (8) выполняются, если $a = b = c = d$. Возьмём в качестве общего значения этих коэффициентов число 10.

Теперь корректно определены все граничные функции. Соответствующая бикубическая поверхность Кунса представлена на рис. 2.

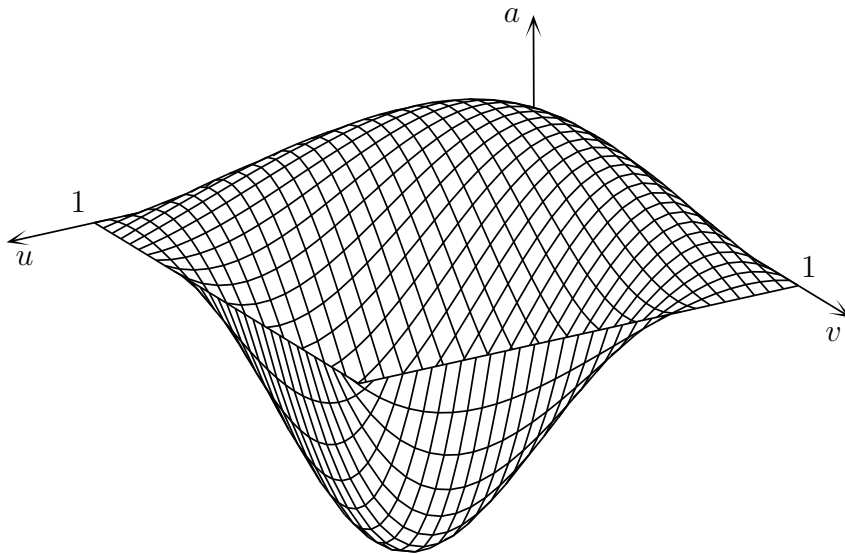


Рис. 2. Бикубическая поверхность Кунса.

5°. Перейдём к случаю, когда f_i и g_j в формуле (7) суть трёхмерные вектор-функции, заданные на отрезке $[0, 1]$, т. е.

$$f_i(v) = (f_{i1}(v), f_{i2}(v), f_{i3}(v)), \quad g_j(u) = (g_{j1}(u), g_{j2}(u), g_{j3}(u)), \quad i, j \in 1:4.$$

При этом $L_k(f_i) = (L_k(f_{i1}), L_k(f_{i2}), L_k(f_{i3}))$. Аналогично определяется $L_k(g_j)$. Поскольку

$$f_i(v)H_j(u) = (f_{i1}(v)H_j(u), f_{i2}(v)H_j(u), f_{i3}(v)H_j(u)),$$

то

$$L_k(f_i(v)H_j(\cdot)) = (f_{i1}(v)L_k(H_j), f_{i2}(v)L_k(H_j), f_{i3}(v)L_k(H_j)) = f_i(v)\delta_{kj}.$$

Пусть вектор-функции f_i и g_j непрерывно дифференцируемы на $[0, 1]$ и выполнены условия согласования

$$L_i(f_j) = L_j(g_i), \quad i, j \in 1 : 4.$$

Тогда отображение $a : D \rightarrow \mathbb{R}^3$ вида (7) определяет *параметрическую поверхность Кунса*, удовлетворяющую граничным условиям (2).

ПРИМЕР 2. Возьмём в качестве H_j следующие функции:

$$\begin{aligned} H_1(x) &= \cos^2 \frac{\pi x}{2}, & H_2(x) &= \frac{2}{\pi} \left(\sin \frac{\pi x}{2} - \sin^2 \frac{\pi x}{2} \right), \\ H_3(x) &= -\frac{2}{\pi} \left(\cos \frac{\pi x}{2} - \cos^2 \frac{\pi x}{2} \right), & H_4(x) &= \sin^2 \frac{\pi x}{2}. \end{aligned}$$

Нетрудно проверить, что для таких H_j выполнены условия (6).

Построим с помощью параметрической поверхности Кунса поверхность тора. Она будет состоять из четырёх порций. Определим граничные вектор-функции для основной порции. Положим

$$\begin{aligned} f_1(v) &= (2 + \cos \pi v, 0, \sin \pi v), & f_4(v) &= (-2 - \cos \pi v, 0, \sin \pi v), \\ g_1(u) &= (3 \cos \pi u, 3 \sin \pi u, 0), & g_4(u) &= (\cos \pi u, \sin \pi u, 0). \end{aligned}$$

Функции $f_1(v)$ и $f_4(v)$ задают полуокружности радиуса 1, лежащие в плоскости XZ , с центрами $(2, 0, 0)$ и $(-2, 0, 0)$ соответственно. Функции $g_1(u)$ и $g_4(u)$ задают полуокружности с центром в начале координат и радиусами 3 и 1 соответственно, лежащие в плоскости XY (рис. 3).

Функции $g_2(u)$ и $g_3(u)$ определяют значения производной по v в точках поверхности с $v = 0$ и $v = 1$, т. е. на кривых, задаваемых функциями $g_1(u)$ и $g_4(u)$. Для построения поверхности тора необходимо, чтобы векторы $g_2(u)$ и $g_3(u)$ были параллельны оси OZ . Кроме того, для выполнения условий согласования требуется, чтобы

$$\begin{aligned} g_2(0) &= f'_1(0) = (0, 0, \pi), & g_2(1) &= f'_4(0) = (0, 0, \pi), \\ g_3(0) &= f'_1(1) = (0, 0, -\pi), & g_3(1) &= f'_4(1) = (0, 0, -\pi). \end{aligned}$$

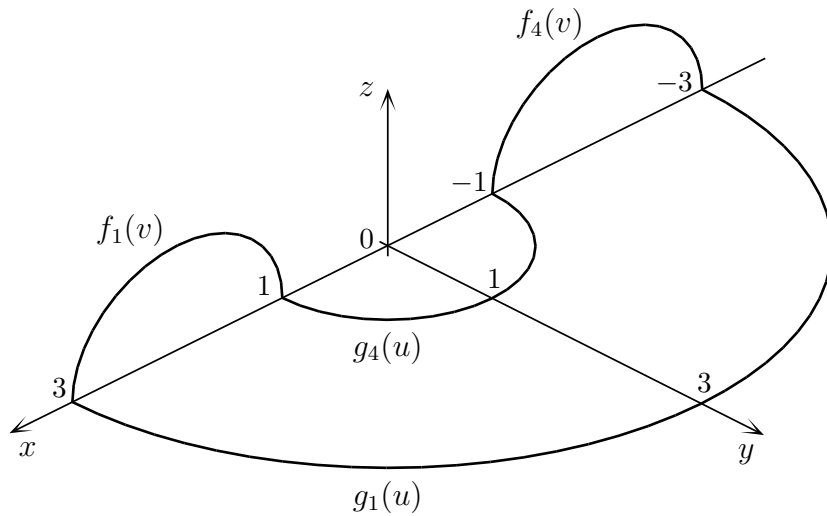


Рис. 3. Граничные функции.

Положим

$$g_2(u) = (0, 0, \pi), \quad g_3(u) = (0, 0, -\pi).$$

Аналогично функции $f_2(v)$ и $f_3(v)$ задают производные по u в точках поверхности, лежащих на кривых $f_1(v)$ и $f_4(v)$, поэтому для построения поверхности тора необходимо, чтобы векторы $f_2(v)$ и $f_3(v)$ были параллельны оси OY . Кроме того, для выполнения условий согласования требуется, чтобы

$$\begin{aligned} f_2(0) = g'_1(0) &= (0, 3\pi, 0), & f'_2(0) = g'_2(0) &= (0, 0, 0), \\ f'_2(1) = g'_3(0) &= (0, 0, 0), & f_2(1) = g'_4(0) &= (0, \pi, 0). \end{aligned}$$

Можно положить, например, $f_2(v) = (0, \pi(2 + \cos \pi v), 0)$. По аналогичным соображениям полагаем $f_3(v) = (0, -\pi(2 + \cos \pi v), 0)$.

Итак, граничные вектор-функции выглядят следующим образом:

$$\begin{aligned} f_1(v) &= (2 + \cos \pi v, 0, \sin \pi v), & f_2(v) &= (0, \pi(2 + \cos \pi v), 0), \\ f_3(v) &= (0, -\pi(2 + \cos \pi v), 0), & f_4(v) &= (-2 - \cos \pi v, 0, \sin \pi v), \\ g_1(u) &= (3 \cos \pi u, 3 \sin \pi u, 0), & g_2(u) &= (0, 0, \pi), \\ g_3(u) &= (0, 0, -\pi), & g_4(u) &= (\cos \pi u, \sin \pi u, 0). \end{aligned} \tag{9}$$

Все 16 условий согласования выполнены. По формуле (7) для граничных функций (9) получим вектор-функцию $a(u, v) = (a_1(u, v), a_2(u, v), a_3(u, v))$. Параметрическая поверхность Кунса, определяемая этой вектор-функцией, изображена на рис. 4.

Докажем, что вектор-функция $a(u, v)$ при $u, v \in [0, 1]$ действительно описывает четверть поверхности тора.

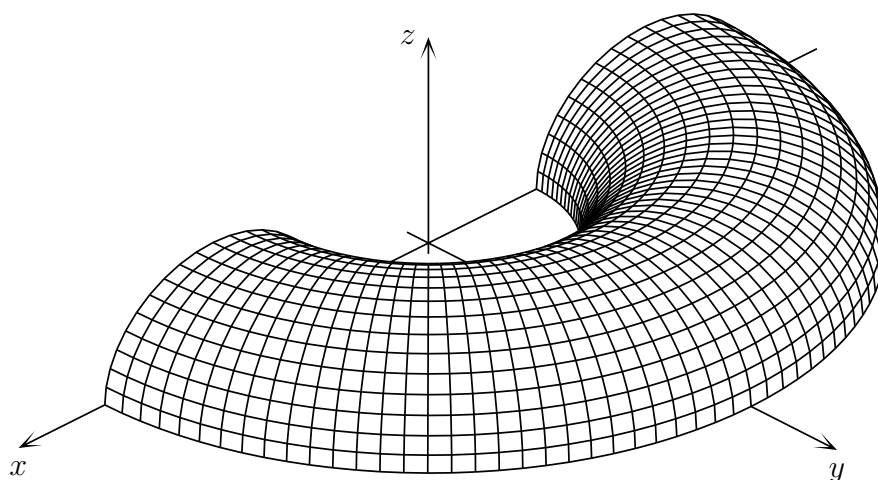


Рис. 4. Параметрическая поверхность Кунса.

Значения $L_i(g_j)$, используемые в формуле (7), образуют матрицу

$$\begin{bmatrix} g_1(0) & g'_1(0) & g'_1(1) & g_1(1) \\ g_2(0) & g'_2(0) & g'_2(1) & g_2(1) \\ g_3(0) & g'_3(0) & g'_3(1) & g_3(1) \\ g_4(0) & g'_4(0) & g'_4(1) & g_4(1) \end{bmatrix} = \begin{bmatrix} (3, 0, 0) & (0, 3\pi, 0) & (0, -3\pi, 0) & (-3, 0, 0) \\ (0, 0, \pi) & (0, 0, 0) & (0, 0, 0) & (0, 0, \pi) \\ (0, 0, -\pi) & (0, 0, 0) & (0, 0, 0) & (0, 0, -\pi) \\ (1, 0, 0) & (0, \pi, 0) & (0, -\pi, 0) & (-1, 0, 0) \end{bmatrix}$$

(индекс j обозначает номер строки, а индекс i — номер столбца). Базисные функции H_1 и H_4 удовлетворяют соотношениям

$$H_1(u) - H_4(u) = \cos \pi u, \quad 3H_1(v) + H_4(v) = 2 + \cos \pi v, \quad H_1(u) + H_4(u) \equiv 1.$$

Приняв эти факты во внимание, запишем

$$\begin{aligned} a_1(u, v) &= (2 + \cos \pi v)(H_1(u) - H_4(u)) + \cos \pi u (3H_1(v) + H_4(v)) - \\ &\quad - 3(H_1(u) - H_4(u))H_1(v) - (H_1(u) - H_4(u))H_4(v) = \\ &= \cos \pi u (2 + \cos \pi v) + (H_1(u) - H_4(u)) \times \\ &\quad \times [2 + \cos \pi v - (3H_1(v) + H_4(v))] = \cos \pi u (2 + \cos \pi v), \\ a_2(u, v) &= \pi (2 + \cos \pi v)(H_2(u) - H_3(u)) + \sin \pi u (3H_1(v) + H_4(v)) - \\ &\quad - 3\pi (H_2(u) - H_3(u))H_1(v) - \pi (H_2(u) - H_3(u))H_4(v) = \\ &= \sin \pi u (2 + \cos \pi v) + \pi (H_2(u) - H_3(u)) \times \\ &\quad \times [2 + \cos \pi v - (3H_1(v) + H_4(v))] = \sin \pi u (2 + \cos \pi v), \\ a_3(u, v) &= \sin \pi v (H_1(u) + H_4(u)) + \pi (H_2(v) - H_3(v)) - \\ &\quad - \pi (H_1(u) + H_4(u))H_2(v) + \pi (H_1(u) + H_4(u))H_3(v) = \\ &= \sin \pi v + \pi (H_2(v) - H_3(v)) [1 - (H_1(v) + H_4(v))] = \sin \pi v. \end{aligned}$$

Значит,

$$a(u, v) = ((2 + \cos \pi v) \cos \pi u, (2 + \cos \pi v) \sin \pi u, \sin \pi v).$$

Отсюда видно, что точка $a(u, v)$ получается из точки

$$(2 + \cos \pi v, 0, \sin \pi v) = f_1(v)$$

поворотом на угол πu вокруг оси OZ . Как следствие, поверхность, задаваемая вектор-функцией $a(u, v)$, получается вращением вокруг оси OZ полуокружности, определяемой вектор-функцией $f_1(v)$. Эта поверхность является четвертью поверхности тора (см. рис. 4). На рис. 5 из четырёх таких порций составлена полная поверхность тора.

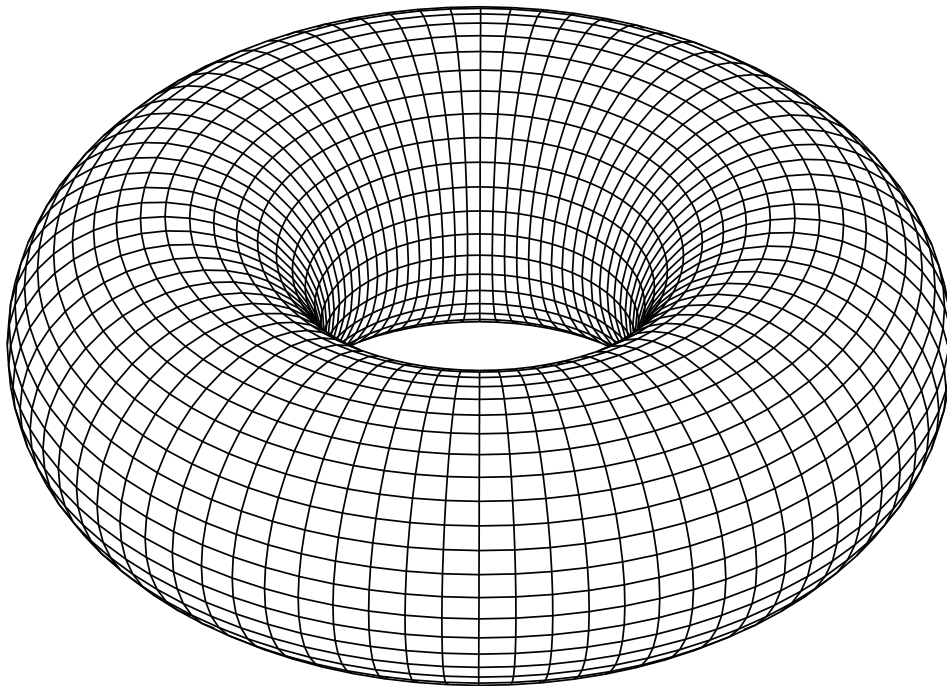


Рис. 5. Поверхность тора.

6°. Дальнейшую информацию о поверхностях Кунса можно найти в книге [2] и приведённом там списке литературы.

ЛИТЕРАТУРА

1. Г. М. Фихтенгольц. *Курс дифференциального и интегрального исчисления*. Том 1. 8-е изд. М.: Физматлит, 2006.
2. G. Farin. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.

СОСТАВНЫЕ ПАРАМЕТРИЧЕСКИЕ ПОВЕРХНОСТИ КУНСА

Н. В. Чашников

10 февраля 2007 г.

1°. Мы будем использовать следующие обозначения из [1].

L_1, L_2, L_3, L_4 — линейные операторы, определяемые для непрерывно дифференцируемых вектор-функций $f : [0, 1] \rightarrow \mathbb{R}^3$ следующим образом:

$$L_1(f) = f(0), \quad L_2(f) = f'(0), \quad L_3(f) = f'(1), \quad L_4(f) = f(1).$$

H_1, H_2, H_3, H_4 — непрерывно дифференцируемые на отрезке $[0, 1]$ функции, удовлетворяющие соотношениям

$$\begin{aligned} H_1(0) &= 1, & H_1'(0) &= 0, & H_1'(1) &= 0, & H_1(1) &= 0; \\ H_2(0) &= 0, & H_2'(0) &= 1, & H_2'(1) &= 0, & H_2(1) &= 0; \\ H_3(0) &= 0, & H_3'(0) &= 0, & H_3'(1) &= 1, & H_3(1) &= 0; \\ H_4(0) &= 0, & H_4'(0) &= 0, & H_4'(1) &= 0, & H_4(1) &= 1. \end{aligned} \tag{1}$$

В качестве H_i могут быть использованы кубические полиномы Эрмита:

$$\begin{aligned} H_1(x) &= 2x^3 - 3x^2 + 1, \\ H_2(x) &= x^3 - 2x^2 + x, \\ H_3(x) &= x^3 - x^2, \\ H_4(x) &= -2x^3 + 3x^2. \end{aligned}$$

В [1] доказано, что если вектор-функции $f_i, g_i : [0, 1] \rightarrow \mathbb{R}^3$, $i \in 1 : 4$ удовлетворяют условиям

$$L_j(f_i) = L_i(g_j), \quad i, j \in 1 : 4, \tag{2}$$

то поверхность, задаваемая вектор-функцией

$$c(u, v) = \sum_{i=1}^4 H_i(u) f_i(v) + \sum_{j=1}^4 H_j(v) g_j(u) - \sum_{i=1}^4 \sum_{j=1}^4 H_i(u) H_j(v) L_i(g_j), \tag{3}$$

будет удовлетворять условиям

$$\begin{aligned} L_i(c(\cdot, v)) &= f_i(v), & v \in [0, 1], & i \in 1 : 4; \\ L_j(c(u, \cdot)) &= g_j(u), & u \in [0, 1], & j \in 1 : 4. \end{aligned} \quad (4)$$

2°. Пусть заданы два набора кривых

$$a_i : [0, n] \rightarrow \mathbb{R}^3, \quad i \in 0 : m, \quad b_j : [0, m] \rightarrow \mathbb{R}^3, \quad j \in 0 : n,$$

причём $a_i \in C^1([0, n])$, $b_j \in C^1([0, m])$, и кривые пересекаются в соответствующих точках:

$$a_i(j) = b_j(i) \quad \forall i \in 0 : m, \quad j \in 0 : n. \quad (5)$$

Кроме того, пусть заданы векторы $d_{ij} \in \mathbb{R}^3$, $i \in 0 : m$, $j \in 0 : n$. Покажем как построить поверхность, натянутую на кривые a_i , b_j .

ПРЕДЛОЖЕНИЕ. *Существует поверхность, задаваемая вектор-функцией $s : [0, m] \times [0, n] \rightarrow \mathbb{R}^3$, которая удовлетворяет следующим условиям:*

- 1) $s = s(\alpha, \beta)$, $s \in C^1$, $s_{\alpha\beta}, s_{\beta\alpha} \in C$;
- 2) $s(i, \beta) = a_i(\beta)$, $\forall i \in 0 : m$, $\beta \in [0, n]$;
- 3) $s(\alpha, j) = b_j(\alpha)$, $\forall j \in 0 : n$, $\alpha \in [0, m]$;
- 4) $s_{\alpha\beta}(i, j) = d_{ij}$, $\forall i \in 0 : m$, $j \in 0 : n$.

Доказательство. Будем строить требуемую поверхность путём соединения параметрических поверхностей Кунса для участков $[i, i+1] \times [j, j+1]$.

Для каждого $i \in 0 : m$ определим вектор-функцию $A_i(\beta)$, положив для β из отрезка $[j, j+1]$, $j \in 0 : n-1$,

$$A_i(\beta) = H_1(\beta - j) b'_j(i) + H_2(\beta - j) d_{ij} + H_3(\beta - j) d_{i,j+1} + H_4(\beta - j) b'_{j+1}(i).$$

Из (1) следует, что

$$A_i(j) = b'_j(i), \quad A'_i(j) = d_{ij} \quad \forall i \in 0 : m, \quad j \in 0 : n, \quad (6)$$

причём эти равенства получаются как по формуле для отрезка $[j-1, j]$, так и по формуле для отрезка $[j, j+1]$. Таким образом, $A_i \in C^1([0, n])$.

Аналогично, для каждого $j \in 0 : n$ определим вектор-функцию $B_j(\alpha)$:

$$\begin{aligned} B_j(\alpha) &= H_1(\alpha - i) a'_i(j) + H_2(\alpha - i) d_{ij} + H_3(\alpha - i) d_{i+1,j} + H_4(\alpha - i) a'_{i+1}(j), \\ &\alpha \in [i, i+1], \quad i \in 0 : m-1. \end{aligned}$$

Как и в предыдущем случае, выполнено

$$B_j(i) = a'_i(j), \quad B'_j(i) = d_{ij} \quad \forall i \in 0 : m, \quad j \in 0 : n, \quad (7)$$

и $B_j \in C^1([0, m])$.

Зафиксируем $i \in 0 : m - 1, j \in 0 : n - 1$ и положим

$$\begin{aligned} f_1(v) &= a_i(j + v), \quad f_2(v) = A_i(j + v), \quad f_3(v) = A_{i+1}(j + v), \quad f_4(v) = a_{i+1}(j + v), \\ g_1(u) &= b_j(i + u), \quad g_2(u) = B_j(i + u), \quad g_3(u) = B_{j+1}(i + u), \quad g_4(u) = b_{j+1}(i + u). \end{aligned}$$

Покажем, что f_k, g_l удовлетворяют условиям (2). Согласно (5), имеем

$$\begin{aligned} L_1(g_1) &= b_j(i) = a_i(j) = L_1(f_1), \\ L_4(g_1) &= b_j(i + 1) = a_{i+1}(j) = L_1(f_4), \\ L_1(g_4) &= b_{j+1}(i) = a_i(j + 1) = L_4(f_1), \\ L_4(g_4) &= b_{j+1}(i + 1) = a_{i+1}(j + 1) = L_4(f_4). \end{aligned}$$

Используя (6) и (7), последовательно получаем

$$\begin{aligned} L_1(g_2) &= B_j(i) = a'_i(j) = L_2(f_1), \\ L_1(g_3) &= B_{j+1}(i) = a'_i(j + 1) = L_3(f_1), \\ L_4(g_2) &= B_j(i + 1) = a'_{i+1}(j) = L_2(f_4), \\ L_4(g_3) &= B_{j+1}(i + 1) = a'_{i+1}(j + 1) = L_3(f_4), \\ L_2(g_1) &= b'_j(i) = A_i(j) = L_1(f_2), \\ L_2(g_4) &= b'_{j+1}(i) = A_i(j + 1) = L_4(f_2), \\ L_3(g_1) &= b'_j(i + 1) = A_{i+1}(j) = L_1(f_3), \\ L_3(g_4) &= b'_{j+1}(i + 1) = A_{i+1}(j + 1) = L_4(f_3), \\ L_2(g_2) &= B'_j(i) = d_{ij} = A'_i(j) = L_2(f_2), \\ L_2(g_3) &= B'_{j+1}(i) = d_{i,j+1} = A'_i(j + 1) = L_3(f_2), \\ L_3(g_2) &= B'_j(i + 1) = d_{i+1,j} = A'_{i+1}(j) = L_2(f_3), \\ L_3(g_3) &= B'_{j+1}(i + 1) = d_{i+1,j+1} = A'_{i+1}(j + 1) = L_3(f_3). \end{aligned}$$

Итак, условия (2) выполнены. По формуле (3) построим вектор-функцию c^{ij} , задающую параметрическую поверхность Кунса.

Определим теперь вектор-функцию $s(\alpha, \beta)$ на $[0, m] \times [0, n]$. Пусть

$$s(\alpha, \beta) = c^{ij}(\alpha - i, \beta - j),$$

где

$$i = \begin{cases} \lfloor \alpha \rfloor, & \text{если } \alpha < m, \\ m - 1, & \text{если } \alpha = m, \end{cases} \quad j = \begin{cases} \lfloor \beta \rfloor, & \text{если } \beta < n, \\ n - 1, & \text{если } \beta = n. \end{cases}$$

Проверим, что для s выполнены условия 1–4 из формулировки предложения.

Так как c^{ij} задаёт поверхность Кунса, то для неё выполнены условия (4), то есть

$$\begin{aligned} c^{ij}(0, v) &= a_i(j + v), & c^{ij}(1, v) &= a_{i+1}(j + v) & \forall v \in [0, 1], \\ c^{ij}(u, 0) &= b_j(i + u), & c^{ij}(u, 1) &= b_{j+1}(i + u) & \forall u \in [0, 1]. \end{aligned}$$

Отсюда сразу видно, что s непрерывна и выполнены условия 2 и 3. Кроме того, из (4) для c^{ij} следует, что

$$\begin{aligned} c_u^{ij}(0, v) &= A_i(j + v), & c_u^{ij}(1, v) &= A_{i+1}(j + v) & \forall v \in [0, 1], \\ c_v^{ij}(u, 0) &= B_j(i + u), & c_v^{ij}(u, 1) &= B_{j+1}(i + u) & \forall u \in [0, 1]. \end{aligned}$$

Докажем теперь непрерывность s_α , s_β , $s_{\alpha\beta}$, $s_{\beta\alpha}$. Достаточно проверить непрерывность для тех точек $(\alpha, \beta) \in (0, m) \times (0, n)$, в которых стыкуются разные поверхности Кунса, то есть либо β , либо α — целое число. Предположим для определённости, что α — целое, то есть $\alpha = i \in 1 : m - 1$. Пусть $j = \lfloor \beta \rfloor$. Тогда

$$\begin{aligned} s_\alpha(i - 0, \beta) &= c_u^{i-1, j}(1, \beta - j) = A_i(\beta) = c_u^{ij}(0, \beta - j) = s_\alpha(i + 0, \beta), \\ s_\beta(i - 0, \beta) &= c_v^{i-1, j}(1, \beta - j) = A'_i(\beta) = c_v^{ij}(0, \beta - j) = s_\beta(i + 0, \beta), \\ s_{\alpha\beta}(i - 0, \beta) &= c_{uv}^{i-1, j}(1, \beta - j) = A'_i(\beta) = c_{uv}^{ij}(0, \beta - j) = s_{\alpha\beta}(i + 0, \beta), \\ s_{\beta\alpha}(i - 0, \beta) &= c_{vu}^{i-1, j}(1, \beta - j) = c_{uv}^{i-1, j}(1, \beta - j) = A'_i(\beta) = \\ &= c_{uv}^{ij}(0, \beta - j) = c_{vu}^{ij}(0, \beta - j) = s_{\beta\alpha}(i + 0, \beta). \end{aligned}$$

Таким образом, s_α , s_β , $s_{\alpha\beta}$ и $s_{\beta\alpha}$ непрерывны на $[0, m] \times [0, n]$. Кроме того, поскольку $s_{\alpha\beta}(i, j) = A'_i(j) = d_{ij}$, то выполнено условие 4.

Итак, для построенной вектор-функции s выполнены условия 1–4, что и требовалось доказать. \square

З а м е ч а н и е. Векторы d_{ij} , участвующие в построении составной поверхности Кунса, можно выбирать различными способами. В частности, можно положить $d_{ij} = 0$, но в таком случае на поверхности возможно появление нежелательных участков уплощения. Чтобы этого избежать, часто используется приём Адини, который заключается в следующем.

Пусть $i \in 1 : m - 1$, $j \in 1 : n - 1$. Возьмём участки кривых $a_{i-1}(\beta)$ и $a_{i+1}(\beta)$ при $\beta \in [j-1, j+1]$, $b_{j-1}(\alpha)$ и $b_{j+1}(\alpha)$ при $\alpha \in [i-1, i+1]$ в качестве граничных кривых и построим по ним билинейную поверхность Кунса:

$$\begin{aligned} c(\alpha, \beta) = & \frac{i+1-\alpha}{2} a_{i-1}(\beta) + \frac{\alpha-i+1}{2} a_{i+1}(\beta) + \frac{j+1-\beta}{2} b_{j-1}(\alpha) + \frac{\beta-j+1}{2} b_{j+1}(\alpha) - \\ & - \frac{(i+1-\alpha)(j+1-\beta)}{4} a_{i-1}(j-1) - \frac{(i+1-\alpha)(\beta-j+1)}{4} a_{i-1}(j+1) - \\ & - \frac{(\alpha-i+1)(j+1-\beta)}{4} a_{i+1}(j-1) - \frac{(\alpha-i+1)(\beta-j+1)}{4} a_{i+1}(j+1). \end{aligned}$$

Теперь в качестве d_{ij} возьмём значение смешанной производной построенной функции:

$$\begin{aligned} d_{ij} = c_{\alpha\beta}(i, j) = & \frac{a'_{i+1}(j) - a'_{i-1}(j)}{2} + \frac{b'_{j+1}(i) - b'_{j-1}(i)}{2} - \\ & - \frac{a_{i-1}(j-1) - a_{i-1}(j+1) - a_{i+1}(j-1) + a_{i+1}(j+1)}{4}. \end{aligned}$$

Таким образом, мы определили значения d_{ij} для $i \in 1 : m - 1$, $j \in 1 : n - 1$. Для оставшихся точек можно положить $d_{ij} = 0$.

ПРИМЕР 1. Пусть $m = 2$, $n = 3$, $d_{ij} = 0$,

$$\begin{aligned} a_0(v) &= (0, 0, 2), & b_0(u) &= (u, 0, (u-1)(u-2)), \\ a_1(v) &= \left(\cos \frac{\pi v}{2}, \sin \frac{\pi v}{2}, 0\right), & b_1(u) &= (0, u, (u-1)(u-2)), \\ a_2(v) &= \left(2 \cos \frac{\pi v}{2}, 2 \sin \frac{\pi v}{2}, 0\right), & b_2(u) &= (-u, 0, (u-1)(u-2)), \\ & & b_3(u) &= (0, -u, (u-1)(u-2)). \end{aligned}$$

Кривые a_i , b_j изображены на рис. 1, а составная поверхность Кунса для них приведена на рис. 2.

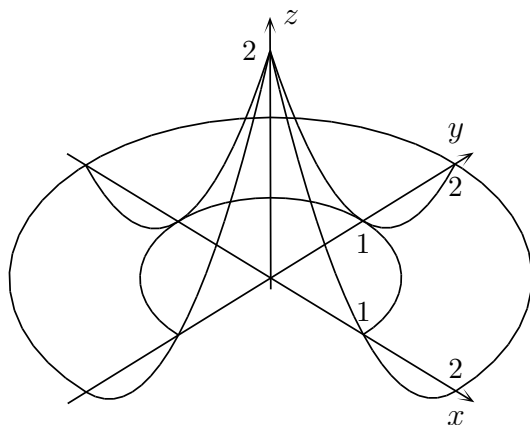


Рис. 1. Кривые a_i , b_j из примера 1.

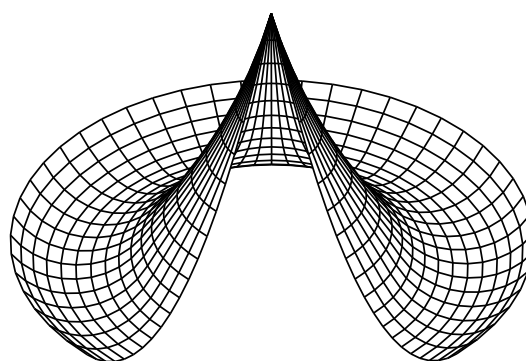


Рис. 2. Составная поверхность Кунса для кривых из примера 1.

ПРИМЕР 2. Пусть $m = 1$, $n = 4$, $d_{ij} = 0$,

$$\begin{aligned} a_0(v) &= \left(\frac{5 + \cos 2\pi v}{2} \cos \frac{\pi v}{2}, \frac{5 + \cos 2\pi v}{2} \sin \frac{\pi v}{2}, 0 \right), \\ a_1(v) &= \left(-\frac{5 + \cos 2\pi v}{2} \sin \frac{\pi v}{2}, \frac{5 + \cos 2\pi v}{2} \cos \frac{\pi v}{2}, 6 \right), \\ b_0(u) &= (3 - 3u, 3u, 6u), \quad b_1(u) = (-3u, 3 - 3u, 6u), \\ b_2(u) &= (3u - 3, -3u, 6u), \quad b_3(u) = (3u, 3u - 3, 6u), \\ b_4(u) &= (3 - 3u, 3u, 6u). \end{aligned}$$

Кривые a_i, b_j изображены на рис. 3. Заметим, что кривые a_0 и a_1 замкнутые, а $b_0(u) \equiv b_4(u)$, поэтому поверхность Кунса будет замкнутой (см. рис. 4).

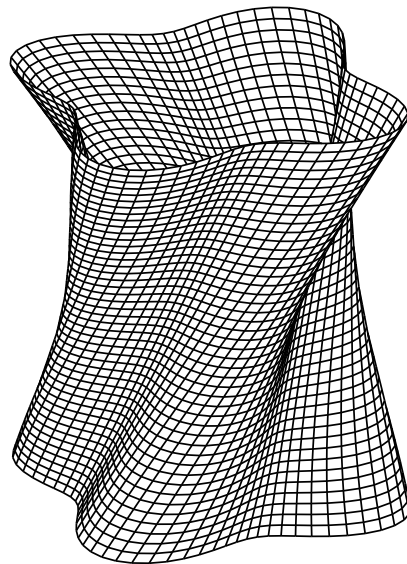
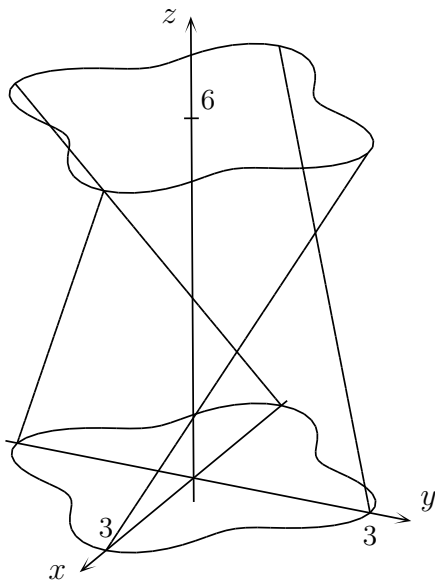


Рис. 3. Кривые a_i, b_j из примера 2. Рис. 4. Составная поверхность Кунса для кривых из примера 2.

ЛИТЕРАТУРА

1. Малозёмов В. Н., Чашников Н. В. *Бикубические поверхности Кунса* // Семинар «DHA & CAGD». Избранные доклады. 23 января 2007 г. (<http://dha.spb.ru/rep07.shtml#0123>).
2. G. Farin. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.

ПОСТРОЕНИЕ СФЕРЫ С ПОМОЩЬЮ ПРОЕКТИВНЫХ ПОВЕРХНОСТЕЙ БЕЗЬЕ

М. И. Григорьев

24 февраля 2007 г.

1°. Пусть в пространстве \mathbb{R}^3 задана матрица полюсов

$$\begin{array}{ccc} P_{00} & P_{01} & P_{02} \\ P_{10} & P_{11} & P_{12} \\ P_{20} & P_{21} & P_{22} \end{array}$$

По строкам этой матрицы построим три кривые Безье второго порядка [1]

$$B_i(v) = \sum_{j=0}^2 P_{ij} b_j^2(v), \quad v \in [0, 1], \quad i \in 0 : 2,$$

где $b_j^2(v) = C_2^j v^j (1-v)^{2-j}$. Кривые $B_i(v)$ будем называть *образующими*. Зафиксируем $v \in [0, 1]$. По точкам $B_0(v)$, $B_1(v)$, $B_2(v)$ можно в свою очередь построить кривую Безье $B(u, v)$, $u \in [0, 1]$. Когда параметр v пробегает весь отрезок $[0, 1]$, кривая $B(u, v)$ описывает поверхность в пространстве \mathbb{R}^3 , которая называется *поверхностью Безье второго порядка, заданной на четырёх-угольнике* (рис. 1). Её аналитическое представление имеет вид

$$B(u, v) = \sum_{i=0}^2 B_i(v) b_i^2(u) = \sum_{i=0}^2 \sum_{j=0}^2 P_{ij} b_i^2(u) b_j^2(v). \quad (1)$$

Из (1) следует, что

$$B(0, v) = B_0(v), \quad B(1, v) = B_2(v), \quad v \in [0, 1].$$

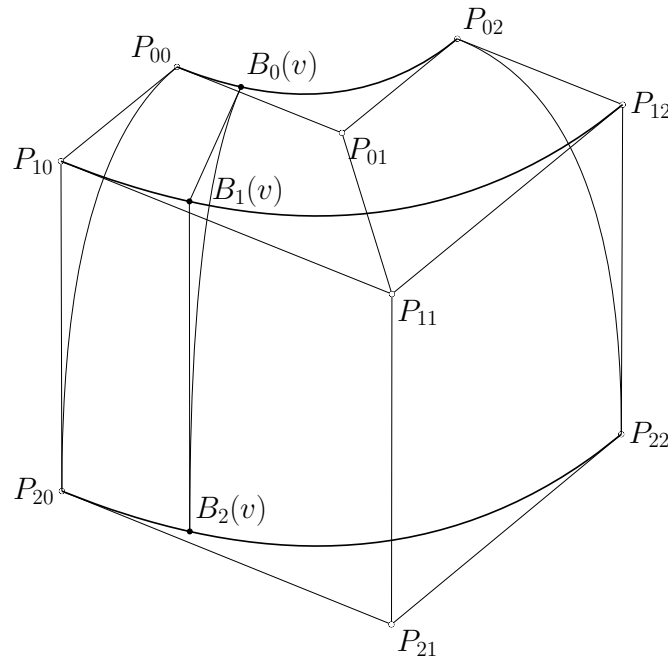


Рис. 1

2°. Припишем каждому полюсу P_{ij} четвертую координату $t = 1$ и рассмотрим полюсы $P'_{ij} = (P_{ij}, 1)$ в четырехмерном пространстве \mathbb{R}^4 . Зафиксируем девять положительных чисел w_{ij} , $i, j \in 0 : 2$, которые будем называть *веса*, и введём полюсы $\hat{P}_{ij} = w_{ij} P'_{ij} = (w_{ij} P_{ij}, w_{ij})$. По ним может быть построена поверхность Безье в \mathbb{R}^4 :

$$\hat{B}(u, v) = \left(\sum_{i=0}^2 \sum_{j=0}^2 w_{ij} P_{ij} b_i^2(u) b_j^2(v), \sum_{i=0}^2 \sum_{j=0}^2 w_{ij} b_i^2(u) b_j^2(v) \right).$$

Спроецируем эту поверхность на гиперплоскость $t = 1$, используя центральную проекцию с центром в начале координат, то есть поделим все координаты точек $\hat{B}(u, v)$ на четвертую, которую затем отбросим. Получим

$$R(u, v) = \frac{\sum_{i=0}^2 \sum_{j=0}^2 w_{ij} P_{ij} b_i^2(u) b_j^2(v)}{\sum_{i=0}^2 \sum_{j=0}^2 w_{ij} b_i^2(u) b_j^2(v)}, \quad u, v \in [0, 1]. \quad (2)$$

Формула (2) определяет поверхность в \mathbb{R}^3 , которая называется *проективной поверхностью Безье второго порядка, заданной на четырёхугольнике*. Её формой при неизменном положении полюсов P_{ij} можно управлять, варьируя веса w_{ij} .

Более подробные сведения о поверхностях вида (2) имеются в [2].

3°. Пусть на плоскости зафиксированы три полюса P_0, P_1, P_2 . По ним можно построить проективную кривую Безье второго порядка [2]

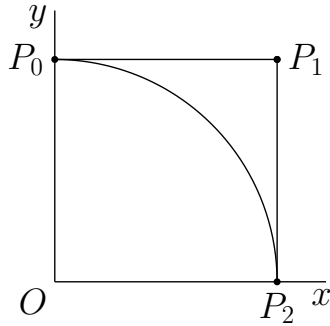


Рис. 2

$$R(u) = \frac{\sum_{i=0}^2 \omega_i P_i b_i^2(u)}{\sum_{i=0}^2 \omega_i b_i^2(u)}, \quad u \in [0, 1], \quad (3)$$

где $\omega_0, \omega_1, \omega_2$ — некоторые положительные числа. Известно [3], что если полюсы P_0, P_1, P_2 расположены в вершинах единичного квадрата так, как показано на рис. 2, и выполнено условие $2\omega_1^2 = \omega_0 \omega_2$, то кривая (3) является четвертью единичной окружности.

4°. Вернёмся к формуле (2) и перепишем её в виде

$$R(u, v) = \frac{\sum_{i=0}^2 \omega_i(v) R_i(v) b_i^2(u)}{\sum_{i=0}^2 \omega_i(v) b_i^2(u)}, \quad (4)$$

где

$$\omega_i(v) = \sum_{j=0}^2 w_{ij} b_j^2(v), \quad R_i(v) = \left(\sum_{j=0}^2 w_{ij} P_{ij} b_j^2(v) \right) / \omega_i(v). \quad (5)$$

Отметим, что кривая на поверхности (2), соответствующая некоторому фиксированному значению параметра v из отрезка $[0, 1]$, является проективной кривой Безье второго порядка, построенной по полюсам $R_0(v), R_1(v), R_2(v)$ с весами $\omega_0(v), \omega_1(v), \omega_2(v)$ соответственно. В свою очередь указанные полюсы лежат на трёх проективных кривых Безье, определяемых формулой (5).

5°. Рассмотрим случай, когда полюсы P_{ij} , $i, j \in 0 : 2$ распределены по вершинам единичного куба так, как показано на рис 3:

$$\begin{aligned} P_{00} &= P_{01} = P_{02} = (0, 0, 1), \\ P_{10} &= (1, 0, 1), \quad P_{11} = (1, 1, 1), \quad P_{12} = (0, 1, 1), \\ P_{20} &= (1, 0, 0), \quad P_{21} = (1, 1, 0), \quad P_{22} = (0, 1, 0). \end{aligned}$$

Очевидно, что в этом случае кривая $R_0(v)$ вырождается в точку $(0, 0, 1)$.

Подберём веса w_{ij} так, чтобы соответствующая проективная поверхность Безье совпала с одной восьмой частью сферы единичного радиуса с центром в точке O . Для этого кривые $R(u, 0)$, $R(u, 1)$ и $R(1, v)$, расположенные соответственно в плоскостях $Y=0$, $X=0$ и $Z=0$, должны быть четвертями окружно-

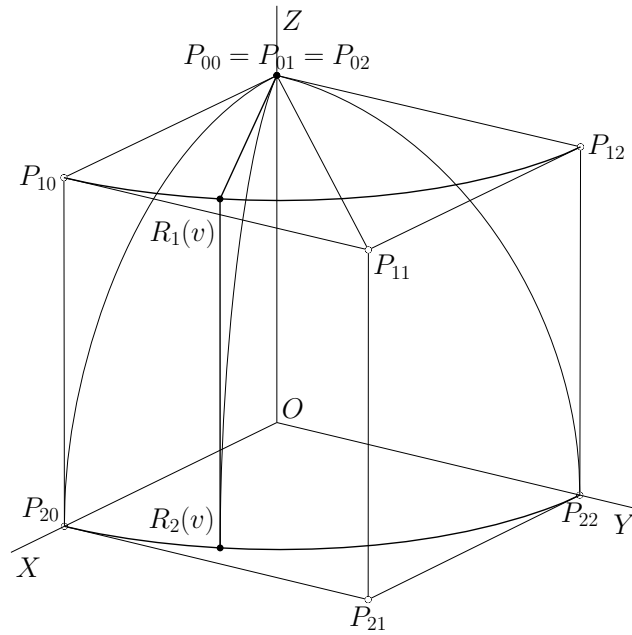


Рис. 3

стей единичного радиуса (см. рис. 3). Согласно (2) и (5)

$$R(u, 0) = \frac{\sum_{i=0}^2 w_{i0} P_{i0} b_i^2(u)}{\sum_{i=0}^2 w_{i0} b_i^2(u)}, \quad R(u, 1) = \frac{\sum_{i=0}^2 w_{i2} P_{i2} b_i^2(u)}{\sum_{i=0}^2 w_{i2} b_i^2(u)},$$

$$R(1, v) = R_2(v) = \frac{\sum_{j=0}^2 w_{2j} P_{2j} b_j^2(v)}{\sum_{j=0}^2 w_{2j} b_j^2(v)}.$$

Нетрудно понять, что мы находимся в условиях п. 3°. Кривые $R(u, 0)$, $R(u, 1)$ и $R(1, v)$ будут четвертями единичных окружностей, если

$$2w_{10}^2 = w_{00} w_{20}, \quad 2w_{12}^2 = w_{02} w_{22}, \quad 2w_{21}^2 = w_{20} w_{22}. \quad (6)$$

Потребуем, чтобы кривая $R_1(v)$, расположенная в плоскости $Z = 1$, также была четвертью единичной окружности. Поскольку и в этом случае мы находимся в условиях п. 3°, то необходимо, чтобы

$$2w_{11}^2 = w_{10} w_{12}. \quad (7)$$

Условиям (6) и (7) удовлетворяют веса

$$w_{00} = w_{20} = 1, \quad w_{10} = \frac{\sqrt{2}}{2}, \quad w_{02} = w_{22} = 1, \quad w_{12} = \frac{\sqrt{2}}{2},$$

$$w_{21} = \frac{\sqrt{2}}{2}, \quad w_{11} = \frac{1}{2}.$$

При этом

$$\begin{aligned}\omega_2(v) &= b_0^2(v) + \frac{\sqrt{2}}{2} b_1^2(v) + b_2^2(v), \\ \omega_1(v) &= \frac{\sqrt{2}}{2} \omega_2(v), \\ \omega_0(v) &= b_0^2(v) + w_{01} b_1^2(v) + b_2^2(v).\end{aligned}\tag{8}$$

Остаётся определить единственный вес w_{01} .

При фиксированном $v \in (0, 1)$ полюсы $R_0(v)$, $R_1(v)$, $R_2(v)$ лежат в вертикальной плоскости и их положение такое же, как положение точек P_0 , P_1 , P_2 в п. 3°. Мы хотим, чтобы проективная кривая (4), построенная по этим полюсам, была четвертью окружности. Как отмечалось, для этого необходимо выполнение условия

$$2\omega_1^2(v) = \omega_0(v) \omega_2(v).$$

На основании (8) получаем $\omega_2(v) = \omega_0(v)$ при всех $v \in (0, 1)$, откуда следует, что $w_{01} = \frac{\sqrt{2}}{2}$.

Подведём итог. Проективная поверхность Безье (2) при выбранных в начале пункта полюсах и весах

$$\begin{aligned}w_{00} &= 1, & w_{01} &= \frac{\sqrt{2}}{2}, & w_{02} &= 1, \\ w_{10} &= \frac{\sqrt{2}}{2}, & w_{11} &= \frac{1}{2}, & w_{12} &= \frac{\sqrt{2}}{2}, \\ w_{20} &= 1, & w_{21} &= \frac{\sqrt{2}}{2}, & w_{22} &= 1\end{aligned}$$

является одной восьмой частью единичной сферы.

С помощью всевозможных отражений этой поверхности относительно плоскостей OXY , OYZ и OXZ можно построить полную сферу.

6°. На рис. 4 изображены восьмая часть сферы и полная сфера, построенные описанным выше методом.

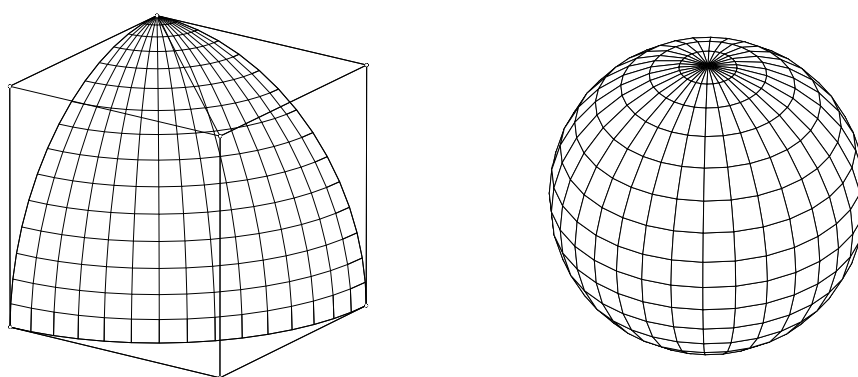


Рис. 4

ЛИТЕРАТУРА

1. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Полиномы Бернштейна и составные кривые Безье* // Журн. вычисл. мат. и матем. физ. 2006. Т. 46. №11. С. 1962-1971.
2. Farin G. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.
3. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Можно ли построить окружность с помощью кривых Безье?* // Семинар «DHA & CAGD». Избранные доклады. 19 декабря 2006 г. (<http://dha.spb.ru/rep06.shtml#1216>).

СИСТЕМЫ МЕРСЕДЕС-БЕНЦ И ЖЁСТКИЕ ФРЕЙМЫ

В. Н. Малозёмов А. Б. Певный

28 февраля 2007 г.

Данный доклад примыкает к докладу [1].

1°. Напомним [2, с. 99–100], что жёстким фреймом в \mathbb{R}^n называется набор векторов $\{\varphi_1, \dots, \varphi_m\}$, такой, что при некотором $A > 0$ (константа фрейма) для любого $x \in \mathbb{R}^n$ выполняется равенство

$$\sum_{k=1}^m (\langle x, \varphi_k \rangle)^2 = A \|x\|^2. \quad (1)$$

Обозначим через Φ матрицу со столбцами $\varphi_1, \dots, \varphi_m$. Для неё

$$\|\Phi^T x\|^2 = \sum_{k=1}^m (\langle x, \varphi_k \rangle)^2.$$

Поскольку

$$\|\Phi^T x\|^2 = \langle \Phi^T x, \Phi^T x \rangle = \langle \Phi \Phi^T x, x \rangle,$$

то равенство (1) можно переписать в виде

$$\langle \Phi \Phi^T x, x \rangle = \langle A I_n x, x \rangle \quad \forall x \in \mathbb{R}^n, \quad (2)$$

где I_n — единичная матрица порядка n . Формула (2) равносильна матричному равенству

$$\Phi \Phi^T = A I_n. \quad (3)$$

Умножив (3) на x , придём к эквивалентному векторному равенству

$$x = \frac{1}{A} \sum_{k=1}^m \langle x, \varphi_k \rangle \varphi_k \quad \forall x \in \mathbb{R}^n. \quad (4)$$

Таким образом, формулы (1), (3), (4) дают эквивалентные определения жёсткого фрейма в \mathbb{R}^n с константой $A > 0$.

Если обозначить через $\text{tr}(\Phi \Phi^T)$ сумму диагональных элементов квадратной матрицы $\Phi \Phi^T$, то в силу (3) получим

$$\text{tr}(\Phi \Phi^T) = \text{tr}(A I_n) = n A.$$

Вместе с тем, как нетрудно проверить, $\text{tr}(\Phi \Phi^T) = \text{tr}(\Phi^T \Phi)$, поэтому

$$nA = \text{tr}(\Phi^T \Phi) = \sum_{k=1}^m \|\varphi_k\|^2.$$

Отсюда следует, что константа фрейма A необходимо равна такой величине:

$$A = \frac{1}{n} \sum_{k=1}^m \|\varphi_k\|^2. \quad (5)$$

Наша цель — дать полное описание множества жёстких фреймов в простейшем частном случае, когда $m = n + 1$ и все векторы φ_k имеют единичную длину. В приводимом ниже анализе важную промежуточную роль будут играть так называемые *системы Мерседес-Бенц* [1].

2°. Набор n -мерных векторов $\{\varphi_1, \dots, \varphi_{n+1}\}$ называется системой Мерседес-Бенц, если выполнены условия

$$\langle \varphi_k, \varphi_j \rangle = -\frac{1}{n} \quad \text{при } k \neq j; \quad \|\varphi_k\| = 1 \quad \text{при } k \in 1 : n + 1. \quad (6)$$

В [1] индуктивно построена одна такая система $\{b_1^n, \dots, b_{n+1}^n\}$ (верхний индекс указывает на размерность вектора).

В общем случае для любой системы Мерседес-Бенц $\{\varphi_1, \dots, \varphi_{n+1}\}$ справедливо равенство

$$\sum_{k=1}^{n+1} \varphi_k = \mathbb{O}. \quad (7)$$

Действительно,

$$\begin{aligned} \left\| \sum_{k=1}^{n+1} \varphi_k \right\|^2 &= \left\langle \sum_{k=1}^{n+1} \varphi_k, \sum_{j=1}^{n+1} \varphi_j \right\rangle = \sum_{k=1}^{n+1} \sum_{j=1}^{n+1} \langle \varphi_k, \varphi_j \rangle = \\ &= \sum_{k=1}^{n+1} \|\varphi_k\|^2 + \sum_{k \neq j} \langle \varphi_k, \varphi_j \rangle = n + 1 - \frac{1}{n} [(n + 1)^2 - (n + 1)] = 0. \end{aligned}$$

ТЕОРЕМА 1. Для того чтобы набор n -мерных векторов $\{\varphi_1, \dots, \varphi_{n+1}\}$ был системой Мерседес-Бенц, необходимо и достаточно, чтобы нашлась ортогональная $(n \times n)$ -матрица U , такая, что

$$\varphi_k = U b_k^n, \quad k \in 1 : n + 1. \quad (8)$$

Доказательство. Достаточность следует из (6), если учесть, что для ортогональной матрицы U выполняются соотношения

$$U U^T = U^T U = I_n.$$

Необходимость. Наряду с матрицей Φ со столбцами $\varphi_1, \dots, \varphi_{n+1}$ введём матрицу B со столбцами b_1^n, \dots, b_{n+1}^n . Тогда (8) можно переписать в виде

$$\Phi = U B. \quad (9)$$

Равенство (9) будем рассматривать как уравнение относительно U .

Добавим к $(n \times (n + 1))$ -матрицам Φ и B $(n + 1)$ -ю строку, все компоненты которой равны $1/\sqrt{n}$. Получившиеся квадратные матрицы обозначим Φ_0 и B_0 . Из определения систем Мерседес-Бенц следует, что

$$\Phi_0^T \Phi_0 = \left(1 + \frac{1}{n}\right) I_{n+1}, \quad B_0^T B_0 = \left(1 + \frac{1}{n}\right) I_{n+1}.$$

Положим $P = \sqrt{\frac{n}{n+1}} \Phi_0$, $Q = \sqrt{\frac{n}{n+1}} B_0$. Поскольку $P^T P = I_{n+1}$, $Q^T Q = I_{n+1}$, то матрицы P и Q являются ортогональными.

Построим ортогональную матрицу U_0 , такую, что

$$\Phi_0 = U_0 B_0. \quad (10)$$

После умножения на $\sqrt{\frac{n}{n+1}}$ придём к равносильному уравнению $P = U_0 Q$ с очевидным решением $U_0 = P Q^T$. Ясно, что U_0 — ортогональная матрица.

Покажем, что U_0 имеет вид

$$U_0 = \begin{bmatrix} U & \mathbb{O} \\ \mathbb{O}^T & 1 \end{bmatrix}. \quad (11)$$

Согласно (7)

$$\sum_{k=1}^{n+1} \varphi_k = \sum_{k=1}^{n+1} b_k^n = \mathbb{O},$$

ПОЭТОМУ

$$\begin{aligned}
 U_0[i, n+1] &= \frac{n}{n+1} \sum_{k=1}^{n+1} \Phi_0[i, k] \times B_0^T[k, n+1] = \\
 &= \frac{n}{n+1} \sum_{k=1}^{n+1} \varphi_k(i) \frac{1}{\sqrt{n}} = 0 \quad \text{при } i \in 1:n, \\
 U_0[n+1, n+1] &= \frac{n}{n+1} \sum_{k=1}^{n+1} \Phi_0[n+1, k] \times B_0^T[k, n+1] = 1, \\
 U_0[n+1, j] &= \frac{n}{n+1} \sum_{k=1}^{n+1} \Phi_0[n+1, k] \times B_0[j, k] = \\
 &= \frac{n}{n+1} \sum_{k=1}^{n+1} \frac{1}{\sqrt{n}} b_k^n(j) = 0 \quad \text{при } j \in 1:n.
 \end{aligned}$$

Формула (11) установлена. Учитывая, что

$$U_0 U_0^T = \begin{bmatrix} U U^T & \mathbb{O} \\ \mathbb{O}^T & 1 \end{bmatrix}$$

и $U_0 U_0^T = I_{n+1}$, заключаем, что U — ортогональная матрица.

Из (10) и (11) следует (9). Теорема доказана. \square

3°. Теперь обратимся к описанию множества жёстких фреймов в \mathbb{R}^n , состоящих из $n+1$ единичных векторов. В этом случае, согласно (5), $A = 1 + \frac{1}{n}$.

ТЕОРЕМА 2. Для того чтобы набор единичных n -мерных векторов $\{\varphi_1, \dots, \varphi_{n+1}\}$ был жёстким фреймом в \mathbb{R}^n , необходимо и достаточно, чтобы имело место представление

$$\varphi_k = \sigma_k U b_k^n, \quad k \in 1:n+1, \quad (12)$$

где $\sigma_k = \pm 1$ и U — некоторая ортогональная матрица.

Доказательство. Достаточность. В [1] установлено, что система $\{b_1^n, \dots, b_{n+1}^n\}$ является жёстким фреймом в \mathbb{R}^n с константой $A = 1 + \frac{1}{n}$. То же самое можно сказать и о системе (12), поскольку

$$\begin{aligned}
 \sum_{k=1}^{n+1} (\langle x, \varphi_k \rangle)^2 &= \sum_{k=1}^{n+1} (\langle x, U b_k^n \rangle)^2 = \sum_{k=1}^{n+1} (\langle U^T x, b_k^n \rangle)^2 = \\
 &= \left(1 + \frac{1}{n}\right) \|U^T x\|^2 = \left(1 + \frac{1}{n}\right) \|x\|^2.
 \end{aligned}$$

Необходимость. Как обычно, через Φ обозначим матрицу со столбцами $\varphi_1, \dots, \varphi_{n+1}$. В силу (3) и (5)

$$\Phi \Phi^T = \left(1 + \frac{1}{n}\right) I_n. \quad (13)$$

Рассмотрим Φ как набор $(n+1)$ -мерных строк $\gamma_1, \dots, \gamma_n$. Согласно (13)

$$\langle \gamma_j, \gamma_k \rangle = \begin{cases} 1 + \frac{1}{n} & \text{при } k = j, \\ 0 & \text{при } k \neq j. \end{cases}$$

Дополним Φ ещё одной строкой γ_{n+1} так, чтобы

$$\langle \gamma_j, \gamma_{n+1} \rangle = 0 \quad \text{при } j \in 1 : n, \quad \|\gamma_{n+1}\|^2 = 1 + \frac{1}{n}.$$

Расширенную матрицу обозначим Φ_1 . Для неё

$$\Phi_1 \Phi_1^T = \left(1 + \frac{1}{n}\right) I_{n+1}.$$

Матрица $P = \sqrt{\frac{n}{n+1}} \Phi_1$ является ортогональной, так как $P P^T = I_{n+1}$. Но тогда и $P^T P = I_{n+1}$, откуда следует, что

$$\Phi_1^T \Phi_1 = \left(1 + \frac{1}{n}\right) I_{n+1}. \quad (14)$$

В частности,

$$(\Phi_1^T \Phi_1)[k, k] = \sum_{j=1}^{n+1} (\Phi_1[j, k])^2 = 1 + \frac{1}{n}, \quad k \in 1 : n+1. \quad (15)$$

В то же время

$$\sum_{j=1}^n (\Phi_1[j, k])^2 = \|\varphi_k\|^2 = 1, \quad k \in 1 : n+1. \quad (16)$$

Вычитая (16) из (15), получаем $(\Phi_1[n+1, k])^2 = \frac{1}{n}$. Значит,

$$\gamma_{n+1}(k) = \frac{\sigma_k}{\sqrt{n}}, \quad k \in 1 : n+1,$$

где $\sigma_k = \pm 1$. Так выглядит добавленная строка.

Введём диагональную матрицу $D = \text{diag}(\sigma_1, \dots, \sigma_{n+1})$ и положим

$$\Phi_0 = \Phi_1 D.$$

У матрицы Φ_0 k -й столбец равен $(\sigma_k \varphi_k, \frac{1}{\sqrt{n}})^T$. Согласно (14)

$$\Phi_0^T \Phi_0 = D \Phi_1^T \Phi_1 D = \left(1 + \frac{1}{n}\right) I_{n+1}. \quad (17)$$

Обозначим $v_k = \sigma_k \varphi_k$ и перепишем (17) в виде

$$\sum_{l=1}^n v_j(l) v_k(l) + \frac{1}{n} = \begin{cases} 1 + \frac{1}{n} & \text{при } k = j, \\ 0 & \text{при } k \neq j. \end{cases}$$

Отсюда следует, что

$$\langle v_j, v_k \rangle = \begin{cases} 1 & \text{при } k = j, \\ -\frac{1}{n} & \text{при } k \neq j. \end{cases}$$

По определению, $\{v_1, \dots, v_{n+1}\}$ — система Мерседес-Бенц.

На основании теоремы 1 заключаем, что существует ортогональная матрица U , такая, что $v_k = U b_k^n$. Поскольку $v_k = \sigma_k \varphi_k$, то

$$\varphi_k = \sigma_k U b_k^n, \quad k \in 1 : n + 1.$$

Теорема доказана. \square

4°. Дальнейшая информация о жёстких фреймах в конечномерных пространствах имеется в [3, 4, 5].

ЛИТЕРАТУРА

1. Малозёмов В. Н., Певный А. Б. *Фрейм Мерседес-Бенц в n -мерном пространстве* // Семинар «DHA & CAGD». Избранные доклады. 16 января 2007 г. (<http://dha.spb.ru/rep07.shtml#0116>).
2. Добеши И. *Десять лекций по вейвлетам*. Пер. с англ. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.
3. Casazza P. G. *Custom building finite frames* // Contemporary Math. 2004. V. 345. P. 61–86.
4. Goyal V. K., Kovačević J., Kelner J. A. *Quantized frame expansions with erasures* // Appl. and Comput. Harmonic Anal. 2001. V. 10. No. 3. P. 203–233.
5. Han D., Larson D. R. *Frames, bases and group representation* // Memoires of Amer. Math. Soc. 2000. V. 147. No. 697. P. 1–94.

ПОВЕРХНОСТИ БЕЗЬЕ НА ТРЕУГОЛЬНИКЕ. ПЕРЕПАРАМЕТРИЗАЦИЯ

И. А. Капелюхин В. Н. Малозёмов А. Н. Сергеев

10 марта 2007 г.

1°. Пусть в пространстве \mathbb{R}^3 задан треугольный массив полюсов

$$\begin{array}{cccccccc}
 P_{00} & P_{01} & P_{02} & \dots & P_{0,n-2} & P_{0,n-1} & P_{0n} \\
 & P_{10} & P_{11} & \dots & P_{1,n-2} & P_{1,n-1} & \\
 & & P_{20} & \dots & P_{2,n-2} & & \\
 & & & \ddots & & \ddots & \\
 & & & & P_{n-1,0} & P_{n-1,1} & \\
 & & & & & P_{n0} &
 \end{array}$$

По этим полюсам с помощью полинома Бернштейна на треугольнике можно построить поверхность Безье [1]:

$$B_0(x, y) = \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} \frac{n!}{i! j! (n-i-j)!} x^i y^j (1-x-y)^{n-i-j}, \quad (1)$$

$$x \geq 0, \quad y \geq 0, \quad x+y \leq 1.$$

Покажем, что поверхность (1) допускает три других представления, в которых вектор параметров изменяется не в треугольнике, а в единичном квадрате.

2°. Введём обозначения

$$\Delta = \{(x, y) \mid x \geq 0, y \geq 0, x+y \leq 1\},$$

$$Q = \{(u, v) \mid 0 \leq u \leq 1, 0 \leq v \leq 1\}.$$

Наряду с (1) рассмотрим полином

$$B_1(u, v) = \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} b_i^n(u) b_j^{n-i}(v), \quad (u, v) \in Q,$$

где $b_k^m(x) = C_m^k x^k (1-x)^{m-k}$ — базисные полиномы Бернштейна.

ПРЕДЛОЖЕНИЕ 1. *Справедливо равенство множеств*

$$\{B_0(x, y) \mid (x, y) \in \Delta\} = \{B_1(u, v) \mid (u, v) \in Q\}. \quad (2)$$

Доказательство. Рассмотрим преобразование

$$x = u, \quad y = (1 - u)v. \quad (3)$$

Поскольку при $(u, v) \in Q$

$$x + y = 1 - (1 - u) + (1 - u)v = 1 - (1 - u)(1 - v) \leq 1,$$

то преобразование (3) сопоставляет точке $(u, v) \in Q$ точку $(x, y) \in \Delta$. Наоборот, если $(x, y) \in \Delta$, то найдётся точка $(u, v) \in Q$, для которой выполняются соотношения (3). Действительно, при $x = 1$ имеем $y = 0$. Условию (3) будет удовлетворять пара $(u, v) \in Q$ с $u = 1$ и любым $v \in [0, 1]$. При $x < 1$, требуемой будет пара $u = x$, $v = y/(1 - x)$ с $v \leq 1$.

После этого замечания обратимся к равенству (2) и обозначим множества, стоящие в левой и правой его частях, через \mathfrak{B}_0 и \mathfrak{B}_1 соответственно. Возьмём точку $P \in \mathfrak{B}_1$. По определению найдётся вектор параметров $(u, v) \in Q$, такой, что

$$\begin{aligned} P &= \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} C_n^i u^i (1 - u)^{n-i} C_{n-i}^j v^j (1 - v)^{n-i-j} = \\ &= \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} C_n^i C_{n-i}^j u^i ((1 - u)v)^j ((1 - u)(1 - v))^{n-i-j}. \end{aligned} \quad (4)$$

Перейдём к вектору параметров $(x, y) \in \Delta$ по формуле (3). Учитывая, что $(1 - u)(1 - v) = 1 - x - y$ и

$$C_n^i C_{n-i}^j = \frac{n!}{i! j! (n - i - j)!},$$

получаем

$$P = \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} \frac{n!}{i! j! (n - i - j)!} x^i y^j (1 - x - y)^{n-i-j}.$$

Значит $P \in \mathfrak{B}_0$. Установлено включение $\mathfrak{B}_1 \subset \mathfrak{B}_0$.

Обратное включение проверяется обратным ходом с использованием того факта, что вектору параметров $(x, y) \in \Delta$ можно сопоставить вектор параметров $(u, v) \in Q$, удовлетворяющий соотношениям (3).

Предложение доказано. \square

Преобразование (3) квадрата Q в треугольник Δ является вырожденным, тем не менее, с его помощью мы достигли цели. Этому способствовало следующее свойство полиномов Бернштейна: при всех $v \in [0, 1]$

$$B_1(1, v) = P_{n0} b_0^n(v) \equiv P_{n0} = B_0(1, 0).$$

3°. Рассмотрим другую форму полинома Бернштейна

$$B_2(s, t) = \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ji} b_i^n(s) b_j^{n-i}(t), \quad (s, t) \in Q.$$

ПРЕДЛОЖЕНИЕ 2. *Справедливо равенство множеств*

$$\{B_1(u, v) \mid (u, v) \in Q\} = \{B_2(s, t) \mid (s, t) \in Q\}. \quad (5)$$

Доказательство. Запишем соотношения

$$\begin{aligned} s &= (1 - u)v, \\ (1 - s)t &= u. \end{aligned} \quad (6)$$

Покажем, что каждой паре $(u, v) \in Q$ можно сопоставить пару $(s, t) \in Q$, такую, что выполняются соотношения (6), и наоборот.

Пусть $(u, v) \in Q$. Если $u > 0$, то соответствующее s меньше единицы, и мы однозначно определяем t :

$$t = \frac{u}{1 - s} = \frac{u}{u + (1 - u)(1 - v)} \leq 1.$$

Если $u = 0$, то $s = v$, и можно взять $t = 0$.

Симметричным образом по $(s, t) \in Q$ определяется требуемая пара $(u, v) \in Q$.

Обратимся к равенству (5) и перепишем его в виде $\mathfrak{B}_1 = \mathfrak{B}_2$. Возьмём точку $P \in \mathfrak{B}_1$ и представим её в виде (4). После этого перейдём к вектору параметров $(s, t) \in Q$ по формулам (6). Учитывая, что

$$(1 - u)(1 - v) = 1 - u - s = 1 - s - (1 - s)t = (1 - s)(1 - t)$$

и $C_n^i C_{n-i}^j = C_n^j C_{n-j}^i$, получаем

$$P = \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} C_n^j C_{n-j}^i ((1 - s)t)^i s^j ((1 - s)(1 - t))^{n-j-i} =$$

$$\begin{aligned}
&= \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} b_j^n(s) b_i^{n-j}(t) = \sum_{j=0}^n \sum_{i=0}^{n-j} P_{ij} b_j^n(s) b_i^{n-j}(t) = \\
&= \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ji} b_i^n(s) b_j^{n-i}(t).
\end{aligned}$$

Значит, $P \in \mathfrak{B}_2$. Установлено включение $\mathfrak{B}_1 \subset \mathfrak{B}_2$.

Обратное включение проверяется обратным ходом. Используется тот факт, что вектору параметров $(s, t) \in Q$ можно сопоставить вектор параметров $(u, v) \in Q$, удовлетворяющий соотношениям (6).

Предложение доказано. \square

4°. В формуле для $B_1(u, v)$ индекс i есть индекс горизонтальной строки треугольного массива полюсов $\{P_{ij}\}$. В формуле для $B_2(s, t)$ тот же индекс является индексом наклонной слева направо строки. Остаётся ещё одна возможность — формировать поверхность Безье на основе наклонных справа налево строк массива $\{P_{ij}\}$.

В этой связи рассмотрим новую форму полинома Бернштейна

$$B_3(s, t) = \sum_{i=0}^n \sum_{j=0}^{n-i} P_{j, n-i-j} b_i^n(s) b_j^{n-i}(t), \quad (s, t) \in Q.$$

ПРЕДЛОЖЕНИЕ 3. *Справедливо равенство множеств*

$$\{B_1(u, v) \mid (u, v) \in Q\} = \{B_3(s, t) \mid (s, t) \in Q\}. \quad (7)$$

Доказательство. Запишем соотношения

$$\begin{aligned}
s &= (1-u)(1-v), \\
(1-s)t &= u.
\end{aligned} \quad (8)$$

Если обозначить $v' = 1 - v$, то формулы (8) и (6) становятся идентичными. Это позволяет утверждать, что каждой паре $(u, v) \in Q$ можно сопоставить пару $(s, t) \in Q$, такую, что выполняются соотношения (8), и наоборот.

Обратимся к равенству (7) и перепишем его в виде $\mathfrak{B}_1 = \mathfrak{B}_3$. Возьмём точку $P \in \mathfrak{B}_1$ и представим её в виде (4). После этого перейдём к вектору параметров $(s, t) \in Q$ по формулам (8). Учитывая, что

$$(1-u)v = 1-u-s = 1-s-(1-s)t = (1-s)(1-t)$$

и $C_n^i C_{n-i}^j = C_{i+j}^i C_n^{i+j}$, получаем

$$P = \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} C_{i+j}^i C_n^{i+j} ((1-s)t)^i ((1-s)(1-t))^j s^{n-i-j} =$$

$$= \sum_{i=0}^n \sum_{j=0}^{n-i} P_{ij} C_n^{i+j} s^{n-i-j} (1-s)^{i+j} C_{i+j}^i t^i (1-t)^j.$$

После замены индекса j на $k = n - i - j$ придём к формуле

$$\begin{aligned} P &= \sum_{i=0}^n \sum_{k=0}^{n-i} P_{i,n-i-k} C_n^k s^k (1-s)^{n-k} C_{n-k}^i t^i (1-t)^{n-i-k} = \\ &= \sum_{i=0}^n \sum_{k=0}^{n-i} P_{i,n-i-k} b_k^n(s) b_i^{n-k}(t) = \sum_{k=0}^n \sum_{i=0}^{n-k} P_{i,n-k-i} b_k^n(s) b_i^{n-k}(t) = \\ &= \sum_{i=0}^n \sum_{j=0}^{n-i} P_{j,n-i-j} b_i^n(s) b_j^{n-i}(t). \end{aligned}$$

Значит, $P \in \mathfrak{B}_3$. Установлено включение $\mathfrak{B}_1 \subset \mathfrak{B}_3$.

Обратное включение проверяется обратным ходом с использованием того факта, что вектору параметров $(s, t) \in Q$ можно сопоставить вектор параметров $(u, v) \in Q$, удовлетворяющий соотношениям (8).

Предложение доказано. \square

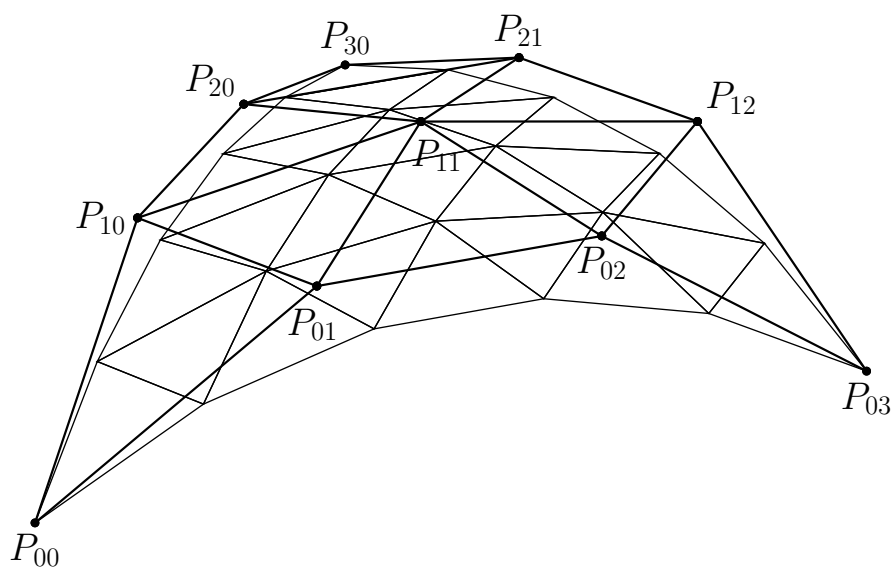
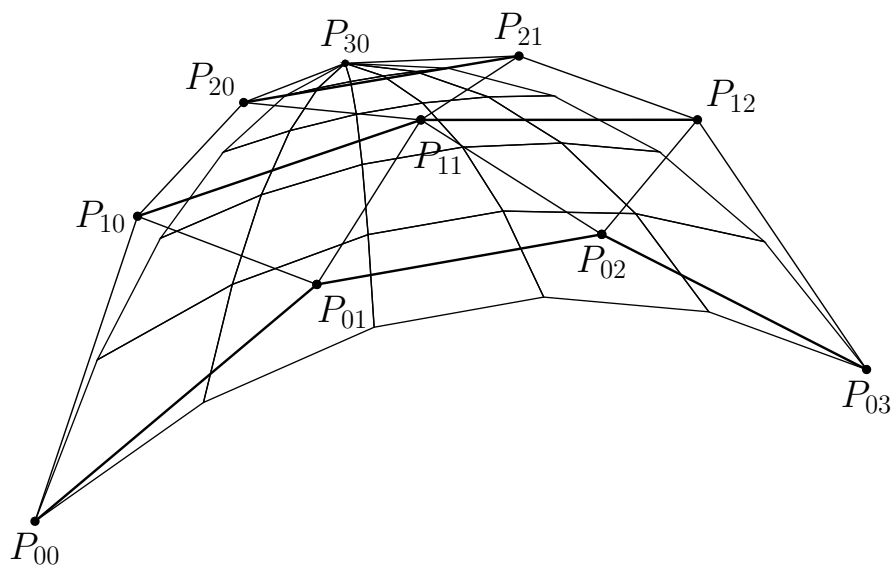
5°. На приводимых ниже рисунках 1–4 изображены поверхности Безье, построенные по одной и той же системе полюсов (в \mathbb{R}^3 при $n = 3$)

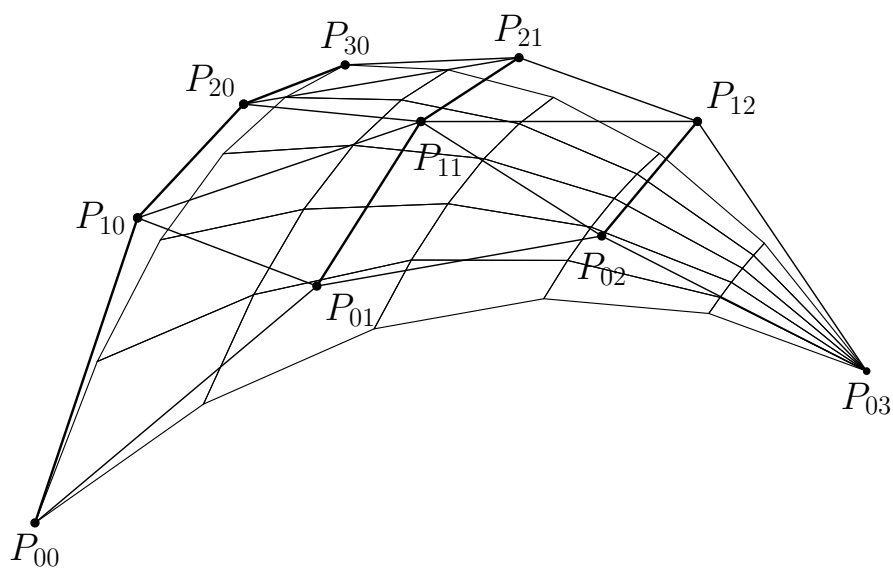
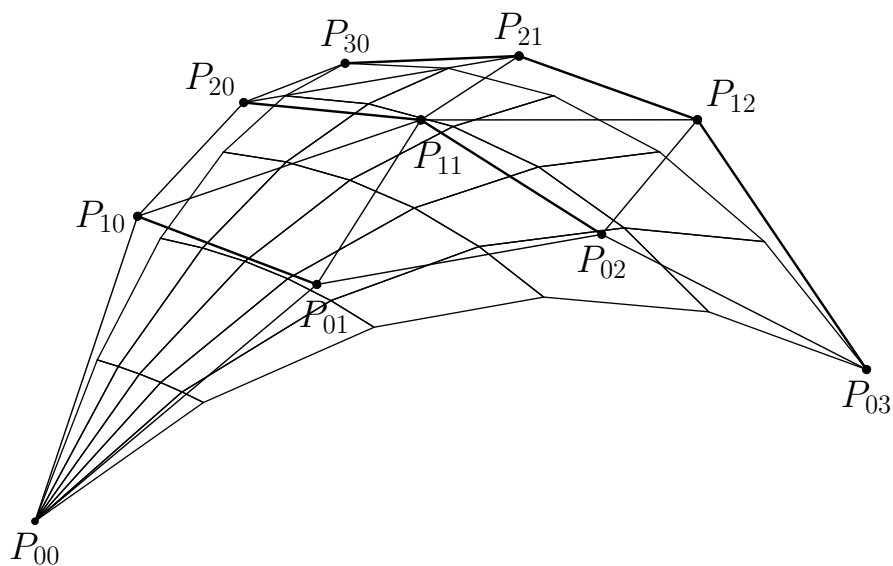
$$\begin{array}{cccc} P_{00} & P_{01} & P_{02} & P_{03} \\ & P_{10} & P_{11} & P_{12} \\ & & P_{20} & P_{21} \\ & & & P_{30}, \end{array}$$

но с использованием разных представлений полинома Бернштейна. Рис. 1 соответствует представлению $B_0(x, y)$, рис. 2 — представлению $B_1(u, v)$, рис. 3 — представлению $B_2(s, t)$, рис. 4 — представлению $B_3(s, t)$. Вычисление значений полиномов проводилось с постоянным шагом по каждому параметру в областях Δ (рис. 1) и Q (рис. 2–4). По доказанному все четыре полинома Бернштейна определяют одну и ту же поверхность Безье. Вопрос о быстром вычислении вырожденных полиномов Бернштейна $B_1(u, v)$, $B_2(s, t)$, $B_3(s, t)$ рассматривался в работе [2].

ЛИТЕРАТУРА

1. Farin G. *Curves and surfaces for CAGD*. 5th ed. San Diego: Academic Press, 2002. xvii+499 pp.
2. Shi-Min Hu. *Conversion between triangular and rectangular Bézier patches* // CAGD. 2001. Vol. 18. P. 667–671.

Рис. 1. График полинома $B_0(x, y)$, $(x, y) \in \Delta$.Рис. 2. График полинома $B_1(u, v)$, $(u, v) \in Q$.

Рис. 3. График полинома $B_2(s, t)$, $(s, t) \in Q$.Рис. 4. График полинома $B_3(s, t)$, $(s, t) \in Q$.

ПОЛЕ ЗАМКНУТЫХ КРИВЫХ БЕЗЬЕ

М. И. Григорьев

В. Н. Малозёмов

24 марта 2007 г.

1°. Возьмём на плоскости четыре точки P_0, P_1, P_2, P_3 , такие, что $P_3 = P_0$ и P_0, P_1, P_2 не лежат на одной прямой. Зафиксируем положительные веса w_0, w_1, w_2, w_3 . По указанным данным построим дробно-рациональную (проективную) кривую Безье третьего порядка [1, с. 227–230]:

$$R_0(u) = \frac{w_0(1-u)^3 P_0 + 3w_1(1-u)^2 u P_1 + 3w_2(1-u) u^2 P_2 + w_3 u^3 P_3}{w_0(1-u)^3 + 3w_1(1-u)^2 u + 3w_2(1-u) u^2 + w_3 u^3}. \quad (1)$$

Поскольку $R_0(0) = P_0$, $R_0(1) = P_3$ и $P_0 = P_3$, то кривая $R_0(u)$ при $u \in [0, 1]$ является замкнутой.

Введём числа

$$\mu_0 = \frac{w_0 w_2}{w_1^2}, \quad \mu_1 = \frac{w_1 w_3}{w_2^2}$$

и рассмотрим ещё одну проективную кривую Безье

$$R_1(t) = \frac{(\mu_0(1-t)^3 + \mu_1 t^3) P_0 + 3(1-t)t[(1-t)P_1 + tP_2]}{\mu_0(1-t)^3 + \mu_1 t^3 + 3(1-t)t}, \quad t \in [0, 1]. \quad (2)$$

ПРЕДЛОЖЕНИЕ 1. *Справедливо равенство множеств*

$$\{R_0(u) \mid u \in [0, 1]\} = \{R_1(t) \mid t \in [0, 1]\}. \quad (3)$$

Доказательство. Обозначим множества, стоящие в левой и правой частях равенства (3), через \mathfrak{B}_0 и \mathfrak{B}_1 соответственно. Проверим сначала, что $\mathfrak{B}_0 \subset \mathfrak{B}_1$.

Если $P \in \mathfrak{B}_0$, то существует $u \in [0, 1]$, такое, что $P = R_0(u)$. Положим $\rho = w_2/w_1$ и

$$t = \frac{\rho u}{\rho u + (1-u)}. \quad (4)$$

Очевидно, что $t \in [0, 1]$. При этом

$$u = \frac{t}{t + \rho(1-t)}. \quad (5)$$

Подставив (5) в (1), получим

$$P = \frac{w_0 \rho^3 (1-t)^3 P_0 + 3 w_1 \rho^2 (1-t)^2 t P_1 + 3 w_2 \rho (1-t) t^2 P_2 + w_3 t^3 P_3}{w_0 \rho^3 (1-t)^3 + 3 w_1 \rho^2 (1-t)^2 t + 3 w_2 \rho (1-t) t^2 + w_3 t^3}. \quad (6)$$

Отметим, что

$$w_0 \rho^3 = \frac{w_0 w_2^3}{w_1^3}, \quad w_1 \rho^2 = w_2 \rho = \frac{w_2^2}{w_1}.$$

Умножим числитель и знаменатель дроби из правой части (6) на w_1/w_2^2 . Учитывая, что $P_3 = P_0$, приходим к представлению $P = R_1(t)$. Включение $\mathfrak{B}_0 \subset \mathfrak{B}_1$ установлено.

Аналогично проверяется обратное включение. Пусть $P = R_1(t)$ при некотором $t \in [0, 1]$. Сделаем замену переменной (4). Получим

$$P = \frac{\mu_0 (1-u)^3 P_0 + 3 \rho (1-u)^2 u P_1 + 3 \rho^2 (1-u) u^2 P_2 + \mu_1 \rho^3 u^3 P_3}{\mu_0 (1-u)^3 + 3 \rho (1-u)^2 u + 3 \rho^2 (1-u) u^2 + \mu_1 \rho^3 u^3}.$$

Умножим числитель и знаменатель последней дроби на w_1^2/w_2 . Вспоминая определения μ_0 , μ_1 и ρ , приходим к представлению $P = R_0(u)$, где $u \in [0, 1]$. Это означает, что $\mathfrak{B}_1 \subset \mathfrak{B}_0$.

Предложение доказано. \square

Согласно предложению 1, любую проективную кривую Безье третьего порядка (1) в случае $P_3 = P_0$ можно привести к стандартной форме (2), зависящей от двух положительных параметров μ_0 и μ_1 .

2°. В дальнейшем будем рассматривать кривые Безье в стандартной форме (2). Пусть $P = R_1(t)$ при некотором $t \in [0, 1]$. Обозначим $\mu(t) = \mu_0 (1-t)^3 + \mu_1 t^3 + 3(1-t)t$,

$$\lambda_0 = \frac{\mu_0 (1-t)^3 + \mu_1 t^3}{\mu(t)}, \quad \lambda_1 = \frac{3(1-t)^2 t}{\mu(t)}, \quad \lambda_2 = \frac{3(1-t) t^2}{\mu(t)}.$$

Тогда

$$P = \lambda_0 P_0 + \lambda_1 P_1 + \lambda_2 P_2, \quad (7)$$

причём коэффициенты λ_0 , λ_1 , λ_2 неотрицательны и в сумме равны единице. Такие коэффициенты называются *барицентрическими координатами* точки P относительно точек P_0 , P_1 , P_2 . Из (7), в частности, следует, что кривая Безье $\mathfrak{B}_1 = \{R_1(t) \mid t \in [0, 1]\}$ лежит в треугольнике $P_0 P_1 P_2$.

Вернёмся к точке P и покажем, что её барицентрические координаты удовлетворяют условию

$$3 \lambda_0 \lambda_1 \lambda_2 = \mu_0 \lambda_1^3 + \mu_1 \lambda_2^3. \quad (8)$$

Действительно,

$$\begin{aligned} 3 \lambda_0 \lambda_1 \lambda_2 &= \frac{27 [\mu_0 (1-t)^3 + \mu_1 t^3] (1-t)^3 t^3}{[\mu(t)]^3} = \\ &= \mu_0 \left[\frac{3(1-t)^2 t}{\mu(t)} \right]^3 + \mu_1 \left[\frac{3(1-t) t^2}{\mu(t)} \right]^3 = \mu_0 \lambda_1^3 + \mu_1 \lambda_2^3. \end{aligned}$$

Если наряду с множеством \mathfrak{B}_1 ввести множество \mathfrak{B}_2 точек P вида (7), барицентрические координаты которых удовлетворяют условию (8), то, по существу, установлено, что $\mathfrak{B}_1 \subset \mathfrak{B}_2$. Проверим обратное включение $\mathfrak{B}_2 \subset \mathfrak{B}_1$.

Возьмём точку P из \mathfrak{B}_2 с барицентрическими координатами $(\lambda_0, \lambda_1, \lambda_2)$. Если $\lambda_1 = \lambda_2 = 0$, то $P = P_0$, так что $P \in \mathfrak{B}_1$. Варианты $\lambda_1 = 0, \lambda_2 > 0$ и $\lambda_1 > 0, \lambda_2 = 0$ невозможны в силу (8). Остаётся рассмотреть случай $\lambda_1 > 0, \lambda_2 > 0$ (в силу (8) и $\lambda_0 > 0$). Положим $t_0 = \frac{\lambda_2}{\lambda_1 + \lambda_2}$. Очевидно, что $t_0 \in (0, 1)$. Покажем, что $P = R_1(t_0)$. Этим завершится доказательство включения $\mathfrak{B}_2 \subset \mathfrak{B}_1$.

Имеем

$$\begin{aligned} \mu_0 (1-t_0)^3 + \mu_1 t_0^3 &= \mu_0 \left(\frac{\lambda_1}{\lambda_1 + \lambda_2} \right)^3 + \mu_1 \left(\frac{\lambda_2}{\lambda_1 + \lambda_2} \right)^3 = \frac{3 \lambda_0 \lambda_1 \lambda_2}{(\lambda_1 + \lambda_2)^3}, \\ 3(1-t_0)t_0 &= \frac{3 \lambda_1 \lambda_2}{(\lambda_1 + \lambda_2)^2}, \end{aligned}$$

поэтому

$$\mu(t_0) = \frac{3 \lambda_1 \lambda_2}{(\lambda_1 + \lambda_2)^2} \left(\frac{\lambda_0}{\lambda_1 + \lambda_2} + 1 \right) = \frac{3 \lambda_1 \lambda_2}{(\lambda_1 + \lambda_2)^3}.$$

Далее,

$$\frac{\mu_0 (1-t_0)^3 + \mu_1 t_0^3}{\mu(t_0)} = \lambda_0, \quad \frac{3(1-t_0)^2 t_0}{\mu(t_0)} = \lambda_1, \quad \frac{3(1-t_0) t_0^2}{\mu(t_0)} = \lambda_2.$$

Равенство (7) принимает требуемый вид $P = R_1(t_0)$.

Доказаны включения $\mathfrak{B}_1 \subset \mathfrak{B}_2$ и $\mathfrak{B}_2 \subset \mathfrak{B}_1$, которые гарантируют, что $\mathfrak{B}_1 = \mathfrak{B}_2$. Полученный результат можно сформулировать так.

ПРЕДЛОЖЕНИЕ 2. *Замкнутая проективная кривая Безье третьего порядка в стандартной форме (2) в барицентрических относительно точек P_0, P_1, P_2 координатах определяется неявным уравнением*

$$\mu_0 \lambda_1^3 + \mu_1 \lambda_2^3 - 3 \lambda_0 \lambda_1 \lambda_2 = 0.$$

3°. Внутри треугольника $P_0P_1P_2$ зафиксируем точку P_* с положительными барицентрическими координатами $(\lambda_0^*, \lambda_1^*, \lambda_2^*)$. Легко понять, как построить кривую Безье вида (2), проходящую через P_* . Для этого нужно выбрать положительные параметры μ_0, μ_1 кривой $R_1(t)$ так, чтобы они удовлетворяли линейному уравнению

$$(\lambda_1^*)^3 \mu_0 + (\lambda_2^*)^3 \mu_1 = 3 \lambda_0^* \lambda_1^* \lambda_2^*.$$

Перебирая все такие пары параметров (μ_0, μ_1) , построим поле замкнутых кривых Безье третьего порядка, проходящих через точку P_* (см. рис. 1). Более того, для любой кривой $R_1(t)$ из этого поля выполняется равенство $R_1(t_*) = P_*$, где аргумент $t_* = \frac{\lambda_2^*}{\lambda_1^* + \lambda_2^*}$ одинаков для всех допустимых μ_0, μ_1 .

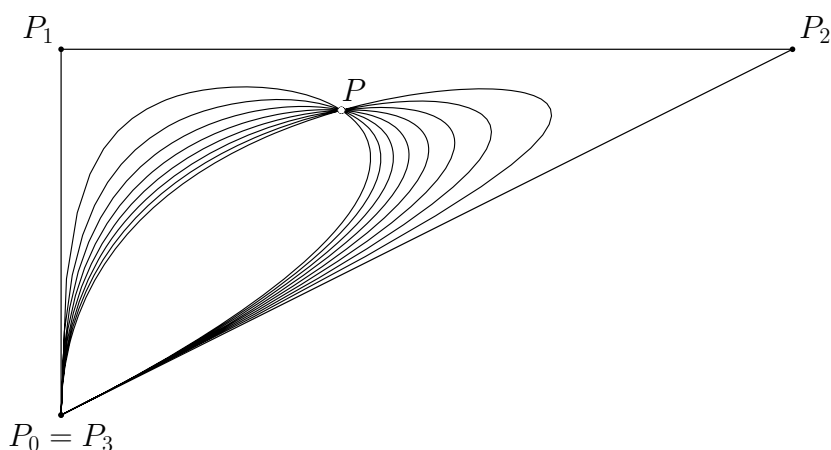


Рис. 1

4°. Рассмотрим внутри треугольника $P_0P_1P_2$ две различные точки P_*, Q_* с положительными барицентрическими координатами $(\lambda_0^*, \lambda_1^*, \lambda_2^*)$ и $(\beta_0^*, \beta_1^*, \beta_2^*)$ соответственно. Поставим задачу: провести через эти точки кривую Безье вида (2).

Предложение 2 позволяет сформулировать следующее утверждение.

ПРЕДЛОЖЕНИЕ 3. Для того чтобы кривая Безье вида (2) проходила через точки P_* и Q_* , необходимо и достаточно, чтобы система линейных уравнений

$$\begin{aligned} (\lambda_1^*)^3 \mu_0 + (\lambda_2^*)^3 \mu_1 &= 3 \lambda_0^* \lambda_1^* \lambda_2^*, \\ (\beta_1^*)^3 \mu_0 + (\beta_2^*)^3 \mu_1 &= 3 \beta_0^* \beta_1^* \beta_2^* \end{aligned} \quad (9)$$

имела положительное решение.

Покажем, что система (9) не имеет положительного решения, если

$$\frac{\lambda_2^*}{\lambda_1^*} = \frac{\beta_2^*}{\beta_1^*} =: k. \quad (10)$$

Допустим противное. В таком случае при некоторых положительных μ_0, μ_1 выполняются соотношения

$$\begin{aligned} \lambda_1^* (\mu_0 + k^3 \mu_1) &= 3k (1 - (1+k) \lambda_1^*), \\ \beta_1^* (\mu_0 + k^3 \mu_1) &= 3k (1 - (1+k) \beta_1^*). \end{aligned}$$

Поделив первое из них на второе, последовательно получим $\lambda_1^* = \beta_1^*$, $\lambda_2^* = \beta_2^*$, $\lambda_0^* = \beta_0^*$. Но это противоречит тому, что P_*, Q_* – различные точки.

При выполнении условия $\lambda_2^*/\lambda_1^* \neq \beta_2^*/\beta_1^*$ система (9) имеет единственное решение. Если это решение положительно, то через точки P_*, Q_* кривую Безье вида (2) провести можно (см. рис. 2).

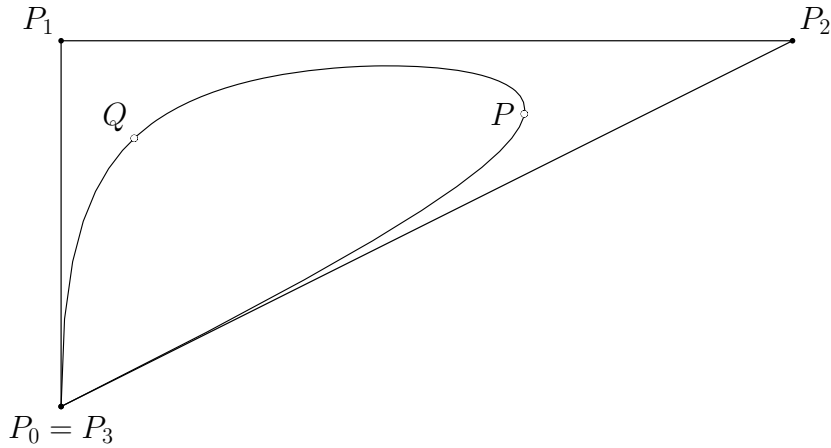


Рис. 2

5°. Условие (10) означает, что точки P_0, P_*, Q_* лежат на одной прямой. Чтобы разобраться в этом, обратимся к общему утверждению.

ПРЕДЛОЖЕНИЕ 4. Зафиксируем $k \in (0, +\infty)$ и положим $t_0 = \frac{k}{k+1}$,

$$Q = (1 - t_0) P_1 + t_0 P_2.$$

Тогда точки, барицентрические координаты $(\lambda_0, \lambda_1, \lambda_2)$ которых удовлетворяют соотношению

$$\lambda_2 = k \lambda_1, \quad \lambda_1 \in \left[0, \frac{1}{k+1}\right],$$

заполняют отрезок $[P_0, Q]$ (см. рис. 3).

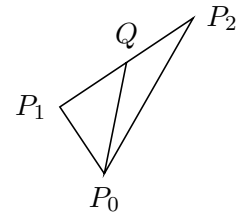


Рис. 3

Доказательство. Нас интересуют точки P вида

$$P = \lambda_0 P_0 + \lambda_1 P_1 + k \lambda_1 P_2.$$

Обозначим $s_0 = 1 - \lambda_0$. Очевидно, что $s_0 = (1+k) \lambda_1$. По условию λ_1 изменяется от 0 до $\frac{1}{k+1}$, поэтому s_0 изменяется от 0 до 1.

Имеем

$$\begin{aligned} P &= (1 - s_0) P_0 + s_0 \left[\frac{1}{1+k} P_1 + \frac{k}{k+1} P_2 \right] = \\ &= (1 - s_0) P_0 + s_0 [(1 - t_0) P_1 + t_0 P_2] = (1 - s_0) P_0 + s_0 Q. \end{aligned} \quad (11)$$

Как отмечалось, s_0 изменяется от 0 до 1. Значит, точки P вида (11) заполняют отрезок $[P_0, Q]$. Предложение доказано. \square

ЛИТЕРАТУРА

1. Farin G. *Curves and surfaces for CAGD*. 5th ed. San Diego: Academic Press, 2002.

ВОССТАНОВЛЕНИЕ СИГНАЛА В СЛУЧАЕ УТРАТЫ ОДНОГО ФРЕЙМОВОГО КОЭФФИЦИЕНТА

М. Н. Истомина

28 марта 2007 г.

1°. Напомним [1], что системой Мерседес-Бенц называется набор единичных n -мерных векторов $\{\varphi_1, \dots, \varphi_{n+1}\}$, удовлетворяющих условию

$$\langle \varphi_i, \varphi_j \rangle = -\frac{1}{n} \quad \text{при } i \neq j. \quad (1)$$

Система Мерседес-Бенц является жёстким фреймом с константой фрейма $A = 1 + \frac{1}{n}$, поэтому любой вектор $x \in \mathbb{R}^n$ можно представить в виде

$$x = \frac{n}{n+1} \sum_{i=1}^{n+1} c_i \varphi_i, \quad (2)$$

где коэффициенты c_i находятся по формуле

$$c_i = \langle x, \varphi_i \rangle, \quad i \in 1 : n+1.$$

Обычно вместо сигнала x по каналам связи передаются коэффициенты его разложения. При передаче часть коэффициентов может потеряться. Допустим, что утрачен один коэффициент c_k с некоторым номером $k \in 1 : n+1$. Это равносильно тому, что из системы $\{\varphi_i\}$ удалили вектор φ_k и получили систему

$$\{\varphi_1, \dots, \varphi_{k-1}, \varphi_{k+1}, \dots, \varphi_{n+1}\}. \quad (3)$$

От разложения (2) можно перейти к разложению по системе (3). Вывод формул для коэффициентов нового разложения является основной целью доклада.

2°. Рассмотрим матрицу Грама системы (3). Так как скалярные произведения различных векторов системы равны $-\frac{1}{n}$ и норма каждого вектора равна единице, то матрица Грама имеет вид

$$G = \{\langle \varphi_i, \varphi_j \rangle\}_{i \neq k, j \neq k} = \begin{bmatrix} 1 & -\frac{1}{n} & \dots & -\frac{1}{n} \\ -\frac{1}{n} & 1 & \dots & -\frac{1}{n} \\ \dots & \dots & \dots & \dots \\ -\frac{1}{n} & -\frac{1}{n} & \dots & 1 \end{bmatrix}.$$

Отметим, что эта матрица от k не зависит. В [1] указан явный вид обратной матрицы

$$G^{-1} = \frac{n}{n+1} \begin{bmatrix} 2 & 1 & \dots & 1 \\ 1 & 2 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 2 \end{bmatrix}. \quad (4)$$

(Легко проверить, что $GG^{-1} = I_n$, где I_n — единичная матрица порядка n .) Отсюда, в частности, следует, что матрица G невырождена, система (3) линейно независима и существует биортогональная система

$$\{\tilde{\varphi}_1, \dots, \tilde{\varphi}_{k-1}, \tilde{\varphi}_{k+1}, \dots, \tilde{\varphi}_{n+1}\}. \quad (5)$$

Биортогональность означает, что

$$\langle \varphi_i, \tilde{\varphi}_j \rangle = \begin{cases} 1 & \text{при } i = j, \\ 0 & \text{при } i \neq j. \end{cases}$$

Разложение вектора x по биортогональной системе (5) выглядит так:

$$x = \sum_{i \neq k} \langle x, \varphi_i \rangle \tilde{\varphi}_i = \sum_{i \neq k} c_i \tilde{\varphi}_i. \quad (6)$$

3°. Введём матрицы, столбцами которых являются векторы систем (3) и (5):

$$\begin{aligned} \Phi_k &= [\varphi_1, \dots, \varphi_{k-1}, \varphi_{k+1}, \dots, \varphi_{n+1}], \\ \tilde{\Phi}_k &= [\tilde{\varphi}_1, \dots, \tilde{\varphi}_{k-1}, \tilde{\varphi}_{k+1}, \dots, \tilde{\varphi}_{n+1}]. \end{aligned}$$

В силу биортогональности $\Phi_k^T \tilde{\Phi}_k = I_n$, так что $\tilde{\Phi}_k = (\Phi_k^T)^{-1}$. Это значит, что построение биортогональной системы равносильно обращению матрицы Φ_k^T .

По определению матрицы Грама $G = \Phi_k^T \Phi_k$. Отсюда следует, что $\Phi_k^T = G \Phi_k^{-1}$. Для $\tilde{\Phi}_k$ получаем представление $\tilde{\Phi}_k = \Phi_k G^{-1}$.

Обозначим $\tilde{c}^{(k)} = (c_1, \dots, c_{k-1}, c_{k+1}, \dots, c_{n+1})$ и перепишем формулу (6) в компактном виде

$$x = \tilde{\Phi}_k \tilde{c}^{(k)} = \Phi_k (G^{-1} \tilde{c}^{(k)}). \quad (7)$$

Согласно (4), компоненты вектора $c^{(k)} = \frac{n+1}{n} G^{-1} \tilde{c}^{(k)}$ можно вычислить по схеме

$$\begin{aligned} s_k &= \sum_{i=1}^{k-1} c_i + \sum_{i=k+1}^{n+1} c_i, \\ c_i^{(k)} &= c_i + s_k, \quad i \in 1 : n+1, \quad i \neq k. \end{aligned} \quad (8)$$

Остаётся развернуть формулу (7):

$$x = \frac{n}{n+1} \sum_{i \neq k} c_i^{(k)} \varphi_i. \quad (9)$$

Подведём итог.

ТЕОРЕМА. Разложение (2) произвольного вектора $x \in \mathbb{R}^n$ по системе Мерседес-Бенц порождает при любом $k \in 1 : n+1$ разложение (9), в котором коэффициенты $c_i^{(k)}$ вычисляются по схеме (8).

4°. Приведём пример. Рассмотрим в \mathbb{R}^2 фрейм Мерседес-Бенц [1]

$$\varphi_1 = \left(-\frac{\sqrt{3}}{2}, -\frac{1}{2}\right), \quad \varphi_2 = \left(\frac{\sqrt{3}}{2}, -\frac{1}{2}\right), \quad \varphi_3 = (0, 1).$$

Возьмём вектор $x = (0, -1)$. Для него $c_1 = \frac{1}{2}$, $c_2 = \frac{1}{2}$, $c_3 = -1$. Допустим, что коэффициент c_3 утерян ($k = 3$). Тогда

$$s_3 = 1, \quad c_1^{(3)} = \frac{3}{2}, \quad c_2^{(3)} = \frac{3}{2}.$$

По теореме должно выполняться равенство

$$x = \frac{2}{3} \left(\frac{3}{2} \varphi_1 + \frac{3}{2} \varphi_2 \right) = \varphi_1 + \varphi_2,$$

что на самом деле имеет место.

ЛИТЕРАТУРА

1. Малозёмов В. Н., Певный А. Б. *Фрейм Мерседес-Бенц в n -мерном пространстве* // Семинар «DHA & CAGD». Избранные доклады. 16 января 2007 г. (<http://dha.spb.ru/rep07.shtml#0116>).

МАКСИМАЛЬНАЯ ИЗБЫТОЧНОСТЬ ГАРМОНИЧЕСКИХ ФРЕЙМОВ

А. Б. Певный

28 марта 2007 г.

Излагаются основные сведения о комплексных гармонических фреймах по статье V. K. Goyal, J. Kovačević, J. A. Kelner [1].

1°. Система векторов $\Phi = \{\varphi_1, \dots, \varphi_m\}$ в \mathbb{C}^n называется *фреймом*, если существуют числа $A, B > 0$, такие, что

$$A \|x\|^2 \leq \sum_{i=1}^m |\langle x, \varphi_i \rangle|^2 \leq B \|x\|^2, \quad x \in \mathbb{C}^n. \quad (1)$$

Справедливо следующее простое утверждение.

ПРЕДЛОЖЕНИЕ 1. Система Φ является фреймом в \mathbb{C}^n тогда и только тогда, когда линейная оболочка системы Φ совпадает со всем пространством \mathbb{C}^n :

$$\mathcal{L}(\Phi) = \mathbb{C}^n. \quad (2)$$

Доказательство. Пусть выполнено (2). Введём обозначение

$$Q(x) = \sum_{i=1}^m |\langle x, \varphi_i \rangle|^2.$$

Нужно доказать, что $Q(x) > 0$ для всех $x \in \mathbb{C}^n$, $x \neq \mathbb{O}$. Допустим противное: существует вектор $x_0 \neq \mathbb{O}$, такой, что $Q(x_0) = 0$. Тогда

$$\langle x_0, \varphi_i \rangle = 0, \quad i \in 1 : m.$$

В силу (2) вектор x_0 разлагается по системе Φ :

$$x_0 = \sum_{i=1}^m c_i \varphi_i.$$

Отсюда

$$\|x_0\|^2 = \sum_{i=1}^m \bar{c}_i \langle x_0, \varphi_i \rangle = 0,$$

что противоречит условию $x_0 \neq \mathbb{O}$.

Пусть выполнены неравенства (1). Допустим, что $\mathcal{L}(\Phi) \neq \mathbb{C}^n$. Тогда существует вектор $x_0 \neq \mathbb{O}$, ортогональный ко всем элементам из $\mathcal{L}(\Phi)$. В частности, $\langle x_0, \varphi_i \rangle = 0$, $i \in 1 : m$. Приходим к равенству $Q(x_0) = 0$, которое противоречит (1). \square

СЛЕДСТВИЕ. Для любого фрейма $m \geq n$.

2°. Избыточность фрейма. По фреймовым коэффициентам $c_i = \langle x, \varphi_i \rangle$, $i \in 1 : m$, сигнал x можно восстановить:

$$x = \sum_{i=1}^m c_i \tilde{\varphi}_i,$$

где $\{\tilde{\varphi}_i\}_{i=1}^m$ — канонический двойственный фрейм (см. [2]).

Допустим, что $m > n$. Для передачи сигнала x по каналам связи часто передаются коэффициенты $\{c_i\}$. Допустим, часть этих коэффициентов при передаче потерялась. Может оказаться, что по оставшимся коэффициентам сигнал x восстановить всё-таки можно.

Будем говорить не об утрате коэффициентов, а об исключении части элементов из фрейма. Мы интересуемся вопросом, когда при таком исключении фрейм останется фреймом.

ОПРЕДЕЛЕНИЕ. Избыточностью фрейма $\Phi = \{\varphi_1, \dots, \varphi_m\}$ в \mathbb{C}^n называется такое число r , что при удалении любых r элементов фрейм остаётся фреймом, и существует подсистема из $r + 1$ векторов, при удалении которой фрейм перестаёт быть фреймом.

Очевидно, что $r \leq m - n$. Действительно, если удалить больше, чем $m - n$ векторов, то останется меньше n векторов, а они по предложению 1 не образуют фрейм.

3°. Примером фреймов с максимальной избыточностью ($r = m - n$) являются гармонические фреймы. Для того чтобы ввести их, зафиксируем натуральные числа m, n , где $m > n > 1$. Обозначим $\omega_m = e^{2\pi i/m}$ — корень m -й степени из единицы. Рассмотрим систему векторов $\varphi_0, \dots, \varphi_{m-1}$ из \mathbb{C}^n с компонентами

$$\varphi_k(j) = \frac{1}{\sqrt{n}} \omega_m^{kj}, \quad k \in 0 : m - 1, \quad j \in 0 : n - 1.$$

Очевидно, что

$$\|\varphi_k\|^2 = \frac{1}{n} \sum_{j=0}^{n-1} |\omega_m^{kj}|^2 = 1, \quad k \in 0 : m-1.$$

ПРЕДЛОЖЕНИЕ 2. Система $\{\varphi_k\}_{k=0}^{m-1}$ является жёстким фреймом в \mathbb{C}^n с константой фрейма $A = \frac{m}{n}$.

Доказательство. Разложим вектор $x \in \mathbb{C}^n$ по системе $\{\varphi_k\}_{k=0}^{m-1}$. Для этого удлинним x , добавив $m - n$ нулевых компонент. Получим вектор $\tilde{x} = (x(0), \dots, x(n-1), 0, \dots, 0) \in \mathbb{C}^m$. Рассмотрим ДПФ от вектора \tilde{x} :

$$\begin{aligned} C(k) &= (\mathcal{F}_m(\tilde{x}))(k) := \sum_{j=0}^{n-1} x(j) \omega_m^{-kj} = \sqrt{n} \sum_{j=0}^{n-1} x(j) \overline{\varphi_k(j)} = \\ &= \sqrt{n} \langle x, \varphi_k \rangle, \quad k \in 0 : m-1. \end{aligned}$$

По формуле обращения ДПФ

$$x(j) = \frac{1}{m} \sum_{k=0}^{m-1} C(k) \omega_m^{kj} = \frac{1}{m} \sum_{k=0}^{m-1} \sqrt{n} \langle x, \varphi_k \rangle \sqrt{n} \varphi_k(j), \quad j \in 0 : n-1,$$

или, в векторной форме записи,

$$x = \frac{n}{m} \sum_{k=0}^{m-1} \langle x, \varphi_k \rangle \varphi_k, \quad x \in \mathbb{C}^n.$$

Это разложение гарантирует, что система $\{\varphi_0, \dots, \varphi_{m-1}\}$ является жёстким фреймом с константой $A = \frac{m}{n}$. \square

Введённый фрейм $\{\varphi_k\}_{k=0}^{m-1}$ называется *гармоническим фреймом*.

4°. Избыточность гармонического фрейма.

ТЕОРЕМА. Избыточность гармонического фрейма равна $m - n$.

Доказательство. Удалим $m - n$ векторов, останется n векторов. Таким образом, нужно доказать, что при выборе любых n векторов из системы $\{\varphi_0, \dots, \varphi_{m-1}\}$ получается фрейм.

Возьмём произвольное подмножество $\{k_1, k_2, \dots, k_n\} \subset \{0, 1, \dots, m-1\}$, где $0 \leq k_1 < k_2 < \dots < k_n \leq m-1$. Подсистема $\{\varphi_{k_1}, \varphi_{k_2}, \dots, \varphi_{k_n}\}$ будет фреймом в \mathbb{C}^n , если она линейно независима, а это будет только тогда, когда определитель, составленный из строк $\varphi_{k_1}, \varphi_{k_2}, \dots, \varphi_{k_n}$, отличен от нуля.

Рассмотрим матрицу

$$\Phi_{n,n} = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & \omega_m^{k_1} & \omega_m^{2k_1} & \dots & \omega_m^{(n-1)k_1} \\ 1 & \omega_m^{k_2} & \omega_m^{2k_2} & \dots & \omega_m^{(n-1)k_2} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \omega_m^{k_n} & \omega_m^{2k_n} & \dots & \omega_m^{(n-1)k_n} \end{bmatrix}.$$

С точностью до множителя $\frac{1}{\sqrt{n}}$ это матрица Вандермонда, поэтому для её определителя справедлива формула

$$\det \Phi_{n,n} = \left(\frac{1}{\sqrt{n}} \right)^n \prod_{i>j} (\omega_m^{k_i} - \omega_m^{k_j}).$$

Так как числа $\omega_m^{k_i}$, $i \in 1 : n$, попарно различны, то $\det \Phi_{n,n} \neq 0$.

Значит, система $\{\varphi_{k_i}\}_{i=1}^n$ является фреймом. □

ЛИТЕРАТУРА

1. Goyal V. K., Kovačević J., Kelner J. A. *Quantized frame expansions with erasures* // Applied and computational harmonic analysis. 2001. V. 10. P. 203–233.
2. Певный А. Б. *Фреймы в конечномерных пространствах и задача минимизации фреймового потенциала* // Семинар «DHA & CAGD». Избранные доклады. 28 марта 2006 г. (<http://dha.spb.ru/rep06.shtml#0328>).

ПОВЕРХНОСТИ КУНСА НА ТРЕУГОЛЬНИКЕ

В. Н. Малозёмов

А. Н. Сергеев

Н. В. Чашников

7 апреля 2007 г.

1°. Пусть $\Delta = \{(u, v, w) \mid u + v + w = 1, u \geq 0, v \geq 0, w \geq 0\}$. Ставится задача: *построить по вектор-функциям $g_1, g_2, g_3: [0, 1] \rightarrow \mathbb{R}^3$ возможно более простую вектор-функцию $s: \Delta \rightarrow \mathbb{R}^3$, удовлетворяющую условиям*

$$s(u, 0, 1 - u) \equiv g_1(u), \quad s(1 - v, v, 0) \equiv g_2(v), \quad s(0, 1 - w, w) \equiv g_3(w). \quad (1)$$

Последовательно подставляя в тождества (1) вместо u, v и w значения 0 и 1, получаем необходимые *условия согласования* на вектор-функции g_1, g_2 и g_3 :

$$\begin{aligned} g_1(0) &= s(0, 0, 1) = g_3(1), \\ g_2(0) &= s(1, 0, 0) = g_1(1), \\ g_3(0) &= s(0, 1, 0) = g_2(1). \end{aligned} \quad (2)$$

Будем считать, что условия (2) выполнены.

Дадим геометрическую интерпретацию этой задачи. Обозначим

$$A = g_1(1) = g_2(0), \quad B = g_2(1) = g_3(0), \quad C = g_3(1) = g_1(0).$$

Вектор-функция $g_1(u)$ при $u \in [0, 1]$ задаёт кривую, соединяющую точки C и A . Аналогично вектор-функции g_2, g_3 задают кривые, соединяющие пары точек A и B , B и C соответственно. Элементы множества Δ можно рассматривать как барицентрические координаты точки на треугольнике. Тогда вектор-функция $s: \Delta \rightarrow \mathbb{R}^3$ задаёт параметрическую поверхность с треугольной областью определения, а условия (1) означают, что кривые g_1, g_2 и g_3 являются граничными для этой поверхности.

2°. Пусть $H: [0, 1] \rightarrow \mathbb{R}$ — произвольная функция, удовлетворяющая условиям $H(0) = 0, H(1) = 1$. Положим

$$\begin{aligned} s(u, v, w) &= H(1 - v) g_1\left(\frac{u}{1 - v}\right) + H(1 - w) g_2\left(\frac{v}{1 - w}\right) + \\ &+ H(1 - u) g_3\left(\frac{w}{1 - u}\right) - H(u)A - H(v)B - H(w)C. \end{aligned} \quad (3)$$

Формально вектор-функция s не определена, если один из аргументов равен единице. Но если $v = 1$, то $H(1 - v) = 0$, поэтому будем считать, что первое слагаемое в (3) равно нулю. Аналогично поступим в случаях $u = 1$ и $w = 1$. Таким образом, можно считать, что вектор-функция $s(u, v, w)$ определена на всём множестве Δ .

ПРЕДЛОЖЕНИЕ 1. Вектор-функция $s(u, v, w)$ вида (3) удовлетворяет условиям (1).

Доказательство. Проверим, что выполняется первое равенство в (1). Имеем

$$\begin{aligned} s(u, 0, 1 - u) &= H(1)g_1(u) + H(u)g_2(0) + H(1 - u)g_3(1) - \\ &\quad - H(u)A - H(0)B - H(1 - u)C = g_1(u). \end{aligned}$$

Аналогично проверяются второе и третье равенства в (1). □

3°. Поверхность, определяемая вектор-функцией (3), называется *поверхностью Кунса “сторона-вершина” на треугольнике*. Чтобы пояснить смысл этого названия, обратимся к геометрической интерпретации формулы (3), в случае $H(t) = t$. Перепишем её в виде

$$s(u, v, w) = s_1(u, v, w) + s_2(u, v, w) + s_3(u, v, w) - 2s_4(u, v, w),$$

где

$$\begin{aligned} s_1(u, v, w) &= (1 - v)g_1\left(\frac{u}{1 - v}\right) + vB, \\ s_2(u, v, w) &= (1 - w)g_2\left(\frac{v}{1 - w}\right) + wC, \\ s_3(u, v, w) &= (1 - u)g_3\left(\frac{w}{1 - u}\right) + uA, \\ s_4(u, v, w) &= uA + vB + wC. \end{aligned}$$

Введём обозначения

$$e_1 = (1, 0, 0), \quad e_2 = (0, 1, 0), \quad e_3 = (0, 0, 1).$$

Тогда точку $p = (u, v, w) \in \Delta$ можно представить в виде $p = ue_1 + ve_2 + we_3$.

ЛЕММА 1. Пусть $p_0 = u_0 e_1 + (1 - u_0)e_3$, где $u_0 \in [0, 1]$. Для того чтобы точка $p = (u, v, w) \in \Delta$ принадлежала отрезку $[p_0, e_2]$, необходимо и достаточно, чтобы

$$u = u_0(1 - v), \quad v \in [0, 1]. \quad (4)$$

Доказательство. Необходимость. Пусть $p \in [p_0, e_2]$. При некотором $t \in [0, 1]$ справедливо равенство

$$p = te_2 + (1 - t)[u_0 e_1 + (1 - u_0)e_3] = (1 - t)u_0 e_1 + te_2 + (1 - t)(1 - u_0)e_3.$$

В частности, $u = (1 - t)u_0$, $v = t$, что равносильно (4).

Достаточность. Пусть для точки $p \in \Delta$ выполняется условие (4). Тогда

$$w = 1 - v - u = 1 - v - u_0(1 - v) = (1 - v)(1 - u_0)$$

и

$$\begin{aligned} p &= u_0(1 - v)e_1 + ve_2 + (1 - u_0)(1 - v)e_3 = \\ &= (1 - v)[u_0 e_1 + (1 - u_0)e_3] + ve_2 = (1 - v)p_0 + ve_2. \end{aligned}$$

Значит, $p \in [p_0, e_2]$. Лемма доказана. \square

ЛЕММА 2. Справедливо равенство множеств

$$\{s_1(p) \mid p \in [p_0, e_2]\} = [g_1(u_0), B]. \quad (5)$$

Доказательство. Обозначим множества, стоящие в левой и правой частях равенства (5), через Q и T соответственно. Нужно показать, что $Q = T$.

Пусть $q \in Q$, то есть $q = s_1(p)$, где $p = (u, v, w) \in [p_0, e_2]$. Если $v = 1$, то $p = (0, 1, 0)$ и $q = s_1(0, 1, 0) = B \in T$. Если же $v < 1$, то по предыдущей лемме $\frac{u}{1-v} = u_0$, поэтому $q = (1 - v)g_1(u_0) + vB \in T$. В обоих случаях из того, что $q \in Q$, следует, что $q \in T$. Значит, $Q \subset T$.

Наоборот, пусть $r \in T$, то есть $r = (1 - t)g_1(u_0) + tB$ при некотором $t \in [0, 1]$. Положим $p = (u_0(1 - t), t, (1 - u_0)(1 - t))$. Ясно, что $p \in \Delta$. Из леммы 1 следует, что $p \in [p_0, e_2]$. Если $t < 1$, то $s_1(p) = (1 - t)g_1(u_0) + tB = r$. Если же $t = 1$, то $r = B$ и $s_1(p) = s_1(0, 1, 0) = B = r$. В обоих случаях $s_1(p) = r$, так что $r \in Q$. Доказано обратное включение $T \subset Q$, а с ним и равенство $T = Q$. \square

Лемма 2 показывает, что поверхность, определяемая вектор-функцией s_1 , состоит из отрезков вида $[g_1(u_0), B]$ при $u_0 \in [0, 1]$. Иными словами, вектор-функция s_1 задаёт линейчатую поверхность, образованную отрезками, соединяющими точки кривой g_1 с точкой B . На рис. 1 приведён пример граничных

кривых, а на рис. 2 изображена поверхность s_1 , построенная для этих кривых. Аналогичным образом вектор-функция s_2 задаёт линейчатую поверхность, образованную отрезками, соединяющими точки кривой g_2 с точкой C (см. рис. 3), а s_3 — линейчатую поверхность, образованную отрезками, соединяющими точки кривой g_3 с точкой A (см. рис. 4). Поверхность, задаваемая вектор-функцией s_4 представляет собой участок плоскости, ограниченный треугольником с вершинами A , B и C (см. рис. 5). Поверхность Кунса приведена на рис. 6.

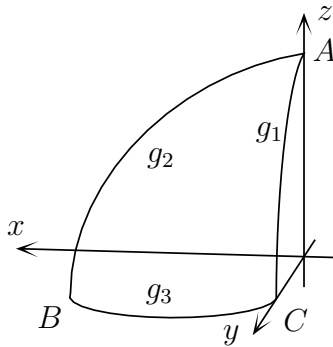
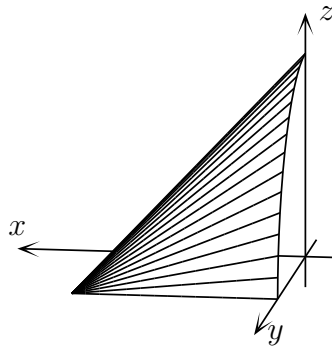
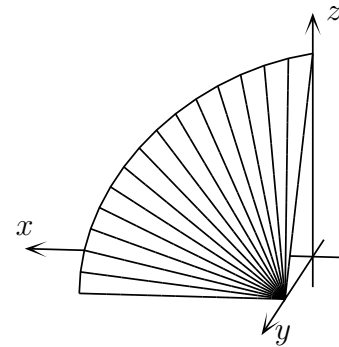
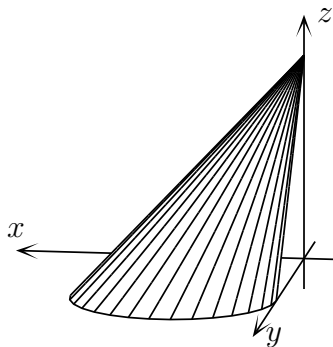
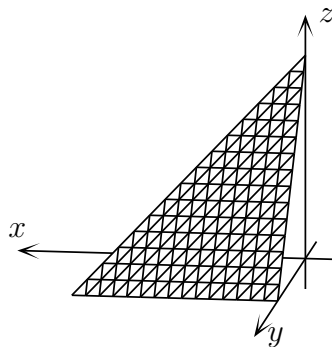
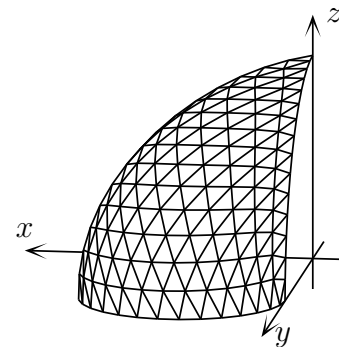
Рис. 1. Кривые g_1 , g_2 , g_3 Рис. 2. Поверхность $s_1(u, v, w)$ Рис. 3. Поверхность $s_2(u, v, w)$ Рис. 4. Поверхность $s_3(u, v, w)$ Рис. 5. Поверхность $s_4(u, v, w)$ 

Рис. 6. Поверхность Кунса

4°. Рассмотрим случай, когда граничные кривые g_1 , g_2 и g_3 являются кривыми Безье второго порядка. Пусть точки C , P_{10} , A — полюсы g_1 , точки A , P_{11} , B — полюсы g_2 , точки B , P_{01} , C — полюсы g_3 . Положим $P_{00} = C$, $P_{20} = A$,

$P_{02} = B$. Тогда для кривых Безье g_1 , g_2 и g_3 справедливы представления

$$\begin{aligned} g_1(u) &= \sum_{i=0}^2 P_{i0} C_2^i u^i (1-u)^{2-i}, \\ g_2(v) &= \sum_{k=0}^2 P_{2-k,k} C_2^k v^k (1-v)^{2-k}, \\ g_3(w) &= \sum_{j=0}^2 P_{0,2-j} C_2^j w^j (1-w)^{2-j}. \end{aligned} \quad (6)$$

По шести полюсам P_{ij} можно построить поверхность Безье на треугольнике (см. [1]):

$$\begin{aligned} b(u, v) &= \sum_{i=0}^2 \sum_{j=0}^{2-i} P_{ij} \frac{2!}{i! j! (2-i-j)!} u^i v^j (1-u-v)^{2-i-j}, \\ u &\geq 0, \quad v \geq 0, \quad u+v \leq 1. \end{aligned} \quad (7)$$

ПРЕДЛОЖЕНИЕ 2. Поверхность Кунса, построенная по формуле (3) для граничных кривых (6) с $H(t) = t^2$, совпадает с поверхностью Безье (7), точнее

$$s(u, v, 1-u-v) = b(u, v) \quad \text{при} \quad u \geq 0, v \geq 0, u+v \leq 1.$$

Доказательство. Преобразуем первое слагаемое в (3):

$$\begin{aligned} H(1-v) g_1\left(\frac{u}{1-v}\right) &= (1-v)^2 \sum_{i=0}^2 P_{i0} C_2^i \left(\frac{u}{1-v}\right)^i \left(\frac{1-v-u}{1-v}\right)^{2-i} = \\ &= \sum_{i=0}^2 P_{i0} C_2^i u^i w^{2-i}. \end{aligned}$$

Аналогично для второго и третьего слагаемых в (3) имеем

$$\begin{aligned} H(1-w) g_2\left(\frac{v}{1-w}\right) &= \sum_{k=0}^2 P_{2-k,k} C_2^k v^k u^{2-k}, \\ H(1-u) g_3\left(\frac{w}{1-u}\right) &= \sum_{j=0}^2 P_{0,2-j} C_2^j w^j v^{2-j}. \end{aligned}$$

Подставим полученные выражения в (3). Придём к формуле

$$s(u, v, w) = (w^2 P_{00} + 2uw P_{10} + u^2 P_{20}) + (u^2 P_{20} + 2vu P_{11} + v^2 P_{02}) +$$

$$\begin{aligned}
& + (v^2 P_{02} + 2wv P_{01} + w^2 P_{00}) - (u^2 A + v^2 B + w^2 C) = \\
& = w^2 P_{00} + v^2 P_{02} + u^2 P_{20} + 2uw P_{10} + 2vu P_{11} + 2wv P_{01}.
\end{aligned}$$

Если в последнем выражении заменить w на $1 - u - v$, то получится правая часть формулы (7). Следовательно, $s(u, v, 1 - u - v) = b(u, v)$, что и требовалось доказать. \square

На рис. 7 приведены полюсы и построенные по ним кривые Безье, а на рис. 8 изображена поверхность Кунса для этих граничных кривых. Она совпадает с соответствующей поверхностью Безье.

Дальнейшую информацию о поверхностях Кунса на треугольнике можно найти в книге [2] и приведённом там списке литературы.

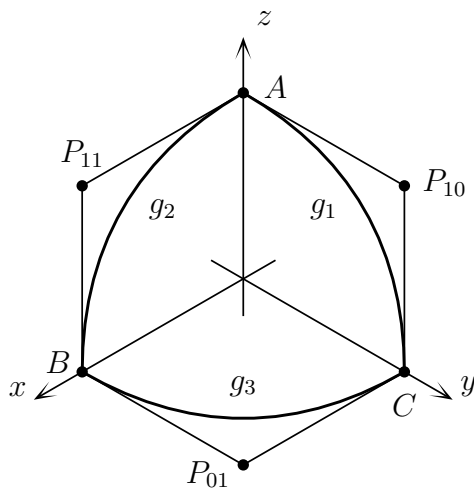


Рис. 7. Граничные кривые

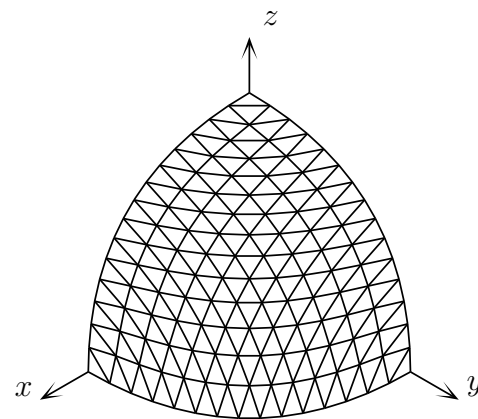


Рис. 8. Поверхность Кунса-Безье

ЛИТЕРАТУРА

1. Капелюхин И. А., Малозёмов В. Н., Сергеев А. Н. *Поверхности Безье на треугольнике. Перепараметризация* // Семинар «DHA & CAGD». Избранные доклады. 10 марта 2007 г. (<http://dha.spb.ru/rep07.shtml#0310>).
2. G. Farin. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.

ЧЕТВЁРТОЕ ОПРЕДЕЛЕНИЕ ЖЁСТКОГО ФРЕЙМА

В. Н. Малозёмов А. Б. Певный

30 мая 2007 г.

1°. Напомним [1], что система ненулевых n -мерных векторов $\{\varphi_1, \dots, \varphi_m\}$ при $m \geq n$ называется жёстким фреймом с константой фрейма $A > 0$, если выполнено одно из трёх эквивалентных условий:

$$\begin{aligned} 1) \quad & x = \frac{1}{A} \sum_{k=1}^m \langle x, \varphi_k \rangle \varphi_k \quad \forall x \in \mathbb{R}^n; \\ 2) \quad & \sum_{k=1}^m [\langle x, \varphi_k \rangle]^2 = A \|x\|^2 \quad \forall x \in \mathbb{R}^n; \\ 3) \quad & \Phi \Phi^T = A I_n, \end{aligned}$$

где Φ — матрица со столбцами $\varphi_1, \dots, \varphi_m$ и I_n — единичная матрица порядка n .

Для константы фрейма A можно получить явное представление. Обозначим через $\text{tr}(S)$ след квадратной матрицы S . Согласно 3),

$$\text{tr}(\Phi \Phi^T) = \text{tr}(A I_n) = n A.$$

Вместе с тем, $\text{tr}(\Phi \Phi^T) = \text{tr}(\Phi^T \Phi)$, поэтому

$$n A = \text{tr}(\Phi^T \Phi) = \sum_{k=1}^m \|\varphi_k\|^2.$$

Отсюда следует, что

$$A = \frac{1}{n} \sum_{k=1}^m \|\varphi_k\|^2.$$

2°. Приводимое ниже утверждение содержит, по существу, ещё одно эквивалентное определение жёсткого фрейма.

ПРЕДЛОЖЕНИЕ 1. Система ненулевых n -мерных векторов $\{\varphi_1, \dots, \varphi_m\}$, $m \geq n$, образует жёсткий фрейм тогда и только тогда, когда

$$\sum_{i,j=1}^m [\langle \varphi_i, \varphi_j \rangle]^2 = \frac{1}{n} \left(\sum_{i=1}^m \|\varphi_i\|^2 \right)^2. \quad (1)$$

Доказательство. Пусть Φ — матрица со столбцами $\varphi_1, \dots, \varphi_m$ и $S = \Phi \Phi^T$. Тогда

$$\begin{aligned} \operatorname{tr}(S) &= \operatorname{tr}(\Phi^T \Phi) = \sum_{i=1}^m \|\varphi_i\|^2, \\ \operatorname{tr}(S^2) &= \operatorname{tr}((\Phi \Phi^T \Phi) \Phi^T) = \operatorname{tr}((\Phi^T \Phi)^2) = \\ &= \sum_{i=1}^m \left(\sum_{j=1}^m \langle \varphi_i, \varphi_j \rangle \langle \varphi_j, \varphi_i \rangle \right) = \sum_{i,j=1}^m [\langle \varphi_i, \varphi_j \rangle]^2. \end{aligned}$$

Равенство (1) принимает вид

$$\operatorname{tr}(S^2) = \frac{1}{n} (\operatorname{tr}(S))^2. \quad (2)$$

Если $\{\varphi_1, \dots, \varphi_m\}$ — жёсткий фрейм, то, согласно 3), $S = A I_n$. В этом случае условие (2), очевидно, выполняется. Проверим обратное, что из (2) следует равенство $S = A I_n$ с $A > 0$.

Матрица $S = \Phi \Phi^T$ симметрична и неотрицательно определена. Обозначим через $\lambda_1, \dots, \lambda_n$ её собственные числа и через h_1, \dots, h_n — соответствующие ортонормированные собственные векторы. Как известно [2, с. 47],

$$S = \sum_{k=1}^n \lambda_k h_k h_k^T.$$

Легко проверить, что

$$\begin{aligned} S^2 &= \sum_{k=1}^n \lambda_k^2 h_k h_k^T, \\ \operatorname{tr}(S) &= \sum_{k=1}^n \lambda_k, \quad \operatorname{tr}(S^2) = \sum_{k=1}^n \lambda_k^2. \end{aligned}$$

Согласно (2), $\sum_{k=1}^n \lambda_k^2 = \frac{1}{n} (\sum_{k=1}^n \lambda_k)^2$ или

$$\left(\frac{1}{n} \sum_{k=1}^n \lambda_k^2 \right)^{1/2} = \frac{1}{n} \sum_{k=1}^n \lambda_k.$$

Получили, что среднее квадратическое неотрицательных чисел $\lambda_1, \dots, \lambda_n$ равно их среднему арифметическому. Это возможно только в случае $\lambda_1 = \dots = \lambda_n =: A$, когда $S = A I_n$. Поскольку по условию векторы φ_i — ненулевые и

$$\sum_{i=1}^m \|\varphi_i\|^2 = \text{tr}(S) = n A,$$

то $A > 0$. Предложение доказано. \square

3°. Выражение, стоящее в левой части (1), называется *фреймовым потенциалом* системы $\{\varphi_1, \dots, \varphi_m\}$ и обозначается $\text{FP}(\Phi)$. Учитывая неравенство между средним квадратическим и средним арифметическим, приходим к такому заключению [3, 4].

ПРЕДЛОЖЕНИЕ 2. Для любой системы $\{\varphi_1, \dots, \varphi_m\}$, $m \geq n$, ненулевых n -мерных векторов справедливо неравенство

$$\text{FP}(\Phi) \geq \frac{1}{n} \left(\sum_{i=1}^m \|\varphi_i\|^2 \right)^2.$$

Равенство достигается только на жёстких фреймах.

4°. Приведём два следствия из предложения 1.

СЛЕДСТВИЕ 1. Система единичных n -мерных векторов $\{\varphi_1, \dots, \varphi_m\}$, $m \geq n$, образует жёсткий фрейм тогда и только тогда, когда

$$\left(\frac{1}{m^2} \sum_{i,j=1}^m [\langle \varphi_i, \varphi_j \rangle]^2 \right)^{1/2} = \frac{1}{\sqrt{n}},$$

т. е. когда среднее квадратическое модулей скалярных произведений $\langle \varphi_i, \varphi_j \rangle$, $i, j \in 1 : m$, равно $\frac{1}{\sqrt{n}}$.

СЛЕДСТВИЕ 2. Система $\{\varphi_1, \dots, \varphi_n\}$, состоящая из n единичных n -мерных векторов, образует жёсткий фрейм тогда и только тогда, когда эта система является ортонормированным базисом в \mathbb{R}^n .

Действительно, в данном случае условие (1) принимает вид

$$\sum_{i,j=1}^n [\langle \varphi_i, \varphi_j \rangle]^2 = n.$$

Учитывая, что φ_i — единичные векторы, приходим к эквивалентному равенству

$$\sum_{i \neq j} [\langle \varphi_i, \varphi_j \rangle]^2 = 0,$$

гарантирующему справедливость следствия 2.

5°. Отдельно рассмотрим случай $m = n + 1$.

ПРЕДЛОЖЕНИЕ 3. Для того чтобы система $\{\varphi_1, \dots, \varphi_{n+1}\}$, состоящая из $n+1$ единичных n -мерных векторов, была жёстким фреймом, необходимо и достаточно, чтобы выполнялось условие

$$|\langle \varphi_i, \varphi_j \rangle| = \frac{1}{n} \quad \text{при } i \neq j. \quad (3)$$

Доказательство. Достаточность. При $m = n + 1$ и единичных φ_i равенство (1) преобразуется к виду

$$\sum_{i \neq j} [\langle \varphi_i, \varphi_j \rangle]^2 = 1 + \frac{1}{n}. \quad (4)$$

Очевидно, что (4) следует из (3).

Необходимость. Возьмём жёсткий фрейм $\{\varphi_1, \dots, \varphi_{n+1}\}$ в \mathbb{R}^n с единичными φ_k . Как известно [1], элементы такого фрейма допускают представление

$$\varphi_k = \sigma_k U b_k^n, \quad k \in 1 : n + 1,$$

где $\sigma_k = \pm 1$, U — некоторая ортогональная матрица и $\{b_1^n, \dots, b_{n+1}^n\}$ — фрейм Мерседес-Бенц, обладающий, в частности, таким свойством

$$\langle b_i^n, b_j^n \rangle = -\frac{1}{n} \quad \text{при } i \neq j.$$

Приняв это во внимание, получим при $i \neq j$

$$|\langle \varphi_i, \varphi_j \rangle| = |\langle U b_i^n, U b_j^n \rangle| = |\langle U^T U b_i^n, b_j^n \rangle| = |\langle b_i^n, b_j^n \rangle| = \frac{1}{n}.$$

Предложение доказано. □

6°. Дальнейшая информация о фреймах в конечномерных пространствах имеется в [3, 4, 5, 6, 7].

ЛИТЕРАТУРА

1. Малозёмов В. Н., Певный А. Б. *Системы Мерседес-Бенц и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 28 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0228>).
2. Малозёмов В. Н. *Линейная алгебра без определителей. Квадратичная функция*. СПб: Изд-во СПбГУ, 1997.

3. Benedetto J. J., Fickus M. *Finite normalized tight frames* // Adv. Comput. Math. 2003. Vol. 18. No. 2–4. P. 357–385.
4. Casazza P. G. *Custom building finite frames* // Contemporary Math. 2004. Vol. 345. P. 61–86.
5. Casazza P. G., Kovačević J. *Equal-norm tight frames with erasures* // Adv. Comput. Math. 2003. Vol. 18. No. 2–4. P. 387–430.
6. Goyal V. K., Kovačević J., Kelner J. A. *Quantized frame expansions with erasures* // Appl. Comput. Harmonic Anal. 2001. Vol. 10. No. 3. P. 203–233.
7. Han D., Larson D. R. *Frames, bases and group representation* // Memoires Amer. Math. Soc. 2000. Vol. 147. No. 697. P. 1–94.

МОДЕЛИРОВАНИЕ ПОВЕРХНОСТЕЙ ВРАЩЕНИЯ

М. И. Григорьев

27 июня 2007 г.

1°. Пусть в \mathbb{R}^3 задана параметрическая кривая $F(u)$, лежащая в плоскости OXZ :

$$F(u) = (f_0(u), 0, f_1(u)), \quad f_0(u) > 0, \quad u \in [a, b].$$

Зафиксируем некоторое значение параметра u из отрезка $[a, b]$ и рассмотрим проективную кривую Безье второго порядка [1]

$$R(u, v) = \frac{P_0(u) b_0^2(v) + \sqrt{\mu} P_1(u) b_1^2(v) + P_2(u) b_2^2(v)}{b_0^2(v) + \sqrt{\mu} b_1^2(v) + b_2^2(v)}, \quad v \in [0, 1], \quad (1)$$

построенную по полюсам

$$\begin{aligned} P_0(u) &= F(u) = (f_0(u), 0, f_1(u)), & P_1(u) &= (f_0(u), f_0(u), f_1(u)), \\ P_2(u) &= (0, f_0(u), f_1(u)) \end{aligned}$$

с некоторым положительным параметром μ (уравнение кривой представлено в стандартной форме [2]). (Здесь $b_i^2(v)$, $i \in 0 : 2$, суть базисные полиномы Бернштейна второго порядка [3].) Отметим, что кривая $R(u, v)$ лежит в плоскости $Z = f_1(u)$.

Когда параметр u пробегает весь отрезок $[a, b]$, кривая $R(u, v)$ порождает поверхность в пространстве \mathbb{R}^3 (рис. 1). Из свойств базисных полиномов Бернштейна следует, что

$$R(u, 0) = P_0(u) = F(u), \quad R(u, 1) = P_2(u).$$

2°. Примем параметр μ равным $1/2$. Зафиксируем некоторое значение параметра u из отрезка $[a, b]$. Полюса $P_0(u)$, $P_1(u)$, $P_2(u)$ расположены в вершинах квадрата с длиной стороны $f_0(u)$, лежащего в плоскости $Z = f_1(u)$. Известно [2], что проективная кривая Безье второго порядка, построенная по таким полюсам с $\mu = 1/2$, является четвертью окружности радиуса $f_0(u)$ (рис. 2).

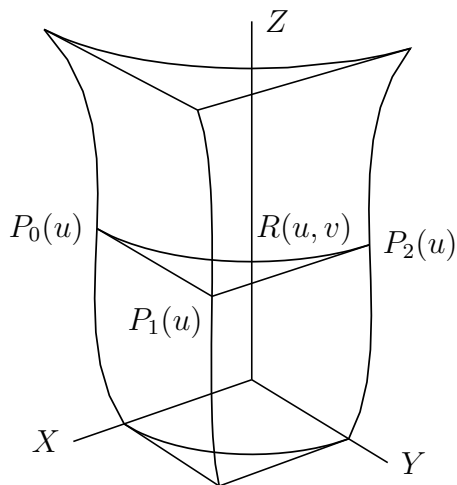


Рис. 1

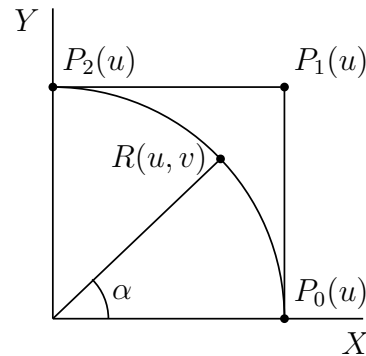


Рис. 2

Зафиксируем также некоторое значение параметра v из отрезка $[0, 1]$. Точка $R(u, v)$ соответствует вращению полюса $P_0(u)$ вокруг оси OZ на угол α , косинус которого равен

$$\cos \alpha = \frac{f_0(u) b_0^2(v) + \frac{\sqrt{2}}{2} f_0(u) b_1^2(v)}{f_0(u)} = b_0^2(v) + \frac{\sqrt{2}}{2} b_1^2(v).$$

Заметим, что величина угла α не зависит от параметра u , значит, вышесказанное верно для всех u из $[a, b]$. То есть кривая на поверхности $R(u, v)$, соответствующая изменению параметра u при данном значении параметра v совпадает с кривой $F(u)$, повернутой на угол α вокруг оси OZ .

Таким образом, сечение поверхности $R(u, v)$ любой плоскостью, проходящей через ось OZ представляет собой кривую $F(u)$, повернутую на соответствующий угол вокруг оси OZ , а сечение $R(u, v)$ любой плоскостью, перпендикулярной оси OZ — четверть окружности. Значит, верно следующее

ПРЕДЛОЖЕНИЕ. Поверхность $R(u, v)$, $u \in [a, b]$, $v \in [0, 1]$ при выбранном значении параметра $\mu = 1/2$ представляет собой четверть поверхности вращения кривой $F(u)$ вокруг оси OZ .

Полная поверхность вращения может быть получена при помощи двух последовательных преобразований: отражения поверхности $R(u, v)$ относительно плоскости OXZ , а затем отражения полученной поверхности относительно плоскости OYZ .

Отметим также, что ограничение $f_0(u) > 0$, $u \in [a, b]$, может быть ослаблено. В случае, если существует $u_* \in [a, b]$ такое, что $f_0(u_*) = 0$, то поверхность $R(u, v)$ будет иметь вырожденную точку $R(u_*, v) = (0, 0, f_1(u_*))$, $v \in [0, 1]$.

3°. Рассмотрим случай, когда $F(u)$ представляет собой проективную кривую Безье n -й степени

$$F(u) = \frac{\sum_{i=0}^n w_i P_i b_i^n(u)}{\sum_{i=0}^n w_i b_i^n(u)}, \quad u \in [0, 1], \quad (2)$$

построенную по полюсам $P_i = (p_{i0}, 0, p_{i1})$, $p_{i0} \geq 0$, $i \in 0 : n$, лежащим в плоскости OXZ , с некоторыми положительными весами w_0, w_1, \dots, w_n . Положим,

$$P_{i0} = P_i = (p_{i0}, 0, p_{i1}), \quad P_{i1} = (p_{i0}, p_{i0}, p_{i1}), \quad P_{i2} = (0, p_{i0}, p_{i1}), \quad i \in 0 : n. \quad (3)$$

Перепишем (1) с учётом (2) и (3). Получим,

$$\begin{aligned} R(u, v) &= \frac{\sum_{i=0}^n w_i (P_{i0} b_i^n(u) b_0^2(v) + \sqrt{\mu} P_{i1} b_i^n(u) b_1^2(v) + P_{i2} b_i^n(u) b_2^2(v))}{(\sum_{i=0}^n w_i b_i^n(u)) (b_0^2(v) + \sqrt{\mu} b_1^2(v) + b_2^2(v))} = \\ &= \frac{\sum_{i=0}^n \sum_{j=0}^2 \omega_{ij} P_{ij} b_i^n(u) b_j^2(v)}{\sum_{i=0}^n \sum_{j=0}^2 \omega_{ij} b_i^n(u) b_j^2(v)}, \end{aligned}$$

где

$$\omega_{i0} = w_i, \quad \omega_{i1} = \sqrt{\mu} w_i, \quad \omega_{i2} = w_i, \quad i \in 0 : n. \quad (4)$$

То есть в данном случае поверхность $R(u, v)$ является проективной поверхностью Безье степени $n \times 2$ [1], построенной по полюсам P_{ij} с весами ω_{ij} , $i \in 0 : n$, $j \in 0 : 2$.

4°. В [4] было установлено, что можно подобрать расположение полюсов и значения весов так, чтобы построенная по ним проективная поверхность Безье второго порядка представляла собой восьмую часть сферы. Аналогичный результат можно получить, воспользовавшись предыдущим пунктом 3°.

Зафиксируем три полюса и три положительных веса:

$$\begin{aligned} P_0 &= (1, 0, 0), & w_0 &= 1, \\ P_1 &= (1, 0, 1), & w_1 &= \frac{\sqrt{2}}{2}, \\ P_2 &= (0, 0, 1), & w_2 &= 1. \end{aligned} \quad (5)$$

Построенная по этим данным проективная кривая Безье второго порядка $F(u)$ является четвертью окружности [2]. Положим $\mu = 1/2$ и построим поверхность вращения $R(u, v)$, которая, очевидно, будет являться восьмой частью сферы. В пункте 3° было показано, что данная поверхность также представляет собой проективную поверхность Безье второго порядка. Положения полюсов этой поверхности могут быть найдены из (3) и (5):

$$\begin{aligned} P_{00} &= (1, 0, 0), & P_{01} &= (1, 1, 0), & P_{02} &= (0, 1, 0), \\ P_{10} &= (1, 0, 1), & P_{11} &= (1, 1, 1), & P_{12} &= (0, 1, 1), \\ P_{20} &= (0, 0, 1), & P_{21} &= (0, 0, 1), & P_{22} &= (0, 0, 1), \end{aligned}$$

а значения весов определяются с помощью (4) и (5):

$$\begin{aligned}\omega_{00} &= 1, & \omega_{01} &= \frac{\sqrt{2}}{2}, & \omega_{02} &= 1, \\ \omega_{10} &= \frac{\sqrt{2}}{2}, & \omega_{11} &= \frac{1}{2}, & \omega_{12} &= \frac{\sqrt{2}}{2}, \\ \omega_{20} &= 1, & \omega_{21} &= \frac{\sqrt{2}}{2}, & \omega_{22} &= 1.\end{aligned}$$

5°. На рис. 3 и рис. 4 приведены примеры поверхностей вращения, построенных при помощи рассмотренного метода.

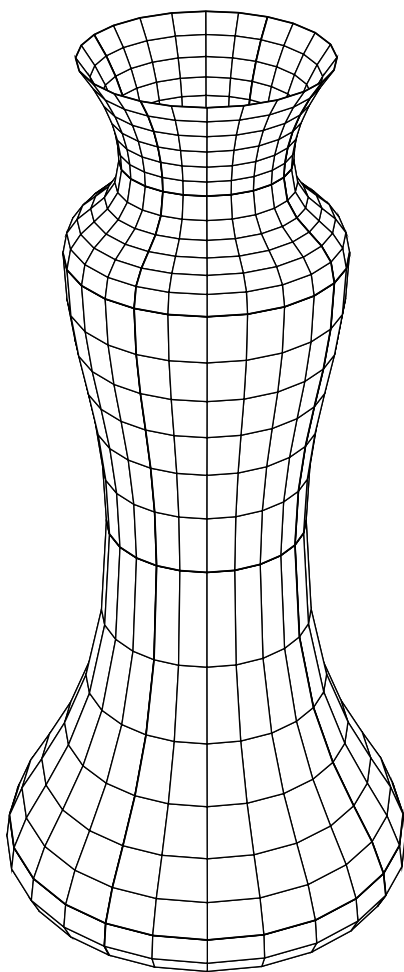


Рис. 3

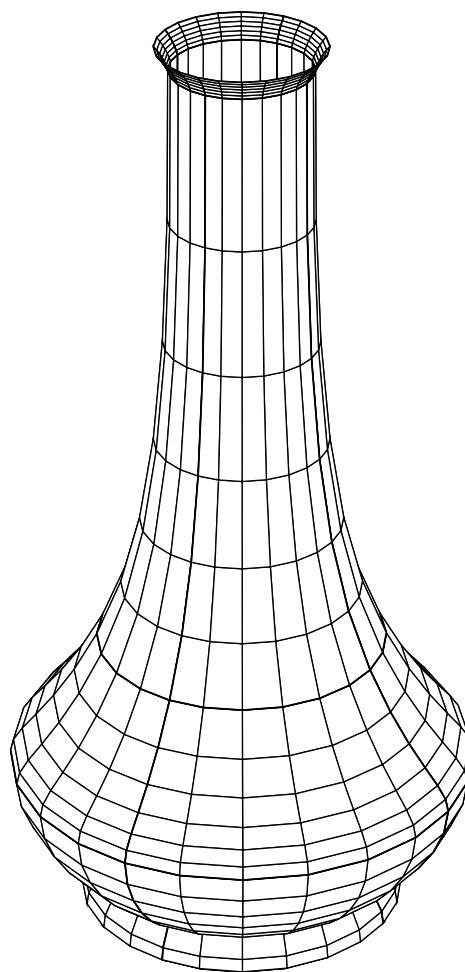


Рис. 4

ЛИТЕРАТУРА

1. Farin G. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.
2. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Можно ли построить окружность с помощью кривых Безье?* // Семинар «DHA & CAGD». Избранные доклады. 16 декабря 2006 г. (<http://dha.spb.ru/rep06.shtml#1216>).
3. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Полиномы Бернштейна и составные кривые Безье* // Журн. вычисл. мат. и матем. физ. 2006. Т. 46. №11. С. 1962-1971.
4. Григорьев М. И. *Построение сферы с помощью проективных поверхностей Безье* // Семинар «DHA & CAGD». Избранные доклады. 24 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0224>).

ДВОЙСТВЕННЫЕ ФРЕЙМЫ

В. Н. Малозёмов

Н. А. Соловьёва

21 августа 2007 г.

Доклад является вариацией на темы из [1, с. 101–106] и [2].

1°. Рассмотрим при $m \geq n$ матрицу $\Phi = \Phi[1 : n, 1 : m]$ с комплексными элементами. Столбцы этой матрицы обозначим $\varphi_1, \dots, \varphi_m$. Набор векторов $\{\varphi_1, \dots, \varphi_m\}$ называется *фреймом* в \mathbb{C}^n , если эрмитова матрица $S = \Phi \Phi^*$ является положительно определённой.

Рассмотрим ещё одну матрицу $\tilde{\Phi} = \tilde{\Phi}[1 : n, 1 : m]$ со столбцами $\tilde{\varphi}_1, \dots, \tilde{\varphi}_m$. Набор векторов $\{\tilde{\varphi}_1, \dots, \tilde{\varphi}_m\}$ называется *двойственным фреймом*, если эрмитова матрица $\tilde{S} = \tilde{\Phi} \tilde{\Phi}^*$ положительно определена и выполнено условие

$$\tilde{\Phi} \Phi^* = I_n, \quad (1)$$

где I_n — единичная матрица порядка n .

Двойственные фреймы существуют. Действительно, матрица $\tilde{\Phi} = S^{-1}\Phi$ удовлетворяет условию (1). Кроме того,

$$\tilde{S} := \tilde{\Phi} \tilde{\Phi}^* = S^{-1}\Phi \Phi^* S^{-1} = S^{-1}.$$

Поскольку S^{-1} — положительно определённая эрмитова матрица, то по определению столбцы матрицы $\tilde{\Phi}$, имеющие вид

$$\tilde{\varphi}_j = S^{-1}\varphi_j, \quad j \in 1 : m, \quad (2)$$

образуют двойственный фрейм. Обозначим его $\{\tilde{\varphi}_1, \dots, \tilde{\varphi}_m\}$. Этот фрейм называется *каноническим двойственным фреймом* по отношению к фрейму $\{\varphi_1, \dots, \varphi_m\}$.

2°. Покажем, что канонический двойственный фрейм обладает экстремальным свойством.

С произвольным двойственным фреймом $\{\psi_1, \dots, \psi_m\}$ свяжем величину

$$P = \sum_{j=1}^m \|\psi_j\|^2.$$

ПРЕДЛОЖЕНИЕ 1. *Канонический двойственный фрейм является единственным двойственным фреймом, на котором величина P достигает наименьшего значения.*

Доказательство. Возьмём произвольный двойственный фрейм $\{\psi_1, \dots, \psi_m\}$, отличный от $\{\tilde{\varphi}_1, \dots, \tilde{\varphi}_m\}$ (если таковой существует). Обозначим через Ψ матрицу со столбцами ψ_1, \dots, ψ_m . Ненулевая матрица $H = \Psi - \tilde{\Phi}$, согласно (1), удовлетворяет условию $H\tilde{\Phi}^* = 0$. Принимая во внимание, что $\tilde{\Phi}^* = \tilde{\Phi}^* S^{-1}$, получаем

$$H\tilde{\Phi}^* = (H\tilde{\Phi}^*) S^{-1} = 0. \quad (3)$$

Теперь запишем

$$\begin{aligned} \sum_{j=1}^m \|\psi_j\|^2 &= \sum_{j=1}^m \sum_{i=1}^n |\psi_j(i)|^2 = \sum_{j=1}^m \sum_{i=1}^n |\Psi[i, j]|^2 = \\ &= \sum_{j=1}^m \sum_{i=1}^n |\tilde{\Phi}[i, j] + H[i, j]|^2 = \sum_{j=1}^m \sum_{i=1}^n |\tilde{\Phi}[i, j]|^2 + \sum_{j=1}^m \sum_{i=1}^n |H[i, j]|^2 + \\ &\quad + 2 \operatorname{Re} \sum_{j=1}^m \sum_{i=1}^n H[i, j] \overline{\tilde{\Phi}[i, j]}. \end{aligned}$$

Поскольку

$$\sum_{j=1}^m \sum_{i=1}^n |\tilde{\Phi}[i, j]|^2 = \sum_{j=1}^m \sum_{i=1}^n |\tilde{\varphi}_j(i)|^2 = \sum_{j=1}^m \|\tilde{\varphi}_j\|^2$$

и в силу (3)

$$\begin{aligned} \sum_{j=1}^m \sum_{i=1}^n H[i, j] \overline{\tilde{\Phi}[i, j]} &= \sum_{i=1}^n \sum_{j=1}^m H[i, j] \tilde{\Phi}^*[j, i] = \\ &= \sum_{i=1}^n (H\tilde{\Phi}^*)[i, i] = 0, \end{aligned}$$

то

$$\sum_{j=1}^m \|\psi_j\|^2 = \sum_{j=1}^m \|\tilde{\varphi}_j\|^2 + \sum_{i=1}^n \sum_{j=1}^m |H[i, j]|^2.$$

Отсюда очевидным образом следует требуемое. \square

В дальнейшем будем использовать только канонические двойственные фреймы.

3°. Умножим обе части равенства (1) справа на вектор $x \in \mathbb{C}^n$. Получим

$$x = \tilde{\Phi}(\Phi^* x). \quad (4)$$

Если учесть, что

$$\begin{aligned} (\Phi^* x)(j) &= \sum_{i=1}^n \Phi^*[j, i] \times x(i) = \sum_{i=1}^n x(i) \times \overline{\Phi[i, j]} = \\ &= \sum_{i=1}^n x(i) \times \overline{\varphi_j(i)} = \langle x, \varphi_j \rangle, \end{aligned}$$

то формулу (4) можно переписать так:

$$x = \sum_{j=1}^m \langle x, \varphi_j \rangle \tilde{\varphi}_j. \quad (5)$$

Вернёмся к равенству (1) и с помощью эрмитова сопряжения преобразуем его к эквивалентному виду

$$\Phi \tilde{\Phi}^* = I_n.$$

Умножим обе части последнего равенства справа на вектор $x \in \mathbb{C}^n$. Получим

$$x = \Phi(\tilde{\Phi}^* x) = \sum_{j=1}^m \langle x, \tilde{\varphi}_j \rangle \varphi_j. \quad (6)$$

Подведём итог.

ПРЕДЛОЖЕНИЕ 2. Для любого вектора $x \in \mathbb{C}^n$ справедливы разложения (5) и (6), в которых $\{\varphi_1, \dots, \varphi_m\}$ — некоторый фрейм и $\{\tilde{\varphi}_1, \dots, \tilde{\varphi}_m\}$ — канонический двойственный фрейм.

4°. Если матрица фрейма $S = \Phi \Phi^*$ имеет вид $S = A I_n$ с $A > 0$, то соответствующий фрейм $\{\varphi_1, \dots, \varphi_m\}$ называется *жёстким*. Элементы канонического двойственного фрейма по отношению к жёсткому фрейму согласно (2) допускают представление

$$\tilde{\varphi}_j = \frac{1}{A} \varphi_j, \quad j \in 1 : m.$$

Разложения (5) и (6) в случае жёсткого фрейма объединятся в одно разложение

$$x = \frac{1}{A} \sum_{j=1}^m \langle x, \varphi_j \rangle \varphi_j.$$

5°. Жёсткий фрейм с $A = 1$ называется *фреймом Парсеваля*.

ПРЕДЛОЖЕНИЕ 3. *Любой фрейм может быть преобразован во фрейм Парсеваля.*

Доказательство. Возьмём фрейм $\{\varphi_1, \dots, \varphi_m\}$ с матрицей фрейма $S = \Phi \Phi^*$. Положим $\widehat{\Phi} = S^{-\frac{1}{2}} \Phi$. Так как

$$\widehat{S} := \widehat{\Phi} \widehat{\Phi}^* = S^{-\frac{1}{2}} \Phi \Phi^* S^{-\frac{1}{2}} = S^{-\frac{1}{2}} S S^{-\frac{1}{2}} = I_n,$$

то столбцы матрицы $\widehat{\Phi}$, имеющие вид

$$\widehat{\varphi}_j = S^{-\frac{1}{2}} \varphi_j, \quad j \in 1 : m,$$

образуют фрейм Парсеваля. Предложение доказано. \square

Отметим, что фрейм Парсеваля совпадает со своим каноническим двойственным фреймом.

ЛИТЕРАТУРА

1. Добеши И. Десять лекций по вейвлетам. Пер. с англ. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.
2. Casazza P. G. Custom building finite frames // Contemporary Math. 2004. V. 345. P. 61–86.

КРОНЕКЕРОВО УМНОЖЕНИЕ МАТРИЦ И КОММУТАТИВНОСТЬ

В. Н. Малозёмов О. В. Просеков

21 августа 2007 г.

1°. Пусть A_n и B_m — квадратные матрицы порядков n и m соответственно и I_n — единичная матрица порядка n . Имеет место следующее свойство коммутативности [1]:

$$(A_n \otimes I_m)(I_n \otimes B_m) = (I_n \otimes B_m)(A_n \otimes I_m). \quad (1)$$

В левой и правой частях равенства (1) стоят разные разложения матрицы $A_n \otimes B_m$.

В данном докладе приводится обобщение формулы (1), важное для теории быстрого преобразования Фурье.

2°. Зафиксируем натуральное число $N = n_1 n_2 \cdots n_s$, где n_ν — натуральные числа, отличные от единицы, и введём обозначения

$$N_\nu = n_{\nu+1} n_{\nu+2} \cdots n_s, \quad \nu \in 0 : s-1; \quad N_s = 1; \\ \Delta_1 = 1; \quad \Delta_\nu = n_1 n_2 \cdots n_{\nu-1}, \quad \nu \in 2 : s+1.$$

Очевидно, что $\Delta_\nu n_\nu N_\nu = N$ при всех $\nu \in 1 : s$.

Будем рассматривать только квадратные матрицы; нижний индекс указывает на их порядок.

ТЕОРЕМА. *Справедливо равенство*

$$\prod_{\nu=1}^s (A_{N_{\nu-1}}^{(\nu)} \otimes I_{\Delta_\nu}) \prod_{\nu=1}^s (I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu}) \prod_{\nu=1}^s (I_{N_\nu} \otimes C_{\Delta_{\nu+1}}^{(\nu)}) = \\ = \prod_{\nu=1}^s (A_{N_{\nu-1}}^{(\nu)} \otimes I_{\Delta_\nu}) (I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu}) (I_{N_\nu} \otimes C_{\Delta_{\nu+1}}^{(\nu)}). \quad (2)$$

3°. Предварительно установим три вспомогательных предложения.

ЛЕММА 1. При $\mu > \nu$

$$(A_{N_{\mu-1}}^{(\mu)} \otimes I_{\Delta_\mu})(I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu}) = (I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu})(A_{N_{\mu-1}}^{(\mu)} \otimes I_{\Delta_\mu}). \quad (3)$$

Доказательство. Поскольку $I_{\Delta_\mu} = I_{n_{\nu+1} \dots n_{\mu-1}} \otimes I_{\Delta_{\nu+1}}$, то согласно (1)

$$\begin{aligned} & (A_{N_{\mu-1}}^{(\mu)} \otimes I_{\Delta_\mu})(I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu}) = \\ & = ((A_{N_{\mu-1}}^{(\mu)} \otimes I_{n_{\nu+1} \dots n_{\mu-1}}) \otimes I_{\Delta_{\nu+1}})(I_{N_\nu} \otimes (B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu})) = \\ & = (I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu})(A_{N_{\mu-1}}^{(\mu)} \otimes I_{\Delta_\mu}). \end{aligned}$$

Лемма доказана. \square

ЛЕММА 2. При $\mu < \nu$

$$(I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu})(I_{N_\mu} \otimes C_{\Delta_{\mu+1}}^{(\mu)}) = (I_{N_\mu} \otimes C_{\Delta_{\mu+1}}^{(\mu)})(I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu}).$$

Доказательство. Воспользуемся тем, что $I_{N_\mu} = I_{N_{\nu-1}} \otimes I_{n_{\mu+1} \dots n_{\nu-1}}$. Согласно (1) получим

$$\begin{aligned} & (I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu})(I_{N_\mu} \otimes C_{\Delta_{\mu+1}}^{(\mu)}) = \\ & = ((I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu})(I_{N_{\nu-1}} \otimes (I_{n_{\mu+1} \dots n_{\nu-1}} \otimes C_{\Delta_{\mu+1}}^{(\mu)}))) = \\ & = (I_{N_\mu} \otimes C_{\Delta_{\mu+1}}^{(\mu)})(I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu}). \end{aligned}$$

Лемма доказана. \square

ЛЕММА 3. При $\mu < \nu$

$$(A_{N_{\nu-1}}^{(\nu)} \otimes I_{\Delta_\nu})(I_{N_\mu} \otimes C_{\Delta_{\mu+1}}^{(\mu)}) = (I_{N_\mu} \otimes C_{\Delta_{\mu+1}}^{(\mu)})(A_{N_{\nu-1}}^{(\nu)} \otimes I_{\Delta_\nu}).$$

Доказательство такое же, как в лемме 2. Матрица $I_{N_\nu} \otimes B_{n_\nu}^{(\nu)}$ заменена на $A_{N_{\nu-1}}^{(\nu)}$.

Замечание. Обозначим

$$D_N^{(\nu)} = (A_{N_{\nu-1}}^{(\nu)} \otimes I_{\Delta_\nu})(I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu}).$$

Последовательное применение лемм 2 и 3 приводит к равенству

$$D_N^{(\nu)} (I_{N_\mu} \otimes C_{\Delta_{\mu+1}}^{(\mu)}) = (I_{N_\mu} \otimes C_{\Delta_{\mu+1}}^{(\mu)}) D_N^{(\nu)} \quad \text{при } \mu < \nu. \quad (4)$$

4°. Обратимся к доказательству теоремы. В качестве первого шага установим, что

$$\prod_{\nu=1}^s (A_{N_{\nu-1}}^{(\nu)} \otimes I_{\Delta_\nu}) \prod_{\nu=1}^s (I_{N_\nu} \otimes B_{n_\nu}^{(\nu)} \otimes I_{\Delta_\nu}) = \prod_{\nu=1}^s D_N^{(\nu)}. \quad (5)$$

Возьмём последний сомножитель в первом произведении из левой части равенства (5). С помощью последовательного применения формулы (3) переместим его на позицию перед последним сомножителем второго произведения. Получим матрицу $D_N^{(s)}$. Точно так же сомножитель с индексом $\nu = s - 1$ первого произведения переместим на позицию перед сомножителем с индексом $\nu = s - 1$ второго произведения. Получим матрицу $D_N^{(s-1)}$. Продолжив аналогично, придём к равенству (5). При этом первый сомножитель из первого произведения остаётся на месте.

Второй шаг сводится к проверке равенства

$$\prod_{\nu=1}^s D_N^{(\nu)} \prod_{\nu=1}^s (I_{N_\nu} \otimes C_{\Delta_{\nu+1}}^{(\nu)}) = \prod_{\nu=1}^s D_N^{(\nu)} (I_{N_\nu} \otimes C_{\Delta_{\nu+1}}^{(\nu)}). \quad (6)$$

С помощью последовательного применения формулы (4) первый сомножитель во втором произведении из левой части равенства (6) переместим на позицию после первого сомножителя в первом произведении; второй сомножитель из второго произведения переместим на позицию после второго сомножителя из первого произведения и т. д. В результате придём к равенству (6). При этом последний сомножитель из второго произведения остаётся на месте.

Теорема доказана.

ЛИТЕРАТУРА

1. Малозёмов В. Н., Просеков О. В. *Перестановки и кронекерово произведение матриц* // Семинар «DHA & CAGD». Избранные доклады. 31 марта 2004 г. (<http://dha.spb.ru/rep04.shtml#0324>).

ПОВЕРХНОСТЬ ВРАЩЕНИЯ КАК ПОВЕРХНОСТЬ КУНСА

Н. В. Чашников

28 августа 2007 г.

1°. Мы будем использовать следующие обозначения из [1].

L_1, L_2, L_3, L_4 — линейные операторы, определённые для непрерывно дифференцируемых вектор-функций $f : [0, 1] \rightarrow \mathbb{R}^3$ следующим образом:

$$L_1(f) = f(0), \quad L_2(f) = f'(0), \quad L_3(f) = f'(1), \quad L_4(f) = f(1).$$

Предположим, что H_1, H_2, H_3, H_4 — непрерывно дифференцируемые на отрезке $[0, 1]$ функции, удовлетворяющие соотношениям

$$\begin{aligned} H_1(0) &= 1, & H_1'(0) &= 0, & H_1'(1) &= 0, & H_1(1) &= 0; \\ H_2(0) &= 0, & H_2'(0) &= 1, & H_2'(1) &= 0, & H_2(1) &= 0; \\ H_3(0) &= 0, & H_3'(0) &= 0, & H_3'(1) &= 1, & H_3(1) &= 0; \\ H_4(0) &= 0, & H_4'(0) &= 0, & H_4'(1) &= 0, & H_4(1) &= 1. \end{aligned} \tag{1}$$

Из этих соотношений следует, что

$$L_i(aH_j) = a\delta_{ij}, \quad i, j \in 1 : 4, \quad a \in \mathbb{R}^3. \tag{2}$$

В [1] доказано, что если вектор-функции $f_i, g_i : [0, 1] \rightarrow \mathbb{R}^3$, $i \in 1 : 4$, удовлетворяют условиям

$$L_j(f_i) = L_i(g_j), \quad i, j \in 1 : 4, \tag{3}$$

то поверхность, задаваемая вектор-функцией

$$c(u, v) = \sum_{i=1}^4 H_i(u) f_i(v) + \sum_{j=1}^4 H_j(v) g_j(u) - \sum_{i=1}^4 \sum_{j=1}^4 H_i(u) H_j(v) L_i(g_j), \tag{4}$$

будет удовлетворять условиям

$$\begin{aligned} L_i(c(\cdot, v)) &= f_i(v), & v &\in [0, 1], & i &\in 1 : 4; \\ L_j(c(u, \cdot)) &= g_j(u), & u &\in [0, 1], & j &\in 1 : 4. \end{aligned} \tag{5}$$

Эта поверхность называется *параметрической поверхностью Кунса*.

2°. Рассмотрим задачу построения поверхности вращения как параметрической поверхности Кунса.

Пусть $x, z: [0, 1] \rightarrow \mathbb{R}$ — непрерывно дифференцируемые функции. Тогда вектор-функция

$$p(u) = (x(u), 0, z(u)), \quad u \in [0, 1],$$

задаёт кривую в \mathbb{R}^3 , лежащую в плоскости OXZ . Зафиксируем число $\alpha \in (0, \pi)$ и рассмотрим поверхность, определяемую вектор-функцией

$$r(u, v) = (x(u) \cos \alpha v, x(u) \sin \alpha v, z(u)), \quad u, v \in [0, 1]. \quad (6)$$

При фиксированных u и v точка $r(u, v)$ получается из точки $p(u)$ вращением на угол αv вокруг оси OZ . Поэтому поверхность, задаваемая вектор-функцией $r(u, v)$, получается из кривой $p(u)$ вращением вокруг оси OZ на угол в пределах от 0 до α .

Подберём теперь граничные функции f_i и g_j и смешивающие функции H_i таким образом, чтобы поверхность Кунса $s(u, v)$ совпала с поверхностью вращения $r(u, v)$. Граничные функции f_i и g_j получаются естественным образом из функции $r(u, v)$:

$$\begin{aligned} f_1(v) &= r(0, v) = (x(0) \cos \alpha v, x(0) \sin \alpha v, z(0)), \\ f_2(v) &= r'_u(0, v) = (x'(0) \cos \alpha v, x'(0) \sin \alpha v, z'(0)), \\ f_3(v) &= r'_u(1, v) = (x'(1) \cos \alpha v, x'(1) \sin \alpha v, z'(1)), \\ f_4(v) &= r(1, v) = (x(1) \cos \alpha v, x(1) \sin \alpha v, z(1)), \\ g_1(u) &= r(u, 0) = (x(u), 0, z(u)), \\ g_2(u) &= r'_v(u, 0) = (0, \alpha x(u), 0), \\ g_3(u) &= r'_v(u, 1) = (-\alpha x(u) \sin \alpha, \alpha x(u) \cos \alpha, 0), \\ g_4(u) &= r(u, 1) = (x(u) \cos \alpha, x(u) \sin \alpha, z(u)). \end{aligned} \quad (7)$$

Нетрудно проверить, что для функций (7) условия (3) выполнены. Осталось подобрать такие функции H_i , чтобы поверхность Кунса, получаемая по формуле (4) для граничных функций (7), совпала с поверхностью вращения (6).

3°. Будем искать $H_i(t)$ в виде

$$A_i + B_i \sin \alpha t + C_i \cos \alpha t + D_i \sin^2 \alpha t,$$

где коэффициенты A_i, B_i, C_i и D_i — вещественные числа. Эти коэффициенты будем подбирать таким образом, чтобы выполнялись условия (1).

Для примера найдём H_1 . Так как

$$\begin{aligned} 1 &= H_1(0) = A_1 + C_1, \\ 0 &= H'_1(0) = \alpha B_1, \end{aligned}$$

то $B_1 = 0$, $A_1 = 1 - C_1$. Далее,

$$0 = H'_1(1) = -\alpha C_1 \sin \alpha + 2\alpha D_1 \sin \alpha \cos \alpha,$$

поэтому $C_1 = 2D_1 \cos \alpha$. Следовательно,

$$\begin{aligned} 0 &= H_1(1) = A_1 + C_1 \cos \alpha + D_1 \sin^2 \alpha = 1 - 2D_1 \cos \alpha + 2D_1 \cos^2 \alpha + \\ &+ D_1 \sin^2 \alpha = 1 + D_1 (2 \cos^2 \alpha + \sin^2 \alpha - 2 \cos \alpha) = 1 + D_1 (1 - \cos \alpha)^2. \end{aligned}$$

Для коэффициентов D_1 , C_1 и A_1 получаем представления

$$D_1 = -\frac{1}{(1 - \cos \alpha)^2}, \quad C_1 = -\frac{2 \cos \alpha}{(1 - \cos \alpha)^2}, \quad A_1 = 1 + \frac{2 \cos \alpha}{(1 - \cos \alpha)^2},$$

так что

$$\begin{aligned} H_1(t) &= A_1 + C_1 \cos \alpha t + D_1 \sin^2 \alpha t = \\ &= \frac{1 + \cos^2 \alpha - 2 \cos \alpha \cos \alpha t - \sin^2 \alpha t}{(1 - \cos \alpha)^2} = \frac{(\cos \alpha - \cos \alpha t)^2}{(1 - \cos \alpha)^2}. \end{aligned}$$

Аналогичным образом можно подобрать H_2 , H_3 и H_4 . Придём к формулам

$$\begin{aligned} H_1(t) &= \frac{(\cos \alpha - \cos \alpha t)^2}{(1 - \cos \alpha)^2}, \\ H_2(t) &= \frac{\sin \alpha t - \sin \alpha}{\alpha} + \frac{(\cos \alpha - \cos \alpha t)(\cos^2 \alpha - \cos \alpha t)}{\alpha \sin \alpha (1 - \cos \alpha)}, \\ H_3(t) &= \frac{(1 - \cos \alpha t)(\cos \alpha - \cos \alpha t)}{\alpha \sin \alpha (1 - \cos \alpha)}, \\ H_4(t) &= 1 - \frac{(\cos \alpha - \cos \alpha t)^2}{(1 - \cos \alpha)^2}. \end{aligned} \tag{8}$$

Заметим, что $H_1(t) + H_4(t) \equiv 1$.

Далее мы покажем явно, что для функций H_2 , H_3 и H_4 выполняются условия (1). Кроме того, будет установлено, что поверхность Кунса, получаемая по граничным функциям (7) с использованием смешивающих функций (8), действительно совпадает с поверхностью вращения $r(u, v)$.

ЛЕММА 1. *Выполнены тождества*

$$H_1(t) - \alpha H_3(t) \sin \alpha + H_4(t) \cos \alpha = \cos \alpha t, \quad \forall t \in [0, 1]; \quad (9)$$

$$\alpha H_2(t) + \alpha H_3(t) \cos \alpha + H_4(t) \sin \alpha = \sin \alpha t, \quad \forall t \in [0, 1]. \quad (10)$$

Доказательство. Имеем

$$\begin{aligned} H_1(t) - \alpha H_3(t) \sin \alpha + H_4(t) \cos \alpha &= H_1(t) (1 - \cos \alpha) - \alpha H_3(t) \sin \alpha + \cos \alpha = \\ &= \frac{1}{1 - \cos \alpha} [(\cos \alpha - \cos \alpha t)^2 - (1 - \cos \alpha t) (\cos \alpha - \cos \alpha t)] + \cos \alpha = \\ &= \frac{1}{1 - \cos \alpha} [(\cos \alpha - \cos \alpha t) (\cos \alpha - 1)] + \cos \alpha = \cos \alpha t. \end{aligned}$$

Соотношение (9) установлено. Разберёмся с (10):

$$\begin{aligned} \alpha H_2(t) + \alpha H_3(t) \cos \alpha &= \sin \alpha t - \sin \alpha + \\ &+ \frac{\cos \alpha - \cos \alpha t}{\sin \alpha (1 - \cos \alpha)} [\cos^2 \alpha - \cos \alpha t + \cos \alpha (1 - \cos \alpha t)] = \\ &= \sin \alpha t - \sin \alpha + \frac{\cos \alpha - \cos \alpha t}{\sin \alpha (1 - \cos \alpha)} [(1 + \cos \alpha) (\cos \alpha - \cos \alpha t)] = \\ &= \sin \alpha t - \sin \alpha + \frac{(\cos \alpha - \cos \alpha t)^2}{\sin \alpha (1 - \cos \alpha)^2} (1 - \cos^2 \alpha) = \\ &= \sin \alpha t - \sin \alpha + \sin \alpha \frac{(\cos \alpha - \cos \alpha t)^2}{(1 - \cos \alpha)^2} = \\ &= \sin \alpha t - H_4(t) \sin \alpha, \end{aligned}$$

что равносильно требуемому. □

ЛЕММА 2. *Для функций (8) выполнены условия (1).*

Доказательство. Ясно, что $H_1(0) = 1$, $H_1(1) = 0$. Далее,

$$H_1'(t) = \frac{2\alpha \sin \alpha t (\cos \alpha - \cos \alpha t)}{(1 - \cos \alpha)^2},$$

поэтому $H_1'(0) = H_1'(1) = 0$. Так как $H_4(t) = 1 - H_1(t)$, то условия на H_4 также выполнены. Осталось проверить условия на H_2 и H_3 .

Подставляя в тождества (9) и (10) значения $t = 0$ и $t = 1$, получаем, что $H_3(0) = H_3(1) = H_2(0) = H_2(1) = 0$.

Теперь продифференцируем (9) и (10) по t :

$$\begin{aligned} H_1'(t) - \alpha H_3'(t) \sin \alpha + H_4'(t) \cos \alpha &= -\alpha \sin \alpha t, \\ \alpha H_2'(t) + \alpha H_3'(t) \cos \alpha + H_4'(t) \sin \alpha &= \alpha \cos \alpha t. \end{aligned}$$

Подставив в эти тождества значения $t = 0$ и $t = 1$, придём к равенствам $H_3'(0) = 0$, $H_3'(1) = 1$, $H_2'(0) = 1$, $H_2'(1) = 0$. Лемма доказана. \square

Из леммы 2 следует, что функции (8) могут быть использованы для построения параметрической поверхности Кунса.

ЛЕММА 3. Пусть

$$q(t) = A + B \sin \alpha t + C \cos \alpha t + D \sin^2 \alpha t, \quad A, B, C, D \in \mathbb{R}^3, \quad (11)$$

и $L_i(q) = 0$ для $i \in 1 : 4$. Тогда $q \equiv 0$.

Доказательство. Отметим, что

$$q'(t) = \alpha B \cos \alpha t - \alpha C \sin \alpha t + 2\alpha D \cos \alpha t \sin \alpha t.$$

По условию имеем

$$\begin{aligned} q(0) &= A + C = 0, \\ q'(0) &= \alpha B = 0, \\ q'(1) &= \alpha B \cos \alpha - \alpha C \sin \alpha + 2\alpha D \cos \alpha \sin \alpha = 0, \\ q(1) &= A + B \sin \alpha + C \cos \alpha + D \sin^2 \alpha = 0. \end{aligned}$$

Из второго равенства видно, что $B = 0$. Из первого и третьего равенств следует, что $A = -C$, $C = 2D \cos \alpha$. Четвёртое равенство преобразуем к виду

$$\begin{aligned} 0 &= (-2 \cos \alpha + 2 \cos^2 \alpha + \sin^2 \alpha) D = \\ &= (1 - 2 \cos \alpha + \cos^2 \alpha) D = (1 - \cos \alpha)^2 D. \end{aligned}$$

Так как $\alpha \in (0, \pi)$, то $D = 0$. Получаем $D = C = A = B = 0$, так что $q \equiv 0$. \square

ТЕОРЕМА. Поверхность Кунса, построенная по граничным функций (7) с использованием смешивающих функций (8), совпадает с поверхностью вращения (6).

Доказательство. Подставим во вторую сумму из правой части формулы (4) значения из (7) и воспользуемся тождествами (9) и (10). Получим

$$\begin{aligned} \sum_{j=1}^4 H_j(v) g_j(u) &= \left(x(u) (H_1(v) - \alpha H_3(v) \sin \alpha + H_4(v) \cos \alpha), \right. \\ &\quad \left. x(u) (\alpha H_2(v) + \alpha H_3(v) \cos \alpha + H_4(v) \sin \alpha), z(u) (H_1(v) + H_4(v)) \right) = \\ &= (x(u) \cos \alpha v, x(u) \sin \alpha v, z(u)) = r(u, v). \end{aligned}$$

Преобразуем две оставшиеся суммы в правой части формулы (4). Согласно (3):

$$\begin{aligned} \sum_{i=1}^4 H_i(u) f_i(v) - \sum_{i=1}^4 \sum_{j=1}^4 H_i(u) H_j(v) L_i(g_j) &= \\ &= \sum_{i=1}^4 H_i(u) \left[f_i(v) - \sum_{j=1}^4 L_j(f_i) H_j(v) \right]. \end{aligned}$$

Обозначим

$$q_i(v) = f_i(v) - \sum_{j=1}^4 L_j(f_i) H_j(v), \quad i \in 1 : 4.$$

Используя линейность L_k и равенство (2), получаем

$$L_k(q_i) = L_k(f_i) - \sum_{j=1}^4 L_k(L_j(f_i) H_j) = L_k(f_i) - \sum_{j=1}^4 L_j(f_i) \delta_{kj} = 0.$$

Кроме того, из формул для $f_i(v)$ и $H_j(v)$ видно, что $q_i(v)$ является многочленом степени два от $\cos \alpha v$ и $\sin \alpha v$. А так как $\cos^2 \alpha v$ можно заменить на $1 - \sin^2 \alpha v$, то $q_i(v)$ имеет вид (11). Таким образом, все условия леммы 3 выполнены. Значит, $q_i(v) \equiv 0$.

Итак,

$$\begin{aligned} \sum_{i=1}^4 H_i(u) f_i(v) + \sum_{j=1}^4 H_j(v) g_j(u) - \sum_{i=1}^4 \sum_{j=1}^4 H_i(u) H_j(v) L_i(g_j) &= \\ &= r(u, v) + \sum_{i=1}^4 H_i(u) q_i(v) = r(u, v). \end{aligned}$$

Теорема доказана. □

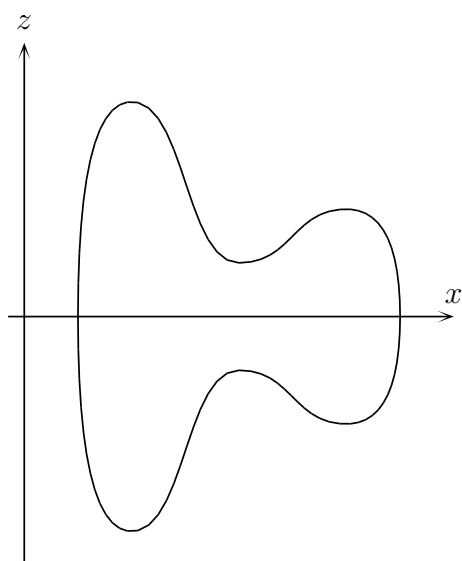


Рис. 1. Кривая

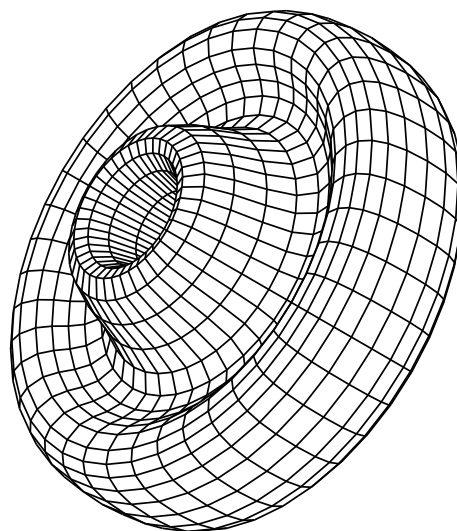


Рис. 2. Поверхность вращения

4°. В случае $\alpha = \pi/2$ функции (8) имеют вид:

$$\begin{aligned} H_1(t) &= \cos^2 \frac{\pi t}{2}, & H_2(t) &= \frac{2}{\pi} \left(\sin \frac{\pi t}{2} - \sin^2 \frac{\pi t}{2} \right), \\ H_3(t) &= -\frac{2}{\pi} \left(\cos \frac{\pi t}{2} - \cos^2 \frac{\pi t}{2} \right), & H_4(t) &= \sin^2 \frac{\pi t}{2}. \end{aligned}$$

Возьмём кривую, лежащую в плоскости OXZ (см. рис. 1), и построим поверхность путём вращения этой кривой вокруг оси OZ на угол $\pi/2$. Такая поверхность может быть реализована как поверхность Кунса. Если построенную поверхность отразить относительно плоскости OYZ , а потом обе эти поверхности отразить относительно плоскости OXZ , то получится полная поверхность вращения (см. рис. 2).

ЛИТЕРАТУРА

1. Малозёмов В. Н., Чашников Н. В. *Бикубические поверхности Кунса*. // Семинар «DHA & CAGD». Избранные доклады. 23 января 2007 г. (<http://dha.spb.ru/rep07.shtml#0123>).

ДИСКРЕТНЫЕ ПЕРИОДИЧЕСКИЕ СПЛАЙНЫ С ВЕКТОРНЫМИ КОЭФФИЦИЕНТАМИ И ГЕОМЕТРИЧЕСКОЕ МОДЕЛИРОВАНИЕ

В. Н. Малозёмов Д. А. Хорохонов Н. В. Чашников

4 сентября 2007 г.

1°. Пусть $N = mn$, где m, n — натуральные числа, отличные от единицы. Напомним, как вводятся дискретные N -периодические B -сплайны ([1], [2, с. 9–12]). B -сплайн первого порядка на основном периоде $0 : N - 1$ задаётся явно

$$Q_1(j) = \begin{cases} n - j & \text{при } j \in 0 : n - 1, \\ 0 & \text{при } j \in n : N - n, \\ j - N + n & \text{при } j \in N - n + 1 : N - 1. \end{cases} \quad (1)$$

B -сплайны более высоких порядков определяются с помощью циклической свёртки

$$Q_\nu = Q_1 * Q_{\nu-1}, \quad \nu = 2, 3, \dots \quad (2)$$

Отметим, что B -сплайн $Q_r(j)$ принимает только целые неотрицательные значения. Более глубоким является следующее свойство:

$$\sum_{p=0}^{m-1} Q_r(j - pn) \equiv n^{2r-1}. \quad (3)$$

В [1] и [2, с. 17] тождество (3) доказывается с использованием дискретного преобразования Фурье (ДПФ) и теоремы о свёртке.

Введём нормализованные B -сплайны

$$\tilde{Q}_r(j) = \frac{1}{n^{2r-1}} Q_r(j), \quad j \in \mathbb{Z}. \quad (4)$$

Для них формулы (1)–(3) примут вид

$$\tilde{Q}_1(j) = \begin{cases} 1 - j/n & \text{при } j \in 0:n-1, \\ 0 & \text{при } j \in n:N-n, \\ j/n - m + 1 & \text{при } j \in N-n+1:N-1; \end{cases} \quad (5)$$

$$\tilde{Q}_\nu = \frac{1}{n}(\tilde{Q}_1 * \tilde{Q}_{\nu-1}), \quad \nu = 2, 3, \dots; \quad (6)$$

$$\sum_{p=0}^{m-1} \tilde{Q}_r(j - pn) \equiv 1. \quad (7)$$

Дадим элементарное (без использования ДПФ) доказательство тождества (7), играющего в дальнейшем важную роль.

Отметим, что в силу определения (5)

$$\sum_{j=0}^{N-1} \tilde{Q}_1(j) = n. \quad (8)$$

Зафиксируем j и представим его в виде $j = ln + r$, где $r \in 0:n-1$, $l \in \mathbb{Z}$. Тогда

$$\begin{aligned} \sum_{p=0}^{m-1} \tilde{Q}_1(j - pn) &= \sum_{p=0}^{m-1} \tilde{Q}_1((l-p)n + r) = \sum_{q=0}^{m-1} \tilde{Q}_1(qn + r) = \\ &= \tilde{Q}_1(r) + \tilde{Q}_1((m-1)n + r) = 1 - \frac{r}{n} + \frac{(m-1)n+r}{n} - (m-1) = 1. \end{aligned}$$

Формула (7) при $r = 1$ установлена. Сделаем индукционный переход от $r - 1$ к r . Согласно (6) и (8) имеем

$$\begin{aligned} \sum_{p=0}^{m-1} \tilde{Q}_r(j - pn) &= \frac{1}{n} \sum_{p=0}^{m-1} \sum_{k=0}^{N-1} \tilde{Q}_1(k) \tilde{Q}_{r-1}(j - pn - k) = \\ &= \frac{1}{n} \sum_{k=0}^{N-1} \tilde{Q}_1(k) \sum_{p=0}^{m-1} \tilde{Q}_{r-1}(j - k - pn) = \frac{1}{n} \sum_{k=0}^{N-1} \tilde{Q}_1(k) = 1, \end{aligned}$$

что и требовалось доказать.

2°. Дискретным N -периодическим сплайном с векторными коэффициентами называется вектор-функция вида

$$\tilde{S}(j) = \sum_{p=0}^{m-1} a_p \tilde{Q}_r(j - pn), \quad j \in \mathbb{Z},$$

где $a_p \in \mathbb{C}^s$. Считаем, что коэффициенты a_p продолжены m -периодически на все целые p .

Рассмотрим вопрос о вычислении значений $\tilde{S}(j)$ при всех $j \in 0:N$. Обозначим

$$\begin{aligned}\tilde{S}_1(j) &= \sum_{p=0}^{m-1} a_p \tilde{Q}_1(j - pn), \\ \tilde{S}_\nu &= \frac{1}{n} (\tilde{Q}_1 * \tilde{S}_{\nu-1}), \quad \nu = 2, 3, \dots\end{aligned}\tag{9}$$

ПРЕДЛОЖЕНИЕ 1. *Справедливо равенство $\tilde{S} = \tilde{S}_r$.*

Доказательство. При $r = 1$ утверждение следует из определений. Сделаем индукционный переход от $r - 1$ к r . Согласно (6) имеем

$$\begin{aligned}\tilde{S}_r(j) &= \frac{1}{n} \sum_{k=0}^{N-1} \tilde{Q}_1(k) \tilde{S}_{r-1}(j - k) = \frac{1}{n} \sum_{k=0}^{N-1} \tilde{Q}_1(k) \sum_{p=0}^{m-1} a_p \tilde{Q}_{r-1}(j - k - pn) = \\ &= \sum_{p=0}^{m-1} a_p \left\{ \frac{1}{n} \sum_{k=0}^{N-1} \tilde{Q}_1(k) \tilde{Q}_{r-1}(j - pn - k) \right\} = \sum_{p=0}^{m-1} a_p \tilde{Q}_r(j - pn) = \tilde{S}(j). \quad \square\end{aligned}$$

3°. Схема (9) допускает эффективную вычислительную реализацию.

ПРЕДЛОЖЕНИЕ 2. *Справедлива формула*

$$\tilde{S}_1(ln + r) = a_l + \frac{r}{n} \Delta a_l, \quad r \in 0:n-1, \quad l \in 0:m-1.\tag{10}$$

Здесь $a_m = a_0$.

Доказательство. В силу m -периодичности

$$\begin{aligned}\tilde{S}_1(ln + r) &= \sum_{p=0}^{m-1} a_p \tilde{Q}_1((l-p)n + r) = \sum_{q=0}^{m-1} a_{l-q} \tilde{Q}_1(qn + r) = \\ &= a_l \tilde{Q}_1(r) + a_{l-m+1} \tilde{Q}_1((m-1)n + r) = a_l \left(1 - \frac{r}{n}\right) + a_{l+1} \frac{r}{n} = a_l + \frac{r}{n} \Delta a_l.\end{aligned}$$

Предложение доказано. □

Формула (10) справедлива и при $r = n$. В этом случае она принимает вид

$$\tilde{S}_1((l+1)n) = a_{l+1}, \quad l \in 0:m-1.\tag{11}$$

При $l \in 0:m-2$ равенство (11) следует из (10) при $r = 0$. При $l = m-1$ имеем $\tilde{S}_1(N) = \tilde{S}_1(0) = a_0 = a_m$, что соответствует (11). Это замечание позволяет утверждать, что наряду с (10) справедлива формула

$$\tilde{S}_1(ln + r + 1) = a_l + \frac{r+1}{n} \Delta a_l, \quad r \in 0:n-1, \quad l \in 0:m-1. \quad (12)$$

Теперь можно записать алгоритм вычисления значений $\tilde{S}_1(j)$ при всех $j \in 0:N$:

$$\begin{aligned} \tilde{S}_1(0) &= a_0; \\ \tilde{S}_1(ln + r + 1) &= \tilde{S}_1(ln + r) + \frac{1}{n} \Delta a_l, \\ r &\in 0:n-1, \quad l \in 0:m-1. \end{aligned} \quad (13)$$

Равенство (13) получено путём вычитания (10) из (12).

Приведём на псевдоязыке программу, реализующую алгоритм (13):

```

s1(0) := a(0);  n1 := 1/n;  j := 0;
for l := 1 to m do begin
  h := n1 * (a(l) - a(l-1));
  for r := 1 to n do begin
    j := j + 1; s1(j) := s1(j-1) + h
  end
end

```

В программе используется набор векторов-коэффициентов $a(0), a(1), \dots, a(m)$, в котором $a(m) = a(0)$. В результате работы программы получаем $\tilde{S}_1(j) = s1(j)$ при $j \in 0:N$.

4°. Обратимся к вопросу о вычислении циклической свёртки

$$y(j) = \frac{1}{n} \sum_{k=0}^{N-1} \tilde{Q}_1(k) x(j-k),$$

где $x(j) = (x_1(j), x_2(j), \dots, x_s(j))$ — векторный N -периодический сигнал.

ПРЕДЛОЖЕНИЕ 3. *Справедливо равенство*

$$y(j) = \frac{1}{n} \left\{ x(j) + \sum_{k=0}^{n-1} \left(1 - \frac{k}{n} \right) [x(j-k) + x(j+k)] \right\}. \quad (14)$$

Доказательство. В силу N -периодичности сигнала x имеем

$$ny(j) = \sum_{k=0}^{n-1} \left(1 - \frac{k}{n} \right) x(j-k) + \sum_{k=N-n+1}^{N-1} \left(1 - \frac{N-k}{n} \right) x(j+(N-k)) =$$

$$= x(j) + \sum_{k=1}^{n-1} \left(1 - \frac{k}{n}\right) [x(j-k) + x(j+k)],$$

что равносильно (14). □

Зафиксируем $j \in 0 : N - 1$ и введём обозначения

$$t_k = 1 - \frac{k}{n}, \quad d_0 = x(j), \quad d_k = x(j-k) + x(j+k) \quad \text{при } k \in 1 : n - 1.$$

Тогда формулу (14) можно переписать в виде

$$y(j) = \frac{1}{n} \sum_{k=0}^{n-1} t_k d_k.$$

Для вычисления последней суммы построим последовательность векторов $\{h_k\}$ по правилу

$$h_k = d_k + h_{k-1}, \quad k = 0, 1, \dots, n - 1; \quad h_{-1} = \mathbb{O}. \quad (15)$$

Учитывая, что $t_k - t_{k+1} = \frac{1}{n}$, получаем

$$\begin{aligned} \sum_{k=0}^{n-1} t_k d_k &= \sum_{k=0}^{n-1} t_k (h_k - h_{k-1}) = \sum_{k=0}^{n-1} t_k h_k - \sum_{k=-1}^{n-2} t_{k+1} h_k = \\ &= t_{n-1} h_{n-1} + \frac{1}{n} \sum_{k=0}^{n-2} h_k = \frac{1}{n} \sum_{k=0}^{n-1} h_k. \end{aligned}$$

Следовательно,

$$y(j) = \frac{1}{n^2} \sum_{k=0}^{n-1} h_k.$$

Вычисление $y(j)$ сведено к сложению векторов h_k , последовательно определяемых формулой (15).

Запишем на псевдоязыке программу, реализующую описанный алгоритм вычисления векторной циклической свёртки $y(j)$ при всех $j \in 0 : N$:

```

n1 := 1/(n*n);
for j := 0 to N-1 do begin
  h := x(j); s := h;
  for k := 1 to n-1 do begin
    h := h + x(j-k) + x(j+k);
    s := s + h
  end;
  y(j) := n1 * s
end;
y(N) := y(0)

```

В программе используются векторные величины $x(-n+1), x(-n), \dots, x(N+n-2)$, при этом в силу N -периодичности

$$\begin{aligned} x(j) &= x(N+j) \quad \text{при } j \in -n+1:-1, \\ x(j) &= x(j-N) \quad \text{при } j \in N:N+n-2. \end{aligned}$$

После работы программы в массиве $y(0:N)$ будут находиться требуемые векторные значения циклической свёртки.

5°. Для вычисления значений сплайна $\tilde{S}_r(j)$ при всех $j \in 0:N$, согласно (9), потребуется один раз применить алгоритм, описанный в п. 3°, и $r-1$ раз алгоритм, описанный в п. 4°.

6°. Рассмотрим задачу векторной сплайн-интерполяции

$$\tilde{S}_r(lm) = z(l), \quad l \in 0:m-1, \quad (16)$$

где $z(l) = (z_1(l), z_2(l), \dots, z_s(l))$. Она распадается на s независимых скалярных подзадач

$$\sum_{p=0}^{m-1} a_{p\nu} \tilde{Q}_r((l-p)n) = z_\nu(l), \quad \nu = 1, \dots, s,$$

каждую из которых (при фиксированном ν) с учётом (4) можно переписать так:

$$\sum_{p=0}^{m-1} a_{p\nu} Q_r((l-p)n) = n^{2r-1} z_\nu(l), \quad l \in 0:m-1. \quad (17)$$

Решение задачи (17) известно ([1], [2, с. 21–22]):

$$a_{p\nu} = \frac{1}{m} \sum_{k=0}^{m-1} \frac{n^{2r-1} Z_\nu(k)}{T_r(k)} \omega_m^{kp}, \quad p \in 0:m-1. \quad (18)$$

Здесь $Z_\nu = \mathcal{F}_m(z_\nu)$ и

$$T_r(k) = \begin{cases} n^{2r-1} & \text{при } k = 0, \\ (2 \sin \frac{\pi k}{m})^{2r} \Lambda_r(k) & \text{при } k \in 1:m-1; \end{cases}$$

$$\Lambda_r(k) = \frac{1}{n} \sum_{q=0}^{n-1} \left(2 \sin \frac{\pi(qm+k)}{N} \right)^{-2r}.$$

Обозначим $\tilde{T}_r(k) = \frac{1}{n^{2r-1}} T_r(k)$, так что

$$\tilde{T}_r(k) = \begin{cases} 1 & \text{при } k = 0, \\ (2 \sin \frac{\pi k}{m})^{2r} \tilde{\Lambda}_r(k) & \text{при } k \in 1:m-1; \end{cases}$$

$$\tilde{\Lambda}_r(k) = \sum_{q=0}^{n-1} \left(2n \sin \frac{\pi(qm+k)}{N} \right)^{-2r}.$$

Тогда формула (18) примет вид

$$a_{p\nu} = \frac{1}{m} \sum_{k=0}^{m-1} \frac{Z_\nu(k)}{\tilde{T}_r(k)} \omega_m^{kp}, \quad p \in 0:m-1.$$

Решением задачи (16) является следующий набор векторов-коэффициентов сплайна \tilde{S}_r : $a_p = (a_{p1}, a_{p2}, \dots, a_{ps})$, $p \in 0:m-1$.

7°. Пусть $x(j) = (x_1(j), x_2(j), \dots, x_s(j))$. Поскольку

$$\sum_{j=0}^{N-1} \|(\Delta^r x)(j)\|^2 = \sum_{j=0}^{N-1} \sum_{\nu=1}^s |(\Delta^r x_\nu)(j)|^2 = \sum_{\nu=1}^s \sum_{j=0}^{N-1} |(\Delta^r x_\nu)(j)|^2,$$

то, принимая во внимание экстремальное свойство интерполяционного сплайна ([1], [2, с. 23–24]), можно утверждать, что векторный интерполяционный сплайн $\tilde{S}_r(j)$ является единственным решением экстремальной задачи

$$\sum_{j=0}^{N-1} \|(\Delta^r x)(j)\|^2 \rightarrow \min,$$

$$x(ln) = z(l), \quad l \in 0:m-1,$$

на множестве дискретных N -периодических вектор-функций $x = x(j)$, $j \in \mathbb{Z}$.

8°. Дискретные периодические сплайны с векторными коэффициентами можно использовать в геометрическом моделировании для построения замкнутых кривых. Чтобы пояснить это, перепишем формулу для $\tilde{S}_r(j)$ в виде

$$\tilde{S}_r(j) = \sum_{p=0}^{m-1} \tilde{Q}_r(j - pn) a_p.$$

Нас интересует случай вещественных a_p , $a_p \in \mathbb{R}^s$. При фиксированном j числа $\tilde{Q}_r(j - pn)$, $p \in 0:m-1$, неотрицательны и в сумме равны единице, так что $\tilde{S}_r(j)$ есть выпуклая комбинация векторов a_p . В геометрическом моделировании векторы a_p называются *полюсами*. Когда j пробегает значения от 0 до N , вектор $\tilde{S}(j)$ описывает замкнутую дискретную кривую в \mathbb{R}^s , содержащуюся в выпуклой оболочке полюсов. Кривую с требуемыми свойствами получают либо при непосредственном задании полюсов, либо при полюсах, определяемых из интерполяционных условий.

ПРИМЕР 1. Моделирование лепестковой кривой.

Пусть $m = 20$, $n = 16$, $r = 2$, $s = 2$. Решим задачу векторной сплайн-интерполяции для точек $z(j)$, приведённых в табл. 1 и изображённых на рис. 1. Коэффициенты a_p интерполяционного сплайна и его значения показаны на рис. 2. Замкнутая ломаная, полученная путём соединения соседних точек сплайна отрезками, представлена на рис. 3.

Таблица 1

j	$z(j)$	j	$z(j)$
0	(0.000, 0.000)	10	(0.000, 1.000)
1	(-0.698, 0.111)	11	(0.111, 0.698)
2	(-0.951, 0.309)	12	(0.000, 0.000)
3	(-0.630, 0.321)	13	(-0.321, -0.630)
4	(0.000, 0.000)	14	(-0.588, -0.809)
5	(0.500, -0.500)	15	(-0.500, -0.500)
6	(0.588, -0.809)	16	(0.000, 0.000)
7	(0.321, -0.630)	17	(0.630, 0.321)
8	(0.000, 0.000)	18	(0.951, 0.309)
9	(-0.111, 0.698)	19	(0.698, 0.111)

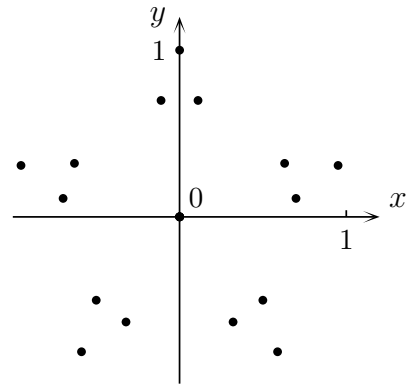


Рис. 1. Точки интерполяции

9°. Обратимся к двумерной задаче векторной сплайн-интерполяции. Пусть $N_1 = m_1 n_1$, $N_2 = m_2 n_2$, где m_1 , n_1 и m_2 , n_2 — натуральные числа, отличные от единицы. Зададим два набора вектор-функций

$$\begin{aligned} f_i &: (0:N_2-1) \rightarrow \mathbb{R}^3, & i &\in 0:m_1-1, \\ g_j &: (0:N_1-1) \rightarrow \mathbb{R}^3, & j &\in 0:m_2-1, \end{aligned}$$

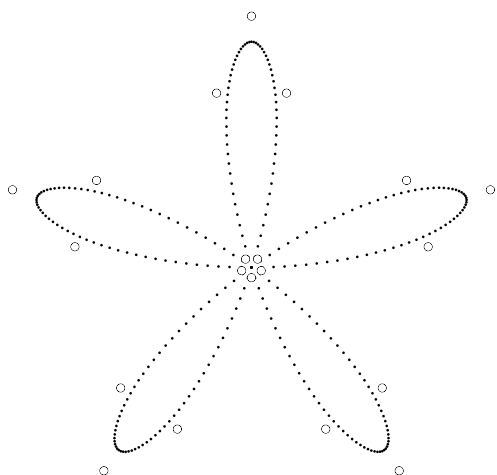


Рис. 2. Полюсы и значения дискретного сплайна

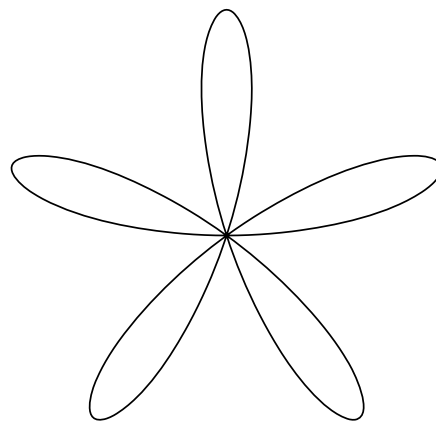


Рис. 3. Пятилистник

для которых выполнены равенства

$$f_i(jn_2) = g_j(in_1), \quad i \in 0:m_1-1, \quad j \in 0:m_2-1. \quad (19)$$

Ставится задача: построить вектор-функцию $c: (0:N_1-1) \times (0:N_2-1) \rightarrow \mathbb{R}^3$, удовлетворяющую условиям

$$c(in_1, \cdot) = f_i, \quad i \in 0:m_1-1, \quad (20)$$

$$c(\cdot, jn_2) = g_j, \quad j \in 0:m_2-1. \quad (21)$$

Выберем два натуральных числа r_1, r_2 . Для каждого $q \in 0:N_2-1$ построим сплайн $\tilde{S}_{r_1}^{(q)}$, решающий интерполяционную задачу

$$\tilde{S}_{r_1}^{(q)}(in_1) = f_i(q), \quad i \in 0:m_1-1. \quad (22)$$

Положим $h_j(p) = g_j(p) - \tilde{S}_{r_1}^{(jn_2)}(p)$ для всех $p \in 0:N_1-1, j \in 0:m_2-1$. Из (22) и (19) следует, что

$$h_j(in_1) = g_j(in_1) - f_i(jn_2) = 0, \quad i \in 0:m_1-1, \quad j \in 0:m_2-1. \quad (23)$$

Далее для каждого $p \in 0:N_1-1$ построим сплайн $\tilde{S}_{r_2}^{(p)}$, решающий интерполяционную задачу

$$\tilde{S}_{r_2}^{(p)}(jn_2) = h_j(p), \quad j \in 0:m_2-1. \quad (24)$$

Положим

$$c(p, q) = \tilde{S}_{r_1}^{(q)}(p) + \tilde{S}_{r_2}^{(p)}(q), \quad p \in 0:N_1-1, \quad q \in 0:N_2-1. \quad (25)$$

Покажем, что функция $c(p, q)$ удовлетворяет условиям (20) и (21).

Согласно (23) и (24), $\tilde{S}_{r_2}^{(in_1)}(jn_2) = 0$ при всех $j \in 0:m_2 - 1$, поэтому $\tilde{S}_{r_2}^{(in_1)}(q) \equiv 0$ при всех $i \in 0:m_1 - 1$. Принимая во внимание (22), получаем

$$c(in_1, q) = \tilde{S}_{r_1}^{(q)}(in_1) = f_i(q), \quad q \in 0:N_2 - 1, \quad i \in 0:m_1 - 1,$$

т. е. выполнено условие (20). В силу (24)

$$\begin{aligned} c(p, jn_2) &= \tilde{S}_{r_1}^{(jn_2)}(p) + \tilde{S}_{r_2}^{(p)}(jn_2) = \\ &= \tilde{S}_{r_1}^{(jn_2)}(p) + h_j(p) = g_j(p), \quad p \in 0:N_1 - 1, \quad j \in 0:m_2 - 1, \end{aligned}$$

т. е. условие (21) также выполнено.

10°. Рассмотрим задачу построения поверхности, имеющей вид замкнутой трубки. Определять форму поверхности будет осто́в, состоящий из двух наборов дискретных кривых. Кривые первого набора f_i будут идти вдоль трубки, кривые второго набора g_j — поперёк. Требуемая поверхность будет задаваться дискретным сплайном (25), N_1 -периодическим по первому аргументу и N_2 -периодическим — по второму.

ПРИМЕР 2. Моделирование трубчатой поверхности.

Начнём с задания плоской кривой, изображающей узел. Положим

$$\begin{aligned} x(t) &= \left(\frac{3}{4} + \frac{1}{4} \cos 3t\right) \cos 2t, \\ y(t) &= \left(\frac{3}{4} + \frac{1}{4} \cos 3t\right) \sin 2t. \end{aligned}$$

При изменении t от 0 до 2π точка $(x(t), y(t))$ описывает замкнутую кривую, представленную на рис. 4. Теперь добавим третью координату $z(t) = \frac{1}{5} \sin 3t$. Вектор-функция $r(t) = (x(t), y(t), z(t))$ определяет замкнутую пространственную кривую, имеющую вид узла.

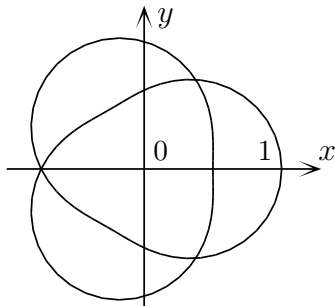


Рис. 4. Плоский узел

Введём две основные кривые, которые будут идти вдоль трубки:

$$\begin{aligned} r_0(t) &= r(t) + \frac{1}{10} \frac{r'(t) \times (0, 0, 1)}{\|r'(t) \times (0, 0, 1)\|}, \\ r_1(t) &= r(t) - \frac{1}{10} \frac{r'(t) \times (0, 0, 1)}{\|r'(t) \times (0, 0, 1)\|}. \end{aligned}$$

Здесь \times — знак векторного умножения. При фиксированном t точки $r_0(t)$ и $r_1(t)$ получаются

из $r(t)$ сдвигом на $\frac{1}{10}$ вдоль двух противоположных направлений, ортогональных вектору $r'(t)$ и оси Oz .

Поперечные сечения будут определять три остовные кривые $v_0(t)$, $v_1(t)$ и $v_2(t)$ — окружности с центрами $r(0)$, $r(2\pi/3)$, $r(4\pi/3)$, радиусом $\frac{1}{10}$, лежащие в плоскостях, ортогональных векторам $r'(0)$, $r'(2\pi/3)$ и $r'(4\pi/3)$ соответственно. Кривые r_0 , r_1 , v_0 , v_1 , v_2 изображены на рис. 5.

Осталось получить дискретные функции f_i и g_j из непрерывных функций r_i и v_j . Пусть $m_1 = 2$, $n_1 = 5$ и $m_2 = 3$, $n_2 = 40$, так что $N_1 = 10$, $N_2 = 120$. Положим

$$\begin{aligned} f_i(q) &= r_i(2\pi q/N_2), \quad q \in 0:N_2-1, \quad i \in 0:1, \\ g_j(p) &= v_j(2\pi p/N_1), \quad p \in 0:N_1-1, \quad j \in 0:2. \end{aligned}$$

На рис. 6 показана трубчатая поверхность, построенная по формуле (25). Остовные кривые выделены жирными линиями.

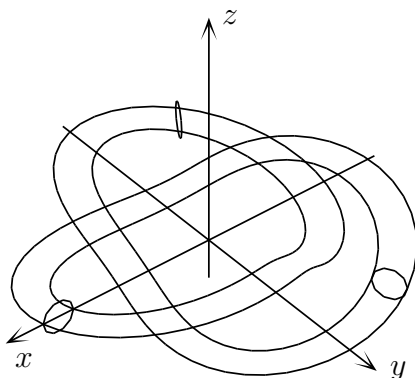


Рис. 5. Остовные кривые

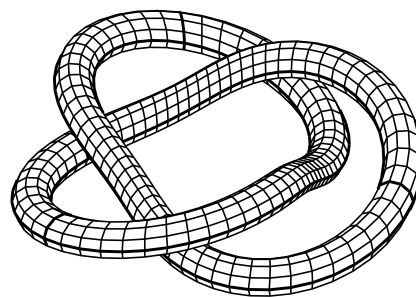


Рис. 6. Узел

ЛИТЕРАТУРА

1. Малозёмов В. Н., Певный А. Б. *Дискретные периодические сплайны и их вычислительные применения* // Журн. вычисл. мат. и матем. физ. 1998. Т. 38. № 8. С. 1235–1246.
2. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Часть третья. СПб.: НИИММ, 2003. 88 с.

ОБОБЩЁННЫЕ ПОВЕРХНОСТИ ВРАЩЕНИЯ

М. И. Григорьев

15 сентября 2007 г.

В данном докладе представлен вариант обобщения понятия классической поверхности вращения. Предложен метод построения обобщённых поверхностей вращения, аналогичный методу из [1].

1°. Напомним, что поверхность вращения в классическом понимании образована вращением некоторой плоской кривой относительно прямолинейной оси, лежащей в плоскости этой кривой. Первое возможное обобщение связано с заменой оси вращения на некоторую пространственную кривую. Кроме того, можно обобщить само понятие вращения так, что сечением такой поверхности становится не окружность, а эллипс с двумя независимыми радиусами.

Итак, пусть $C: [0, 1] \rightarrow \mathbb{R}^3$ задаёт некоторую непрерывно-дифференцируемую кривую. Будем называть её *кривой центров*. Предположим, что $\|C'(t)\| \neq 0$ при любом $t \in [0, 1]$. Обозначим

$$T(t) = C'(t)/\|C'(t)\|, \quad t \in [0, 1].$$

Вектор $T(t)$ является единичным вектором касательной к кривой C .

Пусть далее $f_N, f_B: [0, 1] \rightarrow \mathbb{R}$, $f_t: [0, 1] \rightarrow [0, 1]$ — непрерывные функции. Вектор-функция

$$F(u) = (f_N(u), f_B(u), f_t(u)), \quad u \in [0, 1],$$

определяет параметрическую кривую в \mathbb{R}^3 . Назовём её *кривой радиусов*. Функция $f_t(u)$ управляет положением центров вращения на кривой C .

Выберем также некоторую непрерывную вектор-функцию $B: [0, 1] \rightarrow \mathbb{R}^3$ такую, чтобы для всех t из отрезка $[0, 1]$ вектор $B(t)$ имел единичную длину и был ортогонален вектору $T(t)$. Положим

$$N(t) = B(t) \times T(t), \tag{1}$$

где \times — знак векторного умножения.

Зафиксируем некоторое $u \in [0, 1]$. Рассмотрим точку на кривой центров C , соответствующую значению параметра t , равному $t_u = f_t(u)$. Пара $(N(t_u), B(t_u))$ определяет нормальную плоскость к кривой в этой точке (см. рис. 1). Рассмотрим лежащий в этой плоскости эллипс с центром в точке $C(t_u)$ и радиусами $f_N(u)$, $f_B(u)$:

$$G(u, v) = C(t_u) + (f_N(u) \cos 2\pi v) N(t_u) + (f_B(u) \sin 2\pi v) B(t_u), \quad v \in [0, 1]. \quad (2)$$

Когда параметр u пробегает все значения от 0 до 1, кривая (2) порождает поверхность в пространстве \mathbb{R}^3 , которая называется *обобщённой поверхностью вращения* кривой радиусов F относительно кривой центров C .

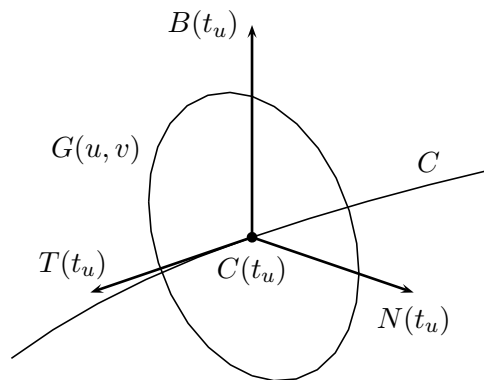


Рис. 1

2°. Пусть на плоскости зафиксированы три полюса P_0 , P_1 , P_2 . По ним можно построить проективную кривую Безье второго порядка [2, с. 212–221]

$$R(v) = (r_x(v), r_y(v)) = \frac{P_0(1-v)^2 + 2wP_1v(1-v) + P_2v^2}{(1-v)^2 + 2wv(1-v) + v^2}, \quad v \in [0, 1], \quad (3)$$

где w — некоторое положительное число. Известно, что если полюсы P_0 , P_1 , P_2 расположены в вершинах единичного квадрата так, как показано на рис. 2, и выполнено условие $w = \sqrt{2}/2$, то кривая (3) является четвертью окружности единичного радиуса [3].

Четверть эллипса можно построить таким же образом. Зафиксируем два положительных числа a, b и рассмотрим кривую

$$\tilde{R}(v) = (a r_x(v), b r_y(v)), \quad v \in [0, 1], \quad (4)$$

построенную по полюсам $\tilde{P}_0(a, 0), \tilde{P}_1(a, b), \tilde{P}_2(0, b)$. Здесь $r_x(v)$ и $r_y(v)$ те же, что и в (3). Очевидно, что если значение w равно $\sqrt{2}/2$, то кривая (4) представляет собой четверть эллипса с радиусами a, b (рис. 3).

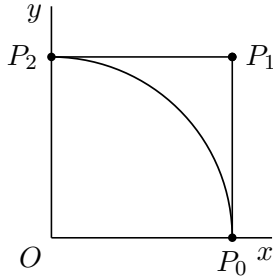


Рис. 2

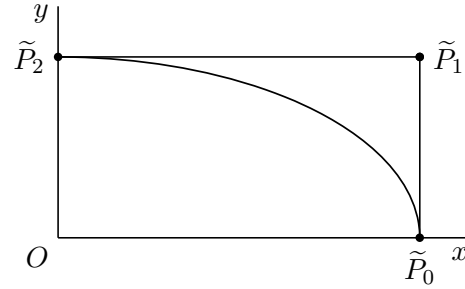


Рис. 3

3°. В [1] было показано, как строить классические поверхности вращения с помощью проективных кривых Безье второго порядка. Подобный подход применим и к обобщённым поверхностям вращения.

Рассмотрим три вектор-функции $P_0, P_1, P_2: [0, 1] \rightarrow \mathbb{R}^3$,

$$\begin{aligned} P_0(u) &= C(t_u) + f_N(u)N(t_u), & P_2(u) &= C(t_u) + f_B(u)B(t_u), \\ P_1(u) &= C(t_u) + f_N(u)N(t_u) + f_B(u)B(t_u). \end{aligned}$$

Зафиксируем $u \in [0, 1]$. Уравнение проективной кривой второго порядка, построенной по полюсам $P_0(u), P_1(u), P_2(u)$ с параметром $w = \sqrt{2}/2$ имеет вид

$$\tilde{G}(u, v) = \frac{P_0(u)(1-v)^2 + \sqrt{2}P_1(u)v(1-v) + P_2(u)v^2}{(1-v)^2 + \sqrt{2}v(1-v) + v^2}, \quad v \in [0, 1].$$

Перепишем эту формулу

$$\tilde{G}(u, v) = C(t_u) + \frac{\tilde{P}_0(u)(1-v)^2 + \sqrt{2}\tilde{P}_1(u)v(1-v) + \tilde{P}_2(u)v^2}{(1-v)^2 + \sqrt{2}v(1-v) + v^2}. \quad (5)$$

Здесь

$$\begin{aligned} \tilde{P}_0(u) &= f_N(u)N(t_u), & \tilde{P}_2(u) &= f_B(u)B(t_u), \\ \tilde{P}_1(u) &= f_N(u)N(t_u) + f_B(u)B(t_u). \end{aligned}$$

На основании пункта 2° заключаем, что кривая (5) является четвертью эллипса с центром в точке $C(t_u)$ и радиусами $f_N(u)$, $f_B(u)$, лежащего в нормальной плоскости.

Когда параметр u пробегает все значения от 0 до 1, кривая $\tilde{G}(u, v)$ порождает поверхность в пространстве \mathbb{R}^3 , которая по построению совпадает с четвертью обобщённой поверхности вращения $G(u, v)$ (рис. 4).

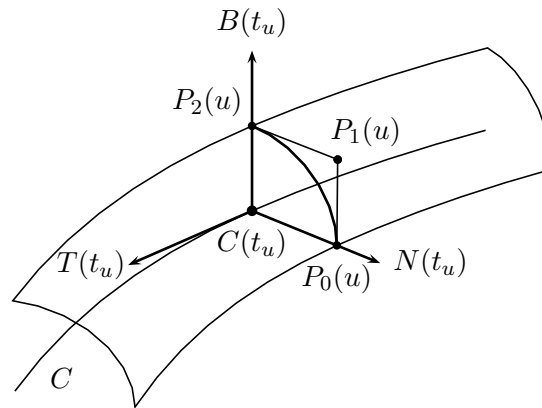


Рис. 4

4°. Укажем некоторые возможные способы выбора вектор-функции B и приведём примеры обобщённых поверхностей вращения.

Рассмотрим сначала простой случай, когда кривая центров C является плоской. Не ограничивая общности можно считать, что кривая C лежит в плоскости Oxz . Положим

$$B(t) \equiv (0, 1, 0). \quad (6)$$

С учётом (1) и (6) имеем

$$N(t) = (T_z(t), 0, -T_x(t)), \quad t \in [0, 1], \quad (7)$$

где $T_x(t)$, $T_z(t)$ — первая и третья компоненты вектор-функции $T(t)$.

На рис. 5 представлены кривая радиусов F (в данном примере f_N совпадает с f_B и $f_t(u) \equiv u$) и кривая центров C . Соответствующая им поверхность вращения изображена на рис. 6.

Когда в качестве кривой центров выбран отрезок оси Oz , и радиусы f_N , f_B тождественно равны, обобщённая поверхность вращения представляет собой обычную поверхность вращения. Пример такой поверхности дан на рис. 7. Порождающие кривая радиусов и кривая центров приведены на рис. 8.

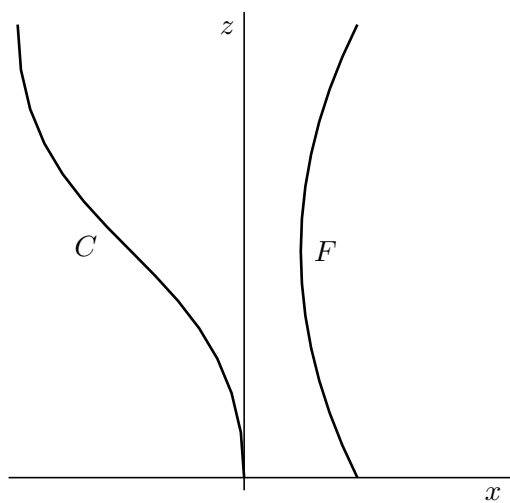


Рис. 5

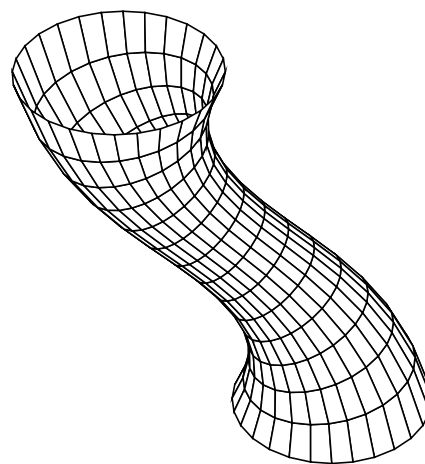


Рис. 6

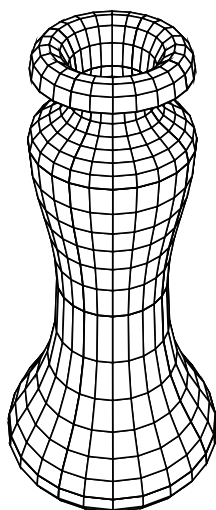


Рис. 7

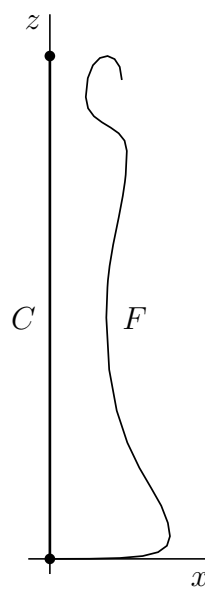


Рис. 8

Вернёмся к общему случаю пространственной кривой центров C . Укажем наиболее простой способ выбора B . Введём дополнительное предположение, что кривая центров обладает гладкостью второго порядка и что

$$\|C''(t)\| > 0, \quad t \in [0, 1]. \quad (8)$$

Положим

$$B(t) = \frac{C'(t) \times C''(t)}{\|C'(t) \times C''(t)\|}, \quad t \in [0, 1]. \quad (9)$$

Выражение (9) определяет бинормальный вектор к кривой центров в точке $C(t)$. Значит, вектор $N(t) = B(t) \times T(t)$ равен вектору главной нормали к кривой C в этой точке, а правая тройка векторов $T(t)$, $N(t)$, $B(t)$ образует базис Френе [4].

На рис. 9 приведён пример обобщённой поверхности вращения, построенной с учётом выбранной в данном пункте вектор-функции $B(t)$. Порождающая кривая радиусов F представлена на рис. 10 (для наглядности приведены также её проекции на координатные плоскости Oxz и Oyz). В качестве кривой центров использована дуга винтовой кривой.

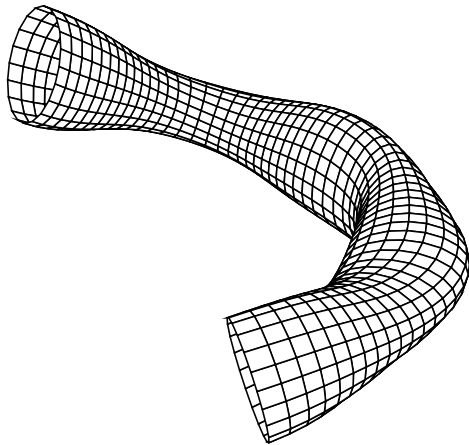


Рис. 9

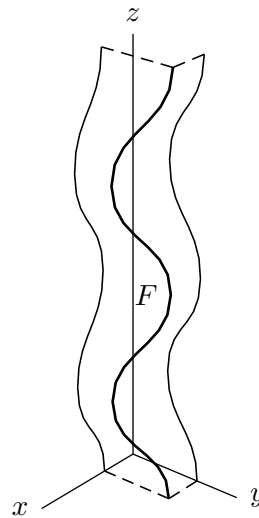


Рис. 10

5°. Условие (8) сильно ограничивает поведение кривой центров. Укажем ещё один способ выбора вектор-функции $B(t)$, не требующий гладкости второго порядка, но предполагающий существование ненулевого вектора N_0 такого, что

$$\|T(t) \times N_0\| \neq 0, \quad t \in [0, 1]. \quad (10)$$

Положим

$$B(t) = \frac{T(t) \times N_0}{\|T(t) \times N_0\|}, \quad t \in [0, 1].$$

Вектор $B(t)$ и в этом случае ортогонален касательному вектору $T(t)$ при каждом $t \in [0, 1]$ и имеет единичную длину.

Поясним геометрический смысл такого выбора. Зафиксируем $t \in [0, 1]$ и рассмотрим две плоскости, проходящие через точку $C(t)$ и имеющие нормальные векторы $T(t)$ и N_0 . Из (10) следует, что эти плоскости не совпадают. Прямая, по которой они пересекаются проходит через точку $C(t)$ и имеет направление $B(t)$.

ЛИТЕРАТУРА

1. Григорьев М. И. *Построение поверхностей вращения* // Семинар «ДНА & CAGD». Избранные доклады. 27 июня 2007 г. (<http://dha.spb.ru/rep07.shtml#0627>).
2. Голованов Н. Н., Илютко Д. П., Носовский Г. В., Фоменко А. Т. *Компьютерная геометрия*. М.: Академия, 2006. 512 с.
3. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Можно ли построить окружность с помощью кривых Безье?* // Семинар «ДНА & CAGD». Избранные доклады. 16 декабря 2006 г. (<http://dha.spb.ru/rep06.shtml#1216>).
4. Погорелов А. И. *Дифференциальная геометрия*. 6-е изд. М.: Наука, 1974. 176 с.

РАВНОУГОЛЬНЫЕ СИСТЕМЫ ВЕКТОРОВ И ЖЁСТКИЕ ФРЕЙМЫ

В. Н. Малозёмов А. Б. Певный

18 сентября 2007 г.

1°. Пусть \mathbb{H}^n — это либо вещественное пространство \mathbb{R}^n , либо комплексное пространство \mathbb{C}^n .

Система векторов $\{\varphi_1, \dots, \varphi_m\}$ из \mathbb{H}^n называется *равноугольной*, если

$$\|\varphi_k\| = 1 \quad \text{при всех } k \in 1 : m \quad \text{и} \quad |\langle \varphi_k, \varphi_s \rangle| = c \quad \text{при } k \neq s.$$

Нас интересует случай $m \geq n$. При $m = n$ любой ортонормированный базис в \mathbb{H}^n образует равноугольную систему, у которой $c = 0$.

Равноугольные системы векторов изучались в работах [1, 2, 3]. В силу нормированности векторов, входящих в равноугольную систему, для константы c выполняется неравенство $c \leq 1$. При $c < 1$ количество элементов m равноугольной системы не превосходит числа $n(n+1)/2$ в вещественном случае ($\mathbb{H}^n = \mathbb{R}^n$) и числа n^2 в комплексном случае ($\mathbb{H}^n = \mathbb{C}^n$). По поводу этих результатов авторы [1] ссылаются на [4]. Авторы [3] рассматривают только вещественный случай и указывают в качестве первоисточника [5]. В докладе приводятся доказательства данных результатов, использующие лишь элементарные сведения из линейной алгебры.

Кроме того, установлен критерий, при выполнении которого равноугольная система будет жёстким фреймом.

2°. Начнём с более простого, с упомянутого критерия.

ТЕОРЕМА 1. *Равноугольная система является жёстким фреймом тогда и только тогда, когда*

$$c = \sqrt{\frac{m-n}{n(m-1)}}. \quad (1)$$

Доказательство. Пусть $\Phi = \{\varphi_1, \dots, \varphi_m\}$ — равноугольная система. Вычислим её фреймовый потенциал:

$$P(\Phi) := \sum_{k,s=1}^m |\langle \varphi_k, \varphi_s \rangle|^2 = m + m(m-1)c^2. \quad (2)$$

Напомним [6], что жёсткий фрейм, состоящий из единичных векторов, характеризуется равенством

$$P(\Phi) = \frac{m^2}{n}. \quad (3)$$

Таким образом, если равноугольная система Φ является жёстким фреймом, то соотношения (2) и (3) выполняются одновременно. Отсюда очевидным образом следует (1).

Наоборот, если у равноугольной системы Φ величина c определяется формулой (1), то согласно (2) для фреймового потенциала $P(\Phi)$ справедливо равенство (3), характеризующее систему Φ как жёсткий фрейм. \square

СЛЕДСТВИЕ. При $m = n$ равноугольная система $\Phi = \{\varphi_1, \dots, \varphi_n\}$ будет жёстким фреймом тогда и только тогда, когда $c = 0$, т. е. когда Φ — ортонормированный базис в \mathbb{H}^n .

3°. При $m = n+1$ примером равноугольной системы, являющейся жёстким фреймом, служит система Мерседес-Бенц $\{b_1^n, \dots, b_{n+1}^n\}$, у которой

$$\langle b_k^n, b_s^n \rangle = -\frac{1}{n} \quad \text{при } k \neq s$$

(см. [7]). Отметим, что если из системы Мерседес-Бенц удалить один элемент, то оставшаяся система, не теряя свойства равноугольности и величины c , уже не будет жёстким фреймом.

4°. Приведём нетривиальный пример равноугольного жёсткого фрейма в \mathbb{R}^3 , состоящего из шести векторов ($n = 3$, $m = 6$). Обозначим

$$\begin{aligned} g_1 &= (\alpha, 1, 0), & g_4 &= (\alpha, -1, 0), \\ g_2 &= (0, \alpha, 1), & g_5 &= (0, \alpha, -1), \\ g_3 &= (1, 0, \alpha), & g_6 &= (-1, 0, \alpha), \end{aligned}$$

где $\alpha > 0$ — параметр, который мы выберем из следующих соображений. Скалярные произведения $\langle g_k, g_s \rangle$ при $k \neq s$ равны либо $\pm\alpha$, либо $\alpha^2 - 1$. Приравняв α к $\alpha^2 - 1$, получим единственный положительный корень $\alpha_0 = \frac{1+\sqrt{5}}{2}$. При $\alpha = \alpha_0$ и $k \neq s$

$$|\langle g_k, g_s \rangle| = \frac{1 + \sqrt{5}}{2}.$$

Введём нормированные векторы

$$\varphi_k = \frac{g_k}{\sqrt{1 + \alpha_0^2}} = \sqrt{\frac{2}{5 + \sqrt{5}}} g_k.$$

Для них

$$|\langle \varphi_k, \varphi_s \rangle| = \frac{1 + \sqrt{5}}{5 + \sqrt{5}} = \frac{1}{\sqrt{5}} \quad \text{при } k \neq s.$$

Вместе с тем, при $n = 3$, $m = 6$

$$\sqrt{\frac{m-n}{n(m-1)}} = \frac{1}{\sqrt{5}}.$$

На основании теоремы 1 заключаем, что при $\alpha = \alpha_0$ векторы $\{\varphi_1, \dots, \varphi_6\}$ образуют равноугольный жёсткий фрейм.

5°. Приведём пример равноугольного жёсткого фрейма в \mathbb{C}^n [8]. При его построении используется тот факт, что при некоторых n и $m = n^2 - n + 1$ существует n целых неотрицательных чисел

$$0 \leq d_1 < d_2 < \dots < d_n \leq m - 1,$$

таких, что

$$\{\langle d_k - d_s \rangle_m \mid k \neq s\} = \{1, 2, \dots, m - 1\}. \quad (4)$$

Здесь $\langle d_k - d_s \rangle_m$ — остаток от деления числа $d_k - d_s$ на m .

Например, при $n = 3$, $m = 7$ можно взять $d_1 = 1$, $d_2 = 2$, $d_3 = 6$. В этом случае

$$\begin{aligned} \langle d_2 - d_1 \rangle_7 &= 1, & \langle d_1 - d_2 \rangle_7 &= 6, \\ \langle d_3 - d_1 \rangle_7 &= 5, & \langle d_1 - d_3 \rangle_7 &= 2, \\ \langle d_3 - d_2 \rangle_7 &= 4, & \langle d_2 - d_3 \rangle_7 &= 3. \end{aligned}$$

Такие последовательности $\{d_k\}_{k=1}^n$ гарантированно можно построить при $n = p^l + 1$, где p — простое и l — натуральное числа [9].

Допустим, что n , $m = n^2 - n + 1$ и $\{d_k\}_{k=1}^n$ уже выбраны. Введём m векторов из \mathbb{C}^n :

$$\varphi_k(j) = \frac{1}{\sqrt{n}} \omega_m^{kd_j}, \quad j \in 1 : n, \quad k \in 1 : m,$$

где $\omega_m = \exp(2\pi i/m)$. Очевидно, что $\|\varphi_k\| = 1$ при всех $k \in 1 : m$. При $k \neq s$ согласно (4) имеем

$$|\langle \varphi_k, \varphi_s \rangle|^2 = \langle \varphi_k, \varphi_s \rangle \langle \varphi_s, \varphi_k \rangle = \left(\frac{1}{n} \sum_{j=1}^n \omega_m^{(k-s)d_j} \right) \left(\frac{1}{n} \sum_{j=1}^n \omega_m^{-(k-s)d_j} \right) =$$

$$\begin{aligned}
&= \frac{1}{n^2} \sum_{j,l=1}^n \omega_m^{(k-s)(d_j-d_l)} = \frac{1}{n} + \frac{1}{n^2} \sum_{j \neq l} \omega_m^{(k-s)(d_j-d_l)_m} = \\
&= \frac{1}{n} + \frac{1}{n^2} \left(\sum_{r=0}^{m-1} \omega_m^{(k-s)r} - 1 \right).
\end{aligned}$$

Как известно [10], сумма по r равна $m \delta_m(k-s)$, а поскольку $k \neq s$ и $|k-s| \leq m-1$, то $m \delta_m(k-s) = 0$. Значит,

$$|\langle \varphi_k, \varphi_s \rangle|^2 = \frac{1}{n} - \frac{1}{n^2} = \frac{n-1}{n^2},$$

так что

$$|\langle \varphi_k, \varphi_s \rangle| = \frac{\sqrt{n-1}}{n} \quad \text{при } k \neq s. \quad (5)$$

Принимая во внимание, что в данном случае

$$\sqrt{\frac{m-n}{n(m-1)}} = \frac{n-1}{\sqrt{n(n^2-n)}} = \frac{\sqrt{n-1}}{n},$$

на основании (5) и теоремы 1 заключаем, что $\{\varphi_1, \dots, \varphi_m\}$ — равноугольный жёсткий фрейм.

6°. Напомним, что векторы в равноугольной системе $\{\varphi_1, \dots, \varphi_m\}$ — единичные, поэтому в равенстве $|\langle \varphi_k, \varphi_s \rangle| = c$ константа c не превосходит единицы. Она равна единице только тогда, когда $\varphi_k = \xi_k \varphi_1$ при $k \in 2 : m$, где комплексные коэффициенты ξ_k по модулю равны единице. В этом случае количество элементов m в равноугольной системе может быть произвольным. Принципиальный факт заключается в том, что при $c < 1$ число m ограничено сверху.

Сначала рассмотрим вещественный случай, $\mathbb{H}^n = \mathbb{R}^n$.

ТЕОРЕМА 2. Пусть $\{\varphi_1, \dots, \varphi_m\}$, $m \geq n$, — равноугольная система в \mathbb{R}^n и $c \in [0, 1)$. Тогда

$$m \leq \frac{n(n+1)}{2}. \quad (6)$$

Доказательство. Введём симметричные матрицы $P_k = \varphi_k \varphi_k^T$, $k \in 1 : m$, с элементами

$$P_k[i, j] = \varphi_k(i) \varphi_k(j), \quad i, j \in 1 : n.$$

Покажем, что если при некоторых вещественных $\lambda_1, \dots, \lambda_m$ будет

$$\sum_{k=1}^m \lambda_k P_k = 0, \quad (7)$$

то необходимо все λ_k равны нулю.

Рассмотрим скалярное произведение матриц

$$\langle P_k, P_s \rangle = \sum_{i,j=1}^n P_k[i, j] P_s[i, j].$$

В силу определения P_k

$$\langle P_k, P_s \rangle = \left(\sum_{i=1}^n \varphi_k(i) \varphi_s(i) \right) \left(\sum_{j=1}^n \varphi_k(j) \varphi_s(j) \right) = [\langle \varphi_k, \varphi_s \rangle]^2.$$

Умножим обе части равенства (7) скалярно на P_s . Получим

$$\sum_{k=1}^m [\langle \varphi_k, \varphi_s \rangle]^2 \lambda_k = 0, \quad s \in 1 : m. \quad (8)$$

Нужно показать, что система (8) имеет только нулевое решение.

Матрица G системы (8) в силу условий $\|\varphi_k\| = 1$ при $k \in 1 : m$ и $|\langle \varphi_s, \varphi_k \rangle| = c$ при $s \neq k$ имеет вид

$$G = \begin{bmatrix} 1 & c^2 & c^2 & \dots & c^2 \\ c^2 & 1 & c^2 & \dots & c^2 \\ c^2 & c^2 & 1 & \dots & c^2 \\ \dots & \dots & \dots & \dots & \dots \\ c^2 & c^2 & c^2 & \dots & 1 \end{bmatrix}.$$

При $c \in [0, 1)$ она невырождена. Более того, она положительно определена. Действительно,

$$\begin{aligned} \langle G\lambda, \lambda \rangle &= \|\lambda\|^2 + c^2 \sum_{s \neq k} \lambda_s \lambda_k = (1 - c^2) \|\lambda\|^2 + c^2 \sum_{s,k=1}^m \lambda_s \lambda_k = \\ &= (1 - c^2) \|\lambda\|^2 + c^2 \left\| \sum_{k=1}^m \lambda_k \right\|^2 \geq (1 - c^2) \|\lambda\|^2. \end{aligned}$$

Значит, система (8) имеет только нулевое решение.

Установлено, что соотношение (7) выполняется только тогда, когда все коэффициенты λ_k равны нулю.

Теперь введём векторы A_k , $k \in 1 : m$, с компонентами $P_k[i, j]$, $i \leq j$. Их размерность равна $n(n+1)/2$. Покажем, что они линейно независимы.

Запишем соотношение

$$\sum_{k=1}^m \lambda_k A_k = \mathbb{O}. \quad (9)$$

В силу симметричности матриц P_k из (9) следует (7), а тогда по доказанному все коэффициенты λ_k необходимо равны нулю. Это гарантирует линейную независимость векторов A_1, \dots, A_m . Неравенство (6) основано на том, что количество линейно независимых векторов не превосходит их размерности.

Теорема доказана. \square

Отметим, что в примере из п. 3° построен равноугольный жёсткий фрейм в \mathbb{R}^3 с максимально возможным количеством элементов ($n = 3, m = 6$).

7°. Обратимся к комплексному случаю, $\mathbb{H}^n = \mathbb{C}^n$.

ТЕОРЕМА 3. Пусть $\{\varphi_1, \dots, \varphi_m\}$, $m \geq n$, — равноугольная система в \mathbb{C}^n и $c \in [0, 1)$. Тогда

$$m \leq n^2. \quad (10)$$

Доказательство проводится по той же схеме, что и предыдущее. Введём матрицы $P_k = \varphi_k \varphi_k^*$, $k \in 1 : m$, с элементами

$$P_k[i, j] = \varphi_k(i) \overline{\varphi_k(j)}, \quad i, j \in 1 : n.$$

Ясно, что P_k — эрмитовы матрицы. В частности, их диагональные элементы вещественны. Покажем, что если при некоторых вещественных $\lambda_1, \dots, \lambda_m$ будет

$$\sum_{k=1}^m \lambda_k P_k = 0, \quad (11)$$

то необходимо все λ_k равны нулю.

Рассмотрим скалярное произведение комплексных матриц

$$\langle P_k, P_s \rangle = \sum_{i,j=1}^n P_k[i, j] \overline{P_s[i, j]}.$$

В силу определения P_k

$$\langle P_k, P_s \rangle = \left(\sum_{i=1}^n \varphi_k(i) \overline{\varphi_s(i)} \right) \left(\sum_{j=1}^n \overline{\varphi_k(j)} \varphi_s(j) \right) = |\langle \varphi_k, \varphi_s \rangle|^2.$$

Умножим обе части равенства (11) скалярно на P_s . Получим

$$\sum_{k=1}^m |\langle \varphi_s, \varphi_k \rangle|^2 \lambda_k = 0, \quad s \in 1 : m.$$

Эта система уравнений не отличается от (8) и так же, как (8), имеет только нулевое решение. Значит, соотношение (11) выполняется только тогда, когда все коэффициенты λ_k равны нулю.

Теперь введём вещественные векторы A_k , $k \in 1 : n$, с компонентами

$$P_k[i, i] \quad \text{при } i \in 1 : n; \quad \operatorname{Re} P_k[i, j], \quad \operatorname{Im} P_k[i, j] \quad \text{при } i < j.$$

Их размерность равна $n + n(n - 1) = n^2$. Покажем, что они линейно независимы. Запишем соотношение

$$\sum_{k=1}^m \lambda_k A_k = \mathbb{O}. \quad (12)$$

В силу эрмитовости матриц P_k из (12) следует (11), а тогда по доказанному все коэффициенты λ_k равны нулю. Это гарантирует линейную независимость векторов A_1, \dots, A_m . Неравенство (10) основано на том, что в евклидовом пространстве количество линейно независимых векторов не превосходит их размерности. Теорема доказана. \square

Идея доказательства теорем 2 и 3 взята из работы [3]. При этом авторы [3] ссылаются на [5].

ЛИТЕРАТУРА

1. Strohmer T., Heath R. W. *Grassmannian frames with applications to coding and communication* // Appl. Comput. Harmonic Anal. 2003. V. 14. No. 3. P. 257–275.
2. Waldron S., Hay N. *On computing all harmonic frames of n vectors in \mathbb{C}^d* // Appl. Comput. Harmonic Anal. 2006. V. 21. P. 168–181.
3. Benedetto J. J., Kolesar J. D. *Geometric properties of Grassmannian frames for \mathbb{R}^2 and \mathbb{R}^3* // EURASIP J. Applied Signal Proc. 2006. Article ID 49850. P. 1–17.
4. Delsarte P., Goetals J. M., Seidel J. J. *Bounds for systems of lines and Jacobi polynomials* // Philips Res. Repts. 1975. V. 30. No. 3. P. 91–105.
5. Lemmens P. W. H., Seidel J. J. *Equiangular lines* // J. of Algebra. 1973. V. 24. No. 3. P. 494–512.
6. Малозёмов В. Н., Певный А. Б. *Четвёртое определение жёсткого фрейма* // Семинар «DHA & CAGD». Избранные доклады. 30 мая 2007 г. (<http://dha.spb.ru/rep07.shtml#0530>).
7. Малозёмов В. Н., Певный А. Б. *Системы Мерседес-Бенц и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 28 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0228>).

8. König H. *Cubatures formulas on spheres* // Math. Res. 1999. V. 107. P. 201–211.
9. Halberstam H., Roth K. *Sequences*. Springer, 1982.
10. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Часть первая. СПб: НИИМ СПбГУ, 2003.

ПРИМЕНЕНИЕ СХЕМЫ КЛЕНШОУ ДЛЯ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ С ТРЁХ- И ПЯТИДИАГОНАЛЬНЫМИ ЦИКЛИЧЕСКИМИ МАТРИЦАМИ

А. Н. Сабаев

25 сентября 2007 г.

1°. Пусть $n \geq 3$. Квадратную матрицу A_n над полем \mathbb{C} вида

$$A_n = \begin{pmatrix} p_1 & 1 & 0 & 0 & \dots & 0 & 0 & q_1 \\ q_2 & p_2 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & q_3 & p_3 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & q_{n-1} & p_{n-1} & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & q_n & p_n \end{pmatrix}$$

будем называть трёхдиагональной циклической матрицей.

Рассмотрим систему линейных уравнений n -го порядка с трёхдиагональной циклической матрицей

$$A_n X_n = F_n, \quad (1)$$

где

$$X_n = (x_1, x_2, \dots, x_n)^T, \quad F_n = (f_1, f_2, \dots, f_n)^T.$$

Введём вспомогательные переменные x_0 и x_{n+1} связанные с переменными системы (1) равенствами

$$x_0 = x_n, \quad x_{n+1} = x_1. \quad (2)$$

Объединим систему (1) с уравнениями (2). Получим равносильную систему

$$\begin{cases} q_k x_{k-1} + p_k x_k + x_{k+1} = f_k, & k \in 1 : n, \\ x_n = x_0, & x_{n+1} = x_1. \end{cases} \quad (3)$$

2°. Покажем, как схема Кленшоу позволяет свести решение системы (3) к решению системы уравнений второго порядка.

Систему (3) можно представить в виде

$$\begin{cases} q_k x_{k-1} + p_k x_k + x_{k+1} = f_k, & k \in 1 : n, \\ x_0 = \sum_{k=1}^n a_k x_k, & x_1 = \sum_{k=1}^{n+1} b_k x_k, \end{cases} \quad (4)$$

где $a_1 = a_2 = \dots = a_{n-1} = 0$, $a_n = 1$; $b_1 = b_2 = \dots = b_n = 0$, $b_{n+1} = 1$.

Определим последовательности $u = \{u_k\}_{k=0}^{n+1}$ и $v = \{v_k\}_{k=0}^{n+2}$ формулами

$$a_k = q_{k+1} u_{k+1} + p_k u_k + u_{k-1}, \quad k = n, n-1, \dots, 1; \quad u_{n+1} = u_n = 0; \quad (5)$$

$$b_k = q_{k+1} v_{k+1} + p_k v_k + v_{k-1}, \quad k = n+1, n, \dots, 1; \quad v_{n+2} = v_{n+1} = 0. \quad (6)$$

Здесь для единообразия формул введены коэффициенты q_{n+2} , q_{n+1} , p_{n+1} , которые могут иметь любые значения из \mathbb{C} .

Такие последовательности существуют:

$$u_n = 0, \quad u_{n-1} = 1; \quad u_{k-1} = -p_k u_k - q_{k+1} u_{k+1}, \quad k = n-1, n-2, \dots, 1; \quad (7)$$

$$v_n = 1, \quad v_{n-1} = -p_n; \quad v_{k-1} = -p_k v_k - q_{k+1} v_{k+1}, \quad k = n-1, n-2, \dots, 1. \quad (8)$$

С учётом введённых последовательностей u и v преобразуем суммы в правых частях последних двух уравнений системы (4)

$$\begin{aligned} x_0 &= \sum_{k=1}^n (q_{k+1} u_{k+1} + p_k u_k + u_{k-1}) x_k = \\ &= \sum_{k=2}^{n+1} u_k q_k x_{k-1} + \sum_{k=1}^n u_k p_k x_k + \sum_{k=0}^{n-1} u_k x_{k+1} = \\ &= u_0 x_1 - u_1 q_1 x_0 + \sum_{k=1}^{n-1} u_k (q_k x_{k-1} + p_k x_k + x_{k+1}); \\ x_1 &= \sum_{k=1}^{n+1} (q_{k+1} v_{k+1} + p_k v_k + v_{k-1}) x_k = \\ &= \sum_{k=2}^{n+2} v_k q_k x_{k-1} + \sum_{k=1}^{n+1} v_k p_k x_k + \sum_{k=0}^n v_k x_{k+1} = \\ &= v_0 x_1 - v_1 q_1 x_0 + \sum_{k=1}^n v_k (q_k x_{k-1} + p_k x_k + x_{k+1}). \end{aligned}$$

Теперь систему (4) можно представить в виде

$$\begin{cases} q_k x_{k-1} + p_k x_k + x_{k+1} = f_k, & k \in 1 : n, \\ (1 + u_1 q_1) x_0 - u_0 x_1 = \sum_{k=1}^{n-1} u_k (q_k x_{k-1} + p_k x_k + x_{k+1}), \\ v_1 q_1 x_0 + (1 - v_0) x_1 = \sum_{k=1}^n v_k (q_k x_{k-1} + p_k x_k + x_{k+1}). \end{cases} \quad (9)$$

Ясно, что система (9) равносильна системе (4).

Отсюда получается равносильная система

$$\begin{cases} q_k x_{k-1} + p_k x_k + x_{k+1} = f_k, & k \in 1 : n, \\ (1 + u_1 q_1) x_0 - u_0 x_1 = \sum_{k=1}^{n-1} u_k f_k, \\ v_1 q_1 x_0 + (1 - v_0) x_1 = \sum_{k=1}^n v_k f_k. \end{cases} \quad (10)$$

Заметим, что последние два уравнения системы (10) составляют замкнутую подсистему относительно x_0 и x_1

$$\begin{cases} (1 + u_1 q_1) x_0 - u_0 x_1 = \sum_{k=1}^{n-1} u_k f_k, \\ v_1 q_1 x_0 + (1 - v_0) x_1 = \sum_{k=1}^n v_k f_k. \end{cases} \quad (11)$$

Неизвестные x_2, \dots, x_{n+1} однозначно вычисляются для каждой пары x_0, x_1 найденной из (11). Для этого нужно воспользоваться первыми n уравнениями системы (10) представленными в виде рекуррентного соотношения

$$x_k = f_{k-1} - p_{k-1} x_{k-1} - q_{k-1} x_{k-2}, \quad k \in 2 : n + 1. \quad (12)$$

Равносильность проделанных преобразований позволяет утверждать, что возможность решения системы (1), а также единственность решения системы (1) определяются свойствами системы (11). Здесь могут представиться три случая.

- 1) Система (11) несовместна. Следовательно исходная система (1) тоже несовместна.

- 2) Система (11) имеет единственное решение. В этом случае исходная система (1) тоже имеет единственное решение.
- 3) Система (11) имеет бесконечное множество решений. В этом случае исходная система (1) тоже имеет бесконечное множество решений.

З а м е ч а н и е 0.1. При проведении вычислений по формуле (12) можно ограничиться индексным множеством $k \in 2 : n - 1$, так как значения неизвестных x_n и x_{n+1} дают последние два уравнения системы (3). Более того, значение x_{n+1} для нахождения решения исходной системы не требуется.

З а м е ч а н и е 0.2. Для системы (11) имеет место матричное представление

$$\left[I_2 + \begin{pmatrix} u_1 & u_0 \\ v_1 & v_0 \end{pmatrix} \begin{pmatrix} q_1 & 0 \\ 0 & -1 \end{pmatrix} \right] \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} = \begin{pmatrix} \sum_{k=1}^{n-1} u_k f_k & \sum_{k=1}^n v_k f_k \end{pmatrix}^T,$$

где I_2 – единичная матрица 2-го порядка.

ПРИМЕР. Решим систему уравнений

$$\begin{pmatrix} 2 & 1 & 0 & 0 & 2 \\ -2 & 3 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & -2 & 3 & 1 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} X_5 = \begin{pmatrix} 3 \\ -1 \\ 1 \\ 2 \\ 2 \end{pmatrix}.$$

Вычислим последовательности u и v , пользуясь формулами (7), (8):

$$\begin{aligned} u_5 &= 0, & u_4 &= 1, \\ u_3 &= -p_4 u_4 - q_5 u_5 = -3 \cdot 1 - 1 \cdot 0 = -3, \\ u_2 &= -p_3 u_3 - q_4 u_4 = -2 \cdot (-3) - (-2) \cdot 1 = 8, \\ u_1 &= -p_2 u_2 - q_3 u_3 = -3 \cdot 8 - 0 \cdot (-3) = -24, \\ u_0 &= -p_1 u_1 - q_2 u_2 = -2 \cdot (-24) - (-2) \cdot 8 = 64; \\ v_5 &= 1, & v_4 &= -p_5 = -1, \\ v_3 &= -p_4 v_4 - q_5 v_5 = -3 \cdot (-1) - 1 \cdot 1 = 2, \\ v_2 &= -p_3 v_3 - q_4 v_4 = -2 \cdot 2 - (-2) \cdot (-1) = -6, \\ v_1 &= -p_2 v_2 - q_3 v_3 = -3 \cdot (-6) - 0 \cdot 2 = 18, \\ v_0 &= -p_1 v_1 - q_2 v_2 = -2 \cdot 18 - (-2) \cdot (-6) = -48. \end{aligned}$$

Вычислим коэффициенты и правые части системы (11)

$$\begin{aligned} 1 + u_1 q_1 &= 1 + (-24) \cdot 2 = -47, & -u_0 &= -64, \\ v_1 q_1 &= 18 \cdot 2 = 36, & 1 - v_0 &= 1 - (-48) = 49, \end{aligned}$$

$$\sum_{k=1}^4 u_k f_k = -24 \cdot 3 + 8 \cdot (-1) - 3 \cdot 1 + 1 \cdot 2 = -81,$$

$$\sum_{k=1}^5 v_k f_k = 18 \cdot 3 - 6 \cdot (-1) + 2 \cdot 1 - 1 \cdot 2 + 1 \cdot 2 = 62.$$

Система (11) принимает вид

$$\begin{cases} -47x_0 - 64x_1 = -81, \\ 36x_0 + 49x_1 = 62. \end{cases}$$

Полученная система имеет единственное решение $x_0 = -1$, $x_1 = 2$. Из (2) следует, что $x_5 = -1$.

Остальные неизвестные вычисляем по формуле (12)

$$x_2 = f_1 - q_1 x_0 - p_1 x_1 = 3 - 2 \cdot (-1) - 2 \cdot 2 = 1,$$

$$x_3 = f_2 - q_2 x_1 - p_2 x_2 = -1 - (-2) \cdot 2 - 3 \cdot 1 = 0,$$

$$x_4 = f_3 - q_3 x_2 - p_3 x_3 = 1 - 0 \cdot 1 - 2 \cdot 0 = 1.$$

Ответ: $X_5 = (2, 1, 0, 1, -1)^T$.

Изложенный выше метод в случае единственности решения (случай 2) может быть реализован следующей программой

```

u1 := 0;   u := 1;
v1 := 1;   v := -p_n;
s1 := 0;   s2 := f_n;
for k := n-1 downto 1 do begin
    s1 := s1 + u * f_k;
    s2 := s2 + v * f_k;
    u2 := u1; u1 := u;
    v2 := v1; v1 := v;
    u := -u1 * p_k - u2 * q_{k+1};
    v := -v1 * p_k - v2 * q_{k+1}
end;
a11 := 1 + u1 * q_1; a12 := -u;
a21 := v1 * q_1;   a22 := 1 - v;
det  := a11 * a22 - a12 * a21;
x[0] := (s1 * a22 - s2 * a12) / det;
x[1] := (a11 * s2 - s1 * a21) / det;
for k := 1 to n-2 do
    x[k+1] := f_k - p_k * x[k] - q_k * x[k-1];
x[n] := x[0];

```

После завершения работы программы массив $x[1:n]$ будет содержать решение системы (1).

3°. Рассмотрим систему линейных уравнений (1) при $n \geq 5$ с матрицей A_n вида

$$A_n = \begin{pmatrix} p_1 & g_1 & 1 & 0 & 0 & \dots & 0 & h_1 & q_1 \\ q_2 & p_2 & g_2 & 1 & 0 & \dots & 0 & 0 & h_2 \\ h_3 & q_3 & p_3 & g_3 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & p_{n-2} & g_{n-2} & 1 \\ 1 & 0 & 0 & 0 & 0 & \dots & q_{n-1} & p_{n-1} & g_{n-1} \\ g_n & 1 & 0 & 0 & 0 & \dots & h_n & q_n & p_n \end{pmatrix},$$

которую будем называть пятидиагональной циклической матрицей.

Введём вспомогательные переменные x_{-1} , x_0 , x_{n+1} , x_{n+2} связанные с переменными системы (1) равенствами

$$x_j = x_{j+n}, \quad j \in -1 : 2. \quad (13)$$

Объединим систему (1) с уравнениями (13). Получим равносильную систему

$$\begin{cases} h_k x_{k-2} + q_k x_{k-1} + p_k x_k + g_k x_{k+1} + x_{k+2} = f_k, & k \in 1 : n, \\ x_j = x_{j+n}, & j \in -1 : 2. \end{cases} \quad (14)$$

Покажем, как схема Кленшоу позволяет свести решение системы (14) к решению системы уравнений четвёртого порядка.

Представим последние четыре уравнения системы (14) в виде

$$x_j = \sum_{k=2}^{n+j} a_k^j x_k, \quad j \in -1 : 2, \quad (15)$$

где $a_2^j = a_3^j = \dots = a_{n+j-1}^j = 0$, $a_{n+j}^j = 1$.

Определим последовательности $u^j = \{u_k^j\}_{k=0}^{n+j+2}$ при $j \in -1 : 2$ рекуррентной формулой

$$a_k^j = h_{k+2} u_{k+2}^j + q_{k+1} u_{k+1}^j + p_k u_k^j + g_{k-1} u_{k-1}^j + u_{k-2}^j, \quad k \in n+j : 2, \quad (16)$$

с начальными условиями

$$u_{n+j+2}^j = u_{n+j+1}^j = u_{n+j}^j = u_{n+j-1}^j = 0. \quad (17)$$

В (16) для единообразия формул введены коэффициенты $\{h_k\}_{k=n+1}^{n+4}$, $\{q_k\}_{k=n+1}^{n+3}$, p_{n+1} , p_{n+2} , g_{n+1} которые могут иметь любые значения из \mathbb{C} .

Такие последовательности существуют

$$u_{n+j+1}^j = u_{n+j}^j = u_{n+j-1}^j = 0, \quad u_{n+j-2}^j = 1; \quad (18)$$

$$u_{k-2}^j = -g_{k-1} u_{k-1}^j - p_k u_k^j - q_{k+1} u_{k+1}^j - h_{k+2} u_{k+2}^j, \quad k = n + j - 1 : 2. \quad (19)$$

Формулы (18) и (19) преобразуем к виду более удобному для вычислений

$$\left\{ \begin{array}{l} u_n^{-1} = 0, \quad u_{n-1}^{-1} = 0, \quad u_{n-2}^{-1} = 0, \quad u_{n-3}^{-1} = 1; \\ u_n^0 = 0, \quad u_{n-1}^0 = 0, \quad u_{n-2}^0 = 1, \quad u_{n-3}^0 = -g_{n-2}; \\ u_n^1 = 0, \quad u_{n-1}^1 = 1, \quad u_{n-2}^1 = -g_{n-1}, \quad u_{n-3}^1 = g_{n-2} g_{n-1} - p_{n-1}; \\ u_n^2 = 1, \quad u_{n-1}^2 = -g_n, \quad u_{n-2}^2 = g_{n-1} g_n - p_n; \quad u_{n-3}^2 = g_{n-2} (p_n - g_n g_{n-1}) + \\ \quad \quad \quad + g_n p_{n-1} - q_n; \end{array} \right. \quad (20)$$

$$u_k^j = -g_{k+1} u_{k+1}^j - p_{k+2} u_{k+2}^j - q_{k+3} u_{k+3}^j - h_{k+4} u_{k+4}^j, \quad k = n - 4 : 0. \quad (21)$$

Преобразуем формулы (15), используя (16):

$$\begin{aligned} x_j &= \sum_{k=2}^{n+j} (h_{k+2} u_{k+2}^j + q_{k+1} u_{k+1}^j + p_k u_k^j + g_{k-1} u_{k-1}^j + u_{k-2}^j) x_k = \\ &= \sum_{k=4}^{n+j+2} u_k^j h_k x_{k-2} + \sum_{k=3}^{n+j+1} u_k^j q_k x_{k-1} + \sum_{k=2}^{n+j} u_k^j p_k x_k + \\ &\quad + \sum_{k=1}^{n+j-1} u_k^j g_k x_{k+1} + \sum_{k=0}^{n+j-2} u_k^j x_{k+2}, \quad j \in -1 : 2. \end{aligned}$$

Выбор начальных условий (17) обеспечивает обнуление части слагаемых

$$\begin{aligned} x_j &= \sum_{k=1}^{n+j-2} u_k^j h_k x_{k-2} - \sum_{k=1}^3 u_k^j h_k x_{k-2} + \sum_{k=1}^{n+j-2} u_k^j q_k x_{k-1} - \sum_{k=1}^2 u_k^j q_k x_{k-1} + \\ &\quad + \sum_{k=1}^{n+j-2} u_k^j p_k x_k - u_1^j p_1 x_1 + \sum_{k=1}^{n+j-2} u_k^j g_k x_{k+1} + \sum_{k=1}^{n+j-2} u_k^j x_{k+2} + u_0^j x_2 = \\ &= -u_2^j h_2 x_0 - u_3^j h_3 x_1 - u_4^j h_4 x_2 - u_2^j q_2 x_1 - u_3^j q_3 x_2 - u_2^j p_2 x_2 + u_0^j x_2 + \\ &\quad + \sum_{k=1}^{n+j-2} u_k^j (h_k x_{k-2} + q_k x_{k-1} + p_k x_k + g_k x_{k+1} + x_{k+2}), \quad j \in -1 : 2. \end{aligned}$$

После простых преобразований система (14) приобретает вид

$$\left\{ \begin{array}{l} h_k x_{k-2} + q_k x_{k-1} + p_k x_k + g_k x_{k+1} + x_{k+2} = f_k, \quad k \in 1 : n, \\ x_j + u_1^j h_1 x_{-1} + (u_2^j h_2 + u_1^j q_1) x_0 + \\ + (h_3 u_3^j + q_2 u_2^j + u_1^j p_1) x_1 - u_0^j x_2 = \sum_{k=1}^{n+j-2} u_k^j f_k, \quad j \in -1 : 2. \end{array} \right. \quad (22)$$

Ясно, что система (22) равносильна системе (14).

Заметим, что последние четыре уравнения системы (22) составляют замкнутую подсистему относительно x_{-1}, x_0, x_1, x_2

$$\begin{aligned} x_j + u_1^j h_1 x_{-1} + (u_2^j h_2 + u_1^j q_1) x_0 + \\ + (h_3 u_3^j + q_2 u_2^j + u_1^j p_1) x_1 - u_0^j x_2 = \sum_{k=1}^{n+j-2} u_k^j f_k, \quad j \in -1 : 2. \end{aligned} \quad (23)$$

Неизвестные x_3, \dots, x_n однозначно вычисляются для каждого набора x_{-1}, x_0, x_1, x_2 найденного из (23). Для этого нужно воспользоваться первыми $n-4$ уравнениями системы (22) и двумя последними уравнениями системы (14) при $j = -1, 0$:

$$\begin{aligned} x_k = f_{k-2} - h_{k-2} x_{k-4} - q_{k-2} x_{k-3} - p_{k-2} x_{k-2} - g_{k-2} x_{k-1}, \quad k \in 3 : n-2; \\ x_{n-1} = x_{-1}, \quad x_n = x_0. \end{aligned}$$

Равносильность проделанных преобразований позволяет утверждать, что возможность решения системы (1), а также единственность решения системы (1), определяются свойствами системы (23). При решении системы (23) могут представиться три случая.

- 1) Система (23) несовместна. Следовательно исходная система (1) тоже несовместна.
- 2) Система (23) имеет единственное решение. В этом случае исходная система (1) тоже имеет единственное решение.
- 3) Система (23) имеет бесконечное множество решений. В этом случае исходная система (1) тоже имеет бесконечное множество решений.

Замечание 0.3. В матричном виде система (23) может быть переписана так

$$\begin{aligned} \left[I_4 + \begin{pmatrix} u_1^{-1} & u_2^{-1} & u_3^{-1} & u_0^{-1} \\ u_1^0 & u_2^0 & u_3^0 & u_0^0 \\ u_1^1 & u_2^1 & u_3^1 & u_0^1 \\ u_1^2 & u_2^2 & u_3^2 & u_0^2 \end{pmatrix} \begin{pmatrix} h_1 & q_1 & p_1 & 0 \\ 0 & h_2 & q_2 & 0 \\ 0 & 0 & h_3 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \right] \begin{pmatrix} x_{-1} \\ x_0 \\ x_1 \\ x_2 \end{pmatrix} = \\ = \begin{pmatrix} \sum_{k=1}^{n-3} u_k^{-1} f_k & \sum_{k=1}^{n-2} u_k^0 f_k & \sum_{k=1}^{n-1} u_k^1 f_k & \sum_{k=1}^n u_k^2 f_k \end{pmatrix}^T, \end{aligned}$$

где I_4 – единичная матрица 4–го порядка.

ЛИТЕРАТУРА

1. Малозёмов В. Н., Певный А. Б. *Программирование и математика* // Вестник молодых учёных. 2005. № 3. С. 3–14.

ВЕЩЕСТВЕННЫЕ ГАРМОНИЧЕСКИЕ ФРЕЙМЫ

А. М. Дурягин Н. А. Соловьёва

9 октября 2007 г.

В докладе используется определение вещественного гармонического фрейма, данное в работе [1]. Акцент делается на быстром вычислении фреймовых коэффициентов.

1°. Обозначим через \mathbb{R}_N линейное пространство вещественнозначных N -периодических сигналов $x = x(j)$, $j \in \mathbb{Z}$. Гармонические фреймы в \mathbb{R}_N вводятся отдельно для случаев нечётного и чётного N . Начнём с нечётного N , $N = 2n + 1$, $n \geq 1$.

При $m \geq N$ рассмотрим сигналы $\varphi_0, \varphi_1, \dots, \varphi_{m-1}$ из \mathbb{R}_N с отсчётами

$$\begin{aligned}\varphi_k(0) &= \frac{1}{\sqrt{N}}; & \varphi_k(j) &= \sqrt{\frac{2}{N}} \cos \frac{2kj\pi}{m}, & j \in 1:n; \\ \varphi_k(n+j) &= \sqrt{\frac{2}{N}} \sin \frac{2kj\pi}{m}, & j \in 1:n.\end{aligned}$$

Нетрудно проверить, что $\|\varphi_k\| = 1$ при всех $k \in 0:m-1$. Отметим также, что

$$\varphi_k(j) + i\varphi_k(n+j) = \sqrt{\frac{2}{N}} \omega_m^{kj}, \quad j \in 1:n, \quad (1)$$

где $\omega_m = \exp(2\pi i/m)$.

ПРЕДЛОЖЕНИЕ 1. Для всех $x \in \mathbb{R}_N$ при $N = 2n + 1$ справедливо разложение

$$x(j) = \frac{N}{m} \sum_{k=0}^{m-1} \langle x, \varphi_k \rangle \varphi_k(j), \quad j \in \mathbb{Z}. \quad (2)$$

Доказательство. Вычислим коэффициенты $a_k = \langle x, \varphi_k \rangle$. Имеем

$$a_k = \frac{1}{\sqrt{N}} x(0) + \sqrt{\frac{2}{N}} \sum_{j=1}^n \left[x(j) \cos \frac{2kj\pi}{m} + x(n+j) \sin \frac{2kj\pi}{m} \right] =$$

$$\begin{aligned}
&= \frac{1}{\sqrt{N}} \left\{ x(0) + \frac{\sqrt{2}}{2} \sum_{j=1}^n \left[x(j) (\omega_m^{kj} + \omega_m^{-kj}) - i x(n+j) (\omega_m^{kj} - \omega_m^{-kj}) \right] \right\} = \\
&= \sqrt{\frac{2}{N}} \left\{ \frac{\sqrt{2}}{2} x(0) + \frac{1}{2} \sum_{j=1}^n \left[(x(j) - i x(n+j)) \omega_m^{kj} + (x(j) + i x(n+j)) \omega_m^{-kj} \right] \right\}.
\end{aligned} \tag{3}$$

Введём сигнал $y_1 \in \mathbb{C}_m$ с отсчётами

$$y_1(j) = \begin{cases} x(j) + i x(n+j) & \text{при } j \in 1 : n, \\ 0 & \text{при } j = 0 \text{ и } j \in n+1 : m-1. \end{cases}$$

Обозначим $Y_1 = \mathcal{F}_m(y_1)$. Тогда равенство (3) можно переписать так:

$$\begin{aligned}
a_k &= \sqrt{\frac{2}{N}} \left\{ \frac{\sqrt{2}}{2} x(0) + \frac{1}{2} (\bar{Y}_1(k) + Y_1(k)) \right\} = \\
&= \sqrt{\frac{2}{N}} \left\{ \frac{\sqrt{2}}{2} x(0) + \operatorname{Re} Y_1(k) \right\}, \quad k \in 0 : m-1.
\end{aligned} \tag{4}$$

Обратимся к формуле (2). Её правую часть обозначим $S(j)$. Согласно (4)

$$S(j) = \frac{\sqrt{N}}{m} x(0) \sum_{k=0}^{m-1} \varphi_k(j) + \frac{\sqrt{2N}}{m} \sum_{k=0}^{m-1} [\operatorname{Re} Y_1(k)] \varphi_k(j), \quad j \in 0 : N-1. \tag{5}$$

Нетрудно проверить, что $S(0) = x(0)$. Это следует из равенства

$$\sum_{k=0}^{m-1} \varphi_k(0) = \frac{m}{\sqrt{N}}$$

и формулы обращения для ДПФ, согласно которой

$$\frac{1}{m} \sum_{k=0}^{m-1} Y_1(k) = y_1(0) = 0.$$

Теперь покажем, что

$$\sum_{k=0}^{m-1} \varphi_k(j) = 0 \quad \text{при } j \in 1 : N-1. \tag{6}$$

Согласно (1) при $j \in 1 : n$ имеем

$$\sum_{k=0}^{m-1} [\varphi_k(j) + i \varphi_k(n+j)] = \sqrt{\frac{2}{N}} \sum_{k=0}^{m-1} \omega_m^{kj} = m \sqrt{\frac{2}{N}} \delta_m(j) = 0.$$

Это гарантирует справедливость равенства (6).

При $j \in 1 : N - 1$ формула (5) приобретает более простой вид

$$S(j) = \frac{\sqrt{2N}}{m} \sum_{k=0}^{m-1} [\operatorname{Re} Y_1(k)] \varphi_k(j).$$

Отметим, что при $j \in 1 : n$

$$S(j) + i S(n + j) = \frac{1}{m} \sum_{k=0}^{m-1} [Y_1(k) + \overline{Y_1(k)}] \omega_m^{kj}.$$

Воспользуемся формулой обращения для ДПФ. Получим

$$S(j) + i S(n + j) = y_1(j) + \overline{y_1(-j)}, \quad j \in 1 : n.$$

Поскольку $y_1(-j) = y_1(m - j)$ и $m - 1 \geq m - j \geq m - n \geq n + 1$, то $y_1(-j) = 0$. Значит,

$$S(j) + i S(n + j) = y_1(j) = x(j) + i x(n + j), \quad j \in 1 : n.$$

Отсюда следует, что $S(j) = x(j)$ при $j \in 1 : N - 1$. Предложение доказано. \square

2°. Перейдём к случаю чётного N , $N = 2n$, $n \geq 1$. При $m \geq N$ в пространстве \mathbb{R}_N рассмотрим сигналы $\psi_0, \psi_1, \dots, \psi_{m-1}$ с отсчётами

$$\begin{aligned} \psi_k(j) &= \sqrt{\frac{2}{N}} \cos \frac{(2j+1)k\pi}{m}, \quad j \in 0 : n-1; \\ \psi_k(n+j) &= \sqrt{\frac{2}{N}} \sin \frac{(2j+1)k\pi}{m}, \quad j \in 0 : n-1. \end{aligned}$$

Нетрудно проверить, что $\|\psi_k\| = 1$ при всех $k \in 0 : m-1$. Отметим также, что

$$\psi_k(j) + i \psi_k(n+j) = \sqrt{\frac{2}{N}} \omega_{2m}^{(2j+1)k} = \sqrt{\frac{2}{N}} \omega_{2m}^k \omega_m^{kj}, \quad j \in 0 : n-1. \quad (7)$$

ПРЕДЛОЖЕНИЕ 2. Для всех $x \in \mathbb{R}_N$ при $N = 2n$ справедливо разложение

$$x(j) = \frac{N}{m} \sum_{k=0}^{m-1} \langle x, \psi_k \rangle \psi_k(j), \quad j \in \mathbb{Z}. \quad (8)$$

Доказательство. Вычислим коэффициенты $a_k = \langle x, \psi_k \rangle$. Имеем

$$\begin{aligned} a_k &= \sqrt{\frac{2}{N}} \sum_{j=0}^{n-1} \left[x(j) \cos \frac{(2j+1)k\pi}{m} + x(n+j) \sin \frac{(2j+1)k\pi}{m} \right] = \\ &= \frac{1}{\sqrt{2N}} \sum_{j=0}^{n-1} \left[x(j) (\omega_{2m}^{(2j+1)k} + \omega_{2m}^{-(2j+1)k}) - i x(n+j) (\omega_{2m}^{(2j+1)k} - \omega_{2m}^{-(2j+1)k}) \right] = \\ &= \frac{\omega_{2m}^k}{\sqrt{2N}} \sum_{j=0}^{n-1} [x(j) - i x(n+j)] \omega_m^{kj} + \frac{\omega_{2m}^{-k}}{\sqrt{2N}} \sum_{j=0}^{n-1} [x(j) + i x(n+j)] \omega_m^{-kj}. \end{aligned} \quad (9)$$

Введём сигнал $y_2 \in \mathbb{C}_m$ с отсчётами

$$y_2(j) = \begin{cases} x(j) + i x(n+j), & \text{при } j \in 0 : n-1, \\ 0, & \text{при } j \in n : m-1. \end{cases}$$

Обозначим $Y_2 = \mathcal{F}_m(y_2)$. Тогда равенство (9) можно переписать так:

$$\begin{aligned} a_k &= \frac{\omega_{2m}^k}{\sqrt{2N}} \overline{Y_2(k)} + \frac{\omega_{2m}^{-k}}{\sqrt{2N}} Y_2(k) = \\ &= \sqrt{\frac{2}{N}} \operatorname{Re} \left\{ \omega_{2m}^{-k} Y_2(k) \right\}, \quad k \in 0 : m-1. \end{aligned} \quad (10)$$

Обратимся к формуле (8). Её правую часть обозначим $S(j)$. Согласно (10)

$$S(j) = \frac{\sqrt{2N}}{m} \sum_{k=0}^{m-1} \operatorname{Re} \left\{ \omega_{2m}^{-k} Y_2(k) \right\} \psi_k(j), \quad j \in 0 : N-1.$$

Дальнейшие действия связаны с соотношением (7). При $j \in 0 : n-1$ получим

$$\begin{aligned} S(j) + i S(n+j) &= \frac{2}{m} \sum_{k=0}^{m-1} \operatorname{Re} \left\{ \omega_{2m}^{-k} Y_2(k) \right\} \omega_{2m}^k \omega_m^{kj} = \\ &= \frac{1}{m} \sum_{k=0}^{m-1} [Y_2(k) + \omega_m^k \overline{Y_2(k)}] \omega_m^{kj} = y_2(j) + \overline{y_2(-j-1)}. \end{aligned}$$

Поскольку $y_2(-j-1) = y_2(m-j-1)$ и $m-1 \geq m-j-1 \geq m-n \geq n$, то $y_2(-j-1) = 0$. Значит,

$$S(j) + i S(n+j) = y_2(j) = x(j) + i x(n+j), \quad j \in 0 : n-1.$$

Отсюда следует, что $S(j) = x(j)$ при $j \in 0 : N-1$. Предложение доказано. \square

3°. Разложения (2) и (8) характеризуют системы сигналов $\{\varphi_0, \varphi_1, \dots, \varphi_{m-1}\}$ и $\{\psi_0, \psi_1, \dots, \psi_{m-1}\}$ как жёсткие фреймы в \mathbb{R}_N при нечётном и чётном N соответственно (см., например, [2]). Эти фреймы называются *гармоническими*. Формулы (4) и (10) обеспечивают быстрое вычисление фреймовых коэффициентов.

ЛИТЕРАТУРА

1. Goyal V. K., Kovačević J., Kelner J. A. *Quantized frame expansions with erasures* // Appl. and Comput. Harmonic Analysis. 2001. V. 10. P. 203–233.
2. Малозёмов В. Н., Певный А. Б. *Системы Мерседес-Бенц и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 28 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0228>).

СМЕШИВАЮЩИЕ ФУНКЦИИ

Н. В. Чашников

27 октября 2007 г.

Данная работа примыкает к [1].

1°. Рассмотрим простейшую задачу геометрического моделирования: соединить кривой две данные точки $a_1, a_2 \in \mathbb{R}^3$. Очевидным решением этой задачи является отрезок с концами a_1 и a_2 , определяемый вектор-функцией

$$r(t) = (1 - t) a_1 + t a_2, \quad t \in [0, 1].$$

Вместо коэффициентов $1 - t$ и t можно использовать любые функции $H_1(t)$ и $H_2(t)$, удовлетворяющие условиям

$$\begin{aligned} H_1(0) &= 1, & H_1(1) &= 0, \\ H_2(0) &= 0, & H_2(1) &= 1. \end{aligned} \tag{1}$$

Функции H_1 и H_2 называют *смешивающими функциями*.

Используя смешивающие функции, можно решить следующую задачу: построить непрерывную кривую, проходящую через точки $a_0, a_1, \dots, a_n \in \mathbb{R}^3$. Для этого определим вектор-функцию $r: [0, n] \rightarrow \mathbb{R}^3$:

$$r(u) = H_1(u - k) a_k + H_2(u - k) a_{k+1}, \quad u \in [k, k + 1], \quad k \in 0 : n - 1.$$

Перейдём теперь к рассмотрению более сложной задачи: построить кривую по заданным конечным точкам $a_1, a_2 \in \mathbb{R}^3$ и касательным векторам в этих точках $b_1, b_2 \in \mathbb{R}^3$. Решение этой задачи можно получить с использованием четырёх смешивающих функций, удовлетворяющих условиям

$$\begin{aligned} H_1(0) &= 1, & H_1'(0) &= 0, & H_1'(1) &= 0, & H_1(1) &= 0; \\ H_2(0) &= 0, & H_2'(0) &= 1, & H_2'(1) &= 0, & H_2(1) &= 0; \\ H_3(0) &= 0, & H_3'(0) &= 0, & H_3'(1) &= 1, & H_3(1) &= 0; \\ H_4(0) &= 0, & H_4'(0) &= 0, & H_4'(1) &= 0, & H_4(1) &= 1. \end{aligned} \tag{2}$$

Тогда для вектор-функции

$$r(t) = H_1(t) a_1 + H_2(t) b_1 + H_3(t) b_2 + H_4(t) a_2, \quad t \in [0, 1], \quad (3)$$

выполнены равенства

$$r(0) = a_1, \quad r'(0) = b_1, \quad r'(1) = b_2, \quad r(1) = a_2,$$

то есть вектор-функция $r(t)$ задаёт кривую в \mathbb{R}^3 с концами a_1 и a_2 и касательными векторами на концах b_1 и b_2 .

Смешивающие функции, удовлетворяющие условиям (2), можно также использовать для решения следующей задачи: построить гладкую кривую, проходящую через точки $a_0, a_1, \dots, a_n \in \mathbb{R}^3$, для которой векторы касательных в точках a_j равны b_j , $j \in 0 : n$. Решением будет кривая, задаваемая функцией $r: [0, n] \rightarrow \mathbb{R}^3$:

$$r(u) = H_1(u - k) a_k + H_2(u - k) b_k + H_3(u - k) b_{k+1} + H_4(u - k) a_{k+1}, \\ u \in [k, k + 1], \quad k \in 0 : n - 1.$$

Кроме того, смешивающие функции, удовлетворяющие условиям (2), можно использовать для построения параметрической поверхности Кунса (см. [2]).

2°. Введём общее определение. Пусть $T \subset C([0, 1])$ — линейное пространство, $L_1, \dots, L_n: T \rightarrow \mathbb{R}$ — линейные функционалы. Функции $H_1, \dots, H_n \in T$, удовлетворяющие условиям

$$L_i(H_j) = \delta_{ij}, \quad i, j \in 1 : n, \quad (4)$$

будем называть смешивающими функциями для функционалов L_1, \dots, L_n .

Рассмотрим интересующие нас частные случаи.

1) $n = 2$, $T = C([0, 1])$, $L_1(f) = f(0)$, $L_2(f) = f(1)$. В этом случае условия (4) принимают вид (1).

2) $n = 4$, $T = C^1([0, 1])$,

$$L_1(f) = f(0), \quad L_2(f) = f'(0), \quad L_3(f) = f'(1), \quad L_4(f) = f(1).$$

В этом случае условия (4) принимают вид (2).

3) $n = 6$, $T = C^2([0, 1])$,

$$L_1(f) = f(0), \quad L_2(f) = f'(0), \quad L_3(f) = f''(0), \\ L_4(f) = f''(1), \quad L_5(f) = f'(1), \quad L_6(f) = f(1).$$

Смешивающие функции H_j , удовлетворяющие условиям (4), можно использовать для построения кривой по заданным концам и производным первого и второго порядка в конечных точках. Кроме того, с их помощью можно построить кривую класса C^2 , проходящую через заданные точки и имеющую в них заданные первые и вторые производные.

В дальнейшем мы будем ссылаться на эти частные случаи как на случаи $n = 2$, $n = 4$ и $n = 6$, полагая, что пространство T и функционалы L_i определяются для данного n так, как описано выше.

Пусть заданы функции $\gamma_1, \dots, \gamma_n \in T$. Будем искать смешивающие функции в виде

$$H_j(t) = \sum_{k=1}^n \alpha_{jk} \gamma_k(t), \quad \alpha_{jk} \in \mathbb{R}, \quad j \in 1 : n. \quad (5)$$

Если учесть линейность функционалов L_i , то равенство (4) примет вид

$$\sum_{k=1}^n \alpha_{jk} L_i(\gamma_k) = \delta_{ij}. \quad (6)$$

Введём матрицы

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix}, \quad G = \begin{pmatrix} L_1(\gamma_1) & L_2(\gamma_1) & \cdots & L_n(\gamma_1) \\ L_1(\gamma_2) & L_2(\gamma_2) & \cdots & L_n(\gamma_2) \\ \vdots & \vdots & \ddots & \vdots \\ L_1(\gamma_n) & L_2(\gamma_n) & \cdots & L_n(\gamma_n) \end{pmatrix}.$$

Тогда равенство (6) можно переписать в виде $AG = E_n$, то есть $A = G^{-1}$.

Таким образом, если для заданных функций γ_k матрица G обратима, то можно взять коэффициенты α_{jk} из матрицы G^{-1} и построить смешивающие функции H_j по формуле (5).

3°. Полиномиальные смешивающие функции.

Пусть $\gamma_k(t) = t^{k-1}$, $k \in 1 : n$. Смешивающие функции H_j будут полиномами степени не выше $n - 1$.

Случай $n = 2$. Имеем $\gamma_1(t) = 1$, $\gamma_2(t) = t$,

$$G = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad G^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Значит, $H_1(t) = 1 - t$, $H_2(t) = t$.

Случай $n = 4$. Имеем $\gamma_1(t) = 1$, $\gamma_2(t) = t$, $\gamma_3(t) = t^2$, $\gamma_4(t) = t^3$,

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 3 & 1 \end{pmatrix}, \quad G^{-1} = \begin{pmatrix} 1 & 0 & -3 & 2 \\ 0 & 1 & -2 & 1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 3 & -2 \end{pmatrix}.$$

Значит,

$$\begin{aligned} H_1(t) &= 2t^3 - 3t^2 + 1, & H_3(t) &= t^3 - t^2, \\ H_2(t) &= t^3 - 2t^2 + t, & H_4(t) &= -2t^3 + 3t^2. \end{aligned}$$

Полученные H_j являются кубическими полиномами Эрмита. Их графики изображены на рис. 1.

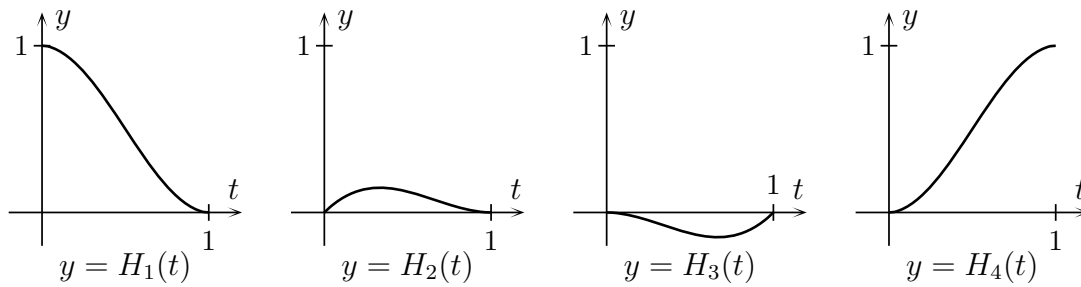


Рис. 1. Кубические полиномы Эрмита

Случай $n = 6$. Имеем, $\gamma_1(t) = 1$, $\gamma_2(t) = t$, $\gamma_3(t) = t^2$, $\gamma_4(t) = t^3$, $\gamma_5(t) = t^4$, $\gamma_6(t) = t^5$,

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 2 & 2 & 1 \\ 0 & 0 & 0 & 6 & 3 & 1 \\ 0 & 0 & 0 & 12 & 4 & 1 \\ 0 & 0 & 0 & 20 & 5 & 1 \end{pmatrix}, \quad G^{-1} = \begin{pmatrix} 1 & 0 & 0 & -10 & 15 & -6 \\ 0 & 1 & 0 & -6 & 8 & -3 \\ 0 & 0 & \frac{1}{2} & -\frac{3}{2} & \frac{3}{2} & \frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{2} & -1 & \frac{1}{2} \\ 0 & 0 & 0 & -4 & 7 & -3 \\ 0 & 0 & 0 & 10 & -15 & 6 \end{pmatrix}.$$

Значит,

$$\begin{aligned} H_1(t) &= -6t^5 + 15t^4 - 10t^3 + 1, \\ H_2(t) &= -3t^5 + 8t^4 - 6t^3 + t, \\ H_3(t) &= (-t^5 + 3t^4 - 3t^3 + t^2)/2, \\ H_4(t) &= (t^5 - 2t^4 + t^3)/2, \\ H_5(t) &= -3t^5 + 7t^4 - 4t^3 + 1, \\ H_6(t) &= 6t^5 - 15t^4 + 10t^3. \end{aligned}$$

В этом случае H_j — полиномы Эрмита пятой степени. Их графики изображены на рис. 2.

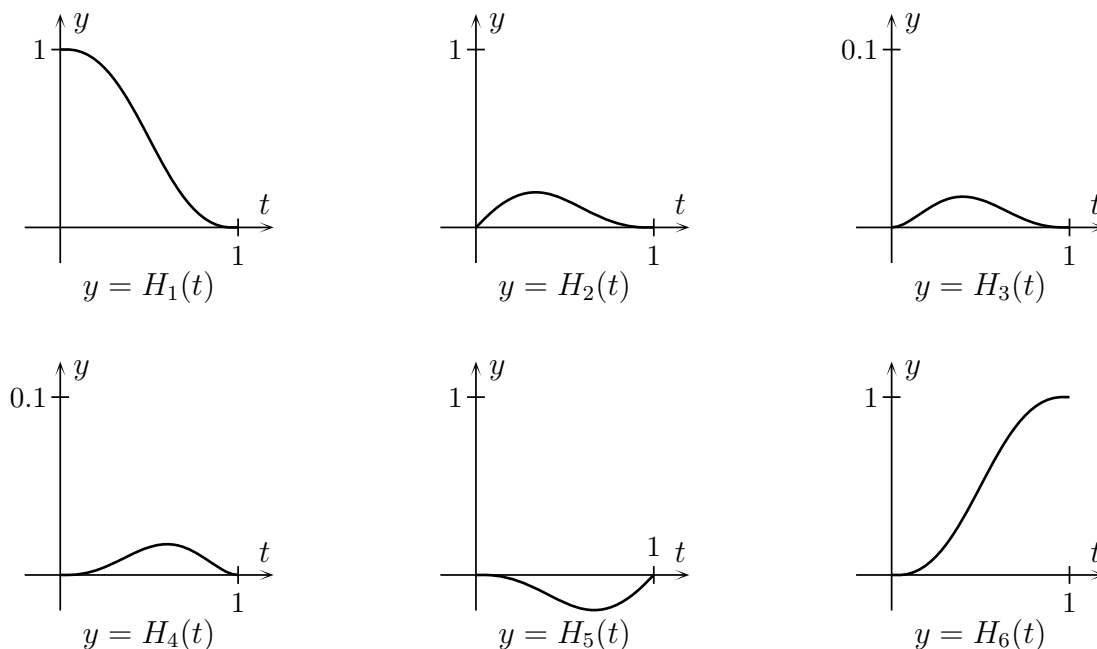


Рис. 2. Полиномы Эрмита пятой степени

4°. Экспоненциальные смешивающие функции.

Пусть функции $\gamma_k(t)$ выбираются из функций $t^i e^{jq t}$, где q — ненулевая константа, i и j — целые неотрицательные числа. Смешивающие функции, построенные для данных γ_k , будем называть экспоненциальными.

Случай $n = 2$. Возьмём $\gamma_1(t) = 1$, $\gamma_2(t) = e^{qt}$. Имеем

$$G = \begin{pmatrix} 1 & 1 \\ 1 & e^q \end{pmatrix}, \quad G^{-1} = \frac{1}{e^q - 1} \begin{pmatrix} e^q & -1 \\ -1 & 1 \end{pmatrix}.$$

Отсюда следует, что

$$H_1(t) = \frac{e^q - e^{qt}}{e^q - 1}, \quad H_2(t) = \frac{e^{qt} - 1}{e^q - 1}.$$

Случай $n = 4$. Возьмём $\gamma_1(t) = 1$, $\gamma_2(t) = t$, $\gamma_3(t) = e^{qt}$, $\gamma_4(t) = te^{qt}$. Имеем

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & q & qe^q & e^q \\ 0 & 1 & e^q(1+q) & e^q \end{pmatrix}.$$

Графики функций $H_j(t)$ при $q = 3$ показаны на рис. 3, а при $q = 10$ — на рис. 4.

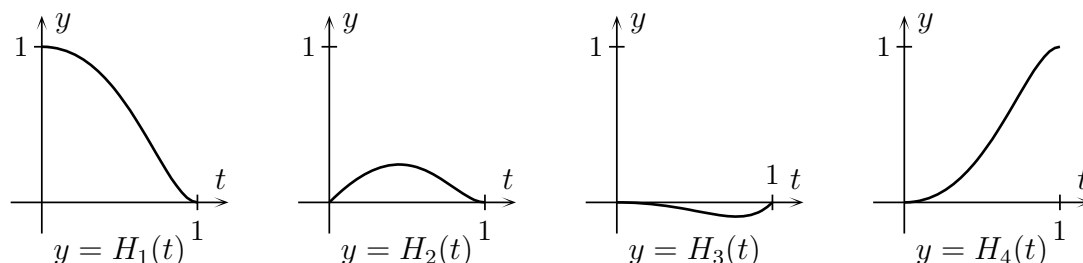


Рис. 3. Экспоненциальные смешивающие функции, $n = 4$, $q = 3$

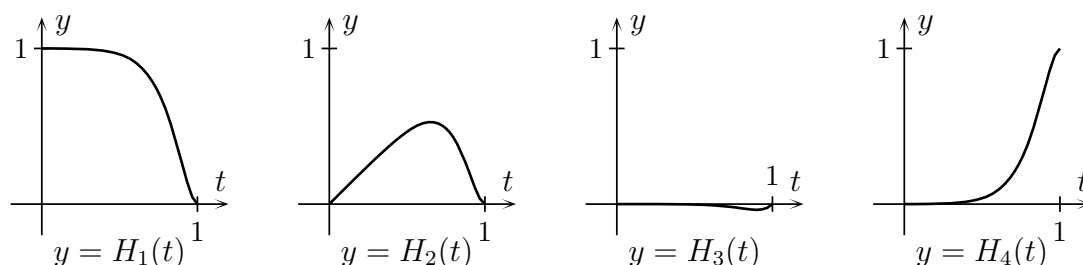


Рис. 4. Экспоненциальные смешивающие функции, $n = 4$, $q = 10$

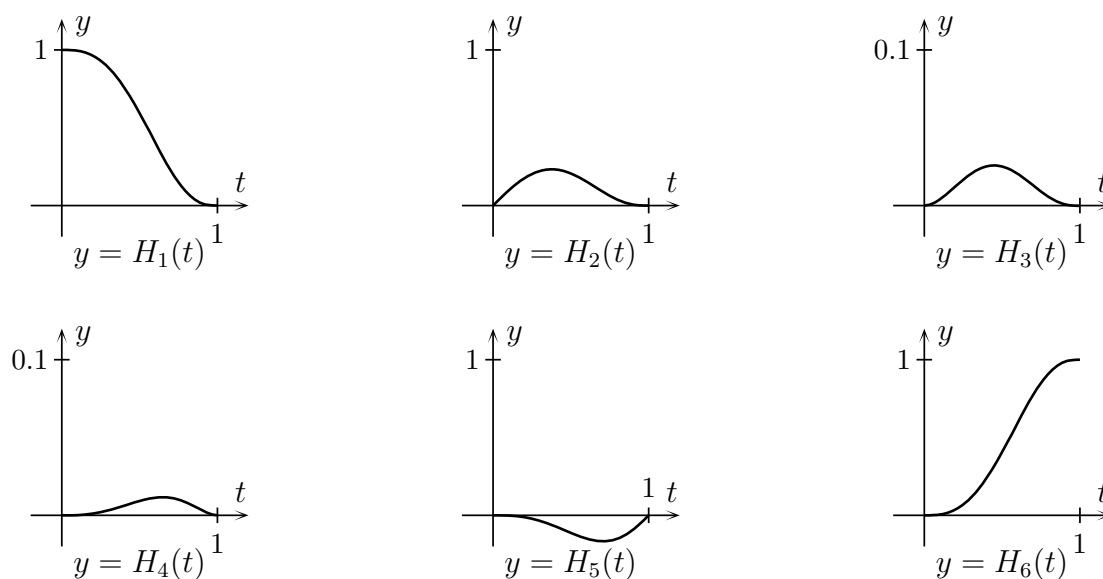
Случай $n = 6$. Возьмём $\gamma_1(t) = 1$, $\gamma_2(t) = t$, $\gamma_3(t) = t^2$, $\gamma_4(t) = e^{qt}$, $\gamma_5(t) = te^{qt}$, $\gamma_6(t) = t^2e^{qt}$. Графики функций $H_j(t)$ при $q = 2$ показаны на рис. 5.

5°. Дробно-рациональные смешивающие функции.

Пусть $\gamma_k(t) = \frac{1}{1 - c_k t}$, где c_1, \dots, c_n — различные вещественные числа, $c_k < 1$ при $k \in 1 : n$. Смешивающие функции будут иметь вид дробно-рациональных функций от t .

Случай $n = 2$. Имеем

$$G = \begin{pmatrix} 1 & \frac{1}{1-c_1} \\ 1 & \frac{1}{1-c_2} \end{pmatrix}, \quad G^{-1} = \frac{1}{c_1 - c_2} \begin{pmatrix} c_1 - 1 & 1 - c_2 \\ (c_1 - 1)(c_2 - 1) & (c_1 - 1)(1 - c_2) \end{pmatrix}.$$

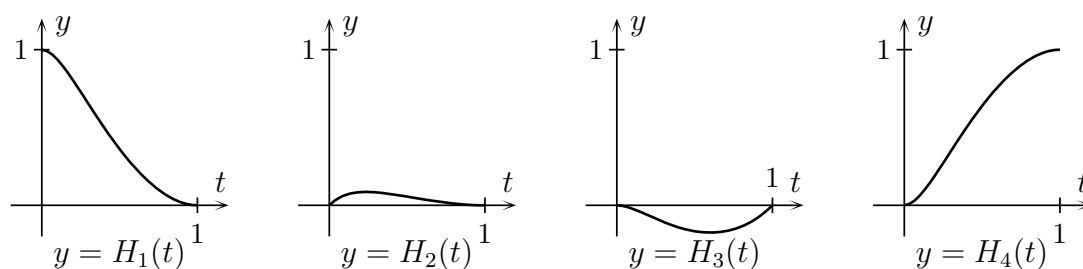
Рис. 5. Экспоненциальные смешивающие функции, $n = 6$, $q = 2$

Значит,

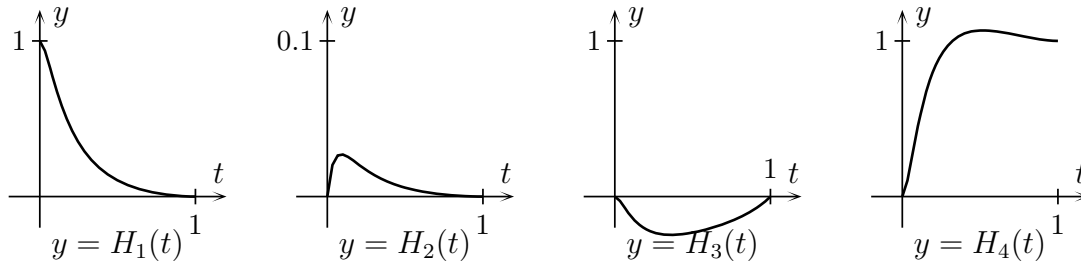
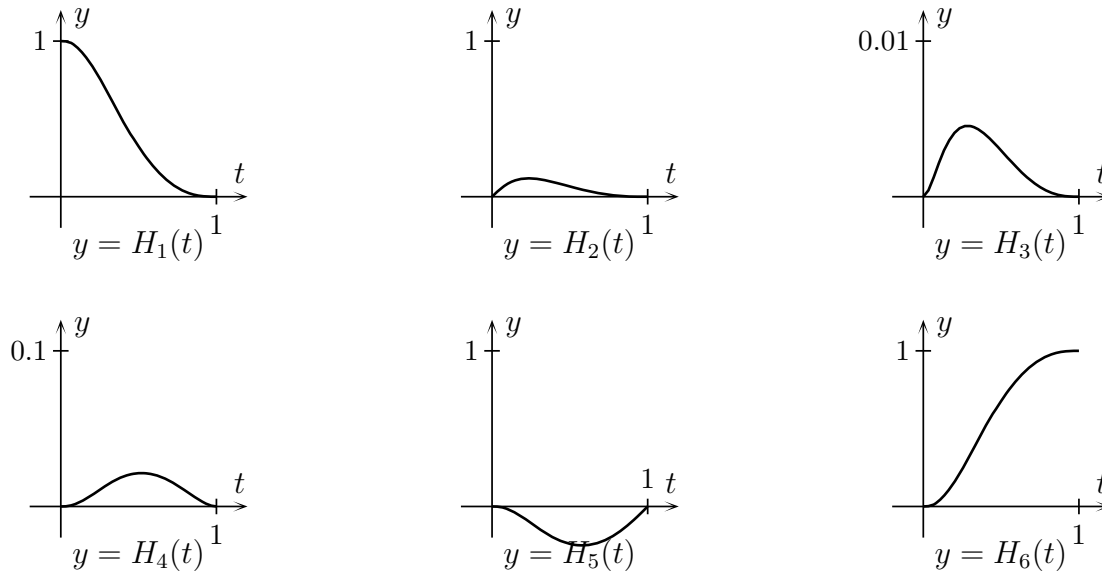
$$H_1(t) = \frac{c_1 - 1}{c_1 - c_2} \frac{1}{1 - c_1 t} + \frac{1 - c_2}{c_1 - c_2} \frac{1}{1 - c_2 t},$$

$$H_2(t) = \frac{1 - c_2}{c_1 - c_2} \frac{1 - c_1}{1 - c_1 t} + \frac{c_1 - 1}{c_1 - c_2} \frac{1 - c_2}{1 - c_2 t}.$$

Случай $n = 4$. Графики смешивающих функций $H_j(t)$ для набора параметров $c = (-2, -1, 0, 0.5)$ показаны на рис. 6, а для набора параметров $c = (-8, -5, -2, 0.75)$ — на рис. 7.

Рис. 6. Дробно-рациональные смешивающие функции, $c = (-2, -1, 0, 0.5)$

Случай $n = 6$. Графики смешивающих функций $H_j(t)$ для набора параметров $c = (-4, -2, -1, 0, 0.2, 0.7)$ показаны на рис. 8.

Рис. 7. Дробно-рациональные смешивающие функции, $c = (-8, -5, -2, 0.75)$ Рис. 8. Дробно-рациональные смешивающие функции, $n = 6$

6°. Логарифмические смешивающие функции.

Пусть $\gamma_1(t) = 1$, $\gamma_k(t) = \ln(1 + c_{k-1}t)$ при $k \in 2 : n$, где c_1, \dots, c_{n-1} — различные вещественные числа, $c_j > -1$, $c_j \neq 0$ для $j \in 1 : n-1$. Смешивающие функции, построенные для таких γ_k , будем называть логарифмическими.

Случай $n = 2$. Имеем $\gamma_1(t) = 1$, $\gamma_2(t) = \ln(1 + c_1t)$,

$$G = \begin{pmatrix} 1 & 1 \\ 0 & \ln(1 + c_2) \end{pmatrix}, \quad G^{-1} = \frac{1}{\ln(1 + c_2)} \begin{pmatrix} \ln(1 + c_2) & -1 \\ 0 & 1 \end{pmatrix}.$$

Значит,

$$H_1(t) = 1 - \frac{\ln(1 + c_2t)}{\ln(1 + c_2)}, \quad H_2(t) = \frac{\ln(1 + c_2t)}{\ln(1 + c_2)}.$$

Случай $n = 4$. Графики смешивающих функций $H_j(t)$ для набора параметров $c = (1, 2, 3)$ показаны на рис. 9.

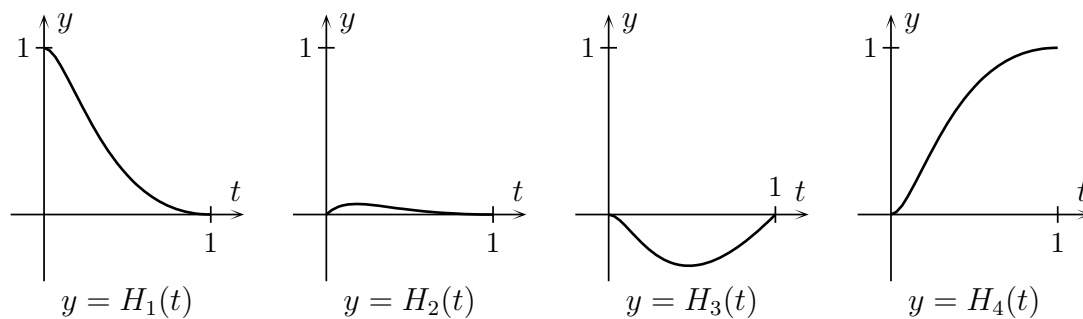


Рис. 9. Логарифмические смешивающие функции, $n = 4$

Случай $n = 6$. Графики смешивающих функций $H_j(t)$ для набора параметров $c = (1, 3, 5, 8, 10)$ показаны на рис. 10.

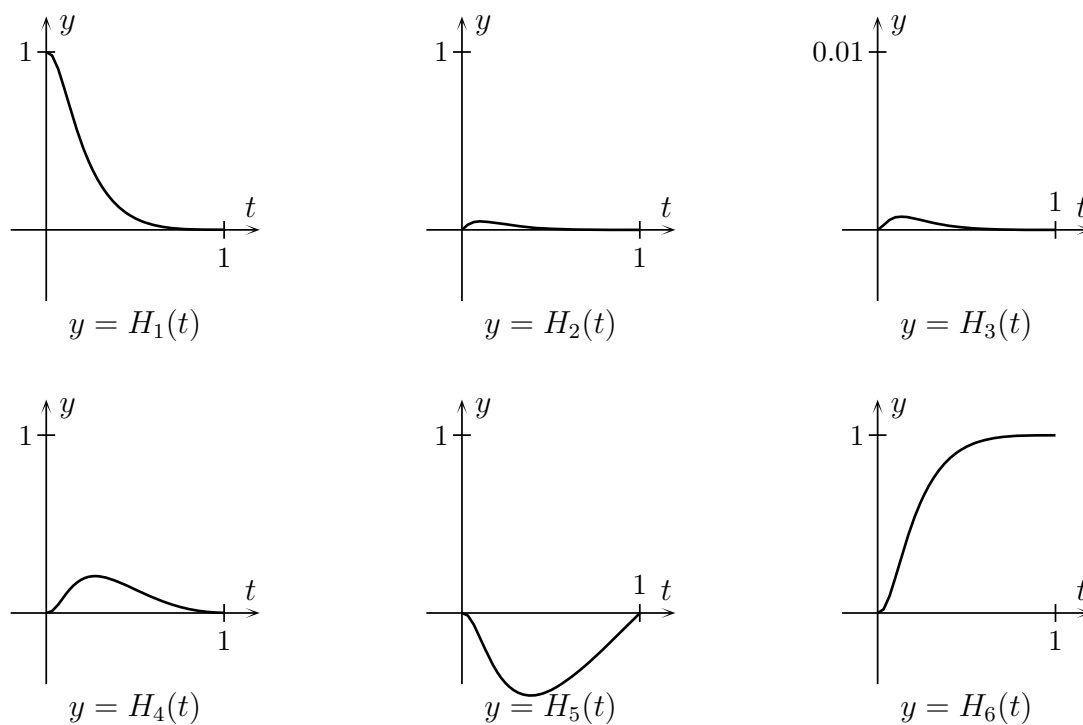


Рис. 10. Логарифмические смешивающие функции, $n = 6$

7°. Тригонометрические смешивающие функции.

Случай $n = 4$. Пусть $\gamma_1(t) = 1$, $\gamma_2(t) = \sin \alpha t$, $\gamma_3(t) = \cos \alpha t$, $\gamma_4(t) = \sin^2 \alpha t$, где $\alpha \in (0, \pi)$. В [3] были найдены смешивающие функции, являющиеся линейными комбинациями функций $\gamma_k(t)$:

$$H_1(t) = \frac{(\cos \alpha - \cos \alpha t)^2}{(1 - \cos \alpha)^2},$$

$$H_2(t) = \frac{\sin \alpha t - \sin \alpha}{\alpha} + \frac{(\cos \alpha - \cos \alpha t)(\cos^2 \alpha - \cos \alpha t)}{\alpha \sin \alpha (1 - \cos \alpha)},$$

$$H_3(t) = \frac{(1 - \cos \alpha t)(\cos \alpha - \cos \alpha t)}{\alpha \sin \alpha (1 - \cos \alpha)},$$

$$H_4(t) = 1 - \frac{(\cos \alpha - \cos \alpha t)^2}{(1 - \cos \alpha)^2}.$$

На рис. 11 показаны графики функций $H_j(t)$ при $\alpha = \pi/2$.

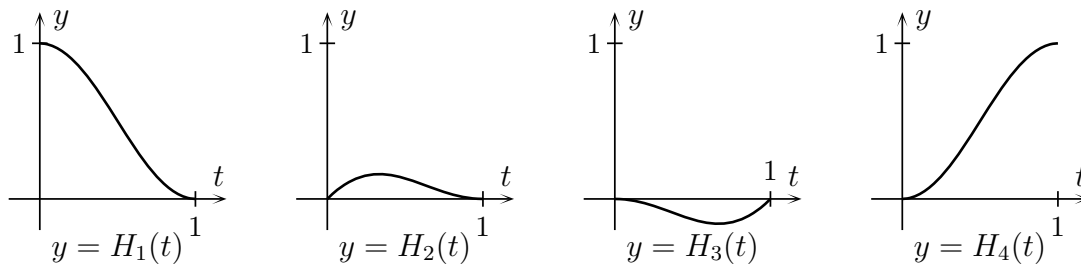


Рис. 11. Тригонометрические смешивающие функции, $n = 4$, $\alpha = \pi/2$

ПРИМЕР 1. Построим по формуле (3) кривую $r(t)$, удовлетворяющую условиям

$$r(0) = 0.7, \quad r'(0) = 1, \quad r'(1) = 2, \quad r(1) = 0.2,$$

используя различные наборы смешивающих функций. На рис. 12 показаны полученные кривые:

$r_1(t)$ — для полиномиальных смешивающих функций,

$r_2(t)$ — для экспоненциальных смешивающих функций с параметром $q = 3$,

$r_3(t)$ — для экспоненциальных смешивающих функций с параметром $q = 10$,

$r_4(t)$ — для дробно-рациональных смешивающих функций с набором параметров $c = (-2, -1, 0, 0.5)$,

$r_5(t)$ — для логарифмических смешивающих функций с набором параметров $c = (1, 2, 3)$,

$r_6(t)$ — для тригонометрических смешивающих функций.

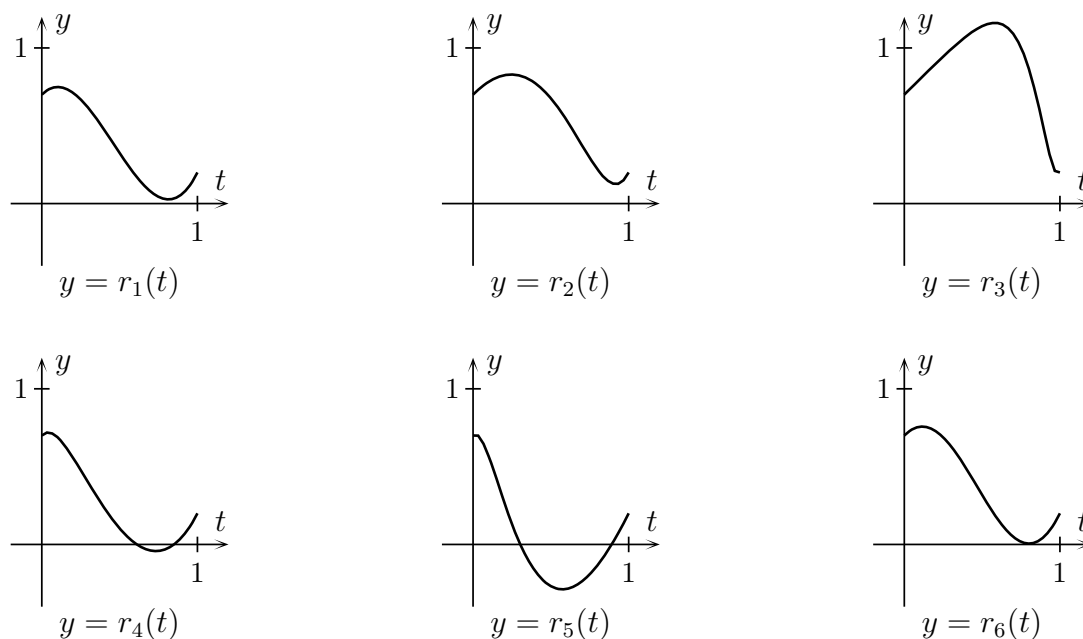


Рис. 12. Построение кривой при помощи различных смешивающих функций

ПРИМЕР 2. Построим параметрическую поверхность Кунса $s(u, v)$ по граничным условиям

$$\begin{aligned} f_1(v) &= \frac{1}{3} (v - 1) (4v - 3) (v + 1/4), & f_2(v) &= \frac{1}{12} (5 - 10v), \\ f_3(v) &= \frac{1}{12} (5 - 10v), & f_4(v) &= \frac{1}{3} v (1 - 4v) (5/4 - v), \\ g_1(v) &= \frac{1}{3} (u - 1) (4u - 3) (u + 1/4), & g_2(u) &= \frac{1}{12} (5 - 10u), \\ g_3(u) &= \frac{1}{12} (5 - 10u), & g_4(v) &= \frac{1}{3} u (1 - 4u) (5/4 - u), \end{aligned}$$

используя различные наборы смешивающих функций. На рисунке рис. 13 изображены полученные поверхности:

$s_1(u, v)$ — для полиномиальных смешивающих функций,

$s_2(u, v)$ — для экспоненциальных смешивающих функций с параметром $q = 10$,

$s_3(u, v)$ — для дробно-рациональных смешивающих функций с набором параметров $c = (-8, -5, -2, 0.75)$,

$s_4(u, v)$ — для логарифмических смешивающих функций с набором параметров $c = (1, 2, 3)$.

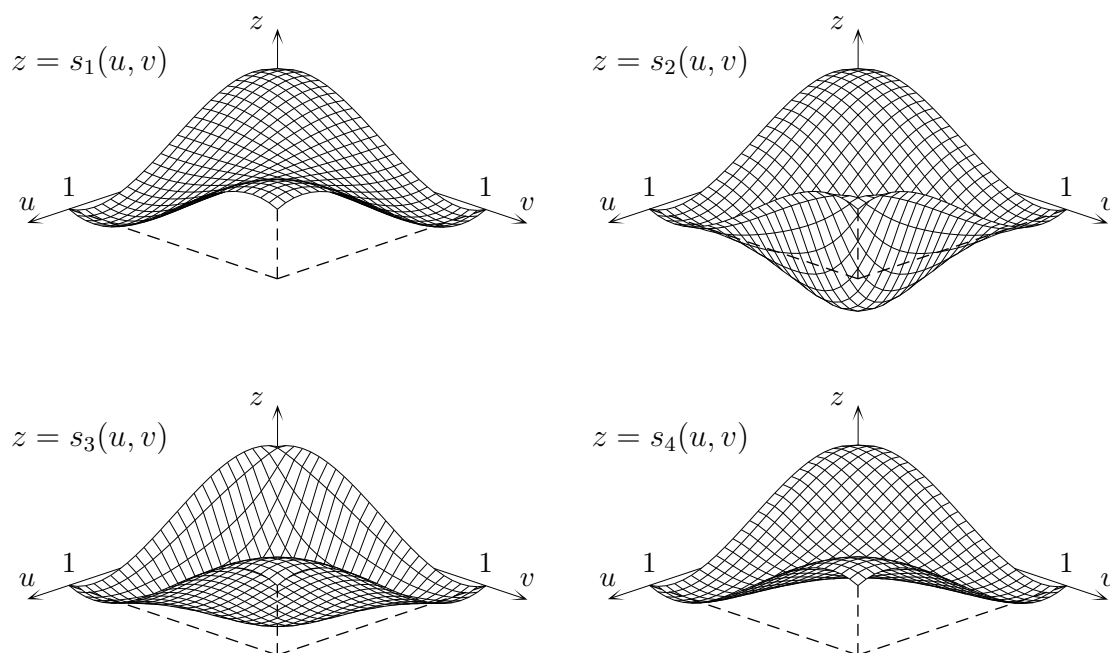


Рис. 13. Поверхности Кунса

ЛИТЕРАТУРА

1. Арайкина М. И. *Построение параметрических гамма-кривых и поверхностей* // Дипломная работа. Научн. рук. доц. А. А. Васильев. Сыктывкарский гос. университет, 2006.
2. Малозёмов В. Н., Чашников Н. В. *Бикубические поверхности Кунса* // Семинар «DHA & CAGD». Избранные доклады. 23 января 2007 г. (<http://dha.spb.ru/rep07.shtml#0123>).
3. Чашников Н. В. *Поверхность вращения как поверхность Кунса* // Семинар «DHA & CAGD». Избранные доклады. 28 августа 2007 г. (<http://dha.spb.ru/rep07.shtml#0828>).

ФРЕЙМЫ ГРАССМАНА

А. М. Дурягин

А. Б. Певный

27 ноября 2007 г.

1°. Пусть $m \geq n$. Через Φ будем обозначать систему из m единичных векторов в пространстве \mathbb{R}^n :

$$\Phi = \{\varphi_1, \dots, \varphi_m\}.$$

Следуя [1], величину

$$M(\Phi) = \max_{k \neq s} |\langle \varphi_k, \varphi_s \rangle|$$

назовём *максимальной корреляцией*. Система единичных векторов Φ^* , для которой

$$M(\Phi^*) = \min_{\Phi} M(\Phi),$$

называется *системой Грассмана*, а если Φ^* — фрейм, то можно говорить о *фрейме Грассмана*.

В задаче минимизации $M(\Phi)$ важную роль играет оценка $M(\Phi)$ снизу, установленная Уэлчем [2].

ТЕОРЕМА 1 (Уэлч, 1974). *Справедливо неравенство*

$$M(\Phi) \geq \sqrt{\frac{m-n}{n(m-1)}}. \quad (1)$$

Доказательство. Рассмотрим фреймовый потенциал системы Φ :

$$P(\Phi) = \sum_{k,s=1}^m |\langle \varphi_k, \varphi_s \rangle|^2.$$

В [3, 4] установлено, что

$$P(\Phi) \geq \frac{m^2}{n}, \quad (2)$$

причём равенство в (2) достигается тогда и только тогда, когда Φ — жёсткий фрейм.

Введём величину

$$V(\Phi) = \sum_{k \neq s} |\langle \varphi_k, \varphi_s \rangle|^2.$$

Величина $V(\Phi)$ отличается от $P(\Phi)$ отсутствием слагаемых $|\langle \varphi_k, \varphi_k \rangle|^2$, $k \in 1 : m$, равных единице. Поэтому $V(\Phi) = P(\Phi) - m$. В силу (2)

$$V(\Phi) \geq \frac{m^2}{n} - m = \frac{m(m-n)}{n}.$$

Оценим $V(\Phi)$ сверху, заменив каждое слагаемое на $[M(\Phi)]^2$. Учитывая, что всего слагаемых $m^2 - m = m(m-1)$, получаем

$$V(\Phi) \leq m(m-1)[M(\Phi)]^2.$$

Значит,

$$[M(\Phi)]^2 \geq \frac{1}{m(m-1)} V(\Phi) \geq \frac{m-n}{n(m-1)},$$

что равносильно (1). □

2°. Величину, стоящую в правой части неравенства (1), называют *границей Уэлча* и обозначают $W(n, m)$:

$$W(n, m) = \sqrt{\frac{m-n}{n(m-1)}}.$$

Если для некоторой системы Φ^* выполняется равенство $M(\Phi^*) = W(n, m)$, то Φ^* доставляет минимум функционалу M . Такая система Φ^* называется *системой Грассмана-Уэлча*. В [1] получена характеристизация систем Грассмана-Уэлча в терминах равноугольности.

Напомним, что система Φ называется *равноугольной*, если

$$|\langle \varphi_k, \varphi_s \rangle| = c \quad \text{при всех } k \neq s,$$

где c — фиксированное число.

ТЕОРЕМА 2. Равенство $M(\Phi) = W(n, m)$ выполняется тогда и только тогда, когда Φ — равноугольный жёсткий фрейм.

Доказательство. Допустим, что для некоторой системы Φ выполняется равенство $M(\Phi) = W(n, m)$. Согласно (2) имеем

$$\frac{m^2}{n} \leq P(\Phi) = \sum_{k=1}^m |\langle \varphi_k, \varphi_k \rangle|^2 + \sum_{k \neq s} |\langle \varphi_k, \varphi_s \rangle|^2 \leq m + m(m-1)[M(\Phi)]^2 =$$

$$= m + m(m-1) \frac{m-n}{n(m-1)} = \frac{m^2}{n}.$$

Отсюда следуют два равенства

$$P(\Phi) = \frac{m^2}{n}, \quad (3)$$

$$\sum_{k \neq s} |\langle \varphi_k, \varphi_s \rangle|^2 = m(m-1) [M(\Phi)]^2. \quad (4)$$

Как отмечалось при доказательстве теоремы 1, равенство (3) гарантирует, что Φ — жёсткий фрейм. Если учесть, что (4) эквивалентно соотношению $|\langle \varphi_k, \varphi_s \rangle| = M(\Phi)$ при $k \neq s$, то получаем, что жёсткий фрейм Φ является равноугольным.

Наоборот, пусть Φ — равноугольный жёсткий фрейм. Тогда $P(\Phi) = \frac{m^2}{n}$ и $|\langle \varphi_k, \varphi_s \rangle| = c$ при $k \neq s$. Отсюда следует, что

$$\frac{m^2}{n} = P(\Phi) = m + m(m-1)c^2.$$

Получаем

$$c = \sqrt{\frac{m-n}{n(m-1)}} = W(n, m).$$

Значит,

$$M(\Phi) := \max_{k \neq s} |\langle \varphi_k, \varphi_s \rangle| = c = W(n, m).$$

Теорема доказана. □

3°. По теореме 2 фреймы Грассмана-Уэлча — это то же самое, что равноугольные жёсткие фреймы. К сожалению, равноугольные системы векторов существуют не для всех пар (n, m) [5]. Поэтому представляет интерес нахождение фреймов Грассмана (минимизирующих функционал $M(\Phi)$) из разных дополнительных соображений. Например, при $n = 2$ фреймы Грассмана можно построить для всех $m \geq 2$. Это сделано в работе [6]. К изложению соответствующего результата мы и переходим.

ТЕОРЕМА 3. Для любой системы $\Phi = \{\varphi_0, \varphi_1, \dots, \varphi_{m-1}\}$, состоящей из m единичных двумерных векторов, справедливо неравенство

$$M(\Phi) \geq \cos \frac{\pi}{m}. \quad (5)$$

Равенство достигается, например, на вещественном гармоническом фрейме Φ^* , у которого

$$\varphi_k^* = \left(\cos \frac{\pi k}{m}, \sin \frac{\pi k}{m} \right), \quad k \in 0 : m-1. \quad (6)$$

Доказательство. Возьмём произвольную систему $\Phi = \{\varphi_0, \varphi_1, \dots, \varphi_{m-1}\}$ единичных векторов вида $\varphi_k = (x_k, y_k)$. Не умаляя общности, можно считать, что векторы φ_k лежат в верхней полуплоскости.

Обозначим через θ_k угол между положительным направлением оси x и вектором φ_k . Можно считать, что

$$0 = \theta_0 \leq \theta_1 \leq \dots \leq \theta_{m-1} \leq \pi$$

(если $\theta_0 > 0$, то повернём все векторы φ_k на угол $-\theta_0$). Ясно, что $\varphi_0 = (1, 0)$.

Обозначим через α_k угол между φ_k и φ_{k+1} , $k \in 0 : m-2$, а через α_{m-1} — угол между φ_{m-1} и отрицательным направлением оси x . Тогда

$$\sum_{k=0}^{m-1} \alpha_k = \pi,$$

причём все α_k неотрицательны. Отметим, что минимальный из углов α_k не превосходит $\frac{\pi}{m}$:

$$\alpha_s := \min_{k \in 0:m-1} \alpha_k \leq \frac{\pi}{m}.$$

Оценим $M(\Phi)$ снизу. Имеем

$$\begin{aligned} |\langle \varphi_k, \varphi_{k+1} \rangle| &\geq \langle \varphi_k, \varphi_{k+1} \rangle = \cos \alpha_k, \quad k \in 0 : m-2; \\ |\langle \varphi_{m-1}, \varphi_0 \rangle| &\geq \langle \varphi_{m-1}, -\varphi_0 \rangle = \cos \alpha_{m-1}. \end{aligned}$$

Значит,

$$M(\Phi) \geq \max\{\cos \alpha_0, \cos \alpha_1, \dots, \cos \alpha_{m-1}\} = \cos \alpha_s \geq \cos \frac{\pi}{m},$$

что соответствует (5).

Для системы Φ^* , состоящей из векторов (6), выполняется равенство $M(\Phi^*) = \cos \frac{\pi}{m}$. Это следует из формулы

$$\langle \varphi_k^*, \varphi_j^* \rangle = \cos \frac{\pi(k-j)}{m}.$$

Теорема доказана. □

З а м е ч а н и е. То, что система Φ^* при $m \geq 2$ образует жёсткий фрейм, хорошо известно [7]. Учитывая, что

$$W(2, 2) = 0 = \cos \frac{\pi}{2}, \quad W(2, 3) = \frac{1}{2} = \cos \frac{\pi}{3},$$

заключаем, что фрейм Φ^* при $m = 2$ и $m = 3$ является фреймом Грассмана-Уэлча.

Покажем, что

$$W(2, m) < \cos \frac{\pi}{m} \quad \text{при } m \geq 4.$$

Перепишем данное неравенство в эквивалентном виде

$$\frac{m-2}{m-1} < 2 \cos^2 \frac{\pi}{m} = 1 + \cos \frac{2\pi}{m}.$$

Справедливость последнего неравенства очевидна, поскольку $\cos \frac{2\pi}{m} \geq 0$ при $m \geq 4$.

Таким образом, при $m \geq 4$ система Φ^* является фреймом Грассмана, но не фреймом Грассмана-Уэлча.

ЛИТЕРАТУРА

1. Strohmer T., Heath R. W. *Grassmannian frames with applications to coding and communication* // Appl. Comput. Harmonic Anal. 2003. V. 14. No. 3. P. 257–275.
2. Welch L. R. *Lower bounds on the maximum cross-correlation of signals* // IEEE Trans. Info. Theory. 1974. V. 20. P. 397–399.
3. Casazza P. G. *Custom building finite frames* // Contemporary Math. 2004. V. 345. P. 61–86.
4. Певный А. Б. *Фреймы в конечномерных пространствах и задача минимизации фреймового потенциала* // Семинар «DHA & CAGD». Избранные доклады. 28 марта 2006 г. (<http://dha.spb.ru/rep06.shtml#0328>).
5. Малозёмов В. Н., Певный А. Б. *Равноугольные системы векторов и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 18 сентября 2007 г. (<http://dha.spb.ru/rep07.shtml\#0918>).
6. Benedetto J. J., Kolesar J. D. *Geometric properties of Grassmannian frames for \mathbb{R}^2 and \mathbb{R}^3* // EURASIP J. Applied Signal Proc. 2006. Article ID 49850. P. 1–17.
7. Дурягин А. М., Соловьёва Н. А. *Вещественные гармонические фреймы* // Семинар «DHA & CAGD». Избранные доклады. 9 октября 2007 г. (<http://dha.spb.ru/rep07.shtml\#1009>).

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА НЕЛИНЕЙНЫХ БУЛЕВЫХ ФУНКЦИЙ

И. В. Агафонова

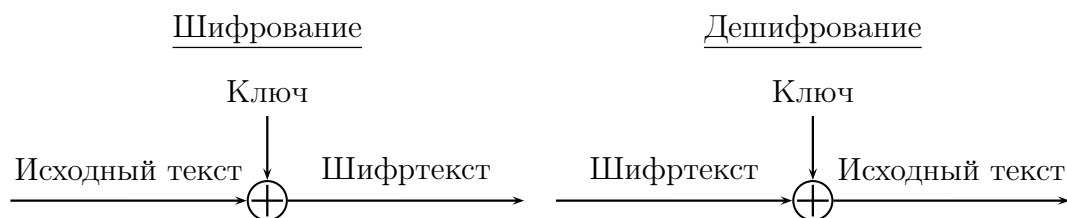
18 декабря 2007 г.

1. О булевых функциях в криптографии

В традиционных системах шифрования, переводящих открытое сообщение в зашифрованное с помощью секретного ключа, решающую роль играет аппарат булевых функций. К этим функциям предъявляется ряд требований, имеющих целью предельно усложнить расшифровку сообщения лицом, не являющимся его адресатом.

Для иллюстрации применения булевых функций приведём схему поточно-го шифрования, когда каждый поступающий символ тут же преобразуется в символ шифртекста.

Поточные шифры основаны на так называемом *шифре Вернама*, имеющем следующую схему:

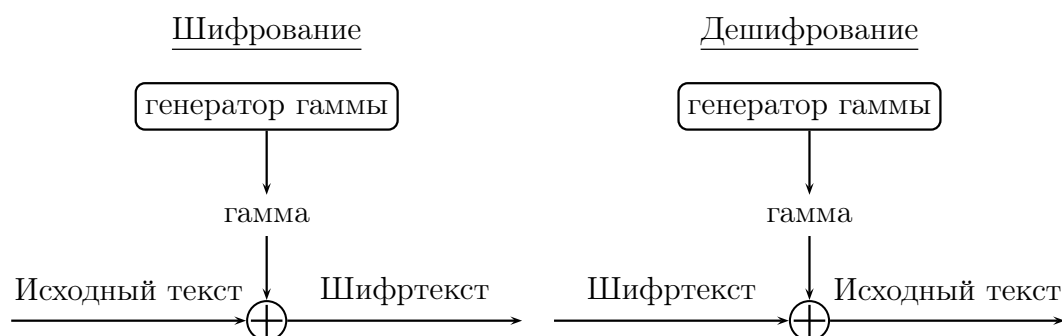


Исходный текст, ключ, шифртекст — бинарные строки одинаковой длины. Операция \oplus означает побитовое сложение по модулю 2. При дешифровании схема та же, что и при шифровании, только исходный текст и шифртекст меняются местами. Другое название шифра Вернама — одноразовый шифр-блокнот (one time pad). Действительно, дважды такой шифр не используют: при сложении двух шифртекстов, соответствующих одному ключу, получается сумма исходных текстов, что даёт много информации об исходных текстах и даже часто позволяет их прочесть.

Шеннон доказал, что при совершенно случайном ключе, используемом один раз, шифр Вернама является абсолютно стойкой криптосистемой, то есть перехват шифртекста не даёт никакой информации о переданном сообщении. Это единственный в настоящее время шифр с таким свойством.

На практике чаще всего отправитель и получатель сообщений выбирают вместо ключа в шифре Вернама псевдослучайную последовательность, которая по оговорённому (не секретному) алгоритму генерируется из короткого секретного ключа. Такая последовательность носит название *ключевой поток* или *гамма* (key stream, gamma).

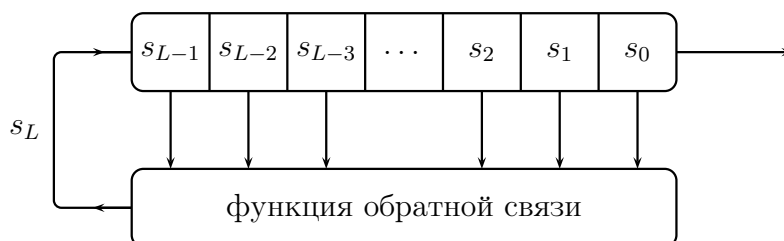
Теперь процесс шифрования выглядит так:



Стандартно секретный ключ размножается до гаммы с помощью устройств, называемых *регистрами сдвига с линейной обратной связью* (Linear Feedback Shift Register, сокращённо LFSR).

Регистр сдвига образован множеством ячеек памяти, в каждой из которых записан один бит информации. В начале работы ячейки содержат секретный ключ. На каждом шаге содержимое ячеек пропускается через функцию, называемую функцией обратной связи.

Значение, вырабатываемое этой функцией, записывается в крайнюю левую ячейку регистра, при этом все биты сдвигаются на одну позицию вправо, а крайний правый бит покидает регистр, и именно он является выходным значением регистра на данном шаге. Вот первый шаг:



Обозначим $s^{(i)} = (s_i, s_{i+1}, \dots, s_{i+L-1})$, $i = 0, 1, \dots$ — текущее состояние регистра. Состояние $s^{(0)}$ — начальное.

Тогда выходной символ s_i есть функция от $s^{(i)}$.

Линейность функции обратной связи означает, что $s_i = \langle c, s^{(i)} \rangle$, где $c = (c_1, c_2, \dots, c_L)$ — заданная последовательность битов длины L , а скалярное произведение определяется формулой

$$\langle x, u \rangle = \bigoplus_i x_i u_i,$$

как это принято в пространстве двоичных векторов¹⁾.

2. Принципы Шеннона

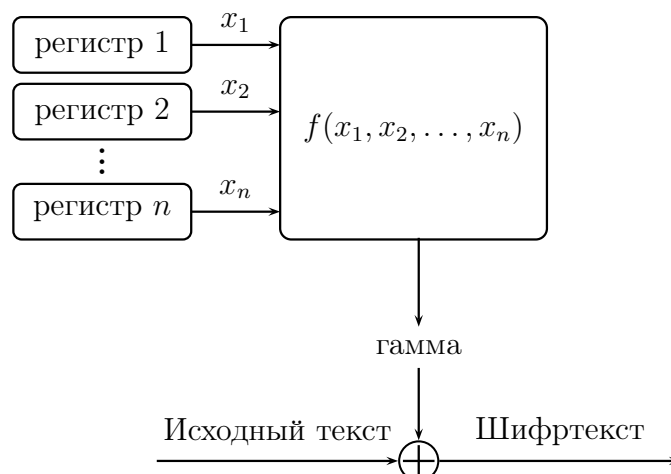
По К. Шеннону, шифрование должно использовать следующие принципы:

- Рассеивание (Diffusion) — распространение влияния одного знака открытого текста на много знаков шифртекста, а также распространение влияния одного элемента ключа на много знаков шифртекста.
- Перемешивание, усложнение, запутывание (Confusion) — свойство шифрующего преобразования усложнять взаимосвязи между элементами данных, что затрудняет восстановление функциональных и статистических связей между открытым текстом, ключом и шифртекстом

Устройство LFSR реализует принцип рассеивания, но не запутывания. Текст, шифруемый посредством только одного LFSR, защищён плохо²⁾. Общепринято для запутывания использовать несколько регистров LFSR. Пусть, например, длина секретного ключа равна L . Этот ключ можно разделить между несколькими регистрами длин L_i так, чтобы $L_1 + L_2 + \dots + L_n = L$, и комбинировать выходы всех n регистров посредством булевой функции f :

¹⁾На выбор вектора коэффициентов $c = (c_1, c_2, \dots, c_L)$ накладывается ограничение, а именно: двоичный многочлен $1 + c_1 x + c_2 x^2 + \dots + c_L x^L$ (он называется ассоциированным многочленом) должен быть примитивным. Если ассоциированный многочлен примитивен, то при любом начальном состоянии регистра выходная последовательность будет иметь максимально возможный период $2L - 1$. Это важно, так как чем больше период, тем больше скрыта детерминированность процесса, тем ближе последовательность к случайной.

²⁾Существует алгоритм Берлекэмп-Мэсси (Berlekamp-Massey), который на основании перехваченной шифровки восстановит и длину регистра L , и коэффициенты ассоциированного многочлена, если только длина перехваченного текста не менее $2L$.



Такая картина уже соответствует реальному механизму шифрования.

Более полувека, минувшие с момента формулирования принципов Шеннона, подтвердили их значимость. За эти годы предпринимались различного вида атаки на криптосистемы, в связи с которыми появились основные криптографические характеристики булевых функций, некоторые из которых больше относятся к рассеиванию, другие больше к запутыванию. Все эти характеристики надо учитывать при конструировании булевых функций. Требуется компромисс между ними, ибо булева функция не может быть оптимальна сразу по всем криптографическим показателям, как это показывают, в частности, теоремы 1 и 2. Этим теоремам в первую очередь и посвящается предлагаемый доклад.

3. Алгебраическая нормальная форма булевых функций

Условимся относительно обозначений.

F_2 — конечное поле из двух элементов, 0 и 1. Операции в F_2 — умножение и сложение по модулю 2.

V_n — n -мерное векторное пространство над полем F_2 , $V_n = (F_2)^n$. Сложение в пространстве V_n побитовое по модулю 2. Через \mathbb{O} обозначен нулевой вектор пространства V_n .

Единичные векторы $e^{(i)}$ с единицей в i -й позиции и нулями в остальных образуют базис пространства V_n .

Булева функция от n переменных есть отображение из V_n в F_2 . Мы будем ниже иметь дело также с *расширенными булевыми функциями* — отображениями из V_n в \mathbb{Z} (множество целых чисел). Рассматривают и ещё более общие *псевдо-булевы функции* — отображения из V_n в \mathbb{R} (множество действительных чисел).

Множество всех булевых функций от n переменных обозначим \mathcal{F}_n .

Число векторов пространства V_n равно 2^n как число всевозможных комбинаций n базисных векторов с коэффициентами 0 и 1. По той же причине число элементов любого линейного подпространства $E \subset V_n$ при $\dim E = m$ равно 2^m .

Булева или расширенная булева функция $f(x)$ задана, если имеется список её значений при всех $x \in V_n$. Например, при $n = 3$, $x = (x_1, x_2, x_3)$, одну из булевых функций можно задать таблицей:

№	x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0	1
1	0	0	1	0
2	0	1	0	0
3	0	1	1	1
4	1	0	0	0
5	1	0	1	0
6	1	1	0	1
7	1	1	1	1

В строках этой таблицы (называемой таблицей истинности) векторы пространства V_n записаны в лексикографическом порядке по возрастанию. Векторам соответствуют двоичные числа от 0 до $2n - 1$, также упорядоченные по возрастанию. Такое упорядочение называется естественным.

При соблюдении естественного упорядочения для задания булевой функции достаточно задать набор её значений $f_i, i \in 0 : n - 1$, так что $f = 10010011$.

Каждая функция из \mathcal{F}_n имеет единственное представление в виде *алгебраической нормальной формы* или АНФ (в отечественной литературе распространён также термин «полином Жегалкина»). АНФ есть выражение булевой функции в виде

$$f(x) = \bigoplus_{N \in P\{1,2,\dots,n\}} a_N \prod_{i \in N} x_i,$$

где $P\{1, 2, \dots, n\}$ — множество всех подмножеств $\{1, 2, \dots, n\}$ (булеан), $a_N \in F_2$.

Так, функция с приведённой выше таблицей истинности имеет представление $f(x) = 1 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_1 x_3$. Для вычисления АНФ заданной функции имеются несложные алгоритмы (см., например, [1, 2]), на которых мы не будем здесь останавливаться.

Степень монома (булева одночлена) $x^N = \prod_{i \in N} x_i$ определяется как $|N|$ (число элементов подмножества N).

Алгебраическая степень булевой функции f есть степень АНФ этой функции (как многочлена от нескольких переменных).

Булева функция степени 1 называется *аффинной*. Её АНФ имеет вид

$$f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus b = \langle a, x \rangle \oplus b,$$

где $b \in F_2$, $a \in V_n$.

Мы видели, что для криптографических целей булева функция не должна быть линейной (точнее, аффинной). Вообще чем меньше функция «похожа на аффинную», тем лучше. В это неформальное пожелание можно вложить различные смысловые оттенки. Вот некоторые из них:

- 1) «Функция с хорошей нелинейностью» далека от множества аффинных функций в смысле какой-либо метрики.
- 2) «Функция с хорошей нелинейностью» должна выражаться полиномом как можно более высокой степени.
- 3) «Функция с хорошей нелинейностью» не должна линейно зависеть ни от одной из своих переменных и не должна приобретать такую зависимость после какой-либо линейной замены переменной. Это свойство формулируют так: функция не должна иметь ненулевых линейных структур.

Собственно термин «нелинейность» принят для показателя нелинейности, использующего понятия веса Хэмминга и расстояния Хэмминга.

Весом Хэмминга или просто *весом* двоичного вектора называется число единиц среди его компонент. *Вес Хэмминга булевой функции* есть вес вектора её значений. Обозначать вес вектора или функции будем $\text{wt}(x)$ и $\text{wt}(f)$.

Расстояние Хэмминга между двумя функциями f и g есть вес функции $f \oplus g$. Другими словами, это число тех $x \in V_n$, на которых $f(x) \neq g(x)$.

Нелинейностью $N(f)$ булевой функции f называется расстояние Хэмминга между f и множеством аффинных функций \mathcal{A}_n .

4. Преобразования Уолша-Адамара

Знаковые функции и функции Уолша

Для количественной оценки нелинейности и других криптографических показателей вычисляют ряд характеристик булевых функций. В первую очередь это спектры Уолша-Адамара.

Определим для булевой или расширенной булевой функции f её *знаковую функцию* или *экспоненту*

$$\exp f(x) = (-1)^{f(x)}.$$

Знаковая функция является расширенной булевой функцией на V_n .

Очевидное преобразование, переводящее 0 в 1 и 1 в -1 , задаёт взаимно однозначное соответствие $\exp f(x) = 1 - 2f(x)$. Таблицу истинности для $\exp f(x)$ часто называют полярной или характерной таблицей истинности для f . Она полностью определяет функцию f .

Рассмотрим линейную булеву функцию $L_a(x) = \langle a, x \rangle$ на V_n . Можем записать её знаковую функцию

$$v(a, x) = \exp(L_a(x)) = (-1)^{\langle a, x \rangle}.$$

Функция $v(a, x)$ — это *дискретная функция Уолша*³⁾. На a и x мы смотрим одновременно и как на двоичные векторы из V_n , и как на целые числа, двоичная запись которых, дополненная при необходимости слева нулями, совпадает с этими векторами.

Нам понадобится ряд утверждений, касающихся знаковых функций и, в частности, дискретных функций Уолша. Все их мы будем доказывать здесь, чтобы не отсылать читателя к дополнительным источникам. Сразу отметим очевидные свойства

$$\begin{aligned} v(a, x) &= v(x, a) & \forall x \in V_n, \quad \forall a \in V_n, \\ |v(a, x)| &= 1 & \forall x \in V_n, \quad \forall a \in V_n, \\ v(\mathbb{O}, x) &= v(x, \mathbb{O}) = 1 & \forall x \in V_n. \end{aligned}$$

Пусть E — некоторое подпространство пространства V_n . Обозначим через E^\perp множество $E^\perp = \{u \in V_n : \langle u, x \rangle = 0 \quad \forall x \in E\}$ (*ортогональное* или *сопряжённое* подпространство к пространству E). Легко убедиться, что множество E^\perp является линейным пространством, причём $\dim E^\perp = n - \dim E$ ⁴⁾.

УТВЕРЖДЕНИЕ 1. Пусть $a \notin E^\perp$ (то есть на линейном подпространстве E линейная функция $\langle a, x \rangle$ принимает не только нулевые значения). Тогда $\sum_{x \in E} v(a, x) = 0$.

Доказательство. Разобьём пространство E на два подмножества:

$$E_0 = \{x \in E : \langle a, x \rangle = 0\}, \quad E_1 = \{x \in E : \langle a, x \rangle = 1\}.$$

По условию, множество E_1 не пусто. Возьмём какой-либо вектор $x^* \in E_1$. Складывая x^* с каждым элементом из E_1 (включая сам x^*), будем получать

³⁾О функциях Уолша см., например, [3].

⁴⁾Действительно, любой вектор $u \in E^\perp$ удовлетворяет системе однородных линейных уравнений $\langle u, b^{(i)} \rangle = 0$, где $\{b^{(i)}, i \in 1 : \dim E\}$ — базис подпространства E . Тогда базис пространства решений имеет размерность $n - \dim E$.

элементы множества E_0 , так что $|E_0| \geq |E_1|$. Складывая x^* с каждым элементом из E_0 , будем получать элементы множества E_1 , так что $|E_1| \geq |E_0|$. Тогда $|E_0| = |E_1|$, так что среди слагаемых будет столько же значений 1, сколько и значений (-1) . Сумма равна 0. \square

Из утверждения 1 выведем две полезные формулы. Так как $V_n^\perp = \{\mathbb{O}\}$, то

$$\sum_{x \in V_n} v(a, x) = \delta_0(a) 2^n, \quad (1)$$

где обозначено $\delta_0(a) = \begin{cases} 1 & \text{при } a = \mathbb{O}, \\ 0 & \text{при } a \neq \mathbb{O}. \end{cases}$

Так как при $a \in E^\perp$ выполняется $\sum_{x \in E} v(a, x) = \sum_{x \in E} (-1)^0 = |E|$, то

$$\sum_{x \in E} v(a, x) = |E| I_{E^\perp}(a), \quad (2)$$

где I_{E^\perp} — индикатор (характеристическое множество) пространства E^\perp .

***F*- и *W*-преобразования**

Преобразованием Уолша-Адамара 1-го рода (или *F*-преобразованием) булевой или расширенной булевой функции f назовём расширенную булеву функцию на V_n , задаваемую формулой

$$F_f(u) = \sum_{x \in V_n} f(x) v(x, u), \quad u \in V_n.$$

Знак \sum соответствует обычному целочисленному суммированию.

Сокращённое наименование «*F*-преобразование» принято здесь в связи с тем, что в литературе по булевым функциям в криптографии его чаще всего называют преобразованием Фурье. (См., например, [2], [4]). Наименованию, связанному с именами Уолша и Адамара, отдано предпочтение в книге [5].

УТВЕРЖДЕНИЕ 2. Для любой расширенной булевой функции f на V_n и любого $a \in V_n$ выполняется равенство $F_{f(x \oplus a)}(u) = v(a, u) F_{f(x)}(u)$.

Доказательство. По определению, $F_{f(x \oplus a)}(u) = \sum_{x \in V_n} f(x \oplus a) v(x, u)$. Прибегнем к замене переменной $x := x \oplus a$. Если x пробегает всё пространство V_n , то и $x \oplus a$ тоже пробегает всё пространство V_n . Поэтому

$$F_{f(x \oplus a)}(u) = \sum_{x \in V_n} f(x) v(x \oplus a, u) = \sum_{x \in V_n} f(x) v(x, u) v(a, u) =$$

$$= v(a, u) \sum_{x \in V_n} f(x) v(x, u) = v(a, u) F_{f(x)}(u).$$

Получена требуемая формула. \square

УТВЕРЖДЕНИЕ 3. Для любой расширенной булевой функции f на V_n выполняется $F_{F_f} = 2^n f$.

Доказательство. Нам требуется показать, что для любого $a \in V_n$ имеет место равенство $\sum_{u \in V_n} F_f(u) v(a, u) = 2^n f(a)$. Согласно утверждению 2,

$$\sum_{u \in V_n} F_f(u) v(a, u) = \sum_{u \in V_n} F_{f(x \oplus a)}(u).$$

Для любой функции $g(x)$ имеем

$$\begin{aligned} \sum_{u \in V_n} F_g(u) &= \sum_{u \in V_n} \sum_{x \in V_n} g(x) v(x, u)(u) = \sum_{x \in V_n} g(x) \sum_{u \in V_n} v(x, u) \stackrel{(1)}{=} \\ &= \sum_{x \in V_n} g(x) \delta_0(x) 2^n = 2^n g(\mathbb{O}). \end{aligned}$$

Применяя этот результат к функции $g(x) = f(x \oplus a)$, получаем

$$\sum_{u \in V_n} F_{f(x \oplus a)}(u) = 2^n f(a),$$

что и требовалось. \square

Из утверждения 3 следует *формула обращения* преобразования Уолша-Адамара 1-го рода:

$$f(x) = 2^{-n} \sum_{u \in V_n} F_f(u) v(u, x).$$

Преобразованием Уолша-Адамара 2-го рода (или W -преобразованием) булевой или расширенной булевой функции f назовём F -преобразование её знаковой функции $W_f(u) = F_f(\exp f(u))$, то есть расширенную булеву функцию на V_n , задаваемую формулой

$$W_f(u) = \sum_{x \in V_n} \exp(\langle x, u \rangle \oplus f(x)), \quad u \in V_n.$$

Соответствующая формула обращения имеет вид

$$\exp f(x) = 2^{-n} \sum_{u \in V_n} W_f(u) v(u, x).$$

Набор коэффициентов $\{F_f(u)\}$ или $\{W_f(u)\}$ некоторой булевой или расширенной булевой функции при всех $u \in V_n$ называется её *спектром Уолша-Адамара* 1-го или 2-го рода соответственно.

Связь между коэффициентами Уолша-Адамара 1-го и 2-го рода даётся формулой

$$W_f(u) = \delta_0(u) 2^n - 2F_f(u). \quad (3)$$

Убедимся, что эта формула верна. По определению,

$$W_f(u) = \sum_{x \in V_n} \exp(\langle x, u \rangle \oplus f(x)).$$

Разобьём эту сумму на две:

$$\begin{aligned} W_f(u) &= \sum_{x \in \text{supp } f} \exp(\langle x, u \rangle \oplus f(x)) + \sum_{x \in V_n \setminus \text{supp } f} \exp(\langle x, u \rangle \oplus f(x)) = \\ &= - \sum_{x \in \text{supp } f} \exp \langle x, u \rangle + \sum_{x \in V_n \setminus \text{supp } f} \exp \langle x, u \rangle = - \sum_{x \in \text{supp } f} v(u, x) + \sum_{x \in V_n \setminus \text{supp } f} v(u, x). \end{aligned}$$

Из (1) следует, что

$$\sum_{x \in V_n \setminus \text{supp } f} v(u, x) = \delta_0(u) 2^n - \sum_{x \in \text{supp } f} v(u, x).$$

В то же время

$$F_f(u) = \sum_{x \in V_n} f(x) v(u, x) = \sum_{x \in \text{supp } f} v(u, x).$$

Формула (3) доказана.

Оценка нелинейности. Бент-Функции

Значение нелинейности функции $f \in \mathcal{F}_n$ вычисляется по формуле

$$N(f) = 2^{n-1} - \frac{1}{2} \max_{a \in V_n} |W_f(a)|. \quad (4)$$

Докажем формулу (4). Вес Хэмминга функции f есть

$$\text{wt}(f) = \sum_{x \in V_n} f(x) = \sum_{x \in V_n} \frac{1 - \exp f(x)}{2}.$$

Так как $\sum_{x \in V_n} \exp f(x) = W_f(\mathbb{O})$, то получаем $\text{wt}(f) = 2^{n-1} - \frac{W_f(\mathbb{O})}{2}$. Тогда

$$\text{wt}(f(x) \oplus \langle a, x \rangle) = 2^{n-1} - \frac{W_{f(x) \oplus \langle a, x \rangle}(\mathbb{O})}{2} = 2^{n-1} - \frac{W_f(a)}{2}.$$

Аффинная функция задаётся либо формулой $g(x) = \langle a, x \rangle$, либо формулой $g(x) = \langle a, x \rangle \oplus 1$. В первом случае расстояние между функциями f и g есть

$$\text{dist}(f, g) = \text{wt}(f \oplus \langle a, x \rangle) = 2^{n-1} - \frac{W_f(a)}{2},$$

во втором

$$\text{dist}(f, g) = \text{wt}(f \oplus \langle a, x \rangle \oplus 1) = 2^n - \text{wt}(f \oplus \langle a, x \rangle) = 2^{n-1} + \frac{W_f(a)}{2}.$$

Таким образом, минимальное расстояние от f до множества аффинных функций — это величина

$$2^{n-1} - \frac{1}{2} \max_{a \in V_n} |W_f(a)|,$$

то есть выполняется (4).

Пример. По полученной формуле подсчитаем нелинейность функции 3-х переменных $f = 10010011$. Она равна 2 и является максимально возможной для функции из \mathcal{F}_3 , как будет видно ниже из неравенства, дающего границу нелинейности.

Найдём сумму квадратов коэффициентов Уолша-Адамара 1-го рода:

$$\begin{aligned} \sum_{u \in V_n} F_f^2(u) &= \sum_{u \in V_n} \sum_{x \in V_n} f(x) v(x, u) \sum_{y \in V_n} f(y) v(y, u) = \\ &= \sum_{u \in V_n} \sum_{x, y \in V_n} f(x) f(y) v(x, u) v(y, u) = \\ &= \sum_{u \in V_n} \sum_{x, y \in V_n} f(x) f(y) v(x \oplus y, u) \stackrel{(1)}{=} \\ &= \sum_{u \in V_n} \sum_{x, y \in V_n} f(x) f(y) \cdot 2^n \delta_0(x \oplus y) = 2^n \sum_{x \in V_n} f^2(x). \end{aligned}$$

Мы доказали равенство Парсеваля

$$\sum_{u \in V_n} F_f^2(u) = 2^n \sum_{x \in V_n} f^2(x).$$

Из этого соотношения находим

$$\sum_{u \in V_n} W_f^2(u) = 2^n \sum_{x \in V_n} (\exp f(x))^2 = 2^n \cdot 2^n = 2^{2n}.$$

Полученное равенство

$$\sum_{u \in V_n} W_f^2(u) = 2^{2n} \tag{5}$$

тоже называется *равенством Парсеваля*.

В силу равенства (5) получаем $\max_{u \in V_n} W_f^2(u) \geq 2^n$, следовательно,

$$\max_{u \in V_n} |W_f(u)| \geq 2^{\frac{n}{2}}.$$

Отсюда и из (4) сразу вытекает неравенство

$$N(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1},$$

так что $2^{n-1} - 2^{\frac{n}{2}-1}$ есть верхняя граница нелинейности.

Функция $f \in \mathcal{F}_n$ называется *бент-функцией*, если при любом $u \in V_n$ выполнено $|W_f(u)| = 2^{\frac{n}{2}}$ (при нечётных n понятие не определяется). Как мы видим, бент-функции при чётном n являются максимально нелинейными.

Спектры аффинно эквивалентных функций

Рассмотрим, как изменится спектр Уолша-Адамара при (невырожденном) аффинном преобразовании входных координат.

Функции g и h из \mathcal{F}_n называются *аффинно эквивалентными*, если существуют невырожденное линейное преобразование L на V_n и вектор $a \in V_n$ такие, что $h(x) = g(Lx \oplus a)$.

Преобразование Lx равносильно умножению на неособенную матрицу L порядка $n \times n$ над полем F_2 .

В этом определении, очевидно, g и h можно поменять местами.

Пусть функции g и h аффинно эквивалентны. Найдём

$$\begin{aligned} W_h(u) &= \sum_{x \in V_n} \exp \langle x, u \rangle \oplus h(x) = \sum_{x \in V_n} \exp \langle x, u \rangle \oplus g(Lx \oplus a) = \\ &\quad (\text{замена } y = Lx \oplus a, \text{ то есть } x = L^{-1}a \oplus L^{-1}y) \\ &= \sum_{y \in V_n} \exp (\langle L^{-1}a \oplus L^{-1}y, u \rangle \oplus g(y)) = \\ &= \exp \langle L^{-1}a, u \rangle \sum_{y \in V_n} \exp (\langle L^{-1}y, u \rangle \oplus g(y)) = \\ &\quad (\text{обозначение } L' = (L^{-1})^T) \\ &= \exp \langle a, L'u \rangle \sum_{y \in V_n} \exp (\langle y, L'u \rangle \oplus g(y)) = v(a, L'u) W_g(L'u). \end{aligned}$$

Если $a = \mathbb{O}$, то есть преобразование чисто линейное, то $v(a, x) = 1$ для всех x . Это означает, что **спектр функции h есть просто перемешанный**

спектр функции g . При $a \neq \mathbb{O}$ часть коэффициентов может ещё поменять знак. Для спектра 1-го рода дело обстоит точно так же, доказательство полностью аналогично приведённому.

В частности, отсюда следует, что бентность является аффинным инвариантом. Но и при таком достоинстве бент-функций их прямое использование в криптосистемах не практикуется, поскольку они не являются уравновешенными.

Функция f из \mathcal{F}_n называется уравновешенной или сбалансированной (balanced), если её вес Хэмминга равен $2n - 1$, то есть она принимает значения 0 и 1 одинаковое число раз.

На функции, используемые в криптографии, накладывается требование уравновешенности, чтобы избежать статистических зависимостей между входом и выходом. Эти зависимости могут использоваться в атаках на шифр.

Уравновешенность функции, как легко видеть, характеризуется условием $W_f(0) = 0$. Для бент-функций это условие не выполняется.

5. Производные булевых функций по направлению. Подпространство линейных структур

Производной по направлению $u \in V_n$ функции $f \in \mathcal{F}_n$ называется булева функция $D_u f(x) = f(x) \oplus f(x \oplus u)$.

Свойства производных

1°. Для любых $u, v, x \in V_n$ верно равенство $D_{u \oplus v} f(x) = D_u f(x) \oplus D_v f(x \oplus u)$.

Для доказательства достаточно воспользоваться определением:

$$\begin{aligned} D_{u \oplus v} f(x) &= f(x) \oplus f(x \oplus u \oplus v) = [f(x) \oplus f(x \oplus u)] \oplus \\ &\oplus [f(x \oplus u) \oplus f(x \oplus u \oplus v)] = D_u f(x) \oplus D_v f(x \oplus u). \end{aligned}$$

2°. Производная функции $f \in \mathcal{F}_n$ по направлению i -го базисного вектора $e^{(i)}$ является константой в том и только в том случае, когда эта функция может быть представлена в виде

$$f(x_1, x_2, \dots, x_n) = \varepsilon x_1 \oplus g(x_2, \dots, x_n), \quad (*)$$

где $\varepsilon \in F_2$ — эта константа.

Доказательство. Не ограничивая общности можно провести рассуждения для $e^{(1)}$.

Пусть $D_{e^{(1)}}f(x) = \varepsilon$ при всех $x \in V_n$. Тогда по определению производной по направлению $(1, 0, \dots, 0)$ выполняется равенство

$$f(x_1 \oplus 1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n) \oplus \varepsilon.$$

В частности, при $x_1 = 0$ имеем

$$f(1, x_2, \dots, x_n) = f(0, x_2, \dots, x_n) \oplus \varepsilon.$$

Подставляя это равенство в тождество⁵⁾

$$f(x_1, x_2, \dots, x_n) = f(0, x_2, \dots, x_n) \oplus x_1 [f(0, x_2, \dots, x_n) \oplus f(1, x_2, \dots, x_n)],$$

получаем

$$\begin{aligned} f(x_1, x_2, \dots, x_n) &= f(0, x_2, \dots, x_n) \oplus x_1 [f(0, x_2, \dots, x_n) \oplus f(0, x_2, \dots, x_n) \oplus \varepsilon] = \\ &= f(0, x_2, \dots, x_n) \oplus x_1 \varepsilon. \end{aligned}$$

Последнее равенство даёт представление $(*)$, если в качестве функции g взять

$$g(x_2, \dots, x_n) = f(0, x_2, \dots, x_n).$$

Обратное утверждение получается сразу из $(*)$ применением определения производной:

$$D_{e^{(1)}}f(x) = \varepsilon x_1 \oplus g(x_2, \dots, x_n) \oplus \varepsilon (x_1 \oplus 1) \oplus g(x_2, \dots, x_n) = \varepsilon.$$

Производная равна ε . □

3°. Производная функции $f \in \mathcal{F}_n$ постоянна по каждому направлению в том и только в том случае, когда эта функция аффинна.

Доказательство. Для аффинной функции то, что производная постоянна, проверяется сразу по определению. Проведём обратное рассуждение.

Производная функции f по базисному вектору $e^{(1)}$ постоянна, и по свойству 2°

$$f(x_1, x_2, \dots, x_n) = \varepsilon_1 x_1 \oplus g_1(x_2, \dots, x_n).$$

Так как производная функции g_1 по $e^{(2)}$, как нетрудно убедиться, равна производной f по $e^{(2)}$ и тоже постоянна, получаем

$$g_1(x_2, \dots, x_n) = \varepsilon_2 x_2 \oplus g_2(x_3, \dots, x_n),$$

⁵⁾Тождество легко проверяется, оно верно и при $x_1 = 0$, и при $x_1 = 1$.

и так далее. На последнем шаге придём к равенству

$$g_{n-2}(x_{n-1}, x_n) = \varepsilon_{n-1} x_{n-1} \oplus g_{n-1}(x_n).$$

Функции одной координаты все аффинны, так что

$$g_{n-1}(x_n) = \varepsilon_n x_n \oplus b, \quad b \in F_2.$$

Функция f получила аффинное представление. □

Вектор $u \in V_n$, по направлению которого производная $D_u f$ постоянна, называют *линейной структурой* функции f .

УТВЕРЖДЕНИЕ 4. Функция $f \in \mathcal{F}_n$ имеет какую-либо ненулевую линейную структуру тогда и только тогда, когда эта функция аффинно эквивалентна функции, для которой вектор $e^{(1)}$ является линейной структурой.

Доказательство. Пусть u — ненулевая линейная структура функции f . Рассмотрим функцию $h(x) = f(Lx)$, где преобразование L обладает свойством $Le^{(1)} = u$ ⁶⁾.

Функции f и h аффинно эквивалентны. Найдём производную

$$\begin{aligned} D_{e^{(1)}} h(x) &= h(x) \oplus h(x \oplus e^{(1)}) = f(Lx) \oplus f(L(x \oplus e^{(1)})) = \\ &= f(Lx) \oplus f(Lx \oplus u) = D_u f(x). \end{aligned}$$

Так как $D_u f(x)$ — константа, то и $D_{e^{(1)}} h(x)$ — константа.

Докажем обратное. Пусть $f(x) = h(Lx \oplus a)$, причём $D_{e^{(1)}} h(x) = \text{const}$. Возьмём $u = L^{-1}e^{(1)}$, так что $Lu = e^{(1)}$. Тогда

$$\begin{aligned} D_u f(x) &= f(x) \oplus f(x \oplus u) = h(Lx \oplus a) \oplus h(L(x \oplus u) \oplus a) = \\ &= h(Lx \oplus a) \oplus h(Lx \oplus Lu \oplus a) = h(Lx \oplus a) \oplus h(Lx \oplus e^{(1)} \oplus a) = \\ &= D_{e^{(1)}} h(Lx \oplus a) = \text{const}. \end{aligned}$$

Значит, u — линейная структура функции f . Очевидно, $u \neq \mathbb{O}$. □

Нетрудно видеть, что множество всех линейных структур функции f является линейным подпространством пространства V_n . Чтобы проверить это, достаточно убедиться, что нулевой вектор \mathbb{O} является линейной структурой⁷⁾ и что $D_{u \oplus v} f = \text{const}$ при $D_u f = \text{const}$ и $D_v f = \text{const}$. Последнее следует из свойства 1° производных.

⁶⁾Матрица такого преобразования имеет первый столбец, совпадающий с u , а остальные столбцы подбираются из V_n так, чтобы обеспечить невырожденность. При $u_1 = 1$ это могут быть столбцы единичной матрицы, то есть векторы $e^{(i)}$, $i = 2, 3, \dots, n$. При $u_1 = 0$ это могут быть $e^{(i)}$, $i \in 1 : n$, $i \neq k$, где индекс k выбран так, чтобы $u_k = 1$.

⁷⁾Это тривиально, $D_{\mathbb{O}} f(x) = f(x) \oplus f(x \oplus \mathbb{O}) = 0$.

6. Автокорреляция и теорема Винера-Хинчина

Автокорреляционной функцией или, кратко, автокорреляцией функции $f \in \mathcal{F}_n$ называется расширенная булева функция $\Delta_f(u)$, имеющая вид

$$\Delta_f(u) = \sum_{x \in V_n} \exp(f(x) \oplus f(x \oplus u)) = W_{D_u f}(\mathbb{O}).$$

УТВЕРЖДЕНИЕ 5. Для любой функции $f \in \mathcal{F}_n$ выполняется

$$\sum_{u \in V_n} \Delta_f(u) = W_f^2(\mathbb{O}).$$

Доказательство. Имеем:

$$\begin{aligned} \sum_{u \in V_n} \Delta_f(u) &= \sum_{u \in V_n} \sum_{x \in V_n} \exp(f(x) \oplus f(x \oplus u)) = \sum_{x \in V_n} \sum_{u \in V_n} \exp(f(x) \oplus f(x \oplus u)) = \\ &\quad (\text{замена } u := x \oplus u) \\ &= \sum_{x \in V_n} \exp f(x) \sum_{u \in V_n} \exp f(u) = W_f(\mathbb{O}) \cdot W_f(\mathbb{O}). \end{aligned} \quad \square$$

Свёртку расширенных булевых функций f и g введём как функцию $c = f * g$, вычисляемую по формуле⁸⁾

$$\begin{aligned} c(x) &= \sum_{y \in V_n} f(x \oplus y) g(y) = \quad (\text{замена переменной } y := x \oplus y) \\ &= \sum_{y \in V_n} f(y) g(x \oplus y). \end{aligned}$$

УТВЕРЖДЕНИЕ 6. Для расширенных булевых функций f и g выполнено равенство $F_{f*g} = F_f \cdot F_g$, где под умножением функций в правой части равенства понимается покомпонентное умножение.

Доказательство. Для любого $u \in V_n$ имеем

$$\begin{aligned} F_{f*g}(u) &= \sum_{x \in V_n} (f * g)(x) v(x, u) = \sum_{x \in V_n} \sum_{y \in V_n} f(y) g(x \oplus y) v(x, u) = \\ &= \sum_{x \in V_n} \sum_{y \in V_n} f(y) g(x \oplus y) v(x \oplus y, u) v(y, u) = \end{aligned}$$

⁸⁾Иногда, как в [3], для чисто булевых функций f и g свёртка определяется чуть иначе: внешняя сумма есть $\bigoplus_{y \in V_n}$. Но при таком определении не выполнена, например, приводимая далее важная теорема Винера-Хинчина.

$$\begin{aligned}
&= \sum_{y \in V_n} \sum_{x \in V_n} f(y) g(x \oplus y) v(x \oplus y, u) v(y, u) = \\
&= \sum_{y \in V_n} f(y) v(y, u) \sum_{x \in V_n} g(x \oplus y) v(x \oplus y, u) = \\
&\quad (\text{замена переменной } x := x \oplus y) \\
&= F_f(u) \cdot F_g(u).
\end{aligned}$$

Утверждение доказано. \square

Следующее утверждение мы приведём в двух равносильных формулировках.

УТВЕРЖДЕНИЕ 7 (Теорема Винера-Хинчина). *Для любой функции $f \in \mathcal{F}_n$ при всех $u \in V_n$ справедливо равенство*

$$F_{\exp f * \exp f}(u) = W_f^2(u),$$

записываемое также в виде

$$F_{\Delta_f}(u) = W_f^2(u).$$

Доказательство. Первое равенство есть результат применения утверждения 6 к паре одинаковых функций, а именно функций $\exp f$. Второе получается из первого. Действительно,

$$\begin{aligned}
(\exp f * \exp f)(u) &= \sum_{x \in V_n} \exp f(x) \exp f(u \oplus x) = \\
&= \sum_{x \in V_n} \exp(f(x) \oplus f(u \oplus x)) = \Delta_f(u). \quad \square
\end{aligned}$$

7. Две числовые характеристики и их совместное ограничение

Нас будет интересовать число ненулевых значений расширенных булевых функций $\Delta_f(u)$ и $W_f(u)$. Обозначим

$$N_{\Delta} = |u \in V_n : \Delta_f(u) \neq 0|,$$

$$N_W = |u \in V_n : W_f(u) \neq 0|.$$

Каждая из этих величин определяется булевой функцией f , и с каждой из них связаны свои криптографические показатели, причём одни показатели будут наилучшими при как можно меньшем значении N_{Δ} , другие — при как можно меньшем значении N_W . Ниже будут сформулированы и доказаны две фундаментальные теоремы, касающиеся этих величин.

ТЕОРЕМА 1. Для любой функции $f \in \mathcal{F}_n$ выполнено неравенство

$$N_\Delta \cdot N_W \geq 2^n. \quad (6)$$

Доказательство. Равенство Парсеваля можно записать в виде

$$\sum_{u \in V_n, W_f(u) \neq 0} W_f^2(u) = 2^{2n}.$$

В этой сумме число слагаемых равно N_W , так что получаем, обозначив $u_0 = \arg \max W_f^2(u)$, следующую цепочку неравенств:

$$\begin{aligned} \frac{2^{2n}}{N_W} &\leq W_f^2(u_0) = \quad (\text{по утверждению 7}) \\ &= \sum_{u \in V_n} \Delta_f(u) v(u, u_0) \leq \sum_{u \in V_n} |\Delta_f(u)| = \sum_{u \in V_n, \Delta_f(u) \neq 0} |\Delta_f(u)| \leq N_\Delta \cdot 2^n. \end{aligned}$$

Последнее неравенство имеет место потому, что величина $|\Delta_f(u)|$, являясь суммой единиц с различными знаками в количестве 2^n , при любом u не превосходит 2^n .

Итоговое неравенство равносильно доказываемому. \square

Далее нам понадобятся обобщения утверждений 6 и 7 на линейное подпространство E пространства V_n . Введём обозначения для функций на E :

$$(f \overset{E}{*} g)(x) = \sum_{y \in E} f(x \oplus y) g(y), \quad x \in E \text{ — свёртка на подпространстве,}$$

$$\Delta_f^E(u) = \sum_{x \in E} \exp(f(x) \oplus f(x \oplus u)), \quad u \in E \text{ — автокорреляция на подпространстве,}$$

$$F_f^E(u) = \sum_{x \in E} f(x) v(x, u), \quad u \in E \text{ — } F\text{-преобразование на подпространстве,}$$

$$W_f^E(u) = \sum_{x \in E} f(x) v(x, u), \quad u \in E \text{ — } W\text{-преобразование на подпространстве.}$$

УТВЕРЖДЕНИЕ 8. Для любого $u \in V_n$ выполнено

$$F_{f \overset{E}{*} g}^E(u) = F_f^E \cdot F_g^E.$$

Доказательство полностью повторяет доказательство утверждения 6 с заменой при суммировании пространства V_n на подпространство E .

УТВЕРЖДЕНИЕ 9 (Теорема Винера-Хинчина для подпространства). Для любого $u \in V_n$ выполнено

$$F_{\Delta_f^E}^E(u) = (W_f^E(u))^2.$$

Доказательство. Имеем

$$\Delta_f^E(x) = \sum_{x \in E} \exp(f(x) \oplus f(x \oplus u)) = \sum_{x \in E} \exp f(x) \cdot \exp f(x \oplus u) = \exp f \overset{E}{*} \exp f.$$

Применяется утверждение 8, роль g и f играет знаковая функция $\exp f$. \square

Функция f называется *бент-функцией на подпространстве E* , если для всех $u \in E$ выполнено равенство

$$|W_f^E(u)| = 2^{\frac{\dim E}{2}}.$$

УТВЕРЖДЕНИЕ 10. Функция f является бент-функцией на подпространстве E тогда и только тогда, когда для любого ненулевого $z \in E$ выполняется равенство $\Delta_f^E(z) = 0$.

Доказательство. Заметим, что

$$\Delta_f^E(\mathbb{O}) = \sum_{x \in E} \exp(f(x) \oplus f(x)) = |E| = 2^{\dim E}.$$

Поэтому $\Delta_f^E(z) = \delta_0(z) 2^{\dim E}$.

Пусть $\Delta_f^E(z) = 0$ при всех $z \in E, z \neq \mathbb{O}$. Используя утверждение 9, находим

$$(W_f^E(u))^2 = F_{\Delta_f^E}^E(u) = \sum_{z \in E} \Delta_f^E(z) v(z, u) = \sum_{z \in E} \delta_0(z) 2^{\dim E} v(z, u).$$

По смыслу $\delta_0(z)$, в этой сумме только одно ненулевое слагаемое, соответствующее $z = \mathbb{O}$. Поэтому $(W_f^E(u))^2 = 2^{\dim E}$, так что f — бент-функция на E . Обратное, пусть $(W_f^E(u))^2 = 2^{\dim E}$, то есть, по утверждению 9, $\sum_{z \in E} \Delta_f^E(z) v(z, u) = 2^{\dim E}$. В то же время при $z = \mathbb{O}$ имеем

$$\Delta_f^E(\mathbb{O}) v(\mathbb{O}, u) = \Delta_f^E(\mathbb{O}) = 2^{\dim E}.$$

Тогда остальные слагаемые этой суммы равны 0. \square

Характеризация частично бент-функций

Частично бент-функцией (partially-bent function) называется булева функция, для которой в неравенстве (6) достигается равенство:

$$N_{\Delta} \cdot N_W = 2^n. \quad (7)$$

ЛЕММА. Равенство $\Delta_f(u) = 2^n \exp \varepsilon$ справедливо тогда и только тогда, когда при всех $x \in V_n$ выполнено $D_u f(x) = \varepsilon$.

Доказательство. Пусть $D_u f(x) = \varepsilon$ при всех x . По определению,

$$\Delta_f(u) = \sum_{x \in V_n} \exp D_u f(x).$$

Значит, $\Delta_f(u) = \sum_{x \in V_n} \exp \varepsilon = 2^n \exp \varepsilon$.

Обратно, пусть $\Delta_f(u) = 2^n \exp \varepsilon$. Так как $\Delta_f(u)$ есть сумма 2^n чисел, равных по модулю единице, то это равенство выполняется лишь в случае, когда все слагаемые этой суммы равны $\exp \varepsilon$, то есть при $D_u f(x) = \varepsilon$. \square

ТЕОРЕМА 2 (впервые доказана в [6]). Равенство (7) равносильно каждому из двух эквивалентных условий:

- 1) При любом u либо $\Delta_f(u) = 0$, либо существует $t \in V_n$ такое, что $\Delta_f(u) = 2^n v(t, u)$.
- 2) Пространство V_n разлагается в прямую сумму двух подпространств E и E' (причём E' имеет чётную размерность) таких, что для всех $x \in E$, $y \in E'$ имеет место разложение

$$f(x \oplus y) = g(x) \oplus h(y),$$

где функция $g(x)$ является линейной на E , а функция $h(y)$ является бент-функцией на E' .

Доказательство проведём по схеме $(7) \longrightarrow 1) \longrightarrow 2) \longrightarrow (7)$.

$$\boxed{(7) \longrightarrow 1)}$$

Возьмём $u_0 = \arg \max W_f^2(u)$. Рассмотрим функцию $\varphi(u) = f(u) \oplus \langle u_0, u \rangle$. Для неё

$$\begin{aligned} \text{(a)} \quad W_{\varphi}(\mathbb{O}) &= \sum_{x \in V_n} \exp (\langle x, \mathbb{O} \rangle \oplus \varphi(x)) = \\ &= \sum_{x \in V_n} \exp \varphi(x) = \sum_{x \in V_n} \exp (f(x) \oplus \langle u_0, x \rangle) = W_f(u_0) \end{aligned}$$

(по определению W -преобразования),

$$\begin{aligned}
 (b) \quad \Delta_\varphi(u) &= \sum_{x \in V_n} \exp(\varphi(x) \oplus \varphi(x \oplus u)) = \\
 &= \sum_{x \in V_n} \exp(f(x) \oplus \langle u_0, x \rangle \oplus f(x \oplus u) \oplus \langle u_0, x \oplus u \rangle) = \\
 &= \sum_{x \in V_n} \exp(f(x) \oplus \langle u_0, u \rangle \oplus f(x \oplus u)) = \\
 &= v(u_0, u) \sum_{x \in V_n} \exp(f(x) \oplus f(x \oplus u)) = v(u_0, u) \Delta_f(u).
 \end{aligned}$$

Таким образом, значения $\Delta_\varphi(u)$ и $\Delta_f(u)$ на одном и том же u либо оба нулевые, либо оба ненулевые.

Вся цепочка неравенств из доказательства теоремы 1 в случае (7) перейдёт в цепочку равенств. В частности, $W_f^2(u_0) = N_\Delta \cdot 2^n$.

Согласно утверждению 5,

$$\sum_{u \in V_n} \Delta_\varphi(u) = W_f^2(\mathbb{O}) \stackrel{(a)}{=} W_f^2(u_0) = N_\Delta \cdot 2^n.$$

Тогда при каждом $u \in V_n$ либо $\Delta_\varphi(u) = 0$, либо $\Delta_\varphi(u) = 2^n$, откуда в силу (b) либо $\Delta_\varphi(u) = 0$, либо $\Delta_f(u) = v(u_0, u) \cdot 2^n$.

1) \longrightarrow 2)

В качестве подпространства E возьмём $E = \{u \in V_n : \Delta_f(u) = v(t, u) \cdot 2^n\}$, то есть носитель функции $\Delta_f(u)$. По лемме, $u \in E$ означает, что u — линейная структура функции f .

Более того, E есть множество всех линейных структур функции f . Действительно, возьмём $z \notin E$. Тогда $\sum_{x \in V_n} \exp D_z f(x) = \Delta_f(z) = 0$. В этом случае половина производных $D_z f(x)$, $x \in V_n$, равна 0, а половина 1, так что z не является линейной структурой.

Итак, E — множество линейных структур, и оно, как мы уже видели, является линейным подпространством.

В качестве E' возьмём прямое дополнение подпространства E до V_n , $V_n = E + E'$. Для любого $z \in E'$ выполняется

$$\Delta_f(z) = \sum_{u \in V_n} \exp D_z f(u) = 0.$$

Представив $u = x \oplus y$, распишем эту сумму:

$$\Delta_f(z) = \sum_{x \in E} \sum_{y \in E'} \exp(f(x \oplus y) \oplus f(x \oplus y \oplus z)).$$

По лемме, условие $x \in E$ равносильно тому, что при всех $s \in V_n$ имеет место равенство $D_x f(s) = \langle t, x \rangle$. Это равенство разбивает при любом s функцию $f(x \oplus s)$ на 2 слагаемых: $f(x \oplus s) = f(s) \oplus \langle t, x \rangle$. В том числе:

$$\begin{aligned} \text{при } s = y & \quad \text{имеем} & f(x \oplus y) = f(y) \oplus \langle t, x \rangle, \\ \text{при } s = y \oplus z & \quad \text{имеем} & f(x \oplus y \oplus z) = f(y \oplus z) \oplus \langle t, x \rangle. \end{aligned} \quad (*)$$

Складывая два эти равенства, получаем

$$f(x \oplus y) \oplus f(x \oplus y \oplus z) = f(y) \oplus f(y \oplus z).$$

Таким образом,

$$\Delta_f(z) = \sum_{x \in E} \sum_{y \in E'} \exp(f(y) \oplus f(y \oplus z)).$$

Во внешней сумме все слагаемые одинаковы, их число равно $2^{\dim E}$, поэтому

$$\Delta_f(z) = 2^{\dim E} \sum_{y \in E'} \exp(f(y) \oplus f(y \oplus z)) = \Delta_f^{E'}(z).$$

Так как $\Delta_f(z) = 0$, то и $\Delta_f^{E'}(z) = 0$ при $z \in E'$, $z \neq \mathbb{O}$.

Последнее равенство означает, по утверждению 10, бентность функции f на подпространстве E' . Значит, $h(y)$ есть просто сужение f на E' (функция, определённая на E' , значения которой совпадают со значениями функции f на E').

Равенство (*) даёт требуемое представление. Функция $g(x) = \langle t, x \rangle$ линейна.

2) \longrightarrow (7)

Пусть любое $u \in V_n$ представляется в виде $u = x \oplus y$, $x \in E$, $y \in E'$, при этом $f(x \oplus y) = \langle t, x \rangle \oplus h(y)$, $h(y)$ является бент-функцией на E' . Скалярное произведение изображает линейную функцию.

По определению,

$$\Delta_f(z) = \sum_{u \in V_n} \exp(f(x) \oplus f(u \oplus z)).$$

Представив $u = x \oplus y$, $x \in E$, $y \in E'$, $z = x_1 \oplus y_1$, $x_1 \in E$, $y_1 \in E'$, придём к равенству

$$\Delta_f(z) = \sum_{x \in E} \sum_{y \in E'} \exp(f(x \oplus y) \oplus f(x \oplus y \oplus x_1 \oplus y_1)).$$

Подставим $f(x \oplus y) = \langle x, t \rangle \oplus h(y)$. Получим

$$\begin{aligned}\Delta_f(z) &= \sum_{x \in E} \sum_{y \in E'} \exp(\langle x, t \rangle \oplus h(y) \oplus \langle x \oplus x_1, t \rangle \oplus h(y \oplus y_1)) = \\ &= \sum_{x \in E} \sum_{y \in E'} \exp(\langle x_1, t \rangle \oplus h(y) \oplus h(y \oplus y_1)) = \\ &= \exp\langle x_1, t \rangle \sum_{x \in E} \sum_{y \in E'} \exp(h(y) \oplus h(y \oplus y_1)) = v(x_1, t) \sum_{x \in E} \Delta_h^{E'}(y_1).\end{aligned}$$

Так как h — бент-функция на E' , то по утверждению 10 при $y_1 \neq \mathbb{O}$ (то есть для $z \notin E$) будет выполнено $\Delta_h^{E'}(y_1) = 0$ и, следовательно, $\Delta_f(z) = 0$, а при $y_1 = \mathbb{O}$ (то есть для $z = x_1 \in E$), как нетрудно посчитать, $\Delta_f(z) = v(x_1, t) \cdot 2^n \neq 0$. Таким образом, $N_\Delta = |E| = 2^{\dim E}$.

Такое же исследование проведём для N_W .

По утверждению 7, $F_{\Delta_f}(u) = W_f^2(u) \forall u \in V_n$. Как было показано в конце раздела 4, аффинное преобразование координат не меняет набор значений W_f^2 . Поэтому мы будем искать не $W_f^2(u)$, а $W_f^2(u \oplus t)$, что более удобно.

$$\begin{aligned}W_f^2(u \oplus t) &= \sum_{z \in V_n} \Delta_f(z) v(z, u \oplus t) = \sum_{z \in E} \Delta_f(z) v(z, u \oplus t) = \\ &= \sum_{z \in E} 2^n v(z, t) v(z, u \oplus t) = 2^n \sum_{z \in E} v(z, u) \stackrel{(2)}{=} \\ &= 2^n |E| I_{E^\perp}(u) = \begin{cases} 0, & \text{если } u \notin E^\perp, \\ 2^n |E|, & \text{если } u \in E^\perp. \end{cases}\end{aligned}$$

Отсюда сразу следует, что $N_W = |E^\perp|$. Так как $\dim E^\perp = n - \dim E$, то $N_W = 2^{n - \dim E}$. Перемножая, получаем то, что требовалось: $N_\Delta \cdot N_W = 2^n$.

Теорема 2 доказана. \square

ЛИТЕРАТУРА

1. Марченков С. С. *Булевы функции*. М.: Физматлит, 2002.
2. Carlet C. *Boolean functions for cryptography and error correcting codes* // In: Crama Y., Hammer P. L. (Eds.), *Boolean Methods and Models*, Cambridge University Press, готовится к выходу. С текстом можно ознакомиться на <http://www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf>
3. Залманзон Л. А. *Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях*. М.: Наука, 1989. 496 с.

4. Логачёв О. А., Сальников А. А., Яценко В. В. *Булевы функции в теории кодирования и криптологии*. М.: МЦНМО, 2004. 470 с.
5. Сачков В. Н. *Введение в комбинаторные методы дискретной математики*. (2-е изд.). М.: МЦНМО, 2004. 424 с.
6. Carlet C. *Partially-bent functions* // Designs, Codes and Cryptography. 1993. V. 3. No. 2. P. 135–145.

ДИСКРЕТНЫЕ ФУНКЦИИ ВИЛЕНКИНА-КРЕСТЕНСОНА

В. Н. Малозёмов О. В. Просеков А. Н. Сабаев

16 января 2008 г.

1°. Нам понадобится известный способ кодирования целых чисел. Пусть $N = n_1 n_2 \cdots n_s$. Число N при каждом $\nu \in 1 : s$ можно представить в виде $N = \Delta_\nu n_\nu N_\nu$. На базе чисел $\Delta_\nu = n_1 n_2 \cdots n_{\nu-1}$ записывается разложение любого $j \in 0 : N - 1$:

$$j = j_s (n_{s-1} n_{s-2} \cdots n_1) + j_{s-1} (n_{s-2} \cdots n_1) + \cdots + j_2 n_1 + j_1 = \sum_{\nu=1}^s j_\nu \Delta_\nu, \quad (1)$$

где $j_\nu \in 0 : n_\nu - 1$. Набор коэффициентов разложения $(j_s, j_{s-1}, \dots, j_1)$ образует *смешанный код* числа j . Запись $j = (j_s, j_{s-1}, \dots, j_1)$ равносильна (1).

Отметим, что при всех $\nu \in 2 : s$

$$\sum_{\alpha=1}^{\nu-1} j_\alpha \Delta_\alpha \leq \sum_{\alpha=1}^{\nu-1} (n_\alpha - 1) \Delta_\alpha = \sum_{\alpha=1}^{\nu-1} (\Delta_{\alpha+1} - \Delta_\alpha) = \Delta_\nu - 1. \quad (2)$$

ПРЕДЛОЖЕНИЕ 1. *Справедлива формула*

$$j_\nu = \langle \lfloor j / \Delta_\nu \rfloor \rangle_{n_\nu}, \quad \nu \in 1 : s. \quad (3)$$

Доказательство. Согласно (1), $j = k n_1 + j_1$. Отсюда следует (3) при $\nu = 1$.

Пусть $\nu \geq 2$. Запишем

$$\frac{j}{\Delta_\nu} = \frac{1}{\Delta_\nu} \sum_{\alpha=1}^{\nu-1} j_\alpha \Delta_\alpha + j_\nu + \sum_{\alpha=\nu+1}^s j_\alpha \frac{\Delta_\alpha}{\Delta_\nu}. \quad (4)$$

В силу (2) первая сумма из правой части (4) строго меньше единицы. Остаётся проверить, что вторая сумма делится на n_ν . Но это очевидно, поскольку

$$\sum_{\alpha=\nu+1}^s j_\alpha \frac{\Delta_\alpha}{\Delta_\nu} = \sum_{\alpha=\nu+1}^s j_\alpha (n_\nu n_{\nu+1} \cdots n_{\alpha-1}).$$

Предложение доказано. □

2°. Для чисел k, j из $0 : N - 1$ введём операцию \oplus покомпонентного сложения их смешанных кодов. Запись $l = k \oplus j$ означает, что $l = (l_s, l_{s-1}, \dots, l_1)$, где $l_\nu = \langle k_\nu + j_\nu \rangle_{n_\nu}$, $\nu \in 1 : s$. В этом случае множество $0 : N - 1$ становится коммутативной группой с групповой операцией \oplus . Обозначим её G . Нейтральным элементом в G является ноль. Противоположный к $j = (j_s, j_{s-1}, \dots, j_1)$ элемент имеет вид $j' = (j'_s, j'_{s-1}, \dots, j'_1)$, где $j'_\nu = \langle n_\nu - j_\nu \rangle_{n_\nu}$, $\nu \in 1 : s$. Как обычно, $k \ominus j = k \oplus j'$. Нетрудно проверить, что

$$(k \ominus j) \oplus j = (k \oplus j) \ominus j = k. \quad (5)$$

Отметим, что при фиксированном $l \in 0 : N - 1$ отображение $j \rightarrow j \oplus l$ является перестановкой множества $\{0, 1, \dots, N - 1\}$. Доказательство основано на том, что уравнение $j \oplus l = k$ при $k \in 0 : N - 1$ имеет решение $j = k \ominus l$.

3°. Обозначим через $L(G)$ множество комплекснозначных функций на G . Это N -мерное комплексное пространство. В качестве базиса можно взять, например, систему дельта-функций $\{\delta_k\}_{k=0}^{N-1}$, где

$$\delta_k(j) = \begin{cases} 1 & \text{при } j = k, \\ 0 & \text{при } j \neq k. \end{cases}$$

Координаты функции $f \in L(G)$ относительно дельта-базиса суть её значения, так как

$$f(j) = \sum_{k=0}^{N-1} f(k) \delta_k(j), \quad j \in 0 : N - 1.$$

Пространство $L(G)$ можно сделать унитарным, введя скалярное произведение

$$\langle f, g \rangle = \sum_{j=0}^{N-1} f(j) \overline{g(j)}.$$

При таком скалярном произведении дельта-базис ортогонален.

Если в $L(G)$ ввести умножение, положив $(fg)(j) = f(j)g(j)$, то $L(G)$ станет \mathbb{C} -алгеброй.

4°. Дискретные функции Виленкина-Крестенсона (ВК-функции) принадлежат $L(G)$ и определяются следующим образом:

$$v_k(j) = \exp\left(2\pi i \sum_{\nu=1}^s \frac{k_\nu j_\nu}{n_\nu}\right) = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu}, \quad k, j \in 0 : N - 1. \quad (6)$$

Здесь $\omega_{n_\nu} = \exp(2\pi i/n_\nu)$. При $n_1 = n_2 = \dots = n_s = 2$ функции v_k называются дискретными функциями Уолша.

Исследуем свойства ВК-функций. Очевидно, что $v_0(j) \equiv 1$ и $v_k(0) = 1$ при всех $k \in 0 : N - 1$. При $k \in 1 : N - 1$ найдётся элемент $j^{(k)} \in 1 : N - 1$, на котором $v_k(j^{(k)}) \neq 1$. Действительно, если $k = (k_s, k_{s-1}, \dots, k_1)$ и $k_\nu \neq 0$, то можно взять $j^{(k)} = (j_s^{(k)}, j_{s-1}^{(k)}, \dots, j_1^{(k)})$ с $j_\nu^{(k)} = 1$ и $j_\alpha^{(k)} = 0$ при $\alpha \neq \nu$. В этом случае, согласно (6), $v_k(j^{(k)}) = \omega_{n_\nu}^{k_\nu} \neq 1$.

Далее, $v_k(j) = v_j(k)$ и

$$1/v_k(j) = \overline{v_k(j)} = v_k(j') = v_{k'}(j), \quad (7)$$

где j' и k' — элементы группы G , противоположные j и k соответственно. Проверим, например, равенство $1/v_k(j) = v_{k'}(j)$. Имеем

$$1/v_k(j) = \prod_{\nu=1}^s \omega_{n_\nu}^{(n_\nu - k_\nu)j_\nu} = \prod_{\nu=1}^s \omega_{n_\nu}^{(n_\nu - k_\nu)n_\nu j_\nu} = v_{k'}(j).$$

ПРЕДЛОЖЕНИЕ 2. При всех $k \in 0 : N - 1$ справедливы соотношения

$$|v_k(j)| \equiv 1, \quad (8)$$

$$v_k(j \oplus l) = v_k(j) v_k(l), \quad j, l \in 0 : N - 1. \quad (9)$$

Доказательство. Тождество (8) очевидно. Легко проверяется и свойство (9):

$$v_k(j \oplus l) = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu(j_\nu + l_\nu)n_\nu} = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu j_\nu n_\nu} \omega_{n_\nu}^{k_\nu l_\nu n_\nu} = v_k(j) v_k(l).$$

Предложение доказано. \square

Формулы (8), (9) свидетельствуют о том, что ВК-функции v_0, v_1, \dots, v_{N-1} являются *характерами* группы G .

ПРЕДЛОЖЕНИЕ 3. При всех $j \in 0 : N - 1$ справедливо равенство

$$v_k(j) v_l(j) = v_{k \oplus l}(j). \quad (10)$$

Доказательство. Учитывая, что $v_k(j) = v_j(k)$, согласно (9) получаем

$$v_k(j) v_l(j) = v_j(k) v_j(l) = v_j(k \oplus l) = v_{k \oplus l}(j).$$

Предложение доказано. \square

Формулы (7), (10) позволяют утверждать, что ВК-функции v_0, v_1, \dots, v_{N-1} образуют коммутативную группу по умножению. Обозначим её \hat{G} . Нейтральным элементом в \hat{G} является v_0 . Элементом, обратным к v_k , согласно (7) будет $v_{k'}$.

Таким образом, множество ВК-функций представляет собой группу характеров \hat{G} группы G . При этом $|\hat{G}| = |G| = N$.

5°. Продолжим изучение ВК-функций.

ПРЕДЛОЖЕНИЕ 4. *Справедливо равенство*

$$\frac{1}{N} \sum_{j=0}^{N-1} v_k(j) = \delta_0(k), \quad k \in 0 : N-1. \quad (11)$$

Доказательство. При $k = 0$ утверждение очевидно. Пусть $k \in 1 : N-1$. Как отмечалось в предыдущем пункте, существует элемент $j^{(k)} \in 1 : N-1$, на котором $v_k(j^{(k)}) \neq 1$. Согласно (9) имеем

$$v_k(j^{(k)}) \sum_{j=0}^{N-1} v_k(j) = \sum_{j=0}^{N-1} v_k(j \oplus j^{(k)}) = \sum_{j=0}^{N-1} v_k(j). \quad (12)$$

Последний переход основан на том, что множество $\{j \oplus j^{(k)}\}_{j=0}^{N-1}$ есть перестановка множества $\{0, 1, \dots, N-1\}$. Из (12) следует, что при $k \in 1 : N-1$

$$\sum_{j=0}^{N-1} v_k(j) = 0.$$

Это равносильно (11). Предложение доказано. \square

Поскольку $v_k(j) = v_j(k)$, то следствием (11) является формула

$$\frac{1}{N} \sum_{k=0}^{N-1} v_k(j) = \delta_0(j), \quad j \in 0 : N-1. \quad (13)$$

ПРЕДЛОЖЕНИЕ 5. *ВК-функции v_0, v_1, \dots, v_{N-1} попарно ортогональны и $\|v_k\|^2 = N$ при всех $k \in 0 : N-1$.*

Доказательство. Учитывая (7), (10) и (11), получаем

$$\langle v_k, v_l \rangle = \sum_{j=0}^{N-1} v_k(j) \overline{v_l(j)} = \sum_{j=0}^{N-1} v_{k \ominus l}(j) = N \delta_0(k \ominus l),$$

что равносильно требуемому. \square

6°. Обозначим через $L(\widehat{G})$ множество комплекснозначных функций на \widehat{G} . Введём дискретное преобразование Виленкина-Крестенсона (ВК-преобразование) $\mathcal{W}_N: L(G) \rightarrow L(\widehat{G})$. Оно сопоставляет функции $f \in L(G)$ функцию $\widehat{f} \in L(\widehat{G})$ со значениями

$$\widehat{f}(k) := \widehat{f}(v_k) = \sum_{j=0}^{N-1} f(j) \overline{v_k(j)}, \quad k \in 0 : N-1.$$

ПРЕДЛОЖЕНИЕ 6. Справедлива формула обращения

$$f(j) = \frac{1}{N} \sum_{k=0}^{N-1} \widehat{f}(k) v_k(j), \quad j \in 0 : N-1. \quad (14)$$

Доказательство. Согласно (7), (9) и (13) имеем

$$\begin{aligned} \frac{1}{N} \sum_{k=0}^{N-1} \widehat{f}(k) v_k(j) &= \frac{1}{N} \sum_{k=0}^{N-1} \left(\sum_{l=0}^{N-1} f(l) \overline{v_k(l)} \right) v_k(j) = \\ &= \sum_{l=0}^{N-1} f(l) \left\{ \frac{1}{N} \sum_{k=0}^{N-1} v_k(j \ominus l) \right\} = \sum_{l=0}^{N-1} f(l) \delta_0(j \ominus l) = f(j). \end{aligned}$$

Предложение доказано. \square

Формула (14) представляет собой разложение произвольной функции $f \in L(G)$ по ортогональному ВК-базису v_0, v_1, \dots, v_{N-1} .

7°. Конечномерное пространство $L(\widehat{G})$ состоит из функций \widehat{f} , областью определения которых является группа $\widehat{G} = \{v_0, v_1, \dots, v_{N-1}\}$. Вместо $\widehat{f}(v_k)$ мы пишем $\widehat{f}(k)$.

В пространстве $L(\widehat{G})$ можно ввести скалярное произведение и норму

$$\langle \widehat{f}, \widehat{g} \rangle = \sum_{k=0}^{N-1} \widehat{f}(k) \overline{\widehat{g}(k)}, \quad \|\widehat{f}\| = \sqrt{\langle \widehat{f}, \widehat{f} \rangle}.$$

ПРЕДЛОЖЕНИЕ 7. Пусть $\widehat{f} = \mathcal{W}_N(f)$, $\widehat{g} = \mathcal{W}_N(g)$. Тогда

$$\langle \widehat{f}, \widehat{g} \rangle = N \langle f, g \rangle. \quad (15)$$

Доказательство. Воспользуемся (14). Получим

$$\langle \widehat{f}, \widehat{g} \rangle = \sum_{k=0}^{N-1} \widehat{f}(k) \sum_{l=0}^{N-1} \overline{\widehat{g}(l)} v_k(l) =$$

$$= \sum_{l=0}^{N-1} \overline{g(l)} \sum_{k=0}^{N-1} \widehat{f}(k) v_k(l) = N \sum_{l=0}^{N-1} \overline{g(l)} f(l) = N \langle f, g \rangle.$$

Предложение доказано. \square

Из (15) следует, что

$$\|\widehat{f}\|^2 = N \|f\|^2. \quad (16)$$

Формулы (16) и (15) называются соответственно *равенством Парсеваля* и *обобщённым равенством Парсеваля*.

8°. *Свёрткой* двух функций f, g из $L(G)$ называется функция $u \in L(G)$ со значениями

$$u(j) = \sum_{l=0}^{N-1} f(l) g(j \ominus l), \quad j \in 0 : N-1.$$

ПРЕДЛОЖЕНИЕ 8. *Справедливо равенство*

$$\widehat{u}(k) = \widehat{f}(k) \widehat{g}(k), \quad k \in 0 : N-1.$$

Доказательство. Имеем

$$\begin{aligned} \widehat{u}(k) &= \sum_{j=0}^{N-1} \left(\sum_{l=0}^{N-1} f(l) g(j \ominus l) \right) \overline{v_k((j \ominus l) \oplus l)} = \\ &= \sum_{l=0}^{N-1} f(l) \overline{v_k(l)} \sum_{j=0}^{N-1} g(j \ominus l) \overline{v_k(j \ominus l)} = \widehat{f}(k) \widehat{g}(k). \end{aligned}$$

Предложение доказано. \square

9°. Обозначим через W_N матрицу ВК-преобразования

$$W_N[k, j] = v_k(j), \quad k, j \in 0 : N-1,$$

и через F_N — матрицу Фурье

$$F_N[k, j] = \omega_N^{kj}, \quad k, j \in 0 : N-1.$$

Напомним, что $N = n_1 n_2 \cdots n_s$.

ПРЕДЛОЖЕНИЕ 9. *Справедлива формула*

$$W_N = F_{n_s} \otimes F_{n_{s-1}} \otimes \cdots \otimes F_{n_1},$$

где \otimes — знак кронекерова умножения матриц.

Доказательство. Как известно, элемент с индексами $k = (k_s, k_{s-1}, \dots, k_1)$, $j = (j_s, j_{s-1}, \dots, j_1)$ кронекерова произведения квадратных матриц $A_{n_s}, A_{n_{s-1}}, \dots, A_{n_1}$ порядков n_s, n_{s-1}, \dots, n_1 соответственно допускает представление

$$(A_{n_s} \otimes A_{n_{s-1}} \otimes \dots \otimes A_{n_1}) \left[\sum_{\nu=1}^s k_\nu \Delta_\nu, \sum_{\nu=1}^s j_\nu \Delta_\nu \right] = \prod_{\nu=1}^s A_{n_\nu}[k_\nu, j_\nu].$$

Пользуясь этим, получаем

$$(F_{n_s} \otimes F_{n_{s-1}} \otimes \dots \otimes F_{n_1})[k, j] = \prod_{\nu=1}^s F_{n_\nu}[k_\nu, j_\nu] = \prod_{\nu=1}^s \omega_N^{k_\nu j_\nu} = v_k(j) = W_N[k, j].$$

Предложение доказано. \square

10°. Вернёмся к определению (6) ВК-функций. С учётом (3) его можно переписать так:

$$v_k(j) = \prod_{\nu=1}^s \omega_{n_\nu}^{k_\nu \lfloor j/\Delta_\nu \rfloor} = \exp \left(2\pi i \sum_{\nu=1}^s \frac{k_\nu}{n_\nu} \left\lfloor \frac{j}{\Delta_\nu} \right\rfloor \right).$$

Обозначим

$$\theta_k(j) = \sum_{\nu=1}^s \frac{k_\nu}{n_\nu} \left\lfloor \frac{j}{\Delta_\nu} \right\rfloor.$$

Тогда

$$v_k(j) = \exp(2\pi i \theta_k(j)), \quad j \in 0 : N - 1. \quad (17)$$

Зафиксируем $k \in 0 : N - 1$. Числу $v_k(j)$ соответствует точка на единичной окружности комплексной плоскости. Когда j возрастает от 0 до $N - 1$, точка $v_k(j)$ движется по единичной окружности против часовой стрелки от положения $v_k(0)$ до $v_k(N - 1)$. Замкнём это движение, положив $v_k(N) = v_k(0) = 1$. Отметим, что формула (17) остаётся справедливой и при $j = N$, поскольку

$$\theta_k(N) = \sum_{\nu=1}^s \frac{k_\nu}{n_\nu} \left\lfloor \frac{\Delta_\nu n_\nu N_\nu}{\Delta_\nu} \right\rfloor = \sum_{\nu=1}^s k_\nu N_\nu =: \text{rev}(k).$$

Таким образом, когда j увеличивается от 0 до N , функция $\theta_k(j)$ возрастает от $\theta_k(0) = 0$ до $\theta_k(N) = \text{rev}(k)$. За это время точка $v_k(j)$ обегает единичную окружность комплексной плоскости $\text{rev}(k)$ раз. Число $\text{rev}(k)$ естественно принять за частоту функции v_k .

11°. Разберёмся с величиной $\text{rev}(k)$. По определению

$$\text{rev}(k) = k_1 (n_2 n_3 \cdots n_s) + k_2 (n_3 \cdots n_s) + \cdots + k_{s-1} n_s + k_s.$$

Это значит, что $\text{rev}(k)$ есть число из множества $0 : N - 1$ со смешанным кодом (k_1, k_2, \dots, k_s) при условии, что для N используется представление $N = n_s n_{s-1} \cdots n_1$ (в отличие от $N = n_1 n_2 \cdots n_s$). Ясно, что $\text{rev}(\text{rev}(k)) = k$. Отсюда, в частности, следует, что отображение $k \rightarrow \text{rev}(k)$ является перестановкой множества $\{0, 1, \dots, N - 1\}$.

Упорядочим ВК-функции по частоте, положив $w_k = v_{\text{rev}(k)}$. Функция w_k имеет частоту k . Перепишем формулу (14) в виде

$$f = \frac{1}{N} \sum_{k=0}^{N-1} \hat{f}(\text{rev}(k)) v_{\text{rev}(k)} = \frac{1}{N} \sum_{k=0}^{N-1} \hat{f}(\text{rev}(k)) w_k.$$

Получили разложение произвольной функции $f \in L(G)$ по ВК-базису, упорядоченному по частоте.

12°. Детальному изучению ВК-функций при $n_1 = n_2 = \cdots = n_s =: n$ посвящена работа [1].

ЛИТЕРАТУРА

1. Малозёмов В. Н., Машарский С. М. *Обобщённые вейвлетные базисы, связанные с дискретным преобразованием Виленкина-Крестенсона* // Алгебра и анализ. 2001. Т. 13. Вып. 1. С. 111–157.

ОБ УНИТАРНЫХ МАТРИЦАХ И СИНГУЛЯРНЫХ РАЗЛОЖЕНИЯХ

В. Н. Малозёмов

Н. А. Соловьёва

30 января 2008 г.

Пусть n — натуральное число, $N = 1 : n$ и $E = E[N, N]$ — единичная матрица. Напомним, что матрица $U = U[N, N]$ с комплексными элементами называется унитарной, если

$$U^*U = UU^* = E.$$

Приводимое ниже утверждение потребовалось в теории конечномерных фреймов.

ПРЕДЛОЖЕНИЕ. *Рассмотрим две системы $\{a_k\}_{k=1}^m$ и $\{b_k\}_{k=1}^m$ векторов из \mathbb{C}^n . Для того чтобы существовала унитарная матрица U , такая, что*

$$a_k = U b_k, \quad k \in 1 : m,$$

необходимо и достаточно, чтобы выполнялось условие

$$\langle a_k, a_s \rangle = \langle b_k, b_s \rangle \quad \text{при всех } k, s \in 1 : m. \quad (1)$$

Доказательство. Необходимость очевидна.

Достаточность. Введём матрицы A и B со столбцами a_1, \dots, a_m и b_1, \dots, b_m соответственно. Тогда условие (1) можно переписать в виде

$$A^*A = B^*B =: D.$$

Требуется доказать, что существует унитарная матрица U , такая, что $A = UB$.

Обозначим через r ранг матрицы D . Такой же ранг имеют матрицы A и B . Если $r = 0$, то матрицы A и B — нулевые. В этом случае в качестве U можно взять любую унитарную матрицу.

Пусть $r \geq 1$. Обозначим $M = 1 : m$, $R = 1 : r$. Матрица $D = D[M, M]$ — эрмитова. Кроме того, она неотрицательно определена. Значит, для D существует представление

$$D = \sum_{k=1}^m \lambda_k \varphi_k \varphi_k^*, \quad (2)$$

в котором $\varphi_1, \dots, \varphi_m$ — ортонормированные собственные векторы и $\lambda_1, \dots, \lambda_m$ — неотрицательные собственные числа, среди которых r положительных. Обозначим $\vartheta_k = \sqrt{\lambda_k}$ и упорядочим ϑ_k по убыванию:

$$\vartheta_1 \geq \vartheta_2 \geq \dots \geq \vartheta_r > 0 = \vartheta_{r+1} = \dots = \vartheta_m.$$

Убрав из правой части (2) нулевые слагаемые, получим

$$D = \sum_{k=1}^r \vartheta_k^2 \varphi_k \varphi_k^*. \quad (3)$$

Введём унитарную матрицу $\Phi[M, M]$ со столбцами $\varphi_1, \dots, \varphi_m$ и диагональную матрицу $\Theta[R, R]$ с положительными диагональными элементами $\Theta[i, i] = \vartheta_i$, $i \in 1 : r$. С помощью матриц Φ и Θ формулу (3) можно переписать так:

$$D[M, M] = \Phi[M, R] \times \Theta^2[R, R] \times \Phi^*[R, M]. \quad (4)$$

Умножим обе части последнего равенства справа на $\Phi[M, R] \times \Theta^{-1}[R, R]$. Учитывая, что $D = A^*A$, получаем

$$A^*[M, N] \times A[N, M] \times \Phi[M, R] \times \Theta^{-1}[R, R] = \Phi[M, R] \times \Theta[R, R].$$

Обозначив

$$\Psi[N, R] = A[N, M] \times \Phi[M, R] \times \Theta^{-1}[R, R],$$

придём к формуле

$$A^*[M, N] \times \Psi[N, R] = \Phi[M, R] \times \Theta[R, R]. \quad (5)$$

Добавим к матрице $\Theta[R, R]$ нулевой блок $\Theta[M \setminus R, R]$. С помощью расширенной матрицы $\Theta[M, R]$ равенству (5) можно придать следующий вид:

$$A^*[M, N] \times \Psi[N, R] = \Phi[M, M] \times \Theta[M, R]. \quad (6)$$

Покажем, что столбцы ψ_1, \dots, ψ_r матрицы $\Psi[N, R]$ ортонормированные. Согласно (4) имеем

$$\begin{aligned} \Psi^*[R, N] \times \Psi[N, R] &= \Theta^{-1}[R, R] \times \Phi^*[R, M] \times (A^*[M, N] \times A[N, M]) \times \\ &\times \Phi[M, R] \times \Theta^{-1}[R, R] = \Theta^{-1}[R, R] \times (\Phi^*[R, M] \times \Phi[M, R]) \times \Theta^2[R, R] \times \\ &\times (\Phi^*[R, M] \times \Phi[M, R]) \times \Theta^{-1}[R, R] = E[R, R], \end{aligned}$$

что и требовалось установить.

Расширим матрицу $\Psi[N, R]$ с ортонормированными столбцами ψ_1, \dots, ψ_r до унитарной. Для этого прежде всего отметим, что векторы ψ_k являются собственными векторами матрицы AA^* . Действительно, согласно (5)

$$\begin{aligned} A[N, M] \times A^*[M, N] \times \Psi[N, R] &= A[N, M] \times \Phi[M, R] \times \Theta[R, R] = \\ &= \Psi[N, R] \times \Theta^2[R, R]. \end{aligned}$$

Получили, что

$$(AA^*)\psi_k = \vartheta_k^2 \psi_k, \quad k \in 1:r. \quad (7)$$

Теперь рассмотрим подпространство $\mathcal{L} = \{x \mid A^*x = \mathbb{O}\}$. Поскольку $\text{rang } A^* = r$, то размерность \mathcal{L} равна $n - r$. Возьмём в \mathcal{L} ортонормированный базис $\psi_{r+1}, \dots, \psi_n$. Отметим, что

$$\langle \psi_k, \psi_s \rangle = 0 \quad \text{при} \quad k \in 1:r, \quad s \in r+1:n.$$

Действительно, согласно (7)

$$\langle \psi_k, \psi_s \rangle = \vartheta_k^{-2} \langle AA^* \psi_k, \psi_s \rangle = \vartheta_k^{-2} \langle A^* \psi_k, A^* \psi_s \rangle = 0.$$

Дополнив матрицу $\Psi[N, R]$ столбцами $\psi_{r+1}, \dots, \psi_n$, получим унитарную матрицу $\Psi[N, N]$.

Вернёмся к базовой формуле (6). Дополним матрицу $\Theta[M, R]$ нулевым блоком $\Theta[M, N \setminus R]$. Придём к равенству

$$A^*[M, N] \times \Psi[N, N] = \Phi[M, M] \times \Theta[M, N].$$

Из него следует, что

$$A^*[M, N] = \Phi[M, M] \times \Theta[M, N] \times \Psi^*[N, N].$$

После перехода к сопряжённым матрицам получим разложение

$$A[N, M] = \Psi[N, N] \times \Theta^*[N, M] \times \Phi^*[M, M]. \quad (8)$$

В этом разложении матрицы Φ и Θ зависят только от D , а матрица Ψ — от A и D . Отметим также, что матрица $\Theta^*[N, M]$ имеет ровно r ненулевых элементов $\Theta^*[k, k] = \vartheta_k$, $k \in 1:r$. Остальные элементы равны нулю.

Формула (8) является следствием равенства $D = A^*A$. Равенство $D = B^*B$ аналогичным образом приводит к разложению

$$B[N, M] = \Psi_0[N, N] \times \Theta^*[N, M] \times \Phi^*[N, N], \quad (9)$$

в котором матрицы Φ^* и Θ^* такие же, как в (8). На основании (8) и (9) получаем

$$A[N, M] = \Psi[N, N] \times \Psi_0^*[N, N] \times B[N, M].$$

Матрица $U = \Psi \Psi_0^*$ — унитарная. Она обеспечивает требуемое равенство $A = UB$. Предложение доказано. \square

СЛЕДСТВИЕ. Если a, b — векторы из \mathbb{C}^n с одинаковыми нормами, то существует унитарная матрица U , такая, что

$$a = U b.$$

ЗАМЕЧАНИЯ.

- 1) По ходу доказательства предложения было, по существу, установлено, что векторы $\psi_1, \dots, \psi_r, \psi_{r+1}, \dots, \psi_n$ являются собственными векторами матрицы AA^* , соответствующими собственным числам

$$\vartheta_1^2 \geq \vartheta_2^2 \geq \dots \geq \vartheta_r^2 > 0 = \vartheta_{r+1}^2 = \dots = \vartheta_n^2.$$

- 2) Формула (8) называется сингулярным разложением матрицы A . При выводе этой формулы мы следовали рассуждениям из [1, с. 55–59].

ЛИТЕРАТУРА

1. Малозёмов В. Н. *Линейная алгебра без определителей. Квадратичная функция*. СПб.: Изд-во СПбГУ, 1997. 80 с.

СИСТЕМ МЕРСЕДЕС-БЕНЦ ПРИ $m > n + 1$ НЕ СУЩЕСТВУЕТ

В. Н. Малозёмов А. Б. Певный

13 февраля 2008 г.

Напомним [1], что система единичных векторов $\{\varphi_1, \dots, \varphi_m\}$ из \mathbb{R}^n при $m = n + 1$ является жёстким фреймом тогда и только тогда, когда выполняется условие

$$|\langle \varphi_k, \varphi_s \rangle| = \frac{1}{n} \quad \text{при } k \neq s.$$

Если $\langle \varphi_k, \varphi_s \rangle = -\frac{1}{n}$ при $k \neq s$, то такой жёсткий фрейм называется системой Мерседес-Бенц [2].

Попытка обобщить понятие системы Мерседес-Бенц приводит к следующему определению: *набор единичных векторов $\{\varphi_1, \dots, \varphi_m\}$ из \mathbb{R}^n при $m \geq n + 1$ называется системой Мерседес-Бенц, если*

- (i) *этот набор является жёстким фреймом,*
- (ii) *$\langle \varphi_k, \varphi_s \rangle = c$ при $k \neq s$, где c — фиксированное число, $c \neq 0$.*

Оказывается, что случай $m = n + 1$ — уникальный.

ТЕОРЕМА. *При $n \geq 2$ и $m > n + 1$ систем Мерседес-Бенц не существует.*

Доказательство проведём от противного. Допустим, что существует набор единичных n -мерных векторов $\{\varphi_1, \dots, \varphi_m\}$, удовлетворяющий условиям (i), (ii). Обозначим через Φ матрицу со столбцами $\varphi_1, \dots, \varphi_m$. В силу (i)

$$\Phi \Phi^T = \frac{m}{n} I_n. \quad (1)$$

Как известно (см., например, [3]), симметричные матрицы $\Phi \Phi^T$ и $\Phi^T \Phi$ порядков n и m соответственно имеют одинаковый набор ненулевых собственных чисел. Согласно (1) у матрицы $\Phi \Phi^T$ одно собственное число $\lambda_1 = m/n$ кратности n . Значит, у матрицы $\Phi^T \Phi$ два собственных числа: $\lambda_1 = m/n$ кратности n и $\lambda_2 = 0$ кратности $m - n$. Учитывая условия $n \geq 2$, $m > n + 1$, приходим к

следующему выводу: матрица $\Phi^T \Phi$ имеет два различных собственных числа, кратности которых не меньше двух.

Теперь отметим, что в силу (ii) матрица $\Phi^T \Phi$ имеет простую структуру: у неё на главной диагонали стоят единицы, а остальные элементы равны c . У такой матрицы два собственных числа: $\lambda'_1 = 1 - c$ кратности $m - 1$ и $\lambda'_2 = 1 + (m - 1)c$ кратности один. Чтобы пояснить это, запишем матрицу $\Phi^T \Phi$ и матрицу P , столбцами которой являются собственные векторы матрицы $\Phi^T \Phi$, при $m = 4$:

$$\Phi^T \Phi = \begin{bmatrix} 1 & c & c & c \\ c & 1 & c & c \\ c & c & 1 & c \\ c & c & c & 1 \end{bmatrix}, \quad P = \begin{bmatrix} -1 & -1 & -1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Поскольку $c \neq 0$, то $\lambda'_1 \neq \lambda'_2$. Значит, матрица $\Phi^T \Phi$ имеет два различных собственных числа, причём кратность одного из них равна единице. Это противоречит выводу, сделанному ранее.

Теорема доказана. \square

З а м е ч а н и е. При $m = n + 1$ противоречия не будет. Два способа нахождения собственных чисел матрицы $\Phi^T \Phi$ приводят к одинаковому результату: у матрицы $\Phi^T \Phi$ два собственных числа $\lambda_1 = 1 + \frac{1}{n}$ кратности n и $\lambda_2 = 0$ кратности один. При этом $c = -\frac{1}{n}$.

ЛИТЕРАТУРА

1. Малозёмов В. Н., Певный А. Б. *Четвёртое определение жёсткого фрейма* // Семинар «DHA & CAGD». Избранные доклады. 30 мая 2007 г. (<http://dha.spb.ru/rep07.shtml#0530>).
2. Малозёмов В. Н., Певный А. Б. *Системы Мерседес-Бенц и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 28 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0228>).
3. Малозёмов В. Н., Соловьёва Н. А. *Об унитарных матрицах и сингулярных разложениях* // Семинар «DHA & CAGD». Избранные доклады. 30 января 2008 г. (<http://dha.spb.ru/rep08.shtml#0130>).

О ЖЁСТКИХ ФРЕЙМАХ СПЕЦИАЛЬНОГО ВИДА

Н. А. Соловьёва

12 марта 2008 г.

В докладе приводится короткое доказательство одного эффектного результата из [1].

Пусть $m > n > 1$. Возьмём унитарную матрицу U порядка n , единичный вектор $\varphi_0 \in \mathbb{C}^n$ и построим последовательность единичных векторов

$$\varphi_k = U\varphi_{k-1}, \quad k = 1, \dots, m-1. \quad (1)$$

Обозначим $\Phi = \{\varphi_0, \varphi_1, \dots, \varphi_{m-1}\}$.

ПРЕДЛОЖЕНИЕ. Если система Φ образует жёсткий фрейм, то найдётся число $c \in \mathbb{C}$, $|c| = 1$, такое, что

$$U^m = c I_n.$$

Доказательство. Разложим векторы φ_{m-1} и $U\varphi_{m-1}$ по фрейму Φ . По определению жёсткого фрейма [2]

$$\begin{aligned} \varphi_{m-1} &= \frac{n}{m} \left(\sum_{k=0}^{m-2} \langle \varphi_{m-1}, \varphi_k \rangle \varphi_k + \varphi_{m-1} \right), \\ U\varphi_{m-1} &= \frac{n}{m} \left(\langle U\varphi_{m-1}, \varphi_0 \rangle \varphi_0 + \sum_{k=1}^{m-1} \langle \varphi_{m-1}, U^* \varphi_k \rangle \varphi_k \right). \end{aligned} \quad (2)$$

Приняв во внимание, что $U^* \varphi_k = U^* U \varphi_{k-1} = \varphi_{k-1}$ при $k \in 1 : m-1$, перепишем последнее равенство в виде

$$\begin{aligned} U\varphi_{m-1} &= \frac{n}{m} \left(\langle U\varphi_{m-1}, \varphi_0 \rangle U U^* \varphi_0 + \sum_{k=1}^{m-1} \langle \varphi_{m-1}, \varphi_{k-1} \rangle U \varphi_{k-1} \right) = \\ &= \frac{n}{m} U \left(\langle U\varphi_{m-1}, \varphi_0 \rangle U^* \varphi_0 + \sum_{k=1}^{m-1} \langle \varphi_{m-1}, \varphi_{k-1} \rangle \varphi_{k-1} \right). \end{aligned}$$

Отсюда следует, что

$$\varphi_{m-1} = \frac{n}{m} \left(\langle U\varphi_{m-1}, \varphi_0 \rangle U^* \varphi_0 + \sum_{k=1}^{m-1} \langle \varphi_{m-1}, \varphi_{k-1} \rangle \varphi_{k-1} \right). \quad (3)$$

Вычтем (3) из (2). После сокращения на общий множитель получим

$$\varphi_{m-1} = \langle U\varphi_{m-1}, \varphi_0 \rangle U^* \varphi_0$$

и

$$U^m \varphi_0 = \langle U\varphi_{m-1}, \varphi_0 \rangle \varphi_0. \quad (4)$$

Обозначим $c = \langle U\varphi_{m-1}, \varphi_0 \rangle = \langle U^m \varphi_0, \varphi_0 \rangle$. Тогда формула (4) примет вид

$$U^m \varphi_0 = c \varphi_0. \quad (5)$$

Равенство норм $\|c \varphi_0\| = \|U^m \varphi_0\| = \|\varphi_0\|$ гарантирует, что $|c| = 1$.

Далее, согласно (1) и (5)

$$U^m \varphi_k = U^m (U^k \varphi_0) = U^k (U^m \varphi_0) = c \varphi_k.$$

Значит,

$$(U^m - c I_n) \varphi_k = \mathbb{O} \quad \text{при } k = 0, 1, \dots, m-1.$$

Напомним, что линейная оболочка элементов жёсткого фрейма совпадает с \mathbb{C}^n , поэтому равенство $(U^m - c I_n) x = \mathbb{O}$ выполняется для всех $x \in \mathbb{C}^n$. Взяв в качестве x последовательно все единичные орты, придём к требуемой формуле $U^m = c I_n$. Предложение доказано. \square

З а м е ч а н и е. Гармонические фреймы можно представить в виде (1). Для этого достаточно положить $\varphi_0(j) = \frac{1}{\sqrt{n}}$ при всех $j \in 1 : n$ и

$$U = \text{diag}(w_1, \dots, w_n),$$

где w_j — попарно различные корни степени m из единицы. Для гармонических фреймов предложение тривиально, причём $c = 1$.

ЛИТЕРАТУРА

1. Casazza P. G., Kovačević J. *Uniform Tight Frames with Erasures* // Adv. Comput. Math. 2003. V. 18. No. 2–4. P. 387–430.
2. Малозёмов В. Н., Певный А. Б. *Системы Мерседес-Бенц и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 28 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0228>).

СОСТАВНЫЕ И ОБОБЩЁННЫЕ ПОВЕРХНОСТИ КУНСА

Н. В. Чашников

15 марта 2008 г.

В докладе введено понятие обобщённой поверхности Кунса, частными случаями которой являются билинейные и бикубические поверхности Кунса [1, 2], а также поверхности Гордона [3]. Показано, что и составные поверхности Кунса [4] можно представить как частный случай обобщённых.

1°. Напомним определение параметрической поверхности Кунса. Воспользуемся следующими обозначениями из [2]:

L_1, L_2, L_3, L_4 — линейные операторы, определяемые для непрерывно дифференцируемых вектор-функций $f: [0, 1] \rightarrow \mathbb{R}^3$ формулами

$$L_1(f) = f(0), \quad L_2(f) = f'(0), \quad L_3(f) = f'(1), \quad L_4(f) = f(1); \quad (1)$$

H_1, H_2, H_3, H_4 — непрерывно дифференцируемые на отрезке $[0, 1]$ функции, удовлетворяющие соотношениям

$$\begin{aligned} H_1(0) &= 1, & H_1'(0) &= 0, & H_1'(1) &= 0, & H_1(1) &= 0; \\ H_2(0) &= 0, & H_2'(0) &= 1, & H_2'(1) &= 0, & H_2(1) &= 0; \\ H_3(0) &= 0, & H_3'(0) &= 0, & H_3'(1) &= 1, & H_3(1) &= 0; \\ H_4(0) &= 0, & H_4'(0) &= 0, & H_4'(1) &= 0, & H_4(1) &= 1. \end{aligned} \quad (2)$$

В качестве H_i можно взять, например, кубические полиномы Эрмита

$$\begin{aligned} H_1(x) &= 2x^3 - 3x^2 + 1, \\ H_2(x) &= x^3 - 2x^2 + x, \\ H_3(x) &= x^3 - x^2, \\ H_4(x) &= -2x^3 + 3x^2. \end{aligned} \quad (3)$$

В [2] доказано, что если вектор-функции $f_i, g_i: [0, 1] \rightarrow \mathbb{R}^3$, $i \in 1 : 4$, удовлетворяют условиям

$$L_j(f_i) = L_i(g_j), \quad i, j \in 1 : 4,$$

то для поверхности, задаваемой вектор-функцией

$$c(u, v) = \sum_{i=1}^4 H_i(u) f_i(v) + \sum_{j=1}^4 H_j(v) g_j(u) - \sum_{i=1}^4 \sum_{j=1}^4 H_i(u) H_j(v) L_i(g_j), \quad (4)$$

выполняются равенства

$$\begin{aligned} L_i(c(\cdot, v)) &= f_i(v), & v \in [0, 1], & \quad i \in 1 : 4; \\ L_j(c(u, \cdot)) &= g_j(u), & u \in [0, 1], & \quad j \in 1 : 4. \end{aligned}$$

2°. Вместо операторов вида (1) можно использовать и другие наборы операторов. Кроме того, наборы операторов для переменных u и v могут быть различными.

Пусть D_u — непустое множество, T_u — некоторое линейное пространство, элементами которого являются вещественные функции над D_u . Кроме того, пусть задан набор линейных функционалов $L_1^u, \dots, L_m^u : T_u \rightarrow \mathbb{R}$ и набор функций $H_1^u, \dots, H_m^u \in T_u$, удовлетворяющих соотношениям

$$L_i^u(H_j^u) = \delta_{ij}, \quad i, j \in 1 : m. \quad (5)$$

Аналогично, пусть задано непустое множество D_v , линейное пространство T_v , состоящее из вещественных функций над D_v , набор линейных функционалов $L_1^v, \dots, L_n^v : T_v \rightarrow \mathbb{R}$ и набор функций $H_1^v, \dots, H_n^v \in T_v$, удовлетворяющих соотношениям

$$L_i^v(H_j^v) = \delta_{ij}, \quad i, j \in 1 : n. \quad (6)$$

Пусть s — натуральное число. Определим множества вектор-функций, координатные функции которых принадлежат T_u и T_v :

$$\begin{aligned} \vec{T}_u &= \{g : D_u \rightarrow \mathbb{R}^s \mid g(u) = (g_1(u), \dots, g_s(u)), \quad g_k \in T_u\}, \\ \vec{T}_v &= \{f : D_v \rightarrow \mathbb{R}^s \mid f(v) = (f_1(v), \dots, f_s(v)), \quad f_k \in T_v\}. \end{aligned}$$

Введём линейные операторы

$$\begin{aligned} \vec{L}_i^u(g) &= (L_i^u(g_1), \dots, L_i^u(g_s)) \quad \text{для} \quad g(u) = (g_1(u), \dots, g_s(u)) \in \vec{T}_u, \quad i \in 1 : m; \\ \vec{L}_j^v(f) &= (L_j^v(f_1), \dots, L_j^v(f_s)) \quad \text{для} \quad f(v) = (f_1(v), \dots, f_s(v)) \in \vec{T}_v, \quad j \in 1 : n. \end{aligned}$$

Из соотношений (5) и (6) следуют тождества

$$\begin{aligned} \vec{L}_i^u(aH_j^u) &= a\delta_{ij}, & a \in \mathbb{R}^s, \quad i, j \in 1 : m; \\ \vec{L}_j^v(aH_i^v) &= a\delta_{ij}, & a \in \mathbb{R}^s, \quad i, j \in 1 : n. \end{aligned} \quad (7)$$

Пусть заданы наборы опорных вектор-функций

$$f_1, \dots, f_m \in \vec{T}_v, \quad g_1, \dots, g_n \in \vec{T}_u,$$

удовлетворяющие условиям согласования

$$\vec{L}_i^u(g_j) = \vec{L}_j^v(f_i), \quad i \in 1 : m, \quad j \in 1 : n. \quad (8)$$

Определим вектор-функцию $c: D_u \times D_v \rightarrow \mathbb{R}^s$:

$$c(u, v) = \sum_{i=1}^m H_i^u(u) f_i(v) + \sum_{j=1}^n H_j^v(v) g_j(u) - \sum_{i=1}^m \sum_{j=1}^n H_i^u(u) H_j^v(v) \vec{L}_i^u(g_j). \quad (9)$$

Поверхность, определяемую вектор-функцией $c(u, v)$, назовём *обобщённой поверхностью Кунса*.

ПРЕДЛОЖЕНИЕ 1. Вектор-функция $c(u, v)$, задаваемая формулой (9), удовлетворяет условиям

$$\begin{aligned} \vec{L}_i^u(c(\cdot, v)) &= f_i(v), \quad i \in 1 : m, \quad v \in D_v, \\ \vec{L}_j^v(c(u, \cdot)) &= g_j(u), \quad j \in 1 : n, \quad u \in D_u. \end{aligned} \quad (10)$$

Доказательство. Согласно линейности операторов \vec{L}_k^u и формулам (7) при $k \in 1 : m$ имеем

$$\begin{aligned} \vec{L}_k^u(c(\cdot, v)) &= \sum_{i=1}^m \vec{L}_k^u(f_i(v) H_i^u) + \sum_{j=1}^n H_j^v(v) \vec{L}_k^u(g_j) - \\ &- \sum_{i=1}^m \sum_{j=1}^n \vec{L}_k^u(\vec{L}_i^u(g_j) H_j^v(v) H_i^u) = \sum_{i=1}^m f_i(v) \delta_{ik} + \sum_{j=1}^n H_j^v(v) \vec{L}_k^u(g_j) - \\ &- \sum_{i=1}^m \sum_{j=1}^n \vec{L}_i^u(g_j) H_j^v(v) \delta_{ik} = f_k(v). \end{aligned}$$

Аналогично с учётом (8) при $k \in 1 : n$ получаем

$$\begin{aligned} \vec{L}_k^v(c(u, \cdot)) &= \sum_{i=1}^m H_i^u(u) \vec{L}_k^v(f_i) + \sum_{j=1}^n \vec{L}_k^v(g_j(u) H_j^v) - \\ &- \sum_{i=1}^m \sum_{j=1}^n \vec{L}_k^v(\vec{L}_j^v(f_i) H_i^u(u) H_j^v) = \sum_{i=1}^m H_i^u(u) \vec{L}_k^v(f_i) + \sum_{j=1}^n g_j(u) \delta_{jk} - \\ &- \sum_{i=1}^m \sum_{j=1}^n \vec{L}_j^v(f_i) H_i^u(u) \delta_{jk} = g_k(u). \end{aligned}$$

Предложение доказано. □

3°. Рассмотрим некоторые частные случаи введённых обобщённых поверхностей Кунса.

В первых двух случаях пространства и функционалы для переменных u и v будут совпадать, то есть $D_v = D_u = D$, $T_v = T_u = T$, $n = m$, $L_i^v = L_i^u = L_i$, $H_i^v = H_i^u = H_i$. Во всех случаях $s = 3$.

1) $D = [0, 1]$, $T = C(D)$, $m = 2$,

$$\begin{aligned} L_1(f) &= f(0), & L_2(f) &= f(1), \\ H_1(x) &= 1 - x, & H_2(x) &= x. \end{aligned}$$

В данном случае при соблюдении условий (8) обобщённая поверхность Кунса совпадает с билинейной поверхностью Кунса (см. [1]).

2) $D = [0, 1]$, $T = C^1(D)$, $m = 4$,

$$\begin{aligned} L_1(f) &= f(0), & L_2(f) &= f'(0), & L_3(f) &= f'(1), & L_4(f) &= f(1), \\ H_1(x) &= 2x^3 - 3x^2 + 1, & H_2(x) &= x^3 - 2x^2 + x, \\ H_3(x) &= x^3 - x^2, & H_4(x) &= -2x^3 + 3x^2. \end{aligned}$$

В этом случае при соблюдении условий (8) получаем бикубическую поверхность Кунса (см. [2]).

3) $D_u = [a, b]$, $D_v = [c, d]$; $a \leq u_1 < \dots < u_m \leq b$, $c \leq v_1 < \dots < v_n \leq d$;

$$\begin{aligned} T_u &= C(D_u), & T_v &= C(D_v); & L_i^u(g) &= g(u_i), & L_j^v(f) &= f(v_j); \\ H_i^u(u) &= \prod_{k \neq i} \frac{u - u_k}{u_i - u_k}, & i &\in 1 : m; & H_j^v(v) &= \prod_{k \neq j} \frac{v - v_k}{v_j - v_k}, & j &\in 1 : n. \end{aligned}$$

В этом случае при соблюдении условий (8) обобщённая поверхность Кунса является поверхностью Гордона (см. [3, с. 410–412]).

4°. Перейдём к рассмотрению составных поверхностей Кунса.

Пусть заданы два набора кривых

$$a_i : [0, n] \rightarrow \mathbb{R}^3, \quad i \in 0 : m, \quad b_j : [0, m] \rightarrow \mathbb{R}^3, \quad j \in 0 : n,$$

причём $a_i \in C^1([0, n])$, $b_j \in C^1([0, m])$, и выполняются условия

$$a_i(j) = b_j(i), \quad i \in 0 : m, \quad j \in 0 : n.$$

Кроме того, пусть заданы векторы $d_{ij} \in \mathbb{R}^3$, $i \in 0 : m$, $j \in 0 : n$.

В [4] показано, как при помощи параметрических поверхностей Кунса построить составную поверхность Кунса, натянутую на кривые a_i и b_j . Для этого определяются наборы кривых $\{A_i\}_{i=0}^m$, $\{B_j\}_{j=0}^n$, исходя из условий

$$\begin{aligned} A_i(j) &= b'_j(i), & A'_i(j) &= d_{ij}, \\ B_j(i) &= a'_i(j), & B'_j(i) &= d_{ij}. \end{aligned}$$

Будем считать, что исходными данными являются наборы вектор-функций a_i , b_j , A_i , B_j , удовлетворяющие условиям

$$\begin{aligned} a_i(j) &= b_j(i), & A'_i(j) &= B'_j(i), \\ a'_i(j) &= B_j(i), & b'_j(i) &= A_i(j). \end{aligned} \quad (11)$$

Для фиксированных $i \in 0 : m - 1$, $j \in 0 : n - 1$ и $u, v \in [0, 1]$ задаются граничные кривые

$$\begin{aligned} f_1(v) &= a_i(j + v), & f_2(v) &= A_i(j + v), \\ f_3(v) &= A_{i+1}(j + v), & f_4(v) &= a_{i+1}(j + v), \\ g_1(u) &= b_j(i + u), & g_2(u) &= B_j(i + u), \\ g_3(u) &= B_{j+1}(i + u), & g_4(u) &= b_{j+1}(i + u). \end{aligned} \quad (12)$$

Для этих кривых по формуле (4) строится параметрическая поверхность Кунса $c^{ij}(u, v)$. Составная поверхность Кунса задаётся формулой

$$s(\alpha, \beta) = c^{ij}(\alpha - i, \beta - j), \quad (13)$$

где $\alpha \in [i, i + 1]$, $\beta \in [j, j + 1]$, $i \in 0 : m - 1$, $j \in 0 : n - 1$. В [4] доказано, что для поверхности, определяемой вектор-функцией $s(\alpha, \beta)$, выполняются условия

$$\begin{aligned} s &\in C^1, & s_{\alpha\beta}, s_{\beta\alpha} &\in C; \\ s(i, \beta) &= a_i(\beta), & s_\alpha(i, \beta) &= A_i(\beta), & i \in 0 : m, & \beta \in [0, n]; \\ s(\alpha, j) &= b_j(\alpha), & s_\beta(\alpha, j) &= B_j(\alpha), & j \in 0 : n, & \alpha \in [0, m]. \end{aligned} \quad (14)$$

5°. Покажем, как для вектор-функций a_i , b_j , A_i , B_j , удовлетворяющих условиям (11), построить обобщённую поверхность Кунса, для которой будут выполнены условия (14).

Пусть $T_u = C^1[0, m]$, $T_v = C^1[0, n]$. Определим функционалы L_i^u , L_j^v и вектор-функции f_i , g_j таким образом, чтобы условия (10) соответствовали (14):

$$\begin{aligned} L_{2i}^u(g) &= g(i), & L_{2i+1}^u(g) &= g'(i), & f_{2i} &= a_i, & f_{2i+1} &= A_i, & \text{для } i \in 0 : m; \\ L_{2j}^v(f) &= f(j), & L_{2j+1}^v(f) &= f'(j), & g_{2j} &= b_j, & g_{2j+1} &= B_j, & \text{для } j \in 0 : n. \end{aligned} \quad (15)$$

Операторы \vec{L}_i^u и \vec{L}_j^v будут задаваться теми же формулами, что и функционалы L_i^u, L_j^v , но для вектор-функций:

$$\begin{aligned}\vec{L}_{2i}^u(g) &= g(i), & \vec{L}_{2i+1}^u(g) &= g'(i), & \text{для } i \in 0 : m; \\ \vec{L}_{2j}^v(f) &= f(j), & \vec{L}_{2j+1}^v(f) &= f'(j), & \text{для } j \in 0 : n.\end{aligned}$$

Нетрудно видеть, что условия согласования (8) для заданных операторов и вектор-функций эквивалентны условиям (11):

$$\begin{aligned}b_j(i) &= \vec{L}_{2i}^u(g_{2j}) = \vec{L}_{2j}^v(f_{2i}) = a_i(j), \\ B_j(i) &= \vec{L}_{2i}^u(g_{2j+1}) = \vec{L}_{2j+1}^v(f_{2i}) = a'_i(j), \\ b'_j(i) &= \vec{L}_{2i+1}^u(g_{2j}) = \vec{L}_{2j}^v(f_{2i+1}) = A_i(j), \\ B'_j(i) &= \vec{L}_{2i+1}^u(g_{2j+1}) = \vec{L}_{2j+1}^v(f_{2i+1}) = A'_i(j).\end{aligned}$$

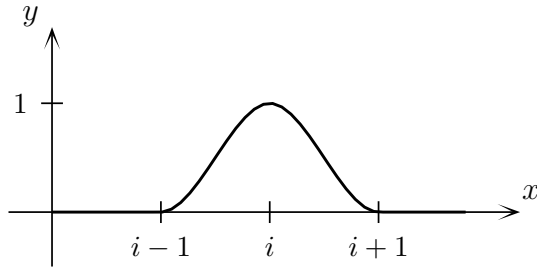
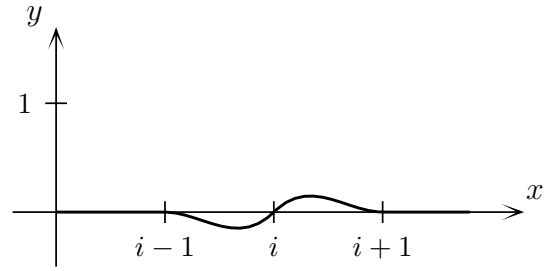
Осталось ввести смешивающие функции H_i^u, H_j^v , удовлетворяющие условиям (5) и (6). Равенства (5) для заданных операторов L_i^u примут вид

$$\begin{aligned}H_{2i}^u(i) &= 1, & (H_{2i+1}^u)'(i) &= 1, \\ H_{2i}^u(j) &= 0, & (H_{2i+1}^u)'(j) &= 0, & \text{при } j \neq i, \\ (H_{2i}^u)'(j) &= 0, & H_{2i+1}^u(j) &= 0, & \text{при } j \in 0 : m.\end{aligned}\tag{16}$$

Положим

$$\begin{aligned}H_{2i}^u(u) &= \begin{cases} H_1(u-i) & \text{при } u \in [i, i+1], \\ H_4(u-i+1) & \text{при } u \in [i-1, i), \\ 0 & \text{иначе;} \end{cases} \\ H_{2i+1}^u(u) &= \begin{cases} H_2(u-i) & \text{при } u \in [i, i+1], \\ H_3(u-i+1) & \text{при } u \in [i-1, i), \\ 0 & \text{иначе;} \end{cases}\end{aligned}\tag{17}$$

где H_1, H_2, H_3 и H_4 — некоторые непрерывно-дифференцируемые функции, удовлетворяющие условиям (2). Ясно, что $H_i^u \in C^1[0, m]$, и условия (16) выполнены. Графики функций H_{2i}^u и H_{2i+1}^u для случая, когда H_1, H_2, H_3 и H_4 являются полиномами Эрмита (3), изображены на рис. 1 и 2.

Рис. 1. Функция H_{2i}^u Рис. 2. Функция H_{2i+1}^u

Аналогичным образом определим функции H_j^v :

$$H_{2j}^v(v) = \begin{cases} H_1(v-j) & \text{при } v \in [j, j+1], \\ H_4(v-j+1) & \text{при } v \in [j-1, j], \\ 0 & \text{иначе;} \end{cases} \quad (18)$$

$$H_{2j+1}^v(v) = \begin{cases} H_2(v-j) & \text{при } v \in [j, j+1], \\ H_3(v-j+1) & \text{при } v \in [j-1, j], \\ 0 & \text{иначе.} \end{cases}$$

Итак, условия (5) и (6) на смешивающие функции, а также условия согласования (8) выполнены. Поэтому обобщённая поверхность Кунса $s(u, v)$, построенная по формуле (9), будет удовлетворять условиям (10). Если положить $s(\alpha, \beta) = c(\alpha, \beta)$, то формулы (10) примут вид (14). Таким образом, полученная обобщённая поверхность Кунса решает задачу построения поверхности, проходящей через заданные кривые и имеющей на них заданные производные.

ПРЕДЛОЖЕНИЕ 2. Если для определения смешивающих функций H_i^u и H_j^v использовались те же функции H_1, H_2, H_3 и H_4 , что и для построения составной поверхности Кунса $s(\alpha, \beta)$, то обобщённая и составная поверхности Кунса совпадают.

Доказательство. Пусть $i \in 0 : m-1$, $j \in 0 : n-1$, $\alpha \in [i, i+1]$, $\beta \in [j, j+1]$. Положим $u = \alpha - i$, $v = \beta - j$. Тогда $s(\alpha, \beta) = c^{ij}(u, v)$.

Из определения H_k^u видно, что $H_k^u(\alpha)$ отлично от нуля только для $k = 2i$, $k = 2i+1$, $k = 2(i+1)$, $k = 2(i+1)+1$. При этом

$$\begin{aligned} H_{2i}^u(\alpha) &= H_1(\alpha - i) = H_1(u), & H_{2i+1}^u(\alpha) &= H_2(\alpha - i) = H_2(u), \\ H_{2(i+1)}^u(\alpha) &= H_4(\alpha - i) = H_4(u), & H_{2(i+1)+1}^u(\alpha) &= H_3(\alpha - i) = H_3(u). \end{aligned}$$

Аналогично, $H_k^v(\beta)$ отлично от нуля только для $k = 2j$, $k = 2j+1$, $k = 2(j+1)$, $k = 2(j+1) + 1$. При этом

$$\begin{aligned} H_{2j}^v(\beta) &= H_1(v), & H_{2j+1}^v(\beta) &= H_2(v), \\ H_{2(j+1)}^v(\beta) &= H_4(v), & H_{2(j+1)+1}^v(\beta) &= H_3(v). \end{aligned}$$

Кроме того, из формул (15) следует, что

$$\begin{aligned} f_{2i}(\beta) &= a_i(\beta) = a_i(j+v), & f_{2i+1}(\beta) &= A_i(\beta) = A_i(j+v), \\ f_{2(i+1)}(\beta) &= a_{i+1}(\beta) = a_{i+1}(j+v), & f_{2(i+1)+1}(\beta) &= A_{i+1}(\beta) = A_{i+1}(j+v), \\ g_{2j}(\alpha) &= b_j(\alpha) = b_j(i+u), & g_{2j+1}(\alpha) &= B_j(\alpha) = B_j(i+u), \\ g_{2(j+1)}(\alpha) &= b_{j+1}(\alpha) = b_{j+1}(i+u), & g_{2(j+1)+1}(\alpha) &= B_{j+1}(\alpha) = B_{j+1}(i+u). \end{aligned}$$

Таким образом, ненулевые слагаемые в $c(\alpha, \beta)$ из формулы (9) совпадают с соответствующими слагаемыми из формулы (4) для граничных вектор-функций (12). Следовательно, $c(\alpha, \beta) = c^{ij}(u, v) = s(\alpha, \beta)$, что и требовалось доказать. \square

На рис. 3 приведён пример кривых a_i , b_j при $m = n = 2$, а на рис. 4 показана составная поверхность Кунса для этих кривых.

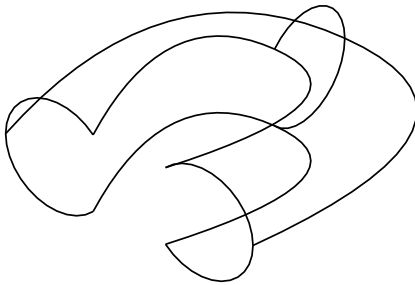


Рис. 3. Кривые a_i , b_j

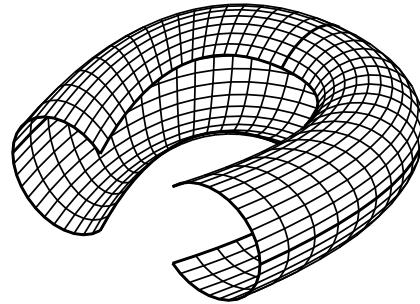


Рис. 4. Составная поверхность Кунса

ЛИТЕРАТУРА

1. Чашников Н. В. *Билинейные поверхности Кунса и поверхности Безье* // Семинар «DHA & CAGD». Избранные доклады. 18 ноября 2006 г. (<http://dha.spb.ru/rep06.shtml#1118>).
2. Малозёмов В. Н., Чашников Н. В. *Бикубические поверхности Кунса* // Семинар «DHA & CAGD». Избранные доклады. 23 января 2007 г. (<http://dha.spb.ru/rep07.shtml#0123>).

3. G. Farin. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.
4. Чашников Н. В. *Составные параметрические поверхности Кунса* // Семинар «ДНА & CAGD». Избранные доклады. 8 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0208>).

СУЩЕСТВОВАНИЕ РАВНОУГОЛЬНЫХ ЖЁСТКИХ ФРЕЙМОВ

В. В. Максименко А. Б. Певный

26 марта 2008 г.

Доклад представляет собой вариации на темы из [1].

1°. Система векторов $\{\varphi_1, \dots, \varphi_m\}$ из \mathbb{R}^n называется *равноугольной*, если

$$|\varphi_k| = 1 \quad \text{при всех } k \in 1:m \quad \text{и} \quad |\langle \varphi_k, \varphi_s \rangle| = c \quad \text{при } k \neq s.$$

Здесь c — фиксированное число. Нас интересует случай $m \geq n$. В докладе [2] выяснено, при каком значении c равноугольная система является жёстким фреймом. Справедливо

ПРЕДЛОЖЕНИЕ 1. *Равноугольная система является жёстким фреймом тогда и только тогда, когда*

$$c = \sqrt{\frac{m-n}{n(m-1)}}.$$

2°. **Необходимое и достаточное условия существования равноугольного жёсткого фрейма.** К сожалению равноугольные жёсткие фреймы существуют не для всех пар (n, m) . Чтобы выяснить для каких существуют, а для каких — нет, нам придётся проделать некоторые построения.

Пусть $\{\varphi_1, \dots, \varphi_m\}$ — равноугольный жёсткий фрейм в \mathbb{R}^n , $m > n > 1$. Из столбцов $\varphi_1, \dots, \varphi_m$ составим матрицу Φ размера $n \times m$. По критерию жёсткого фрейма

$$\Phi \Phi^T = \frac{m}{n} I_n.$$

Рассмотрим теперь матрицу Грама $G = \Phi^T \Phi$. Для её элементов в силу равноугольности имеем

$$G_{ii} = 1, \quad i \in 1:m; \quad G_{ik} = \pm c, \quad i \neq k.$$

Поскольку $\{\varphi_1, \dots, \varphi_m\}$ — жёсткий фрейм, то

$$c = \sqrt{\frac{m-n}{n(m-1)}}.$$

Отсюда, в частности, следует, что $0 < c < 1$. Кроме того, справедливо равенство

$$G^2 = \Phi^T (\Phi \Phi^T) \Phi = \frac{m}{n} G. \quad (1)$$

Рассмотрим матрицу

$$Q = \frac{1}{c} (G - I_m).$$

У неё $Q_{ii} = 0$, $i \in 1 : m$; $Q_{ik} = \pm 1 = \text{sign} \langle \varphi_i, \varphi_k \rangle$ при $i \neq k$.

Вычислим матрицу Q^2 . С учётом равенства (1) имеем

$$\begin{aligned} Q^2 &= \frac{1}{c^2} (G^2 - 2G + I_m) = \frac{1}{c^2} \left(\frac{m}{n} G - 2G + I_m \right) = \\ &= \frac{1}{c^2} \left[\frac{m-2n}{n} (G - I_m) + \frac{m-n}{n} I_m \right] = \\ &= (m-1) I_m + \mu_{m,n} Q, \end{aligned} \quad (2)$$

где

$$\mu_{m,n} = \frac{m-2n}{n c} = (m-2n) \sqrt{\frac{m-1}{n(m-n)}}. \quad (3)$$

Из равенства (2) при $i \neq j$ получим $(Q^2)_{ij} = \pm \mu_{m,n}$, откуда следует, что $\mu_{m,n}$ является целым числом. Это одно из необходимых условий существования равноугольного жёсткого фрейма.

Чтобы сформулировать необходимое и достаточное условие, введём понятие сигнатурной матрицы.

ОПРЕДЕЛЕНИЕ 1. Симметричная матрица Q размера $m \times m$ называется *сигнатурной*, если

$$Q_{ii} = 0, \quad i \in 1 : m; \quad Q_{ik} = \pm 1 \quad \text{при } i \neq k.$$

ТЕОРЕМА 1. Для того чтобы при данных n и m , $m > n > 1$, существовал равноугольный жёсткий фрейм, необходимо и достаточно, чтобы выполнялись условия:

- 1) число $\mu_{m,n}$, определённое равенством (3), является целым;
- 2) существует сигнатурная матрица Q такая, что

$$Q^2 = (m-1) I_m + \mu_{m,n} Q. \quad (4)$$

Доказательство. Необходимость установлена выше. Докажем достаточность. Введём матрицу

$$G = I_m + cQ, \quad \text{где} \quad c = \sqrt{\frac{m-n}{n(m-1)}}.$$

У неё $G_{ii} = 1, i \in 1:m; G_{ik} = \pm c$ при $i \neq k$. Вычислим G^2 . С учётом (4) элементарными вычислениями получим

$$\begin{aligned} G^2 &= I_m + 2cQ + c^2Q^2 = \\ &= I_m + 2cQ + c^2(m-1)I_m + c^2\mu_{m,n}Q = \\ &= \frac{m}{n}(I_m + cQ) = \frac{m}{n}G. \end{aligned}$$

Из равенства $G^2 = \frac{m}{n}G$ следует, что матрица G имеет собственные числа $\frac{m}{n}$ и 0. Обозначим кратность первого числа через p . Тогда 0 имеет кратность $m-p$. Поскольку $G \neq 0$, то $p \geq 1$.

Симметричную матрицу G можно представить в виде

$$G = P^T \Lambda P,$$

где P — ортогональная матрица, $\Lambda = \text{diag}(\frac{m}{n}, \dots, \frac{m}{n}, 0, \dots, 0)$. Рассмотрим матрицу L размера $p \times m$ вида

$$\Lambda = \begin{bmatrix} \sqrt{A} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \sqrt{A} & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sqrt{A} & 0 & \dots & 0 \end{bmatrix},$$

где $A = \frac{m}{n}$. Тогда $L^T L = \Lambda$. Для матрицы $\Phi = L P$ справедливо равенство

$$\Phi^T \Phi = P^T L^T L P = G.$$

Столбцы $\varphi_1, \dots, \varphi_m$ матрицы Φ образуют равноугольную систему. Действительно, $\|\varphi_k\|^2 = \langle \varphi_i, \varphi_i \rangle = G_{ii} = 1, i \in 1:m;$

$$\langle \varphi_i, \varphi_k \rangle = G_{ik} = cQ_{ik} = \pm c, \quad i \neq k.$$

Кроме того, матрицы $\Phi^T \Phi = G$ и $\Phi \Phi^T$ имеют одинаковые ненулевые собственные числа. Следовательно, матрица $\Phi \Phi^T$ имеет только одно собственное число $\frac{m}{n}$ кратности p и, значит,

$$\Phi \Phi^T = \frac{m}{n} I_p.$$

По определению система $\{\varphi_1, \dots, \varphi_m\}$ — жёсткий фрейм в \mathbb{R}^p . Но тогда по предложению 1 справедливо равенство

$$c = \sqrt{\frac{m-p}{p(m-1)}}.$$

Отсюда

$$\frac{m-n}{n(m-1)} = \frac{m-p}{p(m-1)},$$

то есть $p = n$. Построили равноугольный жёсткий фрейм в \mathbb{R}^n . Теорема доказана. \square

3°. Оценки числа элементов равноугольного жёсткого фрейма.

В докладе [2] приведено простое доказательство следующего предложения.

ПРЕДЛОЖЕНИЕ 2. Пусть $m > n > 1$. Если $\{\varphi_1, \dots, \varphi_m\}$ — равноугольный жёсткий фрейм в \mathbb{R}^n , то

$$m \leq \frac{n(n+1)}{2}. \quad (5)$$

Это неравенство в сочетании с теоремой 1 позволяет установить другое ограничение на число m .

ПРЕДЛОЖЕНИЕ 3. Пусть $n \geq 2$, $m > n + 1$. Если $\{\varphi_1, \dots, \varphi_m\}$ — равноугольный жёсткий фрейм в \mathbb{R}^n , то

$$m \leq \frac{(m-n)(m-n+1)}{2}. \quad (6)$$

Доказательство. По теореме 1 фрейму $\{\varphi_1, \dots, \varphi_m\}$ соответствует сигнатурная матрица Q , удовлетворяющая уравнению

$$Q^2 = (m-1)I_m + \mu_{m,n}Q,$$

где $\mu_{m,n}$ задано формулой (3). Заменим в этой формуле n на $m-n$. Отметим, что

$$\mu_{m,m-n} = (2n-m) \sqrt{\frac{m-1}{(m-n)n}} = -\mu_{m,n}.$$

Поэтому сигнатурная матрица $-Q$ удовлетворяет равенству

$$(-Q)^2 = (m-1)I_m + \mu_{m,m-n}(-Q).$$

Поскольку $m-n \geq 2$, $m > m-n$, то по теореме 1 существует равноугольный жёсткий фрейм $\{\psi_1, \dots, \psi_{m-n}\}$ в пространстве \mathbb{R}^{m-n} .

По предложению 2 справедливо неравенство (6).

Предложение доказано. \square

Неравенства (5) и (6) вместе с требованием целочисленности $\mu_{m,n}$ позволяют отбросить многие пары (n, m) , для которых заведомо не существуют равноугольные жёсткие фреймы. Приведём ряд примеров для случая $n \geq 2$, $m > n + 1$.

ПРИМЕР 1. $n = 3$. Неравенство (5) имеет вид $m \leq 6$.

При $m = 5$ не выполнено неравенство (6).

При $m = 6$ оба неравенства (5) и (6) превращаются в равенства. Возникает подозрение, что в случае $(3, 6)$ есть равноугольный жёсткий фрейм. В явном виде он выписан в докладе [2].

ПРИМЕР 2. $n = 4$. Неравенство (5) имеет вид $m \leq 10$.

При $m = 6, 7$ не выполнено неравенство (6).

При $m = 9, 10$ число $\mu_{m,4}$ не целое.

При $m = 8$ выполнены неравенства (5) и (6) и $\mu_{8,4} = 0$. Как будет показано далее, в случае $(4, 8)$ равноугольного жёсткого фрейма не существует.

4°. Нахождение равноугольных жёстких фреймов в случае $m = 2n$ методом перебора сигнатурных матриц. Случай $m = 2n$ является исключительным. При $m = 2n$ число $\mu_{m,n}$ равно нулю и по теореме 1 для существования равноугольного жёсткого фрейма необходимо и достаточно существование сигнатурной матрицы Q , удовлетворяющей равенству

$$Q^2 = (m - 1) I_m. \quad (7)$$

По определению сигнатурная матрица Q симметрична. Поэтому если через Q_i обозначить i -ю строку Q , то условие (7) запишется в виде

$$\langle Q_i, Q_j \rangle = \begin{cases} m - 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

Условие $\langle Q_i, Q_i \rangle = m - 1$ выполняется автоматически, так как каждая строка Q_i содержит один ноль и $m - 1$ элементов, равных ± 1 . Так что нужно только обеспечить ортогональность строк: $\langle Q_i, Q_j \rangle = 0$ при $i \neq j$.

Отметим, что если сигнатурная матрица Q удовлетворяет (7), то после умножения j -го столбца и строки Q_j на -1 снова получим решение (7). Поэтому можно считать, что в первой строке Q_1 стоят единицы:

$$Q_1 = [0 \quad 1 \quad 1 \quad \dots \quad 1].$$

Далее можно пытаться строить строки Q_2, \dots, Q_m так, чтобы каждая строка была ортогональна предыдущим строкам.

При $m = 6$ это удаётся проделать вручную и получить матрицу

$$Q = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 & 1 \\ 1 & -1 & 0 & 1 & -1 & 1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & 1 & -1 & 1 & 0 & -1 \\ 1 & 1 & 1 & -1 & -1 & 0 \end{bmatrix},$$

удовлетворяющую равенству $Q^2 = 5I_6$ (этот же пример приведён в [1]).

При $m = 8$ можно с помощью компьютерной программы перебирать элементы $Q_{ij} = \pm 1$, $i \in 2 : 7$, $j \in i + 1 : 8$. Всего 21 элемент и 2^{21} комбинаций ± 1 . Полный перебор приводит к выводу, что сигнатурной матрицы, удовлетворяющей равенству $Q^2 = 7I_8$, не существует, и, следовательно, не существует равноугольного жёсткого фрейма при $n = 4$, $m = 8$.

При $m = 10$ программа нашла сигнатурную матрицу

$$Q = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 0 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 & 0 & -1 & -1 & 1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 0 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 1 & 0 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & -1 & -1 & 0 & 1 & -1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 0 & -1 \\ 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 0 \end{bmatrix},$$

удовлетворяющую равенству $Q^2 = 9I_{10}$. Далее с помощью компьютерной системы **Maple 9.5** проводим символьные вычисления, указанные в доказательстве теоремы 1: строим матрицу $G = I_{10} + cQ$, находим её ортогональное разложение $G = P^T \Lambda P$, строим матрицу Φ размера 5×10 :

$$\frac{1}{30} \begin{bmatrix} 10\sqrt{3} & -10\sqrt{3} & 10\sqrt{3} & 10\sqrt{3} & 10\sqrt{3} & 10\sqrt{3} & 0 & 0 & 0 & 0 \\ 6\sqrt{5} & 6\sqrt{5} & -6\sqrt{5} & 6\sqrt{5} & -6\sqrt{5} & 6\sqrt{5} & 12\sqrt{5} & 0 & 0 & 0 \\ 2\sqrt{30} & 2\sqrt{30} & -2\sqrt{30} & 2\sqrt{30} & 3\sqrt{30} & -3\sqrt{30} & -\sqrt{30} & 5\sqrt{30} & 0 & 0 \\ 10\sqrt{2} & 10\sqrt{2} & 10\sqrt{2} & -10\sqrt{2} & -5\sqrt{2} & 5\sqrt{2} & -5\sqrt{2} & 5\sqrt{2} & 20\sqrt{2} & 0 \\ 10 & 10 & 10 & -10 & 10 & -10 & 10 & -10 & -10 & 30 \end{bmatrix}.$$

С помощью **Maple 9.5** легко проверяются равенства $\Phi \Phi^T = 2I_5$ и $\Phi^T \Phi = G$. Тем самым столбцы матрицы Φ образуют равноугольный жёсткий фрейм в \mathbb{R}^5 .

Точно так же программа нашла сигнатурные матрицы при $m = 14$ и $m = 18$, а с помощью **Maple 9.5** построены равноугольные жёсткие фреймы в \mathbb{R}^7 и \mathbb{R}^9 .

5°. Необходимое условие существования равноугольного жёсткого фрейма при $m = 2n$. Это условие установлено в работе [3].

ТЕОРЕМА 2. Пусть $n \geq 2$, $m = 2n$. Если существует равноугольный жёсткий фрейм $\{\varphi_1, \dots, \varphi_m\}$ в \mathbb{R}^n , то n — нечётное и $m - 1$ является суммой двух квадратов целых чисел.

В качестве иллюстрации приведём примеры.

При чётном $n = 4$ и $m = 8$ равноугольный жёсткий фрейм не существует.

При $n = 5, 7, 9$ числа $m - 1 = 2n - 1$ являются суммами квадратов двух целых чисел:

$$9 = 3^2 + 0^2, \quad 13 = 3^2 + 2^2, \quad 17 = 4^2 + 1^2.$$

В случаях $(5, 10)$, $(7, 14)$, $(9, 18)$ существование равноугольных жёстких фреймов подтверждается расчётами (см. п. 4).

При $n = 11$, $m = 22$ число $m - 1 = 21$ не представимо в виде суммы двух квадратов и в этом случае по теореме 2 равноугольного жёсткого фрейма не существует.

ЛИТЕРАТУРА

1. Holmes R. B., Paulsen V. I. *Optimal frames for erasures* // Linear Algebra Appl. 2004. V. 377. P. 31–51.
2. Малозёмов В. Н., Певный А. Б. *Равноугольные системы векторов и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 18 сентября 2007 г. (<http://dha.spb.ru/refs07.shtml#0918>).
3. Sustik M. A., Tropp J. A., Dhillon I. S., Heath R. W. *On the existence of equiangular tight frames* // Linear Algebra Appl. 2007. V. 426. P. 619–635.

МАКСИМАЛЬНАЯ ИЗБЫТОЧНОСТЬ ВЕЩЕСТВЕННЫХ ГАРМОНИЧЕСКИХ ФРЕЙМОВ

А. М. Дурягин

28 марта 2008 г.

Аннотация

Из комплексной матрицы Фурье порядка m выбираются первые $k+1$ строк и последние k строк. К столбцам получившейся матрицы размера $(2k+1) \times m$ применяется специальное унитарное преобразование, приводящее к вещественным векторам. Они и образуют вещественный гармонический фрейм, обладающий свойством максимальной избыточности. Такая конструкция впервые появилась в статье [1].

1°. Предварительные сведения. Через Φ будем обозначать систему из m векторов в пространстве \mathbb{C}^n . Система $\Phi = \{\varphi_1, \dots, \varphi_m\}$ в \mathbb{C}^n называется фреймом, если существуют константы $A, B > 0$, такие, что

$$A \|x\|^2 \leq \sum_{i=1}^m |\langle x, \varphi_i \rangle|^2 \leq B \|x\|^2$$

для любого $x \in \mathbb{C}^n$.

Если $A = B$, то Φ — жёсткий фрейм. Система Φ является фреймом в \mathbb{C}^n тогда и только тогда, когда линейная оболочка $\mathcal{L}(\Phi)$ совпадает со всем пространством \mathbb{C}^n (см. доклад [2]).

Если Φ — фрейм, то $m \geq n$.

При $m = n$ система $\{\varphi_1, \dots, \varphi_n\}$ является фреймом в \mathbb{C}^n только в том случае, если $\mathcal{L}(\varphi_1, \dots, \varphi_n) = \mathbb{C}^n$. Это выполняется тогда и только тогда, когда векторы $\varphi_1, \dots, \varphi_n$ линейно независимы, а это равносильно тому, что матрица Φ со столбцами $\varphi_1, \dots, \varphi_n$ невырождена.

2°. Фреймы с максимальной избыточностью.

ОПРЕДЕЛЕНИЕ. Пусть $\Phi = \{\varphi_0, \dots, \varphi_{m-1}\}$, $m > n$, — фрейм в \mathbb{C}^n . Говорят, что Φ обладает *максимальной избыточностью*, если при удалении любых $m - n$ элементов оставшиеся n элементов будут линейно независимыми.

Рассмотрим матрицу Фурье $F_m = \{\omega_m^{kl}\}_{k,l=0}^{m-1} = F_m[M, M]$, где $\omega_m = e^{2\pi i/m}$.

Пусть $n \leq m$. При $n = 2k + 1$ возьмём индексное множество N следующего вида

$$N = \{0, \dots, k, m - k, \dots, m - 1\}. \quad (1)$$

ЛЕММА. Столбцы матрицы $F_m[N, M]$ образуют жёсткий фрейм в \mathbb{C}^n .

Доказательство следует из того, что

$$F_m[N, M]F_m^*[M, N] = mI_n, \quad (2)$$

где $*$ обозначает эрмитово сопряжение.

Замечание. Лемма остаётся справедливой при любом выборе индексного множества N с $|N| = n$. Но в дальнейшем будет важно, что индексное множество N имеет вид (1).

3°. Конструкция гармонического фрейма в случае нечётного n .

Пусть $n = 2k + 1$. Рассмотрим матрицу

$$U[N, N] = \begin{bmatrix} 1 & \mathbb{O} & \mathbb{O} \\ \mathbb{O} & I_k/\sqrt{2} & J_k/\sqrt{2} \\ \mathbb{O} & -iI_k/\sqrt{2} & iJ_k/\sqrt{2} \end{bmatrix},$$

где

$$I_k = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 1 \end{bmatrix}, \quad J_k = \begin{bmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots \\ 1 & 0 & \dots & 0 \end{bmatrix}.$$

Нетрудно проверить равенство $UU^* = I_n$, так что U — унитарная матрица.

Представим матрицу $F_m[N, M]$ как набор столбцов

$$F_m[N, M] = [\varphi_0, \dots, \varphi_{m-1}],$$

где $\varphi_s \in \mathbb{C}^n$. Компоненты $\varphi_s[N]$ имеют вид

$$\varphi_s[N] = (1, \omega_m^s, \omega_m^{2s}, \dots, \omega_m^{ks}, \omega_m^{(m-k)s}, \dots, \omega_m^{(m-1)s})^T.$$

Оказывается, что при умножении векторов φ_s на матрицу U получаются вещественные векторы. Эти векторы образуют жёсткий фрейм в \mathbb{R}^n , который называется вещественным гармоническим фреймом.

ТЕОРЕМА 1. Векторы $f_s = U\varphi_s$, $s \in 0 : m - 1$, образуют жёсткий фрейм в \mathbb{R}^n .

Доказательство. Покажем сначала, что столбцы матрицы

$$D = [f_0, \dots, f_{m-1}]$$

образуют жёсткий фрейм. Действительно,

$$D = [U\varphi_0, \dots, U\varphi_{m-1}] = UF_m[N, M].$$

Отсюда следует, что

$$DD^* = UF_m[N, M]F_m^*[M, N]U^* = UmI_nU^* = mI_n.$$

Теперь покажем, что компоненты вектора $f_s[N] = U\varphi_s[N]$ при $s \in 0 : m - 1$ вещественные.

При умножении первой строки матрицы U на вектор $\varphi_s[N]$ получим компоненту $f_s[0] = 1$. При умножении матрицы $[\mathbb{O}, I_k/\sqrt{2}, J_k/\sqrt{2}]$ на вектор $\varphi_s[N]$ получим компоненты

$$f_s[l] = \frac{\omega_m^{ls} + \omega_m^{(m-l)s}}{\sqrt{2}} = \sqrt{2} \cos \frac{2ls\pi}{m}, \quad l \in 1 : k.$$

При умножении матрицы $[\mathbb{O}, -iI_k/\sqrt{2}, iJ_k/\sqrt{2}]$ на вектор $\varphi_s[N]$ получим компоненты

$$f_s[m - k - 1 + l] = \frac{-i\omega_m^{ls} + i\omega_m^{(m-l)s}}{\sqrt{2}} = \frac{\omega_m^{ls} - \omega_m^{-ls}}{i\sqrt{2}} = \sqrt{2} \sin \frac{2ls\pi}{m}, \quad l \in 1 : k.$$

Таким образом, все компоненты векторов f_s вещественные. Система $\{f_s\}_{s=0}^{m-1}$ образует вещественный жёсткий фрейм. \square

З а м е ч а н и е. В теореме попутно найден явный вид компонент векторов f_s :

$$f_s = \left(1, \sqrt{2} \cos \frac{2s\pi}{m}, \dots, \sqrt{2} \cos \frac{2ks\pi}{m}, \sqrt{2} \sin \frac{2s\pi}{m}, \dots, \sqrt{2} \sin \frac{2ks\pi}{m}\right)^T,$$

где $s \in 0 : m - 1$ и $n = 2k + 1$. Нормированные векторы f_s/\sqrt{n} полностью совпадают с векторами из доклада [3].

ПРИМЕР. Возьмем $k = 1$, $n = 3$, $m = 5$. Тогда $N = \{0, 1, 4\}$. Унитарная матрица U примет вид

$$U = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & -i/\sqrt{2} & i/\sqrt{2} \end{bmatrix}.$$

Имеем

$$\varphi_s = \begin{bmatrix} 1 \\ \omega_5^s \\ \omega_5^{4s} \end{bmatrix} = \begin{bmatrix} 1 \\ \omega_5^s \\ \omega_5^{-s} \end{bmatrix}, \quad s \in 0 : 4,$$

и

$$f_s = U\varphi_s = \begin{bmatrix} 1 \\ \frac{\omega_5^s + \omega_5^{-s}}{\sqrt{2}} \\ \frac{-i\omega_5^s + i\omega_5^{-s}}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ \sqrt{2} \cos \frac{2s\pi}{5} \\ \sqrt{2} \sin \frac{2s\pi}{5} \end{bmatrix}, \quad s \in 0 : 4.$$

4°. Конструкция гармонического фрейма в случае чётного n .

Пусть $n = 2k$. Возьмём множество $N = \{0, \dots, k-1, m-k, \dots, m-1\}$. Рассмотрим матрицу

$$U[N, N] = \begin{bmatrix} I_k/\sqrt{2} & J_k/\sqrt{2} \\ -iI_k/\sqrt{2} & iJ_k/\sqrt{2} \end{bmatrix}.$$

Легко проверить равенство $UU^* = I_n$, так что U — унитарная матрица.

Представим матрицу $F_m[N, M]$ как набор столбцов

$$F_m[N, M] = [\varphi_0, \dots, \varphi_{m-1}],$$

где $\varphi_s \in \mathbb{C}^n$. Компоненты $\varphi_s[N]$ имеют вид

$$\varphi_s[N] = (1, \omega_m^s, \omega_m^{2s}, \dots, \omega_m^{(k-1)s}, \omega_m^{(m-k)s}, \dots, \omega_m^{(m-1)s})^T.$$

Оказывается, что при умножении векторов φ_s с некоторыми коэффициентами на матрицу U получаются вещественные векторы. Эти векторы образуют вещественный жёсткий фрейм.

ТЕОРЕМА 2. Векторы $f_s = U\omega_m^{s/2}\varphi_s$, $s \in 0 : m-1$, образуют жёсткий фрейм в \mathbb{R}^n .

Доказательство. Покажем сначала, что столбцы матрицы

$$D = [f_0, \dots, f_{m-1}]$$

образуют жёсткий фрейм. Действительно,

$$D = [U\omega_m^{0/2}\varphi_0, \dots, U\omega_m^{(m-1)/2}\varphi_{m-1}] = UF_m[N, M]B[M, M],$$

где $B[M, M] = \text{diag}(1, \omega_m^{1/2}, \dots, \omega_m^{(m-1)/2})$. Отсюда следует, что

$$\begin{aligned} DD^* &= UF_m[N, M]B[M, M]B^*[M, M]F_m^*[M, N]U^* = \\ &= UF_m[N, M]I_mF_m^*[M, N]U^* = UmI_nU^* = mI_n. \end{aligned}$$

Теперь покажем, что компоненты вектора $f_s[N] = U\omega_m^{s/2}\varphi_s[N]$ при $s \in 0 : m-1$ вещественные.

При умножении матрицы $[I_k/\sqrt{2}, J_k/\sqrt{2}]$ на вектор $\omega_m^{s/2}\varphi_s[N]$ получим компоненты

$$\begin{aligned} f_s[l] &= \frac{\omega_m^{s/2}}{\sqrt{2}} (\omega_m^{ls} + \omega_m^{(m-1-l)s}) = \frac{1}{\sqrt{2}} (\omega_m^{(2l+1)s/2} + \omega_m^{-(2l+1)s/2}) = \\ &= \sqrt{2} \cos \frac{(2l+1)s\pi}{m}, \quad l \in 0 : k-1. \end{aligned}$$

При умножении матрицы $[-iI_k/\sqrt{2}, iJ_k/\sqrt{2}]$ на вектор $\omega_m^{s/2}\varphi_s[N]$ получим компоненты

$$\begin{aligned} f_s[m-k-1+l] &= -i \frac{\omega_m^{s/2}}{\sqrt{2}} (\omega_m^{ls} - \omega_m^{(m-1-l)s}) = \\ &= -\frac{i}{\sqrt{2}} (\omega_m^{(2l+1)s/2} - \omega_m^{-(2l+1)s/2}) = \sqrt{2} \sin \frac{(2l+1)s\pi}{m}, \quad l \in 1 : k. \end{aligned}$$

Таким образом, все компоненты векторов f_s вещественные. Система $\{f_s\}_{s=0}^{m-1}$ образует вещественный жёсткий фрейм. \square

З а м е ч а н и е. В теореме попутно найден явный вид компонент векторов f_s :

$$f_s = \left(\sqrt{2} \cos \frac{s\pi}{m}, \dots, \sqrt{2} \cos \frac{(2k+1)s\pi}{m}, \sqrt{2} \sin \frac{s\pi}{m}, \dots, \sqrt{2} \sin \frac{(2k+1)s\pi}{m} \right)^T,$$

где $s \in 0 : m-1$ и $n = 2k$. Нормированные векторы f_s/\sqrt{n} полностью совпадают с векторами из доклада [3].

5°. Максимальная избыточность вещественного гармонического фрейма. Следующая теорема для нечётного n установлена в [1]. Нам удалось найти более простое её доказательство и доказать теорему для чётного n .

ТЕОРЕМА 3. *Фрейм $\{f_s\}_{s=0}^{m-1}$ обладает максимальной избыточностью.*

Доказательство. Сначала докажем теорему при нечётном n .

Выберем произвольное множество $J \subset M$ с $|J| = n$. Рассмотрим матрицу $D[N, J] = UF_m[N, J]$. Нужно доказать, что эта матрица невырождена.

Унитарная матрица является неособенной. Введём матрицу $A[J, N] = F_m^*[J, N]$. Эта матрица имеет элементы

$$A[j, l] = \overline{F_m[l, j]} = \omega_m^{-lj}, \quad j \in J, \quad l \in N.$$

Покажем, что она невырождена.

Рассмотрим однородную систему

$$A[J, N] c[N] = \mathbb{O}[J]. \quad (3)$$

Нужно доказать, что эта система имеет только нулевое решение.

Пусть $c[N]$ решение системы. Тогда

$$\sum_{l \in N} \omega_m^{-lj} c[l] = 0, \quad j \in J. \quad (4)$$

Поскольку $N = \{0, 1, \dots, k, m-k, \dots, m-1\}$, то

$$\sum_{l=0}^k \omega_m^{-lj} c[l] + \sum_{l=1}^k c[m-l] \omega_m^{-j(m-l)} = 0, \quad j \in J. \quad (5)$$

Домножим j -е равенство на ω_m^{jk} . Получим

$$\sum_{l=0}^k \omega_m^{j(k-l)} c[l] + \sum_{l=1}^k c[m-l] \omega_m^{j(k+l)} = 0, \quad j \in J. \quad (6)$$

Рассмотрим полином

$$\begin{aligned} P(z) &= \sum_{l=0}^k z^{k-l} c[l] + \sum_{l=1}^k c[m-l] z^{k+l} = \\ &= c[0]z^k + c[1]z^{k-1} + \dots + c[k]z^0 + \\ &+ c[m-1]z^{k+1} + c[m-2]z^{k+2} + \dots + c[m-k]z^{2k}. \end{aligned}$$

Его степень не выше $2k = n-1$. В силу равенства (6) полином $P(z)$ имеет n корней $z_j = \omega_m^j = e^{i2\pi j/m}$, $j \in J$. Здесь $J = \{j_1, \dots, j_n\}$, при этом $0 \leq j_1 < \dots < j_n \leq m-1$. Значит, все корни z_j различны. Приходим к тождеству $P(z) \equiv 0$, из которого следует, что $c[l] = 0$ при всех $l \in N$.

Установлено, что система (3) имеет только нулевое решение. Это гарантирует невырожденность матриц $A[N, J]$ и $D[N, J]$.

Теперь приведём доказательство теоремы для чётного n . Рассмотрим матрицу $D = UF_m[N, M]B[M, M]$, где $B[M, M] = \text{diag}(1, \omega_m^{1/2}, \dots, \omega_m^{(m-1)/2})$.

Выберем произвольное множество $J \subset M$ с $|J| = n$. Рассмотрим матрицу $D[N, J] = UF_m[N, M]B[M, J]$. Отметим, что $B[M \setminus J, J]$ — нулевая матрица, поэтому $D[N, J] = UF_m[N, J]B[J, J]$.

Достаточно проверить, что матрица $A[J, N] = F_m^*[J, N]$ невырождена.

Рассмотрим однородную систему

$$A[J, N] c[N] = \mathbb{O}[J]. \quad (7)$$

Пусть $c[N]$ решение системы. Тогда

$$\sum_{l \in N} \omega_m^{-lj} c[l] = 0, \quad j \in J. \quad (8)$$

Поскольку $N = \{0, 1, \dots, k-1, m-k, \dots, m-1\}$, то

$$\sum_{l=0}^{k-1} \omega_m^{-lj} c[l] + \sum_{l=1}^k c[m-l] \omega_m^{-j(m-l)} = 0, \quad j \in J. \quad (9)$$

Домножим j -е равенство на $\omega_m^{j(k-1)}$. Получим

$$\sum_{l=0}^{k-1} \omega_m^{j(k-l-1)} c[l] + \sum_{l=1}^k c[m-l] \omega_m^{j(k+l-1)} = 0, \quad j \in J. \quad (10)$$

Рассмотрим полином

$$\begin{aligned} P(z) &= \sum_{l=0}^{k-1} z^{k-l-1} c[l] + \sum_{l=1}^k c[m-l] z^{k+l-1} = \\ &= c[0]z^{k-1} + \dots + c[k-1]z^0 + c[m-1]z^k + \dots + c[m-k]z^{2k-1}. \end{aligned}$$

Его степень не выше $2k-1 = n-1$. В силу равенства (10) полином $P(z)$ имеет n различных корней $z_j = \omega_m^j$, $j \in J$. Следовательно, $P(z) \equiv 0$ и, значит, $c[l] = 0$ при всех $l \in N$.

Установлено, что система (7) имеет только нулевое решение. Это гарантирует невырожденность матриц $A[J, N]$ и $D[N, J]$. \square

З а м е ч а н и е. Может возникнуть гипотеза, что при любом выборе индексных множеств

$$N \subset M, \quad J \subset M, \quad |N| = |J| = n < m$$

матрица $F_m[N, J]$ будет невырожденной. Однако это не так, как показывает следующий пример.

Пусть $n = 2$, $m = 4$. Возьмём $N = J = \{1, 3\}$. Тогда

$$F_4[N, J] = \begin{bmatrix} \omega_4^1 & \omega_4^3 \\ \omega_4^3 & \omega_4^9 \end{bmatrix} = \begin{bmatrix} \omega_4^1 & \omega_4^3 \\ \omega_4^3 & \omega_4^1 \end{bmatrix}.$$

Имеем $\det(F_4[N, J]) = \omega_4^2 - \omega_4^6 = 0$, то есть матрица $F_4[N, J]$ вырождена.

ЛИТЕРАТУРА

1. M. Püschel, J. Kovačević. *Real, Tight Frames with Maximal Robustness to Erasures* // Data Compression Conference, 2005. Proceedings. P. 63–72.
2. Певный А. Б. *Гармонические фреймы — фреймы с максимальной избыточностью* // Семинар «DHA & CAGD». Избранные доклады. 28 марта 2007 г. (<http://dha.spb.ru/rep07.shtml#0328>).
3. Дурягин А. М., Соловьёва Н. А. *Вещественные гармонические фреймы* // Семинар «DHA & CAGD». Избранные доклады. 9 октября 2007 г. (<http://dha.spb.ru/rep07.shtml#1009>).

ПОЛИНОМЫ БЕРНШТЕЙНА ОТ ДВУХ ПЕРЕМЕННЫХ

М. И. Григорьев

29 марта 2008 г.

В статье [1] изучались полиномы в форме Бернштейна и их приложение к теории кривых Безье. В данном докладе рассмотрено естественное обобщение таких полиномов на двумерный случай.

1°. Напомним, что базисными полиномами Бернштейна от одной переменной называются полиномы

$$b_k^n(x) = C_n^k x^k (1-x)^{n-k}, \quad k \in 0:n, \quad n = 0, 1, \dots$$

Базисные полиномы Бернштейна от двух переменных определяются следующим образом:

$$b_{ks}^n(x, y) = C_n^{k,s} x^k y^s (1-x-y)^{n-k-s}, \\ k \in 0:n, \quad s \in 0:n-k, \quad n = 0, 1, \dots,$$

где $C_n^{k,s} = \frac{n!}{k!s!(n-k-s)!}$ — так называемые *триномиальные* коэффициенты. В частности,

$$b_{00}^0(x, y) \equiv 1, \quad b_{n0}^n(x, y) = x^n, \quad b_{0n}^n(x, y) = y^n, \quad b_{00}^n(x, y) = (1-x-y)^n; \\ b_{k0}^n(x, 0) = b_k^n(x), \quad k \in 0:n; \quad b_{ks}^n(x, 0) = 0, \quad s \in 1:n, \quad k \in 0:n-s; \\ b_{0s}^n(0, y) = b_s^n(y), \quad s \in 0:n; \quad b_{ks}^n(0, y) = 0, \quad k \in 1:n, \quad s \in 0:n-k.$$

При $x + y = 1$

$$b_{ks}^n(x, y) = 0, \quad k + s \leq n-1; \quad b_{ks}^n(x, y) = b_k^n(x) = b_s^n(y), \quad k + s = n.$$

Отметим также, что

$$b_{ks}^n(x, y) > 0 \quad \text{при} \quad x > 0, \quad y > 0, \quad x + y < 1.$$

Справедливо тождество

$$[xp + yq + (1 - x - y)]^n = \sum_{k=0}^n \sum_{s=0}^{n-k} b_{ks}^n(x, y) p^k q^s. \quad (1)$$

Оно следует из общей формулы

$$\begin{aligned} (x + y + z)^n &= \sum_{k=0}^n C_n^k x^k (y + z)^{n-k} = \\ &= \sum_{k=0}^n \sum_{s=0}^{n-k} C_n^k C_{n-k}^s x^k y^s z^{n-k-s} = \sum_{k=0}^n \sum_{s=0}^{n-k} C_n^{k,s} x^k y^s z^{n-k-s}. \end{aligned} \quad (2)$$

(Здесь мы воспользовались тем фактом, что $C_n^k C_{n-k}^s = C_n^{k,s}$.)

Подставив в (1) $p = q = 1$, получим

$$\sum_{k=0}^n \sum_{s=0}^{n-k} b_{ks}^n(x, y) \equiv 1.$$

2°. Рассмотрим полином от двух переменных в форме Бернштейна

$$B(x, y) = \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} b_{ks}^n(x, y).$$

Введём конечные разности на треугольном массиве коэффициентов

$$\begin{aligned} (\Delta^j a)_{*,s} &= \sum_{\beta=0}^j (-1)^{j-\beta} C_j^\beta a_{*,s+\beta}, \\ (\Delta^{i,j} a)_{ks} &= \left(\Delta^i (\Delta^j a)_{*,s} \right)_k = \sum_{\alpha=0}^i (-1)^{i-\alpha} C_i^\alpha \left(\sum_{\beta=0}^j (-1)^{j-\beta} C_j^\beta a_{k+\alpha,s+\beta} \right) = \\ &= \sum_{\alpha=0}^i \sum_{\beta=0}^j (-1)^{i+j-\alpha-\beta} C_i^\alpha C_j^\beta a_{k+\alpha,s+\beta}. \end{aligned}$$

ПРЕДЛОЖЕНИЕ 1. Полином $B(x, y)$ допускает представление

$$B(x, y) = \sum_{i=0}^n \sum_{j=0}^{n-i} C_n^{i,j} (\Delta^{i,j} a)_{00} x^i y^j. \quad (3)$$

Доказательство. Имеем

$$B(x, y) = \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} C_n^{k,s} x^k y^s (1-x-y)^{n-k-s}.$$

Применив формулу (2) к $(1-x-y)^{n-k-s}$, получим

$$\begin{aligned} B(x, y) &= \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} C_n^{k,s} \sum_{\alpha=0}^{n-k-s} \sum_{\beta=0}^{n-k-s-\alpha} C_{n-k-s}^{\alpha,\beta} (-1)^\alpha (-1)^\beta x^{k+\alpha} y^{s+\beta} = \\ &= \sum_{k=0}^n \sum_{s=0}^{n-k} \sum_{i=k}^{n-s} \sum_{j=s}^{n-i} a_{ks} C_n^{k,s} C_{n-k-s}^{i-k,j-s} (-1)^{i+j-k-s} x^i y^j. \end{aligned}$$

Поменяем порядок суммирования по k и по i (через s). Поскольку

$$\sum_{s=0}^{n-k} \sum_{i=k}^{n-s} = \sum_{i=k}^n \sum_{s=0}^{n-i} \quad \text{и} \quad \sum_{k=0}^n \sum_{i=k}^n = \sum_{i=0}^n \sum_{k=0}^i,$$

то

$$B(x, y) = \sum_{i=0}^n \sum_{k=0}^i \sum_{s=0}^{n-i} \sum_{j=s}^{n-i} a_{ks} C_n^{k,s} C_{n-k-s}^{i-k,j-s} (-1)^{i+j-k-s} x^i y^j.$$

Теперь поменяем порядок суммирования по k и по j (через s). Поскольку

$$\sum_{s=0}^{n-i} \sum_{j=s}^{n-i} = \sum_{j=0}^{n-i} \sum_{s=0}^j \quad \text{и} \quad \sum_{k=0}^i \sum_{j=0}^{n-i} = \sum_{j=0}^{n-i} \sum_{k=0}^i,$$

то

$$B(x, y) = \sum_{i=0}^n \sum_{j=0}^{n-i} \sum_{k=0}^i \sum_{s=0}^j a_{ks} C_n^{k,s} C_{n-k-s}^{i-k,j-s} (-1)^{i+j-k-s} x^i y^j.$$

Воспользуемся равенством

$$C_n^{k,s} C_{n-k-s}^{i-k,j-s} = C_n^{i,j} C_i^k C_j^s.$$

Придём к требуемому представлению

$$\begin{aligned} B(x, y) &= \sum_{i=0}^n \sum_{j=0}^{n-i} C_n^{i,j} x^i y^j \left(\sum_{k=0}^i \sum_{s=0}^j (-1)^{i+j-k-s} C_i^k C_j^s a_{ks} \right) = \\ &= \sum_{i=0}^n \sum_{j=0}^{n-i} C_n^{i,j} (\Delta^{i,j} a)_{00} x^i y^j. \end{aligned}$$

Предложение доказано. □

3°. Зафиксируем два целых неотрицательных числа α, β и положим $r = \alpha + \beta$.

ПРЕДЛОЖЕНИЕ 2. Для частной производной $\frac{\partial^r B(x, y)}{\partial x^\alpha \partial y^\beta}$ полинома в форме Бернштейна при $r \in 1 : n$ справедлива формула

$$\frac{\partial^r B(x, y)}{\partial x^\alpha \partial y^\beta} = A_n^r \sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} (\Delta^{\alpha, \beta} a)_{ks} b_{ks}^{n-r}(x, y), \quad (4)$$

где $A_n^r = n(n-1) \cdots (n-r+1)$.

Доказательство. Продифференцируем тождество (3) по x . Учитывая, что $i C_n^{i,j} = n C_{n-1}^{i-1,j}$, получаем

$$\frac{\partial B(x, y)}{\partial x} = \sum_{i=1}^n \sum_{j=0}^{n-i} (i C_n^{i,j}) (\Delta^{i,j} a)_{00} x^{i-1} y^j = n \sum_{i=0}^{n-1} \sum_{j=0}^{n-i-1} C_{n-1}^{i,j} (\Delta^{i+1,j} a)_{00} x^i y^j.$$

Но $(\Delta^{i+1,j} a)_{00} = (\Delta^{i,j} (\Delta^{1,0} a))_{00}$, так что

$$\begin{aligned} \frac{\partial B(x, y)}{\partial x} &= n \sum_{i=0}^{n-1} \sum_{j=0}^{n-1-i} C_{n-1}^{i,j} (\Delta^{i,j} (\Delta^{1,0} a))_{00} x^i y^j = \\ &= n \sum_{k=0}^{n-1} \sum_{s=0}^{n-1-k} (\Delta^{1,0} a)_{ks} b_{ks}^{n-1}(x, y). \end{aligned}$$

Это соответствует формуле (4) при $\alpha = 1, \beta = 0$.

Далее

$$\frac{\partial B(x, y)}{\partial x} = n \sum_{j=0}^{n-1} \sum_{i=0}^{n-1-j} C_{n-1}^{i,j} (\Delta^{i,j} (\Delta^{1,0} a))_{00} x^i y^j.$$

Продифференцируем данное тождество по y . Учитывая, что $\Delta^{0,1} (\Delta^{1,0} a) = \Delta^{1,1} a$, аналогично предыдущему получаем

$$\begin{aligned} \frac{\partial^2 B(x, y)}{\partial x \partial y} &= n(n-1) \sum_{j=0}^{n-2} \sum_{i=0}^{n-2-j} C_{n-2}^{i,j} (\Delta^{i,j} (\Delta^{1,1} a))_{00} x^i y^j = \\ &= n(n-1) \sum_{k=0}^{n-2} \sum_{s=0}^{n-2-k} (\Delta^{1,1} a)_{ks} b_{ks}^{n-2}(x, y). \end{aligned}$$

Продолжив дифференцирование, придём к (4). □

4°. Рассмотрим $n + 1$ треугольных массивов базисных полиномов Бернштейна

$$\{b_{ks}^i(x, y)\}, \quad k \in 0 : i, \quad s \in 0 : i - k, \quad i \in 0, 1, \dots, n.$$

Положим для удобства

$$\begin{aligned} b_{k,-1}^i(x, y) &\equiv b_{-1,s}^i(x, y) \equiv 0, \quad k, s \in 0 : i + 1; \\ b_{ks}^i(x, y) &\equiv 0, \quad k, s \geq 0, \quad k + s = i + 1, \quad i = 0, 1, \dots, n - 1. \end{aligned} \quad (5)$$

Например, при $i = 3$ получим 15 искусственно добавленных полиномов (см. рис. 1).

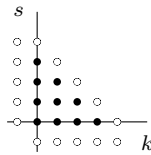


Рис. 1

ПРЕДЛОЖЕНИЕ 3. При любых вещественных x, y справедливы рекуррентные соотношения

$$\begin{aligned} b_{00}^0 &\equiv 1; \\ b_{ks}^i &= (1 - x - y) b_{ks}^{i-1} + x b_{k-1,s}^{i-1} + y b_{k,s-1}^{i-1}, \\ k \in 0 : i, \quad s \in 0 : i - k, \quad i &= 1, \dots, n. \end{aligned} \quad (6)$$

Доказательство. Перепишем тождества (5), заменив в них i на $i - 1$:

$$\begin{aligned} b_{k,-1}^{i-1} &\equiv b_{-1,s}^{i-1} \equiv 0, \quad k, s \in 0 : i; \\ b_{ks}^{i-1} &\equiv 0, \quad k, s \geq 0, \quad k + s = i, \quad i = 1, \dots, n. \end{aligned} \quad (7)$$

Зафиксируем $i \in 1 : n$. При $k = s = 0$ обе части (6) равны $(1 - x - y)^i$. Пусть $k = 0, s \in 1 : i - 1$. Тогда

$$\begin{aligned} &(1 - x - y) b_{0s}^{i-1} + x b_{-1,s}^{i-1} + y b_{0,s-1}^{i-1} = \\ &= (1 - x - y) C_{i-1}^s y^s (1 - x - y)^{i-1-s} + y C_{i-1}^{s-1} y^{s-1} (1 - x - y)^{i-s} = \\ &= (1 - x - y)^{i-s} y^s (C_{i-1}^s + C_{i-1}^{s-1}) = C_i^s y^s (1 - x - y)^{i-s} = b_{0s}^i. \end{aligned}$$

При $k = 0, s = i$ обе части (6) равны y^i .

Аналогично проверяется случай $s = 0, k \in 1 : i$.

Если $k, s \geq 1, k + s = i$, то, согласно (7), $b_{ks}^{i-1} \equiv 0$, так что

$$\begin{aligned} &(1 - x - y) b_{ks}^{i-1} + x b_{k-1,s}^{i-1} + y b_{k,s-1}^{i-1} = \\ &= x C_{i-1}^{k-1,s} x^{k-1} y^s + y C_{i-1}^{k,s-1} x^k y^{s-1} = \\ &= x^k y^s (C_{i-1}^{k-1,s} + C_{i-1}^{k,s-1}) = C_i^{k,s} x^k y^s = b_{ks}^i. \end{aligned}$$

Осталось рассмотреть случай $k, s \geq 1, k + s \in 2 : i - 1$. Имеем

$$\begin{aligned} (1-x-y)b_{ks}^{i-1} + x b_{k-1,s}^{i-1} + y b_{k,s-1}^{i-1} &= (1-x-y)C_{i-1}^{k,s} x^k y^s (1-x-y)^{i-1-k-s} + \\ &+ x C_{i-1}^{k-1,s} x^{k-1} y^s (1-x-y)^{i-k-s} + y C_{i-1}^{k,s-1} x^k y^{s-1} (1-x-y)^{i-k-s} = \\ &= x^k y^s (1-x-y)^{i-k-s} (C_{i-1}^{k,s} + C_{i-1}^{k-1,s} + C_{i-1}^{k,s-1}) = \\ &= C_i^{k,s} x^k y^s (1-x-y)^{i-k-s} = b_{ks}^i. \end{aligned}$$

Мы воспользовались легко проверяемой формулой

$$C_{i-1}^{k,s} + C_{i-1}^{k-1,s} + C_{i-1}^{k,s-1} = C_i^{k,s}.$$

Предложение доказано. □

5°. Зафиксируем произвольные вещественные x, y . Для вычисления значения $B(x, y)$ введём $n+1$ треугольных массивов $\{a_{ks}^i\}$ с помощью рекуррентных соотношений

$$\begin{aligned} a_{ks}^0 &= a_{ks}, \quad k \in 0 : n, \quad s \in 0 : n - k; \\ a_{ks}^i &= (1-x-y)a_{ks}^{i-1} + x a_{k+1,s}^{i-1} + y a_{k,s+1}^{i-1}, \\ k &\in 0 : n - i, \quad s \in 0 : n - i - k, \quad i = 1, \dots, n. \end{aligned} \tag{8}$$

ПРЕДЛОЖЕНИЕ 4. Справедливо равенство $B(x, y) = a_{00}^n$.

Доказательство. При $n = 0$ утверждение тривиально. При $n = 1$ оно проверяется так:

$$\begin{aligned} B(x, y) &= a_{00} b_{00}^1(x, y) + a_{01} b_{01}^1(x, y) + a_{10} b_{10}^1(x, y) = \\ &= a_{00} (1-x-y) + a_{01} y + a_{10} x = a_{00}^1. \end{aligned}$$

Пусть $n \geq 2$. Согласно (6), (7) и (8) имеем

$$\begin{aligned} B(x, y) &= \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} [(1-x-y)b_{ks}^{n-1} + x b_{k-1,s}^{n-1} + y b_{k,s-1}^{n-1}] = \\ &= \sum_{k=0}^{n-1} \sum_{s=0}^{n-k-1} a_{ks}^0 (1-x-y) b_{ks}^{n-1} + \sum_{k=1}^n \sum_{s=0}^{n-k} a_{ks}^0 x b_{k-1,s}^{n-1} + \sum_{k=0}^{n-1} \sum_{s=1}^{n-k} a_{ks}^0 y b_{k,s-1}^{n-1} = \\ &= \sum_{k=0}^{n-1} \sum_{s=0}^{n-k-1} [(1-x-y)a_{ks}^0 + x a_{k+1,s}^0 + y a_{k,s+1}^0] b_{ks}^{n-1} = \sum_{k=0}^{n-1} \sum_{s=0}^{n-1-k} a_{ks}^1 b_{ks}^{n-1}. \end{aligned}$$

Продолжив аналогично, получим

$$\begin{aligned} B(x, y) &= \sum_{k=0}^{n-2} \sum_{s=0}^{n-2-k} a_{ks}^2 b_{ks}^{n-2}(x, y) = \dots = \sum_{k=0}^1 \sum_{s=0}^{1-k} a_{ks}^{n-1} b_{ks}^1(x, y) = \\ &= a_{00}^{n-1} (1 - x - y) + a_{01}^{n-1} y + a_{10}^{n-1} x = a_{00}^n. \end{aligned}$$

Предложение доказано. \square

6°. Обратимся к вопросу о вычислении производных полинома $B(x, y)$. Нам потребуется соотношение

$$\begin{aligned} (1 - x - y) (\Delta^{\alpha, \beta} a^i)_{ks} + x (\Delta^{\alpha, \beta} a^i)_{k+1, s} + \\ + y (\Delta^{\alpha, \beta} a^i)_{k, s+1} = (\Delta^{\alpha, \beta} a^{i+1})_{ks}, \end{aligned} \quad (9)$$

которое непосредственно следует из (8). Действительно,

$$\begin{aligned} \sum_{p=0}^{\alpha} \sum_{q=0}^{\beta} (-1)^{\alpha+\beta-p-q} C_{\alpha}^p C_{\beta}^q [(1 - x - y) a_{k+p, s+q}^i + x a_{k+1+p, s+q}^i + \\ + y a_{k+p, s+1+q}^i] = \sum_{p=0}^{\alpha} \sum_{q=0}^{\beta} (-1)^{\alpha+\beta-p-q} C_{\alpha}^p C_{\beta}^q a_{k+p, s+q}^{i+1} = (\Delta^{\alpha, \beta} a^{i+1})_{ks}. \end{aligned}$$

ПРЕДЛОЖЕНИЕ 5. При фиксированных x, y частные производные от полинома в форме Бернштейна можно вычислить по формуле

$$\frac{\partial^r B(x, y)}{\partial x^{\alpha} \partial y^{\beta}} = A_n^r (\Delta^{\alpha, \beta} a^{n-r})_{00}.$$

Здесь $\alpha + \beta = r$, $r \in 1 : n$.

Доказательство. Согласно (4)

$$\frac{\partial^r B(x, y)}{\partial x^{\alpha} \partial y^{\beta}} = A_n^r \sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} (\Delta^{\alpha, \beta} a)_{ks} b_{ks}^{n-r}(x, y).$$

Воспользуемся приёмом из доказательства предложения 4 и соотношением (9). Запишем

$$\sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} (\Delta^{\alpha, \beta} a^0)_{ks} b_{ks}^{n-r}(x, y) = \sum_{k=0}^{n-r-1} \sum_{s=0}^{n-r-1-k} [(1 - x - y) (\Delta^{\alpha, \beta} a^0)_{ks} +$$

$$\begin{aligned}
& + x (\Delta^{\alpha, \beta} a^0)_{k+1, s} + y (\Delta^{\alpha, \beta} a^0)_{k, s+1} \Big] b_{ks}^{n-r-1}(x, y) = \\
& = \sum_{k=0}^{n-r-1} \sum_{s=0}^{n-r-1-k} (\Delta^{\alpha, \beta} a^1)_{ks} b_{ks}^{n-r-1}(x, y).
\end{aligned}$$

Продолжив данное преобразование, получим

$$\frac{\partial^r B(x, y)}{\partial x^\alpha \partial y^\beta} = A_n^r \sum_{k=0}^1 \sum_{s=0}^{1-k} (\Delta^{\alpha, \beta} a^{n-r-1})_{ks} b_{ks}^1(x, y) = A_n^r (\Delta^{\alpha, \beta} a^{n-r})_{00}.$$

Предложение доказано. \square

Таким образом, $n + 1$ треугольных массивов $\{a_{ks}^i\}$, построенных по формуле (8), дают возможность вычислить как значение полинома $B(x, y)$, так и значения всех его частных производных в фиксированной точке (x, y) .

ЛИТЕРАТУРА

1. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Полиномы Бернштейна и составные кривые Безье* // Журн. вычисл. мат. и матем. физ. 2006. Т. 46. № 11. С. 1962-1971.

ПОЛЯРНАЯ ФОРМА ПОЛИНОМОВ ОТ ДВУХ ПЕРЕМЕННЫХ

М. И. Григорьев А. Н. Сергеев

12 апреля 2008 г.

В докладе результаты из [1] переносятся на двумерный случай.

1°. Точки из \mathbb{R}^2 будем обозначать $\xi = (x, y)$, $\xi_i = (x_i, y_i)$.

Введём основные симметрические полиномы над переменными из \mathbb{R}^2 :

$$\sigma_{00}(\xi_1, \dots, \xi_n) \equiv 1,$$

$$\sigma_{ks}(\xi_1, \dots, \xi_n) = \sum_{I_k \subset N} \sum_{J_s \subset N \setminus I_k} \prod_{i \in I_k} x_i \prod_{j \in J_s} y_j, \quad (1)$$

$$k, s \geq 0, \quad 1 \leq k + s \leq n.$$

Суммирование в правой части (1) ведётся по всем подмножествам I_k множества $N = \{1, \dots, n\}$, содержащим ровно k элементов, и по всем подмножествам J_s множества $N \setminus I_k$, содержащим ровно s элементов. Например,

$$\sigma_{11}(\xi_1, \xi_2, \xi_3) = x_1(y_2 + y_3) + x_2(y_1 + y_3) + x_3(y_1 + y_2),$$

$$\sigma_{21}(\xi_1, \xi_2, \xi_3) = x_1 x_2 y_3 + x_1 x_3 y_2 + x_2 x_3 y_1,$$

$$\sigma_{12}(\xi_1, \xi_2, \xi_3) = x_1 y_2 y_3 + x_2 y_1 y_3 + x_3 y_1 y_2.$$

Отметим, что

$$\sigma_{k0}(\xi_1, \dots, \xi_n) = \sigma_k(x_1, \dots, x_n), \quad k \in 0 : n;$$

$$\sigma_{0s}(\xi_1, \dots, \xi_n) = \sigma_s(y_1, \dots, y_n), \quad s \in 0 : n,$$

где $\sigma_k(x_1, \dots, x_n)$ и $\sigma_s(y_1, \dots, y_n)$ — основные симметрические полиномы над переменными из \mathbb{R} .

Нетрудно понять, что полиномы σ_{ks} являются симметричными относительно своих аргументов, то есть не меняются при их перестановке.

В случае, когда все аргументы полинома σ_{ks} совпадают, получаем

$$\sigma_{ks}(\xi, \dots, \xi) = C_n^k x^k C_{n-k}^s y^s = C_n^{k,s} x^k y^s, \quad (2)$$

где $C_n^{k,s} = \frac{n!}{k! s! (n-k-s)!}$ — так называемые *триномиальные* коэффициенты.

2°. Положим для удобства при $r \in 1 : n - 1$

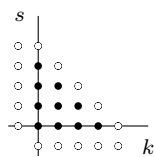


Рис. 1

$$\begin{aligned} \sigma_{k,-1}(\xi_1, \dots, \xi_r) &\equiv 0, & k \in 0 : r + 1, \\ \sigma_{-1,s}(\xi_1, \dots, \xi_r) &\equiv 0, & s \in 0 : r + 1, \\ \sigma_{ks}(\xi_1, \dots, \xi_r) &\equiv 0, & k, s \geq 0, \quad k + s = r + 1. \end{aligned} \quad (3)$$

Например, при $r = 3$ имеем 15 искусственно добавленных полиномов (рис. 1).

ЛЕММА 1. Основные симметрические полиномы (1) удовлетворяют рекуррентному соотношению

$$\begin{aligned} \sigma_{ks}(\xi_1, \dots, \xi_r, \xi_{r+1}) &= \sigma_{ks}(\xi_1, \dots, \xi_r) + x_{r+1} \sigma_{k-1,s}(\xi_1, \dots, \xi_r) + \\ &+ y_{r+1} \sigma_{k,s-1}(\xi_1, \dots, \xi_r), \\ k, s &\geq 0, \quad k + s \leq r + 1, \quad r \in 1 : n - 1. \end{aligned} \quad (4)$$

Доказательство. При $k = s = 0$ утверждение тривиально. При $k = 0, s = r + 1$ обе части (4) равны $y_1 y_2 \cdots y_{r+1}$. Пусть $k = 0, s \in 1 : r$. В этом случае соотношение (4) принимает вид

$$\sigma_s(y_1, \dots, y_r, y_{r+1}) = \sigma_s(y_1, \dots, y_r) + y_{r+1} \sigma_{s-1}(y_1, \dots, y_r).$$

Справедливость этого равенства следует из определения основных симметрических полиномов над \mathbb{R} (см., например, [1]).

Аналогично проводится доказательство при $s = 0, k \in 1 : r + 1$.

Для упрощения дальнейших записей введём обозначения $R = \{1, \dots, r\}$,

$$x_{I_k} = \prod_{i \in I_k} x_i, \quad y_{J_s} = \prod_{j \in J_s} y_j.$$

При $k, s \geq 1, k + s = r + 1$ по определению основных симметрических полиномов над \mathbb{R}^2 имеем

$$\begin{aligned} \sigma_{ks}(\xi_1, \dots, \xi_r, \xi_{r+1}) &= x_{r+1} \sum_{I_{k-1} \subset R} \sum_{J_s = R \setminus I_{k-1}} x_{I_{k-1}} y_{J_s} + \\ &+ y_{r+1} \sum_{I_k \subset R} \sum_{J_{s-1} = R \setminus I_k} x_{I_k} y_{J_{s-1}} = \\ &= x_{r+1} \sigma_{k-1,s}(\xi_1, \dots, \xi_r) + y_{r+1} \sigma_{k,s-1}(\xi_1, \dots, \xi_r). \end{aligned}$$

Это соответствует (4), поскольку, согласно (3), $\sigma_{ks}(\xi_1, \dots, \xi_r) \equiv 0$ при $k + s = r + 1$.

Обратимся к основному случаю $k, s \geq 1, k + s \in 2 : r$. Запишем

$$\begin{aligned} \sigma_{ks}(\xi_1, \dots, \xi_r, \xi_{r+1}) &= \sum_{I_k \subset R} \sum_{J_s \subset R \setminus I_k} x_{I_k} y_{J_s} + \\ &+ x_{r+1} \sum_{I_{k-1} \subset R} \sum_{J_s \subset R \setminus I_{k-1}} x_{I_{k-1}} y_{J_s} + y_{r+1} \sum_{I_k \subset R} \sum_{J_{s-1} \subset R \setminus I_k} x_{I_k} y_{J_{s-1}} = \\ &= \sigma_{ks}(\xi_1, \dots, \xi_r) + x_{r+1} \sigma_{k-1,s}(\xi_1, \dots, \xi_r) + y_{r+1} \sigma_{k,s-1}(\xi_1, \dots, \xi_r). \end{aligned}$$

Лемма доказана. \square

ЛЕММА 2. При любом $r \in 1 : n$ справедливо равенство

$$\begin{aligned} \sigma_{ks}(\xi_1, \dots, \alpha \xi'_r + \beta \xi''_r, \dots, \xi_n) &= \alpha \sigma_{ks}(\xi_1, \dots, \xi'_r, \dots, \xi_n) + \\ &+ \beta \sigma_{ks}(\xi_1, \dots, \xi''_r, \dots, \xi_n), \end{aligned}$$

если $\alpha + \beta = 1$.

Доказательство. В силу симметричности полиномов σ_{ks} достаточно рассмотреть случай $r = n$. Воспользуемся рекуррентным соотношением (4). Получим

$$\begin{aligned} \sigma_{ks}(\xi_1, \dots, \xi_{n-1}, \alpha \xi'_n + \beta \xi''_n) &= \sigma_{ks}(\xi_1, \dots, \xi_{n-1}) + \\ &+ (\alpha x'_n + \beta x''_n) \sigma_{k-1,s}(\xi_1, \dots, \xi_{n-1}) + (\alpha y'_n + \beta y''_n) \sigma_{k,s-1}(\xi_1, \dots, \xi_{n-1}) = \\ &= \alpha (\sigma_{ks}(\xi_1, \dots, \xi_{n-1}) + x'_n \sigma_{k-1,s}(\xi_1, \dots, \xi_{n-1}) + y'_n \sigma_{k,s-1}(\xi_1, \dots, \xi_{n-1})) + \\ &+ \beta (\sigma_{ks}(\xi_1, \dots, \xi_{n-1}) + x''_n \sigma_{k-1,s}(\xi_1, \dots, \xi_{n-1}) + y''_n \sigma_{k,s-1}(\xi_1, \dots, \xi_{n-1})) = \\ &= \alpha \sigma_{ks}(\xi_1, \dots, \xi_{n-1}, \xi'_n) + \beta \sigma_{ks}(\xi_1, \dots, \xi_{n-1}, \xi''_n). \end{aligned}$$

Лемма доказана. \square

3°. Полярной формой полинома степени n от двух переменных вида

$$P(\xi) = P(x, y) = \sum_{k=0}^n \sum_{s=0}^{n-k} C_n^{k,s} a_{ks} x^k y^s \quad (5)$$

называется выражение

$$p(\xi_1, \dots, \xi_n) = \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} \sigma_{ks}(\xi_1, \dots, \xi_n). \quad (6)$$

Очевидно, что полярная форма является симметричной функцией своих аргументов. С порождающим полиномом её связывает соотношение

$$p(\xi, \dots, \xi) = P(\xi).$$

(Здесь мы воспользовались формулой (2).) Значение полярной формы при конкретных значениях аргументов ξ_1, \dots, ξ_n называется полюсом полинома $P(\xi)$ вида (5).

Широко используемым свойством полярной формы является её мультиаффинность.

ПРЕДЛОЖЕНИЕ 1. При любом $r \in 1 : n$ справедливо равенство

$$\begin{aligned} p(\xi_1, \dots, \alpha \xi'_r + \beta \xi''_r, \dots, \xi_n) &= \alpha p(\xi_1, \dots, \xi'_r, \dots, \xi_n) + \\ &+ \beta p(\xi_1, \dots, \xi''_r, \dots, \xi_n), \end{aligned}$$

если $\alpha + \beta = 1$.

Доказательство непосредственно следует из определения полярной формы и леммы 2.

4°. Покажем, как эффективно вычислять полюсы. Зафиксируем ξ_1, \dots, ξ_n и построим $n + 1$ треугольных массивов $\{a_{ks}^i\}$ по правилу

$$\begin{aligned} a_{ks}^0 &= a_{ks}, \quad k \in 0 : n, \quad s \in 0 : n - k; \\ a_{ks}^i &= a_{ks}^{i-1} + x_{n-i+1} a_{k+1,s}^{i-1} + y_{n-i+1} a_{k,s+1}^{i-1}, \\ k &\in 0 : n - i, \quad s \in 0 : n - i - k, \quad i = 1, \dots, n. \end{aligned}$$

ПРЕДЛОЖЕНИЕ 2. Справедливо равенство $p(\xi_1, \dots, \xi_n) = a_{00}^n$.

Доказательство. При $n = 1$ утверждение очевидно. Пусть $n \geq 2$. Согласно рекуррентному соотношению (4) и соглашению (3) имеем

$$\begin{aligned} p(\xi_1, \dots, \xi_n) &= \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} [\sigma_{ks}(\xi_1, \dots, \xi_{n-1}) + x_n \sigma_{k-1,s}(\xi_1, \dots, \xi_{n-1}) + \\ &+ y_n \sigma_{k,s-1}(\xi_1, \dots, \xi_{n-1})] = \sum_{k=0}^{n-1} \sum_{s=0}^{n-1-k} a_{ks} \sigma_{ks}(\xi_1, \dots, \xi_{n-1}) + \\ &+ x_n \sum_{k=1}^n \sum_{s=0}^{n-k} a_{ks} \sigma_{k-1,s}(\xi_1, \dots, \xi_{n-1}) + y_n \sum_{k=0}^{n-1} \sum_{s=1}^{n-k} a_{ks} \sigma_{k,s-1}(\xi_1, \dots, \xi_{n-1}) = \end{aligned}$$

$$\begin{aligned}
&= \sum_{k=0}^{n-1} \sum_{s=0}^{n-1-k} [a_{ks}^0 + x_n a_{k+1,s}^0 + y_n a_{k,s+1}^0] \sigma_{ks}(\xi_1, \dots, \xi_{n-1}) = \\
&= \sum_{k=0}^{n-1} \sum_{s=0}^{n-1-k} a_{ks}^1 \sigma_{ks}(\xi_1, \dots, \xi_{n-1}).
\end{aligned}$$

Продолжив аналогично, придём к требуемому равенству

$$\begin{aligned}
p(\xi_1, \dots, \xi_n) &= \sum_{k=0}^{n-2} \sum_{s=0}^{n-2-k} a_{ks}^2 \sigma_{ks}(\xi_1, \dots, \xi_{n-2}) = \dots = \\
&= \sum_{k=0}^1 \sum_{s=0}^{1-k} a_{ks}^{n-1} \sigma_{ks}(\xi_1) = a_{00}^{n-1} + a_{01}^{n-1} y_1 + a_{10}^{n-1} x_1 = a_{00}^n.
\end{aligned}$$

Предложение доказано. \square

5°. Зафиксируем три точки на плоскости ξ_0, ξ_1, ξ_2 , не лежащие на одной прямой. Введём треугольный массив полюсов полинома $P(\xi)$ вида (5):

$$\begin{aligned}
p(\underbrace{\xi_0, \dots, \xi_0}_{k \text{ раз}}, \underbrace{\xi_1, \dots, \xi_1}_{s \text{ раз}}, \underbrace{\xi_2, \dots, \xi_2}_{(n-k-s) \text{ раз}}) &= p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s}), \\
k \in 0 : n, \quad s \in 0 : n - k.
\end{aligned} \tag{7}$$

Покажем, как по полюсам (7) восстановить значение $P(\xi)$ в любой точке $\xi \in \mathbb{R}^2$.

Разложим ξ по барицентрическим координатам относительно точек ξ_0, ξ_1, ξ_2 :

$$\xi = \alpha \xi_0 + \beta \xi_1 + (1 - \alpha - \beta) \xi_2.$$

Запишем рекуррентную формулу

$$\begin{aligned}
p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s-i}, \xi^i) &= \alpha p(\xi_0^{k+1}, \xi_1^s, \xi_2^{n-k-s-i}, \xi^{i-1}) + \\
&+ \beta p(\xi_0^k, \xi_1^{s+1}, \xi_2^{n-k-s-i}, \xi^{i-1}) + (1 - \alpha - \beta) p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s-i+1}, \xi^{i-1}),
\end{aligned}$$

справедливую в силу мультиаффинности и симметричности полярной формы. Если ввести обозначение

$$z_{ks}^i = p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s-i}, \xi^i),$$

то последняя формула примет вид

$$\begin{aligned}
z_{ks}^i &= (1 - \alpha - \beta) z_{ks}^{i-1} + \alpha z_{k+1,s}^{i-1} + \beta z_{k,s+1}^{i-1}, \\
k \in 0 : n - i, \quad s \in 0 : n - i - k, \quad i &= 1, \dots, n.
\end{aligned} \tag{8}$$

К этому нужно добавить начальные условия

$$z_{ks}^0 = p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s}), \quad k \in 0 : n, \quad s \in 0 : n - k. \quad (9)$$

Выполнив вычисления по формуле (8) при начальных условиях (9), найдём

$$z_{00}^n = p(\xi^n) = p(\xi, \dots, \xi) = P(\xi).$$

Один шаг схемы (8) определяет треугольную процедуру *включения узла*, которая является аналогом процедуры включения узла в одномерном случае (см. [1]).

6°. Зафиксируем числа z_{ks} , $k \in 0 : n$, $s \in 0 : n - k$, и рассмотрим задачу *интерполяции по полюсам*: найти полином $P(\xi)$ вида (5), такой, что

$$p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s}) = z_{ks}, \quad k \in 0 : n, \quad s \in 0 : n - k. \quad (10)$$

ПРЕДЛОЖЕНИЕ 3. *Интерполяционная задача (10) имеет решение при любых правых частях и это решение единственно.*

Доказательство. Напомним, что

$$p(\xi_1, \dots, \xi_n) = \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} \sigma_{ks}(\xi_1, \dots, \xi_n).$$

Значит, (10) есть система линейных уравнений относительно коэффициентов a_{ks} полинома $P(\xi)$.

Рассмотрим однородную систему

$$p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s}) = 0, \quad k \in 0 : n, \quad s \in 0 : n - k, \quad (11)$$

и покажем, что она имеет только нулевое решение. Отсюда будет следовать требуемое заключение.

Возьмём любое решение системы (11). Соответствующий полином вида (5) обозначим $P_0(\xi)$. По условию его полюсы $p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s})$, $k \in 0 : n$, $s \in 0 : n - k$, равны нулю. Применив процедуру включения узла (8), (9), получим, что $P_0(\xi) \equiv 0$. Но тогда и все коэффициенты полинома $P_0(\xi)$ равны нулю.

Предложение доказано. \square

ПРЕДЛОЖЕНИЕ 4. *Единственным решением интерполяционной задачи (10) является полином Бернштейна*

$$B(\xi) = \sum_{k=0}^n \sum_{s=0}^{n-k} z_{ks} C_n^{k,s} \alpha^k \beta^s (1 - \alpha - \beta)^{n-k-s}. \quad (12)$$

Здесь $\xi = \alpha \xi_0 + \beta \xi_1 + (1 - \alpha - \beta) \xi_2$.

Доказательство. Нам известно, что задача (10) имеет единственное решение $P(\xi)$, и числа $z_{ks} = p(\xi_0^k, \xi_1^s, \xi_2^{n-k-s})$ являются полюсами полинома $P(\xi)$. По полюсам с помощью процедуры включения узла (8), (9) восстанавливаются значения $P(\xi)$ в любой точке $\xi \in \mathbb{R}^2$. Вместе с тем (и это замечательный факт!), по той же формуле (8) при $z_{ks}^0 = z_{ks}$, $k \in 0 : n$, $s \in 0 : n - k$, вычисляется значение правой части формулы (12) (см. [2]). Значит, $P(\xi) \equiv B(\xi)$.

Предложение доказано. \square

Отметим, что правая часть (12) не зависит от векторов ξ_0, ξ_1, ξ_2 . Она зависит от коэффициентов α, β и треугольного массива $\{z_{ks}\}$.

ЛИТЕРАТУРА

1. Малозёмов В. Н. *Основные понятия теории полярных форм* // Семинар «DHA & CAGD». Избранные доклады. 2 декабря 2006 г. (<http://dha.spb.ru/rep06.shtml#1202>).
2. Григорьев М. И. *Полиномы Бернштейна от двух переменных* // Семинар «DHA & CAGD». Избранные доклады. 29 марта 2008 г. (<http://dha.spb.ru/rep08.shtml#0329>).

ОБОБЩЁННЫЕ ГАРМОНИЧЕСКИЕ ФРЕЙМЫ

Н. А. Соловьёва

16 апреля 2008 г.

Доклад представляет собой вариации на темы из [1].

1°. Напомним [2], что система ненулевых векторов $\{\varphi_0, \varphi_1, \dots, \varphi_{m-1}\}$ из \mathbb{C}^n при $m \geq n$ называется жёстким фреймом с константой фрейма $A > 0$, если выполнено одно из трёх эквивалентных условий:

- 1) $x = \frac{1}{A} \sum_{k=0}^{m-1} \langle x, \varphi_k \rangle \varphi_k$ для всех $x \in \mathbb{C}^n$;
- 2) $\sum_{k=0}^{m-1} |\langle x, \varphi_k \rangle|^2 = A \|x\|^2$ для всех $x \in \mathbb{C}^n$;
- 3) $\Phi \Phi^* = A I_n$,

где Φ — матрица со столбцами $\varphi_0, \varphi_1, \dots, \varphi_{m-1}$ и I_n — единичная матрица порядка n .

Если $\|\varphi_k\| = 1$ при всех $k \in 0 : m-1$, то константа фрейма A равна $\frac{m}{n}$.

2°. Пусть $m > n > 1$ и w_0, w_1, \dots, w_{n-1} — попарно различные корни m -й степени из единицы. Векторы

$$\varphi_k(j) = \frac{1}{\sqrt{n}} w_j^k, \quad j \in 0 : n-1, \quad k \in 0 : m-1, \quad (1)$$

образуют *гармонический фрейм*. В частности, $\varphi_0(j) = \frac{1}{\sqrt{n}}$ при всех $j \in 0 : n-1$. Если ввести диагональную матрицу $W = \text{diag}(w_0, w_1, \dots, w_{n-1})$, то формулу (1) можно переписать в виде

$$\varphi_k = W^k \varphi_0, \quad k \in 0 : m-1 \quad (W^0 = I_n). \quad (2)$$

Теперь возьмём комплексное число c , $|c| = 1$, и обозначим через c_0, c_1, \dots, c_{n-1} попарно различные корни m -й степени из c . Возьмём также n комплексных чисел b_0, b_1, \dots, b_{n-1} , по модулю равных единице. Векторы

$$\psi_k(j) = \frac{1}{\sqrt{n}} b_j c_j^k, \quad j \in 0 : n-1, \quad k \in 0 : m-1, \quad (3)$$

образуют *обобщённый гармонический фрейм*. В частности, $\psi_0(j) = \frac{1}{\sqrt{n}} b_j$, $j \in 0 : n-1$. Ясно, что $\|\psi_k\| = 1$ при всех $k \in 0 : m-1$.

Введём диагональные матрицы $B = \text{diag}(b_0, b_1, \dots, b_{n-1})$, $V = \text{diag}(c_0, c_1, \dots, c_{n-1})$. Формулу (3) можно переписать двумя способами:

$$\psi_k = V^k \psi_0, \quad k \in 0 : m-1; \quad (4)$$

$$\psi_k = B(V^k \varphi_0), \quad k \in 0 : m-1. \quad (5)$$

ПРЕДЛОЖЕНИЕ 1. *Обобщённый гармонический фрейм $\{\psi_0, \psi_1, \dots, \psi_{m-1}\}$ является жёстким фреймом с константой $A = \frac{m}{n}$.*

Доказательство. Обозначим через Ψ матрицу со столбцами $\psi_0, \psi_1, \dots, \psi_{m-1}$. При $j, s \in 0 : n-1$ имеем

$$(\Psi \Psi^*)[j, s] = \sum_{k=0}^{m-1} \psi_k(j) \overline{\psi_k(s)} \stackrel{(3)}{=} \frac{1}{n} b_j \bar{b}_s \sum_{k=0}^{m-1} (c_j \bar{c}_s)^k.$$

В частности, $(\Psi \Psi^*)[j, j] = \frac{m}{n}$. Если $j \neq s$, то по формуле для суммы членов геометрической прогрессии получим

$$\sum_{k=0}^{m-1} (c_j \bar{c}_s)^k = \frac{1 - c_j^m \bar{c}_s^m}{1 - c_j \bar{c}_s} = \frac{1 - c c}{1 - c_j \bar{c}_s} = 0,$$

так что $(\Psi \Psi^*)[j, s] = 0$. Таким образом,

$$\Psi \Psi^* = \frac{m}{n} I_n.$$

Остаётся сослаться на определение 3) жёсткого фрейма. \square

3°. В следующем предложении установлена связь между обобщёнными гармоническими фреймами и гармоническими.

ПРЕДЛОЖЕНИЕ 2. *Система векторов $\{\psi_k\}_{k=0}^{m-1}$ является обобщённым гармоническим фреймом тогда и только тогда, когда существует гармонический фрейм $\{\varphi_k\}_{k=0}^{m-1}$, комплексное число g , $|g| = 1$, и диагональная матрица B , диагональные элементы которой по модулю равны единице, такие, что*

$$\psi_k = B(g^k \varphi_k), \quad k \in 0 : m-1. \quad (6)$$

Доказательство. Пусть $\{\psi_k\}_{k=0}^{m-1}$ — обобщённый гармонический фрейм. Обозначим $c = e^{i\theta}$, $g = e^{i\theta/m}$, $w_j = g^{-1}c_j$. Тогда

$$w_j^m = g^{-m}c_j^m = g^{-m}c = 1, \quad j \in 0 : n-1,$$

то есть w_0, w_1, \dots, w_{n-1} — попарно различные корни m -й степени из единицы. Поскольку $c_j = g w_j$, то $V = g W$. Согласно (5) и (2)

$$\psi_k = B(g^k W^k \varphi_0) = B(g^k \varphi_k), \quad k \in 0 : m-1.$$

Наоборот, пусть векторы ψ_k определяются формулой (6). Положим $c_j = g w_j$. Тогда $c_j^m = g^m =: c$, то есть c_0, c_1, \dots, c_{n-1} — попарно различные корни m -й степени из c , $|c| = 1$. Очевидно, что $V = g W$. Учитывая (2), получаем

$$\psi_k = B(g^k W^k \varphi_0) = B(V^k \varphi_0), \quad k \in 0 : m-1.$$

Эта формула совпадает с (5), так что $\{\psi_k\}_{k=0}^{m-1}$ — обобщённый гармонический фрейм. Предложение доказано. \square

4°. Пусть по-прежнему $m > n > 1$. Возьмём унитарную матрицу U порядка n , единичный вектор $\eta_0 \in \mathbb{C}^n$ и построим последовательность единичных векторов

$$\eta_k = U \eta_{k-1}, \quad k = 1, \dots, m-1. \quad (7)$$

Обозначим $H = \{\eta_0, \eta_1, \dots, \eta_{m-1}\}$. Если система H — жёсткий фрейм, то её можно преобразовать в обобщённый гармонический фрейм. Для этого воспользуемся спектральным разложением унитарной матрицы U (см., например, [3, с. 248])

$$U = P \Lambda P^*, \quad (8)$$

где P — матрица, столбцами которой являются ортонормированные собственные векторы p_0, p_1, \dots, p_{n-1} матрицы U , и Λ — диагональная матрица, $\Lambda = \text{diag}(\lambda_0, \lambda_1, \dots, \lambda_{n-1})$, с диагональными элементами, по модулю равными единице. Систему векторов

$$\psi_k = P^* \eta_k, \quad k \in 0 : m-1, \quad (9)$$

обозначим через Ψ .

ПРЕДЛОЖЕНИЕ 3. Если H — жёсткий фрейм, то Ψ — обобщённый гармонический фрейм.

Доказательство. Имеем

$$\psi_0(j) = \langle \eta_0, p_j \rangle = \frac{1}{\sqrt{n}} b_j, \quad (10)$$

где $b_j = \sqrt{n} \langle \eta_0, p_j \rangle$. Покажем, что $|b_j| = 1$ при всех $j \in 0 : n-1$.

Разложим вектор η_0 по базису $\{p_0, p_1, \dots, p_{n-1}\}$. Получим

$$\eta_0 = \sum_{j=0}^{n-1} \langle \eta_0, p_j \rangle p_j = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} b_j p_j.$$

Если обозначить через b вектор с компонентами b_0, b_1, \dots, b_{n-1} , то последнюю формулу можно переписать в виде

$$\eta_0 = \frac{1}{\sqrt{n}} P b.$$

Согласно (7) и (8)

$$\eta_k = U^k \eta_0 = \frac{1}{\sqrt{n}} P \Lambda^k P^* P b = \frac{1}{\sqrt{n}} P \Lambda^k b = \frac{1}{\sqrt{n}} \sum_{s=0}^{n-1} b_s \lambda_s^k p_s.$$

Как следствие

$$|\langle \eta_k, p_j \rangle| = \frac{1}{\sqrt{n}} |b_j \lambda_j^k| = \frac{1}{\sqrt{n}} |b_j| \quad \text{при всех } k \in 0 : m-1.$$

По определению 2) жёсткого фрейма (при $x = p_j$)

$$\|p_j\|^2 = \frac{n}{m} \sum_{k=0}^{m-1} |\langle p_j, \eta_k \rangle|^2 = |b_j|^2,$$

так что $|b_j| = 1$ при всех $j \in 0 : n-1$.

Далее

$$\psi_k = P^* \eta_k = P^* U^k \eta_0 = P^* (P \Lambda^k P^*) \eta_0 = \Lambda^k (P^* \eta_0) = \Lambda^k \psi_0. \quad (11)$$

На основании (10) и (11) получаем

$$\psi_k(j) = \frac{1}{\sqrt{n}} b_j \lambda_j^k, \quad j \in 0 : n-1, \quad k \in 0 : m-1. \quad (12)$$

Остаётся показать, что λ_j — попарно различные корни m -й степени из некоторого числа $c \in \mathbb{C}$, $|c| = 1$.

Как известно [4], из того, что система H , построенная по формуле (7), является жёстким фреймом, следует равенство

$$U^m = c I_n,$$

где $c \in \mathbb{C}$, $|c| = 1$. Согласно (8)

$$P \Lambda^m P^* = c I_n,$$

так что $\Lambda^m = c I_n$. Это равносильно соотношению

$$\lambda_j^m = c \quad \text{при всех } j \in 0 : n - 1.$$

Значит, λ_j — корни m -й степени из c . Покажем, что $\lambda_j \neq \lambda_s$ при $j \neq s$.

Не вызовет недоразумений, если мы будем обозначать через Ψ и H матрицы со столбцами $\psi_0, \psi_1, \dots, \psi_{m-1}$ и $\eta_0, \eta_1, \dots, \eta_{m-1}$ соответственно. Согласно (9), $\Psi = P^* H$. Система H является жёстким фреймом. Жёстким фреймом будет и система Ψ , поскольку

$$\Psi \Psi^* = P^* H H^* P = \frac{m}{n} I_n.$$

В частности, $(\Psi \Psi^*)[j, s] = 0$ при $j \neq s$. Распишем это равенство подробно:

$$\sum_{k=0}^{m-1} \psi_k(j) \overline{\psi_k(s)} = 0.$$

В силу (12)

$$\frac{1}{n} b_j \bar{b}_s \sum_{k=0}^{m-1} (\lambda_j \bar{\lambda}_s)^k = 0.$$

Как следствие

$$\sum_{k=0}^{m-1} (\lambda_j \bar{\lambda}_s)^k = 0 \quad \text{при } j \neq s.$$

Ясно, что $\lambda_j \neq \lambda_s$ при $j \neq s$, ибо иначе мы получили бы противоречие с последним равенством. Предложение доказано. \square

З а м е ч а н и е. Предложение 3 позволяет усилить результат из [4]. Справедливо такое утверждение.

Если система H , построенная по формуле (7), является жёстким фреймом, то $U^m = c I_n$, где $c \in \mathbb{C}$, $|c| = 1$. При этом собственные числа унитарной матрицы U суть попарно различные корни m -й степени из c .

5°. Приведём пример к предложению 3.

ПРИМЕР 1. Пусть $n = 2$, $m = 3$. Рассмотрим фрейм Мерседес-Бенц, состоящий из векторов

$$b_0 = (0, 1)^T, \quad b_1 = \left(-\frac{\sqrt{3}}{2}, -\frac{1}{2}\right)^T, \quad b_2 = \left(\frac{\sqrt{3}}{2}, -\frac{1}{2}\right)^T.$$

Как известно [5, с. 100], это жёсткий фрейм. Нетрудно проверить, что $b_k = U b_{k-1}$, $k = 1, 2$, где

$$U = \begin{bmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix}.$$

Матрица U — унитарная с собственными числами $\lambda_0 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = \omega_3$, $\lambda_1 = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = \omega_3^2$ и собственными векторами

$$p_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}, \quad p_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}.$$

Все условия предложения 3 выполнены. Построим обобщённый гармонический фрейм.

Имеем

$$\begin{aligned} P &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix}, & P^* &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}, \\ \psi_0 &= P^* b_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} i \\ -i \end{bmatrix}, \\ \psi_1 &= \frac{1}{\sqrt{2}} \begin{bmatrix} -\frac{\sqrt{3}}{2} - \frac{1}{2}i \\ -\frac{\sqrt{3}}{2} + \frac{1}{2}i \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} i\lambda_0 \\ -i\lambda_1 \end{bmatrix}, \\ \psi_2 &= \frac{1}{\sqrt{2}} \begin{bmatrix} \frac{\sqrt{3}}{2} - \frac{1}{2}i \\ \frac{\sqrt{3}}{2} + \frac{1}{2}i \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} i\lambda_0^2 \\ -i\lambda_1^2 \end{bmatrix}. \end{aligned}$$

В данном случае $b_0 = i$, $b_1 = -i$.

6°. Условие жёсткости фрейма H в предложении 3 можно заменить условиями на унитарную матрицу U и начальный вектор η_0 .

ПРЕДЛОЖЕНИЕ 4. Система векторов Ψ является обобщённым гармоническим фреймом тогда и только тогда, когда

- 1) $|\langle \eta_0, p_j \rangle| = \frac{1}{\sqrt{n}}$ при всех $j \in 0 : n-1$;
- 2) собственные числа $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ матрицы U суть попарно различные корни m -й степени из некоторого числа $c \in \mathbb{C}$, $|c| = 1$.

Доказательство. По построению (формулы (7) и (9))

$$\psi_k(j) = \frac{1}{\sqrt{n}} b_j \lambda_j^k, \quad j \in 0 : n-1, \quad k \in 0 : m-1, \quad (13)$$

где $b_j = \sqrt{n} \langle \eta_0, p_j \rangle$. Если выполнены условия 1) и 2), то по определению Ψ — обобщённый гармонический фрейм.

Наоборот, пусть Ψ — обобщённый гармонический фрейм. Согласно (3), $|\psi_0(j)| \equiv \frac{1}{\sqrt{n}}$, что в применении к формуле (13) даёт $|b_j| = 1$ при всех $j \in 0 : n-1$. Условие 1) выполнено.

Далее по предложению 1 обобщённый гармонический фрейм Ψ является жёстким фреймом. Учитывая этот факт и представление (13), так же, как в конце доказательства предложения 3, получаем $\lambda_j \neq \lambda_s$ при $j \neq s$.

Вместе с Ψ жёстким фреймом будет и система H . Действительно, как отмечалось, $\Psi = P^*H$, так что $H = P\Psi$ и

$$HH^* = P\Psi\Psi^*P^* = \frac{m}{n}I_n.$$

В этом случае $U^m = cI_n$, где $c \in \mathbb{C}$, $|c| = 1$. Отсюда следует, что $\lambda_j^m = c$ при всех $j \in 0 : n-1$, то есть λ_j — корни m -й степени из c . Условие 2) также выполнено. Предложение доказано. \square

7°. Приведём примеры к предложению 4.

ПРИМЕР 2 (условия 1) и 2) выполнены). Пусть $n = 2$, $m = 3$. Рассмотрим унитарную матрицу U с собственными числами $\lambda_0 = 1$, $\lambda_1 = \omega_3$ и ортонормированными собственными векторами

$$p_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad p_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

В этом случае

$$P = P^* = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$U = \frac{1}{2} \begin{bmatrix} 1 + \omega_3 & 1 - \omega_3 \\ 1 - \omega_3 & 1 + \omega_3 \end{bmatrix}.$$

Возьмём начальный вектор $\eta_0 = (1, 0)^T$. Для него

$$|\langle \eta_0, p_0 \rangle| = |\langle \eta_0, p_1 \rangle| = \frac{1}{\sqrt{2}}.$$

Таким образом, условия 1) и 2) выполнены.

Найдём векторы η_1 и η_2 :

$$\eta_1 = \frac{1}{2} \begin{bmatrix} 1 + \omega_3 \\ 1 - \omega_3 \end{bmatrix}, \quad \eta_2 = \frac{1}{2} \begin{bmatrix} 1 + \omega_3^2 \\ 1 - \omega_3^2 \end{bmatrix}.$$

Вычислим векторы ψ_k :

$$\psi_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \psi_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \omega_3 \end{bmatrix}, \quad \psi_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ \omega_3^2 \end{bmatrix}.$$

Получили, что $\{\psi_0, \psi_1, \psi_2\}$ — гармонический фрейм.

ПРИМЕР 3 (нарушено условие 1)). Пусть $n = 2$, $m = 3$. Рассмотрим унитарную матрицу U с собственными числами $\lambda_0 = 1$, $\lambda_1 = \omega_3$ и ортонормированными собственными векторами

$$p_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad p_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

В этом случае $P = P^* = I_2$ и

$$U = \begin{bmatrix} 1 & 0 \\ 0 & \omega_3 \end{bmatrix}.$$

Возьмём начальный вектор $\eta_0 = (1, 0)^T$. Для него

$$|\langle \eta_0, p_0 \rangle| = 1, \quad |\langle \eta_0, p_1 \rangle| = 0,$$

то есть условие 1) нарушено.

Найдём векторы η_1 и η_2 :

$$\eta_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \eta_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Вычислим векторы ψ_k :

$$\psi_0 = \psi_1 = \psi_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Система $\{\psi_0, \psi_1, \psi_2\}$ не является жёстким фреймом, так как линейные комбинации её элементов не порождают пространства \mathbb{C}^2 (см. определение 1) жёсткого фрейма). Согласно предложению 1 она не может быть и обобщённым гармоническим фреймом.

ПРИМЕР 4 (нарушено условие 2)). Рассмотрим унитарную матрицу U второго порядка с собственными числами $\lambda_0 = 1$, $\lambda_1 = i$ и ортонормированными собственными векторами

$$p_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad p_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

В этом случае $P = P^* = I_2$ и

$$U = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

Условие 2) при $m = 3$ нарушено, поскольку $\lambda_0^3 \neq \lambda_1^3$.

Возьмём начальный вектор $\eta_0 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$. Для него

$$|\langle \eta_0, p_0 \rangle| = |\langle \eta_0, p_1 \rangle| = \frac{1}{\sqrt{2}},$$

то есть условие 1) выполнено.

Найдём векторы η_1 и η_2 :

$$\eta_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}, \quad \eta_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

Имеем $\psi_0 = \eta_0$, $\psi_1 = \eta_1$, $\psi_2 = \eta_2$. У матрицы

$$\Psi = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & i & -1 \end{bmatrix}$$

строки не ортогональны. Значит, система $\{\psi_0, \psi_1, \psi_2\}$ не является жёстким фреймом (см. определение 3)) и, тем более, не будет обобщённым гармоническим фреймом (см. предложение 1).

Отметим, что $\psi_3 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}$. При $m = 4$ система $\{\psi_0, \psi_1, \psi_2, \psi_3\}$ образует гармонический фрейм.

ЛИТЕРАТУРА

1. Casazza P. G., Kovačević J. *Uniform Tight Frames with Erasures* // Adv. Comp. Math. 2003. V. 18. No. 2–4. P. 387–430.
2. Малозёмов В. Н., Певный А. Б. *Системы Мерседес-Бенц и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 28 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0228>).
3. Гантмахер Ф. Р. *Теория матриц*. Изд. 2-е. М.: Наука, 1966. 576 с.
4. Соловьёва Н. А. *О жёстких фреймах специального вида* // Семинар «DHA & CAGD». Избранные доклады. 12 марта 2008 г. (<http://dha.spb.ru/rep08.shtml#0312>).
5. Добеши И. *Десять лекций по вейвлетам*. Пер. с англ. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. 464 с.

ОСНОВНАЯ ЛЕММА ТЕОРИИ ПОЛЯРНЫХ ФОРМ ПОЛИНОМОВ ОТ ДВУХ ПЕРЕМЕННЫХ

М. И. Григорьев В. Н. Малозёмов А. Н. Сергеев

26 апреля 2008 г.

Данный доклад является продолжением доклада [1].

1°. Точки из \mathbb{R}^2 будем обозначать $\xi = (x, y)$, $\xi_i = (x_i, y_i)$.

Рассмотрим алгебраический полином степени n от двух переменных вида

$$P(\xi) = P(x, y) = \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} C_n^{k,s} x^k y^s. \quad (1)$$

Пусть $\alpha, \beta \geq 0$, $\alpha + \beta = r$, $r \in 1 : n$. Обозначим

$$P_{\alpha\beta}^{(r)}(\xi) = \frac{\partial^r P(x, y)}{\partial x^\alpha \partial y^\beta}.$$

ЛЕММА 1. *Справедлива формула*

$$P_{\alpha\beta}^{(r)}(\xi) = \frac{n!}{(n-r)!} \sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} a_{k+\alpha, s+\beta} C_{n-r}^{k,s} x^k y^s. \quad (2)$$

Доказательство. Имеем

$$\frac{\partial^\alpha P(x, y)}{\partial x^\alpha} = \frac{\partial^\alpha}{\partial x^\alpha} \left(\sum_{k=\alpha}^n x^k \sum_{s=0}^{n-k} a_{ks} C_n^{k,s} y^s \right) =$$

$$\begin{aligned}
&= \sum_{k=\alpha}^n \sum_{s=0}^{n-k} a_{ks} C_n^{k,s} \frac{k!}{(k-\alpha)!} x^{k-\alpha} y^s = \\
&= \sum_{s=0}^{n-\alpha} y^s \sum_{k=\alpha}^{n-s} a_{ks} C_n^{k,s} \frac{k!}{(k-\alpha)!} x^{k-\alpha}.
\end{aligned}$$

Далее

$$\frac{\partial^{\alpha+\beta} P(x, y)}{\partial x^\alpha \partial y^\beta} = \sum_{s=\beta}^{n-\alpha} \sum_{k=\alpha}^{n-s} a_{ks} C_n^{k,s} \frac{k!}{(k-\alpha)!} \frac{s!}{(s-\beta)!} x^{k-\alpha} y^{s-\beta}.$$

Отметим, что

$$C_n^{k,s} \frac{k! s!}{(k-\alpha)! (s-\beta)!} = \frac{n!}{(n-\alpha-\beta)!} C_{n-\alpha-\beta}^{k-\alpha, s-\beta}.$$

Поэтому

$$\begin{aligned}
P_{\alpha\beta}^{(r)}(\xi) &= \frac{n!}{(n-r)!} \sum_{s=\beta}^{n-\alpha} \sum_{k=\alpha}^{n-s} a_{ks} C_{n-r}^{k-\alpha, s-\beta} x^{k-\alpha} y^{s-\beta} = \\
&= \frac{n!}{(n-r)!} \sum_{k=\alpha}^{n-\beta} \sum_{s=\beta}^{n-k} a_{ks} C_{n-r}^{k-\alpha, s-\beta} x^{k-\alpha} y^{s-\beta} = \\
&= \frac{n!}{(n-r)!} \sum_{k=\alpha}^{n-\beta} \sum_{s=0}^{n-k-\beta} a_{k, s+\beta} C_{n-r}^{k-\alpha, s} x^{k-\alpha} y^s = \\
&= \frac{n!}{(n-r)!} \sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} a_{k+\alpha, s+\beta} C_{n-r}^{k,s} x^k y^s.
\end{aligned}$$

Лемма доказана. \square

2°. Введём полярные формы $p(\xi_1, \dots, \xi_n)$ полинома $P(\xi)$ и $p_{\alpha\beta}(\xi_1, \dots, \xi_{n-r})$ полинома $\frac{(n-r)!}{n!} P_{\alpha\beta}^{(r)}(\xi)$. Согласно (1) и (2)

$$\begin{aligned}
p(\xi_1, \dots, \xi_n) &= \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} \sigma_{ks}(\xi_1, \dots, \xi_n), \\
p_{\alpha\beta}(\xi_1, \dots, \xi_{n-r}) &= \sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} a_{k+\alpha, s+\beta} \sigma_{ks}(\xi_1, \dots, \xi_{n-r}).
\end{aligned}$$

В частности,

$$p(\xi^n) = P(\xi), \quad p_{\alpha\beta}(\xi^{n-r}) = \frac{(n-r)!}{n!} P_{\alpha\beta}^{(r)}(\xi). \quad (3)$$

Пусть $\eta \in \mathbb{R}^2$, $\eta = (\eta_x, \eta_y)$. Рассмотрим полюсы вида

$$p(\eta^{n-q}, \eta + \xi_1, \dots, \eta + \xi_q), \quad q \in 1 : n. \quad (4)$$

ЛЕММА 2. *Полюсы (4) допускают представление*

$$p(\eta^{n-q}, \eta + \xi_1, \dots, \eta + \xi_q) = \sum_{\alpha=0}^q \sum_{\beta=0}^{q-\alpha} p_{\alpha\beta}(\eta^{n-r}) \sigma_{\alpha\beta}(\xi_1, \dots, \xi_q), \quad (5)$$

где $r = \alpha + \beta$.

Доказательство. Напомним рекуррентное соотношение для симметрических полиномов от переменных из \mathbb{R}^2 (см. [1]):

$$\begin{aligned} \sigma_{\alpha\beta}(\xi_1, \dots, \xi_q) &= \sigma_{\alpha\beta}(\xi_1, \dots, \xi_{q-1}) + x_q \sigma_{\alpha-1,\beta}(\xi_1, \dots, \xi_{q-1}) + \\ &+ y_q \sigma_{\alpha,\beta-1}(\xi_1, \dots, \xi_{q-1}), \quad \alpha, \beta \geq 0, \quad \alpha + \beta \leq q, \quad q \in 2 : n. \end{aligned} \quad (6)$$

Здесь приняты соглашения

$$\begin{aligned} \sigma_{-1,\beta}(\xi_1, \dots, \xi_{q-1}) &\equiv \sigma_{\alpha,-1}(\xi_1, \dots, \xi_{q-1}) \equiv 0, \quad \alpha, \beta \in 0 : q; \\ \sigma_{\alpha\beta}(\xi_1, \dots, \xi_{q-1}) &\equiv 0, \quad \alpha, \beta \geq 0, \quad \alpha + \beta = q. \end{aligned} \quad (7)$$

Зафиксируем $q \in 2 : n$. С помощью (6) и (7) начнём преобразовывать правую часть формулы (5):

$$\begin{aligned} &\sum_{\alpha=0}^q \sum_{\beta=0}^{q-\alpha} p_{\alpha\beta}(\eta^{n-r}) [\sigma_{\alpha\beta}(\xi_1, \dots, \xi_{q-1}) + x_q \sigma_{\alpha-1,\beta}(\xi_1, \dots, \xi_{q-1}) + \\ &+ y_q \sigma_{\alpha,\beta-1}(\xi_1, \dots, \xi_{q-1})] = \sum_{\alpha=0}^{q-1} \sum_{\beta=0}^{q-1-\alpha} p_{\alpha\beta}(\eta^{n-r}) \sigma_{\alpha\beta}(\xi_1, \dots, \xi_{q-1}) + \\ &+ x_q \sum_{\alpha=1}^q \sum_{\beta=0}^{q-\alpha} p_{\alpha\beta}(\eta^{n-r}) \sigma_{\alpha-1,\beta}(\xi_1, \dots, \xi_{q-1}) + \\ &+ y_q \sum_{\alpha=0}^{q-1} \sum_{\beta=1}^{q-\alpha} p_{\alpha\beta}(\eta^{n-r}) \sigma_{\alpha,\beta-1}(\xi_1, \dots, \xi_{q-1}) = \\ &= \sum_{\alpha=0}^{q-1} \sum_{\beta=0}^{q-1-\alpha} [p_{\alpha\beta}(\eta^{n-r}) + x_q p_{\alpha+1,\beta}(\eta^{n-r-1}) + y_q p_{\alpha,\beta+1}(\eta^{n-r-1})] \sigma_{\alpha\beta}(\xi_1, \dots, \xi_{q-1}). \end{aligned}$$

Выражение в квадратных скобках приводится к виду

$$\begin{aligned} &\sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} a_{k+\alpha,s+\beta} \sigma_{ks}(\eta^{n-r}) + x_q \sum_{k=0}^{n-r-1} \sum_{s=0}^{n-r-1-k} a_{k+\alpha+1,s+\beta} \sigma_{ks}(\eta^{n-r-1}) + \\ &+ y_q \sum_{k=0}^{n-r-1} \sum_{s=0}^{n-r-1-k} a_{k+\alpha,s+\beta+1} \sigma_{ks}(\eta^{n-r-1}) = \end{aligned}$$

$$\begin{aligned}
&= \sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} a_{k+\alpha, s+\beta} [\sigma_{ks}(\eta^{n-r-1}) + \eta_x \sigma_{k-1, s}(\eta^{n-r-1}) + \eta_y \sigma_{k, s-1}(\eta^{n-r-1})] + \\
&\quad + \sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} a_{k+\alpha, s+\beta} [x_q \sigma_{k-1, s}(\eta^{n-r-1}) + y_q \sigma_{k, s-1}(\eta^{n-r-1})] = \\
&= \sum_{k=0}^{n-r} \sum_{s=0}^{n-r-k} a_{k+\alpha, s+\beta} \sigma_{ks}(\eta^{n-r-1}, \eta + \xi_q) = p_{\alpha\beta}(\eta^{n-r-1}, \eta + \xi_q).
\end{aligned}$$

Значит,

$$\sum_{\alpha=0}^q \sum_{\beta=0}^{q-\alpha} p_{\alpha\beta}(\eta^{n-r}) \sigma_{\alpha\beta}(\xi_1, \dots, \xi_q) = \sum_{\alpha=0}^{q-1} \sum_{\beta=0}^{q-1-\alpha} p_{\alpha\beta}(\eta^{n-r-1}, \eta + \xi_q) \sigma_{\alpha\beta}(\xi_1, \dots, \xi_{q-1}).$$

Продолжив аналогично, придём к требуемому равенству:

$$\begin{aligned}
&\sum_{\alpha=0}^{q-1} \sum_{\beta=0}^{q-1-\alpha} p_{\alpha\beta}(\eta^{n-r-1}, \eta + \xi_q) \sigma_{\alpha\beta}(\xi_1, \dots, \xi_{q-1}) = \\
&= \sum_{\alpha=0}^{q-2} \sum_{\beta=0}^{q-2-\alpha} p_{\alpha\beta}(\eta^{n-r-2}, \eta + \xi_{q-1}, \eta + \xi_q) \sigma_{\alpha\beta}(\xi_1, \dots, \xi_{q-2}) = \dots = \\
&= \sum_{\alpha=0}^1 \sum_{\beta=0}^{1-\alpha} p_{\alpha\beta}(\eta^{n-r-q+1}, \eta + \xi_2, \dots, \eta + \xi_q) \sigma_{\alpha\beta}(\xi_1) = \\
&= p(\eta^{n-q}, \eta + \xi_1, \dots, \eta + \xi_q).
\end{aligned}$$

Поясним последний переход:

$$\begin{aligned}
&p_{00}(\eta^{n-q+1}, \eta + \xi_2, \dots, \eta + \xi_q) + y_1 p_{01}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q) + \\
&+ x_1 p_{10}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q) = \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} [\sigma_{ks}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q) + \\
&+ \eta_x \sigma_{k-1, s}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q) + \eta_y \sigma_{k, s-1}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q)] + \\
&+ y_1 \sum_{k=0}^{n-1} \sum_{s=0}^{n-1-k} a_{k, s+1} \sigma_{ks}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q) + \\
&+ x_1 \sum_{k=0}^{n-1} \sum_{s=0}^{n-1-k} a_{k+1, s} \sigma_{ks}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q) =
\end{aligned}$$

$$\begin{aligned}
&= \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} [\sigma_{ks}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q) + \\
&\quad + (\eta_x + x_1) \sigma_{k-1,s}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q) + \\
&\quad + (\eta_y + y_1) \sigma_{k,s-1}(\eta^{n-q}, \eta + \xi_2, \dots, \eta + \xi_q)] = \\
&= \sum_{k=0}^n \sum_{s=0}^{n-k} a_{ks} \sigma_{ks}(\eta^{n-q}, \eta + \xi_1, \dots, \eta + \xi_q) = p(\eta^{n-q}, \eta + \xi_1, \dots, \eta + \xi_q). \quad (8)
\end{aligned}$$

Равенство (8) остаётся справедливым и при $q = 1$, что соответствует (5) при $q = 1$. Лемма доказана. \square

При $q = n$ формула (5) принимает вид

$$p(\eta + \xi_1, \dots, \eta + \xi_n) = \sum_{\alpha=0}^n \sum_{\beta=0}^{n-\alpha} p_{\alpha\beta}(\eta^{n-r}) \sigma_{\alpha\beta}(\xi_1, \dots, \xi_n).$$

Положим здесь $\xi_1 = \dots = \xi_n =: \xi$. Согласно (3) получим

$$\begin{aligned}
p((\eta + \xi)^n) &= P(\eta + \xi) = \sum_{\alpha=0}^n \sum_{\beta=0}^{n-\alpha} \frac{(n-r)!}{n!} P_{\alpha\beta}^{(r)}(\eta) C_n^{\alpha,\beta} x^\alpha y^\beta = \\
&= \sum_{\alpha=0}^n \sum_{\beta=0}^{n-\alpha} \frac{P_{\alpha\beta}^{(r)}(\eta)}{\alpha! \beta!} x^\alpha y^\beta.
\end{aligned}$$

Таким образом, (5) есть обобщение формулы Тейлора для полиномов степени n от двух переменных.

3°. Рассмотрим два полинома $P_1(\xi)$ и $P_2(\xi)$ степени n с соответствующими полярными формами $p^1(\xi_1, \dots, \xi_n)$ и $p^2(\xi_1, \dots, \xi_n)$.

ЛЕММА 3 (Основная). *Для того чтобы в некоторой точке $\eta \in \mathbb{R}^2$ полиномы $P_1(\xi)$ и $P_2(\xi)$ совпадали вместе со всеми их частными производными до q -го порядка включительно, необходимо и достаточно, чтобы при любых η_1, \dots, η_q из \mathbb{R}^2 выполнялось равенство*

$$p^1(\eta^{n-q}, \eta_1, \dots, \eta_q) = p^2(\eta^{n-q}, \eta_1, \dots, \eta_q). \quad (9)$$

Доказательство. Необходимость. Из условия леммы и (3) следует, что $p_{\alpha\beta}^1(\eta^{n-r}) = p_{\alpha\beta}^2(\eta^{n-r})$ при всех $\alpha, \beta \geq 0$, $r := \alpha + \beta \leq q$. Остаётся сослаться на лемму 2.

Достаточность. Равенство $p^1(\eta^n) = p^2(\eta^n)$ гарантирует, что $P_1(\eta) = P_2(\eta)$.

Пусть $q \in 1 : n$. Возьмём три вектора ξ_1, ξ_2, ξ_3 , не лежащие на одной прямой. Согласно (9) при $k \in 0 : q, s \in 0 : q - k$ имеем

$$p^1(\eta^{n-q}, (\eta + \xi_1)^k, (\eta + \xi_2)^s, (\eta + \xi_3)^{q-k-s}) = p^2(\eta^{n-q}, (\eta + \xi_1)^k, (\eta + \xi_2)^s, (\eta + \xi_3)^{q-k-s}).$$

На основании (5) при тех же k, s получаем

$$\sum_{\alpha=0}^q \sum_{\beta=0}^{q-\alpha} [p_{\alpha\beta}^1(\eta^{n-r}) - p_{\alpha\beta}^2(\eta^{n-r})] \sigma_{\alpha\beta}(\xi_1^k, \xi_2^s, \xi_3^{q-k-s}) = 0. \quad (10)$$

Соотношение (10) имеет прямое отношение к интерполяции по полюсам (см. [1]). Из (10) и однозначной разрешимости задачи интерполяции по полюсам следует, что $p_{\alpha\beta}^1(\eta^{n-r}) = p_{\alpha\beta}^2(\eta^{n-r})$ при $\alpha \in 0 : q, \beta \in 0 : q - \alpha$. Это вместе с (3) гарантирует равенство всех смешанных производных полиномов $P_1(\xi)$ и $P_2(\xi)$ до q -го порядка включительно в точке $\xi = \eta$.

Лемма доказана. \square

4°. По поводу дальнейших результатов, связанных с полярными формами полиномов от двух переменных, см. обзорную статью [2].

ЛИТЕРАТУРА

1. Григорьев М. И., Сергеев А. Н. *Полярная форма полиномов от двух переменных* // Семинар «DHA & CAGD». Избранные доклады. 12 апреля 2008 г. (<http://dha.spb.ru/rep08.shtml#0412>).
2. Seidel H.-P. *An introduction to polar forms* // IEEE Computer Graphics and Applications. 1993. Vol. 13. No. 1. P. 38-46.

АНСАМБЛИ ДИСКРЕТНЫХ ПЕРИОДИЧЕСКИХ СИГНАЛОВ

В. Н. Малозёмов С. М. Машарский

28 мая 2008 г.

1°. Конечное множество \mathcal{Q} сигналов x из \mathbb{C}_N с одинаковой энергией

$$E(x) := \sum_{j=0}^{N-1} |x(j)|^2 = A$$

называется *ансамблем сигналов*. Наиболее интересны ансамбли, в которых сигналы максимально отличаются друг от друга при всех возможных сдвигах по времени.

Два сигнала x, y называются *некоррелированными*, если их взаимная корреляция тождественно равна нулю, т. е.

$$R_{xy}(j) := \sum_{k=0}^{N-1} x(k) \bar{y}(k-j) \equiv 0.$$

Поскольку

$$\overline{R_{yx}(j)} = \sum_{k=0}^{N-1} \bar{y}(k) x(k-j) = \sum_{k=0}^{N-1} x(k) \bar{y}(k+j) = R_{xy}(-j),$$

то одновременно с тождеством $R_{xy}(j) \equiv 0$ выполняется тождество $R_{yx}(j) \equiv 0$. Перепишем эти тождества в эквивалентном виде

$$\langle x, y(\cdot - j) \rangle = 0, \quad \langle y, x(\cdot - j) \rangle = 0 \quad \text{при всех } j \in \mathbb{Z}.$$

Видим, что некоррелированность сигналов x, y соответствует тому, что сигнал x ортогонален всем сдвигам сигнала y и наоборот, сигнал y ортогонален всем сдвигам сигнала x . В частности, сигналы x и y ортогональны. Как следствие получаем, что количество некоррелированных сигналов в ансамбле не превосходит N .

Оказывается, существуют ансамбли, содержащие ровно N некоррелированных сигналов. Например,

$$\mathcal{Q} = \{u_k(j) = \omega_N^{kj} \mid k \in 0 : N-1\}.$$

Ясно, что \mathcal{Q} — ансамбль с $A = N$. При этом

$$R_{u_k, u_s}(j) = \sum_{l=0}^{N-1} u_k(l) \overline{u_s}(l-j) = \sum_{l=0}^{N-1} \omega_N^{l(k-s)+sj} = \omega_N^{sj} N \delta_N(k-s).$$

В частности, $R_{u_k, u_s}(j) \equiv 0$ при $k \neq s$. Значит, ансамбль $\mathcal{Q} = \{u_k\}_{k=0}^{N-1}$ состоит из N некоррелированных сигналов.

Отметим, что $R_{u_k, u_k}(j) = N u_k(j)$, $j \in \mathbb{Z}$.

2°. Введём две характеристики произвольного ансамбля сигналов \mathcal{Q} :

$$R_a = \max_{x \in \mathcal{Q}} \max_{j \in 1:N-1} |R_{xx}(j)|,$$

$$R_c = \max_{\substack{x, y \in \mathcal{Q} \\ x \neq y}} \max_{j \in 0:N-1} |R_{xy}(j)|.$$

Если $R_a = 0$, то все сигналы из \mathcal{Q} являются дельта-коррелированными. Если же $R_c = 0$, то сигналы из \mathcal{Q} попарно некоррелированы. Следующее утверждение показывает, что не существует ансамбля \mathcal{Q} , у которого одновременно и $R_a = 0$, и $R_c = 0$.

ПРЕДЛОЖЕНИЕ 1. Пусть ансамбль \mathcal{Q} состоит из m сигналов и $E(x) = A$ при всех $x \in \mathcal{Q}$. Тогда

$$N \left(\frac{R_c}{A} \right)^2 + \frac{N-1}{m-1} \left(\frac{R_a}{A} \right)^2 \geq 1. \quad (1)$$

Неравенство (1) называется *неравенством Сидельникова-Сарвате* [1, 2, 3].

Доказательство. Нам потребуется формула

$$\sum_{j=0}^{N-1} |R_{xy}(j)|^2 = \sum_{j=0}^{N-1} R_{xx}(j) \overline{R_{yy}}(j). \quad (2)$$

Её справедливость проверяется так:

$$\sum_{j=0}^{N-1} |R_{xy}(j)|^2 = \sum_{j=0}^{N-1} \left(\sum_{k=0}^{N-1} x(k) \overline{y}(k-j) \right) \left(\sum_{l=0}^{N-1} \overline{x}(l) y(l-j) \right) =$$

$$\begin{aligned}
&= \sum_{k,l=0}^{N-1} x(k) \bar{x}(l) \sum_{j=0}^{N-1} y(l-j) \bar{y}(l-j+(k-l)) = \\
&= \sum_{k,l=0}^{N-1} x(k) \bar{x}(l) \sum_{j=0}^{N-1} y(j) \bar{y}(j+(k-l)) = \sum_{k=0}^{N-1} x(k) \sum_{l=0}^{N-1} \bar{x}(l) \overline{R_{yy}}(k-l) = \\
&= \sum_{k=0}^{N-1} x(k) \sum_{l=0}^{N-1} \bar{x}(k-l) \overline{R_{yy}}(l) = \sum_{l=0}^{N-1} \overline{R_{yy}}(l) R_{xx}(l).
\end{aligned}$$

Согласно (2) имеем

$$\begin{aligned}
\sum_{j=0}^{N-1} \left| \sum_{x \in \mathcal{Q}} R_{xx}(j) \right|^2 &= \sum_{j=0}^{N-1} \left(\sum_{x \in \mathcal{Q}} R_{xx}(j) \right) \left(\sum_{y \in \mathcal{Q}} \overline{R_{yy}}(j) \right) = \\
&= \sum_{x,y \in \mathcal{Q}} \sum_{j=0}^{N-1} R_{xx}(j) \overline{R_{yy}}(j) = \sum_{x,y \in \mathcal{Q}} \sum_{j=0}^{N-1} |R_{xy}(j)|^2 = \\
&= \sum_{\substack{x,y \in \mathcal{Q} \\ x \neq y}} \sum_{j=0}^{N-1} |R_{xy}(j)|^2 + \sum_{x \in \mathcal{Q}} \sum_{j=0}^{N-1} |R_{xx}(j)|^2. \tag{3}
\end{aligned}$$

Займёмся оценками. Поскольку $R_{xx}(0) = E(x) = A$, то

$$\begin{aligned}
\sum_{j=0}^{N-1} \left| \sum_{x \in \mathcal{Q}} R_{xx}(j) \right|^2 &\geq \left| \sum_{x \in \mathcal{Q}} R_{xx}(0) \right|^2 = m^2 A^2, \\
\sum_{x \in \mathcal{Q}} \sum_{j=0}^{N-1} |R_{xx}(j)|^2 &= \sum_{x \in \mathcal{Q}} \sum_{j=1}^{N-1} |R_{xx}(j)|^2 + \sum_{x \in \mathcal{Q}} |R_{xx}(0)|^2 \leq \\
&\leq m(N-1) R_a^2 + m A^2.
\end{aligned}$$

Кроме того,

$$\sum_{\substack{x,y \in \mathcal{Q} \\ x \neq y}} \sum_{j=0}^{N-1} |R_{xy}(j)|^2 \leq m(m-1) N R_c^2.$$

На основании (3) получаем

$$m^2 A^2 \leq m(m-1) N R_c^2 + m(N-1) R_a^2 + m A^2$$

или

$$m(m-1) A^2 \leq m(m-1) N R_c^2 + m(N-1) R_a^2.$$

Последнее неравенство равносильно (1). Предложение доказано. \square

3°. Неравенство (1) показывает, что величины R_a и R_c не могут быть одновременно сколь угодно малыми. Мы рассмотрим два крайних случая, когда одна из этих величин равна нулю, а другая принимает наименьшее возможное значение.

ПРЕДЛОЖЕНИЕ 2. Для любого ансамбля \mathcal{Q} , состоящего из N попарно некоррелированных сигналов, неравенство (1) выполняется как равенство.

Доказательство. По условию $m = N$ и $R_c = 0$. Нужно проверить, что $R_a = A$.

Мы установим более сильный результат:

$$|R_{xx}(j)| \equiv A \quad \text{при всех } x \in \mathcal{Q}.$$

При $R_c = 0$ формула (3) принимает вид

$$\sum_{j=0}^{N-1} \left| \sum_{x \in \mathcal{Q}} R_{xx}(j) \right|^2 = \sum_{x \in \mathcal{Q}} \sum_{j=0}^{N-1} |R_{xx}(j)|^2.$$

Отсюда следует, что

$$\sum_{x \in \mathcal{Q}} \sum_{j=0}^{N-1} |R_{xx}(j)|^2 \geq \left| \sum_{x \in \mathcal{Q}} R_{xx}(0) \right|^2 = N^2 A^2. \quad (4)$$

Вместе с тем, по неравенству Коши-Буняковского

$$|R_{xx}(j)|^2 = \left| \sum_{k=0}^{N-1} x(k) \bar{x}(k-j) \right|^2 \leq \sum_{k=0}^{N-1} |x(k)|^2 \sum_{k=0}^{N-1} |x(k-j)|^2 = A^2.$$

Допустив, что при некоторых $x \in \mathcal{Q}$ и $j \in 0 : N-1$ будет $|R_{xx}(j)| < A$, получим

$$\sum_{x \in \mathcal{Q}} \sum_{j=0}^{N-1} |R_{xx}(j)|^2 < N^2 A^2,$$

что противоречит (4). Предложение доказано. \square

4°. Теперь обратимся к ансамблям, состоящим из дельта-коррелированных сигналов. Для таких ансамблей $R_a = 0$, так что неравенство (1) принимает вид $R_c \geq A/\sqrt{N}$. Эта оценка не зависит от количества сигналов m . Она, в частности, обращается в равенство, если

$$|R_{xy}(j)| \equiv \frac{A}{\sqrt{N}} \quad \text{при всех } x, y \in \mathcal{Q}, x \neq y. \quad (5)$$

Приведём пример ансамбля, для которого выполняется условие (5).

Рассмотрим двухпараметрическое семейство сигналов

$$a_{kp}(j) = \omega_N^{k(j^2+pj)}, \quad k, p \in 0 : N-1, \quad \text{НОД}(k, N) = 1. \quad (6)$$

ПРЕДЛОЖЕНИЕ 3. При нечетном N сигналы a_{kp} являются дельта-коррелированными.

Доказательство. Обозначим для простоты $x = a_{kp}$. Имеем

$$\begin{aligned} R_{xx}(j) &= \sum_{l=0}^{N-1} x(l+j) \bar{x}(l) = \sum_{l=0}^{N-1} \omega_N^{k(l^2+2lj+j^2+pl+pj)-k(l^2+pl)} = \\ &= \omega_N^{k(j^2+pj)} \sum_{l=0}^{N-1} \omega_N^{2klj} = N x(j) \delta_N(2kj). \end{aligned} \quad (7)$$

Покажем, что в данном случае $\delta_N(2kj) = \delta_N(j)$ при всех $j \in \mathbb{Z}$. Это эквивалентно равенству $\delta_N(\langle 2kj \rangle_N) = \delta_N(j)$ при $j \in 0 : N-1$.

По условию N взаимно просто как с 2, так и с k , поэтому число $2k$ взаимно просто с N . Отсюда следует, что отображение $j \rightarrow \langle 2kj \rangle_N$ является перестановкой множества $\{0, 1, \dots, N-1\}$ (эйлеровой перестановкой), переводящей ноль в ноль. Это и гарантирует справедливость равенства $\delta_N(\langle 2kj \rangle_N) = \delta_N(j)$ при $j \in 0 : N-1$.

Формула (7) принимает вид $R_{xx}(j) = N\delta_N(j)$, $j \in \mathbb{Z}$. Остаётся сослаться на определение дельта-коррелированного сигнала (см., например, [4, с. 48]).

Предложение доказано. \square

Пусть N — нечётное число. Возьмём два сигнала вида (6)

$$x(j) = \omega_N^{k(j^2+pj)}, \quad y(j) = \omega_N^{s(j^2+pj)}.$$

Будем считать, что $k > s$.

ПРЕДЛОЖЕНИЕ 4. При выполнении условия $\text{НОД}(k-s, N) = 1$ справедливо тождество

$$|R_{xy}(j)| \equiv \sqrt{N}. \quad (8)$$

Доказательство. Имеем

$$|R_{xy}(j)|^2 = \sum_{l=0}^{N-1} x(l+j) \bar{y}(l) \sum_{q=0}^{N-1} \bar{x}(q+j) y(q) =$$

$$= \sum_{l,q=0}^{N-1} \omega_N^{k(l^2+2lj+j^2+pl+pj)-s(l^2+pl)-k(q^2+2qj+j^2+pq+pj)+s(q^2+pq)}.$$

Степень приводится к виду

$$\begin{aligned} k(l-q)(l+q+2j+p) - s(l-q)(l+q+p) = \\ = (k-s)(l-q)(l+q+p) + 2k(l-q)j. \end{aligned}$$

Поэтому

$$\begin{aligned} |R_{xy}(j)|^2 &= \sum_{l,q=0}^{N-1} \omega_N^{(k-s)(l-q)(l+q+p)+2k(l-q)j} = \\ &= \sum_{q=0}^{N-1} \sum_{l=0}^{N-1} \omega_N^{(k-s)l(l+2q+p)+2klj} = \sum_{l=0}^{N-1} \omega_N^{(k-s)l(l+p)+2klj} \sum_{q=0}^{N-1} \omega_N^{2(k-s)lq} = \\ &= N \sum_{l=0}^{N-1} \omega_N^{(k-s)l(l+p)+2klj} \delta_N(\langle 2(k-s)l \rangle_N). \end{aligned} \quad (9)$$

По условию N взаимно просто как с 2, так и с $k-s$. Значит, число $2(k-s)$ взаимно просто с N . В таком случае, отображение $l \rightarrow \langle 2(k-s)l \rangle_N$ является перестановкой множества $\{0, 1, \dots, N-1\}$, переводящей ноль в ноль. Учитывая этот факт, заключаем, что в сумме из правой части (9) отлично от нуля лишь одно слагаемое, соответствующее $l=0$. Приходим к тождеству $|R_{xy}(j)|^2 \equiv N$, равносильному (8). Предложение доказано. \square

Сигналы a_{kp} вида (6) имеют одинаковую энергию $E(a_{kp}) = N$. Согласно предложению 3 при нечётном N любой их набор образует ансамбль \mathcal{Q} с $A = N$ и $R_a = 0$. Предположим, что сигналы a_{kp} из \mathcal{Q} удовлетворяют двум дополнительным условиям:

- у них одинаковы p ;
- для всех пар сигналов a_{kp}, a_{sp} из \mathcal{Q} с $k > s$ разность $k-s$ взаимно проста с N .

Тогда по предложению 4 справедливо тождество

$$|R_{xy}(j)| \equiv \sqrt{N} \quad \text{при всех } x, y \in \mathcal{Q}, x \neq y.$$

Оно совпадает с (5), поскольку в данном случае $A/\sqrt{N} = \sqrt{N}$.

Отметим, что при простом N всем сформулированным условиям удовлетворяют сигналы $a_{1,p}, a_{2,p}, \dots, a_{N-1,p}$ в количестве $N-1$.

Более общие ансамбли дельта-коррелированных сигналов со свойством (5) рассматривались в работе [5].

ЛИТЕРАТУРА

1. Сидельников В. М. *О взаимной корреляции последовательностей* / В сб.: Проблемы кибернетики. М.: Наука, 1971. Вып. 24. С. 15–42.
2. Sarwate D. V. *Bounds on crosscorrelation and autocorrelation of sequences* // IEEE Trans. Inform. Theory. 1979. Vol. IT-25. P. 720–724.
3. Сарвате Д. В., Персли М. Б. *Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей* // ТИИЭР. 1980. Т. 68. № 5. С. 59–90.
4. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. Часть первая. СПб.: НИИММ, 2003. 98 с.
5. Popović B. M. *Generalized chirp-like polyphase sequences with optimum correlation properties* // IEEE Trans. Inform. Theory. 1992. Vol. 38. No. 4. P. 1406–1409.

ПОСТРОЕНИЕ ЗАМКНУТЫХ КРИВЫХ С ПОМОЩЬЮ ДИСКРЕТНЫХ ПЕРИОДИЧЕСКИХ СПЛАЙНОВ

Н. В. Чашников

25 июня 2008 г.

1°. Пусть $N = mn$, где m, n — натуральные числа, отличные от единицы. Мы будем использовать следующие обозначения из [1]:

\tilde{Q}_r — дискретный нормализованный N -периодический B -сплайн порядка r ;
 $\tilde{S}_r(j) = \sum_{p=0}^{m-1} a_p \tilde{Q}_r(j - pn)$ — дискретный N -периодический сплайн порядка r , построенный по полюсам a_0, a_1, \dots, a_{m-1} из \mathbb{R}^s .

Пусть $s = 2$. Значения сплайна $\tilde{S}_r(j)$ при $j \in 0 : N - 1$ образуют набор точек на плоскости. Если соединить соседние точки сплайна отрезками (при этом $\tilde{S}_r(N - 1)$ соединяется с $\tilde{S}_r(0) = \tilde{S}_r(N)$), мы получим замкнутую N -звенную ломаную. При достаточно больших значениях N построенные ломаные можно использовать для моделирования замкнутых кривых.

Положим $r = 2, m = 8, n = 10$. На рис. 1 изображены полюсы a_0, a_1, \dots, a_7 и значения построенного по ним дискретного периодического сплайна. Замкнутая ломаная, полученная путём соединения соседних точек сплайна отрезками, показана на рис. 2.

Значения B -сплайна $\tilde{Q}_2(j)$ при $j \in 0 : N - 1$ отличны от нуля только если $j < 2n$ или $j > N - 2n$. Поэтому при изменении одного полюса изменится только локальный участок ломаной, задаваемой сплайном. На рис. 3 пунктирной кривой показан сплайн, получающийся при замене полюса a_3 на a'_3 .

Порядок расположения полюсов оказывает существенное влияние на вид сплайна. На рис. 4 пунктирной линией изображён сплайн, получающийся при перестановке полюсов a_3 и a_4 .

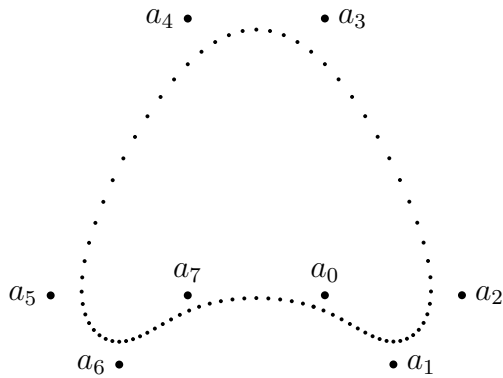


Рис. 1. Полюсы и значения сплайна

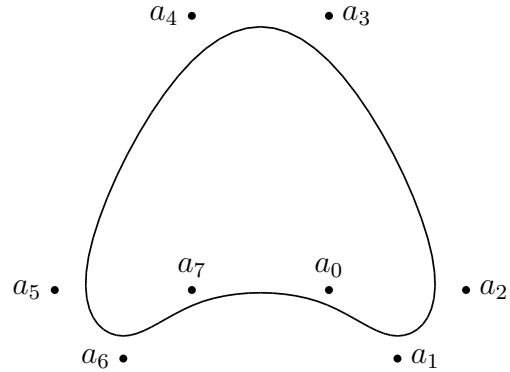


Рис. 2. Замкнутая ломаная

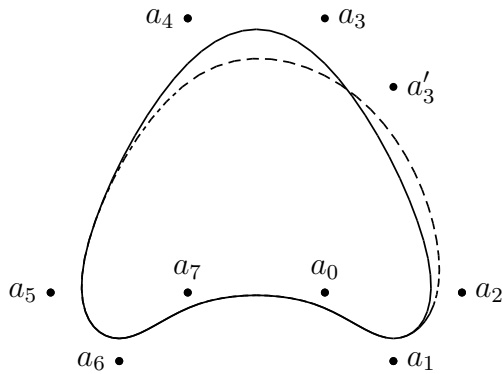


Рис. 3. Изменение полюса

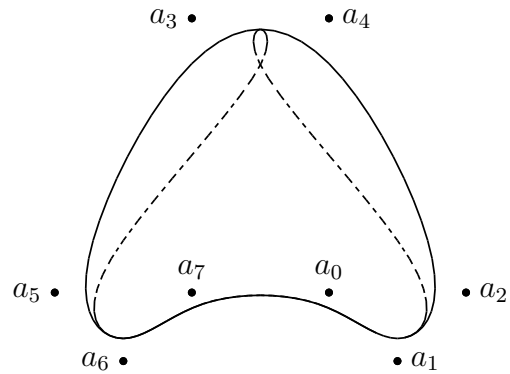


Рис. 4. Изменение порядка полюсов

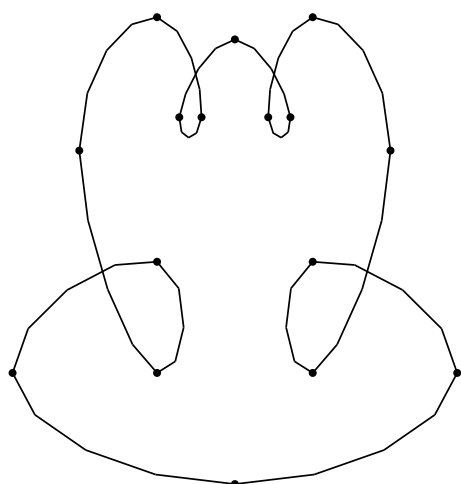
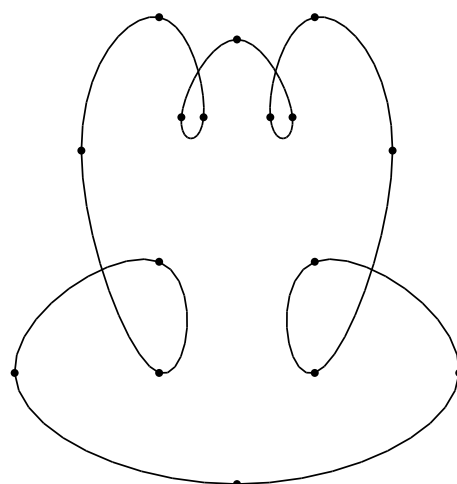
2°. В [1] показано, как построить сплайн \tilde{S}_r , решающий задачу векторной интерполяции

$$\tilde{S}_r(ln) = z(l), \quad l \in 0 : m - 1,$$

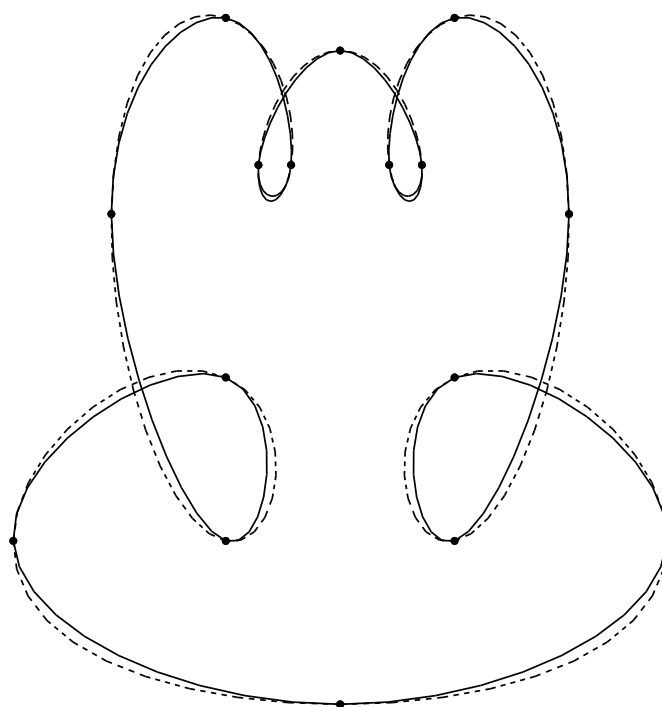
где $z(0), z(1), \dots, z(m-1) \in \mathbb{R}^s$ — заданные векторы.

Используя интерполяционные сплайны, можно строить замкнутые ломаные, проходящие через заданные точки. При этом число n определяет количество отрезков ломаной, лежащих между двумя соседними точками интерполяции. Увеличивая n , можно получить более гладкую ломаную, проходящую через те же точки интерполяции.

Положим $r = 2$, $m = 16$. На рис. 5 и рис. 6 изображены интерполяционные сплайны для одного и того же набора векторов $z(0), z(1), \dots, z(15)$, показанных жирными точками. При этом сплайн на рис. 5 построен при $n = 4$, а на рис. 6 — при $n = 10$.

Рис. 5. Сплайн «Петли», $n = 4$ Рис. 6. Сплайн «Петли», $n = 10$

Порядок сплайна r тоже влияет на вид получающейся ломаной. На рис. 7 кроме сплайна «Петли» порядка 2 (рис. 6) пунктирной линией изображён сплайн порядка 3, построенный по тем же точкам интерполяции с тем же значением n .

Рис. 7. Сплайн «Петли», $r = 2$ и $r = 3$

Задавая нужным образом точки интерполяции, можно получить замкнутую ломаную сколь угодно сложной формы. На рис. 8 изображён сплайн «Овалы», построенный по 12 точкам интерполяции, при $r = 2$, $n = 16$.

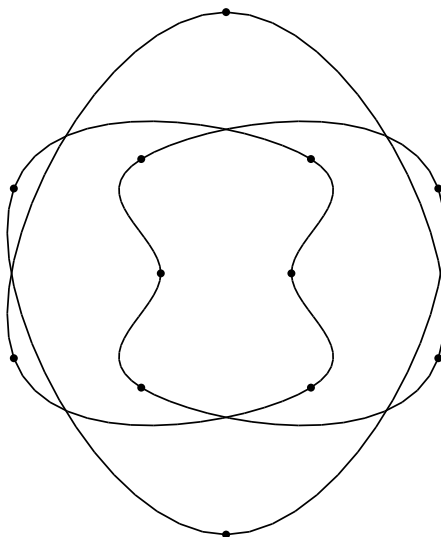


Рис. 8. Сплайн «Овалы»

3°. Дискретные периодические сплайны позволяют строить замкнутые кривые с острыми углами.

На рис. 9 представлен интерполяционный сплайн с тремя острыми углами. Можно получить ещё два острых угла, если перемещать точку b вправо. Петли a и c сначала становятся уже (рис. 10), а затем переходят в острые углы (рис. 11).

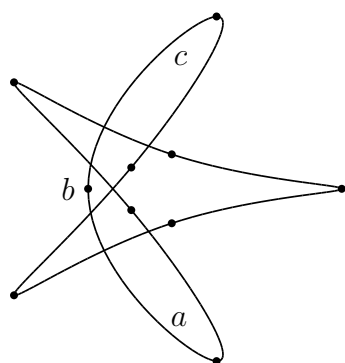


Рис. 9. Исходный сплайн

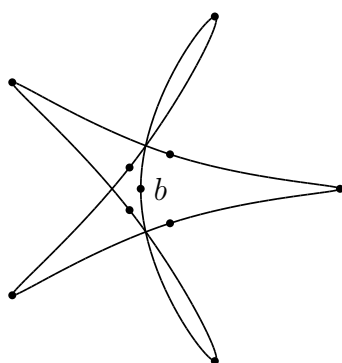


Рис. 10. Узкие петли

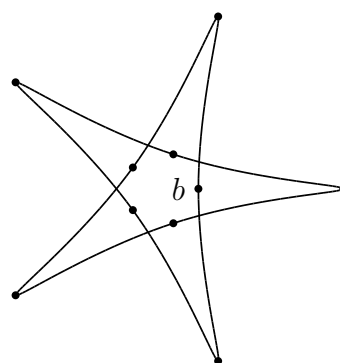


Рис. 11. Острые углы

Аналогичным образом можно получить сплайн с ещё более острым углом, а также сплайн, в котором вершина угла не является точкой интерполяции (см. рис. 12).

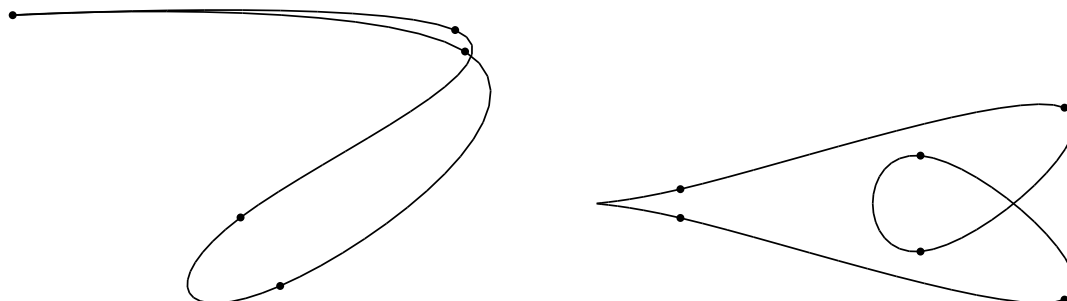


Рис. 12. Сплайны с острыми углами

ЛИТЕРАТУРА

1. Малозёмов В. Н., Хорохонов Д. А., Чашников Н. В. *Дискретные периодические сплайны с векторными коэффициентами и геометрическое моделирование* // Семинар «DHA & CAGD». Избранные доклады. 4 сентября 2007 г. (<http://dha.spb.ru/rep07.shtml#0904>).

ПОСТРОЕНИЕ КРИВЫХ С ПОМОЩЬЮ ОБОБЩЁННЫХ ПОЛИНОМОВ БЕРНШТЕЙНА

М. И. Григорьев В. Н. Малозёмов

25 июня 2008 г.

1°. Напомним, что базисные полиномы Бернштейна

$$b_k^n(x) = C_n^k x^k (1-x)^{n-k}, \quad k \in 0 : n,$$

можно определить с помощью производящей функции:

$$[xy + (1-x)]^n = \sum_{k=0}^n b_k^n(x) y^k.$$

В. С. Виденский рассмотрел более общую производящую функцию и ввёл обобщённые полиномы Бернштейна $p_k^n(x)$ [1, с. 39]:

$$g_n(x, y) := \prod_{i=1}^n [h_i(x) y + (1 - h_i(x))] = \sum_{k=0}^n p_k^n(x) y^k. \quad (1)$$

Здесь $h_1(x), \dots, h_n(x) : [0, 1] \rightarrow [0, 1]$ — непрерывные функции, удовлетворяющие условиям

$$h_i(0) = 0, \quad h_i(1) = 1 \quad \text{при всех } i \in 1 : n. \quad (2)$$

Приведём некоторые свойства базисных полиномов $p_k^n(x)$ при фиксированном n . Согласно (1)

$$\begin{aligned} p_k^n(x) &\geq 0 \text{ на } [0, 1] \text{ при всех } k \in 0 : n; \\ \sum_{k=0}^n p_k^n(x) &\equiv 1. \end{aligned} \quad (3)$$

В силу (2)

$$\begin{aligned} p_k^n(0) &= 0, & k \in 1 : n; & & p_0^n(0) &= 1; \\ p_k^n(1) &= 0, & k \in 0 : n-1; & & p_n^n(1) &= 1. \end{aligned} \quad (4)$$

Покажем, что

$$\sum_{k=0}^n \frac{k}{n} p_k^n(x) = \varphi_n(x), \quad x \in [0, 1], \quad (5)$$

где

$$\varphi_n(x) = \frac{1}{n} \sum_{i=1}^n h_i(x).$$

Для этого продифференцируем $\ln g_n(x, y)$ по y , после чего положим $y = 1$. Получим

$$\sum_{i=1}^n h_i(x) = \sum_{k=1}^n k p_k^n(x),$$

что равносильно (5).

2°. Зафиксируем $x \in (0, 1)$ и рассмотрим треугольный массив $\{p_k^j(x)\}$, $k \in 0 : j$, $j \in 0 : n$.

ПРЕДЛОЖЕНИЕ 1. *Справедливы рекуррентные соотношения*

$$\begin{aligned} p_k^j &= (1 - h_j(x)) p_k^{j-1} + h_j(x) p_{k-1}^{j-1}, & k \in 1 : j-1; & & j \in 2 : n; \\ p_0^j &= (1 - h_j(x)) p_0^{j-1}, & p_j^j &= h_j(x) p_{j-1}^{j-1}, & j \in 1 : n; \\ p_0^0 &= 1. \end{aligned} \quad (6)$$

Доказательство. По определению

$$\prod_{i=1}^j [h_i(x) y + (1 - h_i(x))] = \sum_{k=0}^j p_k^j y^k.$$

При $j = 1$ имеем

$$h_1(x) y + (1 - h_1(x)) = p_0^1 + p_1^1 y.$$

Отсюда следует, что

$$p_0^1 = 1 - h_1(x), \quad p_1^1 = h_1(x).$$

Пусть теперь $j \in 2 : n$. Запишем

$$\begin{aligned} \sum_{k=0}^j p_k^j y^k &= [(1 - h_j(x)) + h_j(x) y] \prod_{i=1}^{j-1} [h_i(x) y + (1 - h_i(x))] = \\ &= [(1 - h_j(x)) + h_j(x) y] \sum_{k=0}^{j-1} p_k^{j-1} y^k = (1 - h_j(x)) \sum_{k=0}^{j-1} p_k^{j-1} y^k + \end{aligned}$$

$$\begin{aligned}
& + h_j(x) \sum_{k=1}^j p_{k-1}^{j-1} y^k = (1 - h_j(x)) p_0^{j-1} + h_j(x) p_{j-1}^{j-1} y^j + \\
& + \sum_{k=1}^{j-1} [(1 - h_j(x)) p_k^{j-1} + h_j(x) p_{k-1}^{j-1}] y^k.
\end{aligned}$$

Сравнивая коэффициенты при одинаковых степенях y , приходим к (6).

Предложение доказано. \square

3°. Введём обобщённый полином Бернштейна с векторными коэффициентами

$$\mathbf{H}(x) = \sum_{k=0}^n \mathbf{a}_k p_k^n(x), \quad x \in [0, 1], \quad (7)$$

где $\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_n$ принадлежат \mathbb{R}^s . Согласно (4)

$$\mathbf{H}(0) = \mathbf{a}_0, \quad \mathbf{H}(1) = \mathbf{a}_n. \quad (8)$$

Зафиксируем $x \in (0, 1)$. Для вычисления $\mathbf{H}(x)$ построим треугольный массив $\{\mathbf{a}_k^j\}$ с помощью рекуррентных соотношений

$$\begin{aligned}
& \mathbf{a}_k^j = (1 - h_{n-j+1}(x)) \mathbf{a}_k^{j-1} + h_{n-j+1}(x) \mathbf{a}_{k+1}^{j-1}, \quad k \in 0 : n - j, \quad j \in 1 : n; \\
& \mathbf{a}_k^0 = \mathbf{a}_k, \quad k \in 0 : n.
\end{aligned} \quad (9)$$

ПРЕДЛОЖЕНИЕ 2. Справедливо равенство $\mathbf{H}(x) = \mathbf{a}_0^n$.

Доказательство. Согласно (6) и (9) имеем

$$\begin{aligned}
\mathbf{H}(x) &= \mathbf{a}_0^n p_0^n + \mathbf{a}_n^n p_n^n + \sum_{k=1}^{n-1} \mathbf{a}_k^n [(1 - h_n(x)) p_k^{n-1} + h_n(x) p_{k-1}^{n-1}] = \\
&= \sum_{k=0}^{n-1} \mathbf{a}_k^n (1 - h_n(x)) p_k^{n-1} + \sum_{k=1}^n \mathbf{a}_k^n h_n(x) p_{k-1}^{n-1} = \\
&= \sum_{k=0}^{n-1} [(1 - h_n(x)) \mathbf{a}_k^n + h_n(x) \mathbf{a}_{k+1}^n] p_k^{n-1} = \sum_{k=0}^{n-1} \mathbf{a}_k^1 p_k^{n-1} = \dots = \\
&= \sum_{k=0}^1 \mathbf{a}_k^{n-1} p_k^1 = (1 - h_1(x)) \mathbf{a}_0^{n-1} + h_1(x) \mathbf{a}_1^{n-1} = \mathbf{a}_0^n.
\end{aligned}$$

Предложение доказано. \square

ПРЕДЛОЖЕНИЕ 3. При всех $j \in 1 : n$ обобщённый полином Бернштейна $\mathbf{H}(x)$ допускает представление

$$\mathbf{H}(x) = \sum_{k=0}^j (\Delta^k \mathbf{a}^{n-j})_0 \sigma_k(h_1(x), \dots, h_j(x)), \quad (10)$$

где $\sigma_0, \sigma_1, \dots, \sigma_j$ — основные симметрические полиномы от j переменных и

$$(\Delta^k \mathbf{a}^{n-j})_i = \sum_{p=0}^k (-1)^{k-p} C_k^p \mathbf{a}_{i+p}^{n-j}(x)$$

— конечная разность k -го порядка.

Доказательство. Напомним рекуррентные соотношения для основных симметрических полиномов:

$$\begin{aligned} \sigma_0(h_1, \dots, h_j) &= 1, \quad \sigma_{j+1}(h_1, \dots, h_j) = 0, \quad j \in 1 : n; \quad \sigma_1(h_1) = h_1; \\ \sigma_k(h_1, \dots, h_{j-1}, h_j) &= \sigma_k(h_1, \dots, h_{j-1}) + h_j \sigma_{k-1}(h_1, \dots, h_{j-1}), \\ k &\in 1 : j, \quad j \in 2 : n. \end{aligned}$$

Перепишем соотношения (9):

$$\begin{aligned} \mathbf{a}_k^0 &= \mathbf{a}_k, \quad k \in 0 : n; \\ \mathbf{a}_k^j &= \mathbf{a}_k^{j-1} + h_{n-j+1}(x) (\Delta \mathbf{a}^{j-1})_k, \quad k \in 0 : n - j, \quad j \in 1 : n. \end{aligned}$$

При $j = 1$ формула (10) принимает вид

$$\begin{aligned} \mathbf{H}(x) &= \mathbf{a}_0^{n-1} \sigma_0(h_1) + (\Delta \mathbf{a}^{n-1})_0 \sigma_1(h_1) = \\ &= \mathbf{a}_0^{n-1} + h_1 (\Delta \mathbf{a}^{n-1})_0 = \mathbf{a}_0^n. \end{aligned}$$

Это равенство верно в силу предложения 2.

Сделаем индукционный переход от j к $j + 1$. Имеем

$$\begin{aligned} \mathbf{H}(x) &= \sum_{k=0}^j [(\Delta^k \mathbf{a}^{n-j-1})_0 + h_{j+1}(x) (\Delta^{k+1} \mathbf{a}^{n-j-1})_0] \sigma_k(h_1, \dots, h_j) = \\ &= \mathbf{a}_0^{n-j-1} + h_{j+1}(x) (\Delta^{j+1} \mathbf{a}^{n-j-1})_0 \sigma_j(h_1, \dots, h_j) + \\ &+ \sum_{k=1}^j (\Delta^k \mathbf{a}^{n-j-1})_0 [\sigma_k(h_1, \dots, h_j) + h_{j+1}(x) \sigma_{k-1}(h_1, \dots, h_j)] = \end{aligned}$$

$$= \sum_{k=0}^{j+1} (\Delta^k \mathbf{a}^{n-j-1})_0 \sigma_k(h_1, \dots, h_j, h_{j+1}).$$

Предложение доказано. \square

Формула (10) наиболее содержательна при $j = n$:

$$\mathbf{H}(x) = \sum_{k=0}^n (\Delta^k \mathbf{a})_0 \sigma_k(h_1(x), \dots, h_n(x)).$$

В этом случае коэффициенты $(\Delta^k \mathbf{a})_0$ не зависят от x .

4°. Вернёмся к определению (7) обобщённого полинома Бернштейна. Согласно (3) вектор $\mathbf{H}(x)$ при фиксированном $x \in [0, 1]$ является выпуклой комбинацией коэффициентов $\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_n$, которые в геометрическом моделировании называются *полюсами*. Когда x изменяется от 0 до 1, вектор $\mathbf{H}(x)$ описывает кривую в пространстве \mathbb{R}^s . Назовём её *обобщённой кривой Безье*. В силу (8) эта кривая выходит из точки \mathbf{a}_0 (при $x = 0$) и заканчивается в точке \mathbf{a}_n (при $x = 1$), не покидая выпуклую оболочку полюсов.

Если $h_i(x) = x$ при всех $i \in 1 : n$, то $p_k^n(x) = b_k^n(x)$, $k \in 0 : n$, и обобщённая кривая Безье становится обычной кривой Безье [2]. Ниже в качестве примера мы построим кривую Безье и обобщённую кривую Безье в \mathbb{R}^2 по полюсам

$$\mathbf{a}_k = \left(\frac{k}{n}, (-1)^k \right), \quad k \in 0 : n. \quad (11)$$

5°. Запишем обычный полином Бернштейна для полюсов (11):

$$\mathbf{B}(x) = \sum_{k=0}^n \mathbf{a}_k b_k^n(x) = \left(\sum_{k=0}^n \frac{k}{n} b_k^n(x), \sum_{k=0}^n (-1)^k b_k^n(x) \right).$$

При $h_i(x) = x$, $i \in 1 : n$, формула (5) принимает вид

$$\sum_{k=0}^n \frac{k}{n} b_k^n(x) = x, \quad x \in [0, 1].$$

В то же время

$$\sum_{k=0}^n (-1)^k b_k^n(x) = \sum_{k=0}^n C_n^k (-x)^k (1-x)^{n-k} = (1-2x)^n.$$

Поэтому

$$\mathbf{B}(x) = (x, (1-2x)^n), \quad x \in [0, 1].$$

Соответствующая кривая Безье при $n = 6$ представлена на рис. 1.

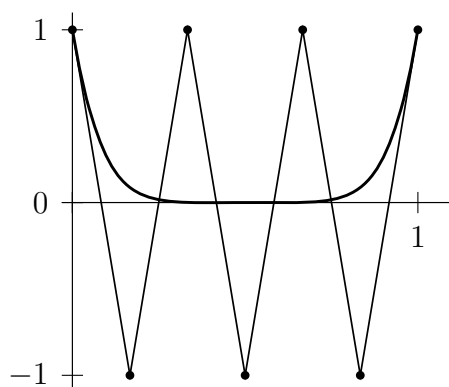


Рис. 1. Кривая Безье

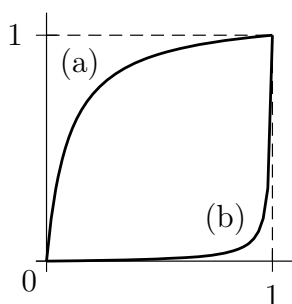
6°. Зафиксируем точки t_1, \dots, t_n из $\mathbb{R} \setminus [0, 1]$ и, следуя [1], рассмотрим дробно-линейные функции

$$h_i(x) = \frac{x(1-t_i)}{x-t_i}, \quad i \in 1:n. \quad (12)$$

Они непрерывны на $[0, 1]$ и удовлетворяют условиям (2). Вычислим первые две производные

$$h'_i(x) = -\frac{t_i(1-t_i)}{(x-t_i)^2}, \quad h''_i(x) = \frac{2t_i(1-t_i)}{(x-t_i)^3}.$$

Имеем $h'_i(x) > 0$ на $[0, 1]$, так что все $h_i(x)$ строго возрастают. Далее $h''_i(x) > 0$ при $t_i > 1$ и $h''_i(x) < 0$ при $t_i < 0$. Значит, при $t_i > 1$ функции $h_i(x)$ строго выпуклы, а при $t_i < 0$ — строго вогнуты. На рис. 2 изображены две функции $h_i(x)$ при $t_i = -0.1$ и $t_i = 1.01$.

Рис. 2. Графики функций $h_i(x)$: (a) при $t_i = -0.1$; (b) при $t_i = 1.01$.

По функциям $h_i(x)$ вида (12) и полюсам (11) построим обобщённый полином Бернштейна

$$\mathbf{H}(x) = \sum_{k=0}^n \mathbf{a}_k p_k^n(x) = \left(\sum_{k=0}^n \frac{k}{n} p_k^n(x), \sum_{k=0}^n (-1)^k p_k^n(x) \right).$$

Согласно (5)

$$\mathbf{H}(x) = \left(\varphi_n(x), \sum_{k=0}^n (-1)^k p_k^n(x) \right), \quad x \in [0, 1].$$

Эта формула определяет обобщённую кривую Безье на плоскости. Обозначим её \mathcal{H} . Кривую \mathcal{H} можно перепараметризовать, положив $x = \varphi_n^{-1}(u)$. Такая замена корректна, поскольку функция $\varphi_n(x)$ строго возрастает на $[0, 1]$ от значения 0 до значения 1. Получим

$$\mathbf{H}(\varphi_n^{-1}(u)) = \left(u, \sum_{k=0}^n (-1)^k p_k^n(\varphi_n^{-1}(u)) \right), \quad u \in [0, 1].$$

Видим, что кривая \mathcal{H} есть график скалярного полинома

$$\tilde{H}(u) = \sum_{k=0}^n (-1)^k p_k^n(\varphi_n^{-1}(u)). \quad (13)$$

На рис. 3 представлена кривая \mathcal{H} при $n = 6$. Узлы t_i выбраны так, как показано на рис. 4.

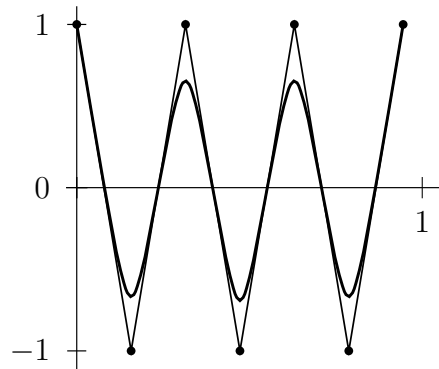


Рис. 3. Обобщённая кривая Безье



Рис. 4. Узлы t_i , $i \in 1 : 6$

На рис. 5 изображены графики базисных функций $p_k^n(\varphi_n^{-1}(u))$ обобщённого полинома (13) в рассматриваемом частном случае.

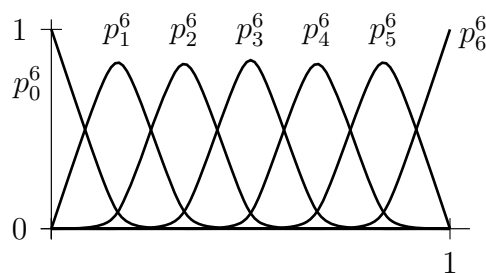


Рис. 5. Графики базисных функций

7°. В принципе, функции $h_1(x), \dots, h_n(x)$ и $\varphi_n(x)$, отображающие отрезок $[0, 1]$ на себя, могут быть и немонотонными. Возьмём в качестве $h_1(x)$ функцию, график которой представлен на рис. 6. Положим $h_2(x) \equiv h_1(x)$, $h_3(x) \equiv x$. На рис. 7 изображены четыре полюса и соответствующая обобщённая кривая Безье третьего порядка.

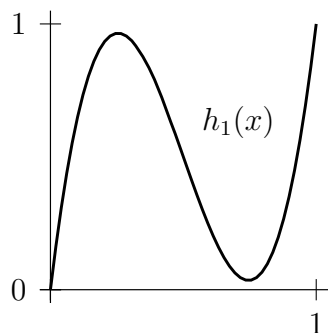
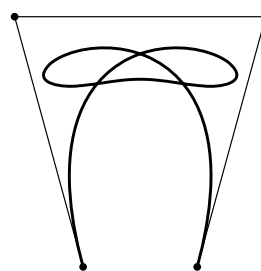
Рис. 6. График функции $h_1(x)$ 

Рис. 7. Обобщённая кривая Безье третьего порядка

ЛИТЕРАТУРА

1. Виденский В. С. *Линейные положительные операторы конечного ранга*. Л.: ЛГПИ им. А. И. Герцена, 1985.
2. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Полиномы Бернштейна и составные кривые Безье* // Журн. вычисл. мат. и матем. физ. 2006. Т. 46. № 11. С. 1962-1971.

МЕТОД ПОПЕРЕМЕННОГО ПРОЕКТИРОВАНИЯ ДЛЯ ПОСТРОЕНИЯ РАВНОУГОЛЬНЫХ ЖЁСТКИХ ФРЕЙМОВ

М. Н. Истомина А. Б. Певный

2 июля 2008 г.

В докладе исследуется метод построения равноугольных жёстких фреймов, предложенный в [1].

1°. Пусть $m > n \geq 2$ и столбцы матрицы $\Phi = [\varphi_1, \varphi_2, \dots, \varphi_m]$ размера $n \times m$ образуют равноугольный жёсткий фрейм в \mathbb{R}^n . Жёсткость фрейма равносильна выполнению равенства $\Phi \Phi^T = A I_n$, где A — константа, I_n — единичная матрица порядка n . Равноугольность означает, что

$$\|\varphi_k\| = 1 \text{ при всех } k \in 1 : m \text{ и } |\langle \varphi_k, \varphi_s \rangle| = c \text{ при } k \neq s.$$

Это определение использовалось в докладе [2]. Для равноугольного жёсткого фрейма константы A и c имеют вид

$$A = \frac{m}{n}, \quad c = \sqrt{\frac{m-n}{n(m-1)}}.$$

Рассмотрим матрицу Грама $G = \{\langle \varphi_i, \varphi_j \rangle\}_{i,j=1}^m = \Phi^T \Phi$. Матрицы G и $\Phi \Phi^T$ имеют одинаковые ненулевые собственные числа. Но $\Phi \Phi^T = A I_n$ имеет собственные числа $\lambda_k = A$, $k \in 1 : n$. Поэтому G имеет n собственных чисел $\lambda_k = A$, $k \in 1 : n$, и $m - n$ собственных чисел $\lambda_k = 0$, $k \in n + 1 : m$.

2°. Для чисел $A = \frac{m}{n}$ и $c = \sqrt{\frac{m-n}{n(m-1)}}$ введём два множества матриц:

$$\mathcal{G}_A = \left\{ G \in \mathbb{R}^{m \times m} \mid G = G^T; G \text{ имеет собственные числа } \underbrace{(A, \dots, A)}_{n \text{ раз}}, 0, \dots, 0 \right\},$$

$$\mathcal{H}_c^0 = \left\{ H \in \mathbb{R}^{m \times m} \mid H = H^T; H[k, k] = 1, k \in 1 : m; |H[k, l]| \leq c \text{ при } k \neq l \right\}.$$

Множество \mathcal{H}_c^0 является ограниченным и выпуклым.

Матрица Грама G равноугольного жёсткого фрейма принадлежит как \mathcal{G}_A , так и \mathcal{H}_c^0 . Справедливо и обратное утверждение.

ПРЕДЛОЖЕНИЕ. Если существует матрица $G_* \in \mathcal{G}_A \cap \mathcal{H}_c^0$, то существует равноугольный жёсткий фрейм из m векторов в пространстве \mathbb{R}^n .

Доказательство. Поскольку $G_* \in \mathcal{G}_A$, то G_* можно представить в виде

$$G_* = P^T \Lambda P,$$

где P — ортогональная матрица,

$$\Lambda = \text{diag}(\underbrace{A, \dots, A}_{n \text{ раз}}, 0, \dots, 0).$$

Введём матрицу V размера $n \times m$:

$$V = \left[\begin{array}{cccc|ccc} \sqrt{A} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \sqrt{A} & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sqrt{A} & 0 & \dots & 0 \end{array} \right].$$

Тогда $V^T V = \Lambda$. Положим $\Phi = VP$ — эта матрица размера $n \times m$ как раз и будет матрицей равноугольного жёсткого фрейма.

Действительно,

$$\Phi^T \Phi = P^T V^T V P = P^T \Lambda P = G_*,$$

то есть G_* является матрицей Грама системы столбцов

$$\Phi = [\varphi_1, \varphi_2, \dots, \varphi_m]. \quad (1)$$

Поскольку матрицы $\Phi \Phi^T$ и $\Phi^T \Phi = G_*$ имеют одинаковые ненулевые собственные числа, то $\Phi \Phi^T$ имеет собственные числа $\lambda_k = A$, $k \in 1 : n$. Других собственных чисел нет. Поэтому

$$\Phi \Phi^T = A I_n,$$

так что система (1) является жёстким фреймом.

Поскольку $G_* \in \mathcal{H}_c^0$, то

$$\begin{aligned} \|\varphi_k\|^2 &= G_*[k, k] = 1, \quad k \in 1 : m, \\ |\langle \varphi_k, \varphi_l \rangle| &= |G_*[k, l]| \leq c, \quad k \neq l. \end{aligned} \quad (2)$$

Введём фреймовый потенциал

$$P(\Phi) = \sum_{k,l=1}^m [\langle \varphi_k, \varphi_l \rangle]^2.$$

Ввиду (2) справедлива оценка

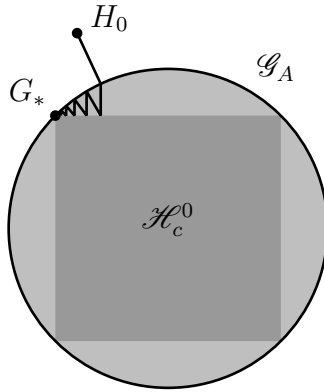
$$\begin{aligned} P(\Phi) &\leq m + (m^2 - m) c^2 = m + m(m-1) \frac{m-n}{n(m-1)} = \\ &= \frac{mn + m(m-n)}{n} = \frac{m^2}{n}. \end{aligned}$$

С другой стороны, для $P(\Phi)$ справедлива оценка [3]

$$P(\Phi) \geq \frac{m^2}{n}.$$

Если хоть в одном из неравенств $|\langle \varphi_k, \varphi_l \rangle| \leq c$ будет строгое неравенство, то $P(\Phi) < \frac{m^2}{n}$, что невозможно. Значит, $|\langle \varphi_k, \varphi_l \rangle| = c$ при всех $k \neq l$, то есть Φ — равноугольный жёсткий фрейм. \square

Замечание. В точке пересечения G_* множеств \mathcal{G}_A и \mathcal{H}_c^0 все ограничения, задающие множество \mathcal{H}_c^0 , выполняются как равенства: $|G_*[k, l]| = c$ при всех $k \neq l$. С геометрической точки зрения G_* является крайней точкой множества \mathcal{H}_c^0 .



Поясним рисунок. Все матрицы G из \mathcal{G}_A имеют одинаковые нормы:

$$\|G\|^2 = \sum_{k,l=1}^m (G[k, l])^2 = \text{tr}(G^2) = nA^2 = \frac{m^2}{n},$$

то есть множество \mathcal{G}_A лежит на сфере S_R радиуса $R = m/\sqrt{n}$.

Все крайние точки множества \mathcal{H}_c^0 имеют вид $G_*[k, k] = 1, \quad k \in 1 : m; \quad G_*[k, l] = \pm c, \quad k \neq l,$ и также лежат на сфере S_R :

$$\|G_*\|^2 = m + m(m-1)c^2 = \frac{m^2}{n} = R^2.$$

Множество \mathcal{G}_A заполняет не всю сферу S_R . Найти точки пересечения \mathcal{G}_A и \mathcal{H}_c^0 нам поможет метод попеременного проектирования.

СЛЕДСТВИЕ. Для существования равноугольного жёсткого фрейма необходимо и достаточно выполнение условия

$$\mathcal{G}_A \cap \mathcal{H}_c^0 \neq \emptyset.$$

3°. Метод попеременного проектирования

Для нахождения общей точки множеств \mathcal{G}_A и \mathcal{H}_c^0 будем решать экстремальную задачу

$$\|G - H\|^2 \rightarrow \min_{G \in \mathcal{G}_A, H \in \mathcal{H}_c^0}, \quad (3)$$

где $\|G - H\|^2 = \sum_{k,l=1}^m (G[k, l] - H[k, l])^2$.

Задачу (3) решаем методом попеременного проектирования (см. статью [1] — там указано, что попеременное проектирование использовал ещё Джон фон Нейман в 1938 г. для определения общей точки двух подпространств в гильбертовом пространстве). В методе строится последовательность матриц

$$H_0, G_0, H_1, G_1, \dots, H_k, G_k, \dots$$

Проектирование матрицы H_k на множество \mathcal{G}_A

Имея матрицу H_k , решаем задачу

$$\|G - H_k\|^2 \rightarrow \min_{G \in \mathcal{G}_A}. \quad (4)$$

Решение этой задачи обозначаем G_k . Это решение существует и строится следующим образом.

Представим H_k в виде

$$H_k = U \Lambda U^T,$$

где U — ортогональная матрица размера $m \times m$,

$$\Lambda = \text{diag}(\lambda_1, \dots, \lambda_m), \quad \lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_m.$$

Следующая замечательная теорема установлена в [1]. Нам удалось найти более простое её доказательство.

ТЕОРЕМА. Матрица

$$G_k = A U_n U_n^T,$$

где U_n — матрица из первых n столбцов матрицы U , является решением задачи (4).

Доказательство. Введём скалярное произведение матриц

$$\langle H, G \rangle = \sum_{i,k=1}^m H[i, k] G[i, k].$$

Если матрица G симметрична, то $\langle H, G \rangle = \text{tr}(HG)$. Действительно,

$$\text{tr}(HG) = \sum_{i=1}^m (HG)[i, i] = \sum_{i=1}^m \sum_{k=1}^m H[i, k] G[k, i] = \sum_{i,k=1}^m H[i, k] G[i, k].$$

При $H = G$ получаем $\|G\|^2 = \text{tr}(G^2)$.

Целевая функция в задаче (4) записывается в виде

$$\|G - H_k\|^2 = \|G\|^2 - 2\langle G, H_k \rangle + \|H_k\|^2.$$

Для $G \in \mathcal{G}_A$ имеем

$$\|G\|^2 = \text{tr}(G^2) = \text{сумме собственных чисел } G^2 = nA^2.$$

Поэтому задача (4) равносильна задаче

$$\langle H_k, G \rangle \rightarrow \max_{G \in \mathcal{G}_A}. \quad (5)$$

У нас $H_k = U\Lambda U^T$, где $\Lambda = \text{diag}(\lambda_1, \dots, \lambda_m)$. Отсюда

$$\langle H_k, G \rangle = \text{tr}(H_k G) = \text{tr}(U\Lambda U^T G) = \text{tr}(U^T G U \Lambda) = \sum_{i=1}^m x_i \lambda_i,$$

где x_i — диагональные элементы матрицы $U^T G U$. Справедливы неравенства $0 \leq \langle U^T G U y, y \rangle \leq A\|y\|^2$ для любого $y \in \mathbb{R}^m$. Поэтому при y , равном i -му орту e_i , получим

$$0 \leq x_i = \langle G U e_i, U e_i \rangle \leq A \|U e_i\| = A, \quad i \in 1 : m.$$

Кроме того, $\sum_{i=1}^m x_i = \text{tr}(U^T G U) = \text{tr}(G U U^T) = \text{tr}(G) = nA$.

Приходим к задаче

$$f(x) := \sum_{i=1}^m \lambda_i x_i \rightarrow \max,$$

$$0 \leq x_i \leq A, \quad \sum_{i=1}^m x_i = nA.$$

Поскольку $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_m$, то решение очевидно: $x^* = (A, \dots, A, 0, \dots, 0)$, где A повторяется n раз, $f(x^*) = A \sum_{i=1}^n \lambda_i$.

Вернёмся к задаче (5). Для любой матрицы $G \in \mathcal{G}_A$

$$\langle H_k, G \rangle = \sum_{i=1}^m x_i \lambda_i \leq f(x^*) = A \sum_{i=1}^n \lambda_i.$$

Для матрицы $G_* = A U_n U_n^T$ (принадлежащей \mathcal{G}_A) будет

$$\langle H_k, G_* \rangle = A \operatorname{tr}(H_k U_n U_n^T) = A \operatorname{tr}(U_n^T H_k U_n). \quad (6)$$

Но столбцы U_n являются собственными векторами, соответствующими собственным числам $\lambda_1, \dots, \lambda_n$. Поэтому $U_n^T H_k U_n = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$. Из (6) получаем

$$\langle H, G_* \rangle = A \sum_{i=1}^n \lambda_i.$$

Значит, G_* — решение задач (5) и (4). \square

Проектирование G_k на множество \mathcal{H}_c^0

Имея матрицу G_k , решаем задачу

$$\|G_k - H\|^2 \rightarrow \min_{H \in \mathcal{H}_c^0}. \quad (7)$$

Решение обозначаем H_{k+1} . Это очень простая задача, так как она распадается на отдельные одномерные подзадачи: для данного числа $G_k[i, j]$, где $i \neq j$, найти число $H[i, j] \in [-c, c]$, которое минимизирует величину $(G_k[i, j] - H[i, j])^2$. Решением будет

$$H_{k+1}[i, j] = \begin{cases} G_k[i, j], & \text{если } G_k[i, j] \in [-c, c], \\ c \operatorname{sign} G_k[i, j] & \text{в противном случае.} \end{cases}$$

4°. Пример несходимости метода к решению задачи (3)

Пусть $n = 2$, $m = 3$. Тогда

$$A = \frac{m}{n} = \frac{3}{2}, \quad c = \sqrt{\frac{m-n}{n(m-1)}} = \frac{1}{2}.$$

В этом случае существует равноугольный жёсткий фрейм Мерседес-Бенц.

Возьмём в качестве начального приближения матрицу

$$H_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} =: I_3.$$

(это центральная точка множества \mathcal{H}_c^0). Справедливо равенство $H_0 = U \Lambda U^T$, где $U = I_3$, $\Lambda = I_3$. Имеем

$$U_n U_n^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

По выше доказанной теореме проекцией H_0 на \mathcal{G}_A является матрица

$$G_0 = A U_n U_n^T = \begin{bmatrix} 3/2 & 0 & 0 \\ 0 & 3/2 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Проекцией G_0 на \mathcal{H}_c^0 является матрица

$$H_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

совпадающая с H_0 . В данном случае $H_k = H_0$ и $G_k = G_0$ для всех k , при этом пара $\{H_0, G_0\}$ не является решением задачи (3). Такую пару можно назвать точкой застревания. При её появлении метод нужно начать заново с нового начального приближения.

5°. Критерий конца итерационного процесса

Зададим малое $\varepsilon > 0$. Если после очередного проектирования на \mathcal{H}_c^0 выполнится неравенство

$$\|G_k - H_{k+1}\| < \varepsilon,$$

то вычисления прекращаем. По матрице H_{k+1} строим сигнатурную матрицу Q , полагая

$$\begin{aligned} Q[i, j] &= \text{sign } H_{k+1}[i, j] \text{ при } i \neq j, \\ Q[i, i] &= 0, \quad i \in 1 : m. \end{aligned} \tag{8}$$

Если матрица Q удовлетворяет уравнению

$$Q^2 = (m - 1) I_m + \mu_{m,n} Q, \tag{9}$$

$$\mu_{m,n} = (m - 2n) \sqrt{\frac{m - 1}{n(m - n)}},$$

то полагаем $G_* = I_m + c Q$ и находим равноугольный жёсткий фрейм по схеме, указанной в предложении из пункта 2° (в докладе [4] показано, что $G_* \in \mathcal{G}_A$).

Можно после нахождения каждой матрицы H_{k+1} строить Q по формуле (8) и проверять условие (9).

6°. Результаты численных расчётов

В качестве примера приведём результаты расчётов для случая $n = 7$, $m = 14$, когда

$$A = \frac{m}{n} = 2, \quad c = \sqrt{\frac{m-n}{n(m-1)}} = \frac{\sqrt{13}}{13}.$$

Вычисления проводились в системе Maple 7. В качестве начального приближения мы брали матрицу, на главной диагонали которой стоят 1, а внедиагональные элементы равны \sqrt{c} .

При $\varepsilon = 0.01$ неравенство $\|G_k - H_{k+1}\| < \varepsilon$ выполнилось на 79-м шаге. Далее строим сигнатурную матрицу по формуле

$$Q = \{Q[i, i] = 0, \quad Q[i, j] = \text{sign } H_{79}[i, j] \text{ при } i \neq j\}$$

и проверяем выполнение равенства $Q^2 = 13 I_{14}$.

Дальнейшие вычисления повторяют собой вычисления, приведённые в работе [4]: построение матрицы $G = I_{14} + cQ$, нахождение её ортогонального разложения $G = P^T \Lambda P$ и построение матрицы Φ размера 7×14 :

$$\Phi^T = \begin{bmatrix} -0.4214 & 0.3771 & 0.0602 & -0.6056 & 0.2329 & 0.1176 & 0.4899 \\ 0.2649 & -0.1165 & 0.1489 & -0.6657 & -0.5434 & 0.3258 & 0.2253 \\ 0.0696 & 0.2487 & 0.1128 & -0.2336 & 0.2358 & 0.8805 & -0.1903 \\ -0.3938 & -0.0810 & 0.7188 & -0.0499 & 0.3574 & -0.4319 & 0.0789 \\ -0.4429 & 0.2692 & 0.6080 & 0.0840 & -0.4522 & 0.3666 & 0.1230 \\ 0.3823 & 0.2731 & 0.1848 & -0.6041 & 0.0578 & -0.6140 & 0.0412 \\ -0.0998 & 0.7667 & -0.2122 & 0.4032 & 0.0553 & 0.2972 & 0.3184 \\ 0.5460 & -0.0037 & 0.7921 & -0.0205 & -0.0267 & 0.1240 & -0.2365 \\ 0.3698 & 0.2590 & 0.2108 & 0.0260 & 0.8129 & 0.0407 & 0.2989 \\ -0.4481 & -0.6048 & 0.1208 & -0.0803 & -0.1906 & 0.0413 & 0.6127 \\ 0.5252 & -0.6295 & -0.0046 & 0.0619 & 0.1867 & 0.4743 & 0.2520 \\ 0.1454 & -0.0839 & 0.4286 & 0.7354 & -0.0093 & -0.0558 & 0.4933 \\ 0.3719 & 0.0702 & -0.3355 & -0.0795 & -0.0595 & -0.1468 & 0.8445 \\ 0.4111 & 0.4470 & 0.1149 & 0.1990 & -0.7211 & -0.2239 & 0.0889 \end{bmatrix}.$$

С помощью системы Maple 7 легко проверяются равенства $\Phi \Phi^T = 2 I_7$ и $\Phi^T \Phi = G$. Значит, столбцы матрицы Φ образуют равноугольный жёсткий фрейм в \mathbb{R}^7 .

Аналогично с помощью Maple 7 построены равноугольные жёсткие фреймы в \mathbb{R}^5 и \mathbb{R}^9 . Для этого потребовалось 291 и 76 итераций соответственно, что явно меньше полного перебора, используемого в [4] для построения сигнатурной матрицы.

ЛИТЕРАТУРА

1. Tropp J. A., Dhillon I. S., Heath R. W., Strohmer T. *Designing structured tight frames via an alternating projection method* // IEEE Trans. of Inform. Theory. 2005. V. 51. No. 1. P. 188–209.
2. Малозёмов В. Н., Певный А. Б. *Равноугольные системы векторов и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 18 сентября 2007 г. (<http://dha.spb.ru/rep07.shtml#0918>).
3. Малозёмов В. Н., Певный А. Б. *Четвёртое определение жёсткого фрейма* // Семинар «DHA & CAGD». Избранные доклады. 30 мая 2007 г. (<http://dha.spb.ru/rep07.shtml#0530>).
4. Максименко В. В., Певный А. Б. *Существование равноугольных жёстких фреймов* // Семинар «DHA & CAGD». Избранные доклады. 26 марта 2008 г. (<http://dha.spb.ru/rep08.shtml#0326>).

ЗАМЕЧАНИЕ О СИСТЕМАХ МЕРСЕДЕС-БЕНЦ

А. Н. Сабаев

16 сентября 2008 г.

Напомним [1], что системой Мерседес-Бенц в \mathbb{R}^n называется система, состоящая из $n + 1$ единичных векторов $\{\varphi_1, \dots, \varphi_{n+1}\}$, таких, что

$$\langle \varphi_k, \varphi_j \rangle = -\frac{1}{n} \quad \text{при } k \neq j.$$

Желая обобщить это понятие, введём следующее определение.

Система единичных векторов $\{\varphi_1, \dots, \varphi_m\}$ из \mathbb{R}^n при $m \geq n + 1$ называется системой Мерседес-Бенц, если

$$\langle \varphi_k, \varphi_j \rangle = c \quad \text{при } k \neq j, \tag{1}$$

где $c \neq 1$.

При $c = 1$ равенство (1) можно переписать в виде

$$\langle \varphi_k, \varphi_j \rangle = \|\varphi_k\| \cdot \|\varphi_j\| \quad \text{при } k \neq j.$$

Отсюда следует, что все векторы φ_k равны между собой, а это — неинтересный случай.

В [2] в определение системы Мерседес-Бенц входило ещё условие фреймовости системы $\{\varphi_1, \dots, \varphi_m\}$. Мы исключили это условие. Тем не менее, результат, установленный в [2], остаётся верным.

ТЕОРЕМА. *При $n \geq 2$ и $m > n + 1$ систем Мерседес-Бенц не существует.*

Доказательство проведём от противного. Предположим, что при некоторых $n \geq 2$ и $m > n + 1$ существует система Мерседес-Бенц $\{\varphi_1, \dots, \varphi_m\}$. Обозначим через Φ матрицу со столбцами $\varphi_1, \dots, \varphi_m$. Поскольку столбцы матрицы Φ линейно зависимы, то найдётся ненулевой вектор $a \in \mathbb{R}^m$, такой, что $\Phi a = \mathbf{0}$. Умножив на Φ^T слева, получим $\Phi^T \Phi a = \mathbf{0}$. Это значит, что система линейных уравнений $\Phi^T \Phi x = \mathbf{0}$ с квадратной матрицей $\Phi^T \Phi$ порядка m имеет нетривиальное решение.

Определитель матрицы $\Phi^T \Phi$ необходимо равен нулю. Запишем этот определитель. В силу (1)

$$\det(\Phi^T \Phi) = \begin{vmatrix} 1 & c & c & \dots & c \\ c & 1 & c & \dots & c \\ c & c & 1 & \dots & c \\ \dots & \dots & \dots & \dots & \dots \\ c & c & c & \dots & 1 \end{vmatrix}.$$

Добавим к первому столбцу все остальные столбцы, после чего вычтем первую строку из всех остальных строк. Получим

$$\det(\Phi^T \Phi) = \begin{vmatrix} 1 + (m-1)c & c & c & \dots & c \\ 0 & 1-c & 0 & \dots & 0 \\ 0 & 0 & 1-c & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1-c \end{vmatrix} = [1 + (m-1)c](1-c)^{m-1}.$$

По определению системы Мерседес-Бенц $c \neq 1$, поэтому $\det(\Phi^T \Phi) = 0$ только при $c = -\frac{1}{m-1}$.

Теперь обозначим через Φ_0 матрицу со столбцами $\varphi_1, \dots, \varphi_{n+1}$. Её столбцы тоже линейно зависимы. Аналогично предыдущему придём к равенству $\det(\Phi_0^T \Phi_0) = 0$, которое возможно только при $c = -\frac{1}{n}$. Значит, величина c , входящая в определение системы Мерседес-Бенц $\{\varphi_1, \dots, \varphi_m\}$, должна одновременно равняться и $-\frac{1}{m-1}$ и $-\frac{1}{n}$, что при $m > n + 1$ невозможно.

Теорема доказана. \square

При $m = n + 1$ системы Мерседес-Бенц существуют. Их полное описание дано в [1].

ЛИТЕРАТУРА

1. Малозёмов В. Н., Певный А. Б. *Системы Мерседес-Бенц и жёсткие фреймы* // Семинар «DHA & CAGD». Избранные доклады. 28 февраля 2007 г. (<http://dha.spb.ru/rep07.shtml#0228>).
2. Малозёмов В. Н., Певный А. Б. *Систем Мерседес-Бенц при $m > n + 1$ не существует* // Семинар «DHA & CAGD». Избранные доклады. 13 февраля 2008 г. (<http://dha.spb.ru/rep08.shtml#0213>).

ПОВЕРХНОСТИ БЕЗЬЕ НА ЧЕТЫРЁХУГОЛЬНИКЕ И ГЛАДКИЕ СОСТАВНЫЕ ПОВЕРХНОСТИ

М. И. Григорьев

20 сентября 2008 г.

1°. Пусть в пространстве \mathbb{R}^s задана матрица полюсов

$$\begin{array}{cccc} \mathbf{a}_{00} & \mathbf{a}_{01} & \cdots & \mathbf{a}_{0n} \\ \mathbf{a}_{10} & \mathbf{a}_{11} & \cdots & \mathbf{a}_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{m0} & \mathbf{a}_{m1} & \cdots & \mathbf{a}_{mn} \end{array} \quad (1)$$

По строкам этой матрицы построим $m + 1$ кривую Безье n -й степени [1]

$$\mathbf{N}_i(v) = \sum_{j=0}^n \mathbf{a}_{ij} b_j^n(v), \quad v \in [0, 1], \quad i \in 0 : m,$$

где $b_j^n(v) = C_n^j v^j (1 - v)^{n-j}$ — базисные полиномы Бернштейна степени n . Кривые $\mathbf{N}_i(v)$ будем называть *образующими*. Зафиксируем $v \in [0, 1]$. По точкам $\mathbf{N}_0(v), \mathbf{N}_1(v), \dots, \mathbf{N}_m(v)$ можно в свою очередь построить кривую Безье $\mathbf{B}(u, v)$, $u \in [0, 1]$. Когда параметр v пробегает весь отрезок $[0, 1]$, кривая $\mathbf{B}(u, v)$ описывает поверхность в пространстве \mathbb{R}^s , которая называется *поверхностью Безье степени $m \times n$, заданной на четырёхугольнике*. Её аналитическое представление имеет вид

$$\mathbf{B}(u, v) = \sum_{i=0}^m \mathbf{N}_i(v) b_i^m(u) = \sum_{i=0}^m \sum_{j=0}^n \mathbf{a}_{ij} b_i^m(u) b_j^n(v). \quad (2)$$

Представим (2) в виде

$$\mathbf{B}(u, v) = \sum_{j=0}^n \sum_{i=0}^m \mathbf{a}_{ij} b_i^m(u) b_j^n(v) = \sum_{j=0}^n \mathbf{M}_j(u) b_j^n(v). \quad (3)$$

Таким образом, образующими для поверхности $\mathbf{B}(u, v)$ являются также кривые Безье m -й степени

$$\mathbf{M}_j(u) = \sum_{i=0}^m \mathbf{a}_{ij} b_i^m(u), \quad u \in [0, 1], \quad j \in 0 : n,$$

построенные по столбцам матрицы (1).

На рис. 1 приведены полюсы и образующие кривые для случая $m = 2$, $n = 3$. Построенная по ним поверхность Безье изображена на рис. 2.

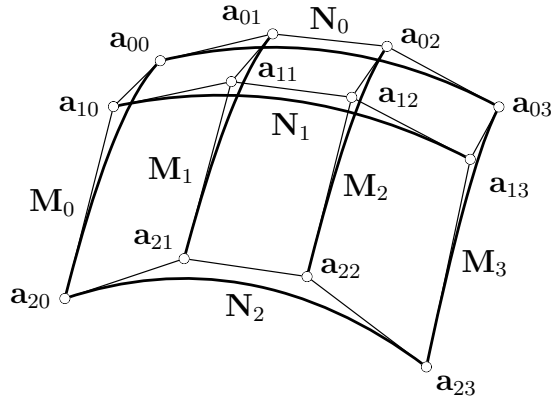


Рис. 1

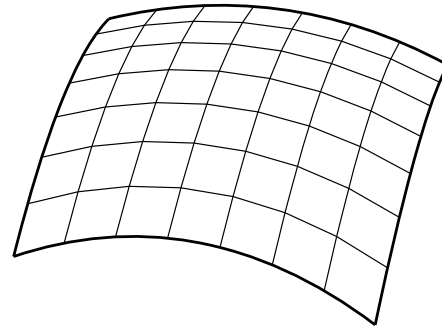


Рис. 2

Напомним некоторые свойства базисных полиномов Бернштейна (приведём их для полиномов n -й степени):

$$\begin{aligned} b_j^n(0) &= 0, & j &\in 1 : n; & b_0^n(0) &= 1; \\ b_j^n(1) &= 0, & j &\in 0 : n-1; & b_n^n(1) &= 1. \end{aligned} \quad (4)$$

Из (2) и (3) с учётом (4) следует, что

$$\begin{aligned} \mathbf{B}(0, v) &= \mathbf{N}_0(v), & \mathbf{B}(1, v) &= \mathbf{N}_m(v), & v &\in [0, 1]; \\ \mathbf{B}(u, 0) &= \mathbf{M}_0(u), & \mathbf{B}(u, 1) &= \mathbf{M}_n(u), & u &\in [0, 1]. \end{aligned} \quad (5)$$

Далее

$$b_j^n(v) \geq 0 \text{ на } [0, 1] \text{ при всех } j \in 0 : n;$$

$$\sum_{j=0}^n b_j^n(v) \equiv 1.$$

Значит

$$b_i^m(u) b_j^n(v) \geq 0 \text{ на } [0, 1] \times [0, 1] \text{ при всех } i \in 0 : m, j \in 0 : n;$$

$$\sum_{i=0}^m \sum_{j=0}^n b_i^m(u) b_j^n(v) \equiv 1.$$

Отсюда следует, что вектор $\mathbf{B}(u, v)$ при фиксированных $u \in [0, 1]$ и $v \in [0, 1]$ является выпуклой комбинацией полюсов \mathbf{a}_{ij} , $i \in 0 : m$, $j \in 0 : n$. С учётом (5) заключаем, что поверхность $\mathbf{B}(u, v)$ ограничена кривыми $\mathbf{M}_0(u)$, $\mathbf{M}_n(u)$, $\mathbf{N}_0(v)$, $\mathbf{N}_m(v)$ и не выходит за пределы выпуклой оболочки своих полюсов.

2°. Зафиксируем $u \in [0, 1]$ и $v \in [0, 1]$. Введём полюсы

$$\mathbf{a}_{ij}^{ks}(u, v), \quad i \in 0 : m - k, \quad k \in 0 : m, \quad j \in 0 : n - s, \quad s \in 0 : n, \quad (6)$$

с помощью рекуррентных соотношений

$$\mathbf{a}_{ij}^{ks} = (1 - u) \mathbf{a}_{ij}^{k-1, s} + u \mathbf{a}_{i+1, j}^{k-1, s}, \quad i \in 0 : m - k, \quad k \in 1 : m; \quad (7)$$

$$\mathbf{a}_{ij}^{ks} = (1 - v) \mathbf{a}_{ij}^{k, s-1} + v \mathbf{a}_{i, j+1}^{k, s-1}, \quad j \in 0 : n - s, \quad s \in 1 : n; \quad (8)$$

$$\mathbf{a}_{ij}^{00} = \mathbf{a}_{ij}, \quad i \in 0 : m, \quad j \in 0 : n.$$

ПРЕДЛОЖЕНИЕ 1. Для полюсов (6) справедливо представление

$$\mathbf{a}_{ij}^{ks}(u, v) = \sum_{\alpha=0}^k \sum_{\beta=0}^s \mathbf{a}_{i+\alpha, j+\beta} b_{\alpha}^k(u) b_{\beta}^s(v). \quad (9)$$

Доказательство. Базисные полиномы $b_{\alpha}^k(u)$, $\alpha \in 0 : k$, $k \in 0 : m$, удовлетворяют рекуррентным соотношениям [1]

$$b_{\alpha}^k(u) = (1 - u) b_{\alpha}^{k-1}(u) + u b_{\alpha-1}^{k-1}(u), \quad \alpha \in 1 : k - 1; \quad k \in 2 : m;$$

$$b_0^k(u) = (1 - u) b_0^{k-1}(u), \quad b_k^k(u) = u b_{k-1}^{k-1}(u), \quad k \in 1 : m;$$

$$b_0^0(u) \equiv 1.$$

С учётом (7) имеем

$$\begin{aligned} \sum_{\alpha=0}^k \sum_{\beta=0}^s \mathbf{a}_{i+\alpha, j+\beta} b_{\alpha}^k(u) b_{\beta}^s(v) &= \sum_{\beta=0}^s \left(\mathbf{a}_{i, j+\beta}^{00} b_0^k(u) + \mathbf{a}_{i+k, j+\beta}^{00} b_k^k(u) + \right. \\ &\quad \left. + \sum_{\alpha=1}^{k-1} \mathbf{a}_{i+\alpha, j+\beta}^{00} [(1 - u) b_{\alpha}^{k-1}(u) + u b_{\alpha-1}^{k-1}(u)] \right) b_{\beta}^s(v) = \\ &= \sum_{\beta=0}^s \left(\sum_{\alpha=0}^{k-1} \mathbf{a}_{i+\alpha, j+\beta}^{00} (1 - u) b_{\alpha}^{k-1}(u) + \sum_{\alpha=1}^k \mathbf{a}_{i+\alpha, j+\beta}^{00} u b_{\alpha-1}^{k-1}(u) \right) b_{\beta}^s(v) = \end{aligned}$$

$$\begin{aligned}
&= \sum_{\beta=0}^s \left(\sum_{\alpha=0}^{k-1} [(1-u) \mathbf{a}_{i+\alpha, j+\beta}^{00} + u \mathbf{a}_{i+\alpha+1, j+\beta}^{00}] b_{\alpha}^{k-1}(u) \right) b_{\beta}^s(v) = \\
&= \sum_{\alpha=0}^{k-1} \sum_{\beta=0}^s \mathbf{a}_{i+\alpha, j+\beta}^{10} b_{\alpha}^{k-1}(u) b_{\beta}^s(v).
\end{aligned}$$

Далее, используя рекуррентные соотношения для $b_{\beta}^s(v)$ и (8), уменьшим на единицу верхний предел суммирования во второй сумме

$$\sum_{\alpha=0}^{k-1} \sum_{\beta=0}^s \mathbf{a}_{i+\alpha, j+\beta}^{10} b_{\alpha}^{k-1}(u) b_{\beta}^s(v) = \sum_{\alpha=0}^{k-1} \sum_{\beta=0}^{s-1} \mathbf{a}_{i+\alpha, j+\beta}^{11} b_{\alpha}^{k-1}(u) b_{\beta}^{s-1}(v).$$

Продолжая аналогично, получаем

$$\begin{aligned}
&\sum_{\alpha=0}^{k-1} \sum_{\beta=0}^{s-1} \mathbf{a}_{i+\alpha, j+\beta}^{11} b_{\alpha}^{k-1}(u) b_{\beta}^{s-1}(v) = \sum_{\alpha=0}^{k-2} \sum_{\beta=0}^{s-1} \mathbf{a}_{i+\alpha, j+\beta}^{21} b_{\alpha}^{k-2}(u) b_{\beta}^{s-1}(v) = \\
&= \dots = \sum_{\alpha=0}^1 \sum_{\beta=0}^1 \mathbf{a}_{i+\alpha, j+\beta}^{k-1, s-1} b_{\alpha}^1(u) b_{\beta}^1(v) = \sum_{\beta=0}^1 \mathbf{a}_{i, j+\beta}^{k, s-1} b_{\beta}^1(v) = \\
&= (1-v) \mathbf{a}_{ij}^{k, s-1} + v \mathbf{a}_{i, j+1}^{k, s-1} = \mathbf{a}_{ij}^{ks}.
\end{aligned}$$

Предложение доказано. □

Формула (9) наиболее содержательна при $k = m$, $s = n$. В этом случае

$$\mathbf{a}_{00}^{mn}(u, v) = \sum_{\alpha=0}^m \sum_{\beta=0}^n \mathbf{a}_{\alpha\beta} b_{\alpha}^m(u) b_{\beta}^n(v) = \mathbf{B}(u, v).$$

Таким образом, значение полинома $\mathbf{B}(u, v)$ можно находить с помощью рекуррентных соотношений (7)–(8). Вычисление начинается с матрицы полюсов (1). На каждом шаге происходит пересчёт полюсов по формуле (7) или (8). Поскольку порядок использования соотношений (7) и (8) произволен, мы получаем пакет алгоритмов для вычисления значения полинома $\mathbf{B}(u, v)$.

Приведём конкретный пример алгоритма вычисления. Итак, начинаем вычисления с матрицы (1). Найдём сначала $m + 1$ полюс $\mathbf{a}_{i0}^{0n}(v)$, $i \in 0 : m$, с помощью рекуррентного соотношения (8). Затем, применяя (7) к полученным полюсам, вычисляем значение $\mathbf{a}_{00}^{mn}(u, v) = \mathbf{B}(u, v)$. Геометрически это соответствует нахождению точек на образующих кривых $\mathbf{N}_i(v)$ по алгоритму

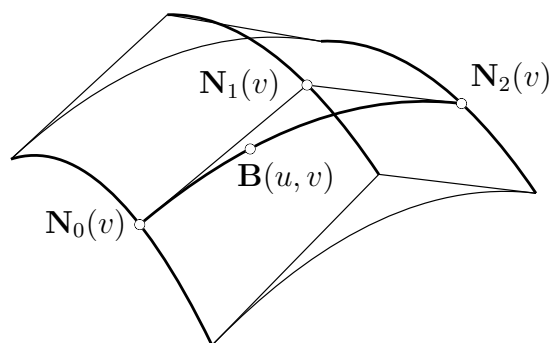


Рис. 3

Кастельжо, а затем вычислению по такому же алгоритму точки на кривой Безье $B(u, v)$ с полюсами $N_i(v)$, лежащей на поверхности (рис. 3).

Отметим, что при $n < m$ рассмотренный алгоритм является наиболее эффективным алгоритмом из всего пакета.

Рассмотрим ещё один вариант алгоритма. Пусть рекуррентные соотношения (7) и (8) применяются поочерёдно. При этом строится последовательность матриц полюсов $\{a_{ij}^{00}\}$, $\{a_{ij}^{10}\}$, $\{a_{ij}^{11}\}$, $\{a_{ij}^{21}\}$ и т. д. Данный алгоритм вычисления представляет собой так называемый *прямой алгоритм Кастельжо* для поверхностей Безье на четырёхугольнике [2]. На рис. 4 показаны этапы вычисления точки на поверхности таким способом при $m = n = 2$.

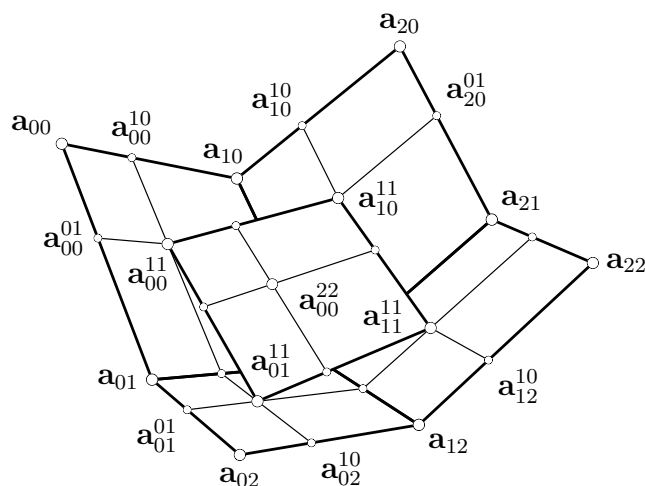


Рис. 4. Прямой алгоритм Кастельжо

3°. Расширим матрицу (1), добавив к ней полюсы $\mathbf{a}_{-i,j}$, $i \in 1 : p$, $j \in 0 : n$ (здесь p — фиксированное натуральное число). По столбцам $\{\mathbf{a}_{-i,j}\}$, $i \in 0 : p$, $j \in 0 : n$, построим $n+1$ кривых Безье степени p , заданных на отрезке $[-1, 0]$:

$$\widetilde{\mathbf{M}}_j(u) = \sum_{i=0}^p \mathbf{a}_{i-p,j} b_i^p(u+1), \quad j \in 0 : n, \quad u \in [-1, 0].$$

По этим кривым построим поверхность Безье степени $p \times n$, заданную на квадрате $[-1, 0] \times [0, 1]$:

$$\mathbf{Q}(u, v) = \sum_{j=0}^n \widetilde{\mathbf{M}}_j(u) b_j^n(v), \quad u \in [-1, 0], \quad v \in [0, 1]. \quad (10)$$

Поверхности $\mathbf{Q}(u, v)$ и $\mathbf{B}(u, v)$ имеют общее ребро $\mathbf{Q}(0, v) = \mathbf{B}(0, v)$, $v \in [0, 1]$.

Рассмотрим составную поверхность Безье

$$\mathbf{S}(u, v) = \begin{cases} \mathbf{Q}(u, v), & u \in [-1, 0], \quad v \in [0, 1]; \\ \mathbf{B}(u, v), & u \in [0, 1], \quad v \in [0, 1]. \end{cases}$$

Введём оператор взятия конечной разности на двухиндексном множестве элементов

$$\begin{aligned} (\Delta^\alpha \mathbf{a}_{*,j})_i &= \sum_{k=0}^{\alpha} (-1)^{\alpha-k} C_{\alpha}^k \mathbf{a}_{i+k,j}; \\ (\Delta^\beta \mathbf{a}_{i,*})_j &= \sum_{s=0}^{\beta} (-1)^{\beta-s} C_{\beta}^s \mathbf{a}_{i,j+s}. \end{aligned}$$

ПРЕДЛОЖЕНИЕ 2. Для того, чтобы поверхность $\mathbf{S}(u, v)$ обладала гладкостью r -го порядка ($r \leq \min\{m, p\}$) необходимо и достаточно выполнение условий

$$A_p^\alpha (\Delta^\alpha \mathbf{a}_{*,j})_{-\alpha} = A_m^\alpha (\Delta^\alpha \mathbf{a}_{*,j})_0, \quad j \in 0 : n, \quad \alpha \in 1 : r, \quad (11)$$

где $A_p^\alpha = \frac{p!}{(p-\alpha)!}$, $A_m^\alpha = \frac{m!}{(m-\alpha)!}$.

Доказательство. Необходимость. Очевидно, что гладкость поверхности $\mathbf{S}(u, v)$ может нарушаться только вдоль ребра $\mathbf{S}(0, v)$, $v \in [0, 1]$. Выпишем условия согласования гладкости полиномов $\mathbf{Q}(u, v)$ и $\mathbf{B}(u, v)$ на этом ребре:

$$\left. \frac{\partial^{\alpha+\beta} \mathbf{Q}(u, v)}{\partial u^\alpha \partial v^\beta} \right|_{u=0} = \left. \frac{\partial^{\alpha+\beta} \mathbf{B}(u, v)}{\partial u^\alpha \partial v^\beta} \right|_{u=0},$$

$$\alpha \in 0 : r, \quad \beta \in 0 : \min\{n, r\}, \quad \alpha + \beta \in 1 : r.$$

Примем в последнем равенстве $\beta = 0$. С учётом (3) и (10) имеем

$$\sum_{j=0}^n \widetilde{\mathbf{M}}_j^{(\alpha)}(0) b_j^n(v) = \sum_{j=0}^n \mathbf{M}_j^{(\alpha)}(0) b_j^n(v), \quad \alpha \in 1 : r, \quad v \in [0, 1],$$

что равносильно

$$\widetilde{\mathbf{M}}_j^{(\alpha)}(0) = \mathbf{M}_j^{(\alpha)}(0), \quad j \in 0 : n, \quad \alpha \in 1 : r. \quad (12)$$

Для производной порядка α полинома в форме Бернштейна $\mathbf{M}_j(u)$ справедлива формула [1]

$$\mathbf{M}_j^{(\alpha)}(u) = A_m^\alpha \sum_{i=0}^{m-\alpha} (\Delta^\alpha \mathbf{a}_{*,j})_i b_i^{m-\alpha}(u). \quad (13)$$

Для полиномов $\widetilde{\mathbf{M}}_j(u)$ формула (13) принимает вид

$$\widetilde{\mathbf{M}}_j^{(\alpha)}(u) = A_p^\alpha \sum_{i=0}^{p-\alpha} (\Delta^\alpha \mathbf{a}_{*,j})_{i-p} b_i^{p-\alpha}(u+1). \quad (14)$$

Значит, с учётом (4), равенство (12) эквивалентно

$$A_p^\alpha (\Delta^\alpha \mathbf{a}_{*,j})_{-\alpha} = A_m^\alpha (\Delta^\alpha \mathbf{a}_{*,j})_0, \quad j \in 0 : n, \quad \alpha \in 1 : r.$$

Достаточность. Пусть выполнены условия (11). Покажем, что все частные производные полиномов $\mathbf{Q}(u, v)$ и $\mathbf{B}(u, v)$ до r -го порядка совпадают на их общем ребре. Зафиксируем два целых числа $\alpha \in 0 : r$, $\beta \in 0 : \min\{n, r\}$ таких, что $\alpha + \beta \in 1 : r$. Имеем

$$\left. \frac{\partial^{\alpha+\beta} \mathbf{B}(u, v)}{\partial u^\alpha \partial v^\beta} \right|_{u=0} = \frac{\partial^\beta}{\partial v^\beta} \sum_{j=0}^n \mathbf{M}_j^{(\alpha)}(0) b_j^n(v).$$

С учётом (11), (13) и (14) получим

$$\mathbf{M}_j^{(\alpha)}(0) = A_m^\alpha (\Delta^\alpha \mathbf{a}_{*,j})_0 = A_p^\alpha (\Delta^\alpha \mathbf{a}_{*,j})_{-\alpha} = \widetilde{\mathbf{M}}_j^{(\alpha)}(0).$$

Значит

$$\frac{\partial^\beta}{\partial v^\beta} \sum_{j=0}^n \mathbf{M}_j^{(\alpha)}(0) b_j^n(v) = \frac{\partial^\beta}{\partial v^\beta} \sum_{j=0}^n \widetilde{\mathbf{M}}_j^{(\alpha)}(0) b_j^n(v) = \left. \frac{\partial^{\alpha+\beta} \mathbf{Q}(u, v)}{\partial u^\alpha \partial v^\beta} \right|_{u=0}.$$

Предложение доказано. \square

Замечание. Условия (11) при каждом $j \in 0 : n$ совпадают с условиями гладкой сшивки до r -го порядка образующих кривых $\mathbf{M}_j(u)$ и $\widetilde{\mathbf{M}}_j(u)$ в их общей точке $\mathbf{M}_j(0) = \widetilde{\mathbf{M}}_j(0)$.

На рис. 5 приведены две поверхности Безье, спитые с сохранением гладкости 1-го порядка. Полюсы, отмеченные на рисунке, связаны условиями (11).

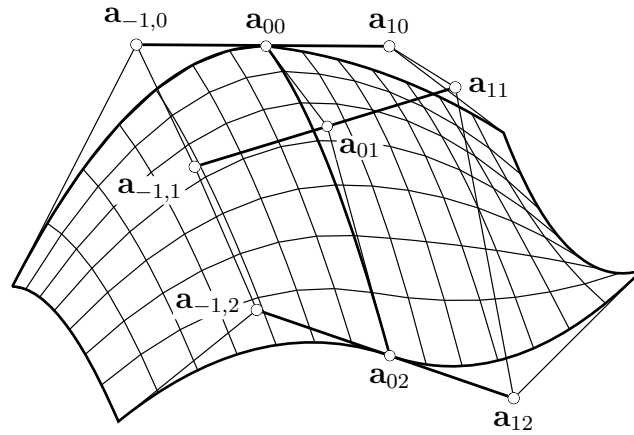
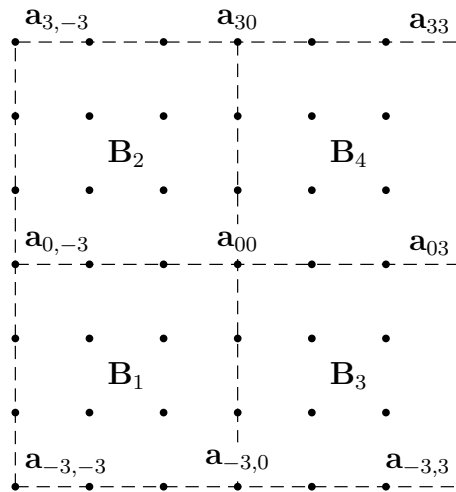


Рис. 5. Сшивки поверхностей Безье по общему ребру

4°. В предыдущем пункте мы получили условия гладкости поверхности, составленной из двух порций Безье на четырёхугольнике. Рассмотрим случай сшивки четырёх порций $\mathbf{B}_i(u, v)$, $i = 1, \dots, 4$, предполагая, что они имеют общие ребра (рис. 6).

Рис. 6. Сшивки четырёх порций $\mathbf{B}_i(u, v)$, $i = 1, \dots, 4$

Для простоты будем считать, что степени всех $\mathbf{B}_i(u, v)$ совпадают и равны $m \times n$. Пусть выбрано $r \in 1 : \min\{m, n\}$. Предположим, что полюсы порции $\mathbf{B}_1(u, v)$, $u \in [-1, 0]$, $v \in [-1, 0]$, зафиксированы и изменяться не могут. Для того, чтобы продолжить \mathbf{B}_1 на $[0, 1] \times [-1, 0]$ с сохранением гладкости r -го порядка, необходимо обеспечить выполнение условий

$$(\Delta^\alpha \mathbf{a}_{*, -j})_0 = (\Delta^\alpha \mathbf{a}_{*, -j})_{-\alpha}, \quad j \in 0 : n, \quad \alpha \in 1 : r.$$

В этом случае необходимо

$$\mathbf{a}_{i,-j} = \sum_{k=0}^i C_i^k (\Delta^k \mathbf{a}_{*, -j})_0 = \sum_{k=0}^i C_i^k (\Delta^k \mathbf{a}_{*, -j})_{-k}, \quad i \in 1:r, \quad j \in 0:n. \quad (15)$$

Остальные $(m-r) \times (n+1)$ полюсов порции $\mathbf{B}_2(u, v)$ выбираются произвольно.

Аналогично продолжая $\mathbf{B}_1(u, v)$ на $[-0, 1] \times [0, 1]$, получаем условия

$$(\Delta^\beta \mathbf{a}_{-i,*})_0 = (\Delta^\beta \mathbf{a}_{-i,*})_{-\beta}, \quad i \in 0:m, \quad \beta \in 1:r,$$

откуда

$$\mathbf{a}_{-i,j} = \sum_{s=0}^j C_j^s (\Delta^s \mathbf{a}_{-i,*})_0 = \sum_{s=0}^j C_j^s (\Delta^s \mathbf{a}_{-i,*})_{-s}, \quad j \in 1:r, \quad i \in 0:m. \quad (16)$$

Свободными остаются $(m+1) \times (n-r)$ полюсов $\mathbf{B}_3(u, v)$.

Теперь, если мы будем продолжать $\mathbf{B}_2(u, v)$ и $\mathbf{B}_3(u, v)$ на $[0, 1] \times [0, 1]$, то придём к следующим выражениям для определения полюсов порции $\mathbf{B}_4(u, v)$:

$$\mathbf{a}_{ij} = \sum_{k=0}^i C_i^k (\Delta^k \mathbf{a}_{*,j})_0 = \sum_{k=0}^i C_i^k (\Delta^k \mathbf{a}_{*,j})_{-k}, \quad i \in 1:r, \quad j \in 1:n; \quad (17)$$

$$\mathbf{a}_{ij} = \sum_{s=0}^j C_j^s (\Delta^s \mathbf{a}_{i,*})_0 = \sum_{s=0}^j C_j^s (\Delta^s \mathbf{a}_{i,*})_{-s}, \quad j \in 1:r, \quad i \in 1:m. \quad (18)$$

Оставшиеся $(m-r) \times (n-r)$ полюсов $\mathbf{B}_4(u, v)$ произвольны.

Отметим, что полюсы \mathbf{a}_{ij} , $i, j \in 1:r$, определяются двумя способами. Покажем, что неоднозначности в данной ситуации не возникает. Обозначим полюсы, получаемые по формулам (17) и (18) соответственно \mathbf{a}_{ij}^u и \mathbf{a}_{ij}^v .

ЛЕММА 1. В случае выполнения условий (15) и (16) справедливо равенство

$$\mathbf{a}_{ij}^u = \mathbf{a}_{ij}^v, \quad i \in 1:r, \quad j \in 1:r.$$

Доказательство. Имеем

$$\begin{aligned} \mathbf{a}_{ij}^u &= \sum_{k=0}^i C_i^k (\Delta^k \mathbf{a}_{*,j})_{-k} = \sum_{k=0}^i C_i^k \left(\Delta^k \sum_{s=0}^j C_j^s (\Delta^s \mathbf{a}_{*,*})_{-s} \right)_{-k} = \\ &= \sum_{s=0}^j C_j^s \left(\Delta^s \sum_{k=0}^i C_i^k (\Delta^k \mathbf{a}_{*,*})_{-k} \right)_{-s} = \sum_{s=0}^j C_j^s (\Delta^s \mathbf{a}_{i,*})_{-s} = \mathbf{a}_{ij}^v. \end{aligned}$$

Лемма доказана. \square

На рис. 7 приведена составная поверхность, сшитая из четырёх поверхностей Безье при $m = n = 3$, $r = 2$. В этом случае управления формой поверхности осуществляется при помощи 25 полюсов.

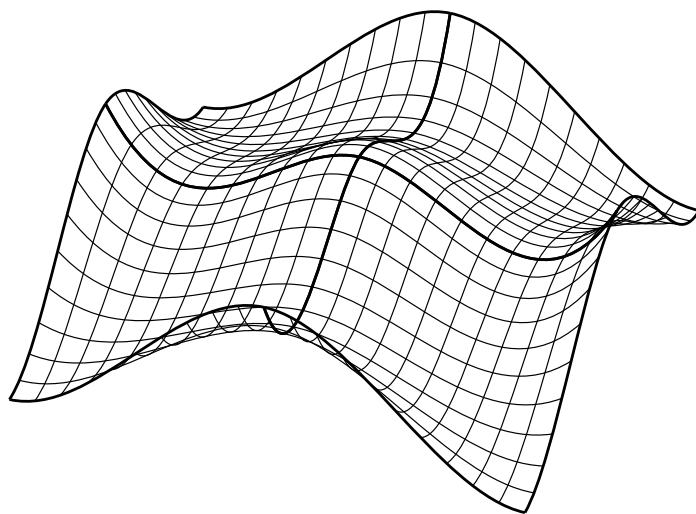


Рис. 7

5°. Приведём два примера C^1 -гладких составных поверхностей Безье. На рис. 8 изображена поверхность, сшитая из 16 порций Безье. На рис. 9 рассмотрен случай нетривиального расположения сшиваемых порций.

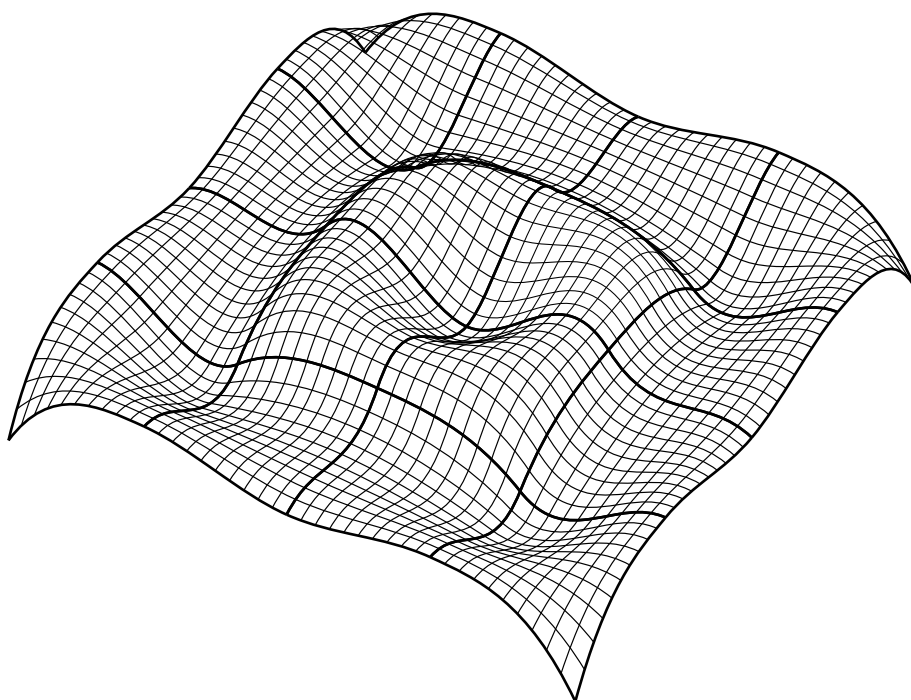


Рис. 8

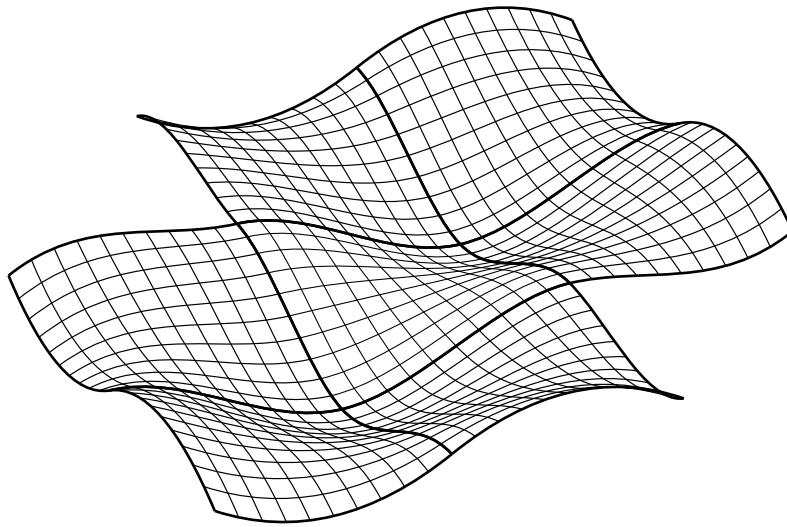


Рис. 9

ЛИТЕРАТУРА

1. Григорьев М. И., Малозёмов В. Н., Сергеев А. Н. *Полиномы Бернштейна и составные кривые Безье* // Журн. вычисл. мат. и матем. физ. 2006. Т. 46. № 11. С. 1962–1971.
2. Farin G. *Curves and surfaces for CAGD*. 5th ed. San Diego: Academic Press, 2002. xvii + 499 pp.

ПОВЕРХНОСТИ КУНСА НА ТРЕУГОЛЬНИКЕ С ГРАНИЧНЫМИ УСЛОВИЯМИ ПЕРВОГО ПОРЯДКА

Н. В. Чашников

4 октября 2008 г.

1°. Пусть $\Delta = \{(u, v, w) \mid u + v + w = 1, u \geq 0, v \geq 0, w \geq 0\}$. Определим операторы D_1 , D_2 и D_3 для вектор-функций $s: \Delta \rightarrow \mathbb{R}^3$:

$$\begin{aligned} D_1 s(u, v, w) &= \lim_{t \rightarrow 0} \frac{s(u, v - t, w + t) - s(u, v, w)}{t} && \text{при } u < 1, \\ D_2 s(u, v, w) &= \lim_{t \rightarrow 0} \frac{s(u + t, v, w - t) - s(u, v, w)}{t} && \text{при } v < 1, \\ D_3 s(u, v, w) &= \lim_{t \rightarrow 0} \frac{s(u - t, v + t, w) - s(u, v, w)}{t} && \text{при } w < 1, \end{aligned} \quad (1)$$

$$\begin{aligned} D_1 s(1, 0, 0) &= -D_2 s(1, 0, 0) - D_3 s(1, 0, 0), \\ D_2 s(0, 1, 0) &= -D_1 s(0, 1, 0) - D_3 s(0, 1, 0), \\ D_3 s(0, 0, 1) &= -D_1 s(0, 0, 1) - D_2 s(0, 0, 1). \end{aligned}$$

Если $(u, v, w) \in \partial\Delta$, то значение $D_i s(u, v, w)$ будем вычислять как соответствующий односторонний предел. Например, если $v = 0, w > 0$, то в выражении для $D_1 s(u, v, w)$ предел будем считать левосторонним, а если $w = 0, v > 0$, то правосторонним.

Заметим, что если найдётся вектор-функция $r: \Omega \rightarrow \mathbb{R}^3$, $\Omega \subset \mathbb{R}^3$, такая, что $r \in C^1(\Omega)$ и $s = r|_{\Delta}$, то

$$D_1 s = s_w - s_v, \quad D_2 s = s_u - s_w, \quad D_3 s = s_v - s_u. \quad (2)$$

Ясно, что в этом случае $D_1 s + D_2 s + D_3 s \equiv 0$. Покажем, что это тождество справедливо и в общем случае.

ЛЕММА. Если вектор-функции s , D_1s , D_3s непрерывны на Δ , то вектор-функция D_2s определена и непрерывна на Δ и выполнено тождество $D_1s + D_2s + D_3s = 0$.

Доказательство. Для угловых точек множества Δ утверждение справедливо по определению. Поэтому будем считать, что $u, v, w < 1$.

Положим $r(u, w) = s(u, 1 - u - w, w)$ для $u, w \in [0, 1]$, $u + w \leq 1$. По определению (1) имеем

$$r_u(u, w) = -D_3s(u, 1 - u - w, w), \quad r_w(u, w) = D_1s(u, 1 - u - w, w).$$

Так как $D_1s, D_3s \in C(\Delta)$, то $r \in C^1$. Следовательно, производная от r по направлению равна скалярному произведению вектора направления на градиент. Значит,

$$D_2s(u, 1 - u - w, w) = \lim_{t \rightarrow 0} \frac{r(u + t, w - t) - r(u, w)}{t} = r_u(u, v) - r_w(u, v).$$

Таким образом, вектор-функция D_2s определена и непрерывна на Δ и

$$D_1s(u, 1 - u - w, w) + D_2s(u, 1 - u - w, w) + D_3s(u, 1 - u - w, w) \equiv 0,$$

что и требовалось. \square

2°. Поставим задачу: *построить по непрерывно дифференцируемым вектор-функциям $g_1, g_2, g_3: [0, 1] \rightarrow \mathbb{R}^3$ и непрерывным вектор-функциям $f_1, f_2, f_3: [0, 1] \rightarrow \mathbb{R}^3$ возможно более простую вектор-функцию $s: \Delta \rightarrow \mathbb{R}^3$, удовлетворяющую условиям*

$$s, D_1s, D_2s, D_3s \in C(\Delta);$$

$$s(u, 0, 1 - u) \equiv g_1(u), \quad s(1 - v, v, 0) \equiv g_2(v), \quad s(0, 1 - w, w) \equiv g_3(w); \quad (3)$$

$$D_1s(u, 0, 1 - u) \equiv f_1(u), \quad D_2s(1 - v, v, 0) \equiv f_2(v), \quad D_3s(0, 1 - w, w) \equiv f_3(w). \quad (4)$$

Как видно, на границе множества Δ заданы значения вектор-функции s и на каждой стороне заданы значения одного из операторов D_i . Покажем, что из этих условий можно вывести значения всех операторов D_i на границе.

Продифференцируем тождества (3). Получим

$$D_2s(u, 0, 1 - u) \equiv g'_1(u), \quad D_3s(1 - v, v, 0) \equiv g'_2(v), \quad D_1s(0, 1 - w, w) \equiv g'_3(w). \quad (5)$$

Положим $h_i(t) = -f_i(t) - g'_i(t)$, $i = 1, 2, 3$. Тогда из леммы и тождеств (4) и (5) следует, что

$$D_3s(u, 0, 1 - u) \equiv h_1(u), \quad D_1s(1 - v, v, 0) \equiv h_2(v), \quad D_2s(0, 1 - w, w) \equiv h_3(w). \quad (6)$$

Выясним необходимые условия согласования на функции g_i и f_i . Последовательно подставляя в тождества (3) вместо u , v и w значения 0 и 1, получаем

$$\begin{aligned} g_1(1) &= s(1, 0, 0) = g_2(0), \\ g_2(1) &= s(0, 1, 0) = g_3(0), \\ g_3(1) &= s(0, 0, 1) = g_1(0). \end{aligned} \quad (7)$$

Аналогично, последовательно подставляя в тождества (4), (5) и (6) вместо u , v и w значения 0 и 1, придём к равенствам

$$g'_1(1) = f_2(0), \quad g'_2(1) = f_3(0), \quad g'_3(1) = f_1(0), \quad (8)$$

$$g'_1(0) = h_3(1), \quad g'_2(0) = h_1(1), \quad g'_3(0) = h_2(1). \quad (9)$$

Условия (9) можно переписать без использования функций h_i :

$$g'_1(0) = -f_3(1) - f_1(0), \quad g'_2(0) = -f_1(1) - f_2(0), \quad g'_3(0) = -f_2(1) - f_3(0). \quad (10)$$

3°. Будем искать вектор-функцию c_1 , удовлетворяющую условиям

$$\begin{aligned} c_1(u, 0, 1-u) &= g_1(u), \quad D_1 c_1(u, 0, 1-u) = f_1(u), \quad u \in [0, 1], \\ c_1(1-v, v, 0) &= g_2(v), \quad D_1 c_1(1-v, v, 0) = h_2(v), \quad v \in [0, 1]. \end{aligned} \quad (11)$$

Зафиксируем $u_0 \in [0, 1]$ и положим $p(t) = c_1(u_0, (1-t)(1-u_0), t(1-u_0))$. Тогда

$$\begin{aligned} p(0) &= c_1(u_0, 1-u_0, 0), \quad p'(0) = (1-u_0)D_1 c_1(u_0, 1-u_0, 0), \\ p(1) &= c_1(u_0, 0, 1-u_0), \quad p'(1) = (1-u_0)D_1 c_1(u_0, 0, 1-u_0). \end{aligned}$$

Таким образом, тождества (11) эквивалентны условиям на вектор-функцию $p(t)$:

$$\begin{aligned} p(0) &= g_2(1-u_0), \quad p'(0) = (1-u_0)h_2(1-u_0), \\ p(1) &= g_1(u_0), \quad p'(1) = (1-u_0)f_1(u_0). \end{aligned}$$

Возьмём в качестве $p(t)$ интерполяционный полином Эрмита

$$p(t) = H_1(t)g_2(1-u_0) + (1-u_0)H_2(t)h_2(1-u_0) + (1-u_0)H_3(t)f_1(u_0) + H_4(t)g_1(u_0),$$

где H_1, H_2, H_3, H_4 — кубические полиномы Эрмита

$$\begin{aligned} H_1(x) &= 2x^3 - 3x^2 + 1, \\ H_2(x) &= x^3 - 2x^2 + x, \\ H_3(x) &= x^3 - x^2, \\ H_4(x) &= -2x^3 + 3x^2. \end{aligned} \quad (12)$$

Итак, для $u_0 < 1$ вектор-функция $c_1(u_0, v, w) = p(\frac{w}{1-u_0})$ удовлетворяет условиям (11). Для случая $u_0 = 1$ положим $c_1(1, 0, 0) = g_1(1)$. Имеем

$$c_1(u, v, w) = \begin{cases} H_1(\frac{w}{1-u})g_2(1-u) + (1-u)H_2(\frac{w}{1-u})h_2(1-u) + \\ \quad + (1-u)H_3(\frac{w}{1-u})f_1(u) + H_4(\frac{w}{1-u})g_1(u), & \text{при } u < 1, \\ g_1(1), & \text{при } u = 1. \end{cases} \quad (13)$$

Дифференцируя первое и третье тождество в (11) и используя лемму получим, что $c_1(u, v, w)$ удовлетворяет и остальным условиям на сторонах $v = 0$ и $w = 0$:

$$\begin{aligned} D_2c_1(u, 0, 1-u) &= g'_1(u), & D_3c_1(u, 0, 1-u) &= h_1(u), \\ D_3c_1(1-v, v, 0) &= g'_2(v), & D_2c_1(1-v, v, 0) &= f_2(v). \end{aligned} \quad (14)$$

ПРЕДЛОЖЕНИЕ 1. Если для вектор-функций g_i, f_i, h_i выполнены условия (7), (8) и (9), то построенная по формуле (13) вектор-функция c_1 , а также вектор-функции D_1c_1, D_2c_1 и D_3c_1 будут непрерывны на Δ .

Доказательство. Заметим, что если $(u, v, w) \in \Delta$ и $u < 1$, то

$$\frac{w}{1-u} = \frac{w}{v+w} \in [0, 1].$$

Поэтому функции $H_i(\frac{w}{1-u})$ и $H'_i(\frac{w}{1-u})$ ограничены.

Кроме того, мы будем пользоваться тождествами

$$\begin{aligned} H_1(t) + H_4(t) &\equiv 1, \\ H_2(t) + H_3(t) &\equiv H_1(t) + t - 1, \\ H'_2(t) + H'_3(t) &\equiv H'_1(t) + 1, \end{aligned}$$

вытекающими из определений полиномов Эрмита (12).

Ясно, что непрерывность требуется проверить только в точке $(1, 0, 0)$. Для вектор-функции $c_1(u, v, w)$ имеем

$$\begin{aligned} \lim_{(u,v,w) \rightarrow (1,0,0)} c_1(u, v, w) &= \lim_{(u,v,w) \rightarrow (1,0,0)} H_1(\frac{w}{1-u})g_2(1-u) + \left(1 - H_1(\frac{w}{1-u})\right)g_1(u) + \\ &\quad + \lim_{(u,v,w) \rightarrow (1,0,0)} (1-u) \left(H_2(\frac{w}{1-u})h_2(1-u) + H_3(\frac{w}{1-u})f_1(u) \right) = \\ &= g_1(1) + \lim_{u \rightarrow 1} H_1(\frac{w}{1-u}) (g_2(1-u) - g_1(u)) + \\ &\quad + \lim_{u \rightarrow 1} (1-u) \left(H_2(\frac{w}{1-u})h_2(1-u) + H_3(\frac{w}{1-u})f_1(u) \right). \end{aligned}$$

По условию согласования (7)

$$\lim_{u \rightarrow 1} g_2(1-u) - g_1(u) = g_2(0) - g_1(1) = 0.$$

Значит, оба оставшихся предела равны нулю как пределы произведений ограниченных функций на функции, стремящиеся к нулю. Следовательно,

$$\lim_{(u,v,w) \rightarrow (1,0,0)} c_1(u, v, w) = g_1(1) = c_1(1, 0, 0).$$

Проверим непрерывность вектор-функции $D_1 c_1(u, v, w)$ в точке $(1, 0, 0)$:

$$\begin{aligned} \lim_{(u,v,w) \rightarrow (1,0,0)} D_1 c_1(u, v, w) &= \lim_{(u,v,w) \rightarrow (1,0,0)} \frac{\partial c_1}{\partial w}(u, v, w) = \\ &= \lim_{(u,v,w) \rightarrow (1,0,0)} \frac{1}{1-u} H'_1\left(\frac{w}{1-u}\right) g_2(1-u) + H'_2\left(\frac{w}{1-u}\right) h_2(1-u) + \\ &\quad + H'_3\left(\frac{w}{1-u}\right) f_1(u) + \frac{1}{1-u} H'_4\left(\frac{w}{1-u}\right) g_1(u) = \\ &= \lim_{(u,v,w) \rightarrow (1,0,0)} \frac{1}{1-u} H'_1\left(\frac{w}{1-u}\right) g_2(1-u) + H'_2\left(\frac{w}{1-u}\right) h_2(0) + \\ &\quad + H'_3\left(\frac{w}{1-u}\right) f_1(1) - \frac{1}{1-u} H'_1\left(\frac{w}{1-u}\right) g_1(u) + \\ &\quad + \lim_{(u,v,w) \rightarrow (1,0,0)} H'_2\left(\frac{w}{1-u}\right) (h_2(1-u) - h_2(0)) + H'_3\left(\frac{w}{1-u}\right) (f_1(u) - f_1(1)). \end{aligned}$$

Функции $H'_2\left(\frac{w}{1-u}\right)$ и $H'_3\left(\frac{w}{1-u}\right)$ ограничены, поэтому второй предел в последнем выражении равен нулю. Из условий согласования (8) и (9) следует, что

$$f_1(1) = -g'_1(1) - h_1(1) = -f_2(0) - g'_2(0) = h_2(0).$$

Поэтому

$$\begin{aligned} \lim_{(u,v,w) \rightarrow (1,0,0)} D_1 c_1(u, v, w) &= \lim_{(u,v,w) \rightarrow (1,0,0)} H'_1\left(\frac{w}{1-u}\right) \left[\frac{g_2(1-u) - g_1(u)}{1-u} \right] + \\ &+ h_2(0) \left[H'_2\left(\frac{w}{1-u}\right) + H'_3\left(\frac{w}{1-u}\right) \right] = h_2(0) + \lim_{(u,v,w) \rightarrow (1,0,0)} H'_1\left(\frac{w}{1-u}\right) \left[\frac{g_2(1-u) - g_1(u)}{1-u} + h_2(0) \right]. \end{aligned}$$

По правилу Лопиталя получаем, что

$$\lim_{u \rightarrow 1} \frac{g_2(1-u) - g_1(u)}{1-u} = g'_1(1) + g'_2(0) = f_2(0) + g'_2(0) = -h_2(0),$$

Следовательно, оставшийся предел равен нулю. Тогда

$$\lim_{(u,v,w) \rightarrow (1,0,0)} D_1 c_1(u, v, w) = h_2(0).$$

А по определению (1)

$$D_1 c_1(1, 0, 0) = -D_2 c_1(1, 0, 0) - D_3 c_1(1, 0, 0) = -f_2(1) - g'_1(1) = h_2(0),$$

то есть вектор-функция $D_1 c_1$ непрерывна в точке $(1, 0, 0)$.

Проверим непрерывность $D_3c_1(u, v, w)$ в точке $(1, 0, 0)$. Имеем

$$\begin{aligned} -\lim_{(u,v,w) \rightarrow (1,0,0)} D_3c_1(u, v, w) &= \lim_{(u,v,w) \rightarrow (1,0,0)} \frac{\partial c_1}{\partial u}(u, v, w) = \\ &= \lim_{(u,v,w) \rightarrow (1,0,0)} \frac{w}{(1-u)^2} H'_1\left(\frac{w}{1-u}\right) g_2(1-u) - H_1\left(\frac{w}{1-u}\right) g'_2(1-u) + \\ &\quad + \left[-H_2\left(\frac{w}{1-u}\right) + \frac{w}{1-u} H'_2\left(\frac{w}{1-u}\right) \right] h_2(1-u) - (1-u) H_2\left(\frac{w}{1-u}\right) h'_2(1-u) + \\ &\quad + \left[-H_3\left(\frac{w}{1-u}\right) + \frac{w}{1-u} H'_3\left(\frac{w}{1-u}\right) \right] f_1(u) + (1-u) H_3\left(\frac{w}{1-u}\right) f'_1(u) + \\ &\quad + \frac{w}{(1-u)^2} H'_4\left(\frac{w}{1-u}\right) g_1(u) + H_4\left(\frac{w}{1-u}\right) g'_1(u). \end{aligned}$$

Как и ранее, можно заменить $h_2(1-u)$ и $f_1(u)$ на их общее предельное значение $f_1(1)$. Получим

$$\begin{aligned} -\lim_{(u,v,w) \rightarrow (1,0,0)} D_3c_1(u, v, w) &= \lim_{(u,v,w) \rightarrow (1,0,0)} \frac{w}{(1-u)^2} H'_1\left(\frac{w}{1-u}\right) (g_2(1-u) - g_1(u)) - \\ &\quad - H_1\left(\frac{w}{1-u}\right) (g'_1(u) + g'_2(1-u)) + g'_1(u) - f_1(1) \left(H_2\left(\frac{w}{1-u}\right) + H_3\left(\frac{w}{1-u}\right) \right) + \\ &\quad + \frac{w}{1-u} \left(H'_2\left(\frac{w}{1-u}\right) + H'_3\left(\frac{w}{1-u}\right) \right) f_1(1) = f_1(1) + g'_1(u) + \\ &\quad + \lim_{(u,v,w) \rightarrow (1,0,0)} \frac{w}{1-u} H'_1\left(\frac{w}{1-u}\right) \left[\frac{g_2(1-u) - g_1(u)}{1-u} + f_1(1) \right] - \\ &\quad - \lim_{(u,v,w) \rightarrow (1,0,0)} H_1\left(\frac{w}{1-u}\right) (g'_1(u) + g'_2(1-u) + f_1(1)). \end{aligned}$$

Так как

$$\lim_{u \rightarrow 1} \frac{g_2(1-u) - g_1(u)}{1-u} = -h_2(0) = -f_1(1)$$

и

$$\lim_{u \rightarrow 1} g'_1(u) + g'_2(1-u) = g'_1(1) + g'_2(0) = g'_1(1) + h_1(1) = -f_1(1),$$

то

$$-\lim_{(u,v,w) \rightarrow (1,0,0)} D_3c_1(u, v, w) = f_1(1) + g'_1(1) = -h_1(1) = -D_3c_1(1, 0, 0).$$

Итак, вектор-функции c_1 , D_1c_1 и D_3c_1 непрерывны на Δ . Из леммы следует, что вектор-функция D_2c_1 также непрерывна на Δ . \square

Определим вектор-функции $c_2(u, v, w)$ и $c_3(u, v, w)$ аналогично c_1 :

$$c_2(u, v, w) = \begin{cases} H_1\left(\frac{u}{1-v}\right) g_3(1-v) + (1-v) H_2\left(\frac{u}{1-v}\right) h_3(1-v) + \\ \quad + (1-v) H_3\left(\frac{u}{1-v}\right) f_2(v) + H_4\left(\frac{u}{1-v}\right) g_2(v) & \text{при } v < 1, \\ g_2(1), & \text{при } v = 1; \end{cases}$$

$$c_3(u, v, w) = \begin{cases} H_1\left(\frac{v}{1-w}\right)g_1(1-w) + (1-w)H_2\left(\frac{v}{1-w}\right)h_1(1-w) + \\ \quad + (1-w)H_3\left(\frac{v}{1-w}\right)f_3(w) + H_4\left(\frac{v}{1-w}\right)g_3(w) & \text{при } w < 1, \\ g_3(1), & \text{при } w = 1. \end{cases}$$

Вектор-функция $c_2(u, v, w)$ удовлетворяет граничным условиям на сторонах $u = 0$ и $w = 0$, а $c_3(u, v, w)$ — на сторонах $u = 0$ и $v = 0$.

4°. Положим

$$c(u, v, w) = \alpha(u, v, w)c_1(u, v, w) + \beta(u, v, w)c_2(u, v, w) + \gamma(u, v, w)c_3(u, v, w), \quad (15)$$

где $\alpha, \beta, \gamma: \Delta \rightarrow \mathbb{R}^3$ — некоторые функции, удовлетворяющие соотношениям

$$\begin{aligned} \alpha(0, 1-w, w) &\equiv 0, & D_i\alpha(0, 1-w, w) &\equiv 0, \\ \beta(u, 0, 1-u) &\equiv 0, & D_i\beta(u, 0, 1-u) &\equiv 0, \\ \gamma(1-v, v, 0) &\equiv 0, & D_i\gamma(1-v, v, 0) &\equiv 0, \\ (\alpha + \beta + \gamma)|_{\partial\Delta} &\equiv 1, & D_i(\alpha + \beta + \gamma)|_{\partial\Delta} &\equiv 0. \end{aligned} \quad (16)$$

Поверхность, задаваемая вектор-функцией $c(u, v, w)$, называется *поверхностью Кунса на треугольнике с граничными условиями первого порядка*.

ПРЕДЛОЖЕНИЕ 2. Если выполнены условия (16), то вектор-функция $c(u, v, w)$, определяемая формулой (15), удовлетворяет условиям (3) и (4).

Доказательство. Имеем

$$\begin{aligned} c(u, 0, 1-u) &= \alpha(u, 0, 1-u)g_1(u) + \gamma(u, 0, 1-u)g_1(u) = \\ &= (1 - \beta(u, 0, 1-u))g_1(u) = g_1(u), \\ c(1-v, v, 0) &= \alpha(1-v, v, 0)g_2(v) + \beta(1-v, v, 0)g_2(v) = \\ &= (1 - \gamma(1-v, v, 0))g_2(v) = g_2(v), \\ c(0, 1-w, w) &= \beta(0, 1-w, w)g_3(w) + \gamma(0, 1-w, w)g_3(w) = \\ &= (1 - \alpha(0, 1-w, w))g_3(w) = g_3(w). \end{aligned}$$

Для функций $\alpha, \beta, \gamma, c_1, c_2$ и c_3 справедливо представление операторов D_i в форме (2). Поэтому

$$\begin{aligned} D_1(\alpha c_1) &= \frac{\partial}{\partial w}(\alpha c_1) - \frac{\partial}{\partial v}(\alpha c_1) = \frac{\partial \alpha}{\partial w} c_1 + \alpha \frac{\partial c_1}{\partial w} - \frac{\partial \alpha}{\partial v} c_1 - \alpha \frac{\partial c_1}{\partial v} = \\ &= (D_1\alpha)c_1 + (D_1c_1)\alpha. \end{aligned}$$

Аналогично

$$D_1(\beta c_2) = (D_1\beta)c_2 + (D_1c_2)\beta, \quad D_1(\gamma c_3) = (D_1\gamma)c_3 + (D_1c_3)\gamma.$$

Проверим первое из условий (4):

$$\begin{aligned} D_1c(u, 0, 1-u) &= D_1\alpha(u, 0, 1-u)c_1(u, 0, 1-u) + \\ &+ \alpha(u, 0, 1-u)D_1c_1(u, 0, 1-u) + D_1\gamma(u, 0, 1-u)c_3(u, 0, 1-u) + \\ &+ \gamma(u, 0, 1-u)D_1c_3(u, 0, 1-u) = D_1\alpha(u, 0, 1-u)g_1(u) + \\ &+ D_1\gamma(u, 0, 1-u)g_1(u) + \alpha(u, 0, 1-u)f_1(u) + \gamma(u, 0, 1-u)f_1(u) = \\ &= (-D_1\beta(u, 0, 1-u))g_1(u) + (1-\beta(u, 0, 1-u))f_1(u) = f_1(u). \end{aligned}$$

Оставшиеся два условия из (4) проверяются аналогично. \square

Осталось подобрать функции α , β и γ , удовлетворяющие условиям (16). Будем искать их в виде многочленов от переменных u , v , w .

Положим $\varphi(u, v) = \alpha(u, v, 1-u-v)$. Тогда $\varphi(u, v)$ — многочлен от u и v , и справедливы равенства

$$\varphi(0, v) = \alpha(0, v, 1-v) = 0, \quad \varphi_u(0, v) = D_2\alpha(0, v, 1-v) = 0.$$

Значит, $\varphi(u, v) = u^2\tilde{\varphi}(u, v)$, где $\tilde{\varphi}(u, v)$ — некоторый многочлен. Следовательно,

$$\alpha(u, v, w) = u^2\tilde{\varphi}(u, v) = u^2\tilde{\varphi}(1-v-w, v).$$

Обозначим $\tilde{\alpha}(v, w) = \tilde{\varphi}(1-v-w, v)$.

Таким образом, $\alpha(u, v, w) = u^2\tilde{\alpha}(v, w)$, где $\tilde{\alpha}(v, w)$ — некоторый многочлен. В этом случае условия $\alpha(0, 1-v, v) \equiv 0$ и $D_i\alpha(0, 1-v, v) \equiv 0$ будут выполнены. Аналогично $\beta(u, v, w) = v^2\tilde{\beta}(u, w)$, $\gamma(u, v, w) = w^2\tilde{\gamma}(u, v)$. Положим

$$\tau(u, v, w) = \alpha(u, v, w) + \beta(u, v, w) + \gamma(u, v, w).$$

Осталось подобрать $\tilde{\alpha}$, $\tilde{\beta}$ и $\tilde{\gamma}$ таким образом, чтобы выполнялись условия $\tau|_{\partial\Delta} \equiv 1$, $D_i\tau|_{\partial\Delta} \equiv 0$.

Имеем $1 = \tau(1, 0, 0) = \tilde{\alpha}(0, 0)$. Далее,

$$0 = D_3\tau(1, 0, 0) = D_3\alpha(1, 0, 0) = \tilde{\alpha}_v(0, 0) - 2\tilde{\alpha}(0, 0),$$

поэтому $\tilde{\alpha}_v(0, 0) = 2$. Кроме того,

$$D_2\tau(1-v, v, 0) = 2(1-v)\tilde{\alpha}(v, 0) - (1-v)^2\tilde{\alpha}_w(v, 0) + v^2(\tilde{\beta}_u(1-v, 0) - \tilde{\beta}_w(1-v, 0)).$$

При $v = 0$ имеем

$$0 = D_2\tau(1, 0, 0) = 2\tilde{\alpha}(0, 0) - \tilde{\alpha}_w(0, 0).$$

Следовательно, $\tilde{\alpha}_w(0, 0) = 2$. А так как $D_2\tau(1-v, v, 0) \equiv 0$, то

$$0 = (D_2\tau(1-v, v, 0))'(0) = -2\tilde{\alpha}(0, 0) + 2\tilde{\alpha}_v(0, 0) - \tilde{\alpha}_{vw}(0, 0) + 2\tilde{\alpha}_w(0, 0).$$

Таким образом, $\tilde{\alpha}_{vw}(0, 0) = 6$.

Итак, свободный член многочлена $\tilde{\alpha}(v, w)$ равен 1, коэффициенты при v и w равны 2, коэффициент при vw равен 6. Предположим, что все остальные коэффициенты в $\tilde{\alpha}(v, w)$ нулевые. Тогда $\tilde{\alpha}(v, w) = 1 + 2v + 2w + 6vw$. Симметричным образом определим $\tilde{\beta}(u, w)$ и $\tilde{\gamma}(u, v)$. Имеем

$$\begin{aligned}\alpha(u, v, w) &= u^2(1 + 2v + 2w + 6vw), \\ \beta(u, v, w) &= v^2(1 + 2u + 2w + 6uw), \\ \gamma(u, v, w) &= w^2(1 + 2u + 2v + 6uv).\end{aligned}\tag{17}$$

Покажем, что $\alpha(u, v, w) + \beta(u, v, w) + \gamma(u, v, w) \equiv 1$ на Δ . Этого будет достаточно для выполнения условий (16). Для $(u, v, w) \in \Delta$ имеем

$$\begin{aligned}1 - (u^2 + v^2 + w^2) &= (u + v + w)^2 - (u^2 + v^2 + w^2) = 2(uv + vw + wu) = \\ &= 2(u + v + w)(uv + vw + wu) = 2(u^2v + u^2w + v^2u + v^2w + w^2u + w^2v) + \\ &\quad + 6uvw = 2u^2(v + w) + 2v^2(u + w) + 2w^2(u + v) + 6uvw(u + v + w) = \\ &= \alpha(u, v, w) + \beta(u, v, w) + \gamma(u, v, w) - (u^2 + v^2 + w^2),\end{aligned}$$

что и требовалось.

Итак, функции α , β и γ , определяемые равенствами (17), удовлетворяют условиям (16). Значит, их можно использовать для построения поверхности Кунса по формуле (15).

ПРИМЕР 1. Пусть граничные кривые представляют собой отрезки, соединяющие точки $(1, 0, 0)$, $(0, 1, 0)$ и $(0, 0, 1)$:

$$g_1(u) = (1 - u, 0, u), \quad g_2(v) = (0, v, 1 - v), \quad g_3(w) = (w, 1 - w, 0).$$

Условий согласования (8) и (10) можно записать следующим образом:

$$\begin{aligned}f_1(0) &= f_1(1) = (1, -1, 0), \\ f_2(0) &= f_2(1) = (-1, 0, 1), \\ f_3(0) &= f_3(1) = (0, 1, -1).\end{aligned}$$

Положим

$$\begin{aligned}f_1(u) &= (1 + 5u(1 - u), -1 + 5u(1 - u), 5u(1 - u)), \\ f_2(v) &= (-1 + 5v(1 - v), 5v(1 - v), 1 + 5v(1 - v)), \\ f_3(w) &= (5w(1 - w), 1 + 5w(1 - w), -1 + 5w(1 - w)).\end{aligned}$$

Заданные вектор-функции удовлетворяют всем условиям согласования. Построенная по ним поверхность Кунса изображена на рис. 1.

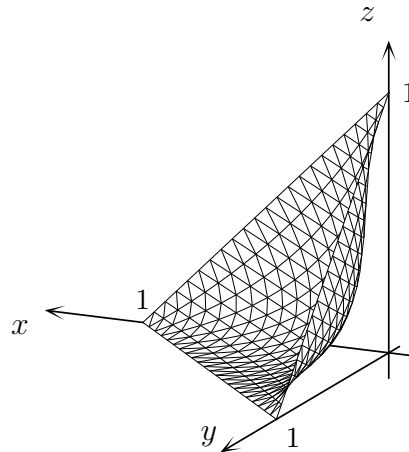


Рис. 1. Поверхность Кунса из примера 1

ПРИМЕР 2. Пусть граничные кривые представляют собой три дуги окружностей (см. рис. 2). Они задаются функциями

$$\begin{aligned} g_1(u) &= \left(1 + \sin \frac{3\pi u}{2}, 0, 1 - \cos \frac{3\pi u}{2} \right), \\ g_2(v) &= \left(0, 1 - \cos \frac{3\pi v}{2}, 1 + \sin \frac{3\pi v}{2} \right), \\ g_3(w) &= \left(1 - \cos \frac{3\pi w}{2}, 1 + \sin \frac{3\pi w}{2}, 0 \right). \end{aligned}$$

Условия согласования (8) и (10) эквивалентны равенствам

$$\begin{aligned} f_1(0) &= \left(-\frac{3\pi}{2}, 0, 0 \right), & f_1(1) &= 0, \\ f_2(0) &= \left(0, 0, -\frac{3\pi}{2} \right), & f_2(1) &= 0, \\ f_3(0) &= \left(0, -\frac{3\pi}{2}, 0 \right), & f_3(1) &= 0. \end{aligned}$$

Положим

$$\begin{aligned} f_1(u) &= \left(-\frac{3\pi}{2} \cos \frac{3\pi u}{2}, \sin \pi u, 0 \right), \\ f_2(v) &= \left(\sin \pi v, 0, -\frac{3\pi}{2} \cos \frac{3\pi v}{2} \right), \\ f_3(w) &= \left(0, -\frac{3\pi}{2} \cos \frac{3\pi w}{2}, \sin \pi w \right). \end{aligned}$$

Поверхность Кунса, построенная по этим вектор-функциям, изображена на рис. 3.

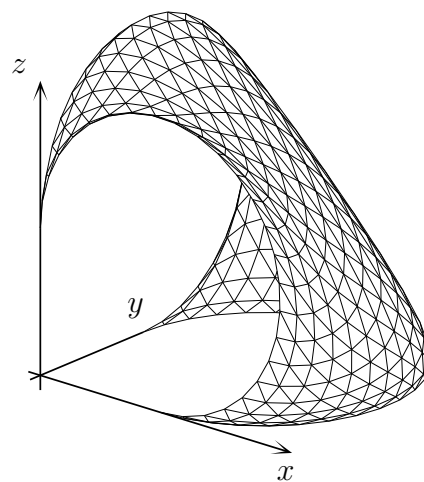
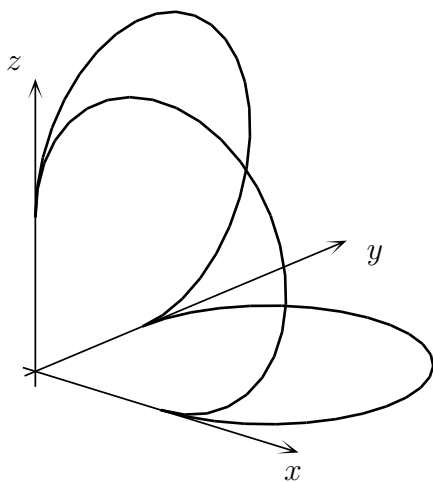


Рис. 2. Граничные кривые из примера 2 Рис. 3. Поверхность Кунса из примера 2

ЛИТЕРАТУРА

1. J. Gregory. *Symmetric smooth interpolation on triangles*. Brunel University, 1973.
2. G. Farin. *Curves and surfaces for CAGD*. 5th ed. Academic Press, 2002.

НЕСКОЛЬКО ЗАМЕЧАНИЙ О ЖЁСТКИХ ФРЕЙМАХ

В. Н. Малозёмов

13 декабря 2008 г.

В докладе представлено содержание обзорной статьи [1].

1°. Пусть $\{\varphi_1, \dots, \varphi_m\}$ — фрейм в \mathbb{R}^n . Обозначим через Φ матрицу со столбцами $\varphi_1, \dots, \varphi_m$, а через S — матрицу фрейма, $S = \Phi\Phi^T$. По определению фрейма симметричная матрица S положительно определена. У S существует обратная матрица S^{-1} , которая также симметрична и положительно определена.

Введём векторы

$$\tilde{\varphi}_k = S^{-1}\varphi_k, \quad k \in 1:m.$$

Матрица $\tilde{\Phi}$ со столбцами $\tilde{\varphi}_1, \dots, \tilde{\varphi}_m$ обладает следующим свойством

$$\tilde{\Phi}\Phi^T = I_n, \tag{1}$$

где I_n — единичная матрица порядка n . Поскольку

$$\tilde{S} := \tilde{\Phi}\tilde{\Phi}^T = S^{-1}\Phi\Phi^TS^{-1} = S^{-1},$$

то система векторов $\{\tilde{\varphi}_1, \dots, \tilde{\varphi}_m\}$ является фреймом. Он называется *каноническим двойственным фреймом*. Умножив (1) на произвольный вектор $x \in \mathbb{R}^n$, придём к разложению

$$x = \sum_{k=1}^m \langle x, \varphi_k \rangle \tilde{\varphi}_k.$$

Это разложение используется при передаче информации. По каналам связи вместо сигнала x передаются коэффициенты $\langle x, \varphi_k \rangle$, $k \in 1:m$. За счёт возникающих погрешностей на приёмник поступает сигнал

$$\hat{x} = \sum_{k=1}^m [\langle x, \varphi_k \rangle + \eta_k] \tilde{\varphi}_k.$$

Будем считать, что η_1, \dots, η_m — независимые случайные величины со средним значением, равным нулю, и дисперсией σ^2 . Ошибка

$$x - \hat{x} = - \sum_{k=1}^m \eta_k \tilde{\varphi}_k$$

обычно измеряется с помощью MSE (mean square error) по формуле

$$\begin{aligned} \text{MSE} &= \frac{1}{n} \mathbf{E} \left\| \sum_{k=1}^m \eta_k \tilde{\varphi}_k \right\|^2 = \frac{1}{n} \mathbf{E} \left[\sum_{k=1}^m \sum_{s=1}^m \eta_k \eta_s \langle \tilde{\varphi}_k, \tilde{\varphi}_s \rangle \right] = \\ &= \frac{\sigma^2}{n} \sum_{k=1}^m \|\tilde{\varphi}_k\|^2. \end{aligned} \quad (2)$$

Обозначим через $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_n > 0$ собственные числа матрицы фрейма S . Тогда собственными числами матрицы $\tilde{S} = S^{-1}$ канонического двойственного фрейма будут $\lambda_1^{-1} \leq \lambda_2^{-1} \leq \dots \leq \lambda_n^{-1}$. След матрицы S связан с её собственными числами равенством

$$\text{tr}(S) = \sum_{i=1}^n \lambda_i.$$

Вместе с тем,

$$\text{tr}(S) = \text{tr}(\Phi \Phi^T) = \text{tr}(\Phi^T \Phi) = \sum_{k=1}^m \|\varphi_k\|^2.$$

Значит,

$$\sum_{k=1}^m \|\varphi_k\|^2 = \sum_{i=1}^n \lambda_i. \quad (3)$$

По тем же причинам

$$\sum_{k=1}^m \|\tilde{\varphi}_k\|^2 = \sum_{i=1}^n \frac{1}{\lambda_i}.$$

С помощью последнего равенства формула (2) для MSE приводится к виду

$$\text{MSE} = \frac{\sigma^2}{n} \sum_{i=1}^n \frac{1}{\lambda_i}.$$

Поставим задачу: среди всех равномерных фреймов $\{\varphi_1, \dots, \varphi_m\}$, у которых $\|\varphi_k\| = a$, $k \in 1 : m$, найти фрейм с наименьшим MSE. С учётом (3)

данная задача формализуется так:

$$\begin{aligned} \text{MSE} &:= \frac{\sigma^2}{n} \sum_{i=1}^n \frac{1}{\lambda_i} \rightarrow \min, \\ \sum_{i=1}^n \lambda_i &= m a^2; \quad \lambda_i > 0, \quad i \in 1:n. \end{aligned} \quad (4)$$

ПРЕДЛОЖЕНИЕ 1. Задача (4) имеет единственное решение

$$\lambda_1^* = \lambda_2^* = \dots = \lambda_n^* = \frac{m}{n} a^2. \quad (5)$$

При этом для минимальной погрешности MSE^* справедлива формула

$$\text{MSE}^* = \frac{n \sigma^2}{m a^2}.$$

Доказательство. Воспользуемся неравенством между средним гармоническим и средним арифметическим положительных чисел $\lambda_1, \dots, \lambda_n$:

$$\frac{n}{\lambda_1^{-1} + \dots + \lambda_n^{-1}} \leq \frac{\lambda_1 + \dots + \lambda_n}{n}.$$

Оно обращается в равенство только тогда, когда $\lambda_1 = \dots = \lambda_n$.

В силу ограничений задачи (4)

$$\sum_{i=1}^n \frac{1}{\lambda_i} \geq \frac{n^2}{m a^2},$$

причём неравенство обращается в равенство только тогда, когда выполняется условие (5). Отсюда очевидным образом следует требуемое. \square

Согласно предложению 1 наилучшим для передачи информации с точки зрения минимизации MSE будет жёсткий фрейм с матрицей фрейма $S = \lambda^* I_n$, где $\lambda^* = \frac{m}{n} a^2$. При $a = \sqrt{\frac{n}{m}}$ получаем равномерный фрейм Парсеваля ($S = I_n$). В этом случае $\text{MSE}^* = \sigma^2$.

2°. Равномерные фреймы Парсеваля существуют. Действительно, возьмём жёсткий фрейм $\{\varphi_1, \dots, \varphi_m\}$ с единичными векторами φ_k . Он характеризуется тем, что любой вектор $x \in \mathbb{R}^n$ допускает представление

$$x = \frac{n}{m} \sum_{k=1}^m \langle x, \varphi_k \rangle \varphi_k.$$

Положим

$$\widehat{\varphi}_k = \sqrt{\frac{n}{m}} \varphi_k, \quad k \in 1 : m.$$

Тогда

$$x = \sum_{k=1}^m \langle x, \widehat{\varphi}_k \rangle \widehat{\varphi}_k.$$

Это равенство характеризует систему векторов $\{\widehat{\varphi}_1, \dots, \widehat{\varphi}_m\}$ как фрейм Парсеваля. Он равномерный, поскольку $\|\widehat{\varphi}_k\| = \sqrt{\frac{n}{m}}$ при всех $k \in 1 : m$.

В частности, при любом $m \geq n$ равномерный фрейм Парсеваля образует (при соответствующей нормировке) вещественный гармонический фрейм (см., например, [2]).

3°. Между фреймами в \mathbb{R}^n и \mathbb{C}^n имеется связь.

ПРЕДЛОЖЕНИЕ 2. *Справедливы утверждения:*

- (α) *фрейм в \mathbb{R}^n с границами A, B является фреймом в \mathbb{C}^n с теми же границами;*
- (β) *если $\{\varphi_k\}_{k=1}^m$ — фрейм в \mathbb{C}^n с границами A, B , то $2m$ векторов $\{\{\operatorname{Re} \varphi_k\}_{k=1}^m, \{\operatorname{Im} \varphi_k\}_{k=1}^m\}$ образуют фрейм в \mathbb{R}^n с теми же границами.*

Доказательство. Пусть $\{\varphi_k\}_{k=1}^m$ — фрейм в \mathbb{R}^n с границами A, B . Это значит, что при любом $x \in \mathbb{R}^n$ выполняются неравенства

$$A \|x\|^2 \leq \sum_{k=1}^m |\langle x, \varphi_k \rangle|^2 \leq B \|x\|^2. \quad (6)$$

Возьмём вектор $x = a + i b$, где $a, b \in \mathbb{R}^n$. Тогда

$$\begin{aligned} \|x\|^2 &= \sum_{j=1}^n |x(j)|^2 = \sum_{j=1}^n \left[|a(j)|^2 + |b(j)|^2 \right] = \|a\|^2 + \|b\|^2, \\ |\langle x, \varphi_k \rangle|^2 &= |\langle a, \varphi_k \rangle + i \langle b, \varphi_k \rangle|^2 = |\langle a, \varphi_k \rangle|^2 + |\langle b, \varphi_k \rangle|^2. \end{aligned}$$

Согласно (6) имеем

$$\begin{aligned} A \|a\|^2 &\leq \sum_{k=1}^m |\langle a, \varphi_k \rangle|^2 \leq B \|a\|^2, \\ A \|b\|^2 &\leq \sum_{k=1}^m |\langle b, \varphi_k \rangle|^2 \leq B \|b\|^2. \end{aligned}$$

Сложив, придём к неравенствам

$$A \|x\|^2 \leq \sum_{k=1}^m |\langle x, \varphi_k \rangle|^2 \leq B \|x\|^2.$$

Значит, $\{\varphi_k\}_{k=1}^m$ — фрейм \mathbb{C}^n с границами A, B .

Наоборот, пусть $\{\varphi_k\}_{k=1}^m$ — фрейм в \mathbb{C}^n с границами A, B . Принимая во внимание, что при $x \in \mathbb{R}^n$

$$\begin{aligned} \langle x, \varphi_k \rangle &= \sum_{j=1}^n x(j) [\operatorname{Re} \varphi_k(j) - i \operatorname{Im} \varphi_k(j)] = \\ &= \langle x, \operatorname{Re} \varphi_k \rangle - i \langle x, \operatorname{Im} \varphi_k \rangle, \\ |\langle x, \varphi_k \rangle|^2 &= |\langle x, \operatorname{Re} \varphi_k \rangle|^2 + |\langle x, \operatorname{Im} \varphi_k \rangle|^2, \end{aligned}$$

по определению фрейма в \mathbb{C}^n получаем

$$A \|x\|^2 \leq \sum_{k=1}^m [|\langle x, \operatorname{Re} \varphi_k \rangle|^2 + |\langle x, \operatorname{Im} \varphi_k \rangle|^2] \leq B \|x\|^2.$$

Это соответствует утверждению (β) . □

4°. Приведём нетривиальный пример жёсткого фрейма в \mathbb{R}^3 , состоящего из векторов единичной длины.

ПРИМЕР. Пусть

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & \sqrt{\frac{5}{6}} & -\sqrt{\frac{5}{6}} \\ \sqrt{\frac{1}{3}} & -\sqrt{\frac{1}{3}} & 1 & 0 & 0 \\ \sqrt{\frac{2}{3}} & \sqrt{\frac{2}{3}} & 0 & \sqrt{\frac{1}{6}} & \sqrt{\frac{1}{6}} \end{bmatrix}.$$

Обозначим через $\varphi_1, \dots, \varphi_5$ столбцы матрицы Φ . Тогда

$$\begin{aligned} \sum_{k=1}^m |\langle x, \varphi_k \rangle|^2 &= \left(x_2 \sqrt{\frac{1}{3}} + x_3 \sqrt{\frac{2}{3}}\right)^2 + \left(-x_2 \sqrt{\frac{1}{3}} + x_3 \sqrt{\frac{2}{3}}\right)^2 + x_2^2 + \\ &+ \left(x_1 \sqrt{\frac{5}{6}} + x_3 \sqrt{\frac{1}{6}}\right)^2 + \left(-x_1 \sqrt{\frac{5}{6}} + x_3 \sqrt{\frac{1}{6}}\right)^2 = \frac{5}{3} (x_1^2 + x_2^2 + x_3^2) = \frac{5}{3} \|x\|^2. \end{aligned}$$

Значит, единичные векторы $\varphi_1, \dots, \varphi_5$ образуют жёсткий фрейм в \mathbb{R}^3 .

5°. Можно дать полное описание жёстких фреймов в \mathbb{R}^2 , состоящих из векторов единичной длины.

ПРЕДЛОЖЕНИЕ 3. Система единичных векторов

$$\varphi_k = (\cos \alpha_k, \sin \alpha_k), \quad k \in 1 : m,$$

образует жёсткий фрейм в \mathbb{R}^2 тогда и только тогда, когда

$$\sum_{k=1}^m e^{2i\alpha_k} = 0. \quad (7)$$

Доказательство. В данном случае

$$\Phi = \begin{bmatrix} \cos \alpha_1 & \dots & \cos \alpha_m \\ \sin \alpha_1 & \dots & \sin \alpha_m \end{bmatrix}.$$

Условие $\Phi \Phi^T = \frac{m}{2} I_2$ принимает вид

$$\sum_{k=1}^m \cos^2 \alpha_k = \frac{m}{2}, \quad \sum_{k=1}^m \sin^2 \alpha_k = \frac{m}{2}, \quad \sum_{k=1}^m \cos \alpha_k \sin \alpha_k = 0. \quad (8)$$

Это эквивалентно двум равенствам

$$\sum_{k=1}^m \cos 2\alpha_k = 0, \quad \sum_{k=1}^m \sin 2\alpha_k = 0. \quad (9)$$

Действительно, импликация (8) \Rightarrow (9) очевидна. Наоборот, из (9) следует, что

$$\sum_{k=1}^m \cos^2 \alpha_k = \sum_{k=1}^m \sin^2 \alpha_k,$$

Учитывая формулу

$$\sum_{k=1}^m \cos^2 \alpha_k = m - \sum_{k=1}^m \sin^2 \alpha_k,$$

приходим к (8).

Остаётся отметить, что (7) представляет собой лишь другую форму записи соотношений (9). \square

6°. Более полный обзор по конечномерным фреймам имеется в статье [3] и книге [4].

ЛИТЕРАТУРА

1. Драбкова Е. С., Новиков С. Я. *Объём фрейма Парсеваля* // Вестник Самарского ун-та. Естественная серия. 2007. № 9/1(59). С. 91–106.
2. Дурягин А. М., Соловьёва Н. А. *Вещественные гармонические фреймы* // Семинар «DHA & CAGD». Избранные доклады. 9 октября 2007 г. (<http://dha.spb.ru/rep07.shtml#1009>).
3. Goyal V. K., Kovačević J., Kelner J. A. *Quantized frame expansions with erasures* // Appl. Comput. Harmonic Anal. 2001. Vol. 10. No. 3. P. 203–233.
4. Christensen O. *An introduction to frames and Riesz bases*. Boston: Birkhäuser, 2002.

Список участников семинара

- Агафонова Ирина Витальевна (кандидат физ.-мат. наук, доцент)
ivagafonova@home.eltel.net
- Григорьев Михаил Игоревич (кандидат физ.-мат. наук)
m_grigoriev@list.ru
- Дурягин Александр Максимович (аспирант)
duriagin@syktsu.ru
- Жёлудев Валерий Александрович (доктор физ.-мат. наук, профессор)
zhel@post.tau.ac.il
- Истомина Марина Николаевна (аспирантка)
istomina@syktsu.ru
- Капелюхин Иван Александрович (студент)
i_kapelyuhin@mail.ru
- Максименко Владимир Валерьевич (аспирант)
хурупр@хурупр.com
- Малозёмов Василий Николаевич (доктор физ.-мат. наук, профессор)
malv@math.spbu.ru
- Машарский Сергей Михайлович (кандидат физ.-мат. наук, доцент)
smash@scientist.com
- Певный Александр Борисович (доктор физ.-мат. наук, профессор)
pevnyi@syktsu.ru
- Просеков Олег Валерьевич (кандидат физ.-мат. наук)
sc2@pisem.net
- Рыбин Сергей Витальевич (кандидат физ.-мат. наук, доцент)
rsvvm2leti@yandex.ru
- Сабаяев Анатолий Николаевич (аспирант)
- Сергеев Александр Николаевич (кандидат физ.-мат. наук, доцент)
aser57@mail.ru
- Соловьёва (Селянинова) Наталья Анатольевна (аспирантка)
vinyo@mail.ru
- Чашников Николай Викторович (аспирант)
nik239@list.ru
- Хорохонов Даниил Александрович (студент)
d.khorokhonov@mail.ru

Предметный указатель

А

Алгоритм Гёрцеля 81
Алгоритм Кастельжо 202, 557
Алгоритм квадратичного решета
268
Ансамбли сигналов 522

Б

Базисные полиномы Бернштейна
53, 492
Банки фильтров 173
Бент-функции 439
Булевы функции 431
-- , автокорреляция 443
-- , нелинейность 433, 437
-- , производная по направлению
440
Быстрое преобразование Фурье 112
--- многомерное 233

Д

Дискретное лифтинговое
преобразование, прямое 67
--- , двойственное 159
Дискретное преобразование Фурье
11, 208
Дискретные периодические
сплайны 371, 529
Дискретные функции
Виленкина-Крестенсона 452
Дискретные функции Уолша 41

И

Избыточность фрейма 337, 484
Интерполяция по полюсам 261, 505

К

Код китайский 37

-- руританский 37
-- самосопряжённый 36
-- смешанный 187
Кодирование индексов
параметрическое 35
Конечные разности 56, 493, 558
Кривые Безье 55, 195, 202
-- замкнутые 328
-- обобщённые 534
-- проективные 281
-- составные 58
Криптография 265, 428
Кroneckerovo умножение матриц
12, 361

Л

Лифтинговая схема, прямая 64
-- , двойственная 156

М

Матрица Фурье 20
Матрица вращений 20
Матрицы перестановок 13
Метод наименьших квадратов 50

Н

Нормализованные *B*-сплайны 371

П

Поверхность Безье 248, 553
-- на треугольнике 321, 345
-- проективная 309
-- составная 558
Поверхность Кунса 248, 295, 364,
412
-- на треугольнике 341, 564
-- обобщённая 468
-- составная 303, 468

Поверхность вращения 352, 364
-- обобщённая 382
Полиномы в форме Бернштейна 53
--- обобщённые 534
--- от двух переменных 492
Преобразование Уолша-Адамара
 1-го рода 435
--- 2-го рода 436
Процедура включения узла 261,
 505

Р

Равноугольные системы векторов
 389
Разделённые разности с кратными
 узлами 241
Рекуррентные соотношения 24, 50,
 54, 77, 160, 191, 202, 213, 225,
 244, 259, 397, 496, 501, 535, 555
Ряды Фурье 48

С

Сигналы 11
-- дельта-коррелированные 523
-- некоррелированные 522
Сингулярное разложение матрицы
 460
Системы Грассмана 423
Системы Мерседес-Бенц 315, 464,
 551
Смешивающие функции 411
Сплайн-интерполяция 65
-- векторная 376
Схема Кленшоу 77, 397

Т

Теорема об отсчётах 141
Теория полярных форм 258
--- полиномов от двух
 переменных 500

Ф

Факторизация Гуда матрицы
 Фурье 30
Факторизация Кули-Тьюки
 матрицы Фурье 20
Факторизация матриц
 перестановок 187
Факторная база 276
Фильтр Баттерворта 153, 173
Фреймовые коэффициенты 334, 406
Фреймовый потенциал 169, 349
Фреймы 166, 578
-- гармонические 339, 406, 484
-- обобщённые 507
-- двойственные 177, 357
Фреймы Грассмана 423
Фреймы Мерседес-Бенц 288
Фреймы Парсеваля 360
Фреймы жёсткие 147, 315, 347, 389,
 466, 575
-- равноугольные 477, 542

Ц

Циклическая матрица 397
Циклическая свёртка 100

Ч

Частично бент-функции 447
Частотный конвертер 91