УДК 519.677 Вестник СПбГУ. Сер. 1, 1999, вып. 1 (№ 1)

В. Н. Малоземов, А. А. Третьяков

СЕКЦИОНИРОВАНИЕ, ОРТОГОНАЛЬНОСТЬ И ПЕРЕСТАНОВКИ*

1°. Пусть n - натуральное число, $N = 2^n$, $N_s = N/2^s$, $\Delta_s = 2^{s-1}$. В евклидовом пространстве $\mathbb{R}^N$ с базисом $e_0, e_1, \dots, e_{N-1}$ введем $n+1$ систему векторов $\{\mu_s(k)\}_{k=0}^{N-1}$, $s = 0, 1, \dots, n$. Сделаем это с помощью рекуррентных соотношений:

$$\mu_0(k) = e_k, \quad k \in 0 : N-1;$$

$$\begin{aligned} \mu_s(2mN_s + l) &= \mu_{s-1}(2mN_s + l) + \mu_{s-1}((2m+1)N_s + l), \\ \mu_s((2m+1)N_s + l) &= \mu_{s-1}(2mN_s + l) - \mu_{s-1}((2m+1)N_s + l), \end{aligned} \tag{1}$$

$$l \in 0 : N_s - 1, \quad m \in 0 : \Delta_s - 1, \quad s \in 1 : n.$$

Прием, использованный при построении системы $\{\mu_s(k)\}$, называется *секционированием* (на s-ом уровне формируются 2^s секций, соответсвующих параметрам $2m$, $2m+1$ при $m \in 0 : \Delta_s - 1$, в каждой из которых содержится N_s векторов $\mu_s(k)$). Такой прием лежит в основе алгоритма Кули-Тьюки для вычисления дискретного преобразования Фурье [1].

В данной заметке показано, что при каждом $s \in 0 : n$ векторы $\{\mu_s(k)\}_{k=0}^{N-1}$ образуют ортогональный базис в $\mathbb{R}^N$. Детально изучена финальная система $\{\mu_n(k)\}_{k=0}^{N-1}$.

2°. Числа i, $j \in 0 : N-1$ запишем в двоичном коде:

$$i = i_{n-1}2^{n-1} + \dots + i_1 2 + i_0, \quad j = j_{n-1}2^{n-1} + \dots + j_1 2 + j_0.$$

Здесь коэффициенты i_k, j_k принимают значения 0 или 1. Положим

$$\{i, j\}_n = \sum_{k=0}^{n-1} i_k j_k.$$

Лемма 1. *При* p, $q \in 0 : 2^{n-1} - 1$ *справедливы равенства*

$$\{2p, 2q\}_n = \{2p+1, 2q\}_n = \{2p, 2q+1\}_n = \{2p+1, 2q+1\}_n - 1 = \{p, q\}_{n-1}.$$

Лемма 2. *При* $i \in 1 : N-1$ *выполняется равенство*

$$\sum_{j=0}^{N-1} (-1)^{\{i,j\}_n} = 0. \tag{2}$$

Лемма 1 тривиальна. Докажем лемму 2.

При $i = N-1$ будет $\{i, j\}_n = \sum_{k=0}^{n-1} j_k$. Обозначим через m_s количество тех $j \in 0 : N-1$, у которых $\sum_{k=0}^{n-1} j_k = s$. Очевидно, что $m_s = C_n^s$. Из равенства $\sum_{s=0}^{n} (-1)^s C_n^s = 0$ следует, что $m_0 + m_2 + \dots = m_1 + m_3 + \dots$. Это гарантирует справедливость (2) при $i = N-1$.

*Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект 96-01-00269)

В общем случае обозначим через l количество ненулевых (равных единице) коэффициентов в двоичном коде числа i. Положим $L = 2^l$. Тогда

$$\sum_{j=0}^{N-1} (-1)^{\{i,j\}_n} = 2^{n-l} \sum_{p=0}^{L-1} (-1)^{\{L-1,p\}_l} = 0.$$

Лемма 2 доказана.

3°. Введем последовательность матриц Адамара [2]:

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; \quad A_{s+1} = \begin{pmatrix} A_s & A_s \\ A_s & -A_s \end{pmatrix}, \; s = 1, 2, ... \tag{3}$$

Будем считать, что индексы строк и столбцов матрицы A_s принимают значения от 0 до $2^s - 1$.

Лемма 3. *Справедлива формула*

$$A_s[i,j] = (-1)^{\{i,j\}_s}, \quad i, j \in 0 : 2^s - 1. \tag{4}$$

Доказательство. При $s = 1$ формула (4) тривиальна. Сделаем индукционный переход от s к $s+1$. Пусть $i = i_s 2^s + p$, $j = j_s 2^s + q$, где $i_s, j_s \in 0 : 1$, $p, q \in 0 : 2^s - 1$. Согласно (3) и (4) получаем

$$A_{s+1}[i,j] = (-1)^{i_s j_s} A_s[p,q] = (-1)^{i_s j_s + \{p,q\}_s} = (-1)^{\{i,j\}_{s+1}}.$$

Лемма доказана.

Из (4) следует, что матрица A_s симметрична. Кроме того, на основании лемм 1 и 3 заключаем, что при $p, q \in 0 : 2^{s-1} - 1$ выполняются равенства

$$A_s[2p, 2q] = A_s[2p+1, 2q] = A_s[2p, 2q+1] = -A_s[2p+1, 2q+1] = A_{s-1}[p,q]. \tag{5}$$

4°. Вернемся к системе векторов $\{\mu_s(k)\}$, определяемой соотношениями (1).

Теорема 1. *Справедливо представление*

$$\mu_s(pN_s + l) = \sum_{q=0}^{2^s-1} A_s[p,q] \mu_0(qN_s + l), \tag{6}$$

где $p \in 0 : 2^s - 1$, $l \in 0 : N_s - 1$, $s \in 1 : n$.

Доказательство. При $s = 1$ согласно (1) имеем

$$\mu_1(l) = \mu_0(l) + \mu_0(N_1 + l),$$

$$\mu_1(N_1 + l) = \mu_0(l) - \mu_0(N_1 + l),$$

$$l \in 0 : N_1 - 1.$$

Это соответствует (6) при $p = 0$ и $p = 1$.

Сделаем индукционный переход от $s - 1$ к s. Рассмотрим два случая.

1) $p = 2m$, $m \in 0 : \Delta_s - 1$. Пользуясь (1), индукционным предположением и (5), при $l \in 0 : N_s - 1$ получаем

$$\mu_s(2mN_s + l) = \mu_{s-1}(mN_{s-1} + l) + \mu_{s-1}(mN_{s-1} + N_s + l) =$$

$$= \sum_{q=0}^{\Delta_s-1} \{A_{s-1}[m,q]\mu_0(qN_{s-1}+l) + A_{s-1}[m,q]\mu_0(qN_{s-1}+N_s+l)\} =$$

$$= \sum_{q=0}^{\Delta_s-1} \{A_s[2m,2q]\mu_0(2qN_s+l) + A_s[2m,2q+1]\mu_0((2q+1)N_s+l)\} =$$

$$= \sum_{k=0}^{2^s-1} A_s[p,k]\mu_0(kN_s+l).$$

2) $p = 2m+1$, $m \in 0 : \Delta_s - 1$. Аналогично предыдущему имеем

$$\mu_s((2m+1)N_s+l) = \mu_{s-1}(mN_{s-1}+l) - \mu_{s-1}(mN_{s-1}+N_s+l) =$$

$$= \sum_{q=0}^{\Delta_s-1} \{A_s[2m+1,2q]\mu_0(2qN_s+l) + A_s[2m+1,2q+1]\mu_0((2q+1)N_s+l)\} =$$

$$= \sum_{k=0}^{2^s-1} A_s[p,k]\mu_0(kN_s+l).$$

Теорема доказана.

Согласно (1) и (4) формулу (6) можно переписать в виде

$$\mu_s(pN_s+l) = \sum_{q=0}^{2^s-1} (-1)^{\{p,q\}_s} e_{qN_s+l}, \tag{7}$$

$$p \in 0 : 2^s - 1, \quad l \in 0 : N_s - 1, \quad s \in 1 : n.$$

При $s = n$ приходим к представлению

$$\mu_n(p) = \sum_{q=0}^{N-1} (-1)^{\{p,q\}_n} e_q, \quad p \in 0 : N-1. \tag{8}$$

Теорема 2. *При каждом $s \in 1 : n$ векторы $\mu_s(0)$, $\mu_s(1)$, ..., $\mu_s(N-1)$ образуют ортогональный базис в $\mathbb{R}^N$, причем $||\mu_s(k)||^2 = 2^s$, $k \in 0 : N-1$.*

Доказательство. Равенство $||\mu_s(k)||^2 = 2^s$ непосредственно следует из (7). Разберемся с ортогональностью.

Векторы $\mu_s(pN_s+l)$ и $\mu_s(p'N_s+l')$ ортогональны при $l \neq l'$, поскольку индексные множества $\{l, l+N_s, ..., l+(2^s-1)N_s\}$ и $\{l', l'+N_s, ..., l'+(2^s-1)N_s\}$ не имеют общих точек. Пусть теперь $l = l'$, но $p \neq p'$. Положим $r = \sum_{k=0}^{s-1} |p_k - p'_k| 2^k$. Очевидно, что $r \in 1 : 2^s - 1$. Согласно (7) и лемме 2 имеем

$$\langle\, \mu_s(pN_s+l),\, \mu_s(p'N_s+l)\,\rangle = \sum_{q=0}^{2^s-1} (-1)^{\{p,q\}_s + \{p',q\}_s} =$$

$$= \sum_{q=0}^{2^s-1} (-1)^{\{p,q\}_s - \{p',q\}_s} = \sum_{q=0}^{2^s-1} (-1)^{\{r,q\}_s} = 0.$$

Теорема доказана.

5°. Вектор $x = (x_0, x_1, ..., x_{N-1})$ при каждом $s \in 0 : n$ допускает представление

$$x = \sum_{k=0}^{N-1} x_s(k)\mu_s(k), \tag{9}$$

где $x_s(k) = 2^{-s}\langle x, \mu_s(k)\rangle$. В частности, $x_0(k) = x_k$, $k \in 0 : N-1$. В силу (1)

$$\begin{gathered} x_s(2mN_s + l) = \tfrac{1}{2}[x_{s-1}(2mN_s + l) + x_{s-1}((2m+1)N_s + l)], \\ x_s((2m+1)N_s + l) = \tfrac{1}{2}[x_{s-1}(2mN_s + l) - x_{s-1}((2m+1)N_s + l)], \end{gathered} \tag{10}$$

$$l \in 0 : N_s - 1, \quad m \in 0 : \Delta_s - 1, \quad s \in 1 : n.$$

Эти формулы позволяют последовательно вычислять коэффициенты разложения (9) при $s = 1, 2, ..., n$. Они называются *формулами декомпозиции.*

Обратив соотношения (10), получим

$$\begin{gathered} x_{s-1}(2mN_s + l) = x_s(2mN_s + l) + x_s((2m+1)N_s + l), \\ x_{s-1}((2m+1)N_s + l) = x_s(2mN_s + l) - x_s((2m+1)N_s + l), \\ l \in 0 : N_s - 1, \quad m \in 0 : \Delta_s - 1, \quad s = n, n-1, ..., 1. \end{gathered} \tag{11}$$

Формулы (11) называются *формулами реконструкции.* С их помощью вычисляются компоненты вектора x, заданного в виде

$$x = \sum_{k=0}^{N-1} x_n(k)\mu_n(k).$$

6°. Вернемся к представлению (8). Если обозначить через $A_n[p, \cdot]$ строку матрицы A_n с индексом p, то, принимая во внимание лемму 3, формулу (8) можно переписать в виде $\mu_n(p) = A_n[p, \cdot]$, $p \in 0 : N-1$. Это значит, что строками матрицы A_n являются векторы $\mu_n(0)$, $\mu_n(1)$, ..., $\mu_n(N-1)$. Как отмечалось, матрица A_n симметрична. Теорема 2 показывает, что она ортогональна, причем $A_n^{-1} = N^{-1}A_n$.

Элементы матрицы A_n принимают значения $+1$ или -1. Обозначим через $\zeta_n(p)$ число перемен знака у элементов строки $A_n[p, \cdot]$. Очевидно, что $\zeta_n(p) \in 0 : N-1$.

Лемма 4. *При $p \in 0 : 2^n - 1$ справедливы равенства*

$$\zeta_{n+1}(p) = 2\zeta_n(p), \quad \textit{если} \quad \zeta_n(p) \quad \textit{четно};$$

$$\zeta_{n+1}(p) = 2\zeta_n(p) + 1, \quad \textit{если} \quad \zeta_n(p) \quad \textit{нечетно};$$

$$\zeta_{n+1}(2^n + p) = 2\zeta_n(p) + 1, \quad \textit{если} \quad \zeta_n(p) \quad \textit{четно};$$

$$\zeta_{n+1}(2^n + p) = 2\zeta_n(p), \quad \textit{если} \quad \zeta_n(p) \quad \textit{нечетно}.$$

Доказательство непосредственно следует из (3).

Обозначим через $\langle p\rangle_2$ остаток от деления целого неотрицательного числа p на 2. Тогда результат леммы 4 можно переформулировать так:

$$\zeta_{n+1}(l2^n + p) = 2\zeta_n(p) + \langle l + \zeta_n(p)\rangle_2, \tag{12}$$

$$l \in 0 : 1, \quad p \in 0 : 2^n - 1.$$

Добавим к этому, что $\zeta_1(0) = 0$, $\zeta_1(1) = 1$.

Формула (12) позволяет вычислить $\zeta_n(p)$ при любых $n \geq 2$ и $p \in 0 : 2^n - 1$. Действительно, пусть $p = p_{n-1}2^{n-1} + \cdots + p_1 2 + p_0$. Положим $r_k = p_{k-1}2^{k-1} + \cdots + p_0$. Тогда $r_1 = p_0$, $r_{k+1} = p_k 2^k + r_k$ при $k \in 1 : n-1$, $r_n = p$. Имеем $\zeta_1(r_1) = p_0$. Далее при $k = 1, 2, ..., n-1$, опираясь на (12), последовательно находим $\zeta_{k+1}(r_{k+1}) = \zeta_{k+1}(p_k 2^k + r_k)$. Окончательно получаем $\zeta_n(p) = \zeta_n(r_n)$.

Пример . Вычислим $\zeta_3(5) = \zeta_3(\boxed{1\,|\,0\,|\,1})$. Имеем $\zeta_1(\boxed{1}) = 1$, $\zeta_2(\boxed{0\,|\,1}) = 3$, $\zeta_3(\boxed{1\,|\,0\,|\,1}) = 6$. Значит, $\zeta_3(5) = 6$.

Лемма 5. *При $p \in 0 : 2^n - 1$ выполняются равенства*

$$\zeta_{n+1}(2p) = \zeta_n(p), \tag{13}$$

$$\zeta_{n+1}(2p+1) = 2^{n+1} - 1 - \zeta_n(p). \tag{14}$$

Доказательство. Запишем двоичные представления:

$$\begin{aligned} p &= \qquad\quad \boxed{p_{n-1}\,|\,\cdots\,|\,p_1\,|\,p_0}, \\ 2p &= \boxed{p_{n-1}\,|\,p_{n-2}\,|\,\cdots\,|\,p_0\,|\,0}, \\ 2p+1 &= \boxed{p_{n-1}\,|\,p_{n-2}\,|\,\cdots\,|\,p_0\,|\,1}. \end{aligned}$$

Согласно (12) имеем $\zeta_2(\boxed{p_0\,|\,0}) = \langle p_0 \rangle_2 = p_0 = \zeta_1(\boxed{p_0})$. Дальнейший процесс вычисления $\zeta_{n+1}(2p)$ и $\zeta_n(p)$ идентичен, так что $\zeta_{n+1}(2p) = \zeta_n(p)$.

Равенство (14) перепишем в виде

$$\zeta_{n+1}(2p) + \zeta_n(2p+1) = 2^{n+1} - 1. \tag{15}$$

Введем обозначения

$$\begin{aligned} r_k^{(0)} &= \boxed{p_{k-1}\,|\,\cdots\,|\,p_0\,|\,0}, \\ r_k^{(1)} &= \boxed{p_{k-1}\,|\,\cdots\,|\,p_0\,|\,1}. \end{aligned}$$

Покажем, что

$$\zeta_{k+1}(r_k^{(0)}) + \zeta_{k+1}(r_k^{(1)}) = 2^{k+1} - 1, \quad k \in 1 : n. \tag{16}$$

При $k = n$ придем к (15).

Пусть $k = 1$. Тогда

$$\zeta_2(r_1^{(0)}) + \zeta_2(r_1^{(1)}) = \zeta_2(\boxed{p_0\,|\,0}) + \zeta_2(\boxed{p_0\,|\,1}) = \langle p_0 \rangle_2 + (2 + \langle p_0 + 1 \rangle_2) =$$
$$= 2 + (\langle p_0 \rangle_2 + \langle p_0 + 1 \rangle_2) = 3 = 2^2 - 1.$$

Сделаем индукционный переход от $k-1$ к k. Согласно (12) запишем

$$\begin{aligned} \zeta_{k+1}(r_k^{(0)}) &= 2\zeta_k(r_{k-1}^{(0)}) + \langle p_{k-1} + \zeta_k(r_{k-1}^{(0)}) \rangle_2, \\ \zeta_{k+1}(r_k^{(1)}) &= 2\zeta_k(r_{k-1}^{(1)}) + \langle p_{k-1} + \zeta_k(r_{k-1}^{(1)}) \rangle_2. \end{aligned} \tag{17}$$

По индукционному предположению $\zeta_k(r_{k-1}^{(0)}) + \zeta_k(r_{k-1}^{(1)}) = 2^k - 1$. В частности, $\zeta_k(r_{k-1}^{(0)})$ и $\zeta_k(r_{k-1}^{(1)})$ имеют разную четность. Сложив теперь равенства (17), получим

$$\zeta_{k+1}(r_k^{(0)}) + \zeta_{k+1}(r_k^{(1)}) = 2(2^k - 1) + 1 = 2^{k+1} - 1.$$

Лемма доказана.

Эта лемма позволяет легко переходить от последовательности ζ_n к последовательности ζ_{n+1}. Сначала по формуле (13) определяются компоненты $\zeta_{n+1}(2p)$ с четными индексами. Затем на основании (15) вычисляются компоненты $\zeta_{n+1}(2p+1)$ с нечетными индексами (как дополнение $\zeta_{n+1}(2p)$ до $2^{n+1}-1$). Например,

$$\zeta_1 = (0,1), \quad \zeta_2 = (0,3,1,2), \quad \zeta_3 = (0,7,3,4,1,6,2,5).$$

Лемма 5 делает очевидным следующий результат.

Теорема 3. *Преобразование*

$$(0,1,...,2^n-1) \to (\zeta_n(0), \zeta_n(1), ..., \zeta_n(2^n-1))$$

является перестановкой.

7°. Напомним, что $\zeta_n(p)$ есть количество перемен знака у компонент вектора $\mu_n(p)$. Перестановку ζ_n можно взять за основу более естественного упорядочения элементов ортогонального базиса $\{\mu_n(p)\}_{p=0}^{N-1}$ пространства $\mathbb{R}^N$. Более естественным будет такой порядок :

$$\mu_n(\zeta_n^{-1}(0)),\ \mu_n(\zeta_n^{-1}(1)),\ ...,\ \mu_n(\zeta_n^{-1}(N-1)).$$

8°. Введем в $\mathbb{R}^N$ еще одну рекуррентную систему базисов :

$$\eta_0(k) = e_k, \quad k \in 0:N-1;$$

$$\begin{gathered} \eta_s(m+2l\Delta_s) = \eta_{s-1}(m+2l\Delta_s) + \eta_{s-1}(m+(2l+1)\Delta_s), \\ \eta_s(m+(2l+1)\Delta_s) = \eta_{s-1}(m+2l\Delta_s) - \eta_{s-1}(m+(2l+1)\Delta_s), \\ l \in 0:N_s-1, \quad m \in 0:\Delta_s-1, \quad s \in 1:n. \end{gathered} \tag{18}$$

Если схему (1) можно связать с прореживанием по времени, то схема (18) соответствует прореживанию по частоте [3].

Теорема 4. *Справедливо представление*

$$\eta_s(p+2l\Delta_s) = \sum_{q=0}^{2^s-1} A_s[p,q]\eta_0(q+2l\Delta_s), \tag{19}$$

$$p \in 0:2\Delta_s-1, \quad l \in 0:N_s-1, \quad s \in 1:n.$$

Доказательство основано на том, что при $p,q \in 0:\Delta_s-1$

$$A_s[p,q] = A_s[\Delta_s+p,q] = A_s[p,\Delta_s+q] = -A_s[\Delta_s+p,\Delta_s+q] = A_{s-1}[p,q].$$

Перепишем формулу (19) в виде

$$\eta_s(p+2l\Delta_s) = \sum_{q=0}^{2^s-1} (-1)^{\{p,q\}_s} e_{q+2l\Delta_s}.$$

При $s=n$ получаем

$$\eta_n(p) = \sum_{q=0}^{N-1} (-1)^{\{p,q\}_n} e_q, \quad p \in 0:N-1. \tag{20}$$

Сравнивая (8) и (20), приходим к выводу о том, что

$$\mu_n(p) = \eta_n(p) \text{ при всех } p \in 0 : N-1. \tag{21}$$

9°. Матрицу A_n, определяемую соотношениями (3), можно представить в виде n-й кронекеровой степени матрицы A_1:

$$A_n = \underbrace{A_1 \otimes A_1 \otimes \cdots \otimes A_1}_{n \text{ раз}}.$$

Это позволяет двумя способами факторизовать матрицу A_n. Обозначим через E единичную матрицу второго порядка. Тогда

$$A_n = \prod_{s=1}^{n} (\underbrace{E \otimes E \otimes \cdots \otimes E}_{(n-s) \text{ раз}} \otimes A_1 \otimes \underbrace{E \otimes \cdots \otimes E}_{(s-1) \text{ раз}}) =$$

$$= \prod_{s=1}^{n} (\underbrace{E \otimes E \otimes \cdots \otimes E}_{(s-1) \text{ раз}} \otimes A_1 \otimes \underbrace{E \otimes \cdots \otimes E}_{(n-s) \text{ раз}}).$$

Последнее равенство соответствует формуле (21).

В заключение отметим, что матрица A_n лишь порядком строк отличается от матрицы Уолша [4, 5].

ЛИТЕРАТУРА

1. *Малозёмов В. Н., Третьяков А. А.* Новый подход к алгоритму Кули-Тьюки // Вестн. С.-Петербург. ун-та. Сер. 1. 1997. Вып. 3 (№ 15). С. 57–60.
2. *Холл М.* Комбинаторика. М., 1970. 424 с. (*M. Hall.* Combinatorial Theory.)
3. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. М., 1989. 448 с. (*Richard E. Blahut.* Fast Algorithms for Digital Signal Processing.)
4. *Walsh J. L.* A closed set of normal orthogonal functions. // Amer. J. Math. 1923. Vol. 45. P. 5–24.
5. *Голубов Б.И., Ефимов А.В., Скворцов В.А.* Ряды и преобразования Уолша. М., 1987. 344 с.

РЕФЕРАТ

УДК 519.677

М а л о з е м о в В. Н., Т р е т ь я к о в А. А. **Секционирование, ортогональность и перестановки** // Вестн. С.-Петербург. ун-та. Сер. 1. 1999. Вып. (№). С. 00–00.

С помощью метода секционирования, известного в теории быстрого преобразования Фурье, в евклидовом пространстве $\mathbb{R}^N$ при $N = 2^n$ построена конечная рекуррентная система ортогональных базисов. Показано, что финальный базис лишь порядком элементов отличается от базиса Уолша.

Библиогр. 5 назв.

SUMMARY

Malozemov V. N., Tretyakov A. A. Partitionning, orthogonality and permutations.

A finite recurrent system of orthogonal bases in the Euclidean space $\mathbb{R}^N$ for $N = 2^n$ is constructed with the help of the partitioning method known in the theory of Fast Fourier Transform. It is shown that the final basis differs from the Walsh basis only by the order of elements.

РЕЗЮМЕ

Малоземов В. Н., Третьяков А.А. Секционирование, ортогональность и перестановки

В евклидовом пространстве $\mathbb{R}^N$ при $N = 2^n$ построена конечная рекуррентная система ортогональных базисов с помощью метода секционирования, известного в теории быстрого преобразования Фурье. Показано, что финальный базис лишь порядком элементов отличается от от базиса Уолша.