SPb. Math. Society Preprint 2007-05 05 Sep 2007

ПАРАМЕТРИЧЕСКИЙ ВАРИАНТ МЕТОДА ПРОСТЫХ МНОЖИТЕЛЕЙ

В. Н. Малозёмов
malv@gamma.math.spbu.ru

О. В. Просеков
sc2@pisem.net

1. ФОРМУЛИРОВКА РЕЗУЛЬТАТОВ

1.1. Пусть $n_1, n_2, \ldots, n_s$ — 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 $p = (p_1, p_2, \ldots, p_s)$ 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 $q = (q_1, q_2, \ldots, q_s)$ назовём *сопряжённым вектором параметров*.

1.2. Введём перестановку $\mathrm{perm}_{n_1,n_2,\ldots,n_s}^{(p_1,p_2,\ldots,p_s)}$, 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 $k = \mathrm{perm}_{n_1}^{(p_1)}(j)$ означает, что $k = \langle j\, p_1 \rangle_{n_1}$. Такая перестановка называется *эйлеровой*.

Матрицу перестановок $Perm_{n_1,n_2,\ldots,n_s}^{(p_1,p_2,\ldots,p_s)}[0 : N-1, 0 : N-1]$ определим обычным способом:

$$Perm_{n_1,n_2,\ldots,n_s}^{(p_1,p_2,\ldots,p_s)}[j,k] = \begin{cases} 1, & \text{если } k = \mathrm{perm}_{n_1,n_2,\ldots,n_s}^{(p_1,p_2,\ldots,p_s)}(j), \\ 0 & \text{в остальных случаях.} \end{cases}$$

Матрицы $Perm_{n_\nu}^{(p_\nu)}$, $\nu \in 1:s$, назовём *матрицами эйлеровых перестановок*. При $p_1 = p_2 = \cdots = p_s = 1$ получим *матрицу руританских перестановок* $Perm_{n_1,n_2,\ldots,n_s}^{(1,1,\ldots,1)}$.

1.3. Сформулируем основные результаты статьи.

ТЕОРЕМА 1. *Справедливо разложение*

$$Perm_{n_1,n_2,\ldots,n_s}^{(p_1,p_2,\ldots,p_s)} = \bigl(Perm_{n_s}^{(p_s)} \otimes Perm_{n_{s-1}}^{(p_{s-1})} \otimes \cdots \otimes Perm_{n_1}^{(p_1)}\bigr) \prod_{\nu=2}^{s} \bigl(I_{N_\nu} \otimes Perm_{\Delta_\nu,n_\nu}^{(1,1)}\bigr)\,.$$

ТЕОРЕМА 2. *При любом векторе параметров $p = (p_1, p_2, \ldots, p_s)$ матрица Фурье F_N допускает представление*

$$F_N = \bigl(Perm_{n_1,n_2,\ldots,n_s}^{(q_1,q_2,\ldots,q_s)}\bigr)^T \bigl(F_{n_s} \otimes F_{n_{s-1}} \otimes \cdots \otimes F_{n_1}\bigr) Perm_{n_1,n_2,\ldots,n_s}^{(p_1,p_2,\ldots,p_s)}\,, \qquad (1)$$

где $q = (q_1, q_2, \ldots, q_s)$ — 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*

$$\operatorname{perm}_{n_1,n_2,\ldots,n_\nu}^{(p_1,p_2,\ldots,p_\nu)}(j + j_\nu\,\Delta_\nu) = \bigl\langle n_\nu \operatorname{perm}_{n_1,n_2,\ldots,n_{\nu-1}}^{(p_1,p_2,\ldots,p_{\nu-1})}(j) + \Delta_\nu \operatorname{perm}_{n_\nu}^{(p_\nu)}(j_\nu)\bigr\rangle_{\Delta_{\nu+1}}\,,$$

где $j \in 0:\Delta_\nu - 1$, $j_\nu \in 0:n_\nu - 1$.

Доказательство. Пусть $j = j_1 + j_2\,\Delta_2 + \cdots + j_{\nu-1}\,\Delta_{\nu-1}$. Пользуясь формулой $\langle k\,n\rangle_{mn} = n\,\langle k\rangle_m$, получаем

$$\operatorname{perm}_{n_1,n_2,\ldots,n_\nu}^{(p_1,p_2,\ldots,p_\nu)}(j + j_\nu\,\Delta_\nu) = \left\langle \sum_{\alpha=1}^{\nu} j_\alpha\,p_\alpha \frac{\Delta_{\nu+1}}{n_\alpha} \right\rangle_{\Delta_{\nu+1}} =$$

$$= \left\langle n_\nu \sum_{\alpha=1}^{\nu-1} j_\alpha\,p_\alpha \frac{\Delta_\nu}{n_\alpha} + j_\nu\,p_\nu\,\Delta_\nu \right\rangle_{\Delta_\nu n_\nu} = \left\langle n_\nu \Bigl\langle \sum_{\alpha=1}^{\nu-1} j_\alpha\,p_\alpha \frac{\Delta_\nu}{n_\alpha} \Bigr\rangle_{\Delta_\nu} + \Delta_\nu \langle j_\nu\,p_\nu\rangle_{n_\nu} \right\rangle_{\Delta_\nu n_\nu} =$$

$$= \bigl\langle n_\nu \operatorname{perm}_{n_1,n_2,\ldots,n_{\nu-1}}^{(p_1,p_2,\ldots,p_{\nu-1})}(j) + \Delta_\nu \operatorname{perm}_{n_\nu}^{(p_\nu)}(j_\nu)\bigr\rangle_{\Delta_{\nu+1}}\,.$$

Лемма доказана. □

ЛЕММА 2. *Для параметрических матриц перестановок при* $\nu \in 2:s$ *справедливо рекуррентное соотношение*

$$Perm^{(p_1,p_2,\ldots,p_\nu)}_{n_1,n_2,\ldots,n_\nu} = \bigl(Perm^{(p_\nu)}_{n_\nu} \otimes Perm^{(p_1,p_2,\ldots,p_{\nu-1})}_{n_1,n_2,\ldots,n_{\nu-1}}\bigr) Perm^{(1,1)}_{\Delta_\nu,n_\nu}\,. \tag{2}$$

Доказательство. Возьмём произвольный $\Delta_{\nu+1}$-мерный вектор x и обозначим $X = Perm^{(p_1,p_2,\ldots,p_\nu)}_{n_1,n_2,\ldots,n_\nu}\, x$. Тогда при $j \in 0:\Delta_\nu - 1$, $j_\nu \in 0:n_\nu - 1$ в силу леммы 1

$$\begin{aligned} X(j + j_\nu\,\Delta_\nu) &= x\bigl(\mathrm{perm}^{(p_1,p_2,\ldots,p_\nu)}_{n_1,n_2,\ldots,n_\nu}(j + j_\nu\,\Delta_\nu)\bigr) = \\ &= x\bigl(\bigl\langle n_\nu\,\mathrm{perm}^{(p_1,p_2,\ldots,p_{\nu-1})}_{n_1,n_2,\ldots,n_{\nu-1}}(j) + \Delta_\nu\,\mathrm{perm}^{(p_\nu)}_{n_\nu}(j_\nu)\bigr\rangle_{\Delta_{\nu+1}}\bigr)\,. \end{aligned} \tag{3}$$

Далее, поскольку $\mathrm{perm}^{(p_1,p_2)}_{n_1,n_2}(j_1 + j_2\,n_1) = \langle j_1\,p_1 n_2 + j_2\,p_2 n_1\rangle_{n_1 n_2}$, то для вектора $Y = Perm^{(1,1)}_{\Delta_\nu,n_\nu}\, x$ имеем

$$Y(j + j_\nu\,\Delta_\nu) = x\bigl(\langle j\,n_\nu + j_\nu\,\Delta_\nu\rangle_{\Delta_\nu n_\nu}\bigr)\,.$$

Найдём компоненты вектора $Z = \bigl(Perm^{(p_\nu)}_{n_\nu} \otimes Perm^{(p_1,p_2,\ldots,p_{\nu-1})}_{n_1,n_2,\ldots,n_{\nu-1}}\bigr)\, Y$. Запишем

$$\begin{aligned} Z(j + j_\nu\,\Delta_\nu) &= \sum_{j'_\nu=0}^{n_\nu-1}\sum_{j'=0}^{\Delta_\nu-1} \bigl(Perm^{(p_\nu)}_{n_\nu} \otimes Perm^{(p_1,p_2,\ldots,p_{\nu-1})}_{n_1,n_2,\ldots,n_{\nu-1}}\bigr)[j_\nu\,\Delta_\nu + j, j'_\nu\,\Delta_\nu + j'] \times \\ \times Y(j'_\nu\,\Delta_\nu + j') &= \sum_{j'_\nu=0}^{n_\nu-1}\sum_{j'=0}^{\Delta_\nu-1} Perm^{(p_\nu)}_{n_\nu}[j_\nu, j'_\nu] \times Perm^{(p_1,p_2,\ldots,p_{\nu-1})}_{n_1,n_2,\ldots,n_{\nu-1}}[j, j'] \times \\ \times Y(j' + j'_\nu\,\Delta_\nu) &= Y\bigl(\mathrm{perm}^{(p_1,p_2,\ldots,p_{\nu-1})}_{n_1,n_2,\ldots,n_{\nu-1}}(j) + \Delta_\nu\,\mathrm{perm}^{(p_\nu)}_{n_\nu}(j_\nu)\bigr) = \\ &= x\bigl(\bigl\langle n_\nu\,\mathrm{perm}^{(p_1,p_2,\ldots,p_{\nu-1})}_{n_1,n_2,\ldots,n_{\nu-1}}(j) + \Delta_\nu\,\mathrm{perm}^{(p_\nu)}_{n_\nu}(j_\nu)\bigr\rangle_{\Delta_{\nu+1}}\bigr)\,. \end{aligned} \tag{4}$$

Сравнивая (3) и (4), приходим к равенству $Z = X$. Отсюда очевидным образом следует (2). Лемма доказана. □

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

$$\begin{aligned} Perm^{(p_1,\ldots,p_s,p_{s+1})}_{n_1,\ldots,n_s,n_{s+1}} &= \bigl(Perm^{(p_{s+1})}_{n_{s+1}} \otimes Perm^{(p_1,\ldots,p_s)}_{n_1,\ldots,n_s}\bigr) Perm^{(1,1)}_{\Delta_{s+1},n_{s+1}} = \\ = \Bigl\{\bigl[Perm^{(p_{s+1})}_{n_{s+1}} \underbrace{I_{n_{s+1}}\ldots I_{n_{s+1}}}_{(s-1)\text{ раз}}\bigr] \otimes \Bigl[\bigl(Perm^{(p_s)}_{n_s} \otimes Perm^{(p_{s-1})}_{n_{s-1}} \otimes \cdots \otimes Perm^{(p_1)}_{n_1}\bigr) \times \end{aligned}$$

$$\times \prod_{\nu=2}^{s} \left(I_{n_{\nu+1}\cdots n_s} \otimes Perm^{(1,1)}_{\Delta_\nu, n_\nu}\right)\Big]\Big\} \left(I_1 \otimes Perm^{(1,1)}_{\Delta_{s+1}, n_{s+1}}\right) =$$

$$= \left(Perm^{(p_{s+1})}_{n_{s+1}} \otimes Perm^{(p_s)}_{n_s} \otimes \cdots \otimes Perm^{(p_1)}_{n_1}\right) \prod_{\nu=2}^{s+1} \left(I_{n_{\nu+1}\cdots n_s n_{s+1}} \otimes Perm^{(1,1)}_{\Delta_\nu, n_\nu}\right).$$

Теорема доказана. □

3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2

Проверим равенство, эквивалентное (1):

$$Perm^{(q_1,q_2,\ldots,q_s)}_{n_1,n_2,\ldots,n_s} F_N \left(Perm^{(p_1,p_2,\ldots,p_s)}_{n_1,n_2,\ldots,n_s}\right)^T = F_{n_s} \otimes F_{n_{s-1}} \otimes \cdots \otimes F_{n_1}. \tag{5}$$

В силу определения кронекерова умножения матриц

$$\begin{gathered}\left(F_{n_s} \otimes F_{n_{s-1}} \otimes \cdots \otimes F_{n_1}\right)\Big[\sum_{\nu=1}^{s} k_\nu\, \Delta_\nu, \sum_{\nu=1}^{s} j_\nu\, \Delta_\nu\Big] = \\ = \prod_{\nu=1}^{s} F_{n_\nu}[k_\nu, j_\nu] = \prod_{\nu=1}^{s} \omega_{n_\nu}^{k_\nu j_\nu}.\end{gathered} \tag{6}$$

Вместе с тем,

$$\left(Perm^{(q_1,q_2,\ldots,q_s)}_{n_1,n_2,\ldots,n_s} F_N \left(Perm^{(p_1,p_2,\ldots,p_s)}_{n_1,n_2,\ldots,n_s}\right)^T\right)\Big[\sum_{\nu=1}^{s} k_\nu\, \Delta_\nu, \sum_{\nu=1}^{s} j_\nu\, \Delta_\nu\Big] =$$

$$= \sum_{l=0}^{N-1}\sum_{l'=0}^{N-1} Perm^{(q_1,q_2,\ldots,q_s)}_{n_1,n_2,\ldots,n_s}\Big[\sum_{\nu=1}^{s} k_\nu\, \Delta_\nu, l\Big] \times F_N[l,l'] \times Perm^{(p_1,p_2,\ldots,p_s)}_{n_1,n_2,\ldots,n_s}\Big[\sum_{\nu=1}^{s} j_\nu\, \Delta_\nu, l'\Big] =$$

$$= F_N\Big[\mathrm{perm}^{(q_1,q_2,\ldots,q_s)}_{n_1,n_2,\ldots,n_s}\Big(\sum_{\nu=1}^{s} k_\nu\, \Delta_\nu\Big), \mathrm{perm}^{(p_1,p_2,\ldots,p_s)}_{n_1,n_2,\ldots,n_s}\Big(\sum_{\nu=1}^{s} j_\nu\, \Delta_\nu\Big)\Big] =$$

$$= \omega_N^{\left(\sum_{\nu=1}^{s} k_\nu\, q_\nu B_\nu\right)\left(\sum_{\nu=1}^{s} j_\nu\, p_\nu B_\nu\right)} = \prod_{\nu=1}^{s} \omega_{n_\nu}^{k_\nu j_\nu \langle q_\nu p_\nu B_\nu\rangle_{n_\nu}} = \prod_{\nu=1}^{s} \omega_{n_\nu}^{k_\nu j_\nu}. \tag{7}$$

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. □

4. ОБСУЖДЕНИЕ ПОЛУЧЕННЫХ РЕЗУЛЬТАТОВ

4.1. Очевидно, что $Perm^{(1)}_{n_\nu} = I_{n_\nu}$. Из теоремы 1 при $p_1 = p_2 = \cdots = p_s = 1$ следует разложение матрицы руританских перестановок:

$$Perm^{(1,1,\ldots,1)}_{n_1,n_2,\ldots,n_s} = \prod_{\nu=2}^{s} \left(I_{N_\nu} \otimes Perm^{(1,1)}_{\Delta_\nu, n_\nu}\right).$$

Более того, само заключение теоремы 1 можно переписать в виде

$$Perm_{n_1,n_2,\dots,n_s}^{(p_1,p_2,\dots,p_s)} = \bigl(Perm_{n_s}^{(p_s)} \otimes Perm_{n_{s-1}}^{(p_{s-1})} \otimes \cdots \otimes Perm_{n_1}^{(p_1)}\bigr) Perm_{n_1,n_2,\dots,n_s}^{(1,1,\dots,1)} .$$

4.2. Теорема 2 при $p_1 = p_2 = \cdots = p_s = 1$ по существу установлена Гудом [2]. 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 [3].

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.

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 $p = (3, 13)$.

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 $N = n_1 n_2 \cdots n_s$ с попарно взаимно простыми сомножителями n_ν.

4.3. В заключение укажем явный вид перестановки, обратной к $\mathrm{perm}_{n_1,n_2,\dots,n_s}^{(p_1,p_2,\dots,p_s)}$. Пусть $k \in 0 : N - 1$. Тогда

$$\bigl(\mathrm{perm}_{n_1,n_2,\dots,n_s}^{(p_1,p_2,\dots,p_s)}\bigr)^{-1}(k) = \sum_{\nu=1}^{s} \langle k\, q_\nu \rangle_{n_\nu} \Delta_\nu ,$$

где q_ν — компоненты сопряжённого с $p = (p_1, p_2, \dots, p_s)$ вектора параметров.

Нужно проверить, что

$$\left\langle \sum_{\nu=1}^{s} \langle k\, q_\nu \rangle_{n_\nu} p_\nu B_\nu \right\rangle_N = k . \tag{8}$$

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 $\bigl\langle\langle k\,q_\mu\rangle_{n_\mu}\,p_\mu B_\mu\bigr\rangle_{n_\mu} = \langle k'\rangle_{n_\mu}$, или $\bigl\langle k\,\langle q_\mu p_\mu B_\mu\rangle_{n_\mu}\bigr\rangle_{n_\mu} = \langle k'\rangle_{n_\mu}$, 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 $|k-k'| \leqslant N-1$, то необходимо $k = k'$. Утверждение доказано.

ЛИТЕРАТУРА

1. Воеводин В. В., Кузнецов Ю. А. *Матрицы и вычисления.* М.: Наука, 1984. 320 с.

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. Свердлик М. Б. *Матричная интерпретация алгоритма БПФ для взаимно простых сомножителей* // Радиотехника и электроника. 1983. № 10. С. 1931–1938.