С. С. АГАЯН, А. К. МАТЕВОСЯН

БЫСТРОЕ ПРЕОБРАЗОВАНИЕ АДАМАРА

В работе вводится понятие s—элементного гиперкаркаса, при помощи которого устанавливаются рекуррентные формулы для одновременного построения s, $s=2,4$, матриц Адамара H_i, $i=1, 2, \ldots, s$, $H_i H_j^T + H_j H_i^T = 0$, $i \neq j$, порядка $N = p_0 p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где $p_1, \ldots, p_k$, в частности, удвоенные порядки имеющихся матриц Вильямсона, $p_0 \geqslant 2$—порядок некоторой матрицы Адамара.

Разработан алгоритм, на основе которого быстрое преобразование Адамара по отношению к построенным выше матрицам производится при помощи

$$N \sum_{i=0}^{k} \alpha_i p_i \leqslant N \sum_{i=0}^{k} p_i \log_{p_i} N$$

сложений и вычитаний.

Приведенный алгоритм при $p_0 = p_1 = \ldots = p_k = 2$ совпадает с известным алгоритмом быстрого преобразования Уолша, а при $p_0 = 12$, $p_1 = \ldots = p_k = 2$ с алгоритмом БПА Прата.

1. Вспомогательные сведения и постановка зада́чи

В последние годы наблюдается все возрастающий интерес к вопросам теории дискретного преобразования Уолша, или к дискретному преобразованию Уолша—Фурье или Уолша—Адамара. Свидетельством этому является тот факт, что только с 1968 по 1971 гг. состоялось четыре международных симпозиума по применению функции Уолша [1].

Дискретное преобразование Уолша от произвольной дискретно-заданной функции $f(i)$, $i=1, 2, \ldots, N$, определяется как соотношение

$$F(j) = \sum_{i=1}^{N} f(i) \psi_j(i, N), \tag{1.1}$$

где $\psi_j(i, N)$, $j=1, 2, \ldots, N$,—дискретные функции Уолша, образованные равномерной $N=2^n$ выборкой непрерывных функций Уолша, которые после определения через функции Радемахера:

$$\Phi_0(t) = \begin{cases} 1 & \text{при } 0 \leqslant t < \frac{1}{2} \\ -1 & \text{при } \frac{1}{2} \leqslant t \leqslant 1 \end{cases}$$

$$\Phi_0(t+1)=\Phi_0(t), \quad \Phi_n(t)=\Phi_0(2^n t), \quad n=0, 1, \ldots, \tag{1.2}$$

примут вид: $\psi_0(t)=1;$

$$\psi_n(t)=\Phi_{n_1}(t)\Phi_{n_2}(t)\ldots\Phi_{n_k}(t), \tag{1.3}$$

где $n_1, n_2, \ldots, n_k$ определяются из соотношения $n=2^{n_1}+2^{n_2}+\ldots+2^{n_k}$ при условии $n_{l+1}>n_l$.

Свойства как непрерывных, так и дискретных функций Уолша исследованы в работах [2—6].

Обратное преобразование Уолша определяется соотношением

$$f(i)=2^{-n}\sum_{j=1}^{N} F(j)\psi_j(i, N). \tag{1.4}$$

Множитель 2^{-n} в формуле (1.4) отражает тот факт, что дискретные функции Уолша имеют фиксированную норму, равную 2^n.

Преобразования (1.1) и (1.4) в матричной записи будут иметь следующий вид:

$$F=H(N)\cdot f \tag{1.5}$$

и

$$f=2^{-n}H(N)F. \tag{1.6}$$

$H(N)$—квадратная ортогональная матрица порядка $N=2^n$ с элементами -1 и $+1$, где $f^T=[f(1), f(2), \ldots, f(N)]$ — вектор начальных данных, $F^T=[F(1), F(2), \ldots, F(N)]$—его Уолш—образ, а T означает знак транспонирования.

Подчеркнем, что:

а) строки матрицы $H(N)$ соответствуют дискретным функциям Уолша;

в) как для прямого, так и для обратного дискретного преобразования Уолша используется одна и та же матрица $H(N)$;

с) матрица $H(N)$ является матрицей Адамара порядка $N=2^n$, а именно квадратной матрицей, состоящей из -1 и $+1$ с попарно ортогональными строками и столбцами.

Дискретное преобразование Уолша (как прямое, так и обратное) требует выполнения N^2 операций сложения или вычитания. Построены алгоритмы быстрого преобразования Уолша, основанные на построении дискретных функций Уолша, производящие $N\log_2 N$ сложений и вычитаний [7].

В работе [8] построен алгоритм быстрого преобразования Адамара для специальной матрицы Адамара порядка $N=12\cdot 2^n$, производящий также порядка $N\log_2 N$ операций. Отметим, что построенные алгоритмы опирались на результаты, полученные в работах [9—10].

С построением алгоритма быстрого преобразования Адамара последнее стало широко применяться для вычисления энергетических спектров, автокорреляционных функций и т. д., где до этого в основном использовалось быстрое преобразование Фурье [11—15].

Преобразование Адамара особо широкое применение имеет в области кодирования и фильтрации изображений [7, 14, 15]. В работах [16, 17] исследованы некоторые вопросы применения преобразования Адамара в системах оптической обработки информации.

Отметим, что к оператору, используемому при кодировании изображений, предъявляются следующие требования: двумерность, существование обратного оператора и быстрореализуемого алгоритма для этой пары операторов. Матричный оператор Адамара удовлетворяет приведенным требованиям и имеет ряд преимуществ над соответствующим методом, базирующемся на быстром преобразовании Фурье [23].

В частности:

а) преобразование Адамара требует только сложения и вычитания действительных чисел, что дает возможность на порядок увеличить скорость по сравнению с преобразованием Фурье, оперирующим с комплексными числами;

в) код изображения, полученный преобразованием Адамара, характеризуется устойчивостью к ошибкам в канале и возможностью уменьшения ширины полосы частот.

Естественно, исследовать следующую задачу:
для любого дискретного преобразования Адамара порядка N

$$F = H(N) \cdot f \tag{1.7}$$

построить алгоритм быстрого преобразования, производящий порядка $N \log_k N$ операций.

Трудность решения этой задачи связана не только с проблемой построения матриц Адамара $H(N)$ любого порядка $N \equiv 0 (\mathrm{mod}\, 4)$ [18], т. е. матрицы, удовлетворяющей условию

$$HH^T = H^T H = NI_N,$$

где I_N — единичная матрица порядка N, но и задания достаточно удобной ее конструкции, что позволило бы построить быстрореализуемый алгоритм для преобразования (1.7).

Основные результаты о построении матриц Адамара можно найти в работах [18, 22].

В настоящей работе приводится рекуррентная формула построения матриц Адамара H_i, $i = 1, 2, \ldots, s$, $s = 2, 4$, удовлетворяющих условию

$$H_i H_j^T + H_j H_i^T = 0, \quad i \neq j,$$

порядка $N = p_0 p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где $p_1, \ldots, p_k$, в частности, удвоенные порядки имеющихся матриц Вильямсона, $p_0 \geqslant 2$ — порядок некоторой матрицы Адамара.

Разработан алгоритм быстрого преобразования Адамара для построенных матриц, производящий

$$N \cdot \sum_{i=0}^{k} \alpha_i p_i \leqslant N \cdot \sum_{i=0}^{k} p_i \log_{p_i} N$$

сложений и вычитаний.

2. Рекуррентные формулы построения матриц Адамара

При построении алгоритма быстрого преобразования Адамара соответственно порядков 2^n и $12 \cdot 2^n$ использовалось следующее рекуррентное построение матриц Адамара

$$H(k+1) = \begin{bmatrix} H(k) & H(k) \\ H(k) & -H(k) \end{bmatrix}, \tag{2.1}$$

где $H(1)$ совпадает:

а) с матрицей $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ при $N = 2^n$,

б) с матрицей Адамара порядка 12, приведенной в работе [8]. Фактически приведенные алгоритмы опирались на представление

$$H(k+1) = X \otimes H(k) + Y \otimes H(k), \tag{2.2}$$

где $X = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix}$ или $X = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$, $Y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

не зависят от k, а $\otimes$—кронекерово произведение [18].

Рассмотрим следующую модификацию этого построения.

Будем искать матрицу $H(k+1)$ в виде:

$$H(k+1) = \sum_{i=1}^{s} X_i \otimes H_i(k), \tag{2.3}$$

где X_i, $i = 1, 2, \ldots, s$, не зависящие от k квадратные (0, −1, +1) матрицы, а $H_i(k)$, $i = 1, 2, \ldots, s$—матрицы Адамара, полученные на k-ом шаге рекурсии. Теперь найдем также такие условия для матрицы X_i и $H_i(k)$, $i = 1, 2, \ldots, s$, чтобы $H(k+1)$ была матрицей Адамара, т. е. удовлетворяла уравнению

$$H(k+1) \cdot H^T(k+1) = m_k I_{m_k}, \tag{2.4}$$

где m_k—порядок матрицы $H(k+1)$.

Из (2.4) сразу заметим, что на матрицы $X_1, X_2, \ldots, X_s$ нужно наложить следующие ограничения

$$1. \quad X_i * X_j = 0, \quad i \neq j, \tag{2.5}$$

$*$—адамарово произведение [23]

$$2. \quad \sum_{i=1}^{s} X_i - (-1, +1) \text{ матрица.}$$

Далее из (2.3) и (2.4) имеем

$$H(k+1) \cdot H^T(k+1) = \left(\sum_{i=1}^{s} X_i X_i^T \right) \otimes m_{k-1} I_{m_{k-1}} +$$

$$+ \sum_{i=1}^{s} \sum_{j=1}^{s} X_i X_j^T \otimes H_i(k) \cdot H_j^T(k). \tag{2.7}$$

В рекуррентном построении возможны два случая:

а) пусть $H_i(k)=H_j(k), \quad i, j=1, 2, \ldots, s,$

тогда для выполнения равенства (2.4) достаточно положить

3. $\sum\limits_{i=1}^{s} X_i X_i^T=kI_k, \quad k$ — порядок $X_i, \quad i=1, 2, \ldots, s,$

4. $\sum\limits_{i=1}^{s} \sum\limits_{\substack{j=1 \\ j\neq i}}^{s} X_i X_j^T=0.$

Матрицы $X_i, \; i=1, 2, \ldots, s,$ удовлетворяющие условиям 1, 2, 3, 4 исследованы в [19] и названы каркасом.

в) Пусть $X_i X_j^T=X_j X_i^T, \quad i, j=1, 2, \ldots, s,$

тогда для выполнения (2.4) достаточно

$$\sum_{i=1}^{s} X_i X_i^T=kI_k,$$

$$\sum_{i=1}^{s} \sum_{\substack{j=1 \\ j\neq i}}^{s} H_i(k) H_j^T(k)=0.$$

Определение: Квадратные (0, —1, +1) матрицы X_i, i=1, 2, ..., s, порядка k, удовлетворяющие условиям

$$
\begin{aligned}
&1. \; X_i * X_j=0, \quad i\neq j, \quad i, j=1, 2, \ldots, s,\\
&2. \; \sum_{i=1}^{s} X_i \quad (-1, +1)\text{—матрица},\\
&3. \; X_i X_j^T=X_j X_i^T, \quad i, j=1, 2, \ldots, s,\\
&4. \; \sum_{i=1}^{s} X_i X_i^T=kI_k,
\end{aligned}
\tag{2.8}
$$

назовем s—элементным гиперкаркасом.

Теперь, объединяя пункты а) и в), заключаем, что для построения матриц Адамара необходимо построить:

1) каркасы новых порядков N

(заметим, что $N\equiv 0 \pmod 4$ [19])

или

2) построить s—элементный гиперкаркас порядка N. Здесь возникает дополнительная задача: для данной матрицы Адамара H_1 построить $s-1$ таких матриц Адамара H_i, $i=2, 3, \ldots, s$, чтобы выполнялось

$$H_i H_j^T + H_j H_i^T=0, \; i\neq j, \quad i, j=1, 2, \ldots, s.$$

Отметим некоторые свойства s—элементного гиперкаркаса.

Если $X_1, X_2, \ldots, X_s$—гиперкаркас порядка n, то множество матриц

а) $\{l_i X_i\}_{i=1}^{s}$ гиперкаркас порядка n, $l_i=\pm 1$, в) $\{l_i X_i \otimes H\}_{i=1}^s$ s-элементный гиперкаркас порядка nm, где H— матрица Адамара порядка m,

с) $\{l_i X_i \otimes Q_i\}_{i=1}^s$ s—элементный гиперкаркас порядка nm, где матрицы Q_i, $i=1, 2, \ldots, s$ порядка m, удовлетворяют следующим условиям:

1. $Q_i * Q_j = 0, \quad i \neq j,$

2. $\sum_{i=1}^{s} Q_i \quad (-1, +1)$ матрица,

3. $Q_i^T = Q_i, \quad Q_i Q_j = Q_j Q_i,$

4. $Q_i Q_i^T = \frac{m}{s} I_m.$

Пример матриц Q_i $i=1, 2, 3, 4$.

$$Q_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad Q_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$Q_3 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \qquad Q_4 = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \tag{2.9}$$

В частности, при $s=2$, матрицы X и Y, образующие двухэлементный гиперкаркас, удовлетворяют условиям

1. $X * Y = 0,$
2. $X \pm Y \quad (-1, +1)$ матрица, (2.10)
3. $XY^T = YX^T,$
4. $XX^T + YY^T = kI_k.$

Справедливы следующие теоремы и леммы.

Теорема 2.1. Пусть существует матрица Адамара порядка n, тогда существует двухэлементный гиперкаркас порядка n.

Доказательство. Пусть h_i, $i=1, 2, \ldots, n$, строки матрицы H. Непосредственной проверкой можно убедиться, что матрицы

$$X = \begin{bmatrix} x_1 h_1 \\ x_2 h_2 \\ \vdots \\ x_n h_n \end{bmatrix}, \quad Y = \begin{bmatrix} (1-x_1)h_1 \\ (1-x_2)h_2 \\ \vdots \\ (1-x_n)h_n \end{bmatrix}, \quad x_i = \begin{cases} 0 \\ 1 \end{cases}, \; i=1, 2, \ldots, n.$$

образуют двухэлементный гиперкаркас.

Теорема 2.2. Пусть A, B, C, D матрицы Вильямсона порядка p, тогда матрицы

$$X=\frac{1}{2}\begin{bmatrix} A+B & C+D \\ C+D & -(A+B)\end{bmatrix}, \qquad Y=\frac{1}{2}\begin{bmatrix} A-B & C-D \\ -(C-D) & A-B\end{bmatrix}$$

образуют двухэлементный гиперкаркас порядка $2p$.

Лемма 2.1. Для любой матрицы Адамара H_1 порядка n можно построить такие матрицы Адамара H_i, $i=1, 2, \ldots, s$, $s=2,4$, чтобы выполнялись равенства

$$H_iH_j^T+H_jH_i^T=0,\ i\neq j,\ i, j=1, 2, \ldots, s. \tag{2.11}$$

Доказательство. Рассмотрим случай $s=2$.

Определим оператор Γ_2, переводящий матрицу A со строками $a_1, a_2, \ldots, a_n$ на матрицу $\Gamma_2[A]$ со строками $a_2, -a_1, \ldots, a_n, -a_{n-1}$.

$$\Gamma_2[A]=\Gamma_2\begin{bmatrix} a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{n-1} \\ a_n\end{bmatrix}=\begin{bmatrix} a_2 \\ -a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_n \\ -a_{n-1}\end{bmatrix}. \tag{2.12}$$

Легко проверить, что искомой матрицей Адамара будет $H_2=\Gamma_2[H_1]$. Случай $s=4$. Введем дополнительно два оператора Γ_3, Γ_4

$$\Gamma_3[A]=\begin{bmatrix} a_3 \\ -a_4 \\ -a_1 \\ a_2 \\ \cdot \\ \cdot \\ \cdot \\ a_{n-1} \\ -a_n \\ -a_{n-3} \\ a_{n-2}\end{bmatrix}, \quad \Gamma_4[A]=\begin{bmatrix} a_4 \\ a_3 \\ -a_2 \\ -a_1 \\ \cdot \\ \cdot \\ \cdot \\ a_n \\ a_{n-1} \\ -a_{n-2} \\ -a_{n-3}\end{bmatrix}, \tag{2.13}$$

полученные матрицы (2.12) и (2.13) обозначим через $H_i=\Gamma_i[H_1]$. Легко проверить, что указанные матрицы с матрицей H_1 удовлетворяют условию (2.11) для $s=4$.

Лемма 2.2. Если $\{A_1, A_2\}$ 2-элементный гиперкаркас порядка k, то $k\equiv(\mathrm{mod}\,2)$.

Доказательство. Пусть $\{A_1, A_2\}$ 2-элементный гиперкаркас порядка k, H_1, H_2 произвольные матрицы Адамара порядка m, удовлетворяющие условию

$$H_1H_2^T+H_2H_1^T=0.$$

Тогда можно проверить, что $H=A_1\otimes H_1+A_2\otimes H_2$ матрица Адамара порядка $N=m\cdot k$, откуда следует, что $N\equiv(\mathrm{mod}\,4)$.

Пусть теперь

$$H_1=\begin{bmatrix} 1 & 1 \\ 1 & -1\end{bmatrix}, \quad H_2=\begin{bmatrix} 1 & -1 \\ -1 & -1\end{bmatrix},$$

тогда получим, что $2k\equiv0(\mathrm{mod}\,4)$. Следовательно $k\equiv0\ (\mathrm{mod}2)$.

Определение [20]. Квадратную матрицу $H(x_1, x_2, \ldots, x_s)$ порядка m, каждый элемент которой принимает одно из $2s$ значений $\pm x_i$ $i=1, 2, \ldots, s$, назовем матрицей типа A, если для разных значений параметров $x_1, x_2, \ldots, x_s$ выполняется равенство.

$$H(x_1^{(1)}, x_2^{(1)}, \ldots, x_s^{(1)}) \cdot H^T(x_1^{(2)}, x_2^{(2)}, \ldots, x_s^{(2)}) + H(x_1^{(2)}, x_2^{(2)}, \ldots, x_s^{(2)}) \times$$

$$\times H^T(x_1^{(1)}, x_2^{(1)}, \ldots, x_s^{(1)}) = \frac{2m}{s}(x_1^{(1)}x_1^{(2)} + x_2^{(1)}x_2^{(2)} + \ldots + x_s^{(1)}x_s^{(2)}) I_m.$$

Лемма 2.3. Пусть $H(x_1, x_2, \ldots, x_s)$, $s=2, 4, 8$, матрица типа A порядка N. Тогда существует s матриц Адамара, удовлетворяющих соотношений (2.11).

Теорема 2.3. Если существует 2-элементный гиперкаркас $\{A_1, A_2\}$ порядка k, то существует 4-элементный гиперкаркас порядка $2k$. Далее, если дополнительно $A_i A_j^T = A_j^T A_i^T$, то существует 8-элементный гиперкаркас порядка $4k$.

Доказательство. Пусть $\{A_1, A_2\}$ — 2-элементный гиперкаркас порядка $k \geqslant 2$. Определим матрицы

$$W_1 = X \otimes A_1, \qquad W_3 = Y \otimes A_1,$$

$$W_2 = X \otimes A_2, \qquad W_4 = Y \otimes A_2,$$

где

$$X = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{или} \quad X = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & 1 \\ 0 & -1 \end{bmatrix}.$$

Легко проверить, что матрицы $\{W_i\}_{i=1}^4$ удовлетворяют условиям (2.8), т. е. образуют 4-элементный гиперкаркас порядка $2k$. Теперь введем матрицы $\{V_i\}_{i=1}^8$

$$V_i = X \otimes W_i, \qquad V_{4+i} = Y \otimes W_i, \qquad i=1, 2, 3, 4.$$

Можно также проверить, что введенные матрицы образуют 8-ми элементный гиперкаркас порядка $4k$.

Перейдем теперь к рекуррентным построениям матриц Адамара.

Теорема 2.4. Пусть $H_1(0)$ и $H_2(0)$ — матрицы Адамара порядка n, такие, что $H_1(0)H_2^T(0) + H_2(0)H_1^T(0) = 0$, а X и Y — 2-элементный гиперкаркас, порядка m, тогда матрицы

$$H_1(i+1) = X \otimes H_1(i) + Y \otimes H_2(i),$$

$$H_2(i+1) = -X \otimes H_2(i) + Y \otimes H_1(i) \tag{2.14}$$

являются матрицами Адамара порядка nm^{i+1}, удовлетворяющим и условию:

$$H_1(i+1)H_2^T(i+1) + H_2(i+1)H_1^T(i+1) = 0.$$

Замечание. Построение могло вестись и по схеме

$$H_1(i+1)=H_1(i)\otimes X+H_2(i)\otimes Y,$$
$$H_2(i+1)=-H_2(i)\otimes X+H_1(i)\otimes Y. \tag{2.15}$$

Следствие. Для любого натурального числа i существует матрица Адамара порядка $2m^l$, где $m=2l$, а l, в частности, порядки существующих матриц Вильямсона: $l\in\{3, 5, \ldots, 33, 35, 37, 43\}$,

Теорема 2.5. Пусть $H_i(0)$, $i=1, 2, 3, 4$ матрицы Адамара порядка n, удовлетворяющие

$$H_i(l)\cdot H_j^T(l)+H_j(l)\cdot H_i^T(l)=0 \tag{2.16}$$

при $l=0$, $i\neq j$, $i, j=1, 2, 3, 4$,
$\{X_i\}_{i=1}^4$—4-элементный гиперкаркас порядка m
тогда

$$H_1(i+1)=X_1\otimes H_1(i)+X_2\otimes H_2(i)+X_3\otimes H_3(i)+X_4\otimes H_4(i),$$
$$H_2(i+1)=X_1\otimes H_2(i)-X_2\otimes H_1(i)+X_3\otimes H_4(i)-X_4\otimes H_3(i),$$
$$H_3(i+1)=X_1\otimes H_3(i)-X_2\otimes H_4(i)-X_3\otimes H_1(i)+X_4\otimes H_2(i),$$
$$H_4(i+1)=X_1\otimes H_4(i)+X_2\otimes H_3(i)-X_3\otimes H_2(i)-X_4\otimes H_1(i)$$

являются матрицами Адамара порядка nm^{i+1}, удовлетворяющими (2.16).

Относительно теоремы (2.5) справедливо замечание, аналогичное замечанию теоремы 2.4.

Замечание. Таким образом, проблема построения матриц Адамара привелась к построению $s=2, 4, 8$ элементного гиперкаркаса.

3. Быстрое преобразование Адамара

Мы приведем алгоритм быстрого преобразования Адамара для матрицы Адамара порядка $N=m_n=mk^n$, построенной по рекурентной формуле

$$H_{m_n}=X\otimes H_{m_{n-1}}+Y\otimes H'_{m_{n-1}}$$
$$H'_{m_n}=-X\otimes H'_{m_{n-1}}+Y\otimes H_{m_{n-1}}, \tag{3.1}$$

где H_{m_n}—матрица Адамара порядка m_n, $H'_{m_{n-1}}=-\Gamma_2[H_{m_{n-1}}]$ (лемма 2.1), а $\{x=\{x_{ij}\}_{i,j=1}^k, Y=\{y_{ij}\}_{i,j=1}^k\}$—2-элементный гиперкаркас порядка k.

Пусть оператор L_i вектору $z^T=[z(1), z(2), \ldots, z(m_n)]$ ставит в соответствие вектор

$$z_i^T=L_i[z^T]=$$
$$=\left[z\left((i-1)\frac{m_n}{k}+1\right), z\left((i-1)\frac{m_n}{k}+2\right), \ldots, z\left((i-1)\frac{m_n}{k}+\frac{m_n}{k}\right)\right].$$

Обозначим через f_l, b_l, c_l следующие вектора:

$$f_l^T = L_l[f(1), f(2), \ldots, f(m_n)],$$

$$b_l^T = L_l[b(1), b(2), \ldots, b(m_n)],$$

$$c_l^T = L_l[c(1), c(2), \ldots, c(m_n)],$$

$$l = 1, 2, \ldots, k,$$

где

$$b_l = H_{m_{n-1}} \cdot f_l,$$

$$c_l = -\Gamma_2[b_l], \tag{3.2}$$

$$l = 1, 2, \ldots, k.$$

В этих обозначениях m_n—точечное преобразование вектора f

$$F = H_{m_n} \cdot f \tag{3.3}$$

можно вычислить по формулам:

$$F(i) = p(i) + q(i), \qquad i = 1, 2, \ldots, N, \tag{3.4}$$

$$\left.\begin{aligned} p(i) &= \sum_{j=1}^{k} b\left((j-1)\frac{m_n}{k} + i\right) \cdot x_{\left[\frac{i-1}{m_n}k\right]+1,j}, \\ q(i) &= \sum_{j=1}^{k} c\left((j-1)\frac{m_n}{k} + i\right) \cdot y_{\left[\frac{i-1}{m_n}k\right]+1,j}, \\ & i = 1, 2, \ldots, N, \end{aligned}\right\} \tag{3.5}$$

где $[x]$ обозначает целую часть x.

На рис. 1 с помощью направленного графа представлена последовательность операций при выполнении m_n—точечного преобразования с использованием k m_{n-1}-точечных преобразований. Входная последовательность $f(1), f(2), \ldots, f(m_n)$ разбивается на k последовательности

$$f_l^T = f\left((l-1)\frac{m_n}{k} + 1\right), f\left((l-1)\frac{m_n}{k} + 2\right), \ldots, f\left((l-1)\frac{m_n}{k} + \frac{m_n}{k}\right),$$

$$l = 1, 2, \ldots, k,$$

после чего вычисляются их преобразования b_l. Затем в соответствии с формулами (3.5) и (3.4) получаем искомый вектор

$$F^T = [F(1), F(2), \ldots, F(m_n)].$$

Оценим количество операций, за которые выполняется преобразование (3.3). Если обозначить число операций m_n—точечного преобразования через D_n, то, как видно из алгоритма проведения преобразования,

$$D_n = kD_{n-1} + m_{n-1}(T_x + T_y) + m_n,$$

где T_x и T_y—число операций матричных преобразований X и Y соответственно.

Рассмотренная схема вычислений может быть использована для расчета m_{n-1} точечных преобразований (3.2) и т. д.

Таким образом, для D_n будет получена оценка

$$D_n = \left(\frac{D_0}{mn} + \frac{T_x + T_y}{k} + 1\right) nk^n m = C(k)nmk^n \leqslant C(k)\, N \log_k N. \tag{3.6}$$

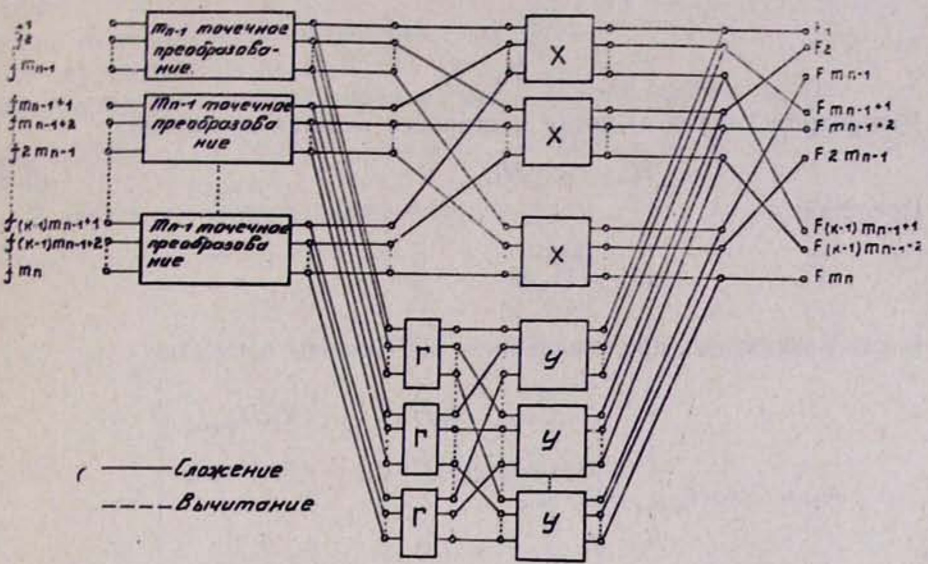

Рис. 1

Отметим, что в общем случае $C(k) \leqslant k$, можно найти более точную оценку величины $C(k)$ путем факторизации матриц X и Y. В частности, при $k=6,10$ найдено, что $C(6)=5$, $C(10)=9$ соответственно, а после факторизации X и Y $C(6)=4$, $C(10)=7$.

Для матриц Адамара порядка $N=2 \cdot 10^4$ $D_n = 28N$, т. е. выполняется в 714 раз меньше операций сложения и вычитания, чем при прямом преобразовании, требующем N^2 операций.

Заметим, что этот же алгоритм применяется для обратного преобразования

$$f = \frac{1}{N} \cdot H^T_{m_n} F.$$

Быстрые преобразования Адамара могут быть получены разложением матрицы преобразования H_{m_n} в произведение $n+1$ матриц с небольшим количеством отличных от нуля элементов

$$H = \prod_{k=1}^{n+1} M_k.$$

Тогда вычисление преобразования вектора f может быть представлено в виде

$$F=M_1\cdot M_2\cdot\ldots\cdot M_{n+1}f$$

или, что то же самое

$$\begin{aligned} f_1&=M_{n+1}\cdot f,\\ f_2&=M_n\cdot f_1,\\ &\ \vdots\\ F&=f_{n+1}=M_1\cdot f_n. \end{aligned} \tag{3.7}$$

Рассмотрим случай а) когда построение ведется по схеме:

$$H_{m_n}=X\otimes H_{m_{n-1}}\ . \tag{3.8}$$

Представим

$$H_{m_n}=\prod_{k=1}^{n+1}A_k.$$

Воспользовавшись представлением (3.8) можем записать:

$$H_{m_n}=X\otimes H_{m_{n-1}}=\begin{bmatrix} x_{11}H_{m_{n-1}} & x_{12}H_{m_{n-1}} & \ldots & x_{1k}H_{m_{n-1}}\\ x_{21}H_{m_{n-1}} & x_{22}H_{m_{n-1}} & \ldots & x_{2k}H_{m_{n-1}}\\ \vdots & \vdots & & \vdots\\ x_{k1}H_{m_{n-1}} & x_{k2}H_{m_{n-1}} & \ldots & x_{kk}H_{m_{n-1}} \end{bmatrix}=$$

$$=\begin{bmatrix} x_{11}I_{m_{n-1}} & x_{12}I_{m_{n-1}} & \ldots & x_{1k}I_{m_{n-1}}\\ x_{21}I_{m_{n-1}} & x_{22}I_{m_{n-1}} & \ldots & x_{2k}I_{m_{n-1}}\\ \vdots & \vdots & & \vdots\\ x_{k1}I_{m_{n-1}} & x_{k2}I_{m_{n-1}} & \ldots & x_{kk}I_{m_{n-1}} \end{bmatrix}\cdot\begin{bmatrix} H_{m_{n-1}} & 0 & \ldots & 0\\ 0 & H_{m_{n-1}} & \ldots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & & H_{m_{n-1}} \end{bmatrix}=A_1\cdot S$$

$H_{m_n}=A_1\cdot S$, где A_1 и S—матрицы порядка m_n. Факторизовав каждый из блоков $H_{m_{n-1}}$ в матрице S будем иметь:

$$H_{m_n}=A_1\cdot A_2\cdot S,$$

где

$$A_2=I_k\otimes X\otimes I_{m_{n-2}},$$

$$S=I_k\otimes I_k\otimes H_{m_{n-2}}.$$

Продолжив таким образом на n-ом шаге получим:

$$H_{m_n}=\prod_{r=1}^{n+1} A_r$$

$$A_r=\underbrace{I_k\otimes I_k\otimes \ldots \otimes I_k}_{r-1}\otimes X\otimes I_{m_{n-r}}, \quad r=1, 2, \ldots, n,$$

$$A_{n+1}=\underbrace{I_k\otimes I_k\otimes \ldots \otimes I_k}_{n}\otimes H_0.$$

Отметим, что в частном случае $\left(X=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, Y=\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}\right)$ матрицы A_r совпадают с матрицами Гуда [2.1].

в) построение по (3.1).

Рассуждая аналогичным образом, как и в предыдущем случае,

$$H_{m_n}=X\otimes H_{m_{n-1}}+Y\otimes H'_{m_{n-1}}=[X\otimes I_{m_{n-1}}+Y\otimes Z_{m_{n-1}}]\ S,\quad S=I_k\otimes H_{m_{n-1}},$$

а Z перестановочная матрица порядка m_n

$$Z=\begin{bmatrix} 0 & 1 & 0 & 0 & \ldots & 0 & 0\\ -1 & 0 & 0 & 0 & \ldots & 0 & 0\\ 0 & 0 & 0 & 1 & \ldots & 0 & 0\\ 0 & 0 & -1 & 0 & \ldots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \ldots & 0 & 1\\ 0 & 0 & 0 & 0 & \ldots & -1 & 0 \end{bmatrix}.$$

Обозначим:

$$M_1=X\otimes I_{m_{n-1}}+(Y\otimes Z_{m_{n-1}}),\quad \text{тогда}\quad H_{m_n}=M_1\cdot S.$$

Продолжив факторизацию для каждого блока $H_{m_{n-1}}$ матрицы S получим, что

$$H_{m_n}=M_1\cdot M_2\cdot S,\qquad \text{где}$$

$$M_2=I_k\otimes[X\otimes I_{m_{n-2}}+Y\otimes Z_{m_{n-2}}],$$

$$S=I_k\otimes I_k\otimes H_{m_{n-2}}.$$

Таким образом,

$$H_{m_n}=\prod_{r=1}^{n+1} M_r,\qquad \text{где}$$

$$M_r=\underbrace{I_k\otimes I_k\otimes \ldots \otimes I_k}_{r-1}\otimes[X\otimes I_{m_{n-r}}+Y\otimes Z_{m_{n-r}}];$$

$$M_{n+1}=I_k\otimes I_k\otimes \ldots \otimes I_k\otimes H_0,\qquad r=1, 2, \ldots, n.$$

Получено разложение H_{m_n} на $n+1$ квадратных матриц порядка m_n, причем в каждой строке M_r число ненулевых элементов равно

$$\begin{cases} k & \text{при} \quad r \neq n+1, \\ m & \text{при} \quad r = n+1. \end{cases}$$

После сделанных замечаний видно, что на вычисление f_i в последовательных преобразованиях (3.7) необходимо

$$\begin{cases} m_n \cdot m, & i=1, \\ m_n \cdot k, & i \neq 1 \text{ операций}, \end{cases}$$

т. е. F вычисляется за $m_n m + n \cdot m_n k = m_n(m+kn) = N \cdot \sum_{i=1}^{n+1} p_i$ операций, где $N = \prod_{i=1}^{n+1} p_i$.

Таким образом, построен быстрый алгоритм для матрицы Адамара порядка $N = mk^n$ вида (3.1). В общем случае матрица Адамара порядка $N = p_0 p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ строится следующим образом. Выбирается матрица Адамара H_0 порядка p_0, гиперкаркас $\{X_1, Y_1\}$ порядка p_1 и α_1 раз применяется формула (3.1). Затем построенная H_1 порядка $p_0 p_1^{\alpha_1}$ берется в качестве исходной, выбирается гиперкаркас $\{X_2, Y_2\}$ порядка p_2, по (3.1) строится H_2 порядка $p_0 p_1^{\alpha_1} \cdot p_2^{\alpha_2}$ и т. д. Легко видеть, что матрицу порядка $p_0 p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ можно также факторизовать вышеуказанным способом и что для этих матриц

$$D_n = N \cdot \sum_{i=1}^{k} \alpha_i p_i \leqslant N \cdot \sum_{i=0}^{k} p_i \log_{p_i} N. \tag{3.9}$$

Учитывая, что в разложении $H = \prod_{i=1}^{n+1} M_i$ каждая из матриц M может быть в свою очередь факторизована, можно получить более точное значение для (3.9)

$$D_n = N \cdot \sum_{i=0}^{k} \alpha_i \cdot C(p_i), \tag{3.10}$$

где $C(p_i)$—константы, зависящие от конструкции гиперкаркаса $\{X_i, Y$ порядка p_i.

В заключение приведем два примера.

Пример 1. Пусть матрицы

$$X = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & -1 & -1 & -1 & 0 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & -1 & -1 & 0 & 0 & 1 & 0 & 0 \\ -1 & -1 & -1 & 1 & -1 & 0 & 0 & 0 & 1 & 0 \\ -1 & -1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & -1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & -1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & -1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & -1 \end{bmatrix},$$

$$
Y=\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1\\
0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 1 & -1\\
0 & 0 & 0 & 0 & 0 & -1 & -1 & 1 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 1 & -1 & -1 & 1 & 0\\
0 & -1 & 1 & 1 & -1 & 0 & 0 & 0 & 0 & 0\\
-1 & 0 & -1 & 1 & 1 & 0 & 0 & 0 & 0 & 0\\
1 & -1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0\\
1 & 1 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\
-1 & 1 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}.
$$

Легко проверяется, что X и Y образуют 2-элементный гиперкаркас порядка 10. В результате факторизации матриц X и Y общее число операций в блоках X и Y (см. рис. 1) сократилось с 80 до 60, C (10) соответственно уменьшилось с 9 до 7. Граф факторизованных преобразований X и Y приведен на рис. 2.

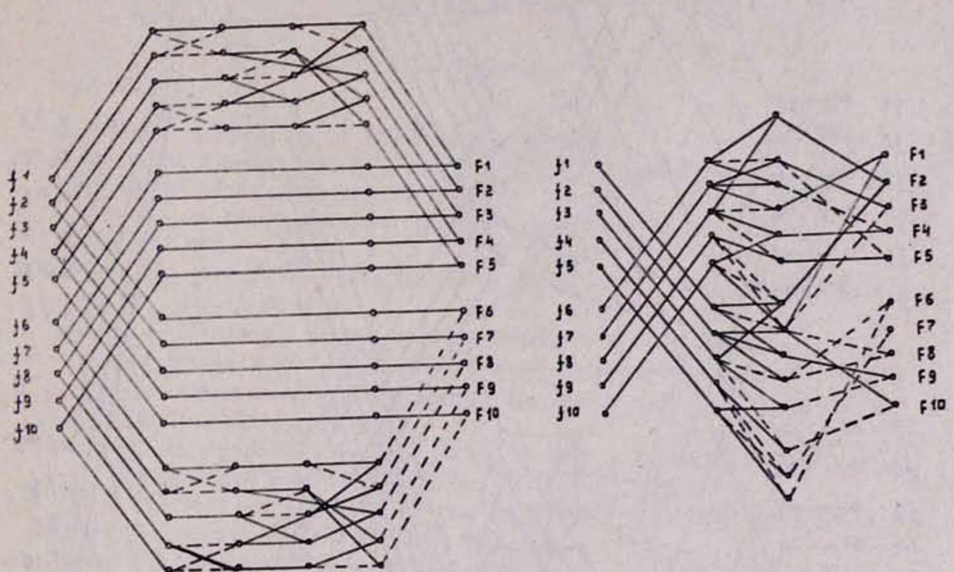

Рис. 2

Пример 2. Приведем полный алгоритм быстрого преобразования Адамара порядка 12, требующий 60 операций сложения и вычитания, для матрицы типа

$$H=X_1\otimes H_1+X_2\otimes H_2,$$

где

$$X_1=\begin{bmatrix} 1 & -1 & -1 & 1 & 0 & 0 \\ -1 & 1 & -1 & 0 & 1 & 0 \\ -1 & -1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 1 & 1 \\ 0 & 1 & 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 1 & 1 & -1 \end{bmatrix},\ X_2=\begin{bmatrix} 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & -1 & 0 & -1 \\ 0 & 0 & 0 & -1 & -1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

H_1 и H_2 любые матрицы Адамара порядка 2.

На рисунке 3 приведен граф полного алгоритма быстрого преобразования Адамара порядка 12 при

$$H_1=\begin{vmatrix} 1 & 1 \\ 1 & -1 \end{vmatrix} \quad H_2=\begin{vmatrix} 1 & -1 \\ -1 & -1 \end{vmatrix}.$$

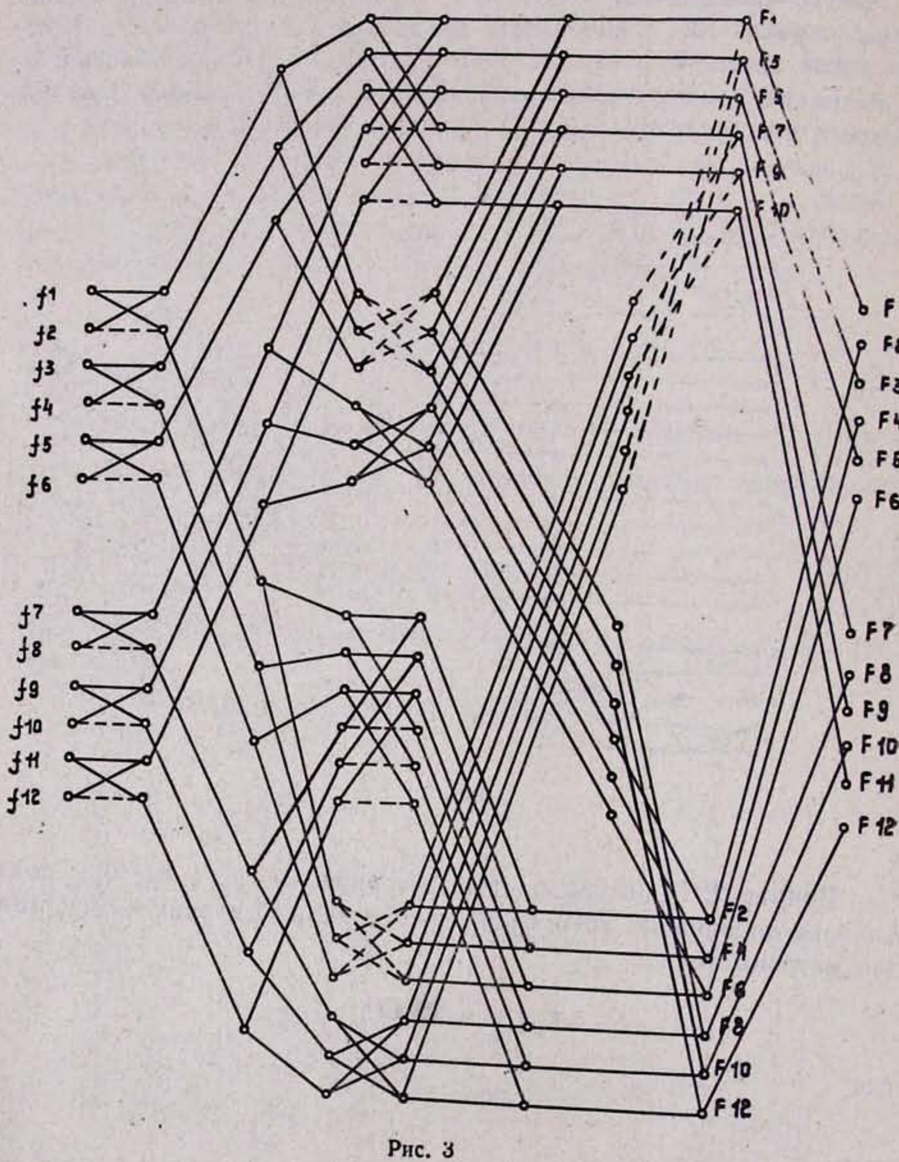

Рис. 3

Վ. Ս. ԱՂԱՅԱՆ, Ա.Կ. ՄԱԹԵՎՈՍՅԱՆ

ՀԱԴԱՄԱՐԻ ԱՐԱԳ ՁԵՎԱՓՈԽՈՒԹՅՈՒՆՆԵՐ

Ներկա աշխատանքում մտցվում է s-էլեմենտանոց հիպերկարկասի գաղափարը, որի միջոցով ստացվում է ռեկուրենտ բանաձև կառուցելու միաժամանակ S, $S=2, 4$ *հատ* $N=p_0 p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ *կարգի և* $H_i H_j^T + H_j H_i^T = 0$, $i \neq j$, $i, j = 1, 2, \ldots, s$ *պայմանին բավարարող Հադամարի մատրիցներ, որտեղ* $p_0, p_1, \ldots, p_k$, *մասնավորապես համընկնում են գոյություն ունեցող Վիլյամսոնի մատրիցների կարգերի հետ։*

Մշակված է Հադամարի արագ ձևափոխության ալգորիթմ, որը վերը նշված մատրիցների համար կատարում է Հադամարի ձևափոխությունը $N \cdot \sum_{i=0}^{k} \alpha_i p_i$ *գործողությունների միջոցով։*

Բերված ալգորիթմը համընկնում է.

ա) բավականաչափ հայտնի Ուոլշի արագ ձևափոխության ալգորիթմի հետ, երբ $p_0 = p_1 = \ldots = p_k = 2$*։*

բ) Պրատի ալգորիթմի հետ, երբ $p_0 = 12$, $p_1 = p_2 = \ldots = p_k = 2$*։*

ЛИТЕРАТУРА

1. *H. D. Frankel*. Applications of Walsh functions,. 1975.
2. *H. F. Harmuth*. Transmission of information by orthogonal functions. Springer-Verlag Berlin. Heidelberg. New York, 1970.
3. *N. J. Fine*. On the Walsh functions. Trans of the American Math. Soc., vol. 65, 1949, p. 372—414.
4. *N. J. Fine*. The generalized Walsh functions. Trans of the American Math. Soc., vol. 69, N1, 1950, p. 66—77.
5. *С. Качмаж, Г. Штайнгауз*. Теория ортогональных рядов. М. Физматгиз, 19, 1958.
6. *Ен*. Функции Уолша и код Грея. «Зарубежная радиоэлектроника», 1972, № 7.
7. *W. K. Pratt, J. Kvine* and *V. G. Andrews*. Hadamard transform image coding. Proc. IEEE, 1969, 57, p. 56—68.
8. *W. K. Pratt*, An algorithm for a Fast Hadamard Matrix Transform of order Twelve. IEEE transactions on computers, 1969, vol. C—18, 1131—1133.
9. *I. J. Good*. The interaction algorithm and praetical Fourier analysis. „J, Royal Stat. Soc." (London) 1958, v. B—20, p. 361—372.
10. *I. J. Good*. The relationship between two fast Fourier Transforms. „IEEE Trans.", 1971, v c—20, N3.
11. *Л. Рабинер, Б. Гоулд*. Теория и применение цифровой обработки сигналов, М., «Мир», 1978.
12. *Л. Сороко, Т. Стриж*. Спектральные вычисления на ЦВМ. Дубна. 1972.
13. *K. G. Beauchamp*. Walsh Functions and their applications. London and New York Academy 1975.
14. *V. C. Andrews, W. K. Pratt*. Digital image processing. Proceeding of the symposium on Applications of Walsh Functions, p. 183—194.
15. *Вишнер*. Специализированный цифровой процессор для обработки изображений «Зарубежная радиоэлектроника», 1972, № 11, стр. 42.
16. *К. Ф. Берковская, Г. К. Григорьев, С. Б. Гуревич, Б. Г. Подласкин, В. П. Поливко*. Преобразование Адамара как метод разложения сигнала в системах оптической обработки информации. В кн.: «Оптическая обработка информации». Л., 1978, стр. 135—147.

17. *К. Ф. Берковская, Г. К. Григорьев, Н. В. Кириллова, К. Л. Муратиков, Б. Г. Подласкин.* Возможности реализации адамаровского спектроанализатора на фотоприемном устройстве типа «маскон». В кн.: Оптическая обработка информации». Л., 1978, стр. 147—164.
18. *Холл.* Комбинаторика. М., 1970.
19. *С. С. Агаян, А. Г. Саруханян.* О гипотезе М. Плоткина. ДАН Арм. ССР, XVI, 1978, № 5.
20. *S. S. Agaiàn, A. G. Sarukhanian.* A note on the Construction of Hadamard matrices. Fourth International Congress of Cybernetics and Systems. Amsterdam 1978, August 22—25.
21. *V. C. Andrews, K. L. Gaspari.* A generalized technique for special analysis. IEEE Trans. On Computers 1970, N1. c—19, 16—25.
22. *W. D. Wallis, A. P. Street, I. S. Wallis.* Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Lecture Notes in Mathematics, Berlin Heidelberg New York, 1972.
23. *Н. С. Бахвалов.* Численные методы. М., 1975.