

МАТЕМАТИКА

УДК 519.1

А. Г. Саруханян

**Разложение матриц Адамара по ортогональным
(-1, +1)-векторам и алгоритм быстрого преобразования Адамара**

(Представлено академиком НАН Армении Г. Г. Хачатряном 2/VI 1996)

В работе исследуется задача разложения любой матрицы Адамара порядка n ($n \equiv 0 \pmod{4}$) по k -мерным ортогональным $(-1, +1)$ -векторам (k — степень двойки) и разработан алгоритм быстрого преобразования Адамара, требующий всего $n \log_2 k + n(n/k - 1)$ операций сложения.

Квадратная $(-1, +1)$ -матрица H_n порядка n называется матрицей Адамара, если выполняется условие

$$H_n H_n^T = H_n^T H_n = nI_n, \quad (1)$$

где T — знак транспонирования, I_n — единичная матрица порядка n .

Матрицу Адамара порядка n вида

$$H_n = \sum_{i=1}^k v_i \otimes A_i, \quad (2)$$

где v_i — ортогональные $(-1, +1)$ -векторы длины k , $\otimes$ — кронекеровское произведение, а A_i — $(0, -1, +1)$ -матрицы, будем называть $A(n, k)$ -матрицей.

Теорема 1. Матрица H_n порядка n является $A(n, k)$ -матрицей тогда и только тогда, когда существуют $(0, -1, +1)$ -матрицы A_i , $i=1, 2, \dots, k$, размерности $n \times n/k$, удовлетворяющие следующим условиям:

$$A_i \otimes A_j = 0, \quad i \neq j, \quad i, j = 1, 2, \dots, k;$$

$$\sum_{i=1}^k A_i \text{ является } (-1, +1)\text{-матрицей};$$

$$\sum_{i=1}^k A_i A_i^T = \frac{n}{k} I_k; \quad (3)$$

$$A_i^T A_j = 0, \quad i \neq j, \quad i, j = 1, 2, \dots, k;$$

$$A_i^T A_i = \frac{n}{k} I_{n/k}, \quad i = 1, 2, \dots, k;$$

где $*$ — адамарово произведение ⁽¹⁾.

Приведем некоторые следствия, вытекающие из этой теоремы.

Следствия 1. Для любой матрицы Адамара порядка n существуют $A(2^{i-1}n, 2^i)$ -матрицы, $i = 1, 2, \dots$

2. Для любых натуральных чисел n и k ($k \leq n$) существует $A(2^n, 2^k)$ -матрица.

3. Если существуют $A(n, k)$ - и $A(m, r)$ -матрицы, то существуют также $A(mn, k)$ -, $A(mn, r)$ - и $A(mn, kr)$ -матрицы.

Теорема 2. Пусть H_n — $A(n, k)$ -матрица. Тогда $n \equiv 0 \pmod{2k}$.

Отметим, что обратное утверждение неверно, т.е. из существования любой матрицы Адамара порядка n , $n \equiv 0 \pmod{2k}$, не вытекает существование $A(n, k)$ -матрицы, $k > 2$.

Теорема 3. Пусть существует $A(n, k)$ -матрица и матрица Адамара порядка m ($m \equiv 0 \pmod{k}$). Тогда существует также матрица Адамара порядка mn/k .

Теорема 4. Пусть существует $A(n, k)$ -матрица и матрица Адамара порядка m . Тогда для любого четного числа r , для которого $m, n \equiv 0 \pmod{r}$, существуют $(0, -1, +1)$ -матрицы $B_{i,j}$, $i = 1, 2, \dots, r/2$,

$j = 1, 2, \dots, k$, размерности $\frac{mn}{r} \times \frac{mn}{kr}$, удовлетворяющие следующим условиям:

$$B_{i,j} * B_{i,j} = 0, \quad i \neq j, \quad i, j = 1, 2, \dots, k, \quad i = 1, 2, \dots, \frac{r}{2};$$

$$\sum_{i=1}^k B_{i,j} - (-1, +1)\text{-матрица}, \quad i = 1, 2, \dots, \frac{r}{2}; \quad (4)$$

$$\sum_{i=1}^k B_{i,j} B_{j,i}^T = 0, \quad i \neq j, \quad i, j = 1, 2, \dots, \frac{r}{2};$$

$$\sum_{i=1}^{r/2} \sum_{j=1}^k B_{i,j} B_{i,j}^T = \frac{mn}{2k} I_{\frac{mn}{r}}.$$

Из этой теоремы вытекают следующие следствия.

Следствие 4 (1.3). Если существуют матрицы Адамара порядка m и n , то существует также матрица Адамара порядка $mn/2$.

Следствие 5 (1.4). Если существуют матрицы Адамара порядка n_i , $i=1,2,3,4$, то существует также матрица Адамара порядка $\frac{n_1 n_2 n_3 n_4}{16}$.

Прямое и обратное преобразования Адамара вектора-столбца $f = \{f_i\}_{i=1}^n$ соответственно определяются формулами (5)

$$F = \frac{1}{n} H_n f, \quad f = H_n^T F, \quad (5)$$

где H_n — матрица Адамара порядка n .

Для преобразования Уолша — Адамара, при котором в (5) H_n является матрицей Адамара порядка $n=2^k$, упорядоченной по Уолшу (а также по Пэли (5)), разработан быстрый алгоритм вычисления F , требующий всего $n \log_2 n$ операций сложения.

Пусть $H_n = v_1 \times A_1 + v_2 \times A_2 + \dots + v_k \times A_k$ является $A(n,k)$ -матрицей. Согласно теореме 1 матрицы A_i удовлетворяют условиям (3).

Преобразуемый вектор f представим в виде

$$f = \sum_{i=1}^{n/k} x_i \times P_i,$$

где $x_i = \{f_{k(i-1)+j}\}_{j=1}^k$, а P_i — вектор-столбец длины n/k , i -ый элемент которого равен 1, а остальные элементы — нули.

Прямое преобразование Адамара принимает вид (нормировочный коэффициент $1/n$ опускаем)

$$H_n f = \sum_{i=1}^k \sum_{j=1}^{n/k} v_i x_j \times A_i P_j. \quad (6)$$

Рассмотрим часть суммы (6) следующего вида:

$$v_i x_j \times A_i P_j + v_2 x_j \times A_2 P_j + \dots + v_k x_j \times A_k P_j. \quad (7)$$

Из условия (3) и определения матрицы P_i вытекает, что $A_i P_j$ — j -ый столбец матрицы A_i , который имеет n/k ненулевых элементов. Произведение $v_i x_j \times A_i P_j$ означает, что i -ый элемент преобразования Уолша — Адамара вектора x_j помещен в n/k местах j -ого столбца матрицы A_i . Следовательно, для вычисления всех элементов n -мерного вектора (7) требуется $k \log_2 k$ операций сложения и n пере-

сылка. Заметим, что выражение (6) включает n/k векторов вида (7). А это означает, что для преобразования Адамара вида (6) требуется

$$D_1 = n \log_2 k + n \left(\frac{n}{k} - 1 \right) \quad (8)$$

операций сложения.

Заметим, что при $n=k$ оценка (8) совпадает с известной классической оценкой быстрого преобразования Уолша — Адамара. Однако в этом случае n должно являться степенью двойки.

Институт проблем информатики и автоматизации

Национальной академии наук Армении и

Ереванского государственного университета

Հ. Գ. ՍԱՐԴԻԽԱՆՅԱՆ

Հաղամարի մատրիցների վերլուծությունը $(-1, +1)$ -վեկտորների միջոցով և Հաղամարի արագ ձևափոխության ալգորիթ

Աշխատանքում ուսումնասիրվում է k չափանի (k -ն ունի երկուսի աստիճանի տեսք) $(-1, +1)$ -վեկտորների միջոցով $n=O(\bmod 4)$ տեսքի կարգ ունեցող Հաղամարի մատրիցների վերլուծության խնդիրը և մշակված է Հաղամարի արագ ձևափոխության ալգորիթը, որը պահանջում է ընդամենը $n \log_2 k + n(n/k - 1)$ գումարման գործողություն:

ЛИТЕРАТУРА —ԳՐԱԿԱՆՈՒԹՅՈՒՆ

¹ J.Seberry, M.Yamada, Contemporary Design Theory: A Collection of Surveys. Wiley-Interscience Series in Discrete Mathematics. John Wiley, N.Y., 1992. ² S.S.Agalan, A.G.Sarukhanian, Math. Notes, v.30, №1, p.603-617 (1981). ³ S.S.Agalan, Lecture Notes in Mathematics, Springer-Verlag, Berlin, v.1168 (1985). ⁴ R.Graiger, J.Seberry, X.-M.Zhang, J. Combin. Theory, ser. A, v.59, p.318-320 (1992). ⁵ N.Ahmed, K.R.Rao, Orthogonal Transforms for Digital Signal Processing, Springer-Verlag, Berlin, Heidelberg, N.Y., 1975.