

БЫСТРЫЙ АЛГОРИТМ ПРОИЗВЕДЕНИЯ ДВУХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЕЛ

*Работа выполнена при финансовой государственной поддержке ведущих научных школ РФ,
грант № 96-15-96095 «Исследования по комплексному анализу и алгебре».*

В статье рассматривается быстрый алгоритм произведения двух элементов алгебры гиперкомплексных чисел размерности $N=2^n$, где n – натуральное число. Указанная размерность дает возможность использовать ортогональные матрицы Уолша–Адамара, что позволяет существенно повысить эффективность алгоритма.

Алгебры гиперкомплексных чисел (в частности, двойных и дуальных чисел, кватернионов, алгебра Кэли) находят применение в различных разделах математики и ее приложений [1–4].

1. Матрицы Уолша–Адамара $H(n)$ порядка $N=2^n$ определяются по следующей рекуррентной формуле [5]:

$$H(k) = \begin{bmatrix} H(k-1) & H(k-1) \\ H(k-1) & -H(k-1) \end{bmatrix}, \quad k=1, 2, \dots, n,$$

причем $H(0)=1$. Тогда, например,

$$H(1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad H(2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Отметим следующие свойства матриц Уолша–Адамара [5]:

1) $H(k)$ – симметрическая матрица;
2) $H(k)$ – «почти ортогональная» матрица в смысле следующего равенства: $H(k)^T \cdot H(k) = 2^k E(k)$, где $E(k)$ – единичная матрица порядка 2^k ;

$$3) H^{-1}(k) = \frac{1}{2^k} H(k).$$

Для изложения алгоритма необходимо обобщение кронекеровского произведения матриц. Под кронекеровским произведением матрицы A размера $m \times n$ на матрицу B будем понимать матрицу C размера $mk \times nl$ вида

$$C = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \dots & \dots & \dots & \dots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix}.$$

Будем обозначать кронекеровское произведение C матриц A и B так: $C=A \otimes B$. Обозначим строки матрицы B через $B_1, B_2, \dots, B_k$, а столбцы – $B^{(1)}, B^{(2)}, \dots, B^{(l)}$. Назовем кронекеровским произведением по строкам матриц A и B матрицу C' вида

$$C' = \begin{bmatrix} A \otimes B_1 \\ A \otimes B_2 \\ \dots \\ A \otimes B_k \end{bmatrix}.$$

В дальнейшем будем обозначать матрицу C' так:

$$C' = A \bar{\otimes} B.$$

Заметим, что аналогично можно определить кронекеровское произведение матриц A и B по столбцам так:

$$C'' = A \bar{\otimes} B = [A \otimes B^{(1)} \quad A \otimes B^{(2)} \quad \dots \quad A \otimes B^{(l)}].$$

В [6] были изучены некоторые свойства матриц C' и C'' . Отметим два из них, которые будут использованы в дальнейшем.

Теорема 1 [6]. Пусть $C=A \otimes B$, $C'=A \bar{\otimes} B$ и $C''=A \bar{\otimes} B$. Тогда матрица C' (C'') приводится к матрице C перестановкой строк (столбцов).

Теорема 2 [6]. Матрицу Уолша–Адамара $H(n)$ можно представить в виде

$$H(n) = [E(n-1) \bar{\otimes} H(1)]^n,$$

где $E(n-1)$ – единичная матрица порядка 2^{n-1} ,

$$H(1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Пример.

$$H(3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}.$$

Как видно из примера, теорема 2 позволяет представить матрицу Уолша–Адамара, которая является плотно заполненной матрицей, в виде степени разреженной матрицы.

2. Перейдем теперь к алгебрам гиперкомплексных чисел. Пусть $\mathbb{H} = \mathbb{R} + i\mathbb{R} + j\mathbb{R} + k\mathbb{R}$, где $1, i, j, k$ – базис алгебры $\mathbb{H}$ с таблицей умножения

	1	i	j	k
1	1	i	j	k
i	i	-1	k	-j
j	j	-k	-1	i
k	k	j	-i	-1

Пусть q_1, q_2, q_3 – кватернионы такие, что $q_1 \cdot q_2 = q_3$, где

$$q_1 = a_0 + a_1 i + a_2 j + a_3 k,$$

$$q_2 = b_0 + b_1 i + b_2 j + b_3 k,$$

$$q_3 = c_0 + c_1 i + c_2 j + c_3 k.$$

В [7] был предложен алгоритм умножения кватернионов. Используем теорему 2 для модификации это-

го алгоритма и его обобщения на другие алгебры гиперкомплексных чисел.

Имеем согласно [7]

$$-[c_0 | c_1 | c_2 | c_3] = \frac{1}{4} [n_0 p_0 | n_1 p_1 | n_2 p_2 | n_3 p_3] A - 2[a_0 b_0 | a_3 b_2 | a_2 b_1 | a_1 b_3],$$

где $[n_0 | n_1 | n_2 | n_3] = [a_0 | a_1 | a_2 | a_3] A$,

$$[p_0 | p_1 | p_2 | p_3] = [b_0 | b_1 | b_2 | b_3] A,$$

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

Поясним идею обобщения и улучшения этого алгоритма для других алгебр гиперкомплексных чисел на примере алгебры псевдокватернионов.

Пусть $\mathcal{L}$ – алгебра псевдокватернионов, т.е. четырехмерная вещественная алгебра $\mathcal{L} = \mathcal{R} + i\mathcal{R} + e\mathcal{R} + f\mathcal{R}$, где $1, i, e, f$ – базис алгебры $\mathcal{L}$ с таблицей умножения

	1	i	e	f
1	1	i	e	f
i	i	-1	f	-e
e	e	-f	1	-i
f	f	e	i	1

Если $z_1, z_2 \in \mathcal{L}$, то $z_1 \cdot z_2 = z_3 \in \mathcal{L}$, где $z_1 = a_0 + a_1 i + a_2 e + a_3 f$, $z_2 = b_0 + b_1 i + b_2 e + b_3 f$, $z_3 = c_0 + c_1 i + c_2 e + c_3 f$. Тогда из равенства $(a_0 + a_1 i + a_2 e + a_3 f)(b_0 + b_1 i + b_2 e + b_3 f) = c_0 + c_1 i + c_2 e + c_3 f$

с учетом таблицы умножения для базиса $\mathcal{L}$ получаем матричное равенство

$$[a_0 \ a_1 \ a_2 \ a_3] B = [c_0 \ c_1 \ c_2 \ c_3],$$

$$\text{где } B = \begin{bmatrix} b_0 & b_1 & b_2 & b_3 \\ -b_1 & b_0 & -b_3 & b_2 \\ b_2 & -b_3 & b_0 & -b_1 \\ b_3 & b_2 & b_1 & b_0 \end{bmatrix}.$$

Матрицу B можно представить в виде $B = L_1 - 2L_2$, где

$$L_1 = \begin{bmatrix} b_0 & b_1 & b_2 & b_3 \\ b_1 & b_0 & b_3 & b_2 \\ b_2 & b_3 & b_0 & b_1 \\ b_3 & b_2 & b_1 & b_0 \end{bmatrix}, L_2 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ b_1 & 0 & b_3 & 0 \\ 0 & b_3 & 0 & b_1 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \quad (115)$$

Согласно [7] матрицу L_1 можно представить в виде

$$L_1 = A \begin{bmatrix} p_0 & 0 & 0 & 0 \\ 0 & p_1 & 0 & 0 \\ 0 & 0 & p_2 & 0 \\ 0 & 0 & 0 & p_3 \end{bmatrix} A^{-1},$$

где $A^{-1} = \frac{1}{4} A$, $[p_0 | p_1 | p_2 | p_3] = [b_0 | b_1 | b_2 | b_3] A$.

$$\text{Тогда } [a_0 | a_1 | a_2 | a_3] A \begin{bmatrix} p_0 & 0 & 0 & 0 \\ 0 & p_1 & 0 & 0 \\ 0 & 0 & p_2 & 0 \\ 0 & 0 & 0 & p_3 \end{bmatrix} A^{-1} -$$

$$-2[a_0 | a_1 | a_2 | a_3] L_2.$$

Обозначая $[a_0 | a_1 | a_2 | a_3] A = [n_0 | n_1 | n_2 | n_3]$, получим

$$[c_0 | c_1 | c_2 | c_3] = [n_0 | n_1 | n_2 | n_3] \begin{bmatrix} p_0 & 0 & 0 & 0 \\ 0 & p_1 & 0 & 0 \\ 0 & 0 & p_2 & 0 \\ 0 & 0 & 0 & p_3 \end{bmatrix} \left(\frac{1}{4} A \right) - 2[a_1 b_1 | a_2 b_3 | a_1 b_3 | a_2 b_1] =$$

$$= \frac{1}{4} [n_0 p_0 | n_1 p_1 | n_2 p_2 | n_3 p_3] A - 2[a_1 b_1 | a_2 b_3 | a_1 b_3 | a_2 b_1].$$

Подобную схему вычислений можно организовать для алгебр гиперкомплексных чисел размерности 2^n , у которых в таблице умножения базиса структурные константы равны ± 1 . Матрица B для таких алгебр представима в виде $B = L_1 - 2L_2$, где матрица L_1 имеет тот же вид, что для алгебр кватернионов и псевдокватернионов, а матрица L_2 подбирается в зависимости от алгебры.

Данная схема организации вычисления произведения позволяет уменьшить число умножений за счет увеличения числа сложений. Оказывается, что применение теоремы 2 позволяет уменьшить и число сложений.

Заметим, что $A = H(2)$, и, следовательно, по теореме 2 имеем

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}^2.$$

В изложенной выше схеме вычислений умножение строки на матрицу A равносильно выполнению 12 операций сложения. Всего в алгоритме таких умножений три, тогда они дают 36 операций сложения.

В то же время при представлении матрицы A в виде квадрата разреженной матрицы умножение на A равносильно выполнению 8 операций сложения (умножение строки на разреженную матрицу дает 4 операции сложения, еще одно умножение на эту же матрицу – 4 операции сложения). Всего при таком представлении матрицы A три умножения строк на матрицу A дают 24 операции сложения.

Итак, вычисление произведения кватернионов или псевдокватернионов обычным способом требует 16 операций умножения вещественных чисел и 12 операций сложения. При использовании изложенной выше схемы вычислений без применения теоремы 2 требуется выполнить 8 операций умножения вещественных чисел и 40 операций сложения. Наконец, при использовании схемы вычислений с применением теоремы 2 необходимо выполнить 8 операций умножения вещественных чисел и 28 операций сложения (умножения на абсолютные константы $1/4$ и 2 , присутствующие в данном алгоритме, не учитываются).

3. Естественно предположить, что с ростом размерности алгебры выигрыш в числе операций за счет использования разреженной матрицы будет расти. Рассмотрим теперь восьмеричную вещественную алгебру Кэли $\mathcal{P} = \mathcal{R} + i_1 \mathcal{R} + i_2 \mathcal{R} + \dots + i_7 \mathcal{R}$, где $1, i_1, i_2, \dots, i_7$ – базис алгебры $\mathcal{P}$ с таблицей умножения

	1	i_1	i_2	i_3	i_4	i_5	i_6	i_7
1	1	i_1	i_2	i_3	i_4	i_5	i_6	i_7
i_1	i_1	-1	i_3	$-i_2$	i_5	$-i_4$	$-i_7$	i_6
i_2	i_2	$-i_3$	-1	i_1	i_6	i_7	$-i_4$	$-i_5$
i_3	i_3	i_2	$-i_1$	-1	i_7	$-i_6$	i_5	$-i_4$
i_4	i_4	$-i_5$	$-i_6$	$-i_7$	-1	i_1	i_2	i_3
i_5	i_5	i_4	$-i_7$	i_6	$-i_1$	-1	$-i_3$	i_2
i_6	i_6	i_7	i_4	$-i_5$	$-i_2$	i_3	-1	$-i_1$
i_7	i_7	$-i_6$	i_5	i_4	$-i_3$	$-i_2$	i_1	-1

Если $W_1, W_2 \in P$, то $W_1 \cdot W_2 = W_3 \in P$,
где $W_1 = a_0 + a_1 i_1 + a_2 i_2 + \dots + a_7 i_7$,
 $W_2 = b_0 + b_1 i_1 + b_2 i_2 + \dots + b_7 i_7$,
 $W_3 = c_0 + c_1 i_1 + c_2 i_2 + \dots + c_7 i_7$.

Тогда из равенства

$(a_0 + a_1 i_1 + a_2 i_2 + \dots + a_7 i_7) \times$
 $\times (b_0 + b_1 i_1 + b_2 i_2 + \dots + b_7 i_7) = c_0 + c_1 i_1 + c_2 i_2 + \dots + c_7 i_7$
с учетом таблицы умножения для базиса P получаем матричное равенство

$$[a_0 | a_1 | a_2 | \dots | a_7] B = [-c_0 | c_1 | c_2 | \dots | c_7],$$

$$\text{где } B = \begin{bmatrix} -b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ b_1 & b_0 & -b_3 & b_2 & -b_5 & b_4 & b_7 & -b_6 \\ \cdot & b_3 & b_0 & -b_1 & -b_6 & -b_7 & b_4 & -b_5 \\ \cdot & -b_2 & b_1 & b_0 & -b_7 & b_6 & -b_5 & b_4 \\ \cdot & b_5 & b_6 & b_7 & b_0 & -b_1 & -b_2 & -b_3 \\ \cdot & -b_4 & b_7 & -b_6 & b_1 & b_0 & b_3 & -b_2 \\ \cdot & -b_7 & -b_4 & b_5 & b_2 & -b_3 & b_0 & b_1 \\ b_7 & b_6 & -b_5 & -b_4 & b_3 & b_2 & -b_1 & b_0 \end{bmatrix}.$$

Матрицу B можно представить в виде $B = L_1 - 2L_2$, где

$$L_1 = \begin{bmatrix} b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 \\ b_1 & b_0 & b_3 & b_2 & b_5 & b_4 & b_7 & b_6 \\ b_2 & b_3 & b_0 & b_1 & b_6 & b_7 & b_4 & b_5 \\ b_3 & b_2 & b_1 & b_0 & b_7 & b_6 & b_5 & b_4 \\ b_4 & b_5 & b_6 & b_7 & b_0 & b_1 & b_2 & b_3 \\ b_5 & b_4 & b_7 & b_6 & b_1 & b_0 & b_3 & b_2 \\ b_6 & b_7 & b_4 & b_5 & b_2 & b_3 & b_0 & b_1 \\ b_7 & b_6 & b_5 & b_4 & b_3 & b_2 & b_1 & b_0 \end{bmatrix},$$

$$L_2 = \begin{bmatrix} b_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & b_3 & 0 & b_5 & 0 & 0 & b_6 \\ 0 & 0 & 0 & b_1 & b_6 & b_7 & 0 & 0 \\ 0 & b_2 & 0 & 0 & b_7 & 0 & b_5 & 0 \\ 0 & 0 & 0 & 0 & 0 & b_1 & b_2 & b_3 \\ 0 & b_4 & 0 & b_6 & 0 & 0 & 0 & b_2 \\ 0 & b_7 & b_4 & 0 & 0 & b_3 & 0 & 0 \\ 0 & 0 & b_5 & b_4 & 0 & 0 & b_1 & 0 \end{bmatrix}.$$

Тогда

$$L_1 = H(3) \begin{bmatrix} p_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & p_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \cdot & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdot & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdot & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \cdot & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdot & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & p_7 \end{bmatrix} H^{-1},$$

где

$$H^{-1}(3) = \frac{1}{8} H(3), [p_0 | p_1 | \dots | p_7] = [b_0 | b_1 | \dots | b_7] H(3).$$

Продолжая подобно как для кватернионов и для псевдокватернионов, получим

$$[-c_0 | c_1 | c_2 | \dots | c_7] = \frac{1}{8} [n_0 p_0 | n_1 p_1 | n_2 p_2 | \dots | n_7 p_7] H_h(3) -$$

$$-2[a_0 b_0 | a_3 b_2 + a_5 b_4 + a_6 b_7 | a_1 b_3 + a_6 b_4 + a_7 b_5 | a_2 b_1 +$$

$$+ a_5 b_6 + a_7 b_4 | a_1 b_5 + a_2 b_6 + a_3 b_7 | a_2 b_7 + a_4 b_1 +$$

$$a_6 b_3 | a_3 b_5 + a_4 b_2 + a_7 b_1 | a_1 b_6 + a_4 b_3 + a_5 b_2].$$

Сравним число операций при обычном умножении чисел Кэли, умножении по алгоритму без применения теоремы 2 и по алгоритму с применением разреженного представления по теореме 2.

При обычном умножении чисел Кэли используются 64 вещественных умножения и 56 сложений, при умножении по алгоритму без применения теоремы 2 – соответственно 30 вещественных умножений и 190 сложений. А при умножении по алгоритму с применением разреженного представления используются 30 вещественных умножений и 46 операций сложения.

Таким образом, используя факторизацию матриц Уолша–Адамара с применением обобщенного кронекерского произведения матриц, удастся существенно повысить эффективность алгоритма.

ЛИТЕРАТУРА

1. Арнальд В.И. Геометрия сферических кривых и алгебра кватернионов // Успехи матем. наук. 1995. Т. 50, вып. 1. С. 4–68.
2. Манин Ю.И. Калибровочные поля и комплексная геометрия. М.: Наука, 1984.
3. Кантор И.Л., Солодовников А.С. Гиперкомплексные числа. М.: Наука, 1973.
4. Яглом И.М. Комплексные числа и их применение в геометрии. М.: Наука, 1976.
5. Ахмед Н., Рао К. Ортогональные преобразования при обработке цифровых сигналов. М.: Связь, 1980.
6. Быков В.И., Кожуховский А.Д., Росошек С.К., Литвин А.И., Иванова В.А. Обобщенные кронекеровские произведения матриц и их применения // Электронное моделирование. 1991. Т. 13, № 5. С. 14–19.
7. Макаров О.М. Алгоритмы умножения двух кватернионов // Журн. вычислит. матем. и матем. физики. 1977. Т. 17, № 6. С. 1574–1575.

Статья представлена кафедрой алгебры механико-математического факультета Томского государственного университета, поступила в научную редакцию «Математика» 24 декабря 1999 г.