

ОБОБЩЕННЫЕ КРОНЕКЕРОВСКИЕ ПРОИЗВЕДЕНИЯ МАТРИЦ

Рассматриваются свойства обобщенных кронекеровских произведений (ОКП) матриц, в сравнении с обычными кронекеровскими произведениями матриц. Используя эти свойства, указывается ряд факторизаций матриц ОДП, которые удобны для реализации их в реальном режиме времени и в векторном режиме на вычислительных устройствах типа ОКМД.

Пусть A и B – матрицы размерности $m \times n$ и $k \times r$ соответственно над коммутативным кольцом R :

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \dots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}; \quad B = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{1r} \\ b_{21} & b_{22} & \dots & b_{2r} \\ \vdots & \vdots & \dots & \vdots \\ b_{k1} & b_{k2} & \dots & b_{kr} \end{bmatrix}.$$

Определение 1. Кронекеровским произведением матриц A и B называется матрица C размерности $mk \times nr$ вида

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

Обозначим строки матрицы B через $B_1, B_2, \dots, B_k$, а столбцы – $B^1, B^2, \dots, B^r$.

Определение 2. Кронекеровским произведением матриц A и B по строкам называется матрица C вида

$$C = A \bar{\otimes} B = \begin{bmatrix} A \otimes B_1 \\ A \otimes B_2 \\ \vdots \\ A \otimes B_k \end{bmatrix}.$$

Определение 3. Кронекеровским произведением матриц A и B по столбцам называется матрица C вида $C = A \tilde{\otimes} B = [A \otimes B^1 A \otimes B^2 \dots A \otimes B^r]$.

В дальнейшем для упрощения выкладок будем рассматривать только квадратные матрицы. Пусть

$$A = (a_{ri}), \quad B = (b_{sj}),$$

где

$$r, i \in \{1, 2, \dots, m\}, \quad s, j \in \{1, 2, \dots, n\},$$

$$C = A \bar{\otimes} B = (c_{kl}),$$

$$C' = A \tilde{\otimes} B = (c'_{k'l'}),$$

$$C'' = A \otimes B = (c''_{k''l''}).$$

Из определений 1 – 3 установим явный вид элементов матриц C, C', C'' :

$$c_{kl} = a_{ri} b_{sj},$$

где $k = (s-1)m + r, l = (i-1)n + j$;

$$c'_{k'l'} = a_{ri} b_{sj},$$

где $k' = (r-1)n + s, l' = (j-1)m + i$;

$$c''_{k''l''} = a_{ri} b_{sj},$$

где $k'' = (r-1)n + s, l'' = (i-1)n + j$.

Теорема 1. Пусть

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

Матрица C'' приводится к матрице C (C') перестановкой строк (столбцов).

Доказательство. Покажем, что существует перестановка строк матрицы C'' , которая приводит ее к матрице C (для матриц C' и C доказательство аналогично). Заметим сразу, что порядки матриц C и C'' равны mn . Сравним явный вид элементов этих матриц. Легко заметить, что произвольный элемент $a_{ri} b_{sj}$ матрицы C'' , находящийся в этой матрице на месте (k'', l'') , в матрице C оказывается на месте (k, l) , где

$$k'' = (r-1)n + s, k = (s-1)m + r,$$

$$l'' = (i-1)n + j, l = (i-1)n + j.$$

Так как $l = l''$, то номер столбца элемента $a_{ri} b_{sj}$ в матрице C'' равен номеру столбца этого же элемента в матрице C . Рассмотрим отображение $\varphi: \{1, \dots, mn\} \rightarrow \{1, \dots, mn\}$, которое ставит в соответствие номеру строки элемента $a_{ri} b_{sj}$ в матрице C'' номер строки этого элемента в матрице C согласно следующей формуле $\varphi: k'' \rightarrow k$, где $k'' = (s-1)n + r$, $k = (r-1)n + s$. Непосредственно проверяется, что φ – инъективное отображение и, следовательно, φ – биекция (так как φ – отображение конечного множества в себя). Это означает, что φ есть искомая перестановка строк матрицы C'' , приводящая к матрице C .

Рассмотрим некоторые свойства обобщенных кронекеровских произведений матриц:

$$1. \quad \alpha A \bar{\otimes} B = \bar{\alpha} A \otimes B = \alpha (A \bar{\otimes} B), \quad (a)$$

$$\alpha A \tilde{\otimes} B = A \tilde{\otimes} \alpha B = \alpha (A \tilde{\otimes} B); \quad (б)$$

$$2. \quad A \bar{\otimes} (B + C) = \bar{\alpha} A \otimes B + \bar{\alpha} A \otimes C, \quad (a)$$

$$A \tilde{\otimes} (B + C) = A \tilde{\otimes} B + A \tilde{\otimes} C; \quad (б)$$

$$3. \quad (A + B) \bar{\otimes} C = \bar{\alpha} A \otimes C + \bar{\alpha} B \otimes C, \quad (a)$$

$$(A + B) \tilde{\otimes} C = A \tilde{\otimes} C + B \tilde{\otimes} C. \quad (б)$$

Свойства 1 – 3 следуют из определений обобщенных кронекеровских произведений матриц.

$$4. \quad A \bar{\otimes} B = B \tilde{\otimes} A, \quad (a)$$

$$A \tilde{\otimes} B = B \bar{\otimes} A; \quad (б)$$

$$5. \quad A \otimes (B \otimes C) = (A \otimes B) \otimes C, \quad (a)$$

$$A \tilde{\otimes} (B \tilde{\otimes} C) = (A \tilde{\otimes} B) \tilde{\otimes} C; \quad (б)$$

$$6. \quad (A \otimes B)^T = A^T \otimes B^T, \quad (a)$$

$$(A \tilde{\otimes} B)^T = A^T \tilde{\otimes} B^T. \quad (б)$$

Для доказательства свойств кронекеровских произведений матриц введены перестановки P и F следующим образом. Определим

$$P(m, n) = E_m \otimes E_n; F(m, n) = E_m \tilde{\otimes} E_n,$$

где E_m и E_n – единичные матрицы порядка m и n соответственно. Будем пользоваться в основном перестановками вида P . Пусть матрица A имеет порядок m , а матрица B имеет порядок n . Тогда перестановку P будем обозначать $P(N, n)$, где $N = mn$. Тогда каждой перестановке $P(N, n)$ соответствует перестановочная матрица. Ее будем обозначать также (если это не приводит к недоразумению). Например, пусть $N = 4$, а $n = 2$, тогда

$$P(4, 2) = E_2 \otimes E_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix};$$

$$P(4, 2)x = \begin{bmatrix} x_0 \\ x_2 \\ x_1 \\ x_3 \end{bmatrix}.$$

Заметим, что

$$F(m, n) = P^T(m, n); PP^T = E; P^T = P^{-1};$$

$$P(A \otimes B) = A \otimes B; (A \otimes B)P^T = A \tilde{\otimes} B.$$

Очень важное свойство кронекеровских произведений матриц $(A \otimes B)(C \otimes D) = AC \otimes BD$ для обобщенных кронекеровских произведений матриц не выполняется. Но, тем не менее, следующие свойства для введенных обобщенных кронекеровских произведений матриц выполняются.

Теорема 2. Если матрица A имеет порядок M , матрица B – порядок N , а векторы $\bar{a}$ и $\bar{b}$ длиной M и N соответственно, то тогда

$$a) \quad (A \otimes B)(\bar{a} \otimes \bar{b}) = A\bar{a} \otimes B\bar{b};$$

$$б) \quad (A \otimes B)(\bar{a} \otimes \bar{b}) = A\bar{a} \otimes B\bar{b} = B\bar{b} \otimes A\bar{a};$$

$$в) \quad (A \tilde{\otimes} B)(\bar{a} \tilde{\otimes} \bar{b}) = B\bar{b} \otimes A\bar{a} = A\bar{a} \otimes B\bar{b}.$$

Используя теорему 2 и введенные выше перестановки, можно доказать теорему.

Теорема 3. Пусть Матрицы A и C – матрицы порядка L , а матрицы B и D – матрицы порядка M , тогда:

$$a) \quad (A \otimes B)(C \otimes D) = AC \otimes BD;$$

$$б) \quad (A \otimes B)(C \otimes D) = (AC \otimes BD);$$

$$в) \quad (A \otimes B)(C \tilde{\otimes} D) = AC \tilde{\otimes} BAD;$$

$$г) \quad (A \tilde{\otimes} B)(C \tilde{\otimes} D) = AC \otimes BD.$$

$$е) \quad (A \otimes B)(C \tilde{\otimes} D) = BD \otimes AC.$$

Доказательство. а) Пусть векторы $\bar{a}$ и $\bar{b}$ имеют размерности L и M соответственно. Тогда

$$(A \otimes B)(C \otimes D)(\bar{a} \otimes \bar{b}) = (A \otimes B)(C\bar{a} \otimes D\bar{b}) = AC\bar{a} \otimes BD\bar{b}.$$

Ввиду произвольного выбора векторов $\bar{a}$ и $\bar{b}$ утверждение а) доказано.

б) Обозначим $N = L * M$. Тогда

$$(A \otimes B)(C \otimes D) = P(N, M)(A \otimes B)(C \otimes D) = P(N, M)(AC \otimes BD) = AC \otimes BD.$$

$$в) \quad (A \otimes B)(C \tilde{\otimes} D) = (A \otimes C)(B \otimes D)P(N, L) = (AC \otimes BD)P(N, L) = (AC \tilde{\otimes} BD).$$

$$г) \quad (A \tilde{\otimes} B)(C \tilde{\otimes} D) = (A \otimes C)P(N, L)P(N, M)(B \otimes D).$$

Как будет показано ниже

$$P(N, L)P(N, M) = P(N, N) = E_n$$

– единичной перестановке. Поэтому

$$(A \tilde{\otimes} B)(C \tilde{\otimes} D) = (A \otimes C)P(N, L)P(N, M)(B \otimes D) = AC \otimes BD.$$

$$е) \quad (A \otimes B)(C \tilde{\otimes} D) = P(N, M)(A \otimes B)(C \tilde{\otimes} D) = P(N, M)(AC \tilde{\otimes} BD) = P(N, M)(BD \otimes AC) = BD \otimes AC.$$

Пусть E_M и E_L – единичные матрицы порядков M и L .

Из вышесказанных свойств следует

Следствие 3.1 (факторизация).

$$(A \otimes B) = (E_M \otimes B)(A \otimes E_L) = (A \otimes E_L)(E_M \otimes B); \quad (a)$$

$$(A \otimes B) = (E_M \otimes B)(A \otimes E_L) = (A \otimes E_L)(E_M \otimes B); \quad (б)$$

$$(A \tilde{\otimes} B) = (E_M \otimes B)(A \tilde{\otimes} E_L) = (A \otimes E_L)(E_M \tilde{\otimes} B). \quad (в)$$

Докажем некоторые свойства введенных выше перестановок в виде утверждений, которые будут использоваться в дальнейшем. Пусть $N = mn$, тогда перестановки $P = (m, n)$ будем обозначать через $P(N, n)$.

Обозначение перестановок в виде $P(N, n)$, где $N = mn$, отчасти удобно, так как показывает сдвиг вправо на n элементов в матрице P от обычного кронекеровского произведения единичных матриц.

Предложение 1. Пусть $N = RST$. Тогда

$$P(N, ST) = P(N, S)P(N, T).$$

Доказательство. Заметим, что в левой части доказуемого равенства, т.е. в матрице P , происходит циклический сдвиг вправо на число элементов ST , а справа в матрицах – сдвиг вправо сначала на S элементов, а затем на T элементов, и что при умножении матриц сдвиги матриц увеличиваются в ST раз. Таким образом,

$$P(N, ST) = P(N, S)P(N, T).$$

Из предложения 1 следует, что, например,

$$P(8, 2)^2 = P(8, 4); P(8, 2)^3 = P(8, 8) = E_8$$

и т. д. В частности, из утверждения 1 следует, что

$$P(NM, M)^{-1} = P(NM, N).$$

Предложение 2. Пусть A – матрица порядка M , а B – матрица порядка N , тогда

$$P(A \otimes B)P^{-1} = B \otimes A.$$

Доказательство. Заметим, что перестановка P производит перестановку строк, а обратная ей перестановка производит перестановку столбцов, так как $P^{-1} = P^T$. Доказательство утверждения 2 следует из замечания к теореме 1. Пусть в кронекеровском произведении матриц A и B перемножаются элементы $a_{rt}b_{sj}$, тогда ему будет соответствовать элемент c_{kl} , где $k = (r-1)n + s, l = (t-1)n + j$. В результате перестановок получим новый элемент $c_{k'l'}$, где $k' = (s-1)m + r, l' = (j-1)m + i$. При кронекеровском перемножении матриц B и A получим $c_{k''l''}$, где $k'' = (s-1)m + r, l'' = (j-1)m + i$. Таким образом, элемент слева равняется элементу справа. Предложение 2 доказано.

Предложение 3.

$$P(A \otimes B)P^{-1} = B \otimes A = A \tilde{\otimes} B; \quad (a)$$

$$P(A \tilde{\otimes} B)P^{-1} = B \tilde{\otimes} A = A \otimes B. \quad (б)$$

Доказательство. Доказательство предложения 3(а) следует из предложения 2 и свойства 4. Доказательство предложения 3 (б) аналогично.

Из предложений 2 и 3 следует, что для того, чтобы поменять в кронекеровских произведениях матрицы местами, надо произвести две перестановки (слева и справа). Перестановка $P(N, n)$ меняет местами строки матриц, а перестановка $P^{-1}(N, n) = P(N, m)$ справа меняет местами столбцы матриц.

Рассмотрим следствия из предложений 2 и 3. Пусть матрица A имеет порядок R , а матрица B – порядок S . Тогда

Следствие 3.2.

$$P(E_R \otimes B)P^{-1} = B \otimes E_R;$$

$$(A \otimes B) = (A \otimes E_S)P(N, R)(B \otimes E_R)P^{-1}(N, R);$$

$$(A \otimes B) = P(N, R)(E_S \otimes A)P^{-1}(N, R)(E_R \otimes B).$$

Следствие 3.3.

$$P(E_R \otimes B)P^{-1} = B \otimes E_R = (E_R \tilde{\otimes} B);$$

$$(A \otimes B) = (A \otimes E_S)P(N, R)(B \otimes E_R)P^{-1}(N, R);$$

$$(A \otimes B) = P(N, R)(E_S \otimes A)P^{-1}(N, R)(E_R \otimes B).$$

Следствие 3.4.

$$P(E_R \tilde{\otimes} B)P^{-1} = B \tilde{\otimes} E_R = (E_R \otimes B);$$

$$(A \tilde{\otimes} B) = (A \otimes E_S)P(N, R)(B \tilde{\otimes} E_R)P^{-1}(N, R);$$

$$(A \tilde{\otimes} B) = P(N, R)(E_S \otimes A)P^{-1}(N, R)(E_R \tilde{\otimes} B).$$

Теорема 4. Пусть $N = N_1 N_2 N_3$, тогда

$$\begin{aligned} P(N, N_3) &= (P(N_1 N_3, N_3) \otimes E_{N_2})(E_{N_1} \otimes P(N_2 N_3, N_3)) = \\ &= (P(N_1 N_3, N_3) \otimes E_{N_2})(P(N_2 N_3, N_3) \otimes E_{N_1}) = \\ &= (E_{N_2} \tilde{\otimes} P_{N_1 N_3})(E_{N_1} \tilde{\otimes} P(N_2 N_3, N_3)). \end{aligned}$$

Доказательство. Возьмем три вектора $\bar{a}, \bar{b}, \bar{c}$ длиной N_1, N_2, N_3 соответственно. Тогда

$$P(N, N_3)(\bar{a} \otimes \bar{b} \otimes \bar{c}) = \bar{c} \otimes \bar{a} \otimes \bar{b}$$

$$\begin{aligned} (P(N_1 N_3, N_3) \otimes E_{N_2})(E_{N_1} \otimes P(N_2 N_3, N_3))(\bar{a} \otimes \bar{b} \otimes \bar{c}) = \\ = (P(N_1 N_3, N_3) \otimes E_{N_2})(\bar{a} \otimes \bar{c} \otimes \bar{b}) = (\bar{c} \otimes \bar{a} \otimes \bar{b}). \end{aligned}$$

Первое выражение доказано. Далее,

$$\begin{aligned} (P(N_1 N_3, N_3) \otimes E_{N_2})(P(N_2 N_3, N_3) \otimes E_{N_1}) = \\ = P(N, N_2 N_3)P(N, N_1 N_3) = P(N, N_3) = \\ = (E_{N_2} \tilde{\otimes} P_{N_1 N_3})(E_{N_1} \tilde{\otimes} P(N_2 N_3, N_3)). \end{aligned}$$

Теорема доказана.

Замечание. Ранее было доказано, что выражение $E_{N_1} \otimes P(N_2 N_3, N_3)$ переставляет векторы $\bar{b}$ и $\bar{c}$ местами, а вектор $\bar{a}$ оставляет на месте. Выражение $(P(N_1 N_3, N_3) \otimes E_{N_2})(\bar{a} \otimes \bar{c} \otimes \bar{b})$ переставляет векторы $\bar{a}$ и $\bar{c}$ местами.

Пусть N_1, N_2, N_3 – целые положительные числа, $N = N_1 N_2 N_3$, A_N означает матрицу порядка N . Тогда справедлива

Теорема 5.

$$\begin{aligned} A_{N_1} \otimes A_{N_2} \otimes A_{N_3} &= P(N, N_1)(E_{N_2 N_3} \otimes A_{N_1}) \times \\ &\times P(N, N_2)(E_{N_1 N_3} \otimes A_{N_2})P(N, N_3)(E_{N_1 N_2} \otimes A_{N_3}) = \\ &= (E_{N_2 N_3} \otimes A_{N_1})(E_{N_1 N_3} \otimes A_{N_2})(E_{N_1 N_2} \otimes A_{N_3}) = \\ &= (A_{N_1} \tilde{\otimes} E_{N_2 N_3})(A_{N_2} \tilde{\otimes} E_{N_1 N_3})(A_{N_3} \tilde{\otimes} E_{N_1 N_2}). \end{aligned}$$

Доказательство.

$$\begin{aligned} A_{N_1} \otimes A_{N_2} \otimes A_{N_3} &= A_{N_1} \otimes (A_{N_2} \otimes A_{N_3}) = \\ &= (A_{N_1} \otimes E_{N_2 N_3})(E_{N_1} \otimes (A_{N_2} \otimes A_{N_3})) = \\ &= (A_{N_1} \otimes E_{N_2 N_3})(E_{N_1} \otimes A_{N_2} \otimes E_{N_3})(E_{N_1 N_2} \otimes A_{N_3}) = \\ &= P_1(E_{N_2 N_3} \otimes A_{N_1})P_1^{-1}P_2(E_{N_1 N_3} \otimes A_{N_2})P_2^{-1}(E_{N_1 N_2} \otimes A_{N_3}), \end{aligned}$$

где $P_1 = P(N, N_1), P_2 = P(N, N_1 N_2)$.

Известно, что $P_1^{-1} = P(N, N_2, N_3), P_2^{-1} = P(N, N_3)$.

Тогда

$$\begin{aligned} A_{N_1} \otimes A_{N_2} \otimes A_{N_3} &= P(N, N_1)(E_{N_2 N_3} \otimes A_{N_1}) \times \\ &\times P(N, N_2)(E_{N_1 N_3} \otimes A_{N_2})P(N, N_3)(E_{N_1 N_2} \otimes A_{N_3}) = \\ &= (E_{N_2 N_3} \otimes A_{N_1})(E_{N_1 N_3} \otimes A_{N_2})(E_{N_1 N_2} \otimes A_{N_3}) = \\ &= (A_{N_1} \tilde{\otimes} E_{N_2 N_3})(A_{N_2} \tilde{\otimes} E_{N_1 N_3})(A_{N_3} \tilde{\otimes} E_{N_1 N_2}). \end{aligned}$$

Теорема доказана.

Пусть теперь $M = N_1 = N_2 = N_3$. Тогда

Следствие 5.1.

$$A \otimes B \otimes C = P(E_{M^2} \otimes A)P(E_{M^2} \otimes B)P(E_{M^2} \otimes C),$$

где $P = P(M^3, M)$.

Теорему 5 можно обобщить.

Пусть $N_1, N_2, \dots, N_m$ – целые положительные числа. Матрица A_{N_i} – матрица порядка N_i . Пусть

$$N = N_1 N_2 \dots N_m, N(k) = N_1 N_2 \dots N_k; N(0) = 1.$$

Тогда

$$A_{N_1} \otimes A_{N_2} \otimes \dots \otimes A_{N_m} = \prod_{k=1}^m E_{N(k-1)} \otimes A_{N_k} \otimes E_{N/N(k)}. \quad \{*\}$$

Но выражение $\{*\}$ можно представить как в теореме 5: $E_{n(k-1)} \otimes A_{N_k} \otimes E_{N/N(k)} = P_k(E_{N/N_k} \otimes A_{N_k})P_k^{-1}$, где $P_k = P(N, N(k))$. Доказана

Теорема 6. Если $P_k = P(N, N(k))$, то

$$A_{N_1} \otimes A_{N_2} \otimes \dots \otimes A_{N_m} = \prod_{k=1}^m P(N, N_k)(E_{N/N_k} \otimes A_{N_k}) = \\ = \prod_{k=1}^m (E_{N/N_k} \otimes \bar{A}_{N_k}) = \prod_{k=1}^m (A_{N_k} \tilde{\otimes} E_{N/N_k}).$$

Рассмотрим свойства применяемых перестановок в рамках теории групп.

Покажем, что множество $G = \{P(N, S)\}$, где S – делитель N , является группой. Множество G изоморфно множеству моноидных матриц порядка N , которые смещены от единичных матриц того же порядка на величину n вправо. Такого вида матрицы называются перестановочными матрицами с n -ичным сдвигом. Это множество образует группу, так как элементы его ортогональны и их определители равны ± 1 . Ввиду ортогональности перестановочных матриц $PP^T = E$. Отсюда $P^{-1} = P^T$. Замкнутость умножения перестановок вытекает из предложения 1; из этого же предложения вытекает коммутативность их умножения. Таким образом, рассматриваемое выше множество G является абелевой группой.

Теорема 7. Пусть $N = 2^M$, тогда множество $\{P(2^M, 2^m) | 0 \leq m < M\}$ является циклической группой с образующей $P(2^M, 2)$. В частности, $P(2^M, 2^m)P(2^M, 2^k) = P(2^M, 2^{m+k})$, где $(m+k) \equiv m+k \pmod{M}$.

Теорема 8. Если p – простое число, то множество $\{P(p^M, p^S) | S/N\}$ есть циклическая группа порядка M с образующей $P(p^M, p)$.

Подойдем к этому вопросу с другой стороны.

Пусть Z – кольцо целых чисел с условием деления. Если a и b – целые числа, $b \neq 0$, то $a = bq + r$, $0 \leq r < b$, где q и r – единственно определенные целые числа. Число q называется частным от деления a на b , r – остатком. Величина $r = a - bq$; если $r = 0$, то $a = bq$ и целое число b называется делителем числа a и записывается в виде b/a . Число $p > 1$ называется простым, если делитель у него $\pm 1, \pm p$. Пусть a и b – целые числа. Число c называется общим делителем, если c/a и c/b . Если $c = \pm 1$, то числа a и b называют взаимно простыми. Наибольший общий делитель чисел a и b будем обозначать через (a, b) . Если $b = p$ и $(a, p) = 1$, то числа a и p – взаимно простые; если $(a, p) = p$, то p/a . Рассмотрим множество $(n) = nZ = \{nk, k \in Z\}$. Множество nZ есть идеал в кольце Z . Оно замкнуто относительно операций сложения и умножения:

$$a) nk + nl = n(k + l);$$

$$b) m(nk) = (mn)k = n(mk).$$

Лемма 1. Всякий идеал в Z имеет вид nZ для всех $n \geq 0$.

Лемма 2. Пусть a и b – целые числа, не равные нулю, тогда $(a, b) = ax_0 + by_0$, для некоторых целых чисел x_0, y_0 .

Лемма 3. Если a/bc и $(a, b) = 1$, то a/c . В частности, если p – простое и p/bc , то p/b или p/c .

Теорема 9. Если $n > 1$, то целое число n можно единственным образом представить в виде $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, где $p_1, p_2, \dots, p_r$ – различные целые числа, а $\alpha_1, \alpha_2, \dots, \alpha_r \neq 0$ – целые.

Следствие 9.1. Если a/c , b/c и $(a, b) = 1$, тогда ab/c .

Рассмотрим некоторые приложения введенных выше обобщенных кронекеровских произведений матриц. В настоящее время ортогональные дискретные преобразования применяются при обработке случайных сигналов, распознавании образов, в телевидении и т.д. Ввиду того, что, например, преобразования Уолша принимают всего два значения $(+1, -1)$, они очень удобны для цифровой обработки информации. Эффективность преобразований Уолша и ряда других ОДП заключается в том, что матрицы этих преобразований допускают факторизацию в виде произведения разреженных матриц. С другой стороны, факторизация матриц ОДП возможна тогда и только тогда, когда она представима в виде кронекеровских произведений матриц. В следующей простой теореме покажем, что обобщенные кронекеровские произведения матриц не выходят из класса обычных кронекеровских произведений матриц.

Теорема 10. Пусть $H(N_1)$ и $H(N_2)$ есть H -матрицы порядков N_1 и N_2 соответственно. Тогда $H(N_1) \bar{\otimes} H(N_2)$ и $H(N_1) \tilde{\otimes} H(N_2)$ есть H -матрицы порядка $N_1 N_2$.

Пусть $N = 2^n$, где n – натуральное число. $H(2) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ – стандартная матрица Уолша – Пэли второго порядка.

Известен рекуррентный алгоритм построения матриц Уолша – Адамара порядка N :

$$H_h(2^n) = \otimes^{(n-1)} H(2) = H(2) \otimes H(2) \otimes \dots \otimes H(2)$$

– $(n-1)$ раз, где $\otimes^{(n-1)}$ – $(n-1)$ -мерная кронекеровская степень.

Используя теоремы 1 и 10, можно получить аналогичный алгоритм построения матриц Уолша – Пэли:

$$H_p(4) = H(2) \bar{\otimes} H(2) = H(2) \tilde{\otimes} H(2);$$

$$H_p(8) = H_p(4) \bar{\otimes} H(2) = H_p(4) \tilde{\otimes} H(2);$$

$$H_p(2^n) = H_p(2^{n-1}) \bar{\otimes} H(2) = H_p(2^{n-1}) \tilde{\otimes} H(2).$$

Следствие 10.1.

$$H_p(2^n) = H_p(2^{n-1}) \overline{\otimes} H(2) = H_p(2^{n-1}) \tilde{\otimes} H(2) = \\ = \overline{\otimes}^{(n-1)} H(2) = \tilde{\otimes}^{(n-1)} H(2),$$

где $\overline{\otimes}^{(n-1)}$, $\tilde{\otimes}^{(n-1)}$ – $(n-1)$ -степени обобщенных кронекеровских произведений матриц.

Используя обобщенные кронекеровские произведения матриц и их основные свойства, можно получить представления матриц ОДП (например, матриц Уолша) в виде произведения разреженных матриц. Матрицу Уолша – Адамара можно представить в виде

$$H_h(N) = [E_{2^{(n-1)}} \overline{\otimes} H(2)]^n = [E_{2^{(n-1)}} \tilde{\otimes} H(2)]^n,$$

где $[]^n$ – обычное произведение n -одинаковых матриц, E_k – единичная матрица порядка k . Матрицу Уолша – Пэли можно представить в виде

$$H_p(N) = \prod_{j=1}^n E_{2^{(j-1)}} \otimes (E_{2^{(n-j)}} \overline{\otimes} H(2)) = \\ = \prod_{j=1}^n E_{2^{(n-j)}} \otimes (E_{2^{(j-1)}} \tilde{\otimes} H(2)).$$

Рассмотренные способы факторизации матриц Уолша являются удобными для их реализации в режиме реального времени, так как для начала вычислений достаточно иметь на входе только два первых отсчета. Они являются также удобными для реализации их в векторном режиме для вычислительных устройств типа ОКМД.

ЛИТЕРАТУРА

1. *Tolimieri R., An M., Iu C.* Algorithms for Discrete Fourier Transform and Convolution. N.Y.: Springer-Verlag. New York Ins., 1989. 350 p.
2. *Быков В.И., Литвин А.И., Кожуховский А.Д. и др.* Обобщенные кронекеровские произведения матриц и их применения // Электронное моделирование. 1991. Т.13. № 5. С. 14–19.
3. *Литвин А.И.* Структура ортогональных дискретных преобразований Уолша – Пэли // Автометрия. 1990. №3. С.106-109.
4. *Литвин А.И.* Кронекеровские произведения матриц и их применения // Электронное моделирование. 1994. Т.16. №2. С. 91–93.

Статья представлена кафедрой алгебры механико-математического факультета Томского государственного университета, поступила в научную редакцию 13 июня 2003 г.