ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—август 2008. Том 15, № 4. 25–29

УДК 519.854, 512.643

О МИНОРНЫХ ХАРАКТЕРИСТИКАХ ВЗАИМНО ОРТОГОНАЛЬНЫХ ЦЕЛОЧИСЛЕННЫХ РЕШЁТОК*)

С. И. Веселов, В. Н. Шевченко

Аннотация. Показано, что базисные матрицы у взаимно ортогональных подрешёток решётки $\mathbb{Z}^n$ имеют одинаковые наборы элементарных делителей.

Ключевые слова: целочисленная решётка, нормальная диагональная форма.

Введение

Под решёткой далее понимается подгруппа аддитивной группы $\mathbb{Z}^n$. Решётка с образующими $h_1, h_2, \ldots, h_k$ обозначается $L(h_1, h_2, \ldots, h_k)$. Линейно независимый набор образующих называется *базисом*. Матрица, составленная из базисных вектор-столбцов, называется *базисной*. *Ортогональной* к решётке $\Lambda \subset \mathbb{Z}^n$ называется решётка $\Lambda^\perp = \{y \in \mathbb{Z}^n \ : \ x^T y = 0 \ \forall x \in \Lambda\}$. Ортогональные решётки встречаются, например, в двойственном описании множества допустимых решений задачи целочисленного линейного программирования: множество $S = \{x \in \mathbb{Z}^n \mid A^T x = a, \ x \geqslant 0\}$ можно представить в виде $S = \{x \in \mathbb{Z}^n \mid x = By + b \geqslant 0, \ y \in \mathbb{Z}^{n-r}\}$, где $r = \operatorname{rank} A, \ b \in S, \ B$ — базисная матрица решётки $L(A)^\perp$.

Для всякого подмножества $I \subseteq N = \{1, 2, \ldots, n\}$ обозначаем через $\sigma(I)$ сумму его элементов и полагаем $\overline{I} = N \setminus I$. Для произвольной матрицы M выражение $M(I)$ обозначает подматрицу, состоящую из строк с номерами из I, $M(I, J)$ — подматрицу, состоящую из строк с номерами из I и столбцов с номерами из J. Известно [4], что миноры взаимно обратных матриц U и V связаны равенством

$$\det V \cdot \det U(I, J) = (-1)^{\sigma(I)+\sigma(J)} \det V(\overline{J}, \overline{I}).$$

Из этого равенства можно вывести следующий результат [3] (см. также [6]): *если* $A \in \mathbb{Z}^{n\times m}, \ \operatorname{rank} A = m, \ B$ — *базисная матрица решётки*

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 05–01–00552).

$L(A)^{\perp}$, то для всякого $I \subset N$, $|I| = m$, справедлива формула

$$|\det A(I)| = \Delta_m(A)|\det B(\overline{I})|.$$

Из неё следует, что для базисных матриц A и B взаимно ортогональных решёток выполняется равенство

$$|\det A(I)| = |\det B(\overline{I})|. \tag{1}$$

Этот факт использован в [3] для оценки длины минимального вектора ортогональной решётки (из (1) следует, что равны объёмы фундаментальных параллелепипедов ортогональных решёток), в [1] — для оценки компонент целого решения системы линейных неравенств, в [2] — для оценки числа вершин выпуклой оболочки множества целых решений системы уравнений и неравенств. В [8] независимо установлено равенство объёмов фундаментальных параллелепипедов взаимно ортогональных решёток. В [7] ортогональные решётки применялись для изучения транспортных многогранников.

В этой статье мы описываем более глубокую, по сравнению с формулой (1), связь между минорными характеристиками базисов взаимно ортогональных целочисленных решёток.

Обозначение $\mathrm{diag}(\alpha_1, \alpha_2, .., \alpha_m)$ используем для матрицы, у которой меньший из размеров равен m, для каждого $i \in \{1, \dots, m\}$ элемент, расположенный на пересечении i- го столбца и i-й строки равен α_i, а остальные элементы равны нулю. *Нормальной диагональной формой* матрицы M с целыми элементами называется матрица

$$\text{НДФ}(M) = \mathrm{diag}(d_1(M), \dots, d_r(M), 0, \dots, 0),$$

где $r = \mathrm{rank}\, M$ и $d_i(M)$ делится на $d_{i-1}(M)$ для каждого $i \in \{2, 3, \dots, r\}$. Ненулевые элементы в НДФ называются *инвариантными множителями.* Вот примеры использования нормальной диагональной формы.

1. Условием разрешимости в целых числах системы линейных уравнений $Ax = b$ с целыми коэффициентами является равенство НДФ(A) =НДФ$(A \mid b)$.

2. Если $A \in \mathbb{Z}^{n \times m}$, $\mathrm{rank}\, A = m$, $b \in \mathbb{Z}^n$, то знаменатели координат вершин множества решений системы линейных неравенств $Ax \leqslant b$ не превышают $\max d_m(\overline{A})$, где максимум выбирается среди всех подматриц $\overline{A}$ матрицы A.

3. Если $A \in \mathbb{Z}^{n\times n}$, $\operatorname{rank} A = n$, то число вершин у выпуклой оболочки множества $\{x \in \mathbb{Z}^n :\ Ax \leqslant b\}$ не превышает $(\log_2 d_n(A)+1)^{n-1}$. Эта оценка сильнее оценки $(\log_2 |A| + 1)^{n-1}$ из [6] и ранее не публиковалась, хотя является результатом непосредственного применения подхода, изложенного в [6].

Мы установим связь между нормальными диагональными формами матриц $A(J)$ и $B(\overline{J})$ для произвольного $J \subset N$.

Ещё несколько обозначений и определений. Пусть E_k — единичная матрица порядка k. Нулевую матрицу всюду обозначаем буквой O, размер матрицы определяется из контекста. $\Delta_i(M)$ обозначает наибольший общий делитель всех миноров i-го порядка матрицы M. *Элементарными делителями* матрицы M называются все отличные от 1 степени $p_1^{k_{1,1}}, \ldots, p_s^{k_{s,r}}$ из разложений

$$d_i(M) = p_1^{k_{1,i}} \cdot \ldots \cdot p_s^{k_{s,i}} \quad (i = 1, 2, \ldots, r = \operatorname{rank} M)$$

инвариантных множителей в произведение степеней простых чисел. *Унимодулярной* называется целочисленная квадратная матрица с определителем, равным ± 1.

1. Основной результат

Лемма. *Пусть* $A \in \mathbb{Z}^{n\times m}$, $B \in \mathbb{Z}^{n\times(n-m)}$, $\Delta_m(A) = \Delta_{n-m}(B) = 1$, $A^T B = O$, $|I| = s$, $l = \min\{s, m\}$. *Если* $D =$НДФ$(A(I)) = \operatorname{diag}(d_1, \ldots, d_l)$, *то*

$$\text{НДФ}(B(\overline{I})) = \begin{cases} \operatorname{diag}(1, \ldots, 1, d_1, \ldots, d_l) & \text{при } m + s \leqslant n, \\ \operatorname{diag}(d_{m+s-n+1}, \ldots, d_l) & \text{при } m + s > n. \end{cases}$$

Доказательство. Не уменьшая общности, рассмотрим лишь $I = \{1, 2, \ldots, s\}$. Предположим, что $m + s \leqslant n$. Пусть P, Q_1, Q_2 — унимодулярные матрицы такие, что $D = Q_1 A(I) P$ и $Q_2 A(\overline{I}) P = (U\ O)^T$, где $U = (u_{i,j})$ — верхне-треугольная $(m\times m)$-матрица (по поводу существования перечисленных матриц см. [1]). Предположим, что нашлось k такое, что НОД$(d_k, u_{k,k}) \neq 1$. Тогда отличен от 1 наибольший общий делитель миноров $(m - k + 1)$-го порядка, расположенных в столбцах $k, \ldots, m$ матрицы $G = (D \quad U \quad O)^T$, поэтому $\Delta_m(G) \neq 1$, следовательно, $\Delta_m(A) \neq 1$, а это противоречит условию леммы. Пусть $r = \operatorname{rank} D$, $D_1 = \operatorname{diag}(d_1, d_2, \ldots, d_r)$. Представим матрицу G в виде

$$G = \begin{pmatrix} D_1 & O & U_1 & U_2 & O \\ O & O & O & U_3 & O \end{pmatrix}^T.$$

Рассмотрим матрицу

$$H = \begin{pmatrix} D_1^{-1}U_1D_1 & O & -D_1 & O & O \\ O & E_{s-r} & O & O & O \\ O & O & O & O & E_{n-m-s} \end{pmatrix}^T.$$

Нетрудно видеть, что $G^T H = O$. Поскольку наибольший общий делитель миноров

$$\begin{vmatrix} D_1^{-1}U_1D_1 & O & O \\ O & E_{s-r} & O \\ O & O & E_{n-m-s} \end{vmatrix} = u_{1,1} \cdot \ldots \cdot u_{r,r},$$

$$\begin{vmatrix} O & -D_1 & O \\ E_{s-r} & O & O \\ O & O & E_{n-m-s} \end{vmatrix} = (-1)^{rs} d_1 \cdot \ldots \cdot d_r$$

равен 1, то $\Delta_{n-m}(H) = 1$. Следовательно, H — базисная матрица решётки $L(G)^\perp$, $(H(I)^T Q_1 \quad H(\overline{I}) Q_2^T)^T$ — базисная матрица решётки $L(AP)^\perp = L(A)^\perp$. Так как для всякой матрицы M справедливы формулы $d_1(M) = \Delta_1(M)$, $d_i(M) = \Delta_i(M)/\Delta_{i-1}(M)$ при $i \geqslant 2$ (см., например, [5]), то $\text{НДФ}(B(\overline{I})) = \text{НДФ}(H(\overline{I})) = \operatorname{diag}(1, \ldots, 1, d_1, \ldots, d_l)$. Случай $s + m \geqslant n$ симметричен уже рассмотренному.

Следствие. *Если P — унимодулярная $(n \times n)$-матрица и $I, J \subset N$, то наборы ненулевых элементов в $\text{НДФ}(P(I, J))$ и $\text{НДФ}(P^{-1}(\overline{J}, \overline{I}))$ могут отличаться лишь количеством единиц.*

Доказательство. Достаточно заметить, что решётки $L(P^{-1}(N, \overline{I}))$ и $L(P^T(I, N))$ взаимно ортогональны.

Теорема. *Базисные матрицы взаимно ортогональных решёток имеют одинаковые наборы элементарных делителей.*

Доказательство. Утверждение непосредственно вытекает из леммы.

ЛИТЕРАТУРА

1. **Веселов С. И.** Доказательство обобщения гипотезы Бороша — Трейбига о диофантовых уравнениях // Дискретн. анализ и исслед. операций. Сер. 1. — 2001. — Т. 8, № 1. — С. 17—22.
2. **Веселов С. И., Чирков А. Ю.** Оценки числа вершин целых полиэдров // Дискретн. анализ и исслед. операций. Сер. 2. — 2007. — Т. 14, № 2. — С. 14—31.

3. **Веселов С. И., Шевченко В. Н.** Оценки минимального расстояния между точками некоторых целочисленных решёток // Комбинаторно-алгебраические методы в прикладной математике. — Горький: Горьковский гос. ун-т, 1980. — С. 26–33.
4. **Гантмахер Ф. Р.** Теория матриц. — М.: Наука, 1988. — 552 с.
5. **Схрейвер А.** Теория линейного и целочисленного программирования. Т. 2. — М.: Мир, 1991. — 342 с.
6. **Шевченко В. Н.** Качественные вопросы целочисленного программирования. — М.: Физматлит, 1995. — 192 с.
7. **Шевченко В. Н.** Многогранники многоиндексных транспортных задач: алгебраический подход. // Российская конференция «Дискретная оптимизация и исследование операций»: Материалы конф. (DAOR'04). — Новосибирск: Изд-во Ин-та математики, 2004. — С. 64—69.
8. **Nguyen P., Stern J.** Merkle—Hellman revisited: a cryptanalysis of the Qu- Vanstone cryptosystem based on group factorizations // Proc. of Crypto'97. — IACR: Springer-Verl., 1997. — P. 198–212. (Lect. Notes Comp. Sci.; Vol. 1294).

Веселов Сергей Иванович,
e-mail: vesi@uic.nnov.ru

Шевченко Валерий Николаевич

Статья поступила
30 октября 2007 г.

Переработанный вариант —
6 мая 2008 г.