ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—март 2001. Серия 1. Том 8, № 1, 17–22

УДК 519.854+511.512

ДОКАЗАТЕЛЬСТВО ОБОБЩЕНИЯ ГИПОТЕЗЫ БОРОША–ТРЕЙБИГА О ДИОФАНТОВЫХ УРАВНЕНИЯХ

С. И. Веселов

Рассматривается система линейных диофантовых уравнений $Ax = a$ над неоднородной решеткой L, имеющая неотрицательное решение. Доказано, что имеется решение, у которого компоненты неотрицательны и не превышают $d \det L$, где d — максимальный по модулю минор матрицы $(A\ a)$, порядок которого равен $\mathrm{rang} A$.

1. Обозначения и формулировка основного результата

Пусть A и B — матрицы размера $m \times n$ и $p \times n$ соответственно с целыми элементами, $\mathrm{rang}\, A = m$, a и b — векторы с целыми координатами;

$a_1, a_2, \dots, a_n$ — столбцы матрицы A; $b_1, b_2, \dots, b_n$ — столбцы матрицы B;

L — подрешетка решетки всех целых p-мерных векторов, $l = \det L$, запись $u \equiv v\ (L)$ означает, что $u - v \in L$;

M — множество неотрицательных целых решений системы

$$Ax = a, \quad Bx \equiv b\ (L); \tag{1}$$

d — максимум среди абсолютных величин миноров порядка m матрицы $(A\, a)$; $N = \{1, \dots, n\}$;

A_i — матрица, полученная из A после удаления i-го столбца;

s_i — наибольший общий делитель миноров m-го порядка матрицы A_i;

D_i — квадратная матрица порядка m с целыми элементами и определителем s_i такая, что матрица $D_i^{-1} A_i$ имеет целые элементы (столбцами матрицы D_i являются базисные векторы решетки, порожденной столбцами матрицы A_i);

$K(A)$ — конус, порожденный столбцами матрицы A.

В статье доказывается следующее утверждение.

Теорема 1. *Если M непусто, то существует элемент $x^0 \in M$ такой, что $x_i^0 \leqslant dl$ для каждого $i \in N$.*

При $l = 1$ это есть гипотеза Бороша–Трейбига [3-6], доказанная в [2].

2. Доказательство теоремы 1

Не уменьшая общности, считаем, что наибольший общий делитель миноров m-го порядка матрицы A равен 1.

Теорема доказывается индукцией по n. Если $n = m$, то справедливость утверждения следует из правила Крамера решения систем линейных уравнений. Предположим, что утверждение справедливо для систем с числом неизвестных, меньшим n. Докажем утверждение для системы с n неизвестными.

Случай 1. Сначала предположим, что из неравенства $u^T A \geqslant 0$ следует $u = 0$. Согласно теореме Минковского — Фаркаша конус $K(A)$ совпадает с m-мерным пространством, порожденным столбцами матрицы A. Следовательно, $-a_i \in K(A_i)$ при любом i. Это означает, что $\operatorname{rang} A_i = m$ и выпуклый конус C, состоящий из решений системы $Ax = 0, x \geqslant 0$, содержит вектор с положительными координатами. Поэтому размерность конуса равна $n - m$.

Введем обозначения:

P — некоторая $(n - m - 1)$-мерная грань конуса C;

$I = \{i |\, x_i = 0$ для всякого $x \in P\}$ (при $n = m + 1$ полагаем $I = N$);

$x' = (x'_1, x'_2, \dots, x'_n)$ — произвольный вектор из M;

H — матрица размера $n \times (n - m)$, в которой совокупность столбцов $h^j = (h_1^j, \dots, h_n^j)^T$ $(j = 1, \dots, n - m)$ является базисом решетки целых решений системы $Ax = 0$;

R — квадратная матрица порядка $n - m$, столбцы которой образуют базис решетки целых решений системы $BHy \equiv 0\ (L)$.

Не уменьшая общности, считаем, что $h^2, h^3, \dots, h^{n-m} \in P$. В этом случае $h_i^1 > 0$ при любом $i \in I$.

Для упрощения обозначений предположим, что $1 \in I$ и

$$\arg\min_{i \in I} x'_i / h_i^1 = 1. \tag{2}$$

Согласно предположению о минорах матрицы A первая компонента любого целого решения системы $Ax = a_1 x_1 + A_1(x_2, x_3, \dots, x_n)^T = 0$ делится на s_1. Следовательно, первая компонента вектора h^1 равна s_1.

Не уменьшая общности, считаем, что H и R имеют следующий вид:

$$H = \begin{pmatrix} s_1 & 0 \\ h & H^1 \end{pmatrix}, \quad R = \begin{pmatrix} t & 0 \\ r & R^1 \end{pmatrix}.$$

Векторы решетки F целых решений системы $Ax = 0, \quad Bx \equiv 0\ (L)$ находятся по формуле

$$x = HRu = \begin{pmatrix} s_1 t & 0 \\ ht + H^1 r & H^1 R^1 \end{pmatrix} u.$$

Отсюда вытекают два следствия:

a) можно подобрать целое число μ так, чтобы получить целое решение

$$x'' = (x_1'', \dots, x_n'')^T = (x_1', \dots, x_n')^T + (s_1 t, (ht + H^1 r)^T)^T \mu$$

системы (1) такое, что $0 \leqslant x_1'' < s_1 t$, причем из (2) получается, что $x_i'' \geqslant 0$ при $i \in I$;

b) существуют матрица B^1 и подрешетка L^1 такие, что пересечение F с плоскостью $x_1 = 0$ описывается системой вида

$$x_1 = 0,\ A_1(x_2, \dots, x_n)^T = 0,\ B^1(x_2, \dots, x_n)^T \equiv 0\ (L^1),$$

причем $|\det L^1| = |\det R^1|$.

Согласно определению множества I для каждого $i \notin I$ в множестве $\{h^2, h^3, \dots, h^{n-m}\}$ найдется вектор, в котором i-я компонента строго больше нуля. Следовательно, при любом $i \notin I$ справедливы неравенства $h_i^2 + \dots + h_i^{n-m} > 0$.

Определим целое число λ из условий

$$\lambda l(h_i^2 + \dots + h_i^{n-m}) + x_i'' \geqslant 0, \text{ где } i \notin I,$$

и зададим вектор y по формуле

$$y = (y_1, \dots, y_n) = \lambda l(h^2 + \dots + h^{n-m}) + x'' \in M.$$

Рассмотрим систему

$$D_1^{-1} A_1 z = D_1^{-1}(a - a_1 y_1), \tag{3}$$

$$B_1 z \equiv b - b_1 y_1\ (L), \tag{4}$$

где матрица B_1 получена из матрицы B удалением первого столбца. Известно, что система имеет целое неотрицательное решение $z = (y_2, y_3, \dots, y_n)$. Так как (4) эквивалентна системе $B^1 y \equiv b^1\ (L^1)$ и наибольший по модулю минор m-го порядка расширенной матрицы системы (3) не превышает

$$\frac{(y_1 + 1)d}{s_1} = \frac{(x_1'' + 1)d}{s_1} \leqslant td,$$

то по предположению индукции система (3)–(4) имеет решение $z^0 = (z_1^0, \dots, z_{n-1}^0)$, компоненты которого не превышают величины

$$td|\det L^1| = td|\det R^1| = ld.$$

В качестве x^0 можно взять $(y_1, z_1^0, \dots, z_{n-1}^0)$.

Случай 2. Теперь предположим, что существует $u \neq 0$ такое, что $u^T A \geqslant 0$. Если $u^T A > 0$, то выпуклая оболочка множества $\overline{M}$, состоящего из неотрицательных решений (в том числе и нецелых) системы $Ax = a$, ограничена и, следовательно, является выпуклой оболочкой своих вершин. Из теории линейного программирования известно, что компоненты вершин не превышают d. Так как $M \subseteq \overline{M}$, то утверждение справедливо.

Если некоторые компоненты матрицы $u^T A$ равны нулю, то строки матрицы $(A\, a)$ можно подвергнуть унимодулярному преобразованию и (с точностью до перестановки столбцов) получить матрицу вида

$$\begin{pmatrix} a_1^1 \dots a_v^1 & a_{v+1}^1 \dots a_n^1 & a^1 \\ 0 \ \dots \ 0 & a_{v+1}^2 \dots a_n^2 & a^2 \end{pmatrix},$$

где подматрица $(a_1^1 \dots a_v^1)$ имеет ранг k и состоит из k строк, а столбцы $(a_{v+1}^2 \dots a_n^2)$ имеют положительную последнюю компоненту.

Положим $a^3 = a^1 - a_{v+1}^1 x'_{v+1} - \dots - a_n^1 x'_n$ и рассмотрим систему

$$a_1^1 x_1 + \dots + a_v^1 x_v = a^3. \tag{5}$$

Докажем, что максимальный по абсолютной величине минор d^1 порядка k расширенной матрицы системы (5) не превосходит d.

Пусть $k \geqslant 2$. Для определенности предположим, что $d^1 = |\det(a_1^1 \dots a_{k-1}^1\ a^3)|$. Покажем, что можно подобрать $I = \{i_1, \dots, i_j\}$, где $j = n - m$, так, что все определители

$$\det\begin{pmatrix} a_1^1 \dots a_{k-1}^1 & a_{i_1}^1 \dots a_{i_j}^1 & a^3 \\ 0 \dots 0 & a_{i_1}^2 \dots a_{i_j}^2 & 0 \end{pmatrix}, \quad \det\begin{pmatrix} a_1^1 \dots a_{k-1}^1 & a_{i_1}^1 \dots a_{i_j}^1 & a_i^1 \\ 0 \dots 0 & a_{i_1}^2 \dots a_{i_j}^2 & a_i^2 \end{pmatrix} (i \notin I)$$

либо неположительны, либо неотрицательны.

Определим $\lambda \neq 0$ так, что $\lambda^T a^3 > 0$ и $\lambda^T a_i^1 = 0$ при $i \in \{1, \dots, k-1\}$. Найдем крайнюю точку $\mu = (\mu_1, \dots, \mu_{m-k})$ множества решений системы

$$u^T a_i^2 + \lambda^T a_i^1 \geqslant 0, \quad i \in \{v+1, \dots, n\}.$$

В качестве I выберем множество номеров линейно независимых неравенств, обращающихся в равенства на μ. Пусть e целое число такое, что $\lambda_e \neq 0$. Строку e каждого определителя заменим на линейную комбинацию строк с коэффициентами $\lambda_1, \dots, \lambda_k, \mu_1, \dots, \mu_{m-k}$. Разложив каждый определитель по строке с номером e, получим

$$Z\lambda_e \lambda^T a^3, \quad Z\lambda_e(\lambda^T a_i^1 + \mu^T a_i^2) \text{ при } i \notin I,$$

где Z есть величина алгебраического дополнения к элементу, расположенному в последнем столбце и в строке с номером e. Очевидно, что все

числа либо неположительны, либо неотрицательны. Далее имеем

$$\begin{aligned}
d &\geqslant \left| \det \begin{pmatrix} a_1^1 \ldots a_{k-1}^1 & a_{i_1}^1 \ldots a_{i_j}^1 & a^1 \\ 0 \ldots 0 & a_{i_1}^2 \ldots a_{i_j}^2 & a^2 \end{pmatrix} \right| \\
&= \Bigg| \sum_{i \in I} \det \begin{pmatrix} a_1^1 \ldots a_{k-1}^1 & a_{i_1}^1 \ldots a_{i_j}^1 & a_i^1 \\ 0 \ldots 0 & a_{i_1}^2 \ldots a_{i_j}^2 & a_i^2 \end{pmatrix} x_i^1 \\
&+ \det \begin{pmatrix} a_1^1 \ldots a_{k-1}^1 & a_{i_1}^1 \ldots a_{i_j}^1 & a^3 \\ 0 \ldots 0 & a_{i_1}^2 \ldots a_{i_j}^2 & 0 \end{pmatrix} \Bigg| \\
&\geqslant \left| \det \begin{pmatrix} a_1^1 \ldots a_{k-1}^1 & a_{i_1}^1 \ldots a_{i_j}^1 & a^3 \\ 0 \ldots 0 & a_{i_1}^2 \ldots a_{i_j}^2 & 0 \end{pmatrix} \right| \geqslant d^1.
\end{aligned}$$

При $k = 1$ следует положить $e = 1$,

$$\lambda_1 = \begin{cases} 1 & \text{при } a^3 > 0, \\ -1 & \text{при } a^3 \leqslant 0 \end{cases}$$

и повторить рассуждения.

По предположению индукции система (5) имеет решение $(x_1^0, \ldots, x_\nu^0)$, в котором компоненты не больше d. Ясно, что x_i' при $i \in \{\nu + 1, \ldots, n\}$ ограничен сверху решением задачи целочисленного программирования: найти $\max x_j$ при условии, что $Ax = a$, $x \geqslant 0$. Следовательно, x_i' не превосходит d. Поэтому в качестве x^0 можно выбрать вектор $(x_1^0, \ldots, x_\nu^0, x'_{\nu+1}, \ldots, x'_n)$.

Сформулируем соответствующий результат относительно системы неравенств.

Лемма 1 [1]. *Пусть* $I \subseteq N$, $|I| = m$, $\overline{A}$ — *матрица, состоящая из столбцов матрицы* A *с номерами из* I, *и* $\overline{H}$ — *матрица, состоящая из строк матрицы* H *с номерами из множества* $N \setminus I$. *Тогда* $|\det \overline{A}| = |\det \overline{H}|$.

Формула $x = HRy + x'$ устанавливает взаимно однозначное соответствие между M и множеством решений системы неравенств

$$HRy + x' \geqslant 0. \tag{6}$$

Из теоремы следует, что если система (6) разрешима в целых числах, то существует решение y^0 такое, что $||HRy^0 + x'||_\infty \leqslant d|\det R|$. Из леммы следует, что $d|\det R|$ равно наибольшей из абсолютных величин миноров n-го порядка матрицы HR и миноров $(n+1)$-го порядка матрицы $(HR\, x')$.

Таким образом, справедливо

Следствие. *Пусть* G — *матрица размера* $m \times n$ *и ранга* n *с целыми элементами,* g — *целый вектор,* d *равно наибольшей из абсолютных*

величин миноров n-го порядка матрицы G и миноров $(n+1)$-го порядка матрицы $(G\ g)$. Если система $Gy + g \geqslant 0$ разрешима в целых числах, то существует решение y^0 такое, что $||Gy^0 + g||_\infty \leqslant d$.

Автор благодарит А. Ю. Чиркова за полезное обсуждение этой работы.

ЛИТЕРАТУРА

1. **Веселов С. И.** Доказательство одной гипотезы о диофантовых линейных уравнениях. М., 1993. 5 с. Деп. в ВИНИТИ 19.03.93, № 667-В93.
2. **Веселов С. И., Шевченко В. Н.** Оценки минимального расстояния между точками некоторых целочисленных решеток // Комбинаторно-алгебраические методы в прикладной математике. Горький: Изд-во Горьк. ун-та, 1980. С. 26-33.
3. **Иванов Н. Н.** Верхние оценки компонент решений задачи целочисленного линейного программирования // Кибернетика. 1988. № 6. С. 112–114.
4. **Шевченко В. Н.** Качественные вопросы целочисленного программирования. М.: Наука; Физматлит, 1995.
5. **Borosh I., Flahive M., Rubin D., Treybig B.** A sharp bound for solutions of linear Diophantine equations // Proc. Amer. Math. Soc. 1989. V. 105, N 4. P. 844–846.
6. **Borosh I.,Treybig L. B.** Bounds on positive integral solutions of linear diophantine equations // Proc. Amer. Math. Soc. 1976. V. 55, N 2. P. 299–304.

Адрес автора:

Нижегородский
государственный университет,
пр. Гагарина, 23,
603600 Нижний Новгород,
Россия

Статья поступила
6 января 2000 г.