Доказательство обобщения гипотезы Бороша-Трейбига о диофантовых уравнениях.

Веселов С.И..

Нижний Новгород.

Обозначения.

$A(m \times n), B(p \times n)$ матрицы с целыми элементами, $rg\, A = m$, причем наибольший общий делитель миноров m - го порядка матрицы A равен 1;

$a_1, a_2, ..., a_n$ - столбцы A, $b_1, b_2, ..., b_n$ - столбцы B;

a, b - векторы с целыми координатами;

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

M - множество неотрицательных целых решений системы

$$Ax = a,\ Bx \equiv b\,(L);$$

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

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

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

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

$x' = (x'_1, x'_2, ..., x'_n)$ - произвольный вектор из M;

$K(A) = \{a_1 u_1 + a_2 u_2 + ... + a_n u_n | u_i \geq 0\,(i = 1, .., n)\}$ - конус, порожденный столбцами матрицы A.

В статье доказывается следующее утверждение.

Теорема. Если M непусто, то существует $x^0 \in M$ такой, что

$$x_i^0 \leq dl, \forall i \in N.$$

При $l = 1$ получается формулировка гипотезы Бороша-Трейбига $[1-3, 6]$, доказанная в $[4]$.

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, чем n и докажем его для системы с n неизвестными.

1. Предположим вначале, что из неравенства $u^T A \geq 0$ следует, что $u = 0$. Согласно теореме Минковского-Фаркаша, $K(A)$ совпадает тогда с m - мерным пространством, порожденным столбцами матрицы A. Следовательно, $-a_i \in K(A_i)$ при любом i, а это означает, во-первых, что $rgA_i = m$, и, во-вторых, что выпуклый конус C, состоящий из решений системы $Ax = 0, x \geq 0$, содержит вектор с положительными координатами, поэтому его размерность равна $n - m$.

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

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

$H(n \times (n-m))$ - матрица, столбцы $h^j = (h_1^j, ..., h_n^j)^T\ (j = 1, ..., n-m)$ которой являются базисом решетки целых решений системы $Ax = 0$;

$R((n - m) \times (n - m))$ - матрица, столбцы которой составляют базис решетки целых решений системы $BHy \equiv 0(L)$.

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

Для упрощения обозначений предположим, что I содержит 1 и

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

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

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

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

Векторы решетки F целых решений системы

$$Ax = 0,\, Bx \equiv 0(L)$$

находятся по формуле

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

Отсюда вытекает два следствия:

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

$$x'' = (x_1'', ..., x_n'')^T = (x_1', ..., x_n')^T + (s_1 t, (\bar{h}t + H^1 r)^T)^T$$

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

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

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

причем $|\det L^1| = |\det R^1|$.

Согласно определению множества I, для каждого $i \notin I$ в множестве $\{h^2, h^3, ..., h^{n-m}\}$ найдется вектор, i - ая компонента которого строго больше нуля. Следовательно, справедливы неравенства $h_i^2 + ... + h_i^{n-m} > 0,\, i \notin I$.Определим целое число λ из условий $\lambda l(h_i^2 + ... + h_i^{n-m}) + x_i'' \ge 0,\, i \notin I$ и построим вектор y по формуле:

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

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 B удалением первого столбца. Нам известно, что система имеет целое неотрицательное решение $z = (y_2, y_3, ..., y_n)$. Так как (4) эквивалентна системе вида $B^1 y \equiv b^1(L^1)$ и наибольший по модулю минор m - го порядка расширенной матрицы системы (3) не превышает $\dfrac{(y_1+1)d}{s_1} = \dfrac{(x_1''+1)d}{s_1} \le td$, то по предположению индукции система (3)-(4) имеет решение $z^0 = (z_1^0, ..., z_{n-1}^0)$ с компонентами, не превышающими $td|detL^1| = td|detR^1| = ld$. В качестве x^0 можно выбрать $(y_1, z_1^0, ..., z_{n-1}^0)$.

2. Предположим теперь, что существует $u \ne 0$ такой , что $u^T A \ge 0$. Если $u^T A > 0$, то выпуклая оболочка множества $\overline{M}$ неотрицательных решений (в том числе и нецелых) системы $Ax = a$ ограничена, следовательно, является выпуклой оболочкой своих вершин. В теории линейного программирования известно, компоненты вершин не превышают d. Так как $M \subseteq \overline{M}$ то утверждение справедливо. Если некоторые компоненты $u^T A$ равны нулю, то можно подвергнуть строки матрицы $(A\, a)$ унимодулярному преобразованию, и, с точностью до перестановки столбцов, получить матрицу вида

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

где подматрица $(a_1^1 ... a_v^1)$ имеет ранг k и состоит из k строк, а столбцы $(a_{v+1}^2 ... a_n^2)$ имеют положительную последнюю компоненту. Положим $a^3 = a^1 - a_{v+1}^1 x_{v+1}^1 - ... - -a_n^1 x_n^1$ и рассмотрим систему $a_1^1 x_1^1 + ... + a_v^1 x_v^1 = a^3$. Докажем, что d^1 - максимальный по абсолютной величине минор k - го порядка расширенной матрицы системы не превышает d.

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

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

либо неположительны, либо неотрицательны.

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

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

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

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

где Z есть величина алгебраического дополнения. Очевидно, что все числа либо неположительны, либо неотрицательны. Далее имеем

$$d \geq |\det \begin{pmatrix} a_1^1 ... a_{k-1}^1 \ a_{i_1}^1 ... a_{i_j}^1 \ a^1 \\ 0 \ ... \ 0 \quad a_{i_1}^2 ... a_{i_j}^2 \ a^2 \end{pmatrix}| =$$

$$|\sum_{i \in I} det \begin{pmatrix} a_1^1 ... a_{k-1}^1 \ a_{i_1}^1 ... a_{i_j}^1 \ a_i^1 \\ 0 \ ... \ 0 \quad a_{i_1}^2 ... a_{i_j}^2 \ a_i^2 \end{pmatrix} x_i^1 + det \begin{pmatrix} a_1^1 ... a_{k-1}^1 \ a_{i_1}^1 ... a_{i_j}^1 \ a^3 \\ 0 \ ... \ 0 \quad a_{i_1}^2 ... a_{i_j}^2 \ 0 \end{pmatrix} x_i^1| \geq$$

$$\geq |\det \begin{pmatrix} a_1^1 ... a_{k-1}^1 \ a_{i_1}^1 ... a_{i_j}^1 \ a^3 \\ 0 \ ... \ 0 \quad a_{i_1}^2 ... a_{i_j}^2 \ 0 \end{pmatrix} x_i^1| \geq d^1.$$

При $k = 1$ следует положить

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

$e = 1$ и повторить рассуждения.

По предположению индукции система (1) имеет решение $(x_1^0, ..., x_\nu^0)$, компоненты которого не больше d. Так как x_i^1 при $i \in \{\nu + 1, ..., n\}$ ограничен сверху решением задачи линейного программирования

$$\begin{array}{l} \max x_i, \\ Ax = a, \ x \geq 0, \end{array}$$

следовательно, не превышает d, то в качестве x^0 можно выбрать вектор $(x_1^0, ..., x_\nu^0, x_{\nu+1}^1, ..., x_n^1)$.

Сформулируем соответствующий результат относительно системы неравенств.

<u>Лемма.</u> [5] . Пусть $I \subseteq N, |\ I\ | = m, \overline{A}$ - матрица, состоящая из столбцов матрицы A с номерами из I, $\overline{H}$ - матрица, состоящая из строк матрицы H, номера которых составляют множество $N \setminus I$. Тогда $|\det \overline{A}| = |\det \overline{H}|$.

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

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

Из теоремы следует, что если (6) разрешима в целых числах, то существует решение y^0 такое, что $||HRy + x'||_\infty \leq d|\det R|$. 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

<u>Следствие.</u> Пусть $G(mxn)$ - матрица 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 $Gy + g \geq 0$ разрешима в целых числах, то существует решение y^0 такое, что $||Gy + g||_\infty \leq d$.

Список литературы.

1. Borosh I.,Treybig B. Bounds on positive integral solutions of linear diophantine equations.// Proc. Amer. Math. Soc. - 1976, v.55,N 2, pp.299-304.

2. Иванов Н.Н. Верхние оценки компонент решений задачи целочисленного линейного программирования. // Кибернетика - 1988, N 6, с. 112-114.

3. Borosh I., Flahive M., Rubin D. and Treybig B. A sharp Bound for solutions of linear diophantine equations.// Proc. Amer. Math. Soc. - 1989, v.105,N 4, pp.844-846.

4. Веселов С.И. Доказательство одной гипотезы о диофантовых линейных уравнениях. // Деп. в ВИНИТИ, 1993, N 667-B93, 5с.

5. Веселов С.И.,Шевченко В.Н. Оценки минимального расстояния между точками некоторых целочисленных решеток. // Комбинаторно-алгебраические методы в прикладной математике.- Горький:Горьк.ун-т,1980 - с. 26-33.

6. Шевченко В.Н. Качественные вопросы целочисленного программирования. // М.: Наука-Физматлит, 1995, 190с.