A SHARP BOUND FOR SOLUTIONS OF LINEAR DIOPHANTINE EQUATIONS

I. BOROSH, M. FLAHIVE, D. RUBIN AND B. TREYBIG

(Communicated by Thomas H. Brylawski)

Abstract. Let $Ax = b$ be an $m \times n$ system of linear equations with rank $m$ and integer coefficients. Denote by $Y$ the maximum of the absolute values of the $m \times m$ minors of the augmented matrix $(A, b)$. It is proved that if the system has an integral solution, then it has an integral solution $x = (x_i)$ with $\max |x_i| \leq Y$. The bound is sharp.

I. Introduction

The existence of small integral solutions to systems of linear equations with integral coefficients has been discussed previously in [1, 2,3,4,5,6,7,8,11]. Two types of problems have been considered.

In the first type the system is assumed to have a nonzero integer solution and the existence of a small solution is proved. A typical result of this type is the classical Siegel's Lemma [7] for homogeneous systems which has been used extensively in the theory of transcendental numbers. This result was generalized in [1] where the existence of a small integral basis for systems of linear homogeneous equations is proved.

In the second type of problems the system is assumed to have a nontrivial nonnegative integral solution and the existence of a small solution with these properties is proved. More work has been devoted recently to this type because of its implications for the complexity of integer programming [11]. In [3] the conjecture was made that for the second type of problems a nonnegative integral solutions exists with components bounded by the $p \times p$ minors of the augmented matrix, where $p$ is the rank of the matrix. This conjecture was proved in several special cases and weaker results were proved in the general case in [4,5]; however, it is still open in the general case.

In [6] the corresponding conjecture for the first type problem is discussed and proved under various additional conditions. In particular it is proved for...
an $m \times n$ system of rank $m$ when $n - m \leq 8$. The object of this paper is to prove this latter conjecture, namely:

If $Ax = b$ is an $m \times n$ system of linear equations of rank $m$ with integer coefficients and if the system has a nonzero integer solution, then it has an integral solution $x = (x_i)$ with $0 < \max |x_i| \leq Y$, where $Y$ is the maximum of the absolute values of the $m \times m$ minors of $(A, b)$.

This bound is sharp as we can see in the case $A = (\mathcal{A} | 0)$ and $\mathcal{A}$ is a unimodular matrix, or if (1) $A$ is an $m \times (m + 1)$ matrix with the property that the gcd of all the $m \times m$ minors of $A$ is 1, and (2) $b = 0$. Such an $A$ can be obtained, for example, by taking $m$ rows of an $(m + 1) \times (m + 1)$ unimodular matrix.

2. The main result

Let $Ax = b$ be a matrix equation of the form

$$
\begin{bmatrix}
    a_{11} & \cdots & a_{1n} \\
    \vdots & \ddots & \vdots \\
    a_{m1} & \cdots & a_{mn}
\end{bmatrix}
\begin{bmatrix}
    x_1 \\
    \vdots \\
    x_n
\end{bmatrix}
= \begin{bmatrix}
    a_{1,n+1} \\
    \vdots \\
    a_{m,n+1}
\end{bmatrix}
$$

where each $a_{ij}$ is an integer. Assume that $n > m$, that the rows of $A$ are linearly independent, and that (1) has a solution $y = (y_i)$, where each $y_i$ is an integer.

The main result of this paper is the following:

**Theorem.** If $Ax = b$ has a solution in integers, it has such a solution within the bound $Y$.

**Proof.** Since $A$ has full row rank, we may assume, without loss of generality, that the first $m$ columns of $A$ are linearly independent. Accordingly, partition $A$ as $(B, N)$, where $B$ is $m \times m$ and nonsingular, and $N$ is $m \times (n - m)$. Similarly, partition $x$ as $(x_B^T, x_N^T)^T$, where $x_B^T = (x_1, x_2, \ldots, x_m)$ and $x_N^T = (x_{m+1}, \ldots, x_n)$. Let $\delta$ be the determinant of $B$.

The system (1) can be expanded as

$$
Bx_B + Nx_N = b
$$

and the general solution to (2) in real numbers is given by

$$
x_B = B^{-1}(b - Nx_N), \quad x_N \text{ arbitrary}.
$$

From (3), it follows that finding integer solutions to (1) is equivalent to finding integer solutions $x_N$ to

$$
B^{-1}b \equiv B^{-1}Nx_N \pmod{1}.
$$

Since (1) is assumed to have a solution in integers, it follows that (4) also has a solution. Gomory [10] has shown that if (4) has an integer solution, then it has a nonnegative integer solution with

$$
x_{m+1} + x_{m+2} + \cdots + x_n \leq |\delta| - 1.
$$
(See also Theorem 5 on p. 275 of [9].)

Let $x_N$ be such a solution to (4), and substitute $x_N$ into (3) to compute $x_B$. Then $x = (x_B^T, x_N^T)^T$ is an integer solution to (1). The proof will be completed when we demonstrate that each component of $x$ has absolute value at most $Y$.

For $i = m + 1, m + 2 \ldots, n$ it follows immediately from (5) that $|x_i| \leq Y$. For $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n - m$ let $\delta_{ij}$ be the determinant of the matrix obtained by replacing the $i$ th column of $B$ with the $j$ th column if $N$ (i.e., by the $(j + m)$ th column of $A$), and let $\delta_{ij0}$ be the determinant of the matrix obtained by replacing the $i$ th column of $B$ with $b$. It now follows from Cramer's rule and (3) that

$$|x_i| = |\delta_{i0} - \delta_{i1}x_{m+1} - \delta_{i2}x_{m+2} - \cdots - \delta_{i,n-m}x_n|/|\delta|$$

$$\leq (|\delta_{i0}| + |\delta_{i1}|x_{m+1} + |\delta_{i2}|x_{m+2} + \cdots + |\delta_{i,n-m}|x_n)/|\delta|$$

$$\leq Y(1 + x_{m+1} + x_{m+2} + \cdots + x_n)/|\delta|$$

$$\leq Y(1 + (|\delta| - 1))/|\delta| \quad \text{(by (5))}$$

$$\leq Y.$$

Hence all components of $x$ are bounded in absolute value by $Y$, completing the proof of the theorem.

References


Department of Mathematics, Texas A&M University, College Station, Texas 77843
Department of Mathematics, University of Lowell, Lowell, Massachusetts 01854
Department of Mathematics, University of North Carolina, Chapel Hill, North Carolina 27599