PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 105, Number 4, April 1989

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

Received by the editors December 11, 1987 and, in revised form, August 17, 1988.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 15A36; Secondary 11D04, 90C10.

Key words and phrases. Linear equation, integral solutions, minors, rank, bound.

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 $A = (A' \mid 0)$ and 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

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

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 δ be the determinant of B.

The system (1) can be expanded as

$$Bx_B + Nx_N = b \tag{2}$$

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

$$x_B = B^{-1}(b - Nx_N), \qquad x_N \text{ arbitrary.} \tag{3}$$

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

$$B^{-1}b \equiv B^{-1}Nx_N (\operatorname{mod} 1). \tag{4}$$

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

$$x_{m+1} + x_{m+2} + \cdots + x_n \leq |\delta| - 1. \tag{5}$$

(See also Theorem 5 on p. 275 of [9].)

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

For $i = m+1, m+2 \dots, n$ it follows immediately from (5) that $|\bar{x}_i| \le Y$. For $i = 1, 2, \dots, m$ and $j = 1, 2, \dots, n-m$ let δ_{ij} be the determinant of the matrix obtained by replacing the ith column of B with the jth column if N (i.e., by the $(j+m)$th column of A), and let δ_{i0} be the determinant of the matrix obtained by replacing the ith column of B with b. It now follows from Cramer's rule and (3) that

$$\begin{aligned}
|\bar{x}_i| &= |\delta_{i0} - \delta_{i1}\bar{x}_{m+1} - \delta_{i2}\bar{x}_{m+2} - \cdots - \delta_{i,n-m}\bar{x}_n|/|\delta| \\
&\le (|\delta_{i0}| + |\delta_{i1}|\bar{x}_{m+1} + |\delta_{i2}|\bar{x}_{m+2} + \cdots + |\delta_{i,n-m}|\bar{x}_n)/|\delta| \\
&\le Y(1 + \bar{x}_{m+1} + \bar{x}_{m+2} + \cdots + \bar{x}_n)/|\delta| \\
&\le Y(1 + (|\delta| - 1))/|\delta| \quad (\text{by}(5)) \\
&\le Y.
\end{aligned}$$

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

References

1. E. Bombieri and J. Vaaler, *On Siegel's Lemma*, Invent Math. **73** (1983), 11–32.
2. I. Borosh, *A sharp bound for positive solutions of homogeneous linear diophantine equations*, Proc. Amer. Math. Soc. **60** (1976), 19–21.
3. I. Borosh and L. B. Treybig, *Bounds on positive integral solutions of linear diophantine equations*, Proc. Amer. Math. Soc. **55** (1976), 299–304.
4. ——, *Bounds on positive integral solutions of linear diophantine equations*. II, Canad. Math. Bull. **22** (3) (1979), 357–361.
5. I. Borosh, M. Flahive, and B. Treybig, *Small solutions of linear diophantine equations*, Discrete Math. **58** (1986), 215–220.
6. ——, *Small solutions of linear diophantine equations*. II. (preprint).
7. J. W. S. Cassels, *An introduction to diophantine approximations*, Cambridge Tracts in Math. Phys., no. 45, Cambridge Univ. Press, New York, 1957.
8. J. von zur Gathen and M. Sieveking, *A bound on solutions of linear equalities and inequalities*, Proc. Amer. Math. Soc. **72** (1978), 155–158.
9. R. S. Garfinkel and G. L. Nemhauser, *Integer programming*, John Wiley and Sons, New York, 1972.
10. R. E. Gomory, *Some polyhedra related to combinatorial problems*, Linear Algebra Appl. **2** (1969), 451–558.
11. C. H. Papadimitriou, *On the complexity of integer programming*, J. Assoc. Comput. Mach. **28** (1981), 765–768.

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