

## BOUNDS ON POSITIVE INTEGRAL SOLUTIONS OF LINEAR DIOPHANTINE EQUATIONS

I. BOROSH AND L. B. TREYBIG

**ABSTRACT.** Assuming the existence of a solution, we find bounds for small solutions  $x$  of the finite matrix equation  $Ax = B$ , where each entry of  $A$ ,  $B$  is an integer, and  $x$  is a nontrivial column vector with nonnegative integer entries.

**0. Introduction.** In [1], [5] and [6] there arise in a topological setting, systems of linear equations with integer coefficients. The problem is to find a bound  $K$  depending on the coefficients only, such that if the given system has a nontrivial solution in nonnegative integers, then it has such a solution with all entries bounded by  $K$ . In [6] L. B. Treybig gives such a bound  $K$  using an inductive definition, and proves that a new solution can be found bounded by  $K$  and with the additional property that each entry is bounded by the corresponding entry of the given solution. The purpose of this paper is to find some easily stated bounds which are much smaller than those given by Treybig [6] but which do not satisfy necessarily the additional property.

*Notation.* Throughout this paper  $A$  will denote an  $m \times n$  matrix,  $B$  an  $m \times 1$  matrix, both with integral entries. We will consider the system of equations

$$(1) \quad Ax = B$$

where  $x$  is a column whose entries are  $x_1, \dots, x_n$ . By  $(A|B)$  we denote the augmented matrix of the system (1). Let  $r$  denote the rank of  $A$ ,  $M_1$  the maximum of the absolute values of all the minors of  $A$  of order  $r$ ,  $M_2$  the maximum of the absolute values of all minors of order  $r$  of  $(A|B)$ , and  $M$  the maximum of the absolute values of all the minors of  $(A|B)$ . All our bounds will be stated in terms of  $m$ ,  $n$ ,  $M_1$ ,  $M_2$ ,  $M$ , and therefore we may assume from now on without loss of generality that  $r = m \leq n$ .  $[x]$  will denote, as usual, the largest integer not exceeding  $x$ .

*Results.* §1 is devoted to the case  $m = 1$ . We prove that the bound in this case is the maximum of the absolute value of the coefficients. It is easy to see that this bound is sharp.

§2 considers the case  $r = n - 1$  and we find the bound  $M_2(1 + 1/M_1)$ . The homogeneous case,  $B = 0$ , is discussed in §3 and the bound  $M$  is obtained.

---

Received by the editors June 21, 1974, and, in revised form, March 10, 1975.

*AMS (MOS) subject classifications* (1970). Primary 15A06; Secondary 10B05.

*Key words and phrases.* Linear equations, integer entries, nonnegative integral solution, bounds, polyhedral convex cones, minors, adjoint matrix.

© American Mathematical Society 1976

§4 deals with the general case. First, we prove that if the homogeneous system  $Ax = 0$  has no nontrivial solution in nonnegative integers  $x_i$ , then every nonnegative solution of (1) in integers satisfies  $\max x_i \leq M_2$ . We then find a bound of the order of  $M^2$  valid in all cases.

The result leads us to conjecture that if (1) has a solution in nonnegative integers, then it has such a solution bounded by  $M_2$ . However, we could not prove this conjecture except for the particular cases already mentioned, nor could we provide an example to disprove it.

#### 1. The case $m = 1$ .

**THEOREM 1.** *Let  $a_1, \dots, a_n$  be integers not all 0, and  $b$  an integer. Suppose the equation*

$$(2) \quad a_1x_1 + a_2x_2 + \dots + a_nx_n = b$$

*has a nontrivial solution in nonnegative integers  $x_1, \dots, x_n$ . Then (2) has such a solution  $y_1, \dots, y_n$  and, in addition,*

$$(3) \quad y_i \leq \max(|a_1|, \dots, |a_n|, |b|), \quad i = 1, \dots, n.$$

**PROOF.** We may assume without loss of generality that not all the  $a_i$  have the same sign, otherwise it is clear that any solution of (2) also satisfies (3). Assume without loss of generality  $a_1 > 0$ ,  $a_2 < 0$ , and  $b \geq 0$ . If  $b = 0$ , we have the obvious solution  $x_1 = -a_2$ ,  $x_2 = a_1$ ,  $x_3 = \dots = x_n = 0$ . We may assume, therefore,  $b > 0$ .

The proof proceeds by induction on  $n$ , and the inductive step is adapted from the method described in [4] for the solution of linear diophantine equations. The case  $n = 1$  is obvious, but we will also need the case  $n = 2$ . Consider the equation

$$(4) \quad a_1x_1 + a_2x_2 = b.$$

Let  $x_1, x_2$  be a nonnegative solution of (4) and let  $k = [x_2/a_1]$ . Since  $a_1x_1 + a_2x_2 = b > 0$ , we have  $-x_1/a_2 - x_2/a_1 > 0$  therefore,  $k = [x_2/a_1] \leq [x_1/-a_2]$ .

Define  $y_1 = x_1 + ka_2$ ,  $y_2 = x_2 - ka_1$ . Then  $(y_1, y_2)$  is a nonnegative solution of (4). We see that  $y_2$  is the remainder of the division of  $x_2$  by  $a_1$ , and therefore  $y_2 < a_1$ .

$$y_1 = x_1 + ka_2 = x_1 + \frac{x_2 - y_2}{a_1} a_2 = \frac{b - a_2y_2}{a_1} \leq \frac{\max(|b|, |a_2|)(1 + y_2)}{a_1}.$$

Since  $1 + y_2 \leq a_1$  and  $a_1 \geq 1$ , we get  $y_1 \leq \max(|b|, |a_2|)$ .

Assume now that Theorem 1 holds for equations with less than  $n$  unknowns. As above, in equation (2), we assume that  $a_1 > 0$ ,  $a_2 < 0$ . Let  $g = \text{g.c.d.}(a_1, a_2)$  and  $x_1, \dots, x_n$  be a nonnegative solution of (2) where no  $x_i = 0$ . Let  $u = |a_1x_1 + a_2x_2|/g$ . Then  $u, x_3, \dots, x_n$  is a nonnegative solution of

$$(5) \quad \varepsilon gu + a_3x_3 + \dots + a_nx_n = b,$$

where  $\varepsilon = +1$  or  $\varepsilon = -1$ , according as  $a_1x_1 + a_2x_2$  is positive or not. By the induction hypothesis, (5) has, therefore, an integral nonnegative solution  $u', y_3, \dots, y_n$  such that

$$\max(u', y_3, \dots, y_n) \leq \max(g, |a_3|, \dots, |a_n|, |b|) \leq \max(|a_1|, \dots, |a_n|, |b|).$$

The equation

$$(6) \quad (a_1/g)x_1 + (a_2/g)x_2 = \epsilon u'$$

has an integral solution since  $\text{g.c.d.}(a_1/g, a_2/g) = 1$ , and since  $a_1 a_2 < 0$ , the homogeneous equation  $(a_1/g)x_1 + (a_2/g)x_2 = 0$  has a positive integral solution. Therefore (6) has an integral positive solution and, by the case previously considered, it has a solution  $y_1, y_2$  such that  $y_1 \geq 0, y_2 \geq 0$ , and

$$\max(y_1, y_2) \leq \max(|a_1|/g, |a_2|/g, u') \leq \max(|a_1|, \dots, |a_n|, |b|).$$

## 2. The case $r = n - 1$ .

**THEOREM 2.** *If  $r = n - 1$  and the system (1) has a nontrivial solution in nonnegative integers  $x_i$ , then the system (1) has such a solution  $(y_1, \dots, y_n)$  satisfying the additional condition*

$$\max y_i \leq M_2(1 + 1/M_1) \leq 2M_2.$$

**PROOF.** Let  $A'$  be an  $m \times m$  submatrix of  $A$  whose minor has the maximal absolute value. Since we assume  $r = m$ , we have  $a = \det A' \neq 0$ , and we may assume without loss of generality that  $a > 0$ , so that  $a = M_1$ . We may also rename the variables in such a way that  $A'$  sits in the left corner of  $A$ . Multiplying the two sides of (1) by  $\text{adj } A'$  we get

$$(7) \quad a \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} x_{m+1} = \begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix},$$

where the  $b_i$  are minors of  $A$ , and the  $c_i$  are minors of  $(A|B)$  for  $i = 1, \dots, m$ . Denote by  $x_1, \dots, x_m, x_{m+1}$  a positive solution of (7) and define

$$(8) \quad k = \min\{[x_{m+1}/a], [x_i/|b_i|]\};$$

the minimum is taken over all  $i = 1, \dots, m$  such that  $b_i < 0$ .

We may assume that not all  $c_i$  are 0, since otherwise the existence of a positive solution implies  $b_i < 0$  for  $i = 1, \dots, m$ , and we get the solution  $x_{m+1} = a, x_i = -b_i, i = 1, \dots, m$ . Define  $y_{m+1} = x_{m+1} - ak, y_i = x_i + b_i k, i = 1, \dots, m$ . It is clear that  $y_1, \dots, y_{m+1}$  is a nonnegative solution of (7). It remains to estimate  $y_1, \dots, y_{m+1}$ .

If  $k = [x_{m+1}/a]$ , then  $y_{m+1}$  is the remainder of the division of  $x_{m+1}$  by  $a$  and, therefore,  $y_{m+1} < a \leq M_2$ .

If  $k = [x_j/|b_j|], 1 \leq j \leq m, b_j < 0$ , then

$$y_{m+1} = x_{m+1} - a[x_j/|b_j|] = x_{m+1} - a(x_j - y_j)/|b_j|$$

and  $y_j < |b_j|$ ; therefore

$$y_{m+1} = (-x_{m+1}b_j - ax_j + ay_j)/|b_j| = (-c_j + ay_j)/|b_j|;$$

$$y_{m+1} \leq (\max(|c_j|, a)(1 + y_j))/|b_j| \leq \max(|c_j|, a) \leq M_2.$$

Let  $i$  be such that  $1 \leq i \leq m$ . If  $b_i \geq 0$ , then  $c_i \geq 0$  and  $ay_i \leq c_i, y_i \leq c_i \leq M_2$ . If  $b_i < 0$  and  $k = [x_i/|b_i|]$ , then  $y_i$  is the remainder of the division of  $x_i$

by  $|b_i|$  and, therefore,  $y_i < b_i \leq M_2$ . If  $b_i < 0$ , and

$$k = [x_{m+1}/a] = (x_{m+1} - y_{m+1})/a,$$

then

$$y_i = x_i + b_i k = (c_i - b_i y_{m+1})/a \leq \sup(|b_i|, |c_i|) \leq M_2.$$

If  $b_i < 0$  and  $k = [x_j/|b_j|] = (x_j - y_j)/|b_j|$  and  $1 \leq j \leq m$ ,  $j \neq i$ , then  $b_j < 0$ ,  $y_j < |b_j|$ .

$$\begin{aligned} ay_i &= ax_i - \frac{ab_i(x_j - y_j)}{b_j} = \frac{b_j(c_i - b_i x_{m+1}) - b_i(c_j - b_j x_{m+1}) + ab_i y_j}{b_j}, \\ y_i &= \frac{b_j c_i - b_i c_j + ab_i y_j}{ab_j} \leq \frac{|b_i| \max(a, |c_j|)(1 + y_j) + |b_j c_i|}{a|b_j|} \\ &\leq \max(a, |c_j|) + |c_i|/a \leq M_2(1 + 1/M_1). \end{aligned}$$

### 3. The homogeneous case.

LEMMA 1. *If  $Ax = 0$  has a nontrivial nonnegative solution and  $n - r \geq 2$ , then there exists a submatrix  $A'$  of  $A$  of order  $m \times (n - 1)$ , such that  $A'x = 0$  has a nontrivial nonnegative solution.*

PROOF. Let  $x$  be a nontrivial nonnegative solution of  $Ax = 0$ . If  $x_i = 0$  for some  $i$ , then  $A'$  is obtained by deleting the column  $i$  from  $A$ . Assume therefore that  $x_i > 0$ ,  $i = 1, \dots, n$ . Since  $n \geq r + 2$ , there exists a solution  $y$  of  $Ax = 0$  such that  $x, y$  are linearly independent. Let

$$\lambda = \max_{i=1, \dots, n} (-y_i/x_i) = -y_l/x_l;$$

then for each  $i$ ,

$$\lambda x_i + y_i \geq -(y_i/x_i)x_i + y_i \geq 0 \quad \text{and} \quad \lambda x_l + y_l = 0.$$

$A'$  is obtained by deleting column  $l$  from  $A$ .

THEOREM 3. *If  $Ax = 0$  has a nontrivial nonnegative solution  $x$  in integers  $x_i$ , then it has such a solution  $y$ , with  $y_i \leq M$ .*

PROOF. By using Lemma 1 we see that we can choose one of the variables to be 0 and get a smaller system  $A'x = 0$  which satisfies the hypothesis. Using Lemma 1 repeatedly we find an  $m \times n'$  matrix  $A'$  of rank  $r'$  such that  $n' = r' + 1$  and which by Cramer's rule has a positive integral solution given by minors of  $A'$ .

### 4. The general case.

THEOREM 4. *If  $Ax = 0$  has no nontrivial nonnegative solution, then every nonnegative integral solution  $y$  of (1) satisfies  $y_i \leq M_2$  for  $i = 1, \dots, n$ .*

PROOF. Applying Gordan's theorem [3, p. 31] to  $A$  we know that there exists a vector  $z = (z_1, \dots, z_m)$  such that all the  $n$  entries of  $zA$  are positive. Let  $C$  denote the set of all  $z$  such that all the entries of  $zA$  are nonnegative.  $C$  is a polyhedral convex cone [2] in the  $m$ -dimensional euclidian space, and each edge  $u$  of  $C$  satisfies  $A^T u \geq 0$  and

$$(8) \quad A'^T u = 0$$

for some  $m \times (m-1)$  submatrix  $A'$  of  $A$  of rank  $(m-1)$ , where  $T$  denotes the transpose. (8) has a nontrivial integral solution whose entries are the minors of order  $m-1$  of  $A'$ .  $C$  is  $m$ -dimensional and therefore its edges are not all contained in any hyperplane; therefore, for any  $i$ ,  $1 \leq i \leq m$ , there exists an edge  $u = (u_1, \dots, u_m)$  whose entries are minors of order  $m-1$  of some submatrix  $A'$  or  $A$  of order  $m \times m-1$  and such that

$$(9) \quad a_{1i}u_1 + \dots + a_{mi}u_m \neq 0.$$

Let  $x$  be any nonnegative integral solution of (1); then  $uAx = ub$ . Let  $uA = (A_1, \dots, A_n)$ ; then  $A_j \geq 0$  for  $u = 1, \dots, m$  since  $u$  is an edge of  $C$ , and  $A_i > 0$ , by (9).  $A_1, \dots, A_n$  and  $ub$  are minors of  $(A|B)$  by the Laplace expansion theorem. They are therefore integers, and

$$A_i x_i \leq M_2, \quad x_i \leq M_2.$$

**THEOREM 5.** *If (1) has a nontrivial nonnegative integral solution  $x = (x_1, \dots, x_n)$ , and  $\sum_{i=1}^n x_i$  is minimal over all such solutions, then*

- (i)  $x_i \leq M$  for at least some  $i$ ,
- (ii)  $x_j \leq Mm(1 + (n-1)M)$  for  $1 \leq j \leq n$ ,
- (iii) if  $Q \geq 1$  and  $w$  is the number of  $x_i$  such that  $x_i > QM$ , then  $w \leq m(1 + nM)/(Q + mM)$ .

**PROOF.** We may assume  $n > m = \text{rank } A$ , since otherwise  $M$  is trivially a bound. Let  $x$  be the minimal solution described in the statement of the theorem and assume that not all the  $x_i$  are bounded by  $M$ . Rename the variables in such a way that  $x_1, \dots, x_v$  are all the  $x_i$  which are bigger than  $M$ , hence  $v \geq 1$ .

**Case I.** There is a  $v \times v$  submatrix of  $X = (a_{ij})$  ( $1 \leq i \leq m$ ,  $1 \leq j \leq v$ ) which is nonsingular. Let  $D$  be the nonzero determinant of this matrix. Then

$$x_p = (a'_{p,v+1}x_{v+1} + \dots + a'_{pn}x_n + b_p)/D$$

for  $1 \leq p \leq v$ , where  $\pm a'_{p,i}$ ,  $\pm b_p$ ,  $D$  are minors of  $(A|B)$ . Thus

$$x_p \leq (n-v)M^2 + M \leq (n-1)M^2 + M$$

for  $1 \leq p \leq v$  and  $x_p \leq M$  for  $v+1 \leq p \leq n$ .

**Case II.** There is no  $v \times v$  submatrix of  $X$  which is nonsingular. We may assume without loss of generality that the first  $q$  rows of  $X$  form a basis for the row space of  $X$ , and we may assume further that the matrix  $Y = (a_{ij})$  ( $1 \leq i, j \leq q$ ) is nonsingular. Let  $D = \det Y \neq 0$ . Solving for  $x_1, \dots, x_q$  we get

$$(10) \quad x_i = (a'_{i,q+1}x_{q+1} + \dots + a'_{iv}x_v + \dots + a'_{in}x_n + b_i)/D$$

where  $\pm a'_{ij}$ ,  $\pm b_i$ ,  $D$  are minors of  $(A|B)$  and  $1 \leq i \leq q$ . Now consider some fixed  $p$  where  $q+1 \leq p \leq v$ . Recall that  $x_p > M$  and  $x_i \leq M$  for  $v+1 \leq i \leq n$ . If  $\sum_{i=1}^q a'_{ip} > -D$ , consider the solution  $y$  of (1) defined by

$$y_j = \begin{cases} x_j & \text{if } q+1 \leq j \leq n \text{ and } j \neq p, \\ x_p - D & \text{if } j = p, \\ x_j - a'_{jp} & \text{if } 1 \leq j \leq q. \end{cases}$$

Then  $\sum_{j=1}^n y_j = \sum_{j=1}^n x_j - D - \sum_{j=1}^q a'_{jp} < \sum_{j=1}^n x_j$ , a contradiction. If  $\sum_{j=1}^q a'_{jp} < -D$ , consider the solution  $y$  of (1) defined by

$$y_j = \begin{cases} x_j & \text{for } q+1 \leq j \leq n, \quad j \neq p, \\ x_p + D & \text{for } j = p, \\ x_j + a'_{jp} & \text{for } 1 \leq j \leq q. \end{cases}$$

As above, we get  $\sum_{j=1}^n y_j < \sum_{j=1}^n x_j$ , a contradiction. Therefore  $\sum_{i=1}^q a'_{ip} = -D$  for  $q < p \leq v$ . We add now all the  $x_i$ ,  $1 \leq i \leq q$ , defined by (10) to obtain:

$$(11) \quad \sum_{i=1}^q x_i = \left\{ -D \sum_{i=q+1}^v x_i + \sum_{i=v+1}^n \left( \sum_{j=1}^q a'_{ji} \right) x_i + \sum_{i=1}^q b_i \right\} / D,$$

$$(12) \quad \sum_{i=1}^v x_i \leq \sum_{i=v+1}^n \left| \sum_{j=1}^q a'_{ji} \right| x_i + \sum_{i=1}^q |b_i|,$$

$$(13) \quad \sum_{i=1}^v x_i \leq q(n-v)M^2 + qM.$$

Thus  $x_i \leq m(n-1)M^2 + mM$  for  $1 \leq i \leq v$ , and  $x_i \leq M$  for  $v+1 \leq i \leq n$ . If  $v = n$ , then (13) implies that  $nM \leq mM$ , so some  $x_i \leq M$ . Note also that (12) holds also for Case I. If  $Q \geq 1$  and  $w$  denotes the number of  $x_i > QM$ , then by (13):

$$wQM \leq q(n-v)M^2 + qM, \quad wQM \leq m(n-w)M^2 + qM,$$

or

$$w \leq m(1 + nM) / (Q + mM).$$

## REFERENCES

1. W. Haken, *Theorie der Normalflächen*, Acta Math. **105**(1961), 245–375. MR25 #4519a.
2. A. J. Goldman and A. W. Tucker, *Polyhedral convex cones*, Linear Inequalities and Related Systems, Ann. of Math. Studies, no. 38, Princeton Univ. Press, Princeton, N.J., 1956, pp. 19–40. MR19, 446.
3. O. L. Mangasarian, *Nonlinear programming*, McGraw-Hill, New York, 1969, p. 31. MR40 #5263.
4. I. Niven and H. S. Zuckerman, *An introduction to the theory of numbers*, 2nd ed., Wiley, New York, 1966, pp. 107–109. MR33 #3981.
5. H. Schubert, *Bestimmung der Primfaktorzerlegung von Verkettungen*, Math. Z. **76** (1961), 116–148. MR25 #4519b.
6. L. B. Treybig, *Bounds in piecewise linear topology*, Trans. Amer. Math. Soc. **201**(1975), 385–405.

DEPARTMENT OF MATHEMATICS, TEXAS A & M UNIVERSITY, COLLEGE STATION, TEXAS 77843