A BOUND ON SOLUTIONS OF LINEAR INTEGER EQUALITIES AND INEQUALITIES

JOACHIM VON ZUR GATHEN AND MALTE SIEVEKING

Abstract. Consider a system of linear equalities and inequalities with integer coefficients. We describe the set of rational solutions by a finite generating set of solution vectors. The entries of these vectors can be bounded by the absolute value of a certain subdeterminant. The smallest integer solution of the system has coefficients not larger than this subdeterminant times the number of indeterminates. Up to the latter factor, the bound is sharp.

Let $A$, $B$, $C$, $D$ be $m \times n$, $m \times 1$, $p \times n$, $p \times 1$-matrices respectively with integer entries. The rank of $A$ is $r$, and $s$ is the rank of the $(m + p) \times n$-matrix $(C \ B)$. Let $M$ be an upper bound on the absolute values of those $(s - 1) \times (s - 1)$- or $s \times s$-subdeterminants of the $(m + p) \times (n + 1)$-matrix $(C \ B)$, which are formed with at least $r$ rows from $(A, B)$.

Theorem. If $Ax = B$ and $Cx \geq D$ have a common integer solution, then they have one with coefficients bounded by $(n + 1)M$.

Let $M_1$, $M_2$, and $M_3$ be upper bounds on the absolute values of the $r \times r$-subdeterminants, the subdeterminants, and the entries of $(A, B)$ respectively. Taking the $n \times n$-identity matrix for $C$ and $D = 0$, we have the following

Corollary. If $Ax = B$ has a nonnegative integer solution, then it has one with coefficients bounded by $(n + 1)M_1$.

S. Cook [4] obtained a bound of the order of $M_3^2n^r$ in this case. I. Borosh and L. B. Treybig conjecture that one can always have the bound $M_1$. For many cases, this bound would be sharp. They give an elegant proof for $M_2^2$ in [2]. In [1], [3] they obtain $M_1$ in the cases where $r = n - 1$ and for homogeneous systems (only nontrivial solutions being considered), and $nrM_1$ if the matrix has no $r \times r$-subdeterminants which are zero. Their work arose from topological questions, while Cook’s and our aim was to prove that the solvable linear integer programs form a $NP$-complete set (see Remarks 2 and 3).

For the proof of the theorem we first note that it suffices to consider the case $s = n$. For if $s < n$, then choose an integer solution $y$, let $e_i$ be 1 or $-1$ according to whether $y_i$ is $> 0$ or $< 0$. To the given system add $n - s$
inequalities $e_i x_i > 0$ so that the resulting system has rank $n$. Then the theorem for this system implies that for the one with rank $s$.

Let $S = \{A = B\} \cap \{C > D\} = \{x \in \mathbb{Q}^n: Ax = B \text{ and } Cx > D\}$, $H = \{A = 0\} \cap \{C > 0\}$. The $i$th row $A_i$ of $A$ corresponds to a linear form on $\mathbb{Q}^n$, which we also denote by $A_i$, and similarly for $C$. Let $I \subseteq \{1, \ldots, p\}$. If $S \cap \bigcap_{i \in I} \{C_i = D_i\}$ is nonempty and the matrix with rows $A_1, \ldots, A_m$ and $C_i$ for $i \in I$ has rank $n$, then the single vector in this set is called a vertex of $S$.

We call $H \cap \bigcap_{i \in I} \{C_i = 0\}$ an edge of $H$, if it is not equal to $\{0\}$, and the matrix with rows $A_1, \ldots, A_m$ and $C_i$ for $i \in I$ has rank $n - 1$. We may assume $\# I = n - r$ for a vertex, and $\# I = n - r - 1$ for an edge. Choose a nonzero vector in each edge of $H$. Let $F$ be the set of all these vectors, and $E$ the set of all vertices of $S$.

**LEMMA.** $S = \text{conv}(F) + \mathbb{Q}_+ F$.

Here $\text{conv}(E) + \mathbb{Q}_+ F$ denotes the set of all $\sum_{e \in E} \lambda_e e + \sum_{f \in F} \mu_f f$ with nonnegative rational numbers $\lambda_e$, $\mu_f$, and $\sum_{e \in E} \lambda_e = 1$. The proof is by induction on $n$. $n = 0$ is trivial, the empty sum being $0$. Obviously $\text{conv}(E) + \mathbb{Q}_+ F \subset S$. So let $n > 0$, $x \in S$.

**Case 1.** $r > 0$.

Suppose that $A_{1k} \neq 0$, and let $u: [A_1 = 0] \to \mathbb{Q}^{n-1}$ be the projection that takes the $k$th coordinate to zero. $u$ is an isomorphism of vector spaces. $A'_j = A_j \circ u^{-1}$ and $C'_i = C_i \circ u^{-1}$ are linear forms on $\mathbb{Q}^{n-1}$, and the rank of the matrix $(A'_i)$ is $n - 1$. Let $B'_j = 0$, $D'_j = D_j - C_j(x)$, $E' = u(E - x)$, $F' = u(F)$. Here $E - x = \{e - x: e \in E\}$. We show that $E'$ contains every vertex and $F'$ a nonzero vector of each edge with respect to $A'$, $B'$, $C'$, $D'$. Let $\{y\} = [A' = B'] \cap \bigcap_{i \in I} \{C_i = D_i\}$ be a vertex of $[A' = B'] \cap \{C' > D'\}$. Then $\{u^{-1}(y) + x\} = [A = B] \cap \bigcap_{i \in I} \{C_i = D_i\}$ is a vertex of $S$, and hence $u^{-1}(y) + x \in E$. Then $y \in E'$. Let $Z = [A' = 0] \cap \{C' > 0\} \cap \bigcap_{i \in I} \{C_i = 0\}$ be an edge of $[A' = 0] \cap \{C' > 0\}$. Then $u^{-1}(Z) = H \cap \bigcap_{i \in I} \{C_i = 0\}$ is an edge of $H$, and hence there is an $f \in u^{-1}(Z) \cap F \setminus \{0\}$. Then $u(f) \in Z \cap F' \setminus \{0\}$.

We have $0 \in [A' = B'] \cap [C' > D']$, and using the induction hypothesis, we obtain $0 \in \text{conv}(E') + \mathbb{Q}_+ F'$,

$$x \in \text{conv}(E') + \mathbb{Q}_+ F'.$$

**Case 2.** $r = 0$.

We assume $B = 0$ and $n > 1$. Then for some $i, j$, $C_i$ and $C_j$ are linearly independent. We can find a $y_1 \in [C_j > 0] \cap [C_i < 0]$. Let $\lambda > D_i/C_i(y_1)$, $(2C_j(x) - D_j)/C_i(y_1)$. Then for $y = \lambda y_1$ we have $C_i(y) < D_i$ and $C_j(2x - y) < D_j$, and hence the intersection of $[C > D]$ with the line

$$l = \{x + \alpha(y - x): \alpha \in \mathbb{Q}\}$$

is a finite interval $[z_1, z_2]$ containing $x$. Thus it is sufficient to prove that $z_1, z_2 \in \text{conv}(E) + \mathbb{Q}_+ F$. Let $z$ be $z_1$ or $z_2$. There is a $j$ with $z \in [C_j = D_j]$, for
otherwise an open interval on \( I \) containing \( z \) would be contained in \([C > D]\).
Suppose that \( C_{jk} \neq 0 \), and let \( u: [C_j = 0] \to \mathbb{Q}^{* - 1} \) be the projection that takes
the \( k \)th coordinate to zero. Let \( C'_i = C_i \circ u^{-1} \) and \( D'_i = D_i - C_i(z) \), \( E' = u((E - z) \cap [C_j = 0]), F' = u(F \cap [C_j = 0]) \). To a vertex of \([C' > D']\) with
index set \( I \) corresponds the vertex of \([C > D]\) with index set \( I \cup \{j\} \), and
similarly for edges. Like in Case 1, it now follows that \( z \in \text{conv}(E) + \mathbb{Q}^+ F \).
This completes the proof of the lemma.

We can now prove the theorem stated at the beginning. By Cramer’s rule,
we can choose the sets \( E \) and \( F \) such that all coefficients of their elements are
bounded by \( M \), and all elements of \( F \) are integer vectors. Let \( x \) be an integer
solution of \( Ax = B \) and \( Cx > D \). Then \( x \in \text{conv}(E) + \mathbb{Q}^+ F \), and it is easy
to see [6, 2.2] that there exists \( F' \subseteq F \) with \( |F'| < n \) and \( x \in \text{conv}(E) + \mathbb{Q}^+ F' \).
Take a representation
\[
x = \sum_{e \in E} \lambda_e e + \sum_{f \in F'} \mu_f f.
\]
Then \( x - \sum_{f \in F'} [\mu_f]f \) is the desired integer solution of \( Ax = B \) and \( Cx > D \)
with coefficients bounded by \( \sum_{e} \lambda_e M + \sum_{f} \mu_f M < (n + 1)M \).

Remarks. 1. The lemma states a decomposition of the set \( S \) of rational
solutions into the sum of a compact convex set and a pointed cone (i.e. one
that does not contain a line). A corresponding decomposition can be made
without the assumption that \( s = n \), by adding the common null space of \( A \)
and \( C \). However, the construction of the generating set \( F \) for the cone
requires a little more care, and the bounds obtained in this way are
considerably worse than the one in the theorem.

2. It follows from the theorem that the set of all \( A, B, C, D \) as above, for
which there exists an integer vector \( x \) with \( Ax = B \) and \( Cx > D \), is in \( NP \). It
is then easy to see that it is an \( NP \)-complete set. The same holds for slight
variations of the problem, such as \((A, B): Ax = B \) has a nonnegative integer
solution\}, \((C, D): Cx > D \) has an integer solution\}, and \((C, D): Cx > D \)
has a nonnegative integer solution\). One easily finds polynomial transfor-
mations between these sets. For terminology concerning \( NP \), see [5], e.g.

3. For any entry \( C_{ij} \) of \( C \), let \( C_{ij} = \sum_k C'_{ijk} \cdot 2^k \) with \( C'_{ijk} \in \{-1, 0, 1\} \), and
for \( x \in \mathbb{Q}^n \) let \( y_{jk} = x_j \cdot 2^k \). Then
\[
Cx > D \iff \text{for all } i, \sum_{j,k} C'_{ijk} y_{jk} > D_i.
\]
Furthermore, for any \( j \)
\[
\text{for all } k, y_{jk} = x_j \cdot 2^k \iff \quad y_{j0} = x_j \text{ and for all } k \text{ there exists } z_{jk} \in \mathbb{Q}^n \text{ with }
\]
\[
z_{jk} = y_{j,k-1} \quad \text{and} \quad y_{jk} = y_{j,k-1} + z_{jk}.
\]
Combining these, we obtain a polynomial transformation from the set of all
solvable systems of linear integer inequalities to the set of those inequalities
(C, D), for which all entries of C are −1, 0, or 1. This set is therefore NP-complete. For C consisting of 0’s and 1’s only, the problem is in P.

REFERENCES

4. S. A. Cook, A proof that the linear diophantine problem is in NP, unpublished manuscript, September 13, 1976.

Seminar für Angewandte Mathematik, Universität Zürich, CH-8032 Zürich, Switzerland (Current address of Joachim von zur Gathen)

Current address (Malte Sieveking): Universität Frankfurt, Fachbereich Mathematik, D-6000 Frankfurt a.M., Germany