Cowles Foundation Paper 848

MATHEMATICS OF OPERATIONS RESEARCH
Vol. 18, No. 3, August 1993
Printed in U.S.A.

SHORTEST INTEGER VECTORS

HERBERT E. SCARF AND DAVID F. SHALLCROSS

Let A be a fixed integer matrix of size m by n and consider all b for which the body $K_b = \{x\colon Ax \leqslant b\}$ is full dimensional. We examine the set of shortest nonzero integral vectors with respect to the family of norms whose unit balls are given by $(K_b - K_b)$. We show that the number of such shortest vectors is polynomial in the bit size of A, for fixed n. We also show the existence, for any n, of a family of matrices M for which the number of shortest vectors has as a lower bound a polynomial in the bit size of M of the same degree as the polynomial bound.

1. Introduction. For any closed convex body K, the difference body $K - K$, being convex and symmetric about the origin, defines a norm

$$\|x\|_{K-K} = \min\left\{\lambda\colon \frac{1}{\lambda}x \in K - K\right\}. \tag{1}$$

We consider a family of convex bodies of the form $K_b = \{x\colon Ax \leqslant b\}$, where A is a fixed m by n integer matrix, and b may vary; and denote $\|x\|_{K_b - K_b}$ as $\|x\|_b$. We shall assume that A has rank n, and that there is a positive vector π, such that $\pi A = 0$, so that K_b will always be bounded. We shall only consider those values of b for which K_b contains more than one point. For a finite-valued norm K_b should in fact be full dimensional. By a^i we will denote the ith row of A. We would like to give good bounds on the number of vectors v for which there exists some b such that v is a shortest nonzero integer vector with respect to the norm $\|\cdot\|_b$.

More specifically, we produce a bound on the number of these shortest vectors that is polynomial in the bit size of A but exponential in n. The dependence on the bit size of A is through the log of $\Delta_n(A)$, defined as the largest absolute value of an n by n subdeterminant of A. If we use the definition of size of A in [6], then $\log_2(n\Delta_n(A))$ is less than the size of A. The argument follows the outlines of the polynomial bound on the number of vertices of the integral hull of a polyhedron, in [3]. For any fixed n we give an example of a family of matrices that shows the polynomial in our bound is of the lowest degree possible.

The length of the shortest integer vector with respect to a norm $\|\cdot\|_b$ is an example of one of Minkowski's successive minima. For any norm $\|\cdot\|$ Minkowski [5, §47] defines n successive minima, $\lambda_1, \ldots, \lambda_n$, where λ_i is the minimum of all λ such that the scaled "unit ball" $\{x\colon \|x\| \leqslant \lambda\}$ contains i linearly independent integer vectors. These minima may be seen as realized by integer vectors $h^1, \ldots, h^n$ given by the rule: h^i is a shortest integer vector linearly independent of $h^1, \ldots, h^{i-1}$. Ties may occur, so that this construction is not unique. Nevertheless, Kannan, Lovász, and Scarf show in [4] that for fixed A, the union over all b of these successive minimizers for the norm

Received March 18, 1991; revised March 11, 1992.
AMS 1980 subject classification. Primary: 10E05, 52A25; Secondary: 90C99.
IAOR 1973 subject classification. Main: Combinatorial analysis.
OR/MS Index 1978 subject classification. Primary: 439 Mathematics/polyhedra.
Key words. Geometry of numbers, norms, symmetric bodies, shortest integer vectors.

0364-765X/93/1803/0516/$01.25

$\|\cdot\|_b$ lies in the union of a set of $n-1$ dimensional hyperplanes, of cardinality polynomial in the bit size of A but exponential in $m-n$.

One conjecture generalizing the current result and the result of Kannan, Lovász, and Scarf would be that the union over all b of the first i successive minimizers lies in the union of a set of $i-1$ dimensional affine spaces, of cardinality polynomial in the bit size of A for fixed m and n. We know of no evidence for the intermediate cases of this conjecture.

2. Upper bound on number of shortest vectors. From now on we will call a vector v *shortest* if there exists a vector b such that v is a shortest nonzero integer vector with respect to $\|\cdot\|_b$.

Define two vectors in $\mathbf{R}^m$ to have the same sign pattern if they have the same coordinates positive, the same coordinates negative, and the same coordinates zero. Shortest vectors are in a weak sense extreme among all integer vectors x with the same sign pattern of Ax.

LEMMA 1. *If $x = \frac{1}{2}(y+z)$, where y and z are integer vectors such that Ay and Az have the same sign pattern (and necessarily so does Ax), then x is not a shortest vector.*

PROOF. Let $w = \frac{1}{2}(y-z) = y - x$. We shall show that w must be shorter than x for any choice of b. Fix b. Let $\|x\|_b = 1/\lambda$, so by the definition (1) there exists $p \in \mathbf{R}^n$, such that $Ap \leqslant b$ and $A(p+\lambda x) \leqslant b$.

$$\mu = \lambda\left(1 + \min_{i:\, a^i x > 0}\left\{\frac{a^i y}{a^i z}, \frac{a^i z}{a^i y}\right\}\right). \tag{2}$$

The minimum is over a nonempty set, because K_b is bounded. $1/\mu$ will be an upper bound on the norm of w.

We will now show that

$$A\left(p + \frac{\mu}{2}y\right) \leqslant b; \qquad A\left(p + \frac{\mu}{2}z\right) \leqslant b, \tag{3}$$

checking each row. First, for any i such that $a^i x \leqslant 0$, we also know that $a^i y \leqslant 0$ and $a^i z \leqslant 0$, so, having selected μ greater than zero, we have

$$a^i\left(p + \frac{\mu}{2}y\right) \leqslant a^i p \leqslant b^i, \tag{4}$$

and

$$a^i\left(p + \frac{\mu}{2}z\right) \leqslant a^i p \leqslant b^i. \tag{5}$$

Second, for i such that $a^i x > 0$, our choice of μ guarantees that

$$a^i\left(p + \frac{\mu}{2}y\right) \leqslant a^i p + \lambda(a^i(y/2) + a^i(z/2)) = a^i(p+\lambda x) \leqslant b^i, \tag{6}$$

and

$$a^i\left(p + \frac{\mu}{2}z\right) \leqslant a^i p + \lambda(a^i(z/2) + a^i(y/2)) = a^i(p+\lambda x) \leqslant b^i. \tag{7}$$

Thus we have (3). Hence, with $q = p + (\mu/2)z$ and $w = (1/2)(y-z)$, we have

$q \in K_b$ and $q + \mu w \in K_b$. From our definition, $\|w\|_b \leqslant 1/\mu$. We conclude, since $\mu > \lambda$, that $\|w\|_b < \|x\|_b$. □

We can also bound the region in which a shortest vector can lie. The proof uses techniques from [2].

LEMMA 2. *If x is a shortest vector, then $|a^k x| \leqslant n\Delta_n(A)$, for $k = 1, \ldots, m$.*

PROOF. Let x be a shortest vector. Let K be the cone of vectors y for which Ay has the same sign pattern as Ax. As K is pointed, every vector in K is a positive combination of at most n extreme rays of K. In particular, we may write x in such a way:

$$x = \sum_{i=1}^{n} \lambda_i p^i, \qquad \lambda_i \geqslant 0 \tag{8}$$

where the p^i are n extreme rays of K, scaled to be integer vectors according to the following scheme.

Each extreme ray p of K satisfies the equations $a^j p = 0$, $j \in S$, for some set S of $n - 1$ linearly independent rows of A depending on p. Let r be the integer vector whose ith coordinate is $(-1)^{i-1}$ times the determinant of the $n - 1$ by $n - 1$ submatrix of A consisting of the rows in S with the ith column removed. It follows that for any i, the product $a^i r$ is the determinant of the n by n submatrix of A with rows $S \cup \{i\}$ and is zero whenever i is already in S. Thus r is a multiple of p. We may choose p to be r or $-r$, whichever points in the correct direction. For any i, the product $a^i p$ will be at most $\Delta_n(A)$ in absolute value.

We now show, for any b, that $\|x\|_b \geqslant \lambda_i \|p^i\|_b$. Let $\|x\|_b = 1/t$. Then there exists w such that $Aw \leqslant b$ and $A(w + tx) \leqslant b$. Now if $a^j x \leqslant 0$ then $a^j(w + t\lambda_i p^i) \leqslant a^j w \leqslant b^j$, and if $a^j x > 0$ then $a^j(w + t\lambda_i p^i) \leqslant a^j(w + t\Sigma_{k=1}^{n} \lambda_k p^k) = a^j(w + tx) \leqslant b^j$. So by definition $\|\lambda_i p^i\|_b \leqslant 1/t = \|x\|_b$.

Since x is by assumption a shortest vector, $\|p^i\|_b \geqslant \|x\|_b \geqslant \lambda_i \|p^i\|_b$, and so $\lambda_i \leqslant 1$ for all i. Now,

$$|a^k x| = \left| \sum_{i=1}^{n} \lambda_j a^k p^i \right| \leqslant n\Delta_n(A). \quad \square \tag{9}$$

We can now establish our polynomial bound:

THEOREM 3. *The number of shortest vectors for a fixed matrix A is at most $m^n 4^n(\psi + 2)^{n-1}$, where ψ is $\lceil \log_2(n\Delta_n(A)) \rceil$.*

PROOF. This proof is by reflecting sets, following [3].

Choose, perhaps sequentially, numbers θ_i, $\frac{1}{2} < \theta_i < 1$, for $i = 1, \ldots, m$, so that no more than n of the hyperplanes $a^i x = \pm\theta_i 2^k$, $i = 1, \ldots, m$, $k = 0, \ldots, \psi + 1$, intersect at any one point. Divide the region $\{x: |a^i x| \leqslant \theta_i 2^{\psi+1}, \forall i\}$ into sets $S(j_1, \ldots, j_m)$, called reflecting sets, of the form

$$S(j_1, \ldots, j_m) = \left\{ x: a^i x \in \begin{array}{ll} [\theta_i 2^{j_i - 1}, \theta_i 2^{j_i}) & j_i \geqslant 1 \\ (-\theta_i, \theta_i) & j_i = 0 \\ (-\theta_i 2^{-j_i}, -\theta_i 2^{-j_i - 1}] & j_i \leqslant -1 \end{array} : \forall i \right\}, \tag{10}$$

where each j_i ranges from $-\psi - 1$ to $\psi + 1$. Lemma 2 guarantees that each shortest vector lies in some one of these reflecting sets. Further, we can show that any

reflecting set contains at most one of the shortest vectors. First we show that if a reflecting set contains two integer points x and y, then all four of $A(2x - y)$, Ax, Ay, and $A(2y - x)$ have the same sign pattern. It is clear from the definition that in a reflecting set with $j_i \neq 0$, all points x have the same sign for $a^i x$. On the other hand, in any reflecting set with $j_i = 0$, any point x has $|a^i x| < \theta_i < 1$, and since A is an integer matrix, if x is an integer vector than $a^i x = 0$. Therefore if x and y lie in the same reflecting set $S(j_1, \ldots, j_m)$, then Ax and Ay have the same sign pattern.

Now let us determine the sign pattern of $A(2x - y)$. If $j_i = 0$, then $a^i(2x - y) = 2a^i x - a^i y = 0$. Otherwise, without loss of generality $j_i > 0$. Since $a^i x \geqslant \theta_i 2^{j_i - 1}$ and $a^i y < \theta_i 2^{j_i}$, we find $a^i(2x - y) > 2\theta_i 2^{j_i - 1} - \theta_i 2^{j_i} = 0$. Thus we can conclude that $A(2x - y)$ (and also $A(2y - x)$) has the same sign pattern as Ax and Ay. By Lemma 1 neither x nor y can be a shortest vector. Therefore, we can bound the number of shortest vectors by counting nonempty reflecting sets.

Furthermore, we can reduce the number of reflecting sets that may simultaneously contain shortest vectors. Many of the reflecting sets constructed are power of two multiples of one another. For example, $S(2, 4, 4, -2) = 2S(1, 3, 3, -1)$. Depending on A, it may be that $S(1, 3, 3, -1) = 2S(0, 2, 2, 0)$. If $S(j_1, \ldots, j_m) = 2^h S(k_1, \ldots, k_m)$, for $h > 0$, these two sets cannot both contain shortest vectors, by the following argument. Let $x \in S(k_1, \ldots, k_m)$ be a shortest vector. Then $2^h x$ is an integer vector in $S(j_1, \ldots, j_m)$. By previous arguments, no other vector $S(j_1, \ldots, j_m)$ can be a shortest vector, but $2^h x$ is 2^h times as long as x in any norm, and so cannot be shortest. We can partition the set of reflecting sets into families of the form $\{S, 2S, 4S, \ldots, 2^h S\}$ such that neither $(1/2)S$ nor $2^{h+1}S$ are reflecting sets. We call S the minimal member of this family. By the above argument, each such family contains at most one shortest vector.

We bound the number of shortest vectors by the number of minimal members of these families of reflecting sets. For any reflecting set $S(j_1, \ldots, j_m)$, consider the reflecting set $S(k_1, \ldots, k_m)$, where $k_i = j_i - 1$ if $j_i > 0$, $k_i = 0$ if $j_i = 0$, and $k_i = j_i + 1$ if $j_i < 0$. It is clear from their definitions that $S(j_1, \ldots, j_m) \subset 2S(k_1, \ldots, k_m)$. Inequalities defining $S(j_1, \ldots, j_m)$ are missing from $2S(k_1, \ldots, k_m)$ only in three cases. If $j_i = 1$, we miss $a^i x \geqslant \theta_i$. If $j_i = 0$, we miss $-\theta_i < a^i x < \theta_i$. If $j_i = -1$, we miss $a^i x \leqslant -\theta_i$. Depending on A, these inequalities might be redundant for $S(j_1, \ldots, j_m)$. If $S(j_1, \ldots, j_m)$ is minimal in its family and so not equal to $2S(k_1, \ldots, k_m)$, an inequality of this type must be nonredundant, so we then have a facet of the form $a^i x = \pm\theta_i$ for some i.

We count the number of minimal reflecting sets by the number of their vertices which lie on such facets. Each vertex is the intersection of 1 hyperplane of the form $a^i x = \pm\theta_i$, and $n - 1$ hyperplanes of the form $a^k x = \pm\theta_k 2^j$, where k is an integer between 1 and m but not equal to i, and j is some integer between 0 and $\psi + 1$. Thus there are at most $m2\binom{m-1}{n-1}(2\psi + 4)^{n-1}$ such vertices. Each vertex lies in at most 2^n reflecting sets; each reflecting set has at least n vertices on the required type of facets. We conclude that the number of reflecting sets, and therefore the number of shortest vectors, is at most:

$$\frac{4^n m\binom{m-1}{n-1}(\psi + 2)^{n-1}}{n}. \quad \square \tag{11}$$

3. Example with many shortest vectors. For each n, and each ϕ, we show the existence of a matrix M, with bit size at most $c_1\phi$, for which there are at least $c_2\phi^{n-1}$

shortest vectors, where c_1 and c_2 are constants depending only on n. Since $\psi = \log_2(n\Delta_n(M))$ is less than the bit size of M, this shows that the exponent on ψ in Theorem 3 is the best possible exponent that does not depend on m. We show the existence of M with the assistance of the following result from [1].

THEOREM 4. *For any $n \geqslant 2$ there exists a set of n independent unit vectors $s_1, \ldots, s_n$, and an infinite set V of integer points, where V is a subset of the vertices of the convex hull of the nonzero integer points in the cone generated by $s_1, \ldots, s_n$. This cone contains no nonzero integer points on its boundary. Further, if we let B^{-1} be the matrix with columns $s_1, \ldots, s_n$, let $\mathbf{1}$ be the vector of ones, and define $V(\phi) = V \cap \{x: Bx \leqslant 2^{\phi}\mathbf{1}\}$, then $V(\phi)$ contains at least $c\phi^{n-1}$ points, where c is a constant depending only on n.*

The vectors $s_1, \ldots, s_n$ may be taken as real eigenvectors of an easily constructed matrix. They are, however, irrational, so we will have to make rational approximations to use them. We will use the following lemma to relate vertices of integer hulls to shortest vectors.

LEMMA 5. *Let K be a pointed cone. Let v be a vertex of the convex hull of nonzero integer points in K. Then v and $-v$ are the only nonzero integer vectors in the convex set $(K - v) \cap (v - K)$, (where $K - v$ denotes the set $\{x - v: x \in K\}$).*

PROOF. Since $v \in K$, we know $2v \in K$. Trivially $0 \in K$. Now $v = 2v - v \in (K - v)$, and $v = v - 0 \in (v - K)$, so v is indeed in $(K - v) \cap (v - K)$. Similarly, so is $-v$. Let x be any integer point other than v, $-v$, and 0. Assume that x lies in $(K - v) \cap (v - K)$. Then both $v + x$ and $v - x$ are nonzero integer points in K. But $v = \frac{1}{2}(v + x) + \frac{1}{2}(v - x)$, contradicting the hypothesis that v was a vertex of the convex hull of nonzero integer points in K. Thus we may conclude that the only integer points in $(K - v) \cap (v - K)$ are v, $-v$, and 0. □

If v is in the interior of K, the convex set $(K - v) \cap (v - K)$ is full dimensional. The vector v is therefore the shortest nonzero integer vector with respect to the norm given by the set $(K - v) \cap (v - K)$. If v is on the boundary of K, this set will not be full dimensional. In this case if K is a closed set, and x is any point in the interior of K, then for sufficiently small $\epsilon > 0$, the convex set $(K - (v + \epsilon x)) \cap ((v + \epsilon x) - K)$ contains a neighborhood of the origin and so is full dimensional, and yet still contains only 0, v and $-v$ as integer vectors. Here v is the shortest nonzero integer vector with respect to the norm given by this expanded set. In either case such a ball is centrally symmetric, and so equals its own difference body scaled by one half. Using B and V from Theorem 4, and letting K be the cone $\{x: Bx \geqslant 0\}$, we see that each v in V is a shortest vector with respect to the norm given by the body $(K - v) \cap (v - K) = \{x: -Bv \leqslant Bx \leqslant Bv\}$. This body is the difference body of $\{x: Bx \leqslant \frac{1}{2}Bv, -Bx \leqslant \frac{1}{2}Bv\}$. Since V is infinite, the matrix M^* defined as the $2n$ by n matrix with one block of B and one block of $-B$ generates an infinite family of norms with distinct shortest vectors.

Of course, as we mentioned above, B has irrational entries, and so does not have a well-defined bitsize. We now perform a two-step process to find a family of rationally defined cones each of which gives many shortest vectors. Assume ϕ is large enough that $V(\phi)$ contains at least two points. These points are necessarily linearly independent. First we "press in" the facets of K until they reach points in $V(\phi)$ as follows. Let $\alpha_i = \min\{b^i x / \sum_{j=1}^{n} b^j x: x \in V(\phi)\}$, where b^i is the ith row of B. The α_i are strictly positive, as $V(\phi)$ is entirely in the interior of $K = \{x: Bx \geqslant 0\}$. The first new

cone is defined as $K_1 = \{x: b^i x - \alpha_i \Sigma_{j=1}^n b^j x \geqslant 0, i = 1, \ldots, n\}$. Note that

$$\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \min_{x \in V(\phi)} b^i x \Big/ \sum_{j=1}^n b^j x$$

$$< \min_{x \in V(\phi)} \sum_{i=1}^n b_i x \Big/ \sum_{j=1}^n b^j x = 1,$$

because these minima can be achieved at the same point only if the set $V(\phi)$ does not contain two linearly independent points. Now let x be any nonzero point in K_1. We know that

$$0 \leqslant \sum_{i=1}^n \left(b^i x - \alpha_i \sum_{j=1}^n b^j x \right) = \left(1 - \sum_{i=1}^n \alpha_i \right) \sum_{j=1}^n b^j x.$$

Since we have determined that $(1 - \Sigma_{i=1}^n \alpha_i) > 0$, we know that $\Sigma_{j=1}^n b^j x \geqslant 0$. This allows us to conclude that $0 \leqslant b^i x - \alpha_i \Sigma_{j=1}^n b^j x \leqslant b^i x$ for all i. We now know that $V(\phi) \subset K_1 \subset K$.

The facets of K_1 may still be irrational, however. We will replace each of the n facets of K_1 with $n - 1$ constraints to get a new cone K_2. Let K_3 be the cone generated by $V(\phi)$. (K_3 will, in general, have too many facets to use directly.) For each i the set $\{x: b^i x - \alpha_i \Sigma_{j=1}^n b^j x = 0\}$ is a supporting hyperplane of K_3 at some ray through 0 and some integer point y^i. The inequality $b^i x - \alpha_i \Sigma_{j=1}^n b^j x \geqslant 0$ for $x \in K_3$ is implied by $n - 1$ constraints defining facets of K_3 incident on this ray. K_2 is defined to be the intersection of these n sets of $n - 1$ constraints. Now we have $V(\phi) \subset K_2 \subset K_1 \subset K$. Since $V(\phi)$ is a subset of the extreme points of the integer hull of the nonzero points of K, we can conclude that $V(\phi)$ is also a subset of the extreme points of the integer hull of the nonzero points of K_2.

If we let A be an $n(n-1)$ by n integer matrix of minimum bitsize such that $K_2 = \{x: Ax \geqslant 0\}$, and let M be the $2n(n-1)$ by n matrix consisting of one block of A and one block of $-A$, then, by Lemma 5, M generates norms with at least $c\phi^{n-1}$ shortest nonzero integer vectors. To determine the bitsize of M, first notice that since for all $v \in V(\phi)$, we have $0 < Bv \leqslant 2^\phi \mathbf{1}$, and B^{-1} has unit vectors for columns; each component of v is of magnitude at most $n2^\phi$. Since each row of M comes from a hyperplane defining a facet of the cone generated by $V(\phi)$, each element of M is a signed determinant of the matrix whose columns are vectors of $V(\phi)$, and so is of magnitude at most $(n-1)!(n2^\phi)^n$. Although apparently large, this bound is of bitsize linear in ϕ. Thus M is of bitsize at most a constant times ϕ, as desired.

There is a more complicated construction of a $2n$ by n matrix $\tilde{M}$ of bitsize at most a constant times ϕ, also generating norms with at least $c\phi^{n-1}$ shortest nonzero integer vectors. Unfortunately, this paper is too short to contain it.

Acknowledgement. The research reported here was supported by the Program in Discrete Mathematics at the Cowles Foundation, Yale University, and by NSF Grant SES-8807167. The authors wish to thank Imre Bárány for many useful conversations and suggestions.

References

Bárány, I., Howe, R. and Lovász, L. (1989). On Integer Points in Polyhedra: A Lower Bound. Cowles Foundation Discussion Paper No. 917.

Cook, W., Gerards, A. M. H., Schrijver, A. and Tardos, É. (1986). Sensitivity Theorems in Integer Linear Programming. *Math. Programming* **34** 251–264.

Cook, W., Hartman, M., Kannan, R. and McDiarmid, C., On Integer Points in Polyhedra. *Combinatorica* (to appear).

Kannan, R., Lovász, L. and Scarf, H. (1990). The Shapes of Polyhedra. *Math. Oper. Res.* **15** 364–380.

Minkowski, H. (1896). *Geometrie der Zahlen* (*Erste Lieferung*). Teubner, Leipzig. (Reprinted: Chelsea, New York, 1953).

Schrijver, A. (1986). *Theory of Linear and Integer Programming*. John Wiley & Sons, New York.

H. E. Scarf: Cowles Foundation for Research in Economics, Yale University, New Haven, Connecticut 06520-2125

D. F. Shallcross: Bell Communications Research, Morristown, NJ 07962