COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA **12** (1) (1992) 27–37

ON INTEGER POINTS IN POLYHEDRA

W. COOK[*], M. HARTMANN[†], R. KANNAN[‡], and C. McDIARMID

Received October 24, 1989
Revised November 7, 1989

We give an upper bound on the number of vertices of P_I, the integer hull of a polyhedron P, in terms of the dimension n of the space, the number m of inequalities required to describe P, and the size φ of these inequalities. For fixed n the bound is $O(m^n\varphi^{n-1})$. We also describe an algorithm which determines the number of integer points in a polyhedron to within a multiplicative factor of $1+\varepsilon$ in time polynomial in m, φ and $1/\varepsilon$ when the dimension n is fixed.

1. Introduction and Notation

In connection with the family of integer programming problems

$$\begin{array}{ll} \text{minimize} & \boldsymbol{c}^T\boldsymbol{x} \\ \text{subject to} & \boldsymbol{x}\in P \\ & \boldsymbol{x}\ \text{integral} \end{array} \tag{1}$$

associated with different cost vectors $\boldsymbol{c}$, two sets of integer points are of fundamental interest. One of these is clearly the set of feasible solutions to the problem (1), the set of integer points in the polyhedron P. Techniques for solving (1) have taken advantage of the equivalence between this problem and the linear programming problem

$$\begin{array}{ll} \text{minimize} & \boldsymbol{c}^T\boldsymbol{x} \\ \text{subject to} & \boldsymbol{x}\in P_I \end{array}$$

where P_I, the *integer hull* of P, is the convex hull of all integer points in P. When problem (1) is bounded, it must have an optimal solution which is a vertex of P_I, and each vertex of P_I is the unique optimal solution of (1) for some $\boldsymbol{c}$, so this set of integer points is also a natural candidate for study.

It is easy to see that the number of vertices of P_I cannot be bounded above by any polynomial $p(n,m)$ in the dimension n of the space and the number m of linear inequalities required to describe P. In fact, there is no function $f(n,m)$ with this property. In order to obtain an upper bound, we must also consider the sizes of the

[*] Supported by Sonderfschungsbereich 303 (DFG) and NSF grant ECS-8611841.

[†] Partially supported by NSF grant DMS-8905645.

[‡] Supported by NSF grants ECS-8418392 and CCR-8805199.

AMS subject classification code (1991): 52 A 25; 90 C 10.

coefficients appearing in the inequalities which describe P. Following Schrijver [19], we define the *size* of an inequality $\boldsymbol{a}^T\boldsymbol{x} \leq \beta$ to be the number of bits necessary to encode it as a binary string.

Our algorithm for approximating the number of integer points in a polytope is a modification of the integer programming algorithm of Kannan [12], which relies on concepts and results from the Geometry of Numbers. The necessary concepts are outlined below (for proofs and further results in the Geometry of Numbers, see Cassels [2], Gruber and Lekkerkerker [9] and Lekkerkerker [13]).

A *lattice* $\mathscr{L}$ in $\mathbf{R}^n$ is the set of all integral linear combinations of m linearly independent vectors $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$, which in turn are said to form a *basis* of $\mathscr{L}$. The *determinant* $d(\mathscr{L})$ of the lattice $\mathscr{L}$ is the m-volume of the m-dimensional parallelopiped spanned by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ (when $m = n$, $d(\mathscr{L})$ is the determinant of the matrix with columns $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$). A consequence of Minkowski's convex body theorem is that such a lattice $\mathscr{L}$ must contain a non-zero vector whose length is at most $\sqrt{m}\, d(\mathscr{L})^{1/m}$.

Let $\boldsymbol{b}_1^*, \ldots, \boldsymbol{b}_m^*$ be the vectors which result from the Gram-Schmidt orthogonalization process defined by $\boldsymbol{b}_1^* = \boldsymbol{b}_1$ and

$$\boldsymbol{b}_{i+1}^* = \boldsymbol{b}_{i+1} - \textstyle\sum_{j=1}^{i} (\boldsymbol{b}_{i+1}^T \boldsymbol{b}_j^* / \|\boldsymbol{b}_j^*\|_2^2) \boldsymbol{b}_j^*$$

for $i = 1, \ldots, m-1$, where $\|\cdot\|_2$ is the l_2-norm. Then $\|\boldsymbol{b}_j^*\|_2$ is the distance from $\boldsymbol{b}_j$ to the subspace spanned by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{j-1}$ and $d(\mathscr{L}) = \prod_{j=1}^m \|\boldsymbol{b}_j^*\|_2$. Kannan [12] gives an algorithm which finds a *Korkhine-Zolotoreff reduced basis* $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m$ for a given lattice $\mathscr{L}$, which has the property that $\boldsymbol{b}_1$ is a shortest non-zero vector in $\mathscr{L}$ and for $j \geq 2$, $\|\boldsymbol{b}_j^*\|_2$ is in fact the length of the shortest non-zero vector in the projection of $\mathscr{L}$ orthogonal to the subspace spanned by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{j-1}$.

Finally, if S is a set of points, $\boldsymbol{y}$ is a vector and α is a scalar, then $|S|$ is the cardinality of S, $conv\{S\}$ is the convex hull of S, $S + \boldsymbol{y} = \{\boldsymbol{x} + \boldsymbol{y} : \boldsymbol{x} \in S\}$ is the translation of S by $\boldsymbol{y}$, $\alpha S = \{\alpha \boldsymbol{x} : \boldsymbol{x} \in S\}$ is the dilation of S by a factor of α, and $B(\boldsymbol{y}, \alpha) = \{\boldsymbol{x} : \|\boldsymbol{x} - \boldsymbol{y}\|_2 \leq \alpha\}$ is the ball of radius α with center $\boldsymbol{y}$.

2. Vertices of the Integer Hull

Shevchenko [20] and Hayes and Larman [11] obtained an upper bound on the number of vertices of the integer hull of the *knapsack polytope*,

$$P = \{\boldsymbol{x} \in \mathbf{R}^n : \boldsymbol{a}^T\boldsymbol{x} \leq \beta, \boldsymbol{x} \geq \boldsymbol{0}\},$$

where $\boldsymbol{a} > 0$ and $\beta > 0$: If the inequality $\boldsymbol{a}^T\boldsymbol{x} \leq \beta$ has size φ, then the number of vertices of P_I is at most φ^n. This result can easily be generalized to give a bound on the number of points of an arbitrary lattice $\mathscr{L}$ contained in the knapsack polytope, and as noted by Schrijver [19], this immediately yields an $O(m^n\varphi^n)$ upper bound for arbitrary polyhedra for fixed n by triangulation. One is then tempted to ask whether or not this bound is tight.

Previously, Rubin [18] found a class of knapsack polytopes in $\mathbf{R}^2$ whose integer hulls have an arbitrarily large number of vertices. The k^{th} polytope in the class is described by the inequalities $F_{2k}x + F_{2k+1}y \leq F_{2k+1}^2 - 1$, $x \geq 0$ and $y \geq 0$, where F_n is the n^{th} Fibonacci number. Rubin shows that the integer hull of the k^{th} polytope has $k+3$ vertices, and the size of the inequality $F_{2k}x + F_{2k+1}y \leq F_{2k+1}^2 - 1$ is clearly linear in k. Recently, Morgan [17] has obtained a class of polytopes in $\mathbf{R}^3$ with $m = 5$ for which the number of vertices of the integer hull grows as φ^2, and more generally Bárány, Howe and Lovász [1] gave a construction which yields a class of polytopes in $\mathbf{R}^n$ with $m = 2n^2$ for which the number of vertices of the integer hull grows as φ^{n-1}. These examples show that the order of φ appearing in the bound obtained below is best possible.

Theorem 2.1. *If P is a rational polyhedron in $\mathbf{R}^n$ which is the solution set of a system of at most m linear inequalities whose size is at most φ, then the number of vertices of P_I is at most $2m^n(6n^2\varphi)^{n-1}$.*

Proof. Clearly we may assume that $n \geq 2$ and that P_I has at least one vertex (otherwise the conclusion is trivial). We will first establish a crude upper bound on the "width" of P_I in the directions $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m$. Theorem 17.1 of Schrijver [19] (see the proof of Corollary 17.1a) implies that if $\boldsymbol{v}$ is a vertex of P_I, then $\|\boldsymbol{v}\|_\infty \leq (n+1)2^{2(n+1)^2\varphi}$, where $\|\cdot\|_\infty$ is the l_∞-norm. If we allow each inequality to have size at most $n\varphi$, we can assume that P is described by the inequalities $\boldsymbol{a}_i^T\boldsymbol{x} \leq b_i$ for $i = 1, \ldots, m$, where each $\boldsymbol{a}_i$ is an integral n-vector, each b_i is integral, and all vertices of P_I lie in the interior of P (we replace the inequality $\boldsymbol{a}_i^T\boldsymbol{x} \leq b_i$ by $2D_i\boldsymbol{a}_i^T\boldsymbol{x} \leq 2D_ib_i + 1$, where D_i is the lowest common denominator of the coefficients of $\boldsymbol{a}_i^T\boldsymbol{x} \leq b_i$). A rough estimate gives

$$\begin{aligned} b_i - \min\{\boldsymbol{a}_i^T\boldsymbol{v} : \boldsymbol{v} \text{ is a vertex of } P_I\} &\leq 2^{n\varphi} + n2^{n\varphi}(n+1)2^{2(n+1)^2\varphi} \\ &< 2^{5n^2\varphi}. \end{aligned}$$

Next we choose real numbers $\theta_1, \ldots, \theta_m$ such that

$$(2) \qquad 2^{-5n^2\varphi}\left(b_i - \min\{\boldsymbol{a}_i^T\boldsymbol{x} : \boldsymbol{x} \text{ is a vertex of } P_I\}\right) < \theta_i \leq 1$$

for $i = 1, \ldots, m$. We first choose $\theta_1 = 1$, and then inductively suppose that the values $\theta_1, \ldots, \theta_k$ have been chosen in such a way that the hyperplanes $\{\boldsymbol{x} : \boldsymbol{a}_i^T\boldsymbol{x} = b_i - 2^{j_i}\theta_i\}$ for $j_i = 1, \ldots, 5n^2\varphi$ and $i = 1, \ldots, k$ are in "general position," i.e., no j hyperplanes of this form intersect in a set of dimension $n - j + 1$ or greater, for $j = 1, \ldots, \min\{k, n\} + 1$. Since there can be at most finitely many values of θ_{k+1} for which the inductive hypothesis fails to hold for $k+1$, we can choose a value for θ_{k+1} in the interval (2) which satisfies the inductive hypothesis for $k+1$.

Now for each vertex $\boldsymbol{v}$ of P_I and each index $i = 1, \ldots, m$ there exists an integer j_i in $\{1, 2, \ldots, 5n^2\varphi\}$ such that $b_i - 2^{j_i}\theta_i \leq \boldsymbol{a}_i^T\boldsymbol{v} \leq b_i - 2^{j_i-1}\theta_i$. Let

$$P(j_1, \ldots, j_m) = \left\{\boldsymbol{x} : b_i - 2^{j_i}\theta_i \leq \boldsymbol{a}_i^T\boldsymbol{x} \leq b_i - 2^{j_i-1}\theta_i, i = 1, \ldots, m\right\}$$

for integers $j_1, \ldots, j_m$ in $\{1, 2, \ldots, 5n^2\varphi\}$. Lovász [15] calls each $P(j_1, \ldots, j_m)$ a *reflecting set* (Hayes and Larman [11] used similar sets, but called them "boxes," since theirs were rectangular). The name "reflecting set" refers to the fact that the reflection of any point $\boldsymbol{p}$ in $P(j_1,\dots,j_m)$ about a point $\boldsymbol{q}$ in $P(j_1,\dots,j_m)$ (which is $2\boldsymbol{q}-\boldsymbol{p}$) lies in the polyhedron P, since

$$\boldsymbol{a}_i^T(2\boldsymbol{q}-\boldsymbol{p}) = 2\boldsymbol{a}_i^T\boldsymbol{q} - \boldsymbol{a}_i^T\boldsymbol{p} \le 2(b_i - 2^{j_i-1}\theta_i) - (b_i - 2^{j_i}\theta_i) = b_i$$

for $i = 1,\dots,m$ (this is illustrated in Figure 1). Note that no reflecting set can contain two distinct vertices of P_I; if $P(j_1,\dots,j_m)$ contained the integral point $\boldsymbol{y} \neq \boldsymbol{v}$, then reflecting $\boldsymbol{y}$ about $\boldsymbol{v}$ we obtain the integral point $2\boldsymbol{v}-\boldsymbol{y}$ which lies in P_I, contradicting the fact that $\boldsymbol{v}$ is a vertex of P_I.

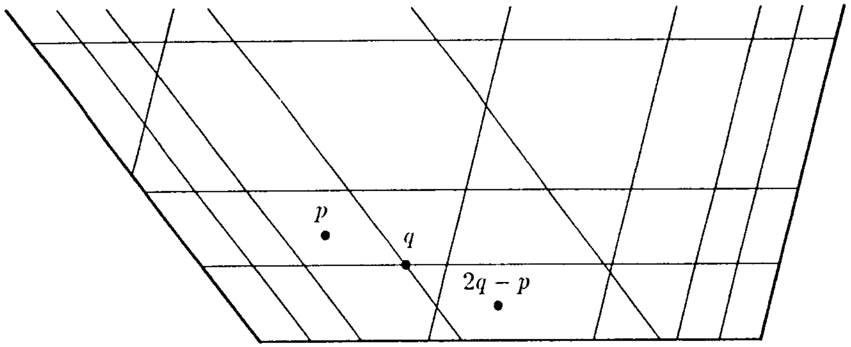

Fig. 1. Reflecting in a reflecting set

Define the polytope

$$P' = \left\{\boldsymbol{x} : b_i - 2^{5n^2\varphi}\theta_i \le \boldsymbol{a}_i^T\boldsymbol{x} \le b_i - \theta_i,\ i = 1,\dots,m\right\}$$

$$= \bigcup_{j_1,\dots,j_m=1}^{5n^2\varphi} P(j_1,\dots,j_m) \subset P.$$

If P is bounded, then P' is described by the inequalities $\boldsymbol{a}_i^T\boldsymbol{x} \le b_i - \theta_i$ for $i = 1,\dots,m$ and $(P')_I = P_I$. On the other hand, if P is unbounded, then we must work with the convex hull of the vertices of P_I, which may be properly contained in $(P')_I$.

Let $U = \{\boldsymbol{u}\colon\ \boldsymbol{u}$ is a vertex of some $P(j_1,\dots,j_m)\}$, and call an element of U a *boundary vertex* if it lies on a face of the polytope P'. If P_I has M vertices, we will show that there are at least M boundary vertices by assigning the labels $1,\dots,M$ to some of the reflecting sets in such a way that we can associate each label with a unique boundary vertex. Since there can be at most $2m\binom{m-1}{n-1}(5n^2\varphi+1)^{n-1}$ boundary vertices, this will prove the theorem.

Let $\boldsymbol{v}_1,\dots,\boldsymbol{v}_M$ be the vertices of P_I, and let $U\backslash conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_M\} = \{\boldsymbol{u}_1,\dots,\boldsymbol{u}_N\}$. We will also assume (without loss of generality) that $\boldsymbol{u}_j \notin conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_M,\boldsymbol{u}_1,\dots,\boldsymbol{u}_{j-1}\}$ for $j = 1,\dots,N$ (choose $\boldsymbol{u}_i$ to be an extreme point of $conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_M,\boldsymbol{u}_1,\dots,\boldsymbol{u}_i\}$ for $i = N,\dots,1$). For each $k = 1,\dots,M$ pick a reflecting set which contains $\boldsymbol{v}_k$ and is not contained in $conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_M\}$ and give it the label k (such a reflecting set always exists, since otherwise $\boldsymbol{v}_k$ would lie in the interior of P_I, a contradiction). These reflecting sets must be distinct, since no reflecting set contains two vertices of P_I. Next we describe a procedure which constructs M disjoint connected sequences of similarly labelled reflecting sets by adding the points $\boldsymbol{u}_1,\dots,\boldsymbol{u}_N$ to the convex hull one-at-a-time. The k^{th} sequence begins with the labelled reflecting set containing $\boldsymbol{v}_k$, and ends with a reflecting set that contains a distinguished boundary vertex.

Let $R_1,\dots,R_M$ be the reflecting sets most recently labelled $1,\dots,M$, and suppose that for some i, each of these M reflecting sets intersects but is not contained in $conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_M,\boldsymbol{u}_1,\dots,\boldsymbol{u}_i\}$. Let j be the smallest index for which $R_k \subseteq conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_M,\boldsymbol{u}_1,\dots,\boldsymbol{u}_j\}$ for some k which has not yet been associated with a boundary vertex. Note that the point $\boldsymbol{u}_j$ must be a vertex of R_k, since otherwise $R_k \subseteq conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_M,\boldsymbol{u}_1,\dots,\boldsymbol{u}_{j-1}\}$. It follows that for any point $\boldsymbol{x} \neq \boldsymbol{u}_j$ in R_k the point $2\boldsymbol{u}_j-\boldsymbol{x}$ must lie outside of $conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_M,\boldsymbol{u}_1,\dots,\boldsymbol{u}_j\}$, since $\boldsymbol{u}_j$ can be expressed as a convex combination of the points $2\boldsymbol{u}_j-\boldsymbol{x}$ and $\boldsymbol{x}$. Because $\boldsymbol{u}_j$ lies on exactly n hyperplanes of the form $\{\boldsymbol{x} : \boldsymbol{a}_i^T\boldsymbol{x} = b_i - 2^{j_i}\theta_i\}$, the index k must be uniquely determined, and we have one of the following two cases:

Case 1: The point $\boldsymbol{u}_j$ is a boundary vertex. In this case, we associate the label with $\boldsymbol{u}_j$.

Case 2: For all $\boldsymbol{x} \in R_k$ sufficiently close to $\boldsymbol{u}_j$ the points $2\boldsymbol{u}_j-\boldsymbol{x}$ lie in an unlabelle reflecting set R for which $R \cap conv\{\boldsymbol{v}_1,\dots,\boldsymbol{v}_m,\boldsymbol{u}_1,\dots,\boldsymbol{u}_j\} = \boldsymbol{u}_j$. In this case, w give the reflecting set R the label k.

Because there are only finitely many reflecting sets, the procedure can be applie only finitely many times, so since the points $\boldsymbol{u}_1,\dots,\boldsymbol{u}_N$ are added to the convex hu one-at-a-time, ultimately a unique boundary vertex is associated with each label k.

Remarks: (2.2) In case P_I is not of full dimension, the bound may be improved. P_I has dimension $0 < d < n$, then by an analogous argument using d-dimensiona reflecting sets which lie in the affine space of P_I, one can show that the number vertices of P_I is at most $2m^d(6n^2\varphi)^{d-1}$.

(2.3) Together with the Upper Bound Theorem [16], our result implies that th number of facets of P_I is $O(\varphi^{(n-1)\lfloor n/2\rfloor})$. The polytopes constructed by Bárán Howe and Lovász [1] have $\Omega(\varphi^{n-1})$ facets. Whether or not the number of facets P_I is also $O(\varphi^{n-1})$ is an interesting open problem.

(2.4) The decomposition of the polytope P' into reflecting sets when $\theta_1 = \cdots$ $\theta_m = 1$ can be used together with Lenstra's algorithm [14] for integer programmin to find a list $\boldsymbol{x}_1,\dots,\boldsymbol{x}_N$ of integral points which contains the vertices of P_I, since reflecting set that contains more than one integer point cannot contain a vertex P_I. This yields an $O((m\varphi)^{2n})$ algorithm which finds the vertices of P_I when n fixed (see Hartmann [10] for details).

(2.5) If the polytope P is only given by an optimization oracle, we can st find the vertices of P_I in time polynomial in φ and the number of vertices of when n is fixed using a slight generalization of a method used by Edmonds, Lová and Pulleyblank [6] to find the affine hull of a polytope given by an optimizati oracle. Given a partial list of vertices of P_I, we first find a list of inequaliti $\boldsymbol{a}_i^T\boldsymbol{x} \le b_i$, $i = 1,\dots,m$ which describes their convex hull, and then find vertic of P_I maximizing $\boldsymbol{a}_i^T\boldsymbol{x}$ over P_I for $i = 1,\dots,m$.

3. Estimating the Number of Integer Points

It is easy to see that determining the number of integer points in a polytope is $\#P$-complete, since determining the number of matchings in a bipartite graph is $\#P$-complete [21]. There is, on the other hand, the possibility that when the dimension n is fixed the number of integer points in a polytope described by m inequalities of size at most φ can be determined in time polynomial in m and φ. In a series of papers, Zamansky and Cherkassky [22–25] develop algorithms for determining the number of integer points in a polytope. In [23], they describe an algorithm which determines the number of integral points in a polytope in $\mathbf{R}^2$ described by m inequalities of size at most φ in time $O(m\varphi)$ and in [25] they give an algorithm that determines the number of integer points in a polytope in $\mathbf{R}^3$ which is, however, not shown to be polynomial. Recently, Dyer [4] has given several reductions of the problem of determining the number of integer points in a polytope. He first reduces this problem to the problem of determining the number of integer points in polynomially many integral simplices using the algorithm described in Remark (2.4), and then further reduces the problem of determining the number of integer points in an integral simplex to the problem of determining the number of integer points in $O(n!)$ integral simplices of a special type. Generalizing a method of Mordell, he shows that in $\mathbf{R}^3$ this reduces to the computation of Dedekind sums, which can be evaluated in polynomial time, yielding a polynomial algorithm for determining the number of integer points in a polytope in $\mathbf{R}^3$. He also reduces the problem in even dimensions to the next lower odd dimension, which yields a polynomial algorithm for determining the number of integer points in a polytope in $\mathbf{R}^4$. Whether there is a polynomial algorithm in dimension $n > 4$ is unknown.

We will give an algorithm which estimates the number of integer points in a polytope to within a multiplicative factor of $1 + \varepsilon$ in polynomial time when the dimension n is fixed. More precisely, we prove the following theorem:

Theorem 3.1. *For any fixed integer $n \geq 1$, there exists an algorithm that, for any polytope P described by m inequalities of size at most φ and any positive rational number ε, finds, in time polynomial in m, φ and $1/\varepsilon$, two integers L and U such that $L \leq |P \cap \mathbf{Z}^n| \leq U$ and $U \leq (1+\varepsilon)L$.*

Proof. First we do some preprocessing to ensure that the polytope is "well-rounded." As in Lenstra's algorithm, we determine whether the polytope is full-dimensional, and if not, find a unimodular tranformation which projects it down to a lower dimensional space in which it is full-dimensional. Then an invertible linear transformation is applied to both the polytope and the integral lattice so that the polytope gets sandwiched between two concentric spheres whose radii differ by a multiplicative factor of $n^{3/2}$. Since all of the preprocessing is described in Grötschel, Lovász and Schrijver [8], we will simply state precisely the problem at the end of the preprocessing: Given independent rational vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ and a rational polytope P, find integers L and U such that $L \leq |P \cap \mathscr{L}| \leq U$ and $U \leq (1+\varepsilon)L$, where $\mathscr{L}$ is the lattice generated by $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ and the following additional condition is satisfied by the input: There is a rational vector $\boldsymbol{p}$ such that $B(\boldsymbol{p}, 1) \subseteq P \subseteq B(\boldsymbol{p}, n^{3/2})$.

At this point, Lenstra's alogorithm uses Lovász's basis reduction algorithm to find a reduced basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ of the lattice $\mathscr{L}$ which has the property that $\prod_{i=1}^n \|\boldsymbol{b}_i\|_2 \leq c^{n^2} d(\mathscr{L})$. Then if $\max\{\|\boldsymbol{b}_1\|_2, \ldots, \|\boldsymbol{b}_n\|_2\}$ is sufficiently small, can easily obtain a point $\boldsymbol{x} \in P \cap \mathscr{L}$. Otherwise, the number of certain hyperpla containing lattice points which intersect P can be bounded by a number depenc only on n. It is not difficult to modify this part of Lenstra's algorithm to estim the number of lattice points in P, since if $\max\{\|\boldsymbol{b}_1\|_2, \ldots, \|\boldsymbol{b}_n\|_2\}$ is sufficiently sm the number of lattice points in P is very nearly $vol\{P\}/d(\mathscr{L})$. However, the modi algorithm has an $O(n^6 c^{n^2} \varepsilon^{-n})$ running time. Our algorithm, which is a modificat of the integer programming algorithm of Kannan [12], uses a stronger reduced b to cut the running time down to $O(n^{cn}\varepsilon^{-n})$. The bulk of the proof of Theorem will be broken up into Propositions 3.2–3.6.

We use the algorithm SHORTEST of Kannan [12] to find a Korkhine-Zoloto reduced basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ of the lattice $\mathscr{L}$ (since SHORTEST requires integral in the vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ are first multiplied by the lowest common denominato of their components, and subsequently the vectors in the reduced basis found SHORTEST are multiplied by D^{-1}). Letting $\|\boldsymbol{b}_i^*\|_2 = \max\{\|\boldsymbol{b}_1^*\|_2, \ldots, \|\boldsymbol{b}_n^*\|_2\}$ $\delta = \min\{\varepsilon, 1\}/4n$, we consider the following two cases:

Case 1: $\|\boldsymbol{b}_i^*\|_2 \leq 2\delta/\sqrt{n}$. In this case, we give the lower and upper bounds explic

$$\left\lceil \frac{(1-\delta)^n vol\{P\}}{d(\mathscr{L})} \right\rceil \leq |P \cap \mathscr{L}| \leq \left\lfloor \frac{(1+\delta)^n vol\{P\}}{d(\mathscr{L})} \right\rfloor,$$

where $vol\{P\}$ is the volume of P. When the dimension n is fixed, $vol\{P\}$ can computed in polynomial time (see Cohen and Hickey [3]), so the bounds can computed in polynomial time. We also have $(1+\delta)^n/(1-\delta)^n \leq (1-\delta)^{-2n}$ $(1-2n\delta)^{-1} \leq 1+\varepsilon$. To show that the bounds are valid, we first note that if

$$R = \left\{ \textstyle\sum_{j=1}^n y_j \boldsymbol{b}_j^* : -\frac{1}{2} \leq y_j < \frac{1}{2}, j = 1, \ldots, n \right\},$$

then R has volume $d(\mathscr{L})$., R is contained in $B(\mathbf{0}, \delta)$ and the rectangular pri $\{R + \boldsymbol{x} : \boldsymbol{x} \in \mathscr{L}\}$ form a partition of $\mathbf{R}^n$. In the first proposition below, we show t if $\boldsymbol{x} \in P \cap \mathscr{L}$, then a slight dilation of P about $\boldsymbol{p}$ contains $R + \boldsymbol{x}$. In the second, show that if $\boldsymbol{x} \notin P \cap \mathscr{L}$, then a slight contraction of P about $\boldsymbol{p}$ does not inters $R + \boldsymbol{x}$. Propositions 3.2 and 3.3 are Propositions 1 and 2 of Dyer, Frieze and Kan [5], although the proofs we give below are new.

Proposition 3.2. : *If $\boldsymbol{x} \in P$, then $B(\boldsymbol{x}, \delta) \subseteq (1+\delta)(P - \boldsymbol{p}) + \boldsymbol{p}$.*

Proof. Without loss of generality, assume that $\boldsymbol{p} = \mathbf{0}$. Let $\boldsymbol{y}$ satisfy $\|\boldsymbol{y}\|_2 \leq \delta$. Si $\boldsymbol{x} \in P$ and $\boldsymbol{y}/\|\boldsymbol{y}\|_2 \in B(\mathbf{0}, 1) \subseteq P$, the point

$$\frac{1}{1+\|\boldsymbol{y}\|_2}(\boldsymbol{x}+\boldsymbol{y}) = \frac{1}{1+\|\boldsymbol{y}\|_2}\boldsymbol{x} + \frac{\|\boldsymbol{y}\|_2}{1+\|\boldsymbol{y}\|_2}\frac{\boldsymbol{y}}{\|\boldsymbol{y}\|_2}$$

lies in P. Then $1 + \|\boldsymbol{y}\|_2 \leq 1 + \delta$ implies that $\boldsymbol{x} + \boldsymbol{y} \in (1+\delta)P$.

For any $\boldsymbol{x} \in P \cap \mathscr{L}$, we have $R + \boldsymbol{x} \subseteq B(\boldsymbol{x}, \delta)$, so $R + \boldsymbol{x} \subseteq (1+\delta)(P - \boldsymbol{p}) + \boldsymbol{p}$ by above claim. Therefore,

$$d(\mathscr{L})|P \cap \mathscr{L}| \leq vol\{(1+\delta)(P - \boldsymbol{p}) + \boldsymbol{p}\} = (1+\delta)^n vol\{P\},$$

which gives the upper bound.

Proposition 3.3. *If* $B(\boldsymbol{x},\delta)\cap(1-\delta)(P-\boldsymbol{p})+\boldsymbol{p}\neq\emptyset$, *then* $\boldsymbol{x}\in P$.

Proof. Again we may assume that $\boldsymbol{p}=\mathbf{0}$. Suppose that $\boldsymbol{x}-\boldsymbol{z}\in(1-\delta)P$ and $\|\boldsymbol{z}\|_2\leq\delta$. Since $(1-\delta)P\subseteq(1-\|\boldsymbol{z}\|_2)P$ and $\boldsymbol{z}/\|\boldsymbol{z}\|_2\in B(\mathbf{0},1)\subseteq P$,

$$\boldsymbol{x}=(1-\|\boldsymbol{z}\|_2)\frac{\boldsymbol{x}-\boldsymbol{z}}{1-\|\boldsymbol{z}\|_2}+\|\boldsymbol{z}\|_2\frac{\boldsymbol{z}}{\|\boldsymbol{z}\|_2}$$

expresses $\boldsymbol{x}$ as a convex combination of two points in P. ∎

Since $R+\boldsymbol{x}\subseteq B(\boldsymbol{x},\delta)$, applying this to those $\boldsymbol{x}$ in $P\cap\mathscr{L}$ implies that $d(\mathscr{L})|P\cap\mathscr{L}|\geq(1-\delta)^n vol\{P\}$, which gives the lower bound.

Case 2: $\|\boldsymbol{b}_i^*\|_2>2\delta/\sqrt{n}$. In this case, we will argue that the number of certain $i-1$ dimensional affine spaces intersecting P is small. Since every $\boldsymbol{x}\in\mathscr{L}$ can be expressed uniquely as $\boldsymbol{x}=z_1\boldsymbol{b}_1+\cdots+z_n\boldsymbol{b}_n$ with $z_1,\ldots,z_n\in\mathbf{Z}$, we have

$$|P\cap\mathscr{L}|=\sum\left\{|P(\boldsymbol{b}_0)\cap\mathbf{Z}^{i-1}|:\boldsymbol{b}_0=z_i\boldsymbol{b}_i+\cdots+z_n\boldsymbol{b}_n,z_i,\ldots,z_n\in\mathbf{Z}\right\},$$

where $P(\boldsymbol{b}_0)=\{\boldsymbol{y}\in\mathbf{R}^{i-1}:y_1\boldsymbol{b}_1+\cdots+y_{i-1}\boldsymbol{b}_{i-1}+\boldsymbol{b}_0\in P\}$. If we can find a finite subset $T\subseteq\mathbf{R}^n$ such that $|P(\boldsymbol{b}_0)\cap\mathbf{Z}^{i-1}|=0$ for all such $\boldsymbol{b}_0\notin T$, then the algorithm will recursively find numbers $L(\boldsymbol{b}_0)$ and $U(\boldsymbol{b}_0)$ such that $L(\boldsymbol{b}_0)\leq|P(\boldsymbol{b}_0)\cap\mathbf{Z}^{i-1}|\leq U(\boldsymbol{b}_0)$ and $U(\boldsymbol{b}_0)\leq(1+\varepsilon)L(\boldsymbol{b}_0)$ for all $\boldsymbol{b}_0\in T$, so we can set $L=\sum_{\boldsymbol{b}_0\in T}L(\boldsymbol{b}_0)$ and $U=\sum_{\boldsymbol{b}_0\in T}U(\boldsymbol{b}_0)$. The following proposition, which is similar to Proposition 2.13 of Kannan [12], indicates how to generate the subset T:

Proposition 3.4. *Suppose that* $z_{j+1},\ldots,z_n$ *are fixed integers for some* $j\geq i$. *Then there is a number* $\overline{z}_j$ *such that for all integers* $y_1,\ldots,y_{j-1}$ *and* z_j *for which* $\|\sum_{k=1}^{j-1}y_k\boldsymbol{b}_k+\sum_{k=j}^{n}z_k\boldsymbol{b}_k-\boldsymbol{p}\|_2\leq n^{3/2}$, *we must have*

$$|z_j-\overline{z}_j|<\frac{2n^3\|\boldsymbol{b}_i^*\|_2}{\varepsilon\|\boldsymbol{b}_j^*\|_2}.$$

Proof. Since $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{j-1}$ are orthogonal to the vector $\boldsymbol{b}_j^*$, projecting the vector $\sum_{k=1}^{j-1}y_k\boldsymbol{b}_k+\sum_{k=j}^{n}z_k\boldsymbol{b}_k-\boldsymbol{p}$ along the direction $\boldsymbol{b}_j^*$, we obtain the vector $(z_j-\overline{z}_j)\boldsymbol{b}_j^*$, where $\overline{z}_j\boldsymbol{b}_j^*$ is the projection of the vector $\boldsymbol{p}-\sum_{k=j+1}^{n}z_k\boldsymbol{b}_k$ along the direction $\boldsymbol{b}_j^*$. We must have $|z_j-\overline{z}_j|\|\boldsymbol{b}_j^*\|_2\leq n^{3/2}$, so that

$$|z_j-\overline{z}_j|\leq\frac{n^{3/2}}{\|\boldsymbol{b}_j^*\|_2}<\frac{n^2\|\boldsymbol{b}_i^*\|_2}{2\delta\|\boldsymbol{b}_j^*\|_2}\leq\frac{2n^3\|\boldsymbol{b}_i^*\|_2}{\varepsilon\|\boldsymbol{b}_j^*\|_2}.$$ ∎

This can be used as the basis of a recursive procedure which generates the values of $z_i,\ldots,z_n$ corresponding to $\boldsymbol{b}_0\in T$.

Proposition 3.5. *At the end of the procedure,*

$$|T|\leq\prod_{j=i}^{n}\left(\frac{4n^3\|\boldsymbol{b}_i^*\|_2}{\varepsilon\|\boldsymbol{b}_j^*\|_2}\right)\leq\frac{(2n)^{7(n-i+1)/2}}{\varepsilon^{n-i+1}}.$$

Proof. The first part follows from Proposition 3.4. For the second part,

$$\prod_{j=i}^{n}\left(\frac{4n^3\|\boldsymbol{b}_i^*\|_2}{\varepsilon\|\boldsymbol{b}_j^*\|_2}\right)\leq\frac{(2n)^{3(n-i+1)}}{\varepsilon^{n+i-1}}\frac{\|\boldsymbol{b}_i^*\|_2^{n-i+1}}{\prod_{j=i}^{n}\|\boldsymbol{b}_j^*\|_2}.$$

Then because $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_n$ is a Korkhine-Zolotoreff reduced basis, $\|\boldsymbol{b}_i^*\|_2$ is the le
of the shortest non-zero vector in the lattice which is the projection of $\mathscr{L}$ orthog
to the subspace spanned by $\boldsymbol{b}_1,\ldots,\boldsymbol{b}_{i-1}$. Since $\prod_{j=i}^{n}\|\boldsymbol{b}_j^*\|_2$ is the determinar
this lattice, Minkowski's convex body theorem implies that

$$|T|\leq\frac{(2n)^{3(n-i+1)}(n-i+1)^{(n-i+1)/2}}{\varepsilon^{n-i+1}}\leq\frac{(2n)^{7(n-i+1)/2}}{\varepsilon^{n-i+1}}.$$

Proposition 3.6. *For any fixed integer* $n\geq1$, *the running time of the algorith*
polynomial in m, φ *and* $1/\varepsilon$.

Proof. The proof is by induction on n, the case $n=1$ being trivial. By Coroll
5.3b and 15.6a of Schrijver [19], the preprocessing can be done in time polyno
in m and φ; therefore $\boldsymbol{v}_1,\ldots,\boldsymbol{v}_n$, P and $\boldsymbol{p}$ must be of size polynomial in m an
Theorems 2.16 and 3.9 of Kannan [12] ensure that the algorithm SHORTEST
in time polynomial in m and φ.

In Case 1, the numbers L and U can be computed in time polynomial in m
φ. In Case 2, we first note that the numbers $\overline{z}_j$ from Proposition 3.4 can be comp
in time polynomial in m and φ, since the vectors $\boldsymbol{b}_j^*$ themselves are computed in
polynomial in m and φ, and the vectors $\boldsymbol{b}_{j+1},\ldots,\boldsymbol{b}_n$ and $\boldsymbol{p}$ are all of size polync
in m and φ. By Proposition 3.5, we have to estimate the number of integer poin
at most $(2n)^{7(n-i+1)/2}\varepsilon^{-(n+i-1)}$ polytopes in $\mathbf{R}^{i-1}$, and by the induction hypot
this can be done in time polynomial in m, φ and $1/\varepsilon$, since the polytopes $P(\boldsymbol{b}_0)$
be described by inequalities of size polynomial in m and φ.

Remarks: (3.7) As in Kannan [12], a more careful analysis of the running
shows it to be $O((2n)^{7n/2}\varepsilon^{-n})$.

(3.8) This algorithm can be modified to estimate the number of integer poir
any bounded convex body K given by a well-guaranteed (strong) separation or
First of all, if K is well-rounded, then for any $0<\rho<1$ the volume of K ca
estimated by $\rho^n|K\cap\rho\mathbf{Z}^n|$ using Propositions 3.2 and 3.3, which can be comp
in $O(\rho^{-n})$ calls to the oracle when n is fixed. It is also an easy matter to cons
a separation oracle for the intersection of K with an affine space. The only
difficulty is in obtaining a guarantee, but the ellipsoid method can be used tog
with simultaneous diophantine approximation (as described in Grötschel, Lovás
Schrijver [8]) to find a maximal set of affinely independent points which lie in t
the convex hull of those lattice points contained in the intersection.

(3.9) For any integer-valued polynomial $p(n)$, the following problem is NP-

BOUNDS: Given a polytope $P=\{\boldsymbol{x}:\boldsymbol{Ax}\leq\boldsymbol{b}\}$, find integers L and U suc
that $L\leq|P\cap\mathbf{Z}^n|+1\leq U$ and $U\leq2^{p(n)}L$.

First note that this problem is easier than the corresponding problem with
$\mathbf{Z}^n|+1$ replaced by $|P\cap\mathbf{Z}^n|$, for which there is a trivial reduction from INTE
PROGRAMMING FEASIBILITY.

The reduction will be from SUBSET SUM, which is known to be *NP*-complete (see Gary and Johnson [7]). Let non-negative integers $a_1, \dots, a_n$ and b give any instance of SUBSET SUM (i.e., decide if there is a set $I \subseteq \{1, \dots, n\}$ such that $\sum_{i \in I} a_i = b$). Without loss of generality, assume that $a_1, \dots, a_n$ and b are all positive. Let $P \subseteq \mathbf{R}^{n+2}$ consist of those $(x_1, \dots, x_n, y, z)$ for which $0 \leq x_i \leq 1$ for $i = 1, \dots, n$, $y \geq 0$, $z \geq 0$, $y + z \leq M - 1$, and $\sum_{i=1}^{n} M a_i x_i + y + z = Mb + M - 1$, where $M = 2^{p(n)} + 1$. It is easy to see that $|P \cap \mathbf{Z}^{n+2}| = MN$, where N is the number of solutions to the instance of SUBSET SUM, so that $L > 1$ if and only if $N > 0$.

References

[1] I. Bárány, R. Howe, and L. Lovász: On integer points in polyhedra: a lower bound, Cowles Foundation Discussion Paper No. 917, Cowles Foundation for Research in Economics, Yale University, 1989.

[2] J. W. S. Cassels: *An Introduction to the Geometry of Numbers* (Springer-Verlag, Berlin, 1971).

[3] J. Cohen, and T. Hickey: Two algorithms for determining volumes of convex polyhedra, *Journal of the Association for Computing Machinery*, **26** (1979), 401–414.

[4] M. Dyer: On counting lattice points in polyhedra, submitted to *SIAM Journal on Computing*.

[5] M. Dyer, A. Frieze, and R. Kannan: A random polynomial time algorithm for approximating the volume of convex bodies, Research Report No. 88-40, Department of Mathematics, Carnegie-Mellon University, 1989.

[6] J. Edmonds, L. Lovász, and W.R. Pulleyblank: Brick decompositions and the matching rank of graphs, *Combinatorica* **2** (1982), 247–274.

[7] M. R. Gary, and D.S. Johnson: *Computers and Intractability, a Guide to the Theory of NP-completeness* (W.H. Freeman and Co., San Francisco, 1979).

[8] M. Grötschel, L. Lovász, and A. Schrijver: *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, Heidelberg, 1988.

[9] P. M. Gruber, and C.G. Lekkerkerker: *Geometry of Numbers*, (Second edition) North Holland, Amsterdam, 1987.

[10] M. Hartmann: Cutting planes and the complexity of the integer hull, Technical Report No. 819, School of Operations Research and Industrial Engineering, Cornell University, 1989.

[11] A. C. Hayes, and D. G. Larman: The vertices of the knapsack polytope, *Discrete Applied Math.* **6** (1983), 135–138.

[12] R. Kannan: Minkowski's convex body theorem and integer programming, *Math. of Operations Research* **12** (1987), 415–440.

[13] C. G. Lekkerkerker: *Geometry of Numbers*, North Holland, Amsterdam, 1969.

[14] H. W. Lenstra, Jr.: Integer Programming in a fixed number of variables, *Math. of Operations Research* **8** (1983) 538–548.

[15] L. Lovász: communicated by H.E. Scarf.

[16] P. McMullen, and G.C. Shephard: *Convex Polytopes and the Upper Bound Conjecture*, Cambridge University Press, Cambridge, 1971.

[17] D. Morgan: The set of vertices of the convex hull of integer points in regions defined by particular linear inequalities, submitted to *Mathematika*.

[18] D. S. Rubin: On the unlimited number of faces in integer hulls of linear programs a single constraint, *Operations Research*, **18** (1970), 940–946.

[19] A. Schrijver: *Theory of Linear and Integer Programming*, Wiley, Chichester,

[20] V. N. Shevchenko: On the number of extreme points in integer programming, *netika* (1981) No. 2, 133–134.

[21] L. G. Valiant: The complexity of enumeration and reliability problems, *SIAM Jo on Computing* **8** (1979) 410–421.

[22] L. Zamansky, and V. Cherkassky: Determination of the number of integer in polyhedra in $\mathbf{R}^3$: polynomial algorithms, *Doklady Akad. Nauk. Ukrain. Ser. A* (1983) No. 4, 13–15.

[23] L. Zamansky, and V. Cherkassky: The formula for finding the number of i points under a line and its application, *Ekonomika i Mat. Metody* **20** (198 6, 1132–1138.

[24] L. Zamansky, and V. Cherkassky: *Effective algorithms for the solution of d optimization problems*, Kiev: Znanie, 1984.

[25] L. Zamansky, and V. Cherkassky: Generalization of the Jacobi-Perron algo for determining the number of integer points in polyhedra, *Dolklady Akad. Ukrain. USSR Ser. A* (1985) No. 10, 11–13.

W. Cook

Bell Communications Research, U.S.A.
and Institut für Ökonometrie und
Operations Research, Universität Bonn,
Germany.
bico@breeze.bellcore.com

M. Hartmann

Department of Operations Research,
University of North Carolina,
U.S.A.
slug@unc.bitnet

R. Kannan

Computer Science Department,
Carnegie-Mellon University,
U.S.A.
kannan@theory.cs.cmu.edu

C. McDiarmid

Institute of Economics and Statistics,
Oxford, United Kingdom.
mcd%vax.oxford.ac.uk
@nsfnet-relay.ac.uk