...AL J. COMPUT.
...20, No. 4, pp. 695–707, August 1991

ON COUNTING LATTICE POINTS IN POLYHEDRA*

MARTIN DYER†

Abstract. Some reductions of the computational problem of counting all the integer lattice points in an arbitrary convex polyhedron in a fixed number of dimensions d are considered. It is shown that only ...dd d need to be studied. In three dimensions the problem is reduced to the computation of Dedekind ...ums. Hence it is shown that the counting problem in three or four dimensions is in polynomial time. A ...rresponding reduction of the five-dimensional problem is also examined, but is not shown to lead to ...olynomial-time algorithms.

Key words. lattice points, polynomial time, Dedekind sums, convex polyhedron

AMS(MOS) subject classifications. 52A15, 52A20, 52A25, 52A43

1. Introduction. Questions concerning the existence of integer lattice points in convex polyhedra have been well studied. The problem of determining whether the polyhedron contains *any* lattice points is the problem of integer programming. This is well known to be NP-complete in general [7], but it is an equally well-known result of Lenstra [14] that this can be done in polynomial time in any fixed dimension. (See also Kannan [10] for subsequent improvements.)

Counting *all* lattice points in a polyhedron is #P-complete, in general [24], but the status of the problem in fixed dimension is less clear. In three and four dimensions, Mordell [15] proved results concerning the numbers of lattice points in the simplex formed by cutting an orthant with a hyperplane. In the special case of pairwise coprime edge lengths (for the orthogonal sides), he established a close connection with the Dedekind sums [19]. Though his concerns were not principally computational, Mordell's paper is one of the main inspirations for the results here. Zamanskii and Cherkaskii [25], [26], [27], [28] also examined the counting problem. They were able to show that it is in polynomial time in $\mathbb{R}^2$. They analysed extensions to $\mathbb{R}^3$ but were unable to find a polynomial-time algorithm for the general three-dimensional case. Cook, Hartmann, Kannan, and McDiarmid [4] examined the problem of *approximately* counting and showed that this is polynomial-time solvable in any fixed dimension. They also showed that, in variable dimension, it is even NP-hard to approximate to within exponential factors.

There has also been interest in counting the numbers of *vertices* of the convex hull of all the lattice points in a polyhedron [23], [9], [17], [4], [2]. It has been shown that this number is bounded by a polynomial in the size of description when the dimension is fixed. This important fact is vital to the development here. Hartmann [8] describes a polynomial-time algorithm for listing all vertices of this convex hull when the dimension is fixed.

There is a wealth of related material, and the reader should note that the literature cited here is in no way comprehensive, nor is it intended to be.

The main contribution of this paper is to show that there is a polynomial-time algorithm for the general lattice point counting problem for polyhedra in both three and four dimensions. The method is based on reduction to counting a particular type of simplex. This reduction is quite general. The problem of counting in even dimensions

...ived by the editors August 31, 1990; accepted for publication (in revised form) November 28, 1990.
...ool of Computer Studies, University of Leeds, Leeds, United Kingdom.

is further reduced to that in lower odd dimensions. The three-dimensional problem is then shown to rest on the computation of Dedekind sums, which can be evaluated in polynomial time.

2. Definitions and notation. Throughout, $[n]=\{1,2,\cdots,n\}$, and $[m,n]=\{m,m+1,\cdots,n\}$. A *sign* means an element of $\{-1,1\}$. If $n\geqq m\geqq 0$ are integers, we write $n^{\langle m\rangle}$ for $n(n-1)\cdots(n-m+1)$ ($=1$ if $m=0$). For $S\subseteq\mathbb{R}^d$, int S, cl S, aff S, and conv S denote the interior, closure, affine hull, and convex hull of S.

We use simplicial decompositions of (convex) polyhedra. Now any closed polyhedron has a unique partition into relatively open faces. We will call $P\subseteq\mathbb{R}^d$ a polyhedron if it is any union of relatively open faces of the closed polyhedron cl P. We write the implied relation as $P\sqsubseteq$ cl P. The adjectives *open* or *closed* will be used if we wish to be more specific. We use the term *simplex* similarly. If P is a polyhedron, any face of cl P will be called a *face* of P, but it will be called *included* or *excluded*, depending on whether or not it actually belongs to P. In particular, vert P denotes the vertex set of P. We must, of course, assume that this list of open faces is supplied as part of the description of P. We observe that the maximum number of such faces is polynomial in the number of facets or vertices of P in any fixed dimension, so the list cannot be too large. A polyhedron $P\subseteq\mathbb{R}^d$ will be called *full* if int $P\neq\emptyset$. For any $S\subseteq\mathbb{R}^d$, we denote by $|S|$ the number of integer lattice points belonging to S (i.e., $|S|\stackrel{\text{def}}{=}|S\cap\mathbb{Z}^d|$). *Counting* S means evaluating $|S|$. For any convex S, the *integer hull* of S is the set $S_I=\text{conv}\,(S\cap\mathbb{Z}^d)$. A polyhedron P is *integral* if cl $P=P_I$, i.e., P has only integer vertices.

We use vector notation in a rather sloppy fashion. Whether a row or column vector is intended will be clear from the context. A vector may also be regarded as the ordered sequence of its coordinates or as the corresponding linked list of its coordinates. We are correspondingly sloppy about the use of the notation "dim," which simply means "dimension." Again, we believe the meaning should be clear from the context. (The multiple usage of the term "dimension" is, perhaps unfortunately, common in mathematics.)

Throughout, e_i is the ith unit vector and e a vector of all 1's. If $a\in\mathbb{R}^d$ and $\alpha\in\mathbb{R}$, the notation $a>\alpha$ (and similar) means $a>\alpha e$. We will write $a\wedge b$ for gcd (a,b). It is well known that the operation "$\wedge$" is then associative and commutative. If $x\in\mathbb{R}$, we use the (nonstandard) notation $\{\!\{x\}\!\}=x-\lfloor x\rfloor$ to denote the "fractional part." We use this principally in § 6, when considering Dedekind sums. It is traditional in this setting to use the "sawtooth" function $((x))=x-\frac{1}{2}(\lfloor x\rfloor+\lceil x\rceil)$. (See, for example, [19], [13].) This function has some nice properties for dealing with Dedekind sums and their relatives but gives no simplification of our results. Consequently, we will not use it.

3. Preliminary observations. Let P be a polyhedron such that cl $P=\{x\in\mathbb{R}^d: Ax\leqq b\}$, where A is an $m\times d$ integer matrix and b an m-vector. We consider the computational problem of determining $|P|$ when the dimension d is fixed. We call this the *d-dimensional counting problem.* Our objective is to perform the computation in polynomial time. When we use the term *polynomial* in this paper, we will usually mean polynomial in the size of the input A, b, as measured in [22]. Observe that we may equally suppose that cl P is given as a list of rational vertices, since (in fixed dimension) there is no difficulty in moving between these representations in polynomial time. Similarly, any reasonable representation of the list of included faces will suffice. We may also observe here that we lose little generality in restricting to the integer lattice since, for any lattice with rational generators, we can reduce to this case by finding a basis (in polynomial time) and then making substitutions. (See [22].)

We consider reductions of the general counting problem to that for "simpler" classes of polyhedra. Thus let us use the following terminology. If $\mathscr{C}$ is any class of polyhedra, let $\mathscr{C}_d = \{C \in \mathscr{C}: \dim(C) \leqq d\}$. If $\mathscr{D}$ is some other class, let us say that $\mathscr{C}_d$ *reduces* to $\mathscr{D}_d$ if counting any $C \in \mathscr{C}_d$ is achievable in polynomial time using an oracle that counts arbitrary $D \in \mathscr{D}_d$. We will say that $\mathscr{C}$ reduces to $\mathscr{D}$ if $\mathscr{C}_d$ reduces to $\mathscr{D}_d$ for all (fixed) d.

We use $\mathscr{A}$ to denote the class of all polyhedra. Thus if the counting problem is polynomial-time solvable in all fixed dimensions, $\mathscr{A}$ reduces to $\varnothing$. Clearly $\mathscr{A}$ reduces to the class of full polyhedra, since if P is not full, we may reduce dimension by making a suitable substitution in the inequality system. The same is true for open polyhedra, since all open faces of a polyhedron P are lower dimensional open polyhedra. Note that, in variable dimension, it is a nontrivial task [5] to determine in polynomial time the affine hull of a polyhedron in some presentations. However, in fixed dimension, this computation is clearly polynomial-time equivalent to finding the affine hull of its (explicitly presented) vertex set, a more straightforward task.

A much deeper fact is that $\mathscr{A}$ reduces to the class of open integral simplices. This may be seen as follows. First, determine the integer hull P_I of P. Because P_I has only polynomially many vertices, this can be done in polynomial time using fixed-dimensional integer programming [14], [10]. See Cook, Hartmann, Kannan, and McDiarmid [4] and Hartmann [8]. We may then triangulate P_I into a simplicial complex, such that all simplices have vertices which are also vertices of P_I. Hence we can partition P_I into open simplices of various dimensions. The conclusion now follows.

4. Reduction to a standard integral simplex. In this section we show that $\mathscr{A}$ reduces to a certain "nice" class of open simplices. For reasons discussed in § 1, it is more convenient to prove the reduction using general simplices. The proof is based on the following lemma.

LEMMA 1. *Let A be a nonsingular $d \times d$ integer matrix; then there exists a unimodular matrix U such that every element in the first row of UA is α, for some integer $\alpha \neq 0$. The matrix U can be determined in polynomial time (even when d is not fixed).*

Proof. Let $a = (\det A)eA^{-1}$. Then a is clearly an integral vector. Reduction of a to Hermite normal form (see [22, Chap. 4]) shows that there is a unimodular matrix V such that $aV = \beta e_1$, for some integer $\beta \neq 0$. Now if $U = V^{-1}$, with first row u_1, then $u_1 = \beta u_1$. Thus $u_1 = \beta^{-1}a$, and we have $u_1 A = \alpha e$, a constant vector, with $\alpha = (\det A/\beta)$. Clearly α is an integer, since u_1, A are integral. Thus U has the required property. It can be determined in polynomial time using a suitable Hermite normal form algorithm. (See [22, Chap. 5].) □

We will need the following lemma on decomposition of simplices.

LEMMA 2. *Let $S \subseteq \mathbb{R}^d$ be a full simplex with vertex set $V = \{p^0, p^1, \cdots, p^d\}$, and let $p \in \mathbb{R}^d$ be any point. Let F_i be the facet of S with* vert $F_i = (V \backslash \{p^i\})$, *and let* $S_i = \text{conv}(\text{vert } F_i \cup \{p\})$. *Then there exist full simplices $S_i' \subseteq S_i$, $(i \in I \subseteq [0, d])$ and signs σ_i such that*

$$|S| = \sum_{i \in I} \sigma_i |S_i'|.$$

Proof. Define

$$\begin{aligned} \sigma_i &= -1 \quad \text{if aff } F_i \text{ strictly separates } p, p^i, \\ &= 0 \quad \text{if aff } F_i \text{ contains } p, \\ &= +1 \quad \text{otherwise.} \end{aligned}$$

Let $I=\{i: \sigma_i \neq 0\}$, $I^+=\{i \in I: \sigma_i=+1\}$, and $I^-=I \backslash I^+$. Then, letting $S'=$ conv $(S \cup \{p\})$, it is straightforward to show that int S_i $(i \in I^+)$ are the d-dimensional simplices of a simplicial complex that triangulates S', and int S_i $(i \in I^-)$ are the d-dimensional simplices of a similar triangulation of $S' \backslash S$. Therefore we may choose full simplices $S_i' \subseteq S_i$ $(i \in I)$ to partition S' and $S' \backslash S$. Since $|S|=|S'|-|S' \backslash S|$, the lemma follows. □

Let $\mathcal{S}$ be the class of open simplices $\{S_d(a)\}$ where, for some $a \in \mathbb{Z}^d$,

$$\text{vert } S_d(a)=\left\{0, \sum_{j=1}^{k} a_j e_j \ (k \in [d])\right\}. \tag{1}$$

We will always assume, below, that $a>0$. This involves no real loss of generality since we are interested only in full simplices, and reflection in a coordinate hyperplane is a unimodular transformation.

We now observe that $S_d(a)$ has the following nice description by facets.

$$S_d(a)=\{x \in \mathbb{R}^d: 1>x_1/a_1>x_2/a_2 \cdots>x_d/a_d>0\}. \tag{2}$$

To see this, note first that all the vertices of $S_d(a)$ are in the closure of the set defined by the inequalities in (2), and only the kth vertex in (1) fails to satisfy the kth inequality as equality. (We are defining the 0th vertex in (1) to be 0, and numbering the $(d+1)$ inequalities in (2) $0, 1, \cdots, d$.)

We now prove the reduction theorem.

THEOREM 1. *Let $S \subseteq \mathbb{R}^d$ be a full integral simplex. Then there exist simplices $\Delta_1, \Delta_2, \cdots, \Delta_r$, where $r \leqq d!$, and signs σ_i $(i \in [r])$ such that*

(a) int $\Delta_i \in \mathcal{S}_d$,

(b) $|S|=\sum_{i=1}^{r} \sigma_i |\Delta_i|$.

For fixed d, a description of $\{\Delta_i: i \in [r]\}$ can be computed in polynomial time.

Proof. We assume by induction that, for a given $t \in [0, d]$, there are full integral simplices $\Delta_1^t, \Delta_2^t, \cdots, \Delta_{r_t}^t$, with $r_t \leqq d^{(t)}$, and corresponding signs σ_i^t $(i \in [r_t])$, such that

(a) vert Δ_i^t can be ordered as $(p^0, p^1, \cdots, p^d)$, for instance, so that, for some integers α_j^i,

$$\begin{aligned} p_j^k &= \alpha_j^i \ (j \in [1, t], k \in [j, d]) \\ &= 0 \ (k \in [0, t], j \in [k+1, d]). \end{aligned}$$

(b) $|S|=\sum_{i=1}^{r_t} \sigma_i^t |\Delta_i^t|$.

The theorem is the case $t=d$ of the induction hypothesis. Since S can always be translated onto a full simplex Δ_1^0, which has its first ordered vertex at 0, the hypothesis holds for $t=0$ with $r=1$ and $\sigma_1^0=1$. Assume, then, that it holds for any $t \in [0, d-1]$. Consider a particular Δ_i^t with vertex ordering satisfying (a) of the induction hypothesis. The last $(d-t)$ coordinates of $p^0, \cdots, p^t$ are all zero, by induction, and those of $p^{t+1}, \cdots, p^d$ form the columns of a $(d-t) \times (d-t)$ integer matrix A. Singularity of this matrix would imply dim $\Delta_i^t<d$, contradicting the assumption that Δ_i^t is full. Hence, by Lemma 1, we can determine a unimodular transformation U for A which will make its first row constant. We apply this transformation to the last $(d-t)$ coordinates of $\mathbb{R}^d$, leaving the first t invariant (i.e., we augment U by a $t \times t$ identity matrix). This transformation preserves the integer lattice, and hence leaves $|\Delta_i^t|$ unaltered. Now, however, $p^{t+1}, \cdots, p^d$ all have their $(t+1)$st component equal to α, for some integer α. Let $p=(\alpha_1^i, \alpha_2^i, \cdots, \alpha_t^i, \alpha, 0, \cdots, 0)$. We now apply Lemma 2 to (Δ_i^t, p) to conclude that Δ_i^t can be replaced by a set of full simplices $\{\Delta_j': j \in J \subseteq [0, d]\}$, where vert $\Delta_j'=$ (vert $\Delta_i^t \backslash \{p^j\}) \cup \{p\}$. Thus $|J| \leqq (d+1)$, but we may bound it more tightly as follows.

Note that p has its first $(t+1)$ coordinates equal to those of $p^{t+1}, \cdots, p^d$. Thus, for $j \in [0, t]$, Δ_j^t has a set of $(d-t+1)$ vertices which lie in $(t+1)$ common hyperplanes, i.e., in an affine subspace of dimension $(d-t-1)$. Thus we can find a hyperplane which includes all the vertices of Δ_j^t. Hence we may assume $J \subseteq [t+1, d]$, and hence $|J| \leqq (d-t)$.

Now $\{\Delta_i^{t+1}: i \in [r_{t+1}]\}$ is formed by replacing each Δ_i^t by the set Δ_j^t $(j \in J)$, derived as above. Then $r_{t+1} \leqq (d-t) r_t \leqq (d-t) d^{(t)} = d^{(t+1)}$, using the induction hypothesis and the bound on $|J|$. The vertex ordering for Δ_j^t may be any having $(p^0, p^1, \cdots, p^t, p)$ as an initial subsequence. Then part (a) of the induction hypothesis for the Δ_i^{t+1} is obvious from the specification of p. Part (b) follows from the final identity of Lemma 2 and (b) of the induction hypothesis for the Δ_i^t. This completes the induction. There is clearly a polynomial-time algorithm for the decomposition which directly mirrors the method of proof. □

Thus $\mathscr{A}$ reduces to $\{P: \text{int } P \in \mathscr{S}\}$. Now $\mathscr{A}$ will reduce to $\mathscr{S}$ immediately if $\mathscr{S}$ is closed under the operation of taking subfaces. We prove this next. Let p^i $(i \in [0, d])$ be the ith ordered vertex of $S_d(a)$. Let F be any face of $S_d(a)$, with vert $F = \{p^i: i \in I_F\}$. Consider the following procedure applied to the d-vector a, viewed as a formal list.

function $b(a, F)$

(1) **for** $i \in [d-1]$ **do**
  if $i \notin I_F$ **then** insert the (g.c.d.) operation $\wedge$ between a_i and a_{i+1}.

(2) Evaluate all the $\wedge$ operations to give the reduced vector b, for instance.

(3) **if** $0 \notin I_F$ **then** delete the first element of b.
  if $d \notin I_F$ **then** delete the last element of b.

(4) $b(a, F) \leftarrow b$.

Clearly $b(a, F)$ is a vector with $\dim b = \dim F$. Call $b = b(a, F)$ a *face-vector* of a. Clearly any face-vector can be obtained in polynomial time. Now we have the following lemma.

LEMMA 3. *If F is an open face of $S_d(a)$ with $\dim F = k$, then $|F| = |S_k(b)|$, where $b = b(a, F)$.*

Proof. Since the g.c.d. operator is associative, it is clearly sufficient to prove this for F a facet and to use induction. If $0 \notin I_F$, then we must have $x_1/a_1 = 1$ on F, and the lemma follows directly. Similarly if $d \notin I_F$, we have $x_d/a_d = 0$. If $i \notin I_F$ $(i \in [d-1])$, we have $x_i/a_i = x_{i+1}/a_{i+1}$ on F. Let $\lambda = a_i \wedge a_{i+1}$, $\alpha = a_i/\lambda$, $\beta = a_{i+1}/\lambda$. It follows from simple divisibility considerations that we must have $x_i = x'\alpha$, $x_{i+1} = x'\beta$ for $x' \in [\lambda - 1]$ at integer points on F. Thus $x_i/a_i = x_{i+1}/a_{i+1} = x'/\lambda$ at all such points. The lemma now follows. □

COROLLARY 1. *$\mathscr{A}$ reduces to $\mathscr{S}$.*

Remark 1. The simplices, $\mathscr{M} = \{M_d(a)\}$, considered by Mordell [15], were

$$M_d(a) = \left\{ x \in \mathbb{R}^d: \sum_{j=1}^{d} x_j/a_j < 1,\ x_1/a_1 > 0,\ x_2/a_2 > 0, \cdots, x_d/a_d > 0 \right\},$$

so vert $M_d(a) = \text{conv}\{0, a_j e_j\ (k \in [d])\}$. For $d \leqq 2$, $\mathscr{M}_d$ and $\mathscr{S}_d$ are essentially the same, but this is not true for $d \geqq 3$. The class $\mathscr{M}$ may appear simpler than $\mathscr{S}$, but we do not know whether $\mathscr{A}$ reduces to $\mathscr{M}$.

5. Even dimensions. The main result of this section is to show that, if d is even, $\mathscr{A}_d$ reduces to $\mathscr{A}_{d-1}$.

If $\gamma \in [3]^{d-1}$, consider the following algorithm applied to $a \in \mathbb{Z}_+^d$.

function $\phi(\gamma, a)$

(1) **for** $i \in [d-1]$ **do**

if $\gamma_i = 1$ **then** split the list between a_i and a_{i+1}.
if $\gamma_i = 2$, **then** insert the operation $\wedge$ between a_i and a_{i+1}.

(2) Evaluate all the g.c.d. operations in the sublists.
Let b_j ($j \in [r]$) be the resulting reduced sublists (i.e., vectors).
Let $k_j = \dim b_j$ and $t = |\{i: \gamma_i = 1\}|$.

(3) $\phi(\gamma, a) \leftarrow (-1)^{d-1-t} \prod_{j=1}^{r} |S_{k_j}(b_j)|$.

Then we have the following theorem.

THEOREM 2. *Let d be even, and let $\Gamma = [3]^{d-1} \setminus \{3e\}$. Then*

$$|S_d(a)| = \frac{1}{2} \sum_{\gamma \in \Gamma} \phi(\gamma, a).$$

Proof. The method is "inclusion-exclusion," using a natural symmetry of $S_d(a)$. Let

$$R_d(a) = [a_1 - 1] \times [a_2 - 1] \times \cdots \times [a_j - 1].$$

If $x \in R_d(a)$ (which we will abbreviate to R) then, from (2), under the bijection $x \mapsto (a - x)$ on R,

$$|S_d(a)| = |\{x \in R: x_1/a_1 < x_2/a_2 < \cdots < x_d/a_d\}|. \tag{3}$$

For $i \in [d-1]$, let us write $\lambda_i(x) = (x_i/a_i - x_{i+1}/a_{i+1})$. For $\rho \in \{<, =, >\}$, let δ_i^{ρ} be the indicator function of $\lambda_i(x)\ \rho\ 0$. Then, from (2) and (3),

$$|S_d(a)| = \sum_{x \in R} \prod_{i=1}^{d-1} \delta_i^{>}(x) = \sum_{x \in R} \prod_{i=1}^{d-1} \delta_i^{<}(x). \tag{4}$$

However, we have $\delta_i^{<}(x) = 1 - \delta_i^{>}(x) - \delta_i^{=}(x)$. Thus the last expression of (4) implies

$$|S_d(a)| = \sum_{x \in R} \prod_{i=1}^{d-1} (1 - \delta_i^{=}(x) - \delta_i^{>}(x)). \tag{5}$$

Expanding the product in (5), we obtain $|S_d(a)|$ as the sum of 3^{d-1} terms, each of the form

$$\sigma \sum_{y \in R} \prod_{i=1}^{d-1} \zeta_i(y), \tag{6}$$

where σ is a sign, and $\zeta_i \in \{\delta_i^{>}, \delta_i^{=}, 1\}$. Each ζ_i is an indicator function, so the product in (6) is the indicator of an intersection of sets. For each i there are three possibilities. The case $\zeta_i = 1$ is equivalent to deleting the $(i+1)$st inequality in (2), so the inequality system "decomposes" on R into

$$\{x_1/a_1 > \cdots > x_i/a_i\} \times \{x_{i+1}/a_{i+1} > \cdots > x_d/a_d\}.$$

This corresponds to "splitting" the vector a, i.e., to $\gamma_i = 1$ in the computation of $\phi(\gamma, a)$. Having $\zeta_i = \delta_i^{=}$ corresponds to replacing the $(i+1)$st inequality in (2) by an equality. This is equivalent to inserting the g.c.d. operation in a, i.e., to $\gamma_i = 2$ in the computation of $\phi(\gamma, a)$ (cf. Lemma 3). Finally, $\zeta_i = \delta_i^{>}$ corresponds to imposing the $(i+1)$st inequality in (2), i.e., to $\gamma_i = 3$ in the computation of $\phi(\gamma, a)$. The sign σ is clearly $(-1)^{d-1-t}$, where t is the number of i for which $\zeta_i = 1$. This corresponds to the sign in the computation of $\phi(\gamma, a)$. Thus each of the 3^{d-1} sums is equal to a unique $\phi(\gamma, a)$. However, using (4), we have $\phi(3e, a) = (-1)^{d-1}|S_d(a)| = -|S_d(a)|$, since d is even. The theorem now follows from (5). □

THEOREM 3. *$\mathcal{A}$ reduces to $\mathcal{S}^o = \{S_d(a) \in \mathcal{S}\ (d\ odd)\}$.*

Proof. For even d, the computation of $\phi(\gamma, a)$ for $\gamma \neq 3e$ involves only determination of $|S_k(b)|$ for $k < d$, and b a face-vector of a with $\dim b = k$. The result follows by induction on d. □

COROLLARY 2. $S_1(p) = p-1$, $|S_2(p,q)| = \frac{1}{2}((p-1)(q-1)-(p \wedge q-1))$.

Proof. The first assertion is obvious. The second follows from this and Theorem 2. □

COROLLARY 3.

$$\sum_{x=1}^{p-1} \lfloor qx/p \rfloor = \tfrac{1}{2}((p-1)(q-1)+(p \wedge q-1)),$$

$$\sum_{x=1}^{p-1} \lceil qx/p \rceil = \tfrac{1}{2}(pq+p-q-p \wedge q).$$

Proof. Using Lemma 3,

$$\sum_{x=1}^{p-1} \lfloor qx/p \rfloor = |\{0 < y/q \leqq x/p < 1\}| = |S_2(q,p)| + |S_1(p \wedge q)|,$$

$$\sum_{x=1}^{p-1} \lceil qx/p \rceil = |\{0 \leqq y/q < x/p < 1\}| = |S_2(q,p)| + |S_1(p)|.$$

The results now follow from these and Corollary 2. □

COROLLARY 4. *Two-dimensional counting can be done in polynomial time.*

Proof. The proof follows from Corollary 2 and Theorem 3. □

Remark 2. The result of Corollary 4 was previously obtained, using different methods, by Zamanskii and Cherkaskii (see [25]-[28]).

Remark 3. For any suitably defined convex body K in $\mathbb{R}^d$ the feasibility question $|K| \geqq 0$ can be answered in polynomial time by fixed-dimensional integer programming. (See Kannan [10, p. 434]. By "suitably defined" here, we mean "given by a (polynomial time) separation oracle.") Hence the integer hull K_I of such a body could be determined in polynomial time by the "gift wrapping" idea (see [18, p. 125]) *provided* K_I has only polynomially many vertices. Since K_I is a polyhedron, counting K could then be achieved as above. We might therefore hope that Corollary 4 would generalise. However, it appears to fail for very simple convex sets in $\mathbb{R}^2$. To see this, consider

$$K(n) = \{(x,y) \in \mathbb{R}^2 : xy \geqq n,\ 1 \leqq (x,y) \leqq n\}.$$

It is easy to see that $|K(n+1)| - |K(n)| = 2n-1$ if and only if n is prime. A polynomial-time algorithm for counting $K(n)$ therefore implies a similar algorithm for primality testing. Thus we might guess that $K_I(n)$ can have nonpolynomially many vertices. It is easy to see that this can happen. Let $m \geqq 114$, and n be the product of the first $\lceil m/\ln m \rceil$ primes. Each prime is at most m by a form of the Prime Number Theorem [21]. Thus $n < 3^m$, say, so m measures the input size of $K(n)$. However, n has at least $2^{m/\ln m}$ (ordered) two-term factorizations, i.e., nonpolynomially many. Each gives a vertex of $K_I(n)$. Thus the approach to counting $K(n)$ used here is doomed at the outset. (See Remark 8 below for an even worse example.)

Remark 4. The proof of Theorem 2 leads to a closed formula for $S_d(a)$. Note that $-1 < \lambda_i(x) < 1$ on R, and thus $\delta_i^{>}(x) = \lceil \lambda_i(x) \rceil$. Thus, from (4),

$$|S_d(a)| = \sum_{x_1=1}^{a_1-1} \sum_{x_2=1}^{a_2-1} \cdots \sum_{x_d=1}^{a_d-1} \left\lceil \frac{x_1}{a_1} - \frac{x_2}{a_2} \right\rceil \left\lceil \frac{x_2}{a_2} - \frac{x_1}{a_1} \right\rceil \cdots \left\lceil \frac{x_d}{a_d} - \frac{x_{d-1}}{a_{d-1}} \right\rceil.$$

Unfortunately, this expression is not directly computable in polynomial time.

We prove one further general reduction, that the elements of a need have no common divisor. We place it here since it has some superficial similarities to Theorem 2. For this, it is convenient to use

$$S'_d(a) = \{1 > x_d/a_d > \cdots > x_1/a_1 \geqq 0\},$$

rather than $S_d(a)$. Let $\gamma \in [2]^{d-1}$, $a \in \mathbb{Z}_+^d$, and $\lambda \in \mathbb{Z}_+$. Consider

function $\zeta(\gamma, a, \lambda)$
(1) **for** $i \in [d-1]$ **do**
  if $\gamma_i = 1$ **then** split the list between a_i and a_{i+1}.
(2) Let b_j $(j \in [r])$ be the resulting sublists of a, $k_j = \dim b_j$.
(3) $\zeta(\gamma, a, \lambda) \leftarrow \binom{\lambda}{r} \prod_{j=1}^{r} |S'_{k_j}(b_j)|$.

Then we have the following lemma.

LEMMA 4. $|S'_d(\lambda a)| = \sum_{\gamma \in [2]^{d-1}} \zeta(\gamma, a, \lambda)$.

Proof. Partition the $x \in S'_d(\lambda a)$ into *boxes* according to $\lfloor x_i/a_i \rfloor = s_i - 1$. A box corresponds to a nonincreasing sequence $s = (s_1, \cdots, s_d)$ such that $s_i \in [\lambda]$. Any such s splits into maximal subsequences for which s_i has the same value. Suppose there are r distinct s_i. There are exactly $\binom{\lambda}{r}$ ways of choosing these distinct values. For each choice, the possible s can then be formed by splitting a d-sequence into r nonempty parts, and then assigning the r values, in decreasing order, to the successive parts. Any split into r parts corresponds to choosing a γ. For a given split, suppose $s_j = \cdots = s_{j+k-1}$ $(= \xi - 1)$ is any part, and let $b = (a_j, \cdots, a_{j+k-1})$ be the corresponding part of a. In $S'_d(a)$, we must have

$$(\xi + 1) > x_j/a_j > \cdots > x_{j+k-1}/a_{j+k-1} \geqq \xi.$$

But this set has a bijection $x_l \mapsto (x_{j+l-1} - \xi a_{j+l-1})$ $(l \in [k])$ with $S'_k(b)$. The lemma now follows. □

Remark 5. This lemma is closely related to the theorem that the number of lattice points in a polyhedron varies polynomially under the operation of subdivision of the lattice. (See, for example, [16].) Unfortunately, it does not seem that we can apply this result directly to get our conclusion here.

THEOREM 4. *$\mathcal{A}$ reduces to $\mathcal{S}^* = \{S_d(a) \in \mathcal{S}^o : a_1 \wedge \cdots \wedge a_d = 1\}$.*

Proof. By induction on d, the result follows from Theorem 3, Lemma 4, and the equation $|S'_d(a)| = |S_d(a)| + |S_{d-1}(a')|$ (where $a' = (a_1, \cdots, a_{d-1})$), which follows from Lemma 3. □

6. Dedekind sums and three dimensions. From Theorem 4, three-dimensional counting clearly reduces to counting $S_3(r, p, q)$, where $p \wedge q \wedge r = 1$. Then, however, using Lemma 3 and Corollary 2,

$$|S_3(r, p, q)| = N - |S_2(r, p \wedge q)| = N - \tfrac{1}{2}(p \wedge q - 1)(r-1),$$

where, if (z, x, y) is the typical point of $\mathbb{R}^3$,

$$N = |\{0 < y/q \leqq x/p < z/r < 1\}|. \tag{7}$$

It clearly suffices to determine N. But since, for any integer $0 < x < p$, there are $\lfloor qx/p \rfloor$ values of y, and $(r - 1 - \lfloor rx/p \rfloor)$ values of z in (7),

$$\begin{aligned} N &= \sum_{x=1}^{p-1} \lfloor qx/p \rfloor (r - 1 - \lfloor rx/p \rfloor), \\ &= (r-1) \sum_{x=1}^{p-1} \lfloor qx/p \rfloor - \sum_{x=1}^{p-1} \lfloor qx/p \rfloor \lfloor rx/p \rfloor, \qquad (8) \\ &= \frac{1}{2}(r-1)((p-1)(q-1) - (p \wedge q - 1)) - \sum_{x=1}^{p-1} \lfloor qx/p \rfloor \lfloor rx/p \rfloor, \end{aligned}$$

using Corollary 2. It thus suffices to determine $\sum_{x=1}^{p-1} \lfloor qx/p \rfloor \lfloor rx/p \rfloor$. Now let

$$D_p^{q,r} \stackrel{\text{def}}{=} \sum_{x=1}^{p-1} \{\!\{qx/p\}\!\}\{\!\{rx/p\}\!\},$$

$$D_p^{q} \stackrel{\text{def}}{=} D_p^{q,1} = \sum_{x=1}^{p-1} (x/p)\{\!\{qx/p\}\!\},$$

$$D_p \stackrel{\text{def}}{=} D_p^{1} = \sum_{x=1}^{p-1} (x/p)^2 = (p-1)(2p-1)/6p.$$

The order of superscipts in $D_p^{q,r}$ is clearly immaterial. Now, using the above notation,

$$\sum_{x=1}^{p-1} \lfloor qx/p \rfloor \lfloor rx/p \rfloor = \sum_{x=1}^{p-1} (qx/p - \{\!\{qx/p\}\!\})(rx/p - \{\!\{rx/p\}\!\})$$

$$= rqD_p - qD_p^r - rD_p^q + D_p^{q,r}.$$

Thus we have only to evaluate the sum $D_p^{q,r}$ in polynomial time in order to have a polynomial-time algorithm for three-dimensional counting. Since $D_p^{q,r}$ has $(p-1)$ terms, it is not obvious that this is possible. However, sums of this type have been well studied, since the D_p^q are (essentially) the "Dedekind sums" [19]. We first show that $D_p^{q,r}$ can be determined using only a polynomial-time algorithm for evaluating D_p^q in the special case $p \wedge q = 1$. We need the following simple lemma. This lemma is well known in relation to Dedekind sums, as is some of the other content of this section, but we give proofs, since they are all fairly short.

LEMMA 5. *If* $\theta \in \mathbb{R}$ *and* $p \wedge q = 1$, *then* $\sum_{x=0}^{p-1} \{\!\{(qx+\theta)/p\}\!\} = \{\!\{\theta\}\!\} + \frac{1}{2}(p-1)$.

Proof. Substitute $x \mapsto q^{-1}x \bmod p$ into the sum. (Because $p \wedge q = 1$, q^{-1} exists and the mapping is bijective.) The sum is then $\sum_{x=0}^{p-1} \{\!\{(x+\theta)/p\}\!\}$. With a further variable change $x \mapsto (x - \lfloor \theta \rfloor) \bmod p$, this is $\sum_{x=0}^{p-1} (x + \{\!\{\theta\}\!\})/p$, giving the result. □

We now prove the claimed reduction.

LEMMA 6. *If* $p \wedge q \wedge r = 1$, $\lambda = p \wedge q$, $(\alpha, \beta) = (p, q)/\lambda$, *then*

$$D_p^{q,r} = D_\alpha^{\beta,r} + \tfrac{1}{4}(\lambda - 1)(\alpha - 1).$$

Proof. Putting $x = \mu\alpha + \nu$ $(\mu \in [0, \lambda - 1],\ \nu \in [0, \alpha - 1])$,

$$D_p^{q,r} = \sum_{\nu=0}^{\alpha-1} \sum_{\mu=0}^{\lambda-1} \{\!\{(r\mu + r\nu/\alpha)/\lambda\}\!\}\{\!\{\beta\nu/\alpha\}\!\}.$$

Using Lemma 5 on the inner sum gives

$$D_p^{q,r} = \sum_{\nu=0}^{\alpha-1} \left(\{\!\{r\nu/\alpha\}\!\} + \frac{1}{2}(\lambda - 1) \right) \{\!\{\beta\nu/\alpha\}\!\}.$$

Applying Lemma 5 again (with $\theta = 0$) on the second term in this sum gives the conclusion. □

Therefore we may suppose that $p \wedge q = 1$.

Remark 6. The assumption $p \wedge q \wedge r = 1$ is not entirely necessary, since if $\lambda = p \wedge q \wedge r$ and $(\alpha, \beta, \gamma) = (p, q, r)/\lambda$, we can easily show that $D_p^{q,r} = \lambda D_\alpha^{\beta,\gamma}$.

LEMMA 7. *If* $p \wedge q = 1$, *then* $D_p^{q,r} = D_p^t$, *where* $t \equiv rq^{-1} \pmod p$.

Proof. Change variable $x \mapsto q^{-1}x \bmod p$ (cf. proof of Lemma 5). □

We have thus reduced to evaluating D_p^q. But, by Lemma 6, we may assume $p \wedge q = 1$ are coprime. All the work required so far can be done in polynomial time using only

the Euclidean algorithm. It remains only to show how to evaluate D_p^q in polynomial time in the case $p \wedge q = 1$. That this can be done is a direct consequence of the famous "reciprocity relation" of Dedekind. Many proofs of this identity, and generalizations, are known (see [19], [13]). Since we have the machinery available, we give a short proof for completeness.

LEMMA 8. *If* $p \wedge q = 1$, *then*

$$D_p^q + D_q^p = \tfrac{1}{4}(p+q-3) + \tfrac{1}{12}(p/q + q/p + 1/pq).$$

Proof. The variable change $x \mapsto q^{-1}x \bmod p$ implies $D_p^{q,q} = D_p$. Thus

$$\sum_{x=1}^{p-1} \lfloor qx/p \rfloor^2 = \sum_{x=1}^{p-1} (qx/p - \{\!\{qx/p\}\!\})^2 = (q^2+1)D_p - 2qD_p^q. \tag{10}$$

Since qx/p, py/q are not integral for $x \in [p-1]$, $y \in [q-1]$,

$$\begin{aligned}
\sum_{x=1}^{p-1} \lfloor qx/p \rfloor^2 &= \sum_{0<y/q<x/p<1} (2y-1) \\
&= \sum_{0<x/p<y/q<1} (2(q-y)-1) \\
&= \sum_{y=1}^{q-1} ((2q-1)-2y)\lfloor py/q \rfloor, \qquad (11) \\
&= \frac{1}{2}(2q-1)(p-1)(q-1) - 2\sum_{y=1}^{q-1} y(py/q - \{\!\{py/q\}\!\}) \\
&= (p-3)qD_q - 2qD_q^p,
\end{aligned}$$

where the first line involves an elementary sum, the second follows by making the variable change $x \mapsto (p-x)$, $y \mapsto (q-y)$, the fourth by using Corollary 3, and the fifth by using (9). The lemma now follows by equating (10) and (11), using (9), and simplifying. □

COROLLARY 5. $D_p^{q,r}$ *can be evaluated in polynomial time.*

Proof. We need only consider D_p^q with $p \wedge q = 1$. If $q > p$, then clearly $D_p^q = D_p^{q'}$, where $q' = q \bmod p$. This, with Lemma 8, implies an algorithm whose behaviour and analysis closely parallel those of the Euclidean algorithm. (Note, since $p \wedge q = 1$, we finally reach $D_1^p = 0$.) □

Remark 7. Lemma 8 is clearly elementary, but was discovered by Dedekind in the context of modular function theory. (See [1, Chap. 3] for an introduction.) The book by Rademacher and Grosswald [19] is an exhaustive account of the known facts on Dedekind sums at the time of publication (1972). The algorithm for the calculation of the sums was probably known from Dedekind onwards, as was its "computational efficiency." More recently, explicitly algorithmic treatments have been given, for example, by Knuth [12], [13].

In consequence of the results of this section, we have Theorem 5.

THEOREM 5. *Three-dimensional counting can be done in polynomial time.* □

From Theorem 3, we can therefore conclude with Theorem 6.

THEOREM 6. *Four-dimensional counting can be done in polynomial time.* □

Remark 8. In $\mathbb{R}^4$, counting more general convex bodies appears even harder than was implied for $\mathbb{R}^2$ by Remark 3. The following observation is due to Kannan [11]. Let

$$B_4(n) = \{x \in \mathbb{R}^4 : x_1^2 + x_2^2 + x_3^2 + x_4^2 \leqq n\}.$$

It is a classical result of Jacobi (see, for example, [6]) that

$$r_4(n) = |B_4(n)| - |B_4(n-1)| = 8 \sum_{4 \nmid m \mid n} m.$$

Thus if n is the product of distinct odd primes p, q, then $r_4(n) = 8(1+p+q+n)$. This, together with $n = pq$, is sufficient to determine p and q. Therefore (this type of) factorization can be done in polynomial time given a counting oracle for $B_4(n)$. In particular, a polynomial-time algorithm for counting $B_4(n)$ would imply a similar algorithm for breaking the RSA cryptosystem [20]. All $r_4(n)$ points are vertices of the integer hull of $B_4(n)$, i.e., "exponentially" many.

7. **Beyond four dimensions.** It is not clear how to extend the result of § 6 to higher dimensions, since we have no polynomial-time algorithm for evaluating sums analogous to the $D_p^{q,r}$, i.e., of the form

$$D_p^{q_1,\cdots,q_{d-1}} = \sum_{x=1}^{p-1} \langle\!\langle q_1 x/p \rangle\!\rangle \langle\!\langle q_2 x/p \rangle\!\rangle \cdots \langle\!\langle q_{d-1} x/p \rangle\!\rangle. \tag{12}$$

It is even unclear to what extent the problem can be reduced to the computation of such sums. The reader may check that such sums are sufficient if and only if $\mathscr{A}$ reduces to the class of d-pyramids $\mathscr{P} = \{P_d(a): d \text{ odd}\}$, where

$$P_d(a) = \{0 < x_i/a_i < x_d/a_d < 1 \ (i \in [d-1])\}.$$

We are unable to prove this in general. However, we are able to show that $\mathscr{A}_6$ reduces to $\mathscr{P}_5$. To establish this, it clearly suffices to show that $\mathscr{S}_5$ reduces to $\mathscr{P}_5$. We will briefly outline this reduction below, leaving the interested reader to supply some of the details. Note that the converse implication is true, however. If we could solve the counting problem in d dimensions, then, by counting polyhedra in the class $P_d(a)$, we could certainly evaluate sums of the form (12).

For $a \in \mathbb{Z}_+^5$, let $a^i = (a_1, \cdots, a_i)$ $(i \in [5])$, and, for given a^i,

$$f_i(y) = |\{1 > x_1/a_1 > \cdots > x_{i-1}/a_{i-1} > y/a_i\}|.$$

Let

$$Y(a) = \{1 > x_1/a_1 > x_2/a_2 > x_3/a_3 > (x_4/a_4, x_5/a_5) > 0\},$$

$$X(a) = \{1 > (x_1/a_1, x_2/a_2) > x_3/a_3 > (x_4/a_4, x_5/a_5) > 0\}.$$

We first reduce $S_5(a)$ to $Y(a)$, then to $X(a)$. Simple counting gives

$$|S_5(a)| + |S_5(a^3, a_5, a_4)| = |Y(a)| - |S_4(a^3, a_4 \wedge a_5)|. \tag{13}$$

Letting $g(x) = (\lceil x \rceil - 1)$, we can also show easily that

$$\begin{aligned} |S_5(a)| &= \sum_{y=1}^{a_4-1} g(a_5 y/a_4) f_4(y) \\ &= \lfloor a_5/a_4 \rfloor \sum_{y=1}^{a_4-1} y f_4(y) + \sum_{y=1}^{a_4-1} g(\langle\!\langle a_5/a_4 \rangle\!\rangle y) f_4(y) \\ &= \lfloor a_5/a_4 \rfloor (|S_5(a^4, a_4)| + |S_4(a^4)|) + |S_5(a^4, a_5 \bmod a_4)|, \end{aligned} \tag{14}$$

$$\begin{aligned} |S_5(a^4, a_4)| &= \sum_{y=1}^{a_3-1} \frac{1}{2} g(a_4 y/a_3)(g(a_4 y/a_3) + 1) f_3(y) \\ &= \frac{1}{2} |Y(a^4, a_4)| + \frac{1}{2} |S_4(a^4)|. \end{aligned} \tag{15}$$

From (13), (14), and (15) we can construct a "Euclidean" algorithm which reduces counting $S_5(a)$ to counting a polynomial number of Y's. Essentially the same method,

after using the bijection $x \mapsto (a-x)$, reduces counting $Y(a)$ to counting a polynomial number of X's. Thus we need only to count $X(a)$. But $|X(a)|$ can be expressed as a single sum over x_3, by a similar argument to that leading from (7) to (8). This sum can then be manipulated into the required form. With a little further work, we can show the following lemma.

LEMMA 9. *Five-dimensional counting is polynomial-time (Turing) equivalent to computing the sums*

$$D_p^{q,r,s,t} = \sum_{x=1}^{p-1} \{\!\{qx/p\}\!\}\{\!\{rx/p\}\!\}\{\!\{sx/p\}\!\}\{\!\{tx/p\}\!\},$$

where $q \mid p$ *and* $q \wedge r \wedge s \wedge t = 1$.

Remark 9. The difficulty of computing these "generalized" Dedekind sums (i.e., sums like (12) with odd $d \geqq 5$) is that the "reciprocity relations" which can be obtained (analogously to Lemma 8) are in terms of three or more such sums. (See, for example, [3].) The "Euclidean algorithm" approach therefore leads to branching (and nonpolynomial behaviour) when the number of "parameters" is greater than two. Thus, it is not clear whether these reciprocity relationships are actually useful from a computational viewpoint. (See, for example, the pitfall in the main idea of [28].)

8. Concluding remarks. By reducing to Dedekind sums, we have shown that counting in up to four dimensions can be done in polynomial time. We have been somewhat vague about the complexity of the algorithm, but the reader may check (using [4], [12], [22] for the necessary estimates) that the running time is dominated by the $O((m\phi)^{2d})$ time needed to determine the integer hull P_I. (Here $d = 2, 3$, or 4 is the dimension of P, m is the number of inequalities in the system defining P, and ϕ is the maximum size of any inequality. See [22].)

Obviously, the major question left unresolved is whether a similar result holds in five dimensions (and hence six). A polynomial-time algorithm for evaluating the sums of Lemma 9 would, of course, settle the counting problem for six dimensions. More generally, we might hope that the corresponding result is true for any fixed number of dimensions, as with integer programming. We conjecture that this is the case, though a solution seems to require some new techniques.

Of course, it may be that d-dimensional counting is not in polynomial time for some $d > 4$. Proving #P-completeness, or even NP-hardness, seems likely to be extremely difficult (even if true). It might be possible to reduce some difficult number theoretic problem like factorization to counting, as was done for $B_4(n)$ in Remark 8. However, this also appears tricky, since there is no apparent relationship between linear inequalities and nonlinear problems like factorization.

A less ambitious aim is to establish whether $\mathscr{A}$ reduces to any "nice" classes of polyhedra other than $\mathscr{S}$, for example, the pyramids $\mathscr{P}$ or the Mordell simplices $\mathscr{M}$. Reduction to $\mathscr{P}$ would be interesting, since it would imply the equivalence of counting to evaluating sums like (12).

Acknowledgments. I am indebted to Ravi Kannan on several counts: for bringing the problem to my attention, for providing several key references, and for many informative discussions. I am grateful also to Alan Frieze and David Applegate for useful conversations.

REFERENCES

[1] T. M. APOSTOL, *Modular Functions and Dirichlet Series in Number Theory*, Springer-Verlag, New York, 1976.

[2] I. BÁRÁNY, R. HOWE, AND L. LOVÁSZ, *On integer points in polyhedra: A lower bound*, Combinatorica, to appear.
[3] L. CARLITZ, *A note on generalized Dedekind sums*, Duke J. Math., 21 (1954) pp. 399–403.
[4] W. COOK, M. HARTMANN, R. KANNAN, AND C. MCDIARMID, *On integer points in polyhedra*, Combinatorica, submitted.
[5] J. EDMONDS, L. LOVASZ, AND W. R. PULLEYBLANK, *Brick decompositions and the matching rank of graphs*, Combinatorica, 2 (1982), pp. 247–274.
[6] G. H. HARDY AND E. M. WRIGHT, *An Introduction to the Theory of Numbers*, Fourth Edition, Oxford University Press, Oxford, 1960.
[7] M. R. GAREY AND D. S. JOHNSON, *Computers and Intractability*, W. H. Freeman, San Francisco, CA, 1979.
[8] M. HARTMANN, *Cutting planes and the complexity of the integer hull*, Ph.D. thesis, Cornell University, Ithaca, NY, 1989.
[9] A. C. HAYES AND D. G. LARMAN, *The vertices of the knapsack polytope*, Discrete Appl. Math., 6 (1983), pp. 135–138.
[10] R. KANNAN, *Minkowski's convex body theorem and integer programming*, Math. Oper. Res., 12 (1987), pp. 415–440.
[11] ———, personal communication.
[12] D. E. KNUTH, *The Art of Computer Programming Vol. II: Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 1973.
[13] ———, *Notes on generalized Dedekind sums*, Acta Arithmetica, 23 (1977), pp. 297–325.
[14] H. W. LENSTRA, *Integer programming with a fixed number of variables*, Math. Oper. Res., 8 (1983), pp. 538–548.
[15] L. J. MORDELL, *Lattice points in a tetrahedron and generalized Dedekind sums*, J. Indian Math. Soc., 15 (1951), pp. 41–46.
[16] I. G. MCDONALD, *The volume of a lattice polyhedron*, Proc. Cambridge Philos. Soc., 59 (1963), pp. 719–726.
[17] D. A. MORGAN, *Upper and lower bound results on the convex hull of integer points in polyhedra*, Mathematika, submitted.
[18] F. P. PREPARATA AND M. I. SHAMOS, *Computational Geometry*, Springer-Verlag, New York, 1985.
[19] H. RADEMACHER AND E. GROSSWALD, *Dedekind sums*, Math. Assoc. Amer. Carus Monograph, No. 16, 1972.
[20] R. RIVEST, A. SHAMIR, AND L. ADLEMAN, *A method for obtaining digital signatures and public key cryptosystems*, Comm. ACM, 21 (1978), pp. 120–126.
[21] J. B. ROSSER AND L. SHOENFELD, *Approximate formulas for some functions of prime numbers*, Illinois J. Math., 6 (1962), pp. 66–94.
[22] A. SCHRIJVER, *The Theory of Linear and Integer Programming*, John Wiley, Chichester, U.K., 1986.
[23] V. N. SHEVCHENKO, *On the number of extreme points in integer programming*, Kibernetika, 2 (1981), pp. 133–134.
[24] L. G. VALIANT, *The complexity of enumeration and reliability problems*, SIAM J. Comput., 8 (1979), pp. 410–421.
[25] L. YA. ZAMANSKII AND V. L. CHERKASKII, *Determination of the number of integer points in polyhedra in $\mathbb{R}^3$: Polynomial algorithms*, Dokl. Akad. Nauk. Ukrain. USSR Ser. A 4 (1983), pp. 13–15.
[26] ———, *A formula for finding the number of integer points under a line and an application*, Ekonomika i Mat. Metody, 20 6 (1984), pp. 1132–1138.
[27] ———, *Effective algorithms for the solution of discrete optimization problems*, Znanie, Kiev, USSR, 1984.
[28] ———, *Generalization of the Jacobi–Perron algorithm for determining the number of integer points in polyhedra*, Dokl. Akad. Nauk. Ukrain. USSR Ser. A 10 (1985), pp. 10–13.