SOLUTION OF THE FROBENIUS PROBLEM AND ITS GENERALIZATION

Ravi Kannan[1]

November 27,1989

Abstract This paper considers the "Frobenius problem" : Given n natural numbers $a_1, a_2, \ldots a_n$ such that their greatest common divisor is 1, find the largest natural number that is not expressible as a nonnegative integer combination of them. This problem can be seen to be NP-hard. For the cases $n = 2, 3$ polynomial time algorithms are known to solve it. Here a polynomial time algorithm is given for every fixed n. This is done by first proving an exact relation between the Frobenius problem and a geometric concept called the "covering radius". Then a polynomial time algorithm is developed for finding the covering radius of any polytope in a fixed number of dimensions. The last algorithm relies on a structural theorem proved here that describes for any polytope K, the set $K + \mathbf{Z}^n = \{x : x \in \mathbf{R}^n \ ; \ x = y + z \ ; \ y \in K \ ; \ z \in \mathbf{Z}^n\}$ which is the portion of space covered by all lattice translates of K. The proof of the structural theorem relies on some recent developments in the Geometry of Numbers. In particular, it uses a theorem of Kannan and Lovàsz [10], bounding the width of lattice-point-free convex bodies and the techniques of Kannan, Lovász and Scarf [11] to study the shapes of a polyhedron obtained by translating each facet parallel to itself. The concepts involved are defined from first principles. In the last section, I develop an algorithm which is polynomial time bounded for fixed p, n to decide the truth / falsity of any sentence of the following form (where Q is a given copolyhedron in $\mathbf{R}^p$ and A, B, b are given matrices of suitable dimensions. See Notation below.)

$$\forall y \in Q/\mathbf{Z}^l \quad \exists x \in \mathbf{Z}^n \quad Ax + By \leq b.$$

The sentence says in words : for every y for which an integer vector $z \in \mathbf{Z}^l$ exists such that (y, z) is in Q, there exists also an integer vector x so

[1] Supported by NSF-Grant CCR 8805199

that $Ax + By \leq b$. The Frobenius problem can be easily reduced to such a sentence.

Notation

$\mathbf{R}^n$ is Euclidean n space. The lattice of all integer vectors in $\mathbf{R}^n$ is denoted $\mathbf{Z}^n$. For any two sets $S, T \subseteq \mathbf{R}^n$, we denote by $S + T$ the set $\{s + t : s \in S; t \in T\}$. For any positive real, λ, we denote by λS, the set $\{\lambda s : s \in S\}$. For any set W in $\mathbf{R}^{n+l}$ and any set V in $\mathbf{R}^l$, we denote by W/V the set

$$\{x : x \in \mathbf{R}^n \text{ such that there exists a } y \in V \text{ with } (x, y) \in W\}.$$

W/V is the set obtained by "projecting out" V from W.

A **copolyhedron** is the intersection of a finite number of half spaces - some of them closed and the others open. ("co" for closed / open.) If a copolyhedron is bounded, I will call it a copolytope.

Some statements in the paper will assert "the algorithm *finds* copolytope P_i.......". The precise meaning of this statement is as follows : suppose P_i is in $\mathbf{R}^n$. The algorithm will find a rational $m \times (n+l)$ matrix C and a rational $m \times 1$ vector b where l is at most some polynomial function of n and for each row of C, either the $\leq$ or the $<$ sign such that P_i equals

$$\{x : x \in \mathbf{R}^n \text{ such that there exists a } y \in \mathbf{R}^l \text{ with } C\begin{pmatrix} x \\ y \end{pmatrix} \begin{pmatrix} \leq \\ < \end{pmatrix} b\}.$$

By a "rational polyhedron", we mean a polyhedron that can be described by a system of inequalities that have rational coefficients; the inequalities may have irrational right hand sides.

In much of the paper A will be a fixed $m \times n$ matrix. If the meaning of A is clear from the context, for any b in $\mathbf{R}^m$, the polyhedron $\{x \in \mathbf{R}^n : Ax \leq b\}$ will be denoted by K_b. In much of the paper, b will vary over some copolyhedron in $\mathbf{R}^m$. Some bounds in the paper will be in terms of the affine dimension j_o of this copolyhedron. Except for Theorem (7.2), this generality is not strictly needed. The reader may restrict attention to the case when $j_o = m$ for the first reading. The "size" of a rational matrix is the number of bits needed to express it. It is assumed that integers are written in binary notation, so it takes a $O(\log M)$ length string to express an integer of magnitude M.

A basis B of the lattice $\mathbf{Z}^n$ is a set of n linearly independent vectors $\{b_1, b_2, \ldots b_n\}$ in $\mathbf{Z}^n$, such that each member of $\mathbf{Z}^n$ can be expressed as an integer linear combination of $\{b_1, b_2, \ldots b_n\}$. The "fundamental parallelopied" corresponding to B is the set $\{x : x = \sum_{i=1}^{n} \lambda_i b_i$ where $\lambda_i \in \mathbf{R}$ satisfy $0 \leq \lambda_i < 1\}$. It is denoted $F(B)$. For each point y in $\mathbf{R}^n$, there is a unique lattice point z such that $z + F(B)$ contains y. The parallelopied $z + F(B)$ is denoted $F(B; y)$. It is an elementary fact that the set of integer solutions to a linear system of congruences i.e., a set of the form $\{(x_1, x_2, \ldots x_n) : \sum_{i=1} n a_i x_i \equiv 0 (mod p)\}$ where a_i, p are natural numbers, is a lattice. This fact will be used once only in the paper, in section 2.

In most of the paper, the only lattices that occur are $\mathbf{Z}^r$ for some natural number r. In section 2, we use more general lattices. A lattice in general is the set of all integer linear combinations of a set of linearly independent vectors in Euclidean space.

1 Introduction

The Frobenius problem can be rephrased as follows : "Given n coins of denominations $a_1, a_2, \ldots a_n$, with GCD$(a_1, a_2, \ldots a_n)$ equal to 1, what is the largest integer amount of money for which change cannot be made with these coins ? " Note that the GCD condition implies that we can in fact make change for any large enough integer amount of money. The simple statement of the Frobenius problem makes it attractive. Not surprisingly, the Frobenius problem is NP-hard in general. This is not proved in this paper. For the special case of $n = 2$, the answer is explicitly known - it is $a_1 a_2 - a_1 - a_2$. The proof of this is elementary. (For example, this follows from Theorem 2.1.) Algorithms to solve the Frobenius problem in the case $n = 3$ were recently developed by Rödseth [15], Selmer and Beyer[20] Greenberg[5] and Scarf and Shallcross [17]. There is a substantial literature on the general problem - see for example [6] and the bibliography in [19], [4]. No polynomial time is known for fixed n greater than 3. This paper develops one for any fixed n. It might seem that this result would follow from the result of Lenstra [13] that Integer Programming in a fixed number of variables can be solved in polynomial time ; but note that a näive solution to the Frobenius problem involves solving (in the worst case) an exponential number of Integer Programs - one each to determine for each natural number b whether b can be expressed as a nonnegative integer combination of $a_1, a_2, \ldots a_n$. Some pruning is possible, but no such direct method is known to work. For an approximation algorithm, see [12].

The Frobenius problem is related to the study of maximal lattice point free convex bodies, a topic of long-standing interest in the Geometry of Numbers. This relation is described by Lovász in [14]. He also formulates a conjecture which he proves would imply a polynomial time algorithm for the Frobenius problem for a fixed number of integers. The structural result of this paper does not prove this conjecture, but does imply a closely related one as shown in section 7 . Scarf and Shallcross [17] have recently observed a somewhat direct relation between maximal lattice free convex bodies and the Frobenius problem. There have been some applications of the Frobenius problem to a sorting method called Shell-Sort - see for example Incerpi and Sedgwick [8] and Sedgwick [18].

In section 2, the Frobenius problem for n coins is exactly related to the "covering radius" of a certain simplex in $\mathbf{R}^{n-1}$. The notion of covering radius for centrally symmetric convex sets is a classical notion in the Geometry of Numbers ; in [10], it was introduced and studied for general convex sets. It is defined as follows :

For a closed bounded convex set P of nonzero volume in $\mathbf{R}^n$, and a lattice L of dimension n also in $\mathbf{R}^n$, the least positive real t so that $tP + L$ equals $\mathbf{R}^n$ is called the "covering radius" of P with respect to L. It will be denoted by $\mu(P, L)$.

In words, the covering radius is the least amount t by which we must "blow up" P and one copy of P placed at each lattice point so that all of space is covered.

Suppose K is a closed bounded convex set in $\mathbf{R}^n$ and v is an element of

$\mathbf{R}^n$. The **width of K along v** is

$$\max\{v \cdot x : x \in K\} - \min\{v \cdot x : x \in K\}.$$

The **width of K** (with respect to the lattice $\mathbf{Z}^n$) is defined to be the minimum width of K along any nonzero integer vector. Note that this differs from the usual definition of the geometric width of K, where the minimum is over all vectors v of length 1, rather than all nonzero integer vectors. The width as defined here is greater than or equal to the geometric width since nonzero integer vectors have length at least one. The following theorem will be used.

Flatness Theorem [10] There is a universal constant c_o such that any closed bounded convex set K in $\mathbf{R}^n$ of width at least $c_o n^2$ contains a point of $\mathbf{Z}^n$.

Remark : The constant c_o will be used throughout the paper. By looking at the case $n = 1$, we see that c_o must be at least 1, a fact that we will use.

Kannan, Lovász and Scarf [11] show that for any fixed $m \times n$ matrix A satisfying some nondegeneracy condition, there is a small finite set V of nonzero integer vectors such that for any "right hand side" b, there is some $v(b)$ belonging to V such that the polytope $K_b = \{x : Ax \leq b\}$ has approximately the smallest width along $v(b)$; more precisely, the width of K_b along $v(b)$ is at most twice the width of K_b along any nonzero integer vector. Section 3 of this paper proves from first principles a result in the same spirit. There are two differences - here, I do not assume any nondegeneracy condition. Secondly, in the result here, b is allowed to vary over some subset of $\mathbf{R}^m$ and the upper bound on the cardinality of V is in terms of the dimension of the affine hull of this subset. Letting the subset be the whole of $\mathbf{R}^m$, we can recover a result similar to [11].

The result of section 3 will be used in the main structural theorem proved in section 4 which describes the set $K + \mathbf{Z}^n$ where K is a polyhedron. The proof of this theorem is by induction ; the inductive proof will need a "uniform" description of $K + \mathbf{Z}^n$ as each facet of K is moved parallel to itself in some restricted fashion. In this context, the theorem of section 3 comes in useful.

Section 5 gives a polynomial time algorithm for finding the covering radius of a polytope in a fixed number of dimensions using the theorem of section 4. Thus also, the Frobenius problem is solved for fixed n in the sense of a polynomial time algorithm.

In both sections 3 and 4, the "right hand side" b is allowed to vary only over a bounded set. Section 6 proves the theorem of section 4 without such a restriction.

The result of section 6 is used to produce a "test set" for Integer Programming - see Theorem (7.1). This theorem is then used to design a decision procedure for sentences of the form mentioned in the Abstract - see Theorem (7.2). In particular, the decision procedure decides in polynomial time (for fixed n, p), the truth / falsity of a sentence of the form

$$\forall y \in \mathbf{Z}^p \quad \exists x \in \mathbf{Z}^n \quad : Ax + By \leq b.$$

This is a generalization of Lenstra's result which gives a polynomial time algorithm for deciding sentences of the form

$$\exists x \in \mathbf{Z}^n \quad : Ax \leq b.$$

It is an interesting open problem to devise such algorithms for sentences with a higher number of alternations, in particular for sentences of the form

$$\exists z \in \mathbf{Z}^p \quad \forall y \in \mathbf{Z}^q \quad \exists x \in \mathbf{Z}^n \quad : Ax + By + Cz \leq b.$$

See Remark 4 of section 8.

2 Frobenius problem to Covering Radius

For $a_1, a_2 \ldots, a_n$ positive integers with $GCD(a_1 \ldots, a_n) = 1$, let $Frob(a_1 \ldots, a_n) =$ largest natural number t such that t is not a nonnegative integer combination of $a_1 \ldots, a_n$. The aim of this section is to relate $Frob(a_1, a_2, \ldots a_n)$ to the covering radius of a certain $n-1$ dimensional simplex. This is done in Theorem (2.5).

(2.1) Theorem [2]

$$Frob(a_1 \ldots, a_n) = \max_{l \in \{1,2\ldots,a_n-1\}} t_l - a_n \tag{2.2}$$

where $t_l =$ the smallest positive integer congruent to l modulo a_n, that is expressible as nonnegative integer combination of $a_1 \ldots, a_{n-1}$.

Proof: The proof is rather simple. Let N be any positive integer. If $N \equiv 0 (mod\ a_n)$, then N is a nonnegative integer combination of a_n alone. Otherwise, if $N \equiv l(mod\ a_n)$, then N is a nonnegative integer combination of $a_1 \ldots, a_n$ iff $N \geq t_l$.

∎

Let $$L = \{(x_1 \ldots, x_{n-1}) : x_i \text{ integers and } \sum_{i=1}^{n-1} a_i x_i \equiv 0(mod\ a_n)\} \tag{2.3}$$

and let $$S = \{(x_1, x_2 \ldots, x_{n-1}) : x_i \geq 0 \text{ reals and } \sum_{i=1}^{n-1} a_i x_i \leq 1\} \tag{2.4}$$

(2.5) Theorem $\mu(S, L) = Frob(a_1, a_2 \ldots, a_n) + a_1 + a_2 + \ldots + a_n$ where $\mu(S, L)$ is the covering radius of S with respect to L.

Proof: Abbreviate $Frob(a_1, a_2, \ldots, a_n)$ by F and $\mu(S, L)$ by μ. First, I show $\mu \leq F + a_1 + a_2 \ldots + a_n$. Suppose $y \in \mathbf{Z}^{n-1}$, and $\sum_1^{n-1} a_i y_i \equiv l(mod\ a_n)$. By definition of $t_l, \exists x_1, \ldots, x_{n-1}, x_n \geq 0$ integers such that $\sum_{i=1}^{n-1} a_i x_i = t_l = l + a_n x_n$; thus with $x' = (x_1 \ldots, x_{n-1})$, we have $(y - x') \in L$ and $(y - x') + t_l S$ contains $y - x' + x' = y$. Since this is true of any $y \in \mathbf{Z}^{n-1}$, and $t_l \leq F + a_n$, we have:

$$\mathbf{Z}^{n-1} \subseteq (F + a_n)S + L \tag{2.6}$$

Further it is clear that $\mathbf{R}^{n-1} \subseteq \mathbf{Z}^{n-1} + (a_1 + \ldots + a_{n-1})S$. To see this, note that for $z \in \mathbf{R}^{n-1}$, we have $\lfloor z \rfloor = (\lfloor z_1 \rfloor, \ldots \lfloor z_{n-1} \rfloor) \in \mathbf{Z}^{n-1}$ and $(z - \lfloor z \rfloor) \in (a_1 + a_2 \ldots + a_{n-1})S$. Hence I have shown

$$\mathbf{R}^{n-1} \subseteq \mathbf{Z}^{n-1} + (a_1 + \ldots + a_{n-1})S \subseteq (F + a_1 + \ldots + a_n)S + L \tag{2.7}$$

Now for the converse: Consider $(F + a_n)S + L$. I claim that $F + a_n$ is the smallest positive real t such that $tS + L$ contains $\mathbf{Z}^{n-1}$. Suppose, for some

$t' < F + a_n, \quad t'S + L$ contains $\mathbf{Z}^{n-1}$. Then for any $l \in \{1, \ldots, a_n - 1\}$, pick a $y \in \mathbf{Z}^{n-1}$, such that $\sum_1^{n-1} a_i y_i \equiv l(mod\ a_n)$. y is in $t'S + x$ for some x in L, so $(y - x)$ is in $t'S$. But $\sum_1^{n-1} a_i(y_i - x_i) \equiv l(mod\ a_n)$ and $y_i - x_i \geq 0\forall_i$, implies that $t_l \leq t'$. Since this is true of any l, we have $F \leq t' - a_n < F$ a contradiction (using Theorem (2.1)). Thus I have shown:

$$F + a_n = \min\{t : t > 0, \text{ real and } tS + L \supseteq \mathbf{Z}^{n-1}\} \tag{2.8}$$

By (2.8), we see that $\exists y \in \mathbf{Z}^{n-1}$, such that for any $x \in L$, with $y_i - x_i \geq 0 \forall i$, we have $\sum_{i=1}^{n-1} a_i(y_i - x_i) \geq F + a_n$. Now let ϵ be any real number with $0 < \epsilon < 1$ and consider the point $p = (p_1, p_2, \ldots p_{n-1})$ defined by $p_i = y_i + (1 - \epsilon)\forall i$. Suppose q is any point of L such that $p_i \geq q_i \forall i$. Then q_i are all integers, so we must have $q_i \leq y_i \forall_i$.

So, $\sum_1^{n-1} a_i(p_i - q_i) = (\sum_1^{n-1} a_i)(1 - \epsilon) + \sum_1^{n-1} a_i(y_i - q_i) \geq (1 - \epsilon) \sum_1^{n-1} a_i + (F + a_n)$

by the above.

Since this argument holds for any $\epsilon \in (0 \;\; 1)$, we have $\mu \geq F + \sum_1^n a_i$.

Together with (2.7) now, Theorem (2.5) is proved.

∎

Remark : By applying a suitable linear transformation, we can "send" L to $\mathbf{Z}^{n-1}$. This sends the simplex S to some simplex whose constraint matrix is still rational. It is easy to see that applying the same linear transformation to S and L leaves the covering radius unchanged. I assume this has been done ; in the coming sections, I will deal only with covering radii of sets with respect to the standard lattice of integer points. It is assumed that the reader is familiar with computational aspects of linear algebra; I omit the details of how the linear trnasformation above is applied etc.. For a thorough introduction to such matters, the reader is referred to [21].

3 Vectors along which K_b have small width

Our main aim is to develop an algorithm to find the covering radius of a polytope $K = \{x : Ax \leq b\}$. As will be explained in the beginning of section

4, it will be useful to deal with K_b where b is allowed to vary over some copolytope. This section will develop the tools needed for section 4. For each fixed b, there is an nonzero integer direction that acheives the minimum width of K_b. The main result of this section is lemma 3.1 which says that we can compute a small number of nonzero integer directions such that as b varies over a large set, for each K_b, one of our directions acheives close to minimum width. This is the third point in the conclusion of lemma 3.1, the first two are technical ones that are needed for theorem 4.1.

(3.1) Lemma : Suppose A is an $m \times n$ matrix of integers of size ϕ. For each $b \in \mathbf{R}^m$, we denote by K_b the polyhedron $\{x : Ax \leq b\}$. Let P be a copolytope in $\mathbf{R}^m$ of affine dimension j_o such that for all $b \in P$, K_b is nonempty and bounded. Let M be $\max\{|b| : b \in P\}$. There is an algorithm that finds a partition of P into copolytopes $P_1, P_2, \ldots P_r$ where r is at most $m^{3n+j_o}\left(2\log_2 M + 12n^2\phi)\right)^{n+j_o}$, and for each copolytope P_i, it finds a nonzero integer vector v_i and $n \times m$ matrices T_i, T_i' such that for all i, $1 \leq i \leq r$ and all $b \in P_i$, we have

1. The point $T_i b$ maximizes the linear function $v_i \cdot x$ over x in K_b.

2. The point $T_i' b$ minimizes the linear function $v_i \cdot x$ over x in K_b and

3. $$\text{either} \qquad \text{Width}_{v_i}(K_b) \leq 1$$
$$\text{or } \forall u \neq 0, u \in \mathbf{Z}^n,\ \text{Width}_{v_i}(K_b) \leq 2\text{Width}_u(K_b).$$

Further, the algorithm works in time polynomial in data and $\log M$ if n, j_o are fixed.

Proof I first describe how to find the nonzero integer vectors $v_1, v_2, \ldots$ with which to prove the theorem and then describe how to find the partition of P. The first m of the vectors will be the rows of A. We note that every K_b of zero volume has width 0 along one of these m vectors. Also, if a K_b has width at most 1 along one of these m directions, it is "taken care of" by that direction. So we only need the rest of the vectors to take care of full-dimensional K_b with width at least 1 along each of the m facet directions.

Since K_b is bounded, we have that K_b is contained in a ball of radius $M2^{4n^2\phi}$ [21, Theorem 10.2] around the origin. Also, K_b has a centroid - say - x_o. (The centroid x_o is the unique point such that $\int_{K_b}(x - x_o)dx = 0$.) Consider $K_b - x_o$. Let this be $\{x : Ax \leq b'\}$. Note that b' belongs to $P' = P+($ column space of A) which is a set of affine dimension at most $n + j_o$. By the above, $0 < b'_i \leq M2^{5n^2\phi}\forall i$. By a property of the centroid (namely, if y_o is the centroid of a bounded convex set K in $\mathbf{R}^n$, then for any $z \in K$, we have $(1 + \frac{1}{n})y_o - \frac{1}{n}z \in K$.) , and the lower bound of 1 on the width of K_b in any of the facet directions, we have that

$$\frac{1}{(n+1)} \leq b'_i \leq M2^{5n^2\phi}\forall i.$$

Let $R \subseteq \mathbf{R}^m$ be the rectangular solid $\{y : \frac{1}{(n+1)} \leq y_i \leq M2^{5n^2\phi}\forall i\}$. Applying lemma (3.3) with $Q =$ the affine hull of P' , we get a finite set V' in $\mathbf{R}^m$ such that for each $y \in R \cap P'$, there is a $y' \in V'$ with $y' \leq y \leq 2y'$. (Note that by that lemma, the set V' can be found in polynomial time when n, j_o are fixed.) For each y' in V' such that $K_{y'}$ is full dimensional, we find the nonzero integer vector that attains the width of $K_{y'}$. This set of nonzero integer vectors suffices as our set of v_i 's. This is so because $y' \leq y \leq 2y'$ implies that $K_{y'} \subseteq K_y \subseteq K_{2y'}$ which implies that for any nonzero vector v, $\text{Width}_v(K_{y'}) \leq \text{Width}_v(K_y) \leq \text{Width}_v(K_{2y'})$. (The nonzero integer vector along which the width of a polyhedron is minimised, can be found in polynomial time for a fixed number of dimensions - see [10 (1986) version].)

We now have a set of vectors $v_1, v_2, \ldots$ such that each of the relevant K_b has "small" width ("Small" will mean either at most 1 or at most twice the minimum width along any nonzero integer direction.) along one of these vectors. For each v_i, we perturb it slightly to get a v'_i with the property that (i) for any $b \in P$, a vertex of K_b achieves the maximum (minimum) of the linear function $v'_i \cdot x$ over K_b iff it achieves the maximum (respectively minimum) of $v_i \cdot x$ over K_b ; and (ii) for each b in P, there is a unique vertex of K_b that achieves the maximum and a unique vertex that achieves the minimum of $v'_i \cdot x$ over K_b. This is possible with an increase in size by at most a polynomial additive term. (For example, see [21].) Consider each of the (at most m^n) nonsingular $n \times n$ submatrices B of A. For each of these we can define an $n \times m$ matrix T by augmenting B^{-1} with 0 columns so that the possible corners of any K_b are of the form Tb for such T. I will denote by $f(T)$ the ordered subset of $\{1, 2, \ldots m\}$ of cardinality n that contains the indices of the rows of A that go into B. Let $f(T) = \{f_1(T), f_2(T), \ldots f_n(T)\}$. We let $f_0(T)$ be zero for all T. If there is degeneracy, it may happen that a vertex v of some K_b equals Tb for more than one T. In that case, we will say that T is the lexicographically least one defining the vertex v if the set $f(T)$ is lexicographically least among all "basis" sets that define v. This can be expressed more precisely as follows : let $g(T)$ be the set of l such that for s with $f_s(T) < l < f_{s+1}(T)$, we have that row l of A is independent of rows $f_1(T), f_2(T), \ldots f_s(T)$ of A. Then, we say that $v = Tb$ satisfies $Av \leq b$ and for each l in $g(T)$, we have the l th component of Av is strictly less than b_l.

We order the T 's and call them $T_1, T_2, \ldots$. There will be one copolytope $P(T_i, T_j, v_k)$ for each triple i, j, k in the partition of P. The copolytope $P(T_i, T_j, v_k)$ will be the set of all b 's in P for which

- $p = T_i b$ and $q = T_j b$ belong to K_b. Further, T_i is the lexicographically least one that defines p and the same for T_j and q.

- The maximum value of $v_k' \cdot x$ over K_b is attained at $T_i b$.

- The minimum value of $v_k' \cdot x$ over K_b is attained at $T_j b$.

- For each $l < k$, there exist $x^{(l)}, y^{(l)}$ in K_b, such that $v_l \cdot (x^{(l)} - y^{(l)}) > v_k \cdot (T_i b - T_j b)$.

- For each $l > k$, there exist $x^{(l)}, y^{(l)}$ in K_b, such that $v_l \cdot (x^{(l)} - y^{(l)}) \geq v_k \cdot (T_i b - T_j b)$. (This and the previous condition say that the width of K_b along v_k is the least among all the directions $\{v_l\}$. The strict inequality in the previous condition is there to ensure that each b belongs to only one $P(T_i, T_j, v_k)$.

(3.2) Claim Each $P(T_i, T_j, v_k)$ defined above is a copolytope. The copolytopes form a partition of P. For each $b \in P(T_i, T_j, v_k)$, we have that

K_b has small width (at most 1 or at most twice the minimum in any integer direction) along v_k and further $T_i b$ maximizes $v_k \cdot x$ over K_b and $T_j b$ minimizes $v_k \cdot x$ over K_b.

Proof To prove the first statement, I will show that each of the above conditions in the definition of $P(T_i, T_j, v_k)$ can be expressed by linear constraints possibly with the introduction of new variables. Only the second and third condition need any explanation at all. The second condition is expressed by complementary slackness of linear programming - namely, we say that the complementary solution is feasible to the dual, i.e., that $v_k B_i^{-1} \geq 0$ where B_i is the $n \times n$ basis matrix corresponding to T_i. Note that in fact, this statement does not involve b, so it need not be included as a constraint, if it is not satisfied, then the $P(T_i, *, v_k)$ is empty for all $* = T_j$, so these pieces need not be included in the partition of P. Condition 3 is treated similarly.

The statement in the claim that the copolytopes form a partition of P is easy to see : if b belongs to $P(T_i, T_j, v_k)$, then the width of K_b along v_k is less than its width along $v_1, v_2, \ldots v_{k-1}$ and at most its width along $v_{k+1}, \ldots$, so v_k is uniquely determined by b. Then clearly, by the perturbation, T_i and T_j are uniquely determined.

The rest of the claim is easy to see.

∎

Now for the lemma : we may return the partition $\{P(T_i, T_j, v_k)\}$ of P, and associated with $P(T_i, T_j, v_k)$, the vector v_k and the matrices T_i, T_j to satisfy the lemma. The upper bound on r, the number of elements in the partition is easily obtained.

∎

(3.3) Lemma Let $R \subseteq \mathbf{R}^m$ be the rectangle $\{y : \alpha \leq y_i \leq \beta \forall i\}$ where $0 < \alpha \leq \beta$ are arbitrary rationals. Let Q be any affine subspace of $\mathbf{R}^m$ with dimension say t. Then there exist a finite set V' in $\mathbf{R}^m$ with $|V'| \leq \left(2m(\log_2 \frac{\beta}{\alpha} + 1)\right)^t$ such that for each $y \in R \cap Q$, there is a $y' \in V'$ with $y' \leq y \leq 2y'$.

Further, given R, Q, the set V' can be found in polynomial time provided n, t are fixed.

Proof : Divide R into sub-rectangles each of the form

$$\{z : \alpha 2^{p_i} \leq z_i \leq \alpha 2^{p_i+1} \text{ for } i = 1, 2 \ldots, m\}$$

where $p_1, p_2 \ldots, p_m$ are natural numbers between 0 and $l = \log_2(\beta/\alpha)$. I will show by induction on the pair t, m that $Q \cap R$ is contained in the union of some

$$2^t m^t (l+1)^t$$

subrectangles of R which clearly proves the lemma.

The case $t = 0$ is clear for all m. The case $m = 0$ is trivial. For higher t, note that if Q intersects a subrectangle, it intersects the boundary of the subrectangle. For any $i, 1 \leq i \leq m$ and any $p_i, 0 \leq p_i \leq l$, consider the $(m-1)$-dimensional rectangle $R' = R \cap \{z : z_i = 2^{p_i}\alpha\}$ and the division of it into subrectangles "induced" by the division of R. Also, let $Q \cap \{z : z_i = 2^{p_i}\alpha\}$ be Q'. If for any i and any p_i, such a Q' equals Q, we have the lemma by induction on m. So assume this is not the case. Then, Q' is a $(t-1)$-dimensional affine space. Applying the inductive assumption, we know that there are $(2(m-1)(l+1))^{t-1}$ subrectangles whose union contains $Q' \cap R'$. Each such subrectangle is a facet of 2 subrectangles of R. Thus there are $2.(2(m-1)(l+1))^{t-1}\ m\ (l+1)$ subrectangles of R whose union contains $Q \cap R$.

To get the required algorithm, note that in the case where some Q' equals Q, we get one "problem of size " $t, m-1$ and in the other case, we get $m(l+1)$ problems each of "size" $t-1, m-1$.

∎

(3.4) Lemma : Suppose K is a rational polyhedron in $\mathbf{R}^n$ and $v \in \mathbf{Z}^n \setminus \{0\}$ satisfies

$$\text{either } \ \text{Width}_v(K) \leq 1$$

$$\text{or } \forall u \neq 0, u \in \mathbf{Z}^n, \ \text{Width}_v(K) \leq 2\text{Width}_u(K).$$

Suppose also that y is in K and $v \cdot y = \alpha$. For $\beta \in \mathbf{R}$, denote by $H(\beta)$ the set $\{x \in \mathbf{R}^n : v \cdot x = \beta\}$. Let $s = 2c_o n^2 + 1$ (where c_o is the constant from the Flatness theorem of section 1). Then for all $\gamma \in (\alpha \ \ \alpha + 1]$, we have

$$(K + \mathbf{Z}^n) \cap H(\gamma) = \left[K + \left(\bigcup_{k=-s}^{s} (\mathbf{Z}^n \cap H(k)) \right) \right] \quad \cap \quad H(\gamma).$$

Proof : It is easy to see that we may assume that $y = 0$ and $\alpha = 0$ since both sides in the above equation are unchanged by translations of K (provided of course, $H(\gamma)$ is also suitably translated). Now suppose x belongs to $H(\gamma)$ for some $\gamma \in (0 \ \ 1]$ and x belongs to $K + \mathbf{Z}^n$. So $x - K$ intersects $\mathbf{Z}^n$, hence there exists a real number $t \in [0 \ \ 1]$ such that $x - tK$ intersects $\mathbf{Z}^n$, but the interior of $x - tK$ does not. (This uses the fact that K is closed and $0 \in K$.) Then the width of tK along some nonzero integer vector must be at most $c_o n^2$ by the Flatness Theorem from which it follows that the width of tK along v must be at most $2c_o n^2$. Then if z is in $(x - tK) \cap \mathbf{Z}^n$, we have $|v \cdot (z - x)| \leq 2c_o n^2$, thus we have $|v \cdot z| \leq s$ which implies that x belongs to

$$\left[K + \left(\bigcup_{k=-s}^{s} (\mathbf{Z}^n \cap H(k)) \right) \right]$$

proving the lemma.

▮

4 The structure of $K_b + \mathbf{Z}^n$ as b varies over a bounded set

In this section, the main structural theorem is stated and proved. The idea of the theorem is to describe the set $K + \mathbf{Z}^n$ where K is a polyhedron . We assume K is described by m linear inequalities $Ax \leq b$ where A is an $m \times n$ matrix and b an $m \times 1$ vector. If it happens that K is contained in the fundamental parallelopiped $F(B)$ corresponding to some basis B of $L = \mathbf{Z}^n$, then clearly, $K + L = (K \cap F(B)) + L$. This of course is not true in general.

In spirit, the theorem below states that in general, it is enough to look at the portion of $K + L$ (where $L = \mathbf{Z}^n$), contained in some parallelopipeds which are lattice translates of the fundamental parallelopiped corresponding to some bases (note the plural) of L. Further, we need to consider only a "small" number of lattice translates. The number of bases of L as well as the number of lattice translates is bounded above by a function of n alone. The proof of the theorem will be by induction; in the body of the inductive proof, we will look at sets of the form $K' + L'$ where K' is the intersection of K with some lattice hyperplane and L' the intersection of L with the subspace parallel to the hyperplane. We will need to derive a "uniform" description of these sets as the hyperplane is translated parallel to itself. The sections then can be all described as $\{y : A'y \leq b'\}$ where the b' varies as an affine function of b and the position of the hyperplane. To facilitate such an inductive proof, we will consider a more general setting than $K + L$, namely $K_b + L$ where $K_b = \{x : Ax \leq b\}$ and now, we let b vary over a copolytope P in $\mathbf{R}^m$. The theorem will say that for fixed n and the affine dimension of P, we can partition P into a polynomial number of copolytopes such that in each part, there is an uniform description of $K_b + L$.

(4.1) Theorem Let A be an $m \times n$ matrix of integers of size ϕ. Let P be a copolytope in $\mathbf{R}^m$ of affine dimension j_o such that for all $b \in P$, the set $K_b = \{x : Ax \leq b\}$ is nonempty and bounded. Let $M = (\max_{b \in P}(|b| + 1))$. There is an algorithm which for any fixed n, j_o runs in time polynomial in $\phi, \log M$ and finds a partition of $P \times \mathbf{R}^n$ into subsets $S_1, S_2, \ldots S_r$ such that

1. $r \leq (n\phi m \log M)^{j_o n^{dn}}$, where d is a constant independent of n, m, M, ϕ.
2. Each S_i is of the form $S'_i/\mathbf{Z}^l$ where S'_i is a copolyhedron in $\mathbf{R}^{m+n+l}$ and $l \leq (3c_o n)^{3n}$.
3. Letting $S_i(b) = \{x \in \mathbf{R}^n : (b, x) \in S_i\}$, we have for all i and all $b \in P$, $S_i(b) + \mathbf{Z}^n = S_i(b)$.

The algorithm also finds corresponding to each S_i, a collection $\mathcal{B}_i$ of at most $(3c_o n)^{3n}$ bases of $\mathbf{Z}^n$. Corresponding to each basis B in each $\mathcal{B}_i$, it finds an affine transformation $T(B) : \mathbf{R}^m \to \mathbf{R}^n$ and a set $Z(B)$ of at most n^n points of $\mathbf{Z}^n$ such that for all i and all $b \in P$, we have

$$(K_b + \mathbf{Z}^n) \cap S_i(b) =$$
$$\left[\left\{ \bigcup_{B \in \mathcal{B}_i} ((K_b + Z(B)) \cap F(B; T(B)b)) \right\} + \mathbf{Z}^n \right] \cap S_i(b).$$

/*END OF STATEMENT OF THE THEOREM*/

Remark Reminder on some notation : $F(B; y)$ is the lattice translate of the fundamental parallelopiped $F(B)$ corresponding to the basis B, that contains the point y.

Proof : The proof is by induction on n. First, I do the case $n = 1$. Here each row of A can be assumed to be ± 1 ; say the first k rows are $+1$ and the rest -1. We will have $S_1, S_2, \ldots S_k \subseteq P \times \mathbf{R}^1$ defined by

$$S_i = \{(b, x) : b \in P; b_i < b_1, b_i < b_2, \ldots b_i < b_{i-1}, b_i \leq b_{i+1}, b_i \leq b_{i+2} \ldots b_i \leq b_k\}.$$

In words, S_i consists of all (b, x) for which i is the minimum j such that $b_j = \min\{b_l : l = 1, 2, \ldots k\}$. For $(b, x) \in S_i$, we have $b_i \in K_b$. Let $\mathcal{B}_i = \{\{1\}\}$ for all i and let $T(B)$ be the affine transformation defined by $T(B)b = b_i$ for the single basis B in $\mathcal{B}_i$. Finally, let $Z(B) = \{0, -1\}$ for all B. It is easy to check that the theorem is valid with these quantities; this completes the proof for $n = 1$.

It is useful to remark that the role of $T(B)$ is to “get a hold of a point” $T(B)b$ that is guaranteed to be in K_b. We then know that we have all the information needed regarding $K_b + \mathbf{Z}$ by just looking at the intersection of K_b with the parallelopiped containing that point and a neighbouring parallelopiped.

Now we go to general n. First, we may restrict attention to each of the copolytopes that lemma (3.1) partitions P into in turn. So without loss of generality, assume that we know a linear transformations T, T' and a nonzero integer vector v such that for all $b \in P$, we have K_b has “small” width (i.e., width of at most 1 or a width at most twice the minimum width along a nonzero integer direction) along v and Tb minimizes $v \cdot x$ over x in K_b and $T'b$ maximizes $v \cdot x$ over x in K_b.

After a suitable unimodular transformation, we may assume that v is the first unit vector e_1.

Let now $e_1 \cdot Tb = \alpha$. For any real number γ, let $H(\gamma) = \{x \in \mathbf{R}^n : e_1 \cdot x = \gamma\}$. Let $L = \mathbf{Z}^n$.

The idea now will be to obtain an expression for $(K_b + L) \cap H(\gamma)$ as γ varies over $(\alpha \quad \alpha + 1]$. The inductive assumption will enable us to get an expression for each such section and then we will put the sections together.

For any $\beta \in \mathbf{R}$, let $Q(b, \beta) = K_b \cap H(\beta)$. We can find an integer $m \times (n-1)$ matrix C, an $m \times m$ affine transformation D and an $m-$ vector d such that

$$\forall b, \beta \quad Q(b, \beta) = \{(\beta, \hat{x}) : \hat{x} \in \mathbf{R}^{n-1} \text{ satisfies } C\hat{x} \le Db + \beta d\}.$$

Let $\hat{Q}(b, \beta) = \{\hat{x} \in \mathbf{R}^{n-1} : C\hat{x} \le Db + \beta d\}$.

For $\gamma \in (\alpha \quad \alpha + 1]$, we have by lemma (3.4), (with $s = 2c_o n^2 + 1$)

$$\begin{aligned} &(K_b + L) \cap H(\gamma) = \\ &\Big(K_b + \cup_{k=-s}^{s} (L \cap H(k))\Big) \cap H(\gamma) = \\ &\cup_{k=-s}^{s} \{(K_b \cap H(\gamma - k)) + (L \cap H(k))\} = \\ &\cup_{k=-s}^{s} ((Q(b, \gamma - k) + L') + ke_1) \end{aligned} \tag{4.2}$$

where $L' = L \cap H(0) = 0 \times \mathbf{Z}^{n-1}$. As stated earlier, γ will vary over the range $(\alpha \quad \alpha + 1]$, so $\beta = \gamma - k$ will vary over the range $(\alpha - s \quad \alpha + s + 1]$. Let $I(b) = \{\beta \in (\alpha - s \quad \alpha + s + 1] : Q(b, \beta) \ne \emptyset\}$ which is equal to $(\alpha - s \quad \alpha + s + 1] \cap [Tb \quad T'b]$. Let $b' = Db + \beta d$. As b varies over P, and β varies over $I(b)$, b' varies over some copolytope P' of affine dimension at most $j_o + 1$. Further, clearly, we can obtain a natural number ν' so that it is bounded in size by a polynomial in the size of A and $\log(\max_{b \in P}(|b| + 1))$ and P' is contained in a ball of radius ν' about the origin in $\mathbf{R}^m$. Also, for all $b' \in P'$, we have $\hat{Q}(b') = \{\hat{x} : C\hat{x} \le b'\}$ is nonempty and bounded.

Applying the inductive assumption on $\hat{Q}(b') + \mathbf{Z}^{n-1}$ will give us a partition of $P' \times \mathbf{R}^{n-1}$; clearly, we may substitute $b' = Db + \beta d$ to make this a partition of $P_0 \times \mathbf{R}^{n-1}$ where $P_0 = \{(b, \beta) : b \in P; \beta \in I(b)\}$. So by induction, we get

(4.3) a partition of $P_0 \times \mathbf{R}^{n-1}$ into subsets $R_1, R_2, \dots R_t$ such that

1. each R_i is of the form $R_i'/\mathbf{Z}^l$ where R_i' is a copolyhedron in $\mathbf{R}^{m+n+l}$ and $l \leq (3c_o(n-1))^{3(n-1)}$ and for all $(b, \beta) \in P_0$,

2. $R_i(b, \beta) + \mathbf{Z}^{n-1} = R_i(b, \beta)$. (Reminder on notation : $R_i(b, \beta) = \{x \in \mathbf{R}^{n-1} : (b, \beta, x) \in R_i\}$.)

For technical convenience, we let $R_0 = \{(b, \beta, x) : T'b < \beta \leq \alpha + s + 1; b \in P\}$ and $R_{t+1} = \{(b, \beta, x) : \alpha - s < \beta < Tb; b \in P\}$. Now $R_0, R_1, \dots R_{t+1}$ form a partition of $P \times (\alpha - s \;\; \alpha + s + 1]$.

We also get corresponding to each subset R_i, for $1 \leq i \leq t$ a collection $\mathcal{B}_i$ of bases of $\mathbf{Z}^{n-1}$ containing at most $(3c_o(n-1))^{3(n-1)}$ bases, and corresponding to each basis B, an affine transformation $T(B)$ and a set $Z(B)$ of points in $\mathbf{Z}^{n-1}$ so that for all $i = 1, 2, \dots t$ and all $(b, \beta) \in P_0$, we have

$$\left(\hat{Q}(b, \beta) + \mathbf{Z}^{n-1}\right) \cap (R_i(b, \beta)) =$$

$$\left\{ \bigcup_{B \in \mathcal{B}_i} \left[(\hat{Q}(b, \beta) + Z(B)) \cap F(B; T(B) \begin{pmatrix} b \\ \beta \end{pmatrix}) \right] + \mathbf{Z}^{n-1} \right\} \cap R_i(b, \beta) \qquad (4.4)$$

We let $\mathcal{B}_0 = \mathcal{B}_{t+1} = \emptyset$. Since, $\hat{Q}(b, \beta) = \emptyset$ for $\beta \notin [Tb \;\; T'b]$, (4.4) is now valid for all (b, β) in $P \times (\alpha - s \;\; \alpha + s + 1]$.

The subsets of $P \times \mathbf{R}^n$ with which I prove the theorem are obtained as follows : Let $J = \langle i_{-s}, i_{-s+1}, \dots i_0, \dots i_s \rangle$ be any $(2s+1)$ - tuple of integers each in the range $[0 \;\; t+1]$. There will be one subset S_J in the partition of $P \times \mathbf{R}^n$ for each such J. It is defined as the set of $(b, \beta, x) : b \in P, \beta \in \mathbf{R}, x \in \mathbf{R}^{n-1}$ such that

$$\exists z \in \mathbf{Z} : \beta + z \in (\alpha \;\; \alpha + 1], \quad (b, \beta + z - k, x) \in R_{i_k} \text{ for } k = -s, -s+1, \dots s \qquad (4.5)$$

Note here that b "comes from" P and (β, x) "come from" $\mathbf{R}^n$. It is obvious that the sets S_J are of the form $S_J'/\mathbf{Z}^l$ where the S_J' is a copolyhedron and l is not too high. (In fact, $l \leq 1 + (2s+1)(3c_o(n-1))^{3(n-1)} \leq (3c_on)^{3n}$.) To show for any b, the intersection of $S_J(b)$ and $S_{J'}(b)$ is empty for $J \neq J'$, we proceed as follows : J and J' must differ in one of their "coordinates", say, in the k th coordinate J has j and J' has j' with $j \neq j'$. For any $b \in P$, and

$\beta \in (\alpha - s \quad \alpha + s + 1]$, we have that $R_j(b, \beta)$ and $R_{j'}(b, \beta)$ do not intersect, from this it follows that $S_J(b)$ and $S_{J'}(b)$ do not intersect.

The other two properties required of the collection $\{S_J\}$ - that their union is $P \times \mathbf{R}^n$ for any fixed b and they are invariant under $\mathbf{Z}^n$ also follow easily.

The bound on the number of S_J given by item 1 is argued by induction on n as follows : It is obvious for $n = 1$. For other n, by lemma (3.1), the partition of P incurs us a factor of at most $(mn \log M\phi)^{c(n+j_o)}$ for some constant c. Then we may apply the inductive assumption for t, the number of pieces into which $P' \times \mathbf{R}^{n-1}$ is partitioned. The ϕ and $\log M$ passed on to this problem are easily checked to be at most $n^{c'}$ times the original ϕ and $\log M$ and of course the $n + j_o$ passed on is the same as before, since n is decreased by 1 and j_o increased by 1. Further, the number of J is at most $(t+2)^{2s+1}$. So we get, by induction, the number of J is at most $(mn \log M\phi)^{j_o n^{dn}}$ for a suitable choice of d.

We must now associate a certain set of bases of $\mathbf{Z}^n$ with each S_J. I do this after giving an idea of what the set must be. For each J, say $J = \langle i_{-s}, i_{-s+1}, \ldots i_0, \ldots i_s \rangle$, and for $\gamma \in (\alpha \quad \alpha + 1]$, we get using (4.2),

$$((K_b + L) \cap H(\gamma)) \cap S_J(b) =$$

$$\gamma \times \left[\bigcup_{k=-s}^{s} \left(\hat{Q}(b, \gamma - k) + \mathbf{Z}^{n-1} \right) \right] \quad \cap \quad S_J(b) \tag{4.6}$$

$$\subseteq \bigcup_{k=-s}^{s} \gamma \times \left\{ \left(\hat{Q}(b, \gamma - k) + \mathbf{Z}^{n-1} \right) \cap R_{i_k}(b, \gamma - k) \right\}$$

where the last containment comes from the fact that for γ in the range $(\alpha \quad \alpha + 1]$, if $(b, \gamma, \hat{x})$ belongs to S_J, then $(b, \gamma - k, \hat{x})$ belongs to R_{i_k}. Now, by (4.4), we get,

$$\left(\hat{Q}(b, \gamma - k) + \mathbf{Z}^{n-1} \right) \quad \cap \quad R_{i_k}(b, \gamma - k) = \tag{4.7}$$

$$\left\{ \mathbf{Z}^{n-1} + \left\{ \bigcup_{B \in \mathcal{B}_{i_k}} \left[\left(\hat{Q}(b, \gamma - k) + Z(B) \right) \cap F(B; T(B) \begin{pmatrix} b \\ \gamma - k \end{pmatrix}) \right] \right\} \right\} \quad \cap \quad R_{i_k}(b, \gamma - k).$$

We can write $T(B)\binom{b}{\beta}$ as $T_0'b + w'\beta$ where T_0' is an affine transformation and w' is an $(n-1) \times 1$ vector. Let T_0 be the $n \times m$ matrix with 0 's in the first row and T_0' in the other rows ; let w be the n vector $\binom{0}{w'}$. Let $z \in \mathbf{Z}^{n-1}$ be such that

$$w' \in F(B) + z.$$

We "complete " B to a basis B' of L as follows : if $B = \{b_1, b_2, \dots b_{n-1}\}$, then we let $B' = \{(0, b_1), (0, b_2), \dots (0, b_{n-1}), (1, z)\}$.

To define $T(B')$, we proceed as follows : let $B \in \mathcal{B}_{i_k}$. Let $y = T(B)\binom{b}{\gamma-k} = T_0'b + w'(\gamma - k)$. Let $y' = (0, y)$ and let $y_o = (\gamma - k)e_1 + y'$. Then as γ varies over $(\alpha \quad \alpha+1]$, $\quad y_o$ varies on the straight line segment p from $T_0 b + (\alpha - k)(e_1 + w) = z_o$, say, to $z_o + e_1 + w$. We can express z_o as Ub where U is an affine transformation. Then it is easy to see that $p \subseteq F(B'; Ub) + C$, for a set C of at most n corners of $F(B')$. So we get, for γ in $(\alpha \quad \alpha+1]$,

$$\left[0 \times F(B; T(B)\begin{pmatrix} b \\ \gamma - k \end{pmatrix})\right] + (\gamma - k)e_1 \subseteq C + F(B'; Ub) \qquad (4.8)$$

We will let $U = T(B')$ be the affine transformation corresponding to B'. We let $Z(B') = (0 \times Z(B)) - C$. So, we have $|Z(B')| \leq n|Z(B)| \leq n^n$ using the inductive assumption. The collection $\mathcal{B}_J$ of bases of L corresponding to S_J is defined as the set of B' defined as above - one for each B in each R_{i_k} for $k = -s, -s+1, \dots 0, \dots s$.

Now, for γ belonging to $(\alpha \quad \alpha+1]$, we have

$$(\gamma - k) \times \left[\left(\hat{Q}(b, \gamma - k) + Z(B)\right) \cap F\left(B; T(B)\begin{pmatrix} b \\ \gamma - k \end{pmatrix}\right)\right]$$
$$\subseteq [(K_b + Z(B')) \cap F(B'; Ub)] + C \qquad (4.9)$$

By substituting this into (4.7), we get

$$(\gamma - k) \times \left(\hat{Q}(b, \gamma - k) + \mathbf{Z}^{n-1}\right) \quad \cap \quad (\gamma - k) \times R_{i_k}(b, \gamma - k)$$
$$\subseteq \bigcup_{B \in \mathcal{B}_{i_k}} [(K_b + Z(B')) \cap F(B'; Ub)] + \mathbf{Z}^n.$$

Substituting this into (4.6), we get

$$((K_b + L) \cap H(\gamma)) \cap S_J(b) \subseteq$$

$$\bigcup_{k=-s}^{s} ke_1 + \bigcup_{B \in \mathcal{B}_{i_k}} [(K_b + Z(B')) \cap F(B'; Ub)] + \mathbf{Z}^n \qquad (4.10).$$

Since $ke_1 + \mathbf{Z}^n = \mathbf{Z}^n$ and the right hand side of (4.10) is invariant under adding $\mathbf{Z}^n$, we have

$$(K_b + \mathbf{Z}^n) \quad \cap \quad S_J(b) =$$

$$\bigcup_{B' \in \mathcal{B}_J} [(K_b + Z(B')) \cap F(B'; Ub)] + \mathbf{Z}^n \quad \cap \quad S_J(b).$$

This completes the proof of the theorem.

$\blacksquare$

5 Algorithm to find the covering radius

(5.1) Proposition : There is a polynomial $p(\cdot)$ such that for any rational polytope Q of nonzero volume and rational lattice L, with total size N, $\mu = \mu(Q, L)$ is a rational number of size at most $p(N)$.

Proof : We have $\mu \leq c_o n^2/\lambda_1^*$ [10] . But λ_1^* is equal to the dot product of an integer vector with the difference of two vertices of Q, so we have $\lambda_1^* \geq 1/M$ where M is an integer with number of bits bounded above by some polynomial in N. Thus $\mu \leq c_o n^2 M$. The diameter of Q (the maximum Euclidean distance between two points in Q) is bounded above by an integer with number of bits bounded above by some polynomial in N. From these two facts, we can derive an integer D with polynomial number of bits such that the Euclidean distance between any two points in μQ is at most D. Since μ is invariant under translations, we can translate Q so that 0 belongs to the interior of Q. Let $Q = \{x : a^{(i)}x \leq b_i; i = 1, 2, \ldots m\}$ where b_i are all now strictly positive.

In what follows, we say that a point x in space is "covered" by a lattice point z if $x \in z + \mu Q$. Let R be the fundamental parallelopiped of L corresponding to some basis of L. Let T be the set of all points of L at distance at most D from R. Then, each point of R is covered by a point of T. There is a "last" point x_0 in R that is covered and thus for each $l \in T$, we have that x_0 does not lie in the interior of $l + \mu Q$, i.e., there exists an integer $i(l), 1 \leq i(l) \leq m$, such that $a^{(i(l))}(x_0 - l) \geq \mu b_{i(l)}$. Thus, there is a function $i : T \rightarrow 1, 2, \ldots m$ such that we have that μ is the maximum value of the following linear program : (using the fact that $b_j > 0 \forall j$)

$$\max t : x \in R \quad ; \quad \frac{a^{i(l)}}{b_{i(l)}}(x - l) \geq t \forall l \in T$$

The maximum value must be attained at a basic feasible solution of this linear program whose coefficients are rationals whose sizes are polynomially bounded in N and thus the proposition follows.

∎

Given a rational polyhedron $K_b = \{x : Ax \leq b\}$ in $\mathbf{R}^n$, we wish to compute its covering radius. Since this is a fraction with numerator and denominator polynomially bounded in size, we can do this by binary search provided for any rational t, we can check whether $tK_b + \mathbf{Z}^n$ equals $\mathbf{R}^n$. Without loss of generality, we may assume that $t = 1$. We appeal to the theorem of the last section to find the $S_i, \mathcal{B}_i$ etc. where P is assumed to be the singleton $\{b\}$. Then we check in turn for each S_i whether there exists an $x \in S_i(b)$ so that $x \notin K + \mathbf{Z}^n$. We will formulate the last as several mixed integer programs each with polynomially many constraints and a fixed number of integer variables (for fixed n). For each B in $\mathcal{B}_i$, and for each $z \in Z(B)$, we wish to assert that the unique lattice translate $x(B)$ of x that falls in the parallelopiped $F(B; T(B)b)$ is not in $K_b + z$. To express this by linear constraints, we consider all mappings f of the following sort : f takes two arguments - a B in $\mathcal{B}_i$ and a z in $Z(B)$. The range of f is $\{1, 2, \ldots m\}$. We will consider each possible such mapping f and for each solve a mixed integer program that asserts that there exists an x in $S_i(b)$ such that for each $B \in \mathcal{B}_i$ and for each $z \in Z(B)$, there is a $y(B)$ in $\mathbf{Z}^n$ such that $x + y(B)$ belongs to $F(B; T(B)b)$ and $x + y(B) - z$ violates the $f(B, z)$ th constraint among the m constraints $Ax \leq b$. If any of the MIP's is feasible , then we know that

$K_b + \mathbf{Z}^n \neq \mathbf{R}^n$, otherwise $K_b + \mathbf{Z}^n = \mathbf{R}^n$. We use the algorithm from [9] to solve each MIP in polynomial time.

Here, $j_o = 1$ and $M = |b|$. So the number of S_i 's is at most $(n\phi m \log|b|)^{n^{dn}}$ by 1. of Theorem (4.1). The number of f 's is at most $m^{(cn)^{4n}}$ again from Theorem (4.1). The number of integer variables in each MIP is at most $(O(n))^{4n}$. So the total running time of the algorithm for checking if $K + \mathbf{Z}^n = \mathbf{R}^n$ is

$$(n\phi m|b|)^{n^{en}}$$

for some constant e. A similar bound with a different constant obviously applies to the algorithm for finding the covering radius and solving the Frobenius problem.

This concludes the description of the algorithm to find the covering radius of a polytope in a fixed number of dimensions.

6 The case of unbounded right hand sides

This section proves Theorem (6.1) which extends Theorem (4.1) to the case when P is a copolyhedron. In this case, the parameter ϕ, the size of the matrix A will essentially substitute $\log(\max_{b\in P})|b|$. Here is a precise statement of the theorem.

(6.1) Theorem Let A be an $m \times n$ matrix of integers of size ϕ. Let P be a copolyhedron in $\mathbf{R}^m$ of affine dimension j_o such that for all $b \in P$, the set $K_b = \{x : Ax \leq b\}$ is nonempty and bounded. There is an algorithm which for any fixed n, j_o runs in time polynomial in the size of the input and finds subsets a partition of $P \times \mathbf{R}^n$ into subsets $R_1, R_2, \ldots R_r$ such that

1. $r \leq (n\phi m)^{j_o n^{en}}$ where e is a constant.
2. Each R_i is of the form $R'_i/\mathbf{Z}^l$ where R'_i is a copolyhedron in $\mathbf{R}^{m+n+l}$ and $l \leq n^{O(n)}$.
3. Letting $R_i(b) = \{x \in \mathbf{R}^n : (b, x) \in R_i\}$, we have for all i and all $b \in P$, $R_i(b) + \mathbf{Z}^n = R_i(b)$.

The algorithm also finds corresponding to each R_i, a collection $\mathcal{B}_i$ of at most $n^{O(n)}$ bases of $\mathbf{Z}^n$. Corresponding to each basis B in each $\mathcal{B}_i$, it finds an affine transformation $T(B) : \mathbf{R}^m \rightarrow \mathbf{R}^n$ and a set $Z(B)$ of at most n^n points of $\mathbf{Z}^n$ such that for all i and all $b \in P$, we have

$$(K_b + \mathbf{Z}^n) \cap R_i(b) =$$

$$\left[\left\{ \bigcup_{B \in \mathcal{B}_i} ((K_b + Z(B)) \cap F(B; T(B)b)) \right\} + \mathbf{Z}^n \right] \cap R_i(b).$$

/*END OF STATEMENT OF THE THEOREM*/

I will prove the theorem by using Theorem (4.1). To do so, I will show using lemma (6.2) below that for any $b \in P$, the description of $K_b + \mathbf{Z}^n$ can be easily obtained from the description of $K_c + \mathbf{Z}^n$ where c has all its components in the range $[0 \;\; n2^{3\phi}]$. Further, I will show that c is a "piecewise affine" function of b ; i.e., that P can be partitioned into polynomially many copolyhedra such that for each copolyhedron in the partition, there is an affine function that maps b to c. This proof will use lemma (6.3). Throughout this section, I let M denote $n2^{3\phi}$.

Lemma (6.2) : Let A be an $m \times n$ matrix of integers of size ϕ. Suppose b is any point in $\mathbf{R}^m$ with $b \geq 0$. (So, 0 is in K_b.) Define $b' = (b'_1, b'_2, \ldots b'_m)$ by : $b'_i = \min\{b_i, n2^{3\phi}\}$. Then,

$$K_b + \mathbf{Z}^n = K_{b'} + \mathbf{Z}^n.$$

Proof : The proof is based on the following fact due to Cook, Gerards, Schrijver and Tardos [3] : Let Δ be the maximum absolute value of any subdeterminant of A. If a point p belongs to K_b, and if K_b contains some point in $\mathbf{Z}^n$, then there is a point $q \in \mathbf{Z}^n \cap K_b$ with $|p_i - q_i| \leq n\Delta$ for $i = 1, 2, \ldots n$. (This fact is true for any "right hand side" b.)

It is clear that

$$K_b + \mathbf{Z}^n \supseteq K_{b'} + \mathbf{Z}^n.$$

Now, I will prove the converse. Suppose x is any point in $K_b + \mathbf{Z}^n$. Then $K_b - x$ contains an integer point; it also contains $-x$. So, by the above fact, there is an integer point z in $K_b - x$ with $|z_i + x_i| \leq n\Delta$ for all i. By Theorem

3.2 of [21], Δ is at most $2^{2\phi}$. It is now easy to see that $z+x$ belongs to $K_{b'}$ finishing the proof of the lemma.

∎

Suppose $v \cdot x = v_o$ is a hyperplane in Euclidean space. It partitions space into two "regions" - $\{x : v \cdot x \leq v_o\}$ and $\{x : v \cdot x > v_o\}$. Similarly, a set of l hyperplanes in $\mathbf{R}^m$ partition $\mathbf{R}^m$ into (at most) 2^l "regions" each region being determined by which side of each hyperplane it is on. There is another well-known upper bound on the number of regions - it is

$$\sum_{k=0}^{m} \binom{l}{k}.$$

For $l \leq m$, the sum is 2^l and the result is obvious. For $l > m$, we proceed by induction. The number of regions formed by the first $l-1$ of the hyperplanes is at most $\sum_{k=0}^{m} \binom{l-1}{k}$ by induction. Now imagine adding the l th hyperplane. I claim that the number of existing regions that the l th hyperplane intersects is at most $\sum_{k=0}^{m-1} \binom{l-1}{k}$ - to see this, note that the intersections of the existing regions with the l th hyperplane form a partition of the l th hyperplane (an $m-1$ dimensional affine space). Each region intersected by the l th hyperplane is divided into two by it. So we get the total number of regions formed by all the l hyperplanes is at most

$$\sum_{k=0}^{m} \binom{l-1}{k} + \sum_{k=0}^{m-1} \binom{l-1}{k} = \sum_{k=1}^{m} \left(\binom{l-1}{k-1} + \binom{l-1}{k} \right) + 1$$

which proves the claim. The lemma below follows immediately.

Lemma (6.3) Suppose V is a j dimensional affine subspace of $\mathbf{R}^m$. For any set of l hyperplanes in $\mathbf{R}^m$, the number of regions in the partition of $\mathbf{R}^m$ by the l hyperplanes that V intersects is at most

$$\sum_{k=0}^{j} \binom{l}{k} \leq l^j.$$

Further, if j is fixed, then given the hyperplanes and V, we can find the regions intersected by V in polynomial time.

Proof : The first part is already proved. For the algorithm, we go again to the first part of the proof and see that a problem with parameters l, j is reduced to two problems one with parameters $l-1, j$ and the other $l-1, j-1$. If the running time of the algorithm is $T(l,j)$, we get the recurrence $T(l,j) \leq T(l-1,j) + T(l-1,j-1) + O(1)$ which solves to $T(l,j)$ is in $O(l^j)$.

∎

Suppose as in the Theorem (6.1), P is a copolyhedron of affine dimension j_o in $\mathbf{R}^m$. Consider each of the (at most m^n) nonsingular $n \times n$ submatrices B of A. For each of these we can define an $n \times m$ matrix T by augmenting B^{-1} with 0 columns so that the possible corners of any K_b are of the form Tb for such T. For each such T, and each i, $1 \leq i \leq m$, consider the hyperplane $\{b : a^{(i)}Tb = b_i\}$ in $\mathbf{R}^m$. (Reminder : $a^{(i)}$ is the i th row of A.) There are at most m^{n+1} such hyperplanes and so by lemma (6.3) , we have that P intersects at most $m^{(n+1)j_o}$ of the regions that these hyperplanes partition $\mathbf{R}^m$ into. It is not difficult to see that for fixed n, j_o, we can find these regions in polynomial time. For each such region U, there is a T_U such that $T_U b$ is in K_b for all $b \in U$; in other words $b - AT_U b$ is a nonnegative vector for all $b \in U$. Consider the m hyperplanes $(b - AT_U b)_i = M$ for $i = 1, 2, \ldots m$. By applying lemma (6.3) again, we see that U intersects at most m^{j_o} of the regions that these m hyperplanes partition space into. We partition U into these m^{j_o} or less parts. Thus we have found so far in polynomial time, a partition of P into copolyhedra $P_1, P_2, \ldots P_t$ with

$$t \leq m^{(n+2)j_o}$$

and associated with copolyhedron P_k in the above partition, we have an affine transformation $T(P_k)$ and an $I(P_k) \subseteq \{1, 2, \ldots m\}$ such that for all $b \in P_k$,

$$0 \leq (b - AT(P_k)b)_i \leq M \forall i \in I(P_k) \qquad \text{and}$$
$$(b - AT(P_k)b)_i > M \forall i \notin I(P_k).$$

For each $b \in P_k$, let $b' = b - AT(P_k)b$, let b'' be defined by $b''_i = b'_i$ for $i \in I(P_k)$ and $b''_i = M$ for other i. Let $b''' = b'' + AT(P_k)b$. Note that there is a linear transformation that maps each b to b'''. Now by lemma (6.2), we see that for all $b \in P_k$, we have

$$K_{b'} + \mathbf{Z}^n = K_{b''} + \mathbf{Z}^n.$$

Note that b'' belongs to the copolytope

$$P' = \{b : b \in P; |b| \leq M\}$$

We apply the main theorem (4.1) with this copolytope. I will show that an easy argument then gives us Theorem (6.1). To this end, let S_i be one of the sets in the partition of $P' \times \mathbf{R}^n$ that Theorem (4.1) yields. Corresponding to each such S_i we define one subset R_{ik} of $P_k \times \mathbf{R}^n$ for each k. Namely,

$$R_{ik} = \{(b, x) : b \in P_k \ ; \ (b'', x - T(P_k)b) \in S_i\}$$

It is easy to see that the R_{ik} have all properties 1,2, and 3 in the statement of Theorem (6.1) with a suitable choice of constant e. By Theorem (4.1), we have for all b in P_k,

$$\begin{aligned}(K_{b'} + \mathbf{Z}^n) \cap S_i(b'') \quad &= \quad (K_{b''} + \mathbf{Z}^n) \cap S_i(b'') = \\ \left[\left\{\bigcup_{B \in \mathcal{B}_i} ((K_{b''} + Z(B)) \cap F(B; T(B)b''))\right\} + \mathbf{Z}^n\right] &\cap S_i(b'').\end{aligned}$$

Translating the sets on both sides of the above equation by $T(P_k)b$, we obtain

$$\begin{gathered}(K_b + \mathbf{Z}^n) \cap R_{ik}(b) = \\ \left[\left\{\bigcup_{B \in \mathcal{B}_i} ((K_{b'''} + Z(B)) \cap F(B; T(B)b'' + T(P_k)b))\right\} + \mathbf{Z}^n\right] \cap R_{ik}(b).\end{gathered}$$

Since $K_{b'''} \subseteq K_b$, we may replace $K_{b'''}$ on the right hand side (rhs) of the above equation by K_b. (Note that then we would have lhs contained in the rhs. The converse is obvious.) Further, there is an affine transformation, say, Q that takes b to b''. So, we may now define the affine transformation corresponding to the basis B to be

$$T(B)Q + T(P_k)$$

to complete the proof of Theorem (6.1).

∎

7 Test sets for Integer Programs, $\forall\exists$ sentences and maximal lattice-free K_b

For linear programming problems, we know that if there is a feasible solution, there is a basic feasible one. This can be expressed as follows :

Suppose as before A is an $m \times n$ matrix of rank n. Consider as before, each of the (at most m^n) nonsingular $n \times n$ submatrices B of A. For each of these we can define an $n \times m$ matrix T by augmenting B^{-1} with 0 columns so that the possible corners of any K_b are of the form Tb for such T. Then we can say that for all possible right hand sides b, if K_b is nonempty, then one of the Tb belongs to K_b. This section proves a similar theorem for Integer Programs.

(7.1) Theorem : Let A be an $m \times n$ matrix of integers of size ϕ with the property that $\{x : Ax \leq 0\} = \{0\}$ (or equivalently, K_b is bounded for all b). Let P be a copolyhedron in $\mathbf{R}^m$ of affine dimension j_o. For n, j_o fixed, there is a polynomial time algorithm that finds a partition of P into $P_1, P_2, \ldots P_r$ with $r \leq (mn\phi)^{j_o n^{dn}}$ and each P_i of the form $P_i'/\mathbf{Z}^l$ where P_i' is a coplyhedron and l is a constant and for each P_i, finds a set $\mathcal{T}_i$ of pairs (T, T') affine transformations where $T : \mathbf{R}^m \to \mathbf{R}^n$ and $T' : \mathbf{Z}^n \to \mathbf{Z}^n$ such that for all i and for all $b \in P_i$,

$$K_b \cap \mathbf{Z}^n \neq \emptyset \quad \Longleftrightarrow \quad \exists (T, T') \in \mathcal{T}_i \; : \; T'\lfloor Tb \rfloor \in K_b.$$

Further, for each i, the set $\mathcal{T}_i$ contains at most $(O(n))^{4n}$ pairs (T, T').

Proof : First, we may replace P by $\{b : b \in P, \exists x : Ax \leq b\}$. So assume without loss of generality that for all b in P, we have $K_b \neq \emptyset$ and bounded.

Let $L = \mathbf{Z}^n$. Note that $K_b \cap L$ is empty iff $K_b + L$ does not contain 0. We apply Theorem (6.1) to get the partition of $P \times \mathbf{R}^n$ into $R_1, R_2, \ldots R_r$. Let $P_i = \{b : 0 \in R_i(b)\}$. It is easy to see that P_i is of the form $P_i'/\mathbf{Z}^l$ where P_i' is a copolyhedron and l is a constant (for fixed n).

Also, from Theorem (6.1), we have for b in P_i,

$$(K_b + \mathbf{Z}^n) \cap \mathbf{Z}^n =$$

$$\left[\left\{\bigcup_{B \in \mathcal{B}_i} (K_b + Z(B)) \cap F(B; T(B)b)\right\} + \mathbf{Z}^n\right] \cap \mathbf{Z}^n.$$

The left hand side in the above equation is empty if and only if for each B, the unique lattice point $z_B(b)$ in $F(B; T(B)b)$ has the property that $z_B(b) - Z(B)$ does not intersect K_b. It is quite straightforward to see that for each $p \in Z(B)$, we can find a pair of affine transformations (T, T') as required in the statement of Theorem (7.1), such that $z_B(b) - p = T'(\lfloor Tb \rfloor)$. This completes the proof of the theorem.

∎

I now give a decision procedure for deciding the truth or falsity of certain sentences in Presberger arithmetic.

(7.2) Theorem : There is an algorithm which takes as input an $m \times n$ matrix A and an $m \times p$ matrix B and an $m \times 1$ matrix b all made up of integers and a copolyhedron Q in $\mathbf{R}^{p+l}$ by a set of defining inequalities, decides whether the following sentence is true.

$$\forall y \in Q/\mathbf{Z}^l \quad \exists x \in \mathbf{Z}^n : \qquad Ax + By \leq b.$$

Further for fixed n, p, l, the algorithm runs in time bounded by a polynomial in the length of the input.

Remark : Note $\mathbf{R}^p$ and $\mathbf{Z}^p$ are both special cases of sets of the form $Q/\mathbf{Z}^l$. The first is obvious. For the second, we can make $l = p$ and $Q = \{(y, y) : y \in \mathbf{R}^p\}$. Also, it is easy to see that the Frobenius problem : given $a_1, a_2, \ldots a_n, a_{n+1}$, is $Frob(a_1, a_2, \ldots a_n) \leq a_{n+1}$? is a special case of such a sentence.

Proof : Let $Q/\mathbf{R}^l = Q'$. The set Q' includes the set $Q/\mathbf{Z}^l$ - the set of all the y of interest. For y in Q', the quantity $b - By$ is in an affine subspace P of $\mathbf{R}^m$ of dimension p or less. So by Theorem (7.1), we can find in polynomial time (since n, p are fixed) a partition of P into $P_1, P_2, \ldots P_r$ with

$$r \leq (n\phi m)^{pn^{dn}}$$

and for each P_i, a collection $\mathcal{T}_i$ of pairs of affine transformations (T, T') satisfying the conditions of that theorem. The sentence

$$\forall y \in Q/\mathbf{Z}^l \quad \exists x \in \mathbf{Z}^n : \qquad Ax + By \leq b$$

is false iff there is some P_i with the property that

$$\exists y \in P_i \cap Q/\mathbf{Z}^l : \forall (T, T') \in \mathcal{T}_i : T'\lfloor T(b - By) \rfloor \notin \{x : Ax \leq b - By\}.$$

This will be true iff one of the Mixed Integer programs set up below is feasible : Consider each of the $m^{(cn)^{4n}}$ maps f from pairs (T, T') in $\mathcal{T}_i$ to $\{1, 2, \ldots m\}$. For each such map, we will have one MIP that asserts that there exists a $y \in P_i \cap Q/\mathbf{Z}^l$ with $(T'\lfloor T(b - By) \rfloor)$ violating the $f(T, T')$ th constraint for each (T, T'). Note that the floor of a real variable w can be expressed using a new integer variable which is constrained to be in the interval $(w - 1 \;\; w]$. Also the condition that $y \in Q/\mathbf{Z}^l$ can be expressed by introducing l new integer variables. Each P_i is of the form $P_i'/\mathbf{Z}^k$ and we deal with this analogously. For convenience, order the pairs (T, T') and refer to them as $(T, T')_i$. The MIP will read as follows :

$$\exists y \in \mathbf{R}^p, z \in \mathbf{Z}^l, z_1, z_2, \ldots \in \mathbf{Z}^n : (y, z) \in Q; y \in P_i$$
$$T_i(b - By) - 1 < z_i \leq T_i(b - By); (AT_i'z_i)_{f(T,T')_i} > b_{f(T,T')_i}.$$

Clearly, we may solve each MIP for each P_i in turn and if one of them is feasible, return false for the sentence otherwise, true.

It is not difficult to see that the required bound on the running time.

∎

The rest of the section discusses properties of the set of right hand sides b for which $K_b \cap \mathbf{Z}^n$ is empty.

Let
$$LF(A, P) = \{b : b \in P, K_b \cap \mathbf{Z}^n = \emptyset\}.$$

Let $P_1, P_2, \ldots$ be the partition of P that Theorem (7.1) yields. Let
$$LF(A, P) = \cup_i LF(A, P_i).$$

$LF(A, P_i)$ can be described by linear constraints with the introduction of some extra integer variables as the following shows : we consider all mappings f of the following sort : f takes as argument a pair (T, T') in $\mathcal{T}_i$ and its range is $\{1, 2, \ldots m\}$. Let $V(i, f)$ be the set of b satisfying

- b belongs to P_i.
- $T'(\lfloor Tb \rfloor)$ violates constraint number $f(T, T')$ of the m constraints $Ax \leq b$.

To express the floor, we can introduce a new integer variable and linear constraint. Thus, we see that $LF(A, P_i)$ is the union of a polynomial number of sets each of the form copolyhedron/$\mathbf{Z}^l$ where l is a constant for fixed n, j_o. We use this discussion in a slightly different context below.

Suppose as above A is a fixed $m \times n$ matrix of integers with $\{x : Ax \leq 0\} = \{0\}$. For any $b \in \mathbf{R}^m$, as before, we let $K_b = \{x : x \in \mathbf{R}^n; Ax \leq b\}$. We say that a K_b is maximal-lattice-point free if it has no points of $\mathbf{Z}^n$ in its interior and any convex set that strictly contains K_b does. We can replace the last condition by the requirement that every facet of K_b have a lattice point interior to it [14]. By a theorem of Bell [1] and Scarf [16], a maximal lattice free K_b has at most 2^n facets. We choose all subsets of the m inequalities $Ax \leq b$ of cardinality at most 2^n, and for each subset, we will study the positions of the facets that result in maximal lattice free sets; we only incur an extra factor of m^{2^n} by this which is polynomially bounded for fixed n. Then arguing as for the case of lattice-point-free sets and adding the condition that each facet have a lattice point, we get the following theorem.

(7.3) Theorem : Suppose n is fixed. Then for any $m \times n$ integral matrix A, there exists a collection of sets $\{U_1, U_2, \ldots U_t\}$, where t is bounded by a polynomial in the size of A, and each U_i is of the form $U'_i/\mathbf{Z}^l$, where l is a constant, and U'_i is a copolyhedron such that the collection of maximal lattice point free sets K_b is precisely the collection$\{K_b : b \in U_1 \cup U_2 \cup \ldots U_t\}$.

Remark : Note that a similar theorem is not true for just lattice-point-free b - there we would have also needed to assume that m was fixed or else at least the affine dimension of P over which b varied was fixed. The theorem of Bell and Scarf helps us dispense with this assumption for *maximal* lattice point free sets.

8 Remarks

Remark 1 : The time bounds for the decision procedure for the sentences of Theorem (7.2) have a double exponential dependence on n, the number of variables in the inner quantifier. While this may seem prohibitive, it will be shown in a forthcoming paper that the following problem is NP-complete - given a sentence of the form in Theorem (7.2) in which $n+p$ is $O(\log($ length of the sentence $))$, decide whether it is true or false. (In other words, even if the number of variables is restricted to be very small, the problem still remains NP-hard.) A substantial improvement in the double exponential dependence would thus result in faster simulations of general nondeterministic Turing machines by deterministic ones.

Remark 2 : The question arises : what can be said about the Frobenius problem when n is not fixed. In a forthcoming paper, I will show that for variable n, in deterministic polynomial time, we can find an approximation to the Frobenius number to within a factor of 2^n. With a nondeterministic algorithm, we can come within a factor of $O(n^3)$ in polynomial time.

Remark 3 : Related to the Frobenius problem is the following : Given $a_1, a_2, \ldots a_n$, with GCD$(a_1, a_2, \ldots a_n)$ equal to 1, find the total number of natural numbers that cannot be expressed as a nonnegative integer combination of $a_1, a_2, \ldots a_n$. It is easy to see that this number is within a factor of 2 of $F = Frob(a_1, a_2, \ldots a_n)$: just note that for any integer x, $1 \leq x \leq F$, either x or $F - x$ cannot be expressed as a nonnegative integer combination of $a_1, a_2, \ldots a_n$. No polynomial time algorithm is known to find this number exactly in fixed dimension.

Remark 4 : Lenstra's result quoted earlier gives a polynomial time algorithm to decide the truth or falsity of a Σ_1 sentence over Presberger arithmetic, (using terminology from Logic) i.e., a sentence of the form :

$$\exists x_1, x_2, \ldots x_n \in \mathbf{Z} : x \in P_1 \cup P_2 \cup P_3 \ldots P_l$$

where P_i are polyhedra. Actually, Σ_1 sentences may have a conjunctions, disjunctions and negations of linear constraints. Negations may be replaced by the opposite inequality. We may then use Lemma (6.3) to convert the linear constraints into "disjunctive normal form", i.e., into a disjunction of groups where each group is a conjunction of constraints, or equivalently, a polyhedron. By Lemma (6.3), this does not increase the size by more than a polynomial in fixed dimension. The details of the conversion to "disjunctive normal form" are left to the reader. Also, note that Lenstra's result as stated works only for the case of one polyhedron ; but obviously, we may repeat the procedure for each P_i. The algorithm is polynomial time bounded provided n is fixed.

Theorem (7.2) gives an algorithm for deciding certain so-called Π_2 sentences (using terminology from Logic) , i.e., sentences of the form

$$\forall y \in \mathbf{Z}^p \quad \exists x \in \mathbf{Z}^n : \qquad (x, y) \in P.$$

This algorithm is polynomial time bounded provided $n+p$ is fixed. A general Π_2 sentence over Presberger arithmetic could require (x, y) to belong to a union of polytopes rather than just one (cf. last paragraph) . If it is the union of l polytopes, then using $O(\log l)$ extra integer variables, we can write it as a conjunction of constraints. So if l also fixed, we have a polynomial time algorithm for deciding such sentences. It is an interesting open problem to remove this restriction that l be fixed.

More interestingly, we do not know decision procedure for Σ_3 sentences which runs in polynomial time for fixed number of variables. This and similar algorithms for higher levels of the hierarchy in Presberger arithmetic remain interesting open problems.

Acknowledgments I thank Imre Bárány, Bill Cook, Mark Hartmann, Laci Lovász, Herb Scarf and David Shallcross for many helpful discussions.

References

1. D.E.Bell, *A theorem concerning the integer lattice*, Studies in Applied Mathematics, 56, (1976/77) pp187-188 (see Math. Rev. 57# 2590)

2. A.Brauer and J.E.Shockley, *On a problem of Frobenius*, Journal für reine und angewnadte Mathematik, 211 (1962) pp 399-408 (see Math. Rev. 47#127)

3. W.Cook, A.M.H.Gerards, A.Schrijver and E.Tardos, *Sensitivity theorems in integer linear programming* , Mathematical Programming 34 (1986) pp 251-264

4. P.Erdös and R.Graham, *On a linear diophantine problem of Frobenius*, Acta Arithmetica, 21 (1972).

5. H.Greenberg, *Solution to a linear diophantine equation for nonnegative integers*, Journal of Algorithms 9, pp 343-353, (1988).

6. M.Hujter and B.Vizvári, *The exact solution to the Frobenius problem with three variables*, Journal of the Ramanujan Math. Soc., 2 (1987) pp 117-143; (see Math. Rev. 89f:11039).

7. M.Grötschel, L.Lovász and A.Schrijver, *Geometric algorithms and combinatorial optimization*, Springer-Verlag (1988)

8. J. Incerpi and R.Sedgwick, *Improved upper bounds on ShellSort*, Journal of Computer and Systems Sciences, Vol. 31, No. 2, October 1985 pp 210-224. (see Math. Rev. 87j# 68025)

9. R.Kannan, *Minkowski's Convex body theorem and integer programming*, Mathematics of Operations Research, Volume 12, Number 3, (1987) pp415-440.

10. R.Kannan and L.Lovász, *Covering minima and lattice point free convex bodies*, in Lecture Notes in Computer Science 241, ed. K.V.Nori, Springer-Verlag (1986) pp 193-213. Final version in Annals of Mathematics, Volume 128, No.3, pp 577-602 (1988). (see Math. Rev. 89b:11055, 89i:52020)

11. R.Kannan, L.Lovász and H.E.Scarf, *The shapes of polyhedra*, Cowles Foundation Discussion paper No. 883, September (1988). To appear in Mathematics of Operations Research.

12. H.Krawczyk and A.Paz, , *The diophantine problem of Frobenius : A close bound*, Discrete Applied Mathematics 23 (1989) pp 289-291.

13. H.W.Lenstra, *Integer programming with a fixed number of variables*, Mathematics of Operations Research, Volume 8, Number 4 Nov (1983) pp 538-548

14. L.Lovász, *Geometry of Numbers and Integer Programming*, Proceedings of the 13 th International Symposium on Mathematical Programming, M.Iri and K.Tanabe eds., Mathematical Programming (1989) pp 177-201.

15. O.J.Rödseth, *On a linear diophantine problem of Frobenius*, Journal für reine und angewante Mathematik, 301, (1978), pp 171-178. (see Math. Rev. 58#27741)

16. H.E.Scarf, *An observation on the structure of production sets with indivisibilities*, Proceedings of the National Academy of Sciences, USA, 74, pp 3637-3641 (1977).

17. H.E.Scarf and D.Shallcross, *The Frobenius problem and maximal lattice free bodies*, Manuscript (1989).

18. R.Sedgwick, *A new upper bound for ShellSort*, Journal of Algorithms, 7 (1986), pp 159-173. (see Math. Rev. 87e:68015)

19. E.S.Selmer, *On the linear diophantine problem of Frobenius*, Journal für reine und angewandte Mathematik, 293/294 (1977) pp 1-17. (see Math. Rev.56#246)

20. E.S.Selmer and O.Beyer, *On the linear diophantine problem of Frobenius in three variables* Journal für reine und angewandte Mathematik, Band 301, (1978), pp 161-170. (see Math. Rev.58#27740)

21. A.Schrijver, , *Theory of Linear and Integer Programming*, Wiley (1986).

22. B.Vizvári, *An application of Gomery cuts in number theory*, Periodica Mathematica Hungaria 18 (1987) pp 213-228. (see Math. Rev. 89d:11017)