Annual Review of Computer Science, Volume 2, 1987. Annual Reviews Inc.

Algorithmic Geometry of Numbers

Ravindran Kannan

1 Introduction

Many computational problems have benefited greatly from the study of the mathematical structure underlying the problems. In linear programming, the simplex algorithm, duality theory and sensitivity analysis can be understood through basic linear algebra. The more recent polynomial-time algorithms of Khaciyan [37] and Karmarkar [36] are based on solid geometry. The converse has also been true of linear programming, particularly, the simplex algorithm - it provides elegant proofs of structural results like Farkas' lemma.

Problems of a more combinatorial nature like the graph matching problem also illustrate this phenomenon - the development of algorithms like the Edmonds[12] matching algorithm and the study of the underlying polyhedral structure have gone hand in hand, each benefiting the other. There are many other areas of computer science - Cryptography, primality testing and factorization, graph isomorphism, graph embeddings, computational geometry - which have used various branches of mathematics. In general, all of these areas share one feature - the mathematics used by each area is what may be broadly classified as discrete mathematics (combinatorics, algebra) or continuous mathematics (geometry, analysis, topology); rarely does one area combine the two types of mathematics in significant proportions.

Many other combinatorial problems like the Traveling salesman problem, vertex coloring in a graph, knapsack and integer linear programming problems have, of course, resisted attempts so far to devise polynomial-time algorithms. The elegant theory of NP-completeness pioneered by Cook [6] and Karp [35] has been developed [17] to show that these and many other problems are equivalent as far as polynomial-time algorithms go. It has come to be widely believed that these and other NP-hard problems will not admit of polynomial-time algorithms. However, there is not a substantial body of evidence to back up such a belief. First, the known lower-bounds on computational resources needed to solve problems are a far cry from a non-polynomial lower bound on the computation time for any of these combinatorial problems; it is unclear that current lower bound techniques will ever yield such strong results. Further, it is difficult to assert that very sophisticated techniques have failed to produce efficient algorithms for NP-hard problems, for, there have not been many such techniques until recently. Thus, it is important to study the mathematical structure underlying NP-hard problems and develop new techniques for solving them.

There are, of course, other important reasons for studying mathematical structure. This may help devise more efficient algorithms than naive enumeration although the algorithms may not be polynomial-time bounded. Also, they may help solve significant special cases in polynomial-time.

An important beginning in this direction was made by H.W. Lenstra's polynomial-time algorithm for integer programming in a fixed number of dimensions [47]. This algorithm pioneered the subject of this article - Algorithmic Geometry of Numbers. The fundamental basis reduction algorithm of Lovász which first appeared in Lenstra, Lenstra, Lovász [46] was used in Lenstra's algorithm for integer programming and has since been applied in myriad contexts -starting with factorization of polynomials (A.K. Lenstra, [45]). Classical Geometry of Numbers has a special feature in that it studies the geometric properties of (convex) sets like volume, width etc. which come from the realm of continuous mathematics in relation to lattices which are discrete objects. This makes it ideal for applications to integer programming and other discrete optimization problems which seem inherently harder than their "continuous" counterparts like linear programming.

In addition to the applications to algorithms, Algorithmic Geometry of Numbers has sparked a study of mathematical structure in pure Geometry Numbers [34], [22], [41] from a somewhat newer perspective, where sharper bounds (especially polynomial ones as opposed to super polynomial bounds) are sought. The very recent origin of the subject makes it difficult to assert at this point that the mathematics, or the algorithms, will have as pervasive an influence as the more established fields like say linear programming or the theory of NP-completeness; but there is evidence that the influence of the new subject will be substantial. The recent origin, however, gives us the advantage of being able to present a fairly self-contained introduction to the classical mathematics as well as to the algorithms in the subject and survey applications to cryptography, diophantine approximation, approximation of linear inequalities, factorization of polynomials among others. The attempt here has been to present nearly complete intuitive idea of various results from which the interested reader can work out the details rigorously. The ideas of Lenstra's integer programming algorithm and Lovász's basis reduction algorithm are explained in full. Briefer descriptions of several other results are given.

2 Convex bodies and Integer points

2.1 Minkowski's theorems

The fundamental question addressed in Geometry of Numbers is to find conditions on the volume (and other geometric properties) of a convex set in Euclidean space that would be sufficient to imply the existence of certain points with all integer coordinates in the set. Classical Geometry of Numbers generally concentrates on convex sets that are symmetric with respect to the origin - abbreviated 0-symmetric. (A set is 0-symmetric if, whenever it contains a point x, it also contains $-x$.) Minkowski's convex body theorem which may be considered the fundamental theorem of Geometry of Numbers asserts that whenever a 0-symmetric convex set in Euclidean $n-$space $\mathbf{R}^n$ has volume greater than 2^n, it contains a point with integer coordinates not all zero. We will now give an equivalent version of this statement with a proof.

Suppose K is a convex body in Euclidean n-space $\mathbf{R}^n$ and is symmetric about the origin. For any positive real number t, denote by tK the set $\{x : x/t \in K\}$; thus tK is a dilation of K by a factor of t. It is interesting to ask for what $t\,'s$ does tK contain a point with integer coordinates, not all of which are zero. Minkowski's theorem states that this happens whenever t exceeds $2V^{-1/n}$ where V is the volume of K. The proof is very simple: Let Y be the set of all points in $\mathbf{R}^n$ with integer coordinates and consider the set of convex bodies $\{\frac{1}{2}\ tK\ +\ y\ :\ y\ \in\ Y\}$. There is one point of Y per unit volume in space, each has a copy of $1/2\ tK$ centered at it and the volume of $1/2\ tK$ exceeds 1. So it can be rigorously argued that two such bodies - say $1/2\ tK\ +\ y_1$ and $1/2\ tk\ +\ y_2,\ y_1 \neq y_2$ must intersect. With $y\ =\ y_1\ - y_2,\ 1/2\ tK\ +\ y$ and $1/2\ tK$ intersect, say, at a point w. Then w is in $1/2tK$, so is $-w$, by symmetry. Further, $(w-y)$ is in $1/2tK$, so $1/2(w-y-w)\ =\ -y/2$ is in $1/2\ tK$ by convexity. So $-y$, a non-zero point with integer coordinates is in tK.

Defining the "first minimum" $\Lambda_1(\cdot)$ of the convex body K to be the infimum over all t such that tK contains a non-zero point of Y, we see that $\Lambda_1(K)\ \leq\ 2V^{-1/n}$. More generally, Minkowski defined the "successive minima" $\Lambda_1(K), \Lambda_2(K) \ldots, \Lambda_n(K)$ as follows: $\Lambda_i(K)$ is the infimum over all t such that tK contains i linearly independent points of Y. The "second theorem" of Minkowski strengthens the convex body theorem by showing that the product $\Lambda_1(K)\Lambda_2(K)\ldots\Lambda_n(K)$ is majorized by $2^n/V$. The proof of this theorem remains hard [4 or 44].

It is interesting to look at a special family of convex bodies - ellipsoids. If K is an ellipsoid, (open or closed) there is an invertible linear transformation τ that maps it into the sphere S of unit radius and origin as center (we denote this by $\tau K = S$). Noting that tK intersects $Y - \{0\}$ iff tS intersects $\tau Y - \{0\}$, we see that $\Lambda_i(K)$ is the smallest positive real t such that there are i linearly independent elements of τY each of (Euclidean) length at most t. In particular, $\Lambda_1(K)$ is the length of the shortest non-zero vector of the "lattice" τY. Describing τ by a matrix (τ_{ij}), it is easy to see that $(\Lambda_1(K))^2$ is the minimum of the quadratic form $\sum_{j=1}^n \sum_{i=1}^n (\tau_{ij}\ y_i\ y_j)$ where $y = (y_1, .., y_n)$ runs over $Y - \{0\}$. The study of quadratic forms dates back at least to Lagrange [9, Volume III] and historically has been a motivation for Geometry of Numbers. As we discuss in the next section, the so-called shortest vector problem for lattices is the problem of computing $\Lambda_1(K)$ for an ellipsoid K.

2.2 Lattices and the shortest vector problem

A lattice in $\mathbf{R}^n$ is the set of all integer linear combinations of a set of linearly independent vectors in $\mathbf{R}^n$. If $b_1, b_2..., b_m$ are the linearly independent vectors ($m \leq n$), the lattice "generated" by $b_1, b_2..., b_m$ denoted $L(b_1, b_2..., b_m)$ is the set $\{\Sigma\ \lambda_i\ b_i\ :\ \lambda_i \in \mathbf{Z}\}$ .The independent vectors $b_1, b_2.., b_m$ are called a basis of the lattice. It is not difficult to see that a set S in $\mathbf{R}^n$ is a lattice iff it is closed under subtractions ($x, y \in S \Rightarrow x - y \in S$) and is discrete, i.e., there is a positive real δ such that for any two distinct elements x, y in S, $|x - y| \geq \delta$. If we write $b_1, b_2.., b_m$ as the rows of an $m \times n$ "basis matrix" B, it is easy to see that for any unimodular $m \times m$ matrix U (integer matrix with determinant ± 1), the rows of UB generate the same lattice as the rows of B: just observe that each row of UB belongs to $L(b_1, b_2... b_m)$ and vice versa. It is also easy to see that if B_1 and B_2 are two different basis matrices of the same lattice, there is a unimodular matrix U such that $B_1 = UB_2$. (There is a natural correspondence between lattices and quadratic forms. With a lattice L with basis matrix B, we can associate the quadratic form yBB^ty^t [1] and study the values of the form as y ranges over $\mathbf{Z}^n$; by the above, this set of values is obviously independent of the basis chosen.)

It now follows that the "determinant" of the lattice $L(b_1, b_2.., b_m)$ defined to be the m-dimensional volume of the parallelopiped spanned by the origin, $b_1, b_2..., b_m$ is an invariant of the lattice. We denote by $d(L)$, the determinant of the lattice. The determinant is also the product of the lengths of the orthogonal vectors obtained by doing the familiar Grahm-Schmidt process on $b_1, ..., b_m$. In detail, define $b_1^*, b_2^*.., b_m^*$ as follows: b_1^* equals b_1 and for $i \geq 2$, b_i^* equals component of b_i orthogonal to the space spanned by $b_1, b_2..., b_{i-1}$. The determinant of the lattice, then, is the product of the lengths of the b_i^*. Using traditional algorithms, all these quantities may be computed in polynomial-time.

It will be useful for conceptual understanding of many of the algorithms to define the unit vectors $u_1, u_2, \ldots u_m$ by $u_i = b_i^*/|b_i^*|$. These vectors form an orthonormal basis for the vector space spanned by $b_1, b_2..., b_m$. We can represent the basis vectors in the coordinate system with the u_i as the axes vectors. Then the basis matrix (with each row as a basis vector) is lower triangular :

[1] ^{t} denotes the transpose of a matrix.

$$\begin{pmatrix} b_{11} & 0 & 0 & . & . & . & . & . & 0 \\ b_{21} & b_{22} & 0 & . & . & . & . & . & 0 \\ . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & b_{ii} & 0 & . & . \\ . & . & . & . & . & b_{i+1,i} & b_{i+1,i+1} & . & . \\ . & . & . & . & . & . & . & . & 0 \\ . & . & . & . & . & . & . & . & 0 \\ . & . & . & . & . & . & . & . & 0 \\ b_{m1} & b_{m2} & . & . & . & . & . & . & b_{mm} \end{pmatrix}$$

The lower triangular representation of the basis matrix

Here, obviously, $b_{ii} = |b_i^*|$. In practice, we do not actually change the coordinate system, for example, $|b_i^*|$ may be irrational even if the entries of b_j are all rational.

Suppose we are given a basis $b_1, b_2 ..., b_m$ of a lattice L in $\mathbf{R}^n$. A very natural and simply stated computational problem is to find the (a) shortest (in Euclidean length) non-zero vector in L. We call this the shortest vector problem (SVP). Most of the computational applications of Geometry of Numbers are based on the SVP, its relaxation (that of finding an approximately shortest vector) and certain related problems.

It is not known to date whether the SVP is NP-complete. No deterministic or random polynomial-time algorithm is known for it either; these remain important open questions in the area. The Lovász basis reduction algorithm finds a non-zero vector in the lattice whose length is at most $2^{m/2}$ times the length of the shortest one; it runs in polynomial-time. This algorithm is the foundation of many other algorithms in the area; it is the cornerstone of Algorithmic Geometry of Numbers. The factor of $2^{m/2}$ has subsequently been improved to c^m for any constant c with the running-time remaining polynomial [58]; it would be interesting to approximate to a subexponential factor in polynomial-time. Before the papers of Lenstra [47] and Lenstra, Lenstra and Lovász [46], there were some algorithms known for the SVP [8], [54], [39, section 3], [10]; but these are not even polynomial time bounded when the number of dimensions is fixed. An algorithm that solves the SVP exactly in polynomial time when the number of dimensions is fixed is given in [31].

The existence of short non-zero vectors in lattices is in fact implied by Minkowski's theorems, as we presently describe. For a lattice L, in $\mathbf{R}^n$ of dimension m, let us define $\Lambda_i(L)$ to be the least positive real t, such that there are i linearly independent elements of L each of (Euclidean) length at most t. (We are abusing notion slightly here; if ρ is the linear transformation that maps L into the lattice $\mathbf{Z}^m$ generated by m unit vectors, $\Lambda_i(L)$ equals Λ_i of the convex body ρK according to our earlier definition, where K is the intersection of the sphere of unit radius centered at the origin in $\mathbf{R}^n$ with the vector space spanned by L. Note that ρK is an ellipsoid.). Then Minkowski's Convex body theorem implies that

$$(\Lambda_1(L))^m \leq 2^m d(L)/V_m$$

and Minkowski's second theorem implies

$$\Lambda_1(L)\,\Lambda_2(L)\ldots\Lambda_m(L) \leq 2^m d(L)/V_m$$

where V_m is the volume of the unit sphere in m-dimensions.

Both implications follow easily from two observations: since $d(\mathbf{Z}^m) = 1$, determinant of ρ equals $1/d(L)$ and the volume of ρK equals $V_m/d(L)$. Using estimates for V_m, we have

$$\Lambda_1(L) \leq \sqrt{m}(d(L))^{1/m}$$

and a (stronger) inequality for the product of the minima.

Lovász [48] has shown that the computational problem of finding a non-zero vector in a lattice L of length at most a polynomial times $\Lambda_1(L)$ is polynomial-time equivalent to that of finding one of length within a polynomial factor of $(d(L))^{1/m}$. Neither is known at the present time to be polynomial-time computable.

2.3 Reduced bases of a lattice

The successive minima $\Lambda_1(L), \Lambda_2(L), \ldots \Lambda_n(L)$ of an n dimensional lattice L described in the last section are an important set of constants for the lattice. If the minima are realized by n elements $v_1, v_2 \ldots v_n$ of the lattice, the set $\{v_1, v_2 \ldots v_n\}$, of course spans the vector space spanned by L; however, it does not, in general, form a basis of the lattice. It is of interest to consider a basis of a lattice consisting of "short" vectors. We will define several notions of "reduced basis" of a lattice; a reduced basis consists of short vectors. First we make an intuitive connection between the vectors comprising a basis of a lattice being short and their being "nearly orthogonal" to each other. For a 2-dimensional lattice L with $b_1,\ b_2$, as a basis, $d(L) = |b_1|\ |b_2| \sin\theta$ where θ is the acute angle between b_1 and b_2. So it is clear that since $d(L)$ is an invariant, if $|b_1|$ and $|b_2|$ are small, then θ is large, i.e., the vectors are "close to " orthogonal. If L is an n-dimensional lattice with basis $b_1,\ b_2...,\ b_n$ let θ_i be the angle between b_i and the vector space spanned by $b_1, \ldots b_{i-1}$ for $i = 2, 3.., n$. Then $d(L)$ equals $|b_1|\ |b_2| \ldots |b_n| (\sin\ \theta_2)\ (\sin\theta_3)...(\sin\ \theta_n)$, so if $|b_1|,\ |b_2| \ldots, |b_n|$ are small, $\theta_2 \ldots, \theta_n$ are large (not necessarily individually). i.e., the i^{th} basis vector is "nearly orthogonal" to the previous ones. There is, in a sense, a converse to this argument. Suppose we are given a basis which is nearly orthogonal in the sense that $|b_1|\ |b_2|...|b_n|/d(L) = M$ is small. Then the shortest of the basis vectors is clearly at most $(Md(L))^{1/n}$ (cf Minkowski $\Lambda_1(L) \leq \sqrt{n}\ (d(L))^{1/n}$), though it may be considerably longer than $\Lambda_1(L)$. More can be said; we can "quickly" compute a shortest non-zero vector v in L from such a basis: suppose $v = \sum_{i=1}^{n} \lambda_i\ b_i\ , \lambda_i \in \mathbf{Z}$. Then by Cramer's rule for solving simultaneous linear equations, and Hadamar's inequality,

$$|\lambda_i| \leq |b_1|\ |b_2| \ldots |b_{i-1}|\ |v|\ |b_{i+1}| \quad |b_n|/d(L) \leq M$$

since $|v| \leq |b_i|$. So v may be found by enumerating relatively few candidates for $\lambda_1,\ \lambda_2 \ldots,\ \lambda_n$. The ratio $|b_1|\ |b_2| \ldots |b_n|/d(L)$ was considered by Hermite [25] who first showed that every lattice has a basis with the ratio bounded above by a function of its dimension alone, actually $2^{O(n^2)}$. when the dimension is n. The ratio has been called the "orthogonality defect" [58] of the basis $b_1 \ldots, b_n$.

For a vector space, there is always a completely orthogonal basis - for example, the Grahm -Schmidt process finds one from any given basis. From simple 2-dimensional examples, it can be seen that a lattice may not always have a completely orthogonal basis. For example, consider the lattice generated by two vectors of equal length at an angle of 60°. However, it is interesting that there is always a basis with orthogonality defect bounded above by a function of the dimension of the lattice alone as Hermite showed. There are different notions of "reduced basis" in Geometry of Numbers. However, they all share the property that their orthogonality defect is bounded by a function of the dimension alone. Minkowski defined a basis $b_1,\ b_2, \ldots,\ b_n$ of a lattice L to be reduced if for each $i, 1 \leq i \leq n$ b_i is a shortest vector in L so that $\{b_1 \ldots, b_i\}$ forms a subset of some basis of L. (i.e., $\{b_1 \ldots, b_i\}$ forms a so-called primitive set of L). He showed [52] that the orthogonality defect of his reduced basis , which is different from the one used by Hermite, is $2^{O(n^2)}$. (Contrast this with the fact that an n dimensional lattice L contains n linearly independent vectors

$v_1, v_2 \ldots, v_n$ with $|v_1||v_2|\ldots|v_n|/d(L) \leq 2^n$ - a consequence of Minkowski's second theorem pointed out in section 2.1.)

There is a second natural notion of a reduced basis due to Korkhine and Zolotarav [40] which has turned out to be more useful computationally. Instead of requiring b_2 to be the shortest vector which along with b_1, forms a primitive set, it requires the component of b_2 orthogonal to b_1(i.e.,$b_2^* = b_2 - \frac{b_2 \cdot b_1}{b_1 \cdot b_1} b_1$) to be as short as possible still preserving the primitiveness of $\{b_1, b_2\}$. In general, the component b_i^* of b_i orthogonal to the vector space spanned by $\{b_1,\ b_2 \ldots, b_{i-1}\}$ is required to be as short as possible while still maintaining the primitiveness of $\{b_1,\ b_2 \ldots, b_i\}$. Equivalently, we can stipulate that the component of b_i orthogonal to $V_{i-1} =$ the span of $\{b_1,\ b_2 \ldots, b_{i-1}\}$ is the shortest (nonzero) vector of the lattice L' obtained by projecting L orthogonal to V_{i-1}.

We will call a basis satisfying these conditions plus the condition that for each i, $1 \leq i \leq n$, $(b_i - b_i^*)$ belongs to the rectangular solid $\{\sum_{j=1}^{i-1} \alpha_j\ b_j^*\ :\ \frac{-1}{2} < \alpha_j \leq \frac{1}{2}$ for $j = 1, 2, \ldots, i-1\}$ a $K - Z$ reduced basis. We will see in section 3 that the last condition which we refer to as *properness* of the basis is easily achieved by adding suitable integer multiples of $b_{i-1}.b_{i-2} \ldots, b_1$ to b_i (in that order) and that this does not affect the previous conditions. The next paragraph contains an equivalent definition of $K - Z$ reduced.

A basis is $K - Z$ reduced if in the lower triangular representation of the basis discussed in section 2.2, each diagonal entry b_{ii} is the length of the shortest nonzero vector in the lattice generated by the rows of the $(n-i+1) \times (n-i+1)$ submatrix consisting of the last $n-i+1$ rows and columns; and furthermore, each entry b_{ij} below the diagonal satisfies $-b_{jj}/2 < b_{ij} \leq b_{jj}/2$. The last condition is equivalent to properness.

It has been shown that $K - Z$ reduced basis has orthogonality defect at most n^n [58]; this is the best known for any basis. Lovász's algorithm finds a third reduced basis, we will define it later; it has an orthogonality defect of $2^{O(n^2)}$ [46] which we prove in section 3. The Lovász reduced basis shares a feature with $K - Z$ reduced basis in that it puts requirements on the components of each basis vector orthogonal to the previous ones. But it is weaker than the $K - Z$ reduced basis. For both of these bases, Babai [1] has shown the following fact : let α_i be the angle between b_i and the subspace spanned by **all the other** basis vectors. Then

$$\sin \alpha_i \geq (\sqrt{2}/3)^n$$

.

This obviously implies the corresponding lower bound on $\sin \theta_i$ for the angle θ_i between b_i and the subspace spanned by the previous basis vectors.

Interestingly, Minkowski reduced bases have been studied more extensively than $K - Z$ reduced bases [4, 44]. There has been some work on $K - Z$ reduced bases and algorithms for them predating Lenstra's paper [55,53]; a survey of these and other results may be found in [56]. One of the reasons for the greater emphasis on Minkowski reduced bases is perhaps the fact that in the context of quadratic forms they are more natural than reduced bases involving projections orthogonal to subspaces like the $K - Z$ reduced basis and Lovász reduced basis. Lovász's algorithm demonstrated that reduced basis involving projections may be more useful for computational purposes. Further evidence of this was provided by Kannan [31] where a polynomial time algorithm for finding a $K - Z$ reduced basis for fixed number of dimensions was given and was used to develop faster algorithms for integer programming and other lattice problems; this is described in section 5. Schnorr's [58] proof that the orthogonality defect of a $K - Z$ reduced basis was $O(n^n)$ gives an explanation of the computational advantage enjoyed by the basis over a Minkowski reduced basis. Lagarias, Lenstra and Schnorr [41] proved some nice structural properties of $K - Z$ reduced basis and used these to prove sharper "transferrance " bounds than the classical ones obtained by using Minkowski reduced basis and successive minima [4,section XI.3] ; their work is described in section 7. Projections also play a crucial role in the study of structure of lattice point-free convex bodies undertaken by Kannan and Lovász [34] described in section 7. This study was motivated by efficiency of algorithms. Thus, the renewed interest in using projections orthogonal to certain lattice vectors spurred on because of the computational advantages seems to be proving of value for purely structural reasons too.

2.4 Dual Lattices

If L is any lattice, the dual (or polar) lattice of L, denoted L^* is the set

$$L^* = \{y : y \in \text{ span of } L;\ y.x \in \mathbf{Z}\ \forall x \in L\}$$

It is easily checked that if L is an n dimensional lattice in $\mathbf{R}^n$ and $b_1, b_2, \ldots b_n$ is a basis of L, then with B equal to the "basis matrix" of L (consisting of $b_1, b_2 \ldots b_n$ as its rows), $(B^{-1})^t$ is a basis of the lattice L^* and therefore the determinant of L^* is the reciprocal of the determinant of L. Thus, we have by Minkowski's convex body theorem,

$$\Lambda_1(L)\Lambda_1(L^*) \leq n$$

This is the first of the so called "transferrance results" which connect the "primal" and dual lattice. It has been shown by a counting argument that the upper bound on $\Lambda_1(L)\Lambda_1(L^*)$ cannot be improved by more than a constant [Conway and Thompson quoted in 50] .

2.5 Gauss's basis reduction algorithm in 2 dimensions

The earliest basis reduction algorithm is due to Gauss [20, Article 171] for finding reduced basis in 2-dimensional lattices. (The notions of Minkowski reduced and $K-Z$ reduced basis coincide in two dimensions and Gauss's algorithm finds them.) He stated it in terms of quadratic forms; here we describe it for lattices. The Lovász basis reduction algorithm may be viewed as an efficient generalization of this to n-dimensions. Suppose b_1, b_2 forms the current basis of the lattice and assume after renaming them, if necessary, that $|b_1| \leq |b_2|$. A simple way to shorten b_2 (and preserve a basis of the lattice) is to replace b_2 by the shortest vector of the form $b_2 - mb_1,\ m \in \mathbf{Z}$. It is easy to check that m equal to the integer nearest to $(b_2 \cdot b_1)/(b_1 \cdot b_1)$ achieves this and that $(b_2 - mb_1) = b_2'$ has a component of length at most $|b_1|/2$ along the direction of b_1. Now if $|b_2'| \geq |b_1|$, we stop, else we swap them and repeat the procedure. It readily follows that at the end of the procedure, the acute angle between b_1 and b_2 is at least 60 degrees, so they are "fairly" orthogonal and also that the basis is reduced. The procedure must terminate since there are only a finite number of lattice elements of any given length or less. If we slightly modify Gauss's algorithm to say: if $|b_2'| \geq (1-\epsilon)\,|b_1|$, we stop, else, we swap them and repeat the procedure, where ϵ is any positive constant, then the length of the shortest basis vector falls by a factor at least $(1-\epsilon)$ each iteration and so it is easy to prove that the number of iterations of the algorithm is $O(\log_2 |b_1^{(0)}|)$ where $b_1^{(0)}$ is the initial b_1. Thus, the running - time is bounded above by a polynomial. In this case, the basis b_1, b_2 at the end satisfies :

$$|b_2| \geq (1-\epsilon)|b_1| \quad ; \qquad |b_2.b_1| \leq |b_1.b_1|/2$$

whence we have also $|b_2^*| \geq \sqrt{(1-\epsilon)^2 - (1/4)}\ |b_1|$.

2.6 Basic computational problems on lattices

The following basic questions on lattices are all solvable in polynomial-time (in any variable number of dimensions) when the data are rational numbers.

1). **Membership**: Given a set (of possibly) dependent vectors $b_1, b_2 \ldots, b_n$ and another vector v; find if v is an integer linear combination of $b_1, b_2 \ldots, b_n$.

2). **Homogeneous equations:** Given a system of homogeneous linear equations $A\,x = 0$ find a basis of the lattice $L = \{x : A\,x = 0$; each component of x is an integer $\}$. L is a lattice since it is closed under subtractions and it is discrete.

3). **Finding a basis:** Given a set $b_1,\ b_2 \ldots, b_m$ (of possibly dependent) vectors, find a basis of the lattice L of all integer linear combinations of $b_1 \ldots, b_m$. (We need the rationality of $b_1, b_2 \ldots, b_m$ to argue that L is discrete and hence a lattice; consider, for example, the set of all integer linear combinations of $\sqrt{2}$ and 1 on the real line.)

The first problem was solved by von zur Gathen and Sieveking [18] who gave a polynomial-time algorithm to solve a system of linear diophantine equations. Problem 2 was independently solved by Kannan and Bachem [32] and Voytakov and Frumkin [64]. A solution to 3 follows as a simple corollary to the procedures developed in either of these two papers. The solution of [32] involves finding a "triangular" basis of a lattice (or the so-called Hermite normal form of a matrix) which we describe below since it has other applications, for example, in Lenstra's algorithm to handle non full-dimensionality of the given polytope.

It is a classical result of Hermite that every n-dimensional sublattice of $\mathbf{Z}^n$ (the elements of $\mathbf{R}^n$ with integer coordinates) has a basis $b_1, b_2 \ldots, b_n$ where $b_i \cdot e_j = 0$ for $j \le i-1$. ($e_1 \ldots, e_n$ are the unit vectors along the coordinate axes.) Thus if the vector $b_1,\ b_2, \ldots, b_n$ are represented as the rows of an $n \times n$ matrix, it is upper triangular, and so will call this basis a triangular basis of the lattice. Such a basis exists whenever the lattice only contains vectors with rational coordinates and does not in general when the coordinates are real. The first fact is Hermite's theorem and follows from the fact that $\mathbf{Z}$ is a Euclidean ring. To see the second statement, consider, for example, the lattice in $\mathbf{R}^2$ with basis vectors $(\sqrt{2}\ 1)$ and $(1\ \sqrt{2})$.

Suppose B is any given basis matrix of a lattice $L \subseteq \mathbf{Z}^n$. By Hermite's theorem, there is a unimodular matrix U such that UB is upper triangular. With some additional technical conditions, we can ensure the uniqueness of UB, this unique matrix is called the Hermite normal form of the matrix B. Hermite's proof was constructive and led directly to an algorithm . The main difficulty in deriving a polynomial-time algorithm was to keep the sizes (number of bits) of all numbers bounded by a polynomial in the length of the input. This was first accomplished in [32]. Several polynomial-time algorithms are now known. ([5], [11], [27]) The normal form as well as the algorithm can be extended to rectangular matrices with possibly dependent rows. More precisely, given a $m \times n$ matrix B of integers, we can find in polynomial-time a unimodular $m \times m$ matrix U and a permutation matrix P such that for $i = 1, 2, \ldots, m$, the i^{th} row of UBP has its first min $(i-1,\ n)$ entries equal to 0. All three problems mentioned at the beginning of this subsection can be solved in polynomial-time using this. We only touch upon (2).

Given the $m \times n$ matrix A of problem (2), let B be its transpose and find U, P as in the last paragraph. Let C be the transpose of UBP. C is lower triangular and $C = P^t A V$ with ($V = U^t$). So

$$L = \{x : Ax = 0;\ x \in \mathbf{Z}^n\} = \{V\,y : C\,y = 0;\ y \in \mathbf{Z}^n\}$$

(since V, V^{-1} have integer entries). So it suffices to find a basis for $L' = \{y : C\,y = 0, y \in \mathbf{Z}^n\}$. If C has rank γ, it is easily checked (by the lower-triangularity of C) that $\{e_{\gamma+1},\ e_{\gamma+2},\ \ldots e_n\}$ for a basis of L'. (If $\gamma = n,\ L' = \{0\}$, of course).

2.7 Rounding convex bodies

In integer programming, as well as in general, it is useful to transform given convex bodies into "well-rounded" ones. We will make this precise presently. It is a classical theorem of John that if K is any convex body in $\mathbf{R}^n$, there is an ellipsoid E such that E is contained in K and the dilation of E about its center by a factor of n contains K.

In fact E can be taken to be the ellipsoid of largest volume in K. If τ is the linear transformation that sends E to the sphere S of unit radius, then $S \subseteq \tau K \subseteq S'$, where S' is concentric with S and has radius n. Unfortunately, we do not know how to find the ellipsoid E, given, say, a convex polytope K by its inequalities. Lovász [48, theorem $2 \cdot 4 \cdot 1$] has developed an ingenious polynomial-time algorithm to produce a "weak" John ellipsoid E for a polytope K; it has the property that E is contained in K and a dilation of E by a factor of $(n+1)\sqrt{n}$ contains K. This is based on Khaciyan's [37] ellipsoid algorithm for linear programming. Here is a very brief description of it : by the ellipsoid algorithm, we can find an ellipsoid F with center c such that $c \in K$ and $K \subseteq F$. Suppose the end points of the axes of F are $c \pm a_i$ (for $i = 1, 2, \ldots, n$). We check if $c \pm a_i/(n+1)$ belong to K for $i = 1, 2 \ldots, n$. If all these $2n$ points are in K, so is their convex hull Q. But Q contains the ellipsoid F' with center c obtained from F by shrinking by a factor of $1/(n+1)\sqrt{n}$. So F' would suffice as the answer. Suppose now that for example $c + a_1/(n+1)$ is not in K. Then it does not satisfy one of the inequalities describing K; we can use this inequality as a cut in the sense of the ellipsoid algorithm to produce a new ellipsoid $\hat{F}$ so that again $\hat{F} \supseteq K$. If the center $\hat{c}$ of $\hat{F}$ does not belong to K, we use a cut passing through the center to get a smaller ellipsoid; if $\hat{c} \in K$, we apply the same procedure to $\hat{F}$ that we did to F. It is not difficult to see that either cut reduces the volume of the ellipsoid by a factor and this guarantees polynomial-time termination. At the end of the process, we must clearly have an ellipsoid with the required properties.

The transformation that sends the final (concentric) ellipsoids into spheres, makes the polytope K well-rounded in the sense of the following definition.

Definition : A convex body K in $\mathbf{R}^n$ is well-rounded if there are two concentric spheres S and S' of radii r and r' such that

$$S \subseteq K \subseteq S' \qquad r/r' \leq (n+1)\sqrt{n}$$

Such a process can be carried out not only for polytopes, but closed convex sets K described only by a "separation oracle" of Grötschel, Lovász and Schrijver [21] . The separation oracle for K is a black box which when presented with y, either says $y \in K$ or gives a hyperplane $c \cdot x = c_o$ which separates y and K.

3 The Lovász Basis Reduction Algorithm

3.1 Definition of Lovász reduced basis, the algorithm

As we mentioned earlier, the complexity of the SVP is unknown. Clearly, no polynomial-time is known for finding either the Minkowski-reduced or the $K-Z$ reduced bases. In fact, it is easy to see that finding a Minkowski-reduced basis is NP-hard. $K-Z$ reduced bases can be found by repeatedly finding shortest non-zero vectors in projected lattices, so the problem of finding a $K-Z$ reduced basis is polynomial-time (Cook) equivalent to the SVP; so its complexity is open. The question is to find a suitable definition of a "reduced basis" that has the following desirable properties: it has a low orthogonality defect; the shortest vector in the basis is approximately a shortest vector in the lattice; and the reduced basis can be found in polynomial-time. The basis reduction algorithm presented in Lenstra, Lenstra and Lovász [46] accomplishes all these. We will slightly modify their definition and the algorithm (but keeping the spirit of it) for ease of presentation. Choose any δ in the interval $(0\ \frac{\sqrt{3}}{2})$. Suppose $b_1, b_2 \ldots, b_n$ are linearly independent and generate a lattice L. Let $b_1^*, b_2^* \ldots, b_n^*$ be the orthogonal basis of the vector space spanned by L obtained by doing the Grahm-Schmidt procedure on $b_1, b_2 \ldots, b_n$. (Of course the b_i^* may not belong to L.) The basis $b_1, b_2 \ldots, b_n$ of L is called a reduced basis if it is proper (cf section 2.3) and for each i, $1 \leq i \leq n-1$,

$$|b_{i+1}^*| \geq \delta |b_i^*|$$

Again, it is easier to conceptualize it in terms of the lower triangular representation of the basis matrix. A basis is Lovász reduced if it is proper and for all i, $b_{i+1,i+1} \geq \delta b_{ii}$. It is easy to show that every K-Z reduced basis is also Lovász reduced : from the definition of K-Z reduced, we have $(b_{i+1,i})^2 + (b_{i+1,i+1})^2 \geq (b_{ii})^2$ since, b_{ii} is the length of the shortest vector in the lattice generated by the bottom right $(n-i+1) \times (n-i+1)$ submatrix of the basis matrix. Properness implies $|b_{i+1,i}| \leq |b_{ii}|/2$, so we have $b_{i+1,i+1} \geq (\sqrt{3}/2) b_{ii}$. This should also explain the reason for choosing δ in the interval $(0\ \ \sqrt{3}/2)$.

First we will argue that a Lovász reduced basis has the desired properties and then give the algorithm for finding it. For ease of exposition, we take δ to be $1/2$, although any δ in the interval $(0\ \sqrt{3}/2)$ would do just as well. First, note that we obviously have

$$(*)\quad |b_j^*| \leq |b_i^*|\, 2^{i-j}\ \forall\ 1 \leq j \leq i \leq n$$

Any non-zero vector v in L must be of the form $\sum_{i=1}^{j} \lambda_i\ b_i$ with $\lambda_j \neq 0$ and $\lambda_i \in \mathbf{Z}$, so $|v| \geq |\lambda_j|\, |b_j^*| \geq |b_j^*| \geq |b_1^*|\, 2^{1-j}$. So we have $|b_1^*| = |b_1| \leq 2^n \Lambda_1(L)$. Next we will bound the orthogonality defect. By properness,

$$|b_i| \leq \left(|b_i^*| + \frac{1}{2} \sum_{j=1}^{i-1} |b_j^*| \right) \leq 2^n\, |b_i^*| \quad \text{by}(*)$$

Multiplying together the n such inequalities, it follows that the orthogonality defect is at most 2^{n^2}. (We have not taken care to present the sharpest estimates.)

We will give the algorithm again assuming $\delta = 1/2$. Pick any positive $\epsilon < 1$ satisfying $\delta^2 + 1/4 < (1-\epsilon)^2$. For convenience, let $\epsilon = (1 - \sqrt{3}/2)$. We need some notion: Suppose $b_1, b_2 \ldots, b_n$ is the current basis of the lattice. Let V_i be the vector space spanned by $b_1 \ldots, b_i$ (for $i = 1, 2 \ldots, n$) and $V_0 = \{0\}$ and for any vector v, denote by v/V_i the component of v orthogonal to V_i. We proceed as follows: For the current basis $B = \{b_1, b_2 \ldots, b_n\}$, we compute $b_1^*, b_2^* \ldots, b_n^*$ by Grahm -Schmidt process. Suppose for some i, $|b_{i+1}^*| < |b_i^*|\big/2$. We run the modified - Gauss - algorithm with $\epsilon = (1 - \sqrt{3}/2)$ on $b_i\big/V_{i-1} = x$ (say) and $b_{i+1}\big/V_{i-1} = y$ (say); let u and v be the reduced basis obtained at the end; let U be the 2×2 unimodular matrix so that

$$U \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$$

$$\text{Let } \begin{pmatrix} \hat{b}_i \\ \hat{b}_{i+1} \end{pmatrix} = U \begin{pmatrix} b_i \\ b_{i+1} \end{pmatrix}.$$

Obviously, $\hat{B} = \{b_1,\ b_2 \ldots, b_{i-1},\ \hat{b}_i,\ \hat{b}_{i+1}, b_{i+2}, \ldots, b_n\}$ is a basis of L; we replace the current basis with this and repeat this process until $|b_{i+1}^*| > |b_i^*|/2$ is satisfied for all i. Finally, we render the basis proper by ensuring for $i = 1, 2 \ldots, n$ (in that order) that $b_i - b_i^*$ belong the rectangle

$\{\sum_{j=1}^{i-1} \alpha_j\, b_j^* : -\frac{1}{2} < \alpha_j \leq \frac{1}{2}\}$: for each i, this is a accomplished by subtracting suitable (integer) multiples of $b_{i-1},\ b_{i-2}\ldots, b_1$ (in that order) from b_i. This process does not affect any of the b_i^*, so at the end, the basis is reduced.

Again, it is useful to go to the lower triangular representation of the basis matrix to understand the process to make the basis proper. To make the basis proper, we wish to make each off-diagonal entry at most half the diagonal entry in its column. This is easily seen to be acieved by doing the following : for $i = 1, 2\ldots, n$, subtract from row i a suitable integer multiple of row j for $j = i-1, i-2\ldots 1$ in that order. The lower triangularity ensures that subtraction of a multiple of row j from row i does not affect the i, k entries for $k > j$. Of course, the whole process does not change the diagonal entries as claimed.

We have to argue polynomial-time termination. This is obvious for the final stage of making the algorithm proper. For the first stage of ensuring $|b_{i+1}^*| \geq |b_i^*|/2$, we proceed as follows: Each modified -Gauss algorithm runs in polynomial-time as argued before and at the end of the procedure, we have (arguing as in section 2.5) $|v| \geq (1-\epsilon)\,|u| = \sqrt{3}|u|/2$. Further, the component of v along the direction of u is at most $|u|/2$, so the component z of v orthogonal to u is at least $|u|/\sqrt{2}$. Letting $b_1^*\ldots, b_{i-1}^*,\ \hat{b}_i^*,\ \hat{b}_{i+1}^*,\ b_{i+2}^*\ldots, b_n^*$ denote the orthogonal basis corresponding to $\hat{B}$, we see that $|\hat{b}_{i+1}^*| = |z|$ and $|\hat{b}_i^*| = |u|$, so $|\hat{b}_{i+1}^*| \geq |\hat{b}_i^*|/\sqrt{2}$. Further, of course $|b_i^*|\,|b_{i+1}^*| = |\hat{b}_i^*|\,|\hat{b}_{i+1}^*|$ and before the Gauss procedure, we had $|b_{i+1}^*| < |b_i^*|/2$. Combining these three inequalities, we see that $|\hat{b}_i^*| < |b_i^*|/2^{1/4}$.

To complete the proof, consider the quantity

$$D = \prod_{i=1}^{n} |b_i^*|^{(n-i)}$$

We have argued that D falls by a factor of at least $2^{1/4}$ at each iteration; then combined with upper and lower bounds on D, it is not difficult to show that the number of iterations is bounded by a polynomial in the length of the (rational) data. It is more difficult (but only a technical matter) to show that the sizes (number of bits) of all numbers are bounded by a polynomial in the length of input; we do not give this proof here.

3.2 Remarks on the algorithm and time analysis

We proved bounds on the length of the first vector in a Lovász reduced basis and the orthogonality defect. The question arises : are these the best possible bounds ? The answer is nearly yes as the following example shows. Consider the lattice generated by the rows of a lower triangular matrix B defined by : $B_{ij} = 0$ for $j > i$; $B_{ii} = \rho^{i-1}$ and $B_{ij} = \rho^{j-1}/2$ for $i > j$ where $\rho = \sqrt{3}/2$. It is easily checked that this is a Lovász reduced basis for any choice of δ. The length of each basis vector is 1. The determinant of the lattice is $\rho^{n(n-1)/2}$, so the orthogonality defect is the reciprocal of this. By Minkowski's theorem there is a nonzero vector in the lattice of length at most $\sqrt{n}\rho^{n-1}/2$, so each of the basis vectors is off by an exponential factor. The same applies when any subset of the entries of the basis matrix is multiplied by -1.

The time analysis of the basis reduction algorithm is in terms of two parameters : n, the dimension of the lattice and B the maximum length of one of the initial basis vectors which are all assumed to have integer entries. Let us first consider the number of calls to the Gauss procedure : the initial value of D is at most B^{n^2} and it is always an integer; so the number of calls is at most $O(n^2 \log B)$. The actual implementation proposed by the Lenstra, Lenstra and Lovász paper is different from the description here - it actually does not call the Gauss procedure as a subroutine, but goes into the guts of it. More importantly, they do not perform Gram-Schmidt procedure after each change of basis, but update the orthogonal basis. Also, they continually keep the basis proper to avoid large numbers. With these modifications, they show that a reduced basis may be found using $O(n^4 \log B)$ operations on operands of size $O(n \log B)$. It can be shown that the algorithm as we have described it in the last section also takes polynomial number of operations on polynomial size operands, but the complexity will not be as good. Recently, the complexity of the basis reduction algorithm has been improved to $O(n^4 \log B)$ operations on $O(n+\log B)$ bit integers [59]. See also [29] and [60].

4 Lenstra's algorithm for integer programming

The integer programming optimization problem is the problem of maximizing (or minimizing) a linear function $c \cdot x$ over the integer points (points of Y) in a polyhedron P in $\mathbf{R}^n$ described by a set of linear inequalities with rational coefficients. This problem can be polynomial-time reduced to the integer programming feasibility question: given a polyhedron P, determine whether P contains an integer point in it. Further it has been shown [19] that if P does contain an integer point, then it must contain one whose coordinates have sizes (number of bits) bounded by a polynomial in the length of description of P; so adding these bounds, we may assume that P is a polytope (a bounded polyhedron). Further, we may assume that P has non-zero volume: if necessary, restrict to the affine subspace of $\mathbf{R}^n$ spanned by P and use unimodular transformations to transform the lattice into the standard one. This can be done in polynomial-time using the Hermite Normal Form algorithm of [32]. Lenstra [47] describes these technical matters in detail. So by integer programming, we will henceforth mean the problem of determining whether a polytope P in $\mathbf{R}^n$ of non-zero volume has an integer point in it.

This problem is known to be NP-hard in general [35]. However, the question of interest was to find a polynomial-time algorithm for the problem when n, the number of dimensions is fixed. For $n = 2$, algorithms were given in [26], [30], and [57]. In an important breakthrough, Lenstra [47] used ideas from the Geometry of Numbers to solve the problem for general (fixed) n. To describe his algorithm, we introduce some terminology.

Suppose K is a convex body (set of non-zero volume) in $\mathbf{R}^n$. The difference body of K written $(K - K)$ is the body $\{x - y : x, y \in K\}$ and the dual (body) of K written K^* equals $\{v : v \cdot x \leq 1 \text{ for all } x \text{ in } K\}$. Thus if K is a closed and bounded convex body, $(K - K)^*$ is precisely the set of all vectors v such that the "width" of K along v $(= \max\{v \cdot x : x \in K\} - \min\{v \cdot x : x \in K\})$ is at most 1. For fixed n, Lenstra gave a polynomial-time algorithm that accomplishes the following: it either finds an integer point in the given polytope P or finds an *integer vector* v in $c^{n^2}\,(P - P)^*$, (incidentally proving that such a vector exists if $P \cap \mathbf{Z} = \emptyset$) where c is an absolute constant[2]. We will presently describe this algorithm; but note that v has the following property: every integer point must lie on a hyperplane H of the form $\{x : v \cdot x = z,\}$, z an integer; further $\max\{v \cdot x : x \in P\} - \min\{v \cdot x : x \in P\} \leq c^{n^2}$, so at most $c^{n^2} + 1$ such hyperplanes H intersect P. So it suffices to determine for these H, whether $P \cap H$ contains an integer point. The $P \cap H$ are all $(n-1)$-dimensional polytopes, so we have reduced the n-dimensional problem to $c^{n^2} + 1$ problems in $(n-1)$ dimensions giving a recursive procedure for integer programming. The factor c^{n^2} has gone through several improvements to be described in section 7.

It is conceptually easier to first describe Lenstra's algorithm assuming P is an ellipsoid, then do it for polytopes. For an ellipsoid E, there is an invertible linear transformation τ that sends E into a sphere S of unit radius. Clearly, $E \cap Y$ is non-empty iff $S \cap \tau Y$ is. (Y is the standard lattice of integer points.) Using the basis-reduction algorithm of the last section, we find a reduced

[2] Reminder on notation : For a convex body S and a positive real number t, tS denotes the set $\{x : x/t \in S\}$

basis $b_1,\ b_2\ldots,\ b_n$ of τY. Renumber the basis vectors if necessary so that $|b_n|\ \geq\ |b_i|\forall i$. Let the center of S be $c\ =\ \sum_{j=1}^{n}\ \alpha_j\ b_j$ where the α_j are reals.

If $[\alpha_j]$ is the integer nearest to α_j, then $c'\ =\ \sum\ [\alpha_j]\ b_j$ belongs to τY and further $|c-c'|\ \leq\ \sum\ |b_j|/2\ =\ M$ (say). So if the radius of $S(=1)$ is at least M, clearly c' is in S, so E contains a point of Y namely $\tau^{-1}c'$. On the other hand, if M is greater than 1, we will show the existence of a v in $(c^{n^2}\ (E-E)^*\ \cap Y)$. Suppose $M>1$. Let V be vector space spanned by $b_1,\ b_2\ldots,b_{n-1}$ and consider the family of hyperplanes $V+zb_n,\ z\ \in\ \mathbf{Z}$. These cover τY and further the distance between 2 adjacent such planes is $|b_n^*|$ where b_n^* is the component of b_n orthogonal to V. Then, letting $L'\ =\ L(b_1,b_2,\ldots,b_{n-1})$, and using the fact that the basis $b_1,\ldots\ b_n$ is reduced,

$$\prod_{i=1}^{n}|b_i|\ \leq\ 2^{n^2}\ d(\tau Y)\ \leq\ 2^{n^2}\ |b_n^*|\ d(L')\leq\ 2^{n^2}\ |b_n^*|\ \prod_{i=1}^{n-1}|b_i|$$

$$\text{So}\quad |b_n^*|\ \geq\ 2^{-n^2}\ |b_n|\ \geq\ \frac{2M}{n2^{n^2}}\ \geq c_o^{-n^2}$$

for a suitable constant c_o. Thus we see that the number of hyperplanes of the sort $V+z\ b_n,\ z\ \in\ \mathbf{Z}$ that intersect S is at most c^{n^2}, c constant. Now applying τ^{-1}, we see that $\{\tau^{-1}V\ +\ z\tau^{-1}b_n\},\ z\ \in\ \mathbf{Z}$ cover Y, and at most c^{n^2} elements of this family intersect E; this gives us a v - namely the normal to $\tau^{-1}V$ that makes a unit dot product with $\tau^{-1}b_n$. Indeed, it is easy to see that $v\ =\ \tau^t\ b_n^*/|b_n^*|^2$ where τ^t is the transpose of τ. The fact that the family of hyperplanes $\{x\ :\ v\cdot x\ =\ z\}\ z\in\mathbf{Z}$ covers Y implies that the components of v must be integers. In 1 dimension, the problem can be easily solved. This completes the description of Lenstra's recursive algorithm for ellipsoids. Note that equivalently, we have described an algorithm that given a sphere in $\mathbf{R}^n$ and a general lattice $L\ =\ (\tau Y$ for some linear transformation $\tau)$, finds either a point of L in the sphere or reduces the problem to lower dimensional ones.

For a general polytope P we proceed as follows to determine whether $P\cap Y$ is nonempty : We apply the Lovász algorithm (of section 2.7) to determine a weak - John ellipsoid E for P, i.e, an ellipsoid E such that $E\subseteq P$ and a dilation E' of E by a factor of $(n+1)\ \sqrt{n}$ (about the center) contains P. By our preceding algorithm, we either find a point of Y in E (hence in P) or find a integer vector v such that the width of E along v is at most c^{n^2}. Clearly, then, the width of E' along v is at most $c^{n^2}\ (n+1)\ \sqrt{n}\ \leq\ d^{n^2}$ for some constant d. Thus the width of P along v is at most this too and we again have a reduction to lower dimensional problems.

This completes the description of Lenstra's algorithm for polytopes ; the proof of the polynomial-time bound is technical, but straight-forward; the interested reader is referred to Lenstra's paper.

It is possible to see that the same procedure can be carried out for all convex bodies described by a separation oracle (cf section 2), not just polytopes. Using this, it is not difficult to see that mixed integer programming problem with a fixed number of integer variables can be solved in polynomial time; this generalizes Khaciyan's polynomial time algorithm for the case when the number of integer variables is zero.

The theoretical foundations of the Lenstra algorithm have been studied further; they can formulated in terms of the dual lattice and the dual convex body. We do so more fully in a later section.

5 Faster algorithms for Integer Programming and other lattice problems

5.1 Introduction

In this section, we will examine faster ways of solving integer programs as well as other lattice problems: shortest vector problem, its "inhomogeneous version" called the closest vector problem (to be defined).

As we remarked in section 2.3, the SVP may be solved once we have a basis of low orthogonality defect. Since the Lovász basis reduction algorithm gives such a basis (of orthogonality defect at most 2^{n^2}), the SVP may be solved by enumerating at most 2^{n^3} candidates. Kannan [31] showed that with a "partial" $K-Z$ reduced basis on hand, only $(O(n))^{n/2}$ candidates need to be enumerated; further the "partial" $K-Z$ reduced basis may be found by $K-Z$ reducing lower dimensional lattices. The overall dependence of the complexity of SVP on n is $O(n^n)$. A similar complexity is achieved for the so-called closest vector problem in the paper. The paper deals also with integer programming. Instead of looking for a few hyperplanes cutting the polytope, this algorithm looks for affine subspaces of arbitrary dimension. Using a $K-Z$ reduced basis, it either finds an integer point in the given polytope P(in $\mathbf{R}^n$) or finds for some i, (chosen by the algorithm), $1 \leq i \leq n$ an $(n-i)$ dimensional subspace of $\mathbf{R}^n$ such that its translates cover $\mathbf{Z}^n$ and at most $(2n)^{\frac{5}{2}i}$ such translates intersect P. Thus an n-dimensional problem is reduced to $(2n)^{\frac{5}{2}i}$ problems each in $(n-i)$ variables paying a polynomial factor $O(n^{5/2})$ per variable instead of an exponential one as in Lenstra's algorithm. These results are described in this section in some detail. Helfrich [24] has made some improvements in the algorithms of this paper.

The closest vector problem (CVP) is: given linearly independent vectors $b_1,\ b_2\ldots,\ b_n$ in $\mathbf{R}^n$ and a vector b, find the closest (in Euclidean distance) vector to b in $L(b_1,\ b_2\ldots,\ b_n)$. Unlike the SVP, this problem is known to be NP-hard [63 ,31].

5.2 The algorithms

First, we look at (simplified versions of) the algorithm of [31]. For the SVP, the algorithm first finds a basis $b_1,\ b_2\ldots,\ b_n$ so that three conditions are met:

(1) With $V_1 =$ Span $\{b_1\}$, $b_2/V_1,\ b_3/V_1,\ldots,b_n/V_1$ form a $K-Z$ reduced basis for the $(n-1)$-dimensional lattice they generate. (Reminder on notation : b/V is the component of b orthogonal to the subspace V.)

(2) $|b_2^*| \geq \delta\ |b_1|$ where δ is some fixed constant in $(0\ \sqrt{3/2})$. Say $\delta = 1/2$ for convenience.

(3) The basis is proper. (cf section 2.3)

(1) Can be achieved by applying (recursively) the procedure for lower dimensional lattices. Properness can be now acieved without violating (1) as mentioned in section 2. If now (2) is violated replace b_2 by $b_2 - [\frac{b_2.b_1}{b_1.b_1}]b_1$ and then swap b_1 and b_2 and redo (1); it is clear by the geometric decrease in $|b_1|$ that this calls for only polynomially many iterations. With this basis on hand, we show that only a "few" candidates need to be enumerated to find a shortest vector of L.

Let $b_1^*,\ b_2^*,\ldots,b_n^*$ be the vectors obtained by doing Grahm -Schmidt process on $b_1,\ b_2\ldots,\ b_n$ satisfying (1), (2) and (3). Suppose $v = \sum_{i=1}^n \lambda_i\ b_i$ is a shortest non-zero vector in L. If $\lambda_j \neq 0$ for some j, then v has a non-zero component orthogonal to $V_{k-1} =$ span$\{b_1\ldots,b_{k-1}\}$ for every $k \leq j$ and so by (1), $|v| \geq |b_k^*|$. Thus we may assume, without loss of generality, that $|b_j^*| \leq |b_1|\ \forall j$, else we can discard $b_j,\ b_{j+1},\ldots,\ b_n$. It is clear that $|v| \geq |\lambda_n|\ |b_n^*|$. Of course, we must have $|v| \leq |b_1|$. So $|\lambda_n| \leq |b_1|/|b_n^*|$. Thus, there are at most $1+2|b_1|/|b_n^*|$ "candidates" for λ_n in finding v. In a similar vein, it can be argued that the number of candidates for λ_i once $\lambda_{i+1},\ \lambda_{i+2}\ldots,\lambda_n$ are fixed is at most $1 + 2|b_1|/|b_i^*| \leq 3|b_1|/|b_i^*|$. (This uses the fact that $|b_i^*| \leq |b_1|$.) We thus have a total of at most

$$\prod_{i=1}^{n} 3|b_1|/|b_i^*|$$

candidates. The denominator is $d(L)$, so by Minkowski's convex body theorem, we would have a bound on the whole quantity if we could assert $|b_1| \leq s\ \Lambda_1(L)$ where s is small (cf section 2.2). This is indeed the case: either $v = b_1$ whence $|b_1| = \Lambda_1(L)$ or $v = \sum \lambda_i\ b_i$ with one of $\lambda_2,\ \lambda_3 \ldots,\ \lambda_n$ non-zero whence by the preceding argument, $|v| \geq |b_2^*| \geq 1/2|b_1|$. In any case, $|b_1| \leq 2\Lambda_1(L)$. This gives a bound of $6^n\ n^{n/2}$ on the number of candidates (since $\Lambda_1(L) \leq \sqrt{n}(d(L))^{1/n}$). We may enumerate all these candidates and take the one that yields the shortest nonzero vector. To complete the recursive procedure, we must find an entire $K - Z$ reduced basis, which of course is easily done by taking any basis containing the shortest nonzero vector in the lattice as the first vector and ensuring (1) one more time. There are many technical details for which the reader is referred to the paper . The time bound proved in the paper is $O(n^n\ s)$ arithmetic operations (additions, subtractions, multiplications, divisions and comparisons of two rational numbers) on operands of size $O(n^2\ s)$ where s is the length of the original input basis. The upper bound on the size of the operands in this as well as many of the algorithms described in this paper turns out to be very complicated, but purely technical. We have omitted all such proofs in this brief article, however, they are quite important for algorithms that manipulate numbers.

Now we consider the inhomogeneous version - the CVP. Here, given a sphere S of radius, say, r and a lattice L, we wish to determine whether $S \cap L$ is nonempty. First find an $K - Z$ reduced basis $b_1, b_2 \ldots, b_n$ of L. Let

$$|b_i^*| = \max\{|b_j^*| : j = 1, 2 \ldots, n\}$$

If $r \geq \sqrt{n}\ |b_i^*|$, it is easy to argue that S contains a point of L. (indeed, to any point p in space, there is a point p' of L such that $|p - p'| \leq \frac{1}{2}(\sum |b_j^*|^2)^{1/2}$). So assume not. Let H be the subspace of $\mathbf{R}^n$ spanned by $b_1, b_2, \ldots, b_{i-1}$. An argument similar to one used to bound the number of candidates to find the SVP now shows that the number of translates of H containing integer points that intersect S is at most

$$\prod_{j=i}^{n} (1 + 2r/|b_j^*|) \cdot$$

(Any translate of H that contains an integer point is of the form $H + \sum_{j=i}^{n} \lambda_j b_j$ where λ_j are integers. Thus, the idea is to bound the number of "candidates" for $\lambda_i, \lambda_{i+1}, \ldots \lambda_n$ such that the distance between the centre of S and the affine set $H + \sum_{j=i}^{n} \lambda_j b_j$ is at most r.) Using the bound $r \leq \sqrt{n}\ |b_i^*|$ and Minkowski's convex body theorem, we see that this number is bounded by

$$(2n + \sqrt{n})^{n-i+1}$$

Once a candidate $\lambda_i, \lambda_{i+1}, \ldots \lambda_n$ is fixed, it clearly suffices to find the point of $(H + \sum_{j=i}^{n} \lambda_j b_j) \cap L$ closest to c' the projection of c into this affine set. This is a $i - 1$ dimensional CVP. Thus an n-dimensional CVP is reduced to this many $(i - 1)$ dimensional $CVP's$.

For integer programming, such an argument is extended to polytopes from spheres by using Lovász's rounding algorithm just as Lenstra's approach does.

This method of bounding the number of candidates will be used later in section 7 to solve the approximate version of the CVP. It will be useful for that purpose to formulate the result as follows

: the number of candidates that we need to enumerate the solve the CVP for a lattice L, given a basis $b_1, b_2, \dots b_n$ is bounded above by

$$\prod_{j=1}^{n}(1 + \left\lfloor(\sum_{k=1}^{j}|b_k^*|^2)^{1/2}/|b_j^*|\right\rfloor).$$

It is also clear that we can replace $(\sum_{k=1}^{j}|b_k^*|^2)^{1/2}$ by any other upper bound on the distance from any point in span $(b_1, b_2, \dots b_j)$ to the lattice $L(b_1, b_2, \dots b_j)$.

6 Applications of the basis reduction algorithm

6.1 Introduction

As mentioned earlier, the basis reduction algorithm has a wide range of applications. We will describe some of these in this section. To cover more ground, we begin with an annotated bibliography of the papers.

A.K.Lenstra [45] reduced the problem of factorization of polynomials with rational coefficients into irreducible factors over the rationals to the problem of finding short vectors in lattices. The Lenstra, Lenstra, Lovász [46] paper shows that the Lovász basis reduction algorithm finds short enough vectors to give a polynomial time algorithm for factorization. A variant of this method independently due to Schönhage [60] and Kannan, Lenstra and Lovász [33] is described in section 6.3.

Lenstra, Lenstra and Lovász [46] show that the classical problem of simultaneous diophantine approximation can be approximately solved by the basis reduction algorithm in polynomial time. This is described in section 6.1.

Shamir [61] cracked the famous Merkle-Hellman crypto system.

Lagarias and Odlysko [42] considered "low-density " subset sum problems . Suppose $a_1, a_2, \dots a_n$; b are integer coefficients and we wish to solve the subset sum problem : $\sum_{i=1}^{n} a_i x_i = b$; $x_i \in \{0, 1\}$. They show that if the a_i are uniformly and independently distributed in the range $[0 \quad M]$ and *there is guaranteed to be a solution to the problem*, then with high probability, we can find one in polynomial time provided $M > c^{n^2}$ where c is a constant. Nothing can be said of the cases when there is no solution. Frieze [14] considerably simplified and improved their result. Furst and Kannan [16] show that there is a nondeterministic polynomial time algorithm that will yield proofs of *infeasibility* for all but a vanishing fraction of the infeasible subset sum problems when the a_i are integers in the interval $[0 \quad M]$ provided M is greater than c^n, c a constant. Further, they show that when the a_i are in the interval $[0 \quad N]$, with $N > c^{n^2}$, there is a deterministic polynomial time algorithm that will determine for all but a vanishing fraction of the problems whether or not they are feasible and if feasible, find a solution.

Landau and Miller [43] devised a polynomial time algorithm for the classical problem of solvability by radicals - given a polynomial with integer coefficients, determine if the roots equal expressions involving $+, -, \times, /, \sqrt[n]{}$ for arbitrary natural numbers n and the integers.

Hastad, Just, Lagarias and Schnorr [23] gave a polynomial time algorithm that given a vector x with n components, finds a n vector v of integers not all zero such that $v \cdot x = 0$ and whenever $u \cdot x = 0$, u integral and nonzero, $|v| \leq 2^n|u|$; or determines that no nonzero integral vector u exists such that $u \cdot x = 0$. Here, x is a vector of reals given as an oracle.

Frieze, Hastad, Kannan, Lagarias and Shamir [15] give a polynomial time algorithm that with high probability reconstructs the values of the variables $x_1, x_2, \dots x_n$ given some linear congruences satisfied by the variables and some bits obtained by truncating the binary expansions of the values of the variables. This algorithm is essentially optimal in the use of information in that it will solve problems with high probability as soon as the variables become uniquely determined by their constraints. They have some cryptoanalytic applications of this algorithm.

Frank and Tardös [13] give a method of approximating linear inequalities by so as to preserve "small" integer solutions. Their method is described in section 6.4.

Lovász and Scarf [49] use the results described in section 7 to prove some structural results about integer programming.

6.2 Simultaneous diophantine approximation

Suppose $\alpha_1,\ \alpha_2 \ldots, \alpha_n$ are an arbitrary set of real numbers. For many applications, it is interesting to approximate them by n rationals $p_1/q, p_2/q \ldots, p_n/q$ all with the same (integer) denominator q. This is the problem of simultaneous diophantine approximation. More precisely, we ask given reals $\alpha_1, \alpha_2 \ldots, \alpha_n, \epsilon > 0$ and a natural number Q, when is it possible to prove the existence of integers $p_1, p_2 \ldots, p_n$ and q so that $O < \ q\ \leq Q$ and

$$|\alpha_i - p_i/q|\ \leq \epsilon/q\ \ \forall i$$

Writing the inequalities as $|q\alpha_i - p_i| \leq \epsilon$ and with the change of variables $p'_i = -p_i$, we see that the requirements can be formulated as:

$$-\epsilon \leq Ax\ \leq\ \epsilon$$

where x is the vector of unknowns $(p'_1, p'_2, \ldots p'_n, q)$ and

$$A = \begin{pmatrix} 1 & 0 & 0 & . & . & . & \alpha_1 \\ 0 & 1 & 0 & . & . & . & \alpha_2 \\ 0 & 0 & 1 & . & . & . & \alpha_3 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & . & . & . & 0 & 1 & \alpha_n \\ 0 & . & . & . & . & 0 & \epsilon/Q \end{pmatrix}$$

Let P be the parallelopiped $\{x : -\epsilon \leq Ax \leq \epsilon\}$ in $\mathbf{R}^{n+1}$. Then we are asking for conditions under which P contains an integer point other than the origin (assuming $|\epsilon| < 1$). P is, of course convex and symmetric about the origin and has volume $=\ 2^{n+1}\epsilon^{n+1}/det(A)\ =\ 2^{(n+1)}\,Q\epsilon^n$. So by Minkowski's convex body theorem, we have a solution whenever $Q\ \geq\ \epsilon^{-n}$. Clearly, we can make q positive after multiplying by -1 if necessary. Dirichlet's fundamental theorem on simultaneous diophantine approximation states precisely this:

For any n arbitrary reals $\alpha_1, \alpha_2 \ldots, \alpha_n$, and two reals ϵ, Q satisfying $\epsilon > 0, Q \geq \epsilon^{-n}$, there are integers $p_1, p_2 \ldots, p_n, q$, with $0 < q \leq Q$ and $|q\alpha_i - p_i|\ \leq\ \epsilon$ for all i.

Now the question is how to find this good approximation. There is a simple and elegant reformulation of this as a question on lattices. As the vector x varies over $\mathbf{Z}^{n+1}$, Ax varies over the lattice L generated by the columns of A, so the question is to find non-zero vectors in L that have L_∞-norm at most ϵ. Obviously, this can be solved in exponential time by the algorithms of section 5 to solve the SVP in the L_∞-norm. Using the Lovász basis reduction algorithm we can find approximately L_2 -shortest vector of L, whence clearly, we can also find an approximately L_∞-shortest vector. (noting that for any vector v in $\mathbf{R}^m$, $|v|_\infty\ \leq\ |v|_2\ \leq\ \sqrt{m}|v|_\infty$). Let us work out the degree of approximation. The determinant of L is ϵ/Q, so $\Lambda_1(L)\ \leq\ \sqrt{n+1}\,(\epsilon/Q)^{1/(n+1)}$ by Minkowski 's theorem ; thus the basis reduction algorithm finds a non-zero vector v of L such that $|v|_2 \leq 2^{(n+1)/2}\sqrt{n+1}\,(\epsilon/Q)^{1/(n+1)}$ and of course $|v|_\infty \leq |v|_2$. As we argued earlier, we would like $|v|_\infty \leq \epsilon$. This would hold if

$$2^{(n+1)/2}\sqrt{n+1}\,(\epsilon/Q)^{1/(n+1)} \leq \epsilon$$

It can be checked that (except for small values of n), this is true whenever

$$Q \geq 2^{n^2}\epsilon^{-n}$$

This completes the description of the algorithm for simultaneous diophantine approximation. We will make use of the algorithm of this section in rounding integer inequalities in section 6.4. A number of other applications are discussed in [48]. In fact one of Lovász's main motivations for developing the basis reduction algorithm was to do simultaneous diophantine approximation.

6.3 Factorization of polynomials

A.K. Lenstra [45] reduced the problem of polynomial factorization to one of finding short vectors in lattices. This combined with the basis reduction algorithm, gave a polynomial-time for factoring polynomials with rational coefficients to its irreducible factors (over the rationals) [46]. Schonhage [60] and Kannan, Lenstra and Lovász [33] gave another algorithm which used the approximate roots of the polynomials in the complex plane rather than over the p-adic numbers. It is this algorithm that we outline here. We need a few definitions: A complex number α is said to be algebraic if it is the root of a polynomial with integer coefficients. There is a unique primitive polynomial (a polynomial with integer coefficients with greatest common divisor equal to 1) satisfied by each algebraic number; this is called the minimal polynomial of the number. If $f(x)$ is a polynomial with integer coefficients and with α as a root, the minimal polynomial of α is an irreducible factor of $f(x)$. It is well-known that given $f(x)$, an approximation $\bar{\alpha}$ of each root of α (so that $|\bar{\alpha}-\alpha| \leq \epsilon$, for a specified ϵ) may be found in time polynomial in the number of bits needed to represent $f(x)$ and the number of bits of the approximation, i.e. , $\lceil \log_2(1/\epsilon)\rceil$. We will show that if ϵ is suitably small, then with $\bar{\alpha}$ on hand, we may find the minimal polynomial $h(x)$ of the *actual root* α which is of course an irreducible factor of $f(x)$. For ease of description, we will initially make the assumption that we have the exact α; of course, we discard this later.

Suppose the degree of $f(x)$ is n and the (unknown) degree of $h(x)$ is $m \leq n$. It can be shown that $|h|_\infty \leq |f|_\infty 2^n$ where for a polynomial $p(x)$ with integer coefficients, $|p|_\infty$ is the maximum absolute value of any coefficient of $p(x)$. (Collins, quoted in [39], page 391)) We omit the subscript ∞ in what follows. Let $\beta_0,\ \beta_2 \ldots, \beta_m$ be the real parts of the powers of α, i.e. of $1, \alpha^1,\ \alpha^2, \ldots, \alpha^m$ respectively and let $\gamma_0,\ \gamma_1 \ldots,\ \gamma_m$ be the respective imaginary parts. Then the unknowns $h = (h_0,\ h_1 \ldots, h_m)$ (the coefficients of $h(x)$) are integers satisfying

$$|h_i| \leq 2^n\,|f|\ \forall i \qquad \sum h_i\,\beta_i = 0 \qquad \sum h_i\,\gamma_i = 0$$

Interestingly, it can be shown that even if we relax this system to a system of inequalities below, every non-zero integer solution must be either h or an integer multiple of it:

$$|h_i| \leq |f|\,2^{2n}\ \forall i \qquad |\sum h_i\,\beta_i| \leq \delta \qquad |\sum h_i\,\gamma_i| \leq \delta \tag{$*$}$$

where $\delta = 2^{-2n^2}|f|^{-(2n)}$. (see proposition 1.6 of [33]) These can be written in matrix notation:

$$-\delta \leq A\,h \leq \delta$$

with

$$A = \begin{pmatrix} C & 0 & 0 & 0 & . & . & . & . \\ 0 & C & 0 & 0 & . & . & . & . \\ 0 & 0 & C & 0 & . & . & . & . \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ 0 & . & . & . & . & . & . & C \\ 1 & \beta_1 & \beta_2 & . & . & . & . & \beta_m \\ 0 & \gamma_1 & \gamma_2 & . & . & . & . & \gamma_m \end{pmatrix}$$

where $C = \delta/(|f|2^{2n})$.

Analogous to the last section, we consider the lattice L generated by the columns of A. We know that for the minimal polynomial $h(x)$ of α, Ah is an element of L with L_∞ - norm at most $\delta/2^n$ and that for any vector g which is not an integer multiple of h, Ag has L_∞ -norm greater than δ. This implies that a Lovász-reduced basis of L must contain as a first vector an integer multiple of Ah, which must, per force be Ah or $-Ah$ since we have a basis of L. This completes the description of how to fund h with α on hand.

Suppose we have now only an approximation $\bar{\beta}_0, \bar{\beta}_1 \ldots, \bar{\beta}_m$ to the β's and $\bar{\gamma}_0, \bar{\gamma}_1 \ldots, \bar{\gamma}_m$ to the γ's. Let $\bar{A}$ be the matrix corresponding to A with these approximations. Let $\bar{L}$ be the lattice $\bar{A}\,\mathbf{Z}^{m+1}$. Since the $\bar{\beta}$ and $\bar{\gamma}$ are close to β and $\gamma's$'s, it is possible to show that $\bar{A}h$ is a vector in $\bar{L}$ with "small" norm. Further, any integer vector g which is a not multiple of h, violates one of the inequalities of $(*)$, so it violates either one of the first $(m+1)$ inequalities or $\max(|\sum g_i\beta_i|, |\sum g_i\gamma_i|) > \delta$ whence for a suitably small ϵ, $\max(|\sum g_i\bar{\beta}_i|,\ |\sum g_i\ \bar{\gamma}_i|) > \delta - \epsilon$; in either case we can argue that $\bar{A}g$ has a "large" norm. So in a Lovász reduced basis of $\bar{L}$, the first vector must be h.

The running-time of the original factorization algorithm of Lenstra, Lenstra and Lovász was $O(n^{12} + n^9(\log|f|)^3)$ bit operations where the polynomial f to be factored had integer coefficients of maximum magnitude $|f|$ and degree n. Kaltofen [29] improved the time and Schönage [60] has further improved it is to $O(n^{6+\epsilon} + n^4(log|f|)^{2+\epsilon})$ bit operations.

Kannan, Lenstra and Lovász [33] also give an efficient algorithm for solving the following problem which they use in the factorization algorithm : given a sufficiently good rational approximation to the real and imaginary parts of an algebraic number, find the minimal polynomial satisfied by it. This shows in a natural way that the bits of an algebraic number are not random. Further, it gives a way of computing with algebraic numbers by keeping their approximations. The reader is referred to their paper for details.

6.4 Approximation of linear inequalities

Suppose we have a linear inequality $a \cdot x \leq \alpha$ with arbitrary rational coefficients. The hyperplane H corresponding to this inequality divides space into three regions - $\{x : ax > b\}, \{x : ax = b\}$ and $\{x : ax < b\}$. A natural question which turns out to have a lot of applications is: can we find a linear inequality with "small" integer coefficients that preserves the sets "small" integer points in each of three regions? More precisely, given a real $n-$ vector a, a real number α and a natural number N, we wish to find an integer vector $\bar{a}$ and an integer "right hand side" $\bar{\alpha}$ in time polynomial in the size number of bits of a, α and N so that every integer vector x with $|x|_\infty \leq N$ satisfies

$$a \cdot x > \alpha \Leftrightarrow \bar{a} \cdot x > \bar{\alpha} \qquad a \cdot x = \alpha \Leftrightarrow \bar{a} \cdot x = \bar{\alpha} \qquad a \cdot x < \alpha \Leftrightarrow \bar{a} \cdot x < \bar{\alpha};$$

further we require that $\bar{a}$ and $\bar{\alpha}$ are bounded in size (number of bits) by a polynomial in n, the number of variables and the size of N. Frank and Tardos [13] gave an algorithm to do so. We will describe their interesting algorithm in this section. First, we wish to point out that it is a little surprising that they can do this: Consider the inequality

$$x_1 + \epsilon x_2 \leq 0$$

where ϵ is a very "small" positive rational. If ϵ is small enough, it is clear that the best approximation using "small" integer coefficients to the direction of the vector $(1\ \epsilon)$ is given by the vector $(1\ 0)$. Unfortunately, the inequality $x_1 + 0x_2 \leq 0$ is a bad replacement for the original inequality. For example, $x_1 = 0, x_2 = 1$ satisfies $x_1 + \epsilon x_2 > 0$, but not $x_1 + 0x_2 > 0$. So indeed, the best approximation to the direction of the original inequality will not do; we may have to use a slightly worse approximation. If $\epsilon < 1/N$, then we see that the sign of $(N+1)x_1 + x_2$ is the same as the sign (positive, negative or zero) of $x_1 + \epsilon x_2$ for integers x_1, x_2 with $|x_1|, |x_2| \leq N$. (To see this, note that if x_1 is nonzero, the sign of both $x_1 + \epsilon x_2$ and $(N+1)x_1 + x_2$ is the sign of x_1 and if $x_1 = 0$, they are both equal to the sign of x_2).

Now we give the Frank, Tardös algorithm in general. First note that it suffices to deal with homogeneous inequalities since $a \cdot x - \alpha$ equals $(a\ \alpha) \cdot (x\ 1)$. So assume we are given the rational vector a with n components. The algorithm will find in polynomial-time an integer vector $\bar{a}$ with

$$|\bar{a}|_\infty \leq \ 2^{n^3} N^{n^2}$$

such that for all integer x with $|x|_\infty \leq N$, the sign of $a \cdot x$ equals the sign of $\bar{a} \cdot x$ (sign is positive, negative or zero). We let $f(n) = 2^{n^3} N^{n^2}$ in the sequel. We may assume that a is non-zero, so after a suitable division, we may assume $|a|_\infty = 1$, and further that $a_1 = 1$. Let $\epsilon = 1/(2Nn)$. Using the simultaneous diophantine approximation algorithm of section 6.1, find integers $p_1, p_2 \ldots, p_n, q$ such that

$$|a_i - p_i/q| \leq \frac{\epsilon}{q}$$

and

$$0 < q \leq 2^{n^2} \epsilon^{-n}$$

Clearly, we must have $p_1 = q$. Consider the vector $a^{(1)} = (1, p_2/q, p_3/q, \cdots, p_n/q)$. If x is any integer vector with $|x|_\infty \leq N$ and $a^{(1)} \cdot x \neq 0$, then we claim that the sign of $a \cdot x$ and $a^{(1)} \cdot x$ are the same: $|a^{(1)} \cdot x| \geq 1/q$ and $|a \cdot x - a^{(1)} \cdot x| \leq |a - a^{(1)}|\ |x| \ \leq \ \epsilon Nn/q \ \leq 1/2q$ establish this. So we need only worry about x's such that $a^{(1)} \cdot x = 0$. To handle this, let $a' = a - a^{(1)}$. Note that a' has at most $(n-1)$ non-zero coordinates; recursively find a integer vector v with $|v|_\infty \leq f(n-1)$ so that for all integer x with $|x|_\infty \leq N$, the sign of $v \cdot x$ and the sign of $a' \cdot x$ are the same. Our final resulting vector $\bar{a}$ will be

$$\bar{a} = 2Nnf(n-1)(qa^{(1)}) + v$$

The correctness argument is as follows: consider any integer x with $|x|_\infty \leq N$. If $a^{(1)} \cdot x \neq 0$, it is easy to see that sign of $\bar{a} \cdot x$ and the sign of $a^{(1)} \cdot x$ are the same. We have already argued that the sign of $a^{(1)} \cdot x$ and $a \cdot x$ are the same for this case. Now suppose $a^{(1)} \cdot x = 0$. Then the sign of $\bar{a} \cdot x$ equals the sign of $v \cdot x$ which equals the sign of $a' \cdot x$ which equals the sign of $a \cdot x$. To complete the argument, a simple calculation shows that $|\bar{a}|_\infty \leq f(n)$ for all but small values of n. (noting that $|a^{(1)}|_\infty = 1$.)

Frank and Tardos [13] have applied their rounding algorithm to several problems of interest to us like integer programming. In both Lenstra's algorithm and Kannan's (sections 4,5), the successive reductions to lower dimensional problems may cause the sizes of coefficients to increase nonpolynomially. Indeed, both the original papers only proved nonpolynomial bounds on the sizes; using the rounding algorithm of this section, they can be kept polynomially bounded which improves their running-time and makes them aesthetically better. The fundamental nature of the problem of rounding inequalities seems to indicate a great potential for this method. Perhaps one application of such ideas might be to develop a strongly polynomial-time algorithm for linear programming . This interesting question remains unsolved. A stronger result would be to find a polynomial-time algorithm which given a $m \times n$ system of linear inequalities $Ax \leq b$ with rational coefficients, finds $\bar{A}, \bar{b}$ with integer entries and size bounded by a polynomial in n and m such that $Ax \leq b$ is feasible if and only if $\bar{A}x \leq \bar{b}$ is. Now, $Ax \leq b$ is feasible iff there is a basic feasible solution, and every basic feasible solution has rational components with denominators bounded above by a number M which we can calculate. Unfortunately M depends on the size of A, b as well as m, n. If it depended on only m, n, we may round each of the inequalities in $Ax \leq b$ to preserve all "small" rational solutions with denominators at most M by slightly modifying the procedure that rounds preserving all integer solutions. Since this is not possible, some simultaneous rounding of all the inequalities in $Ax \leq b$ seems to be called for.

7 Structure of lattice point-free convex bodies and applications

7.1 Structural theorems

The structural result that allows the reduction of an n dimensional integer programming problem to lower dimensional ones is the fact that if K is a convex body which does not contain any integer points, then there is an integer vector v such that the "width" of K along v (=$\max\{v\,.\,x\ : x \in K\} - \min\{v\,.\,x\ : x \in K\}$) is bounded above by a function of n alone. Lenstra proved a bound of c^{n^2} as mentioned in section 4. This bound has since been improved to $O(n^{5/2})$ by Hastad [private communication] and subsequently to $O(n^2)$ by Kannan and Lovász [34]. The best known lower bound is $\Omega(n)$. It is of algorithmic as well as structural interest to analyze further convex bodies free of integer points and more generally, points of a lattice L. Such an analysis can be considered a natural extension to convex bodies that are not necessarily symmetric with respect to the origin of the so-called "transferrance" theorems of classical Geometry of Numbers [4 ,44]. We will first describe a general setting for the study. Then we will describe some of the results and connections to classical theory.

The result on the width of convex bodies free of integer points easily extends to general lattices. Suppose L is an n dimensional lattice in $\mathbf{R}^n$ and K is a convex body free of points of L. Let τ be the linear transformation that sends L into the standard lattice Y of integer points. Then, τK does not contain any integer points and thus, there is an integer vector v so that the width of τK along v is at most say $f(n)$. For any vector x in space, $v.x$ equals $\tau^t v.\tau^{-1}x$, so the width of K along $\tau^t v$ equals the width of τK along v and is therefore at most $f(n)$. By the same argument on dot products, $\tau^t v$ belongs to the dual lattice L^* (cf section 2.4) of L. So, we have proved that if K is a convex body free of points of a lattice L (this is refereed to as "L admissible" in Geometry of Numbers), then there is an element y of L^* so that the width of K along y is at most $f(n)$. There is another way to state this in terms of dual bodies (cf section 4). The width of a closed, bounded convex body K along a vector y is the least positive real number t so that y belongs to $t(K-K)^*$, thus the result says that if K does not contain any points of L, then there is a y in $L^* \cap f(n)(K-K)^*$. This has the flavour of the theorems of alternatives like the Farkas lemma of linear programming, Menger's theorem etc. We will remark on this further later.

In classical geometry of Numbers, the following quantities are defined for any *0-symmetric* convex body K and lattice L in $\mathbf{R}^n$:

$$\Lambda_i(K,L) = \inf\{t : tK \text{ contains } i \text{ linearly independent points of } L\}$$

and [3]

$$\mu(K,L) = \inf\{t : tK + L = \mathbf{R}^n\}$$

With V equal to the volume of K, it is easy to see from Minkowski's theorems that

$$\Lambda_1(K,L)^n \leq 2^n d(L)/V$$

$$\Lambda_1(K,L)\Lambda_2(K,L)\ldots\Lambda_n(K,L) \leq 2^n d(L)/V$$

¿From the first inequality and its dual version, it follows that

$$\Lambda_1(K,L)\Lambda_1(K^*,L^*) \leq 4/(VV^*)^{1/n}$$

where V^* is the volume of the dual body K^* to K. It is a recent theorem of Bourgain and Milman [2] that for any centrally symmetric convex body K in $\mathbf{R}^n$ and its dual K^* the product of the volumes is at least $(cn)^{-n}$ where c is an absolute constant. (For a sphere of radius 1 and its dual - itself - the product of the volumes is $(dn)^{-n}$ for an absolute constant d, so this result cannot be improved substantially.) This purely geometric result, thus implies that

$$\Lambda_1(K,L)\Lambda_1(K^*,L^*) \leq c_o n$$

(This was first observed in [34].) Suppose now K does not contain any points of the lattice L other than the origin. Then, clearly, $\Lambda_1(K,L) \geq 1$ and thus $\Lambda_1(K^*,L^*) \leq c_o n$; i.e., there is a nonzero element v of L^* so that the width of K along v is at most $2c_o n$, by using the central symmetry of K. Stronger results can be obtained by similar arguments using the second theorem of Minkowski. Such theorems are called "transferrance theorems" - they connect the non-existence of nonzero lattice points in a 0-symmetric convex body K with the existence of points of the dual lattice in a dilation of the dual body, or equivalently, the width of the body K along dual lattice directions. As stated at the outset of this section, our concern is to extend these results to convex bodies not necessarily symmetric about the origin assuming they contain no points at all of the lattice - there is, of course, no need now to include the origin. For this, we follow the developement of Kannan and Lovász [34].

They consider what they call the "covering minima" of a general convex body (i.e., one that is not necessarily centrally symmetric) K in $\mathbf{R}^n$ with respect to a lattice L. For $i = 1,2,\ldots n$, they define the i^{th} *covering minimum* $\mu_i(K,L)$ to be the infimum over all positive reals t such that $(\{tx : x \in K\} + L)$ intersects every $n-i$ dimensional affine subspace of span(L). It is not difficult to see that the covering minima are invariant under translations of K, so this definition makes sense whether or not 0 belongs to K. Since, 0-dimensional affine subsapces are points, it is clear that $\mu_n(K,L)$ is the "covering radius" defined earlier as $\mu(K,L)$ for 0-symmetric bodies. They prove the "transferrance" theorem :

$$\mu_n(K,L)\,\Lambda_1((K-K)^*,L^*) \leq cn^2$$

where c is an absolute constant. This can be used to bound the width of convex sets K free of points of L as follows : if $K \cap L$ is empty, it is obvious that $\mu_n(K,L) \geq 1$, thus by the above

[3] Notation : For two sets P,Q $P+Q$ denotes the set $\{p+q : p \in P, q \in Q\}$

transferrance theorem, $\Lambda_1((K-K)^*, L^*) \le cn^2$, i.e., there is a nonzero element v in L^* such that the width of K along v is at most $O(n^2)$. We now give the simple proof of the transferrance result.

Let Λ_1 denote $\Lambda_1((K-K), L)$ in this proof and Λ_1^* denote $\Lambda_1((K-K)^*, L^*)$ and $\mu_n = \mu_n(K, L)$ (Note that $(K-K)$ and $(K-K)^*$ are 0-symmetric.) For the case $n = 1$, it is easy to see that $\mu_1(K, L) = \Lambda_1$ and thus the transferrance result easily follows. We proceed by induction on n. Let v be acieve the first minimum of L with respect to $K - K$. After translating K appropriately, we may assume that $0, v \in \Lambda_1 K$. Let $V = \mathrm{span}(v)$ and let $K' = K/V$; $L' = L/V$.[4] Then we assert that

$$\mu_n \le \mu_{n-1}(K', L') + \Lambda_1 \tag{$*$}$$

Let $\mu' = \mu_{n-1}(K', L')$. Suppose p is any point in space. Let l be the line through p parallel to v. By definition, $\mu' K' + L'$ contains $\mathrm{span}(L)/V$, thus $\mu' K + L$ intersects l. Clearly, it must intersect l at a point q so that $p - q = \alpha v$ for some $\alpha \in [0\ 1)$. Since $0, v \in \Lambda_1 K$, we have $p - q \in \Lambda_1 K$, so $p = p - q + q$ is in $(\mu' + \Lambda_1)K + L$. Since this is true of an arbitrary point p, the inequality (*) follows. To complete the inductive proof of the transferrance bound, we have by induction $\mu' \Lambda_1(K'^*, L'^*) \le c(n-1)^2$ and it is easily checked that $K'^* \subseteq K^*$; $L'^* \subseteq L^*$, so $\Lambda_1(K'^*, L'^*) \ge \Lambda_1^*$. Further, as pointed out earlier $\Lambda_1 \Lambda_1^* \le c_o n$, so $\mu_n \Lambda_1^* \le c_o n + c(n-1)^2$ and the transferrance bound follows with a suitable choice of c.

In the case that K is a sphere, (*) may be replaced by the stronger

$$\mu_n^2 \le \Lambda_1^2 + (\mu')^2$$

and it follows that

$$\mu_n \le cn^{3/2}$$

by induction, a result that was first proved by Lagarias, Lenstra and Schnorr [41].

As briefly mentioned in the introduction, the transferrance theorems have the flavour of theorems of the alternative. Using these we can produce good characterizations in the sense of Edmonds [12] for the closest vector problem (CVP), but only "approximate" good characterizations. This is perhaps expected because of the NP-hardness of the CVP which means that a good characterization for it would make NP=co-NP. We will make some definitions and explain this application.

Kannan and Lovász prove some more general results bounding the other covering minima which we do not go into here. They address the question of what more can be said of lattice free convex bodies than the fact that their width along one direction in the dual lattice is small.

In an interesting paper, Hastad [22] has shown a transferrance result which is not subsumed by the results mentioned so far. Suppose L is an n dimensional lattice in $\mathbf{R}^n$ and x is any point in $\mathbf{R}^n$. Let $d(x, L)$ denote the distance of x to the closest point in L. For any real number α let us denote by $\{\{\alpha\}\}$ the distance from α to the nearest integer. Suppose v is any nonzero element of the dual lattice L^* to L. Since $v.y$ is an integer for any $y \in L$, it is clear that $d(x, L) \ge \{\{v.x\}\}/|v|$. Khintchine [38] had shown that for any x, there exists a dual lattice vector v such that $\{\{v.x\}\}/|v| \ge d(x, L)/(n!)^2$. Hastad has replaced the $(n!)^2$ by n^2, a substantial improvement.

7.2 Approximating the shortest and closest vectors

We say that a deterministic algorithm approximates the SVP to a factor of $f(n)$, if given any n independent vectors $b_1, b_2, \dots b_n$, the algorithm finds a nonzero vector $v \in L = L(b_1, b_2, \dots b_n)$ such

[4]Reminder : K/V is the projection of K orthogonal to V.

that $|v| \leq f(n)\Lambda_1(L)$. We will say the same of a nondeterministic algorithm if it produces a nonzero v in L and a proof that $|v| \leq f(n)\Lambda_1(L)$. (Note that if the time taken by the nondeterministic algorithm is t, then the length of the proof is at most t.) Similar definitions are made for the CVP as well.

Several relationships are known among these problems. Kannan [31] showed that if can solve the SVP exactly in deterministic polynomial time, then we can approximate the CVP to a factor of $\sqrt{n}$ in deterministic polynomial time. Lagarias, Lenstra and Schnorr [41] showed that we can approximate the SVP to a factor of n and the CVP to a factor of $n^{3/2}$ both in nondeterministic polynomial time. We presently describe their algorithms, using the transferrance bounds.

Every lattice has a nice basis in the following sense. Suppose L is an $n-$dimensional lattice and L^* its dual lattice. Let $c_1, c_2, \ldots c_n$ be a $K-Z$ reduced basis of L^* and consider a corresponding basis $b_1, b_2, \ldots b_n$ of L (i.e., the unique $b_1, b_2 \ldots, b_n$ satisfying $b_j \cdot c_i = 0$ if $i \neq n-j+1$ and $b_j \cdot c_{n-j+1} = 1$). Suppose as usual $b_1^*, b_2^*, \ldots b_n^*$ are obtained by doing Gram-Schmidt process on $b_1, b_2, \ldots, b_n$. Then the following relationships hold [5]

$$|b_i^*| \geq \Lambda_1(L)/n \qquad |b_i^*| \geq \mu_i(L(b_1, b_2, \ldots b_i))/n^{3/2}$$

We prove these now. Let V be the span of c_1. Then it is clear that $c_2/V, c_3/V, \ldots c_n/V$ is a $K-Z$ reduced basis of L^*/V. Further, $b_1, b_2, \ldots b_{n-1}$ forms a basis of the dual lattice say L' of L^*/V. Clearly, $\Lambda_1(L') \geq \Lambda_1(L)$, so using induction on n, we see that it suffices to show the two inequalities for $i = n$. But, it is easily seen from the definition of $b_1, b_2, \ldots, b_n$ that $|b_n^*| = 1/|c_1| = 1/\Lambda_1(L^*)$. By section 2.4, we know that $\Lambda_1(L^*)\Lambda_1(L) \leq n$, so the first inequality follows. The second one follows from the transferrance theorem that $\mu_n(L)\Lambda_1(L^*) \leq n^{3/2}$.

For approximating the SVP nondeterministically, we just guess such a basis and in addition a shortest nonzero vector. By the fact that $\Lambda_1(L) \geq \min |b_i^*|$, the algorithm follows. For the CVP, we again guess such a basis and by a remark at the end of section 5, we may approximate the closest vector by enumerating at most one candidate.

In the deterministic case, it is possible to show using the transferrance bound that the problem of approximating the CVP to a factor of $n^{3/2}(f(n))^2$ is polynomial time Turing reducible (i.e., Cook reducible) to the problem of approximating the SVP to a factor of $f(n)$ for any nondecreasing function $f(n)$. Suppose we wish to find a point of a lattice L close to a point x. First, observe that if we can approximate the SVP to a factor of $f(n)$, we can easily find an "approximately K-Z " reduced basis of a lattice L - i.e., a basis $b_1, b_2, \ldots b_n$ such that it is proper and if $b_1^*, b_2^*, \ldots b_n^*$ is the orthogonal set obtained by Gram-Schmidt process, then $|b_i^*| \leq f(n-i+1)\Lambda_1(L/\text{span }(b_1, b_2 \ldots b_{i-1}))$. Find such a basis of the given lattice L. It is easy to find an element $b \in L$ such that $|b - x| \leq \frac{1}{2}(\sum |b_i^*|^2)^{1/2}$. Also, it is easy to see that $(L/\text{ span }(b_1, b_2, \ldots b_{i-1}))^* \subseteq L^*$, so that $|b_i^*|\Lambda_1(L^*) \leq f(n)c_o n \forall\, i$, whence we have

$$|b - x| \leq c_o n^{3/2} f(n)/\Lambda_1(L^*)$$

We may also find a nonzero vector v in L^* such that $|v| \leq f(n)\Lambda_1(L^*)$. Let H_0 be the hyperplane nearest to x of the sort $\{y : v \cdot y = z\}$, $\quad z$ an integer. Suppose p is the closest point of L to x. Then there are two cases to consider. If p does not lie on H_0, $\quad |p - x| \geq 1/(2|v|) \geq 1/(2f(n)\Lambda_1(L^*)) \geq |b-x|/O(n^{3/2}(f(n))^2)$ whence b is good enough as the answer. In the case that p does lie on H_0, we can recursively find an element $b' \in L \cap H_0$ such that $|b' - x'| \leq O(n^{3/2})(f(n))^2|p - x'|$ where x' is the projection of x into H_0. In this case, $|b'-x|^2 = |b'-x'|^2 + |x-x'|^2 \leq O(n^3)(f(n))^4|p-x'|^2 + |x-x'|^2 \leq O(n^3)(f(n))^4|p-x|^2$ from which it follows that b' suffices as the answer. Of course, we do not know

[5] For a lattice L, we let $\mu_i(L)$ denote $\mu_i(S, L)$ where S is the sphere of unit radius with the origin as centre.

which of the two cases we are in ; but note that we can find b in polynomial time and recursively also find b' and the closer of b, b' to x will suffice as the answer.

Babai [1] gave a polynomial time deterministic algorithm that approximates the closest vector to a factor of $2^{n/2}$; this follows from the previous argument and the Lovász basis reduction algorithm with $\delta = 1/\sqrt{2}$.

8 References

1. L.Babai, *On Lovász's lattice reduction and the nearest lattice point problem* Combinatorica 5 (1985)

2. J.Bourgain and V.D.Milman, *Sectiones euclidennes et volume des corps symetriques convexes dans* $\mathbf{R}^n$ C.R. Acad. Sc. Paris. , t. 300, Série I,n 13, (1985) pp 435-438

3. H.F.Blichfeldt, *The minimum value of quadratic forms and the closest packing of spheres* Math. Annalen 101 pp 605-608 (1929)

4. J.W.S.Cassels, *An introduction to the geometry of numbers* Springer Verlag (1971)

5. T.J.Chou and G.E.Collins, *Algorithms for the solution of linear diophantine equations* SIAM Journal on Computing, 11 (1982)

6. S.A.Cook, *The complexity of theorem proving procedures* Proc. 3rd Ann. ACM Symposium on Theory of Computing, Assoc. Comput. Mach., New York (1971) pp 151-158

7. W.Cook, C.Cullard and Gy.Turan, *Complexity of cutting planes* , Technical report , Institut für Operations Research , University of Bonn (1985).

8. R.R.Coveyou and R.D.MacPherson , *Fourier analysis of uniform random number generators* Journal of the ACM 14 (1967) pp 100 -119

9. L.E.Dickson , *History of the Theory of Numbers* Chelsea Publishing Co. (1971)

10. U.Dieter, *How to compute shortest vectors in lattices* Mathematics of Computation 29 (1975) pp 827-833

11. P.Domich, R.Kannan, L.E.Trotter, *Hermite normal form computation using modulo determinant arithmetic* to apear in Mathematics of Computation

12. J.Edmonds, *Paths, trees and flowers*, Canadian Journal of Mathematics, 17, (1965) pp 449-467

13. A.Frank and E.Tardos, *An application of simultaneous approximation in combinatorial optimization* , Report Institut für Ökonometrie und Operations Research , Uni. Bonn, W.Germany (1985) to appear in Combinatorica.

14. A.M.Frieze , *On the Lagarias-Odlyzko algorithm for the subset sums problem*, SIAM Journal on Computing, Vol 15, (1986) pp 536-540

15. A.Frieze, J.Hastad, R.Kannan, J.C.Lagarias, A.Shamir, *Reconstructing truncated integer variables satisfying linear congruences*, to appear in SIAM Journa on Computing.

16. M.L.Furst and R.Kannan, *Proofs of infeasibility for almost all subset sum problems* , In preparation (1985)

17. M.Garey and D.S.Johnson, *Computers and Intractability : A Guide to the Theory of NP-completeness* W.H.freeman and co., San Francisco (1979)

18. J. von zur Gathen and M.Sieveking, *Weitere zum Erfullungsprobleme polynomial ëquivalente kombinatorische Aufgaben* in : Lecture Notes in Computer Science 43 (Springer , Berlin 1976)

19. J.von zur Gathen and M.Sieveking, *A bound on the solutions of linear integer equalities and inequalities* Proc. Amer. Math. Soc. 72 (1978) pp 155-158

20. C.F.Gauss, *Disquisitiones Arithmeticae*, English edition, (Translated by A.A.Clarke) Springer-Verlag (166)

21. M.Grötschel, L.Lovász and A.Schrijver, *Geometric methods in combinatorial optimization* , in : Progress in Combinatorial Optimization (W.R.Pulleyblank, ed.), Proc. Silver Jubilee Conference on Comb. Opt. , Univ. of Waterloo, Vol. 1, (1982), Academic Press , N.Y. (1984)

22. J.Hastad *Dual Witnesses*, Manuscript (1986). To appear in Combinatorica.

23. J.Hastad, B.Just, J.Lagarias and C.P.Schnorr *Polynomial time algorithms for finding integer relations among real numbers*, Manuscript (1986)

24. B.Helfrich, *Algorithms to construct Minkowski reduced Hermite reduced lattice bases*, Uni. Frankfurt Technical report, to appear in Theoretical Computer Science. (1985)

25. C.Hermite, Second letter to Jacobi, Oeuvres, I , Journal für Mathematik, 40, (1905) pp 122-135

26. D.Hirschberg and C.K.Wong, *A polynomial-time algorithm for the knapsack problem with two variables*, J. Assoc. Comput. Mach. 23, (1976) pp 147-154

27. C.S.Iliopoulos, *Worst-case complexity bounds for computing the canonical structure of finite Abelian groups and the Hermite and Smith normal forms of an integer matrix* to appear in SIAM Journal on Computing

28. F.John, *Extremum problems with inequalities as subsidiary conditions*, Studies and Essays presented to R.Courant (1948)

29. E.Kaltofen, *On the complexity of finding short vectors in integer lattices*, Proceedings of EUROCAL (1983)

30. R.Kannan, *A polynomial algorithm for the two variable integer programming problem* , J. Assoc. Comput. Mach. 27, (1980) pp 118-122

31. R.Kannan, *Minkowski's Convex Body Theorem and integer programming*, Technical report 86-105, Computer Science dept., Carnegie-Mellon Univ. (1986) To appear in Mathematics of Operations Research

32. R.Kannan and A.Bachem, *Polynomial time algorithms for computing the Smith and Hermite normal forms of an integer matrix*, SIAM Journal on Computing, 8 (1979) pp 499-507

33. R.Kannan, A.K.Lenstra and L.Lovász, *Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers*, in Proc. 16 th Annual ACM symposium on Theory of Computing, (1984) pp 191-200

34. R.Kannan, L.Lovász, *Covering minima and lattice point free convex bodies*, Universität Bonn, Institut für Operations Research technical report (1986)

35. R.M.Karp, *Reducibility among combinatorial problems* in R.E.Miller and J.W.Thatcher (eds.) Complexity of Computer Computations , Plenum Press, New York pp 85-103 (1972)

36. N.Karmarkar, *A new polynomial time algorithm for linear programming*, Combinatorica 4, pp373-396 (1984)

37. L.G.Khaciyan, *A Polynomial Algorithm in Linear Programming*, Dokl. Akad. Nauk SSSR 244 pp 1093-1096. (English Translation : Soviet Math. Dokl 20 (1979) pp 191-194)

38. A.Ya. Khintchine *A quantitative formulation of Kronenecker's theory of approximation* [in Russian] Izv. Akad. Nauk SSSR. (Ser. Mat.) 12 pp 113-122 (1948)

39. D.E.Knuth, *The art of computer programming*, Volume 2 (1969) Addison-Wesley

40. A.Korkine and G.Zolotareff, *Sur les formes quadratiques*, Math. Annalen 6, (1873) pp 366-389

41. J.Lagarias, H.W.Lenstra and C.P.Schnorr, *Korkine-Zolotarev bases and successive minima of a lattice and its reciprocal lattice*, Manuscript, (1986)

42. J.Lagarias, A.Odlysko, *Solving low density subset sum problems* Proc. of the 24 th IEEE Symposium on Foundations of Computer Science, (1983) pp 1-13.

43. S.Landau and G.L.Miller ,*Solvability by radicals is in polynomial time* 15 th Annual ACM Symposium on Theory of Computing (1983) pp 140-151

44. C.G.Lekkerkerker, *Geometry of Numbers* North Holland , Amsterdam, (1969)

45. A.K.Lenstra, *Lattices and factorization of polynomials* , Report IW 190/81, Mathematisch Centrum, Amsterdam (1981)

46. A.K.Lenstra, H.W.Lenstra and L.Lovász, *Factoring polynomials with rational coefficients* Mathematische Annalen 261 (1982), pp513-534

47. H.W.Lenstra, *Integer programming with a fixed number of variables* First announcement (1979). Mathematics of Operations research, Volume 8, Number 4 Nov (1983) pp 538-548

48. L.Lovász, *An algorithmic theory of numbers, graphs and convexity*, NSF-CBMS Regional Conference Series, SIAM (1986)

49. L.Lovász and H.Scarf Private Communication

50. J.Milnor and D.Husemoller, *Symmetric bilinear forms* Springer-Verlag, Berlin (1973).

51. H.Minkowski, *Geometrie der Zahlen* Leipzig, Tuebner (1910)

52. H.Minkowski, *Diskontinuitätsbereich für arithmetische Äquivalenz*, Ges. Abh. (Collected works) II, pp 53-100

53. N.V.Novikova, *Korkine-Zolotarev Reduction domains of positive quadratic forms in $n \leq 8$ variables and a Reduction Algorithm for these domains*, Dokl. Acad. Nauk SSSR 270 (1983) (English Trans. : Soviet Math. Dokl. 27 (1983) pp 557-560)

54. B.Rosser, *A generalization of the Euclidean algorithm to several dimensions* Duke Journal of Mathematics (1942) pp 59 - 95

55. S.S.Ryskov, *The geometry of positive quadratic forms* , Proc. Intl. Congress Math. (Vancouver, B.C.) (1974). Vol. 1, pp 501-506 (Russian)

56. S.S.Ryskov and E.P.Baranovskii, *Classical methods in the Theory of Lattice packings* Uspeki Mat. Nauk 34 (1979) pp 3-63 (English Trans. : Russian Math Surveys 34 (1979) pp 1-68)

57. H.E.Scarf, *Production sets with indivisibilities* Part I : Generalities, Econometrica 49 pp1-32 , Part II :The case of two activities , ibid, pp 395-423 (1981)

58. C.P.Schnorr, *A hierarchy of polynomial time basis reduction algorithms* in : Coll. Math. Soc. Janos Bolyai, 44 , Theory of Algorithms Pécs (hungary) (1984)

59. C.P.Schnorr, *A more efficient basis reduction algorithm*, Univ. of Frankfurt, manuscript (1986)

60. A.Schönhage,*Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm* , in Lecture Notes in Computer Science Ed. Paredaens, Springer-Verlag Volume 172 (1984) pp 436-448

61. A.Shamir , *A polynomial time algorithm for breaking the Merkle-Hellman crypto system* , in Proc. of the 23 rd IEEE Symposium on the Foundations of Computer Science , (1982), pp 145-152

62. G.Strang *Linear algebra and its applications* Academic press (1980)

63. P.van Emde Boas, *Another NP-complete problem and the complexity of computing short vectors in a lattice* Report 81-04, Mathematische Instituut, Uni. Amsterdam (1981)

64. A.A.Voytakov and M.A.Frumkin, *An algorithm for finding the general integral solution of a system of linear eqautions*, in Issledovaniya po Diskretnoi Optimalizatsic, A.Frumkin ed., Nauka, Moscow, pp 128-140. (In Russian.)