CMU-CS-84-126

Lattice Based Algorithms

Ketan Mulmuley

Computer Science Department
Carnegie-Mellon University
Schenley Park
Pittsburgh, PA 15213

The research reported in this paper was supported in part by funds from the Computer Science Department of Carnegie-Mellon University, and by the Defense Advanced Research Projects Agency (DOD), ARPA Order No. 3597, monitored by the Air Force Avionics Laboratory under Contract F33615-81-K-1539. The views and conclusions contained in it are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency or the US Government.

Lattice Based Algorithms

1. Abstract

In this paper we examine the application of geometry of numbers in algorithm design. We consider two algorithms in detail. The first one is a polynomial time algorithm, due to Lenstra,Lenstra, and Lovasz, to factorize a polynomial in one variable with rational coefficients. The second one is a polynomial time algorithm, due to H.W. Lenstra, to solve the integer programming problem with a fixed number of variables. Both the algorithms start by building a certain lattice in Euclidian space. The key step is to find a set of generators, small enough in size, for this lattice. This step, called the basis reduction, will treated in detail in this paper.

The outline of the paper is as follows. In section 2 we present the required results from the geometry of numbers. In section 3 we describe LLL's basis reduction algorithm. In section 4 we prove the conjecture that a more elegant version of LLW's basis reduction algorithm indeed terminates; even for real lattices. For integer lattices we derive an explicit bound for the complexity of the algorithm. Unfortunately this bound is exponential unlike a polynomial bound for the original algorithm. Finally we present in section 5 the factorization algorithm and section 6 the integer programming algorithm.

2. Lattices

A lattice L in $\mathbf{R}^n$ is a set generated by finitely many linearly independent vectors $b_1, \ldots, b_k$ of $\mathbf{R}^n$; $L = \{\sum_{i=1}^{k} z_i b_i \mid z_i \in \mathbf{Z}\}$. We call $b_1, \ldots, b_k$ a basis of the lattice.

Basis is not uniquely determined by a lattice. Suppose $b_1, \ldots, b_n$ is a basis of a lattice L in $\mathbf{R}^n$. Let M be an $n \times n$ matrix with integral coefficients such that $det M = \pm 1$. Then $b'_1, \ldots, b'_n$, where $b'_i = M\, b_i$, also form a basis for L. This is because $M^{-1} = adj(M)/det\, M = \pm adj(M)$ is also an integral matrix and we have $b_i = M^{-1}\, b'_i$. Conversely if $b'_1, \ldots, b'_n$ is a basis of L and $b'_i = M\, b_i$, where M is an $n \times n$ integral matrix, then $det\, M = \pm 1$. To prove this we note that there exists an integral matrix N such that $b_i = N\, b'_i$, as $b'_1, \ldots, b'_n$ form a basis. Further M and N are the inverses of each other. Hence $det(M)\, det(N) = 1$. As M and N are integer matrices, this implies that $det(M) = \pm 1$ and $det(N) = \pm 1$.

Above mentioned integer transformations with determinant ± 1 are called unimodular transformations. The particularly interesting unimodular transfomations are:

(1) Adding an integer multiple of one of the basis vectors to another.

(2) Multiplying some basis vector by -1.

It should now be clear that the positive real number $|det(b_1, \ldots, b_n)|$ depends only on L and not on the choice of the basis; it is called the determinant of L and is denoted by $d(L)$. We can interpret $d(L)$ as the volume of the parallelopiped $\sum_{i=1}^{n} [o, 1).b_i$, where $[0, 1) = \{x \in \mathbf{R} \mid 0 \leq x < 1\}$. This inerpretation leads to the inequality of Hadamard:

$$d(L) \leq \prod_{i=1}^{n} |b_i| \tag{2.1}$$

We shall prove later in this section that L has a basis $b_1, \ldots, b_n$ such that the following opposite inequality holds:

$$\prod_{i=1}^{n} |b_i| \leq c.d(L) \tag{2.2}$$

where c is a constant depending only on n . In the next section we also give a constructive proof of this existence. The algorithm given there can reduce in polynomial time any given basis of L into the one satisfying (2.2).

If every point of lattice M is also a point of a lattice L then we say that M is a sublattice of L. Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be the bases of M and L respectively. Then there are integers v_{ij} such that:

$$a_i = \sum v_{ij} b_j$$

The integer

$$D = |det(v_{ij})| = det(a_1, \ldots, a_n)/det(b_1, \ldots, b_n) = d(M)/d(L)$$

is called the index of M in L. From the last expression it follows that the index is independent of the choice of the bases. Since $a_1, \ldots, a_n$ are independent, $D \geq 1$. Thus

$$d(L) \leq d(M) \tag{2.3}$$

One of the most important theorems in the geometry of numbers is:

2.1. Theorem. *(Minkowski): Let $S \subset \mathbf{R}^n$ be a point set of volume $V(S)$ (possibly infinite) which is symmetric about origin and convex. Let L be an n-dimensional lattice of determinant $d(L)$. Suppose that either*

$$V(S) > m.2^n\, d(L) \quad or$$

$$V(S) = m.2^n\, d(L) \quad and\ S\ is\ compact.$$

Then S contains at least m pairs of nonzero vectors $\pm v_1, \ldots, \pm v_m$ belonging to L.

This theorem has many important consequences. One of them is the following basis independent characterization of a lattice.

A necessary and sufficient condition that a set $L \in \mathbf{R}^n$ be a lattice is that it should satisfy the following two properties:

(1) If a and b are in L then $a \pm b$ is in L; i.e. L is a group under addition.

(2) There exists a real $r > 0$ such that the only point of L in the sphere $|x| < r$ is 0.

This criterion is very useful. For example let H be any l-dimensional, $l < n$, subspace in $\mathbf{R}^n$ and L be any lattice in $\mathbf{R}^n$. By above criterion $M = L \cap H$ is also a lattice. Furthermore every basis of M can be extended to a basis of L. To see this, let L' be projection of L on G, the orthogonal complement of H. Let $c_1, \ldots, c_{n-l}$ be the vectors in L such that their projections on G form a basis of L'. It is clear that given any $d \in L$ there exist integers z_j such that the projection of $e = d - \sum_{j=1}^{n-l} z_j c_j$ on G is zero; then $e \in H \cap L = M$. It follows that there exist integers k_i such that $e = \sum_{i=1}^{l} k_i b_i$. Now $d = \sum_{j=1}^{n-l} z_j c_j + \sum_{i=1}^{l} k_i b_i$. Thus $b_1, \ldots, b_l, c_1, \ldots, c_{n-l}$ is the desired basis of L.

It is very easy now to determine whether a given set of vectors can be extended to a basis of a lattice L in $\mathbf{R}^n$. Let $a_1, \ldots, a_m$ be such a set of linearly independent vectors. If this set can be extended to basis of L then clearly

Whenever $\sum_{j=1}^{m} r_j a_j \in L$, r_j *are integers*

Coversely if above condition holds then $a_1, \ldots, a_m$ form a basis of $L \cap H$, where H is the subspace spanned by $a_1, \ldots, a_m$, and thus can be extended to a basis of L.

Even if $a_1, \ldots, a_m$ can not be extended to a basis of L, one can find an interesting basis for L as follows. Let H_j, $1 \le j \le n$, be the subspace spanned by $a_1, \ldots, a_j$. Let $L_j = L \cap H_j$. We start with a basis for L_1, extend it to a basis for L_2, ... and so to a basis for L_m which can be finally extended to a basis for L. This basis, $b_1, \ldots, b_n$, of L has a property that

$$
\begin{aligned}
a_1 &= v_{11} b_1 \\
a_2 &= v_{21} b_1 + v_{22} b_2 \\
&\cdots \\
&\cdots \\
a_m &= v_{m1} b_1 + v_{m2} b_2 + \cdots + v_{mm} b_m
\end{aligned}
$$

for some integers v_{ij}.

The problem which often arises in lattice theory is to determine if a lattice L has any point in a set S. Sometimes one also needs to know the number of linearly independent points of L in S. To deal with this problem we introduce the notion of successive minima.

Let $F(\mathbf{x})$ be an n-dimensional distance function. This means : F is (1) nonnegative i.e. $F(\mathbf{x}) \ge 0$. (2) continuous (3) homogenous i.e. for all real $t \ge 0$, $F(t\mathbf{x}) = t F(\mathbf{x})$. If for some integer k in $1 \le k \le n$ and some number λ the set

$$\lambda S : F(\mathbf{x}) < \lambda$$

conatains k linearly independent points, then so does βS for every $\beta > \lambda$. We define the kth successive minimum $\lambda_k = \lambda_k(F, L)$ of the distance function F with respect to the lattice L to be the lower bound of the numbers λ such that λS contains k linearly independent points. Clearly

$$\lambda_1 \le \lambda_2 \le \ldots \le \lambda_n$$

A common example of a distance function is $F(\mathbf{x}) = |\mathbf{x}|$. In this case $\lambda_1(F, L)$ is the length of the shortest vector in L. It is very easy to find an upper bound for it. let $S = \{x \mid |x_i| \le d(L)^{1/n}\}$ – S has volume $2^n d(L)$ – and $m = 1$ in **Theorem 2.1.** It follows that $\lambda_1(|\,|, L)$, length of the shortest vector in L, is at the most $\sqrt{n}(d(L))^{1/n}$. Minkowski also gave bounds for the product of successive minima.

2.2. Theorem. *Let $F(\mathbf{x})$ be a distance function. Suppose $F(\mathbf{x}) < 1$ is a bounded symmetric convex set of volume V_F. Let $\lambda_1, \ldots, \lambda_n$ be the successive minima of a lattice L with respect to F. Then*

$$\frac{2^n}{n!} d(L) \le \lambda_1 \cdots \lambda_n V_F \le 2^n d(L)$$

The existence of a reduced basis satisfying (2.2) is closely related to the existence of an upper bound on the product of successive minima provided by the above theorem. To see this we first prove the following lemma due to Mahler.

2.3. lemma. Let $a_1, \ldots, a_n$ be linearly independent points of an n-dimensional lattice L. Then there exists a basis $b_1, \ldots, b_n$ of L such that

$$|b_j| \le max\{|a_j|, 1/2 \sum_{i=1}^{j} |a_i|\} \text{ for } 1 \le j \le n$$

∎

Proof. Let $c_1, \ldots, c_n$ be a basis of L such that

$$\begin{aligned} a_1 &= v_{11}c_1 \\ a_2 &= v_{21}c_1 + v_{22}c_2 \\ &\cdots \\ &\cdots \\ a_n &= v_{n1}c_1 + v_{n2}c_2 + \cdots + v_{nn}c_n \end{aligned} \tag{2.4}$$

for some integers v_{ij}, where $v_{ii} \neq 0$. We shall take b_j of the shape

$$b_j = c_j + t_{j\,j-1}a_{j-1} + \cdots + t_{j1}a_1 \tag{2.5}$$

where t_{ji} are the integers to be determined. Clearly $b_1, \ldots, b_n$ is a basis for L.

We distinguish two cases for each j. If $v_{jj} = \pm 1$, we put $b_j = \pm a_j$. This cetainly has a shape (2.5) and also $|b_j| = |a_j|$.

Otherwise $|v_{jj}| \geq 2$. on solving (2.4) for c_j we have

$$c_j = v_{jj}^{-1}a_j + k_{j\,j-1}a_{j-1} + \cdots + k_{j1}a_1$$

where k_{ji} are some real numbers. Choose t_{ji} in (2.5) such that $|k_{ji} + t_{ji}| \leq 1/2$. Then

$$b_j = l_{jj}a_j + l_{j\,j-1} + \cdots + l_{j1}a_1$$

where $|l_{jj}| = |v_{jj}^{-1}| \leq 1/2$ and $|l_{ji}| = |k_{ji} + t_{ji}| \leq 1/2$, for $i < j$. Then obviosly,

$$|b_j| \leq 1/2 \sum_{i=1}^{j} |a_i|$$

This proves the lemma. ∎

Now let $\lambda_1, \ldots, \lambda_n$ be the successive minima of L with respect to $|\ |$. There obviosly exist the linearly independent vectors $a_1, \ldots, a_m$ such that $|a_j| \leq \lambda_j$, for $1 \leq j \leq n$. By above lemma there exists a basis $b_1, \ldots, b_n$ of L such that

$$|b_j| \leq max\{\lambda_j, \sum_{i=1}^{j} \lambda_i\} \leq max(1, n/2)\lambda_j \leq n\lambda_j$$

Using **Theorem 2.2** we have

$$\prod_{i=1}^{n} |b_i| \leq n^n . \prod_{i=1}^{n} \lambda_i \leq \frac{n^n . 2^n}{V} d(L)$$

where V is the volume of the sphere $|x| < 1$. Thus for some constant basis $b_1, \ldots, b_n$ indeed satisfies (2.2).

In the next section we give a 'constructive' proof for the existence of such a reduced basis.

3. Basis Reduction

Let L be an n-dimensional lattice with basis $b_1, \ldots, b_n$. We denote by $b_i(j)$ the projection of b_i onto the orthogonal complement of the space spanned by $b_1, \ldots, b_{j-1}$, for $i \geq j \geq 2$. $b_i(1)$ is same as b_i. We denote $|b_i(j) - b_i(j+1)|/|b_j(j)|$, where $i > j$, by μ_{ij}. Note that $b_1(1), \ldots, b_n(n)$

are same as the vectors obtained by Gram-Schmidt orthogonalization of $b_1, \ldots, b_n$ and thus form an orthogonal basis of $\mathbf{R}^n$. The following equality holds:

$$b_i = b_i(i) - \sum_{j=1}^{i-1} \pm\mu_{ij} b_j(j)$$

We shall call the basis $b_1, \ldots, b_n$ reduced if

$$\mu_{ij} \leq 1/2 \qquad \text{for all } i > j. \tag{3.1}$$

$$|b_i(i-1)|^2 \geq \tfrac{3}{4}|b_{i-1}(i-1)|^2 \tag{3.2}$$

Suppose we are given an arbitrary integer basis $b_1, \ldots, b_n$ of L. We give an algorithm, due to Lenstra, Lenstra, and Lovasz, to reduce this basis in polynomial time into the one satisfying (2.2). In the course of the algorithm the $b_1, \ldots, b_n$ will have changed several times, but always in such a way that they form a basis for L.

At each step of the algorithm we shall have a current subscript $k \in \{1, \ldots, n+1\}$. We begin with $k = 2$.

Inductively assume that for the current value of k the following conditions are satisfied:

$$|\mu_{ij}| \leq 1/2 \qquad \text{for } 1 \leq j < i < k. \tag{3.3}$$

$$|b_i(i-1)|^2 \geq \tfrac{3}{4}|b_{i-1}(i-1)|^2 \qquad \text{for } 1 < i < k \tag{3.4}$$

These conditions are trivially satisfied for $k = 2$.

Now one proceeds as follows. If $k = n+1$ the the basis is reduced and the algorithm terminates. Suppose $k \leq n$. Then we first achieve that

$$|\mu_{k\,k-1}| \leq 1/2 \qquad \text{if } k > 1 \tag{3.5}$$

If this does not hold, let r be the integer nearest to $\mu_{k\,k-1}$, and replace b_k by $b_k - rb_{k-1}$. After this (3.5) holds.

Consider two cases.

Case1: Suppose $k > 1$ and $|b_k(k-1)|^2 < \frac{3}{4}|b_{k-1}(k-1)|^2$. We interchange b_k and b_{k-1} and then replace k by $k-1$. Now we are in situation described by (3.3) and (3.4) and we proceed from there.

Case2: Suppose $k = 1$ or $|b_k(k-1)|^2 \geq \frac{3}{4}|b_{k-1}(k-1)|^2$.

In this case we first achieve that

$$|\mu_{kj}| \leq 1/2 \qquad \text{for} 1 \leq j \leq k-1. \tag{3.6}$$

For $j = k-1$ this is already true by (3.5). If (3.6) is not true for all j, let l be the largest index $< k$ with $|\mu_{kl}| > 1/2$ and let r be the integer nearest to μ_{kl}. Replace b_k by $b_k - rb_l$ (note that this does not disturb μ_{km}, where $k > m > l$). Repeat the process until (3.6) is satisfied.

Replace k by $k+1$. Now we are in a situation described by (3.3) and (3.4). We proceed from there.

We remark that in the algorithm we need to keep track of only the numbers $|b_i(i)|^2$, μ_{ij} and the vectors b_i. All these quantities are rational. Also in both the cases the new values of these quantities can be computed from the old ones very easily.

To show that the algorithm terminates, we need to introduce one new quantity. Given any k ineger n-vectors $c_1, \ldots, c_k$, it is easy to show that:

$$d^2(L(c_1, \ldots, c_k)) = Det[(c_i, c_j)]_{1 \le i,j \le k} \quad (3.7)$$

Here (,) denotes the ordinary inner product in $\mathbf{R}^n$. It is clear that $d^2(L(c_1, \ldots, c_k))$ is an integer. We also have the easy identity:

$$d^2(L(c_1, \ldots, c_k)) = \prod_{j=1}^{k} |c_j(j)|^2 \quad (3.8)$$

Now we show that the above basis reduction algorithm terminates. As before $b_1, \ldots, b_n$ will denote a basis at any stage of the algorithm. Let d_i denote $d^2(L(b_1, \ldots, b_i))$. And let $D = \prod_{i=1}^{n}$. In case 1 of the algorithm d_{k-1} is reduced by a factor of at least 3/4 and all other d_is are undisturbed. Hence D decreases by a factor of at least 3/4. Suppose at start of the algorithm $|b_i|^2 \le B$, for all $i \le n$. Then by Hadamard's inequality we have at start of the algorithm $d_i \le B^i$, for all $i < n$; Hence $D \le B^{n(n-1)/2}$ initially. As D is a nonnegative integer, it follows from independence of the basis vectors that $D \ge 1$ throughout the algorithm. Hence the number of times algorithm passes through case 1 is at the most $O(n^2 \log B)$. In case 1, the value of k is decreased by 1, and in case 2 it is increased by 1. As $k \le n+1$ throughout the algorithm, the number of times we pass through case 2 is also $O(n^2 \log B)$. Thus the number of iterations is $O(n^2 \log B)$. With a slightly detailed argument one can show that the number of arithmetic operations needed is no more than $O(n^4 \log B)$. All the quanties involved in the algorithm are rational numbers which can be expressed as the ratio of two integers. Later on we shall show that the length of these integers is bounded by $O(n \log B)$. Thus using the classical algorithms for the arithmetic operations we find that the number of bit operations needed by the basis reduction algorithm is $O(n^6 (\log B)^3)$.

We show that a reduced basis produced by the above algorithm has many desirable properties. The following lemma can be easily proved:

3.1. Lemma. If a basis $b_1, \ldots, b_n$ is reduced in the sense of (3.1) and (3.2) then we have $|b_j|^2 \le 2^{i-1} . |b_i(i)|^2$ for $1 \le j \le i \le n$. ∎

If $b_1, \ldots, b_n$ is a reduced basis for a lattice L then by the above lemma it follows that $\prod_{i=1}^{n} |b_i| \le 2^{n(n-1)/4} . \prod_{i=1}^{n} |b_i(i)|$. But $d(L) = d(b_1, \ldots, b_n) = d(b_1(1), \ldots, b_n(n)) = \prod_{i=1}^{n} |b_i(i)|$, as $b_1(1), \ldots, b_n(n)$ are orthogonal. Hence:

$$\prod_{i=1}^{n} |b_i| \le 2^{n(n-1)/4} . d(L)$$

Thus (2.2) is indeed satisfied. Further a reduced basis also provides us with a good approximation to successive minima.

3.2. Theorem. *Let $\lambda_1, \ldots, \lambda_n$ denote the successive minima of $|\ |^2$ on L. Let $b_1, \ldots, b_n$ be a reduced basis for L. Then:*

$$2^{1-i} \lambda_i \le |b_i|^2 \le 2^{n-1} \lambda_i \qquad \textit{for } 1 \le i \le n$$

Proof. The left inequality follows from lemma (2.1) easily. To prove the other inequality, let $x_1, \ldots, x_j \in L$ be linearly independent. We show that,

$$|b_j|^2 \le 2^{n-1} . max\{|x_1|^2, \ldots, |x_j|^2\} \quad (3.9)$$

Write $x_k = \sum_{i=1}^{n} r_{ik} b_i$ with $r_{ik} \in \mathbf{Z}$. For fixed k let $i(k)$ denote the largest
$x_k = \sum_{j=1}^{i(k)} r_{jk} b_j$. Then $1 \le k \le j$, $|x_k|^2 \ge |b_{i(k)}(i(k))|^2$. Renumber x_k s
claim that $j \le i(j)$; otherwise $x_1, \ldots, x_j$ would be dependent as they would
From $j \le i(j)$ and Lemma (3.1) we obtain

$$|b_j|^2 \le 2^{i(j)-1} \cdot |b_{i(j)}(i(j))|^2 \le 2^{n-1} |b_{i(j)}(i(j))|^2 \le 2^{n-1} |x_j|^2$$

From this (3.9), and hence the theorem, follows.

3.3. Corollary. Let L be an n-dimensional lattice with reduced basis b_1,

$$|b_1|^2 \le 2^{n-1} \cdot |x|^2$$

for every nonzero $x \in L$. ∎

4. Variation Of The Basis Reduction Algorithm

It is possible to replace the constant 3/4 in (3.4) by any constant c <
of the algorithm remains polynomial. We ask: what happens if the replac
Before considering the complexity issue one must first show that the algorit
this replacement. We shall refer to this new algorithm by NEW-REDUCE in
REDUCE is same as the previous basis reduction algorithm except that we ap
two basis vectors b_{k-1} and b_k, when

$$|b_k(k-1)|^2 < |b_{k-1}(k-1)|^2$$

We show that NEW-REDUCE terminates even when the intial basis vect
real coordinates.

Assume that initially $|b_i|^2 \le B$ for $1 \le i \le n$; this implies $|b_i(i)|^2 \le |b_i|$
that throughout NEW-REDUCE $max\{|b_i(i)|^2 : 1 \le i \le n\}$ is nonincreasing. In c
unchanged. Consider case 1. By c_i and ν_{ij} we shall denote the vectors and n
replace b_i and μ_{ij} respectively. The new basis is given by:

$$c_{k-1} = b_k, \quad c_k = b_{k-1}, \quad c_i = b_i \quad \text{for } i \ne k-1, k$$

We have $|c_{k-1}(k-1)| = |b_k(k-1)| < |b_{k-1}(k-1)|$, by (4.1). Also $|c_k(k)| \le |c_k(k-1)|$
Thus indeed $max\{|b_i(i)|^2 \mid 1 \le i \le n\}$ is nonincreasing and we have

$$|b_i(i)|^2 \le B$$

throughout NEW-REDUCE. Let $d_i = d^2(b_1, \ldots, b_i) = d^2(b_1(1), \ldots, b_i(i)$ and D
before. By Hadamard's inequality we have $d_i \le |B|^i$ and hence $D \le B^{n(n-1)/2}$ thro
REDUCE.

We show, using an argument in LLL, that $|b_i|^2$ are nicely bounded throughout
NEW-REDUCE. For that we first prove that before and after every iteration of N
the following inequalities hold:

$$|b_i|^2 \le nB \qquad \text{for } i \ne k$$

$$|b_k|^2 \leq n^2(4B)^n \qquad \text{if } k \neq n+1 \tag{4.3}$$

$$|\mu_{ij}| \leq 1/2 \qquad \text{for } 1 \leq j < i,\ i < k \tag{4.4}$$

$$|\mu_{ij}| \leq (nB^j)^{1/2} \qquad \text{for } 1 \leq j < i,\ i > k \tag{4.5}$$

$$|\mu_{kj}| \leq 2^{n-k}(nB^{n-1})^{1/2} \qquad \text{for } 1 \leq j < k, \text{ if } k \neq n+1 \tag{4.6}$$

Here (4.2), for $i < k$, is trivial from (4.4), and (4.3) follows from (4.6). Using that

$$|\mu_{ij}|^2 \leq |b_i|^2/|b_j(j)|^2 = d_{j-1}|b_i|^2/d_j \leq B^{j-1}|b_i|^2 \tag{4.7}$$

we see that (4.5) follows from (4.2). (4.3) is same as (3.3). It remains to prove (4.2), for $i > k$, and (4.6). At the begining of we even have $|b_i|^2 \leq B$ and $\mu_{ij}{}^2 \leq B^j$, by (4.7), so it suffices to consider the situation at the end of case 1 and case 2. Taking into account that k changes in these cases, we see that in case 1 the set of vectors $\{b_i \mid i \neq k\}$ is unchanged, and that in case 2 the set $\{b_i \mid i > k\}$ is replaced by a subset. Hence the inequalities (4.2) are preserved. At the end of case 2, the new values for μ_{kj} (if $k \neq n+1$)are the old values of $\mu_{k-1\,j}$, so here (4.6) follows from the inequality (4.5) of the of the previous stage. To prove (4.6) at the end of case 1 we assume that it is valid at the previous stage, and we follow what happens to $|\mu_{kj}|$. To achieve (3.5) it is, for $j < k-1$, replaced by $\mu_{kj} - r\mu_{k-1\,j}$, with $|r| < 2|\mu_{k\,k-1}|$ and $|\mu_{k-1\,j}| \leq 1/2$, so by (4.6),

$$|\mu_{kj} - r\mu_{k-1\,j}| < |\mu_{kj}| + |\mu_{k\,k-1}| \leq 2^{n-k-1}(nB^{n-1})^1/2 \tag{4.8}$$

Thus in the notation introduced in the begining of this section we have

$$|\nu_{k-1\,j}| \leq 2^{n-(k-1)}(nB^{n-1})^{1/2} \qquad \text{for } j < k-1$$

and since $k-1$ is the new value for k this exactly the inequality (4.6) to be proved.

We also have to estimate $|b_i|^2$ and μ_{ij} at the other points of the algorithm. For this it suffices to remark that the maximum of $|\mu_{k1}|, \ldots, |\mu_{k\,k-1}|$ is at most doubled when (3.5) is achieved and the same thing happens in case 2 for at most $k-2$ values of l. Combining this with (4.6) and (4.5) we conclude that throughout the course of the algorithm we have

$$|\mu_{ij}| \leq 2^{n-1}(nB^{n-1})^{1/2} \qquad \text{for } 1 \leq j < i \leq n$$

and therefore finally

$$|b_i|^2 \leq n^2(4B)^n \qquad \text{for } 1 \leq i \leq n$$

Remark that the above argument could be exdended to show that length of the representations of all the quantities involved in the previous basis reduction algorithm is bounded by O($n\, logB$).

Let us call a basis b of L ***well bounded*** if $|b_i|^2 \leq n^2(4B)^n$, for $1 \leq i \leq n$. It is clear that basis remains ***well bounded*** throughout NEW-REDUCE. As any bounded volume contains only finite number of lattice points, there are only finite number of ***well bounded*** bases. Consequently the set

$$A = \{\tfrac{|b_k(k-1)|}{|b_{k-1}(k-1)|} \qquad | \ 1 \leq k \leq n, b \text{ is a } \textit{well founded} \text{ basis and } \tfrac{|b_k(k-1)|}{|b_{k-1}(k-1)|} < 1\}$$

is finite. Hence there exists a $c < 1$ such that

$$\forall x \in A.\ x < c$$

Whenever case 1 occurs in NEW-REDUCE $|b_k(k-1)|/|b_{k-1}(k-1)| \in A$ and hence $|b_k(k-1)|/|b_{k-1}(k-1)| < c$. This means that D decreases by the factor $< c$. As $D < B^{n(n-1)/2}$ initially, by the argument of section 3 we conclude that number of iterations is of the order $O(n^2 \log B/(\log 1/c))$. Thus NEW-REDUCE indeed terminates. Unfortunately it is not possible to estimate c in terms of n and B for real lattices.

For integer lattices an explicit bound on the number of iterations can be found. So suppose that $b_1, \ldots, b_n$ are integer vectors at the start of (and hence throughout) NEW-REDUCE. Case 1 is applied, i.e. b_k and b_{k-1} are swapped, whenever

$$|b_k(k-1)|^2/|b_{k-1}(k-1)|^2 < 1$$

Note that

$$|b_k(k-1)|^2 = d^2(L(b_1,\ldots,b_{k-2},b_k))/d^2(L(b_1,\ldots,b_{k-2})) \text{ and}$$
$$|b_{k-1}(k-1)|^2 = d^2(L(b_1,\ldots,b_{k-2},b_{k-1}))/d^2(L(b_1,\ldots,b_{k-2}))$$

Hence

$$\frac{|b_k(k-1)|^2}{|b_{k-1}(k-1)|^2} = \frac{d^2(L(b_1,\ldots,b_{k-2},b_k))}{d^2(L(b_1,\ldots,b_{k-2},b_{k-1}))} = \frac{d^2(L(b_1,\ldots,b_{k-2},b_k))}{d_{k-1}}$$

From (3.7) it follows that $d^2(L(b_1,\ldots,b_{k-2},b_k))$ and d_{k-1} are integers. Hence whenever case 1 is applicable, i.e. $|b_k(k-1)|^2/|b_{k-1}(k-1)|^2 < 1$, we have

$$\frac{|b_k(k-1)|^2}{|b_{k-1}(k-1)|^2} \leq 1 - \frac{1}{d_{k-1}} \leq 1 - \frac{1}{B^{k-1}} \leq 1 - \frac{1}{B^n}$$

Let $c = 1 - \frac{1}{2B^n}$, then whenever case 1 is applicable we have $|b_k(k-1)|^2/|b_{k-1}(k-1)|^2 < c$. As $\log 1/c \geq 1/2B^n$, the number of iterations, as before, is

$$O(n^2 \log B/(\log 1/c)) \leq O(B^n n^2 \log B)$$

It is unfortunate that the bound on number of iterations is exponential as opposed to polynomial bound for the previous basis reduction algorithm. But probably there is some room for improvement.

5. Lattices And Factorization

In this section we describe a polynomial-time algorithm, due to Lenstra,Lenstra, and Lovasz, to solve the following problem: given a non-zero polynomial $f \in \mathbf{Q}[x]$ with rational coefficients, find the decomposition of f into irreducible factors in $\mathbf{Q}[x]$. It is well known that this is equivalent to factoring *primitive* polynomials$f \in \mathbf{Z}[x]$ into irreducible factors in $\mathbf{Z}[x]$. A polynomial $f \in \mathbf{Z}[x]$ is primitive if the greatest common divisor of its coefficients is 1.

We shall denote by p a prime number and by k a positive integer. We shall write $\mathbf{Z}/p^k\mathbf{Z}$ for the ring of integers modulo p^k, and $\mathbf{F}_p$ for the field $\mathbf{Z}/p\mathbf{Z}$.

Let $f \in \mathbf{Z}[x]$ of degree n be polynomial to factorized. Suppose we are given in addition $h \in \mathbf{Z}[x]$ which has following properties:

h has leading coefficient 1. (5.1)

$(h \ mod \ p^k)$ divides $(f \ mod \ p^k)$ in $(\mathbf{Z}/p^k\mathbf{Z})[x]$. (5.2)

$(h \ mod \ p)$ is irreducible in $\mathbf{F}_p[x]$. (5.3)

$(h \ mod \ p)^2$ does not divide $(f \ mod \ p)$ in $\mathbf{F}_p[x]$ (5.4)

Let $l = deg(h)$; so $0 < l \leq n$.

It is easy to see that f has an irreducible factor h_0 in $\mathbf{Z}[x]$ for which $(h \ mod \ p)$ divides $(h_0 \ mod \ p)$. By (5.4) this factor is uniquely determined upto sign. Further if g divides f in $\mathbf{Z}[x]$ then the following can be proved to be equivalent:

(1) $(h \ mod \ p)$ divides $(g \ mod \ p)$ in $\mathbf{F}_p[x]$.

(2) $(h \ mod \ p^k)$ divides $(g \ mod \ p^k)$ in $(\mathbf{Z}/p^k\mathbf{Z})[x]$.

(3) h_0 divides g in $\mathbf{Z}[x]$.

In particular $(h \ mod \ p^k)$ divides $(h_0 \ mod \ p^k)$ in $\mathbf{Z}/p^k\mathbf{Z}[x]$.

We shall now see how one can construct h_0 using only the factor $(h \ mod \ p^k)$ if k is sufficiently large. First we define a lattice L such that h_0 is contained in it. Fix an integer $m \geq deg(h_0)$. Let L be the collection of all the polynomials in $\mathbf{Z}[x]$ of degree $\leq m$ that when taken modulo p^k are divisible by $(h \ mod \ p^k)$ in $(\mathbf{Z}/p^k\mathbf{Z})[x]$; thus $h_0 \in L$. This is a subset of the $(m+1)$ dimensional real vector space $\mathbf{R} + \mathbf{R}.x + \cdots + \mathbf{R}.x^m$. This vector space is identified with $\mathbf{R}^{m+1}$ by identifying $\sum_{i=0}^{m} a_i x^i$ with $(a_0, \ldots, a_m)$. Length of a polynomial g, $||g||$, is defined to be length of the corresponding vector. It is easy to see that L is a lattice in $\mathbf{R}^{m-1}$. By (5.1) it follows that the following is the basis of L:

$$\{p^k x^i : 0 \leq i < l\} \cup \{hx^j : 0 \leq j \leq m - l\}$$

Also $d(L) = p^{kl}$.

5.1. Theorem. *Let $b \in L$ be such that $gcd(h_0, b) = 1$ in $\mathbf{Z}[x]$ (as h_0 is irreducible this equivalent to saying that h_0 is not a factor of b). Then*

$$p^{kl} \leq ||h_0||^m ||b||^m$$

Proof. Let M be the set of all polynomials of the form $ch_0 + db$, where c and d are some polynomials in $\mathbf{Z}[x]$ such that $deg(c) < deg(b)$ and $deg(d) \deg(h_0)$. As $gcd(h_0, b) = 1$, every polynomial in M can be uniquely represented in the above form. Hence M is a $(deg\, b + deg\, h_0)$-dimensional lattice with a basis:

$$\{h_0 x^i : 0 \leq i < deg(b)\} \cup \{bx^i : 0 \leq i < deg(h_0)\}$$

It follows from Hadamard's inequality that $d(M) \leq ||b||^{deg\, h_0}.||h_0||^{deg\, b} \leq ||b||^m ||h_0||^m$. Let N be a $deg(b) + deg(h_0)$-dimensional lattice with the following basis:

$$\{p^k x_i \mid 0 \leq i < l\} \cup \{hx^j \mid 0 \leq j < deg(b) + deg(h_0)\}$$

Note that N is very similar to L. In fact N is the set of polynomials of degree $< deg(b) + deg(h_0)$ are divisible by $(h \ mod \ p^k)$ in $(\mathbf{Z}/p^k\mathbf{Z})[x]$. Also $d(N) = p^{kl}$. M is obviously a sublattice of N. Hence by (2.3), $d(N) = p^{kl} \leq d(M) \leq ||b||^m ||h_0||^m$. This proves the theorem. ∎

Write $h_0 = \sum_{i=0}^{m} a_i x^i$. As $h_0 | f$ over $\mathbf{Z}[x]$, it follows from MIGNOTTE [8] that:

$|a_i| \leq \binom{m}{i} ||f||$ for all $0 \leq i \leq m$

Hence $||h_0|| \leq (\sum_{i=0}^{m} \binom{m}{i}^2 ||f||^2)^{1/2} \leq \binom{2m}{m}^{1/2} = B$. If we take k such that:

$B^{2m} < p^{kl}$

then from the above theorem it follows that any $b \in L$ which does not contain h_0 as a factor satisfies:

$||b|| \geq (p^{kl}/||h_0||)^{1/m} \geq (||B||^{2m}/||B||^m)^{1/m} = B$

Hence the shortest vector in L is a multiple of h_0; it can be found by Dieter's algorithm. If $m = deg(h_0)$ then the shortest vector can only be an integral multiple of h_0. As the value of m is unknown to us at the start, we can simply try the algorithm for $m = deg(h_0)$ to $n-1$. If a vector is found with length $\leq B$ then we test if it is a factor of f over $\mathbf{Z}[x]$, if not guess for m was wrong. If such a vector can not be found for any of the above values of m then f was irreducible. Otherwise we have found h_0 with $m = deg(h_0)$. Alternately we can make an intelligent guess for m such that $m \geq deg(h_0)$.If the guess is right then shortest vector will be some multiple of h_0; thus h_0 can be found.

If we choose k such that $p^{kl} > B^{2m} 2^{m(n-1)/2}$ then by similar argument one shows that every polynomial in L which is not a multiple of h_0 has length $> 2^{(n-1)/2} B$. As L contains a vector h_0 with length $\leq B$, by corollary (3.3), every reduced basis, b of L satisfies $|b_1| \leq 2^{(n-1)/2} B$; hence b_1 will be a multiple of h_0. Thus we can use the basis reduction algorithm instead.

To complete the algorithm we need to find h which satisfies (5.1) to (5.4). We can assume without loss of generality that f has no multiple factors. Otherwise we find $g = gcd(f, f')$, where f' is the derivative of f. Let $f_0 = f/g$. Then f_0 has no multiple factors; hence can be factorized by the following algorithm. We can factorize g recursively in the same way.

By employing the subresultant algorithm [4] we calculate the resultant $R(f, f')$, which is nonzero as f has no multiple factors. Next we choose a prime number p which does not divide $R(f, f')$ and decompose (f *mod* p) into irreducible factors using Berlecamp's algorithm []. Note that $R(f.f')$ upto sign is equal to (characteristic of f) $\times$ (leading coeff. of f). Hence $p \not| R(f, f')$ guarantees that (f *mod* p) has degree n and that it has no multiple factors in $\mathbf{F}_p[x]$. Hence (5.4) is valid for every irreducible factor (h *mod* p) of (f *mod* p) in $\mathbf{F}_p[x]$. Leading coefficient of (h *mod* p) in $\mathbf{F}_p[x]$ can always be chosen to be 1 as $\mathbf{F}_p$ is a field. Thus (5.1) is also satisfied.

Next we modify h, without modifying (h *mod* p), in such a way that (5.2) holds for the value of k computed in the algorithm above in addtion to (5.1), (5.3) and (5.4). This can be achieved by Hensel's lemma []. Thus we find h which satisfies (5.1) to (5.4).

Now one can find h_0 as explained before. The same procedure can be applied recursively to f/h_0 until the factorization is complete.

As the basis reduction, Berlecamp's factorization over prime field and 'lifting' through Hensel's lemma can all be done in polynomial time, it is obvious that the algorithm is polynomial time.

6. Integer Programming

The integer linear programming problem is as follows. Given $m \times n$ and $m \times 1$ matrices A and b of integers, determine whether there is a x in $\mathbf{Z}^n$ such that $Ax \leq b$. The general problem is

NP-complete, however if the number of variables is fixed the problem can be solved in polynomial time. In this section we give such an algorithm, due to H.W.Lenstra.

Consider the closed convex set $K = \{x : \mathbf{R}^n \mid Ax \leq b\}$. We want to decide if $K \cap \mathbf{Z}^n = \phi$. It can be shown that if $K \cap \mathbf{Z}^n \neq \phi$ then it is possible to find a $z \in K \cap \mathbf{Z}^n$ whose coefficients are bounded by some constant $c(n, a)$, where a is a bound on absolute values of the coefficients in A or b. If necessary, we add these inequalities for all the coefficients. Hence without loss of generality we can assume that K is bounded.

It is possible that K has zero volume. This will happen if the dimension, d, of K is less than n. In this case we reduce the problem to an equivalent problem in a lower dimension so that K has nonzero volume in that dimension.

Towards this end one attempts to find independent vertices $v_0, \ldots, v_{d-1}$ of K such that $K - v_0$ lies in a d-dimensional affine space V spanned by $v_1 - v_0, \ldots, v_{d-1} - v_0$; d can be equal to n. By maximizing some arbitary nonzero linear function, f, on K one finds a vertex v_0 of K. For maximization of linear functions one can use Khachian's polynomial time algorithm. Suppose, inductively, that vertices $v_0, \ldots, v_c$ of K have been found for which $v_1 - v_0, \ldots, v_c - v_0$ are linearly independent, with $c < n$. Note that every l dimensional affine space W in $\mathbf{R}^n$ can be characterized by some $n - l$ linear functions $f_1, \ldots, f_{n-l}$ as:

$$W = \{x \in \mathbf{R}^n \mid f_1(x) = \ldots = f_{n-l}(x) = 0\}$$

Let $f_1, \ldots, f_{n-c}$ be the linear functions charecterizing V_c, the affine spanned by the vertices $v_0, \ldots, v_c$. Maximize $\pm f_1, \ldots, \pm f_{n-c}$ on K. If K does not lie in V_c then this will give some vertex v_{c+1} of K such that $\pm f_1(v_{c+1}), \ldots, \pm f_{n-c}(v_{c+1})$ are not all zero. If this occurs then $v_1 - v_0, \ldots, v_{c+1} - v_0$ are linearly independent and the inductive step of the algorithm is completed.

Else K lies in V_c; so $c = d$. If $c = d < n$ then we reduce the problem to an equivalent one d dimension. If $c = d = n$ then the next stage of the algorithm can be bypassed.

So assume that $d < n$. V_d as usual is the affine space spanned by $v_0, \ldots, v_d$. Note that the coordinates of $v_0, \ldots, v_d$ are all rational. We next change the basis of $\mathbf{R}^n$ such that the hyperplane spanned by new basis vectors $b_1, \ldots, b_d$ is parallel to V_d *without disturbing* the lattice $\mathbf{Z}^n$. This means that a transformation matrix U should be an integer matrix with determinant ± 1. Such an U can be found in polynomial time by the Hermite normal form algorithm of Kannan and Bachem[3]. In this new coordinate system V_d can be characterized as:

$$V_d = \{x \mid x_{d+1} = c_{d+1}, \ldots, x_n = c_n\}$$

for some easily computable constants $c_{d+1}, \ldots, c_n$. As K is contained in V_d, if $c_{d+1}, \ldots, c_n$ are not all integers then we know that the original problem was unsolvable. Othewise substitute $x = U^{-1}[y_1, \ldots, y_d, c_{d+1}, \ldots, c_n]^T$ in our original system $Ax \leq b$. We then see that the problem is equivalent to an integer problem with d variables $y_1, \ldots, y_d$.

Without loss of generality we can now assume that in the original problem

(1) K is bounded.

(2) K is full dimensional; i.e it has positive volume and dimension n.

In the next stage we find in polynomial time a homogenous transformation τ such that τK is 'spherical'. More precisely,

$$B(p, r) \subset \tau K \subset B(p, R), \qquad R/r \leq 2n^{3/2} \tag{6.1}$$

where $B(y, s)$ is ball of radius s with y as centre.

Denote by $vol(v_0, \ldots, v_n)$ the volume of the n-simplex spanned by $v_0, \ldots, v_n$. Then we try to find in polynomial time the vertices $v_0, \ldots, v_n$ such that $vol(v_0, \ldots, v_n)$ is sufficiently maximal. More precisely, for any other vertex v of K:

$$vol(v_0, \ldots, v_{i-1}, v, v_{i-1}, \ldots, v_n) \leq \tfrac{3}{2} vol(v_0, \ldots, v_{i-1}, v_i, v_{i-1}, \ldots v_n) \quad \text{for all } i \tag{6.2}$$

Consider any vertex v_i. We want to know if there exists a vertex v of K which after replacing v_i will increase the volume of the n-simplex by a factor $> 3/2$. Let H_i be the hyperplane spanned by $v_0, \ldots, v_{i-1}, v_{i-1}, \ldots, v_n$. Let g_i be the function which characterizes H_i, i.e.:

$$H_i = \{x \mid g_i(x) = 0\}$$

Then

$$\begin{aligned} &vol(v_0, \ldots, v_{i-1}, v, v_{i-1}, \ldots, v_n)/vol(v_0, \ldots, v_{i-1}, v_i, v_{i-1}, \ldots, v_n) \\ &\quad = |g_i(v - v_j)|/|g_i(v_i - v_j)| \end{aligned}$$

as for any $x \in H_i$,$|g_i(v - x)|$ is proportional to the perpendicular distance of v from H_i. Thus it suffices to check by Khachian's algorithm whether there exists a vertex v of K such that

$$|g_i(v - v_j)|/|g_i(v_i - v_j)| > 3/2$$

As every replacement increases volume by 3/2 and K is bounded, after some polynomial number of iterations the replacement will stop and (6.2) will hold.

Let τ be an endomorphism such that $\tau(v_0), \ldots, \tau(v_n)$ span a regular simplex. Let $p = \frac{1}{n-1}\sum_{j=0}^{n} \tau(v_j)$. It can be shown that for certain r and R (6.1) is satisfied. Of course τ can be irrational, in that case one has to consider a rational approximation to τ.

The original problem is now equivalent to checking whether $\tau K \cap L = \phi$, where L is the lattice generated by the columns of τ. Remember that:

$$B(p, r) \subset \tau K \subset B(p, R), \qquad R/r \leq c_1$$

where $c_1 = 2n^{3/2}$. Let $b_1, \ldots, b_n$ be the reduced basis for L found by the basis reduction algrithm given before. It is easy to see that there exists a $q \in L$ such that $p - q \in \sum_{i=1}^{n} r_i b_i$ where $-1/2 \leq r_i \leq 1/2$. Then $|p - q| \leq 1/2(|b_1| + \cdots + |b_n|)$. Assume without loss of generality that $|b_n| = max\{|b_i|\}$. Then $|p - q| \leq \frac{1}{2}n|b_n|$. If $q \in \tau K$ then we are done. Suppose $q \notin \tau K$. Then $q \notin B(p, r)$. Hence:

$$r < \tfrac{1}{2}n|b_n| \tag{6.3}$$

Let M be the lattice generated by $b_1, \ldots, b_{n-1}$ and H be the hyperplane generated by $b_1, \ldots, b_{n-1}$. We have:

$$L = M + \mathbf{Z}b_n \subset H + \mathbf{Z}b_n = \textstyle\bigcup_{k \in \mathbf{Z}}(H + kb_n) \tag{6.4}$$

Hence L is contained in the union of countably many parallel hyperplanes seperated by some distance h. As $d(L) = h.d(M)$ and the basis is reduced,

$$\textstyle\prod_{i=1}^{n} |b_i| \leq c_2.d(L) = c_2.h.d(M) \leq c_2.h.\prod_{i=1}^{n1} |b_i|$$

where $c_2 = 2^{n(n-1)\ 4}$. Hence,

$$h > c_2^{-1} |b_n| \tag{6.5}$$

Let t be the number of hyperplanes which cut τK. Then $t - 1 \leq \frac{2R}{h}$. By (6.1),(6.3) and (6.5) we conclude that $t = O(c1.c2.n)$. Hence the number of values for k that have to be considered in (6.4) is bounded by a constant depending on only n.

If we fix the value of k then we need restrict our attention to only those $x = \sum_{i=1}^{n} y_i b_i$ for which $y_n = k$. This leads to an integer programming problem with $n - 1$ variables $y_1, \ldots, y_{n-1}$. Each of the $O(c_1 c_2 n)$ lower dimendional problems can be treated recursively. The case of dimension $n = 0$ can serve as a basis for the recursion. The algorithm is polynomial time but severely depends on n. This is so because c_1 and c_2 are exponential in n.

Note that if $K \bigcap \mathbf{Z}^n$ is nonempty then the algorithm actually produces an element belonging to the intersection.

ACKNOWLEDMENT: I wish to thank Ravi Kannan for helpful discussions.

7. Bibliography

(1) Cassels, J.W.S: An Introduction To The Geometry Of Numbers, Springer, Heidelberg 1959.

(2) Gacs,Peter,Lovasz Laszlo: Khachian's Algorithm For Linear Programming, Technical Report, Stanford University.

(3) Kannan,R.,Bachem,A.: Polynomial Algorithms For computing The Smith And Hermite Norm Forms Of an Integer Matrix, SIAM J. on comp. 8(1979).

(4) Knuth,D.E: The Art Of Computer Programming, Vol 2, Seminumerical Algorithms, Addison-Wesley, Reading, second edition 1981.

(5) Lenstra,A.K: Lattices And Factorization Of Polynomials, Preprint,Mathematisch Centrum, Amsterdam 1981.

(6) Lenstra,A.K, Lenstra, H.W.,Jr.,Lovasz,L.: Factoring Polynomials With Rational Coefficients, Report 82-05, Mathematisch Instituut,Universiteit Amsterdam 1982.

(7) Lenstra,H.W,Jr. :Integer Programming With a Fixed Number Of Variables, Report 81-03, Mathematisch Instituut, University van Amsterdam 1981.

(8) Mignotte,M.:An Inequality About Factors Of Polynomials,Math. Comp. 28 (1974),1153-1157. Van Der Waerden,B.L.: Algebra,Vol 1,Frederick Ungar Publishing Co., New York, 1970.