NOTES ON IRRATIONALITY AND TRANSCENDENCE

Frits Beukers

September 17, 2007

2 Lattices and Lattice-reduction

2.1 Lattices

Consider $\mathbb{R}^n$ with the standard inner product, which we denote by $\mathbf{v} \cdot \mathbf{w}$.

Lemma 2.1.1 *Let G be an additive subgroup of $\mathbb{R}^n$. Then G is discrete in $\mathbb{R}^n$ if and only if there exist $\mathbb{R}$-linear independent elements $\mathbf{v}_1, \ldots, \mathbf{v}_r \in G$ such that $G = \{x_1\mathbf{v}_1 + \ldots + x_r\mathbf{v}_r \mid x_1, \ldots, x_r \in \mathbb{Z}\}$*

Proof Suppose $G = \{x_1\mathbf{v}_1 + \ldots + x_r\mathbf{v}_r \mid x_1, \ldots, x_r \in \mathbb{Z}\}$ with $\mathbf{v}_1, \ldots, \mathbf{v}_r$ $\mathbb{R}$-linear independent. Let μ be the minimum of $|x_1\mathbf{v}_1 + \ldots + x_r\mathbf{v}_r|$ as $x_1, \ldots, x_r$ run over all real numbers such that $x_1^2 + \cdots + x_r^2 = 1$. Since the $\mathbf{v}_i$ are independent this minimum is non-zero. Hence we have for any $x_1, \ldots, x_n \in \mathbb{R}$ that

$$|x_1\mathbf{v}_1 + \ldots + x_r\mathbf{v}_r| \geq \mu\sqrt{x_1^2 + \cdots + x_r^2}.$$

Hence for any non-zero $\mathbf{v} \in G$ we get $|\mathbf{v}| \geq \mu$, hence G is discrete.
Suppose conversely that G is discrete. Let r be the dimension of the $\mathbb{R}$-linear span of G and choose r $\mathbb{R}$-independent elements $\mathbf{w}_1, \ldots, \mathbf{w}_r$ of G. Consider the set

$$F = \{\mathbf{x} \in G \mid \mathbf{x} = \mu_1\mathbf{w}_1 + \cdots + \mu_r\mathbf{w}_r,\ \forall i : 0 \leq \mu_i \leq 1\}.$$

Since G is discrete, the set F is finite. For each $i = 1, \ldots, r$ we choose $\mathbf{v}_i \in F$ such that $\mathbf{v}_i = \mu_i\mathbf{w}_i + \cdots + \mu_r\mathbf{w}_r$ with $\mu_i > 0$ and minimal. Since $\mathbf{w}_i \in F$, such an element allways exists. Clearly the $\mathbf{v}_i$ are also $\mathbb{R}$-linear independent. Let $\mathbf{v} \in G$ and write $\mathbf{v} = \sum_{i=1}^r \lambda_i\mathbf{v}_i$. Let for each i, ν_i be equal to λ_i minus its largest integral part. Then $\mathbf{v}' := \sum_{i=1}^r \nu_i\mathbf{v}_i$ is also an element of G. We assert that $\nu_i = 0$ for all i. Suppose not, then choose j minimal such that $\nu_j > 0$. Then $\mathbf{v}'$ written with respect to the $\mathbf{w}_i$ looks like $\mathbf{v}' = \nu_j\mu_j\mathbf{w}_j + \cdots$, contradicting the minimality in our choice of $\mathbf{v}_j$. □

Definition 2.1.2 *A lattice in $\mathbb{R}^n$ is a discrete subgroup of the additive group $\mathbb{R}^n$.*

A set of independent generators of a lattice L is called a *(lattice) basis*. The *rank* of a lattice L is the usual one in the sense of linear algebra and it equals the number of elements of a lattice basis.

Lemma 2.1.3 *Let* $\mathbf{w}_1, \ldots, \mathbf{w}_r$ *and* $\mathbf{v}_1, \ldots, \mathbf{v}_r$ *be any two bases of a lattice* L*. Then there exists an* $r \times r$*-matrix* M *with integral entries* m_{ij} *and* $\det(M) = \pm 1$ *such that* $\mathbf{w}_i = \sum_{j=1}^{r} m_{ij}\mathbf{v}_j$ *for* $i = 1, \ldots, r$*.*

Proof Since $\{\mathbf{v}_i\}_i$ and $\{\mathbf{w}_i\}_i$ are bases of L, there exist $r \times r$-matrices M, N with integral entries m_{ij}, n_{ij} resepctively such that $\mathbf{w}_i = \sum_{j=1}^{r} \mathbf{v}_j$ and $\mathbf{v}_i = \sum_{j=1}^{r} n_{ij}\mathbf{w}_j$ for all i. Hence $MN = \mathrm{Id}_r$ and $\det(M)\det(N) = 1$. Since both determinants are integers we conclude that $\det(M) = \det(N) = \pm 1$. □

Definition 2.1.4 *Let* L *be a lattice of rank* r *and let* $\mathbf{v}_1, \ldots, \mathbf{v}_r$ *be any basis of* L*. Then the set*

$$\{\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \cdots + \lambda_r\mathbf{v}_r \mid 0 \leq \lambda_i < 1\}$$

is called a fundamental domain of L*.*

Let V be the space spanned by L and let F be a fundamental doamin. Notice that to any point in $\mathbf{x} \in V$ there exists a unique point $\mathbf{y} \in F$ such that $\mathbf{x} - \mathbf{y} \in L$. In this way the fundamental domain is a set of representatives for the quotient group V/L. Moreover, by standard linear algebra the volume of such a fundamental domain is the square root of $\det(\mathbf{v}_i \cdot \mathbf{v}_j)$. Thus we see that.
The matrix $(\mathbf{v}_i \cdot \mathbf{v}_j)_{i,j=1,\ldots,r}$ is called the *Gram-matrix* of $\mathbf{v}_1, \ldots, \mathbf{v}_r$. Note that the Gram-matrix is symmetric with positive eigenvalues. Hence its determinant is positive and we can take its square root.

Definition 2.1.5 *Let* L *be a lattice in* $\mathbb{R}^n$*. Let* $\mathbf{v}_1, \ldots, \mathbf{v}_r$ *be a basis of* L*. Then we define the* <u>determinant</u> *of a lattice by* $\sqrt{\det(\mathbf{v}_i \cdot \mathbf{v}_j)}$*. Notation:* $d(L)$*.*

In particular,

$$\mathrm{Vol}(F) = \sqrt{\det(\mathbf{v}_i \cdot \mathbf{v}_j)} = d(L).$$

Using the above Lemma one can verify that the determinant of a lattice is independent of the choice of basis, as it should be.
An explanation for the term determinant of a lattice is given by the following important special case.

Lemma 2.1.6 *Consider a lattice* L *in* $\mathbb{R}^n$ *of maximal rank* n*. Let* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *be a basis of* L*. Denote* $\mathbf{v}_i = (v_{i1}, \ldots, v_{in})$*. Then the determinant of* L *is given by* $|\det(v_{ij})|$*.*

Proof Let V be the $n \times n$-matrix whose entry on the i-th row and j-th column is denoted by v_{ij}. Let W be the matrix whose at the i-th and j-th column is $\mathbf{v}_i \cdot \mathbf{v}_j$. Then notice that $W = V \cdot V^t$ where V^t is the transpose of V. Hence

$$\det(L) = \sqrt{\det(W)} = \sqrt{\det(V)^2} = |\det(V)|.$$

□

From the theory of lattices we have two theorems which we shall not prove here.

Theorem 2.1.7 (Minkowski) *Let L be a lattice of rank r and determinant $d(L)$. Let C be a closed convex set in the space spanned by L. We assume that C is symmetric around the origin. If the r-dimensional volume of C is bigger or equal than $2^r d(L)$, then C contains an element of $L \setminus \mathbf{0}$.*

Corollary 2.1.8 *Let L be a lattice of rank r and determinant $d(L)$. Let $\mathbf{v}$ be a shortest non-trivial vector in L. Then*

$$|\mathbf{v}| \leq 2\left(d(L)/\mathrm{Vol}(B_r)\right)^{1/r},$$

where B_r is the unit sphere in $\mathbb{R}^r$.

The proof of the Corollary goes like this. Consider the sphere in $\mathbb{R}^r$ with center at the origin and radius $\rho = 2(d(L)/\mathrm{Vol}(B_r))^{1/r}$. Then its volume is equal to $\mathrm{Vol}(B_r)\rho^r = 2^r d(L)$. According to Minkowski's Theorem this sphere contains a non-trivial vector. Hence the shortest non-trivial vector in L has length $\leq \rho$, which proves the Corollary. □

We add that $\mathrm{Vol}(B_r) = \pi^{r/2}/\Gamma(1+r/2)$. As B_r contains the (hyper)-cube all of whose vertices have coordinates $\pm 1/\sqrt{r}$ we have that $\mathrm{Vol}(B_r) \geq (2/\sqrt{r})^r$. As a consequence we find that $|\mathbf{v}| \leq \sqrt{r} d(L)^{1/r}$.
An important question with many applications is the following one.

Question 2.1.9 *Given a basis of a lattice L. Determine a non-zero vector in L with minimal length.*

A possible application would be the determination of $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$ for a prime p with $p \equiv 1 \pmod 4$.

Example Let p be a prime with $p \equiv 1 \pmod 4$. Find $z \in \mathbb{Z}$ such that $z^2 \equiv -1 \pmod p$ (there exist algorithms to do this quickly). Consider the lattice

$$L = \{(x, y) \in \mathbb{Z}^2 |\ x \equiv zy \pmod p\}.$$

Check that $(p, 0)$ and $(z, 1)$ form a basis of L. Hence $d(L) = p$. Denote a shortest non-zero vector in L by (a, b). By Minkowski's theorem we have that $|(a, b)|^2 \leq 4p/\pi$, hence $a^2 + b^2 < 2p$. On the other hand, $a^2 + b^2 \equiv (bz)^2 + b^2 \equiv 0 \pmod p$. Hence p divides $a^2 + b^2$ and we conclude that $p = a^2 + b^2$.

Here is another theorem about the relation between lattices and convex sets.

Theorem 2.1.10 *Let L be a lattice of rank r and determinant $d(L)$. Let C be a convex set in the space spanned by L with positive r-dimensional volume V. Denote by λC the set $\{\lambda \mathbf{x} | \mathbf{x} \in C\}$ for every real number λ. Denote by $N(\lambda)$ the number of lattice points in λC. Then,*

$$\lim_{\lambda \to \infty} \frac{N(\lambda)}{\lambda^r} = \frac{V}{d(L)}.$$

Corollary 2.1.11 *Let L be a lattice of rank r and let M be a sublattice of L of the same rank. Then the additive group L/M has finite order $[L:M]$ and we have that*

$$[L:M] = \frac{d(M)}{d(L)}.$$

We can see this by application of the previous theorem, when we use for C a fundamental domain of M. Clearly, $[L:M]$ equals the number of points of L contained in C. For any integer $m > 0$ the domain mC contains $m^r[L:M]$ points. Application of the Theorem now gives us

$$\lim_{m\to\infty} \frac{m^r[L:M]}{m^r} = \frac{\mathrm{Vol}(C)}{d(L)} = \frac{d(M)}{d(L)},$$

from which our Corollary follows. □

2.2 Siegel's Lemma

One of the most important tools in transcendence theory and diophantine approximation is the so-called Siegel Lemma. It allows us to show the existence of 'small' integral solutions to systems of linear equations.

Theorem 2.2.1 (Siegel's Lemma) *Let a_{ij} with $i = 1,\ldots,m$ and $j = 1,\ldots,n$ be integers, not all zero, and suppose that $A = \max_{i,j}|a_{ij}|$. Then the system of linear equations*

$$\sum_{i=1}^{n} a_{ij}x_j = 0, \qquad i = 1,\ldots,m$$

has a non-trivial solution in the integers $x_1, x_2, \ldots, x_n$ with the property that

$$\max_j |x_j| \le (nA)^{m/(n-m)}.$$

A remarkable application is for example the following. Take 10 integers $a_1, a_2, \ldots, a_{10}$ of ten digits each. Suppose we want to find integers $x_1, x_2, \ldots, x_{10}$, not all zero, such that

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0.$$

Siegel's Lemma with $A = 10^{10}, m = 1, n = 10$ tells us that we can find such x_i of absolute value at most 16. Surprisingly small given the size of the numbers a_i.

Proof of Siegel's Lemma. Choose an integer Q. For every i let n_i be the number of coefficients a_{ij} that are ≥ 0. Then the number of negative coefficients a_{ij} is of course $n - n_i$.
Let $B(Q)$ be the box consisting of points $(x_1,\ldots,x_n)$ with $x_1,\ldots,x_n$ integers with $0 \le x_i \le Q$. Consider the map $\phi : B(Q) \to \mathbb{Z}^m$ given by $\phi : (x_1,\ldots,x_n) \mapsto (\sum_{j=1}^n a_{1j}x_j, \ldots, \sum_{j=1}^n a_{mj}x_j)$. The image of $B(Q)$ is contained in the box

$$[(n_1-n)AQ, n_1AQ] \times [(n_2-n)AQ, n_2AQ] \times \cdots \times [(n_m-n)AQ, n_mAQ].$$

The number of points with integral coordinates in this box is precisely $(nAQ+1)^m$. The number of points in $B(Q)$ is precisely $(Q+1)^n$. So if $(Q+1)^n > (nAQ+1)^m$, then ϕ is not surjective and we find two integral vectors $\mathbf{x}_1, \mathbf{x}_2$ in $B(Q)$ such that $\phi(\mathbf{x}_1 - \mathbf{x}_2) = 0$. In other words, $\mathbf{x}_1 - \mathbf{x}_2$ is a solution of our system of equations. In addition, the components of this difference are all bounded by Q in absolute value. A straightforward calculation shows that $(Q+1)^n > (nAQ+1)^m$ is satisfied if we choose $Q = [(nA)^{m/(n-m)}]$. □

2.3 Lattice reduction in dimension 2

In case $n = 2$ there is a very efficient algorithm to find shortest vectors in lattices. Let L be a lattice in $\mathbb{R}^2$ with basis $\mathbf{v}_1, \mathbf{v}_2$ and assume $|\mathbf{v}_2| \geq |\mathbf{v}_1|$.
Algorithm **Euclid**:

loop:

Choose $k \in \mathbb{Z}$ such that $-\frac{1}{2}\mathbf{v}_1 \cdot \mathbf{v}_1 < (\mathbf{v}_2 - k\mathbf{v}_1) \cdot \mathbf{v}_1 \leq \frac{1}{2}\mathbf{v}_1 \cdot \mathbf{v}_1$

$\mathbf{v}_2 := \mathbf{v}_2 - k\mathbf{v}_1$.

If $|\mathbf{v}_2| \geq |\mathbf{v}_1|$ stop

Else interchange $\mathbf{v}_1$ and $\mathbf{v}_2$ and goto **loop**.

We assert that this algorithm terminates and that $\mathbf{v}_1$ is a shortest non-zero vector in L and $\mathbf{v}_2$ is a shortest vector in $L \setminus \{c\mathbf{v}_1 |\ c \in \mathbb{R}\}$.
Proof First we show termination. At the start of every loop the vector $\mathbf{v}_1$ is strictly smaller than at the start of the previous loop. Since every bounded disc contains only finitely many elements of L (L is discrete), the algorithm terminates.
We now show correctness of our algorithm. Let $\mathbf{v}_1, \mathbf{v}_2$ be the result of the algorithm. In particular we have that $|\mathbf{v}_2 \cdot \mathbf{v}_1| \leq \frac{1}{2}|\mathbf{v}_1|^2$ and $|\mathbf{v}_2| \geq |\mathbf{v}_1|$. Choose any non-zero $\mathbf{v} \in L$. There exist $a, b \in \mathbb{Z}$ such that $\mathbf{v} = a\mathbf{v}_1 + b\mathbf{v}_2$. Notice that

$$\begin{aligned} |\mathbf{v}|^2 &= a^2|\mathbf{v}_1|^2 + 2ab(\mathbf{v}_1 \cdot \mathbf{v}_2) + b^2|\mathbf{v}_2|^2 \\ &\geq a^2|\mathbf{v}_1|^2 - |ab||\mathbf{v}_1|^2 + b^2|\mathbf{v}_2|^2 \\ &\geq (a^2 - |ab| + b^2)|\mathbf{v}_1|^2 \geq |\mathbf{v}_1|^2 \end{aligned}$$

Hence $\mathbf{v}_1$ is a shortest vector. Now suppose $\mathbf{v}$ independent of $\mathbf{v}_1$, i.e. $b \neq 0$. Then,

$$\begin{aligned} |\mathbf{v}|^2 &\geq a^2|\mathbf{v}_1|^2 - |ab||\mathbf{v}_1|^2 + \frac{1}{4}b^2|\mathbf{v}_1|^2 + \frac{3}{4}b^2|\mathbf{v}_2|^2 \\ &= (|a| - |b|/2)^2|\mathbf{v}_1|^2 + \frac{3}{4}b^2|\mathbf{v}_2|^2 \\ &\geq |\mathbf{v}_2|^2 \quad \text{if } |b| > 1 \end{aligned}$$

If $b = \pm 1$ then

$$|\mathbf{v}|^2 \geq a^2|\mathbf{v}_1|^2 - |a||\mathbf{v}_1|^2 + |\mathbf{v}_2|^2 \geq |\mathbf{v}_2|^2.$$

Hence $\mathbf{v}_2$ is a shortest vector independent of $\mathbf{v}_1$. □

Lemma 2.3.1 *Let* $\mathbf{v}_1$ *be the result of the previous algorithm. Then* $|\mathbf{v}_1| \leq (4/3)^{1/4} d(L)^{1/2}$.

Proof We have $|\mathbf{v}_2| \geq |\mathbf{v}_1|$ and $|\mathbf{v}_1 \cdot \mathbf{v}_2| \leq \frac{1}{2}|\mathbf{v}_1|^2$. Notice that

$$\begin{aligned} d(L)^2 &= \begin{vmatrix} |\mathbf{v}_1|^2 & \mathbf{v}_1 \cdot \mathbf{v}_2 \\ \mathbf{v}_1 \cdot \mathbf{v}_2 & |\mathbf{v}_2|^2 \end{vmatrix} \\ &= |\mathbf{v}_1|^2 |\mathbf{v}_2|^2 - |\mathbf{v}_1 \cdot \mathbf{v}_2|^2 \\ &\geq |\mathbf{v}_1|^4 - \frac{1}{4}|\mathbf{v}_1|^4 = \frac{3}{4}|\mathbf{v}_1|^4 \end{aligned}$$

Taking fourth roots on both sides yields our inequality. □

Notice that the inequality sign of the previous Lemma becomes equality precisely when $|\mathbf{v}_1| = |\mathbf{v}_2|$ and $|\mathbf{v}_1 \cdot \mathbf{v}_2| = \frac{1}{2}|\mathbf{v}_1|^2$. This case corresponds to the hexagonal lattice.
The most important feature of Euclid's algorithm is its remarkably short runtime as shown by Exercise 2.7.10.

2.4 Lattice reduction in any dimension

In case $n \geq 3$ there are hardly any polynomial time, general purpose methods with a shortest lattice vector as garantueed output. However, in 1982 L.Lovasz, H.W.Lenstra and A.K.Lenstra proposed an algorithm which produces in polynomial time a lattice vector whose length is at most a known factor larger than the shortest possible length. Before describing the algorithm we review the Gram-Schmidt orthogonalisation procedure. Let $\mathbf{v}_1, \ldots, \mathbf{v}_r$ be (not necessarily independent) vectors in $\mathbb{R}^n$. Define recursively,

$$\begin{aligned} \mathbf{v}_1^* &= \mathbf{v}_1 \\ \mathbf{v}_i^* &= \mathbf{v}_i - \sum_{j<i}{}' \frac{\mathbf{v}_i \cdot \mathbf{v}_j^*}{|\mathbf{v}_j^*|^2} \mathbf{v}_j^* \qquad (i = 2, \ldots, r) \end{aligned}$$

where the ' sign in the summation denotes deletion of terms where $\mathbf{v}_j^* = 0$. The vectors $\mathbf{v}_i^*$ consist of (possibly) some zero vectors and an orthogonal basis of the space spanned by $\mathbf{v}_1, \ldots, \mathbf{v}_r$.
Notice that $|\mathbf{v}_k^*| \leq |\mathbf{v}_k|$ for all k and that $\det(\mathbf{v}_i \cdot \mathbf{v}_j) = \det(\mathbf{v}_i^* \cdot \mathbf{v}_j^*)$. Hence,

$$\det(\mathbf{v}_i \cdot \mathbf{v}_j) = \prod_{i=1}^{r} |\mathbf{v}_i^*|^2 \leq \prod_{i=1}^{r} |\mathbf{v}_i|^2.$$

This inequality is known as *Hadamard's inequality*. In particular, when $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is a basis of $\mathbb{R}^n$ we obtain

$$|\det(\mathbf{v}_1, \ldots, \mathbf{v}_n)| \leq \prod_{i=1}^{n} |\mathbf{v}_i|.$$

In the sequel, whenever we have a set of vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r$, we denote by $\mathbf{v}_1^*, \ldots, \mathbf{v}_r^*$ the result of the Gram-Schmidt procedure. The so-called *Gram-Schmidt coefficients* $\mathbf{v}_i \cdot \mathbf{v}_j^* / |\mathbf{v}_j^*|^2$ are denoted by μ_{ij}. We take $\mu_{ij} = 0$ if $\mathbf{v}_j^* = 0$.
In practice we shall only be interested in the inner products $\mathbf{v}_i \cdot \mathbf{v}_j^*$. To compute these products we use the following algorithm.
Algorithm **Gram-Schmidt**

$G := (\mathbf{v}_i \cdot \mathbf{v}_j)$

for i from 1 to n) do

if $G_{ii} \neq 0$ then

for j from $i+1$ to n do

substract G_{ij}/G_{ii} times the i-th column from the j-th column

od fi od

When the algorithm terminates the matrix G has the products $\mathbf{v}_i \cdot \mathbf{v}_j^*$ as entries.
We are now ready to discuss LLL-reduction.

Definition 2.4.1 *Let L be a lattice. A basis $\mathbf{b}_1, \ldots, \mathbf{b}_r$ of L is called LLL-reduced if*

$$|\mu_{ij}| \leq \frac{1}{2} \quad \text{whenever } 1 \leq j < i \leq r$$

and

$$|\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*|^2 \geq \frac{3}{4}|\mathbf{b}_{i-1}^*|^2 \quad \text{whenever } 1 < i \leq r.$$

The second condition can be rewritten as $|\mathbf{b}_i^*|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)|\mathbf{b}_{i-1}^*|^2$ and is known as Lovasz's condition. The vector $b_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*$ can be interpreted as the projection of b_i on the orthogonal complement of $\mathbf{b}_1, \ldots, \mathbf{b}_{i-2}$. In the special case $r = 2$ the conditions read, $|\mathbf{b}_2 \cdot \mathbf{b}_1| \leq |\mathbf{b}_1|^2$ and $|\mathbf{b}_2|^2 \geq \frac{3}{4}|\mathbf{b}_1|^2$.

Theorem 2.4.2 *Let $\mathbf{b}_1, \ldots, \mathbf{b}_r$ be an LLL-reduced basis of a lattice L. Then,*

1. $d(L) \leq \prod_{i=1}^r |\mathbf{b}_i| \leq 2^{r(r-1)/4} d(L)$.
2. $|\mathbf{b}_1| \leq 2^{(r-1)/4} d(L)^{1/r}$
3. *For every non-zero $\mathbf{x} \in L$ we have $|\mathbf{b}_1| \leq 2^{(r-1)/2}|\mathbf{x}|$.*
4. *For any linear independent vectors $\mathbf{x}_1, \ldots, \mathbf{x}_t \in L$ we have $|\mathbf{b}_j| \leq 2^{(r-1)/2} \max(|\mathbf{x}_1|, \ldots, |\mathbf{x}_t|)$ for $1 \leq j \leq t$.*

Proof First note the following inequalities,

$$\begin{aligned} |\mathbf{b}_i|^2 &= |\mathbf{b}_i^*|^2 + \mu_{i,i-1}^2|\mathbf{b}_{i-1}^*|^2 + \cdots + \mu_{i,1}^2|\mathbf{b}_1^*|^2 \\ &\leq |\mathbf{b}_i^*|^2 + \frac{1}{4}|\mathbf{b}_{i-1}^*|^2 + \cdots + \frac{1}{4}|\mathbf{b}_1^*|^2. \end{aligned}$$

Furthermore, $|\mathbf{b}_j^*|^2 \geq \frac{1}{2}|\mathbf{b}_{j-1}^*|^2$ as a consequence of the Lovasz condition. Hence $|\mathbf{b}_j^*|^2 \leq 2^{i-j}|\mathbf{b}_i^*|^2$ whenever $j \leq i$. Hence for all i we have

$$\begin{aligned} |\mathbf{b}_i|^2 &\leq \left[1 + \frac{1}{4}(2 + 2^2 + \cdots + 2^{i-1})\right] |\mathbf{b}_i^*|^2 \\ &= \frac{2^{i-1}+1}{2}|\mathbf{b}_i^*|^2 \leq 2^{i-1}|\mathbf{b}_i^*|^2. \end{aligned}$$

We are now ready to prove the statements of our theorem. First of all,

$$d(L) = \prod_{i=1}^{r} |\mathbf{b}_i^*| \leq \prod_{i=1}^{r} |\mathbf{b}_i| \leq 2^{r(r-1)/4} \prod_{i=1}^{r} |\mathbf{b}_i^*| = 2^{r(r-1)/4} d(L).$$

This proves part 1).
Secondly, whenever $1 \leq j < i \leq r$ we have

$$|\mathbf{b}_j| \leq 2^{(j-1)/2} |\mathbf{b}_j^*| \leq 2^{(i-j)/2} 2^{(j-1)/2} |\mathbf{b}_i^*| = 2^{(i-1)/2} |\mathbf{b}_i^*|.$$

Application of the latter inequality to the case $j = 1$ yields

$$|\mathbf{b}_1|^r \leq 2^{r(r-1)/4} |\mathbf{b}_1^*| |\mathbf{b}_2^*| \cdots |\mathbf{b}_r^*| = 2^{r(r-1)/4} d(L).$$

Hence $|\mathbf{b}_1| \leq 2^{(r-1)/4} d(L)^{1/r}$, which proves part 2).
Note that part 3) is a special case of 4) with $t = 1$.
For the proof of part 4) we choose k minimal such that $\mathbf{x}_1, \ldots, \mathbf{x}_t$ lie in the span of $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Suppose $\mathbf{x}_i = \sum_{1 \leq j \leq k} r_{ij} \mathbf{b}_j = \sum_{1 \leq j \leq k} s_{ij} \mathbf{b}_j^*$. Choose i such that $r_{ik} \neq 0$. Notice that the r_{ij} are integers and that $r_{ik} = s_{ik}$. Since $\mathbf{x}_1, \ldots, \mathbf{x}_t$ are independent we have $k \geq t$. Observe that

$$|\mathbf{x}_i|^2 \geq s_{ik}^2 |\mathbf{b}_k^*|^2 = r_{ik}^2 |\mathbf{b}_k^*|^2 \geq |\mathbf{b}_k^*|^2.$$

So, whenever $j < k$,

$$|\mathbf{b}_j|^2 \leq 2^{k-1} |\mathbf{b}_k^*|^2 \leq 2^{k-1} |\mathbf{x}_i|^2 \leq 2^{r-1} \max(|\mathbf{x}_1|^2, \ldots, |\mathbf{x}_t|^2).$$

In particular, since $k \geq t$, this inequality holds whenever $j \leq t$. □

Let us now give an informal description of the LLL-reduction procedure applied to any k-tuple of vectors $\mathbf{b}_1, \ldots, \mathbf{b}_k$.

Algorithm **LLL-reduction**. Suppose $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ are LLL-reduced (true if $k = 2$). Replace $\mathbf{b}_k$ by $\mathbf{b}_k - \sum_{j<k} a_j \mathbf{b}_j$ with $a_j \in \mathbb{Z}$ in such a way that $|\mu_{k,j}| \leq 1/2$ whenever $j < k$. Suppose $|\mathbf{b}_k^*|^2 \geq (3/4 - \mu_{k,k-1}^2) |\mathbf{b}_{k-1}^*|^2$. Then $\mathbf{b}_1, \ldots, \mathbf{b}_k$ is LLL-reduced and we can stop. If the Lovasz condition is not satisfied we interchange $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$, apply LLL-reduction to $\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}$ and repeat the procedure.

Now apply LLL-reduction to the basis $\mathbf{b}_1, \ldots, \mathbf{b}_r$ of a lattice L. It is clear that if the algorithm terminates we have obtained an LLL-reduced basis of L. It remains to show that the algorithm actually terminates. To this end we introduce the quantities

$$d_i = \det((\mathbf{b}_s \cdot \mathbf{b}_t)_{s,t=1,\ldots i})$$

for $i = 1, \ldots, r$. In particular, $d_r = d(L)^2$. Let

$$D = \prod_{i=1}^{r-1} d_i.$$

During the LLL-reduction this quantity changes only value when two vectors $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$ are interchanged. In fact, only d_{k-1} changes value in that case. A simple computation shows that the new value will be $d'_{k-1} = d_{k-1}|\mathbf{b}^*_k + \mu_{k,k-1}\mathbf{b}^*_{k-1}|^2/|\mathbf{b}^*_{k-1}|^2$. Since we had to interchange $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$ the Lovasz condition is apparently not satisfied and so we get $d'_{k-1} \leq \frac{3}{4}d_{k-1}$. Hence D gets reduced by a factor $3/4$. Note that D has a lower bound which depends only on the lattice and not on the choice of basis. This can be seen as follows. Let l be the length of the shortest non-zero vector in L. Minkowski's theorem applied to the lattice generated by the first i vectors shows that $l \leq \sqrt{i}d_i^{1/2i}$ for each $i = 1, \ldots, r$. Hence $d_i \geq (l^2/i)^i$ and so, $D \geq (l^2/r)^{r(r-1)/2}$. In particular we see that the number of interchanges in the LLL-reduction is bounded by $O(\log D + r^2 \log(\sqrt{r}/l))$ and so the algorithm terminates.

2.5 Implementations of the LLL-algorithm

It turns out to be possible to give very simple implementations of the LLL-algorithm. Here we shall give a version which requires only operations on the Gram-matrix and an auxiliary matrix which keeps a record of the transformation between the original basis and the transformed basis. Our first observation is that the matrix $(\mathbf{b}_i \cdot \mathbf{b}^*_j)_{i,j=1,\ldots,r}$ can be obtained by putting the Gram-matrix of $(\mathbf{b}_i \cdot \mathbf{b}_j)$ into column echelon form by the algorithm **Gram-Schmidt** sketched above. The second observation is that replacement of $\mathbf{b}_k$, say, by $\mathbf{b}_k - \sum_{j<k} a_j\mathbf{b}_j$ does not change the corresponding vectors $\mathbf{b}^*_i$. The third observation is more subtle. If we interchange $\mathbf{b}_{k-1}$ and $\mathbf{b}_k$ and apply Gram-Schmidt to the newly ordered set, we obtain a new orthogonal system $\{\mathbf{b}^{**}_i\}_i$. Notice however, that $\mathbf{b}^{**}_i = \mathbf{b}^*_i$ if $i \neq k, k-1$ and that

$$\mathbf{b}^{**}_{k-1} = \mathbf{b}^*_k + \frac{\mathbf{b}_k \cdot \mathbf{b}^*_{k-1}}{|\mathbf{b}^*_{k-1}|^2}\mathbf{b}^*_{k-1}$$

and

$$\begin{aligned}\mathbf{b}^{**}_k &= \mathbf{b}^*_{k-1} - \frac{\mathbf{b}_{k-1} \cdot \mathbf{b}^{**}_{k-1}}{|\mathbf{b}^{**}_{k-1}|^2}\mathbf{b}^{**}_{k-1} \\ &= \mathbf{b}^*_{k-1} - \frac{\mathbf{b}_k \cdot \mathbf{b}^*_{k-1}}{|\mathbf{b}^{**}_{k-1}|^2}\mathbf{b}^{**}_{k-1}\end{aligned}$$

Based on these observations we can propose the following implementation. Suppose we want to carry out LLL-reduction on the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. We introduce the $n \times n$ matrix H to keep a record of the relation between the (partially) reduced set of vectors and the original $\mathbf{b}_i$. We initialise H either to the matrix whose rows are the $\mathbf{b}_i$ or to the $n \times n$-identity matrix. The $n \times n$-matrix G will be used to carry out the reduction. We initialise it by the reduced Gram matrix $(\mathbf{b}_i \cdot \mathbf{b}^*_j)$. For the purpose of the algorithm we concatenate the matrices G and H to $(G|H)$. We have two procedures which will be the building blocks of our LLL-reduction. These procedures affect the matrix $(G|H)$ which is assumed to be a global variable. The integer k in the input is assumed to satisfy $1 \leq k \leq n$.

Procedure **reduce**(k,l). We assume that $l<k$ and that the G-part of $(G|H)$ is in lower triangular form. If $G_{l,l}=0$ we do nothing. If $G_{l,l}\neq 0$ we choose the nearest integer q to $G_{k,l}/G_{l,l}$ and substract q times the l-th row of $(G|H)$ from the k-th row of $(G|H)$.

Procedure **swap**(k). We assume that the G-part of $(G|H)$ is in lower diagonal form. Interchange the k-th and $k-1$-st row in $(G|H)$. Interchange the k-th and $k-1$-st column in G. Add $G_{k-1,k}/G_{k,k}$ times the k-th column to the $k-1$-st column of G. Add a suitable multiple of the $k-1$-st column of G to the k-th column so that the element at place $k-1,k$ becomes zero.

The LLL-algorithm proceeds as follows. We initialise G and H to the reduced Gram matrix and the matrix of $\mathbf{b}_i$'s respectively and then apply the following procedure with $k=n$.

Procedure **LLL**(k).

if $k=1$ then stop fi;

LLL$(k-1)$; lovasz:=False;

while lovasz=False do

if $G_{k-1,k-1}=0$ then stop fi;

reduce$(k,k-1)$;

$\mu := G_{k-1,k}/G_{k-1,k-1}$;

lovasz:=$(G_{k,k}\geq (0.75-\mu^2)G_{k-1,k-1})$;

if lovasz=True then

for l from 1 to $k-1$ do **reduce**$(k,k-l)$) od;

else **swap**(k); **LLL**$(k-1)$ fi;

If we do not know the $\mathbf{b}_i$ explicitly, but only the Gram matrix, we can initialise H to the $n\times n$ identity matrix. After finishing the algorithm the matrix H will be the transformation matrix between the $\mathbf{b}_i$ and the reduced basis.
One may notice that we can apply this algorithm without any change to a set of vectors $\mathbf{b}_i$ which is not necessarily $\mathbb{R}$-linear independent, but where it is known that they generate a (discrete) lattice. Let $\mathbf{b}'_1,\ldots,\mathbf{b}'_n$ be the outcome of **LLL**. If the rank of the $\mathbf{b}_i$ is r, then $\mathbf{b}'_i=0$ for $i=1,\ldots,n-r$ and the remaining $\mathbf{b}'_i$ will be a reduced based of the lattice generated by the $\mathbf{b}_i$. In the case of dependent input vectors we have to recheck our termination proof of **LLL**. However, we can simply use the quantities $d'_k=\prod_{i=1,G_{i,i}\neq 0}^{k} G_{i,i}$ instead of the d_k.

2.6 Small linear forms

The first application was by its inventors, who used it to construct a polynomial time algorithm to factor polynomials in $\mathbb{Z}[x]$. The application we have in mind here is finding $\mathbb{Z}$-linear combinations of a given set of real numbers with very small values. What is meant by 'small' is indicated by the following theorem of Dirichlet.

Theorem 2.6.1 *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ and $A = \sum_{i=1}^{r} |\alpha_i|$. To every $M \in \mathbb{N}$ there exist $m_1, \ldots, m_n \in \mathbb{Z}$, not all zero, such that $|m_i| < M$ for all i and $|m_1\alpha_1 + \cdots + m_n\alpha_n| < A/M^{n-1}$.*

Proof We may assume that $\alpha_i \geq 0$ for all i. Consider the set

$$B = \{k_1\alpha_1 + \cdots + k_n\alpha_n \mid \forall i : \ k_i \in \mathbb{Z}, 0 \leq k_i < M\}$$

Note that $\#B = M^n$ and $0 \leq x \leq A(M-1)$ for each $x \in B$. Divide the interval $[0, A(M-1)]$ into $M^n - 1$ subintervals of equal length. Since $\#B = M^n$ there exist at least one interval containing at least two elements of B, say $k_1\alpha_1 + \cdots + k_n\alpha_n$ and $k_1'\alpha_1 + \cdots + k_n'\alpha_n$. We have applied the so-called "box principle" or "pigeon hole principle" here. Let $m_i = k_i - k_i'$ for all i then we conclude that $|m_1\alpha_1 + \cdots + m_n\alpha_n| \leq A(M-1)/(M^n - 1) < A/M^{n-1}$ and not all m_i are zero. □

Given M and α_i we would like to find such m_i. Using the LLL-algorithm we are able to solve the weaker problem of finding integers $m_1, \ldots, m_n$ such that $(m_1^2 + \cdots + m_n^2)^{1/2} < 2^{(n-1)/4}M$ and $|m_1\alpha_1 + \cdots + m_n\alpha_n| < 2^{(n-1)/4}A/M^{n-1}$.
To solve the weaker problem we choose N such that $A^2N^2 = M^{2n} - 1$ and apply LLL-reduction to the lattice L generated by the row vectors of

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & N\alpha_1 \\ 0 & 1 & 0 & \cdots & 0 & N\alpha_2 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & N\alpha_n \end{pmatrix}$$

With the standard inner product on $\mathbb{R}^{n+1}$. The determinant of the lattice is given by $d(L)^2 = 1 + N^2(\alpha_1^2 + \cdots + \alpha_n^2)$. This can be bounded above by $d(L)^2 \leq 1 + A^2N^2 = M^{2n}$, hence $d(L) \leq M^n$. The LLL-algorithm produces a vector whose length is bounded by $2^{(n-1)/4}d(L)^{1/n} \leq 2^{(n-1)/4}M$. Hence

$$(m_1^2 + \ldots + m_n^2)^{1/2} \leq 2^{(n-1)/4}M$$

and

$$|m_1\alpha_1 + \cdots + m_n\alpha_n| \leq 2^{(n-1)/4}M/N < 2^{(n-1)/4}A/M^{n-1}.$$

A special case of the above occurs if we suspect the numbers $\alpha_1, \ldots, \alpha_n$ to satisfy a $\mathbb{Z}$-linear relation and we want to verify this. To this end we proceed as follows. If we really want to find a zero relation we must assume that we have some device to test the zeroness for any $\mathbb{Z}$-linear combination of the α_i. Let us call this our 'oracle'.
First we normalise the α_i such that $\sum_i |\alpha_i|^2 = 1$. Suppose we want to test whether or not there exist $m_1, \ldots, m_n \in \mathbb{Z}$ with $(\sum_i |m_i|^2)^{1/2} \leq M$ and $m_1\alpha_1 + \cdots + m_n\alpha_n = 0$.

Choose $N > M^n$ and apply LLL-reduction to the rows of

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & N\alpha_1 \\ 0 & 1 & 0 & \cdots & 0 & N\alpha_2 \\ \vdots & & & & & \vdots \\ 0 & 0 & 0 & \cdots & 1 & N\alpha_n \end{pmatrix}$$

The determinant of the lattice is $\sqrt{1+N^2}$. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be the reduced basis we have found. Suppose that a zero relation exists. Then we denote $(m_1, \ldots, m_n, 0)$ by $\mathbf{x}$ and note that $|\mathbf{x}| \leq M$.
From the properties of a reduced basis it would then follow that $|\mathbf{b}_1| \leq 2^{(n-1)/4}M$. So, if this inequality does not hold we have a contradiction and conclude that the relation between the α_i cannot exist.
If the inequality does hold we still know nothing. One possibility would be to increase N and try the same procedure again. In particular if the same vector $\mathbf{b}_1$ keeps popping up for increasing N, this may be a good candidate for a relation. We might feed it to our oracle to test for its zeroness. If the answer is still: 'not zero' we have still no clue to the answer of our problem.
One might wonder how far we should increase N before we have certainty about whether or not we have a relation. To that end we have to be more subtle than before. Choose t to be the biggest number such that

$$|\mathbf{b}_j| \leq 2^{(n-1)/2} \max(M, |\mathbf{b}_1|, \ldots, |\mathbf{b}_{j-1}|)$$

for $j = 1, \ldots, t$. If $t = n$ we find, using $|\mathbf{x}| \leq M$ and induction on j, that $|\mathbf{b}_j| \leq 2^{(n-1)j/2}M$ for all j. Hence

$$d(L) \leq \prod_{j=1}^{n} |\mathbf{b}_j| \leq 2^{(n^2-1)n/4}M^n,$$

which contradicts $d(L) > N$ for the choice $N = 2^{n^3/4}M^n$, say. So, assuming we have chosen N that large, we conclude that $t < n$ and any possible dependence relation $\mathbf{x}$ is a linear combination of $\mathbf{b}_1, \ldots, \mathbf{b}_t$. Suppose $t = 1$. We can test the relation given by $\mathbf{b}_1$ for its zeroness. If the answer is yes we have our desired relation. If the answer is no, we can be sure that there is no relation, since any such relation had to be a multiple of $\mathbf{b}_1$. Suppose $t > 1$. Then we denote the $n+1$-st component of $\mathbf{b}_i$ by β_i and now repeat the above procedure for the numbers $\beta_1, \ldots, \beta_t$. At every such step the number of components is decreased until we hit a zero relation or conclude that it cannot exist.

2.7 Exercises

Exercise 2.7.1 *Show that every prime p which is 1 or 3 modulo 8 can be written in the form $p = x^2 + 2y^2$ with $x, y \in \mathbb{Z}$.*

Exercise 2.7.2 *We are given the lattice $\mathbb{Z}^2$. How many distinct sublattices of index 2 are there?*

Exercise 2.7.3 *Let p be an odd prime. Let L be the set of solutions $(x,y) \in \mathbb{Z}^2$ to the congruence equation $2x+3y \equiv 0 \pmod{p}$.*

1. *Using Siegel's Lemma show that there is a non-zero element of L with $\max(|x|,|y|) \leq (3p)^{1/2}$. (Hint: consider the equation $2x+3y+pz=0$ in $x,y,z \in \mathbb{Z}$).*
2. *Show that L forms a sublattice of $\mathbb{Z}^2$.*
3. *Find a basis for L and determine its determinant.*
4. *Show, using Minkowski's theorem, that L contains a non-zero point with $\max(|x|,|y|) \leq p^{1/2}$.*
5. *Show,using Minkowski's theorem, that L contains a non-zero point of length $\leq (4p/\pi)^{1/2}$.*

Exercise 2.7.4 *Show that the solutions $(x,y,z) \in \mathbb{Z}^3$ to the equation*

$$3x+4y+5z=0$$

form a sublattice of $\mathbb{Z}^3$. Determine a basis of this lattice and its determinant.

Exercise 2.7.5 *Consider the lattice L from the previous exercise. We shall look at an alternative method to compute its determinant without calculating a basis of L. We extend L to a rank 3 lattice by adding the normal vector $(3,4,5)$. More precisely, define the lattice*

$$M = \{\mathbf{x} + t(3,4,5) \mid \mathbf{x} \in L, t \in \mathbb{Z}\}.$$

1. *Determine a solution (x_0,y_0,z_0) of $3x+4y+5z=1$.*
2. *Show that to every point $(x,y,z) \in \mathbb{Z}^3$ there exists a unique integer t with $0 \leq t < 50$ such that $(x,y,z) - t(x_0,y_0,z_0) \in M$.*
3. *Determine the index of M in $\mathbb{Z}^3$ and thus the determinant of M.*
4. *Determine the determinant of L using the previous item.*

Exercise 2.7.6 *Let $a_1,a_2,\ldots,a_n$ be n integers, not all zero, whose greatest common divisor is 1. Consider the set S of all $(x_1,x_2,\ldots,x_n) \in \mathbb{Z}^n$ satisfying*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0.$$

Show that S is a lattice with determinant $|\mathbf{a}|$, where $\mathbf{a} = (a_1,\ldots,a_n)$. (Hint: see the previous exercise).

Exercise 2.7.7 *Let $a_1,a_2,\ldots,a_n$ be n integers, not all zero, whose greatest common divisor is 1. Consider the set S of all $(x_1,x_2,\ldots,x_n) \in \mathbb{Z}^n$ satisfying*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0.$$

We denote $\mathbf{a} = (a_1,\ldots,a_n)$ and the different norms

$$||\mathbf{a}||_\infty = \max_i |a_i|, \quad ||\mathbf{a}||_1 = |a_1| + \cdots + |a_n|, \quad ||\mathbf{a}||_2 = \sqrt{a_1^2 + \cdots + a_n^2}.$$

1. *Show, using Siegel's lemma, that there exists a non-trivial element of S such that $\max_i |x_i| < (n||\mathbf{a}||_\infty)^{1/(n-1)}$.*

2. *Adapt the proof of Siegel's lemma to show that there is a non-zero element of S with $\max_i |x_i| < ||\mathbf{a}||_1^{1/(n-1)}$ (Hint: show that we can assume that $a_i \geq 0$ for all i).*

3. *We like to improve the above results by using Minkowski's theorem and the result of Exercise 2.7.6. We are also given that the $n-1$-dimensional area of the intersection of a hyperplane in $\mathbb{R}^n$ with a unit cube (i.e. all sides 1) is at least 1.*

   Apply Minkowski's theorem to show that there is a non-trivial element of S such that $\max_i |x_i| \leq ||\mathbf{a}||_2^{1/(n-1)}$.

4. *Show, using the last item, that there exists a non-trivial element of S with $\max_i |x_i| \leq (\sqrt{n}||\mathbf{a}||_\infty)^{1/(n-1)}$, an improvement of our first item.*

Exercise 2.7.8 *This one is not very easy. Let L be a sublattice of $\mathbb{Z}^n$. We assume that L is primitive. This means that $L = V \cap \mathbb{Z}^n$ where V is the real vectorspace spanned by the elements of L. We consider the orthogonal complement*

$$L^\perp = \{\mathbf{x} \in \mathbb{Z}^n \mid \mathbf{x} \cdot \mathbf{l} = 0 \text{ for all } \mathbf{l} \in L\}.$$

Notice that $L^\perp$ is a sublattice of $\mathbb{Z}^n$. Show that if L and $L^\perp$ are non-trivial, then they have the same determinant.
Show also that the statement is not true if L is not primitive.

Exercise 2.7.9 *Let L be a lattice with base $\mathbf{b}_1, \ldots, \mathbf{b}_r$. Show that the length of every non-zero vector in L is bounded below by the smallest eigenvalue of the Gram-matrix of the $\mathbf{b}_i$.*

Exercise 2.7.10 *Let l be the length of the shortest non-zero vector in a lattice of rank 2. Let v_1, v_2 be the initial basis of the lattice. Prove that the algorithm Euclid ends in $O(\log(|v_1|/l))$ iterations.*

Exercise 2.7.11 *Let c be a real number in $]1/\sqrt{3}, 1[$. Suppose we replace the stopping condition $|\mathbf{v}_2| \geq |\mathbf{v}_1|$ in our previous algorithm by $|\mathbf{v}_2| \geq c|\mathbf{v}_1|$. Let $\mathbf{v}_1$ be the result of our new algorithm. Show that for any non-zero $\mathbf{v} \in L$ we have $|\mathbf{v}| \geq c|\mathbf{v}_1|$*

Exercise 2.7.12 *Let $m = \max_{i=1,\ldots,r} |\mathbf{b}_i|$. Show that the number of swaps occurring in the LLL-algorithm is bounded by $cr^2 \log(m\sqrt{r}/l)$ where $c > 0$ is a constant and l is the length of the shortest non-zero vector in L.*