4. LLL

In this chapter we investigate the Lenstra-Lenstra-Lovász algorithm for lattice reduction: it is designed to find short vectors in a lattice.

Lattices

A *lattice* in $\mathbb{R}^m$ is a discrete $\mathbb{Z}$-module. Here *discrete* means: that any bounded subset of $\mathbb{R}^m$ contains (at most) finitely many lattice elements; and a $\mathbb{Z}$-module is just an additive subgroup of the vector space.

Most obvious example: $\mathbb{Z}^n$ in $\mathbb{R}^m$ for $n \leq m$.

Remark. Note that in some texts a lattice is required to be of full rank m, so it contains a basis for $\mathbb{R}^m$. Not here.

Lemma 1. *L is a lattice in $\mathbb{R}^m$ if and only there exist $n \leq m$ and n independent vectors $v_1, \ldots, v_n \in \mathbb{R}^m$ such that $L = \mathbb{Z} \cdot v_1 + \cdots + \mathbb{Z} \cdot v_n$.*

If $w_1, \ldots, w_n$ is a maximal independent set then $M = \mathbb{Z} \cdot w_1 + \cdots + \mathbb{Z} \cdot w_n$ is a subgroup of L, and every $v \in L$ can be written as $v = r_1 \cdot v_1 + r_2 \cdot v_2 + \cdots r_n \cdot v_n$. Take $r_i = k_i + h_i$, met $k_i \in \mathbb{Z}$; then

$$v = \sum k_i \cdot v_i + \sum h_i \cdot v_i = z + y,$$

with $z \in L$ and y in the bounded box P of $\sum x_i \cdot v_i$ with $0 \leq x_i < 1$. But $y = v - z \in L$, so in the finite set $P \cap L$. Hence L is the sum of finitely many cosets $M + y$, so $k \cdot y \in L$ for some $k \in \mathbb{N}$ and every $y \in P \cap L$. Thus L is contained in $\frac{1}{k}M$, which is generated by $\frac{1}{k}v_i$.

Lemma 2. *$v_1, \ldots, v_n$ of $L = \langle w_1, \ldots, w_n \rangle$ form a basis for L if and only if the transformation matrix $(\alpha_{ij})_{i,j=1}^n$ is in $\mathrm{GL}_n(\mathbb{Z})$.*

Quadratic form

An alternative way of specifying a lattice is by means of its Gram matrix. For this our space $\mathbb{R}^m$ needs to be equiped with a positive definite quadratic form. A *quadratic form* for a vector space V over a field K of characteristic not equal to 2 is a map q from V to K such that $q(\lambda \cdot v) = \lambda^2 \cdot v$ for $\lambda \in K$ and $v \in V$, and such that $\frac{1}{2}(q(v+w) - q(v) - q(w))$ is a symmetric bilinear form on V. The form is *positive definite* for $K = \mathbb{R}$ if $q(v) > 0$ for every non-zero v.

Gram matrices

If V has basis $b_1, b_2, \ldots, b_n$ and the coordinate vector of x is $(x_1, \ldots, x_n)^\mathsf{T}$, then

$$q(x) = \sum q_{ij} x_i x_j = (x_1, \ldots x_n) Q_{ij} (x_1, \ldots, x_n)^\mathsf{T},$$

where $q_{ij} = B(b_i, b_j)$, the value of the bilinear form, and Q_{ij} is the positive definite symmetric $n \times n$ matrix with entries q_{ij}.

The matrix Q is called the *Gram matrix* for the lattice L.

We think of q as the squared *length*, and B as the inner product; we will sometimes simply write $|\cdot|$ for $\sqrt{q(\cdot)}$ and $\langle \cdot, \cdot \rangle$ for $B(\cdot, \cdot)$.

Determinant

Note that a base change for L changes the Gram matrix Q into $P \cdot Q \cdot P^{\mathsf{T}}$ for some $P \in \mathrm{GL}_n(\mathbb{Z})$; so the Gram matrix is unique up to similarity by an orthogonal matrix (isometry), and $\det Q > 0$ is invariant.

The *determinant* $d(L)$ of L is $d(L) = \sqrt{\det Q}$.

A geometric interpretation of this is that Q_{ij} are the values $B(b_i, b_j)$, the *inner products* of the basis vectors for the lattice, and hence $Q = U^{\mathsf{T}} \cdot U$, where U is the coefficient matrix when writing the b_i on an orthonormal basis. Hence

$$\det L = \sqrt{\det} Q = |\det U| = \mathrm{vol}(b_1, b_2, \ldots, b_n),$$

the volume of the parallepiped spanned by the basis vectors, which we called P before.

Gram-Schmidt orthogonalisation

The goal of lattice reduction is to change basis (without changing the lattice) in order to improve, that is to *shorten* the basis. Since the volume of the lattice is an invariant, it is equivalent to require that the basis becomes *more orthogonal*.

This shows the relation with *Gram-Schmidt orthogonalisation*

Algorithm [Gram-Schmidt orthogonalisation]
Let $v_1, v_2, \ldots, v_n$ form a basis for V. Define inductively for $i = 1, 2, \ldots n$ vectors ${v_i}^*$ by:

${v_1}^* = v_1$, and for $i \geq 2$:

$$ {v_i}^* = v_i - \sum_{j=1}^{i-1} \mu_{ij} {v_j}^*, $$

where

$$ \mu_{ij} = \frac{< v_i, {v_j}^* >}{< {v_j}^*, {v_j}^* >}. $$

The vector ${v_i}^*$ is the projection of v_i onto the orthogonal complement of $\mathbb{R}\cdot v_1+\cdots+\mathbb{R}\cdot v_{i-1} = \mathbb{R}\cdot {v_1}^* + \cdots + \mathbb{R}\cdot {v_{i-1}}^*$.

The result, basis ${v_1}^*, \ldots, {v_n}^*$, is orthogonal, and can be turned into an orthonormal basis by dividing the entries by their lengths.

Note that M, expressing the ${v_i}^*$ in the v_j

$$V^* = \begin{pmatrix} {v_1}^* & {v_2}^* & \cdots & {v_n}^* \end{pmatrix} = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix} \cdot M$$

is *upper triangular* with ones on the diagonal:

$$\begin{pmatrix} 1 & -\mu_{21} & -\mu_{31}+\mu_{32}\mu_{21} & \cdots & -\mu_{n1}+\mu_{n2}\mu_{21}+\cdots \\ 0 & 1 & -\mu_{32} & \cdots & -\mu_{n2}+\mu_{n3}\mu_{32}+\cdots \\ 0 & 0 & 1 & \cdots & -\mu_{n3}+\mu_{n4}\mu_{43}+\cdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

so $\det V^* = \det(V\cdot M) = \det V \cdot \det M = \det V$.

Corollary.

$$d(L)^2 = \prod_{i=1}^{n} |b_i^*|^2.$$

Immediate since the b_i^* are orthogonal:

$d(L)^2 = |\det B|^2 = (\det B^*)^2 = \det {B^*}^{\mathsf{T}} \det B^*$

but $< {b_i}^*, {b_j}^* >= \delta_{ij} \cdot |b_i^*| \cdot |b_j^*|$.

The vectors b_i^* have the desired property, but are not generally in the lattice. The reason is of course that the μ_{ij} are not necessarily integers.

Corollary. (Hadamard-inequality)

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

This follows from

$$\begin{aligned} |b_i|^2 &= < b_i, b_i >= \\ &= < b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*, b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^* >= \\ &= |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2, \end{aligned}$$

and the previous Corollary.

Minkowski reduction

Minkowski showed in a theoretic sense *how short* vectors of minimal length in a lattice basis can be: he defined Minkowski reduced bases for a lattice as bases minimal with respect to the partial ordering of bases given by using the length as order and calling a basis $a_1, a_2, \ldots, a_n$ shorter than $b_1, b_2, \ldots, b_n$ when for $1 \leq i < k$ the lengths of a_i and b_i agree, but a_k is shorter than b_k. This reduced basis is not unique; more seriously, for $n > 3$ nobody knows how to find such basis!

Minkowski theorem

Minkowski formulated the following theorem for convex bodies (with every pair $x, y \in C$ also $x + \lambda(y - x)$ (voor $0 \leq \lambda \leq 1$ will be in C):

Theorem *If C is convex in $\mathbb{R}^n$, symmetric around the origine (so, with $x \in C$ also $-x \in C$), and if L is a lattice in $\mathbb{R}^n$ then:*

$$\text{vol}(C) > 2^n d(L) \quad \Rightarrow \quad \exists\ \vec{0} \neq \vec{r} \in L \cap C.$$

Intuitively this seems clear.

Successive minima

For $j = 1, 2, \ldots, n$ will M_j be the smallest positive integer such that there exist independent vectors $r_1, r_2, \ldots, r_j$ in L for which $|r_i|^2 \leq M_j$ for $1 \leq i \leq j$.

Hence M_1 is (square of) the length of a shortest vector in L.

Theorem. For every $n \geq 1$ there exists constant $\gamma_n \in \mathbb{R}_{>0}$ for which

$$\prod_{i=1}^{n} M_i \leq \gamma_n d(L)^2,$$

for every lattice L in $\mathbb{R}^n$.

The best possible γ_n is called Hermite's constant; its value is only known for $1 \leq n \leq 8$:

$$\gamma_1 = 1, \gamma_2 = \sqrt{\frac{4}{3}}, \gamma_3 = \sqrt[3]{2}, \gamma_4 = \sqrt[4]{4}, \gamma_5 = \sqrt[5]{8},$$

$$\gamma_6 = \sqrt[6]{\frac{64}{3}}, \gamma_7 = \sqrt[7]{64}, \gamma_8 = \sqrt[8]{256}.$$

Generally, $\gamma_n \leq \gamma_{n-1}^{\frac{n-1}{n-2}}$.

One of the problems with successive minima is that for $n > 4$ the existence of independent vectors b_i if length $\sqrt{M_n}$ does not mean that there is a basis of such vectors in the lattice.

Example

For example, in $\mathbb{R}^5$, take the lattice spanned by

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}.$$

Because also the fifth standard base vector is in the lattice, is will be clear that $M_1 = M_2 = M_3 = M_4 = M_5 = 1$, but there is no basis of 5 vectors of length 1!

Gauss reduction

In dimension 2 there is an easy algorithm to compute the shortest vector in a lattice. This generalizes the Euclidean algorithm.

Let a and b generate the lattice.

If $q(a) < q(b)$ interchange a and b.

Compute the nearest integer r to $B(a,b)/B(b,b)$.

If $q(a) - 2rB(a,b) + r^2q(b) \geq q(b)$ then terminate; else replace a by b and b by $a - r \cdot b$.

This works since

$$q(a - x \cdot b) = x^2 \cdot q(b) - 2x \cdot B(a,b) + q(a).$$

LLL-reduction

A basis $b_1, b_2, \ldots b_n$ for the lattice L is called *LLL-reduced* if for $1 \leq j < i \leq n$:

$$[R] \qquad \mu_{ij} = \frac{< b_i, b_j^* >}{< b_j^*, b_j^* >} \leq \frac{1}{2},$$

en voor $2 \leq i \leq n$:

$$[L] \qquad |b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \geq \frac{3}{4} |b_{i-1}^*|.$$

The latter is equivalent with

$$[L'] \qquad |b_i^*|^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2)|b_{i-1}^*|^2 \geq \frac{1}{2}|b_{i-1}^*|^2.$$

Theorem *If $b_1, b_2, \ldots, b_n$ form an LLL-reduced basis voor L, then:*

(i) $d(L) \leq \prod_{i=1}^{n} |b_i| \leq 2^{n\frac{n-1}{4}} d(L)$,

(ii) $|b_j| \leq 2^{\frac{i-1}{2}} |b_i^*|$, *for* $1 \leq j \leq i \leq n$,

(iii) $|b_1| \leq 2^{\frac{n-1}{4}} \sqrt[n]{d(L)}$,

(iv) $|b_1| \leq 2^{\frac{n-1}{2}} |r|$, *for all* $0 \neq r \in L$,

(v) $|b_j| \leq 2^{\frac{n-1}{2}} \max(|r_1|, \ldots, |r_t|)$, *for independent* $r_1, \ldots, r_t \in L$ *en* $j \leq t$.

Proof The first part of (i) is the Hadamard inequality we saw before; the second part will follow from (ii), $|b_i^*| \le |b_i|$ and $d(L) = \prod |b_i^*|$.

From [L'] we see that $|b_j^*|^2 \le 2^{i-j}|b_i^*|^2$ for $j \le i$ by induction, hence

$$|b_i|^2 = |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}|b_j^*|^2,$$

which is at most

$$(1 + \frac{1}{4}(2^i - 2)) \cdot |b_i^*|^2 \le 2^{i-1} \cdot |b_i^*|^2,$$

proving (ii).

We obtain (iii) from (ii) by taking $j = 1$ in (ii), taking the product over all i, and taking n-th roots.

For (iv) write $r = \sum z_i \cdot b_i = \sum s_i \cdot b_i^*$ with $z_i \in \mathbb{Z}$ and $s_i \in \mathbb{R}$. Then $s_i = z_i$ for the largest i with non-zero s_i, hence

$$|r|^2 \geq s_i \cdot |b_i^*|^2 \geq |b_i^*|^2,$$

but

$$2^{n-1}|b_i^*|^2 \geq 2^{i-1}|b_i^*|^2 \geq |b_1|^2$$

by (ii).

Finally, as above, we write $r_j = \sum_i z_{ij} b_i$ and then

$$|r_j|^2 \geq |b_{i(j)}^*|^2,$$

for the maximal $i = i(j)$ with z_{ij} non-zero. Renumbering to get $i(1) \leq i(2) \leq \cdots \leq i(t)$ we find that $j \leq i(j)$ and therefore

$$|b_j|^2 \leq 2^{i(j)-1} \cdot |b_{i(j)}^*|^2 \leq 2^{n-1}|r_j|^2,$$

implying (v).

The LLL algorithm alternates between *reduction steps*, in which an integral version of a Gram-Schmidt type combination of vectors is subtracted from another, and *swaps* where the latter vector is moved up front in accordance with its relative size.

Example (Using the notation from Cohen)

Let a basis b_1, b_2, b_3 for $\mathbb{R}^3$ be given by the columns of

$$\begin{pmatrix} 1 & -1 & 3 \\ 1 & 0 & 5 \\ 1 & 2 & 6 \end{pmatrix}.$$

Then $b_1^* = b_1$ and $B_1 = 3$.

$\mu_{21} =< b_2, b_1^* > /B_1 = \frac{1}{3}$, so

$$b_2^* = b_2 - \frac{1}{3} b_1^* = \begin{pmatrix} -\frac{4}{3} \\ -\frac{1}{3} \\ \frac{5}{3} \end{pmatrix}$$

and $B_2 = \frac{42}{9} = \frac{14}{3}$.

$\mu_{31} = < b_3, b_1^* > / B_1 = \frac{14}{3}$, so

$$b_3^* = b_3 - \frac{14}{3} b_1^* = \begin{pmatrix} -\frac{5}{3} \\ \frac{1}{3} \\ \frac{4}{3} \end{pmatrix}$$

and $\mu_{32} = < b_3, b_2^* > / B_2 = \frac{13}{14}$, so

$$b_3^* = b_3^* - \frac{13}{14} b_2^* = \begin{pmatrix} -\frac{18}{42} \\ \frac{27}{42} \\ -\frac{9}{42} \end{pmatrix} = \begin{pmatrix} -\frac{6}{14} \\ \frac{9}{14} \\ -\frac{3}{14} \end{pmatrix},$$

and $B_3 = \frac{9}{14}$.

In the REDuction step we then get

$$b_3 = b_3 - b_2 = \begin{pmatrix} 3 \\ 5 \\ 6 \end{pmatrix} - \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 4 \\ 5 \\ 4 \end{pmatrix}.$$

Apply SWAP and continue with the columns of

$$\begin{pmatrix} 1 & 4 & -1 \\ 1 & 5 & 0 \\ 1 & 4 & 2 \end{pmatrix}.$$

Then $b_1^* = b_1$ is unchanged,
$\mu_{21} =< b_2, b_1^* > /3 = \frac{13}{3}$, so

$$b_2^* = b_2 - \mu_{21} b_1^* = \begin{pmatrix} -\frac{1}{3} \\ \frac{2}{3} \\ -\frac{1}{3} \end{pmatrix},$$

and $B_2 = \frac{2}{3}$.

As $\lfloor \mu_{21} \rceil = 4$, we get

$$b_2 = b_2 - 4b_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

We need to swap again and arrive at the reduced basis

$$\begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$