Topics: Lattice Basis Reduction

Book: Chapter 9.1.1

Summary

The *LLL-algorithm* (or: *Lovász' basis reduction algorithm*) finds in polynomial time a reduced basis for a given lattice. The algorithm has a huge number of applications in mathematics and computer science. The algorithm is named after Arjen Lenstra, Hendrik Lenstra and László Lovász, who introduced the algorithm and showed how it can be used to factor univariate polynomials in their paper *Factoring Polynomials with Rational Coefficients*. A different application, which we will discuss next week, is to solving ILP's in a fixed number of variables in polynomial time.

Lattices

A *lattice* is a discrete subgroup of $\mathbb{R}^n$. More concretely, it is a set $\Lambda \subseteq \mathbb{R}^n$ of the form

$$\Lambda = \{\lambda_1 a^1 + \cdots + \lambda_d a^d : \lambda_1, \ldots, \lambda_k \in \mathbb{Z}\},$$

where $a^1, \ldots, a^d$ are linearly independent vectors that are called a *basis* of the lattice. We allow for the possibility that $d < n$. The book only considers the case that Λ has *full rank*, that is $d = n$.

It is convenient to collect the basis vectors a^j as the columns of a matrix A and say that A is a basis of the lattice $\Lambda(A)$. A given lattice can have several different bases.

Theorem 1 (Theorem 9.1)**.** *Two matrices $A, B \in \mathbb{R}^{n\times d}$ of rank $d \leq n$ are bases of the same lattice if and only if $B = AU$ for some unimodular $U \in \mathbb{Z}^{d\times d}$.*

An important invariant of a lattice is its *determinant* defined by $\det \Lambda = \sqrt{B^\mathsf{T} B}$ if $\Lambda = \Lambda(B)$. This does not depend on the basis B as follows directly from the above theorem.

Hadamard inequality

Geometrically, the determinant of a lattice is the volume (with respect to the linear span of the lattice) of the parallelepiped spanned by the vectors in a basis. In particular, we have the *Hadamard inequality*:

$$\prod_{j=1}^{d} \|b^j\| \geq \det \Lambda(B).$$

The *orthogonality defect*

$$\delta(B) = \frac{\det \Lambda(B)}{\prod_{j=1}^{d} \|b^j\|}$$

measures how far away from orthogonal the lattice basis is. It was shown by Hermite that each lattice has an almost orthogonal basis in the following sense.

Theorem 2 (Hermite (1850))**.** *For every positive integer d there is a constant $c(d)$ such that every lattice of rank d has a basis B with $\delta(B) \leq c(d)$. We may take $c(d) = (\frac{4}{3})^{d(d-1)/4}$.*

Minkowski (1896) showed that in fact we can take $c(n) = \frac{2^d}{V_d} \approx \left(\frac{2n}{\pi e}\right)^{n/2}$ where V_d is the volume of the unit ball in $\mathbb{R}^d$. The LLL-algorithm produces a basis B with $\delta(B) \leq 2^{\frac{d(d-1)}{4}}$, see Theorem 9.2.

Lattice Reduction Algorithm

Given a set of independent vectors $b^1, \ldots, b^d \in \mathbb{R}^n$, the *Gram-Schmidt process* produces orthogonal vectors $g^1, \ldots, g^d \in \mathbb{R}^n$ by setting

- $g^1 = b^1$
- g^j is the projection of b^j onto the orthogonal complement of $\text{span}(b^1, \ldots, b^{j-1})$ when $j \geq 2$.

If G is the matrix with columns $g^1, \ldots, g^d$, then we have $B = GR$, where $R \in \mathbb{R}^{d \times d}$ is upper triangular with 1 at all the diagonal positions. The off-diagonal entries are given by

$$R_{ij} = \frac{\langle b^j, g^i \rangle}{\langle g^i, g^i \rangle}, \qquad (1 \leq i < j \leq d).$$

Note that $g^1, \ldots, g^k$ are an othogonal basis for the linear space spanned by $b^1, \ldots, b^k$ (but are not necessarily elements of the lattice). The lattice basis B is called *reduced* if

(i) $R_{ij} \in [-\frac{1}{2}, \frac{1}{2}]$ for $1 \leq i < j \leq d$,

(ii) $\left\|g^j + R_{j-1,j} \cdot g^{j-1}\right\|^2 \geq \frac{3}{4} \cdot \left\|g^{j-1}\right\|$ for $2 \leq j \leq d$.

The LLL-algorithm takes as input a lattice basis consisting of rational vectors $b^1, \ldots, b^d$ and produces a reduced basis for the same lattice. By scaling, we may assume that the basis consists of *integral* vectors. When the basis B is changed, the corresponding Gram-Schmidt basis, and hence the marices G and R, are assumed to be recomputed. The algorithm can be described as follows.

STEP 1. For $j = d, \ldots, 2$ modify b^j by adding integral multiples of $b^1, \ldots, b^{j-1}$ so that (i) holds.

STEP 2. If condition (2) is satisfied, we are done. Otherwise, let j be an index for which (ii) fails. Swap the vectors b^j and b^{j-1} are go to STEP 1.

The fact that the algorithm terminates in polynomial time (Theorem 9.6) follows by considering the quantity $\Phi(B) := \left\|g^1\right\|^{2d} \cdot \left\|g^2\right\|^{2d-2} \cdots \left\|g^d\right\|^2$ and the following two observations:

- In each STEP 2, the new value of $\Phi(B)$ is at most $\frac{3}{4}$ times the previous value.
- $\Phi(B)$ is a positive integer.

Shortest lattice vector

The *Shortest Vector Problem (SVP)* asks to find a vector $v \in \Lambda(B) \setminus \{0\}$ of minimum length. This is a difficult problem, but the LLL-algorithm gives a lattice vector that is not far from optimal.

Theorem 3 (Exercise 9.5)**.** *Let $B \in \mathbb{R}^{n \times d}$ be a reduced basis of Λ and let $v \in \Lambda \setminus \{0\}$ be a shortest nonzero lattice vector. Then*

$$\left\|b^1\right\| \leq 2^{(d-1)/2} \cdot \|v\|.$$

To illustrate a useful application of the LLL-algorithm, consider the following. Let $\alpha_1, \ldots, \alpha_d \in \mathbb{R}$ be numbers that are known up to a certain digital precision and we want to find an integer linear relation $c_1\alpha_1 + \cdots + c_d\alpha_d = 0$ where $c_1, \ldots, c_d \in \mathbb{Z}$ should be small in absolute value. Such a relation (if it exists) can be found by taking $b^j = \binom{e_j}{M\alpha_j} \in \mathbb{R}^{d+1}$, where e_j denotes the j-th standard basis vector and M is a very large number. The vector in $\Lambda(B)$ will be of the form $(c_1, \ldots, c_d, M(c_1\alpha_1 + \cdots + c_d\alpha_d))$. Hence short vectors in the lattices correspond to approximate integral relations with small coefficients.

If we take $\alpha_j = y^j$ for some real number y, then this gives us a way to guess a polynomial $f(x)$ with small integer coefficients for which $f(y) = 0$.