Lattices

Michael E. Pohst

Institut für Mathematik
Technische Universität Berlin

May 21, 2013

Introduction of lattices I

Let $\mathbf{b}_1, \ldots, \mathbf{b}_k \in \mathbb{R}^n$ be linearly independent.
Definition

$$\Lambda := \left\{ \sum_{i=1}^{k} \lambda_i \mathbf{b}_i \;\middle|\; \lambda_1, \ldots, \lambda_k \in \mathbb{Z} \right\}$$

is called a **lattice** of **dimension** k.
$d(\Lambda) := \det\left((\mathbf{b_i}^t \cdot \mathbf{b_j})_{1 \leq i,j \leq k} \right)^{1/2}$ is called **discriminant** of Λ, and

$$\Pi(\Lambda) := \left\{ \mathbf{x} \in \mathbb{R}^n \;\middle|\; \mathbf{x} = \sum_{i=1}^{k} \xi \mathbf{b_i}, 0 \leq \xi_i < 1 \; (1 \leq i \leq k) \right\}$$

is said to be the **fundamental parallelotope** of Λ.
We note that $\Pi(\Lambda)$ depends on the choice of the **basis** $\mathbf{b_1}, ..., \mathbf{b_k}$, whereas $d(\Lambda)$ is independent of the choice of the basis.

Introduction of lattices II

Lemma Let $\Lambda' \subseteq \Lambda$ be k-dimensional lattices with bases $\mathbf{a_1}, ..., \mathbf{a_k}$, $\mathbf{b_1}, ..., \mathbf{b_k}$, respectively.

1. There is a matrix $U \in \mathbb{Z}^{k \times k}$ with $(\mathbf{a_1}, \ldots, \mathbf{a_k}) = (\mathbf{b_1}, \ldots, \mathbf{b_k})\mathbf{U}$.
2. $d(\Lambda') = |\det(U)|\, d(\Lambda)$.
3. $(\Lambda : \Lambda') = \frac{d(\Lambda')}{d(\Lambda)}$.
4. $d(\Lambda) = \text{ vol}_k(\Pi(\Lambda))$.

Lattices are discrete

Theorem For $\mathbf{x} \in \mathbb{R}^n$ and $C > 0$ there exist only finitely many $\mathbf{y} \in \Lambda$ with $\|\mathbf{x} - \mathbf{y}\| \leq C$.

Different viewpoint of lattices

Lattices have the essentiell property that their bases belong to a finite dimensional Euclidean space.
Hence, we may just require the existence of a basis $b_1, ..., b_k$ in such a Euclidean space. In it we have a scalar product $\langle \, , \rangle$. For lattice vectors $x = \xi_1 b_1 + ... + \xi_k b_k, \; y = \eta_1 b_1 + ... + \eta_k b_k$ with $\xi_j, \, \eta_j \in \mathbb{Z}$ we obtain

$$\begin{aligned} \langle x, \, y \rangle &= \textstyle\sum_{i=1}^{k} \sum_{j=1}^{k} \xi_i \eta_j \langle b_i, \, b_j \rangle \\ &= (\xi_1, ..., \xi_k) A (\eta_1, ..., \eta_k)^{tr} \end{aligned}$$

with the **Gram matrix** $A = (\langle b_i, \, b_j \rangle) \in \mathbb{R}^{k \times k}$.
We note that A is a positive definite matrix.

Examples from Number Fields I

Let F be an algebraic number field of degree n. We introduce a scalar product on F in the usual way:

$$\langle\, ,\rangle : F \times F \to \mathbb{R} : (x, y) \mapsto \sum_{j=1}^{n} x^{(j)}\overline{y^{(j)}}\ .$$

By abuse of language we say that

$$T_2(x) := \langle x, x\rangle$$

is the T_2-**norm** of an element $x \in F$.

Examples from Number Fields II

(i) Let R be an order of F with $\mathbb{Z}$–basis $b_1, ..., b_n$. Then R becomes an n–dimensional lattice with respect to the Gram matrix $A = (\langle b_i,\ b_j \rangle)$.

(ii) Let U be the unit group of R. Considering vectors whose coordinates are logarithms of the absolute values of the conjugates of elements of U we turn the multiplicative structure into an additive one for those vectors of logarithms. The image of U becomes a lattice. (This will be made precise tomorrow.)

Examples from Number Fields II

(i) Let R be an order of F with $\mathbb{Z}$–basis $b_1, ..., b_n$. Then R becomes an n–dimensional lattice with respect to the Gram matrix $A = (\langle b_i, \, b_j \rangle)$.
(ii) Let U be the unit group of R. Considering vectors whose coordinates are logarithms of the absolute values of the conjugates of elements of U we turn the multiplicative structure into an additive one for those vectors of logarithms. The image of U becomes a lattice. (This will be made precise tomorrow.)

Computation of short vectors I

Let $A \in \mathbb{R}^{k\times k}$ be positive definite. We calculate an upper triangualar matrix $Q \in \mathbb{R}^{k\times k}$ satisfying

$$\mathbf{x}^t \cdot A \cdot \mathbf{x} = \sum_{i=1}^{k} q_{ii} \left(x_i + \sum_{j=i+1}^{k} q_{ij} x_j \right)^2 .$$

1. Set $Q \leftarrow A$.
2. For $i = 1, \ldots, k-1$ set $q_{ji} \leftarrow q_{ij}$, $q_{ij} \leftarrow \frac{q_{ij}}{q_{ii}}$ $(i+1 \le j \le k)$ and update Q: $q_{\mu\nu} \leftarrow q_{\mu\nu} - q_{\mu i} q_{i\nu}$ $(i+1 \le \mu \le \nu \le k)$.
3. Set $q_{ij} \leftarrow 0$ $(1 \le j < i \le k)$.

Computation of short vectors II

For $A \in \mathbb{R}^{k \times k}$ positive definite and some constant $C > 0$ we calculate all $\mathbf{0} \neq \mathbf{x} \in \mathbb{Z}^k$ satisfying $\mathbf{x}^t \cdot A \cdot \mathbf{x} \leq C$.

1. Compute $Q \in \mathbb{R}^{k \times k}$ with the previous algorithm.
2. Set $i \leftarrow k, T_i \leftarrow C, U_i \leftarrow 0$.
3. (Bounds for x_i) Set $Z \leftarrow \sqrt{\frac{T_i}{q_{ii}}}, B_i \leftarrow \lfloor Z - U_i \rfloor$ and $x_i \leftarrow \lceil -Z - U_i \rceil - 1$.
4. Set $x_i \leftarrow x_i + 1$. In case $x_i \leq B_i$ go to 5.
5. Set $i \leftarrow i + 1$ and go to 4.
6. In case $i = 1$ go to 7, else set $i \leftarrow i - 1, U_i \leftarrow \sum_{j=i+1}^{k} q_{ij} x_j$, $T_i \leftarrow T_{i+1} - q_{i+1,i+1}(x_{i+1} + U_{i+1})^2$ und go to 3.
7. For $\mathbf{x} = 0$ terminate, else output $\mathbf{x}$, $-\mathbf{x}$, $Q(\mathbf{x})$ and return to 4.

Successive minima

Definition For $i \in \{1, \ldots, k\}$ we call

$$M_i := \min\{\gamma > 0 \mid \exists x_1, \ldots, x_i \in \Lambda \text{ linearly independent with } \|x_\nu\|^2 \leq \gamma \ (1 \leq \nu \leq i)\}$$

i-**th successive minimum** of the lattice Λ.

Theorem

1. There exist linearly independent $\mathbf{y}_1, \ldots, \mathbf{y}_k \in \Lambda$ satisfying $\|\mathbf{y}_i\|^2 = M_i$ $(1 \leq i \leq k)$.

Successive minima

Definition For $i \in \{1, \dots, k\}$ we call

$$\begin{aligned} M_i \ := \ & \min\{\gamma > 0 \mid \\ & \exists x_1, \dots, x_i \in \Lambda \text{ linearly independent with} \\ & \|x_\nu\|^2 \leq \gamma \ (1 \leq \nu \leq i)\} \end{aligned}$$

i-**th successive minimum** of the lattice Λ.

Theorem

1. There exist linearly independent $\mathbf{y}_1, \dots, \mathbf{y}_k \in \Lambda$ satisfying $\|\mathbf{y}_i\|^2 = M_i$ $(1 \leq i \leq k)$.
2. $\mathbf{v} \in \Lambda$ satisfying $\|\mathbf{v}\|^2 = M_1$ can be extended to a basis of Λ.

Successive minima

Definition For $i \in \{1, \ldots, k\}$ we call

$$\begin{aligned} M_i \quad := \quad & \min\{\gamma > 0 \mid \\ & \exists x_1, \ldots, x_i \in \Lambda \text{ linearly independent with} \\ & \|x_\nu\|^2 \leq \gamma \ (1 \leq \nu \leq i)\} \end{aligned}$$

i-**th successive minimum** of the lattice Λ.

Theorem

1. There exist linearly independent $\mathbf{y}_1, \ldots, \mathbf{y}_k \in \Lambda$ satisfying $\|\mathbf{y}_i\|^2 = M_i$ $(1 \leq i \leq k)$.
2. $\mathbf{v} \in \Lambda$ satisfying $\|\mathbf{v}\|^2 = M_1$ can be extended to a basis of Λ.

Minkowski's Theorem

Theorem There exist constants $C > 0$ which depend only on k with

$$M_1 \cdot \ldots \cdot M_k \leq C\, d(\Lambda)^2$$

for all k-dimensional lattices Λ. The minimal constant with this property is called **Hermite's constant** and denoted by γ_k^k.

Example Let us consider the lattice Λ whose basis is given by the columns of the matrix:

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

Hadamard's Theorem

For $\mathbf{b}_1, \ldots, \mathbf{b}_k$ let $\mathbf{b}_1^*, \ldots, \mathbf{b}_k^* \in \mathbb{R}^n$ be the corresponding orthogonal basis determined by the method of E. Schmidt:

$$\mathbf{b}_i^* := \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^* \qquad (1 \leq i \leq k),$$

$$\mu_{ij} := \frac{\mathbf{b}_i^t \mathbf{b}_j^*}{{\mathbf{b}_j^*}^t \mathbf{b}_j^*} \qquad (1 \leq j < i \leq k).$$

Theorem

$$d(\Lambda) = \prod_{i=1}^{k} \|\mathbf{b}_i^*\| \leq \prod_{i=1}^{k} \|\mathbf{b}_i\| \ .$$

Hadamard's Theorem

For $\mathbf{b}_1, \ldots, \mathbf{b}_k$ let $\mathbf{b}_1^*, \ldots, \mathbf{b}_k^* \in \mathbb{R}^n$ be the corresponding orthogonal basis determined by the method of E. Schmidt:

$$\mathbf{b}_i^* := \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^* \qquad (1 \leq i \leq k),$$

$$\mu_{ij} := \frac{\mathbf{b}_i^t \mathbf{b}_j^*}{\mathbf{b}_j^{*\,t} \mathbf{b}_j^*} \qquad (1 \leq j < i \leq k).$$

Theorem

$$d(\Lambda) = \prod_{i=1}^{k} \|\mathbf{b}_i^*\| \leq \prod_{i=1}^{k} \|\mathbf{b}_i\| \ .$$

Corollary $d(\Lambda)^2 \leq M_1 \cdot \ldots \cdot M_k$.

Hadamard's Theorem

For $\mathbf{b}_1, \ldots, \mathbf{b}_k$ let $\mathbf{b}_1^*, \ldots, \mathbf{b}_k^* \in \mathbb{R}^n$ be the corresponding orthogonal basis determined by the method of E. Schmidt:

$$\mathbf{b}_i^* := \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{ij} \mathbf{b}_j^* \qquad (1 \leq i \leq k),$$

$$\mu_{ij} := \frac{\mathbf{b}_i^t \mathbf{b}_j^*}{\mathbf{b}_j^{*\,t} \mathbf{b}_j^*} \qquad (1 \leq j < i \leq k).$$

Theorem

$$d(\Lambda) = \prod_{i=1}^{k} \|\mathbf{b}_i^*\| \leq \prod_{i=1}^{k} \|\mathbf{b}_i\| \ .$$

Corollary $d(\Lambda)^2 \leq M_1 \cdot \ldots \cdot M_k$.

LLL–reduced bases

Definition A lattice basis $\mathbf{b}_1, \dots, \mathbf{b}_k$ is called **LLL–reduced** if it satisfies the following conditions:

1. $|\mu_{ij}| \leq \frac{1}{2}$ $(1 \leq j < i \leq k)$,
2. $\|\mathbf{b}_i^* + \mu_{i,i-1}\mathbf{b}_{i-1}^*\|^2 \geq \frac{3}{4}\|\mathbf{b}_{i-1}^*\|^2$ $(1 < i \leq k)$.

Theorem A LLL–reduced basis $\mathbf{b}_1, \dots, \mathbf{b}_k$ satisfies:

1. $\prod_{i=1}^{k} \|\mathbf{b}_i\| \leq 2^{\frac{1}{4}k(k-1)} d(\Lambda)$,
2. $\|\mathbf{b}_1\| \leq 2^{\frac{1}{4}(k-1)} d(\Lambda)^{\frac{1}{k}}$,
3. $\|\mathbf{b}_1\|^2 \leq 2^{k-1}\|\mathbf{x}\|^2 \ \forall\, \mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}$,

LLL–algorithm

1. Set $\mathbf{c}_i \leftarrow \mathbf{b}_i, C_i \leftarrow \|\mathbf{c}_i^*\|^2$ $(1 \leq i \leq k)$ and $m \leftarrow 2$.
2. Set $\ell \leftarrow m-1$.
3. For $|\mu_{m\ell}| > \frac{1}{2}$ set

$$r \leftarrow \operatorname{sign}(\mu_{m\ell})\lfloor|\mu_{m\ell}| + \frac{1}{2}\rfloor, \quad c_m \leftarrow c_m - rc_\ell,$$

$$\mu_{mj} \leftarrow \mu_{mj} - r\mu_{\ell j} \quad (1 \leq j \leq \ell - 1), \quad \mu_{m\ell} \leftarrow \mu_{m\ell} - r.$$

For $\ell < m-1$, go to 5.
4. For $C_m < (\frac{3}{4} - \mu_{m,m-1}^2)C_{m-1}$ go to 6.

LLL–algorithm

5. Set $\ell \leftarrow \ell - 1$. For $\ell > 0$ go to 3.
For $m = k$, terminate, else set $m \leftarrow m + 1$ and go to 2.

6. (Exchange $\mathbf{c}_{m-1}$ and $\mathbf{c}_m$) Set $\mu \leftarrow \mu_{m,m-1}$, $C \leftarrow C_m + \mu^2 C_{m-1}$ and

$$\mu_{m,m-1} \leftarrow \mu \frac{C_{m-1}}{C}, C_m \leftarrow \frac{C_{m-1} C_m}{C}, C_{m-1} \leftarrow C, \begin{pmatrix} \mathbf{c}_{m-1} \\ \mathbf{c}_m \end{pmatrix} \leftarrow \begin{pmatrix} \mathbf{c}_m \\ \mathbf{c}_{m-1} \end{pmatrix}$$

Also set

$$\begin{pmatrix} \mu_{m-1,j} \\ \mu_{mj} \end{pmatrix} \leftarrow \begin{pmatrix} \mu_{mj} \\ \mu_{m-1,j} \end{pmatrix} \quad (1 \leq j \leq m-2),$$

and for $i = m+1, \ldots, k$ eventually

$$\begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix} \leftarrow \begin{pmatrix} 1 & \mu_{m,m-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\mu \end{pmatrix} \begin{pmatrix} \mu_{i,m-1} \\ \mu_{im} \end{pmatrix}.$$

For $m > 2$ set $m \leftarrow m - 1$. Go to 2.

Construction of a lattice from sublattices I

Let $\mathbf{c}_1, \ldots, \mathbf{c}_k \in \Lambda$ be linearly independent. For arbitrary non-zero $\mathbf{c}_{k+1} \in \Lambda$ we calculate $m_1, \ldots, m_{k+1} \in \mathbb{Z}$ with

$$\sum_{i=1}^{k+1} m_i \mathbf{c}_i = 0 \qquad (|m_1| + \ldots + |m_{k+1}| > 0) \ .$$

Also we determine $\mathbf{c}_1', \ldots, \mathbf{c}_k' \in \Lambda$ with

$$\sum_{i=1}^{k+1} \mathbb{Z} \cdot \mathbf{c}_i = \sum_{i=1}^{k} \mathbb{Z} \cdot \mathbf{c}_i' \ .$$

Construction of a lattice from sublattices II

Originally, this problem was solved with LLL–reduction applied to a lattice with basis given by the columns of the matrix:

$$\left(\begin{array}{ccccccc} 1 & 0 & & & & & 0 \\ 0 & 1 & 0 & & & & 0 \\ & & \cdot & \cdot & \cdot & & \\ & & \cdot & \cdot & \cdot & & \\ 0 & & & & & 0 & 1 \\ 2^{\lambda}\mathbf{c}_1 & \cdot & \cdot & \cdot & \cdot & 2^{\lambda}\mathbf{c}_k & 2^{\lambda}\mathbf{c}_{k+1} \end{array}\right) .$$

If we choose $\lambda > 0$ sufficiently large (in dependence of the input data) then a LLL–reduced basis contains a vector whose last *n* coordinates are 0.

Example

Solve $A\mathbf{x} = \mathbf{b}$ in integers for

$$A = \begin{pmatrix} -8 & 5 & 7 & -7 & 3 & -7 & 4 & 9 & -6 \\ 1 & -2 & 0 & -10 & -4 & 3 & 8 & 5 & 2 \\ -7 & 3 & 6 & 5 & 1 & 2 & 5 & 0 & -6 \\ -9 & -3 & 4 & 9 & -2 & 6 & 1 & -10 & -9 \\ -2 & 1 & -5 & -4 & 3 & 7 & -8 & -8 & -5 \\ -1 & 1 & -8 & 4 & -8 & -1 & -9 & 8 & 6 \end{pmatrix}$$

and $\mathbf{b}^t = (3, -1, -1, -7, 9, 8)$.

MLLL–algorithm

The MLLL–algorithm is applied to the columns of the matrix $(A, \mathbf{b})$. When it terminates the last row of the transformation matrix contains the solution:

$$\begin{pmatrix} 11297648 \\ 5877935 \\ 25586565 \\ -4243288 \\ -13007950 \\ 7269435 \\ -14476828 \\ -28 \\ 0 \end{pmatrix} .$$

Non–integral lattices

In algorithmic algebraic number theory we would like to apply the MLLL–algorithm also to non-integral lattices.

During interactive calculations one easily observes when a linear combination represents $\mathbf{0}$.

A criterion for termination is not easy, however, since round-off errors occur.

Let $\mathbf{b}_1, ..., \mathbf{b}_{\mu-1}$ be linearly independent and

$$\Lambda_\mu \; = \; \sum_{j=1}^{\mu} \mathbb{Z}\mathbf{b}_j$$

be a sublattice of the considered lattice Λ. In case $\mathbf{b}_\mu^* \neq \mathbf{0}$ we obtain for the discriminant

$$d(\Lambda_\mu) \; = \; \prod_{j=1}^{\mu} \parallel \mathbf{b}_j^* \parallel$$

and for the length of a shortest vector, say $\mathbf{y} \neq \mathbf{0}$, the estimate

$$\parallel \mathbf{y} \parallel^2 \leq \; (\gamma_\mu^\mu d(\Lambda_\mu)^2)^{1/\mu} \; .$$

If we can get a lower bound for the first successive minimum M_1 of Λ_μ the estimate

$$M_1^\mu \;\leq\; (\gamma_\mu^\mu d(\Lambda_\mu)^2) \;=\; \gamma_\mu^\mu \prod_{j=1}^{\mu} \parallel \mathbf{b}_j^* \parallel^2$$

yields a lower bound for $\parallel \mathbf{b}_\mu^* \parallel$.

In the case of unit computations of orders in algebraic number fields we have the following option.

The coordinates of the considered lattice vectors are logarithms of the absolute values of the conjugates of algebraic numbers which are no roots of unity.

For field degrees $d \leq 2300$ the best known result was proved by **Matveev** in 1991:

An algebraic integer $\alpha \neq 0$ of degree $d \geq 2$ which is not a root of unity has one conjugate whose absolute value is larger than

$$\exp\left(\frac{3\log(d/2)}{d^2}\right) \ .$$

From this we immediately obtain a lower bound for M_1. Hence, the MLLL–algorithm can also be used for calculations in lattices coming from units (in logarithmic space) and it produces provably correct results.

Minkowski's Convex Body Theorem

Let $C \subseteq \mathbb{R}^n$ be a convex, $\mathbf{0}$–symmetric set and Λ be an n–dimensional lattice. Then C contains a lattice vector $\mathbf{x} \neq \mathbf{0}$ if one of the following conditions is satisfied:
1. $\text{vol}(C) > 2^n d(\Lambda)$;
2. $\text{vol}(C) \geq 2^n d(\Lambda)$ and C is compact.

Hermite normal form

For every matrix $A = (a_{ij}) \in \mathbb{Z}^{m \times n}$ there exists a unimodular matrix $U \in \mathbb{Z}^{n \times n}$ such that $H = H(A) = (h_{ij}) := AU$ is a lower triangular matrix whose entries satisfy

1. $h_{ii} \geq 0$ for $1 \leq i \leq \min(m, n)$,

2. in case $h_{ii} > 0$ we also have $0 \leq h_{ij} < h_{ii}$ for $j < i$.

Free modules over principal ideal domains

Let M be a free module with basis $b_1, ..., b_k$ over a principal ideal domain R.
1. Every submodule $\tilde{M}$ of M is a free module of rank $\leq k$.
2. Let i be a fixed index with $0 \leq i < n$. Then $b_1, ..., b_{i-1}, c$ with $c \in M$ can be extended to a basis of M precisely if the coefficients in the basis presentation $c = \gamma_1 b_1 + ... + \gamma_k b_k$ satisfy $\gcd(\gamma_i, ..., \gamma_k) = 1$.