Denis SIMON
Université de Caen
www.math.unicaen.fr/~simon

Reduction of indefinite quadratic forms and applications

WORKSHOP PARI/GP
IHP, September 2004

The 3-dimensional case : the idea of Gauss

We want to solve $Q(x) = 0$, with $Q \in \mathcal{M}_3(\mathbb{Z})^{sym}$.

- **Step 1, Minimization : build another quadratic equation $Q'(y) = 0$ with $\det Q' = -1$.**

- **Step 2, Reduction : find a basis, in which $Q' \simeq \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.**

- **Step 3 : from a solution of $Q'(y) = 0$, rebuild a solution of $Q(x) = 0$**

Ingredients of the minimization

- **Factorization of the** $\det Q$**.**
- **Linear algebra** $\mod p$**.**
- **Square roots** $\mod p$**.**

Gram-Schmidt orthogonalization

Notation: $\mathbf{b}_i \cdot \mathbf{b}_j := \mathbf{b}_i^t Q \mathbf{b}_j$.
Start with a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$.

<u>**Formulae :**</u> **(defined by induction)**

$$\mathbf{b}_i^* = \mathbf{b}_i - \sum_{j=1}^{i-1} \mu_{i,j} \mathbf{b}_j^*$$

with

$$\mu_{i,j} = \mathbf{b}_i \cdot \mathbf{b}_j^* / \mathbf{b}_j^* \cdot \mathbf{b}_j^* \ .$$

The basis $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ **is orthogonal.**

LLL for definite quadratic forms

Algorithm : **Let** $\frac{1}{4} < c < 1$**. Start with a basis** $\mathbf{b}_1, \ldots, \mathbf{b}_n$ **of** $\mathbb{Z}^n$

1- Set $k = 2$.

2- Compute the $\mathbf{b}_i^*$ and the $\mu_{i,j}$ using Gram-Schmidt.

3- for $i = n, \cdots, 1$, for $j = 1, \cdots, i-1$ set $q = \lfloor \mu_{i,j} \rceil$, $\mathbf{b}_i = \mathbf{b}_i - q\mathbf{b}_j$ and $\mu_{i,j} = \mu_{i,j} - q$.

4- If $(\mathbf{b}_k^*)^2 + \mu_{k,k-1}^2 \left(\mathbf{b}_{k-1}^*\right)^2 < c\left(\mathbf{b}_{k-1}^*\right)^2$, exchange $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$, and set $k = \max(k-1, 2)$. Otherwise, set $k = k+1$.

5- If $k < n$, go to step 2, otherwise, return the basis $(\mathbf{b}_i)$.

Bounds for the definite LLL

Theorem : **Let** $Q \in \mathcal{M}_n(\mathbb{Z})^{sym}$ **with** $\det Q \neq 0$**. Let** $\frac{1}{4} < c < 1$**.**
Apply LLL to Q**, then :**
it finishes (after a polynomial number of steps) with a reduced basis $\mathbf{b}_1$**,...,**$\mathbf{b}_n$ **such that**

$$|(\mathbf{b}_1)^2|^n \leqslant \gamma^{n(n-1)/2} |\det(Q)| \ ,$$

where $\gamma = \left(c - \frac{1}{4}\right)^{-1} > \frac{4}{3}$**.**

LLL for indefinite quadratic forms

Algorithm : **Let** $\frac{1}{4} < c < 1$. **Start with a basis** $\mathbf{b}_1, \ldots, \mathbf{b}_n$ **of** $\mathbb{Z}^n$

1- Set $k = 2$.

2- Compute the $\mathbf{b}_i^*$ and the $\mu_{i,j}$ using Gram-Schmidt.

3- for $i = n, \cdots, 1$, for $j = 1, \cdots, i-1$ set $q = \lfloor \mu_{i,j} \rceil$, $\mathbf{b}_i = \mathbf{b}_i - q\mathbf{b}_j$ and $\mu_{i,j} = \mu_{i,j} - q$.

4- If $\left| (\mathbf{b}_k^*)^2 + \mu_{k,k-1}^2 \left(\mathbf{b}_{k-1}^*\right)^2 \right| < c \left| \left(\mathbf{b}_{k-1}^*\right)^2 \right|$, exchange $\mathbf{b}_k$ and $\mathbf{b}_{k-1}$, and set $k = \max(k-1, 2)$. Otherwise, set $k = k + 1$.

5- If $k < n$, go to step 2, otherwise, return the basis $(\mathbf{b}_i)$.

Bounds for the indefinite LLL

Theorem : **Let** $Q \in \mathcal{M}_n(\mathbb{Z})^{sym}$ **with** $\det Q \neq 0$**. Let** $\frac{1}{4} < c < 1$**.**
Apply the modified LLL to Q**, then :**

- **EITHER** **it finishes (after a polynomial number of steps) with a reduced basis** $\mathbf{b}_1, \ldots, \mathbf{b}_n$ **such that**

$$|(\mathbf{b}_1)^2|^n \leqslant \gamma^{n(n-1)/2} |\det(Q)| \ ,$$

where $\gamma = \left(c - \frac{1}{4}\right)^{-1} > \frac{4}{3}$**.**
If furthermore Q **is indefinite, we have**

$$1 \leqslant |(\mathbf{b}_1)^2|^n \leqslant \frac{3}{4} \gamma^{n(n-1)/2} |\det(Q)| \ .$$

- **OR** **it crashes ...**

Bounds for the indefinite LLL

... because it has found a SOLUTION of $Q(\mathbf{x}) = 0$!!