Geodesic continued fractions and LLL

Frits Beukers

Paris, 20 December 2013

Quadratic forms

In two variables: $Q(x, y) = ax^2 + 2bxy + cy^2$
In n variables:

$$Q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} q_{ij} x_i x_j, \quad q_{ij} = q_{ji} \in \mathbb{R}.$$

Coefficient matrix in the case $n = 2$:

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}.$$

We consider only positive definite forms, i.e. $q(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \mathbb{R}^n$ and $q(\mathbf{x}) = 0 \iff \mathbf{x} = \mathbf{0}$.
The determinant of Q is defined by $D(Q) = |\det(q_{ij})|$.
For $Q = ax^2 + 2bxy + cy^2$ we get $D(Q) = |b^2 - ac|$.

Minima

We shall be interested in

$$\mu_Q := \min_{\mathbf{x} \in \mathbb{Z}^n \setminus \mathbf{0}} Q(\mathbf{x}).$$

Theorem (Hermite)

For every $n \geq 2$ there exists γ_n such that $\mu_Q \leq \gamma_n D(Q)^{1/n}$ for all positive definite forms Q in n variables.

Some values: $\gamma_2 = 2/\sqrt{3}, \gamma_3 = 2^{1/3}, \gamma_4 = \sqrt{2}, \ldots$
In general: $\gamma_n \leq 2n/3$.

Reduction of forms

The form $Q = ax^2 + 2bxy + cy^2$ is called *reduced* if

$$-a \leq 2b \leq a \leq c.$$

For a reduced binary form Q we have $\mu_Q = a$ (with $x = 1, y = 0$).

Reduction of quadratic binary form $ax^2 + 2bxy + cy^2$ modulo $SL(2, \mathbb{Z})$.
Loop:

- if $a < |2b|$, replace x by $x - ky$ with $k = \lfloor b/a + 1/2 \rfloor$.
- if $a > c$ replace x by $-y$ and y by x.
- if the resulting form is reduced then STOP else goto **Loop**.

Example

We reduce the form $13x^2 + 62xy + 74y^2$.

- replace x by $x - 2y$: $13x^2 + 10xy + 2y^2$.
- replace $x \to -y,\ y \to x$: $2x^2 - 10xy + 13y^2$.
- replace x by $x + 3y$: $2x^2 + 2xy + y^2$.
- replace $x \to -y,\ y \to x$: $x^2 - 2xy + 2y^2$.
- replace x by $x + y$: $x^2 + y^2$.

Concatenation of all substitutions shows:
$13(-7x-5y)^2+62(-7x-5y)(3x+2y)+74(3x+2y)^2 = x^2+y^2$.
Minimum 1 attained when $x = 1, y = 0$ hence
$13 \cdot (-7)^2 + 62 \cdot (-7) \cdot 3 + 74 \cdot 3^2 = 1$.

Relation with continued fractions

Let $\alpha \in \mathbb{R}$. Choose $1 >> t > 0$ and consider

$$Q_t(x, y) = (x - \alpha y)^2 + ty^2.$$

Then $D(Q) = t$. There exist integers p, q with $q > 0$ such that

$$(p - \alpha q)^2 + tq^2 \leq 2\sqrt{t}/\sqrt{3}.$$

Hence (because $|ab| \leq (a^2 + b^2)/2$):

$$|p - \alpha q|(q\sqrt{t}) \leq \sqrt{t}/\sqrt{3}$$

and so

$$|p - \alpha q| \leq \frac{1}{q\sqrt{3}}.$$

The upper half plane

Let $\mathcal{H}$ be the complex upper half plane. There is a 1-1 correspondence

Positive definite binary quadratic forms modulo scalar factors $\longleftrightarrow \mathcal{H}$

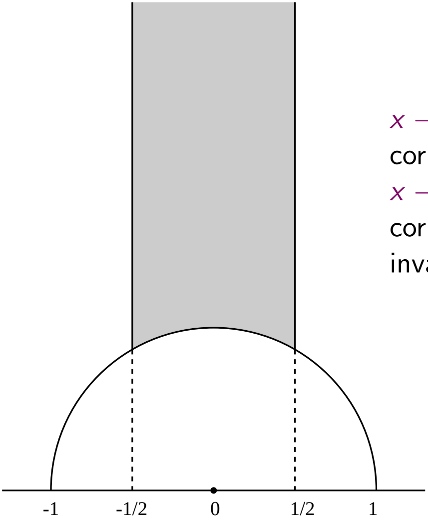
given by

$$ax^2 + 2bxy + cy^2 \longleftrightarrow \frac{-b + \sqrt{b^2 - ac}}{a}.$$

In particular,

$$(x - \alpha y)^2 + ty^2 \longleftrightarrow \alpha + i\sqrt{t}.$$

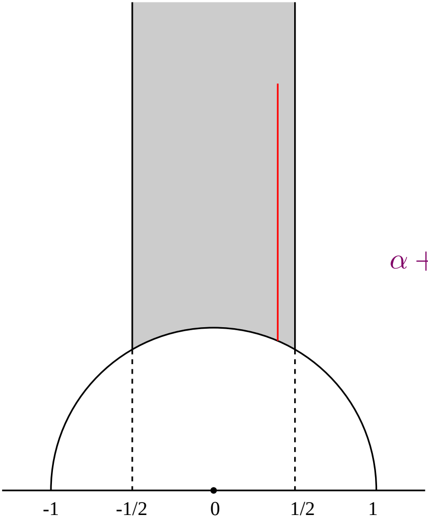
Hermite's algorithm



$x \to x + y, y \to y$
corresponds to $z \to z - 1$
$x \to -y, y \to x$
corresponds to $z \to -1/z$
invariant metric:

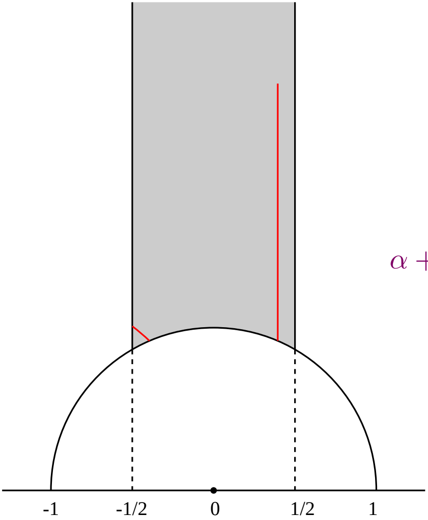
$$ds = \frac{|dz|}{\mathrm{Im}(z)}$$

Hermite's algorithm



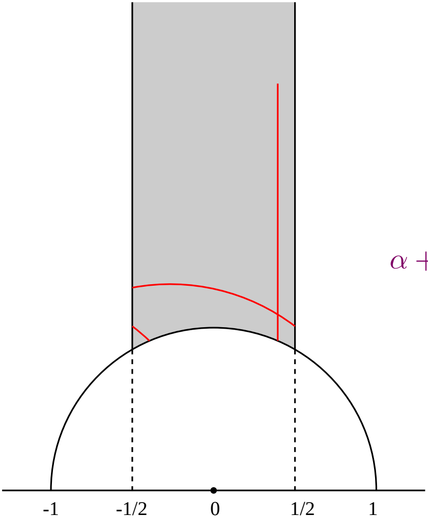
$\alpha + i\sqrt{t}, \ t \downarrow 0$

Hermite's algorithm



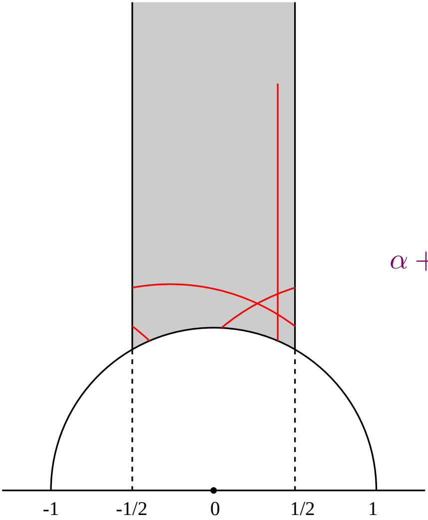
$\alpha + i\sqrt{t},\ t \downarrow 0$

Hermite's algorithm



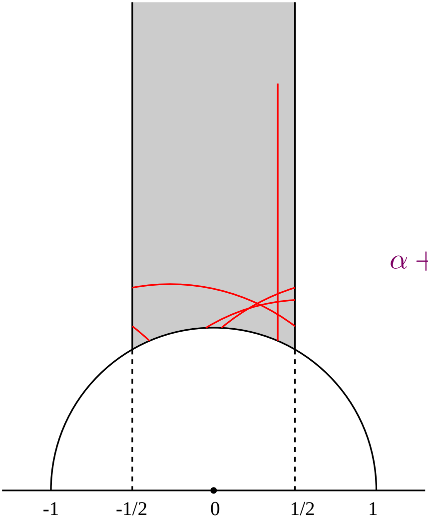
$\alpha + i\sqrt{t},\ t \downarrow 0$

Hermite's algorithm



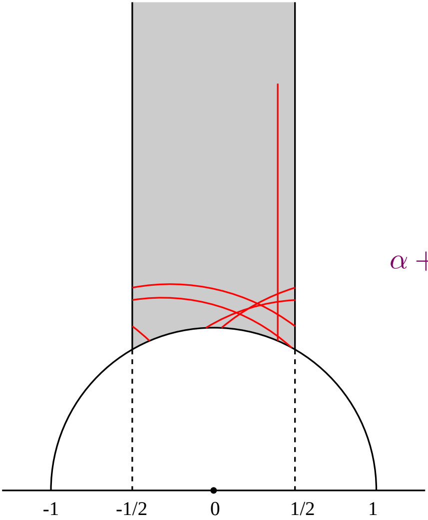
$\alpha + i\sqrt{t},\ t \downarrow 0$

Hermite's algorithm



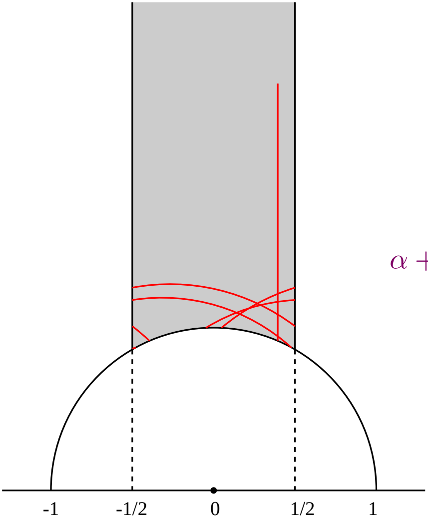
$\alpha + i\sqrt{t},\ t \downarrow 0$

Hermite's algorithm



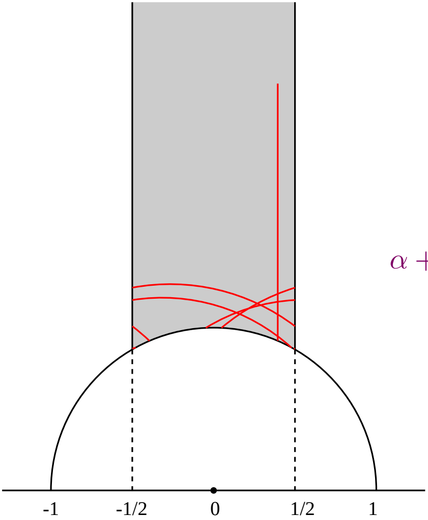
$\alpha + i\sqrt{t},\ t \downarrow 0$

Hermite's algorithm



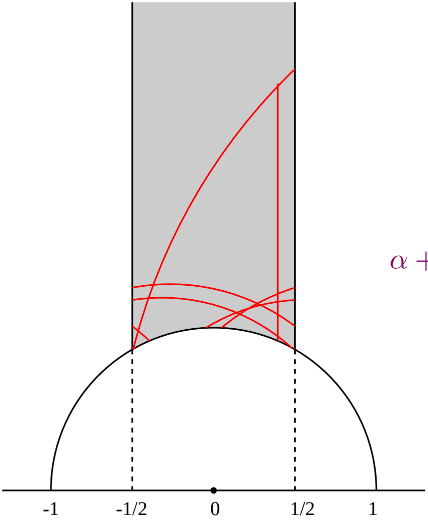
$\alpha + i\sqrt{t},\ t \downarrow 0$

Hermite's algorithm



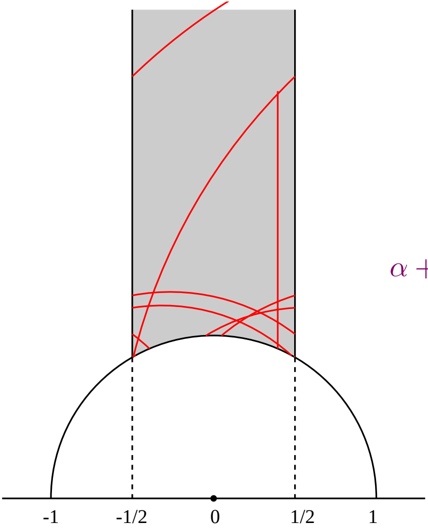
$\alpha + i\sqrt{t},\ t \downarrow 0$

Hermite's algorithm



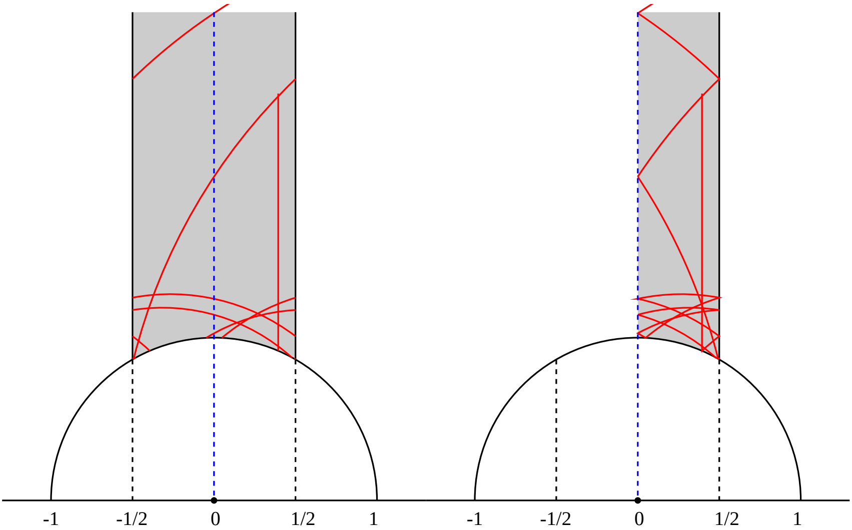
$\alpha + i\sqrt{t},\ t \downarrow 0$

Hermite's algorithm



$\alpha + i\sqrt{t}, \ t \downarrow 0$

Hermite's algorithm



Simultaneous approximation

Theorem (Dirichlet)

Let $\alpha_1, \ldots, \alpha_d \in \mathbb{R}$. Then there exist infinitely many $(p_1, \ldots, p_d, q) \in \mathbb{Z}^{d+1}$ with $q > 0$ such that

$$\left|\alpha_i - \frac{p_i}{q}\right| \leq \frac{1}{q^{1+1/d}}, \quad i = 1, 2, \ldots, d.$$

Theorem (Schweiger)

There exists $\delta > 0$ such that for almost all pairs α_1, α_2 the Jacobi-Perron algorithm gives us

$$\left|\alpha_i - \frac{p_i}{q}\right| \leq \frac{1}{q^{1+\delta}}, \quad i = 1, 2.$$

Geodesic approach (J.Lagarias)

Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d) \in \mathbb{R}^d$ and $t > 0$. Consider the quadratic form

$$Q_t(\mathbf{x}, y) = (x_1 - \alpha_1 y)^2 + \cdots + (x_d - \alpha_d y)^2 + ty^2$$

.

Proposition (Hermite, Lagarias)

Suppose that $\mathbf{x} = \mathbf{p} \in \mathbb{Z}^d$ and $y = q \in \mathbb{Z}_{\geq 0}$ minimize the form $Q_t(\mathbf{x}, y)$. Then

$$||\mathbf{p} - \boldsymbol{\alpha} q|| \leq \frac{\sqrt{d+1}}{q^{1/d}}.$$

Minkowski reduction

Definition

A positive definite quadratic form Q in $x_1, \ldots, x_n$ is called *Minkowski reduced* if

- $Q(\mathbf{e}_1) \leq Q(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}^n,\ \mathbf{x} \neq \mathbf{0}$.
- For all $j > 1$: $Q(\mathbf{e}_j) \leq Q(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{Z}^n$ such that $\mathbf{e}_1, \ldots, \mathbf{e}_{j-1}, \mathbf{x}$ can be extended to a $\mathbb{Z}$-basis of $\mathbb{Z}^n$.

Minkoswki reducedness can be characterized by a finite set of linear conditions on the coefficients of Q.

Conditions for 3 variables

Recall: reducedness conditions for $Q = ax^2 + 2bxy + cy^2$,

$$-a \leq 2b \leq a \leq c.$$

Consider the positive definite form

$$Q(x, y, z) = ax^2 + 2bxy + 2cxz + dy^2 + 2eyz + fz^2.$$

Minkowski reducedness conditions:

$$\begin{aligned} &a \leq d \leq f, \quad |2b| \leq a, |2c| \leq a, |2e| \leq d \\ &a + d \geq 2(\pm b \pm c \pm e), \quad \text{zero or two minus signs.} \end{aligned}$$

Unfortunately, the number of conditions grows exponentially in n.

A symmetric space

Let $\mathcal{Q}_n$ be the set of positive definite quadratic forms in n variables. Consider $\Phi : GL(n, \mathbb{R}) \to \mathcal{Q}_n$ given by

$$\Phi : M \mapsto M^T M.$$

It is surjective and $\Phi(M) = \Phi(M')$ if and only if there exists orthogonal U such that $M' = UM$. Hence Φ gives bijection

$$O(n, \mathbb{R}) \backslash GL(n, \mathbb{R}) \longleftrightarrow \mathcal{Q}_n.$$

The group $GL(n, \mathbb{R})$ (and in particular $GL(n, \mathbb{Z})$) acts via
$g : M \mapsto Mg$ and $g : Q \mapsto g^T Q g$.
Space of $GL(n, \mathbb{Z})$ equivalence classes of positive definite quadratic forms modulo scalars:

$$\mathbb{R}^\times O(n, \mathbb{R}) \backslash GL(n, \mathbb{R}) / GL(n, \mathbb{Z}).$$

Geodesics

$GL(n, \mathbb{R})$-invariant metric:

$$ds^2 = \mathrm{tr}((dY.Y^{-1}).(dY.Y^{-1})^T).$$

Geodesics on the space of quadratic forms:

$$e^{\lambda_1 s} l_1(\mathbf{x})^2 + \cdots + e^{\lambda_n s} l_n(\mathbf{x})^2, \; s \in \mathbb{R}$$

where $l_1(\mathbf{x}), \ldots, l_n(\mathbf{x})$ are independent linear forms.
In particular,

$$(x_1 - \alpha_1 y)^2 + \cdots + (x_d - \alpha_d y)^2 + ty^2$$

is a geodesic in $\mathcal{Q}_{d+1}$.

LLL reduction

Any quadratic form Q in $x_1, \ldots, x_n$ can be rewritten as

$$\begin{aligned}
Q(\mathbf{x}) &= b_1(x_1 + \mu_{12}x_2 + \cdots + \mu_{1n}x_n)^2 \\
&\quad + b_2(x_2 + \mu_{23}x_3 + \cdots + \mu_{2n}x_n)^2 \\
&\quad \vdots \\
&\quad + b_{n-1}(x_{n-1} + \mu_{n-1,n}x_n)^2 + b_n x_n^2.
\end{aligned}$$

Example:

$$\begin{aligned}
Q &= ax^2 + 2bxy + 2cxz + dy^2 + 2eyz + fz^2 \\
&= a(x + by/a + cz/a)^2 + d'y^2 + 2e'yz + f'z^2 \\
&= a(x + by/a + cz/a)^2 + d'(y + e'z/d')^2 + f''z^2
\end{aligned}$$

LLL reducedness

Any quadratic form Q in $x_1, \ldots, x_n$ can be rewritten as

$$\begin{aligned} Q(\mathbf{x}) &= b_1(x_1 + \mu_{12}x_2 + \cdots + \mu_{1n}x_n)^2 \\ &\quad + b_2(x_2 + \mu_{23}x_3 + \cdots + \mu_{2n}x_n)^2 \\ &\quad \vdots \\ &\quad + b_{n-1}(x_{n-1} + \mu_{n-1,n}x_n)^2 + b_n x_n^2. \end{aligned}$$

Let $\omega \in (3/4, 1]$ (slack-factor). Then Q is called LLL-reduced if:

- $|\mu_{ij}| \leq 1/2$ for all $i < j$.
- $b_{i+1} + \mu_{i,i+1}^2 b_i \geq \omega b_i$ for all $i < n$.
  (Lovasz condition)

LLL reduction

LLL-reduction consists of

- *shifts* $x_i \to x_i + ax_j$ with $j > i$ and $a \in \mathbb{Z}$
- *swaps* $x_i \leftrightarrow x_{i+1}$ for some $i < n$.

LLL-reduction algorithm:

- Perform shifts so that $|\mu_{i,i+1}| \leq 1/2$ for all $i < n$. Then enter the following
- **Loop**: find i such that $\omega b_i > b_{i+1} + \mu_{i,i+1}^2 b_i$,
  - If such i exists, swap $x_i \leftrightarrow x_{i+1}$ and fix $\mu_{i-1,i}, \mu_{i,i+1}$ and $\mu_{i+1,i+2}$ by a shift. REPEAT the **Loop**.
  - If no such i exists, EXIT the **Loop**.
- Now the Lovasz conditions hold and $|\mu_{i,i+1}| \leq 1/2$ for $i < n$ (partial LLL-reduction). Perform shifts so that $|\mu_{ij}| \leq 1/2$ for all $i < j$.

LLL properties

Theorem (LLL)

Let Q be a form in n variables with coefficients $\leq M$. Then the number of swaps in the LLL-reduction is bounded by $O(n^2 \log(n^2 M/\mu_Q))$.

Theorem (LLL)

Let Q be a positive definite form in n variables and suppose Q is LLL-reduced with $\omega = 3/4$. Then

- $Q(\mathbf{e}_1) \leq 2^{(n-1)/2} d(Q)^{1/n}$.
- For every $\mathbf{x} \in \mathbb{Z}^n$ with $\mathbf{x} \neq \mathbf{0}$ we have $Q(\mathbf{e}_1) \leq 2^{n-1} Q(\mathbf{x})$.

A continued fraction algorithm

Let $\alpha_1, \ldots, \alpha_d \in [-1/2, 1/2]$.
We initialize with the form

$$Q_t^{(0)} = (x_1 - \alpha_1 y)^2 + \cdots + (x_d - \alpha_d y)^2 + ty^2.$$

When $t = 1$ it is LLL-reduced. Define $P^{(0)}$ as the $(d+1) \times (d+1)$ identity matrix. We enter the following loop.

Loop:

- Determine the minimum of the set $\{t | Q_t^{(k)} \text{ is LLL} - \text{reduced}\}$ and call it t_k.
- Perform an LLL-reduction on $Q_{t_k - \epsilon}^{(k)}$ for infinitesimal $\epsilon > 0$ and let $\mathbf{x} \to A_k \mathbf{x}$ be the corresponding substitution of variables.
- Define $Q_t^{(k+1)}(\mathbf{x}) = Q_t^{(k)}(A_k \mathbf{x})$ and $P^{(k+1)} = P^{(k)} A_k$.

Property: Let $(p_1, p_2, \ldots, p_d, q)$ be the first column of $P^{(k)}$. Then

$$||\mathbf{p} - \boldsymbol{\alpha} q|| \leq \frac{2^{d/4}}{q^{1/d}}.$$

Explicit formulas

Let $(q_{ij})_{i,j}$ be the matrix of the quadratic form Q.
Define for all $1 \leq i < j \leq n$

$$B_{ij} = \begin{vmatrix} q_{11} & \cdots & q_{1,i-1} & q_{1j} \\ q_{21} & \cdots & q_{2,i-1} & q_{2j} \\ \vdots & & \vdots & \vdots \\ q_{i1} & \cdots & q_{i,i-1} & q_{ij} \end{vmatrix}.$$

Then

$$\mu_{ij} = B_{ij}/B_{ii}, \quad b_i = B_{i,i}/B_{i-1,i-1}.$$

Explicit inequalities

The inequality $|\mu_{ij}| \leq 1/2$ translates into

$$-B_{ii} \leq 2B_{ij} \leq B_{ii},\ j = i+1, \ldots, n.$$

The inequality $b_{i+1} + \mu_{i,i+1}^2 b_i \geq \omega b_i$ translates into

$$C_{i,i} \geq \omega B_{i,i}$$

where $C_{i,i}$ is the i, i subdeterminant of $B_{i+1,i+1}$.
We have

$$C_{i,i} B_{i,i} = B_{i+1,i+1} B_{i-1,i-1} + B_{i,i+1}^2.$$

Special forms

Observation

Consider the family of forms

$$Q_t = (x_1 - \alpha_1 y)^2 + \cdots + (x_d - \alpha_d y)^2 + ty^2, \quad t > 0.$$

Let $B_{ij}(t)$ be the corresponding subdeterminants. Then $B_{ij}(t)$ is linear in t for all $i \leq j$.

More precisely, $B_{ij}(t) \in \mathbb{Z}[t, \alpha_1, \ldots, \alpha_d]$. It is linear in t with coefficient in $\mathbb{Z}$ and quadratic in the α_i.

Properties

Properties of the geodesic LLL-algorithm:

- The value of t_k is determined by a finite set of linear inequalities.
- All transformation matrices $P^{(k)}$ are distinct.
- If $\alpha_i \notin \mathbb{Q}$ for at least one i, then $\lim_{k\to\infty} t_k = 0$.
- If $\alpha_i \in \mathbb{Q}$ for all i, the algorithm breaks off.
- The first column of $P^{(k)}$ only changes when the swap $x_1 \leftrightarrow x_2$ is made.

Outlook

- Literature
- Experiments
- Is it useful?

The end