

Using layered lattices

Erwin L. Torreao Dassen,
Universiteit Leiden, The Netherlands

Amsterdam, May 7, 2010
Public Key Cryptography and the Geometry of Numbers



Statement of a problem

Recall from yesterday's first lecture:

Short vectors in a lattice can represent good solutions to a problem and the shortest an optimal one.

Example

Let $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ be a morphism of free groups and let $a \in \mathbb{Z}^m$. Define $q : \mathbb{Z}^n \times \mathbb{Z} \rightarrow \mathbb{R}$ by

$$q(y, z) = \|y\|^2 + M \cdot z^2 + N \|f(y) - z \cdot a\|^2$$

for given constants $0 \ll M \ll N$. Then, for big enough M and N an element $x = (y, z)$ of a reduced basis for L satisfies:

$$\begin{aligned} y \in \ker f &\iff q(x) < M \\ f(y) = b &\iff M < q(x) < 4M < N \end{aligned}$$

Drawbacks

- ▷ There is much freedom in the choice of M, N , they only have to be “big”.
- ▷ “Big” here depends on the particular instance of the problem and of the algorithm (for example LLL) we want to use to find short vectors.
- ▷ These constants carry computational overhead so it would be best to avoid them altogether.
- ▷ Solution: regard them as symbols. This amounts to setting $M = \infty$ and $N = \infty^2$. We are led to the concept of a *layered lattice*.

Definitions

Recall that a lattice is a pair (L, q) where L is a free abelian group of finite rank and $q : L \rightarrow \mathbb{R}$ is a map satisfying:

- (i) $x \neq 0 \implies q(x) \neq 0$
- (ii) $q(x + y) + q(x - y) = 2q(x) + 2q(y)$
- (iii) $q(L) \subset \mathbb{R}$ is well-ordered.

Definitions

Recall that a lattice is a pair (L, q) where L is a free abelian group of finite rank and $q : L \rightarrow \mathbb{R}$ is a map satisfying:

- (i) $x \neq 0 \implies q(x) \neq 0$
- (ii) $q(x + y) + q(x - y) = 2q(x) + 2q(y)$
- (iii) $q(L) \subset \mathbb{R}$ is well-ordered.

From now on denote by V the real vector space \mathbb{R}^n equipped with the anti-lexicographic order and let $V_k = \bigoplus_{l \leq k} \mathbb{R}e_l$, $i = 1, \dots, n$.

A *layered lattice* is a triple (L, V, q) where L is a free abelian group and $q : L \rightarrow V$ is a map such that the following holds.

- (i) $x \neq 0 \implies q(x) \neq 0$
- (ii) $q(x + y) + q(x - y) = 2q(x) + 2q(y)$
- (iii) $\{q(x) : x \in L\} \subset V$ is well-ordered.

Characterization

V_i is the unique k -dimensional convex subspaces of V :

$$u \in V_l, v \in V_k \setminus V_l \implies \forall \lambda \in \mathbb{R}, \lambda u < |v|.$$

The *layers* of L are the (pure) subgroups

$$L_k = \{x \in L : q(x) \in V_k\}, \quad k = 1, \dots, n$$

Theorem

(L, q) is a layered lattice if and only if for all $k \in \{1, \dots, n\}$,

$$(L_k/L_{k-1}, V_k/V_{k-1} \simeq \mathbb{R}, q)$$

is a lattice.

Our example revisited

Let $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ be a morphism of groups and $a \in \mathbb{Z}^m$ we define

$$q : \mathbb{Z}^n \times \mathbb{Z} \rightarrow V = \mathbb{R}^3$$

by

$$q(y, z) = (\|y\|^2, z^2, \|f(y) - z \cdot a\|^2).$$

Then (\mathbb{Z}^{n+1}, q, V) is a layered lattice.

- ▷ The first layer, L_1 equals the kernel of f .

Our example revisited

Let $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ be a morphism of groups and $a \in \mathbb{Z}^m$ we define

$$q : \mathbb{Z}^n \times \mathbb{Z} \rightarrow V = \mathbb{R}^3$$

by

$$q(y, z) = (\|y\|^2, z^2, \|f(y) - z \cdot a\|^2).$$

Then (\mathbb{Z}^{n+1}, q, V) is a layered lattice.

- ▷ The first layer, L_1 equals the kernel of f .
- ▷ We have $L_1 \subseteq L_2$ and the elements of L_2 parametrize solutions of $f(y) = z \cdot a$. Note that the rank of L_2/L_1 is at most 1.

Our example revisited

Let $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ be a morphism of groups and $a \in \mathbb{Z}^m$ we define

$$q : \mathbb{Z}^n \times \mathbb{Z} \rightarrow V = \mathbb{R}^3$$

by

$$q(y, z) = (\|y\|^2, z^2, \|f(y) - z \cdot a\|^2).$$

Then (\mathbb{Z}^{n+1}, q, V) is a layered lattice.

- ▷ The first layer, L_1 equals the kernel of f .
- ▷ We have $L_1 \subseteq L_2$ and the elements of L_2 parametrize solutions of $f(y) = z \cdot a$. Note that the rank of L_2/L_1 is at most 1.
- ▷ If L_2/L_1 has rank 0 then $b \neq 0$ and there is no *rational* solution.

Our example revisited

Let $f : \mathbb{Z}^n \rightarrow \mathbb{Z}^m$ be a morphism of groups and $a \in \mathbb{Z}^m$ we define

$$q : \mathbb{Z}^n \times \mathbb{Z} \rightarrow V = \mathbb{R}^3$$

by

$$q(y, z) = (\|y\|^2, z^2, \|f(y) - z \cdot a\|^2).$$

Then (\mathbb{Z}^{n+1}, q, V) is a layered lattice.

- ▷ The first layer, L_1 equals the kernel of f .
- ▷ We have $L_1 \subseteq L_2$ and the elements of L_2 parametrize solutions of $f(y) = z \cdot a$. Note that the rank of L_2/L_1 is at most 1.
- ▷ If L_2/L_1 has rank 0 then $b \neq 0$ and there is no *rational* solution.
- ▷ If the rank of L_2/L_1 equals 1 then a basis for it will give us the minimal z for which there is a solution $f(y) = z \cdot a$.

If $q(y, z) < (0, 2, 0)$ we have $f(y) = a$.

Mimicking LLL

- ▷ We want to have a concept of reduced basis which, in particular, generate the layers of L (*layered basis*).
- ▷ Secondly, this basis should induce a reduced basis (in the usual sense) on the quotients L_k/L_{k-1} .

It turns out that the definition of a reduced basis generalize readily to layered lattices (provided we have a Gram-Schmidt procedure). And a reduced basis in this sense has the two properties listed above. Furthermore, the *steps* of the LLL algorithm also generalize.

Layered Euclidean spaces

We now move to the geometry of layered lattices.

Definition

A layered Euclidean space is a pair $(E, V, \langle \cdot, \cdot \rangle)$ where E is a finite dimensional real vector space, and

$$\langle \cdot, \cdot \rangle : E \times E \rightarrow V$$

is a bilinear symmetric map satisfying the following properties.

- ▶ $\forall x \neq 0, \langle x, x \rangle > 0$
- ▶ $\forall x, y, \exists \lambda \in \mathbb{R}$ such that $\langle x, y \rangle \leq \lambda \langle y, y \rangle$

The layers of E are the subspaces $E_k = \{x \in E : \langle x, x \rangle \in V_k\}$.

Embedding theorem

It is easy to see that for $k = 1, \dots, n$ the quotients

$$(E_k/E_{k-1}, V_k/V_{k-1}, \langle \cdot, \cdot \rangle)$$

are Euclidean spaces and one can prove a generalization of the *embedding theorem*.

Theorem

Let (L, V, q) be a layered lattice. Then $(\mathbb{R} \otimes L, V, \langle \cdot, \cdot \rangle)$ where

$$\langle x, y \rangle = \frac{1}{4}(q(x+y) - q(x-y))$$

is a layered Euclidean space. Furthermore, the layers are compatible, i.e., for all $k \in \{1, \dots, n\}$, $L_k/L_{k-1} \subset E_k/E_{k-1}$ is a lattice embedded in an Euclidean space. Reciprocally, any “layered basis” of E generates, as a group, a layered lattice.

The Gram-Schmidt process

Definition

Let E be a layered Euclidean space and $x, y \in E$. We say x is orthogonal to y and write $x \perp y$ if

$$\langle x, y \rangle \ll \langle y, y \rangle$$

where \ll is the relation

$$u \ll v \iff \forall \lambda \in \mathbb{R}, \lambda u < v.$$

Given a set $S \subset E$ the orthogonal complement is the set

$$S^\perp = \{x \in E : \forall y \in S, x \perp y\}.$$

Remark: Orthogonality is *not* a symmetrical relation in this generalized setting.

The Gram-Schmidt process

Nonetheless, one can verify that the orthogonal complement enjoys some good properties.

Theorem

Let $S \subset E$ be a subspace of a layered Euclidean space. Then S^\perp is a subspace and we have a direct sum decomposition $E = S \oplus S^\perp$.

Sketch of the proof

That S^\perp is a subspace follows directly from the definition (and here S could be an arbitrary subset). It is also easy to see that $S \cap S^\perp = \{0\}$.

Let $S_k = S \cap E_k$ for $k = 1, \dots, n$. We look at the linear map

$$\phi : E \rightarrow \bigoplus_k \text{Hom}(S_k/S_{k-1}, V_k/V_{k-1})$$

$$y \mapsto (x_k + S_{k-1} \mapsto \langle x_k, y \rangle + V_{k-1})_k$$

The Gram-Schmidt process

The crucial observation is that $\ker \phi = S^\perp$:

$$\begin{aligned} y \in S^\perp &\iff \forall x \in S, \langle x, y \rangle = 0 \\ &\iff \forall k, \forall x \in S_k : \langle x, y \rangle \equiv 0 \pmod{V_{k-1}} \iff y \in \ker \phi. \end{aligned}$$

With this the result follows. We have that

$$\ker \phi|_S = \ker \phi \cap S = S^\perp \cap S = \{0\}$$

so $\phi|_S$ is injective. The dimension of the codomain equals the dimension of S hence $\phi|_S$ is an isomorphism.

Finally, we have

$$\dim S^\perp = \dim \ker \phi = \dim E - \dim S$$

thus $E = S \oplus S^\perp$. □

The Gram-Schmidt process

Let $\{b_1, \dots, b_m\}$ be a basis of E and for each $i = 1, \dots, m$ let

$$B_i = \text{span} \{b_1, \dots, b_{i-1}\}.$$

The Gram-Schmidt basis associated to the basis above is the unique basis $\{b_1^*, \dots, b_m^*\}$ given by the decompositions

$$b_i = (b_i - b_i^*) + b_i^* \in B_i \oplus B_i^\perp, \quad i = 1, \dots, m.$$

- ▷ As before we have $b_1^* = b_1$ and $\text{span} \{b_1^*, \dots, b_{i-1}^*\} = B_i$.
- ▷ The G.-S. basis associated to a basis induces orthogonal bases in each layer, i.e., in E_i/E_{i-1} .
- ▷ It is still easy to calculate the $\mu_{i,j}$, i.e., the constants such that

$$b_i = b_i^* + \sum_{j < i} \mu_{i,j} b_j^*.$$

The LLL algorithm

A basis of a layered lattice is called *reduced* if:

- a) It is size reduced, i.e., $\forall i, \forall j < i, |\mu_{i,j}| \leq 1/2$.
- b) For all $i < n$ we have $q(b_i^*) < 2 \cdot q(b_{i+1}^*)$.

The algorithm proceeds as usual. It obtains a reduced basis by picking the smallest i for which a) or b) is violated and correcting it by either performing a swap of the b_i, b_{i+1} (in case b)) or subtracting from b_i an integer multiple of b_j (in a)).

But will it finish? In polynomial time?

LLL terminates

Classical case:

- ▷ Show that the partial discriminants, i.e.,

$$\prod_{i=1}^m \prod_{j < i} q(b_j^*) = \prod_{i=1}^m D(L_i), \quad L_i = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_i$$

is bounded below and is divided by at least a constant factor with each swap.

- ▷ Since the number of size-reductions between a swap is also bounded this shows that LLL terminates.

LLL terminates

In our case:

▷ We have two quantities:

$$\prod_{j=1}^i q(b_j^*) \sim D(L_i) \in S^i(V), \quad D(L_i) = \det(\langle b_j, b_h \rangle)_{j,h \leq i}.$$

▷ Fortunately this weaker relation is enough for our purpose:

$$\prod_{i=1}^m \prod_{j < i} q(b_j^*) \sim \prod_{i=1}^m D(L_i) \in S^{\binom{m}{2}}(V).$$

Recall: $S^k(V) = V^{\otimes k} / \{ \text{“commuting relations”} \}$. Algorithmically, this is the degree- k part of a polynomial algebra on the $e_1, \dots, e_n \in V$.

Main theorem

The following result establishes that our algorithm terminates.

Theorem

Let L be a layered lattice of rank m . Then the set

$$\left\{ \prod_{i=1}^m D(L_i) : \{b_1, \dots, b_m\} \text{ a basis of } L \right\} \subset S^{\binom{m}{2}}(V)$$

is well-ordered.

Main theorem

The following result establishes that our algorithm terminates.

Theorem

Let L be a layered lattice of rank m . Then the set

$$\left\{ \prod_{i=1}^m D(L_i) : \{b_1, \dots, b_m\} \text{ a basis of } L \right\} \subset S^{\binom{m}{2}}(V)$$

is well-ordered.

This theorem is an easy consequence of a harder result:

Proposition

For any $k \in \mathbb{Z}_{\geq 0}$ and E a layered Euclidean space, the space $(\bigwedge^k E, S^k(V))$ is a layered Euclidean space with inner-product given on generators by

$$\langle x_{i_1} \wedge \cdots \wedge x_{i_k}, y_{i_1} \wedge \cdots \wedge y_{i_k} \rangle = \det(\langle x_{i_p}, y_{i_q} \rangle)_{pq}.$$

Sketch of the proof of the main theorem

- ▷ Let L a layered lattice of rank m and K a sublattice of rank i . Let b_1, \dots, b_i be a basis of K . We have

$$\langle b_1 \wedge \dots \wedge b_i, b_1 \wedge \dots \wedge b_i \rangle = D(K).$$

- ▷ Since a layered basis of E induces canonically a layered basis of $(\bigwedge^k E, S^k(V))$, from the proposition, the pair $(\bigwedge^i L, S^i(V), q)$ is a layered lattice.
- ▷ Vectors in this lattice are canonically identified with rank i sublattices of L . It follows that $\{D(K) : K \text{ a rank } i \text{ sublattice of } L\} \subset S^i(V)$ is well-ordered (from our definition).
- ▷ The invariant we use is an m -fold product of discriminants and, hence, well-ordered as well.

To do:

Right now:

- ▷ Estimating the running-time of the algorithm.
- ▷ Implement.
- ▷ Study more applications.

Tentative future:

- ▷ Apply this theory to the problem of compactification of moduli spaces of lattices.

For a very good account on lattices and lattice basis reduction:

- ▷ Lenstra, H.W. Jr., *Lattices*. Surveys in algorithmic number theory. MSRI Publications, vol. 44, Cambridge University Press, 2008.