Short Bases of Lattices over Number Fields

Claus Fieker Damien Stehlé

University of Sydney/ Magma

LIP – CNRS/ENSL/U. Lyon/INRIA/UCBL

ANTS-IX, July 2010

Introduction

Let K be a number field (possibly $\mathbb{Q}$). Then we have a canonical ring associated to K namely $\mathbb{Z}_K$, the ring of integers of K. (for $\mathbb{Q}$ we obtain $\mathbb{Z}$).

A lattice M over K is a torsion free, discrete and finitely generated $\mathbb{Z}_K$ module that comes equiped with some quadratic form.

Lattices arise naturally in a large number of problems originating in different areas of mathematics, from cryptography, geometry to representation theory to name a few.

A common theme in most applications is to find a representation for the lattice that is "small".

For lattices over $\mathbb{Z}$, the solution usually is to apply the LLL-algorithm to find a "short" basis for M.

For our more general lattices, despite a few partial results, no corresponding reduction theory is known.

Classical Lattices

Since $\mathbb{Z}$ is PID, all $\mathbb{Z}$-lattices have a basis. Via any fixed basis the quadratic form can be represented as a positive definite matrix.
The LLL algorithm will find, in time polynomial in the input, a new basis for the lattice that is "short" and "nearly orthogonal". In particular the new basis approximates the lattice minima.
A key idea underlying the algorithm is to try to approximate an orthogonal basis for the vector space generated by the lattice M.
Crucial to the proof is the fact that any real or rational number can be approximated by an integer with an error bounded by $|1/2|$.

Modules over the Ring of Integers

Let now K be a number field. Since in general $\mathbb{Z}_K$ is not a PID any more, the lattice is no longer free (it still is projective). To overcome this problem two possibilities are used:

- use $n+1$ (or more) generators
- use of pseudo-bases with coefficient ideals

We use the second way as this preserves some of the most important properties of the basis:

- Cardinality of pseudo basis is degree of the vector space
- A pseudo basis contains a basis for the vector space
- Elements have a unique representation wrt it.

Over $\mathbb{Z}$ we have $M = \sum \mathbb{Z} b_i$ where the b_i form a basis, here all we get is

$$M = \sum \mathfrak{a}_i \alpha_i$$

where the $\mathfrak{a}_i$ are ideals in K and the α_i a basis for the vector space.

Relative HNF

We have

$$M = \sum \mathfrak{a}_i \alpha_i$$

where the $\mathfrak{a}_i$ are ideals in K and the α_i a basis for the vector space. For the rest of the talk we are going to restrict to *integral* lattices, ie $M \subseteq \mathbb{Z}_K^n$ for some n. For simplicity we are also assuming that $n = \dim_K M \otimes K =$ length of any pseudo basis.
In analogy to the Hermite form over $\mathbb{Z}$, we have a similar upper or lower triangular echelon form for modules, algorithms have been developed by Bosma-Pohst and Cohen. Those algorithms can be used to compute a (canonical) pseudo-basis from any generating set of (pseudo) elements.

The Result

Theorem

There exists a polynomial algorithm that, given a module M via some pseudo basis, will find a "short" pseudo basis

$$M = \sum \mathfrak{b}_i \beta_i$$

where

- $1 \in \mathfrak{b}_i$ *(or, alternatively, $\beta_i \in M$)*
- $N(\mathfrak{b}_i) \in [2^{-d^2}, 1]$
- $\|\beta_i\| \leq 2^{O(dn)} \lambda_i(M)$

Where the $O()$ depends on K (a fixed (reduced) integral basis), $K : \mathbb{Q} = d$, $\|.\|$ is a norm induced by the quadratic form on M and the λ_i are the lattice minima.

Overview of Idea

Algorithm

- *Let M be a $\mathbb{Z}$-lattice (given via some $\mathbb{Z}$-basis)*
- *Let c_1, ..., c_n be independent elements*
- *Compute $T \in \mathit{Mat}(n, \mathbb{Z})$ such that* $(c_1, \ldots, c_n) = (b_1, \ldots, b_n)T$
- *Compute $H = ST$ where H is in Hermite form*
- *Set* $(\tilde{b}_1, \ldots, \tilde{b}_n) =: (b_1, \ldots, b_n)S^{-1}$
- *Perform a size reduction on* $(\tilde{b}_1, \ldots, \tilde{b}_n)$

Since S is unimodular, $\tilde{b}_i$ still forms a basis. Since the transformation to c_i is in HNF (triangular), the new vectors cannot be too much longer than the c_i.

Change of Basis

To adopt this technique, we have to account for the presence of the coefficient ideals in the pseudo-basis. The key tool is the following:

Theorem

Let $M = \sum \mathfrak{a}_i \alpha_i$ *and* $N = \sum \mathfrak{b}_i \beta_i$. *Assume* $(\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n)T$ *for some* $T \in \mathit{Gl}(n, K)$. *Then*

- $N \subseteq M$ *iff* $T_{i,j} \in \mathfrak{b}_i \mathfrak{a}_j^{-1}$
- $M \subseteq N$ *iff* $(T^{-1})_{i,j} \in \mathfrak{a}_i \mathfrak{b}_j^{-1}$
- $N = M$ *iff* $N \subseteq M$ *and* $\prod \mathfrak{a}_i = \det T \prod \mathfrak{b}_i$

Adapted Basis

The application of the previous theorem is mostly immediate:
Assume $M = \sum \mathfrak{a}_i \alpha_i$ and that c_1, …, c_n is a maximal independent system of (short) elements. Then we have $(c_1, \dots, c_n) = (\alpha_1, \dots, \alpha_n)T$.
We form the module $\Gamma = \sum \mathfrak{a}_i^{-1} T_i$ where T_i are the columns of T.
The Hermite form algorithm applied to Γ finds

- A pseudo basis $\Gamma = \sum \mathfrak{b}_i H_i$ where H is triangular (and in HNF)
- A transformation S (automorphism of Γ) mapping $(H_1, \dots, H_n) = (T_1, \dots, T_n)S$, thus $S_{i,j} \in \mathfrak{b}_i^{-1}\mathfrak{a}_j$

Set $(\beta_1, \dots, \beta_n) := (\alpha_1, \dots, \alpha_n)S^{-1}$, then $M = \sum \mathfrak{b}_i^{-1}\beta_i$ and the transformation to the "short" elements c_i is triangular.

Size Reduction

The size-reduction is immediate: We compute a orthogonal basis from the pseudo-basis and try to approximate the coefficients.

Algorithm

```
Let $\Gamma = \sum \mathfrak{a}_i \alpha_i$ a module with pseudo basis and
$B : \Gamma \otimes K \times \Gamma \otimes K \to K$ a (hermitian) scalar product.
For $i$ in $2, \ldots, n$ do
    For $j$ in $i-1, \ldots, 1$ compute
        $\mu := B(\alpha_j, \alpha_i)/B(\alpha_j, \alpha_j)$
        Find $x \in \mathfrak{a}_j \mathfrak{a}_i^{-1}$ approximating $\mu$
        Set $\alpha_i := \alpha_i - x\alpha_j$
```

The size reduction now will not change the triangular shape of the transformation, but will potentially make the elements shorter - and is important for the analysis as this will bound the distance to the orthogonal basis.

To obtain the bounds on the norm of the coefficient ideals, we note that this is essentially the statement of the finiteness of the class number. Given any ideal $\mathfrak{a}$, we find a short element α in $\mathfrak{a}^{-1}$, thus $\mathfrak{a}\alpha$ is of bounded norm. If α is a LLL-short element we obtain the bounds stated.

In order to find a short representation of those ideals we are applying a special form of 2-element presentation.

Finding Short Vectors

To find the initial short vectors we construct the corresponding $\mathbb{Z}$-lattice Γ via any fixed $\mathbb{Z}$-bases for the coefficient ideals. In Γ we compute a short basis using the usual lattice techniques (repeated LLL with increasing reduction parameters, Seysen reduction in not too large dimension).

From the short $\mathbb{Z}$-basis we then select K-independent elements aiming to obtain short elements that generate a submodule of small index.

Small Ideals

Theorem

There exists a probabilistic polynomial time algorithm that, given an ideal $\mathfrak{a} = \sum \mathbb{Z}\alpha_i$ *and a probability* $t \in]0,1]$ *finds* x_1, $x_2 \in \mathfrak{a}$ *such that*

- $\mathfrak{a} = x_1\mathbb{Z}_K + x_2\mathbb{Z}_K$ *with probability* $1 - t$
- $\|x_1\|, \|x_2\| \leq C_K N(\mathfrak{a})^{4/d}$

The constant C_K *depends on* K, *the choice of an integral basis and the* $\mathbb{Z}$*-reduction algorithm used.*

Thus the ideal can be represented in $O(\log(N(\mathfrak{a})))$ bits - in contrast to the $O(d \log N(\mathfrak{a}))$ bits coming from the naive approach.

Example

Let $G := \langle \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \rangle$ be the group Q_8 with 8 elements. It is well known that G can be realized over any field where $-1 = \square + \square$, equivalently, over any normal complex field where the 2-adic completions have even degree. In particular, any imaginary quadratic field where the 2 is inert or ramified works. Using some Galois cohomology, Magma computes over $\mathbb{Q}(s) := \mathbb{Q}(\sqrt{-101})$:

$$\langle \frac{1}{9334017} \begin{pmatrix} 3196257s - 20190 & s - 30704 \\ -5205600s - 30767884740 & -3196257s + 20190 \end{pmatrix}, \\ \frac{1}{9334017} \begin{pmatrix} 924360s + 3196257 & 304s + 1 \\ 358973136s - 19438628994 & -924360s - 3196257 \end{pmatrix} \rangle$$

which is horrible.

Example

To find a better version we want to apply the lattice reduction. We need to find a module M and a quadratic (hermitian) form. We use

$$M := \langle g\mathbb{Z}_K^2 \mid g \in G \rangle$$

Similarly, we obtain a quadratic form:

$$H := \sum_{g \in G} g^* g = t \begin{pmatrix} 1 & \frac{1}{101}(-10514s - 101) \\ \frac{1}{101}(10514s - 101) & 1186914 \end{pmatrix}$$

for some $t \in \mathbb{Q}_{>0}$.

Our choices define a $\mathbb{Z}$-lattice with Gram-matrix:

$$\begin{pmatrix} 1 & 0 & 3196256 & 3185742 \\ 0 & 101 & 10514 & 10514 \\ 3196256 & 10514 & 10216053604449 & 10182448168561 \\ 3185742 & 10514 & 10182448168561 & 10148953276870 \end{pmatrix}$$

which LLL reduces to the identity matrix.

Example

Using the 1st two LLL basis vectors in M

$$\begin{pmatrix}1\\0\end{pmatrix}, \frac{1}{9334017}\begin{pmatrix}3196257s-20190\\s-30704\end{pmatrix}$$

Of length 2 and 202. The original "basis" vectors had length 2 and 20432107208898. Representing the group wrt the new basis we get

$$\left\langle \begin{pmatrix}10 & 1\\-101 & -10\end{pmatrix}, \begin{pmatrix}0 & -\frac{s}{101}\\-s & 0\end{pmatrix} \right\rangle$$

which is much better.

Concluding remarks

- Implemented in MAGMA (in the packages).
- The article contains group theoretic examples.
- Relationship to crypto: Ideal-SIS, Ring-LWE and NTRU lattices.

Open questions:

- Optimizing the bit-complexity.
- The structuredness is exploited to compactify the representation, but not to speed up computations.
- Can we exploit the new module representation to speed up enumeration of short module vectors?

Concluding remarks

- Implemented in MAGMA (in the packages).
- The article contains group theoretic examples.
- Relationship to crypto: Ideal-SIS, Ring-LWE and NTRU lattices.

Open questions:

- Optimizing the bit-complexity.
- The structuredness is exploited to compactify the representation, but not to speed up computations.
- Can we exploit the new module representation to speed up enumeration of short module vectors?