JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

HUGUETTE NAPIAS

A generalization of the LLL-algorithm over euclidean rings or orders

Journal de Théorie des Nombres de Bordeaux, tome 8, nº 2 (1996), p. 387-396

<http://www.numdam.org/item?id=JTNB_1996__8_2_387_0>

Journal de Théorie des Nombres
de Bordeaux 8 *(1996), 387–396*

A generalization of the LLL-algorithm over euclidean rings or orders

par Huguette NAPIAS

Résumé. De nombreux réseaux célèbres ($\mathbb{D}_4$, $\mathbb{E}_8$, le réseau K_{12} de Coxeter-Todd, le réseau Λ_{16} de Barnes-Wall, le réseau Λ_{24} de Leech, les réseaux 2-modulaires de dimension 32 de Quebbemann et de Bachoc, ...) sont munis de structures algébriques sur divers anneaux euclidiens, entiers d'Eisenstein ou quaternions de Hurwitz, par exemple. Les procédés usuels de réduction, et en particulier l'algorithme LLL, deviennent plus performants lorsqu'on les adapte à ces structures,

Abstract. Numerous important lattices ($\mathbb{D}_4$, $\mathbb{E}_8$, the Coxeter-Todd lattice K_{12}, the Barnes-Wall lattice Λ_{16}, the Leech lattice Λ_{24}, as well as the 2-modular 32-dimensional lattices found by Quebbemann and Bachoc) possess algebraic structures over various Euclidean rings, e.g. Eisenstein integers or Hurwitz quaternions. One obtains efficient algorithms by performing within this frame the usual reduction procedures, including the well known LLL-algorithm.

1. Introduction.

The LLL-algorithm for basis reduction, one of the most important and useful algorithm in the geometry of numbers, due to Lenstra, Lenstra, Lovász [9] can be generalized to Euclidean rings or orders. Many lattices built with codes over rings or orders have an algebraic and additive structure. We present here a new version of the LLL-algorithm which reduces a basis (or a system of generator vectors) while preserving the algebraic structure of the lattice.

We can apply it to the ring of the integers of the five quadratic imaginary fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, the Hurwitz order $\mathfrak{M}$ and a maximal order of the quaternion algebra ramified at 3 and ∞. The lattices can be given via a basis or a set of generators (in the case of a set of generators, this reduction avoids using the Hermite Normal Form algorithm).

Manuscrit reçu le 26 mars 1996

2. The LLL-algorithm over a Euclidean ring (or order).

First, we fix some notation. We denote by A a Euclidean ring contained in a field $\mathbb{K}$: CM number field or quaternion field over a number field, which can be identified to a vector space $\mathbb{R}^m$, endowed with an involution $\sigma : x \mapsto \bar{x}$. We equip $\mathbb{K}^n$ with the Hermitian product $x.y = \sum_{p=1}^{n} x_p\, \bar{y}_p$. We assume that the Norm map $N\ :\ x \mapsto\mid x \mid = x\sigma(x)$ sends $\mathbb{K}$ in $\mathbb{R}$ and A in $\mathbb{Z}$.

Here, we are interested in the case where the field $\mathbb{K}$ is commutative (when $\mathbb{K}$ is a skewfield, the notion of a determinant has no sense, but we can substitute for it the reduced norm).

Definition.

The basis $b_1, b_2, \ldots, b_n$ of a lattice Λ is called A-LLL-reduced if

a) $\mid \mu_{r,s} \mid \leq C_1 \quad$ *for* $\quad 1 \leq s < r \leq n,$

b) $\| \, b_r^* + \mu_{r,r-1} b_{r-1}^* \, \|^2 \geq C_2 \, \| \, b_{r-1}^* \, \|^2 \quad$ *for* $\quad 2 \leq r \leq n,$

where the vectors b_r^* $(1 \leq r \leq n)$ and the elements of $\mathbb{K}$, $\mu_{r,s}$ $(1 \leq s < r \leq n)$ are inductively defined in the Gram-Schmidt orthogonalization process [9], and the two reals C_1 and C_2 are such that $0 < C_1 < C_2 < 1$.

Remarks: The constant C_2 depends on C_1, it can be replaced by any value strictly bigger than C_1 but it must be strictly smaller than 1 to make sure that the algorithm terminates. The constant C_1 is equal to $\sup\{\inf\{N(y-x) \mid x \in \mathrm{A}\} \mid y \in \mathbb{K}\}$ and depends on the field $\mathbb{K}$ [8].

In the following, the Hermitian norm $b_r^*.b_r^*$ will be denoted by B_r $(1 \leq r \leq n)$.

PROPERTIES.

Let $b_1, b_2, \ldots, b_n$ be an A-LLL-reduced basis of a lattice Λ. Then,

i) $\det(\Lambda) \leq \prod_{1 \leq p \leq n} \| \, b_p \, \|^2 \leq (C_2 - C_1)^{\frac{-n(n-1)}{2}} \det(\Lambda).$

ii) $\| \, b_s \, \|^2 \leq (C_2 - C_1)^{1-r} B_r \quad$ *for* $\quad 1 \leq s \leq r \leq n.$

iii) $\| \, b_1 \, \|^2 \leq (C_2 - C_1)^{\frac{1-n}{2}} \det(\Lambda)^{\frac{1}{n}}.$

iv) For all $x \in \Lambda, x \neq 0$, we have $\| b_1 \|^2 \leq (C_2 - C_1)^{1-n} \| x \|^2$.

v) More generally, for a system of linearly independent vectors $x_1, x_2, \ldots, x_t$ of Λ,
we have $\| b_r \|^2 \leq (C_2 - C_1)^{1-n} \max(\| x_1 \|^2, \| x_2 \|^2, \ldots, \| x_t \|^2)$ for $1 \leq r \leq t$.

For the proof of these properties, see [12].

Remark: Most of the time, the lattices we considered have "integer" entries ("integer" means elements of A). So, we generalize the version of the LLL-algorithm [5] which runs with elements of $\mathbb{Z}$. We have the following proposition:

PROPOSITION.

We set $d_p = \prod_{1 \leq s \leq p} B_s$ for $1 \leq p \leq n$ and $d_0 = 1$. Let be $\lambda_{r,s} = \mu_{r,s} d_s$ for $s < r$ and

$\lambda_{r,r} = d_r$. For $s \leq r$ fixed, we define the sequence u_p by $u_0 = b_r . b_s$ and for all p such that $1 \leq p < s$,

$$u_p = \frac{d_p u_{p-1} - \lambda_{r,p} \bar{\lambda}_{s,p}}{d_{p-1}}.$$

Then $\lambda_{r,s}$ and $u_p \in A$ and $u_{s-1} = \lambda_{r,s}$.

For the proof of this proposition, see [12].

Remarks: In the case where the field $\mathbb{K}$ is commutative, the elements d_p are also equal to $\det(b_r . b_s)_{1 \leq r,s \leq p}$.

The sequence $(u_p)_{1 \leq p \leq n}$ is defined in such a way that it can be used when $\mathbb{K}$ is a skewfield.

At the beginning of the algorithm, we compute the u_p $(1 \leq p \leq n)$ instead of using the Gram-Schmidt orthogonalization process.

So, we have for a basis two new conditions of A-LLL-reduction equivalent to the previous ones:

$a')\quad \mid \lambda_{r,s} \mid \leq C_1 d_s^2 \quad$ for $\quad 1 \leq s < r$,

$b')\quad d_r d_{r-2} + \mid \lambda_{r,r-1} \mid \geq C_2 d_{r-1}^2 \quad$ for $\quad 2 \leq r \leq n$.

When the lattice Λ is given via a set of generators, the Hermitian norms of some vectors b_s^* are equal to zero. The definition of d_p is replaced by $d_p = \prod\limits_{\substack{1 \leq s \leq p \\ B_s \neq 0}} B_s$.

In this case, we no more have the equivalence between the conditions $b)$ and $b')$. So, we implemented the algorithm using the first two previous conditions of A-LLL-reduction and the Gram-Schmidt orthogonalization process.

We give the two algorithms, the first for a basis, and the second one for an arbitrary set of generators.

First algorithm:

Input: A basis b_p $(1 \leq p \leq n)$ of a lattice Λ.

Output: An A-LLL-reduced basis.

Init: Set $r := 2$, $r_{max} := 1$, $d_0 := 1$, $d_1 := b_1.b_1$.

Computing $\mathbf{u_p}$: If $r \leq r_{max}$, goto **Finished?**.

Otherwise: set $r_{max} := r$, for $s = 1, \ldots, r$ set $u := b_s.b_r$, for $t = 1, \ldots, s-1$ set $u := \frac{d_t u - \lambda_{r,t} \bar{\lambda}_{s,t}}{d_{t-1}}$, if $s < r$ set $\lambda_{r,s} := u$, if $s = r$ set $d_r := u$.

Reduction: Execute $\mathbf{REDI(r, r-1)}$.

A-LLL-condition: If $d_r d_{r-2} + \mid \lambda_{r,r-1} \mid < C_2 d_{r-1}^2$: execute **SWAPI** $(\mathbf{r})$, set $r := \max(2, r-1)$ and goto **Reduction**.

Otherwise: for $s = r-2, \ldots, 1$ execute $\mathbf{REDI(r, s)}$ and set $r := r + 1$.

Finished? If $r \leq n$ goto **Computing $\mathbf{u_p}$** else terminate.

$\mathbf{REDI(r, s)}$: Set $q := \lfloor \frac{\lambda_{r,s}}{d_s} \rceil$, $b_r := b_r - q b_s$, $\lambda_{r,s} := \lambda_{r,s} - q d_s$, for $t = 1, \ldots, s-1$ set $\lambda_{r,t} := \lambda_{r,t} - q \lambda_{s,t}$ and return.

$\mathbf{SWAPI(r)}$: Interchange b_r and b_{r-1} and if $r > 2$ for $s = 1, \ldots r-2$ interchange $\lambda_{r,s}$ and $\lambda_{r-1,s}$, set $\lambda := \lambda_{r,r-1}$, $\lambda_{r,r-1} := \bar{\lambda}_{r,r-1}$, for $s =$

$r+1,\dots,r_{max}$ set $\lambda_1 := \lambda_{s,r}$, $\lambda_2 := \lambda_{s,r-1}$, $\lambda_{s,r} := \frac{\lambda_2 d_r - \lambda_1 \lambda}{d_{r-1}}$, $\lambda_{s,r-1} := \frac{\lambda_1 d_{r-2} + \bar{\lambda}\lambda_2}{d_{r-1}}$, $d_{r-1} := \frac{d_{r-2} d_r + |\lambda|}{d_{r-1}}$ and return.

For $\alpha \in \mathbb{K}$, the symbol $\lfloor \alpha \rceil$ means the nearest element of A (in the sense of the norm) to α.

Second algorithm:

Input: A set of generators b_p $(1 \le p \le n)$ of a lattice Λ.

Output: An A-LLL-reduced basis.

Init: Set $r := 2$, $r_{max} := 1$, $b_1^* := b_1$, $B_1 := b_1.b_1$.

Gram-Schmidt: If $r \le r_{max}$ goto **Finished?**.

Otherwise: set $r_{max} := r$, for $s = 1,\dots,r-1$ set $a_{r,s} := b_r.b_s - \sum_{t=1}^{s-1} a_{r,t}\bar{\mu}_{s,t}$ and $\mu_{r,s} := \frac{a_{r,s}}{B_s}$, and set $B_r := b_r.b_r - \sum_{s=1}^{r-1} a_{r,s}\bar{\mu}_{r,s}$.

Reduction: Execute $\mathbf{RED(r, r-1)}$.

A-LLL-condition: If $B_r < (C_2 - \mid \mu_{r,r-1} \mid) B_{r-1}$: execute $\mathbf{SWAP(r)}$, set $r := \max(2, r-1)$ and goto **Reduction**.

Otherwise: for $s = r-2,\dots,1$ execute $\mathbf{RED(r, s)}$ and set $r := r+1$.

Finished? If $r \le n$ goto **Gram-Schmidt** else terminate.

$\mathbf{RED(r, s)}$: set $q := \lfloor \mu_{r,s} \rceil$, $b_r := b_r - q b_s$, $\mu_{r,s} := \mu_{r,s} - q$, for $t = 1,\dots,s-1$ set $\mu_{r,t} := \mu_{r,t} - q\mu_{s,t}$ and return.

$\mathbf{SWAP(r)}$: Interchange b_r and b_{r-1} and if $r > 2$ for $s = 1,\dots,r-2$ interchange $\mu_{r,s}$ and $\mu_{r-1,s}$, set $\mu := \mu_{r,r-1}$, $B := B_r + \mid \mu \mid B_{r-1}$,

if $B = 0$ (i.e. $B_r = \mid \mu \mid = 0$), for $s = r+1,\dots,r_{max}$ interchange $\mu_{s,r}$ and $\mu_{s,r-1}$, b_r^* and b_{r-1}^*, B_r and B_{r-1}.

if $B_r = 0$ and $\mid \mu \mid \neq 0$, set $B_{r-1} := B$, $b_{r-1}^* := \mu b_{r-1}^*$, $\mu_{r,r-1} := \frac{\bar{\mu}}{|\mu|}$, for $s = r+1,\dots,r_{max}$ set $\mu_{s,r-1} := \frac{\mu_{s,r-1}\bar{\mu}}{|\mu|}$,

if $B_r \neq 0$ and $\mid \mu \mid \neq 0$, set $\mu_{r,r-1} := \frac{\bar{\mu} B_{r-1}}{B}$, $b := b_{r-1}^*$, $b_{r-1}^* := b_r^* + \mu b$, $b_r^* := -\mu_{r,r-1} b_r^* + \frac{B_r}{B} b$, $B_r := \frac{B_{r-1} B_r}{B}$, $B_{r-1} := B$, for $s = r+1,\dots,r_{max}$ set $\nu := \mu_{s,r}$, $\mu_{s,r} := \mu_{s,r-1} - \nu\mu$, $\mu_{s,r-1} := \nu + \mu_{s,r}\mu_{r,r-1}$ and return.

The running time of these two algorithms is the same as the ordinary LLL-algorithm over $\mathbb{Z}$ or $\mathbb{R}$. For the proof of the validity of these algorithms, see [5] and [12].

Remarks: Both algorithms were implemented on a SPARC 20. To save time, we worked with real numbers. However, rounding errors may occur which can generate some instabilities.

3. Applications.

3.1. Application to the ring of Gaussian integers, the ring of Eisenstein integers and the Hurwitz order.

We denote by $\mathbb{Z}[i]$ the ring of Gaussian integers ($i^2 = -1$), $\mathbb{Z}[j]$ the ring of Eisenstein integers ($j^2 + j + 1 = 0$) and $\mathfrak{M}$ the Hurwitz order $\mathbb{Z}[i, j, \frac{-1+i+j+k}{2}]$ (the unique maximal order of the quaternion algebra ramified at 2 and ∞, $\mathbb{Q}[i, j, k]$ with $i^2 = -1, j^2 = -1$ and $ij = -ji = k$, which contains $\mathbb{Z}[i, j, k]$).

Definition.

A basis b_p ($1 \leq p \leq n$) of a lattice Λ is called $\mathbb{Z}[i]$ (resp. $\mathbb{Z}[j]$, resp. $\mathfrak{M}$)-LLL-reduced when,

a) $C_1 = \frac{1}{2}$ (resp. $\frac{1}{3}$, resp. $\frac{1}{2}$),

b) $C_2 = \frac{3}{4}$ (resp. $\frac{2}{3}$, resp. $\frac{3}{4}$).

[C_1 is the usual constant which occurs in the Euclidean algorithm.]

Ch. Bachoc obtained three lattices denoted by $BC_{32}, BC_{40}, BC_{48}$ ([1], [2]) with codes over $\mathfrak{M}/2\mathfrak{M}$, in relative dimensions $8, 10, 12$. The bases are not composed of minimal vectors. We applied to them the following process: $\mathfrak{M}$-LLL-reduction and permutation of the vectors of the reduced basis to order in the increasing way the diagonal elements (which represent the Hermitian norms) until we obtain a basis of minimal vectors. After one iteration for BC_{32}, two for BC_{40} and three for BC_{48}, the previous process stops. We give the Hermitian diagonals before $\mathfrak{M}$-LLL-reduction and after each iteration. [Note that we cannot prove *a priori* that such a process will stop.]

	BC_{32}	BC_{40}
Before $\mathfrak{M}$ -LLL-reduction	$[3, 6, 4, 4, 4, 4, 4, 4]$	$[3, 3, 4, 4, 6, 5, 3, 4, 4, 4]$
After each iteration	$[3, 3, 3, 3, 3, 3, 3, 3]$	$[3, 3, 3, 3, 3, 3, 3, 3, 4, 4]$ $[3, 3, 3, 3, 3, 3, 3, 3, 3, 3]$

	BC_{48}
Before $\mathfrak{M}$ -LLL-reduction	$[5, 4, 4, 6, 4, 4, 4, 4, 4, 4, 4, 4]$
After each iteration	$[4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 6, 6]$ $[4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4]$

Using the scalar product $\langle x, y\rangle = \mathrm{Trd}(x.y)$, where $\mathrm{Trd}(x)$ is the reduced trace of x, we can build these lattices over $\mathbb{Z}$. The usual LLL-algorithm together with permutations of the bases vectors does not yield a basis of minimal vectors for BC_{40} nor for BC_{48}.

3.2. Two lattices of ranks 10 and 40 over $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

Definition.

A basis b_p $(1 \leq p \leq n)$ of a lattice Λ is called $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$-LLL-reduced when,

a) $C_1 = \frac{4}{7}$,

b) $C_2 = \frac{5}{7}$.

We consider two lattices which have a structure over $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ (the lattice of rank 10

found by G. Nebe and W. Plesken [13] and rediscovered by Ch. Bachoc [2], realizes the maximal Bergé-Martinet constant known in dimension 20, the second one is an extension

of the first). Replacing $\mathfrak{M}$ by $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ in the previous process, we obtain a basis of minimal vectors for the lattice of rank 10 (after 8 iterations), but not for the other (after 101 iterations, 34 minimal vectors appeared).

In the following table, we give the diagonal elements of the lattice of rank 10 before

$\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$-LLL-reduction and after each iteration.

Before $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ -LLL-reduction	$[5,5,5,5,5,9,9,9,9,9]$
After each iteration	$[4,4,4,4,4,4,4,5,5,5]$ $[4,4,4,4,4,4,4,4,5,5]$ $[4,4,4,4,4,4,4,5,5,5]$ $[4,4,4,4,4,4,4,4,4,5]$ $[4,4,4,4,4,4,4,4,5,5]$ $[4,4,4,4,4,4,4,4,4,5]$ $[4,4,4,4,4,4,4,5,5,5]$ $[4,4,4,4,4,4,4,4,4,4]$

For the lattice of rank 40, we give the diagonal elements before $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$-LLL-reduction

$[5^{20}, 9^{20}]$ (i.e. the 20 first elements have a Hermitian norm equal to 5 and the 20 others a Hermitian norm equal to 9) and after the 101st iteration $[4^{34}, 5^3, 6^3]$. Considering a matrix of the lattice of rank 10 with minimal vectors, we can build a matrix of the lattice of rank

40 which has minimal vectors, but not $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$-LLL-reduced (the previous process brings some no shortest vectors).

3.3. A lattice of rank 20 over $\mathfrak{M}_3$.

In the quaternion field ramified at 3 and ∞, $\mathbb{Q}[i,j,k]$, with $i^2 = -1, j^2 = -3$ and $ij = -ji = k$, we denote by $\mathfrak{M}_3$ a maximal order $\mathbb{Z}[i, \omega, \omega']$ with $\omega = \frac{-1+i}{2}$ and $\omega' = i\omega$, which contains $\mathbb{Z}[i,j,k]$.

Definition.

A basis b_p $(1 \leq p \leq n)$ of a lattice Λ is called $\mathfrak{M}_3$-LLL-reduced when, *a)* $C_1 = \frac{2}{3}$,

b) $C_2 = \frac{3}{4}$.

G. Nebe builds a unimodular lattice of rank 20 which has an algebraic structure over $\mathfrak{M}_3$, generated by 40 vectors and stable by $\mathrm{SL}_2(41)$ (private communications). Using the second algorithm, we obtain a $\mathfrak{M}_3$-LLL-reduced basis. With the previous process, we find a vector of Hermitian norm 12. Considering the scalar product $\langle x, y\rangle = \frac{1}{3}\operatorname{Trd}(x.y)$ we build a lattice over $\mathbb{Z}$, with a vector of norm 8. But we cannot prove that this lattice is extremal in the sense of the theory of modular forms since it might contain vectors of norm 6.

References

[1] Ch. Bachoc, *Voisinage au sens de Kneser pour les réseaux quaternioniens*, Comm. Math. Helvet. 70 (1995), 350–374.

[2] Ch. Bachoc, *Applications of coding theory to the construction of modular lattices*, to appear.

[3] Ch. Batut, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to PARI-GP*.

[4] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press, London, 1978.

[5] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Graduate Texts in Mathematics, n°138, 1995.

[6] C. Fieker and M. E. Pohst, *On lattices over number fields, preprint.*

[7] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers* (1954), Oxford university press.

[8] F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields, preprint.*

[9] A.K. Lenstra, H.W. Lenstra, Jr and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. 261 (1982), 515–534.

[10] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, to appear.

[11] J. Martinet, *Structures algébriques sur les réseaux*, Number Theory, S. David éd. (Séminaire de Théorie des Nombres de Paris, 1992 – 93), Cambridge University Press, Cambridge, 1995, pp. 167–186.

[12] H. Napias, *Etude expérimentale et algorithmique de réseaux euclidiens*, Thèse, Univ. Bordeaux I (1996).

[13] G. Nebe, W. Plesken, *Memoirs A.M.S.*, vol. 116, number 556, pp. 1–144.

[14] M. Pohst, *A modification of the LLL-algorithm*, J. Symb. Comp. 4 (1987), 123–128.

Huguette NAPIAS
Laboratoire d'Algorithmique Arithmétique
Université Bordeaux I
351, cours de la Libération,
33405 TALENCE cedex
e-mail : napias@math.u-bordeaux.fr