Chin. Ann. Math.
32B(6), 2011, 857–862
DOI: 10.1007/s11401-011-0680-1

Chinese Annals of Mathematics, Series B

Greedy Algorithm Computing Minkowski Reduced Lattice Bases with Quadratic Bit Complexity of Input Vectors*

Hao CHEN[1] Liqing XU[1]

Abstract The authors present an algorithm which is a modification of the Nguyen-Stehle greedy reduction algorithm due to Nguyen and Stehle in 2009. This algorithm can be used to compute the Minkowski reduced lattice bases for arbitrary rank lattices with quadratic bit complexity on the size of the input vectors. The total bit complexity of the algorithm is $O(n^2 \cdot (4n!)^n \cdot (\frac{n!}{2^n})^{\frac{n}{2}} \cdot (\frac{4}{3})^{\frac{n(n-1)}{4}} \cdot (\frac{3}{2})^{\frac{n^2(n-1)}{2}} \cdot \log^2 A)$, where n is the rank of the lattice and A is maximal norm of the input base vectors. This is an $O(\log^2 A)$ algorithm which can be used to compute Minkowski reduced bases for the fixed rank lattices. A time complexity $n! \cdot 3^n (\log A)^{O(1)}$ algorithm which can be used to compute the successive minima with the help of the dual Hermite-Korkin-Zolotarev base was given by Blomer in 2000 and improved to the time complexity $n! \cdot (\log A)^{O(1)}$ by Micciancio in 2008. The algorithm in this paper is more suitable for computing the Minkowski reduced bases of low rank lattices with very large base vector sizes.

Keywords Lattice, Successive minima, Minkowski reduced bases, Greedy reduction
2000 MR Subject Classification 11H55, 68U05

1 Introduction

Let $\mathbf{b}_1, \cdots, \mathbf{b}_n$ be n linearly independent vectors in the Euclid space $\mathbb{R}^n$ of dimension n. The discrete point sets $\mathbf{L} = \{x_1\mathbf{b}_1 + \cdots + x_n\mathbf{b}_n : x_1, \cdots, x_n \in \mathbb{Z}\}$ is rank n lattice in $\mathbb{R}^n$. Its volume is defined as $\mathrm{vol}(\mathbf{L}) = \det^{\frac{1}{2}}((\mathbf{b}_i \cdot \mathbf{b}_j))_{1 \le i,j \le n}$, where $((\mathbf{b}_i \cdot \mathbf{b}_j))_{1 \le i,j \le n}$ is the Gram matrix. The orthogonality defect of the lattice base $\mathbf{b}_1, \cdots, \mathbf{b}_n$ is defined as $\frac{\prod_{i=1}^{n} \|\mathbf{b}_i\|}{\mathrm{vol}(\mathbf{L})}$. We recall the following definitions of successive minima, Voronoi cell and Minkowski reduced bases (see [3, 7]).

Definition 1.1 *$D(\mathbf{L}) = \{\mathbf{x} :\in \mathbb{R}^n : \|\mathbf{x}\| \le \|\mathbf{x} - \mathbf{v}\|$ for any non-zero $\mathbf{v} \in \mathbf{L}\}$ is called the Voronoi cell of the lattice $\mathbf{L}$.*

Definition 1.2 *$\lambda_i(\mathbf{L}) = \min\{r :$ the ball of radius r contains i linearly independent lattice vectors of $\mathbf{L}\}$, for $i = 1, \cdots, n$, are called the successive minima of the lattice $\mathbf{L}$.*

Manuscript received December 17, 2010. Revised June 10, 2011.
[1]Software Engineering Institute, East China Normal University, Shanghai 200062, China.
E-mail: haochen@sei.ecnu.edu.cn
*Project supported by the National Natural Science Foundation of China (No. 10871068) and the Danish National Research Foundation and National Natural Science Foundation of China Joint Grant (No. 11061130539).

It is well-known that there are n linearly independent vectors in $\mathbf{L}$ whose norms attain the successive minima. However, for lattice with rank bigger than or equal to 5, it is possible that these lattice vectors are not the base of the lattice (see [3, 7]).

Definition 1.3 *Let $[\mathbf{b}_1, \cdots, \mathbf{b}_n]_{\leq}$ be an base of the lattice with increasing Euclid norms (i.e., $\|\mathbf{b}_1\| \leq \cdots \leq \|\mathbf{b}_n\|$). It is a Minkowski reduced base if inductively for every i, the $\mathbf{b}_i$ is the shortest vector $\mathbf{b}$ such that $[\mathbf{b}_1, \cdots, \mathbf{b}_{i-1}, \mathbf{b}]_{\leq}$ can be extended to a lattice base.*

We should note that the sets of the Euclid norms of Minkowski reduced bases are not unique and are also not the successive minima for $n \geq 5$ rank lattices (see [3, 7, 10]). However, the first 4 norms of any Minkowski reduced lattice base are exactly the first 4 numbers in the successive minima (see [3, 10]). It is also known that the norms of any Minkowski reduced lattice base are the exponential approximation of the successive minima (see [3, 7]).

Lemma 1.1 (see [3, 7]) *The lattice base $[\mathbf{b}_1, \cdots, \mathbf{b}_n]_{\leq}$ is a Minkowski reduced base if and only if for arbitrary index i and arbitrary integers $x_1, \cdots, x_n$ satisfying $\gcd(x_i, \cdots, x_n) = 1$, we have $\|x_1\mathbf{b}_1 + \cdots + x_n\mathbf{b}_n\| \geq \|\mathbf{b}_i\|$. If the above base is not Minkowski reduced, there exist an index j_1, some integers $x_1, \cdots, x_{j_1-1}$ and non-zero integers $x_{j_1}, \cdots, x_{j_m}$ where $j_1 < \cdots < j_m$ satisfying $\gcd(x_{j_1}, \cdots, x_{j_m}) = 1$, such that $\|x_1\mathbf{b}_1 + \cdots + x_{j_1-1}\mathbf{b}_{j_1-1} + x_{j_1}\mathbf{b}_{j_1} + \cdots + x_{j_m}\mathbf{b}_{j_m}\| < \|\mathbf{b}_{j_1}\|$.*

Minkowski reduced bases for a lattice in the Euclid spaces have very nice properties such as exponential approximation to the successive minima. It is desirable to have an algorithm to compute these nice lattice bases quickly. An algorithm to construct Minkowski lattice bases by using LLL reduced base and Kannan enumeration algorithm was given in [6]. Nguyen and Stehle [10] proposed some greedy algorithms for computing Minkowski bases in low dimensions $2, 3, 4$. As indicated in [10], the greedy reduction with the help of Tammela lists of Minkowski conditions (see [12, 13]) can output the Minkowski lattice bases for lattices of ranks 5 and 6. For the fixed dimension, Helfrich's algorithm in [6] can be used to compute the Minkowski reduced bases in cubic time $O((\log(\max\{\|\mathbf{b}_1\|, \cdots, \|\mathbf{b}_n\|\}))^3)$ of the bit length of the input vectors. However, the hidden coefficient grows exponentially fast. The greedy algorithm in [10] for computing Minkowski reduced base for lattices with rank $2, 3, 4$ is very fast for low rank lattices, and its bit complexity is in the quadratic of the length of $\max\{\|\mathbf{b}_1\|, \cdots, \|\mathbf{b}_n\|\} = \|\mathbf{b}_n\|$ which is the maximal norm of the input base $[\mathbf{b}_1, \cdots, \mathbf{b}_n]_{\leq}$. On the other hand, Tammela [12, 13] gave lists of these $(x_1, \cdots, x_7)$ in the above lemma for which the corresponding conditions for a non-Minkowski reduced base has to be satisfied. As indicated in [11], with the help of Tammela list of Minkowski conditions in [12] the greedy type reduce algorithm can output the Minkowski reduced base for lattice with rank 5 or 6. However, for lattices with ranks more than 7, no such list is known though it has been known by Minkowski that there are only finitely many conditions. This is the motivation of the present work.

By using the Hermite-Korkin-Zolotarev (HKZ) base of the dual lattice, Blomer [2] gave an algorithm to compute the successive minima of a lattice with rank n with time complexity $n! \cdot 3^n \cdot (\log A)^{O(1)}$, where $\log A$ is the input size. This was improved to an algorithm with

complexity $n! \cdot (\log A)^{O(1)}$ by Micciancio [9]. If the dual HKZ base has been computed, then the algorithm in [2, 9] needs bit complexity $n! \cdot n^{O(1)} \cdot (\log A)^{O(1)}$ for computing the successive minima. However, we should note in that circumcise, the assumption that HKZ base of the dual lattice has been found is cost-consuming with bit complexity $n^{\frac{n}{2}} \cdot (\log A)^{O(1)}$. In practice, the cost of finding the HKZ base is very high. Secondly, the input size depending cost $(\log A)^{O(1)}$ is not figured out exactly. For the fixed dimension, Eisenbrand and Rote gave quasi-linear (in $\log A$) algorithms for computing the orthogonality-defect bounded bases and the shortest lattice vector in [5]. It would be interesting if their method can be extended to compute the Minkowski-reduced lattice bases.

In this paper, we give a modification of the greedy reduce algorithm in [10]. Our novel greedy algorithm can compute a Minkowski reduced lattice base for lattice of arbitrary rank with a bit complexity $O(\log^2 A)$ where $A = \max\{\|\mathbf{b}_1\|, \cdots, \|\mathbf{b}_n\|\}$ is the maximal norm of input base and the hidden constant is dependent on the lattice rank. It can be thought as an extended version of the algorithm in [10] with the greedy step executed more rounds for excluding these vectors without the conditions in Lemma 1.1. We also need to use the quadratic bit complexity LLL algorithm (called L^2 algorithm in [11]) to get an LLL reduced base with only quadratic bit complexity. The main advantage of our algorithm is that the bit complexity of the algorithm in the fixed dimension is the quadratic of the maximal of the length of the input vectors.

2 Greedy Algorithm for Minkowski Reduced Bases

***L*² Algorithm** In [11], an algorithm with $O(n^5(n + \log A)\log A)$ bit complexity to output an LLL reduced base from arbitrary given lattice base was presented. It is well-known that the orthogonality defect of an LLL reduced base is upper bounded by $(\frac{4}{3})^{\frac{n(n-1)}{4}}$. Thus we can assume without generality that the input lattice base's orthogonality defect is bounded by $(\frac{4}{3})^{\frac{n(n-1)}{4}}$.

We recall the following greedy step in [10].

Greedy Step = CVP For the input $(\mathbf{x}, \mathbf{L}'(\mathbf{B}'))$ where $\mathbf{L}'(\mathbf{B}')$ is a sublattice with the base $\mathbf{B}'$ and $\mathbf{x} \in \mathbb{R}^n$ not in a sublattice $\mathbf{L}'(\mathbf{B}')$, search the closest vector $\mathbf{y} \in \mathbf{L}'(\mathbf{B}')$ by checking the integral vectors $\mathbf{y}$ in $\mathbf{L}'(\mathbf{B}')$, such that $\mathbf{y} - \pi_{\mathbb{R}\mathbf{L}'(\mathbf{B}')}(\mathbf{x})$ is in the Voronoi cell $D(\mathbf{L}(\mathbf{B}'))$ and attains the shortest norm, where $\pi_{\mathbf{T}}$ is the projection to the subspace $\mathbf{T} \subset \mathbb{R}^n$. The output is the lattice vector $\mathbf{x} - \mathbf{y}$ (see [5]).

Proposition 2.1 *If* $\mathbf{B}'$ *is a Minkowski reduced base for the sublattice* $\mathbf{L}'(\mathbf{B}')$*, the bit complexity of the above Greedy step is bounded by* $(4n!(\frac{3}{2})^{\frac{n(n-1)}{2}})^n \cdot \log^2 A$.

Proof From [3, 7], the orthogonality defect of the Minkowski reduced base of $\mathbf{L}'(\mathbf{B}')$ is upper bounded by $(\frac{3}{2})^{\frac{r(r-1)}{2}}$, where $r = \text{rank}(\mathbf{L}'(\mathbf{B}'))$. From [4], the coordinates of Voronoi cell in a base with upper bound orthogonality defect $C_{\text{orthogonality}}$ is upper bounded by $u!C_{\text{orthogonality}}(1+(1-\frac{1}{C^2_{\text{orthogonality}}})^{\frac{u-1}{2}})$, where u is the lattice rank. Thus the coordinates of the Voronoi cell of a rank r lattice with a Minkowski reduced base is upper bounded by $r!2(\frac{3}{2})^{\frac{r(r-1)}{2}}$. There are at most $(4r!(\frac{3}{2})^{\frac{r(r-1)}{2}})^r$ points that need to be searched.

In this paper, we use the search algorithm of CVP for the purpose that the bit complexity factor on $\log A$ is quadratic. For many works on CVP algorithms, we refer to [8, 9] and the references therein.

We need the following algorithm in [9, p. 129] to find a base from any n linearly independent lattice vectors.

Finding-Base $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$ *For the input of n linearly independent lattice vectors* $\|\mathbf{v}_1\| \leq \cdots \leq \|\mathbf{v}_n\|$ *in any rank n lattice* $\mathbf{L}$*, the algorithm outputs a lattice base* $\mathbf{r}_1, \cdots, \mathbf{r}_n$ *satisfying* $\|\mathbf{r}_k\| \leq \max\{1, \frac{\sqrt{k}}{2}\}\|\mathbf{v}_k\|$*. We can always assume* $\mathrm{span}(\mathbf{r}_1) = \mathrm{span}(\mathbf{v}_1)$.

By checking the proof in [9, pp. 129–130], we have the following bound on the bit complexity of the above algorithm immediately.

Proposition 2.2 (see [9, pp. 129–130]) *The bit complexity of this algorithm is* $n^3 \log^2 A$.

Proposition 2.3 *Suppose that* $[\mathbf{b}_1, \cdots, \mathbf{b}_n]_{\leq}$ *is not a Minkowski reduced base and i is the smallest index, such that the condition in Lemma* 1.1 *is not satisfied and* $x_1, \cdots, x_n$ *are integers in Lemma* 1.1 *such that* $\|x_1\mathbf{b}_1 + \cdots + x_n\mathbf{b}_n\| < \|\mathbf{b}_i\|$ *holds for some* $\mathbf{b}_i$*. Let j be the largest index, such that* x_j *is not zero. Then this index j satisfies* $j > i$ *and* $|x_j| < \frac{\|\mathbf{b}_i\|}{\|\mathbf{b}_j^*\|} < \frac{\|\mathbf{b}_j\|}{\|\mathbf{b}_j^*\|}$*, where* $\mathbf{b}_1^*, \cdots, \mathbf{b}_n^*$ *is the Gram-Schmidt orthogonalization of the base* $\mathbf{b}_1, \cdots, \mathbf{b}_n$.

Proof It is clear that $x_1\mathbf{b}_1 + \cdots + x_j\mathbf{b}_j = x_1'\mathbf{b}_1^* + x_2'\mathbf{b}_2^* + \cdots + x_{j_1}'\mathbf{b}_{j_1}^* + x_j\mathbf{b}_j^*$. Here $x_1', \cdots, x_{j_1}'$ may not even be integers. The conclusion follows from Lemma 1.1 and $\|x_1'\mathbf{b}_1^* + x_2'\mathbf{b}_2^* + \cdots + x_{j_1}'\mathbf{b}_{j-1}^* + x_j\mathbf{b}_j^*\| \geq |x_j|\|\mathbf{b}_j^*\|$.

The following is our modified greedy reduction algorithm for a Minkowski reduced lattice base.

Greedy Reduction Computing a Minkowski Reduced Base

Input Any base $\mathbf{B}$ of a lattice $\mathbf{L}$ with rank n;

Output A Minkowski reduced base of $\mathbf{L}$.

Step 1 Doing the reduction in [11] for the base $\mathbf{B}$, an LLL reduced base is found with bit complexity $O(n^5(n + \log A)\log A)$, where the hidden constant is independent of the dimension and the input vector lengths. We order the output base in the increasing norm order $[\mathbf{a}_1, \cdots, \mathbf{a}_n]_{\leq}$. The orthogonality defect of this input base in the next steps is at most $(\frac{4}{3})^{\frac{n(n-1)}{4}}$.

Step 2 For the sublattice $\mathbf{L}_{n-1}$ generated by $[\mathbf{a}_1, \cdots, \mathbf{a}_{n-1}]_{\leq}$, do the $n-1$ dimension Greedy reduction with bit complexity $T(n-1)$ to get a Minkowski reduced base $[\mathbf{b}_1, \cdots, \mathbf{b}_{n-1}]_{\leq}$ of this sublattice.

Step 3 For the input $(\mathbf{L}_{n-1}, x\mathbf{a}_n)$ where x takes over all integers satisfying $|x| \leq (\frac{4}{3})^{\frac{n(n-1)}{4}}$, do the Greedy step. The bit complexity is upper bounded by $2 \cdot (\frac{4}{3})^{\frac{n(n-1)}{4}} \cdot T(n-1)$. Let the shortest output vector be $\mathbf{a}_n' = x_{\mathrm{new}}\mathbf{a}_n + \sum_{i \leq n-1} x_i\mathbf{b}_i$, where $x_{\mathrm{new}} \neq 0$.

Step 4 If $\|\mathbf{a}_n'\| \geq \|\mathbf{b}_{n-1}\|$, the algorithm terminates. Otherwise, substituting the new $\mathbf{a}_n'$ in the ordering base $\{\mathbf{b}_1, \cdots, \mathbf{b}_{n-1}, \mathbf{a}_n\}$ in the increasing norm order, we can get n linearly independent lattice vectors $[\mathbf{a}_1'', \cdots, \mathbf{a}_n'']_{\leq}$ of the lattice $\mathbf{L}$. Suppose that $\mathbf{b}_1, \cdots, \mathbf{b}_{k-1}$ is before $\mathbf{a}_n'$. Then $\gcd(x_{\mathrm{new}}, x_{n-1}, \cdots, x_k) = 1$ from the definition of the Minkowski condition (see Lemma 1.1).

Step 5 For the $n-k$ linearly independent lattice vectors $[\mathbf{a}'_n, \mathbf{b}_{k+1}, \cdots, \mathbf{b}_{n-1}]_{\leq}$, do the finding-base $(\mathbf{a}'_n, \mathbf{b}_{k+1}, \cdots, \mathbf{b}_{n-1})$. Then we get a new base $[\mathbf{b}_1^{\text{new}}, \cdots, \mathbf{b}_n^{\text{new}}]_{\leq}$ of the lattice $\mathbf{L}$ with the orthogonality defect at most $(\frac{n!}{2^n})^{\frac{1}{2}} \cdot (\frac{4}{3})^{\frac{n(n-1)}{4}}$. Here it should be noted that $\mathbf{a}'_n = \mathbf{b}_k^{\text{new}}$ is not changed.

***i*-th round** Execute Steps 1–5 to the lattice base $[\mathbf{b}_1^{\text{new}}, \cdots, \mathbf{b}_n^{\text{new}}]_{\leq}$.

Theorem 2.1 *The above Steps* 1–5 *will execute at most n rounds and a Minkowski reduced base will be found.*

Proof The point here is that $\mathbf{a}'_{ni}$ at the i-th round is not shorter than $\mathbf{a}'_{n(i-1)}$ of the $(i-1)$-th round, that is, $\|\mathbf{a}'_{ni}\| \leq \|\mathbf{a}'_{n(i-1)}\|$. Thus after the i-th round, $\mathbf{a}'_{ni}$ is always after $\mathbf{a}'_{n(i-1)}$ in the norm-ordering base of the lattice. After at most n rounds the algorithm will terminate. The output lattice base is certainly a Minkowski reduced base, since the algorithm will exclude all integer combinations not satisfying the condition of Lemma 1.1.

Theorem 2.2 *The bit complexity of the above algorithm will be at most* $O(n^2 \cdot (4n!)^n \cdot (\frac{n!}{2^n})^{\frac{n}{2}} \cdot (\frac{4}{3})^{\frac{n(n-1)}{4}} \cdot (\frac{3}{2})^{\frac{n^2(n-1)}{2}} \cdot \log^2 A)$.

Proof It is observed that the orthogonality defect is decreasing in Steps 2–4 and is increased by a factor at most $(\frac{n!}{2^n})^{\frac{1}{2}}$ in the Step 5. Since the algorithm execute at most n rounds, the orthogonality defect is upper bounded by $(\frac{n!}{2^n})^{\frac{n}{2}} \cdot (\frac{4}{3})^{\frac{n(n-1)}{4}}$. Thus we have $T(n) \leq 2n \cdot (\frac{n!}{2^n})^{\frac{n}{2}} \cdot (\frac{4}{3})^{\frac{n(n-1)}{4}} \cdot (4n!(\frac{3}{2})^{\frac{n(n-1)}{2}})^n \cdot \log^2 A + T(n-1)$, the worst-case bit complexity is upper bounded by $2n^2 \cdot (4n!)^n \cdot (\frac{n!}{2^n})^{\frac{n}{2}} \cdot (\frac{4}{3})^{\frac{n(n-1)}{4}} \cdot (\frac{3}{2})^{\frac{n^2(n-1)}{2}} \cdot \log^2 A$.

From Theorem 2.2 it can be seen that the factor of n is very bad and the factor of $\log A$ is quadratic. Our greedy algorithm is more suitable for low rank lattices with very large lattice base vectors.

If Steps 2–5 are only used in at most d rounds for the rank d lattices, we call such an algorithm Minkowski(d). We have the following result.

Theorem 2.3 *If* $\mathbf{L}$ *is a rank n lattice with the base* $\mathbf{B}$*. Suppose that the orthogonality defect of B is upper bounded by C. Then by using the fact that at most* $2n(\frac{n!}{2^n})^{\frac{n}{2}}C$ *calls to the Greedy step and n calls to the algorithm* $Minkowski(n-1)$*, a Minkowski reduced lattice base of the rank n lattice* $\mathbf{L}$ *can be found.*

Actually for the fixed dimension, Eisenbrand and Rote [5] gave an algorithm for computing the orthogonality-defect bounded lattice bases with bit complexity $O(M(\log A)(\log\log A)^{O(1)})$, where $M(\log A)$ is the bit complexity of $\log A$-bit integer multiplication. If we use Eisenbrand-Rote algorithm in [5, Section 6] in Step 1, we have the following result.

Theorem 2.4 *Let* $\mathbf{L} \subset \mathbb{Z}^n$ *be a rank n lattice with a base* $\mathbf{B}$ *with bit length* $\log A$*. Then the Minkowski reduced lattice base of* $\mathbf{L}$ *can be found with bit complexity* $O(M(\log A)(\log\log A)^{O(1)})$*, where the hidden constant only depends on the rank n.*

References

[1] Ajtai, M., Kumar, R. and Sivakumar, D., A sieve algorithm for the shortest lattice vector problem, Proceedings on 33rd Annual ACM Symposium on Theory of Computing, ACM, Heraklion, Greece, 2001, 601–610.

[2] Blomer, J., Closest vectors, successive minima and dual HKZ bases of lattice, Proceedings of the 27th International Colloquium on Automata, Languages and Programming, Lecture Notes in Computer Science, **1835**, Springer-Verlag, New York, 2000, 248–259.

[3] Cassels, J. W. S., An Introduction to the Geometry of Numbers, 2nd ed., Springer-Verlag, New York, 1972.

[4] Delone, D. N., Ryshkov, S. S. and Shtogrin, M. I., A theorem due to Sandakova concerning positive quadratic forms, *Metematicheskie Zametki*, **1**(3), 1967, 253–262.

[5] Eisenbrand, F. and Rote, G., Fast reduction of ternary quadratic forms, Proceedings of 2001 Cryptography and Lattice Conference, Lecture Notes in Computer Science, **2146**, Springer-Verlag, Heidelberg, 2001, 32–44.

[6] Helfrich, B., Algorithms to construct Minkowski reduced and Hermite reduced lattice bases, *Theor. Comp. Sci.*, **41**, 1985, 125–139.

[7] Henk, M., Geometry of Numbers. http://fma2.math.uni-magdeburg.de/henk/index.html

[8] Micciancio, D., Efficient reductions among lattice problems, Proceedings of the 19th annual ACM-SIAM Symposium on Discrete Algorithms, ACM-SIAM, San Francisco, California, 2008, 84–93.

[9] Micciancio, D. and Goldwasser, S., Complexity of lattice problems, A Cryptographic perspective, Kluwer Academic Publishers, Boston, 2002.

[10] Nguyen, P. Q. and Stehle, D., Low dimensional basis reduction revisited, Proceedings of the 6th Algorithmic Number Theory Symposium, Lecture Notes in Computer Science, **3076**, Springer-Verlag, New York, 2004, 338–357; *ACM Transactions on Algorithms*, **5**(4), 2009, 46. DOI: 10.1145/1597036.1597050

[11] Nguyen, P. Q. and Stehle, D., Floating-point LLL revisited, Proc. Eurocrypt 2005, full version, An LLL algorithm with quadratic complexity, *SIAM J. Comp.*, **39**(3), 2009, 874–903.

[12] Tammela, P. P., On the reduction theory of positive quadratic forms, *Soveit Math. Dolklady*, **14**, 1973, 651–655.

[13] Tammela, P. P., Minkowski reduction region for positive quadratic forms in seven variables, *J. Soviet Math.*, **16**, 1981, 863–857.