IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 16, Issue 3 Ser. III (May – June 2020), PP 26-32
www.iosrjournals.org

The closest vector problem in some lattices of type A

Arnaud GirèsFobasso Tchinda[1], EmmanuelFouotsa[2]
[1](Department of Mathematics, Faculty of Science, University of Yaoundé I, Cameroon)
[2](Department of Mathematics,Higher Teacher Training College, University of Bamenda, Cameroon)

Abstract: *Lattice-based cryptographic constructions hold a great promise for postquantum cryptography, as they enjoy very strong security proofs based on worst-case hardness relatively efficient implementations, as well as great simplicity. LéoDucas and Wessel van Woerden in [5] proposed a polynomial algorithm allowing solving the Closest Vector Problem (CVP) in the tensor product of two lattices of type A. And as anopen problem, theses authors asked to extend this resolution in the case of three lattices and in the general case of k lattices of type A. Our goal is therefore to propose a solution of this problem. We use the associativity of the lattice of type A and the same techniques to solve this problem in the tensor product of three lattices of type A and even in the tensor product of a finite number of lattices of type A. So we will determine a polynomial algorithm to solve CVP in* $A_{n+1}\otimes A_{m+1}\otimes A_{p+1}$.

Key Word: *Lattice based cryptography, root lattice, closest vector problem, tensored root lattices, graph, completed graph, cycle.*
AMS Subject Classification 2010: 11H71 - 11T71 - 94B75 - 94B35.

Date of Submission: 14-05-2020 Date of Acceptance: 29-05-2020

I. Introduction

Searching for the nearest vector in a lattice is a difficult mathematical problem [6], used in cryptography to build robust and secure cryptosystems [9] resistant to quantum computers [12]. The fact of determining a basis whose vectors are relatively closed and almost orthogonal makes it possible to easily find the nearest vector in a lattice of integers [13]. The polynomial LLL reduction algorithm has been generalized by Napias on the Euclidean rings of integers [11]. As a result, Conway and Sloane [3] set up polynomial algorithms to solve the problem of the nearest vector in root lattices of type A. In order to improve the tolerance of the error of the cryptosystem, L éoDucas and Wessel van Woerden used the isomorphisms of root lattice defined in [5] to build a polynomial algorithm to solve the problem of the nearest vector in the tensor product of two root lattices and in the direct sum of a finite number of root lattices of type A [14].

In this work, we propose a polynomial algorithm to solve the problem of the nearest vector in the tensor product $A_{n+1}\otimes A_{m+1}\otimes A_{p+1}$. Indeed, there is already an algorithm to solve this problem in A_n [5]. A motivation could be to use the full characterization of the Voronoi relevant vector in this case in term of simple cycle in the complete directed tripartite graph $K_{n+1,m+1,p+1}$. So we need to establish the relationship between the Voronoi relevant vectors in the tensor product $A_{n+1}\otimes A_{m+1}\otimes A_{p+1}$ and the complete directed tripartite graphs $K_{n+1,m+1,p+1}$. Subsequently, we will modify some parameters of the polynomial algorithm in [3] to solve this problem in $A_{n+1}\otimes A_{m+1}\otimes A_{p+1}$.

This work is organized as follows: In Section II, we review the definitions of lattices, graphs, tensor product and basic properties of the root lattices of type A and simple graph to understand the results of further sections. In Section III, we present the characterization of the Voronoi relevant vector in the tensor product of three root lattices of type A and give the polynomial algorithm to solve the problem of the nearest vector in $A_{n+1}\otimes A_{m+1}\otimes A_{p+1}$. In Section IV, we willgeneralize this result in the case of the tensor product of k root lattices of type A.

II. LatticeandgraphBackground

Throughout this paper, for some positive integer d, we use the Euclidean product on$\mathbb{R}^d$that is defined by:

$$\langle x,y \rangle = x_1y_1 + x_2y_2 + \ldots + x_dy_d$$

for $x = (x_1,x_2,\ldots,x_d)$ and $y = (y_1,y_2,\ldots,y_d)$ in $\mathbb{R}^d$. The Euclidean norm on $\mathbb{R}^d$is defined as follows: $\|x\| =\sqrt{\langle x, y \rangle}$. All definitions in this section are taken form [5, 13].

Definition 1.A lattice is a discrete additive subgroup of $\mathbb{R}^d$, for some positive integer d. We deal exclusively with any lattice $\Lambda$of rank r, which is generated as the set of all integer linear combinations of r linearly independent vectors $b_1, b_2, \ldots b_r$ in $\mathbb{R}^d$ as follows:

$$\Lambda = \{\sum_{i=1}^{r} z_i . b_i : (z_1, z_2, \ldots, z_r) \in \mathbb{Z}^r\} \qquad (1)$$

Obviously, $r \leq n$. Another lattice Λ' in $\mathbb{R}^d$ of the same rank r such that $\Lambda' \subset \Lambda$ is called a full rank sublattice of Λ. A generator matrix of Λ is a matrix whose rows form a base of Λ. The linear subspace of $\mathbb{R}^d$ spanned by the elements of Λ is denoted span(Λ). The dual lattice of Λ is defined as $\Lambda^* = \{x \in \mathbb{R}^d : \langle \Lambda, x\rangle \subset Z\}$, where $\langle \Lambda, x\rangle = \{\langle y, x\rangle : y \in \Lambda\}$. It is easy to see that $(\Lambda^*)^* = \Lambda$. The minimum distance of a lattice Λ w.r.t Euclidian norm, denoted $\|\Lambda\|$, is the length of a shortest lattice nonzero vector, i.e., $\|\Lambda\| = \min_{0 \neq x \in \Lambda} \|x\|$.
Given that we are going to associate the oriented graphs in our work, the definitions below will allow a better understanding for the rest of the work.

Definition 2.

1. A graph G is a ordered pair (V,E) where :
   - V is a finite set of vertices (also called nodes or points);
   - $E \subset \{ (x,y) / (x,y) \in V^2 \text{ and } x \neq y\}$ is a subset of $V \times V$. The elements of E are called the edges of the graph.
2. A graph G is connected if it is possible from any vertex, to join all the others vertices following the edges.
3. A complete graph is a graph that has an edge between every simple vertex in the graph. We label K_n the complete graph with n vertices.
4. A graph G is said to be tripartite if there exists a partition $\{V_1, V_2, V_3\}$ of V such that each edge of G connects a vertex of V_1 to a vertex of V_2 and to a vertex of V_3.
5. A cycle of a graph, also called a circuit is a non-empty trail in which the only repeated are the first and the ending vertices.
6. A simple cycle is a cycle with no repeated vertices (except for the beginning and the ending vertex).

Inspired by the characterization of the tensor product of two and three root lattices of type A, we will generalize the characterization of the tensor product of a finite number of root lattices of type A as below.

Definition 3. Let $\Lambda_1 \subset \mathbb{R}^{n1}$ and $\Lambda_2 \subset \mathbb{R}^{n2}$ be lattices of respectively ranks n_1 and n_2, let $a_1, \ldots a_{n1} \in \mathbb{R}^{n1}$ and $b_1, \ldots, b_{n2} \in \mathbb{R}^{n2}$ be respective bases. The tensor product $\Lambda_1 \otimes \Lambda_2 \subset \mathbb{R}^{n1n2}$ is defined as the lattice with basis $\{a_i \otimes b_j : i \in 1, \ldots, n_1;\ j \in 1, \ldots, n_2\}$.
Here $x \otimes y = (x_1, \ldots, x_{n1}) \otimes (y_1, \ldots, y_{n2})$ with $x \in \mathbb{R}^{n1}$ and $y \in \mathbb{R}^{n2}$ is defined as the natural embedding in $\mathbb{R}^{n1n2}$ as follows:

$$(x_1y_1, x_1y_2, \ldots, x_1y_{n2}, x_2y_1, \ldots, x_{n1}y_{n2}) \in \mathbb{R}^{n1n2}.$$

For three lattices, the tensor product $\Lambda_1 \otimes \Lambda_2 \otimes \Lambda_3 \subset \mathbb{R}^{n1n2n3}$ (with $\Lambda_3 \subset \mathbb{R}^{n3}$ and it basis $c_1, \ldots, c_{n3} \in \mathbb{R}^{n3}$) is defined as the lattice with basis $\{a_i \otimes b_j \otimes c_k : i=1, \ldots, n_1;\ j=1, \ldots, n_2;\ k=1, \ldots, n_3\}$.
Here $x \otimes y \otimes z = (x \otimes y) \otimes z = (x_1y_1, x_1y_2, \ldots, x_1y_{n2}, x_2y_1, \ldots, x_{n1}y_{n2}) \otimes (z_1, \ldots, z_{n3})$;
Thus, $x \otimes y \otimes z = (x_1y_1z_1, x_1y_1z_2, \ldots, x_1y_1z_{n3}, x_1y_2z_1, \ldots, x_{n1}y_{n2}z_{n3}) \in \mathbb{R}^{n1n2n3}$.

Definition 4. Let $\Lambda_1 \subset \mathbb{R}^{n1}$, $\Lambda_2 \subset \mathbb{R}^{n2}, \ldots, \Lambda_k \subset \mathbb{R}^{nk}$ be lattices of respectively ranks n_1, $n_2, \ldots, n_k$; let $a_1^{(1)}, \ldots, a_{n1}^{(1)} \in \mathbb{R}^{n1}$; $a_1^{(2)}, \ldots, a_{n2}^{(2)} \in \mathbb{R}^{n2}; \ldots;$ $a_1^{(k)}, \ldots, a_{nk}^{(k)} \in \mathbb{R}^{nk}$ be respective bases. The tensor product $\Lambda_1 \otimes \Lambda_2 \otimes \ldots \otimes \Lambda_k \subset \mathbb{R}^{n1n2..nk.}$ is defined as the lattice with basis $\{a_{i(1)}^{(1)} \otimes a_{i(2)}^{(2)} \otimes \ldots \otimes a_{i(k)}^{(k)} : i(1)=1, \ldots, n_1; \ldots; i(k)=1, \ldots, n_k\}$.
Here, we use the associativity to compute $x^{(1)} \otimes x^{(2)} \otimes \ldots \otimes x^{(k)}$ as below :

$$x^{(1)} \otimes x^{(2)} \otimes \ldots \otimes x^{(k)} = (x_1^{(1)}x_1^{(2)} \ldots x_1^{(k)}, x_1^{(1)}x_1^{(2)} \ldots x_2^{(k)}, \ldots, x_{n1}^{(1)}x_{n2}^{(2)} \ldots x_{n3}^{(k)}) \in \mathbb{R}^{n1n2..nk.}$$

Closest Vector Problem 1. Let $\Lambda \subset \mathbb{R}^d$ be a lattice and $t \in \text{span}(\Lambda)$. The aim is to construct a vector x in Λ that minimizes the distance $\|t-x\|$. Such an x is also called a closest vector to t.
The following example recalls the definition of the root lattice of type A below, gives its dual lattice, and provides a generator matrix for both.

Example 2.1.[5, Lemmas 2. and 3.] Let n be a positive integer. The subset A_n of $\mathbb{R}^{n+1}$ defined by:

$$A_n = \{x \in Z^{n+1} : \langle x, [1] \rangle = 0\} ;$$

where $[1] = (1,1,\ldots,1)$ is a lattice of rank n in $\mathbb{R}^{n+1}$ with a generator matrix

$$B = \begin{pmatrix} 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & -1 & 0 \\ 0 & \cdots & 0 & 0 & 1 & -1 \end{pmatrix} \qquad (2)$$

A generator matrix of its dual $(A_n)^*$ is the n× (n+1) – matrix B* given by

$$B^* = \frac{1}{n+1}\begin{pmatrix} n & -1 & -1 & \cdots & -1 \\ -1 & n & -1 & \cdots & -1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ -1 & \cdots & n & -1 & -1 \\ -1 & \cdots & -1 & n & -1 \end{pmatrix} \qquad (3)$$

Definition 5. (Voronoi region)[5] The Voronoi region of a lattice Λ is defined by:

$$V(\Lambda) := \{x\in \mathrm{span}(\Lambda): \|x\| \leq \|x-v\|\ \forall v\in\Lambda\}$$
$$= \{x\in \mathrm{span}(\Lambda): 2\langle x,v\rangle \leq \langle v,v\rangle\ \forall v\in\Lambda\}$$

Consistingofallpointsinspan(Λ)thathave0asaclosestvector.Itismeansthatitisthesetof pointsofspan(Λ)havingthenearestvector0inthelatticeΛ. TheVoronoiregionisjusttheintersectionofhalfspacesH_v:={x∈span(Λ):2⟨x,v⟩≤⟨v,v⟩} forallv∈Λ\{0}.Notethattheonlyhalfspaces$H_v$inthisintersectionthatmatterarethose correspondingtoafacet (rank(Λ)-1dimensionalfaceofV(Λ)), {x∈span(Λ):||x||≤||x−v||}∩ V(Λ)oftheVoronoiregion.Suchv∈ΛarecalledVoronoirelevantvectors.

Definition 6. (Voronoirelevant vectors)[5]: Let Λ be a lattice. Let v ∈Λ\{0}; v is an Voronoirelevantvectorsifthereexistx∈span(Λ)suchthat:||x||=||x−v||and∀w∈Λ\{0}||x||<||x−w||.

These are also the minimal set RV (Λ) ⊂ Λof the vectors such that

$$V(\Lambda) = \cap H_v, \text{ with } v \in RV(\Lambda)$$

Voronoi showed that for v∈Λ\{0}we have that v is a Voronoi relevant vector if and only if 0 and v are the only closest vectors to $\frac{v}{2}$ in Λ.

Lemma 1. [5]Lett∈span(Λ)andx∈Λ.Thereexistsavectory∈Λsuchthat||(x+y) −t||<||x− t|| ifandonlyifthereexistsaVoronoirelevantvectorv∈RV (Λ)suchthat||(x+v) −t||<||x−t||.

Proof.

We suppose that there exists y∈ Λ such that ||(x+y)-t||<||x-t||;
we know that: ||(x+y)-t|| = ||t-(x+y)|| and ||x-t|| = ||t-x||;
thus ||t-(x+y)||<||t-x||;
by Definition 10, we deduce that (t-x) is not in the set V(Λ);
it is means that there exists a vector v∈ RV(Λ) such that ||t-x||>||(t-x)-v||;
thus there exists a vector v∈ Λ such that ||(x+v)-t||<||x-t||.
Inversely, we suppose now there exists v∈ RV (Λ) such that ||(x+y)-t||<||x-t||;
SinceRV (Λ) ⊂Λ, then there exist a vector v∈ Λ such that ||(x+y)-t||<||x-t||;
for y = v, we have the result.

Proposition 1.Let Λ be a lattice. A vector v∈Λ\{0} is Voronoirelevant vector if and only if ⟨v,x⟩<⟨x ,x ⟩, for all x ∈ Λ \{0, v }.

Proof.

We remark that $\|\frac{1}{2}v - x\|^2 - \|\frac{1}{2}v\|^2 = \|\frac{1}{2}v\|^2 - \langle v,x\rangle + \|x\|^2 - \|\frac{1}{2}v\|^2 = \|x\|^2 - \langle v,x\rangle$;
Thus $\|\frac{1}{2}v - x\|^2 = \langle x,x\rangle - \langle v,x\rangle$;
Then, for a v∈Λ\{0} and all x∈Λ\{0,v} we have that:
$\|\frac{1}{2}v - x\|^2 - \|\frac{1}{2}v\|^2 > \|\frac{1}{2}v\|^2$ iff⟨x,x⟩>⟨v,x⟩.

The construction of the tensor product of two root lattices of type A is done as below.

Let m,n ≥ 1, we consider the lattice $A_n \otimes A_m \subset \mathbb{Z}^{(n+1)(m+1)}$ of rank nm. Note that this lattice consists of all elements $x = (x_{11}, x_{12}, \ldots, x_{1(n+1)}, x_{21}, \ldots, x_{(n+1)(m+1)}) \in \mathbb{Z}^{(n+1)(m+1)}$ which satisfy the following conditions :

(1) $\sum_{i=1}^{n+1} x_{ij} = 0$ for j=1,…,m+1

(2) $\sum_{j=1}^{m+1} x_{ij} = 0$ for i=1,…,n+1

Remark 1. From the root lattice tensor product constructions, it follows that $A_n \otimes A_m$ is a subgroup of lattice $A_{(n+1)(m+1)-1}$. To solve CVP in the tensor product of three lattices of type A, it will be enough to use associativity and solve C V P first in $A_n \otimes A_m$ then in $A_{(n+1)(m+1)-1} \otimes A_p$.

Definition 7. Let $t \in \{-1,0,1\}^{(n+1)(m+1)}$ be given. We will define the subgraph $G_t = (V_t, E_t) \subset K_{(n+1),(m+1)} = (V, E)$ corresponding to t. Let E_t consist of the following directed edges:

- Theedge(u_i,v_j)foreacht_{ij}thathasvalue-1;
- Theedge(v_j,u_i)foreacht_{ij}thathasvalue1.

III. ClosestVectorProblemin$A_n \otimes A_m \otimes A_p$

In this section, we will characterize the Voronoi relevant vector in $A_n \otimes A_m \otimes A_p$ (m,n,p ≥ 1) in order to determine a polynomial algorithm to solve the closest vector problem in this lattice. We will use the same techniques as for the case of the tensor product of two root lattices of type A. But in this case of the tensor product of three root lattices of type A, we will use the complete directed tripartite graph.

Definition 8. Let m,n,p ≥ 1, be three positives integers that are not all zero. We call root lattice $A_n \otimes A_m \otimes A_p \subset \mathbb{Z}^{(n+1)(m+1)(p+1)}$ of rank nmp all of elements

$x = (x_{111},\dots, x_{11(p+1)}, x_{121},\dots, x_{12(p+1)},, x_{(n+1)(m+1)(p+1)}) \in \mathbb{Z}^{(n+1)(m+1)(p+1)}$ which satisfy the following conditions :

(1) $\sum_{i=1}^{n+1} x_{ijk} = 0$ for j =1,…,m+1 and k = 1,…,p+1

(2) $\sum_{j=1}^{m+1} x_{ijk} = 0$ for i =1,…,n+1 and k = 1,…,p+1

(3) $\sum_{k=1}^{p+1} x_{ijk} = 0$ for i =1,…,n+1 and j = 1,…,m+1

We will use the indices i, j and k throughout this section.

Characterizing the Voronoi relevant vectors.

As announced we construct a polynomial algorithm to solve the closest vector problem for the lattice $A_n \otimes A_m \otimes A_p$. For this, we characterize the Voronoi relevant of $A_n \otimes A_m \otimes A_p$. First we will limit our search space.

Many of the results present here are due by LéoDucas and Wessel van Woerden **[5].**

Proposition 2. For all voronoi relevant vectors $u \in A_n \otimes A_m \otimes A_p$ we have $|u_{ijk}| < 6$ for all i =1,…,n+1; j =1,…,m+1 and k = 1,…,p+1.

Proof.

Let $u \in A_n \otimes A_m \otimes A_p$ be a Voronoi relevant vector. We suppose that there exist i, j, k such that $|u_{ijk}| \geq 6$; because of symmetry of the Voronoi region we can assume without loss of generality that $|u_{111}| \geq 6$. And because u is a Voronoi relevant vector iff –u is also a relevant vector, we can also assume that $u_{ijk} \geq 6$.

Let $x^{ijk} \in A_n \otimes A_m \otimes A_p$ foralli=2,...,n+1; j=2,...,m+1andk=2,...,p+1 begivenby $x_{111}=x_{1jk}=x_{ij1}=x_{i1j}=1; x_{11k}=x_{1j1}=x_{i11}=x_{ijk}=-1$ and 0 otherwise.

Note that $\langle x^{ijk}, x^{ijk}\rangle = 8$ foralli,j,k.Thenby Definition2,weget:$u_{111}+u_{1jk}+u_{ij1}+u_{i1j} - u_{11k} - u_{1j1} - u_{i11} - u_{ijk} = \langle u, x^{ijk}\rangle < 8$ for all i=1,...,n+1; j=1,...,m+1andk=1,...,p+1.

Because these are all integers, we even have that :$u_{111}+u_{1jk}+u_{ij1}+u_{i1k} - u_{11k} - u_{1j1} - u_{i11} - u_{ijk} \leq 7$.

Summingmultipleoftheserelationsfor afixedj=2,...,m+1gives:

$mu_{111} - mu_{11k} + mu_{i1k} - mu_{i11} + \sum_{j=2}^{m+1}.(u_{1jk} + u_{ij1} - u_{1j1} - u_{ijk}) \leq 7(m+1-1)$. Summing multiple of these relations for a fixed k = 2,…,p+1 gives : $mpu_{111} - mpu_{i11} + \sum_{k=2}^{p+1}.(mu_{i1k} - mu_{11k}) + \sum_{k=2}^{p+1}.(\sum_{j=2}^{m+1}.(u_{1jk} + u_{ij1} - u_{1j1} - u_{ijk})) \leq 7(m+1-1)(p+1-1)$;

therefore $-mu_{i11} = \sum_{k=2}^{p+1}.mu_{i1k}$ and $-mu_{111} = \sum_{k=2}^{p+1}.mu_{11k}$;

as becomes: $mpu_{111} - mpu_{i11} - mu_{i11} + mpu_{i11} + \sum_{k=2}^{p+1}.(\sum_{j=2}^{m+1}.(u_{1jk} + u_{ij1} - u_{1j1} - u_{ijk})) \leq 7(m+1-1)(p+1-1)$;

furthermore, $\sum_{k=2}^{p+1}.(\sum_{j=2}^{m+1}.(u_{1jk} + u_{ij1} - u_{1j1} - u_{ijk})) = \sum_{k=2}^{p+1}.(-u_{11k} - u_{i11} + u_{111} + u_{i1k}) = u_{111} - pu_{i11} + pu_{111} - u_{i11}$;

so the inequations becomes: $mpu_{111} - mpu_{i11} - mu_{i11} + mpu_{i11} + u_{111} - pu_{i11} + pu_{111} - u_{i11} \leq 7(m+1-1)(p+1-1)$;

thus, $(m+1)(p+1)(u_{111} - u_{i11}) \leq 7(m+1-1)(p+1-1)$; so $u_{111} - u_{i11} \leq \frac{7(m+1-1)(p+1-1)}{(m+1)(p+1)}$;

by hypothesis we have $u_{111} \geq 6$, then we now get that: $u_{i11} \geq \frac{7(m+1-1)(p+1-1)}{(m+1)(p+1)} + 6$;

and thus $u_{i11} \geq -1 + \frac{7(m+1+p+1-1)}{(m+1)(p+1)}$; and we also have (7(m+1)(p+1)-1) > (m+1)(p+1) for all (p+1),(m+1) ≥ 3.

So $u_{i11} \geq 0$ for all i = 2,…,n+1 and $u_{111} \geq 6$; but in that case:

$0 = \sum_{i=1}^{n+1} . u_{i11} \geq 6+0+0+\ldots+0 = 6$ which gives a contradiction.

Therefore $|u_{ijk}| < 6$ for all i =1,…,n+1; j =1,…,m+1 and k = 1,…,p+1.

Remark 2. From the Proposition 2, we can deduce that all Voronoirelevant vectorsof $A_n \otimes A_m \otimes A_p$ must lie in X = $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}^{(n+1)(m+1)(p+1)} \cap (A_n \otimes A_m \otimes A_p)$. As for the case of two root lattices we have determined the set of coordinates of the Voronoirelevant vector in $A_n \otimes A_m$ but the characterization of its elements according to a certain subgraphs ofthecompletedirectedtripartitegraph $K_{n+1,m+1,p+1}=(V,E)$ isverydifficult.Thisisthereason why,we will use the associativity of the lattice of type A and the results obtained by LéoDucas and WesselvanWoerdenin [5]tosolveCVPinthetensorproductofmorethantwolatticesoftype A.

Sincethetensorproductsof $A_{(n+1)(m+1)-1} \otimes A_p$ and $A_{n+1} \otimes A_{(m+1)(p+1)-1}$ areusedtosolveCVP in $A_n \otimes A_m \otimes A_p$,thefollowingpropositiongivesusthecharacterizationoftheVoronoirelevant vector in $A_{(n+1)(m+1)-1} \otimes A_p$.

Proposition3.(Voronoirelevantvectorsof $A_{(n+1)(m+1)-1} \otimes A_p$ and $A_n \otimes A_m \otimes A_p$)

Now consider X = {-1,0,1}. The Voronoi relevant vectors of $A_{(n+1)(m+1)-1} \otimes A_p$ are precisely all u∈ X \{0} such that G_u consists of a simple cycle.

The Voronoi relevant vectors of $A_n \otimes A_m \otimes A_p$ are also precisely all s∈ X \{0} such that G_s consists of a simple cycle.

Proof. Just use (Theorem 2, [5]) and associativity.

Since G_u and G_s areconnectedandthattheindegreeofeachnodeisexactly1, wecanjust thatthewholegraphconsistsofasingledirectedsimplecycle.

From Theorem 2, [5]we can deduce that the number ofVoronoi relevant vectors of $A_n \otimes A_m \otimes A_p$ is equal to:

$$\sum_i \binom{(n+1)(m+1)}{i} \binom{p+1}{i} . i!. (i-1)!$$

Where i = 2,…,min{(n+1)(m+1) , (p+1)}.

Finding the closest vectorin $A_n \otimes A_m \otimes A_p$

The Voronoirelevantvectorsof $A_n \otimes A_m \otimes A_p$ beingcharacterized,wewillinthefollowing present a polynomial algorithm allowing solving CVP in this type of lattice.

Lemma 2. Let x∈ $A_n \otimes A_m \otimes A_p$, and let t∈span($A_n \otimes A_m \otimes A_p$) be our target. If there exists a Voronoi relevant vector u∈RV($A_n \otimes A_m \otimes A_p$) such that ||(x+u)-t|| < ||x-t|| we can find such a Voronoi relevant vector in O(((n+1)(m+1)-1+p)((n+1)(m+1)-1)p) operations. If it doesn't exist this will be directed by algorithm.

Proof. Just use (Lemmas 3 and 8, [5]) and associativity.

Remark 3. Let $b^{ijk} \in A_n \otimes A_m \otimes A_p$ be given by: $b^{ijk}_{i,j,k} = b^{ijk}_{i,j+1,k+1} = b^{ijk}_{i+1,j,k+1} = b^{ijk}_{i+1,j+1,k} = 1$; $b^{ijk}_{i,j,k+1} = b^{ijk}_{i,j+1,k} = b^{ijk}_{i+1,j,k} = b^{ijk}_{i+1,j+1,k+1} = -1$ and 0 otherwise for all i =1,…,(n+1); j =1,..,(m+1) and k=1,…,p+1. Note that B = $\{b^{ijk}$: i =1,…,(n+1); j =1,..,(m+1) and k=1,…,p+1} is a basis of $A_n \otimes A_m \otimes A_p$. Because the basis B is so sparse we can efficiently encode elements in this basis.

Lemma 3. For any t∈span($A_n \otimes A_m \otimes A_p$), we can find an x∈ $A_n \otimes A_m \otimes A_p$ such that

$||x-t|| \leq 2\sqrt{(n+1)(m+1)(p+1)}$ in O(((n+1)(m+1)-1)p)) operations.

Proof. Just use (Lemmas 7, [5]) and associativity.

In Lemma 5, if $\sum_{ij} a_{ij} b^{ij} \in$ span($A_n \otimes A_m \otimes A_p$)∩($2^{-d}\mathbb{Z}^{(n+1)(m+1)(p+1)}$) from the transformation, it is clear that $a_{ij} \in 2^{-d}\mathbb{Z}$. Since $A_n \otimes A_m \otimes A_p$ has only integer vectors, we can that if $t \in 2^{-d}\mathbb{Z}^{(n+1)(m+1)(p+1)}$ then the squared distance to the targetwill in each iteration improve with at least 2^{-i+1} which exactly what we need to bound the number of iterations.

Algorithm1: ApolynomialCVPalgorithmforthelattice $A_n \otimes A_m \otimes A_p$.

Require: n,m,p,d ≥ 1 andt= $\sum_{ij} a_{ij} b^{ij} \in$ span($A_n \otimes A_m \otimes A_p$). with $a_{ij} \in 2^{-d}\mathbb{Z}$.

Ensure: a closest vector **x** to **t** in $A_n \otimes A_m \otimes A_p$.

```
Find(a_qr)_q,r, such that t = Σ_qr a_qr b^qr ;
a := Σ_qr ⌊a_qr⌉ b^qr , b := a ;
for i=1,…, d (outer loop) do
    t_i := Σ_qr 2^-i ⌊2^-i a_qr⌉ b^qr ;
    construct weighted K_(n+1)(m+1),(p+1) (with u := a - t_i);
    construct weighted K_(n+1),(m+1)(p+1) (with s := a - t_i);
    while K_(n+1)(m+1),(p+1)(a - t_i) has a negative cycle G_u do (inner loop)
    a := a+u;
    x_i := a ;
    while K_(n+1),(m+1)(p+1)(a - t_i) has a negative cycle G_s do (inner loop)
    b := b+u;
    y_i := a;
    if ||x_d – t|| < || y – t|| then
    x_d is a closest vector to t;
        else
    y_d is a closest vector to t;
```

Proposition 4. Given a target $t=\sum_{ij} a_{ij}\, b^{ij} \in \mathrm{span}(A_n \otimes A_m \otimes A_p)$. with $a_{ij} \in 2^{-d}\mathbb{Z}$ and with $d \geq 1$ we can find a closest vector to t in $A_n \otimes A_m \otimes A_p$ in $O(d.((n+1)(m+1)-1)p)^2 \min\{(n+1)(m+1)-1),p\})$ arithmetic operations with the previous algorithm.

Proof. Just use (Theorem 3, [5]) and associativity.

Remark 4. In general, the optimal parenthesis would be that which contains the vector $(A_n \otimes A_m \otimes A_p)$. This means that we could first check if the vector $t \in \mathrm{span}(A_n \otimes A_m \otimes A_p)$. This means that we could first check if the vector t is either in $\mathrm{span}(A_n \otimes A_{(m+1)(p+1)-1})$ or in $\mathrm{span}(A_{(n+1)(m+1)1} \otimes A_p)$, and this will allow us to gain in a good number of operations. Note also that the search for this optimal parenthesis becomes more complex when the number of lattices increases.

IV. Closest Vector Problem in $A_{n1} \otimes A_{n2} \otimes ... \otimes A_{nk}$

According to the previous remark, we can generalize the resolution of CVP in the tensor product of k root lattices of type A.

Let k lattices $A_{n1}, ..., A_{nk}$ of type A.

Definition 9. Let $n_1, ..., n_k \geq 1$, be k positives integers that are not all zero. We call root lattice $A_{n_1} \otimes A_{n_2} \otimes ... \otimes A_{n_k} \subset \mathbb{Z}^{(n1+1)...(nk+1)}$ of rank $n_1.n_2...n_k$ all of the elements

$x = (x_{11\ldots1}, x_{11\ldots1(nk+1)}, x_{121\ldots1}, \ldots, x_{(n1+1)\ldots(nk+1)} \in \mathbb{Z}^{(n1+1)...(nk+1)}$ satisfying conditions:

- $\sum_{i^{(1)}=1}^{n_1+1} x_{i^{(1)} i^{(2)} \ldots i^{(k)}} = 0$ for $i^{(2)} = 1,\ldots,n_2+1;\ \ldots;\ i^{(k)} = 1,\ldots,n_k+1$
- $\sum_{i^{(2)}=1}^{n_2+1} x_{i^{(1)} i^{(2)} \ldots i^{(k)}} = 0$ for $i^{(2)} = 1,\ldots,n_1+1;\ \ldots;\ i^{(k)} = 1,\ldots,n_k+1$
- …….. …… …….. ……………………
- $\sum_{i^{(k)}=1}^{n_k+1} x_{i^{(1)} i^{(2)} \ldots i^{(k)}} = 0$ for $i^{(1)} = 1,\ldots,n_1+1;\ \ldots;\ i^{(k-1)} = 1,\ldots,n_{(k-1)}+1$

We will use the indices $i^{(1)},\ldots,i^{(k)}$ throughout this section.

We note that by gradually regrouping these lattices, and two by two, and by using the associativity of the tensor product, solving CVP in $A_{n1} \otimes A_{n2} \otimes ... \otimes A_{nk}$ amounts to solving the same problem in $(A_{n1} \otimes A_{n2}) \otimes A_{n3} \otimes ... \otimes A_{nk}$.

Step by step, solving CVP in $A_{n1} \otimes A_{n2} \otimes ... \otimes A_{nk}$ could be reduced to solving it in $A_{n1} \otimes A_{(n2+1)\ldots(nk+1)-1}$, or in $A_{(n1+1)(n2+1)-1} \otimes A_{(n3+1)\ldots(nk+1)-1}$, or in …

Thus, we will have several sublattices when the number k is large. Therefore, the closest vector associated to the vector associated with the lattice will be quite simply be the one whose norm will be smallest among all the vectors which will be determined in the aforementioned lattices. The previous section illustrates well the case for k=3.

V. Conclusion

In this project, we have shown that we can use the optimal parenthesis to solve the closest vector problem in the tensor product of three root lattices of type A; and this optimal parenthesis could also allow to generalize this resolution in the case of a finite number of root lattices of type A, this having previously solved the problem of optimal parenthesis which becomes complex when the numbers of root lattices becomes large.

In our future work, we will use the characterization of the Voronoi relevant vectors and the oriented complete k –graphs to solve CVP in the tensor product of k lattices of type A

References

[1]. D.Aggarwal,D.Dadush,N.Stephens-Davidowitz,Solvingtheclosestvectorproblemin2^ntime-thediscrete gaussian strikes again,2015.
[2]. R.K.Ahuja,T.L.Magnanti,J.B.OrlinNetworkFlows:Algorithms,andApplications.,UpperSadldeRiver,NJ, USA: Prentice-Hall.,1993.
[3]. J. H. Conway, N. J. A. Sloane, Sphere packings, lattices and groups, Grundlehren der mathematischenWis-senschaften,SpringerNewYork,1998.
[4]. T.H.Cormen,C.E.Leiserson,R.L.Rivest,C.Stein,Introductiontoalgorithms,TheMITPress,3rded.,2009.
[5]. L. Ducas, W. P. J. van Woerden, The closest vector problem in tensored root lattices of type A and their duals, Des.CodesCryptogr.,2017.
[6]. O. Golddreich, S. Goldwasser, S. Halevi, Public-key cryptosystems from lattice reduction problems, Crypto 97, LectureNotesincomputerscience294,(1997),112–131.
[7]. V.Lyubashevsky,C.Peikert,O.RegevOnidealLatticesandLearningwithErrors over Rings,2010,1–23.
[8]. R.G.McKilliam,A.J.Grant,I.V.L.ClarksonFindingaclosestpointinalatticeofvoronoi'sfirstkind,2014.
[9]. D.MicciancioLatticealgorithmsandapplications,UniversityofCalifornia,SanDiego,Spring2014.
[10]. D. Micciancio, P. Voulgaris, A deterministic single exponential time algorithm for most lattice problems based onvoronoicellcomputations,inproceedingsoftheForty-secondACMsymposiumonTheoryofComputing,STOC'10, 2010, 351–358.
[11]. H. Napias, A generalization of the LLL-algorithm over euclidean rings or orders, Journal de Théorie deNom-bresdeBordeaux,**8**.(1996),387–396.
[12]. P. W. Shor, Polynomial time algorithms for prime factorization and discete logarithms on a quantum computer, SIAMJ.computing**26**(1997)1484–1509.
[13]. D. Stehle, Algorithme de réduction de réseaux et application à la recherche de pires des cas pour l'arrondi de fonctionsmathématiques,Thèsededoctoratsoutenuele2décembre2005,àl'UniversitéHenriPoincarré- Nancy 1,France.
[14]. W. P. J. van Woerden, The closest vector problem in cyclotomic lattices, Bachelor thesis, in Mathematicalinsti-tute,LeidenUniversity,24june2016.

Arnaud GirèsFobassoTchinda, et. al. "The closest vector problem in some lattices of type A."*IOSR Journal of Mathematics (IOSR-JM)*, 16(3), (2020): pp. 26-32.