On the Optimality of Gauss's Algorithm over Euclidean Imaginary Quadratic Fields

Christian Porter Department of EEE Imperial College London London, SW7 2AZ, United Kingdom Email: c.porter17@imperial.ac.uk Shanxiang Lyu College of Cyber Security Jinan University Guangzhou 510632, China Email: s.lyu14@imperial.ac.uk Cong Ling Department of EEE Imperial College London London, SW7 2AZ, United Kingdom Email: c.ling@imperial.ac.uk

Abstract—In this paper, we continue our previous work on the reduction of algebraic lattices over imaginary quadratic fields for the special case when the lattice is spanned over a two dimensional basis. In particular, we show that the algebraic variant of Gauss's algorithm returns a basis that corresponds to the successive minima of the lattice in polynomial time if the chosen ring is Euclidean.

I. INTRODUCTION

Lattice reduction algorithms over algebraic number fields have attracted great attention in recent years. In network information theory, efficient techniques for finding the network coding matrices in compute-and-forward boil down to designing a lattice reduction algorithm where the direct-sums are defined by the space of codes [1]–[3]. In cryptography, analyzing the bit-level security of ideal lattice based NTRU or fully homomorphic encryption schemes through a sub-field algorithm has been shown effective [4], [5].

Since the Lenstra-Lenstra-Lovász (LLL) algorithm is one of the most celebrated lattice reduction algorithms to date, its extension from over real/rational space to higher dimensional space has been studied extensively. Napias first generalised the LLL algorithm to lattices spanned over imaginary quadratic rings and certain quaternion fields [6]; later Fieker, Pohst and Stehle investigated more fundamental properties of algebraic lattices [7], [8]. Recently Kim and Lee proposed an efficient LLL algorithm over bi-quadratic field whose quantization step requires a Euclidean domain [4], while our work on LLL over imaginary quadratic fields showed that a Euclidean domain is needed to make the algorithm convergent [9].

As a special case of the LLL algorithm for (real/rational) lattices over two dimensions, conventional Gauss's algorithm has been proved to return the two vectors corresponding to the successive minima of the lattice [10]. However, the algebraic analog of Gauss's algorithm, has not, so far, been analyzed. It remains unknown whether the algebraic Gauss's algorithm possesses the optimality properties as its counter-part.

To address this issue, we take a modest step to investigate Gauss's algorithm over Imaginary Quadratic Fields. When the ring of integers is a Euclidean domain, we prove that Gauss's algorithm returns a basis corresponding to the successive minima of an algebraic lattice. This result is further explained through numerical examples. Specifically, we show how the algorithm finds the two successive minima when the domain is Euclidean, and how the algorithm fails to work when it is non-Euclidean.

II. PRELIMINARIES

We begin by defining some familiar concepts in algebraic number theory and lattice theory. Let K be a complex quadratic extension of \mathbb{Q} , i.e. $K = \mathbb{Q}(\sqrt{-d})$ for some positive square-free integer d that is not equal to 1. Then recall the ring of integers of K (maximal order), \mathcal{O}_K , is $\mathbb{Z}[\xi]$, where

$$\xi = \begin{cases} \sqrt{-d} & \text{if } -d \equiv 2,3 \mod 4, \\ \frac{1+\sqrt{-d}}{2} & \text{if } -d \equiv 1 \mod 4. \end{cases}$$

Definition II.1. A field K is said to be *norm-Euclidean* if, for all $x \in K$, there exists $q \in \mathcal{O}_K$ its ring of integers such that

$$|\operatorname{Norm}_{K/\mathbb{Q}}(x-q)| < 1,$$

where Norm_{K/\mathbb{Q}} denotes the algebraic norm of K. We denote the value $\mathcal{M}(K) := \max_{x \in K} \min_{q \in \mathcal{O}_K} |\operatorname{Norm}_{K/\mathbb{Q}}(x-q)|$ the *Euclidean minimum* of K.

Proposition 1. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with ring of integers \mathcal{O}_K . Then we have

$$\mathcal{M}(K) = \begin{cases} \frac{1+d}{4} & \text{if } -d \equiv 2, 3 \mod 4, \\ \frac{(1+d)^2}{16d} & \text{if } -d \equiv 1 \mod 4. \end{cases}$$

Hence, K *is norm-Euclidean if and only if* $d \in \{1, 2, 3, 7, 11\}$.

For imaginary quadratic fields, we may analytically extend the norm function to all complex numbers using the absolute value. Moreover, we have $\max_{x \in K} \min_{q \in \mathcal{O}_K} |\operatorname{Norm}_{K/\mathbb{Q}}(x - q)| = \max_{x \in \mathbb{C}} \min_{q \in \mathcal{O}_K} |x - q|^2$ as the maximum distance with respect to the absolute value is achieved at a rational point. We say that $x \in \mathbb{C}$ is fully $\mathbb{Z}[\xi]$ -reduced if $|x| \leq |x - q|$ for all $q \in \mathbb{Z}[\xi]$.

Lemma 1. Let $x \in \mathbb{C}$ be fully $\mathbb{Z}[\xi]$ -reduced. Then $|\Re(x)| \leq 1/2, |\Im(x)| \leq \sqrt{d}/2$ if $\xi = \sqrt{-d}$ or $|\Re(x)| \leq 1/2, |\Im(x)| \leq \frac{1}{\sqrt{d}} \left(-|\Re(x)| + \frac{1+d}{4}\right)$ if $\xi = \frac{1+\sqrt{-d}}{2}$.



Fig. 1. Left: lattice generated by $\mathbb{Z}[\sqrt{-2}]$, tesselated by rectangles, Right: lattice generated by $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$, tesselated by "stretched" hexagons.

Proof. Define the map $\phi(x + iy) = (x, y)$ for all $x + iy \in$ \mathbb{C} . Then |x + iy| = ||(x, y)||. When $-d \equiv 2, 3 \mod 4$, $\mathbb{Z}[\xi]$ generates the lattice with basis $(1,0), (0,\sqrt{d})$, otherwise $\mathbb{Z}[\xi]$ generates the lattice with basis $(1,0), (1/2, \sqrt{d}/2)$. The bounds that form the fundamental region of these lattices correspond to the bounds given in the proposition (see fig. 1 for reference).

A $\mathbb{Z}[\xi]$ -module Λ is an abelian group with a binary operation over $\mathbb{Z}[\xi]$ that satisfies the axioms of scalar multiplication. In general, modules need not have a basis, and those that are are denoted free modules. A subset of Λ forms a basis for Λ if the basis is linearly independent over $\mathbb{Z}[\xi]$ and also spans Λ over $\mathbb{Z}[\xi]$. We denote discrete free $\mathbb{Z}[\xi]$ -submodules of \mathbb{C}^n algebraic lattices. Algebraic lattices can be expressed by a basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ whose linear sum with scalar multiplication over $\mathbb{Z}[\xi]$ span Λ .

Definition II.2. The *j*th successive minima of an algebraic lattice is the smallest such number λ_j such that the ball of radius λ_i (under an appropriate norm) contains j linearly independent lattice vectors over $\mathbb{Z}[\xi]$.

A. Classical Gauss's algorithm

Aside from Euclid's famous greatest divisor algorithm, Gauss's lattice reduction algorithm is one of the first examples of a lattice reduction algorithm. Gauss defined the notion of a reduced basis over two dimensions as the following.

Definition II.3. An ordered basis $\{\mathbf{b}_1, \mathbf{b}_2\} \in \mathbb{R}^n$ of a two dimensional lattice is reduced if $\|\mathbf{b}_1\| \le \|\mathbf{b}_2\| \le \|\mathbf{b}_2 + p\mathbf{b}_1\|$ for all $p \in \mathbb{Z}$.

The following algorithm returns a reduced basis in the sense of Gauss. Notice we get a basis whose Gram-Schmidt coefficients round to zero, as such $|\mu_{12}|, |\mu_{21}| \leq 1/2$. Then taking an arbitrary vector in the lattice $\mathbf{v} = x\mathbf{b}_1 + y\mathbf{b}_2$ where $x, y \in \mathbb{Z}$, we get

$$\|\mathbf{v}\|^{2} = x^{2} \|\mathbf{b}_{1}\|^{2} + 2xy \langle \mathbf{b}_{1}, \mathbf{b}_{2} \rangle + y^{2} \|\mathbf{b}_{2}\|^{2}$$

$$\geq x^{2} \|\mathbf{b}_{1}\|^{2} - |xy| \|\mathbf{b}_{1}\|^{2} + y^{2} \|\mathbf{b}_{1}\|^{2}$$

$$= (x - y)^{2} \|\mathbf{b}_{1}\|^{2} + |xy| \|\mathbf{b}_{1}\|^{2}.$$

input : An ordered basis $\{\mathbf{b}_1, \mathbf{b}_2\} \in \mathbb{R}^n$ of a two dimensional lattice spanned over \mathbb{Z} .

output: A Gauss reduced basis.

while $\|\mathbf{b}_1\| < \|\mathbf{b}_2\|$ do $\mu_{12} = \langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \| \mathbf{b}_1 \|^2;$ $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu_{12} \rceil \mathbf{b}_1 ;$ swap $\mathbf{b_1}, \mathbf{b_2}$ end

If x is nonzero, since $(x-y)^2$, $|xy| \in \mathbb{N}$ and at least one must be nonzero, b_1 must be the shortest vector. If y is nonzero, letting $f(x, y) = (x - y)^2 + |xy|$ we have

$$\begin{aligned} \|\mathbf{v}\|^2 &= y^2 (\|\mathbf{b}_2\|^2 - \|\mathbf{b}_1\|^2) \\ &+ (x^2 + y^2) \|\mathbf{b}_1\|^2 + 2xy \langle \mathbf{b}_1, \mathbf{b}_2 \rangle \\ &\geq y^2 (\|\mathbf{b}_2\|^2 - \|\mathbf{b}_1\|^2) + f(x, y) \|\mathbf{b}_1\|^2 \\ &\geq (y^2 - 1) (\|\mathbf{b}_2\|^2 - \|\mathbf{b}_1\|^2) + \|\mathbf{b}_2\|^2, \end{aligned}$$

and since y is nonzero, $y^2 - 1 \ge 0$ so \mathbf{b}_2 corresponds to the second successive minima for the lattice.

III. ALGEBRAIC LATTICE REDUCTION IN TWO DIMENSIONS

For our work, we use the complex Euclidean (l_2) norm to measure the length of lattice vectors and the regular complex inner product. Unlike algebraic lattices spanned over other rings, we do not need to embed the ring structure before measuring the norm, as the Euclidean norm already takes the complex conjugate into account. Define the quantisation function $q_K : \mathbb{C} \to \mathbb{Z}[\xi]$ such that $q_K(x) = \arg \min_{\mu \in \mathbb{Z}[\xi]} |x - \mu|$. A specific definition of how the quantisation function works can be found in [9].

Lagrange and Gauss have given the reduction criteria for a two dimensional real basis. We first generalize this criteria to over complex quadratic rings.

Definition III.1. A basis $\mathbf{b}_1, \mathbf{b}_2 \in \mathbb{C}^n$ is Gauss reduced if $\|\mathbf{b}_1\| \le \|\mathbf{b}_2\| \le \|\mathbf{b}_2 + p\mathbf{b}_1\|$ for all $p \in \mathbb{Z}[\xi]$.

The following algorithm, which is a special case of algebraic LLL in two dimensions, computes a Gauss reduced basis.

input : An ordered basis $\{\mathbf{b}_1, \mathbf{b}_2\} \in \mathbb{C}^n$ of a two dimensional algebraic lattice $\boldsymbol{\Lambda}$ and a relevant ring $\mathbb{Z}[\xi]$ that we want to reduce the basis over.

output: A Gauss reduced basis.

while $\|\mathbf{b}_1\| < \|\mathbf{b}_2\|$ do $\mu_{12} = \langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \|\mathbf{b}_1\|^2;$ $\mathbf{b}_2 = \mathbf{b}_2 - q_K(\mu_{12})\mathbf{b}_1$; swap $\mathbf{b_1}, \mathbf{b_2}$

end

Theorem 2. Let $\mathbf{b}_1, \mathbf{b}_2$ be an output basis of the algorithm above. Then $\|\mathbf{b}_1\| = \lambda_1, \|\mathbf{b}_2\| = \lambda_2$ if $\mathbb{Z}[\xi]$ is the ring of integers of a norm-Euclidean domain (i.e., d = 1, 2, 3, 7, 11).

Proof. We first show that the Gram-Schmidt coefficients are fully $\mathbb{Z}[\xi]$ -reduced, i.e. the GS coefficients of the output basis are rounded to zero. Let \mathbf{b}_2 be the input vector in the last run of the algorithm before $\mathbf{b}_2, \mathbf{b}_1$ are output as the reduced basis, and let μ_{12} be the GS coefficient between $\mathbf{b}_1, \mathbf{b}_2$. Then $q_K(\langle \mathbf{b}_1, \mathbf{b}_2 \rangle / \|\mathbf{b}_1\|^2) = q_K(\frac{1}{\|\mathbf{b}_1\|^2}(\langle \mathbf{b}_1, \mathbf{b}_2 \rangle - q_K(\mu_{12})\|\mathbf{b}_1\|^2)) = q_K(\epsilon)$, where $\epsilon = \mu_{12} - q_K(\mu_{12})$ has already been fully reduced, by the definition of the quantisation function. Since no swap has occurred (since the basis has been output), $\|\mathbf{b}_1\| \leq \|\mathbf{b}_2\|$ so the same argument follows for the GS coefficient between $\mathbf{b}_2, \mathbf{b}_1$.

To prove that $\|\mathbf{b}_1\| = \lambda_1$, we denote an arbitrary lattice vector $\mathbf{v} = p_1\mathbf{b}_1 + p_2\mathbf{b}_2$ where $p_1, p_2 \in \mathbb{Z}[\xi]$, and analyze its norm function:

$$\|\mathbf{v}\|^{2} = |p_{1}|^{2} \|\mathbf{b}_{1}\|^{2} + |p_{2}|^{2} \|\mathbf{b}_{2}\|^{2} + 2\Re(\overline{p_{1}}p_{2}\langle\mathbf{b}_{1},\mathbf{b}_{2}\rangle).$$
(1)

We examine the cases $-d \equiv 1, 2 \mod 4$ and $-d \equiv 3 \mod 4$ separately. When the chosen ring is in the form of $\xi = \sqrt{-d}$, we let $p_1 = x + y\sqrt{-d}$, $p_2 = z + w\sqrt{-d}$ where $x, y, z, w \in \mathbb{Z}$. Then $\overline{p_1}p_2 = (xz + dyw) + \sqrt{-d}(xw - yz)$, and

$$2\Re(\overline{p_1}p_2\langle \mathbf{b}_1, \mathbf{b}_2\rangle) = 2(xz + dyw)\Re(\langle \mathbf{b}_1, \mathbf{b}_2\rangle) - 2\sqrt{d}(xw - yz)\Im(\langle \mathbf{b}_1, \mathbf{b}_2\rangle).$$

Since the GS coefficients are fully reduced, we have:

$$\begin{cases} 2(xz + dyw)\Re(\langle \mathbf{b}_1, \mathbf{b}_2 \rangle) \ge -|xz + dyw| \|\mathbf{b}_1\|^2,\\ -2\sqrt{d}(xw - yz)\Im(\langle \mathbf{b}_1, \mathbf{b}_2 \rangle) \ge -d|xw - yz| \|\mathbf{b}_1\|^2. \end{cases}$$

Based on this, the r.h.s. of Eq. (1) can be lower bounded:

$$\|\mathbf{v}\|^2 \ge Q_1'(x, y, z, w) \|\mathbf{b}_1\|^2, \tag{2}$$

where

$$Q'_{1}(x, y, z, w) \triangleq (x^{2} + dy^{2} + z^{2} + dw^{2} - |xz + dyw| - d|xw - yz|).$$

Letting $Q_1(x, y, z, w) \triangleq (x^2 + dy^2 + z^2 + dw^2 - (xz + dyw) - d(xw - yz))$, we note that the codomain of Q'_1 is a subset of the codomain of Q_1 (this can be seen by changing the signs of x, y, z, w around until the functions are equivalent), showing positive-definiteness of Q_1 immediately yields that Q'_1 is also positive-definite. The 4-D symmetric matrix w.r.t. quadratic form $Q_1(x, y, z, w)$ can be written as

$$\mathbf{Q}_{1} = \begin{bmatrix} 1 & 0 & -\frac{1}{2} & -\frac{d}{2} \\ 0 & d & \frac{d}{2} & -\frac{d}{2} \\ -\frac{1}{2} & \frac{d}{2} & 1 & 0 \\ -\frac{d}{2} & -\frac{d}{2} & 0 & d \end{bmatrix}.$$

The four eigenvalues of \mathbf{Q}_1 are:

$$\begin{array}{c} \frac{d-\sqrt{5d^2-6d+9}+3}{4}, \\ \frac{d+\sqrt{5d^2-6d+9}+3}{4}, \\ \frac{3d-\sqrt{13d^2-6d+1}+1}{4}, \\ \frac{3d+\sqrt{13d^2-6d+1}+1}{4}. \end{array}$$

We therefore conclude that \mathbf{Q}_1 has four positive eigenvalues and hence being positive definite with only d = 1, 2 in this case. Along with $Q(x, y, z, w) \in \mathbb{Z}$, we arrive at $\|\mathbf{v}\|^2 \ge$ $\|\mathbf{b}_1\|^2$ when d = 1, 2.

When the chosen ring is in the form of $\xi = \frac{1+\sqrt{-d}}{2}$, like before, letting $p_1 = x + y \frac{1+\sqrt{-d}}{2}$, $p_2 = z + w \frac{1+\sqrt{-d}}{2}$, we have $\overline{p_1}p_2 = (xz+1/2(yz+xw) + \frac{1+d}{4}yw) + (\sqrt{-d}/2)(xw-yz)$. Then

$$2\Re(\overline{p_1}p_2\langle \mathbf{b}_1, \mathbf{b}_2\rangle) = 2(xz + 1/2(yz + xw) + \frac{1+d}{4}yw)\Re(\langle \mathbf{b}_1, \mathbf{b}_2\rangle) - \sqrt{d}(xw - yz)\Im(\langle \mathbf{b}_1, \mathbf{b}_2\rangle).$$

Using the following inequality from the "fully-reduced" constraints:

$$|\Im(x)| \le \frac{1}{\sqrt{d}} \left(-|\Re(x)| + \frac{1+d}{4} \right),$$

similarly to before, we obtain the inequality

$$\begin{aligned} \|\mathbf{v}\|^2 &\geq (x^2 + xy + \frac{1+d}{4}y^2 + z^2 + zw + \frac{1+d}{4}w^2 \\ &- \frac{1+d}{4}|xw - yz|)\|\mathbf{b}_1\|^2 - |\Re(\langle \mathbf{b}_1, \mathbf{b}_2 \rangle)| \\ &\times (|2xz + \frac{1+d}{2}yw + xw + yz| - |xw - yz|). \end{aligned}$$

Focusing on the term $(|2xz + \frac{1+d}{2}yw + xw + yz| - |xw - yz|)$, we note that one of the xw, yz on the left hand term must annihilate with one on the right hand term, and one must sum to two times the variable (the choice of which does not matter for our case, as the overall function is symmetric in xw, yz). We choose xw to annihilate and yz to coalesce. Then clearly, all terms whose coefficient is $|\Re(\langle \mathbf{b}_1, \mathbf{b}_2 \rangle)|$ are negative, so the minimum is achieved at $|\Re(\langle \mathbf{b}_1, \mathbf{b}_2 \rangle)| = 1/2 ||\mathbf{b}_1||^2$. Once again, to show the above is greater than or equal to $||\mathbf{b}_1||^2$ for all x, y, z, w, we construct a "larger" quadratic form, $Q_2(x, y, z, w)$, and show its positive-definiteness, where:

$$Q_{2}(x, y, z, w) \triangleq (x^{2} + xy + \frac{1+d}{4}y^{2} + z^{2} + zw) + \frac{1+d}{4}w^{2} - \frac{1+d}{4}xw + \left(\frac{1+d}{4} - 1\right)yz - xz - \frac{1+d}{4}yw.$$

The symmetric matrix w.r.t. the quadratic form $Q_2(x, y, z, w)$ and its corresponding eigenvalues are respectively:

$$\mathbf{Q}_{2} = \begin{bmatrix} 1 & 1/2 & -\frac{1}{2} & -\frac{1+a}{8} \\ 1/2 & \frac{1+d}{4} & \frac{1}{2}\left(\frac{1+d}{4}-1\right) & -\frac{1+d}{8} \\ -\frac{1}{2} & \frac{1}{2}\left(\frac{1+d}{4}-1\right) & 1 & 1/2 \\ -\frac{1+d}{8} & -\frac{1+d}{8} & 1/2 & \frac{1+d}{4} \end{bmatrix},$$

$$\left\{ \begin{array}{l} \frac{2D+2-\sqrt{9D^2-10D^3+10-4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}-\sqrt{D^2-2D+2}}{4},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10-4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}-\sqrt{D^2-2D+2}}{4},\\ \frac{2D+2-\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}+\sqrt{D^2-2D+2}}{4},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}+\sqrt{D^2-2D+2}}{4},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}+\sqrt{D^2-2D+2}}{4},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}+\sqrt{D^2-2D+2}}{4},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}+\sqrt{D^2-2D+2}}{4},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}}+\sqrt{D^2-2D+2}}{4},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}}+\sqrt{D^2-2D+2}}{2},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}}+\sqrt{D^2-2D+2},\\ \frac{2D+2+\sqrt{9D^2-10D^3+10+4\frac{D^3-D^2+2}{\sqrt{D^2-2D+2}}}}+\sqrt{D^2-2D+2},\\ \frac{2D+2+\sqrt{D^2-2D+2}}{\sqrt{D^2-2D+2}},\\ \frac{2D+2+\sqrt{D^2-2D+2}{\sqrt{D^2-2D+2}},\\ \frac{2D+2+\sqrt{D^2-2D+2}}{\sqrt{D^2-2D+2}},\\ \frac{2D+2+\sqrt{D^2-2D+2}{\sqrt{D$$

where $D = \frac{1+d}{4}$. Through checking the eigenvalues, it shows that \mathbf{Q}_2 is positive definite when d = 3, 7, 11; therefore $\|\mathbf{v}\|^2 \ge \|\mathbf{b}_1\|^2$ is reached.

To prove that $\|\mathbf{b}_2\| = \lambda_2$, we leverage the technique in [11]. For both cases of ξ , we construct a vector $p_1\mathbf{b}_1 + p_2\mathbf{b}_2$ with $p_1, p_2 \in \mathbb{Z}[\xi], p_2 \neq 0$. When the chosen ring is in the form of $\xi = \sqrt{-d}$, we have

$$\begin{aligned} &|p_{1}\mathbf{b}_{1}+p_{2}\mathbf{b}_{2}\|^{2}=|p_{2}|^{2}(\|\mathbf{b}_{2}\|^{2}-\|\mathbf{b}_{1}\|^{2})\\ &+(|p_{1}|^{2}+|p_{2}|^{2})\|\mathbf{b}_{1}\|^{2}+2\Re(\overline{p_{1}}p_{2}\langle\mathbf{b}_{1},\mathbf{b}_{2}\rangle)\\ &\geq |p_{2}|^{2}(\|\mathbf{b}_{2}\|^{2}-\|\mathbf{b}_{1}\|^{2})+Q_{1}(x,y,z,w)\|\mathbf{b}_{1}\|^{2}\\ &\geq (|p_{2}|^{2}-1)(\|\mathbf{b}_{2}\|^{2}-\|\mathbf{b}_{1}\|^{2})+\|\mathbf{b}_{2}\|^{2}\\ &\geq \|\mathbf{b}_{2}\|^{2}.\end{aligned}$$

This shows \mathbf{b}_2 is the shortest lattice vector that is independent of \mathbf{b}_1 . The proof for the case $\xi = \frac{1+\sqrt{-d}}{2}$ follows the same way by replacing $Q_1(x, y, z, w)$ with $Q_2(x, y, z, w)$.

IV. NUMERICAL EXAMPLES

Example 1 (Euclidean domain). Consider the field $K = \mathbb{Q}(\sqrt{-3})$ and its maximal ring of integers $\mathbb{Z}[\omega]$. Suppose the input lattice basis is

$$\mathbf{B} = \left[\begin{array}{cc} 4+\omega & 1+4\omega \\ -1+5\omega & 1+2\omega \end{array} \right]$$

The algebraic reduction on this basis will consist of a swap, a size reduction, and another swap, to yield the reduced basis

$$\tilde{\mathbf{B}} = \begin{bmatrix} -3 + 3\omega & 1 + 4\omega \\ 2 - 3\omega & 1 + 2\omega \end{bmatrix},$$

which satisfies $\|\tilde{\mathbf{b}}_1\|^2 = \lambda_1^2 = 16$, and $\|\tilde{\mathbf{b}}_2\|^2 = \lambda_2^2 = 28$. On the contrary, if we turn **B** into a real basis and perform real LLL (whose Lovasz's parameter is 1) on it, the square norm of the reduced vectors are respectively 16, 16, 31, and 28. In its reduced basis, the first two vectors are not independent over K, and the second shortest vector is in the last position. In this scenario only the Minkowski reduction on the real basis can have the same effect as our algebraic lattice reduction, whose reduced vectors respectively have square norms 16, 16, 28, and 28.

Example 2 (non-Euclidean domain). Consider the field $K = \mathbb{Q}(\sqrt{-5})$ and its maximal ring of integers $\mathbb{Z}[\sqrt{-5}]$. By Proposition 1, this field is an example of a non-norm Euclidean field. We begin with the following basis:

$$\mathbf{B} = \begin{bmatrix} 2+3\sqrt{-5} & 8+\sqrt{-5} \\ 2+\sqrt{-5} & 2 \end{bmatrix}.$$

Performing algebraic reduction on this basis consists of a single size reduction, resulting in the basis

$$\tilde{\mathbf{B}} = \begin{bmatrix} 2+3\sqrt{-5} & 6-2\sqrt{-5} \\ 2+\sqrt{-5} & -\sqrt{-5} \end{bmatrix}$$

Such a basis is reduced in the sense of Gauss whose vectors have square lengths of 58 and 61. However, running real LLL over the corresponding four dimensional basis returns reduced vectors with respective square lengths 20, 30, 26, 39. As such, we conclude that the algebraic Gauss's algorithm does not guarantee an output that corresponds to the successive minima of the lattice if the chosen field is not Euclidean.

V. CLOSING REMARKS

In this paper, we have shown that it is possible to successfully build a polynomial time algorithm that returns a basis that corresponds to the successive minima. However, we have not addressed the lattice reduction problem for non-Euclidean imaginary quadratic domains. Indeed, all the quadratic forms listed in this paper become non-positive definite when the respective field is not Euclidean (this can be easily seen by example), however this does not immediately imply that reduction fails over these fields. In our second numerical example, we have shown that our definition of Gauss reduction, although converges to a "reduced" basis, returns a basis that is much larger than the actual successive minima of the lattice. The first question that could be addressed in further research is whether the algorithm is optimal for any lattices spanned over non-Euclidean imaginary quadratic rings, and if not, is it guaranteed that there exists a unimodular transformation that maps any basis to a new basis that corresponds to the successive minima of the lattice. In the event that the answer to the first question is negative and the second is positive, does there exist a modified algorithm (possibly also polynomial time) that is optimal over lattices over the said non-Euclidean ring? Another area to explore is reduction over "trace-Euclidean" domains, i.e. domains where, for all $x \in K$, there exists a $q \in \mathcal{O}_K$ such that $|\operatorname{Trace}_{K/\mathbb{Q}}((x-q)(x-q))| < 1$ (for imaginary quadratic fields, trace-Euclideanity is equivalent to norm-Euclideanity).

REFERENCES

- N. E. Tunali, Y. Huang, J. J. Boutros, and K. R. Narayanan, "Lattices over Eisenstein integers for compute-and-forward," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5306–5321, 10 2015.
- [2] Y. Huang, K. R. Narayanan, and P. Wang, "Lattices over algebraic integers with an application to compute-and-forward," *IEEE Trans. Information Theory*, vol. 64, no. 10, pp. 6863–6877, 2018.
- [3] M. A. V. Castro and F. E. Oggier, "Lattice network coding over euclidean domains," in 22nd European Signal Processing Conference, EUSIPCO 2014, Lisbon, Portugal, September 1-5, 2014, 2014, pp. 1148–1152.
- [4] T. Kim and C. Lee, "Lattice reductions over euclidean rings with applications to cryptanalysis," in *Proc. Cryptography and Coding - 16th IMA International Conference, IMACC, Oxford, UK, 2017*, ser. Lecture Notes in Computer Science, vol. 10655. Springer, 2017, pp. 371–391.
- [5] M. R. Albrecht, S. Bai, and L. Ducas, "A subfield lattice attack on overstretched NTRU assumptions - cryptanalysis of some FHE and graded encoding schemes," in Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 2016, pp. 153–178.

- [6] H. Napias, "A generalization of the LLL-algorithm over euclidean rings or orders," *Journal de Théorie des Nombres de Bordeaux*, vol. 8, no. 2, pp. 387–396, 1996.
- [7] C. Fieker and M. Pohst, "On lattices over number fields," in Algorithmic Number Theory, Second International Symposium, ANTS-II, Talence, France, May 18-23, 1996, Proceedings, ser. Lecture Notes in Computer Science, vol. 1122. Springer, 1996, pp. 133–139.
- [8] C. Fieker and D. Stehlé, "Short bases of lattices over number fields," in Proc. Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, ser. Lecture Notes in Computer Science, vol. 6197. Springer, 2010, pp. 157–173.
- [9] S. Lyu, C. Porter, and C. Ling, "Performance limits of lattice reduction over imaginary quadratic fields with applications to computeand-forward," in *IEEE Information Theory Workshop*, *ITW 2018*, *Guangzhou, China*, 2018.
- [10] D. Micciancio and S. Goldwasser, Complexity of Lattice Problems. Boston, MA: Springer, 2002.
- [11] H. Yao and G. W. Wornell, "Lattice-reduction-aided detectors for MIMO communication systems," in *Proc. Global Telecommunications Conference (GLOBECOM), Taipei, Taiwan, 2002.* IEEE, 2002, pp. 424–428.