WELL-ROUNDED TWISTS OF IDEAL LATTICES FROM IMAGINARY QUADRATIC FIELDS

NAM H. LE, DAT T. TRAN, HA T. N. TRAN

Abstract. In this paper, we investigate the properties of well-rounded twists of a given ideal lattice of an imaginary quadratic field K. We show that every ideal lattice I of K has at least one well-rounded twist lattice. Moreover, we provide an explicit algorithm to compute all well-rounded twists of I.

1. Introduction

A lattice of full rank in a Euclidean space is called *well-rounded* if its set of minimal vectors spans the whole space. Well-rounded lattices are important in discrete optimization, in particular in the study of sphere packing, sphere covering, and kissing number problems [9], as well as in coding theory [1, 2, 6, 7].

A *well-rounded twist* of a lattice is defined in [3]. A method for computing all well-rounded twists of a given ideal lattice I of a real quadratic field K is also presented in this paper. It requires us to compute all principal ideals $\langle x\rangle \subset I$ such that $N(x)^2 \leq N(I)^2\Delta_K/3$ and its generator x where Δ_K is the discriminant of K (see Section 3 in [3]). It is known that finding all ideals of norm bounded and finding a generator of a principal ideal are hard problems, especially when Δ_K is large (see [8]). This method is therefore infeasible and hence one cannot always compute all well-rounded twists of a given ideal lattice I. In contrast, we can show that this task is feasible for an arbitrary imaginary quadratic field K. Indeed, in this paper we prove that every ideal lattice I of K has at least one well-rounded twist lattice (see Proposition 10). This result can be considered as a particular case of the one in [11] which proves that every lattice (in any dimension) has at least a well-rounded twist. However, in our proof, we make use of an independent idea and argument from the ones in [11]. Indeed Proposition 10 is implied from the proofs of Lemma 3 and Theorem 2. We remark that a similar result for real quadratic fields has not been proved in [3]. Moreover, we provide algorithms to compute all well-rounded twists of I (see Section 4). In particular, we give an upper bound for the number of such well-rounded twists (see Corollary 3). The main idea is as below.

Let K be an imaginary quadratic field and let I be an integral ideal of K with a $\mathbb{Z}$-basis $B = \{u, v\}$. We define the function

$$F(B) = F(u,v) = \frac{1}{4}\left[\left(\Im(u^2) + \Im(v^2)\right)^2 - \Im(uv)^2\right]$$

here we denote by $\Im(z)$ the imaginary part of $z \in \mathbb{C}$ (see 3 for an explicit formula). Note that a well-rounded twist of I is determined by a good basis of I (see Definition 4). By Proposition 6, the basis B is good if and only if $F(B) \leq 0$. This inequation only has finitely many solutions as a result of Proposition 8. In addition, it provides us a necessary condition for finding all good bases B, that is the imaginary part of u^2 and of v^2, denoted by $\Im(u^2)$ and $\Im(v^2)$, in absolute value are at most $\mathrm{vol}(I)$ (see ii) in Proposition 8). Thus one first lists all elements $x \in I$ such that $\left(\Im(x^2)\right)^2 \leq \mathrm{vol}^2(I)$. Theorem 1 says that there are only finitely many possibilities for x. After that, for each x found, we solve $F(x,y) \leq 0$ for all possible y such that $\{x, y\}$ is a good basis of I. Finally, Theorem 2 shows that given such an x, there are at most two good bases of the form $\{x, y\}$, up to similarity. The proof of this theorem also gives us explicit formulae to compute those bases. Hence, we can construct all good bases of the ideal I demonstrated in Section 4.

Employing the algorithms presented in Section 4, we can first find all well-rounded twists of an ideal lattice I of K and after that check which lattices are similar using Remark 6. A natural question arisen from our work is how to compute only similar classes instead of all well-rounded twists of I. In other words, assume that we have computed a list $\mathcal{L}$ of some well-rounded twists lattice of I, we would like to find a method to eliminate well-rounded twists J that are similar to the ones in $\mathcal{L}$ before explicitly computing a basis for J. Another question is how to compute all well-rounded twists of ideal lattices in higher degree number fields. These open questions requires us a further research in the future.

The structure of this paper is as follows. In Section 2, we recall some basic definitions and properties of well-rounded lattices in $\mathbb{R}^2$ as well as of good bases and twists of a lattice. Our main results (Theorem 1, Theorem 2 and Theorem 10) are presented in Section 3. Based on the results of this section, we construct algorithms to compute all well-rounded twists of an ideal I of K and demonstrate them by an example in Section 4. We prove the correctness and analyze the complexity of these algorithms in Section 5.

2. Background

In this section we recall some basic definitions and properties of well-rounded lattices (twists) in $\mathbb{R}^2$, and then of well-rounded ideal lattices arisen from imaginary quadratic fields.

Definition 1. *Two planar lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^2$ are called similar, denoted $\Lambda_1 \sim \Lambda_2$, if there exists a positive real number α and a 2×2 real orthogonal matrix U such that $\Lambda_2 = \alpha U \Lambda_1$.*

See [4] for more details. Moreover, if B is a basis of Λ_1 then αUB is a basis of Λ_2 and if B' is a basis of Λ_2 then there exists a basis B of Λ_1 such that $B' = \alpha UB$ (we call B and B' are two similar bases). Thus, one has the following result.

Proposition 1. *Suppose Λ_1, Λ_2 are two lattices of $\mathbb{R}^2$. Then $\Lambda_1 \sim \Lambda_2$ if and only if there exist bases $B_1 = \{x_1, y_2\}$ and $B_2 = \{x_2, y_2\}$ of Λ_1 and Λ_2 respectively such that $|\cos(x_1, y_1)| = |\cos(x_2, y_2)|$ and $\dfrac{\|x_1\|}{\|y_1\|} = \dfrac{\|x_2\|}{\|y_2\|}$, where (x_i, y_i) is the angle between two vectors x_i and $y_i, i = 1, 2$.*

In this section, we will denote by Λ a lattice in $\mathbb{R}^2$ and by $B = \{x, y\}$ a basis of Λ with $x = (a, c), y = (b, d) \in \mathbb{R}^2$.

Definition 2. *For each real number $\alpha > 0$, we define the matrix*

$$T_\alpha = \begin{bmatrix} \alpha & 0 \\ 0 & \dfrac{1}{\alpha} \end{bmatrix}.$$

The lattice $T_\alpha \Lambda$ is called ***the twisting lattice*** *or* ***the twist*** *of Λ with respect to α.*

Proposition 2. *Let $B = \{x = (a, c), y = (b, d)\}$ be a basis of a lattice Λ. Then for all $\alpha > 0$, there exist $x' = (e, f) \in \mathbb{R}^2$ and $f > 0$ such that the lattice generated by $T_\alpha B$ is similar to the lattice generated by $B' = \{(1, 0), x'\}$.*

Proof. By Proposition 1, we prove that there exists $x' \in \mathbb{R}^2$ such that $\dfrac{\|T_\alpha x\|}{\|T_\alpha y\|} = \dfrac{1}{\|x'\|}$ and $|\cos(T_\alpha x, T_\alpha y)|$ is equal to the absolute value of the cosine of the angle between $(1, 0)$ and x'. We consider

$$z = \frac{1}{\alpha^4 a^2 + c^2}\left(ab\alpha^4 + cd, \alpha^2(ad - bc)\right),$$

then $\|z\| = \dfrac{1}{\alpha^4 a^2 + c^2}\sqrt{(ab\alpha^4 + cd)^2 + \alpha^4(ad - bc)^2} = \sqrt{\dfrac{\alpha^4 b^2 + d^2}{\alpha^4 a^2 + c^2}} = \dfrac{\|T_\alpha y\|}{\|T_\alpha x\|}$.

It also implies that $\|-z\| = \dfrac{\|T_\alpha y\|}{\|T_\alpha x\|}$. There are two cases:

- **Case 1:** If $ad - bc > 0$, we choose $x' = z$.
- **Case 2:** If $ad - bc < 0$, we choose $x' = -z$.

For both cases, it is clear that $|\cos(T_\alpha x, T_\alpha y)|$ is equal to the absolute value of the cosine of the angle between $(1, 0)$ and x'. □

Remark 1. *This proposition is shown in particular case of the following statement: every planar lattice is similar to a lattice with a basis B' as described in Proposition 2 and hence planar lattices are identified with $SO_2(\mathbb{R})\backslash SL_2(\mathbb{R})/SL_2(\mathbb{Z})$ (see [11]).*

The idea of Proposition 2 is similar to [3] (see the function in [15] in this paper). For each given basis B, there are two vectors satisfying Proposition 2. However, we can add the condition that $\|x'\| \geq 1$ to have the uniqueness of x'. We denote x' by $\tau(\alpha, B)$ to emphasize that it depends on α and B.

Definition 3. *Let Λ be a lattice in $\mathbb{R}^2$.*

*i) The **set of the minimal vectors** of Λ is*

$$S(\Lambda) = \{x \in \Lambda : \|x\| = \lambda_1(\Lambda)\},$$

where $\lambda_1(\Lambda) = \min\limits_{0 \neq x \in \Lambda} \|x\|$.

*ii) The lattice Λ is called **well-rounded** if $span_{\mathbb{R}}(S(\Lambda)) = \mathbb{R}^2$.*

*iii) If Λ is well-rounded and $\{x_1, x_2\}$ is its basis such that $x_1, x_2 \in S(\Lambda)$, then $\{x_1, x_2\}$ is called a **minimal basis** of A.*

*iv) A basis $\{x_1, x_2\}$ is **twistable** if there exists a matrix T_α such that $\|T_\alpha x\| = \|T_\alpha y\|$.*

Remark 2. *Note that if $S(\Lambda)$ contains two independent vectors then these vectors form a minimal basis for Λ. This fact is not true for lattices of higher dimension (see [10] for more details).*

The following lemma is a result of Proposition 1 and the definition of well-rounded lattices.

Lemma 1. *Two well-rounded lattices are similar if and only if there exist their minimal bases $B_1 = \{x_1, y_2\}$ and $B_2 = \{x_2, y_2\}$ such that $|\cos(x_1, y_1)| = |\cos(x_2, y_2)|$.*

Proposition 3. *Let $\beta = \dfrac{d^2 - c^2}{a^2 - b^2}$. Then B is twistable if and only if $\beta > 0$. If this is the case, then α is unique and $\alpha = \beta^{1/4}$.*

Proof. See Proposition 1 of [3]. □

To emphasize that α and β are functions depending on the basis B of Λ, we will write $\alpha_\Lambda(B)$ and $\beta_\Lambda(B)$ for α, β. Note that $\alpha_\Lambda(B) = (\beta_\Lambda(B))^{1/4}$.

Proposition 4. *If B is a twistable basis with the twisting matrix T_α, then*

$$\cos\theta_{T\alpha B} = \frac{ac+bd}{ad+bc}.$$

Proof. See Proposition 2 in [3]. □

Proposition 5. *If $\left|\frac{ac+bd}{ad+bc}\right| \leq \frac{1}{2}$ then B is twistable.*

Proof. See Proposition 3 of [3]. □

In this case, since $|\cos\theta_{T_\alpha B}| \leq \frac{1}{2}$ where $\beta = \frac{d^2-c^2}{a^2-b^2}$ and $\alpha = \beta^{1/4}$, the lattice $T_\alpha\Lambda$ is well-rounded. Moreover, $\{T_\alpha x, T_\alpha y\}$ is a minimal basis of $T_\alpha\Lambda$.

Definition 4. *We call a basis B of Λ* ***good for twisting*** *or a* ***good basis*** *if*

$$\left|\frac{ac+bd}{ad+bc}\right| \leq \frac{1}{2}. \tag{1}$$

This definition is equivalent to the following statement: there exists $\alpha > 0$ such that $T_\alpha\Lambda$ is well-rounded with a minimal basis $T_\alpha B$.

By transforming inequation (1), a basis B is a good basis if

$$a^2c^2 + abcd + b^2d^2 - \frac{(ad-bc)^2}{4} \leq 0 \text{ and } ad+bc \neq 0. \tag{2}$$

From the first inequality of (2), one may define the polynomial

$$\begin{aligned} F(B) =& (ac)^2 + abcd + (bd)^2 - \frac{(ad-bc)^2}{4} \\ =& \left(ac+bd+\frac{ad+bc}{2}\right)\left(ac+bd-\frac{ad+bc}{2}\right). \end{aligned} \tag{3}$$

Frow now, we only need to consider the basis $B = \{(a,c);(b,d)\}$ where $ad+bc \neq 0$.

We have the following result that is similar to Theorem 1 in [3].

Proposition 6. *Let Λ be a lattice in $\mathbb{R}^2$.*

(i) A basis B is good for twisting if and only if $F(B) \leq 0$.

(ii) If B is good for twisting, then $\min\{(ac)^2, (bd)^2\} \leq \frac{\mathrm{vol}^2(\Lambda)}{4}$.

Proof. (i) This fact can be easily implied from the definition of F.

(ii) Recall that $\mathrm{vol}^2(\Lambda) = (ad - bc)^2$. Since B is good for twisting, it follows that

$$\begin{aligned} 0 \geq (ac)^2 + abcd + (bd)^2 - \frac{\mathrm{vol}^2(\Lambda)}{4} &= \frac{(ac)^2 + (bd)^2}{2} + \frac{(ac+bd)^2}{2} - \frac{\mathrm{vol}^2(\Lambda)}{4} \\ &\geq \frac{(ac)^2 + (bd)^2}{2} - \frac{\mathrm{vol}^2(\Lambda)}{4}. \end{aligned}$$

Hence $\min\left\{(ac)^2, (bd)^2\right\} \leq \dfrac{\mathrm{vol}^2(\Lambda)}{4}$.

□

For D positive and squarefree, we put $K = \mathbb{Q}(\sqrt{-D})$ and

$$\delta = \begin{cases} \sqrt{-D}, & \text{if } -D \not\equiv 1 \mod 4 \\ \dfrac{1+\sqrt{-D}}{2}, & \text{if } -D \equiv 1 \mod 4 \end{cases}.$$

The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\delta]$. The embeddings $\sigma_1, \sigma_2 : K \longrightarrow \mathbb{C}$ are given by

$$\sigma_1(x + y\delta) = x + y\delta, \quad \sigma_2(x+y\delta) = \begin{cases} x - y\delta \text{ if } D \not\equiv 1 \pmod 4 \\ x + y(1-\delta) \text{ if } D \equiv 1 \pmod 4). \end{cases}$$

We have $\sigma_2 = \overline{\sigma_1}$. Hence we denote by σ_K the embedding from K into $\mathbb{R}^2$ defined by $\sigma_K = (\Re\sigma_2, \Im\sigma_2)$, where $\Re$ and $\Im$ stand for the real and imaginary parts, respectively.

Now let $I \subset \mathcal{O}_K$ be an ideal and $\{t, y + g\delta\}$ its $\mathbb{Z}$-basis where $0 \leq y < t$, $g|y, t$ and $0 < g \leq t$. This basis is called the **canonical basis** of I.

Suppose $u, v \in I$ form a $\mathbb{Z}$-basis of I, then we can represent the lattice $\Lambda_K(I) = \sigma_K(I)$ as

$$\Lambda_K(I) = \begin{pmatrix} \Re(u) & \Re(v) \\ -\Im(u) & -\Im(v) \end{pmatrix} \mathbb{Z}^2 = \begin{pmatrix} \dfrac{u+\overline{u}}{2} & \dfrac{v+\overline{v}}{2} \\ \dfrac{\overline{u}-u}{2i} & \dfrac{\overline{v}-v}{2i} \end{pmatrix} \mathbb{Z}^2.$$

where $\Re(z) = \dfrac{z+\overline{z}}{2}, \Im(z) = \dfrac{z-\overline{z}}{2i}$.

Proposition 7. *Let $B = \{u, v\}$ be a twistable basis of I. Then* $\cos\theta_{T_\alpha B} = \dfrac{\Im(u^2) + \Im(v^2)}{2\Im(uv)}$.

Proof. Proposition 4 provides that

$$\cos T_\alpha B = \frac{\dfrac{\overline{u}^2 - u^2}{4i} + \dfrac{\overline{v}^2 - v^2}{4i}}{\dfrac{\overline{uv} - uv}{2i}} = \frac{\Im(u^2) + \Im(v^2)}{2\Im(uv)}.$$

□

3. Main results

From now on, we follow the notations used in Section 2. The second inequality of (2) becomes

$$\Re(u)\Im(v) + \Re(v)\Im(u) \neq 0 \tag{4}$$

Applying Proposition 6, we obtain a similar result as the one in Theorem 2 in [3] as below.

Proposition 8. *Let I be an ideal with a basis $B = \{u, v\}$. Then, we have the following statements.*

(i) A basis B is good for twisting if and only if $F(u, v) \leq 0$, in which case the twisting matrix T_α is given by $\alpha = \left(\dfrac{\Im(v)^2 - \Im(u)^2}{\Re(u)^2 - \Re(v)^2}\right)^{\frac{1}{4}}$.

(ii) If B is good for twisting, then

$$\min\left\{\left(\Im(u^2)\right)^2, \left(\Im(v^2)\right)^2\right\} \leq \mathrm{vol}^2\left(\Lambda_K(I)\right).$$

(iii) A basis $\{u, v\}$ is good for twisting if and only if so is the basis $\{v, u\}$. Moreover, their well-rounded twisting lattices are similar.

Proof. The two first statements are corollaries of Proposition 6. The last one can be implied by applying (i) and Proposition 2. □

From (3), one obtains that $F(B) = F_1(B)F_2(B)$ where

$$F_1(B) = \frac{\overline{u}^2 - u^2}{4i} + \frac{\overline{v}^2 - v^2}{4i} + \frac{\overline{uv} - uv}{4i} = -\frac{1}{2}\left(\Im(u^2) + \Im(v^2) + \Im(uv)\right) \text{ and} \tag{5}$$

$$F_2(B) = \frac{\overline{u}^2 - u^2}{4i} + \frac{\overline{v}^2 - v^2}{4i} - \frac{\overline{uv} - uv}{4i} = -\frac{1}{2}\left(\Im(u^2) + \Im(v^2) - \Im(uv)\right).$$

A similar version for Proposition 5 of [3] is the following.

Proposition 9. *Let $I \subset \mathcal{O}_K$ be an ideal. The hexagonal lattice is a twist of $\Lambda_K(I)$ if and only if I has a basis $B = \{u, v\}$ such that $F(B) = 0$.*

Proof. We use the fact that $F(u, v) = 0$ if and only if $\Im(u^2) + \Im(v^2) = \pm\Im(uv)$. Equivalently, one has $|\cos\theta_{T_\alpha B}| = \dfrac{1}{2}$. In this case, the twist lattice of Λ is hexagonal. □

Our goal is to compute all good bases of a given ideal lattice $\Lambda_K(I)$, up to similarity. Now we fix a suitable element $x \in I$ and find all good bases of the form $\{x, y\}$ of I.

Definition 5. *For $x \in I$, we say that x can be extended to a (good) basis if there exists $y \in I$ such that $\{x, y\}$ is a (good) basis of I.*

Let $\{u, v\}$ be any basis of I and write $x = au + cv$ for $a, c \in \mathbb{Z}$ without loss the generality, we can assume $a \geq 0$. Then x can be extended to a basis if and only if there exists $y = bu + dv \in I$ such that $ad - bc = \pm 1$. This occurs if and only if $(a, c) = 1$. Combining with Proposition 8 we obtain the following initial strategy to compute all well-rounded twists of a given ideal lattice $\Lambda_K(I)$, up to similarity.

□ **Step 1:** Find a basis $\{u, v\}$ of I.

□ **Step 2:** List all $x = au + cv \in I$ such that $\left(\Im(x^2)\right)^2 \leq \mathrm{vol}^2(\Lambda_K(I)), a \geq 0$ and $\gcd(a, c) = 1$.

□ **Step 3:** For each x found in **Step 2**, we solve $F(x, y) \leq 0$ for all possible y such that $\{x, y\}$ is a basis of I. Note that such basis must satisfy the condition (4).

Remark 3. *In* ***step 2****, we have to list all elements x such that $\left(\Im(x^2)\right)^2 \leq \mathrm{vol}^2(\Lambda_K(I))$. For example, $I = \mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-5})$. We consider the elements a and $c\sqrt{-5}$ $(a, c \in \mathbb{Z})$. The square of a or $c\sqrt{-5}$ $(a, c \in \mathbb{Z})$ has zero imaginary part. It means the inequation $\left(\Im(x^2)\right)^2 \leq \mathrm{vol}^2\left(\Lambda_K(I)\right)$ may have infinitely many solutions. We can avoid this by using an idea given by Theorem 2.*

Lemma 2. *Let $I \neq (0)$ be an integral ideal of $\mathcal{O}_K$. For all $x \neq 0$ and $x \in I$, we can choose a $\mathbb{Z}$-basis $B = \{u, v\}$ of I such that $\Im(uv)$ and $\Im(vx)$ are non-zero.*

Proof. Fix the canonical basis $B = \{t, y + g\delta\}$ of I. Clearly, we have $\Im\left(t(y + g\delta)\right) \neq 0$. If $\Im(x) = 0$, we choose $u = t, v = y + g\delta$ for $t, g > 0, y \geq 0$ such that $y < t$, $g|t, y$ and $tg|N(y + g\delta)$. Then the basis $B' = \{u, v\}$ satisfies $\Im(uv) \neq 0$ and $\Im(vx) \neq 0$. If $\Im(x) \neq 0$, we choose $u = y + g\delta, v = t$, then $B' = \{u, v\}$ satisfies that $\Im(uv), \Im(vx)$ are non-zero. □

There are only finitely many $x \in I$ such that it can extend to a good basis. The proof of Lemma 3 describes accurately a method to find all those elements.

Lemma 3. *Suppose that D is square-free and positive such that $-D \not\equiv 1 \pmod 4$. Then there are finitely many elements $z \in I$ such that z can extend to a good basis of I, up to similarity.*

Proof. Fix $\left\{t, y + g\sqrt{-D}\right\}$ the canonical basis of I where $0 \leq y < t$, $g|t, y$ and $tg|(y^2 + g^2 D)$. An arbitrary element of I has the form $z = (at + cy) + cg\sqrt{-D}$ for some $a, c \in \mathbb{Z}$. By Proposition 8, we only consider the existence of an extendable basis $\{z, z'\}$ with $\left(\Im(z^2)\right)^2 \leq \mathrm{vol}^2(\Lambda_K(I))$. It is equivalent to $|c(at + cy)| \leq \frac{t}{2}$. There are three cases.

Case 1: Solve the inequation $0 < |c(at+cy)| \leq \frac{t}{2}$. There are finitely many pairs (a,c) satisfying the inequalities.

Case 2: If $c = 0$, then $z = at$. Thus z can be extended to a good basis if and only if there exists $z' = (bt+dy) + dg\sqrt{-D}$ such that $\{z, z'\}$ is a good basis of I. It occurs when $ad = \pm 1$. In other words, one has $a = \pm 1$.

Case 3: If $c \neq 0$ and $at + cy = 0$, then z can be extended to a good basis if there exists an element $(bt+dy) + dg\sqrt{-D}$ such that $\begin{vmatrix} -\frac{cy}{t} & b \\ c & d \end{vmatrix} = \pm 1$. It is equivalent to that $c(dy+bt) = \pm t$. Therefore c is a divisor of t. Because $t \neq 0$, there are finitely many such pairs (a,c).

□

If $-D \equiv 1 \pmod 4$, the canonical basis of an ideal I of $\mathcal{O}_K$ with $K = \mathbb{Q}(\sqrt{-D})$ is $t, y + g\frac{1+\sqrt{-D}}{2}$ where $0 \leq y < t$, $g|t, y$. We can write an arbitrary element of I as $\frac{2at+2cy+cg}{2} + \frac{cg\sqrt{-D}}{2}$. By Proposition 8, if this element can be extended to a good basis of I, then $|(2at+2cy+cg)c| \leq t$. By using an argument similar to the one in the proof of Lemma 3, one obtains the following lemma.

Lemma 4. *Suppose that D is a square-free and positive integer such that $-D \equiv 1$ (mod 4). Then there are finitely many elements $z \in I$ such that z can be extended to a good basis of I, up to similarity.*

From Lemma 3 and Lemma 4, the following result is obtained.

Theorem 1. *Let I be a nonzero ideal of $\mathcal{O}_K$. Then there are finitely many elements in I that can be extended to a good basis of I.*

From the proof of Lemma 3 and Lemma 4, we can list all elements of I which can be extended to a basis of I. The proofs of two lemmas also yield an explicit method to find those elements. We replace **Step 2** of strategy (in page 6) by *listing all elements of I which can be extended to a basis of I.* The next result gives us a more efficient method to compute these bases.

Lemma 5. *Let I be an integral ideal with the basis $\{u, v\}$. Assume that an element $x = au + cv \in I$, that can be extended to a basis $B = \{x, y\}$ with $y = bu + dv$. Then we have the following.*

(i) If $a = 0$, then we can choose $x = v, y = u + dv$ and hence

$$F_1(B) = -\frac{\Im(x^2)}{2}d^2 + \left(-\Im(uv) - \frac{\Im(x^2)}{2}\right) d - \frac{\Im(x^2) + \Im(u^2) + \Im(uv)}{2} \tag{6}$$

$$F_2(B) = -\frac{\Im(x^2)}{2}d^2 + \left(-\Im(uv) + \frac{\Im(x^2)}{2}\right) d - \frac{\Im(x^2) + \Im(u^2) - \Im(uv)}{2}. \tag{7}$$

(ii) If $a \neq 0$ and $ad - bc = 1$, then

$$\begin{aligned} a^2F_1(B) = &-\frac{\Im(x^2)}{2}b^2 - \left[a\left(\frac{2\Im(uv)}{2} + \frac{\Im(x^2)}{2}\right) + 2c\frac{\Im(v^2)}{2}\right] b \\ &- a^2\left(\frac{\Im(x^2)}{2} + \frac{\Im(uv)}{2}\right) - \frac{\Im(v^2)}{2}(1 + ac) \end{aligned} \tag{8}$$

$$\begin{aligned} a^2F_2(B) = &-\frac{\Im(x^2)}{2}b^2 - \left[a\left(\frac{2\Im(uv)}{2} - \frac{\Im(x^2)}{2}\right) + 2c\frac{\Im(v^2)}{2}\right] b \\ &- a^2\left(\frac{\Im(x^2)}{2} - \frac{\Im(uv)}{2}\right) - \frac{\Im(v^2)}{2}(1 - ac). \end{aligned} \tag{9}$$

Proof. (i) From (5), we have

$$\begin{aligned} F_1(B) &= -\frac{1}{2}\left(\Im(x^2) + \Im(y^2) + \Im(xy)\right) = \frac{-\Im(x^2)}{2} - \frac{\Im((u + dv)^2)}{2} + \frac{\Im(v(u + dv))}{2} \\ &= \frac{-\Im(x^2)}{2} - \frac{1}{2}\left(\frac{(u^2 - \overline{u}^2) + d^2(v^2 - \overline{v}^2) + 2d(uv - \overline{uv})}{2i}\right) - \frac{1}{2}\frac{v(u + dv) - \overline{v(u + dv)}}{2i} \\ &= \frac{-\Im(x^2)}{2}d^2 - \left(\Im(uv) + \frac{\Im(x^2)}{2}\right) d - \frac{\Im(x^2) + \Im(u^2) + \Im(uv)}{2}. \end{aligned}$$

It is the result of (6). By using a similar computation, we obtain the result in (7).

(ii) Here we have $ad - bc = 1$, $d = \dfrac{1 + bc}{a}$. Using equation (5) leads to the following.

$$\begin{aligned} a^2F_1(B) &= -\frac{a^2}{2}\left(\Im(x^2) + \Im((bu + dv)^2) + \Im((au + cv)(bu + dv))\right) \\ &= -\frac{a^2}{2}\left(\Im(x^2) + \Im\left(\left(bu + \frac{1 + bc}{a}v\right)^2\right) + \Im\left((au + cv)\left(bu + \frac{1 + bc}{a}v\right)\right)\right) \\ &= -\frac{a^2}{2}\left[\Im(x^2) + \Im\left(bx + v\right)^2 + a\Im\left((au + cv)(bx + v)\right)\right] \\ &= -\frac{a^2\Im(x^2)}{2} - \frac{\Im(x^2)}{2}b^2 - \frac{\Im(v^2)}{2} - \frac{2b\Im\left((au + cv)v\right)}{2} - \frac{ab\Im(x^2)}{2} - \frac{a^2\Im(uv) + ac\Im(v^2)}{2} \\ &= -\frac{\Im(x^2)}{2}b^2 - \left[a\left(\Im(uv) + \frac{\Im(x^2)}{2}\right) + c\Im(v^2)\right] b - a^2\left(\frac{\Im(x^2)}{2} + \frac{\Im(uv)}{2}\right) - \frac{\Im(v^2)}{2}(1 + ac). \end{aligned}$$

Thus (8) is proved. The result in (9) can be obtained by using a similar computation. □

When $\Im(x^2) \neq 0$, the right sides of (6) and (7) are degree two polynomials in d with the same discriminants. Indeed, we have (note that $v = x$)

$$\Delta_{F_1(B)} = \left(-\Im(uv) - \frac{\Im(x^2)}{2}\right)^2 - 4\frac{\Im(x^2)}{2}\left(\frac{\Im(x^2) + \Im(u^2) + \Im(uv)}{2}\right)$$

$$= -\frac{3\left(\Im(x^2)\right)^2}{4} + \Im(uv)^2 - \Im(x^2)\Im(u^2) = -\frac{3\Im(x^2)}{4} + \frac{(uv - \overline{uv})^2 - (u^2 - \overline{u}^2)(v^2 - \overline{v}^2)}{(2i)^2}$$

(10)

$$= \left(\frac{u\overline{v} - v\overline{u}}{2i}\right)^2 - \frac{3\left(\Im(x^2)\right)^2}{4} = \mathrm{vol}^2\left(\Lambda_K(I)\right) - \frac{3\left(\Im(x^2)\right)^2}{4}.$$

Similarly, one obtains that $F_2(B)$ has the same discriminant as of $F_1(B)$. Analogously, the discriminants of polynomials (in b) on the right side of (8) and (9) are

$$a^2\left(\mathrm{vol}^2\left(\Lambda_K(I)\right) - \frac{3\left(\Im(x^2)\right)^2}{4}\right). \tag{11}$$

The next result is an analogy to Theorem 3 in [3].

Theorem 2. *Let I be an ideal of $\mathcal{O}_K$ and let $x \in I$ such that $\left(\Im(x^2)\right)^2 \leq \mathrm{vol}^2(\Lambda_K(I))$. Then x can be extended to at most two good bases of I, up to similarity.*

Proof. Let us fix a basis $\{u, v\}$ of I such that $\Im(uv) \neq 0$ and $\Im(vx) \neq 0$. Such a basis exists by Lemma 2. The condition $\Im(vx) \neq 0$ implies that $a\Im(uv) + c\Im(v^2) \neq 0$. Express $x = au + cv$ for some $a, c \in \mathbb{Z}$, and suppose that $y = bu + dv$ for some $b, d \in \mathbb{Z}$ and $\{x, y\}$ is a good basis. We will employ the inequality $F(x, y) \leq 0$ and the equality $ad - bc = \pm 1$ to solve for all possible b and d. We consider two cases.

- **Case 1:** If $a = 0$, then $ad - bc = \pm 1$. It implies that $b = \pm 1$ and $c = \pm 1$, so $x = \pm v$ and $y = \pm u + dv$. By possibly replacing x with $-x$ and y with $-y$, which does not change the similarity class of the given basis, we may assume that our basis $\{x, y\}$ is of the form $\{x, y\} = \{v, u + dv\}$. We will show that there are at most two integers d such that this is a good basis.

  Let $f_i(d) = F_i(x, y)$ and $F_i(x, y)$ are as in (6) and (7). By Proposition 6, we must find all d such that $f_1(d)$ and $f_2(d)$ have opposite signs, or such that at least one of them are zero. Using (6) and (7), we divide our proof into 2 cases.

  - **Case 1.1.** If $\Im(x^2) = 0$, the functions in (6) and (7) become

$$f_1(d) = -\Im(uv)d - \frac{\Im(u^2) + \Im(uv)}{2} \text{ and}$$
$$f_2(d) = -\Im(uv)d - \frac{\Im(u^2) - \Im(uv)}{2}.$$

There are at least one of $f_1(d)$ and $f_2(d)$ which are equal to zero if and only if $d = \beta_1$ or $d = \beta_2$ where

$$\beta_1 = \frac{\Im(u^2) + \Im(uv)}{-2\Im(uv)} \text{ and } \beta_2 = \frac{\Im(u^2) - \Im(uv)}{-2\Im(uv)}. \tag{12}$$

In addition, $f_1(d)$ and $f_2(d)$ have opposite signs if $d \in (\beta_1, \beta_2)$. Therefore, $d \in [\beta_1, \beta_2]$. However, $\beta_2 - \beta_1 = 1$, there are at most two values of d satisfying the condition.

- **Case 1.2.** If $\Im(x^2) \neq 0$, the functions in (6) and (7) are second degree polynomials with the same discriminants $\Delta = \mathrm{vol}^2\left(\Lambda_K(I)\right) - \dfrac{3\left(\Im(x^2)\right)^2}{4}$ by (10). The polynomial $f_1(d)$ has two roots

$$\beta_{11} = \frac{-\left(-\Im(uv) - \dfrac{\Im(x^2)}{2}\right) + \sqrt{\Delta}}{-\Im(x^2)}, \beta_{12} = \frac{-\left(-\Im(uv) - \dfrac{\Im(x^2)}{2}\right) - \sqrt{\Delta}}{-\Im(x^2)}. \tag{13}$$

The polynomial $f_2(d)$ has two roots

$$\beta_{21} = \frac{-\left(-\Im(uv) + \dfrac{\Im(x^2)}{2}\right) + \sqrt{\Delta}}{\Im(x^2)}, \beta_{22} = \frac{-\left(-\Im(uv) + \dfrac{\Im(x^2)}{2}\right) - \sqrt{\Delta}}{-\Im(x^2)}. \tag{14}$$

There are at least one of $f_1(d)$ and $f_2(d)$ which are equal to zero if and only if $d \in \{\beta_{11}, \beta_{12}, \beta_{21}, \beta_{22}\}$. In these cases, we have $F(B) = f_1(d) f_2(d) = 0$, then one obtains four hexagonal twist lattices (by Proposition 9). Therefore, they are all similar. Thus there is at most one d, up to similarity. In addition, $f_1(d)$ and $f_2(d)$ have opposite signs if and only if $d \in (\beta_{11}, \beta_{21}) = J_1$ or $d \in (\beta_{12}, \beta_{22}) = J_2$. These open intervals have width one. As a result they only contain at most one integer. Hence, there are at most two d satisfying the condition.

- **Case 2:** If $a \neq 0$, then $d = \dfrac{1+bc}{a}$. Multiplying by -1 if necessary we may assume $a > 0$. We again explicitly compute all $y = bu + dv \in I$ such that $\{x, y\}$ is a good basis of I, up to similarity. By possibly replacing y with $-y$ we may assume $ad - bc = 1$, and solve for d in terms of b as $d = \dfrac{1+bc}{a}$. Setting $f_i(b) = F_i(x, y)$, we wish to find all integers b such that $d = \dfrac{1+bc}{a} \in \mathbb{Z}$, and that either $f_1(b)$ and $f_2(b)$ have opposite signs or such that at least one of them are zero. From (8) and (9), one can consider two cases as below.

- **Case 2.1.** If $\Im(x^2) = 0$, the functions in (8) and (9) become

$$a^2 f_1(b) = -\left(a\Im(uv) + c\Im(v^2)\right) b - a^2\left(+\frac{\Im(uv)}{2}\right) - \frac{\Im(v^2)}{2}(1+ac) \text{ and}$$

$$a^2 f_2(b) = -\left(a\Im(uv) + c\Im(v^2)\right) b - a^2\left(-\frac{\Im(uv)}{2}\right) - \frac{\Im(v^2)}{2}(1-ac).$$

The condition $a\Im(uv)+c\Im(v^2) \neq 0$ follows that $a^2 f_1(b)$ and $a^2 f_2(b)$ are linear polynomials in b. The roots of $a^2 f_1(b)$ and $a^2 f_2(b)$ are respectively

$$\beta_1 = \frac{a^2\left(\frac{\Im(uv)}{2}\right) + \frac{\Im(v^2)}{2}(1+ac)}{-\left(a\Im(uv)+c\Im(v^2)\right)} \text{ and } \beta_2 = \frac{a^2\left(\frac{-\Im(uv)}{2}\right) + \frac{\Im(v^2)}{2}(1-ac)}{-\left(a\Im(uv)+c\Im(v^2)\right)}. \tag{15}$$

There are at least one of $f_1(b)$ and $f_2(b)$ which are equal to zero if and only if $b = \beta_1$ or $b = \beta_2$. In addition, $a^2 f_1(b)$ and $a^2 f_2(b)$ have opposite signs if and only if $b \in [\beta_1, \beta_2] = J$. The interval J has width a, so the equation $bc+1 \equiv 0 \mod a$ has at most one solution in J. Therefore, there are at most two pairs (b,d) satisfying the above condition as we expect.

- **Case 2.2.** If $\Im(x^2) \neq 0$, the functions in (6) and (7) are second degree polynomials with the same discriminants $\Delta = a^2\left(\operatorname{vol}^2(\Lambda_K(I)) - \frac{3\left(\Im(x^2)\right)^2}{4}\right)$ by (11). Then the polynomial $a^2 f_1(b)$ has two roots

$$\beta_{11} = \frac{\left[a\left(\Im(uv) + \frac{\Im(x^2)}{2}\right) + c\Im(v^2) + \sqrt{\Delta}\right]}{-\Im(x^2)} \text{ and} \tag{16}$$
$$\beta_{12} = \frac{\left[a\left(\Im(uv) + \frac{\Im(x^2)}{2}\right) + c\Im(v^2) - \sqrt{\Delta}\right]}{-\Im(x^2)}.$$

The polynomial $a^2 f_2(b)$ has two roots

$$\beta_{21} = \frac{\left[a\left(\Im(uv) - \frac{\Im(x^2)}{2}\right) + c\Im(v^2) + \sqrt{\Delta}\right]}{-\Im(x^2)} \text{ and} \tag{17}$$
$$\beta_{22} = \frac{\left[a\left(\Im(uv) - \frac{\Im(x^2)}{2}\right) + c\Im(v^2) - \sqrt{\Delta}\right]}{-\Im(x^2)}.$$

There are at least one of $a^2 f_1(b)$ and $a^2 f_2(b)$ which are equal to zero if and only if $b \in \{\beta_{11}, \beta_{12}, \beta_{21}, \beta_{22}\}$. In these cases, we have four hexagonal twist lattices (by Proposition 9) and therefore, they are similar. Moreover, there is at most one d, up to similarity. In addition, $a^2 f_1(b)$ and $a^2 f_2(b)$ have opposite signs if and only if $d \in (\beta_{11}, \beta_{21}) = J_1$ or $d \in (\beta_{12}, \beta_{22}) = J_2$. This open intervals have width a, so they contain at most one integer which is a solution of $bc+1 \equiv 0 \mod a$. Hence, there are at most two expected pairs (b, d).

□

If $-D \not\equiv 1 \mod 4$, the ring of integers O_K of $K = \mathbb{Q}(\sqrt{-D})$ has the canonical basis $\{u = 1, v = \sqrt{-D}\}$. Using the proof of Theorem 2, one can show that O_K only has the following good bases $x = au + cv$, $y = bu + dv$ for $(a, c, b, d) \in \{(1, 0, 0, 1), (1, 0, 0, -1), (0, 1, 1, 0)\}$. Since all well-rounded lattices defined by these bases are similar, one obtains that O_K has only one well-rounded twist up to similarity. We have the following corollary that is an analogy with the result of Corollary 3 in [3].

Corollary 1. *Let D be a square-free integer such that $-D \not\equiv 1 \pmod 4$, and let $K = \mathbb{Q}(\sqrt{-D})$. Then the lattice Λ_K has a unique well-rounded twist, which is an orthogonal lattice, up to similarity.*

Proof. The canonical basis of $\mathcal{O}_K$ is $\left\{1, \sqrt{-D}\right\}$ and $\mathrm{vol}(\Lambda_K) = \sqrt{D}$. Suppose that $x = a + c\sqrt{-D}$ can be extended to a good basis. By Proposition 8, it is sufficient to consider the case in which $|ac| \leq \frac{1}{2}, (a, c) = 1$ and $a \geq 0$. It implies $(a, c) \in \{(0, 1), (0, -1), (1, 0)\}$.

- If $(a, c) = (0, 1)$ then $x = \sqrt{-D}$. By Theorem 2, the basis to which x extends is $\{\sqrt{-D}, 1\}$. The well-rounded twist lattice of this basis is orthogonal.
- If $(a, c) = (0, -1)$, the result is the same with the case $(a, c) = (0, 1)$.
- If $(a, c) = (1, 0)$ then $x = 1$, by Theorem 2, the basis to which x extends is $\{1, \sqrt{-D}\}$. Thus the well-rounded twist lattice of this basis is orthogonal.

Therefore, for all cases, O_K has a unique well-rounded twist which is similar to an orthogonal lattice, up to similarity. □

Corollary 2. *Let D be a square-free integer such that $-D \equiv 1 \pmod 4$, and let $K = \mathbb{Q}(\sqrt{-D})$. Then the lattice Λ_K has a unique well-rounded twist, which is a hexagonal lattice, up to similarity.*

Proof. The canonical basis of $\mathcal{O}_K$ is $\left\{1, \frac{1+\sqrt{-D}}{2}\right\}$ and $\mathrm{vol}(\Lambda_K) = \frac{\sqrt{D}}{2}$. Suppose that $x = a + c\left(\frac{1+\sqrt{-D}}{2}\right)$ can be extended to a good basis. By Proposition 8, it is sufficient to consider the case in which $|(2a + c)c| \leq 1, (a, c) = 1$ and $a \geq 0$. It implies $(a, c) \in \{(1, 0), (1, -2), (0, 1), (1, -1)\}$. By using a similar argument as the one of Theorem 2, we can compute all tuples (a, c, b, d) such that $F(au + cv, bu + dv) \leq 0$, where $u = 1, v =$

$\dfrac{1+\sqrt{-D}}{2}$. One can easily checks that the value of F at all bases are equal to zero. Therefore, these bases have only one well-rounded twist lattice, which is hexagonal, up to similarity. □

Remark 4. *Our results on well-rounded twist lattices of the ring of integers O_K (Corollaries 1 and 2) are more general compared to Lemma 2.2 in [5] which states that the lattices O_K is well-rounded (without twisting) if and only if $D = 1, 3$. Indeed, when $D = 1$ then $O_K = \mathbb{Z}[i]$ which is well-rounded and orthogonal, and is a particular case of Corollary 1. When $D = 3$, then $O_K = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ which is well-rounded and hexagonal, and is a particular case of Corollary 2.*

Now let I be an integral ideal of $K = \mathbb{Q}(\sqrt{-D})$ with the canonical basis $\{t, y + g\delta\}$. In case $y \neq 0$, we can easily apply a similar argument as in the proof of Theorem 2 to find upper bounds for the number of well-rounded twists of I which are presented in Corollaries 3 and 4 as below. Note that these results may not be true for real quadratic fields and a similar result has not been proved in [3].

Corollary 3. *Let D be a squarefree integer with $-D \not\equiv 1 \pmod 4$ and let I be an ideal of $\mathbb{Q}(\sqrt{-D})$ with the canonical basis $\{t, y + g\delta\}$. Then I has at most $6 + 2\left\lceil \frac{y+1}{2} \right\rceil$ well-rounded twists.*

Proof. The result can be easily obtained from counting the number solutions of the inequations $|(at + cy)c| \leq \frac{t}{2}$, $a \geq 0$, and $(a, c) = 1$ and by applying Theorem 2. □

Moreover, Corollary 3 can be implied immediately from Algorithm 1. Similarly, one has the following result when $-D \equiv 1 \pmod 4$.

Corollary 4. *Let D be a squarefree integer with where $-D \equiv 1 \pmod 4$ and let I be an ideal of $\mathbb{Q}(\sqrt{-D})$ with the canonical basis $\{t, y + g\delta\}$. Then I has at most $6 + 2\left\lceil \frac{2y+g+1}{2} \right\rceil$ well-rounded twists.*

Proposition 10. *Every ideal of $\mathcal{O}_K$ has at least one well-rounded twist lattice.*

Proof. We prove this theorem for the case $-D \not\equiv 1 \mod 4$, the case $-D \equiv 1 \mod 4$ can be proved using a similar argument.

As in the proof of Lemma 3, one can see that $z = 1.t + 0.(y + g\sqrt{-D}) = t$ is an element of I which can be extended to a good basis. Moreover, since $\Im(z^2) = 0$, by setting $u = t$

and $v = y + g\sqrt{-D}$ and using (15), one has $\beta_1 = \dfrac{t+2y}{-2t}$ and $\beta_2 = \dfrac{-t+2y}{-2t}$. There are at most two integers and at least one integers in the interval $[\beta_1, \beta_2]$. Using an argument similar to the one in the proof of Theorem 2, we obtain a good basis of I. It provides that I has a well-rounded twist lattice. □

Remark 5. *In [11], it is proved that every lattice (in any dimension) has at least a well-rounded twist, thus, Proposition 10 can be considered as a particular case of the mentioned result. Our proof, however, uses an independent argument and result from the ones in [11]. Indeed Proposition 10 is implied from the proofs of Lemma 3 and Theorem 2. We remark that a similar result has not been proved in [3] for real quadratic fields.*

4. Algorithms and a numerical example

The proof of Theorem 2 gives us explicit formulae (see 12, 13, 14, 15, 16 and 17) to compute all well-rounded twists of an ideal I given by any $\mathbb{Z}$-basis $\{u, v\}$ of I. In practice, I is given by the canonical basis that can be efficiently computed if two generators of I over O_K are provided. We also note that the conditions $\Im(uv) \neq 0$ and $\Im(vx) \neq 0$ in Theorem 2 is necessary only if $\Im(x^2) = 0$. We can exchange the two vectors in the canonical basis of I to have these conditions. Moreover, the canonical basis provides us simpler formulae for $\beta_1, \beta_2, \beta_{11}, \beta_{12}, \beta_{21}, \beta_{22}$ than the ones in a general case shown as below.

In case $-D \not\equiv 1 \pmod 4$, then $\{t, y + g\sqrt{-D}\}$ is the canonical basis of I. Let $u = t, v = y + g\sqrt{-D}$.

1. If $a = 0, \Im(x^2) = 0$, from $ad - bc = \pm 1$, one has $c = \pm 1$. In these cases, since $\Im(uv) = tg\sqrt{D} \neq 0$, equations in (12) become $\beta_1 = \dfrac{-1}{2}, \beta_2 = \dfrac{1}{2}$. It implies that $d = 0$ and $b = \pm 1$. We only receive the tuple $(0, 1, 1, 0)$ as others give the same well-rounded twist lattices, up to similarity.
2. If $a = 0, \Im(x^2) \neq 0$, then it implies $c^2 = 1$. Let $\alpha = \dfrac{t}{2y}$. Then (13) and (14) become

$$\beta_{11} = -\frac{1}{2} - \alpha - \sqrt{\alpha^2 - \frac{3}{4}}, \quad \beta_{21} = \beta_{11} + 1 \tag{18}$$

$$\beta_{12} = -\frac{1}{2} - \alpha + \sqrt{\alpha^2 - \frac{3}{4}}, \quad \beta_{22} = \beta_{12} + 1. \tag{19}$$

3. If $a \neq 0, \Im(x^2) = 0$ and $c = 0$, the equation (15) becomes

$$\beta_1 = \frac{-1}{2} - \frac{y}{t}, \beta_2 = \beta_1 + 1, \tag{20}$$

where $u = t, v = y + g\sqrt{-D}$. If $a \neq 0, \Im(x^2) = 0$ and $c \neq 0$, the equation (15) becomes

$$\beta_1 = -\frac{a}{2}, \beta = \frac{a}{2}, \tag{21}$$

where $u = y + g\sqrt{-D}, v = t$.

4. If $a \neq 0, \Im(x^2) \neq 0$, denote by $\beta = \dfrac{t}{2c(at+cy)}$, then (16),(17) become

$$\{\beta_{11}, \beta_{12}\} = \left\{\frac{-ac-2}{2c} + a\beta \pm a\sqrt{\beta^2 - \frac{3}{4}}\right\}, \tag{22}$$

$$\{\beta_{21}, \beta_{22}\} = \left\{\frac{ac-2}{2c} + a\beta \pm a\sqrt{\beta^2 - \frac{3}{4}}\right\}. \tag{23}$$

In the case $-D \equiv 1 \pmod 4$, then $\left\{t, y + g\dfrac{1+\sqrt{-D}}{2}\right\}$ is the canonical basis of I. Let $u = t, v = y + g\dfrac{1+\sqrt{-D}}{2}$.

1. If $a = 0, \Im(x^2) = 0$, it implies that $\dfrac{2y+g}{2}g\sqrt{D} = 0$, which cannot happen.

2. If $a = 0, \Im(x^2) \neq 0$, then $c^2 = 1$. Let $\alpha = \dfrac{t}{2y+g}$. Then (13),(14) become

$$\beta_{11} = -\frac{1}{2} - \alpha - \sqrt{\alpha^2 - \frac{3}{4}}, \beta_{21} = \beta_{11} + 1 \tag{24}$$

$$\beta_{12} = -\frac{1}{2} - \alpha + \sqrt{\alpha^2 - \frac{3}{4}}, \beta_{22} = \beta_{12} + 1. \tag{25}$$

3. If $a \neq 0, \Im(x^2) = 0$ and $c = 0$, then (15) becomes

$$\beta_1 = -\frac{1}{2} - \frac{2y+g}{2t} \text{ and } \beta_2 = \beta_1 + a. \tag{26}$$

where $u = t, v = y + g\dfrac{1+\sqrt{-D}}{2}$. If $a \neq 0, \Im(x^2) = 0$ and $c \neq 0$, then (15) becomes

$$\beta_1 = -\frac{a}{2}, \beta_2 = \frac{a}{2}. \tag{27}$$

where $u = y + g\dfrac{1+\sqrt{-D}}{2}, v = t$.

4. If $a \neq 0, \Im(x^2) \neq 0$, denote by $\beta = \dfrac{t}{c(2at+2cy+cg)}$, then (16),(17) become

$$\{\beta_{11}, \beta_{12}\} = \left\{\frac{-ac-2}{2c} + a\beta \pm a\sqrt{\beta^2 - \frac{3}{4}}\right\}, \tag{28}$$

$$\{\beta_{21}, \beta_{22}\} = \left\{\frac{-ac+2}{2c} + a\beta \pm a\sqrt{\beta^2 - \frac{3}{4}}\right\}. \tag{29}$$

Finally, we have a more efficient strategy to find all good bases of an ideal lattice I compared to the one in page 6 as follows.

□ **Step 1*:** Find the canonical basis $\{u, v\} = \{t, y + g\delta\}$ of I.

□ **Step 2*:** List all elements of I which can be extended to a basis of I.

□ **Step 3*:** For each x found in **Step 2**, identifying all good bases $\{x, y\}$ by using the formulae above. Note that such basis must satisfy the condition (4).

In **Step 2***, in case $-D \not\equiv 1 \mod 4$, we want to find $x = au + cv = (at + cy) + cg\sqrt{-D}$ which can be extended to a good basis of I. It is equivalent to $|(at + cy)c| \leq \frac{t}{2}$. Lemma 3 provides us an idea to list all pairs (a, c).

In **Case 1**, the inequality $0 < |(at + cy)c| \leq \frac{t}{2}$ implies $0 < |c| \leq \frac{t}{2}$ and $a \leq \frac{y+1}{2}$. If $a = 0$, then $c = \pm 1$ and we also have $0 < y \leq \frac{t}{2}$. For each $a \in \left[1, \frac{y+1}{2}\right]$, we must find c satisfing that

$$-\frac{t}{2} \leq (at + cy)\, c \leq \frac{t}{2}. \tag{30}$$

Let $\alpha = \frac{t}{2y}$ $(\alpha > 0)$, by considering (30) as the inequation system in c, we obtain

$$-a\alpha - \sqrt{a^2\alpha^2 + \alpha} \leq c \leq -a\alpha - \sqrt{a^2\alpha^2 - \alpha} \tag{31}$$

$$-a\alpha + \sqrt{a^2\alpha^2 - \alpha} \leq c \leq -a\alpha + \sqrt{a^2\alpha^2 + \alpha}. \tag{32}$$

Since $-1 < -a\alpha + \sqrt{a^2\alpha^2 - \alpha}$ and $-a\alpha + \sqrt{a^2\alpha^2 + \alpha} < 1$ for all $a \geq 1$, the inequality (32) implies that $c = 0$, it is contradict to $|c| > 0$. Moreover, if $a \geq 2$, then $\left(-a\alpha - \sqrt{a^2\alpha^2 - \alpha}\right) - \left(-a\alpha - \sqrt{a^2\alpha^2 + \alpha}\right) < 1$ and if $a = 1$, then $\left(-a\alpha - \sqrt{a^2\alpha^2 - \alpha}\right) - \left(-a\alpha - \sqrt{a^2\alpha^2 + \alpha}\right) \leq \sqrt{2}$. Therefore, for each $a \geq 2$, we get at most one c and when $a = 1$, we have at most two c.

In **Case 3**, if $y = 0$, then $a = 0$ and $c = \pm 1$. If $y \neq 0$, one has the conditions $at + cy = 0$ and $\gcd(a, c) = 1$. Thus, $c = -\frac{t}{\gcd(t, y)}$ and $a = \frac{y}{\gcd(t, y)}$.

Similarly, in the case $-D \equiv 1 \mod 4$, one obtains $a \leq \frac{2y + g + 1}{2}$ and then chooses nonzero c satisfying (31), $2at + 2cy + g \neq 0$ and $\gcd(a, c) = 1$ where $\alpha = \frac{t}{2y + g}$. Moreover, the conditions $2at + 2cy + cg = 0$ and $\gcd(a, c) = 1$ imply that $a = \frac{2y + g}{\gcd(2t, 2y + g)}$ and $c = -\frac{2t}{\gcd(2t, 2y + g)}$.

In the case $-D \not\equiv 1$ (mod 4), a good basis of I has a following form

$$\left\{at + c(y + g\sqrt{-D}), bt + d(y + g\sqrt{-D})\right\}.$$

Condition (4) can be rewritten as follow.

$$(at + cy)d + (bt + dy)cg \neq 0. \tag{33}$$

We compute all good bases of $\Lambda_K(I)$ by the following algorithm.

Algorithm 1. *(For $-D \not\equiv 1 \mod 4$)*

- ***Input:*** *D, t, y, g where $\left\{t, y + g\sqrt{-D}\right\}$ is the canonical basis of I.*
- ***Output:*** *The list L of all tuples (a, c, b, d) where $\left\{at + c(y + g\sqrt{-D}), bt + d(y + g\sqrt{-D})\right\}$ is a good basis of I, up to similarity.*

Step 1: *Add $(1, 0, b, 1)$ into L where $b \in \left[-\frac{1}{2} - \frac{y}{t}, \frac{1}{2} - \frac{y}{t}\right]$.*

Step 2: *If $y = 0$, then add $(0, 1, 1, 0)$ into L.*

Step 3: *If $y \neq 0$, then*

3.1. Compute $c = -\frac{t}{\gcd(t, y)}$ and $a = \frac{y}{\gcd(t, y)}$, then replace $\{a, c\}$ with $\{-c, -a\}$. Using (21) to compute $\beta_1, \beta_2 = \beta_1 + a$. Add $(a, c, -b, -d)$ satisfies (33) into L where $d \in [\beta_1, \beta_2]$ such that $1 + dc$ is a multiple of a and $b = \frac{1 + cd}{a}$.

3.2. If $t \geq 2y$, then compute $\alpha = \frac{t}{2y}$ and compute β_{11}, β_{12} using (18),(19). Let $\beta_{21} = \beta_{11} + 1$ and $\beta_{22} = \beta_{12} + 1$. Add all tuples $(0, 1, 1, d)$ satisfies (33) into L where $d \in [\beta_{11}, \beta_{21}] \cup [\beta_{12}, \beta_{22}]$. For each integer a in $\left[1, \frac{y+1}{2}\right]$, compute all nonzero integers c satisfying (31) and $at + cy \neq 0$ and $\gcd(a, c) = 1$. Compute $\beta = \frac{t}{2c(at + cy)}$ and β_{11}, β_{12} by using (22). Let $\beta_{21} = \beta_{11} + a, \beta_{22} = \beta_{12} + a$. Add (a, c, b, d) satisfies (33) into L where $b \in [\beta_{11}, \beta_{21}] \cup [\beta_{12}, \beta_{22}]$ satisfying that $1 + bc$ is a multiple of a and $d = \frac{1 + bc}{a}$.

3.3. If $t < 2y$, for each integer a in $\left[1, \frac{y+1}{2}\right]$, compute all nonzero integers c satisfying (31), $at + cy \neq 0$ and $\gcd(a, c) = 1$. Compute $\beta = \frac{t}{2c(at + cy)}$ and β_{11}, β_{12} by using (22). Let $\beta_{21} = \beta_{11} + a$ and $\beta_{22} = \beta_{12} + a$. Add (a, c, b, d) satisfies (33) into L where $b \in [\beta_{11}, \beta_{21}] \cup [\beta_{12}, \beta_{22}]$ satisfying that $1 + bc$ is a multiple of a and $d = \frac{1 + bc}{a}$.

Example 1. *Consider $K = \mathbb{Q}(\sqrt{-201})$ and $I = \langle 6 + 3\sqrt{-201}\rangle$ an ideal of K. We will find all good bases of I as follow.*

The canonical basis of I is $\left\{615, 6 + 3\sqrt{-201}\right\}$. Here $D = -201, t = 615, y = 6, g = 3$. We follow all the steps of Algorithm 1 as below.

Step 1: Since $b \in \left[\frac{-209}{410}, \frac{201}{410}\right]$, we have $b = 0$. Add $(1, 0, 0, 1)$ into L.

Step 2: We ignore Step 2 since $y = 6 \neq 0$.

Step 3: 3.1. We have $c = -\dfrac{615}{\gcd(615,6)} = -205$ and $a = \dfrac{6}{\gcd(615,6)} = 2$. Replace (a,c) with $(-c,-a)$, one has $a = 205, c = -2$. Then using (21), one obtains $\beta_1 = -102.5, \beta_2 = 102.5$. We choose $d \in [\beta_1, \beta_2]$ such that $\dfrac{1-2d}{205}$ is an integer. Thus $d = -102$ and hence $b = 1$. We add $(2, -205, -1, 102)$ into L.

3.2. Since $t \geq 2y$, one obtains

$$\alpha = \frac{t}{2y} = \frac{205}{4}, \beta_{11} \approx -102.99, \beta_{21} \approx -101.99, \beta_{12} \approx -0.5, \beta_{22} \approx 0.5.$$

Then, $d \in [-102.99, -101.99] \cup [-0.5, 0.5]$. Thus $d = -102$ or $d = 0$. Hence, we add $(0,1,1,-102), (0,1,1,0)$ into L.

Since $a \in \left[1, \dfrac{7}{2}\right]$, then $a \in \{1,2,3\}$.

- When $a = 1$, one implies $c = -102$ that satisfies (31) and $\gcd(a,c) = 1$. Then $\beta = \dfrac{-205}{204}, \beta_{11} \approx -0.99, \beta_{21} \approx 0.01, \beta_{12} \approx -2.01, \beta_{22} \approx -1.01$. It implies $b \in \{0,-2\}$ and $d \in \{1, 205\}$, respectively.
- When $a = 2$, then $c = -205$. Since $at + cy = 2.615 - 205.6 = 0$, then we eliminate the pair $(2,-205)$.
- When $a = 3$, there is no value c satisfying (31).

Thus, L contains there are 6 tuples listed the following table of which each column contains tuples defining the same lattice.

(1,0,0,1)	(2,-205,-1,102)	(0,1,1,-102)
(0,1,1,0)	(1,-102,-2,205)	(1,-102,0,1)

Therefore, there are 3 well-rounded twists of I, up to similarity, defined by the following tuples $\Big\{(1,0,0,1), (2,-205,-1,102), (0,1,1,-102)\Big\}$.

Remark 6. *Once can easily checks the similarity of well-rounded twists defined by tuples (a,b,c,d) in L obtained from above algorithms by computing $|\cos\theta_{T_\alpha B}|$ (see Lemma 1). Indeed, one has $|\cos\theta_{T_\alpha B}| = \left|\dfrac{(at+cy)c + (bt+dy)d}{(at+cy)d + (bt+dy)c}\right|$ in case $-D \not\equiv 1 \mod 4$ and*

$$|\cos\theta_{T_\alpha B}| = \left|\frac{\left(at + c.\dfrac{2y+g}{2}\right)c + \left(bt + d.\dfrac{2y+g}{2}\right)d}{\left(at + c.\dfrac{2y+g}{2}\right)d + \left(bt + d.\dfrac{2y+g}{2}\right)c}\right| \text{ in case } -D \equiv 1 \mod 4.$$

In the case $-D \equiv 1 \pmod 4$, a good basis of I has a following form

$$\left\{at + c\left(y + g\frac{1+\sqrt{-D}}{2}\right), bt + d\left(y + g\frac{1+\sqrt{-D}}{2}\right)\right\}.$$

Condition (4) can be rewritten as follow.

$$\left(at + c.\frac{2y+g}{2}\right)d + \left(bt + d.\frac{2y+g}{2}\right)c \neq 0. \tag{34}$$

We compute all good bases of $\Lambda_K(I)$ by the following algorithm.

Algorithm 2. *(For $-D \equiv 1 \mod 4$)*

- ***Input:*** *D, t, y, g where $\left\{t, y + g\frac{1+\sqrt{-D}}{2}\right\}$ is the canonical basis of I.*
- ***Output:*** *The list L of all tuples (a, c, b, d) where $\left\{at + c\left(y + g\frac{1+\sqrt{-D}}{2}\right), bt + d\left(y + g\frac{1+\sqrt{-D}}{2}\right)\right\}$ is a good basis of I.*

Step 1: *Add $(1, 0, b, 1)$ into L where b is an integer belonging to*

$$\left[-\frac{1}{2} - \frac{2y+g}{2t}, \frac{1}{2} - \frac{2y+g}{2t}\right].$$

Step 2: *2. 1. Compute $a = \dfrac{2y+g}{\gcd(2t, 2y+g)}$ and $c = -\dfrac{2t}{\gcd(2t, 2y+g)}$, then replace $\{a, c\}$ with $\{-c, -a\}$. Using (27) to compute $\beta_1, \beta_2 = \beta_1 + a$. Add $(a, c, -b, -d)$ satisfies (34) into L where $d \in [\beta_1, \beta_2]$ such that $1 + dc$ is a multiple of a and $b = \dfrac{1+bc}{a}$.*

2. 2. If $t \geq 2y + g$, compute $\alpha = \dfrac{t}{2y+g}$ and β_{11} and β_{12} by using (24) and (25). Let $\beta_{21} = \beta_{11} + 1$ and $\beta_{22} = \beta_{12} + 1$. Add all tuples $(0, 1, 1, d)$ satisfies (34) into L where $d \in [\beta_{11}, \beta_{21}] \cup [\beta_{12}, \beta_{22}]$. For each integer a in $\left[1, \dfrac{2y+g+1}{2}\right]$, compute all nonzero integers c satisfying (31), $\gcd(a, c) = 1$ and $2at + 2cy + cg \neq 0$. Compute $\beta = \dfrac{t}{c(2at + 2cy + cg)}$ and β_{11}, β_{12} using (28). Let $\beta_{21} = \beta_{11} + a, \beta_{22} = \beta_{12} + a$. Add (a, c, b, d) satisfies (34) into L where $b \in [\beta_{11}, \beta_{21}] \cup [\beta_{12}, \beta_{22}]$ satisfying that $1 + bc$ is a multiple of a and $d = \dfrac{1+bc}{a}$.

2. 3. If $t < 2y + g$, for each integer a in $\left[1, \dfrac{2y+g+1}{2}\right]$, compute all nonzero integers c satisfying (31), $\gcd(a, c) = 1$ and $2at + 2cy + cg \neq 0$. Compute $\beta = \dfrac{t}{c(2at + 2cy + cg)}$ and $\beta_{11}, \beta_{12}, \beta_{21} = \beta_{11} + a, \beta_{22} = \beta_{12} + a$ using (28). Add (a, c, b, d) satisfies (34) into L where $b \in [\beta_{11}, \beta_{21}] \cup [\beta_{12}, \beta_{22}]$ satisfying that $1 + bc$ is a multiple of a and $d = \dfrac{1+bc}{a}$.

5. Analysis of Algorithm 1 and Algorithm 2

In this section, we will prove the correctness and the complexity of Algorithms 1 and 2.

5.1. **Correctness.** Let I be an ideal with the canonical basis $\{t, y+g\delta\}$. We prove that tuples (a, c, b, d) outputted from Algorithm 1 form good bases $\{z, z'\}$ where $z = at + c\,(y+g\delta)$ and $z' = bt + d\,(y+g\delta)$.

Definition 6. *Suppose that I is an ideal of $\mathcal{O}_K$ and $\{t, y+g\delta\}$ its canonical basis. A* ***good tuple*** *is a tuple (a, c, b, d) of integer numbers satisfying that $\{z, z'\}$ is a good basis of I where $z = at + c\,(y+g\delta)$, $z' = bt + d\,(y+g\delta)$. A pair (a, c) is called* ***extendable*** *for I if $z = at + c\,(y+g\delta)$ can be extended to a good basis of I.*

We prove the correctness of Algorithm 1 as below.

Proposition 11. *All tuples (a, c, b, d) in the output of Algorithm 1 are good tuples of I. Inversely, the output of Algorithm 1 completely exports all good tuples of I, up to similarity.*

Proof. We notice that (a, c, b, d) is a good tuple if and only if (a, c) is extendable. By the argument of given in the proof of Lemma 3, the pair (a, c) is extendable if and only if $\gcd(a, c) = 1$ and $|c(at + cy)| \leq \frac{t}{2}$. Hence, it is trivial to prove this proposition using the computation shown before Algorithm 1. □

Similarly, we can show the correctness of Algorithm 2 as below.

Proposition 12. *All tuples (a, c, b, d) in output of Algorithm 2 are good tuples of I. Inversely, the output of Algorithm 2 completely exports all good tuples of I, up to similarity.*

5.2. **Complexity.** In this section, we provide an upper bound for the number of loops and operations in Algorithms 1 and 2.

Lemma 6. *The total number of loops of Algorithm 1 is at most $y + 2$. In addition, an upper bound for the number of operations (expect addition) of each loop in Algorithm 1 is 57.*

Proof. It is easy to see the first statement. Since the maximum number of operations in Algorithm 1 occurs when $a \in \left[1, \frac{y+1}{2}\right]$ and it took us 57 operations (expect addition), the second statement is obtained. □

Lemma 7. *The largest number computed in Algorithm 1 is $\frac{5t(y+1)+8}{8}$.*

Proof. First, we have $|c| \leq \frac{t}{2}$ and $a \leq \frac{y+1}{2}$. Using (18) and (19), one obtains that $-\frac{1}{2} - 2\alpha \leq \beta_{11}, \beta_{12} \leq -\frac{1}{2}$.

In case of applying (22), since $c < 0$ and $a > 0$, one has

$$\frac{1}{2} \leq \left| \frac{ac-2}{2c} + a\beta \pm a\sqrt{\beta^2 - \frac{3}{4}} \right| \leq \frac{|ac-2|}{2} + 2a|\beta| \leq \frac{t(y+1)+8}{8} + \frac{t(y+1)}{2} = \frac{5t(y+1)+8}{8}.$$

In the other words, we have the following inequality $|\beta_{ij}| \leq \dfrac{5t(y+1)+8}{8}$.
If we employ (20),(21) to compute β_1, then $|\beta_1| \leq y+1$.
Thus $\dfrac{5t(y+1)+8}{8}$ is the maximum number computed in Algorithm 1. □

Similarly, we have the following results for Algorithm 2.

Lemma 8. *In Algorithm 2, the total number of loops of is at most* $2y+g+2$ *and an upper bound for the number of operations of each loop is* 65*. In addition, the largest number computed in this algorithm is* $\dfrac{5t(2y+g+1)+4}{4}$.

Acknowledgement

The third author acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC) (funding RGPIN-2019-04209 and DGECR- 2019-00428).

References

[1] K. A. K. Banihashemi, A. H. Inverse determinant sums and connections between fading channel information theory and algebra. *IEEE Transactions on Information Theory*, 44(1):162–171, 1998.

[2] M. T. Damir, O. Gnilke, L. Amorós, and C. Hollanti. Analysis of some well-rounded lattices in wiretap channels. In *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pages 1–5. IEEE, 2018.

[3] M. T. Damir and D. Karpuk. Well-rounded twists of ideal lattices from real quadratic fields. *Journal of Number Theory*, 196:168–196, 2019.

[4] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On well-rounded ideal lattices ii. *Int. J. Number Theory*, 09(01):139–154, 2013.

[5] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *Int. J. Number Theory*, 8(1):189–206, 2012.

[6] O. W. Gnilke, A. Barreal, A. Karrila, H. T. N. Tran, D. A. Karpuk, and C. Hollanti. Well-rounded lattices for coset coding in mimo wiretap channels. In *Telecommunication Networks and Applications Conference (ITNAC), 2016 26th International*, pages 289–294. IEEE, 2016.

[7] O. W. Gnilke, H. T. N. Tran, A. Karrila, and C. Hollanti. Well-rounded lattices for reliability and security in rayleigh fading siso channels. In *Information Theory Workshop (ITW), 2016 IEEE*, pages 359–363. IEEE, 2016.

[8] H. W. Lenstra. Algorithms in algebraic number theory. *Bulletin of the American Mathematical Society*, 26(2):211–244, 1992.

[9] J. Martinet. *Perfect lattices in Euclidean spaces*, volume 327. Springer Science & Business Media, 2013.

[10] P. Q. Nguyen. Hermite's constant and lattice algorithms. In *The LLL Algorithm*, pages 19–69. Springer, 2009.

[11] O. N. Solan. Stable and well-rounded lattices in diagonal orbits. *Israel Journal of Mathematics*, 234(2):501–519, 2019.