CANONICAL BASIS TWISTS OF IDEAL LATTICES FROM REAL QUADRATIC NUMBER FIELDS

MOHAMED TAOUFIQ DAMIR AND LENNY FUKSHANSKY

Abstract. Ideal lattices in the plane coming from real quadratic number fields have been investigated by several authors in the recent years. In particular, it has been proved that every such ideal has a basis that can be twisted by the action of the diagonal group into a Minkowski reduced basis for a well-rounded lattice. We explicitly study such twists on the canonical bases of ideals, which are especially important in arithmetic theory of quadratic number fields and binary quadratic forms. Specifically, we prove that every fixed real quadratic field has only finitely many ideals whose canonical basis can be twisted into a well-rounded or a stable lattice in the plane. We demonstrate some explicit examples of such twists. We also briefly discuss the relation between stable and well-rounded twists of arbitrary ideal bases.

1. Introduction

Euclidean lattices, metrized free $\mathbb{Z}$-modules in real vector spaces, are central to number theory and discrete geometry. In addition to their arithmetic and geometric appeal, lattices are also key to discrete optimization, often providing solutions to classical optimization questions like sphere packing, covering and kissing number problems. They are also extensively used in applied areas, such as coding theory, cryptography and other areas of digital communications; see the famous book by Conway and Sloane [5] for a wealth of information on the theory of lattices and their numerous connections and applications. In this paper, we focus on certain geometric properties of lattices that are of utmost interest for both, theory and applications. One of the main sources of lattices possessing these special properties is the classical Minkowski construction from ideals in rings of integers of algebraic number fields: not only does this construction allow for a nice and compact description of the resulting lattices, but also algebraic properties of an ideal often inform the geometry of the corresponding lattice.

Let $L \subset \mathbb{R}^n$ be a free $\mathbb{Z}$-module of rank $k \leq n$, then

$$L = B\mathbb{Z}^n = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_k\},$$

where $\boldsymbol{b}_1, \dots, \boldsymbol{b}_n \in \mathbb{R}^n$ are $\mathbb{R}$-linearly independent basis vectors for L and $B = (\boldsymbol{b}_1 \ \dots \ \boldsymbol{b}_n) \in \mathrm{GL}_n(\mathbb{R})$ is the corresponding basis matrix. Then for any $U \in \mathrm{GL}_n(\mathbb{Z})$, BU is also a basis matrix for L, i.e. $L = BU\mathbb{Z}^n$ for any $U \in \mathrm{GL}_n(\mathbb{Z})$.

2010 *Mathematics Subject Classification.* Primary 11R11, 11H06, 11H55.

Key words and phrases. Well-rounded lattices, stable lattices, ideal lattices, real quadratic fields.

Damir was partially supported by the Academy of Finland through grants #276031, #282938, and #303819 awarded to C. Hollanti. Fukshansky was partially supported by the Simons Foundation grant #519058.

Let $f(\boldsymbol{x}) = f(x_1, \dots, x_n) \in \mathbb{R}[x_1, \dots, x_n]$ be a positive definite quadratic form, i.e. $f(\boldsymbol{x}) = \boldsymbol{x}^t Q \boldsymbol{x}$, where Q is an $n \times n$ symmetric positive definite coefficient matrix for f. Then $Q = A^t A$ for some $A \in \mathrm{GL}_n(\mathbb{R})$, so

$$f(\boldsymbol{x}) = (A\boldsymbol{x})^t (A\boldsymbol{x}). \tag{1}$$

Thus we will use notation f_A for the form f as in (1) with coefficient matrix $A^t A$ for some $A \in \mathrm{GL}_n(\mathbb{R})$.

We will use the term *lattice* to refer to a pair (L, f_A), where the form f_A is used to define the norm of vectors in L. If $A = I_n$, the $n \times n$ identity matrix, then f_A is $\| \ \|^2$, the square of the usual Euclidean norm, in which case we simply write L instead of (L, f_{I_n}). In general, let $\boldsymbol{x} = B\boldsymbol{y} \in L$, i.e. $\boldsymbol{y} \in \mathbb{Z}^n$, so

$$f_A(\boldsymbol{x}) = (AB\boldsymbol{y})^t (AB\boldsymbol{y}) = \boldsymbol{y}^t (AB)^t (AB)\boldsymbol{y} = \|(AB)\boldsymbol{y}\|^2. \tag{2}$$

In other words, a lattice (L, f_A) can be identified with the lattice AL, which we will refer to as the *twist* of L by A. Now, for a lattice L we define its rank, $\mathrm{rk}(L)$, to be the cardinality of its basis, and its determinant

$$\det(L) := \left|\det(B^\top B)\right|^{1/2},$$

where B is a basis matrix for L.

There are two important classes of lattices we will discuss. A lattice L is called *well-rounded* (abbreviated WR) if there exist n linearly independent vectors $\boldsymbol{c}_1, \dots, \boldsymbol{c}_n \in L$ such that

$$\|\boldsymbol{c}_1\| = \cdots = \|\boldsymbol{c}_n\| = |L|,$$

where $|L| := \min_{\boldsymbol{x} \in L \setminus \{\boldsymbol{0}\}} \|\boldsymbol{x}\|$. On the other hand, L is called *stable* if for each sublattice $L' \subseteq L$,

$$\det(L)^{1/rk(L)} \leq \det(L')^{1/rk(L')},$$

and L is called unstable otherwise. Well-roundedness and stability are independent properties for lattices of rank greater than two: WR lattices can be unstable and stable lattices do not have to be WR. On the other hand, in the plane WR lattices form a proper subset of stable lattices [8]. There is an important equivalence relation on the space of lattices: two lattices are called *similar* if they are related by a dilation and an orthogonal transformation; geometric properties, like well-roundedness and stability are preserved under the similarity, hence we can talk about WR or stable similarity classes of lattices.

Both of these types of lattices are very important in reduction theory of algebraic groups. In particular, they were studied in the context of the diagonal group action on the space of lattices. Let

$$\mathcal{A} = \left\{ A = (a_{ij}) \in \mathrm{GL}_n(\mathbb{R}) : a_{ij} = 0 \ \forall \ i \neq j, \ a_{ii} > 0 \ \forall \ i, \ \prod_{i=1}^n a_{ii} = 1 \right\} \tag{3}$$

be the group of real positive diagonal matrices with determinant 1. This group acts on the space of lattices in $\mathbb{R}^n$ by left multiplication: $L \mapsto AL$ for each $A \in \mathcal{A}$ and lattice $L \subset \mathbb{R}^n$. A celebrated result of McMullen [13] in connection with his work on Minkowski's conjecture asserts that any bounded $\mathcal{A}$-orbit of lattices contains a well-rounded lattice. Inspired by McMullen's work, Shapira and Weiss proved [17] that the orbit closure of a lattice under the action of $\mathcal{A}$ also contains a stable lattice.

Throughout this note, let K be a totally real number field of degree n with the ring of integers $\mathcal{O}_K$, $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{R}$ be the embeddings of K, and define the Minkowski embedding

$$\sigma_K = (\sigma_1, \dots, \sigma_n) : K \hookrightarrow \mathbb{R}^n.$$

Let $I \subset K$ be a full module, i.e. a $\mathbb{Z}$-module of rank n, for instance $\mathcal{O}_K$ or any (fractional) ideal. We define $L_K(I) := \sigma_K(I)$, i.e. the image of I under Minkowski embedding, then $AL_K(I)$ is a lattice in $\mathbb{R}^n$ for any $A \in \mathrm{GL}_n(\mathbb{R})$.

Proposition 1.1. *With notation as above, there exist $A, B \in \mathcal{A}$ such that the lattice $AL_K(I)$ is WR and $BL_K(I)$ is stable.*

Proof. By the similarity relation, we can assume that $L_K(I)$ is unimodular without loss of generality. Consider the orbit of $L_K(I)$ under the action of $\mathcal{A}$, i.e. the set

$$\mathcal{A}L_K(I) = \{AL_K(I) : A \in \mathcal{A}\}.$$

Since $L_K(I)$ comes from a full module in a totally real number field, Theorem 3.1 of [13] implies that the orbit $\mathcal{A}L_K(I)$ is compact. Then Theorem 1.3 of [13] implies that this orbit contains a WR lattice and Theorem 1.1 of [17] implies that it also contains a stable lattice, i.e. there exist some $A, B \in \mathcal{A}$ such that the lattice $AL_K(I)$ is WR and the lattice $BL_K(I)$ is stable. □

Remark 1.1. The proofs of Theorem 1.3 of [13] and of Theorem 1.1 of [17] are not constructive, meaning that they do not help to explicitly find $A, B \in \mathcal{A}$ such that the lattice $AL_K(I)$ is WR and $BL_K(I)$ is stable.

Now let $I \subseteq \mathcal{O}_K$ be an ideal. Let $\alpha \in K$ be totally positive, i.e. $\sigma_i(\alpha) > 0$ for all $1 \leq i \leq n$, then the pair (I, α) gives rise to the *ideal lattice* $(L_K(I), f_{A(\alpha)})$, where

$$A(\alpha) = \begin{pmatrix} \sqrt{\sigma_1(\alpha)} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sqrt{\sigma_n(\alpha)} \end{pmatrix}.$$

Ideal lattices have been extensively studied by a number of authors, especially E. Bayer-Fluckiger (see [1] for a survey of this topic); a systematic study of WR ideal lattices has been initiated in [11] and [10], where it was shown that WR ideal lattices $(L_K(I), \| \|^2)$ from quadratic number fields are relatively sparse. The situation is different if we allow a more general quadratic norm form f_A. Notice that $A(\alpha) \in \mathcal{A}$ if and only if $\alpha \in \mathcal{O}_K$ is a totally positive unit. More generally, $\mathcal{A}_1(K) := \{A(\alpha) : \alpha \in K \text{ is totally positive}\}$ is also a multiplicative group of (positive) diagonal matrices so that

$$\mathcal{A} \cap \mathcal{A}_1(K) = \{A(\alpha) : \alpha \in K \text{ is totally positive and } \mathbb{N}_K(\alpha) = 1\},$$

where $\mathbb{N}_K$ stands for the number field norm on K. In fact, notice that the set

$$\mathcal{A}_1'(K) = \left\{ \mathbb{N}_K(\alpha)^{-1/n} \mathcal{A}(\alpha) : A(\alpha) \in \mathcal{A}_1(K) \right\}$$

is a proper subset of $\mathcal{A}$, while the lattices $(L_K(I), f_{A(\alpha)})$ and $(L_K(I), f_{\mathbb{N}_K(\alpha)^{-1/n}A(\alpha)})$ are scalar multiples of each other, and hence have the same properties.

Question 1. *By Proposition 1.1, we know that, given $L_K(I)$, there exists $A, B \in \mathcal{A}$ such that $AL_K(I)$ is WR and $BL_K(I)$ is stable, but do there exist such $A, B \in \mathcal{A}_1(K)$?*

In this note, we consider the two-dimensional situation, for which this question was answered in the affirmative for WR lattices in [2] (specifically, see Corollary 3.1). Further, the authors construct explicit examples of principal ideal lattices (i.e., those coming from full rings of integers) similar to the square and the hexagonal lattices. Of course, this immediately implies the same affirmative answer for stable lattices, since in two dimensions WR lattices are stable; in fact, unlike the WR situation, there are infinitely many stable ideal lattices from real quadratic number fields even without twisting by a matrix, as proved in [8]. Our goal here is to further explicitly investigate well-roundedness and stability properties of planar ideal lattices. First we need some more notation.

Definition 1.1. Given a particular basis matrix B for a lattice L, we will say that B is *WR twistable* (respectively, *stable twistable*) if there exists $A \in \mathcal{A}$ such that $AB\mathbb{Z}^n$ is WR (respectively, stable) with AB being the shortest basis matrix, as discussed in Section 2. We will refer to the resulting lattices as a *WR twist* (respectively, *stable twist*) of the original lattice by the matrix A, respectively.

While WR twistable bases have been discussed in [6], to the best of our knowledge stable twistable bases have not previously been investigated. A criterion to determine whether a given basis for an ideal lattice from a real quadratic number field K is WR twistable or not was given in [6]: this criterion in particular implies there can be only finitely many such bases for a fixed ideal lattice. Further, Proposition 7 of [6] asserts that a basis is WR twistable by some $A \in \mathcal{A}$ if and only if it is WR twistable by some $A(\alpha) \in \mathcal{A}_1(K)$, and an explicit construction of such corresponding twists is given.

In this note, we focus on the twistable properties of the particularly important kind of basis for ideals in quadratic number fields, the so-called canonical basis. We always talk about twists by matrices $A(\alpha) \in \mathcal{A}_1(K)$ for some totally positive $\alpha \in K$, referring to such twists as a twist by α.

Let $D \in \mathbb{Z}_{>0}$ be squarefree and let $K = \mathbb{Q}(\sqrt{D})$. Let $I \subseteq \mathcal{O}_K$ be an ideal. Notice that $\mathcal{O}_K = \mathbb{Z}[\delta]$, where

$$\delta = \begin{cases} -\sqrt{D} & \text{if } D \not\equiv 1 \pmod 4 \\ \frac{1-\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod 4 \end{cases} \tag{4}$$

The embeddings $\sigma_1, \sigma_2 : K \to \mathbb{R}$ are given by

$$\sigma_1(x + y\sqrt{D}) = x + y\sqrt{D},\ \ \sigma_2(x + y\sqrt{D}) = x - y\sqrt{D}$$

for each $x + y\sqrt{D} \in K$. The number field norm on K is given by

$$\mathbb{N}_K(x + y\sqrt{D}) = \sigma_1(x + y\sqrt{D})\sigma_2(x + y\sqrt{D}) = \left(x + y\sqrt{D}\right)\left(x - y\sqrt{D}\right).$$

Now $I \subseteq \mathcal{O}_K$ is an ideal if and only if

$$I = \{ax + (b + g\delta)y : x, y \in \mathbb{Z}\}, \tag{5}$$

for some $a, b, g \in \mathbb{Z}_{\geq 0}$ such that

$$b < a,\ \ g \mid a, b,\ \text{ and } ag \mid \mathbb{N}(b + g\delta). \tag{6}$$

Such integral basis $a, b + g\delta$ is unique for each ideal I and is called the *canonical basis* for I (see Section 6.3 of [4] for a detailed exposition): it is important in the arithmetic theory of binary quadratic forms and quadratic number fields. For instance, canonical basis is used to determine reduced ideals and compute the ideal class group in quadratic fields (see, e.g., the classical work of H. H. Mitchell [14] as well as a more recent paper [18]), and it is employed for number field computations in several modern computer algebra systems; it has also been used in the previous study of geometric properties of ideal lattices in the plane (see [11], [10], [8], [6]). It is then easy to check that $L_K(I) = B\mathbb{Z}^2$, where

$$B = \begin{pmatrix} a & b - g\sqrt{D} \\ a & b + g\sqrt{D} \end{pmatrix}, \tag{7}$$

when $D \not\equiv 1 (\operatorname{mod} 4)$, and

$$B = \begin{pmatrix} a & \frac{2b+g}{2} - \frac{g\sqrt{D}}{2} \\ a & \frac{2b+g}{2} + \frac{g\sqrt{D}}{2} \end{pmatrix}, \tag{8}$$

when $D \equiv 1 (\operatorname{mod} 4)$. Then any other basis matrix for $L_K(I)$ is of the form BU for some $U \in \mathrm{GL}_2(\mathbb{Z})$. We can now state our result about WR K-twists of canonical bases of planar ideal lattices from real quadratic number fields.

Theorem 1.2. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field and $\mathcal{O}_K$ its ring of integers. There can be at most finitely many ideals in $\mathcal{O}_K$, up to similarity of the resulting ideal lattices, with the canonical basis being WR twistable: if this is the case for some ideal I with canonical basis $a, b + g\delta$, then*

$$b < \begin{cases} g\sqrt{D} & \text{if } D \not\equiv 1 \ (\operatorname{mod} 4), \\ \frac{(\sqrt{D}-1)g}{2} & \text{if } D \equiv 1 \ (\operatorname{mod} 4). \end{cases}$$

The canonical basis for $\mathcal{O}_K$ is WR twistable if and only if $K = \mathbb{Q}(\sqrt{5})$.

Remark 1.2. In fact, the assertion that the canonical basis of $\mathcal{O}_K$ is WR twistable if and only if $K = \mathbb{Q}(\sqrt{5})$ also follows from Corollary 2 of [6].

The set of similarity classes of planar WR lattices is parameterized by a curve, while the set of similarity classes of planar stable lattices is two-dimensional (see [9] for details). The results of [9] also indicate that the set of stable ideal lattices in the plane is likely order of magnitude larger than the set of WR ideal lattices: at least this is true for planar arithmetic lattices. With this in mind, it is somewhat surprising that the number of ideal lattices with stable twistable canonical basis is not much larger than with WR twistable canonical basis: this is an interesting property of the canonical basis.

Theorem 1.3. *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field and $\mathcal{O}_K$ its ring of integers. There can be at most finitely many ideals in $\mathcal{O}_K$, up to similarity of the resulting ideal lattices, with the canonical basis being stable twistable: if this is the case for some ideal I with canonical basis $a, b + g\delta$, then*

$$b < \begin{cases} \frac{2}{\sqrt{3}} g\sqrt{D} & \text{if } D \not\equiv 1 \ (\operatorname{mod} 4), \\ \frac{g}{2}\left(\frac{2}{\sqrt{3}}\sqrt{D} - 1\right) & \text{if } D \equiv 1 \ (\operatorname{mod} 4). \end{cases}$$

The canonical basis for $\mathcal{O}_K$ is stable twistable if and only if $K = \mathbb{Q}(\sqrt{5})$.

While our results prove finiteness of the number of ideals in each fixed number field with WR or stable twistable canonical basis, there are still more ideals with stable twistable than with WR twistable canonical basis as we demonstrate in Section 4. We set some additional notation in Section 2, including convenient explicit criteria to check if the canonical basis of a planar ideal lattice is WR or stable twistable, or not. We prove Theorem 1.2 and give some explicit examples of ideal lattices with WR twistable canonical basis in Section 3. In Section 4 we prove Theorem 1.3 and show examples of ideal lattices with stable twistable (but not WR twistable) canonical basis in Section 3. Finally, in Section 5 we make some remarks on the relation between stable and WR twists of arbitrary ideal bases.

Let us conclude this section with a few additional words of motivation for our results. Our theorems reveal certain new properties of the canonical basis for ideals in quadratic number fields. Canonical bases have an advantage of being convenient for computations, including explicit computations of WR and stable lattices, as demonstrated in [11], [10] and [8]. Knowing which of those that are not WR or stable to start with can be twisted into WR or stable shortest bases is helpful. Further, this information may find some future applications when choosing ideal lattice bases for lattice codes constructions. In Section 6 we include some additional details on applications of the WR and stable twists of lattice bases in communication theory and in arithmetic theory of quadratic forms and lattices. We are now ready to proceed.

2. Notation and setup

We start here with a basic review of some general lattice theory background. If rank of L is $n \geq 2$, we define the *successive minima* of L to be the real numbers

$$0 < \lambda_1 \leq \dots \leq \lambda_n$$

such that

$$\lambda_i = \inf \left\{ \mu \in \mathbb{R} : \dim_{\mathbb{R}} \{ \boldsymbol{x} \in L : \| \boldsymbol{x} \| \leq \mu \} = i \right\}.$$

Then $\lambda_1 = |L|_{\| \ \|^2}$, and L is WR if and only if $\lambda_1 = \dots = \lambda_n$. Linearly independent vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_n \in L$ such that $\|\boldsymbol{x}_i\| = \lambda_i$ are called *vectors corresponding to successive minima*. They do not necessarily form a basis for L. On the other hand, L has a *Minkowski reduced basis* $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n$, defined by the conditions that

$$\|\boldsymbol{v}_1\| = \lambda_1, \ \|\boldsymbol{v}_i\| = \min \left\{ \|\boldsymbol{x}\| : \boldsymbol{v}_1, \dots \boldsymbol{v}_{i-1}, \boldsymbol{x} \text{ are extendable to a basis for } L \right\}.$$

In general, $\|\boldsymbol{v}_i\| \geq \lambda_i$, and when $n \geq 5$ these inequalities can be strict, although a theorem of van der Waerden asserts that for all $i \geq 4$,

$$\|\boldsymbol{v}_i\| \leq \left(\frac{5}{4} \right)^{i-4} \lambda_i, \tag{9}$$

and there is a conjecture that the constant in the upper bound of (9) can be improved. When $n \leq 4$, a Minkowski reduced basis for a lattice L always consists of vectors corresponding to successive minima. For each $n \geq 2$, there are finitely many inequalities that have to be satisfied by the vectors $\boldsymbol{v}_1, \dots, \boldsymbol{v}_n \in L$ to be a Minkowski reduced basis for L. The number of such inequalities depends only on n, but it grows fast with n. The explicit list of non-redundant inequalities is known only for $n \leq 7$ (it is called Tammela's list); see §§2.2-2.3 of [16] for Tammela's list, as well as more information on Minkowski reduction and relation to successive minima.

Let $L = (\boldsymbol{v}_1\ \boldsymbol{v}_2)\ \mathbb{Z}^2$ be a planar lattice. The necessary and sufficient conditions for the basis $\boldsymbol{v}_1, \boldsymbol{v}_2$ to be Minkowski reduced (and hence to correspond to successive minima λ_1, λ_2) are as follows:

$$\|\boldsymbol{v}_1\| \leq \|\boldsymbol{v}_2\|,\ 2|\boldsymbol{v}_1^t \boldsymbol{v}_2| \leq \|\boldsymbol{v}_1\| \|\boldsymbol{v}_2\|. \tag{10}$$

In order for L to be WR we need $\lambda_1 = \lambda_2$, i.e.

$$\|\boldsymbol{v}_1\| = \|\boldsymbol{v}_2\|,\ 2|\boldsymbol{v}_1^t \boldsymbol{v}_2| \leq \|\boldsymbol{v}_1\|^2, \tag{11}$$

and in order for L to be stable we need

$$\sqrt{\det(L)} \leq \|\boldsymbol{v}_1\|,\ 2|\boldsymbol{v}_1^t \boldsymbol{v}_2| \leq \|\boldsymbol{v}_1\| \|\boldsymbol{v}_2\|. \tag{12}$$

The angle θ between $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ must therefore be in the interval $[\pi/3, 2\pi/3]$, and $|\cos\theta|$ is an invariant of the lattice. Two planar WR lattices L_1, L_2 are similar if and only if these values are the same (see [7]). There is an easy way to "deform" a non-WR lattice into a WR one.

Lemma 2.1. *Let $L = (\boldsymbol{v}_1\ \boldsymbol{v}_2)\ \mathbb{Z}^2 \subset \mathbb{R}^2$ be a lattice of full rank, where $\boldsymbol{v}_1, \boldsymbol{v}_2$ is a Minkowski reduced basis matrix, so $\|\boldsymbol{v}_1\| = \lambda_1, \|\boldsymbol{v}_2\| = \lambda_2$ for the successive minima $\lambda_1 \leq \lambda_2$ of L. Let $\boldsymbol{u}_1 = \lambda_2 \boldsymbol{v}_1$, $\boldsymbol{u}_2 = \lambda_1 \boldsymbol{v}_2$, then the lattice $M = (\boldsymbol{u}_1\ \boldsymbol{u}_2)\ \mathbb{Z}^2$ is a well-rounded lattice with successive minima equal to $\lambda_1 \lambda_2$.*

Proof. This follows immediately from Lemma 3.6 of [7]. □

Remark 2.1. In principle, there is a deformation of a lattice into a WR lattice in higher dimensions too, but it is more complicated. Such a deformation is described in Remark 3.3 of [12].

We now come back to the ideal lattices. Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic number field and $\alpha = p + q\sqrt{D} \in K$ be totally positive, then

$$A(\alpha) = \begin{pmatrix} \sqrt{p + q\sqrt{D}} & 0 \\ 0 & \sqrt{p - q\sqrt{D}} \end{pmatrix},$$

where $p \pm q\sqrt{D} > 0$; in fact, we can assume without loss of generality that p, q are positive rational numbers. Let B as in (7) or (8) be the canonical basis matrix for an ideal lattice $L_K(I)$, where $I \subseteq \mathcal{O}_K$ is the corresponding ideal. Then B is WR twistable (respectively, stable twistable) if

$$C := A(\alpha)B = \begin{cases} \begin{pmatrix} a\sqrt{p + \sqrt{D}} & (b - g\sqrt{D})\sqrt{p + \sqrt{D}} \\ a\sqrt{p - \sqrt{D}} & (b + g\sqrt{D})\sqrt{p - \sqrt{D}} \end{pmatrix} & \text{if } D \not\equiv 1 \pmod 4, \\ \begin{pmatrix} a\sqrt{p + \sqrt{D}} & \left(\frac{(2b+g) - g\sqrt{D}}{2}\right)\sqrt{p + \sqrt{D}} \\ a\sqrt{p - \sqrt{D}} & \left(\frac{(2b+g) + g\sqrt{D}}{2}\right)\sqrt{p - \sqrt{D}} \end{pmatrix} & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

is a Minkowski reduced basis for WR (respectively, stable) lattice $C\mathbb{Z}^2$. These conditions can be described by explicit inequalities, stemming from (11) and (12). First assume that $D \not\equiv 1 (\operatorname{mod} 4)$, then B is WR twistable by $\alpha = p + q\sqrt{D}$ if and only if

$$a^2 p = (Dg^2 + b^2)p - 2qbgD,\ \left|b^2 - g^2 D + a^2\right| \leq ab, \tag{13}$$

and B is stable twistable by α if and only if

$$\begin{aligned} -4D^2g^2q^2 + 6bDgpq + Dg^2p^2 - 3b^2p^2 \geq 0, \\ \min\left\{a^2p, (Dg^2+b^2)p - 2Dbgq\right\} \geq ag\sqrt{D(p^2-q^2D)}. \end{aligned} \tag{14}$$

On the other hand, if $D \equiv 1 (\operatorname{mod} 4)$, then B is WR twistable by $\alpha = p + q\sqrt{D}$ if and only if

$$\begin{aligned} 2a^2p = \frac{1}{2}\left((D+1)p - 2Dq)\right)g^2 - 2b(Dq-p)g + 2b^2p, \\ \left|4a^2+4b^2+4bg-(D-1)g^2\right| \leq 2a(2b+g), \end{aligned} \tag{15}$$

and B is stable twistable by α if and only if

$$\begin{aligned} -D^2g^2q^2 + 3Dgbpq + \frac{3}{2}Dg^2pq - 3b^2p^2 - 3bgp^2 - \frac{3}{4}g^2p^2 + \frac{1}{4}Dg^2p^2 \geq 0 \\ \min\left\{2a^2p, ag(p-Dq)+2abp\right\} \geq ag\sqrt{D(p^2-q^2D)}. \end{aligned} \tag{16}$$

We can now use these criteria to analyze the WR and stable twistable properties of the canonical bases for ideals in real quadratic number fields.

3. Proof of Theorem 1.2

In this section we prove Theorem 1.2 step by step. Let $K = \mathbb{Q}(\sqrt{D})$ for a squarefree integer $D > 1$. Let $I \subseteq \mathcal{O}_K$ be an ideal with the canonical basis $a, b + g\delta$ as described in (6). Suppose this basis is WR twistable by some totally positive $\alpha = p + q\sqrt{D} \in K$. First assume that $K = \mathbb{Q}(\sqrt{D})$ with $D \not\equiv 1 \ (\operatorname{mod} 4)$, then by (13) we must have

$$p = \left(\frac{2bgD}{b^2+g^2D-a^2}\right)q \text{ and } \left|b^2-g^2D+a^2\right| \leq ab.$$

We should remark that the first identity holds, unless the denominator $b^2 + g^2D - a^2 = 0$, which is not possible: if this is the case, then (13) implies that $b = 0$, and so $a^2 = g^2D$, which contradicts D being squarefree. Since p must be positive, we have $a^2 < b^2 + g^2D$. If $b^2 > g^2D$, we have

$$a^2 < (b^2 - g^2D) + a^2 \leq ab,$$

meaning that $a < b$, which contradicts the choice of the canonical basis. Hence we must have $b^2 < g^2D$: equality is not possible since D is squarefree. If $I = \mathcal{O}_K$, then $a = 1, b = 0, g = 1$, and so we must have $|1 - D| \leq 0$, which is a contradiction. Hence $\mathcal{O}_K$ cannot have WR twistable canonical basis.

Now suppose that $D \equiv 1 \ (\operatorname{mod} 4)$, then by (15) we must have

$$p = \left(\frac{2gD(2b+g)}{4b^2+g^2(D+1)+4b-4a^2}\right)q,$$

unless $4b^2 + g^2(D+1) + 4b - 4a^2 = 0$, in which case $2b + g = 0$: this is not possible, since $g \mid b$. Additionally, (15) implies that

$$\left|4a^2+4b^2+4bg-(D-1)g^2\right| \leq 2a(2b+g). \tag{17}$$

Since p must be positive, we have $a^2 < b^2 + b + \frac{g^2(D+1)}{4}$. If $b^2 + bg > \frac{(D-1)g^2}{4}$, then we get

$$4a^2 < 4a^2 + 4b^2 + 4bg - (D-1)g^2 \leq 2a(2b+g),$$

and so $a < b + g/2$, which contradicts the fact that $g \mid a - b$. Hence we must have $b^2 + bg \leq \frac{(D-1)g^2}{4}$, which means that $b < \frac{(\sqrt{D}-1)g}{2}$: again, equality is not possible since D is squarefree. If $I = \mathcal{O}_K$, then $a = 1, b = 0, g = 1$, so $p = \frac{2Dq}{D-3}$. Hence $\alpha = q\left(\frac{2D}{D-3} + \sqrt{D}\right)$, which again is not totally positive unless $D = 5$ (otherwise $D \geq 13$, and so $2D/(D-3) < \sqrt{D}$). If $D = 5$, then we can take $\alpha = 5 + \sqrt{5}$, obtaining the matrix

$$A(\alpha)B = \begin{pmatrix} \sqrt{5+\sqrt{5}} & \frac{(1-\sqrt{5})\sqrt{5+\sqrt{5}}}{2} \\ \sqrt{5-\sqrt{5}} & \frac{(1+\sqrt{5})\sqrt{5-\sqrt{5}}}{2} \end{pmatrix}$$

with orthogonal columns, both of norm $= \sqrt{10}$. Hence $\mathcal{O}_K$ cannot have WR twistable canonical basis for any real quadratic number field $K \neq \mathbb{Q}(\sqrt{5})$.

Finally notice that if I is an ideal with canonical basis $a, b + g\delta$ and $I' = \frac{1}{g}I$ is the corresponding ideal with canonical basis $\frac{a}{g}, \frac{b}{g} + \delta$, then the lattices $L_K(I)$ and $L_K(I')$ are similar, and so are there twists by the same element $\alpha \in K$. Therefore our upper bounds on b mean that there can be at most finitely many ideals in $\mathcal{O}_K$, up to similarity of the resulting ideal lattices, with the canonical basis being WR twistable.

This finishes the proof of Theorem 1.2. Notice that this theorem implies that the canonical basis is rarely WR twistable, however such examples still exist. We demonstrate a couple here.

Example 1. *Let $D = 139 \equiv 3 \pmod 4$ and $K = \mathbb{Q}(\sqrt{139})$. Let $I \subset \mathcal{O}_K$ be an ideal generated by the canonical basis*

$$9,\ 7 - \sqrt{139},$$

i.e. $g = 1$, $b = 7 < \sqrt{139}$, $a = 9 \mid \mathbb{N}(b - \sqrt{D}) = 7^2 - 139 = -90$. This basis is WR twistable by the totally positive element

$$\alpha = \frac{1946}{107} + \sqrt{139} \in K$$

with the resulting WR lattice having the Minkowski reduced basis matrix

$$\frac{1}{107}\begin{pmatrix} 9\sqrt{208222 + 11449\sqrt{139}} & (7-\sqrt{139})\sqrt{208222 + 11449\sqrt{139}} \\ 9\sqrt{208222 - 11449\sqrt{139}} & (7+\sqrt{139})\sqrt{208222 - 11449\sqrt{139}} \end{pmatrix}$$

and cosine of the angle between these basis vectors being $-1/14$. The common value of the successive minima of this lattice is $\sqrt{\frac{315252}{107}} \approx 54.27964973...$

Example 2. *Let $D = 141 \equiv 1 \pmod 4$ and $K = \mathbb{Q}(\sqrt{141})$. Let $I \subset \mathcal{O}_K$ be an ideal generated by the canonical basis*

$$5,\ 4 + \frac{1-\sqrt{141}}{2},$$

i.e. $g = 1$, $b = 4 < \sqrt{141}/2$, $a = 5 \mid \mathbb{N}\left(b + \frac{1-\sqrt{D}}{2}\right) = \frac{(8+1)^2-141}{4} = -15$. This basis is WR twistable by the totally positive element

$$\alpha = \frac{1269}{61} + \sqrt{141} \in K$$

with the resulting WR lattice having the Minkowski reduced basis matrix

$$\frac{1}{61}\begin{pmatrix} 5\sqrt{77409+3721\sqrt{141}} & \left(\frac{9-\sqrt{141}}{2}\right)\sqrt{77409+3721\sqrt{141}} \\ 5\sqrt{77409-3721\sqrt{141}} & \left(\frac{9+\sqrt{141}}{2}\right)\sqrt{77409-3721\sqrt{141}} \end{pmatrix}$$

and cosine of the angle between these basis vectors being $2/9$*. The common value of the successive minima of this lattice is* $\sqrt{\frac{63450}{61}} \approx 32.25157258...$

4. Proof of Theorem 1.3

Here we prove Theorem 1.3. As above, let $K = \mathbb{Q}(\sqrt{D})$ for a squarefree integer $D > 1$ and let $I \subseteq \mathcal{O}_K$ be an ideal with the canonical basis $a, b + g\delta$ as described in (6). Suppose this basis is stable twistable by some totally positive $\alpha = p + q\sqrt{D} \in K$. First assume that $K = \mathbb{Q}(\sqrt{D})$ with $D \not\equiv 1 \pmod 4$. If we consider the first condition of (14) as a quadratic inequality in p, then its leading coefficient is negative unless $b \leq g\sqrt{D/3}$ and it has negative discriminant unless $b \leq 2g\sqrt{D/3}$. Hence the canonical basis can be stable twistable only if

$$b < \frac{2}{\sqrt{3}} g\sqrt{D}.$$

As always, equality is not possible since b is an integer and D is squarefree. Now assume that $I = \mathcal{O}_K$, then $a = 1, b = 0, g = 1$, so the inequalities of (14) become:

$$D(p^2 - 4Dq^2) \geq 0,\ p \geq \sqrt{D(p^2 - Dq^2)}.$$

Combining these inequalities, we obtain $(1 - 3D)p^2 \geq 0$, which is not possible. Hence $\mathcal{O}_K$ cannot have a stable twistable canonical basis.

Now suppose that $D \equiv 1 \pmod 4$. Considering the first condition of (16) as a quadratic inequality in p, we see that its leading coefficient is negative unless $b \leq \frac{g}{2}\left(\sqrt{D/3} - 1\right)$ and it has negative discriminant unless $b \leq \frac{g}{2}\left(2\sqrt{D/3} - 1\right)$. Hence the canonical basis can be stable twistable only if

$$b < \frac{g}{2}\left(2\sqrt{D/3} - 1\right).$$

Again, equality is not possible since b is an integer and D is squarefree. Now assume that $I = \mathcal{O}_K$, then $a = 1, b = 0, g = 1$, so the inequalities of (16) become:

$$\frac{p^2}{4}(D-3) + \frac{3}{2}Dpq - D^2q^2 \geq 0,\ 2p > \sqrt{D(p^2 - q^2D)}.$$

These inequalities lead to

$$q\left(\frac{D\sqrt{4D-3} - 3}{D-3}\right) < p < q\left(\frac{D}{\sqrt{D-4}}\right),$$

which means that we must have $\frac{D\sqrt{4D-3}-3}{D-3} < \frac{D}{\sqrt{D-4}}$. This only holds for $D = 5$, which, as we know, yields even a WR twist. By the same reasoning as in the proof of Theorem 1.2, our upper bounds on b mean that there can be at most finitely many ideals in $\mathcal{O}_K$, up to similarity of the resulting ideal lattices, with the canonical basis being stable twistable. This finishes the proof of Theorem 1.3.

Finally, let us demonstrate a couple examples of stable twists of ideal lattice canonical bases that are not WR twistable.

Example 3. *Let* $D = 1327 \equiv 3 \pmod 4$ *and* $K = \mathbb{Q}(\sqrt{1327})$. *Let* $I \subset \mathcal{O}_K$ *be an ideal generated by the canonical basis*

$$39,\ 38 - \sqrt{1327},$$

i.e. $g = 1$, $b = 38$, $a = 39 \mid \mathbb{N}(b - \sqrt{D}) = 38^2 - 1327 = 117$. *Notice, in particular, that*

$$g\sqrt{D} = 36.42801120... < b < 42.06344416... = \frac{2}{\sqrt{3}} g\sqrt{D},$$

hence this basis cannot be WR twistable, by Theorem 1.2. On the other hand, this basis is stable twistable by the totally positive element

$$\alpha = 63 + \sqrt{1327} \in K$$

with the resulting stable lattice having the Minkowski reduced basis matrix

$$\begin{pmatrix} 39\sqrt{63 + \sqrt{1327}} & (38 - \sqrt{1327})\sqrt{63 + \sqrt{1327}} \\ 39\sqrt{63 - \sqrt{1327}} & (38 + \sqrt{1327})\sqrt{63 - \sqrt{1327}} \end{pmatrix}$$

and cosine of the angle between these basis vectors being 0.4951063950.... *The determinant of this lattice is* 146048.2881... *and values of the successive minima are* $\sqrt{147442}$ *and* $\sqrt{191646}$, *respectively.*

Example 4. *Let* $D = 125173 \equiv 1 \pmod 4$ *and* $K = \mathbb{Q}(\sqrt{125173})$. *Let* $I \subset \mathcal{O}_K$ *be an ideal generated by the canonical basis*

$$183,\ 182 + \frac{1 - \sqrt{125173}}{2},$$

i.e. $g = 1$, $b = 182$, $a = 183 \mid \mathbb{N}\left(\frac{(2b+1)-\sqrt{D}}{2}\right) = 2013$. *Notice, in particular, that*

$$\frac{g(\sqrt{D} - 1)}{2} = 176.3989824... < b < 203.7653503... = \frac{g}{2}\left(\frac{2}{\sqrt{3}}\sqrt{D} - 1\right),$$

hence this basis cannot be WR twistable, by Theorem 1.2. On the other hand, this basis is stable twistable by the totally positive element

$$\alpha = 611 + \sqrt{125173} \in K$$

with the resulting stable lattice having the Minkowski reduced basis matrix

$$\begin{pmatrix} 183\sqrt{611 + \sqrt{125173}} & \left(\frac{365}{2} - \frac{\sqrt{125173}}{2}\right)\sqrt{611 + \sqrt{125173}} \\ 183\sqrt{611 - \sqrt{125173}} & \left(\frac{365}{2} + \frac{\sqrt{125173}}{2}\right)\sqrt{611 - \sqrt{125173}} \end{pmatrix}$$

and cosine of the angle between these basis vectors being 0.4853755919.... *The determinant of this lattice is* 32252383.1... *and values of the successive minima are* $\sqrt{33252444}$ *and* $\sqrt{40923558}$, *respectively.*

5. Further remarks on stable and WR twistable bases

Here we include some further heuristic remarks on stable and WR twistable bases beyond the canonical ones discussed above. Let

$$\mathbb{H} = \{x + iy \in \mathbb{C} : y > 0\}$$

be the upper half-plane. Following [9], define

$$\mathcal{D} := \{\tau = a + bi \in \mathbb{H} : -1/2 < a \leq 1/2, |\tau| \geq 1\}$$

and

$$\mathcal{F} := \{\tau = a + bi \in \mathbb{H} : 0 \leq a \leq 1/2, |\tau| \geq 1\},$$

so $\mathcal{F}$ is "half" of $\mathcal{D}$. Then $\mathcal{D}$ is the standard fundamental domain of $\mathbb{H}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$ by fractional linear transformations and $\mathcal{F}$ is the space of similarity classes of planar lattices. As in [9], this can be illustrated by Figure 1 with the subsets of WR and stable similarity classes marked accordingly.

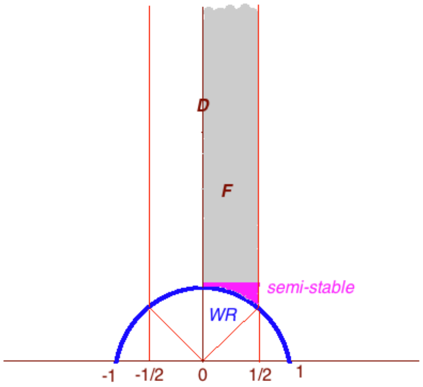

Figure 1. Similarity classes of lattices in $\mathbb{R}^2$ with WR and stable subregions marked by colors.

Let K be a real quadratic field and $I \subseteq \mathcal{O}_K$ an ideal. For each lattice $(L_K(I), f_{\mathcal{A}(\alpha)})$ for a totally positive $\alpha \in K$, let us write $\langle L_K(I), f_{\mathcal{A}(\alpha)} \rangle$ for its similarity class. As shown in [2], sets of similarity classes of the form

$$\mathcal{G}(I) := \left\{ \langle L_K(I), f_{\mathcal{A}(\alpha)} \rangle : \alpha \in K \text{ totally positive} \right\}$$

correspond to closed geodesics in $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$, and every closed geodesic will necessary intersect the WR locus $\mathcal{W}$ in the upper-half plane (the blue arc in Figure 1); denote by $\mathcal{I} := \mathcal{W} \cap \mathcal{G}(I)$ the set of such intersection points.

The set $\mathcal{I}$ is completely defined by a relation described in [6]. Let $B = \{x, y\}$ be a basis for the ideal I, and define

$$F(B) = \mathbb{N}(x)^2 + \mathbb{N}(y)^2 + \mathbb{N}(x)\mathbb{N}(y) - \mathbb{N}(I)^2 \Delta_K/4,$$

where Δ_K is the discriminant of the number field K. We say that two bases B and B' are *equivalent* if $F(B) = F(B')$: this is indeed an equivalence relation. Then the set $\mathcal{I}$ is in bijective correspondence with the equivalence classes of bases B with $F(B) < 0$. This implies finiteness of $|\mathcal{I}|$. Furthermore, as the geodesics $\mathcal{G}(I)$ are closed, the number of arcs "inside" the stable locus is at most twice $|\mathcal{I}|$, except when the only WR twist of our ideal lattice is orthogonal as in Figure 2.

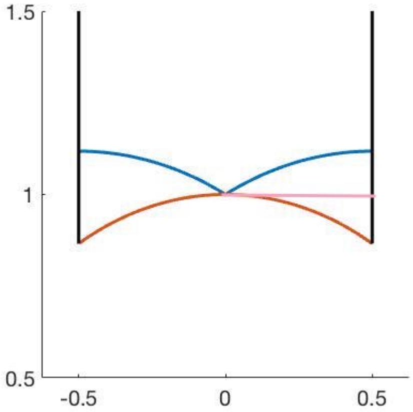

FIGURE 2. Geodesic $\mathcal{G}(I)$ (blue) intersects the WR locus (red) in one point (orthogonal lattice), which is also a stable twist.

For example, if $I = \mathcal{O}_K$ this will happen if and only if $D = s^2 + 1$ (respectively $D = s^2 + 4$) for $D \not\equiv 1 \pmod 4$ (respectively $D \equiv 1 \pmod 4$). In general, this will be the case if for every basis $B = \{x, y\}$ of I such that $\mathbb{N}(x) < \mathbb{N}(I)\sqrt{\Delta_K}/4$, we have $\mathbb{N}(x) = -\mathbb{N}(y)$.

Figure 3 illustrates an example of the intersection of $\mathcal{G}(I)$ with the WR locus for $I = \mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{59})$.

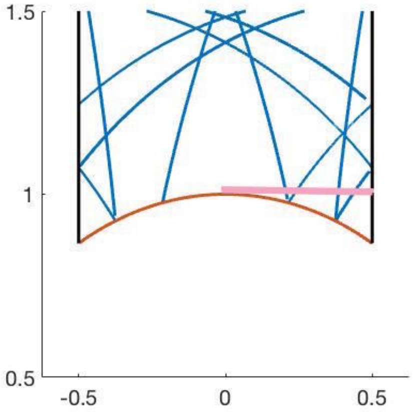

FIGURE 3. Geodesic $\mathcal{G}(\mathcal{O}_{\mathbb{Q}(\sqrt{59})})$ intersects the WR locus.

Before intersecting the WR locus, the geodesic $\mathcal{G}(I)$ crosses "continuously" the stable locus, which yields infinitely many stable twists: in other words, this insures the existence of infinitely many totally positive $\alpha \in K$ such that $\mathcal{A}(\alpha)B$ is stable for a fixed WR twistable basis. In summary, every WR twistable basis will give rise to infinitely many stable twists, except in the cases where the ideal I admits only the orthogonal WR twist. The converse is not true: there exist bases that are stable twistable, but not WR twistable, as demonstrated by Examples 3 and 4.

6. Applications of WR and stable lattice twists

In this section we discuss some applications of WR and stable twistable lattice bases. First we highlight a connection between such bases and the theory of error control in wireless communication. We assume a single-input single-output (SISO) Rayleigh flat fading channel model:

$$\boldsymbol{y} = H\boldsymbol{x} + \boldsymbol{v}, \tag{18}$$

where $\boldsymbol{x}$ is the transmitted codeword taken from some finite codebook in $\mathbb{C}^n$, $H = \operatorname{diag}(h_1, \dots, h_n)$ describes the random channel response, and $\boldsymbol{v} \in \mathbb{C}^n$ is a random additive white Gaussian noise with variance $\sigma^2_{\boldsymbol{v}}$.

To study the communication reliability of a given code C we consider the codeword error probability $P_e(C)$. The goal is to choose C to be a subset of a lattice that minimizes $P_e(C)$. Considering $\Lambda \subset \mathbb{R}^n$, it is proved in [15] that the lattices (of fixed volume) that minimize $P_e(C)$ for Rayleigh fading channel are those with maximal $d_{\min}(\Lambda)$, where

$$d_{\min}(\Lambda) = \min_{\boldsymbol{x} \in \Lambda \setminus \{\boldsymbol{0}\}} \prod_{i=1}^{n} |x_i|.$$

This criterion is restricted to the so called fully diverse lattices, i.e. the lattices with non-vanishing $d_{\min}(\Lambda)$. Let us prove that the existence of twistable bases allows one to restrict this optimization problem to the set of WR or stable lattices without loss of generality.

Proposition 6.1. *Let Λ be a lattice with maximal $d_{\min}(\Lambda)$ in its dimension. Then there exists a WR lattice L and a stable lattice M, such that*

$$d_{\min}(\Lambda) = d_{\min}(L) = d_{\min}(M).$$

Proof. Let $\Lambda \subset \mathbb{R}^n$ be a fully diverse lattice. Notice that $d_{\min}(\Lambda)$ is invariant under the action of $\mathcal{A}$, i.e $d_{\min}(A\Lambda) = d_{\min}(\Lambda)$ for any $A \in \mathcal{A}$. In [13] Mcmullen showed that if the orbit closure $\overline{\mathcal{A}\Lambda}$ is compact then $\mathcal{A}\Lambda$ meets the set of WR lattices. Hence we only need to show that the full diversity of Λ will ensure the compactness of $\overline{\mathcal{A}.\Lambda}$, and this is a straightforward application of the Mahler compactness criterion. Namely, for a set E of unimodular lattices we have

$$\overline{E} \text{ is compact } \iff \lambda_1(L) > 0 \text{ for all } L \in E.$$

If Λ is a fully diverse lattice, then $d_{\min}(\Lambda) > 0$. Hence, by the AM-GM inequality, we have

$$0 < \sqrt{n} \prod_{i=1}^{n} |x_i| \leq \|\boldsymbol{x}\|$$

for any $\boldsymbol{x} \in \Lambda$. In particular, taking $\boldsymbol{x} \in \Lambda$ such that $\|\boldsymbol{x}\| = \lambda_1(\Lambda)$, we see that $\lambda_1(L) > 0$ for any $L \in \mathcal{A}\Lambda$.

For stable lattices the argument is the same replacing the result of [13] with the analogous result of [17] which guarantees that if the orbit closure $\overline{\mathcal{A}\Lambda}$ is compact then $\mathcal{A}\Lambda$ meets the set stable lattices. □

Remark 6.1. Notice that $d_{\min}(\Lambda) > 0$ for Λ arising from a real number field. Margulis conjectured that the converse is also true. More precisely, if a lattice $\Lambda \subset \mathbb{R}^n$ for $n \geq 3$ has $d_{\min}(\Lambda) > 0$ then Λ comes from an order in a number field. In other words, Margulis's conjecture asserts that all fully diverse lattices come from orders in totally real number fields, and this motivates the choice of number theoretic constructions in this context.

Let us also briefly discuss the use of WR and stable twists in the arithmetic theory. Let K be a real number field of degree n. The Euclidean minimum of K is defined as

$$M(K) := \inf\left\{\alpha \in \mathbb{R}_{>0} : \forall x \in K \ \exists y \in \mathcal{O}_K \text{ such that } |\mathbb{N}(x-y)| \leq \alpha\right\}.$$

The Euclidean minimum measures how far is K from having a Euclidean algorithm. In fact, if $M(K) < 1$ then $\mathcal{O}_K$ is a Euclidean ring. Furthermore, for an ideal I in $\mathcal{O}_K$ we can define

$$M(I) := \inf\left\{\alpha \in \mathbb{R}_{>0} : \forall x \in K \ \exists y \in I \text{ such that } |\mathbb{N}(x-y)| \leq \alpha\right\}.$$

Now, for a lattice $\Lambda \subset \mathbb{R}^n$, its covering radius is

$$\mu(\Lambda) := \sup_{\boldsymbol{y} \in \mathbb{R}^n} \min\left\{\|\boldsymbol{x} - \boldsymbol{y}\| : \boldsymbol{x} \in \Lambda\right\}$$

and the Hermite thickness of Λ is

$$\tau(\Lambda) := \frac{\mu(\Lambda)^2}{\det(\Lambda)^{1/n}}.$$

Then for an ideal $I \subseteq \mathcal{O}_K$, define

$$\tau_{\min}(I) := \min\{\tau(L_K(I), f_{A(\alpha)}) : \alpha \in K \text{ totally positive}\}.$$

Theorem 6.2 ([3]). *For all number fields K of degree n,*

$$M(I) \leq \left(\frac{\tau_{\min}(I)}{n}\right)^{n/2} \sqrt{|\Delta_K|}\ \mathbb{N}(I),$$

where Δ_K is the discriminant of K.

This theorem motivates the study of the covering radii in the orbit of the action of $\mathcal{A}_1(K)$ on $L_K(I)$. Furthermore, it has been proved that $\mu(\Lambda) \leq \frac{\sqrt{n}}{2}$ for any unimodular WR lattice of dimension $n \leq 9$ (not true for $n \geq 30$), and it is conjectured to be true for stable lattices in any dimension. Combining these observations, we have

$$M(K) \leq \frac{\sqrt{|\Delta_K|}}{4}$$

when K is a real quadratic number field. Notice that this bound automatically implies that $\mathbb{Q}(\sqrt{d})$ is a Euclidean domain for $d = 5, 2, 3, 13$.

Acknowledgment. We would like to thank Laia Amoros, Camilla Hollanti and David Karpuk for many helpful conversations on the subject of this paper. A part of the work was done during a stay of the first author at Claremont McKenna College (CMC): M.T. Damir would like to thank CMC for its hospitality. We also thank the anonymous referee for some helpful suggestions.

References

[1] E. Bayer-Fluckiger. Ideal lattices. In *A panorama of number theory or the view from Baker's garden (Zurich, 1999)*, pages 168–184. Cambridge Univ. Press, Cambridge, 2002.

[2] E. Bayer-Fluckiger and G. Nebe. On the Euclidean minimum of some real number fields. *J. Théor. Nombres Bordeaux*, 17(2):437–454, 2005.

[3] Eva Bayer-Fluckiger and Gabriele Nebe. On the euclidean minimum of some real number fields. *Journal de théorie des nombres de Bordeaux*, 17(2):437–454, 2005.

[4] D. A. Buell. *Binary Quadratic Forms.* Springer-Verlag, 1989.

[5] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups, 3rd edition.* Springer-Verlag, 1999.

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

[7] L. Fukshansky. Revisiting the hexagonal lattice: on optimal lattice circle packing. *Elem. Math.*, 66(1):1–9, 2011.

[8] L. Fukshansky. Stability of ideal lattices from quadratic number fields. *Ramanujan J.*, 37(2):243–256, 2015.

[9] L. Fukshansky, P. Guerzhoy, and F. Luca. On arithmetic lattices in the plane. *Proc. Amer. Math. Soc.*, 145(4):1453–1465, 2017.

[10] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On well-rounded ideal lattices, II. *Int. J. Number Theory*, 9(1):139–154, 2013.

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

[12] L. Ji. Well-rounded equivariant deformation retracts of Teichmüller spaces. *Enseign. Math.*, 60(1-2):109–129, 2014.

[13] C. McMullen. Minkowski's conjecture, well-rounded lattices and topological dimension. *J. Amer. Math. Soc.*, 18(3):711–734, 2005.

[14] H. H. Mitchell. On classes of ideals in a quadratic field. *Ann. of Math. (2)*, 27(4):297–314, 1926.

[15] Frédérique Oggier, Emanuele Viterbo, et al. Algebraic number theory and code design for rayleigh fading channels. *Foundations and Trends® in Communications and Information Theory*, 1(3):333–415, 2004.

[16] A. Schürmann. *Computational geometry of positive definite quadratic forms*, volume 48 of *University Lecture Series.* American Mathematical Society, Providence, RI, 2009.

[17] U. Shapira and B. Weiss. Stable lattices and the diagonal group. *J. Eur. Math. Soc. (JEMS)*, 18(8):1753–1767, 2016.

[18] Y. Yamamoto. Real quadratic number fields with large fundamental units. *Osaka, J. Math.*, 8:261–270, 1971.

Department of Mathematics and Systems Analysis, Aalto University, P.O. Box 11100, FI-00076 Aalto, Finland

E-mail address: mohamed.damir@aalto.fi

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711, USA

E-mail address: lenny@cmc.edu