On integral well-rounded lattices

Lenny Fukshansky
Claremont McKenna College

Karlsruhe Institute of Technology

Mathematics Colloquium
July 19, 2012

Introduction to lattices

A **lattice** Λ in the Euclidean space $\mathbb{R}^N$ is a discrete subgroup, which is the same as a free $\mathbb{Z}$-module. In other words,

$$\Lambda = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{a}_1, \dots, \boldsymbol{a}_L\}$$

for some $\mathbb{R}$-linearly independent vectors

$$\boldsymbol{a}_1, \dots, \boldsymbol{a}_L, \tag{1}$$

where $L \leq N$. These vectors form a **basis** for Λ and L is called the **rank** of Λ. If $L = N$, then Λ is co-compact in $\mathbb{R}^N$ and we say that it has **full rank**. Define the **basis matrix** corresponding to the choice of the basis (1) to be the $N \times L$ matrix

$$A = \begin{pmatrix} \boldsymbol{a}_1 & \dots & \boldsymbol{a}_L \end{pmatrix},$$

then

$$\Lambda = A\mathbb{Z}^L.$$

WR Lattices

Let $N \geq 2$ be an integer, and let $\Lambda \subseteq \mathbb{R}^N$ be a lattice of full rank. Define the **minimum** of Λ to be

$$|\Lambda| = \min_{\boldsymbol{x} \in \Lambda \setminus \{\boldsymbol{0}\}} \|\boldsymbol{x}\|^2,$$

where $\| \ \|$ stands for the usual Euclidean norm on $\mathbb{R}^N$. Let

$$S(\Lambda) = \{\boldsymbol{x} \in \Lambda : \|\boldsymbol{x}\|^2 = |\Lambda|\}$$

be the set of *minimal vectors* of Λ. We say that Λ is a **well-rounded** lattice (abbreviated WR) if $S(\Lambda)$ spans $\mathbb{R}^N$.

WR lattices come up in connection with sphere packing, covering, and kissing number problems, coding theory, Minkowski conjecture and Woods covering conjecture in the geometry of numbers, and the linear Diophantine problem of Frobenius, just to name a few of the contexts.

Still, the WR condition is special enough so that one would expect WR lattices to be rather sparce among all lattices.

WR similarity classes in $\mathbb{R}^2$

Two lattices Λ_1, Λ_2 are called **similar** if

$$\Lambda_2 = \alpha A \Lambda_1$$

for some real number α and orthogonal matrix A. This is an equivalence relation.

A WR lattice can only be similar to another WR lattice, hence we can talk about **similarity classes** of WR lattices.

A lattice $\Lambda \subset \mathbb{R}^2$ is WR if and only if $S(\Lambda)$ contains two vectors $\boldsymbol{x}, \boldsymbol{y}$ with the angle θ between them lying in the interval $[\pi/3, \pi/2]$. Such vectors form a **minimal basis** for Λ, and the angle between them is an invariant of the lattice, we denote it by $\theta(\Lambda)$.

Two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^2$ are similar if and only if $\theta(\Lambda_1) = \theta(\Lambda_2)$. Similarity classes of all WR lattices in the plane are then indexed by values of the angle in the interval $[\pi/3, \pi/2]$.

Examples of WR lattices in $\mathbb{R}^2$

The **integer lattice**

$$\mathbb{Z}^2 := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 : x, y \in \mathbb{Z} \right\}.$$

The **hexagonal lattice**

$$\Lambda_h := \begin{pmatrix} 1 & -\frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix} \mathbb{Z}^2.$$

WR sublattices of $\mathbb{Z}^2$, not similar to $\mathbb{Z}^2$:

$$\begin{pmatrix} 4 & 4 \\ 3 & -3 \end{pmatrix} \mathbb{Z}^2, \quad \begin{pmatrix} 7 & 7 \\ 5 & -5 \end{pmatrix} \mathbb{Z}^2, \quad \begin{pmatrix} 7 & -1 \\ 4 & 8 \end{pmatrix} \mathbb{Z}^2.$$

WR sublattices of Λ_h, not similar to Λ_h:

$$\begin{pmatrix} \frac{5}{2} & \frac{-1}{2} \\ \frac{\sqrt{3}}{2} & \frac{3\sqrt{3}}{2} \end{pmatrix} \mathbb{Z}^2, \quad \begin{pmatrix} \frac{7}{2} & -1 \\ \frac{\sqrt{3}}{2} & 2\sqrt{3} \end{pmatrix} \mathbb{Z}^2, \quad \begin{pmatrix} 4 & \frac{-1}{2} \\ \sqrt{3} & \frac{5\sqrt{3}}{2} \end{pmatrix} \mathbb{Z}^2.$$

Distribution questions

Due to the importance of WR lattices, it is interesting to understand how are they distributed. The first part of this talk will be motivated by the following two general questions.

Question 1. *Let $\Omega \subset \mathbb{R}^N$ be a lattice of full rank. Does Ω contain any WR sublattices?*

Question 2. *If so, how are they distributed? More specifically, define $\mathcal{N}_{\text{WR}}(\Omega, B) =$*

$$\left| \{ \Lambda \subseteq \Omega : \Lambda \text{ is WR and } |\Omega : \Lambda| \leq B \} \right| .$$

What is the asymptotic behavior of $\mathcal{N}_{\text{WR}}(\Omega, B)$ as $B \to \infty$?

These questions are not currently well understood for $N \geq 3$. We will therefore concentrate on the known results in $\mathbb{R}^2$.

Some more notation

Given a full-rank lattice

$$\Omega = A\mathbb{Z}^2 \subset \mathbb{R}^2,$$

the **Gram matrix** corresponding to the basis matrix A is the 2×2 non-singular symmetric matrix

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} := A^t A,$$

which is the coefficient matrix of the corresponding quadratic **norm-form**

$$Q_A(X,Y) = \begin{pmatrix} X & Y \end{pmatrix} A^t A \begin{pmatrix} X \\ Y \end{pmatrix}.$$

The lattice is called **integral** if the entries a, b, c of the matrix $A^t A$ are integers. This property is independent of the choice of the basis for Ω. Integral lattices are of particular importance in number theory and arithmetic theory of quadratic forms.

And a little more (following S. Kühnlein)

More generally, define

$$\delta(\Omega) = \dim_{\mathbb{Q}} \left(\mathrm{span}_{\mathbb{Q}}\{a, b, c\} \right),$$

which is again independent of the choice of the basis for Ω. The lattice is called **arithmetic** if $\delta(\Omega) = 1$. Notice that this happens if and only if

$$\Omega = \alpha\Omega'$$

for some $\alpha \in \mathbb{R}$ and Ω' an integral lattice. In other words, every arithmetic lattice is similar to some integral lattice.

On the other hand, $\delta(\Omega)$ can also be 2 or 3. If $\delta(\Omega) = 2$, then there exist $x, y, z \in \mathbb{Z}$ such that

$$xa + yb + zc = 0,$$

and define $\sigma(\Omega)$ to be the squarefree part of $y^2 - 4xz$. This is an invariant of the lattice, which Kühnlein calls the **strange invariant**.

Kühnlein's criterion

The following characterization gives a complete answer to Question 1 for $N = 2$.

Theorem 1 (Kühnlein, 2011). *Let $\Omega \subset \mathbb{R}^2$ be a lattice of full rank.*

- *If $\delta(\Omega) = 1$, then Ω contains infinitely many non-similar WR sublattices.*

- *If $\delta(\Omega) = 3$, then Ω does not contain any WR sublattices.*

- *If $\delta(\Omega) = 2$ and $\sigma(\Omega) = 1$, then Ω contains infinitely many non-similar WR sublattices.*

- *If $\delta(\Omega) = 2$ and $\sigma(\Omega) \neq 1$, then Ω does not contain any WR sublattices.*

Counting principle

To answer Question 2, define the **WR zeta-function** of a planar lattice Ω to be

$$\zeta_{\mathsf{WR}}(\Omega, s) = \sum_{\mathsf{WR}\ \Lambda \subseteq \Omega} |\Omega : \Lambda|^{-s} = \sum_{n=1}^{\infty} a_n n^{-s},$$

where $a_n = a_n(\Omega) :=$

$$|\{\Lambda \subseteq \Omega : \Lambda \text{ is WR and } |\Omega : \Lambda| = n\}|$$

and s is a complex variable. Then

$$\mathcal{N}_{\mathsf{WR}}(\Omega, B) = \sum_{n=1}^{B} a_n(\Omega),$$

and asymptotic behavior of $\mathcal{N}_{\mathsf{WR}}(\Omega, B)$ can be obtained from analytic properties of the zeta-function $\zeta_{\mathsf{WR}}(\Omega, s)$ using a Tauberian-type theorem.

Estimates: non-arithmetic case

As can be expected, the analytic properties of $\zeta_{\mathsf{WR}}(\Omega, s)$ (and hence the asymptotic behavior of $\mathcal{N}_{\mathsf{WR}}(\Omega, B)$) are different in the arithmetic and non-arithmetic cases.

We start with the non-arithmetic case.

Theorem 2 (Kühnlein, 2011)**.** *Suppose that $\delta(\Omega) = 2$, $\sigma(\Omega) = 1$, then the abscissa of convergence of $\zeta_{\mathsf{WR}}(\Omega, s)$ is 1 and the limit*

$$\lim_{s \to 1+} (s-1)\zeta_{\mathsf{WR}}(\Omega, s)$$

exists and is nonzero. Further,

$$\mathcal{N}_{\mathsf{WR}}(\Omega, B) = O(B)$$

as $B \to \infty$.

Estimates: arithmetic case

We now discuss the arithmetic case.

Theorem 3 (F., 2012). *Suppose $\delta(\Omega) = 1$, then abscissa of convergence of $\zeta_{\mathsf{WR}}(\Omega, s)$ is 1, and for $s \in \mathbb{R}$ the limit*

$$\lim_{s \to 1+} (s-1)^2 \zeta_{\mathsf{WR}}(\Omega, s)$$

exists and is nonzero. Further,

$$\mathcal{N}_{\mathsf{WR}}(\Omega, B) = O(B \log B)$$

as $B \to \infty$.

Remark 1. The proof uses a convenient parameterization of integral WR lattices in the plane, obtained by F., Henshaw, Liao, Prince, Sun, Whitehead (2011). The result of Theorem 3 in case $\Omega = \mathbb{Z}^2$ has been obtained by F. in 2007 using a different method. In addition, the fact that abscissa of convergence of $\zeta_{\mathsf{WR}}(\Omega, s)$ is 1 for any arithmetic planar lattice Ω was proved by Kühnlein in 2011, also by a different method.

Further counting (F., et al. – 2011)

We consider a different counting problem.

Question 3. *Let* $\Delta \in \mathbb{R}_{>0}$ *and let* $\mathrm{IWR}(\Delta)$ *be the set of integral WR planar lattices, up to rotation and reflection, with determinant* $= \Delta$. *How big is this set for a fixed* Δ*?*

Theorem 4. $\mathrm{IWR}(\Delta)$ *is finite for any* Δ, *and nonempty if and only if* $\Delta = ka\sqrt{D}$ *with* $k, a, D \in \mathbb{Z}_{>0}$, D *squarefree, and* a *such that the equation* $a^2D = x^2 - y^2$ *has integer solutions with* $x \leq 2y$. *Let* $M = ka$, *then*

$$|\mathrm{IWR}(\Delta)| \leq \frac{1}{2} \sum_{r|M} 2^{\omega(rD)}.$$

Moreover,

$$|\mathrm{IWR}(\Delta)| \ll \sum_{r|M} \sum_{g|r} \mu\left(\frac{r}{g}\right) \frac{\tau(g^2D)}{\sqrt{\omega(gD)}},$$

where $\tau(u)$ *is the number of divisors,* $\omega(u)$ *is the number of prime divisors, and* $\mu(u)$ *is the Möbius function of an integer* u. *The constant in the Vinogradov notation* $\ll$ *does not depend on* Δ.

Ideal lattices

A particularly important class of integral lattices are **ideal lattices**, which were extensively studied in the 1990's and 2000's by many authors, including E. Bayer-Fluckiger and her co-authors. We consider the simplest kind of ideal lattices, those of **trace type**.

Let K be a number field, $\mathcal{O}_K$ its ring of integers, and

$$d = [K : \mathbb{Q}] = r_1 + 2r_2,$$

where r_1 is the number of real embeddings and r_2 the number of pairs of complex conjugate embeddings of K. In fact, let

$$\sigma_1, \dots, \sigma_{r_1} : K \to \mathbb{R}$$

and

$$\tau_1, \bar{\tau_1}, \dots, \tau_{r_2}, \bar{\tau_{r_2}} : K \to \mathbb{C}$$

be these embeddings.

The **canonical embedding** $\sigma_K : K \to \mathbb{R}^d$ is defined by $\sigma_K =$

$$(\sigma_1, \dots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \dots, \Re(\tau_{r_2}), \Im(\tau_{r_2})),$$

where $\Re$ and $\Im$ stand for real and imaginary parts, respectively.

For each ideal $I \subseteq \mathcal{O}_K$,

$$\Lambda_K(I) := \sigma_K(I)$$

is a lattice of full rank in $\mathbb{R}^d$, called an **ideal lattice** (of trace type). The lattice

$$\Lambda_K := \sigma_K(\mathcal{O}_K)$$

is called a **principal ideal lattice** (of trace type).

In addition to their importance in number theory, ideal lattices appear in many different contexts, including cryptography, coding theory, and discrete optimization problems. This motivates us to better understand their geometric properties.

WR ideals

We will call an ideal $I \subseteq \mathcal{O}_K$ **well-rounded** (WR) if the corresponding ideal lattice $\Lambda_K(I)$ is WR. We investigate the following two questions.

Question 4. *For which number fields K is the ring of integers $\mathcal{O}_K$ WR?*

Question 5. *For which number fields K the ring of integers $\mathcal{O}_K$ contains WR ideals?*

Theorem 5 (F., Petersen (2010))**.** *$\mathcal{O}_K$ is WR if and only if K is cyclotomic. On the other hand, infinitely many real and imaginary quadratic number fields ($K = \mathbb{Q}(\sqrt{\pm D})$) contain WR ideals.*

Remark 2. There are only two quadratic cyclotomic number fields: $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$, whose rings of integers give rise to the principal ideal lattices $\mathbb{Z}^2$ and the hexagonal lattice Λ_h, respectively.

WR ideals: quadratic fields

We can say more in the case of quadratic number fields. We say that a positive squarefree integer D satisfies the ν-**nearsquare condition** if it has a divisor d with $\sqrt{\frac{D}{\nu}} \leq d < \sqrt{D}$, where $\nu > 1$ is a real number. We also write K **WR** to indicate that a number field K contains WR ideals.

Theorem 6 (F., et al., 2011). *If D satisfies the 3-nearsquare condition, then the rings of integers of quadratic number fields $K = \mathbb{Q}(\sqrt{\pm D})$ contain WR ideals; the statement becomes if and only if when $K = \mathbb{Q}(\sqrt{-D})$. This in particular implies that a positive proportion (more than 1/5) of real and imaginary quadratic number fields contain WR ideals, more specifically*

$$\liminf_{N \to \infty} \frac{\left|\left\{\mathbb{Q}(\sqrt{\pm D}) \text{ WR} : 0 < D \leq N\right\}\right|}{\left|\left\{\mathbb{Q}(\sqrt{\pm D}) : 0 < D \leq N\right\}\right|}$$

$$\geq \frac{\sqrt{3}-1}{2\sqrt{3}}.$$

WR ideals: imaginary quadratics

Theorem 7 (F., et al., 2011)**.** *Moreover, for every D satisfying the 3-nearsquare condition the corresponding imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-D})$ contains only finitely many WR ideals, up to similarity of the corresponding lattices, and this number is*

$$\ll \min \left\{ 2^{\omega(D)-1}, \frac{2^{\omega(D)}}{\sqrt{\omega(D)}} \right\}. \qquad (2)$$

Remark 3. In fact, two WR ideal lattices coming from the same imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ are similar if and only if the corresponding ideals are in the same ideal class, hence their number up to similarity is no greater than the class number h_K. Moreover, Siegel's estimate implies that

$$h_K \text{ is about } O(\sqrt{D}) \text{ as } D \to \infty.$$

On the other hand, (2), a bound on the number of **WR ideal classes**, is usually about

$$\frac{(\log D)^{\log 2}}{\sqrt{\log \log D}}.$$

WR ideals: real quadratics

Question 6. *Do there exist real quadratic number fields $\mathbb{Q}(\sqrt{D})$ with positive squarefree D not satisfying the 3-nearsquare condition containing WR ideals?*

Computational evidence suggests that the answer to this question is **no**, however at the moment we only have partial results in this direction.