On distribution of integral well-rounded lattices in the plane

Lenny Fukshansky
Claremont McKenna College

Special Session on "Arithmetic of Quadratic Forms and Integral Lattices"

First Joint Meeting of AMS and SoMaChi
December 15-18, 2010

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**

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

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

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

WR sublattices of Λ_h, not similar to Λ_h:

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

Number field lattices

Let K be a number field, $[K : \mathbb{Q}] = d$, $\mathcal{O}_K$ the ring of integers, and $\sigma : K \to \mathbb{R}^d$ the canonical embedding. Then $\sigma(\mathcal{O}_K)$ is a lattice of full rank in $\mathbb{R}^d$. These number field lattices are also important in coding theory and discrete optimization.

Question 1. *For which number fields K is the lattice $\sigma(\mathcal{O}_K)$ WR?*

Theorem 1 (F., Petersen (2010))**.** *Lattice $\sigma(\mathcal{O}_K)$ is WR if and only if K is cyclotomic.*

In dimension two there are only two number fields like this: $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, which give rise to $\mathbb{Z}^2$ and the hexagonal lattice Λ_h, respectively. This observation motivates the investigation of WR sublattices of $\mathbb{Z}^2$ and Λ_h.

WR similarity classes in $\mathbb{Z}^2$ and Λ_h

Let WR($\mathbb{Z}^2$) and WR(Λ_h) be sets of all WR sublattices of $\mathbb{Z}^2$ and Λ_h, respectively. Given a lattice Γ, we will write $\langle\Gamma\rangle$ for its similarity class. Let $\mathrm{Sim}_{\mathrm{WR}}(\mathbb{Z}^2)$ and $\mathrm{Sim}_{\mathrm{WR}}(\Lambda_h)$ be the sets of similarity classes of WR sublattices of $\mathbb{Z}^2$ and Λ_h, respectively.

Lemma 2 (F. (2009))**.** $\mathrm{Sim}_{\mathrm{WR}}(\mathbb{Z}^2)$ *is in bijective correspondence with the set of* **Primitive Pythagorean Triples (PPTs)** (p, r, q) *such that* $\gcd(p, r, q) = 1$,

$$p^2 + r^2 = q^2,$$

and $r = \min\{p, r\} \leq q/2$*: cosine of the angle* θ *determining the similarity class is* r/q*.*

Lemma 3 (F., Moore, Ohana, Zeldow (2010))**.** $\mathrm{Sim}_{\mathrm{WR}}(\Lambda_h)$ *is in bijective correspondence with the set of pairs of* **Primitive Eisenstein Triples (PETs)** (a, b, c) *and* $(b - a, b, c)$ *such that* $\gcd(a, b, c) = 1$,

$$a^2 - ab + b^2 = c^2,$$

and $a \leq b$*: cosine of the angle* θ *determining the similarity class is* $|b - 2a|/2c$*.*

Structure of $\mathrm{Sim}_{\mathrm{WR}}(\mathbb{Z}^2)$ **(F. (2009))**

The set of PPTs (p, r, q) admits a free action (by left multiplication) of the noncommutative monoid G_P generated by the matrices $A = \begin{bmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{bmatrix}$, $C = \begin{bmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{bmatrix}$ in $\mathrm{GL}_3(\mathbb{Z})$ and the 3×3 identity matrix I_3: for each $M \in G_P$ define

$$M(p, r, q) = M \begin{pmatrix} p \\ r \\ q \end{pmatrix}.$$

It is a well known fact that for every PPT (p, r, q), $M(p, r, q)$ is also a PPT. Moreover, every PPT (p, r, q) can be obtained in a unique way by applying a sequence of linear transformations A, B, C to $(3, 4, 5)$. This action gives a bijection between PPTs and elements of G_P, and allows to induce $\mathrm{Sim}_{\mathrm{WR}}(\mathbb{Z}^2)$ with algebraic and combinatorial structure.

Theorem 4. *The set* $\mathrm{Sim}_{\mathrm{WR}}(\mathbb{Z}^2)$ *has algebraic structure of an infinitely generated free noncommutative monoid with the class* $\langle \mathbb{Z}^2 \rangle$ *serving as identity. As a combinatorial object,* $\mathrm{Sim}_{\mathrm{WR}}(\mathbb{Z}^2)$ *has the structure of a regular rooted infinite tree, where each vertex has infinite degree, which is precisely the Cayley digraph of this monoid.*

More specifically, as a monoid $\mathrm{Sim}_{\mathrm{WR}}(\mathbb{Z}^2)$ is isomorphic to the following submonoid of G_P:

$$H = \Big\{A^2NB, A^kB, ABNB, C^2NB, C^kB, CBNB \\ (AC)^kA^2NB, (AC)^kABNB, (AC)^kAB, \\ (CA)^kC^2NB, (CA)^kCBNB, (CA)^kCB \ : \\ N \in G_P, k \in \mathbb{Z}_{>0}\Big\}.$$

We can also give a detailed description of each similarity class in $\mathrm{Sim}_{\mathrm{WR}}(\mathbb{Z}^2)$.

Let (p, r, q) be a PPT with $r/q \le 1/2$, so that it corresponds to a similarity class in $\mathrm{Sim}_{\mathsf{WR}}(\mathbb{Z}^2)$. Then there exist unique $m, n \in \mathbb{Z}_{>0}$ with

$$n < m,\ \gcd(m, n) = 1,\ 2 \nmid (m + n),$$

and either $n < m < \sqrt{3}n$ or $(2 + \sqrt{3})n < m$, such that

$$p = \max\{m^2 - n^2, 2mn\},\ q = m^2 + n^2,$$

and $r = \sqrt{q^2 - p^2}$. Define the lattice

$$\Omega(m, n) := \begin{bmatrix} m & -n \\ n & m \end{bmatrix} \mathbb{Z}^2.$$

Theorem 5. *A lattice Γ is in the similarity class of (p, r, q) if and only if*

$$\Gamma = \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{x}, \begin{bmatrix} \frac{\sqrt{q^2-p^2}}{q} & -\frac{p}{q} \\ \frac{p}{q} & \frac{\sqrt{q^2-p^2}}{q} \end{bmatrix} \boldsymbol{x} \right\}$$

for some $\boldsymbol{x} \in \Omega(m, n)$. Moreover, every lattice of the form $\Omega(m, n)$ parametrizes in this way some similarity class (p, r, q) determined by (m, n) as above.

Structure of $\mathsf{Sim}_{\mathsf{WR}}(\Lambda_h)$ (F., Moore, Ohana, Zeldow (2010))

Let $G_E = \langle U, M_1, M_2, M_3 \rangle$ be the noncommutative monoid generated by the 3×3 matrices

$$U, M_1, M_2, M_3 \in \mathsf{GL}_3(\mathbb{Z}),$$

defined as follows:

$$U = \begin{bmatrix} -1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ M_1 = \begin{bmatrix} 3 & -4 & 4 \\ 7 & -7 & 8 \\ 6 & -6 & 7 \end{bmatrix},$$

$$M_2 = \begin{bmatrix} -4 & 3 & 4 \\ -7 & 7 & 8 \\ -6 & 6 & 7 \end{bmatrix},\ M_3 = \begin{bmatrix} 1 & 3 & 4 \\ 0 & 7 & 8 \\ 0 & 6 & 7 \end{bmatrix}.$$

Lemma 6. *G_E acts on the set of PETs by left multiplication:*

$$M(a,b,c) = M \begin{pmatrix} a \\ b \\ c \end{pmatrix}$$

is a PET for every $M \in G_E$ and PET (a,b,c).

Let $M_4 = M_1 U$, $M_5 = M_2 U$, and let

$$G'_E = \langle M_1, \ldots, M_5 \rangle$$

be corresponding noncommutative monoid.

Lemma 7. G'_E *acts on* $\mathsf{Sim}_{\mathsf{WR}}(\Lambda_h)$ *by left multiplication of PETs.*

Conjecture 8. *Computational evidence (using SAGE) suggests that there are no relations between the generators* $M_1, \ldots, M_5$ *of* G'_E*, and that every element of* $\mathsf{Sim}_{\mathsf{WR}}(\Lambda_h)$ *can be obtained from the pair of PETs corresponding to* $\langle \Lambda_h \rangle$ *by the action of some* $M \in G'_E$*. This conjecturally implies a combinatorial structure on the set* $\mathsf{Sim}_{\mathsf{WR}}(\Lambda_h)$ *of two quinary trees joint at the roots.*

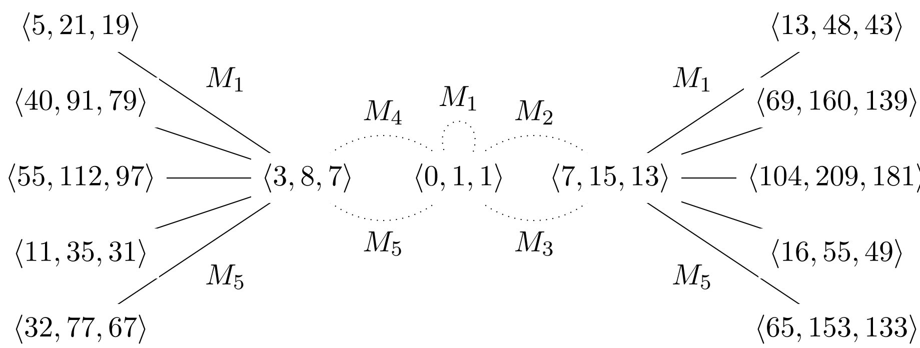

FIGURE 1. Structure of the set $\mathrm{Sim}_{\mathrm{WR}}(\Lambda_{\mathrm{h}})$ induced by the action of the monoid G'_E

Theorem 9. *Let $(a,b,c),(b-a,b,c)$ be a pair of PETs with $a \le b$, then there exist uniquely $m,n \in \mathbb{Z}_{>0}$ with $\gcd(m,n)=1$, $1 \le \frac{m}{n} \le 2$ and $3 \nmid (m+n)$ so that*

$$a = m(2n-m),\ b = n(2m-n),\ c = m^2 - mn + n^2.$$

The similarity class of this pair is $\langle \Gamma(m,n) \rangle$, where

$$\Gamma(m,n) = \frac{1}{2}\begin{bmatrix} m+n & m-2n \\ (m-n)\sqrt{3} & m\sqrt{3} \end{bmatrix} \mathbb{Z}^2 \subseteq \Lambda_h.$$

Moreover, for each $\Gamma \in \langle \Gamma(m,n) \rangle$,

$$|\Gamma| \ge |\Gamma(m,n)| = n^2 - mn + m^2,$$

and

$$|\Lambda_h : \Gamma| = \frac{\det(\Gamma)}{\det(\Lambda_h)} \ge |\Lambda_h : \Gamma(m,n)| = (2m-n)n,$$

i.e. $\Gamma(m,n)$ is a minimal lattice of its class. In fact, $\langle \Gamma(m,n) \rangle =$

$$\left\{ \sqrt{k} A \Gamma(m,n) : k \in \mathbb{Z}_{>0},\ A \text{ orthogonal } \right\},$$

where all the possible values of k and the corresponding matrices A, as well as all possible values of $|\Lambda_h : \Gamma(m,n)|$, are explicitly determined.

Minima and determinant sets for WR($\mathbb{Z}^2$) (F. (2008))

Let $\mathfrak{M} := \left\{|\Lambda| : \Lambda \in \mathrm{WR}(\mathbb{Z}^2)\right\}$

$$= \{a^2 + b^2 : a, b \in \mathbb{Z}\} \setminus \{0\}.$$

Let $\mathcal{D} := \{\det(\Lambda) : \Lambda \in \mathrm{WR}(\mathbb{Z}^2)\}$

$$= \left\{(a^2 + b^2)cd \;:\; a, b \in \mathbb{Z}_{\geq 0},\ \max\{a, b\} > 0, \right.$$
$$\left. c, d \in \mathbb{Z}_{>0},\ 1 \leq \frac{c}{d} \leq \sqrt{3}\right\}$$

A classical result of E. Landau (1908) implies that $\mathfrak{M}$ has asymptotic density 0 in $\mathbb{Z}$, i.e.

$$\lim_{M \to \infty} \frac{|\{m \in \mathfrak{M} : m \leq M\}|}{M} = 0.$$

Theorem 10. *The set $\mathcal{D}$ has positive lower density:*

$$\liminf_{M \to \infty} \frac{|\{u \in \mathcal{D} : u \leq M\}|}{M} \geq \frac{3^{\frac{1}{4}} - 1}{2 \cdot 3^{\frac{1}{4}}} \approx 0.12008216\ldots$$

Counting in $\mathsf{WR}(\mathbb{Z}^2)$ (F. (2008))

For each $u \in \mathbb{Z}_{>0}$, let

$$\mathcal{N}(u) = |\{\Lambda \in \mathsf{WR}(\mathbb{Z}^2) : \det(\Lambda) = u\}|,$$

so $\mathcal{N}(u) \neq 0$ if and only if $u \in \mathcal{D}$. An explicit formula for $\mathcal{N}(u)$ in terms of some arithmetic functions has been determined. Asymptotically, we have:

Theorem 11. *For each $u \in \mathbb{Z}_{>0}$,*

$$\mathcal{N}(u) \leq O\left(\left(\frac{\sqrt{2}\log u}{\omega(u)}\right)^{2\omega(u)}\right),$$

where $\omega(u)$ is the number of distinct prime divisors of u. Moreover,

$$\mathcal{N}(u) < O\left((\log u)^{\log 8}\right),$$

for all $u \in \mathcal{D}$ outside of a subset of asymptotic density 0. However, there exist infinite sequences $\{u_k\}_{k=1}^{\infty} \subset \mathcal{D}$ such that for every $k \geq 1$

$$\mathcal{N}(u_k) \geq (\log u_k)^k.$$

For instance, there exists such a sequence with $u_k \leq \exp\left(O(k(\log k)^2)\right)$ and $\omega(u_k) = O(k \log k)$.

Zeta function

Define **zeta-function of WR sublattices** of $\mathbb{Z}^2$ to be

$$\begin{aligned}\zeta_{\mathsf{WR}(\mathbb{Z}^2)}(s) &= \sum_{\Lambda \in \mathsf{WR}(\mathbb{Z}^2)} (\det(\Lambda))^{-s} \\ &= \sum_{u=1}^{\infty} \mathcal{N}(u) u^{-s},\end{aligned}$$

where $s \in \mathbb{C}$ is a complex variable.

Since $\mathcal{N}(u)$ can behave quite sporadically, it makes sense to study basic analytic properties of $\zeta_{\mathsf{WR}(\mathbb{Z}^2)}(s)$.

Theorem 12 (F. (2008-2009)). $\zeta_{\mathsf{WR}(\mathbb{Z}^2)}(s)$ *has a pole of order two at* $s = 1$ *in the sense that*

$$0 < \lim_{s \to s_0^+} |s - s_0|^2 \sum_{u=1}^{\infty} |a_u u^{-s}| < \infty,$$

and is analytic for all $s \in \mathbb{C}$ *with* $\Re(s) > 1$.

Further results in $\mathsf{WR}(\Lambda_h)$ **(F., Moore, Ohana, Zeldow (2010))**

- We describe the set of all possible index values

$$\mathcal{J} := \{|\Lambda_h : \Gamma| : \Gamma \in \mathsf{WR}(\Lambda_h)\}.$$

- For a fixed $J \in \mathcal{J}$, we describe procedures to find

$$\mathcal{N}(J) := |\{\Gamma \in \mathsf{WR}(\Lambda_h) : |\Lambda_h : \Gamma| = J\}|,$$

  and to find a lattice $\Gamma \in \mathsf{WR}(\Lambda_h)$ with $|\Lambda_h : \Gamma| = J$ that maximizes $|\Gamma|$.

- We show that a lattice $\Gamma \in \mathsf{WR}(\Lambda_h)$ of fixed index J maximizes $|\Gamma|$ if and only if it minimizes the values of **Epstein zeta function**

$$E_\Gamma(s) = \sum_{\boldsymbol{x} \in \Gamma \setminus \{\boldsymbol{0}\}} \frac{1}{\|\boldsymbol{x}\|^{2s}}$$

  for all real $s > 1$. This is not so for non-WR lattices (Bernstein, Sloane, Wright (1997)).