

On Integral Well-rounded Lattices in the Plane

Lenny Fukshansky · Glenn Henshaw · Philip Liao ·
Matthew Prince · Xun Sun · Samuel Whitehead

Received: 6 November 2011 / Revised: 22 May 2012 / Accepted: 29 May 2012 /
Published online: 6 June 2012
© Springer Science+Business Media, LLC 2012

Abstract We investigate distribution of integral well-rounded lattices in the plane, parameterizing the set of their similarity classes by solutions of the family of Pell-type Diophantine equations of the form $x^2 + Dy^2 = z^2$ where $D > 0$ is squarefree. We apply this parameterization to the study of the greatest minimal norm and the highest signal-to-noise ratio on the set of such lattices with fixed determinant, also estimating cardinality of these sets (up to rotation and reflection) for each determinant value. This investigation extends previous work of the first author in the specific cases of integer and hexagonal lattices and is motivated by the importance of integral well-rounded lattices for discrete optimization problems. We briefly discuss an application of our results to planar lattice transmitter networks.

L. Fukshansky (✉) · P. Liao
Dept. of Mathematics, Claremont McKenna College, 850 Columbia Avenue, Claremont, CA 91711,
USA
e-mail: lenny@cmc.edu

P. Liao
e-mail: PLiao14@students.claremontmckenna.edu

G. Henshaw
Dept. of Mathematics and Computer Science, Wesleyan University, Middletown, CT 06459, USA
e-mail: ghenshaw@wesleyan.edu

M. Prince
Dept. of Mathematics, Harvey Mudd College, Claremont, CA 91711, USA
e-mail: mthwate@gmail.com

X. Sun
School of Mathematical Sciences, Claremont Graduate University, Claremont, CA 91711, USA
e-mail: foxfur_32@hotmail.com

S. Whitehead
Dept. of Mathematics, Pomona College, Claremont, CA 91711, USA
e-mail: scw22009@myail.pomona.edu

Keywords Integral lattices · Well-rounded lattices · Binary and ternary quadratic forms · Epstein zeta function

1 Introduction and Statement of Results

Let $N \geq 1$ be an integer, and let $\Lambda \subset \mathbb{R}^N$ be a lattice of full rank. Given a basis $\mathbf{a}_1, \dots, \mathbf{a}_N$ for Λ we can write $A = (\mathbf{a}_1, \dots, \mathbf{a}_N)$ for the corresponding basis matrix, and then $\Lambda = A\mathbb{Z}^N$. The corresponding norm form is defined as

$$Q_A(\mathbf{x}) = \mathbf{x}^t A^t A \mathbf{x},$$

and we say that the lattice is *integral* if the coefficient matrix $A^t A$ of this quadratic form has integer entries; it is easy to see that this definition does not depend on the choice of a basis. The matrix $A^t A$ is called a *Gram matrix* of the lattice Λ . Integral lattices are central objects in arithmetic theory of quadratic forms and in lattice theory. We define $\det(\Lambda)$ to be $|\det(A)|$, again independent of the basis choice, and (squared) *minimum* or *minimal norm*

$$|\Lambda| = \min\{\|\mathbf{x}\|^2 : \mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}\} = \min\{Q_A(\mathbf{y}) : \mathbf{y} \in \mathbb{Z}^N \setminus \{\mathbf{0}\}\},$$

where $\|\cdot\|$ stands for the usual Euclidean norm. Then each $\mathbf{x} \in \Lambda$ such that $\|\mathbf{x}\|^2 = |\Lambda|$ is called a *minimal vector*, and the set of minimal vectors of Λ is denoted by $S(\Lambda)$. A lattice Λ is called *well-rounded* (abbreviated WR) if the set $S(\Lambda)$ contains N linearly independent vectors. These vectors do not necessarily form a basis for lattices in any dimension N , however they are known to form a basis for all $N \leq 4$ (see, for instance [15]); we will refer to such a basis as a *minimal basis* for Λ . WR lattices are important in discrete optimization, in particular in the investigation of sphere-packing, sphere-covering, and kissing-number problems (see [12]), as well as in coding theory (see [1]). Properties of WR lattices have also been investigated in [13] in connection with Minkowski's conjecture and in [8] in connection with the linear Diophantine problem of Frobenius. A particularly interesting and important class of WR lattices are the integral well-rounded lattices (abbreviated IWR). The main objective of the current paper is to study the properties of IWR lattices in the plane, extending some of the previous results of Refs. [3], [4], and [6] with a view toward discrete optimization problems. Specifically, our investigation is motivated by the following three questions, which are the direct analogs of the questions asked about sublattices of the hexagonal lattice in [2]:

Question 1 Which IWR lattice Λ of a fixed determinant Δ maximizes the minimal norm? Since the density of circle-packing associated with Λ is equal to $\pi|\Lambda|/\Delta$, this choice of Λ also maximizes the packing density.

Question 2 Which IWR lattice Λ of a fixed determinant Δ maximizes the signal-to-noise ratio (defined below)?

Question 3 How many IWR lattices of a fixed determinant Δ are there, up to rotation and reflection? This number is known to be finite.

Given a lattice $\Lambda \in \mathbb{R}^N$, we can regard its nonzero points as transmitters which interfere with the transmitter at the origin, and then a standard measure of the *total interference* of Λ is given by $E_\Lambda(2)$, where

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

is the Epstein zeta-function of Λ , and the signal-to-noise ratio of Λ is defined by

$$\text{SNR}(\Lambda) = 10 \log_{10} \frac{1}{9E_\Lambda(2)}, \tag{2}$$

as in Ref. [2]. To maximize $\text{SNR}(\Lambda)$ on the set of all planar IWR lattices of a fixed determinant Δ is the same as to minimize $E_\Lambda(2)$ on this set. In fact, $E_\Lambda(s)$ for each real $s \geq 3$ is maximized by the same planar WR lattice of fixed determinant Δ that maximizes $|\Lambda|$, and vice versa (this follows from an old result of S. S. Ryskov [16]; see Lemma 3.1 below). Moreover, Lemma 3.2 and Remark 3.1 below suggest that it may likely be so for $s = 2$ as well. This would mean that Questions 1 and 2 are equivalent, which is not always so for non-WR lattices, as demonstrated in [2].

Suppose that we have a network of transmitters positioned at the points of a planar lattice Λ . The plane is tiled with translates of the Voronoi cell of Λ , which are the cells serviced by the corresponding transmitters at their centers. The packing density of Λ is precisely the proportion of the plane covered by the transmitter network. IWR lattices allow for transmitters of the same power and for integral distances between transmitters in the network, which simplifies positioning. Hence a lattice that answers Question 1 maximizes coverage and the lattice that answers Question 2 maximizes signal-to-noise ratio for a 2-dimensional lattice transmitter network with a fixed cell area Δ and integral distances between transmitters. Our Lemma 3.2 and Remark 3.1 below suggest that this may be done simultaneously. We present an algorithm for finding a lattice answering Question 1 for each possible value of Δ in Theorem 1.3. It is also interesting to understand how many choices for positioning a network of equal-power transmitters with integral distances between them and fixed cell area are there—this is an application of Question 3; we estimate this number in Theorem 1.4. We refer the reader to Ref. [17] for further information about transmitter networks on planar lattices.

To discuss the proposed questions in further detail, we build on a convenient description of IWR lattices which we outline next. An important equivalence relation on lattices is geometric similarity: two lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^N$ are called *similar*, denoted $\Lambda_1 \sim \Lambda_2$, if there exists a positive real number α and an $N \times N$ real orthogonal matrix U such that $\Lambda_2 = \alpha U \Lambda_1$. It is easy to see that similar lattices have the same algebraic structure, i.e., for every sublattice Γ_1 of a fixed index in Λ_1 there is a sublattice Γ_2 of the same index in Λ_2 so that $\Gamma_1 \sim \Gamma_2$. Most geometric and optimization properties of lattices (such as packing density, covering thickness, kissing number, signal-to-noise ratio, etc.) are invariant on similarity classes. Moreover, a WR lattice can only be similar to another WR lattice, so it makes sense to speak of WR similarity classes of lattices. If $\Lambda \subset \mathbb{R}^2$ is a full rank WR lattice, then its set of minimal vectors

$S(\Lambda)$ contains 4 or 6 vectors, and this number is 6 if and only if Λ is similar to the hexagonal lattice

$$\mathcal{H} := \begin{pmatrix} 2 & 1 \\ 0 & \sqrt{3} \end{pmatrix} \mathbb{Z}^2$$

(see, for instance Lemma 2.1 in [7]). Any two linearly independent vectors $\mathbf{x}, \mathbf{y} \in S(\Lambda)$ form a minimal basis. While this choice is not unique, it is always possible to select \mathbf{x}, \mathbf{y} so that the angle θ between these two vectors lies in the interval $[\pi/3, \pi/2]$, and any value of the angle in this interval is possible. From now on when we talk about a minimal basis for a WR lattice in the plane, we will always mean such a choice. Then the angle between minimal basis vectors is an invariant of the lattice, and we call it the *angle of the lattice* Λ , denoted $\theta(\Lambda)$; in other words, if \mathbf{x}, \mathbf{y} is any minimal basis for Λ and θ is the angle between \mathbf{x} and \mathbf{y} , then $\theta = \theta(\Lambda)$ (see [5] for details and proofs of the basic properties of WR lattices in \mathbb{R}^2). In fact, it is easy to notice that two WR lattices $\Lambda_1, \Lambda_2 \subset \mathbb{R}^2$ are similar if and only if $\theta(\Lambda_1) = \theta(\Lambda_2)$ (see [5] for a proof). Therefore the set of all similarity classes of WR lattices in \mathbb{R}^2 is bijectively parameterized by the set of all possible values of the angle, which is the interval $[\pi/3, \pi/2]$. On the other hand, this parameterization becomes less trivial if we talk about similarity classes of planar IWR lattices. In other words, one may wonder what are the possible values of $\theta(\Lambda)$ in the interval $[\pi/3, \pi/2]$ if Λ is IWR?

The following parameterization follows from the classical theory of integral lattices and quadratic forms (see, for instance Chap. 1 of [12]).

Proposition 1.1 *Let $\Lambda \subset \mathbb{R}^2$ be an IWR lattice, then*

$$\cos \theta(\Lambda) = \frac{p}{q}, \quad \sin \theta(\Lambda) = \frac{r\sqrt{D}}{q} \tag{3}$$

for some $p, r, q, D \in \mathbb{Z}_{>0}$ such that

$$p^2 + Dr^2 = q^2, \quad \gcd(p, q) = 1, \quad \frac{p}{q} \leq \frac{1}{2}, \quad \text{and } D \text{ squarefree}, \tag{4}$$

and so Λ is similar to

$$\Omega_D(p, q) := \begin{pmatrix} q & p \\ 0 & r\sqrt{D} \end{pmatrix} \mathbb{Z}^2. \tag{5}$$

Moreover, for every p, r, q, D satisfying (4), $\Omega_D(p, q)$ is an IWR lattice with the angle $\theta(\Omega_D(p, q))$ satisfying (3), and $\Omega_D(p, q) \sim \Omega_{D'}(p', q')$ if and only if $(p, r, q, D) = (p', r', q', D')$. In addition, if Λ is any IWR lattice similar to $\Omega_D(p, q)$, then

$$|\Lambda| \geq \left| \frac{1}{\sqrt{q}} \Omega_D(p, q) \right|, \tag{6}$$

where the lattice $\frac{1}{\sqrt{q}} \Omega_D(p, q)$ is also IWR. Due to this property, we call $\frac{1}{\sqrt{q}} \Omega_D(p, q)$ a minimal IWR lattice in its similarity class.

Remark 1.1 Notice in particular that the integer lattice $\mathbb{Z}^2 = \Omega_1(1, 1)$ and the hexagonal lattice $\mathcal{H} = \Omega_3(1, 2)$.

Hence we see that the set of similarity classes of planar IWR lattices is in bijective correspondence with the set of 4-tuples (p, r, q, D) satisfying (4). Here is an explicit characterization of this set of 4-tuples, which will be useful to us.

Lemma 1.2 *Let D be a positive squarefree integer and $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$ and $\sqrt{\frac{D}{3}} \leq \frac{m}{n} \leq \sqrt{3D}$. Now $p, r, q, D \in \mathbb{Z}_{>0}$ satisfy (4) if and only if*

$$p = \frac{|m^2 - Dn^2|}{2^e \gcd(m, D)}, \quad r = \frac{2mn}{2^e \gcd(m, D)}, \quad q = \frac{m^2 + Dn^2}{2^e \gcd(m, D)}, \quad (7)$$

where

$$e = \begin{cases} 0 & \text{if either } 2 \mid D, \text{ or } 2 \mid (D + 1), mn \\ 1 & \text{otherwise.} \end{cases} \quad (8)$$

We prove Lemma 1.2 in Sect. 2. Further, let us say that an IWR planar lattice Λ is of type D for a squarefree $D \in \mathbb{Z}_{>0}$ if it is similar to some $\Omega_D(p, q)$ as in (5). The type is uniquely defined, i.e., Λ cannot be of two different types. Moreover, a planar IWR lattice Λ is of type D for some squarefree $D \in \mathbb{Z}_{>0}$ if and only if all of its IWR finite index sublattices are also of type D . If this is the case, Λ contains a sublattice similar to $\Omega_D(p, q)$ for every 4-tuple (p, r, q, D) as in (4). Hence the set of planar IWR lattices is split into types which are indexed by positive squarefree integers with similarity classes inside of each type D being in bijective correspondence with solutions to the ternary Diophantine equation $p^2 + r^2D = q^2$ as parameterized in Lemma 1.2.

Remark 1.2 In fact, the set of similarity classes of IWR lattices of a fixed type can be endowed with a semigroup structure, coming from the geometric group law on rational points of a Pell conic; we include a brief discussion of this fact in Sect. 2 below (Lemma 2.2). The correspondence between IWR lattices and solutions to the Pell-type equations as described above follows from the theory of integral quadratic forms, as we indicated; it can also be obtained by an elementary argument, however we do not include it here in the interest of brevity of the exposition.

In Sect. 3 we discuss a possible connection between Questions 1 and 2, and then use the above-described correspondence to provide an algorithmic procedure in answer to Question 1.

Theorem 1.3 *A positive real number Δ is a determinant value of IWR lattices if and only if $\Delta = M\sqrt{D}$ where $M, D \in \mathbb{Z}_{>0}$ with D squarefree so that the set*

$$\text{mn}(M) = \left\{ (m, n) \in \mathbb{Z}_{>0}^2 : \gcd(m, n) = 1, \sqrt{\frac{D}{3}} \leq \frac{m}{n} \leq \sqrt{3D}, \frac{2mn}{2^e \gcd(m, D)} \mid M \right\}, \quad (9)$$

where e is as in (8), is not empty. Fix such a Δ , and let $(m, n) \in \text{mn}(M)$ be the pair that maximizes the expression

$$\frac{m}{n} + D \frac{n}{m}$$

on $\text{mn}(M)$. Now define p, r, q as in (7) for this choice of m, n and let $k = M/r$. Then

$$\Lambda = \sqrt{\frac{k}{q}} \Omega_D(p, q) \tag{10}$$

is an IWR lattice with $\det(\Lambda) = \Delta$ and $|\Lambda| = kq$ which maximizes $|\Lambda|$ among all planar IWR lattices with determinant Δ . This lattice can be found in a finite number of steps for each fixed Δ .

Remark 1.3 Some examples of such norm-maximizing lattices are presented in Table 1 below.

In Sect. 4 we obtain the following counting estimate, which answers Question 3.

Theorem 1.4 For $\Delta \in \mathbb{R}_{>0}$, define $\text{IWR}(\Delta)$ to be the set of all planar IWR lattices, up to rotation and reflection, with determinant $= \Delta$. Then the set $\text{IWR}(\Delta)$ is finite for any Δ , and it is only nonempty if $\Delta = M\sqrt{D}$ with the set $\text{mn}(M)$ as in (9) nonempty. In this latter case, the cardinality of the set $\text{IWR}(\Delta)$ satisfies

$$|\text{IWR}(\Delta)| \leq \frac{1}{2} \sum_{r|M} 2^{\omega(rD)}. \tag{11}$$

Moreover,

$$|\text{IWR}(\Delta)| \ll \sum_{r|M} \sum_{g|r} \mu\left(\frac{r}{g}\right) \frac{\tau(g^2D)}{\sqrt{\omega(gD)}}, \tag{12}$$

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 .

We are now ready to proceed.

2 Parameterization Lemmas

In this section we start by proving Lemma 1.2. The following lemma is used in the proof, which we state here for the reader’s convenience.

Lemma 2.1 (Lemma 2.1 of [6]) Consider the Diophantine equation

$$\alpha x^2 + \beta xy + \gamma y^2 = \delta z^2, \tag{13}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ with $\beta^2 \neq 4\alpha\gamma$ and $\delta \neq 0$. Then either this equation has no integral solutions with $z \neq 0$, or all such solutions (x, y, z) of (13) are rational multiples of

$$\begin{aligned} x &= \gamma n(an - 2bm) - (\alpha a + \beta b)m^2, \\ y &= \alpha m(bm - 2an) - (\gamma b + \beta a)n^2, \\ z &= \pm c(\alpha m^2 + \beta mn + \gamma n^2), \end{aligned} \tag{14}$$

where $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$ and $m \geq 0$; here (a, b, c) is any integral solution to (13) with $c \neq 0$. In this later case, every multiple of (14) is a solution to (13) by homogeneity of (13).

Proof of Lemma 1.2 We start by applying Lemma 2.1 to the equation $p^2 + Dr^2 = q^2$ for a fixed squarefree D : since $(p, r, q) = (1, 0, 1)$ is an integral solution of this equation with $q \neq 0$, the lemma guarantees that all positive integral solutions of this equation with $q \neq 0$ are rational multiples of

$$p_0 = |m^2 - Dn^2|, \quad r_0 = 2mn, \quad q_0 = m^2 + Dn^2, \tag{15}$$

where m, n range over all relatively prime non-negative integers, not both 0. In order for (p, r, q, D) to satisfy (4), we need two more conditions: $\gcd(p, q) = 1$ and $p/q \leq 1/2$. First consider p_0, r_0, q_0 as in (15) and notice that the fact that $p_0^2 + Dr_0^2 = q_0^2$ implies that $\gcd(p_0, q_0) = \gcd(r_0, q_0) = \gcd(p_0, r_0, q_0)$. Since $\gcd(m, n) = 1$, it is easy to notice that $\gcd(p_0, q_0) = 2^e \gcd(m, D)$, where e is as in (8). Hence if we define p, r, q as in (7), we ensure that they are relatively prime, and this covers all the relatively prime solutions of our equation for each fixed D . Finally, we need to select only the solutions with $p/q \leq 1/2$, which means that

$$-1/2 \leq \frac{m^2 - Dn^2}{m^2 + Dn^2} \leq 1/2,$$

and so we must have

$$\sqrt{\frac{D}{3}} \leq \frac{m}{n} \leq \sqrt{3D}. \tag{16}$$

This completes the proof of the theorem. □

We also briefly mention the algebraic structure of the planar IWR lattices.

Lemma 2.2 *Let $D > 0$ be squarefree and let $\mathcal{C}(D)$ be the set of similarity classes of all IWR lattices of type D . Let us write $C_D(p, q)$ for each such class, i.e., for each (p, q) satisfying (4):*

$$C_D(p, q) = \{ \Lambda : \Lambda \sim \Omega_D(p, q) \}, \tag{17}$$

and so

$$\mathcal{C}(D) = \{ C_D(p, q) : (p, q) \text{ satisfy (4)} \}.$$

Then the set $\mathcal{C}(D)$ has the structure of an abelian semigroup, induced by the composition law on rational points of the Pell conic corresponding to D .

Proof A Pell conic is a curve given by the equation $x^2 - Dy^2 = 1$. The following commutative composition law on the set of rational points on a Pell conic is defined in [11]:

$$(x_1, y_1) + (x_2, y_2) = (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1). \quad (18)$$

In [11], this operation is also described geometrically by analogy with addition on an elliptic curve. Notice that a rational point $(x, y) = (q/p, r/p)$ is on this curve if and only if

$$p^2 + r^2D = q^2. \quad (19)$$

Then (18) induces the following commutative composition law on the set of solutions (p, r, q) of (19):

$$(p_1, r_1, q_1) + (p_2, r_2, q_2) = \frac{1}{g}(p_1p_2, r_1q_2 + r_2q_1, q_1q_2 + Dr_1r_2), \quad (20)$$

where $g = \gcd(p_1p_2, r_1q_2 + r_2q_1, q_1q_2 + Dr_1r_2)$. It is easy to check that the set of solutions of (19) is closed under this operation. Moreover, since $D > 0$,

$$\frac{q_1q_2 + Dr_1r_2}{p_1p_2} \geq \frac{q_1}{p_1} \times \frac{q_2}{p_2},$$

and so whenever $p_1/q_1, p_2/q_2 \leq 1/2$, we will have

$$\frac{p_1p_2}{q_1q_2 + Dr_1r_2} \leq \frac{1}{4}.$$

This ensures that $\mathcal{C}(D)$ is closed under this operation, and hence has a structure of an abelian semigroup, although not a monoid: the point $(1, 0, 1)$, which serves as identity, is not in $\mathcal{C}(D)$. \square

3 Optimization Properties

In this section we investigate Questions 1 and 2. Let Λ be a planar IWR lattice, then

$$\Lambda = \sqrt{\frac{k}{q}} U \Omega_D(p, q) \quad (21)$$

for some (p, r, q, D) as in (4), $k \in \mathbb{Z}_{>0}$, and a 2×2 real orthogonal matrix U . Now suppose that $\Delta = M\sqrt{D}$, $M \in \mathbb{Z}_{>0}$, is fixed and let $\Lambda \in \text{IWR}(\Delta)$ be given as in (21) so that $kr = M$. Then

$$|\Lambda| = kq = \frac{Mq}{r}, \quad (22)$$

and so to maximize $|\Lambda|$ on $\text{IWR}(\Delta)$ we need to maximize q/r . A trivial upper bound for $|\Lambda|$ is given by $\frac{2\Delta}{\sqrt{3}}$: this is just a restatement of the fact that $\Delta = |\Lambda| \sin \theta(\Lambda)$ and $\theta \in [\pi/3, \pi/2]$.

We start by discussing a connection between the problems of maximizing $|\Lambda|$ and minimizing $E_\Lambda(s)$ on sets of WR lattices of fixed determinant in \mathbb{R}^2 . This discussion is an adaptation and correction of Lemma 5.2 of [6].

Lemma 3.1 *Let Δ be a positive real number, and let $\text{WR}_2(\Delta)$ be the set of all full rank WR lattices in \mathbb{R}^2 with determinant Δ . Then for any fixed real number $s \geq 3$, $E_\Lambda(s)$ is a decreasing function of $|\Lambda|$ on $\text{WR}_2(\Delta)$.*

Proof Let $Q_\Lambda(x, y)$ be the quadratic form of Λ corresponding to a minimal basis; then

$$Q_\Lambda(x, y) = |\Lambda|(x^2 + y^2 + 2xy \cos \theta), \tag{23}$$

where $\theta = \theta(\Lambda) \in [\pi/3, \pi/2]$ and $|\Lambda|$ is as in (22). Now

$$\cos \theta = \frac{\sqrt{|\Lambda|^2 - \Delta^2}}{|\Lambda|} = \sqrt{1 - \frac{\Delta^2}{|\Lambda|^2}}, \tag{24}$$

and $0 \leq \cos \theta \leq 1/2$. Lemma 1 of [16] guarantees that $E_\Lambda(s)$ is a decreasing function of $\cos \theta$ for any real $s \geq 3$, and (24) implies that $\cos \theta$ is an increasing function of $|\Lambda|$. Hence $E_\Lambda(s)$ is a decreasing function of $|\Lambda|$ on $\text{WR}_2(\Delta)$ for $s \geq 3$. \square

In fact, it seems likely that the statement of Lemma 3.1 should hold for smaller real values of s as well. At the very least, we have the following bounds.

Lemma 3.2 *With notation as in Lemma 3.1, let $s > 1$ be real. Then there exist real constants $C_1(s)$ and $C_2(s)$, dependent only on s , such that*

$$\frac{C_1(s)}{|\Lambda|^s} \leq E_\Lambda(s) \leq \frac{C_2(s)}{|\Lambda|^s} \tag{25}$$

for every $\Lambda \in \text{WR}_2(\Delta)$.

Proof Combining (23) and (24), we obtain

$$Q_\Lambda(x, y) = Tx^2 + Ty^2 + 2xy\sqrt{T^2 - \Delta^2},$$

where $T = |\Lambda|$. The Epstein zeta-function of Λ is then given by

$$\begin{aligned} E_\Lambda(s) &= \sum_{x,y \in \mathbb{Z} \setminus \{0\}} Q_\Lambda(x, y)^{-s} = \sum_{x,y \in \mathbb{Z} \setminus \{0\}} \frac{1}{(Tx^2 + Ty^2 + 2xy\sqrt{T^2 - \Delta^2})^s} \\ &= \sum_{x,y \in \mathbb{Z}_{>0}} \left(\frac{2}{(Tx^2 + Ty^2 + 2xy\sqrt{T^2 - \Delta^2})^s} \right. \\ &\quad \left. + \frac{2}{(Tx^2 + Ty^2 - 2xy\sqrt{T^2 - \Delta^2})^s} \right). \end{aligned}$$

Now recall that since $\theta \in [\pi/3, \pi/2]$, we must have $\frac{\sqrt{3}T}{2} \leq \Delta \leq T$, and so $0 \leq \sqrt{T^2 - \Delta^2} \leq T/2$. Hence for each fixed real $s > 1$, we have

$$E_\Delta(s) \leq \frac{2}{T^s} \sum_{x,y \in \mathbb{Z}_{>0}} \left(\frac{1}{(x^2 + y^2)^s} + \frac{1}{(x^2 + y^2 - xy)^s} \right), \tag{26}$$

and

$$E_\Delta(s) \geq \frac{2}{T^s} \sum_{x,y \in \mathbb{Z}_{>0}} \left(\frac{1}{(x^2 + y^2)^s} + \frac{1}{(x^2 + y^2 + xy)^s} \right). \tag{27}$$

Since both series in the bounds of (26) and (27) converge, we have (25). □

Remark 3.1 Since WR lattice Λ with fixed $|\Lambda|$ and $\det(\Lambda)$ is unique up to multiplication by an orthogonal matrix U (which does not change the value of $E_\Lambda(s)$ for any s), Lemmas 3.1 and 3.2 make it natural to expect that the total interference of Λ is minimized on $WR_2(\Delta)$ (and so $SNR(\Lambda)$ is maximized) if and only if $|\Lambda|$ is maximized.

We are now ready to answer Question 1.

Proof of Theorem 1.3 We will now discuss a finite procedure to maximize q/r , and hence $|\Lambda|$, on the set $IWR(\Delta)$ using finiteness of this set along with Lemma 1.2. First we notice that r has to be a divisor of $M = \Delta/\sqrt{D}$, hence we can start by going through the list of all possible divisors of M . For each such divisor r , consider all possible decompositions

$$r = \frac{2mn}{2^e \gcd(m, D)}$$

with relatively prime m, n so that $m/n \in [\sqrt{D/3}, \sqrt{3D}]$, as in (7). Out of all such decompositions, we want to pick one which maximizes the ratio

$$q/r = \frac{m^2 + Dn^2}{2mn} = \frac{1}{2} \left(\frac{m}{n} + D \frac{n}{m} \right).$$

This can be done in a finite number of steps, since there are finitely many values for r , a divisor of M , and for each r there are finitely many such m, n . Hence we can choose Λ maximizing $|\Lambda|$ and $SNR(\Lambda)$ on $IWR(\Delta)$ to be as in (10). In particular, our argument confirms that Δ is a determinant value of an IWR lattice if and only if it is of the form $M\sqrt{D}$ with the set $mn(M)$ as in (9) nonempty. This completes the proof. □

Remark 3.2 Let us write $m/n = \sqrt{D}x$ for appropriate $x \in [1/\sqrt{3}, \sqrt{3}]$. Then

$$q/r = \frac{\sqrt{D}}{2}(x + 1/x).$$

Table 1 Examples of IWR lattices Λ with $\det(\Lambda) = \Delta$ that maximize $|\Lambda|$ on $\text{IWR}(\Delta)$

Δ	$ \Lambda $	Λ
$24\sqrt{5}$	61	$\sqrt{\frac{1}{61}}\Omega_5(29, 61)$
$24\sqrt{7}$	69	$\sqrt{\frac{3}{23}}\Omega_7(9, 23)$
$20\sqrt{11}$	75	$\sqrt{\frac{1}{3}}\Omega_{11}(7, 15)$
$24\sqrt{13}$	98	$\sqrt{\frac{2}{49}}\Omega_{13}(7, 15)$
$24\sqrt{17}$	104	$\sqrt{\frac{8}{13}}\Omega_{17}(4, 13)$
$105\sqrt{19}$	510	$\sqrt{\frac{15}{34}}\Omega_{19}(15, 34)$
$96\sqrt{23}$	522	$\sqrt{\frac{6}{87}}\Omega_{23}(41, 87)$

Now, the function $f(x) = x + 1/x$ assumes its maximal values on the interval $[1/\sqrt{3}, \sqrt{3}]$ at the endpoints and has a minimum at $x = 1$. Hence, to maximize q/r one should consider m, n with m/n close to the endpoints of the interval $[\sqrt{D/3}, \sqrt{3D}]$. Keeping these considerations in mind can reduce the number of computational steps necessary to find maximizer for $|\Lambda|$ in $\text{IWR}(\Delta)$ in each particular case.

We give some computational examples in Table 1.

4 Counting Estimates

Here we prove the counting estimates of Theorem 1.4.

Proof of Theorem 1.4 Let $\Delta = M\sqrt{D}$, as above, so that $\text{mn}(M)$ defined in (9) is nonempty. First we observe that such sets are in fact finite up to rotation and reflection—this is an immediate consequence of a more general fact that there are only finitely many isometry classes of integral lattices of fixed determinant in a fixed dimension (see remarks on p. 432 of [12]). Suppose now that $\Lambda \in \text{IWR}(\Delta)$, then we can assume without loss of generality that

$$\Lambda = \sqrt{\frac{k}{q}}\Omega_D(p, q),$$

where $k = M/r$ and p, r, q are as in (7) for some $(m, n) \in \text{mn}(M)$. Hence the choice of p, r, q determines Λ uniquely. For each $r \mid M$ define

$$f(r) = \left| \left\{ (p, q) \in \mathbb{Z}_{>0}^2 : q^2 - p^2 = r^2D, \gcd(p, q) = 1, 0 < \frac{p}{q} \leq \frac{1}{2} \right\} \right|, \tag{28}$$

then

$$|\text{IWR}(\Delta)| = \sum_{r \mid M} f(r).$$

Hence we want to produce estimates on $f(r)$. Define

$$f_1(r) = |\{(p, q) \in \mathbb{Z}_{>0}^2 : q^2 - p^2 = r^2D, \gcd(p, q) = 1\}|,$$

and

$$f_2(r) = \left| \left\{ (p, q) \in \mathbb{Z}_{>0}^2 : q^2 - p^2 = r^2D, 0 < \frac{p}{q} \leq \frac{1}{2} \right\} \right|, \tag{29}$$

and notice that

$$f(r) \leq \min\{f_1(r), f_2(r)\}, \tag{30}$$

meaning that

$$|\text{IWR}(\Delta)| \leq \sum_{r|M} \min\{f_1(r), f_2(r)\}. \tag{31}$$

The function $f_1(r)$ is well studied; in particular, the following formula follows from Theorem 6.2.4 of [14]:

$$f_1(r) = \begin{cases} 2^{\omega(r^2D)-1} & \text{if } 2 \nmid r^2D, r^2D > 1 \\ 2^{\omega(r^2D)-1} & \text{if } 8 \mid r^2D, r^2D \text{ has odd prime divisors} \\ 1 & \text{if } r^2D \text{ is a power of } 2 \\ 0 & \text{otherwise,} \end{cases} \tag{32}$$

hence $f_1(r) \leq 2^{\omega(r^2D)-1} = 2^{\omega(rD)-1}$. Now (11) follows upon combining (31), (32).

Next we estimate $f_2(r)$. Let $c = r^2D$, and let us write

$$a = q - p, \quad b = q + p, \tag{33}$$

then $q = (a + b)/2$, $p = (b - a)/2$, and $ab = c$. Let $\alpha := p/q$, and assume that $0 < \alpha \leq 1/2$. Then let $v = \frac{1+\alpha}{1-\alpha}$, and observe that

$$1 < v = \frac{b}{a} \leq 3.$$

Since $ab = c$, we have $b = \sqrt{vc}$, and so

$$\sqrt{c} < b \leq \sqrt{3c}.$$

Therefore

$$f_2(r) = |\{b \in \mathbb{Z}_{>0} : b \mid c, \sqrt{c} < b \leq \sqrt{3c}\}|. \tag{34}$$

For a positive integer t , Hooley’s Δ -function of t (see [9] for detailed information) is defined as

$$\Delta(t) = \max_x |\{b \in \mathbb{Z}_{>0} : b \mid t, e^x < b \leq e^{x+1}\}|.$$

Take $x = \log \sqrt{c}$, then

$$\{b \in \mathbb{Z}_{>0} : b \mid c, \sqrt{c} < b \leq \sqrt{3c}\} \subseteq \{b \in \mathbb{Z}_{>0} : b \mid c, e^x < b \leq e^{x+1}\},$$

since $\sqrt{3} < e$, and so $f_2(r) \leq \Delta(c)$. Therefore an estimate on $f_2(r)$ would follow from estimates on $\Delta(c)$, some of which can be found in Sect. 2 of [3]; in particular, equations (10)–(13) of [3] imply that the bound

$$f_2(r) \leq O\left(\frac{\tau(c)}{\sqrt{\omega(c)}}\right) \leq O\left(c^{\frac{(1+\varepsilon)\log^2}{\log \log c}}\right) \tag{35}$$

holds for any $\varepsilon > 0$, assuming c is greater than some $c_0(\varepsilon)$ for the second inequality; here the constant in O -notation is independent of c .

Next notice that if $q^2 - p^2 = r^2 D$ and $g \mid p, q$, then $g \mid r$, since D is squarefree. This implies that

$$f_2(r) = \sum_{g \mid r} f\left(\frac{r}{g}\right). \tag{36}$$

Recall that the Möbius function is defined by

$$\mu(u) = \begin{cases} (-1)^{\omega(u)} & \text{if } u \text{ is squarefree} \\ 0 & \text{otherwise;} \end{cases}$$

then, applying the Möbius inversion formula to (36), we obtain

$$f(r) = \sum_{g \mid r} \mu\left(\frac{r}{g}\right) f_2(g) \ll \sum_{g \mid r} \mu\left(\frac{r}{g}\right) \frac{\tau(g^2 D)}{\sqrt{\omega(g^2 D)}} \tag{37}$$

by (35). This establishes (12) upon the observation that $\omega(g^2 D) = \omega(g D)$. □

Remark 4.1 Theorems 431 and 432 of [10] state that normal orders of $\omega(u)$ and $\tau(u)$ are $\log \log u$ and $2^{\log \log u}$, respectively. This implies that one would normally expect

$$\frac{\tau(u)}{\sqrt{\omega(u)}} \leq 2^{\omega(u)}$$

for a randomly chosen integer u (in the appropriate sense).

Acknowledgements We would like to thank the Fletcher Jones Foundation-supported Claremont Colleges fellowship program, under the auspices of which this work was done during the Summer of 2011. We thank Professor Wai Kiu Chan and the anonymous referees for their useful comments on the subject of this paper. The first author also acknowledges partial support from the Simons Foundation (grant #208969) and from NSA (Young Investigator Grant #1210223).

References

1. Banihashemi, A.H., Khandani, A.K.: On the complexity of decoding lattices using the Korkin–Zolotarev reduced basis. *IEEE Trans. Inf. Theory* **44**(1), 162–171 (1998)

2. Bernstein, M., Sloane, N.J.A., Wright, P.E.: On sublattices of the hexagonal lattice. *Discrete Math.* **170**(1–3), 29–39 (1997)
3. Fukshansky, L.: On distribution of well-rounded sublattices of \mathbb{Z}^2 . *J. Number Theory* **128**(8), 2359–2393 (2008)
4. Fukshansky, L.: On similarity classes of well-rounded sublattices of \mathbb{Z}^2 . *J. Number Theory* **129**(10), 2530–2556 (2009)
5. Fukshansky, L.: Revisiting the hexagonal lattice: on optimal lattice circle packing. *Elem. Math.* **66**(1), 1–9 (2011)
6. Fukshansky, L., Moore, D., Ohana, R.A., Zeldow, W.: On well-rounded sublattices of the hexagonal lattice. *Discrete Math.* **310**(23), 3287–3302 (2010)
7. Fukshansky, L., Petersen, K.: On ideal well-rounded lattices. *Int. J. Number Theory* **8**(1), 189–206 (2012)
8. Fukshansky, L., Robins, S.: Frobenius problem and the covering radius of a lattice. *Discrete Comput. Geom.* **37**(3), 471–483 (2007)
9. Hall, R., Tenenbaum, G.: *Divisors*. Cambridge Univ. Press, Cambridge (1988)
10. Hardy, G.H., Wright, E.M.: *An Introduction to the Theory of Numbers*, 5th edn. Clarendon Press, New York (1979)
11. Lemmermeyer, F.: Conics—a poor man’s elliptic curves. <http://www.fen.bilkent.edu.tr/~franz/publ/conics.pdf>
12. Martinet, J.: *Perfect Lattices in Euclidean Spaces*. Springer, Berlin (2003)
13. McMullen, C.: Minkowski’s conjecture, well-rounded lattices and topological dimension. *J. Am. Math. Soc.* **18**(3), 711–734 (2005)
14. Mollin, R.A.: *Fundamental Number Theory with Applications*. CRC Press, Boca Raton (1998)
15. Pohst, M.: On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. *ACM SIGSAM Bull.* **15**(1), 37–44 (1981)
16. Ryskov, S.S.: The two-dimensional ζ -function with real parameter. *Dokl. Akad. Nauk SSSR* **184**, 288–291 (1969)
17. van den Heuvel, J.: Radio channel assignment on 2-dimensional lattices. *Ann. Comb.* **6**(3–4), 463–477 (2002)