Fall 2022

On Coherence and the Geometry of Certain Families of Lattices

David Booth Kogan
Claremont Graduate University

On coherence and the geometry of certain families of lattices

BY

DAVID BOOTH KOGAN

Claremont Graduate University
2022

This dissertation has been duly read, reviewed, and critiqued by the Committee listed below, which hereby approves the manuscript of David Booth Kogan as fulfilling the scope and quality requirements for the degree of Doctor of Philosophy in Mathematics.

Lenny Fukshansky, Chair
Claremont McKenna College
Professor of Mathematics

Stephan Ramon Garcia
Pomona College
Professor of Mathematics

Allon Percus
Claremont Graduate University
Professor of Mathematics

ABSTRACT

On coherence and the geometry of certain families of lattices

by

David Booth Kogan

Claremont Graduate University: 2022

The coherence of a lattice is, roughly speaking, a measure of non-orthogonality of its minimal vectors. It was introduced to lattices (by analogy with frame theory) by L. Fukshansky and others as a possible route to gaining insight into packing density, a central problem in lattice theory. In this work, we introduce the related measure of average coherence, explore connections between packing density and coherence, and prove several properties of certain families of lattices, most notably nearly orthogonal lattices, cyclotomic lattices, and cyclic lattices.

To my family

ACKNOWLEDGEMENTS

First, I wish to thank Professor Lenny Fukshansky. Without his attention, advice, patience, and generosity, there is no way this thesis could have come to fruition. His questions and suggestions have greatly improved not just my research, but my ability as a mathematician as well. Professor Percus, you were spot-on when you sat down with me and said "I know a professor at Claremont McKenna who is going to love getting his hands on you."

Next, I wish to thank my committee, Professors Stephan Garcia and Allon Percus, for agreeing to help guide this journey, and for what I have learned from you. I also wish to thank the Coordinator of the Intitute of Mathematical Sciences, Charlotte Ballesteros, for her help and attention, which were necessary.

Last but not least, I wish to thank my family, especially my mother Nan Booth. Your help and support have been integral to my success. I truly could not have done this without you.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

LIST OF TABLES

Table

CHAPTER I

Introduction

1.1 A brief history of lattices

The theory of Euclidean lattices[1] is a classical and important area of study which lies in the intersection of number theory and discrete geometry. A *lattice* is a discrete free $\mathbb{Z}$-module in a Euclidean space (usually $\mathbb{R}^n$ or $\mathbb{C}^n$). Equivalently, given a basis $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\}$ with $\boldsymbol{b}_i \in \mathbb{R}^n, k \leq n$, a lattice L may be defined as

$$L = \text{span}_{\mathbb{Z}}(B) = \left\{ \sum_{i=1}^{k} \alpha_i \boldsymbol{b}_i : \boldsymbol{b}_i \in \mathbb{R}^n, \alpha_i \in \mathbb{Z} \right\} = B\mathbb{Z}^k.$$

We should note some authors consider a lattice to be the combination (L, S) with S a specified positive definite bilinear form.

The study of integral combinations of basis elements is classical, stretching back to the ancient problems of Diophantine equations and finding Pythagorean triples, through Fermat's theorem on expressing odd primes as the sums of two squares, Lagrange's celebrated four square theorem, and Gauss's *Disquisitiones Arithmeticae*.

A *quadratic form* is a polynomial in which every term has degree 2. $x^2+3xy-4y^2$, $2t^2-tv$, and $3xy$ are all examples of integral quadratic forms.[2] There is a "dictionary"

[1] Other areas of mathematics use the term "lattice" to mean a partially ordered set that meets certain conditions on inclusion. This is not that sort of lattice.

[2] Historically, there have been competing definitions of an integral quadratic form. For instance,

that relates quadratic forms to lattices: similarity classes of lattices correspond with equivalence classes of quadratic forms ([49], §1.7).

It was in this guise that much of the historic work on lattices was done. The solution of the lattice packing density problem in 2 dimensions is usually credited to Lagrange. In 3 dimensions, it was solved by Gauss; Korkine and Zolotareff solved the problem in dimensions 4 and 5, and Blichfeldt solved dimensions $6-8$. The only other lattice proven to be an optimal lattice sphere packing is the Leech lattice Λ_{24} ([15]), which is in fact optimal among all packings in 24 dimensions (see generally [19] and [49], as well as [16] and [65]).

A closely related problem is the kissing number problem: how many spheres may simultaneously touch a central sphere. Even less has been proven in this space, with solutions only known in dimensions $2, 3, 4, 8$, and 24 (see [67], [43], [58], and [55]).

1.2 Definitions

In this section we define several terms that will play a major part throughout this work. We define the *determinant* of a lattice L to be the absolute value of the determinant of any basis matrix of the lattice. If $L = B\mathbb{Z}^n$ then

$$\det(L) := \sqrt{\det(B^\top B)}.$$

If B is $n \times n$, then $\det(L) = |\det(B)|$. Because a lattice is discrete, it must have non-zero vectors of shortest length. We define the *minimum*[3] of a lattice L to be

$$|L| := \min\{\|\boldsymbol{x}\| : \boldsymbol{x} \in L \setminus \{\mathbf{0}\}\},$$

Gauss used what is now called the "classically integral form" which is the form $ax^2 + 2bxy + cy^2$. The advantage of this is that the matrix of the associated symmetric bilinear form has only integer entries, even off the diagonal. In modern usage, a quadratic form is integral so long as all coefficients are integers.

[3]Sometimes called the *minimal length* or *minimal norm*.

where $\|\ \|$ indicates the standard Euclidean norm, and the set of all such minimal vectors is denoted

$$S(L) = \{\boldsymbol{x} \in L : \|\boldsymbol{x}\| = |L|\}.$$

Several important properties of lattices are defined based on its set of minimal vectors. A lattice L is called *weakly eutactic* if there exist real numbers $c_1, \ldots, c_n$, called *eutaxy coefficients*, such that

$$\|\boldsymbol{v}\|^2 = \sum_{\boldsymbol{x} \in S(L)} c_i(\boldsymbol{v}, \boldsymbol{x}_i)^2$$

for all $\boldsymbol{v} \in \mathbb{R}^n$. If all eutaxy coefficients are positive, L is called *eutactic*, and if $c_1 = \cdots = c_n > 0$, the lattice L is called *strongly eutactic*; for instance, the integer lattice $\mathbb{Z}^n$ is strongly eutactic. Further, L is *perfect* if the set $\{\boldsymbol{x}\boldsymbol{x}^\top : \boldsymbol{x} \in S(L)\}$ spans the space of $n \times n$ real symmetric matrices,[4] i.e. if

$$\operatorname{span}_{\mathbb{R}} \left\{\boldsymbol{x}\boldsymbol{x}^\top : \boldsymbol{x} \in S(L)\right\} = \left\{X \in \mathbb{R}^{n \times n} : X = X^\top\right\}.$$

A lattice $L \in \mathbb{R}^n$ is called well-rounded (WR) if it possesses n linearly independent minimal vectors, i.e. if

$$\operatorname{span}_{\mathbb{R}} \{\boldsymbol{x} \in S(L)\} = \mathbb{R}^n.$$

Two lattices L_1, L_2 in $\mathbb{R}^n$ are called *similar* (written $L_1 \sim L_2$) if there exists a positive constant α and an $n \times n$ real orthogonal matrix U such that $L_2 = \alpha U L_1$. This is an equivalence relation on the space of lattices in $\mathbb{R}^n$ with equivalence classes referred to as *similarity classes* of lattices in $\mathbb{R}^n$. The space of similarity classes of lattices in $\mathbb{R}^n$ can be identified with $(\mathbb{R}_+ \times \mathcal{O}_n(\mathbb{R})) \setminus \mathrm{GL}_n(\mathbb{R}) / \mathrm{GL}_n(\mathbb{Z})$, i.e., lattices modulo left multiplication by positive constants and orthogonal matrices (see [49], §1.7). Many properties of a lattice are preserved under similarity, including coherence

[4]Here and throughout vectors are always written as columns.

and packing density.

One of the central lattice properties of interest is its sphere packing efficiency. To begin, we define a *fundamental domain*. A fundamental domain of a lattice is full set of coset representatives under the group action of translation by lattice points. In other words, if L is a lattice of full rank in $\mathbb{R}^n$, a fundamental domain is a convex set $\mathcal{F}$ such that

$$\mathbb{R}^n = \bigcup_{\boldsymbol{x} \in L} (\mathcal{F} + \boldsymbol{x}),$$

with

$$(\mathcal{F} + \boldsymbol{x}) \cap (\mathcal{F} + \boldsymbol{y}) = \emptyset$$

for $\boldsymbol{x} \neq \boldsymbol{y} \in L$. While there are infinitely many fundamental domains for any lattice, all have the same measure of $\det(L)$, and there are two primary ones. The *fundamental parallelotope* $\mathcal{F}$ of a lattice L with basis $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n$ is a fundamental domain of L, defined as

$$\mathcal{F} = \left\{ \sum_{i=1}^{n} t_i \boldsymbol{b}_i : 0 \leq t_i < 1 \right\}.$$

Another important region is called the *Voronoi cell* of a lattice, and can be constructed as the set of points in $\mathbb{R}^n$ closer to $\mathbf{0}$ than any other lattice point, i.e.

$$V = \{ \boldsymbol{x} \in \mathbb{R}^n : \|\boldsymbol{x}\| \leq \|\boldsymbol{x} - \boldsymbol{y}\| \ \forall \boldsymbol{y} \in L \}.$$

The Voronoi cell of a lattice is a closure of a fundamental domain.

To every lattice we may attach a packing, that is, a fitting of n-balls in $\mathbb{R}^n$ such that no point is contained in two or more balls, by centering a ball at each lattice point and growing them uniformly until any further expansion would cause two balls to overlap. It is clear that each ball in a lattice packing has radius $\frac{|L|}{2}$ and is enclosed within one, and only one, Voronoi cell translate (see, for example, Figure 1.2). We are now ready to define packing density properly.

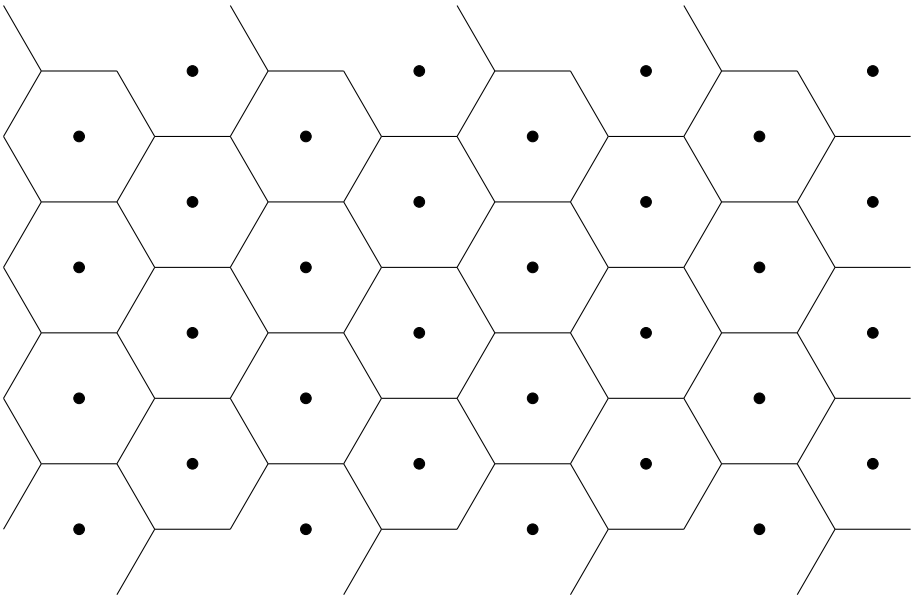

Figure 1.1: The lattice points and Voronoi cells of the hexagonal lattice, A_2, which we will introduce in the next section.

The *packing density* of a lattice L is the proportion of space its lattice packing occupies. From the definition of a fundamental domain, it is clear that this is the same as the proportion of a Voronoi cell covered by the ball around its lattice point. Thus, the packing density $\delta(L)$ of a lattice is

$$\delta(L) := \frac{\omega_n |L|^n}{2^n \det L}$$

where ω_n is the volume of a unit ball in $\mathbb{R}^n$.

The packing density function is continuous over the space of lattices (see e.g. [49], Chap. 2). Any lattice L for which $\delta(L)$ attains a local maximum is called an *extreme lattice*. A celebrated theorem of Voronoi states a lattice is extreme if and only if it is perfect and eutactic[5] [66], and a later paper by Ash shows all critical points of the density function occur at eutactic lattices [1].

Remark 1.2.1. When discussing the packing density of a lattice, we consider only the

[5]Korkine and Zolotareff had earlier proved that perfection was a necessary condition for an extreme form. See [41].

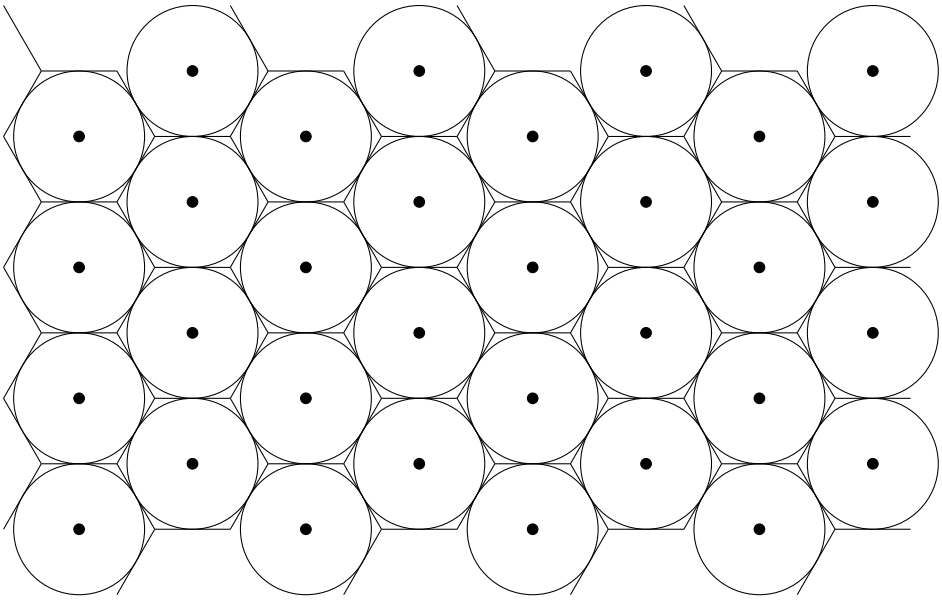

Figure 1.2: The lattice packing around the hexagonal lattice, A_2, with Voronoi cells.

space of WR lattices. There are two reasons for this. The first is that any perfect lattice, and any eutactic lattice, is necessarily WR. The second is that minima of the packing density only make sense with certain restrictions on what lattices are considered, otherwise we can always attain a worse packing through modification of the lattice.

Another property defined on $S(L)$ is *coherence*, which we borrow from the theory of frames. In [35] the concept of frame coherence was applied to lattices (see also Table 1 of [10]).We define the *maximal coherence* of the lattice L to be

$$\mathcal{C}(L) = \max\left\{\frac{|(\boldsymbol{x},\boldsymbol{y})|}{|L|} : \boldsymbol{x},\boldsymbol{y} \in S(L), \boldsymbol{x} \neq \pm\boldsymbol{y}\right\},$$

where $(\ ,\ )$ stands for the usual scalar product of vectors. Notice that

$$0 \leq \mathcal{C}(L) \leq 1/2,$$

since the angle between any two minimal vectors of a lattice is in the interval $[\pi/3, 2\pi/3]$

(see, for instance, Lemma 3.1 of [25]).

A related measure, *average coherence*, was introduced to frames in [4] and [5], and we adapted the concept to lattices in [30] (see chapter III). We define the average coherence of a lattice L to be

$$\mathcal{A}(L) := \frac{1}{|S'(L)| - 1} \cdot \max_{\boldsymbol{x} \in S'(L)} \left\{ \sum_{\boldsymbol{y} \in S'(L) \setminus \{\boldsymbol{x}\}} \frac{|(\boldsymbol{x}, \boldsymbol{y})|}{\|\boldsymbol{x}\| \|\boldsymbol{y}\|} \right\},$$

where $S'(L)$ is any half-set of $S(L)$ where just one of $\pm\boldsymbol{x} \in S(L)$ is taken to be in $S'(L)$.

Because lattices are additive groups, we define the index of a sublattice L' in a lattice L as the number of cosets of L modulo L'. It is a known fact that

$$[L : L'] = \frac{\det(L')}{\det(L)}$$

(see e.g. [49], Prop. 1.1.5[6]).

One way of producing a lattice is by embedding a number field[7] into real space. Let K be a number field of degree d over $\mathbb{Q}$, and let $\mathcal{O}_K$ be its ring of integers. Let

$$\sigma_1, \ldots, \sigma_{r_1}, \tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2} : K \hookrightarrow \mathbb{C}$$

be its embeddings into the field of complex numbers, where $r_1 + 2r_2 = d$ and $\sigma_1, \ldots, \sigma_{r_1}$ are real embeddings, whereas $\tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2}$ are pairs of complex conjugate embeddings. The *Minkowski embedding* of K into $\mathbb{R}^d$ is then defined as

$$\Sigma_K := (\sigma_1, \ldots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \ldots, \Re(\tau_{r_2}), \Im(\tau_{r_2})) : K \hookrightarrow \mathbb{R}^d,$$

[6] What we call $\det(L)$, [49] calls the discriminant of the lattice, $\Delta(L)$.

[7] A number field is a finite algebraic extension of $\mathbb{Q}$. For further discussion of the algebra involved, we refer the reader to e.g. [47].

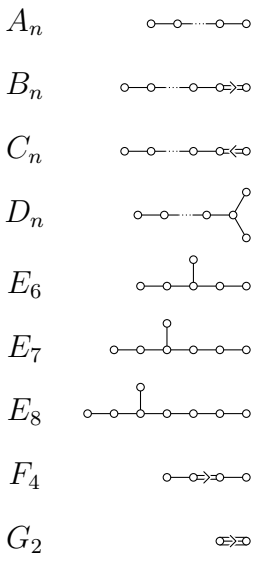

Figure 1.3: The Dynkin diagrams of the semi-simple Lie algebras. Roots are represented by circles, and connected by a single line if they are at a 120° angle to each other, a double line for a 135° angle, and a triple line for a 150° angle. If the roots are of different lengths, an arrow points towards the smaller root. A_n, D_n, E_6, E_7 and E_8 are the only systems generated by roots of the same length, and thus the only ones with associated root lattices.

and the image of $\mathcal{O}_K$ under this embedding, $\Lambda_K := \Sigma_K(\mathcal{O}_K)$, is a Euclidean lattice of full rank in $\mathbb{R}^d$.

Once we have a lattice, we can define another lattice in relation to it. Given a lattice $L \in \mathbb{R}^n$, we define its *dual lattice* to be $L^* := \{\boldsymbol{x} \in \mathbb{R}^n : (\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z}\ \forall \boldsymbol{y} \in L\}$.

1.3 Certain families of lattices

Several families of lattices will be discussed in this work. Nearly orthogonal, cyclotomic, and cyclic lattices each have a chapter devoted to them, and will be defined again there; here we introduce them along with other families.

Our first family are the famous root lattices. These have an immediate and obvious connection to root systems in Lie algebras, as the minimal vectors ("roots") of a root lattice *are*, in fact, the root system of some semi-simple Lie algebra. They follow the same naming convention, although there are no root lattices corresponding to the families B_n and C_n, and exceptional algebras F_4 and G_2 because those are generated by roots of different lengths, as can be seen in their Dynkin diagrams (Figure 1.3).

The root lattice A_n is defined as

$$A_n = \left\{ \boldsymbol{x} \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0 \right\},$$

and is a rank n lattice. The root lattice D_n is defined as

$$D_n = \left\{ \boldsymbol{x} \in \mathbb{Z}^{n} : \sum_{i=1}^{n} x_i \equiv 0 \pmod 2 \right\},$$

and is a rank n lattice. The root lattice E_8 is defined as

$$E_8 = D_8 \cup \left(\frac{1}{2} \left(\sum_{i=1}^{8} \boldsymbol{e}_i \right) + D_8 \right),$$

and is a rank 8 lattice. The root lattices E_7 and E_6 can be described as sublattices of E_8 orthogonal to the vector $\boldsymbol{e}_7 + \boldsymbol{e}_8$ and to the pair of vectors $\boldsymbol{e}_7 + \boldsymbol{e}_8$ and $\boldsymbol{e}_6 + \boldsymbol{e}_8$, respectively, and are rank 7 and 6 lattices, respectively.[8] It is well known that the root lattices are all local maxima of the packing density function, and further that $A_2, A_3 \cong D_3, D_4, D_5, E_6, E_7$, and E_8 all achieve the absolute maximum lattice packing density in their respective dimensions (see e.g. [19], §1.5).

Closely related to the root lattices are the Coxeter-Barnes lattices, A_n^r (called simply Coxeter lattices when $r|n+1$), which are best defined as lattices of rank n in $\mathbb{R}^{n+1}$ spanned over $\mathbb{Z}$ by the basis

$$\boldsymbol{e}_1 - \boldsymbol{e}_2, \ldots, \boldsymbol{e}_1 - \boldsymbol{e}_n, \ \frac{1}{r} \left(n\boldsymbol{e}_1 - \sum_{i=2}^{n} \boldsymbol{e}_i \right),$$

where $\boldsymbol{e}_i$ are standard basis vectors in $\mathbb{R}^{n+1}$. The Coxeter-Barnes lattice A_n^r can then be thought of as the unique sublattice of A_n^* containing the root lattice A_n as a sublattice to index $[A_n^r : A_n] = r$. The Coxeter lattices are also known to be extreme

[8] Unless otherwise specified, $\boldsymbol{e}_i$ always refers to the i-th canonical basis vector of whichever real space we are currently discussing, in this case $\mathbb{R}^8$.

for $n \geq 6, r \neq n+1$.

Next come nearly orthogonal lattices, introduced by [56]. These will be more thoroughly defined in §2.1. Broadly speaking, we call a basis of a lattice *nearly orthogonal* if any ordering of it produces successive subspaces each of which is sufficiently close to orthogonal to the next basis vector. Let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be an ordered basis for a lattice L in $\mathbb{R}^n$, and define a sequence of angles $\theta_1, \ldots, \theta_{n-1}$ as follows: each θ_i is the angle between $\boldsymbol{b}_{i+1}$ and the subspace $\text{span}_{\mathbb{R}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i\}$. For a given value $\theta \in [0, \pi/2]$, we will say that B is a *weakly θ-orthogonal* basis if $\theta_i \geq \theta$ for each $1 \leq i \leq n-1$, and *θ-orthogonal* if every ordering of it is weakly θ-orthogonal. If $\theta = \frac{\pi}{3}$, we simply call the basis nearly orthogonal.

An *ideal lattice* is one formed by applying the Minkowski embedding to a fractional ideal of the ring of itegers of some number field K. When K is a cyclotomic field, $\mathbb{Q}(\zeta_n)$, we call the embedding of its ring of integers a *cyclotomic lattice*. These will be discussed in detail in chapter III.

There is another interesting class of lattices we would like to introduce. A lattice $L \subset \mathbb{R}^n$, not necessarily of full rank, is called *cyclic* in $\mathbb{R}^n$ if it closed under the rotation shift linear operator $\rho : \mathbb{R}^n \to \mathbb{R}^n$, given by

$$\rho(c_1, c_2, \ldots, c_n) = (c_n, c_1, \ldots, c_{n-1}),$$

i.e. if $\rho(L) = L$. These lattices are discussed in detail in chapter V.

We should also note that many lattices fall into many categories. For instance, the Coxeter lattices are simple cyclic (see chapter V) for $n \geq 5, r = \frac{n+1}{2}$ (see [49], §5.2)

There are many other famous families of lattices not covered in this paper, such as the Barnes-Wall lattices ([6]), Craig's lattices ([21]), and laminated lattices (some of the lattices mentioned here are laminated lattices, including but not limited to

L	A_n	$D_n (n \geq 4)$	E_6	E_7	E_8	$A_n^{\frac{n+1}{2}} (n \text{ odd}, n \geq 9)$
$\lvert L\rvert^2$	2	2	2	2	2	N
$\det L^2$	$n+1$	4	3	2	1	D
$\mathcal{C}(L)$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{n-3}{2(n-1)}$
$\mathcal{A}(L)$	$\frac{2}{n+2}$	$\frac{2(n-2)}{n^2-n-1}$	$\frac{2}{7}$	$\frac{8}{31}$	$\frac{28}{119}$	$\frac{2(n-5)}{n^2+n-2}$
$s(L)$	$\frac{n(n+1)}{2}$	$n(n-1)$	36	63	120	$\frac{n(n+1)}{2}$

Table 1.1:

$$N = \begin{cases} \frac{n-3}{2} & \text{if } n \equiv 1 \bmod 4 \\ \frac{n-3}{4} & \text{if } n \equiv -1 \bmod 4 \end{cases} \quad \text{and} \quad D = \begin{cases} 2(\frac{n+1}{2})^{n-1} & \text{if } n \equiv 1 \bmod 4 \\ (\frac{n+1}{4})^{n-1} & \text{if } n \equiv -1 \bmod 4 \end{cases}$$

A_2, E_8, and Λ_{24}, the famous Leech lattice [17]). For detailed expositions of these and more, we refer the reader to [19] and [49].

1.4 Motivation and coherence

This course of study arose, as so many do, in response to a question about generalization of an observation. Notice that in the plane $\mathbb{R}^2$ the minimal packing density is attained by $\mathbb{Z}^2$ and the maximal packing density is attained by A_2. It is also the case that the lowest maximal coherence is attained by $\mathbb{Z}^2$ and highest maximal coherence is attained by A_2. This led to the following motivating question:

Question 1. *What connection does the packing density of a lattice have to its coherence?*

The answer to this question, at least with respect to maximal coherence, is "not a lot." It is possible to exhibit infinite families of extreme lattices with maximal coherence strictly less than $\frac{1}{2}$, and infinite families of lattices with coherence $\mathcal{C}(L) = \frac{1}{2}$ that are not extreme. For instance, the Coxeter lattices A_n^r are extreme with coherence

$C(A_n^r) < \frac{1}{2}$ for $n \geq 7$ odd and $r = \frac{n+1}{2}$. Further, any well-rounded nearly orthogonal lattice L in dimension $n \geq 3$ with $|S(L)| > 2n$ has coherence $\mathcal{C}(L) = \frac{1}{2}$ but is not extreme.

Nevertheless, there are good reasons to think harder about this question. Coherence of a lattice is, in some sense, a measure of the non-orthogonality of the set of minimal vectors of a lattice. Let us suppose that a lattice L possesses a basis of minimal vectors. This is not a trivial assumption; consider the following lattice:

Example 1. *Let* $\boldsymbol{x} = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$ *and* $\boldsymbol{e}_i$ *be the canonical basis vectors within* $\mathbb{R}^5$. *If* $B = (\boldsymbol{e}_1\ \boldsymbol{e}_2\ \boldsymbol{e}_3\ \boldsymbol{e}_4\ \boldsymbol{x})$, *then* $L = B\mathbb{Z}^5$ *does not possess a basis of minimal vectors.*

Remark 1.4.1. This construction is classical, and was certainly known by Minkowski. See also [18] and [50] for lattices generated by minimal vectors but not possessing a minimal basis.

However, assuming we have a minimal basis, then the *orthogonality defect* of that basis, $\nu(B)$, is directly proportional to the packing density of the lattice:

$$\nu(B) := \frac{\prod_{j=1}^{k} \|\boldsymbol{b}_j\|}{\det L} = \frac{|L|^k}{\det(L)} = \frac{2^k}{\omega_k}\delta(L)$$

Recall the root lattices A_n defined in section 1.3. While their coherence is $\mathcal{C}(A_n) = \frac{1}{2}$ for any n, they possess $\frac{n(n+1)}{2}$ pairs of minimal vectors. However, only $2(n-1)$ of these pairs are not mutually orthogonal. One would then expect a more accurate measure of their non-orthogonality to progress like $\frac{1}{n}$, and, indeed, its average coherence is

$$\mathcal{A}(A_n) = \frac{2}{n+2}.$$

CHAPTER II

Nearly orthogonal lattices

2.1 Introduction

Let L be a lattice of rank $n \geq 2$ in $\mathbb{R}^n$, and denote its *minimal norm* as

$$|L| = \min \{\|\boldsymbol{x}\| : \boldsymbol{x} \in L \setminus \{\mathbf{0}\}\},$$

where $\| \ \|$ is the Euclidean norm on $\mathbb{R}^n$. Then its set of *minimal vectors* is

$$S(L) = \{\boldsymbol{x} \in L : \|\boldsymbol{x}\| = |L|\}.$$

Recall that the *maximal coherence* of the lattice L is defined to be

$$\mathcal{C}(L) = \max \left\{ \frac{|(\boldsymbol{x}, \boldsymbol{y})|}{|L|^2} : \boldsymbol{x}, \boldsymbol{y} \in S(L), \boldsymbol{x} \neq \pm \boldsymbol{y} \right\},$$

where $(\ ,\ )$ stands for the usual scalar product of vectors. Notice that

$$0 \leq \mathcal{C}(L) \leq 1/2,$$

*This chapter is based on joint work with Lenny Fukshansky, published as [31]

since the angle between any two minimal vectors of a lattice is in the interval $[\pi/3, 2\pi/3]$ (see, for instance, Lemma 3.1 of [25]). The coherence of lattices was recently introduced in [35] by analogy with coherence of frames, an important notion in signal processing. Generally, one can think of coherence of a set of vectors as a measure of how far are they from being orthogonal. Various techniques in error-correcting coding and signal recovery employ overdetermined equal-norm spanning sets in Euclidean vector spaces that are as close to orthogonal as possible. Since lattices are frequently used in signal processing and digital communications, we want to better understand the coherence properties of such sets coming from minimal vectors of lattices.

A classical optimization problem studied on lattices is the sphere packing problem. Recall that there is a sphere packing associated with every lattice L, and it consists of spheres of radius $|L|/2$ centered at the points of L, whose density is the proportion of the space it occupies, which can be computed as

$$\delta(L) = \frac{\omega_n |L|^n}{2^n \det L},$$

where ω_n is the volume of a unit ball in $\mathbb{R}^n$. The space of lattices in $\mathbb{R}^n$ can be identified with $\mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z})$, i.e., nonsingular real $n \times n$ matrices modulo right multiplication by nonsingular integer $n \times n$ matrices, and δ is a continuous function on this space. Lattices that are local maxima of δ are called *extreme*. In [35] some heuristics were presented, speculating that there may be an inverse correlation between the maximal coherence and packing density on lattices. Our goal here is to investigate this correlation on the important class of nearly orthogonal lattices.

Recall that two lattices L_1, L_2 in $\mathbb{R}^n$ are called *similar* (written $L_1 \sim L_2$) if there exists a positive constant α and an $n \times n$ real orthogonal matrix U such that $L_2 = \alpha U L_1$. This is an equivalence relation on the space of lattices in $\mathbb{R}^n$ with equivalence classes referred to as *similarity classes* of lattices in $\mathbb{R}^n$. The space of similarity classes

of lattices in $\mathbb{R}^n$ can be identified with $(\mathbb{R}_+ \times \mathcal{O}_n(\mathbb{R})) \setminus \mathrm{GL}_n(\mathbb{R}) / \mathrm{GL}_n(\mathbb{Z})$, i.e., lattices modulo left multiplication by positive constants and orthogonal matrices. Metric topology on this space is induced by the usual Euclidean norm on the space of $n \times n$ real matrices viewed as vectors in $\mathbb{R}^{n^2}$. It is easy to notice that if $L_1 \sim L_2$, then $\delta(L_1) = \delta(L_2)$ and $\mathcal{C}(L_1) = \mathcal{C}(L_2)$. In particular, extreme lattices can only be similar to extreme lattices, and δ is a continuous function on the space of similarity classes of lattices in $\mathbb{R}^n$.

Recall that a lattice L is called *well-rounded* (WR) if

$$\mathrm{span}_{\mathbb{R}} S(L) = \mathrm{span}_{\mathbb{R}} L.$$

Because WR lattices can only be similar to WR lattices, we write WR_n for the space of similarity classes of WR lattices. It is a well-known fact that extreme lattices must be WR, which is why the study of the packing density function on the space of lattices is usually restricted to WR lattices. Detailed further information on lattices, their geometric properties, and packing density can be found in [49] and [19].

We focus on the important class of nearly orthogonal lattices as defined in [56]. These lattices appear to be useful in image processing, signal recovery, and related areas (see, for instance [56] and [13]). Let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be an ordered basis for a lattice L in $\mathbb{R}^n$, and define a sequence of angles $\theta_1, \ldots, \theta_{n-1}$ as follows: each θ_i is the angle between $\boldsymbol{b}_{i+1}$ and the subspace $\mathrm{span}_{\mathbb{R}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_i\}$. It is then clear that each $\theta_i \in [0, \pi/2]$. For a given value $\theta \in [0, \pi/2]$, we will say that B is a *weakly θ-orthogonal* basis if $\theta_i \geq \theta$ for each $1 \leq i \leq n-1$. A basis B is called *θ-orthogonal* if every ordering of it is weakly θ-orthogonal. Notice that if some lattice L has a (weakly) θ-orthogonal basis, then so does every lattice in its similarity class: we will call such lattices (weakly) θ-orthogonal. Let us then write $\mathrm{WO}_n(\theta)$ for the space of similarity classes of all weakly θ-orthogonal lattices, and $\mathrm{WO}_n^*(\theta)$ for the space of similarity classes of

all θ-orthogonal lattices in $\mathbb{R}^n$. We will also write simply WO_n (respectively, WO_n^*) for $\mathrm{WO}_n(\pi/3)$ (respectively, $\mathrm{WO}_n^*(\pi/3)$), which will be especially important to us; we will call lattices in WO_n (respectively, WO_n^*) *weakly nearly orthogonal* (respectively, *nearly orthogonal*) and refer to their corresponding (weakly) $\pi/3$-orthogonal bases as (weakly) nearly orthogonal bases. It is shown in [56] that if L has a weakly nearly orthogonal basis B, then B contains a minimal vector of L. As discussed in [56], not every lattice has a weakly nearly orthogonal basis. Let us define

$$\mathcal{W}_n(\theta) = \mathrm{WR}_n \cap \mathrm{WO}_n(\theta) \text{ and } \mathcal{W}_n^*(\theta) = \mathrm{WR}_n \cap \mathrm{WO}_n^*(\theta),$$

i.e., the set of similarity classes of WR lattices in $\mathbb{R}^n$ that have a (weakly) θ-orthogonal basis; we will write simply $\mathcal{W}_n$ for $\mathcal{W}_n(\pi/3)$ (respectively, $\mathcal{W}_n^*$ for $\mathcal{W}_n^*(\pi/3)$).

Each similarity class can be represented by a lattice with minimal norm 1: for the remainder of this chapter, we will always use such representatives. When we write $L \in \mathcal{W}_n(\theta)$, we will mean the similarity class of L where $|L| = 1$. Let us also write $\mathfrak{a}(\boldsymbol{x}, \boldsymbol{y})$ for the angle between the two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$. For a given basis B of a lattice L, we define

$$\begin{aligned} \mu(B) &:= \min\{|\cos \mathfrak{a}(\boldsymbol{b}_i, \boldsymbol{b}_j)| : 1 \le i \ne j \le n\}, \\ \nu(B) &:= \max\{|\cos \mathfrak{a}(\boldsymbol{b}_i, \boldsymbol{b}_j)| : 1 \le i \ne j \le n\}). \end{aligned} \tag{2.1}$$

In this chapter, we investigate geometric properties and packing density of WR nearly orthogonal lattices. To do so, we examine the minimal vectors of these lattices and the angles between them. Here is our first result in this direction.

Theorem 2.1.1. *Let $L \in \mathcal{W}_n^*$ with a nearly orthogonal basis $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$. Then $B \subseteq S(L)$, and so $\mu(B) \le \nu(B) \le \mathcal{C}(L)$. Let $\varepsilon > 0$ and let $\mathbb{B}_\varepsilon(L)$ be a ball of radius ε centered at L in the space of similarity classes of lattices in $\mathbb{R}^n$. The following statements are true:*

1. *If $\mu(B) < 1/2$, then there exists $L' \in \mathcal{W}_n^* \cap \mathbb{B}_\varepsilon(L)$ with nearly orthogonal basis*

B' such that $\mu(B') > \mu(B)$ and

$$\delta(L') = \frac{\sqrt{1-\mu(B)^2}}{\sqrt{1-\mu(B')^2}}\,\delta(L) > \delta(L).$$

2. *If $\nu(B) > 0$, then there exists $L'' \in \mathcal{W}_n^* \cap \mathbb{B}_\varepsilon(L)$ with nearly orthogonal basis B'' such that $\nu(B'') < \nu(B)$ and*

$$\delta(L'') = \frac{\sqrt{1-\nu(B)^2}}{\sqrt{1-\nu(B'')^2}}\,\delta(L) < \delta(L).$$

3. *If $n \geq 3$, then $\mu(B) < 1/2$ for every nearly orthogonal basis B of any lattice $L \in \mathcal{W}_n^*$. If $n = 2$, $\mu(B) = 1/2$ if and only if L is the hexagonal lattice, in which case this is true for any nearly orthogonal basis B of L.*

4. *$\mathcal{C}(L) = 0$ if and only if $L = \mathbb{Z}^n$.*

Loosely speaking, Theorem 2.1.1 asserts that a lattice $L \in \mathcal{W}_n^*$ can be locally modified to increase or decrease the packing density by respectively increasing or decreasing maximal coherence. We prove Theorem 2.1.1 in Section 2.2. Here is an immediate consequence of this theorem.

Corollary 2.1.2. *If $n \geq 3$, then $\mathcal{W}_n^*$ does not contain any extreme lattices. If $n = 2$, the hexagonal lattice is the unique extreme lattice, which is contained in $\mathcal{W}_2^*$. On the other hand, $\mathcal{W}_n^*$ for every $n \geq 2$ contains a unique minimum of the packing density function on the set of WR lattices, the integer lattice $\mathbb{Z}^n$.*

The fact that $\mathcal{W}_n(\theta)$ with $\theta > \pi/3$ cannot contain extreme lattices already follows from results of [56] in a different manner. Recall that a lattice L is called *weakly eutactic* if there exist real numbers $c_1, \ldots, c_n$, called *eutaxy coefficients*, such that

$$\|\boldsymbol{v}\|^2 = \sum_{\boldsymbol{x} \in S(L)} c_i(\boldsymbol{v}, \boldsymbol{x}_i)^2 \tag{2.2}$$

for all $\boldsymbol{v} \in \mathbb{R}^n$. If eutaxy coefficients are positive, L is called *eutactic*, and if $c_1 = \cdots = c_n > 0$, the lattice L is called *strongly eutactic*; for instance, the integer lattice $\mathbb{Z}^n$ is strongly eutactic. Further, L is *perfect* if the set $\{\boldsymbol{x}\boldsymbol{x}^\top : \boldsymbol{x} \in S(L)\}$ spans the space of $n \times n$ real symmetric matrices. Both eutactic and perfect lattices are necessarily WR, and eutaxy and perfection properties are preserved on similarity classes, as is well-roundedness. A famous theorem of Voronoi (1908, [66]) asserts that L is extreme if and only if L is eutactic and perfect. Notice that in order for L to be perfect $S(L)$ needs to contain at least $\frac{n(n+1)}{2}$ pairs of $\pm$ minimal vectors, the dimension of the space of $n \times n$ real symmetric matrices. On the other hand, if $L \in \mathcal{W}_n(\theta)$ with $\theta > \pi/3$ and B is its weakly θ-orthogonal basis, then Corollary 1 of [56] states that $S(L) = \pm B$. Hence L cannot be perfect, since $n < \frac{n(n+1)}{2}$ for all $n \geq 2$. This, however, does not imply our result for $\mathcal{W}_n^*$. Indeed, while we do prove that $B \subseteq S(L)$ for any nearly orthogonal basis B of any lattice $L \in \mathcal{W}_n^*$, it is possible to construct lattices in $\mathcal{W}_n^*$ with larger sets of minimal vectors.

Theorem 2.1.3. *Let $n \geq 2$. For each $0 \leq m \leq [n/2]$ there exists a strongly eutactic lattice $L_{n,m} \in \mathcal{W}_n^*$ with*

$$|S(L_{n,m})| = 2(n+m).$$

In particular, if $m = [n/2]$, then

$$|S(L_{n,m})| = \begin{cases} 3n & \text{if } n \text{ is even} \\ 3n-1 & \text{if } n \text{ is odd.} \end{cases}$$

Furthermore, for each even number k between $3n$ and $4n-2$, inclusive, there exists a lattice $L \in \mathcal{W}_n$ such that $|S(L)| = k$. On the other hand, $|S(L)| \leq 4n-2$ for every $L \in \mathcal{W}_n$, and if $|S(L)| > 3n$ then L cannot be in $\mathcal{W}_n^*$.

We prove Theorem 2.1.3 in Section 2.3, in particular constructing explicit families of lattices. Notice that the set $\mathcal{W}_n^*$ contains strongly eutactic lattices. Further, in Ex-

ample 4 we exhibit a 3-dimensional irreducible non-perfect eutactic (but not strongly eutactic) lattice, which is in $\mathcal{W}_3$, but not in $\mathcal{W}_3^*$. On the other hand, since perfect lattices must have at least $n(n+1)$ minimal vectors, Theorem 2.1.3 implies an immediate corollary.

Corollary 2.1.4. *For every $n \geq 3$, the set $\mathcal{W}_n$ does not contain any perfect lattices. Hence there are no extreme lattices in $\mathcal{W}_n$ for $n \geq 3$.*

There is another consequence of Theorem 2.1.3 that we want to record: we also prove it in Section 2.3. Clearly, lattices in $\mathcal{W}_n$ contain bases of minimal vectors. In fact, WR nearly orthogonal lattices satisfy a stronger property, which they have in common with such lattices as root lattices A_n, for instance.

Corollary 2.1.5. *Let $L \in \mathcal{W}_n^*$. Then any n linearly independent vectors from $S(L)$ form a basis for L.*

Let us now look at the coherence of WR nearly orthogonal lattices in more details. Define a dimensional constant

$$c_n = \frac{\sqrt{(n-2)^2 + 16(n-1)} - (n-2)}{8(n-1)}. \tag{2.3}$$

We prove the following result.

Theorem 2.1.6. *The following statements are true.*

1. *For a lattice $L \in \mathcal{W}_n^*$, $\mathcal{C}(L) = 1/2$ if and only if $|S(L)| > 2n$.*
2. *Let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ in $\mathbb{R}^n$ be a collection of linearly independent unit vectors such that*

$$\max_{1 \leq i < j \leq n} |(\boldsymbol{b}_i, \boldsymbol{b}_j)| \leq c_n.$$

Then $L = \operatorname{span}_{\mathbb{Z}} B$ is in $\mathcal{W}_n^*$.

We prove Theorem 2.1.6 in Section 2.4, where we also demonstrate a family of lattices A_n^* outside of $\mathcal{W}_n$ with maximal coherence $1/n$, which tends to $\mathcal{W}_n$ with respect to maximal coherence as $n \to \infty$ in the sense that $\lim_{n\to\infty}(c_n/(1/n)) = 1$. This shows that c_n is asymptotically sharp, so WR lattices with maximal coherence $< 1/n$ tend to be nearly orthogonal as $n \to \infty$. For comparison, Proposition 1.1 of [63] implies that the maximal coherence of the set of the first k shortest vectors of a random lattice in $\mathbb{R}^n$ (where k does not depend on n) tends to $O(1/\sqrt{n})$ as $n \to \infty$. In Section 2.4, we also prove a result in the spirit of Diophantine approximation about an infinite family of integral WR lattices in the plane with maximal coherence tending to 0. We are now ready to proceed.

2.2 Packing density

In this section we prove Theorem 2.1.1. We start with several auxiliary lemmas.

Lemma 2.2.1. *Let $\boldsymbol{b}_1, \boldsymbol{b}_2 \in \mathbb{R}^n$ be nonzero vectors with the angle $\pi/3 \le \theta_1 \le 2\pi/3$ between them. Then*

$$\min\{\|\alpha\boldsymbol{b}_1 + \beta\boldsymbol{b}_2\| : \alpha, \beta \in \mathbb{Z} \text{ not both } 0\} = \min\{\|\boldsymbol{b}_1\|, \|\boldsymbol{b}_2\|\}. \tag{2.4}$$

If $\|\boldsymbol{b}_1\| = \|\boldsymbol{b}_2\|$ and $\alpha, \beta \neq 0$, then $\|\alpha\boldsymbol{b}_1 + \beta\boldsymbol{b}_2\| = \|\boldsymbol{b}_1\|$ if and only if either $\theta_1 = \pi/3$ and the pair $(\alpha, \beta) = \pm(1, -1)$, or $\theta_1 = 2\pi/3$ and the pair $(\alpha, \beta) = \pm(1, 1)$.

Proof. Assume $\min\{\|\boldsymbol{b}_1\|, \|\boldsymbol{b}_2\|\} = \|\boldsymbol{b}_1\|$. Let $\boldsymbol{x} = \alpha\boldsymbol{b}_1 + \beta\boldsymbol{b}_2$ for some $\alpha, \beta \in \mathbb{Z}$, not both 0. If $\alpha = 0$ or $\beta = 0$, then we immediately have $\|\boldsymbol{x}\| \ge \|\boldsymbol{b}_1\|$. Suppose that

$\alpha, \beta \neq 0$, then

$$\begin{aligned} \|\boldsymbol{x}\|^2 &= \alpha^2\|\boldsymbol{b}_1\|^2 + 2\alpha\beta\|\boldsymbol{b}_1\|\|\boldsymbol{b}_2\|\cos\theta_1 + \beta^2\|\boldsymbol{b}_2\|^2 \\ &\geq \alpha^2\|\boldsymbol{b}_1\|^2 - |\alpha\beta|\|\boldsymbol{b}_1\|\|\boldsymbol{b}_2\| + \beta^2\|\boldsymbol{b}_2\|^2 \\ &= (|\alpha|\|\boldsymbol{b}_1\| - |\beta|\|\boldsymbol{b}_2\|)^2 + |\alpha\beta|\|\boldsymbol{b}_1\|\|\boldsymbol{b}_2\| \geq \|\boldsymbol{b}_1\|^2 \end{aligned} \tag{2.5}$$

and

$$\|\boldsymbol{x}\| = \|\boldsymbol{b}_1\| \iff \|\boldsymbol{b}_2\| = \|\boldsymbol{b}_1\|,\ \cos\theta_1 = \pm 1/2,\ \text{and}\ \alpha\beta = \pm 1. \tag{2.6}$$

This completes the proof. □

Lemma 2.2.2. *Let $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$ be nonzero non-coplanar vectors in $\mathbb{R}^n$, $n \geq 3$. Let θ_{ij} be the angle between $\boldsymbol{b}_i$ and $\boldsymbol{b}_j$, $1 \leq i \neq j \leq 3$, and let ξ be the angle between $\boldsymbol{z} = \boldsymbol{b}_1 + \boldsymbol{b}_2$ and $\boldsymbol{b}_3$. Suppose that*

$$\cos\theta_{13} = \cos\theta_{23} = \alpha > 0.$$

Then $|\cos\xi| > \alpha$, and hence $\boldsymbol{b}_3$ makes a smaller angle with the plane spanned by $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ than with each of them.

Proof. Notice that $\cos\xi = \frac{(\boldsymbol{z}, \boldsymbol{b}_3)}{\|\boldsymbol{z}\|\|\boldsymbol{b}_3\|}$, where

$$(\boldsymbol{z}, \boldsymbol{b}_3) = (\boldsymbol{b}_1, \boldsymbol{b}_3) + (\boldsymbol{b}_2, \boldsymbol{b}_3) = \alpha\|\boldsymbol{b}_3\|(\|\boldsymbol{b}_1\| + \|\boldsymbol{b}_2\|) > \alpha\|\boldsymbol{b}_3\|\|\boldsymbol{b}_1 + \boldsymbol{b}_2\|.$$

Further, the angle $\boldsymbol{b}_3$ makes with the plane spanned by $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ is $\leq \xi$, since the vector $\boldsymbol{z} = \boldsymbol{b}_1 + \boldsymbol{b}_2$ lies in that plane. The conclusion follows. □

Lemma 2.2.3. *Let $L \in \mathcal{W}_n$ and*

$$B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$$

be a weakly nearly orthogonal basis for L. Then for each $1 \leq k \leq n$, the lattice

$$L_k = \operatorname{span}_{\mathbb{Z}} \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_k\}$$

is also WR.

Proof. Arguing toward a contradiction, suppose this is not true. Since L is WR, there must exist some $1 < k < n$ such that L_k is not WR, but L_{k+1} is. This means that the number of linearly independent minimal vectors of L_k is $1 \leq m < k$; call these vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$. On the other hand, $L_k \subsetneq L_{k+1}$ and L_{k+1} must contain $k+1$ linearly independent minimal vectors. Now, every vector $\boldsymbol{y} \in L_{k+1}$ is of the form

$$\boldsymbol{y} = \alpha \boldsymbol{x} + \beta \boldsymbol{b}_{k+1}$$

for some $\boldsymbol{x} \in L_k$ and $\alpha, \beta \in \mathbb{Z}$. Then, by Lemma 2.2.1,

$$|L_{k+1}| = \min\{\|\boldsymbol{y}\| : \boldsymbol{y} \in L_{k+1} \setminus \{\boldsymbol{0}\}\} = \min\{|L_k|, \|\boldsymbol{b}_{k+1}\|\}.$$

Suppose first that $\|\boldsymbol{b}_{k+1}\| < |L_k|$. Then $\|\boldsymbol{y}\| = |L_{k+1}|$ if and only if $\boldsymbol{y} = \pm \boldsymbol{b}_{k+1}$: since $k+1 \geq 2$, this contradicts L_{k+1} being WR. Next assume that $|L_k| < \|\boldsymbol{b}_{k+1}\|$. Then $\|\boldsymbol{y}\| = |L_{k+1}|$ if and only if $\boldsymbol{y} \in S(L_k)$. However, there are only $m < k$ such linearly independent vectors, again contradicting L_{k+1} being WR. Hence the only remaining option is that

$$\|\boldsymbol{x}_1\| = \cdots = \|\boldsymbol{x}_m\| = \|\boldsymbol{b}_{k+1}\|.$$

In this case,

$$S(L_k) \cup \{\pm \boldsymbol{b}_{k+1}\} \subseteq S(L_{k+1}), \tag{2.7}$$

but only $m+1 < k+1$ of these vectors are linearly independent. Additionally, some vectors of the form $\boldsymbol{x} \pm \boldsymbol{b}_{k+1}$ for some $\boldsymbol{x} \in S(L_k)$ may be in $S(L_{k+1})$. However, they are

linearly dependent with the vectors in (2.7). This means that the number of linearly independent vectors in $S(L_{k+1})$ is $\leq m+1 < k+1$, contradicting the assumption that L_{k+1} is WR. Hence every L_k must be WR, and this completes the proof. $\square$

Lemma 2.2.4. *Let $L \in \mathcal{W}_n^*$ and B a nearly orthogonal basis for L. Then $B \subseteq S(L)$.*

Proof. First suppose that B is weakly θ-orthogonal, where $\theta > \pi/3$. Then Corollary 1 of [56] guarantees that $S(L) = \pm B$. Assume then that for some $1 \leq i \leq n-1$, the angle θ_i between $\boldsymbol{b}_i$ and subspace spanned by $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}$ is equal to $\pi/3$.

We argue by induction on $n \geq 2$. If $n = 2$, let $\boldsymbol{b}_1, \boldsymbol{b}_2$ be a nearly orthogonal basis for L; assume $\|\boldsymbol{b}_1\| \leq \|\boldsymbol{b}_2\|$. Then Theorem 1 of [56] guarantees that $|L| = \|\boldsymbol{b}_1\|$. Let $\theta_1 = \pi/3$ be the angle between $\boldsymbol{b}_1, \boldsymbol{b}_2$. Since L is WR, there must exist some

$$\boldsymbol{x} = \alpha \boldsymbol{b}_1 + \beta \boldsymbol{b}_2 \in L$$

such that $\beta \neq 0$ and $\|\boldsymbol{x}\| = \|\boldsymbol{b}_1\|$. If $\alpha = 0$, then $\boldsymbol{x} = \beta \boldsymbol{b}_2$, and so we must have $\beta = \pm 1$ and $\|\boldsymbol{b}_2\| = \|\boldsymbol{b}_1\|$. If $\alpha \neq 0$, then $\|\boldsymbol{b}_2\| = \|\boldsymbol{b}_1\|$ by (2.5) and (2.6) above. In either case, $\boldsymbol{b}_1, \boldsymbol{b}_2 \in S(L)$.

Next assume the lemma is true in all dimensions $\leq n-1$. Let us prove it for dimension n. Let

$$B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}, \boldsymbol{b}_n\}$$

be a nearly orthogonal basis for a lattice $L \in \mathcal{W}_n^*$. Theorem 1 of [56] guarantees that at least one of these basis vectors is a shortest vector for L, and we can assume that B is ordered so that it is $\boldsymbol{b}_1$. Let $L_{n-1} = \text{span}_{\mathbb{Z}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}\}$; then Lemma 2.2.3 implies that $L_{n-1} \in \mathcal{W}_{n-1}^*$ and

$$|L_{n-1}| = \|\boldsymbol{b}_1\| = |L|, \tag{2.8}$$

and $\|\boldsymbol{b}_n\| \geq |L|$. We should remark that when we write $\mathcal{W}_{n-1}^*$ here (and below),

we are identifying $\mathbb{R}^{n-1}$ with $\operatorname{span}_{\mathbb{R}} L_{n-1}$. By the induction hypothesis, we have $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1} \in S(L_{n-1}) \subseteq S(L)$. Hence we only need to prove that $\boldsymbol{b}_n \in S(L)$. Since L is WR, there must exist some $\boldsymbol{y} \in S(L) \setminus L_{n-1}$. Again, $L = \operatorname{span}_{\mathbb{Z}}\{L_{n-1}, \boldsymbol{b}_n\}$, so

$$\boldsymbol{y} = \alpha \boldsymbol{x} + \beta \boldsymbol{b}_n$$

for some $\boldsymbol{x} \in L_{n-1}$ and $\alpha, \beta \in \mathbb{Z}$ with $\beta \neq 0$. By Lemma 2.2.1,

$$|L| = \|\boldsymbol{y}\| = \min\{|L_{n-1}|, \|\boldsymbol{b}_n\|\}.$$

Combining this observation with (2.8) we have, in particular

$$\min\{\|\alpha \boldsymbol{b}_1 + \beta \boldsymbol{b}_n\| : \alpha, \beta \in \mathbb{Z},\ \beta \neq 0\} = \|\boldsymbol{b}_1\|,$$

while $\|\boldsymbol{b}_n\| \geq \|\boldsymbol{b}_1\|$ and the angle between $\boldsymbol{b}_1$ and $\boldsymbol{b}_n$ is in the interval $[\pi/3, 2\pi/3]$. Then (2.5) and (2.6) imply that $\boldsymbol{b}_n \in S(L)$, and we are done. □

We are now ready to prove the theorem.

Proof of Theorem 2.1.1. First notice that, by Lemma 2.2.4, $B \subseteq S(L)$. To prove parts (1) and (2) of the theorem, we argue by induction on $n \geq 2$. First suppose that $n = 2$. Let $L \in \mathcal{W}_2^*$ and let $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2\}$ be a nearly orthogonal basis for L. In this case $\mu(B) = \nu(B) = \mathcal{C}(L)$, and assume that $0 < \mathcal{C}(L) < 1/2$. Then

$$L = \operatorname{span}_{\mathbb{Z}} \{\boldsymbol{b}_1, \boldsymbol{b}_2\}$$

with $|L| = \|\boldsymbol{b}_1\| = \|\boldsymbol{b}_2\| = 1$ and the angle θ_1 between $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ lies in the interval $(\pi/3, \pi/2)$. The packing density of L is

$$\delta(L) = \frac{\pi |L|^2}{\det L} = \frac{\pi}{\sin \theta_1}.$$

Let us write $U(\theta_1)$ for the counterclockwise rotation matrix by the angle θ_1:

$$U(\theta_1) = \begin{pmatrix} \cos\theta_1 & -\sin\theta_1 \\ \sin\theta_1 & \cos\theta_1 \end{pmatrix}.$$

Without loss of generality, we can assume that $\boldsymbol{b}_2 = U(\theta_1)\boldsymbol{b}_1$. For a given $\varepsilon > 0$, let $\theta_1' \in [\pi/3, \theta_1)$ and $\theta_1'' \in (\theta_1, \pi/2]$ be such that

$$\begin{aligned} (\sin\theta_1 - \sin\theta_1')^2 + (\cos\theta_1 - \cos\theta_1')^2 < \varepsilon, \\ (\sin\theta_1 - \sin\theta_1'')^2 + (\cos\theta_1 - \cos\theta_1'')^2 < \varepsilon. \end{aligned} \tag{2.9}$$

Then the lattices

$$L' = \mathrm{span}_{\mathbb{Z}}\left\{\boldsymbol{b}_1, U(\theta_1')\boldsymbol{b}_1\right\},\ L'' = \mathrm{span}_{\mathbb{Z}}\left\{\boldsymbol{b}_1, U(\theta_1'')\boldsymbol{b}_1\right\}$$

with nearly orthogonal bases $B' = \{\boldsymbol{b}_1, U(\theta_1')\boldsymbol{b}_1\}$, $B'' = \{\boldsymbol{b}_1, U(\theta_1'')\boldsymbol{b}_1\}$, respectively, are in $\mathcal{W}_2^* \cap \mathbb{B}_\varepsilon(L)$,

$$1/2 \geq \mu(B') > \mu(B) = \nu(B) > \nu(B'') \geq 0,$$

and

$$\begin{aligned} \delta(L') &= \frac{\pi}{\sin\theta_1'} = \frac{\pi}{\sqrt{1-\mu(B')^2}} > \frac{\pi}{\sqrt{1-\mu(B)^2}} = \frac{\pi}{\sin\theta_1} = \delta(L), \\ \delta(L'') &= \frac{\pi}{\sin\theta_1''} = \frac{\pi}{\sqrt{1-\nu(B'')^2}} < \frac{\pi}{\sqrt{1-\nu(B)^2}} = \frac{\pi}{\sin\theta_1} = \delta(L). \end{aligned}$$

Hence

$$\delta(L') = \frac{\sqrt{1-\mu(B)^2}}{\sqrt{1-\mu(B')^2}}\,\delta(L),\ \delta(L'') = \frac{\sqrt{1-\nu(B)^2}}{\sqrt{1-\nu(B'')^2}}\,\delta(L).$$

Now suppose the statement is true in any dimension $\leq n-1$. Let us prove it for n. We start with part (1), so let $L \in \mathcal{W}_n^*$ and let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be a nearly orthogonal basis for L so that $\mu(B) < 1/2$. Then $B \subseteq S(L)$ by Lemma 2.2.4. Let

$L_{n-1} = \operatorname{span}_{\mathbb{Z}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}\}$, then by Lemmas 2.2.3 and 2.2.4, $L_{n-1} \in \mathcal{W}_{n-1}^*$ and $B_{n-1} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}\} \subseteq S(L_{n-1})$. Further, since we can reorder B as we like, we can assume that $\mu(B_{n-1}) = \mu(B) < 1/2$, and thus we can apply induction hypothesis to L_{n-1}. Then there exists $L'_{n-1} \in \mathcal{W}_{n-1}^* \cap \mathbb{B}_\varepsilon(L_{n-1})$ with the nearly orthogonal basis $B'_{n-1} = \{\boldsymbol{b}'_1, \ldots, \boldsymbol{b}'_{n-1}\}$ such that

$$\mu(B'_{n-1}) > \mu(B_{n-1}),\ \delta(L'_{n-1}) = \frac{\sqrt{1-\mu(B_{n-1})^2}}{\sqrt{1-\mu(B'_{n-1})^2}}\,\delta(L_{n-1}).$$

Since we agreed to pick representatives of similarity classes that have minimal norm 1, we have

$$|L'_{n-1}| = \|\boldsymbol{b}'_1\| = \cdots = \|\boldsymbol{b}'_{n-1}\| = |L_{n-1}| = |\boldsymbol{b}_n\| = |L| = 1,$$

by Lemma 2.2.4. Now, let $L' = \operatorname{span}_{\mathbb{Z}}\{L'_{n-1}, \boldsymbol{b}_n\}$. Since $L'_{n-1} \subset \operatorname{span}_{\mathbb{R}} L_{n-1}$, $\boldsymbol{b}_n$ makes the same angle θ_{n-1} with $\operatorname{span}_{\mathbb{R}}\{\boldsymbol{b}'_1, \ldots, \boldsymbol{b}'_{n-1}\}$ and with $\operatorname{span}_{\mathbb{R}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}\}$, and so $L' \in \mathcal{W}_n^*$ with near orthogonal basis $B' = \{\boldsymbol{b}'_1, \ldots, \boldsymbol{b}'_{n-1}, \boldsymbol{b}_n\}$ and $|L'| = |L|$,

$$\mu(B') = \mu(B'_{n-1}) > \mu(B_{n-1}) = \mu(B),$$

and so $\delta(L') = \frac{\sqrt{1-\mu(B)^2}}{\sqrt{1-\mu(B')^2}}\,\delta(L)$, since

$$\det L' = (\det L'_{n-1})\|\boldsymbol{b}_n\| \sin\theta_{n-1},\ \det L' = (\det L_{n-1})\|\boldsymbol{b}_n\| \sin\theta_{n-1}.$$

This completes the proof of (1). The proof of (2) is completely analogous with μ replaced by ν and the corresponding inequalities reversed.

To prove part (3), assume $n \geq 3$ and suppose $\mu(B) = 1/2$ for some $L \in \mathcal{W}_n^*$ with a nearly orthogonal basis $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$. This means that all the angles between these basis vectors are equal to $\pi/3$ or $2\pi/3$. In particular, $\boldsymbol{b}_3$ makes such an angle with $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$. But then Lemma 2.2.2 implies that $\boldsymbol{b}_3$ makes an angle $< \pi/3$ with the plane spanned by $\boldsymbol{b}_1, \boldsymbol{b}_2$, contradicting near-orthogonality of the basis B. Therefore

we must have $\mu(B) < 1/2$ when $n \geq 3$. On the other hand, if $n = 2$ and $L \in \mathcal{W}_2^*$, then for any nearly orthogonal basis B, $\mu(B) \leq \mathcal{C}(L)$ is simply the cosine of the angle between the minimal basis vectors, which is in the interval $[\pi/3, \pi/2]$ and is equal to $\pi/3$ precisely in the case of the hexagonal lattice $\begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix} \mathbb{Z}^2$.

Finally, for part (4) notice that $\mathcal{C}(L) = 0$ if and only if all the angles between minimal vectors are equal to $\pi/2$, which happens precisely in the case of the integer lattice $\mathbb{Z}^n$. □

2.3 Minimal vectors

In this section we construct families of latices in $\mathcal{W}_n$ with many minimal vectors, but also prove that for any $L \in \mathcal{W}_n$, $|S(L)| \leq 4n - 2$. This will establish Theorem 2.1.3. We begin with two constructions. We write A_2 for the 2-dimensional root lattice (isometric to the hexagonal lattice), normalized to have minimal norm 1. We also write $\oplus$ for the orthogonal direct sum of lattices.

Lemma 2.3.1. *Let $n \geq 2$. For each $0 \leq m \leq n/2$, let*

$$L_{n,m} = \bigoplus_{i=1}^{m} A_2 \bigoplus_{j=1}^{n-2m} \mathbb{Z}, \tag{2.10}$$

where a direct sum is taken to be empty if the upper limit on the index is 0. This is a strongly eutactic lattice contained in $\mathcal{W}_n^*$ with

$$|S(L_{n,m})| = 2m + 2n.$$

If we take $m = [n/2]$, we have

$$|S(L_{n,m})| = \begin{cases} 3n & \text{if } n \text{ is even} \\ 3n-1 & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} \subset \mathbb{R}^n$ be a basis of unit vectors satisfying the following condition:

$$\begin{gathered} \forall\ 1 \le i \le n\ \exists \text{ at most one } 1 \le t \le n \text{ such that:} \\ (\boldsymbol{b}_i, \boldsymbol{b}_t) = 1/2 \text{ and } \forall\ 1 \le k \le n, k \ne i, t,\ (\boldsymbol{b}_i, \boldsymbol{b}_k) = 0. \end{gathered} \tag{2.11}$$

Notice that such a basis is nearly orthogonal. Indeed, let $1 \le i \le n$ and let V be a subspace of $\mathbb{R}^n$ spanned by some of the other vectors of B, say

$$V = \operatorname{span}_{\mathbb{R}}\{\boldsymbol{b}_{j_1}, \ldots, \boldsymbol{b}_{j_m} : 1 \le j_1, \ldots, j_m \le n, j_k \ne i\ \forall\ k = 1, \ldots, m\}.$$

Let

$$\boldsymbol{x} = \sum_{k=1}^{m} a_k \boldsymbol{b}_{j_k} \in V$$

be a unit vector for some real coefficients $-1 \le a_1, \ldots, a_m \le 1$. Since $\boldsymbol{b}_i$ is orthogonal to every other vector of B except for (possibly) $\boldsymbol{b}_t$ and $(\boldsymbol{b}_i, \boldsymbol{b}_t) = 1/2$, we have $|(\boldsymbol{x}, \boldsymbol{b}_i)| \le 1/2$. Thus $\boldsymbol{b}_i$ makes an angle $\ge \pi/3$ with each such subspace V. Thus if $L = \operatorname{span}_{\mathbb{Z}} B$, then $L \in \mathcal{W}_n^*$.

Now, let $0 \le m \le n/2$ and let $L_{n,m}$ be as in (2.10). Then $L_{n,m}$ is spanned over $\mathbb{Z}$ by a unit basis

$$\boldsymbol{b}_{11}, \boldsymbol{b}_{12}, \ldots, \boldsymbol{b}_{m1}, \boldsymbol{b}_{m2}, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{n-2m},$$

where each pair $\boldsymbol{b}_{i1}, \boldsymbol{b}_{i2}$ spans a copy of A_2 and hence has inner product $1/2$, $\boldsymbol{c}_j$'s span $\mathbb{Z}^{n-2m}$, and hence are orthogonal to each other, and each pair $\boldsymbol{b}_{i1}, \boldsymbol{b}_{i2}$ is orthog-

onal to every other pair and to all $\boldsymbol{c}_j$'s. Hence this basis satisfies condition (2.11), therefore $L_{n,m} \in \mathcal{W}_n^*$.

Let us count the number of minimal vectors in $L_{n,m}$. Notice that each of the m copies of A_2 in the orthogonal direct sum contributes 6 minimal vectors:

$$\pm\boldsymbol{b}_{i1}, \pm\boldsymbol{b}_{i2}, \pm(\boldsymbol{b}_{i1} - \boldsymbol{b}_{i2}),$$

and each of the $n - 2m$ copies of $\mathbb{Z}$ contributes two minimal vectors: $\pm\boldsymbol{c}_j$. There are no other minimal vectors. Hence we have

$$|S(L_{m,n})| = 6m + 2(n - 2m) = 2m + 2n.$$

Finally notice that $L_{n,m}$ is an orthogonal direct sum of strongly eutactic lattices with equal minimal norm. Therefore it is strongly eutactic by Theorem 3.6.13 of [49]. This completes the proof of the lemma. □

Lemma 2.3.2. *For every $n \geq 2$ there exist $L \in \mathcal{W}_n$ such that $|S(L)| \geq 4n - 2$.*

Proof. To prove this lemma, we demonstrate another construction. Let $\boldsymbol{b}_1, \boldsymbol{b}_2 \in \mathbb{R}^n$ be unit vectors with angle $\pi/3$ between them, and let Π_1 be the plane spanned by them. Then $\boldsymbol{b}_1 - \boldsymbol{b}_2$ is also a unit vector in Π_1 by Lemma 2.2.1. Let $\boldsymbol{b}_3$ be a unit vector in $\mathbb{R}^n$ making an angle $\pi/3$ with Π_1 and with $\boldsymbol{b}_1 - \boldsymbol{b}_2$, i.e., the orthogonal projection of $\boldsymbol{b}_3$ onto Π_1 is along the line spanned by $\boldsymbol{b}_1 - \boldsymbol{b}_2$. Then $\boldsymbol{b}_1 - \boldsymbol{b}_2 - \boldsymbol{b}_3$ is also a unit vector. Let $\boldsymbol{b}_4$ be a unit vector in $\mathbb{R}^n$ making an angle of $\pi/3$ with $\boldsymbol{b}_1 - \boldsymbol{b}_2 - \boldsymbol{b}_3$ and with the 3-dimensional subspace spanned by $\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3$. Once again, $\boldsymbol{b}_1 - \boldsymbol{b}_2 - \boldsymbol{b}_3 - \boldsymbol{b}_4$ is also a unit vector. Continuing in the same manner, we construct a basis $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ and take $L = \operatorname{span}_{\mathbb{Z}} B$. Then $L \in \mathcal{W}_n$ by construction. Further, for $n \geq 2$ the vectors

$$\pm\boldsymbol{b}_k \ \forall\ 1 \leq k \leq n, \ \pm\left(\boldsymbol{b}_1 - \sum_{i=2}^{k} \boldsymbol{b}_i\right) \ \forall\ 2 \leq k \leq n$$

are contained in $S(L)$. The number of these vectors is $4n-2$. $\square$

Example 2. *Let us show examples of our constructions in the proofs of Lemmas 2.3.1 and 2.3.2 above for $n = 3, 4$. For an example of the first construction when $n = 3$, we can take*

$$L_1 = \mathrm{span}_{\mathbb{Z}} \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{3}} \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} \right\},$$

which is a lattice in $\mathcal{W}_3^*$ with 8 minimal vectors. For $n = 4$, take

$$L_2 = \mathrm{span}_{\mathbb{Z}} \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} \right\},$$

which is a lattice in $\mathcal{W}_4^*$ with 12 minimal vectors. The presented bases for these lattices satisfy (2.11).

Here is also a 3-dimensional example of the second construction:

$$L_3 = \mathrm{span}_{\mathbb{Z}} \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{2} \\ 1-\sqrt{2} \\ -(1+\sqrt{2}) \end{pmatrix} \right\}.$$

This is a lattice in $\mathcal{W}_3$ with 10 minimal vectors, however it is not in $\mathcal{W}_3^*$, since the ordering of the minimal basis

$$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{2} \\ 1-\sqrt{2} \\ -(1+\sqrt{2}) \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

is not weakly nearly orthogonal: indeed, the cosine of the angle between the plane spanned by the first two of these vectors and the third one is $\sqrt{2/5} > 1/2$. *In fact, since every* 3*-dimensional lattice constructed as in the proof of Lemma 2.3.2 is isometric to* L_3*, all of them would be in* $\mathcal{W}_3$*, but not in* $\mathcal{W}_3^*$. *Furthermore, this implies that construction of Lemma 2.3.2 never produces lattices in* $\mathcal{W}_n^*$ *for* $n \geq 3$*: just reorder the first three vectors as in the example* L_3.

Remark 2.3.1. It is perhaps worth noting that the property of being nearly orthogonal is not preserved under the tensor product. Consider the examples above: if $L = L_1 \otimes L_2$, then $L \notin \mathcal{W}_{12}^*$. Writing $L_1 = \text{span}_{\mathbb{Z}} \{\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3\}$ and $L_2 = \text{span}_{\mathbb{Z}} \{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_4\}$, and denoting by $\boldsymbol{a}_i \otimes \boldsymbol{b}_j$ the concatenation of successive columns of the matrix $\boldsymbol{a}_i \boldsymbol{b}_j^\top$, we find the subspace $\text{span}_{\mathbb{R}} \{\boldsymbol{a}_1 \otimes \boldsymbol{b}_1, \boldsymbol{a}_1 \otimes \boldsymbol{b}_2, \boldsymbol{a}_1 \otimes \boldsymbol{b}_3, \boldsymbol{a}_1 \otimes \boldsymbol{b}_4, \boldsymbol{a}_2 \otimes \boldsymbol{b}_1\}$ forms an angle of $\arcsin(\frac{3}{4}) < \frac{\pi}{3}$ with $\boldsymbol{a}_2 \otimes \boldsymbol{b}_2$, and thus $L \notin \mathcal{W}_{12}^*$.

Lemma 2.3.3. *For any* $L \in \mathcal{W}_n$, $|S(L)| \leq 4n - 2$.

Proof. We argue by induction on n. If $n = 2$, the hexagonal lattice has largest set of minimal vectors, which has cardinality $6 = 4 \times 2 - 2$. Now assume the statement is true in all dimensions $\leq n - 1$. We prove it in dimension $n > 2$. Let $L \in \mathcal{W}_n$, and let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be a weakly nearly orthogonal basis for L. Then the lattice $L' = \text{span}_{\mathbb{Z}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-1}\} \in \mathcal{W}_{n-1}$ by Lemma 2.2.3, and hence has at most $4(n-1)-2 = 4n-6$ minimal vectors by induction hypothesis. Suppose that $\boldsymbol{y} \in S(L)$ is not contained in L'. Then either $\boldsymbol{y} = \boldsymbol{b}_n$ or

$$\boldsymbol{y} = \alpha \boldsymbol{x} + \beta \boldsymbol{b}_n$$

for some $\boldsymbol{x} \in L'$, $\beta \neq 0$, and

$$\|\boldsymbol{y}\| = |L'| = |L| = \|\boldsymbol{b}_n\|.$$

If $\boldsymbol{y} \neq \boldsymbol{b}_n$, Lemma 2.2.1 implies that $\|\boldsymbol{x}\| = \|\boldsymbol{b}_n\|$ and the angle between $\boldsymbol{x}$ and $\boldsymbol{b}_n$ is $\pi/3$. By Lemma 2.2.2, there can exist no more than one vector in L' with which $\boldsymbol{b}_n$ makes an angle $\pi/3$: otherwise it would make an angle $< \pi/3$ with the subspace $\mathrm{span}_{\mathbb{R}} L'$. Hence the total number of minimal vectors of L which are outside of L' is no greater than 4, and so

$$|S(L)| \leq |S(L')| + 4 \leq 4n - 2.$$

□

Corollary 2.3.4. *For every $n \geq 3$ and $m \geq 1$ such that*

$$m \leq \begin{cases} \frac{n-2}{2} & \text{if } n \text{ is even} \\ \frac{n-1}{2} & \text{if } n \text{ is odd,} \end{cases} \tag{2.12}$$

there exist $L \in \mathcal{W}_n$ such that

$$|S(L)| = \begin{cases} 3n + 2m & \text{if } n \text{ is even} \\ 3n - 1 + 2m & \text{if } n \text{ is odd.} \end{cases} \tag{2.13}$$

Proof. We argue by induction on $n \geq 3$. If $n = 3$, we must have $m = 1$, and so

$$3n - 1 + 2m = 9 - 1 + 2 = 10 = 4n - 2.$$

If $n = 4$, again we have $m = 1$, so

$$3n + 2m = 12 + 2 = 14 = 4n - 2.$$

Hence the existence of such a lattice L in $\mathcal{W}_3$ or $\mathcal{W}_4$ follows directly from Lemma 2.3.2. Assume then that $n > 4$, and the result holds in all dimensions $\leq n - 1$. Let us prove

it for n. First notice that if there is equality in (2.12), then the result again follows from Lemma 2.3.2. Hence let us assume that m is strictly less than the right hand side of (2.12), that is

$$m \leq \begin{cases} \frac{n-4}{2} = \frac{(n-2)-2}{2} & \text{if } n-2 \text{ is even} \\ \frac{n-3}{2} = \frac{(n-2)-1}{2} & \text{if } n-2 \text{ is odd.} \end{cases}$$

By the induction hypothesis, there must exist $L' \in \mathcal{W}_{n-2}$ with

$$|S(L')| = \begin{cases} 3(n-2)+2m & \text{if } n-2 \text{ is even} \\ 3(n-2)-1+2m & \text{if } n-2 \text{ is odd.} \end{cases}$$

Let us embed L' into the $(n-2)$-dimensional coordinate subspace in $\mathbb{R}^n$ corresponding to the last two coordinates being 0 and let V be the orthogonal complement of this subspace in $\mathbb{R}^n$. Let L'' be a lattice of unit minimal norm in V, similar to A_2, i.e., spanned by a pair of unit vectors $\boldsymbol{c}_1, \boldsymbol{c}_2$ with angle $\pi/3$ between them. Then $S(L'') = \{\pm\boldsymbol{c}_1, \pm\boldsymbol{c}_2, \pm(\boldsymbol{c}_1 - \boldsymbol{c}_2)\}$. Now, let $L = L' \oplus L''$. Then $S(L) = S(L') \cup S(L'')$, and so $|S(L)| = |S(L')| + 6$. This establishes (2.13). □

Example 3. *Here we present an explicit construction of the first case where there exists a lattice between the two extreme ends of Lemmas 2.3.1 and 2.3.2 (when $n = 5$). First, we construct a 4-dimensional lattice $L_4 \in \mathcal{W}_4$ with $|S(L)| = 14$ by following the procedure in Lemma 2.3.2. This gives*

$$L_4 = \text{span}_{\mathbb{Z}} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 \\ \sqrt{3} \\ 0 \\ 0 \end{pmatrix}, \frac{1}{4}\begin{pmatrix} 1 \\ -\sqrt{3} \\ 2\sqrt{3} \\ 0 \end{pmatrix}, \frac{1}{8}\begin{pmatrix} 1 \\ -\sqrt{3} \\ -2\sqrt{3} \\ 4\sqrt{3} \end{pmatrix} \right\}.$$

Then, to produce a 5-dimensional lattice $L_5 \in \mathcal{W}_5$ with $|S(L)| = 16 = 3n + 1$, we

need simply to add a copy of $\mathbb{Z}$ *orthogonal to the subspace of* $\mathbb{R}^5$ *spanned by the basis of* L_4*. This gives us*

$$L_5 = \mathrm{span}_{\mathbb{Z}} \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \frac{1}{2} \begin{pmatrix} 1 \\ \sqrt{3} \\ 0 \\ 0 \\ 0 \end{pmatrix}, \frac{1}{4} \begin{pmatrix} 1 \\ -\sqrt{3} \\ 2\sqrt{3} \\ 0 \\ 0 \end{pmatrix}, \frac{1}{8} \begin{pmatrix} 1 \\ -\sqrt{3} \\ -2\sqrt{3} \\ 4\sqrt{3} \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

By the same argument as at the end of Example 2, lattices produced using Corollary 2.3.4 are again in $\mathcal{W}_n$*, but not in* $\mathcal{W}_n^*$*, since they still follow the construction of Lemma 2.3.2.*

The strongly eutactic lattices constructed in Lemma 2.3.1 are orthogonal direct sums of copies of A_2 and $\mathbb{Z}$, which is not so surprising. It is more interesting that $\mathcal{W}_n$ can contain irreducible eutactic lattices which are also not in $\mathcal{W}_n^*$; we now demonstrate such an example for $n = 3$.

Example 4. *Let us consider eutactic lattices in dimensions* 2 *and* 3*. In* $\mathbb{R}^2$*, there are only two eutactic lattices:* $\mathbb{Z}^2$ *and* A_2*, and both of them are in* $\mathcal{W}_2^*$ *by Lemma 2.3.1. In dimension* 3*, there are five eutactic lattices:* $\mathbb{Z}^3$*,* $A_2 \perp \mathbb{Z}$*,* A_3*,* A_3^* *and* K_3' *(see Example 9.5.1 (6) on p. 345 of [49]). The lattices* $\mathbb{Z}^3$ *and* $A_2 \perp \mathbb{Z}$ *are in* $\mathcal{W}_3^*$ *by Lemma 2.3.1. The root lattice* A_3 *has* 12 *minimal vectors, and hence is not in* $\mathcal{W}_3$ *by Theorem 2.1.3. The lattice* A_3^* *is also not in* $\mathcal{W}_3$ *(see Example 5 below). The one remaining lattice is* K_3' *(see Section 8.5 of [49] for its construction), which is spanned by a unit basis*

$$\boldsymbol{b}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ \boldsymbol{b}_2 = \begin{pmatrix} -1/2 \\ \sqrt{3}/2 \\ 0 \end{pmatrix}, \ \boldsymbol{b}_3 = \begin{pmatrix} -1/2 \\ 0 \\ \sqrt{3}/2 \end{pmatrix}.$$

This lattice has 10 *minimal vectors:* $\pm\boldsymbol{b}_i$ *for* $1 \leq i \leq 3$, $\pm(\boldsymbol{b}_1 + \boldsymbol{b}_2)$, $\pm(\boldsymbol{b}_1 + \boldsymbol{b}_3)$. *It is irreducible, eutactic, but not perfect, and not strongly eutactic. We will show that* $K_3' \in \mathcal{W}_3$, *but* $K_3' \notin \mathcal{W}_3^*$. *Indeed, let* θ_{ij} *be the angle between* $\boldsymbol{b}_i$ *and* $\boldsymbol{b}_j$, $1 \leq i < j \leq 3$. *Also define*

$$\Pi_1 = \mathrm{span}_{\mathbb{R}}\{\boldsymbol{b}_1, \boldsymbol{b}_2\},\ \Pi_2 = \mathrm{span}_{\mathbb{R}}\{\boldsymbol{b}_2, \boldsymbol{b}_3\},$$

and let ν_1 *be the angle between* $\boldsymbol{b}_3$ *and* Π_1, ν_2 *the angle between* $\boldsymbol{b}_1$ *and* Π_2. *It is then easy to check that*

$$|\cos\theta_{12}| = |\cos\theta_{13}| = \frac{1}{2},\ |\cos\theta_{23}| = \frac{1}{4}.$$

Also, $|\cos\nu_1| = \frac{1}{2}$, *and hence* $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \boldsymbol{b}_3\}$ *is a weakly nearly orthogonal basis, so* $K_3' \in \mathcal{W}_3$. *On the other hand, let*

$$\boldsymbol{x} = \frac{1}{2}(\boldsymbol{b}_2 + \boldsymbol{b}_3) = \begin{pmatrix} -1/2 \\ \sqrt{3}/4 \\ \sqrt{3}/4 \end{pmatrix} \in \Pi_2,$$

and let μ *be the angle between* $\boldsymbol{b}_1$ *and* $\boldsymbol{x}$. *Notice that*

$$|\cos\nu_2| \geq |\cos\mu| = \sqrt{\frac{2}{5}} > \frac{1}{2}.$$

This means that the ordering of the basis $\{\boldsymbol{b}_2, \boldsymbol{b}_3, \boldsymbol{b}_1\}$ *is not weakly nearly orthogonal, and hence* $K_3' \notin \mathcal{W}_3^*$. *Notice also that* K_3' *is not similar to the lattice* L_3 *in Example 2.*

Remark 2.3.2. A theorem of A. Ash [1] (see also [2]) asserts that all the critical points of the packing density function δ occur at eutactic lattices. By Voronoi's theorem, we know that these are maxima if and only if the corresponding eutactic lattice is also perfect. Non-perfect eutactic lattices may or may not be minima: combining our observations on eutactic lattices in $\mathcal{W}_n$ with our Theorem 2.1.1, we see that many of

them are not minima, not even among well-rounded lattices. On the other hand, two lattices L_1 and L_2 are said to be in the same *minimal class* if there exists $U \in \mathrm{GL}_n(\mathbb{R})$ such that $L_2 = UL_1$ and $S(L_2) = US(L_1)$. Theorem 9.4.1 of [49] asserts that δ attains its minimum on a given minimal class at a weakly eutactic lattice, if one exists (each minimal class has no more than one weakly eutactic lattice).

Finally we show that lattices in $\mathcal{W}_n^*$ cannot have too many minimal vectors, consistent with examples L_3, L_4, L_5, and K_3' demonstrated above.

Lemma 2.3.5. *Let $n \geq 3$ and $L \in \mathcal{W}_n$ be such that $|S(L)| > 3n$. Then $L \notin \mathcal{W}_n^*$.*

Proof. Let $L \in \mathcal{W}_n^*$ and let $B = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ be its nearly orthogonal basis. We want to prove that $|S(L)| \leq 3n$. Suppose that for some $1 \leq k \leq n$

$$\boldsymbol{x}_1 = \alpha_1 \boldsymbol{b}_k + \boldsymbol{y} \in S(L), \ \boldsymbol{x}_2 = \alpha_2 \boldsymbol{b}_k + \boldsymbol{z} \in S(L),$$

where $0 \neq \alpha_1, \alpha_2 \in \mathbb{Z}$ and $\boldsymbol{0} \neq \boldsymbol{y}, \boldsymbol{z} \in \mathrm{span}_{\mathbb{Z}} B \setminus \{\boldsymbol{b}_k\}$. Then by Lemma 2.2.1, we must have $\alpha_1, \alpha_2 = \pm 1$, $\boldsymbol{y}, \boldsymbol{z} \in S(L)$, and the angles between $\boldsymbol{b}_k$ and $\boldsymbol{y}$, $\boldsymbol{z}$ equal to $\pi/3$ or $2\pi/3$. In this case Lemma 2.2.2 implies that the angle $\boldsymbol{b}_k$ makes with the space spanned by the rest of vectors of B is less than $\pi/3$, which contradicts the assumption that L is in $\mathcal{W}_n^*$. Hence there can be at most one $\pm$ pair of vectors in $S(L)$ besides $\pm\boldsymbol{b}_k$ which is expressible as an integral linear combination of the vectors of B with a nonzero coefficient in front of $\boldsymbol{b}_k$, and this is true for every $1 \leq k \leq n$. Thus a maximal possible number of minimal vectors for L is achieved by the construction described in Lemma 2.3.1 with $3n$ or $3n-1$ vectors, depending on whether n is even or odd. □

Proof of Theorem 2.1.3. The theorem now follows upon combining Lemmas 2.3.1, 2.3.2, 2.3.3 and 2.3.5 with Corollary 2.3.4. □

Proof of Corollary 2.1.5. We argue by induction on $n \geq 2$. If $n = 2$, then $|S(L)| = 4$ unless L is the hexagonal lattice, in which case it has 6 minimal vectors. In either case, the result is immediate by direct verification. Suppose now the result is established in all dimensions $\leq n-1$. Let us prove it for n. By Lemma 2.3.5, $|S(L)| \leq 3n$, out of which n pairs of vectors are the nearly orthogonal basis vectors $\pm B = \pm\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$. Let $X = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\} \subset S(L)$ be any n linearly independent vectors. Then at least $n - [n/2]$ of them are vectors from $\pm B$. Let $\boldsymbol{b}_k$ be one of these vectors. There is at most one other vector, say $\boldsymbol{x}_1 \in X$, which is a linear combination of some $\boldsymbol{b}_i$'s with ± 1 coefficients and a nonzero coefficient in front of $\boldsymbol{b}_k$: we can write this $\boldsymbol{x}_1$ as $\boldsymbol{x}_1' \pm \boldsymbol{b}_k$. Then

$$\mathrm{span}_{\mathbb{Z}}\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n\} = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{x}_1', \ldots, \boldsymbol{x}_n\},$$

and $\mathrm{span}_{\mathbb{Z}}(X \setminus \{\boldsymbol{b}_k\}) \subseteq L_k' := \mathrm{span}_{\mathbb{Z}}(B \setminus \{\boldsymbol{b}_k\})$ with $X \setminus \{\boldsymbol{b}_k\} \subset S(L_k')$. Applying the induction hypothesis to L_k', we see that $X \setminus \{\boldsymbol{b}_k\}$ is a basis for L_k'. Since $L = \mathrm{span}_{\mathbb{Z}}\{L_k', \boldsymbol{b}_k\}$, we conclude that X is a basis for L. □

2.4 Coherence

We now discuss the maximal coherence of lattices in some more details. As indicated in [35], one might expect that many extreme lattices have maximal coherence $= 1/2$. Certainly this is true for the standard root lattices A_n, D_n, E_6, E_7 and E_8, as witnessed by the Coxeter-Dynkin diagrams (see, for instance, Theorem 4.6.3 of [49]; see also Figure 1.3). On the other hand, there are also extreme lattices that have maximal coherence less than $1/2$. Consider, for instance, the Coxeter-Barnes lattice A_n^r, which is best defined as a lattice of rank n in $\mathbb{R}^{n+1}$ spanned over $\mathbb{Z}$ by the basis

$$\boldsymbol{e}_1 - \boldsymbol{e}_2, \ldots, \boldsymbol{e}_1 - \boldsymbol{e}_n, \ \frac{1}{r}\left(n\boldsymbol{e}_1 - \sum_{i=2}^{n} \boldsymbol{e}_i\right),$$

where $\boldsymbol{e}_i$ are standard basis vectors in $\mathbb{R}^{n+1}$. Let $n \geq 7$ and $1 < r < n+1$ be a divisor of $n+1$. With parameters as specified, these lattices are known to be perfect and strongly eutactic, hence extreme (see Theorem 5.2.1 of [49]). If $r = (n+1)/2$, these lattices have maximal coherence $< 1/2$ (see Proposition 5.2.3 of [49]).

These considerations raise a question: what is the maximal coherence of a WR nearly orthogonal lattice? Well, it can be $1/2$, as in the constructions in Lemmas 2.3.1 and 2.3.2 above. In fact, this is the case for any $L \in \mathcal{W}_n^*$ with $|S(L)| > 2n$. The following proposition is part (1) of Theorem 2.1.6.

Proposition 2.4.1. *Let $L \in \mathcal{W}_n^*$. Then $\mathcal{C}(L) = 1/2$ if and only if $|S(L)| > 2n$.*

Proof. Let $L \in \mathcal{W}_n^*$ and B be a weakly nearly orthogonal basis for L. Suppose $|S(L)| = 2n$. Then $S(L) = \pm B$ by Lemma 2.2.4. Assume $\mathcal{C}(L) = 1/2$. Then there are some two vectors, say, $\boldsymbol{b}_i, \boldsymbol{b}_j \in S(L)$ so that the angle between them is $\pi/3$ or $2\pi/3$. Lemma 2.2.1 then implies that one of the vectors $\boldsymbol{b}_i \pm \boldsymbol{b}_j$ is also in $S(L)$, contradicting the fact that $S(L) = \pm B$. Hence, if $|S(L)| = 2n$, maximal coherence must be $< 1/2$.

Now suppose $|S(L)| > 2n$. Then $\pm B \subsetneq S(L)$, so there must exist some $\boldsymbol{x} \in S(L) \setminus \pm B$. Suppose that this $\boldsymbol{x}$ is a linear combination of some $m \geq 2$ vectors of B, say

$$\boldsymbol{x} = \sum_{k=1}^{m} \alpha_k \boldsymbol{b}_{i_k},$$

where $2 \leq m \leq n$, $1 \leq i_1 < \cdots < i_m \leq n$, $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$. We will prove that $\mathcal{C}(L) = 1/2$. If $m = 2$, then $\boldsymbol{x} = \alpha_1 \boldsymbol{b}_{i_1} + \alpha_2 \boldsymbol{b}_{i_2} \in S(L)$ and

$$\|\boldsymbol{x}\| = \|\boldsymbol{b}_{i_1}\| = \|\boldsymbol{b}_{i_2}\|.$$

Lemma 2.2.1 then implies that $\alpha_1, \alpha_2 = \pm 1$ and the angle between $\boldsymbol{b}_{i_1}$ and $\boldsymbol{b}_{i_2}$ is $\pi/3$ or $2\pi/3$. This implies that $\mathcal{C}(L) = 1/2$. Assume now $m > 2$. Let $\boldsymbol{y} = \sum_{k=1}^{m-1} \alpha_k \boldsymbol{b}_{i_k}$,

then $\boldsymbol{x} = \boldsymbol{y} + \alpha_m \boldsymbol{b}_{i_m}$. Since $\boldsymbol{y} \in \mathrm{span}_{\mathbb{R}}\{\boldsymbol{b}_{i_1}, \ldots, \boldsymbol{b}_{i_{m-1}}\}$, the angle θ between $\boldsymbol{y}$ and $\boldsymbol{b}_{i_m}$ is in the interval $[\pi/3, 2\pi/3]$. Then Lemma 2.2.1 implies that

$$\|\boldsymbol{x}\| \geq \min\{\|\boldsymbol{y}\|, \|\boldsymbol{b}_{i_m}\|\} = \|\boldsymbol{b}_{i_m}\| = \|\boldsymbol{x}\|,$$

which is only possible if $\boldsymbol{y} \in S(L)$, $\alpha_m = \pm 1$ and $\theta = \frac{\pi}{3}$ or $\frac{2\pi}{3}$. Hence $\mathcal{C}(L) = \frac{1}{2}$. $\square$

On the other hand, $\mathbb{Z}^n \in \mathcal{W}_n^*$ and intuition suggests that lattices with very low maximal coherence should be in $\mathcal{W}_n^*$. One can ask, "how low is low enough?" In other words, does there exist some dimensional constant c_n such that whenever $\mathcal{C}(L) \leq c_n$, the lattice L is necessarily in $\mathcal{W}_n^*$?

Example 5. *Define a cyclic frame*

$$\boldsymbol{b}_1 := \frac{1}{\sqrt{n^2+n}} \begin{pmatrix} -n \\ 1 \\ \vdots \\ 1 \end{pmatrix}, \ldots, \boldsymbol{b}_n := \frac{1}{\sqrt{n^2+n}} \begin{pmatrix} 1 \\ \vdots \\ -n \\ 1 \end{pmatrix},$$

and

$$\boldsymbol{b}_{n+1} := \frac{1}{\sqrt{n^2+n}} \begin{pmatrix} 1 \\ 1 \\ \vdots \\ -n \end{pmatrix} = -(\boldsymbol{b}_1 + \cdots + \boldsymbol{b}_n).$$

Let $L = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$, then $S(L) = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n, \boldsymbol{b}_{n+1}\}$ and L is similar to the lattice A_n^*, the dual of the root lattice $A_n := V \cap \mathbb{Z}^{n+1}$, i.e.,

$$A_n^* := \{\boldsymbol{x} \in V : (\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{Z} \ \forall \ \boldsymbol{y} \in A_n\}.$$

Then $\mathcal{C}(L) = 1/n$, $|S(L)| = 2n + 2$; see [35], [10], [49] for further details on this

lattice. On the other hand, L is not contained in $\mathcal{W}_n$ by Proposition 2.4.1, since $\mathcal{C}(L) < 1/2$ while $|S(L)| > 2n$.

Thus Example 5 shows that a WR lattice with maximal coherence even as low as $1/n$ still does not have to be nearly orthogonal, i.e., $c_n < 1/n$. This being said, we can prove the following criterion, which is part (2) of Theorem 2.1.6.

Proposition 2.4.2. *Let $B = \{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ in $\mathbb{R}^n$ be a collection of linearly independent unit vectors such that*

$$\max_{1 \le i < j \le n} |(\boldsymbol{b}_i, \boldsymbol{b}_j)| \le c_n, \tag{2.14}$$

where c_n is as in (2.3). Then $L = \operatorname{span}_{\mathbb{Z}} B$ is in $\mathcal{W}_n^*$.

Proof. Let us prove that if (2.14) holds, then B is a nearly orthogonal basis for $L = \operatorname{span}_{\mathbb{Z}} B$. Without loss of generality, assume that $B = \{\boldsymbol{b}_1, \dots, \boldsymbol{b}_n\}$ is an arbitrary ordering of B. Then we only need to prove that (2.14) forces the angle θ between $\Pi_{k-1} := \operatorname{span}_{\mathbb{R}}\{\boldsymbol{b}_1, \dots, \boldsymbol{b}_{k-1}\}$ and $\boldsymbol{b}_k$ to be $\ge \pi/3$ for every $2 \le k \le n$. Let $\boldsymbol{x} \in \Pi_{k-1}$ be a vector so that

$$\mathfrak{a}(\boldsymbol{x}, \boldsymbol{b}_k) = \theta.$$

Let us write $\boldsymbol{x} = \sum_{i=1}^{k-1} \alpha_i \boldsymbol{b}_i$ for some $\alpha_1, \dots, \alpha_{k-1} \in \mathbb{R}$. Then

$$\|\boldsymbol{x}\|^2 = \sum_{i,j=1}^{k-1} \alpha_i \alpha_j (\boldsymbol{b}_i, \boldsymbol{b}_j) \ge \sum_{i=1}^{k-1} \alpha_i^2 - 2c_n \sum_{1 \le i < j \le k-1} |\alpha_i \alpha_j|,$$

and so

$$|\cos\theta| = \frac{|(\boldsymbol{x}, \boldsymbol{b}_k)|}{\|\boldsymbol{x}\|} \le \frac{\sum_{i=1}^{k-1} |\alpha_i| |(\boldsymbol{b}_i, \boldsymbol{b}_k)|}{\|\boldsymbol{x}\|} \le \frac{c_n \sum_{i=1}^{k-1} |\alpha_i|}{\sqrt{\sum_{i=1}^{k-1} \alpha_i^2 - 2c_n \sum_{1 \le i < j \le k-1} |\alpha_i \alpha_j|}}.$$

We want this quantity to be $\leq 1/2$, which is equivalent to saying that

$$4c_n^2 \left(\sum_{i=1}^{k-1} |\alpha_i| \right)^2 \leq \sum_{i=1}^{k-1} \alpha_i^2 - 2c_n \sum_{1 \leq i < j \leq k-1} |\alpha_i \alpha_j|. \tag{2.15}$$

Manipulating (2.15), we obtain

$$f(\alpha_1, \ldots, \alpha_{k-1}) := \frac{\sum_{1 \leq i < j \leq k-1} |\alpha_i \alpha_j|}{\sum_{i=1}^{k-1} \alpha_i^2} \leq \frac{1 - 4c_n^2}{8c_n^2 + 2c_n}. \tag{2.16}$$

In other words, $|\cos\theta| \leq 1/2$ if and only if (2.16) holds for all $\alpha_1, \ldots, \alpha_{k-1} \in \mathbb{R}$. Hence we want to maximize $f(\alpha_1, \ldots, \alpha_{k-1})$ and prove that this maximum is no bigger than the right hand side of (2.16). We can assume without loss of generality that all α_i are nonnegative. For every $1 \leq i \leq k-1$,

$$f_i := \frac{\partial}{\partial \alpha_i} f(\alpha_1, \ldots, \alpha_{k-1}) = \frac{\left(\sum_{j=1}^{k-1} \alpha_j^2 \right) \left(\sum_{j \neq i} \alpha_j \right) - 2\alpha_i \left(\sum_{1 \leq l < j \leq k-1} \alpha_l \alpha_j \right)}{\left(\sum_{j=1}^{k-1} \alpha_j^2 \right)^2}.$$

Then $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{k-1})$ is a critical point of f if and only if $f_i(\boldsymbol{\alpha}) = 0$ for all $1 \leq i \leq k-1$, which is equivalent to

$$\alpha_i = \frac{1}{2} \left(\frac{\sum_{j=1}^{k-1} \alpha_j^2}{\sum_{1 \leq i < j \leq k-1} \alpha_i \alpha_j} \right) \left(\sum_{j=1, j \neq i}^{k-1} \alpha_j \right) = \frac{1}{2f(\boldsymbol{\alpha})} \sum_{j=1, j \neq i}^{k-1} \alpha_j. \tag{2.17}$$

Summing (2.17) over all i, we obtain:

$$\sum_{i=1}^{k-1} \alpha_i = \frac{1}{2f(\boldsymbol{\alpha})} \sum_{i=1}^{k-1} \sum_{j=1, j \neq i}^{k-1} \alpha_j = \frac{k-2}{2f(\boldsymbol{\alpha})} \sum_{i=1}^{k-1} \alpha_i,$$

which means that $\boldsymbol{\alpha}$ is a critical point of f if and only if $\frac{k-2}{2f(\boldsymbol{\alpha})} = 1$, i.e., $f(\boldsymbol{\alpha}) = \frac{k-2}{2}$. Notice that this happens when $\alpha_1 = \cdots = \alpha_{k-1} \neq 0$:

$$f(\alpha_1, \ldots, \alpha_1) = \frac{\binom{k-1}{2} \alpha_1^2}{(k-1)\alpha_1^2} = \frac{k-2}{2},$$

i.e., f is constant on the line $\{\alpha_1 = \cdots = \alpha_{k-1}\} \setminus \{0\}$. Computing the Hessian matrix of f at any point $\boldsymbol{\alpha}$ with equal positive coordinates, we obtain:

$$H(f) = \frac{1}{k-1} \begin{pmatrix} -(k-2) & 1 & \dots & 1 \\ 1 & -(k-2) & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & -(k-2) \end{pmatrix}.$$

It is a $(k-1)\times(k-1)$ symmetric matrix with a simple eigenvalue 0 and eigenvalue -1 of multiplicity $k-2$. Hence, as a symmetric bilinear form on the tangent space to the graph of f along the entire line $\{\alpha_1 = \cdots = \alpha_{k-1}\} \setminus \{0\}$, $H(f)$ is negative semidefinite with 1-dimensional radical $\operatorname{span}_{\mathbb{R}}\{(1,\dots,1)^\top\}$. This implies that f assumes its maximum at $(\alpha,\dots,\alpha) \neq \mathbf{0}$. Hence we have $|\cos\theta| \leq 1/2$ if and only if

$$\frac{k-2}{2} \leq \frac{1-4c_n^2}{8c_n^2+2c_n},$$

for all $k \leq n$. This is equivalent to saying that

$$4(n-1)c_n^2 + (n-2)c_n - 1 \leq 0.$$

For positive c_n, equality in this inequality holds if and only if c_n is as in (2.14). □

Remark 2.4.1. Notice that c_n defined in (2.14) is not much smaller than $1/n$. For instance, for $n = 1000$, $c_n = 0.00099801587...$ as compared to $1/n = 0.001$. Furthermore,

$$\begin{aligned} \lim_{n\to\infty} (c_n/(1/n)) &= \left(\lim_{n\to\infty} \frac{n}{8(n-1)}\right) \lim_{n\to\infty} \left(\sqrt{(n-2)^2+16(n-1)} - (n-2)\right) \\ &= \frac{1}{8} \lim_{n\to\infty} \frac{16(n-1)}{\sqrt{(n-2)^2+16(n-1)} + (n-2)} = 1. \end{aligned}$$

This suggests that asymptotically as $n \to \infty$ the family of lattices A_n^* of Example 5 comes as close as possible to $\mathcal{W}_n^*$ with respect to maximal coherence.

Approximation of WR lattices with respect to maximal coherence has previously been considered in [24], where a sequence of integer lattices approximating the hexagonal lattice in the plane was constructed (Theorem 1.6 of [24]). Here we also construct an infinite family of integral WR planar lattices with arbitrarily small maximal coherence and controlled minimal norm and denominator, thus approximating $\mathbb{Z}^2$. This is a result in the spirit of Diophantine approximation.

Proposition 2.4.3. *Let $0 < \varepsilon \leq 1/2$ and D be a positive squarefree integer. There exists an integral well-rounded lattice*

$$L = \begin{pmatrix} \sqrt{q} & p/\sqrt{q} \\ 0 & r\sqrt{D}/\sqrt{q} \end{pmatrix} \mathbb{Z}^2 \subset \mathbb{R}^2, \tag{2.18}$$

where $p, q, r \in \mathbb{Z}_{>0}$ and $p^2 + r^2 D = q^2$, so that $0 < \mathcal{C}(L) = p/q < \varepsilon$ with

$$q \leq \frac{2D}{1-\varepsilon}\left(\frac{1}{\varepsilon} + 2\sqrt{\frac{1}{\varepsilon} - 1}\right).$$

For this L, we have

$$|L| = \sqrt{q} \leq \sqrt{\frac{2D}{1-\varepsilon}\left(\frac{1}{\varepsilon} + 2\sqrt{\frac{1}{\varepsilon} - 1}\right)}$$

and

$$\det(L) = r\sqrt{D} \leq 2\sqrt{D}\left(\sqrt{\frac{1}{\varepsilon^2} - 1} + \sqrt{\frac{1}{\varepsilon} + 1}\right).$$

Proof. Let $\gamma = m/(n\sqrt{D}) > 1$ be a rational multiple of $1/\sqrt{D}$ such that

$$\gamma \leq \sqrt{\frac{1+\varepsilon}{1-\varepsilon}}. \tag{2.19}$$

We can assume without loss of generality that $\gcd(m,n)=1$. Then

$$\sqrt{D} < m/n \leq \sqrt{3D}.$$

Let $p = m^2 - Dn^2$, $q = m^2 + Dn^2$ and $r = 2mn$, then $p^2 + r^2 D = q^2$ and

$$\frac{p}{q} = \frac{\gamma^2 Dn^2 - Dn^2}{\gamma^2 Dn^2 + Dn^2} = \frac{\gamma^2 - 1}{\gamma^2 + 1} \leq \varepsilon.$$

Further,

$$q = m^2 + Dn^2 = (\gamma^2 + 1)Dn^2, \tag{2.20}$$

and, by (2.19),

$$\frac{m}{n} \leq \frac{\sqrt{D(1+\varepsilon)}}{\sqrt{1-\varepsilon}} = \frac{\sqrt{D(\frac{1}{\varepsilon}+1)}}{\sqrt{\frac{1}{\varepsilon}-1}}.$$

We can then take $m = \left\lfloor \sqrt{D(\frac{1}{\varepsilon}+1)} \right\rfloor$ and $n = \left\lfloor \sqrt{\frac{1}{\varepsilon}-1} \right\rfloor + 1$. Combining this observation with (2.20) and (2.19), we obtain

$$\begin{aligned} q &\leq \left(\frac{1+\varepsilon}{1-\varepsilon} + 1\right) D \left(\left\lfloor \sqrt{\frac{1}{\varepsilon} - 1} \right\rfloor + 1 \right)^2 \\ &\leq \frac{2D}{1-\varepsilon} \left(\frac{1}{\varepsilon} + 2\sqrt{\frac{1}{\varepsilon} - 1} \right). \end{aligned}$$

The rest follows by Proposition 1.1 of [29]. □

CHAPTER III

Cyclotomic lattices

3.1 Introduction

Let $L \subset \mathbb{R}^d$ be a lattice of full rank $d \geq 1$ in the Euclidean space $\mathbb{R}^d$, where we will always write $\| \ \|$ for the corresponding Euclidean norm. As usual, we define the *minimum* of L to be

$$|L| := \min \{\|\boldsymbol{x}\| : \boldsymbol{x} \in L \setminus \{\mathbf{0}\}\},$$

and the set of *minimal vectors* of L to be

$$S(L) := \{\boldsymbol{x} \in L : \|\boldsymbol{x}\| = |L|\}.$$

The lattice L is called *well-rounded* (WR) if $\operatorname{span}_{\mathbb{R}} S(L) = \mathbb{R}^d$. There is a stronger condition for L to be *generated by minimal vectors* if $\operatorname{span}_{\mathbb{Z}} S(L) = L$ (see [60]), and an even stronger condition for L to have a *basis of minimal vectors*, i.e. for $S(L)$ to contain a basis for L (see [50]). We can associate a sphere packing to the lattice L by placing maximal non-overlapping spheres of equal radius at the lattice points. Then the radius of these spheres, called the *packing radius* of L, will be $|L|/2$ and the

*This chapter is based on joint work with Lenny Fukshansky, to be published in *Communications in Mathematics*; see [30]

density of this lattice packing will be

$$\delta(L) := \frac{\omega_d |L|^d}{2^d \det(L)},$$

where ω_d is the volume of a unit ball in $\mathbb{R}^d$ and $\det(L)$ is the determinant of L, as usual. Given a basis matrix $B = \begin{pmatrix} \boldsymbol{b}_1 & \dots & \boldsymbol{b}_d \end{pmatrix}$ for L, we define the *orthogonality defect* of B as

$$\nu(B) := \frac{\prod_{j=1}^{d} \|\boldsymbol{b}_j\|}{\det(L)},$$

i.e. the ratio of the volume of a rectangular box with sides $\|\boldsymbol{b}_1\|, \dots, \|\boldsymbol{b}_d\|$ to the volume of the parallelepiped spanned by the column vectors of B. Naturally, the Hadamard inequality $\nu(B) \geq 1$ holds with equality if and only if B is an orthogonal basis. If $B \subseteq S(L)$, then

$$\nu(B) = \frac{|L|^d}{\det(L)} = \frac{2^d}{v_d} \delta(L) \tag{3.1}$$

is an invariant of the lattice L, which we will call the orthogonality defect of L and denote by $\nu(L)$. Hence for a lattice with a basis of minimal vectors the packing density is proportionate to the orthogonality defect, i.e. to maximize the packing density one wants a lattice with a "least orthogonal" minimal basis. Orthogonality defect figures prominently in lattice theory, especially in connection with algorithmic lattice problems (see [53]).

Another measure of orthogonality for a collection of vectors is given by coherence and comes from signal processing. Given a finite set of vectors $S \subset \mathbb{R}^d$, we define its *maximal coherence* as

$$\mathcal{C}(S) := \max \left\{ \frac{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|}{\|\boldsymbol{x}\| \|\boldsymbol{y}\|} : \boldsymbol{x} \neq \boldsymbol{y} \in S \right\},$$

where $\langle\ ,\ \rangle$ stand for the usual Euclidean inner product, and we define its *average*

coherence as

$$\mathcal{A}(S) := \frac{1}{|S|-1} \max \left\{ \sum_{\boldsymbol{y} \in S \setminus \{\boldsymbol{x}\}} \frac{|\langle \boldsymbol{x}, \boldsymbol{y} \rangle|}{\|\boldsymbol{x}\| \|\boldsymbol{y}\|} : \boldsymbol{x} \in S \right\}.$$

It is easy to see that $\mathcal{A}(S) = 0$ if and only if S is an orthogonal collection of vectors, which in particular implies $|S| \leq d$. An important problem in signal processing is the construction of sufficiently large sets S ($|S| > d$) with sufficiently low coherence. Special attention among such low-coherence sets is usually given to frames, which are overdetermined spanning sets with certain additional properties, especially to the uniform tight frames: a finite set $S \subset \mathbb{R}^d$ is called a *uniform tight frame* if all vectors in S have the same norm and there exists a real constant $\gamma > 0$ such that

$$\|\boldsymbol{v}\| = \gamma \sum_{\boldsymbol{x} \in S} \langle \boldsymbol{v}, \boldsymbol{x} \rangle^2,$$

for every $\boldsymbol{v} \in \mathbb{R}^d$ (see [68] for a comprehensive exposition of tight frame theory).

We can extend the notion of coherence to lattices as follows. Notice that minimal vectors of a lattice L come in $\pm$ pairs: $\boldsymbol{x} \in S(L)$ if and only if $-\boldsymbol{x} \in S(L)$. Then define $S'(L)$ to be a subset of $S(L)$ constructed by selecting one vector out of each such pair, and define maximal and average coherence of L to be

$$\mathcal{C}(L) := \mathcal{C}(S'(L)), \ \mathcal{A}(L) := \mathcal{A}(S'(L)),$$

respectively. These values do not depend on the specific choice of vectors in $S'(L)$ out of each $\pm$ pair. If L has a basis of minimal vectors, then $\mathcal{A}(L)$ becomes a certain alternative measure of its "non-orthogonality": $\mathcal{A}(L) \geq 0$ with equality if and only if $S'(L)$ is an orthogonal basis for L. Maximal coherence on lattices has previously been introduced in [35] and studied on nearly orthogonal lattices in [31], but average coherence has not previously been extended to lattices, as far as we know. Average coherence for frames was introduced in [5]. Our definition of average coherence slightly

differs from the one introduced in [5]: in their definition, the absolute value is outside of the sum. We choose to move absolute value inside to ensure that the average coherence does not depend on the choice of the vectors in $S'(L)$: it does not matter which vector from each $\pm$ pair in $S(L)$ is selected.

While there can be a relation between average coherence and orthogonality defect in some special cases, there does not appear to be a general dependence. On the other hand, it is interesting to understand which lattices with relatively large sets of minimal vectors simultaneously have small average coherence and large orthogonality defect. To this end, given a lattice $L \subset \mathbb{R}^d$ with a basis of minimal vectors, we define its *orthogonality product measure* (referred to from here on simply as *product measure*) to be

$$\Pi(L) := \frac{|S'(L)|\nu(L)}{d \cdot \mathcal{A}(L)}. \tag{3.2}$$

Then a lattice L with large $|S'(L)|$ (as compared to the dimension d), small $\mathcal{A}(L)$ and large $\nu(L)$ will have large $\Pi(L)$. We can then ask which lattices have large $\Pi(L)$. In this note, we investigate average coherence and product measure on the family of cyclotomic lattices, a special family of ideal lattices. We start out by recalling the ideal lattices.

Let K be a number field of degree d over $\mathbb{Q}$, and let $\mathcal{O}_K$ be its ring of integers. Let

$$\sigma_1, \ldots, \sigma_{r_1}, \tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2} : K \hookrightarrow \mathbb{C}$$

be its embeddings into the field of complex numbers, where $r_1 + 2r_2 = d$ and $\sigma_1, \ldots, \sigma_{r_1}$ are real embeddings, whereas $\tau_1, \bar{\tau}_1, \ldots, \tau_{r_2}, \bar{\tau}_{r_2}$ are pairs of complex conjugate embeddings. The *Minkowski embedding* of K into $\mathbb{R}^d$ is then defined as

$$\Sigma_K := (\sigma_1, \ldots, \sigma_{r_1}, \Re(\tau_1), \Im(\tau_1), \ldots, \Re(\tau_{r_2}), \Im(\tau_{r_2})) : K \hookrightarrow \mathbb{R}^d,$$

and the image of $\mathcal{O}_K$ under this embedding, $\Lambda_K := \Sigma_K(\mathcal{O}_K)$, is a Euclidean lattice of full rank in $\mathbb{R}^d$. Furthermore,

$$\det(\Lambda_K) = 2^{-r_2}|\Delta_K|^{1/2}, \tag{3.3}$$

where Δ_K stands for the discriminant of K. Such lattices are called *number field lattices*; they form a special case of the more general *ideal lattices* (of trace type), which are given by the same construction on an arbitrary fractional ideal in K. This construction of ideal lattices is classical: it can be found, for instance, in [9] (pp. 94–99) or [64] (Chapter 5.3), as well as in [8].

We focus specifically on cyclotomic fields. Let $\zeta_n = e^{\frac{2\pi i}{n}}$ for $n > 2$ be the n-th primitive root of unity and $K = \mathbb{Q}(\zeta_n)$ be the corresponding n-th cyclotomic number field, then $d = [K : \mathbb{Q}] = \phi(n)$ and the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$. Then the group of n-th roots of unity

$$\mathcal{R}_n := \left\{\zeta_n^k : 1 \leq k \leq n\right\}$$

is precisely the set of all roots of unity contained in $\mathcal{O}_K$. We refer to the lattice Λ_K as the *n-th cyclotomic lattice*. We give a more detailed description of cyclotomic lattices and their properties in Section 3.2, in particular explaining that they have bases of minimal vectors and

$$|S'(\Lambda_K)| = \begin{cases} n & \text{if } n \text{ is odd,} \\ \frac{1}{2}n & \text{if } n \text{ is even.} \end{cases}$$

Further, we demonstrate the well-known fact that in the cyclotomic case the orthogonality defect

$$\nu(\Lambda_K) = \left(\frac{\phi(n)}{\prod_{p|n} p^{e_p - \frac{1}{p-1}}}\right)^{\frac{\phi(n)}{2}}, \tag{3.4}$$

where $n = \prod_{p|n} p^{e_p}$ and the product in the denominator is over all primes dividing n. We also define the average coherence $\mathcal{A}(\alpha)$ for any $\alpha \in S'(\Lambda_K)$, as well as $\mathcal{A}(\Lambda_K)$,

the average coherence of the lattice Λ_K, in (3.9) and (3.10), respectively. Finally, cyclotomic lattices are *strongly eutactic*, meaning that their sets of minimal vectors form uniform tight frames in their respective Euclidean spaces.

Cyclotomic lattices have been extensively studied in the context of lattice theory (see Section 8.7 of [19] and references therein), and their structure is generally understood. One goal of this note is to attract some attention to the notions of average and maximal coherence on lattices. We use cyclotomic lattices as a simple and attractive case study. As it turns out, there is a particularly simple and elegant arithmetic formula for the average coherence of this family of lattices.

Theorem 3.1.1. *Let $n > 2$ be an integer, and let Λ_K be the corresponding cyclotomic lattice for $K = \mathbb{Q}(\zeta_n)$. Then*

$$\mathcal{C}(\Lambda_K) = \begin{cases} 0 & \text{if } n \text{ is power of } 2, \\ \frac{1}{p-1} & \text{if } p \text{ is the smallest odd prime dividing } n. \end{cases}$$

Additionally, for any $\alpha \in S'(\Lambda_K)$,

$$\mathcal{A}(\alpha) = \mathcal{A}(\Lambda_K) = \begin{cases} \frac{2^{\omega(n)}-1}{n-1} & \text{if } n \text{ is odd}, \\ \frac{2^{\omega(n)}-2}{n-2} & \text{if } n \text{ is even}, \end{cases} \tag{3.5}$$

where ω is the number of prime divisors function. Combining (3.5) *with* (3.4)*, we readily obtain an explicit formula for $\Pi(\Lambda_{\mathbb{Q}(\zeta_n)})$, which depends only on n:*

$$\Pi(\Lambda_{\mathbb{Q}(\zeta_n)}) = \begin{cases} \frac{n(n-2)\phi(n)^{\frac{\phi(n)}{2}-1}}{2(2^{\omega(n)}-2)\left(\prod_{p|n} p^{e_p-\frac{1}{p-1}}\right)^{\frac{\phi(n)}{2}}} & \text{if } 2 \mid n, \\ \frac{n(n-1)\phi(n)^{\frac{\phi(n)}{2}-1}}{(2^{\omega(n)}-1)\left(\prod_{p|n} p^{e_p-\frac{1}{p-1}}\right)^{\frac{\phi(n)}{2}}} & \text{if } 2 \nmid n. \end{cases}$$

We prove Theorem 3.1.1 in Section 3.3. In Section 3.4, we demonstrate several examples, aiming to determine values of n for which $\Pi(\Lambda_{\mathbb{Q}(\zeta_n)})$ is the largest in a fixed

dimension $d = \phi(n)$. For comparison purposes, we also compute the coherence and product measure values for the standard root lattices. Of course, it is easy to see that the product measure values for cyclotomic lattices are not nearly as large as for the root lattices in the same dimensions. On the other hand, root lattices are truly exceptional (in particular, they are local maxima of the packing density function in their dimensions; see, for instance, Chapter 4 of [49] for details), and there are very few of them. Cyclotomic lattices present a larger family of lattices with interesting properties (in even dimensions given by the values of the Euler ϕ-function), including numerous examples of lattices with low maximal coherence. In fact, as we discuss at the end of Section 3.4, the maximal and average coherence of cyclotomic lattices, in contrast with the root lattices, are about the same on the average as $n \to \infty$, which can also make them potentially interesting from the standpoint of signal processing, since this means that any pair of frequencies represented by the minimal vectors is equally mutually incoherent. We are now ready to proceed.

3.2 Cyclotomic lattices

In this section we give an alternative, and for our purposes more convenient, description of cyclotomic lattices. Let $K = \mathbb{Q}(\zeta_n)$. For $n > 2$, K only has the complex embeddings

$$\tau_1, \boldsymbol{\tau}_1, \ldots, \tau_{d/2}, \boldsymbol{\tau}_{d/2} : K \hookrightarrow \mathbb{C},$$

so $r_1 = 0$ and $d = \phi(n) = 2r_2$. For each $\alpha \in \mathcal{O}_K$, the trace of α is given by

$$\mathrm{Tr}_K(\alpha) := \sum_{k=1}^{d/2} (\tau_k(\alpha) + \boldsymbol{\tau}_k(\alpha)).$$

Using the notation of Section 8.7 of [19] (see also [7]), we can think of the cyclotomic lattice Λ_K as the free $\mathbb{Z}$-module $\mathcal{O}_K$ equipped with the bilinear form

$$\langle \alpha, \beta \rangle := \frac{1}{2} \operatorname{Tr}_K(\alpha\bar{\beta})$$

for any $\alpha, \beta \in \mathcal{O}_K$. It is easy to verify that $\langle \alpha, \beta \rangle$ is equal to the usual dot product of the vectors $\Sigma_K(\alpha)$ and $\Sigma_K(\beta)$ in $\mathbb{R}^d$. Then for any $\alpha = a + bi \in \mathcal{O}_K = \mathbb{Z}[\zeta_n]$, so $\alpha\bar{\alpha} = a^2 + b^2$, and hence

$$\langle \alpha, \alpha \rangle = \sum_{k=1}^{d/2} \tau_k(a^2 + b^2) = \sum_{k=1}^{d/2} \left(\Re(\tau_k(\alpha))^2 + \Im(\tau_k(\alpha))^2 \right).$$

By the results of [36], Λ_K is WR with $|\Lambda_K|^2 = \frac{\phi(n)}{2}$ and $\alpha \in S(\Lambda_K)$ if and only if it is a root of unity, i.e.

$$S(\Lambda_K) = \{\pm\alpha : \alpha \in \mathcal{R}_n\} = \begin{cases} \mathcal{R}_n & \text{if } 2 \mid n \\ \mathcal{R}_{2n} & \text{if } 2 \nmid n, \end{cases}$$

since

$$-1 = e^{\pi i} = \begin{cases} e^{\frac{2(n/2)\pi i}{n}} & \text{if } 2 \mid n \\ e^{\frac{2n\pi i}{2n}} & \text{if } 2 \nmid n. \end{cases}$$

Let $\alpha, \beta \in S(\Lambda_K)$, then

$$\langle \alpha, \beta \rangle = \frac{1}{2} \operatorname{Tr}_K(\alpha\bar{\beta}),$$

where $\alpha\bar{\beta}$ is also a root of unity. Suppose that $\alpha\bar{\beta}$ is m-th primitive root of unity of for some $m \mid n$, then it is a root of m-th cyclotomic polynomial $\Phi_m(x)$. Notice that the trace of an algebraic number is the negative of the second coefficient of its minimal polynomial. It is a well-known fact that

$$\Phi_m(x) = x^{\phi(m)} - \mu(m)x^{\phi(m)-1} + \ldots,$$

where μ is the Möbius function. Hence $\mathrm{Tr}_{\mathbb{Q}(\alpha\bar{\beta})}(\alpha\bar{\beta}) = \mu(m)$, and therefore

$$\langle \alpha, \beta \rangle = \frac{1}{2} \mathrm{Tr}_K(\alpha\bar{\beta}) = \frac{[K : \mathbb{Q}(\alpha\bar{\beta})]}{2} \mathrm{Tr}_{\mathbb{Q}(\alpha\bar{\beta})}(\alpha\bar{\beta}) = \frac{\phi(n)}{2\phi(m)}\mu(m). \tag{3.6}$$

Further, if $\alpha = \zeta_n^{k_1}$ and $\beta = \zeta_n^{k_2}$, then $m = \frac{n}{\gcd(k_1 - k_2, n)}$, and so the cosine of the angle between these two vectors is

$$c(\alpha, \beta) := \frac{\langle \alpha, \beta \rangle}{\sqrt{\langle \alpha, \alpha \rangle \langle \beta, \beta \rangle}} = \frac{\phi(n)}{\phi(n)\phi(m)}\mu(m) = \frac{\mu\left(\frac{n}{\gcd(k_1 - k_2, n)}\right)}{\phi\left(\frac{n}{\gcd(k_1 - k_2, n)}\right)}. \tag{3.7}$$

Define $s := |S(\Lambda_K)|$, so

$$s = \begin{cases} n & \text{if } n \text{ is even} \\ 2n & \text{if } n \text{ is odd} \end{cases}. \tag{3.8}$$

Then we can write

$$S(\Lambda_K) = \left\{ \zeta_n^k, \zeta_n^{k+\frac{s}{2}} : 1 \leq k \leq s/2 \right\},$$

where $\zeta_n^{k+\frac{s}{2}} = -\zeta_n^k$ and $c\left(\zeta_n^k, \zeta_n^{k+\frac{s}{2}}\right) = -1$, as expected. Hence let

$$S'(\Lambda_K) = \left\{ \zeta_n^k : 1 \leq k \leq s/2 \right\},$$

so the coherence of the lattice Λ_K is given by

$$\mathcal{C}(\Lambda_K) = \max \left\{ |c(\alpha, \beta)| : \alpha, \beta \in S'(\Lambda_K), \alpha \neq \beta \right\}.$$

Then for any $\alpha = \zeta^{k_1}, \beta = \zeta^{k_2} \in S'(\Lambda_K)$, we have $|k_1 - k_2| \leq s/2 - 1$, and therefore $c(\alpha, \beta) \neq \pm 1$. Additionally, for each $\alpha \in S'(\Lambda_K)$ define its average coherence to be

$$\mathcal{A}(\alpha) = \frac{1}{|S'(\Lambda_K)| - 1} \sum_{\beta \in S'(\Lambda_K) \setminus \{\alpha\}} |c(\alpha, \beta)|. \tag{3.9}$$

The average coherence of Λ_K is then given by

$$\mathcal{A}(\Lambda_K) = \max\{\mathcal{A}(\alpha) : \alpha \in S'(\Lambda_K)\}. \tag{3.10}$$

Now, the discriminant of the cyclotomic field $K = \mathbb{Q}(\zeta_n)$ is given by

$$\Delta_K = (-1)^{\frac{\phi(n)}{2}} n^{\phi(n)} \prod_{p|n} p^{-\frac{\phi(n)}{p-1}},$$

where the product is over all primes p dividing n (see, for instance, Section 8.7.3 of [19]). Combining these observations with (3.1), (3.3), and the fact that $|\Lambda_K|^2 = \phi(n)/2$, we obtain (3.4).

We also briefly comment on the structure of cyclotomic lattices, which is well known (see, for instance, Section 8.7 of [19]). Two lattices $L_1, L_2 \subset \mathbb{R}^k$ are called *similar*, denoted $L_1 \sim L_2$, if there exists a nonzero real constant γ and a $k \times k$ real orthogonal matrix U such that $L_2 = \gamma U L_1$; if $\gamma = \pm 1$, L_1 and L_2 are *isometric*, denoted $L_1 \cong L_2$. For any lattice $L \subset \mathbb{R}^d$ of rank d, its *dual* is the lattice

$$L^* := \left\{ \boldsymbol{x} \in \mathbb{R}^d : \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z} \ \forall \ \boldsymbol{y} \in L \right\}.$$

Recall that the root lattice A_n is defined as

$$A_n = \left\{ \boldsymbol{x} \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0 \right\}, \tag{3.11}$$

which is a lattice of rank n, as is its dual A_n^*. With this notation, the following is true:

1. If $n = p$ is an odd prime, then $\Lambda_K \sim A_{p-1}^*$,
2. If $n = p^k$ is an odd prime power, then $\Lambda_K \sim \bigoplus_{j=1}^{p^{k-1}} A_{p-1}^*$,

3. If $n = p^k q^l$ is a product of two distinct odd primes, then

$$\Lambda_K \sim \left(\bigoplus_{j=1}^{p^{k-1}} A_{p-1}^* \right) \otimes \left(\bigoplus_{j=1}^{q^{l-1}} A_{q-1}^* \right).$$

Lattices A_n^* are known to be strongly eutactic. Further, tensor products of strongly eutactic lattices as well as direct sums of isometric strongly eutactic lattices are strongly eutactic (see Chapter 3 of [49]). This observation, along with the above properties, implies that cyclotomic lattices in general are strongly eutactic.

3.3 Coherence of cyclotomic lattices

In this section we prove Theorem 3.1.1 in a series of several lemmas. Throughout this section, $K = \mathbb{Q}(\zeta_n)$ for the specified choices of n and Λ_K is the corresponding cyclotomic lattice.

Lemma 3.3.1. *Suppose $n = 2^m$ for some $m \geq 1$, then Λ_K is an orthogonal lattice, which is similar to $\mathbb{Z}^{2^{m-1}}$. In particular, $\mathcal{C}(\Lambda_K) = 0$.*

Proof. First notice that $\phi(2^m) = 2^{m-1}$, thus Λ_K is a lattice of rank 2^{m-1} with 2^m minimal vectors. Let $\alpha, \beta \in S'(\Lambda_K)$ and suppose $\alpha\bar{\beta}$ is k-th primitive root of unity for some $k \mid 2^m$. Then $k = 2^l$ for some $0 \leq l \leq m$, and by (3.6),

$$\langle \alpha, \beta \rangle = \frac{1}{2} \frac{\phi(2^m)}{\phi(2^l)} \mu(2^l) = 0,$$

unless $l = 0$ or 1. If $l = 0$ or 1, then $\alpha\bar{\beta}$ is first or second root of unity, i.e. $\alpha\bar{\beta} = \pm 1$, which implies that $\alpha = \pm\beta$. Therefore $c(\alpha, \beta) = 0$ for any pair of distinct minimal vectors in $S'(\Lambda_K)$, and so $S(\Lambda_K)$ consists of $\phi(n) = n/2 = 2^{m-1}$ plus-minus pairs of orthogonal basis vectors of equal norm. Hence $\Lambda_K \sim \mathbb{Z}^{2^{m-1}}$. □

Lemma 3.3.2. *Assume that n is not a power of 2, and let p be the smallest odd prime dividing n. Then*

$$\mathcal{C}(\Lambda_K) = \frac{1}{p-1}.$$

Proof. Let $\alpha = \zeta_n^{k_1} \in S'(\Lambda_K)$, then

$$\{\beta \in S'(\Lambda_K) : \beta \neq \alpha\} = \left\{\zeta_n^{k_2} : 1 \leq k_2 \leq s/2, k_2 \neq k_1\right\},$$

and so $k_1 - k_2$ takes on all nonzero integer values between $k_1 - 1$ and $k_1 - s/2$. In particular, $k_1 - k_2 < s/2$, which means that $c(\alpha, \beta) \neq \pm 1$. Since p is the smallest odd prime dividing n, $2 < p \leq s/2$. Then let $k_1 = p + 1$ and $k_2 = 1$, and for the corresponding $\alpha = \zeta_n^{k_1}$, $\beta = \zeta_n^{k_2}$, (3.7) gives

$$|c(\alpha, \beta)| = \frac{1}{p-1}.$$

On the other hand, $\frac{n}{\gcd(k_1-k_2,n)} \neq 1$ is a divisor of n, which cannot be equal to 2: $\frac{n}{\gcd(k_1-k_2,n)} = 2$ implies n is even and $|k_1 - k_2| = n/2 = s/2$, however we know that $|k_1 - k_2| \leq s/2 - 1$. Hence it cannot be smaller than p, and so (3.7) guarantees that $\mathcal{C}(\Lambda_K) \leq \frac{1}{p-1}$. Thus we have the result. □

Lemma 3.3.3. *Assume n is odd and squarefree. Then*

$$\mathcal{A}(\Lambda_K) = \frac{\tau(n) - 1}{n - 1},$$

where $\tau(n)$ is the number of divisors of n.

Proof. Since n is odd, we have $s/2 = n$. Let $\alpha = \zeta_n^k \in S'(\Lambda_K)$ for some $1 \leq k \leq s/2$,

then by (3.7),

$$\begin{aligned}\mathcal{A}(\alpha) &= \frac{1}{s/2-1}\sum_{j=1,\ j\neq k}^{s/2}\frac{1}{\phi\left(\frac{n}{\gcd(j-k,n)}\right)} = \frac{1}{n-1}\sum_{m=1-k,\ m\neq 0}^{n-k}\frac{1}{\phi\left(\frac{n}{\gcd(m,n)}\right)} \\ &= \frac{1}{n-1}\sum_{d|n,\ d\neq n}\frac{a_d}{\phi(n/d)},\end{aligned}$$

where $a_d =$ the number of times $\gcd(m,n) = d$ for nonzero $1-k \leq m \leq n-k$. Notice that the set $\{1-k,\ldots,n-k\}$ is a complete residue system modulo n, as is the set $\{1,\ldots,n\}$ and hence the number of times $\gcd(m,n) = d$ for nonzero $1-k \leq m \leq n-k$ equals the number of times $\gcd(m,n) = d$ for $1 \leq m \leq n$. Therefore we can write

$$\mathcal{A}(\alpha) = \frac{1}{n-1}\sum_{d|n, d\neq n}\frac{a_d}{\phi(n/d)},$$

where

$$a_d = |\{1 \leq m \leq n : \gcd(m,n) = d\}| = \phi(n/d),$$

which is independent of k and thus of the choice of α. Hence we have

$$\mathcal{A}(\Lambda_K) = \frac{1}{n-1}\sum_{d|n,\ d\neq n}\frac{\phi(n/d)}{\phi(n/d)} = \frac{1}{n-1}\sum_{d|n,\ d\neq n}1 = \frac{\tau(n)-1}{n-1}.$$

□

Lemma 3.3.4. *Assume n is even and squarefree. Then*

$$\mathcal{A}(\Lambda_K) = \frac{\tau(n)-2}{n-2},$$

where $\tau(n)$ is the number of divisors of n.

Proof. Since n is even, we have $s/2 = n/2$. Let $\alpha = \zeta_n^k \in S'(\Lambda_K)$ for some $1 \leq k \leq$

$s/2$, then by (3.7),

$$\begin{aligned}\mathcal{A}(\alpha) &= \frac{1}{s/2-1}\sum_{j=1,\ j\neq k}^{s/2}\frac{1}{\phi\left(\frac{n}{\gcd(j-k,n)}\right)} = \frac{2}{n-2}\sum_{m=1-k,\ m\neq 0}^{\frac{n}{2}-k}\frac{1}{\phi\left(\frac{n}{\gcd(m,n)}\right)} \\ &= \frac{2}{n-2}\sum_{d|n,\ d<\frac{n}{2}}\frac{b_d}{\phi(n/d)},\end{aligned}$$

where b_d = the number of times $\gcd(m,n) = d$ for nonzero $1-k \leq m \leq \frac{n}{2}-k$. Notice that, if $d \neq 1,2$, then for any such m there is a unique $m' = m + n/2$ so that $\gcd(m',n) = \gcd(m,n) = d$ and $\frac{n}{2} - k \leq m' \leq n-k$. Therefore for each divisor $d \neq 1,2$ of n with $d < n/2$, $b_d = \frac{\phi(n/d)}{2}$. On the other hand,

$$\gcd(m,n) = 1 \Leftrightarrow \gcd(m',n) = 2,\ \gcd(m,n) = 2 \Leftrightarrow \gcd(m',n) = 1,$$

so $b_1 + b_2 = \phi(n) = \phi(n/2)$. Further, observe that $d \mid n$ with $d < n/2$ if and only if $d \mid \frac{n}{2}$ and $d \neq n/2$. Hence

$$\begin{aligned}\mathcal{A}(\Lambda_K) &= \frac{2}{n-2}\left(\frac{\phi(n/2)}{\phi(n/2)} + \sum_{d|n,\ d<\frac{n}{2},\ d\neq 1,2}\frac{\phi(n/d)}{2\phi(n/d)}\right) \\ &= \frac{2}{n-2}\left(1 + \frac{1}{2}(\tau(n)-4)\right) = \frac{\tau(n)-2}{n-2},\end{aligned}$$

since the number of divisors d of n such that $d < n/2$ is $\tau(n) - 2$: we count all the divisors except for n and $n/2$. □

Corollary 3.3.5. *Let $n > 2$ be an integer and let $n' = \prod_{p|n} p$ be its squarefree part. Let Λ_K be the corresponding cyclotomic lattice for $K = \mathbb{Q}(\zeta_n)$. Then for any $\alpha \in S'(\Lambda_K)$,*

$$\mathcal{A}(\alpha) = \mathcal{A}(\Lambda_K) = \begin{cases} \frac{\tau(n')-1}{n-1} & \text{if } n \text{ is odd,} \\ \frac{\tau(n')-2}{n-2} & \text{if } n \text{ is even.} \end{cases}$$

Proof. For each $\alpha = \zeta_n^k \in S'(\Lambda_K)$, we have

$$\mathcal{A}(\alpha) = \frac{1}{|S'(\Lambda_K)| - 1} \sum_{\beta \in S'(\Lambda_K) \setminus \{\alpha\}} |c(\alpha, \beta)| = \frac{2}{s-2} \sum_{j=1,\ j \neq k}^{s/2} \frac{\left|\mu\left(\frac{n}{\gcd(j-k,n)}\right)\right|}{\phi\left(\frac{n}{\gcd(j-k,n)}\right)},$$

where for each $\beta = \zeta_n^j \in S'(\Lambda_K)$,

$$c(\alpha, \beta) = \frac{\mu\left(\frac{n}{\gcd(k-j,n)}\right)}{\phi\left(\frac{n}{\gcd(k-j,n)}\right)} = 0,$$

unless $\frac{n}{\gcd(k-j,n)}$ is squarefree, i.e. a divisor of n'. Thus

$$\mathcal{A}(\alpha) = \frac{2}{s-2} \sum_{m=1-k,\ m \neq 0}^{\frac{s}{2}-k} \frac{\left|\mu\left(\frac{n}{\gcd(m,n)}\right)\right|}{\phi\left(\frac{n}{\gcd(m,n)}\right)} = \frac{2}{s-2} \sum_{\frac{n}{d} | n',\ d < \frac{s}{2}} \frac{c_d}{\phi(n/d)}, \tag{3.12}$$

where

$$c_d = \left| \left\{ 1 - k \leq m \leq \frac{s}{2} - k : \gcd(m, n) = d \right\} \right|.$$

Notice that every divisor d of n such that n/d divides n' is of the form $d = d'(n/n')$, where $d' \mid n'$. Let $s' = n'$ if n' is even and $2n'$ if n' is odd, then

$$c_d = \left| \left\{ 1 - k \leq m \leq \frac{s'}{2} - k : \gcd(m, n') = d' \right\} \right| = \begin{cases} a_{d'} & \text{if } 2 \nmid n' \\ b_{d'} & \text{if } 2 \mid n', \end{cases}$$

where $a_{d'}$ and $b_{d'}$ are as in Lemmas 3.3.3 and 3.3.4, respectively. The result then follows by combining (3.12) with these lemmas. □

Proof of Theorem 3.1.1. Notice that for any positive integer n with its squarefree part n', $\tau(n') = 2^{\omega(n)}$. The statement of the theorem now follows by combining Lemmas 3.3.1 and 3.3.2 with Corollary 3.3.5. □

3.4 Coherence and orthogonality defect

Throughout this section, let us write $\mathcal{C}_n$, $\mathcal{A}_n$, ν_n and Π_n for $\mathcal{C}(\Lambda_{\mathbb{Q}(\zeta_n)})$, $\mathcal{A}(\Lambda_{\mathbb{Q}(\zeta_n)})$, $\nu(\Lambda_{\mathbb{Q}(\zeta_n)})$, and $\Pi(\Lambda_{\mathbb{Q}(\zeta_n)})$, respectively. We aim to understand the behavior of these functions as n ranges through natural numbers. The first observation is that for odd n, $\Lambda_{\mathbb{Q}(\zeta_{2n})} = \Lambda_{\mathbb{Q}(\zeta_n)}$, and the formulas from Section 3.1 yield

$$\mathcal{C}_{2n} = \mathcal{C}_n,\ \mathcal{A}_{2n} = \mathcal{A}_n,\ \nu_{2n} = \nu_n,\ \Pi_{2n} = \Pi_n,$$

as expected.

Let us start by briefly recalling the order of the arithmetic function $\phi(n)$ (see Chapter 18 of [37] for further details). For all $n > 2$,

$$\frac{n}{e^{\gamma}\log\log n + \frac{3}{\log\log n}} < \phi(n) < n, \tag{3.13}$$

where $\gamma = 0.57721\ldots$ is Euler's constant. In fact, $\phi(n) < \frac{n}{e^{\gamma}\log\log n}$ for infinitely many n, although the average order of $\phi(n)$ is

$$\frac{1}{n}\sum_{m=1}^{n}\phi(m) = \frac{3n}{\pi^2} + O(\log n).$$

Recall now that $s/2$, the cardinality of $S'(\Lambda_{\mathbb{Q}(\zeta_n)})$ is n or $n/2$, depending on the parity of n, whereas the rank of $\Lambda_{\mathbb{Q}(\zeta_n)}$ is $\phi(n)$. Since it is desirable to have the number of minimal vectors as large as possible, compared to the dimension, we may want to consider values of n for which $\phi(n)$ is close to the lower bound of (3.13).

A particularly interesting situation from the standpoint of signal processing and of lattice theory arises when $2\phi(n)/s$ and $\mathcal{A}_n$ are small, while ν_n is large: this would mean that $S(\Lambda_{\mathbb{Q}(\zeta_n)})$ is a configuration of many vectors (in comparison to dimension) which are incoherent and non-orthogonal. Such configurations can be useful, for instance, in recovering signals transmitted with erasures (see [38]). To this end, we

observe that the values of n that maximize Π_n for each fixed dimension $\phi(n)$ are large n with small prime factors and small prime factor powers, and similarly for maximizing ν_n. On the other hand, values of n minimizing $\mathcal{A}_n$ are large n (for a fixed value of $\phi(n)$) with few prime factors, whereas $\mathcal{C}_n$ is minimized by n with large prime factors. In particular, it appears that large Π_n is more correlated with large ν_n than with small $\mathcal{A}_n$. Indeed, consider the examples in Table 3.1: the values marked in bold are maximal among all n with that value of $\phi(n)$ for ν_n and Π_n, and minimal for $\mathcal{C}_n$ and $\mathcal{A}_n$. We have also computed many additional examples, and the same observations seem to hold.

Further, although there is a general positive correlation between $\mathcal{A}_n$ and ν_n (see for instance dimension 24 in Table 3.1), there are nevertheless sequences of closely related values of n where the correlation is negative. Observe, for instance, dimension 72 in Table 3.1. Take $n \in \{111, 117, 135, 228, 252\}$. If we arrange these in order of number of minimal vectors of $\Lambda_{\mathbb{Q}(\zeta_n)}$, we have $s \in \{222, 228, 234, 252, 270\}$. These lattices respectively have $\mathcal{A}_n$ values of $0.0\overline{27}, 0.0265..., 0.0259..., 0.024$, and $0.0224...$. However, as $\mathcal{A}_n$ decreases, we see an increase in ν_n, from $\nu_{111} = \nu_{222} = 2447.5...$ to $\nu_{135} = \nu_{270} = 1.124... \cdot 10^5$.

This is not a unique occurrence. It appears in many dimensions, most notably in those which are multiples of 24. For instance, we find 4 such sequences in dimension 192, and all but one cyclotomic lattice in dimension 192 occurs in such a sequence. It is perhaps worth noting that the prime factorization of the number of minimal vectors in such a sequence (e.g. 222, 228, 234, 252, 270) all have the same number of distinct prime factors, and at each step at least one large prime factor is converted into lower prime factors. For instance, $222 = 2 \cdot 3 \cdot 37$ while $228 = 2^2 \cdot 3 \cdot 19$, which converts the 37 to $2 \cdot 19$. This reduction of the largest term in the denominator of (3.4) drives up ν_n but holds $\omega(n)$ constant so drives down $\mathcal{A}_n$ as n increases.

$\phi(n)$	n	$\mathcal{C}_n$	$\mathcal{A}_n$	ν_n	Π_n
6	7	**0.166...**	0.166...	**1.666...**	11.662...
6	$9 = 3^2$	0.5	**0.125**	1.539...	**18.475...**
8	$15 = 3 \cdot 5$	0.5	0.214...	**3.640...**	**31.857...**
8	$16 = 2^4$	**0**	**0**	1	–
8	$20 = 2^2 \cdot 5$	0.25	0.157...	2.048	16.213...
8	$24 = 2^3 \cdot 3$	0.5	0.090...	1.777...	29.333...
24	$35 = 5 \cdot 7$	0.25	0.088...	**66.194...**	1094.055...
24	$39 = 3 \cdot 13$	0.5	0.078...	27.953...	575.369...
24	$45 = 3^2 \cdot 5$	0.5	0.068...	48.263...	**1327.257...**
24	$52 = 2^2 \cdot 13$	**0.083...**	0.04	4.975...	134.741...
24	$56 = 2^3 \cdot 7$	0.166...	0.037...	7.706...	242.742...
24	$72 = 2^3 \cdot 3^2$	0.5	**0.028...**	5.618...	294.979...
24	$84 = 2^2 \cdot 3 \cdot 7$	0.5	0.073...	43.297...	1035.542...
72	73	**0.013...**	0.013...	5.200...	379.606...
72	$91 = 7 \cdot 13$	0.166...	0.033...	56350.535...	$2.136... \cdot 10^6$
72	$95 = 5 \cdot 19$	0.25	0.031...	32670.615...	$1.350... \cdot 10^6$
72	$111 = 3 \cdot 37$	0.5	0.027...	2447.523...	$1.383... \cdot 10^5$
72	$117 = 3^2 \cdot 13$	0.5	0.025...	21841.954...	$1.372... \cdot 10^6$
72	$135 = 3^3 \cdot 5$	0.5	0.022...	$\mathbf{1.124... \cdot 10^5}$	$\mathbf{9.415... \cdot 10^6}$
72	$148 = 2^2 \cdot 37$	0.027...	0.013...	13.798...	1035.267...
72	$152 = 2^3 \cdot 19$	0.055...	0.013...	51.545...	4081.677...
72	$216 = 2^3 \cdot 3^3$	0.5	**0.009...**	177.376...	28469.292...
72	$228 = 2^2 \cdot 3 \cdot 19$	0.5	0.026...	9142.921...	$5.452... \cdot 10^5$
72	$252 = 2^2 \cdot 3^2 \cdot 7$	0.5	0.024.	81171.032...	$5.918... \cdot 10^6$
160	$187 = 11 \cdot 17$	0.1	0.016...	$1.163... \cdot 10^9$	$8.428... \cdot 10^{10}$
160	$205 = 5 \cdot 41$	0.25	0.014...	$3.928... \cdot 10^8$	$3.594... \cdot 10^{10}$
160	$328 = 2^3 \cdot 41$	**0.025**	0.006...	233.162...	77912.090...
160	$352 = 2^5 \cdot 11$	0.1	0.005...	104646.972...	$2.014... \cdot 10^7$
160	$400 = 2^4 \cdot 5^2$	0.25	**0.005...**	$1.684... \cdot 10^6$	$4.191... \cdot 10^8$
160	$440 = 2^3 \cdot 5 \cdot 11$	0.25	0.013...	$1.763... \cdot 10^{11}$	$1.769... \cdot 10^{13}$
160	$492 = 2^2 \cdot 3 \cdot 41$	0.5	0.012...	$2.318... \cdot 10^7$	$2.911... \cdot 10^9$
160	$528 = 2^4 \cdot 3 \cdot 11$	0.5	0.011...	$1.040... \cdot 10^{10}$	$1.505... \cdot 10^{12}$
160	$600 = 2^3 \cdot 3 \cdot 5^2$	0.5	0.010...	$1.675... \cdot 10^{11}$	$3.131... \cdot 10^{13}$
160	$660 = 2^2 \cdot 3 \cdot 5 \cdot 11$	0.5	0.021...	$\mathbf{1.753... \cdot 10^{16}}$	$\mathbf{1.699... \cdot 10^{18}}$

Table 3.1: Examples of coherence, average coherence, orthogonality defect and product measure values for cyclotomic lattices

For comparison purposes, we also record here the values of coherence, average coherence, orthogonality defect and product measure for the standard irreducible root lattices. We start by briefly recalling some standard notation. A lattice is called *irreducible* if it is not a direct sum of nonzero sublattices. A *root* in a lattice is a vector of squared-norm equal to 2, and an irreducible lattice is called a *root lattice* if it is generated by its roots. In this case, the roots are the minimal vectors of the lattice. There are precisely two infinite families of irreducible root lattices, denoted A_n and D_n, as well as the three exceptional examples E_6, E_7 and E_8. We already defined A_n in (3.11), and now recall that

$$D_n = \left\{ \boldsymbol{x} \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \in 2\mathbb{Z} \right\}, \; E_8 = D_8 \cup \left\{ \frac{1}{2} \left(\sum_{i=1}^{8} \boldsymbol{e}_i \right) + D_8 \right\}, \tag{3.14}$$

where $\boldsymbol{e}_i$ are the standard basis vectors in the corresponding $\mathbb{Z}^n$. Additionally,

$$E_7 = \{ \boldsymbol{x} \in E_8 : \langle \boldsymbol{x}, \boldsymbol{e}_7 + \boldsymbol{e}_8 \rangle = 0 \}, \; E_6 = \{ \boldsymbol{x} \in E_7 : \langle \boldsymbol{x}, \boldsymbol{e}_6 + \boldsymbol{e}_8 \rangle = 0 \}. \tag{3.15}$$

We refer the reader to [49] (Chapter 4) or [19] (Chapter 4) for the detailed information on the properties of root lattices. We will mention that, due to the remarkable symmetry properties of root lattices, their minimal vectors are indistinguishable in the following sense. Let L be a root lattice. Then for each vector $\boldsymbol{x} \in S(L)$ there is the same number of vectors $\boldsymbol{y} \in S(L)$ that have nonzero inner product $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ ([49], Proposition 4.10.12). Standard integrality conditions limit the only other possible inner product value to $|\langle \boldsymbol{x}, \boldsymbol{y} \rangle| = 1$. With this in mind, the calculation of the average coherence of root lattices becomes straightforward, using Proposition 4.2.2 and Theorems 4.3.3, 4.4.4, 4.5.2 and 4.5.3 of [49]. The values held by the coherence, average coherence, orthogonality defect and product measure on the corresponding root lattices A_n for $n \geq 2$, D_n for $n \geq 4$, E_6, E_7, and E_8 are given in Table 3.2.

Lattice L	$\lvert S'(L)\rvert$	$\mathcal{C}(L)$	$\mathcal{A}(L)$	$\nu(L)$	$\Pi(L)$
A_n	$\frac{n(n+1)}{2}$	0.5	$\frac{2}{n+2}$	$\frac{2^{\frac{n}{2}}}{n+1}$	$(n+2)2^{\frac{n-4}{2}}$
D_n	$n(n-1)$	0.5	$\frac{2(n-2)}{n^2-n-1}$	$2^{\frac{n-4}{2}}$	$\frac{(n-1)(n^2-n-1)}{n-2}2^{\frac{n-6}{2}}$
E_6	36	0.5	$\frac{2}{7}$	$\frac{8}{3}$	56
E_7	63	0.5	$\frac{8}{31}$	$4\sqrt{2}$	13.138...
E_8	120	0.5	$\frac{28}{119}$	16	1020

Table 3.2: Coherence, average coherence, orthogonality defect and product measure values for root lattices

This data suggests that root lattices are generally better than cyclotomic lattices at simultaneously minimizing average coherence and maximizing orthogonality defect, but are worse at minimizing maximal coherence. Indeed, suppose some large p is the smallest prime dividing n and let $d = \phi(n)$, then $\Lambda_{\mathbb{Q}(\zeta_n)}$ is a lattice in $\mathbb{R}^d$ with maximal coherence $1/(p-1)$, while A_d and D_d are root lattices in the same dimension with maximal coherence $1/2$.

In fact, an interesting feature of the cyclotomic lattices, in contrast with the root lattices, is that their maximal and average coherence are about the same on the average as $n \to \infty$. Indeed, $\mathcal{C}_n = 1/(\eta(n) - 1)$, where $\eta(n)$ is the smallest prime divisor of n. Now, the average order of $\eta(n)$ is known to be $(1 + o(1))n/2\log n$ as $n \to \infty$ (see [39]). Hence the average order of $\mathcal{C}_n$ is $\frac{2\log n}{n}$. On the other hand, the average order of $\omega(n)$ is $\log\log n$ (see Theorem 430 of [37]). Combining this observation with (3.5), we see that the average order of $\mathcal{A}_n$ is $\frac{\log 2\log n}{n}$.

CHAPTER IV

Lemmas concerning average coherence

4.1 Some lemmas on average coherence

We feel we should note here a few lemmas about average coherence not used in any of the other chapters, but which may prove useful in future.[1] Recall that we define the *average coherence* of a lattice L to be

$$\mathcal{A}(L) := \frac{1}{|S'(L)| - 1} \cdot \max_{\boldsymbol{x} \in S'(L)} \left\{ \sum_{\boldsymbol{y} \in S'(L) \setminus \{\boldsymbol{x}\}} \frac{|(\boldsymbol{x}, \boldsymbol{y})|}{\|\boldsymbol{x}\| \|\boldsymbol{y}\|} \right\},$$

where $S'(L)$ is any half-set of $S(L)$ where just one of $\pm\boldsymbol{x} \in S(L)$ is taken to be in $S'(L)$.

Lemma 4.1.1. *Suppose lattice $L = L_1 \perp L_2$ is the orthogonal sum of two lattices $L_1 \in \mathbb{R}^{d_1}$ and $L_2 \in \mathbb{R}^{d_2}$ of equal minimal norm. Let $\mathcal{A}(L_1) = a_1, \mathcal{A}(L_2) = a_2, s(L_1) = n_1$, and $s(L_2) = n_2$. Then,*

$$\mathcal{A}(L) = \frac{1}{n_1 + n_2 - 1} \cdot \max\left\{a_1(n_1 - 1), a_2(n_2 - 1)\right\}.$$

Proof. It is clear that $\boldsymbol{x} \in L$ is a minimal vector of L if and only if its natural

[1] Although unused in chapter III, one may recover the formula for the average coherence of cyclotomic lattices using this; it is considerably less efficient and elegant than the formula presented in that chapter.

projection onto either L_1 or L_2 is a minimal vector of that lattice, and thus $|L| = |L_1| = |L_2|$. Let $\boldsymbol{x}_{1,i}$ and $\boldsymbol{x}_{2,j}$ be minimal vectors in L_1 and L_2, respectively, and let $\tilde{\boldsymbol{x}}_{1,i}$ and $\tilde{\boldsymbol{x}}_{2,j}$ be their natural embeddings into $\mathbb{R}^{d_1+d_2}$, i.e. $\tilde{\boldsymbol{x}}_{1,i} = (\boldsymbol{x}_{1,i}, 0, \ldots, 0)$ and $\tilde{\boldsymbol{x}}_{2,j} = (0, \ldots, 0, \boldsymbol{x}_{2,j})$. It is then clear from construction that $|(\tilde{\boldsymbol{x}}_{1,i}, \tilde{\boldsymbol{x}}_{2,j})| = 0$.

What this means is that, when computing inner products of minimal vectors, we need only look at ones "from" the same lattice L_1 or L_2, and so we may freely pull back from $\tilde{\boldsymbol{x}}_{k,i}$ to $\boldsymbol{x}_{k,i}$.

Thus

$$\mathcal{A}(L) = \frac{1}{n_1 + n_2 - 1} \cdot \max_k \left\{ \max_i \left\{ \sum_{j \neq i}^{n_k} \frac{|(\tilde{\boldsymbol{x}}_{k,i}, \tilde{\boldsymbol{x}}_{k,j})|}{|L|^2} \right\} \right\}.$$

Pulling back, this becomes

$$\mathcal{A}(L) = \frac{1}{n_1 + n_2 - 1} \cdot \max_k \left\{ \max_i \left\{ \sum_{j \neq i}^{n_k} \frac{|(\boldsymbol{x}_{k,i}, \boldsymbol{x}_{k,j})|}{|L|^2} \right\} \right\},$$

which is simply

$$\mathcal{A}(L) = \frac{1}{\sum n_i - 1} \cdot \max_k \{a_k(n_k - 1)\}.$$

□

In fact, it is clear from the proof that this seamlessly generalizes to the orthogonal sum of any number of lattices of equal minimal norm, leading immediately to the following corollary:

Corollary 4.1.2. *Suppose lattice $L = L_1 \perp \cdots \perp L_n$ is the orthogonal sum of n lattices $L_i \in \mathbb{R}^{d_i}$ of equal minimal norm. Let $\mathcal{A}(L_i) = a_i$ and $s(L_i) = n_i$. Then,*

$$\mathcal{A}(L) = \frac{1}{\sum_{i=1}^{i=n} n_i - 1} \cdot \max_i \{a_i(n_i - 1)\}.$$

Now consider the tensor product of lattices. Here, the picture is much more complicated. It is not always the case that $S(L_1 \otimes L_2) = \{x \otimes y : x \in S(L_1), y \in S(L_2)\}$,

and in fact due to a proposition of Coulangeon and Nebe [20], if all minimal vectors of $L_1 \otimes L_2$, $\text{rank}(L_1), \text{rank}(L_2) \geq 2$, are *split*, i.e. of the form $x \otimes y$ for $x \in L_1, y \in L_2$, then $L_1 \otimes L_2$ cannot be perfect, and hence cannot be extreme.

To the best of our knowledge, there is no general way to know even the size of minimal vectors in a tensor product. An unpublished theorem of Steinberg (see [54], theorem 9.6) says that for all dimensions $n \geq 292$ there exist unimodular lattices $L, M \in \mathbb{R}^n$ with $|L \otimes M| < |L| \cdot |M|$. However, Coulangeon and Nebe state they are unaware of any explicit example containing non-split minimal vectors.

Nevertheless, some lattices are amenable to an easy calculation. Kitaoka ([40], ch. 7) describes a family of lattices he called *E-type*, which admit a very nice formula.

Definition 4.1.1. A lattice L is of E-type if and only if

$$S(L \otimes M) \subset \{x \otimes y : x \in L, y \in M\}$$

for any lattice M.

In fact, Lemma 7.1.1 of [40], which for convenience we reproduce in relevant part, states that for an E-type lattice L, $S(L \otimes M) = S(L) \otimes S(M) = \{x \otimes y : x \in S(L), y \in S(M)\}$. In this case, then, a formula can be derived.

Lemma 4.1.3. (Kitaoka) *Let L, M be positive lattices. Then we have*

$$|L \otimes M| \leq |L| \cdot |M|$$

and if L is of E-type, then we have

$$|L \otimes M| = |L| \cdot |M|, S(L \otimes M) = S(L) \otimes S(M)$$

where $S(L) \otimes S(M)$ denotes $\{x \otimes y : x \in S(L), y \in S(M)\}$ for abbreviation.

Moreover we have that if L, M are of E-type, then $L \perp M$ and $L \otimes M$ are also of E-type.

Lemma 4.1.4. *Let L_1 be an E-type lattice as defined above, with minimal norm $|L_1|$ and average coherence $\mathcal{A}(L_1) = a_1$. Let L_2 be a lattice, not necessarily of E-type, of minimal norm $|L_2|$ and average coherence $\mathcal{A}(L_2) = a_2$, and let $L = L_1 \otimes L_2$ be their tensor product. Finally, let $s(L_1) = n_1$, and $s(L_2) = n_2$. Then:*

$$\mathcal{A}(L) = \frac{(a_1(n_1 - 1) + 1) \cdot (a_2(n_2 - 1) + 1) - 1}{n_1 n_2 - 1}.$$

Proof. $|S'(L)| = |S'(L_1)||S'(L_2)| = n_1 n_2$ (notice that "$S(L) \otimes S(M)$" counts $-x \otimes y$ and $x \otimes -y$ twice for the same vector, $-(x \otimes y)$). Then by definition

$$\mathcal{A}(L) = \frac{1}{|S'(L)| - 1} \cdot \max_i \left\{ \sum_{\boldsymbol{z}_k \in S'(L) \setminus \{\boldsymbol{z}_i\}} \frac{|(\boldsymbol{z}_i, \boldsymbol{z}_k)|}{|L_1|^2 |L_2|^2} \right\}.$$

However, all minimal vectors are split tensors, so $(x \otimes y, x' \otimes y') = (x, x') \cdot (y, y')$ and so

$$\mathcal{A}(L) = \frac{1}{|S'(L)| - 1} \cdot \max_{i,j} \left\{ \sum_{(m,n) \neq (i,j)} \frac{|(\boldsymbol{z}_{i,j}, \boldsymbol{z}_{m,n})|}{|L_1|^2 |L_2|^2} \right\}.$$

Splitting $\boldsymbol{z}_{i,j}$ to $\boldsymbol{z}_{i,j} = \boldsymbol{x}_i \otimes \boldsymbol{y}_j$ (where it is understood each $\boldsymbol{x}$ and $\boldsymbol{y}$ is a minimal vector of its respective lattice), we have

$$\mathcal{A}(L) = \frac{1}{|S'(L)| - 1} \cdot \max_{i,j} \left\{ \sum_{(m,n) \neq (i,j)} \frac{|(\boldsymbol{x}_i, \boldsymbol{x}_m) \cdot (\boldsymbol{y}_j, \boldsymbol{y}_n)|}{|L_1|^2 |L_2|^2} \right\}.$$

The double sum omitting only the case $(m, n) = (i, j)$ may be rewritten as

$$\mathcal{A}(L) = \frac{1}{|S'(L)| - 1} \cdot \max_{i,j} \left\{ \sum_{m=1}^{n_1} \sum_{n=1}^{n_2} \frac{|(\boldsymbol{x}_i, \boldsymbol{x}_m) \cdot (\boldsymbol{y}_j, \boldsymbol{y}_n)|}{|L_1|^2 |L_2|^2} - \frac{|(\boldsymbol{x}_i, \boldsymbol{x}_i) \cdot (\boldsymbol{y}_j, \boldsymbol{y}_j)|}{|L_1|^2 |L_2|^2} \right\}.$$

However, $(\boldsymbol{x}_i, \boldsymbol{x}_i) = |L_1|^2$ by definition, and similarly $(\boldsymbol{y}_j, \boldsymbol{y}_j) = |L_2|^2$. Thus, we have

$$\mathcal{A}(L) = \frac{1}{|S'(L)| - 1} \cdot \max_{i,j} \left\{ \sum_{m=1}^{n_1} \sum_{n=1}^{n_2} \frac{|(\boldsymbol{x}_i, \boldsymbol{x}_m) \cdot (\boldsymbol{y}_j, \boldsymbol{y}_n)|}{|L_1|^2 |L_2|^2} - 1 \right\}.$$

Because i and j are independent, we may examine each part of the numerator of the double sum separately, giving

$$\mathcal{A}(L) = \frac{1}{|S'(L)| - 1} \cdot \left(\max_{i} \left\{ \sum_{m=1}^{n_1} \frac{|(\boldsymbol{x}_i, \boldsymbol{x}_m)|}{|L_1|^2} \right\} \max_{j} \left\{ \sum_{n=1}^{n_2} \frac{|(\boldsymbol{y}_j, \boldsymbol{y}_n)|}{|L_2|^2} \right\} - 1 \right).$$

But

$$\max_{i} \left\{ \sum_{m=1}^{n_1} \frac{|(\boldsymbol{x}_i, \boldsymbol{x}_m)|}{|L_1|^2} \right\} = \max_{i} \left\{ \sum_{m \neq i} \frac{|(\boldsymbol{x}_i, \boldsymbol{x}_m)|}{|L_1|^2} + \frac{(\boldsymbol{x}_i, \boldsymbol{x}_i)}{|L_1|^2} \right\} = \mathcal{A}(L_1) \cdot (n_1 - 1) + 1$$

and the same manipulation shows

$$\max_{j} \left\{ \sum_{n=1}^{n_2} \frac{|(\boldsymbol{y}_j, \boldsymbol{y}_n)|}{|L_2|^2} \right\} = \max_{j} \left\{ \sum_{n \neq j} \frac{|(\boldsymbol{y}_j, \boldsymbol{y}_n)|}{|L_2|^2} + \frac{(\boldsymbol{y}_j, \boldsymbol{y}_j)}{|L_2|^2} \right\} = \mathcal{A}(L_2) \cdot (n_2 - 1) + 1$$

completing the proof.

□

The final part of lemma 4.1.3 leads to the following immediate corollary:

Corollary 4.1.5. *Suppose $L_1, \ldots, L_k$ are all E-type lattices with average coherence $\mathcal{A}(L_i) = a_i$ and $s(L_i) = n_i$. Then if $L = L_1 \otimes \cdots \otimes L_k$, L is an E-type lattice and we have*

$$\mathcal{A}(L) = \frac{\prod_{i=1}^{k} (a_i(n_i - 1) + 1) - 1}{\prod_{i=1}^{k} n_i - 1}$$

Proof. The result follows immediately from repeated application of Lemma 4.1.4. □

Consider now the product of sums and the sum of products. As before, we will make the assumption of E-type lattices within each tensor product.

Lemma 4.1.6. *Suppose lattice* $L = (L_{1,1} \otimes \cdots \otimes L_{1,k_1}) \perp \cdots \perp (L_{m,1} \otimes \cdots \otimes L_{m,k_m})$ *and suppose further that lattices* $L_{i,j}$ *are of E-type and that all lattices have been scaled such that each product has the same minimal norm, i.e.*

$$|(L_{1,1} \otimes \cdots \otimes L_{1,k_1})| = \cdots = |(L_{m,1} \otimes \cdots \otimes L_{m,k_m})|.$$

Letting $L'_i = L_{i,1} \otimes \cdots \otimes L_{i,k_i}$ *and, as in previous lemmas, letting* $n_{i,j} = s(L_{i,j})$, $a_{i,j} = \mathcal{A}(L_{i,j})$, $n'_i = s(L'_i)$, *and* $a'_i = \mathcal{A}(L'_i)$, *we have*

$$L = L'_1 \perp \cdots \perp L'_m.$$

Then

$$\mathcal{A}(L) = \frac{\max_i \{a'_i(n'_i - 1)\}}{\sum_{i=1}^m n'_i - 1} = \frac{\max_i \left\{\prod_{j=1}^{k_i}(a_{i,j}(n_{i,j} - 1) + 1) - 1\right\}}{\sum_{i=1}^m (\prod_{j=1}^{j=k_i} n_{i,j}) - 1}$$

Proof. By assumption, the L'_i have equal minimal norm. The compact version of the result is then immediate from Lemma 4.1.1. The expanded version comes from Corollary 4.1.5 applied to L'_i. □

Lemma 4.1.7. *Suppose lattice* $L = (L_{1,1} \perp \cdots \perp L_{1,k_1}) \otimes \cdots \otimes (L_{m,1} \perp \cdots \perp L_{m,k_m})$ *and suppose further that lattices* $L_{i,j}$ *are of E-type and have the same minimal norm. Letting* $L'_i = L_{i,1} \perp \cdots \perp L_{i,k_i}$ *and, as in previous lemmas, letting* $n_{i,j} = s(L_{i,j})$, $a_{i,j} = \mathcal{A}(L_{i,j})$, $n'_i = s(L'_i)$, *and* $a'_i = \mathcal{A}(L'_i)$, *we have*

$$L = L'_1 \otimes \cdots \otimes L'_m.$$

Then

$$\mathcal{A}(L) = \frac{\prod_{i=1}^m (a'_i(n'_i - 1) + 1) - 1}{\prod_{i=1}^m n'_i - 1} = \frac{\prod_{i=1}^m (\max_j \{a_{i,j}(n_{i,j} - 1)\} + 1) - 1}{\prod_{i=1}^m (\sum_{j=1}^{j=k_i} n_{i,j}) - 1}$$

Proof. By assumption, all lattices $L_{i,j}$ are of E-type; thus, by Lemma 4.1.3, all lattices L'_i are also of E-type. Corollary 4.1.5 then yields the compact version of the result. The expanded version comes from Lemma 4.1.1 applied to L'_i. □

CHAPTER V

Cyclic and well-rounded lattices

5.1 Introduction

Let $n \geq 2$, and write $\| \ \|$ for the Euclidean norm on $\mathbb{R}^n$. Let $L \subset \mathbb{R}^n$ be a lattice of rank n, and recall that its *minimum* is

$$|L| := \min \{\|\boldsymbol{x}\| : \boldsymbol{x} \in L \setminus \{\mathbf{0}\}\}.$$

Recall that the set of *minimal vectors* of L is

$$S(L) := \{\boldsymbol{x} \in L : \|\boldsymbol{x}\| = |L|\}.$$

Let us write $\mathbb{R}_+$ for the set of all positive real numbers and $\mathcal{O}_n(\mathbb{R})$ for the group of real orthogonal $n \times n$ matrices. We define the equivalence relation of *similarity* on lattices in $\mathbb{R}^n$ as follows: two lattices L_1 and L_2 are called *similar*, denoted $L_1 \sim L_2$, if there exists $\alpha \in \mathbb{R}_+$ and $U \in \mathcal{O}_n(\mathbb{R})$ such that $L_2 = \alpha U L_1$. This is an equivalence relation on the space of lattices in $\mathbb{R}^n$, and we will write $\langle L \rangle$ for the similarity class of L.

*This chapter is based on joint work with Lenny Fukshansky, published as [32], first published in *Moscow Journal of Combinatorics and Number Theory* in 2022, published by Mathematical Sciences Publishers.

Recall that L is *well-rounded* (WR) if $\operatorname{span}_{\mathbb{R}} S(L) = \operatorname{span}_{\mathbb{R}} L$. We can further define L to be *generated by its minimal vectors* if $L = \operatorname{span}_{\mathbb{Z}} S(L)$, and we say L *has a basis of minimal vectors* if $S(L)$ contains a basis for L. Notice that $S(L_1)$ is taken to $S(L_2)$ under similarity, and hence these conditions are preserved. Thus we write WR_n for the set of similarity classes of WR lattices in $\mathbb{R}^n$, WR'_n for the set of similarity classes generated by minimal vectors, and WR''_n for the set of similarity classes having a basis of minimal vectors. Then

$$\mathrm{WR}''_n \subseteq \mathrm{WR}'_n \subseteq \mathrm{WR}_n,$$

where the first containment is known to be proper for all $n \geq 10$ ([50]; see also [18]) and the second containment is proper for all $n \geq 5$ (see Example 1). WR lattices are central objects in lattice theory and discrete optimization; see [49] for many more details, as well as [51].

A lattice $L \subset \mathbb{R}^n$ of rank k can be written as $L = B\mathbb{Z}^k$, where $1 \leq k \leq n$ and B is an $n \times k$ basis matrix of rank k. The *determinant* of L is then defined as

$$\det(L) = \sqrt{\det(B^\top B)}.$$

A lattice L is called *semi-stable* if for any sublattice M of rank $1 \leq k \leq n$,

$$\det(L)^{1/n} \leq \det(M)^{1/k},$$

and L is called *stable* if this inequality is strict for all $M \neq L$. The stability condition is again preserved under similarity, and we write St_n for the set of semi-stable similarity classes in $\mathbb{R}^n$. Semi-stable lattices, alongside well-rounded lattices, are of great interest in lattice theory and reduction theory (see [11] and [62]).

There is another interesting class of lattices we would like to introduce. A lattice

$L \subset \mathbb{R}^n$, not necessarily of full rank, is called *cyclic* in $\mathbb{R}^n$ if it closed under the rotation shift linear operator $\rho : \mathbb{R}^n \to \mathbb{R}^n$, given by

$$\rho(c_1, c_2, \ldots, c_n) = (c_n, c_1, \ldots, c_{n-1}), \tag{5.1}$$

i.e. if $\rho(L) = L$. This property is not preserved under similarity: indeed, the integer lattice $\mathbb{Z}^2$ is cyclic and is similar to $\begin{pmatrix} 1 & -a \\ a & 1 \end{pmatrix} \mathbb{Z}^2$, which is not cyclic for any irrational a. On the other hand, a full-rank lattice $L \subset \mathbb{R}^n$ is similar to a cyclic lattice if and only if L has an isometry with minimal polynomial $x^n - 1$. Cyclic lattices have been especially studied in the context of lattice-based cryptography, e.g. [52], [59].

Reduction theory aims to specify some "canonical" choice of representatives of similarity classes, and from this point of view it is interesting to understand the relation between the classes of lattices defined above. In general, these conditions on lattices are independent: stable lattices do not need to be well-rounded, and there are families of well-rounded nearly orthogonal lattices that are not semi-stable (see Lemma 1.1 of [27]). Further, well-rounded lattices are also not necessarily nearly-orthogonal (see Chapter II in general). The situation, however, is much simpler in dimension two: here we have the following chain of inclusions:

$$\mathrm{WR}_2'' = \mathrm{WR}_2' = \mathrm{WR}_2 = \mathcal{W}_2^* = \mathcal{W}_2 \subsetneq \mathrm{St}_2 \,.$$

One can ask where cyclic lattices fit in this picture. This is our first observation.

Theorem 5.1.1. *Every WR lattice $L \subset \mathbb{R}^2$ is similar to a unique cyclic lattice*

$$M(x) = \begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix} \mathbb{Z}^2 \tag{5.2}$$

with $x \in [0, 2-\sqrt{3}]$. *Further, if* $K \subseteq \mathbb{R}$ *is a subfield such that* $L \subset K^2$, *then* $x \in K$.

We prove Theorem 5.1.1 in Section 5.2, where our main tool is the circulant preconditioner for arbitrary matrices originally defined by Tony Chan [12] in the context of certain numerical linear optimization problems. Notice, on the other hand, that the converse of Theorem 5.1.1 is not true: not all cyclic lattices in the plane are WR. In fact, not all of them are even stable: for instance, the cyclic lattice $\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \mathbb{Z}^2$ is not stable.

Using Theorem 5.1.1, for each WR lattice $L \subset \mathbb{R}^2$, let $x_L \in [0, 2-\sqrt{3}]$ be the unique real number so that $L \sim M(x_L)$ as in (5.2). This description of similarity classes allows for a way to count them. Given a real number field K, we will say that a lattice $L \subset \mathbb{R}^2$ is *defined over* K if $L \subset K^2$. Further, we say that a similarity class is defined over K if it contains a lattice defined over K. Theorem 5.1.1 guarantees that if a well-rounded lattice L is defined over K, then so is $M(x_L)$. Then WR similarity classes defined over K are precisely those containing $M(x)$ as in (5.2) with $x \in K$. We can define the height of a similarity class $\langle L \rangle$ defined over K to be the Weil height of x_L, denoted $H(\langle L \rangle)$. With this notation, we can prove the following estimate.

Theorem 5.1.2. *Let* K *be a real number field of degree* d, *then for any* $T \geq 1$,

$$|\{\langle L \rangle \text{ defined over } K : H(\langle L \rangle) \leq T\}| \leq \frac{\pi}{2\sqrt{12}} \left(1 + 4^{2(d+1)} \left(2+\sqrt{3}\right)^d T^{2d}\right).$$

We review all the necessary notation of height functions and prove Theorem 5.1.2 in Section 5.3. Our main tool there is a counting estimate for algebraic numbers of bounded height due to Loher and Masser([44]). Notice that introducing the height machinery allows for explicit counting: any set of points of explicitly bounded height over a fixed number field is necessarily finite by Northcott's theorem ([57]). Indeed, our approach here is different from some previous counting estimates on planar well-

rounded lattices, where the lattices in question would be taken to be sublattices of a fixed lattice in the plane and counted with respect to index (see [23], [24], [26], [34], [3], [42]). Instead, we are counting *all* similarity classes defined over a fixed number field. In contrast, arithmetic similarity classes of well-rounded lattices have been counted with respect to a somewhat differently defined height in [28]: these lattices are defined over quadratic number fields. We compare the estimate obtained in [28] with our Theorem 5.1.2 in Section 5.3.

In higher dimensions well-rounded lattices cannot be so nicely parameterized by cyclic ones (Lemma 5.2.2). This being said, there are plenty of important lattices that are cyclic. Indeed, the condition that a lattice L of rank n is cyclic is equivalent to the condition that $\mathrm{Aut}(L)$, the automorphism group of L, contains the permutation matrix corresponding to the standard n-cycle $(1 \dots n)$, which is not trivial (for a generic lattice $\mathrm{Aut}(L) = \{\pm I_n\}$), and lattices with large automorphism groups are of special interest in lattice theory and the arithmetic theory of quadratic forms. We distinguish a special subclass of cyclic lattices: we will say that a lattice L of rank n is *simple cyclic* if there exists $\boldsymbol{a} \in L$ so that

$$L = \Lambda(\boldsymbol{a}) := \mathrm{span}_{\mathbb{Z}} \left\{ \boldsymbol{a}, \rho(\boldsymbol{a}), \dots, \rho^{n-1}(\boldsymbol{a}) \right\},$$

i.e. simple cyclic lattices are generated by the rotation shifts of a single vector. We discuss basic properties of cyclic lattices in more details in Section 5.4. In Section 5.5 we prove the following observation on the cyclic properties of the root lattices.

Theorem 5.1.3. *The following statements hold for the root lattices and their duals:*

1. *For every $n \geq 2$, the root lattice A_n and its dual A_n^* are both simple cyclic lattices of rank n in $\mathbb{R}^{n+1}$.*

2. *For every $n \geq 2$, the root lattice D_n and its dual D_n^* are both cyclic of full rank in $\mathbb{R}^n$. Further, D_n and D_n^* are simple cyclic if and only if n is odd.*

3. *The self-dual root lattice E_8 is cyclic, but not simple cyclic, in $\mathbb{R}^8$.*

4. *The root lattices E_6, E_7 are non-cyclic sublattices of E_8 in $\mathbb{R}^8$.*

We briefly recall the definitions and necessary properties of the classical root lattices in Section 5.5 before proving Theorem 5.1.3 in a series of lemmas. Finally, in Section 5.6 we focus on lattices coming from rings of integers of Galois number fields. We prove the following result, where the lattices in question are viewed as cyclic under the rotational shift operator as in (5.1), but on $\mathbb{C}^n$ instead of $\mathbb{R}^n$.

Theorem 5.1.4. *Let K be a Galois number field and Λ_K be the lattice coming from the ring of integers $\mathcal{O}_K$ via a standard embedding into $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R} \subseteq \mathbb{C}^d$. Then Λ_K is cyclic in $\mathbb{C}^d$ if and only if $K/\mathbb{Q}$ is a cyclic extension. Further, it is simple cyclic if and only if $K/\mathbb{Q}$ is tamely ramified. In particular, a cyclotomic lattice $\Lambda_{\mathbb{Q}(\zeta_n)}$ with $\zeta_n = e^{2\pi i/n}$ is cyclic if and only if $n = 2, 4, p^k$, or $2p^k$ for an odd prime p and integer $k \geq 1$, and it is simple cyclic if and only if $n = 2, p$, or $2p$.*

We recall all the necessary number field notation in Section 5.6. Further, we comment on well-roundness properties of such cyclic lattices Λ_K and discuss some non-cyclotomic examples (Remark 5.6.1). We are now ready to proceed.

5.2 Approximations by circulant matrices

In this section we define circulant approximation to a matrix and use it to prove Theorem 5.1.1. For an $n \times n$ real matrix A, write $\|A\|$ for its Frobenius norm, i.e. the Euclidean norm of A viewed as a vector in $\mathbb{R}^{n^2}$. Let $\langle\ ,\ \rangle$ stand for the corresponding

inner product on vectors and on matrices. For each vector $\boldsymbol{c} = (c_1, \ldots, c_n) \in \mathbb{R}^n$, let

$$\mathrm{P}(\boldsymbol{c}) = \begin{pmatrix} c_1 & c_2 & \ldots & c_n \\ c_n & c_1 & \ldots & c_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ c_2 & c_3 & \ldots & c_1 \end{pmatrix} \tag{5.3}$$

be the corresponding $n \times n$ circulant matrix. Let

$$\Pi_n = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{pmatrix}$$

be a permutation matrix of order n. Then Π_n^k for $0 \leq k \leq n-1$ is also a permutation matrix.

We can now define a circulant approximation to an $n \times n$ matrix A (also called a circulant preconditioner), as in [12], [14], by $\mathrm{P}(A) := \mathrm{P}(c_1, \ldots, c_n)$, where

$$c_k = \frac{1}{n} \left\langle A, \Pi_n^{k-1} \right\rangle,$$

for each $1 \leq k \leq n$; in other words, each entry c_k of this circulant matrix is the average of the corresponding diagonal of A wrapped around to extend to full length. This circulant approximation $\mathrm{P}(A)$ was introduced by T. Chan [12], who showed that it minimizes $\|A - C\|$ among all circulant matrices C.

Let $L \subset \mathbb{R}^n$ be a full-rank lattice with a basis $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$. Write $A = (\boldsymbol{a}_1 \ \ldots \ \boldsymbol{a}_n)$ for the corresponding basis matrix. Define $\mathrm{P}_A(L) = \mathrm{P}(A^\top)^\top \mathbb{Z}^n$ to be the corresponding cyclic lattice, which we call a *cyclic approximation* to L. Let us consider this

construction for $n = 2$, in which case $L = A\mathbb{Z}^2$, where

$$A = (\boldsymbol{a}_1\ \boldsymbol{a}_2) = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}, \text{ and so } \mathrm{P}_A(L) = \frac{1}{2}\begin{pmatrix} a_{11}+a_{22} & a_{12}+a_{21} \\ a_{12}+a_{21} & a_{11}+a_{22} \end{pmatrix}\mathbb{Z}^2. \quad (5.4)$$

We can assume that at least one of $a_{11} + a_{22}$, $a_{12} + a_{21}$ is nonzero: if both of them are, replace $\boldsymbol{a}_1$ with $-\boldsymbol{a}_1$ (or $\boldsymbol{a}_2$ with $-\boldsymbol{a}_2$).

Lemma 5.2.1. *Suppose that $L \subset \mathbb{R}^2$ is well-rounded and A is a minimal basis matrix. Then L is similar to $\mathrm{P}_A(L)$.*

Proof. Assuming A as above is a minimal basis matrix is equivalent to saying that

$$\|\boldsymbol{a}_1\|^2 = a_{11}^2 + a_{12}^2 = a_{21}^2 + a_{22}^2 = \|\boldsymbol{a}_2\|^2, \quad (5.5)$$

and cosine of the angle $\theta(\boldsymbol{a}_1, \boldsymbol{a}_2)$ between $\boldsymbol{a}_1$ and $\boldsymbol{a}_2$ satisfies

$$|\cos\theta(\boldsymbol{a}_1, \boldsymbol{a}_2)| = \frac{|\langle\, \boldsymbol{a}_1, \boldsymbol{a}_2\rangle\,|}{\|\boldsymbol{a}_1\|\|\boldsymbol{a}_2\|} = \frac{|a_{11}a_{21} + a_{12}a_{22}|}{a_{11}^2 + a_{12}^2} \le \frac{1}{2}.$$

Let us write

$$B = (\boldsymbol{b}_1\ \boldsymbol{b}_2) = \begin{pmatrix} a_{11}+a_{22} & a_{12}+a_{21} \\ a_{12}+a_{21} & a_{11}+a_{22} \end{pmatrix},$$

so $\mathrm{P}_A(L) = \frac{1}{2}B\mathbb{Z}^2$. Clearly $\|\boldsymbol{b}_1\| = \|\boldsymbol{b}_2\|$, and so L is similar to $\mathrm{P}_A(L)$ if and only if

$$|\cos\theta(\boldsymbol{a}_1, \boldsymbol{a}_2)| = |\cos\theta(\boldsymbol{b}_1, \boldsymbol{b}_2)|.$$

Observe a basic algebraic identity for any four real numbers p, q, s, t:

$$\frac{p+q}{s+t} = \frac{p}{s} \text{ if and only if } pt = qs. \quad (5.6)$$

Using (5.6) along with (5.5), we notice that

$$\begin{aligned}\cos\theta(\boldsymbol{b}_1,\boldsymbol{b}_2) &= \frac{2(a_{11}+a_{22})(a_{12}+a_{21})}{(a_{11}+a_{22})^2+(a_{12}+a_{21})^2} \\ &= \frac{(a_{11}a_{21}+a_{12}a_{22})+(a_{11}a_{12}+a_{21}a_{22})}{(a_{11}^2+a_{12}^2)+(a_{11}a_{22}+a_{12}a_{21})} = \cos\theta(\boldsymbol{a}_1,\boldsymbol{a}_2),\end{aligned}$$

because

$$(a_{11}a_{21}+a_{12}a_{22})(a_{11}a_{22}+a_{12}a_{21}) = (a_{11}a_{12}+a_{21}a_{22})(a_{11}^2+a_{12}^2).$$

Hence L is similar to $\mathrm{P}_A(L)$. □

Proof of Theorem 5.1.1. Write $L = A\mathbb{Z}^2$ as in (5.4), then by Lemma 5.2.1, L is similar to $\mathrm{P}_A(L)$ as in (5.4). Notice that

$$(a_{11}+a_{22})(a_{12}+a_{21}) = 0 \tag{5.7}$$

if and only if $\mathrm{P}_A(L)$ is similar to $\mathbb{Z}^2$, which is precisely $M(x)$ as in (5.2) with $x = 0$. On the other hand, (5.7) does not hold if and only if $\mathrm{P}_A(L)$ is similar to $M(x)$ with

$$x = \frac{a_{12}+a_{21}}{a_{11}+a_{22}}. \tag{5.8}$$

Suppose now that $x \neq y$ are such that

$$\begin{pmatrix} 1 & x \\ x & 1 \end{pmatrix}, \begin{pmatrix} 1 & y \\ y & 1 \end{pmatrix}$$

are minimal basis matrices for $M(x)$ and $M(y)$, respectively, and $M(x)$ is similar to $M(y)$. Then absolute values of cosines of the angles between these minimal basis

vectors are equal and $\leq 1/2$, in particular

$$\frac{2|x|}{x^2+1} = \frac{2|y|}{y^2+1}.$$

This is true if and only if $y = -x$ or $y = \pm 1/x$. Hence, to ensure uniqueness, we can take $0 < x \leq 1$. Additionally, we need

$$\frac{2x}{x^2+1} \leq \frac{1}{2},$$

which means $0 < x \leq 2 - \sqrt{3}$. Combining this with the case $x = 0$ completes the proof of the first part of the theorem. The second part follows from the fact that x is given by either $\pm$ the expression in (5.8) or its inverse, which therefore lies in the same field that contains a_{ij}'s. □

Remark 5.2.1. There is a standard parameterization of well-rounded similarity classes in the plane by lattices of the form

$$\Lambda(a,b) = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mathbb{Z}^2,$$

where $0 \leq a \leq 1/2$ with $a^2 + b^2 = 1$ (see, for instance, [28]). However, if a lattice L is similar to some such $\Lambda(a,b)$, they are not necessarily defined over the same field, unlike the parameterization of our Theorem 5.1.1.

Our observations above imply, in particular, that in $\mathbb{R}^2$ well-rounded lattices are always similar to cyclic lattices. Unsurprisingly, this is not true in higher dimensions.

Lemma 5.2.2. *A well-rounded lattice of rank ≥ 3 is not necessarily similar to a cyclic lattice.*

Proof. We can give a simple dimensional argument. First, consider the set WR''_n, i.e. similarity classes of WR lattices with a basis of minimal vectors. For all $n \geq 2$, the

set WR_n'' is determined by $n \times n$ matrices $A = (a_{ij})$ with

$$a_{11} = 1,\ a_{21} = \cdots = a_{n1} = 0,\ \sum_{j=1}^{n} a_{ij}^2 = 1\ \forall\ 2 \leq i \leq n,$$

also satisfying some inequalities. Since inequalities do not reduce the dimension, this space has dimension

$$n^2 - n - (n-1) = (n-1)^2.$$

Of course, for $n \geq 5$, $\mathrm{WR}_n'' \neq \mathrm{WR}_n$, however each WR lattice L has only finitely many sublattices with a basis consisting of some minimal vectors of L, and each WR lattice with a basis of minimal vectors is contained in only finitely many WR lattices with these vectors among the minimal (see [48]). Hence, the sets WR_n and WR_n'' have the same dimension.

On the other hand, the space of similarity classes of cyclic lattices in $\mathbb{R}^n$ is determined by $n \times n$ matrices $A = (a_{ij})$ with

$$a_{11} = 1,\ a_{ij} = \rho^j(a_{i1})\ \forall\ 2 \leq i \leq n.$$

This space has dimension

$$n - 1 < (n-1)^2\ \forall\ n \geq 3.$$

Thus the space of WR similarity classes is too big to be parameterized by cyclic lattices. Notice, however, that when $n = 2$ these dimensions coincide. □

5.3 Counting WR similarity classes

Let K be a number field of degree $d := [K : \mathbb{Q}] \geq 1$. We write

$$M(K) = M_\infty(K) \cup M_f(K),$$

for the set of places of K, split into the subsets $M_\infty(K)$ of archimedean and $M_f(K)$ of non-archimedean places. The archimedean places correspond to the embeddings

$$\sigma_1, \ldots, \sigma_d : K \hookrightarrow \mathbb{C}$$

of K as usual: $M_\infty(K) = \{v : v = v(\sigma_i) \text{ for some } 1 \leq i \leq d\}$, where for each $1 \leq i \leq d$ and $x \in K$,

$$|x|_{v(\sigma_i)} = |\sigma_i(x)| = |\bar{\sigma}_i(x)| = |x|_{v(\bar{\sigma}_i)}$$

since complex conjugate embeddings give rise to the same place (we regard places in $M_\infty(K)$ without repetition). We order the embeddings so that σ_1 extends to the identity map on $\mathbb{C}$ and so $v_1 = v(\sigma_1)$ is the place corresponding to it. For each $v \in M(K)$ let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree, then for each $u \in M(\mathbb{Q})$, $\sum_{v|u} d_v = d$. We normalize the absolute values so that for each nonzero $x \in K$ the product formula reads

$$\prod_{v \in M(K)} |x|_v^{d_v} = 1.$$

Let $n \geq 2$, and for any place $v \in M(K)$ and $\boldsymbol{x} = (x_1, \ldots, x_n) \in K^n$ we define the corresponding sup-norm $|\boldsymbol{x}|_v = \max\{|x_1|_v, \ldots, |x_n|_v\}$. Then the height $H : K^n \to \mathbb{R}_{\geq 0}$ is given by

$$H(\boldsymbol{x}) = \prod_{v \in M(K)} |\boldsymbol{x}|_v^{\frac{d_v}{d}}.$$

The Weil height $h : K \to \mathbb{R}_{\geq 1}$ is then defined by $h(x) = H(1, x)$. This height is absolute, meaning that $H(\boldsymbol{x})$ is the same when computed over any number field K containing the coordinates of $\boldsymbol{x}$: this is due to the normalizing exponent $1/d$ in the definition.

We also define local and "anti-local" heights following [44]. Let $\boldsymbol{x} \in \overline{\mathbb{Q}}^n$ and let K' be an extension of K containing the coordinates of $\boldsymbol{x}$. For each archimedean $v \in M(K)$, define

$$H_v(\boldsymbol{x}) = \prod_{w \in M(K'), w|v} |\boldsymbol{x}|_w^{\frac{d_w}{[K':\mathbb{Q}]}}, \; H^v(\boldsymbol{x}) = \prod_{w \in M(K'), w \nmid v} |\boldsymbol{x}|_w^{\frac{d_w}{[K':\mathbb{Q}]}},$$

so that $H(\boldsymbol{x}) = H_v(\boldsymbol{x})H^v(\boldsymbol{x})$.

Lemma 5.3.1. *Let K be a number field of degree d and $\alpha \in \overline{\mathbb{Q}}$. Let $K' = K(\alpha)$ and let $u \in M_\infty(K)$. For real $T \geq 1$, define*

$$S_K(\alpha, T) = \{x \in K : |x|_u \leq |\alpha|_u, h(x) \leq T\}.$$

Then

$$|S_K(\alpha, T)| \leq \frac{\pi}{\sqrt{12}} \left(1 + 4^{2(d+1)}(Th(\alpha))^{2d}\right).$$

Proof. Define

$$S'_K(\alpha, T) = \{x \in K : |x|_u \leq |\alpha|_u, H(\alpha, x) \leq T\},$$

and notice that for $x \in S_K(\alpha, T)$, we have

$$Th(\alpha) \geq h(x)h(\alpha) \geq H(\alpha, x),$$

which means that $|S_K(\alpha, T)| \leq |S'_K(\alpha, Th(\alpha))|$. Notice that

$$H(\alpha, x) = H_u(\alpha, x)H^u(\alpha, x),$$

and so

$$\begin{aligned} |x|_u \leq |\alpha|_u \Leftrightarrow H_u(\alpha, x) &= \prod_{w \in M(K'), w|u} \max\{|\alpha|_w, |x|_w\}^{\frac{d_w}{[K':\mathbb{Q}]}} \\ &\leq |\alpha|_u^{\frac{1}{[K':\mathbb{Q}]} \sum_{w|u} d_w} = |\alpha|_u^{\frac{[K':K]}{[K':\mathbb{Q}]}} = H_u(\alpha). \end{aligned}$$

Hence

$$S'_K(\alpha, Th(\alpha)) = \{x \in K : H_u(\alpha, x) \leq H_u(\alpha), H(\alpha, x) \leq Th(\alpha)\},$$

and so if

$$H_u(\alpha, x) \leq H_u(\alpha),\ H^u(\alpha, x) \leq Th(\alpha) H^u(\alpha), \tag{5.9}$$

then $x \in S'_K(\alpha, Th(\alpha))$, since $H(\alpha) = H^u(\alpha)H^u(\alpha) = 1$ by the product formula. Let $N_K(\alpha, T)$ be the number of elements $x \in K$ satisfying conditions (5.9), then

$$|S_K(\alpha, T)| \leq |S'_K(\alpha, Th(\alpha))| \leq N_K(\alpha, T),$$

and by the Proposition in Section 3 of [44],

$$N_K(\alpha, T) \leq \frac{\pi}{\sqrt{12}} \left(1 + 4^{2(d+1)} (Th(\alpha))^{2d}\right).$$

This completes the proof of the lemma. □

Proof of Theorem 5.1.2. By Theorem 5.1.1,

$$|\{\langle L \rangle \text{ defined over } K : H(\langle L \rangle) \leq T\}| = \frac{1}{2} \left| \left\{ x \in K : |x|_{v_1} \leq 2 - \sqrt{3}, h(x) \leq T \right\} \right|,$$

where $1/2$ accounts for the fact that we are only considering positive x. The theorem

then follows from Lemma 5.3.1 combined with the fact that

$$\begin{aligned} h(2-\sqrt{3}) &= \prod_{v\in M(\mathbb{Q}(\sqrt{3}))} \max\left\{1, |2-\sqrt{3}|_v\right\}^{d_v/2} = \prod_{v|\infty} \max\left\{1, |2-\sqrt{3}|_v\right\}^{1/2} \\ &= \max\left\{1, 2-\sqrt{3}\right\}^{1/2} \max\left\{1, 2+\sqrt{3}\right\}^{1/2} = \sqrt{2+\sqrt{3}}. \end{aligned}$$

□

Remark 5.3.1. We can compare the estimate of Theorem 5.1.2 in the case where K is a quadratic number field to the estimate obtained in [28]. As indicated in [28], an arithmetic well-rounded lattice in the plane is of the form

$$L(a,b) = \begin{pmatrix} 1 & \frac{a}{b} \\ 0 & \frac{\sqrt{b^2-a^2}}{b} \end{pmatrix} \mathbb{Z}^2,$$

where $a, b \in \mathbb{Z}$ are relatively prime with $0 < a \leq b/2$, or $a = 0, b = 1$. These are precisely the WR lattices similar to those with integer-valued quadratic norm forms. Such a lattice $L(a,b)$ is similar to the cyclic lattice $M(x)$ as in (5.2) with

$$x = \frac{a}{\sqrt{b^2-a^2}+b}. \tag{5.10}$$

Notice that for x as in (5.10), $h(x)$ is of the order of magnitude $O(\sqrt{b})$. Then bounding b by T, the upper bound of our Theorem 5.1.2 grows like $O(T^2)$, which is consistent with the growth order of $N_3(T)$ in Theorem 1.1 of [28]. On the other hand, $N_3(T)$ counts *all* arithmetic lattices with $b \leq T$, whereas our Theorem 5.1.2 counts only those defined over a fixed number field. The difference, however, is that the set of WR lattices defined over a fixed quadratic field is far more general than those corresponding to x as in (5.10), i.e. not nearly all of them are arithmetic. For

instance, the WR lattices

$$\begin{pmatrix} 1 & \frac{1}{\sqrt{5}} \\ 0 & \frac{2}{\sqrt{5}} \end{pmatrix} \mathbb{Z}^2 \sim \begin{pmatrix} 1 & \frac{1}{2+\sqrt{5}} \\ \frac{1}{2+\sqrt{5}} & 1 \end{pmatrix} \mathbb{Z}^2$$

are defined over $\mathbb{Q}(\sqrt{5})$, but are not arithmetic.

5.4 Cyclic lattices

In this section we discuss some basic properties of cyclic lattices. Let $\boldsymbol{c} \in \mathbb{R}^n$ be a nonzero vector and $\mathrm{P}(\boldsymbol{c})$ be the corresponding circulant matrix as in (5.3). Let us write

$$\boldsymbol{c}(x) = \sum_{k=1}^{n} c_k x^{k-1} \tag{5.11}$$

for the polynomial of degree $n-1$ with $\boldsymbol{c}$ as its coefficient vector. It is a well-known fact that

$$\det \mathrm{P}(\boldsymbol{c}) = \prod_{j=1}^{n} \boldsymbol{c}(\omega_n^j), \tag{5.12}$$

where ω_n is a primitive n-th root of unity. Therefore $\mathrm{P}(\boldsymbol{c})$ is singular if and only if $\boldsymbol{c}(x)$ is divisible by some cyclotomic polynomial $\Phi_d(x)$ for $d \mid n$. Otherwise, the simple cyclic lattice $\Lambda(\boldsymbol{c}) = \mathrm{P}(\boldsymbol{c})^\top \mathbb{Z}^n$ has full rank.

Lemma 5.4.1. *A full-rank lattice $L \subset \mathbb{R}^n$ is cyclic if and only if its dual L^* is cyclic. Further, L is simple cyclic if and only if L^* is simple cyclic.*

Proof. Recall that

$$L^* = \{\boldsymbol{x} \in \mathbb{R}^n : \langle \boldsymbol{x}, \boldsymbol{y} \rangle \in \mathbb{Z} \ \forall \ \boldsymbol{y} \in L\}.$$

Assume that L is cyclic. Let $\boldsymbol{x} \in L^*$ and $\boldsymbol{y} \in L$, then

$$\langle \rho(\boldsymbol{x}), \boldsymbol{y} \rangle = x_n y_1 + x_1 y_2 + x_2 y_3 + \cdots + x_{n-1} y_n = \left\langle \boldsymbol{x}, \rho^{-1}(\boldsymbol{y}) \right\rangle \in \mathbb{Z},$$

since $\rho^{-1}(\boldsymbol{y}) = \rho^{n-1}(\boldsymbol{y}) \in L$. Thus $\rho(\boldsymbol{x}) \in L^*$ for every $\boldsymbol{x} \in L^*$, hence L^* is cyclic. Conversely, suppose L^* is cyclic, then $L = (L^*)^*$ is cyclic by the argument above.

Now suppose L is simple cyclic. Then $L = \mathrm{P}(\boldsymbol{c})^\top \mathbb{Z}^n$ for some $\boldsymbol{c} \in L$, and so

$$L^* = \left(\mathrm{P}(\boldsymbol{c})^\top\right)^{-\top} \mathbb{Z}^n = \mathrm{P}(\boldsymbol{c})^{-1} \mathbb{Z}^n.$$

Since the transpose and inverse of a circulant matrix are both also circulant, we can conclude that L^* has a circulant basis matrix, and hence L^* is also simple cyclic. Conversely, if L^* is simple cyclic, then $L = (L^*)^*$ is simple cyclic by the argument above. □

Cyclic sublattices of $\mathbb{Z}^n$ can be constructed algebraically. Indeed, let R_n be the quotient ring $\mathbb{Z}[x]/\langle x^n - 1\rangle$ and define a map $\phi : R_n \to \mathbb{Z}^n$ that sends a polynomial $\boldsymbol{c}(x) = \sum_{k=1}^n c_k x^{k-1} \in R_n$ to its vector of coefficients $\boldsymbol{c} \in \mathbb{Z}^n$. The map ϕ is a free $\mathbb{Z}$-module isomorphism, which maps ideals in R_n to sublattices in $\mathbb{Z}^n$. In fact, a sublattice $L \subseteq \mathbb{Z}^n$ is cyclic if and only if $L = \phi(I)$ for some ideal $I \subseteq R_n$: the cyclic rotation operator ρ on $\mathbb{Z}^n$ corresponds to multiplication by x in R_n, i.e.,

$$\phi(x\boldsymbol{c}(x)) = \rho(\boldsymbol{c}).$$

Further details on cyclic sublattices of $\mathbb{Z}^n$ that were extensively studied in the context of lattice cryptography can be found in [52] and [59]. In fact, cyclic sublattices of $\mathbb{Z}^n$ are a special case of the more general class of ideal lattices from quotient polynomial rings (see [46] and [22] for more details on these). The following simple observation will be useful to us (see also Propositions 2.1 and 2.2 of [22]). We provide a proof here for self-containment.

Lemma 5.4.2. *Let $I = \langle \boldsymbol{c}(x)\rangle$ be an ideal in $R_n = \mathbb{Z}[x]/\langle x^n - 1\rangle$. Then $\phi(I) = \Lambda(\boldsymbol{c}) \subseteq \mathbb{Z}^n$ has full rank if and only if $\boldsymbol{c}(x)$ is not a zero-divisor in R.*

Proof. The polynomial $\boldsymbol{c}(x)$ is not a zero-divisor in R_n if and only if for any nonzero $\boldsymbol{a}(x) = \sum_{k=0}^{n} a_k x^{k-1} \in R_n$,

$$\boldsymbol{a}(x)\boldsymbol{c}(x) = \sum_{k=1}^{n} a_k x^{k-1} \boldsymbol{c}(x) \neq 0.$$

This is equivalent to the statement that

$$\sum_{k=1}^{n} a_k \rho^{k-1}(\boldsymbol{c}) \neq \mathbf{0}$$

in $\Lambda(\boldsymbol{c}) = \phi(I)$, i.e. $\boldsymbol{c}, \rho(\boldsymbol{c}), \ldots, \rho^{n-1}(\boldsymbol{c})$ are linearly independent, meaning that $\Lambda(\boldsymbol{c})$ has full rank. □

Lemma 5.4.3. *A full-rank sublattice $L \subseteq \mathbb{Z}^n$ is simple cyclic if and only if $L = \phi(I)$ where $I \subseteq R_n$ is a principal ideal such that the quotient ring R_n/I is finite.*

Proof. A sublattice $L \subseteq \mathbb{Z}^n$ is cyclic if and only if $L = \phi(I)$ for some ideal $I \subseteq R_n$ and

$$|R_n/I| = |\phi(R_n)/\phi(I)| = |\mathbb{Z}^n/L|\,.$$

Hence R_n/I is finite if and only if L is a full-rank sublattice of $\mathbb{Z}^n$. Further, $L = \Lambda(\boldsymbol{c})$ for some $\boldsymbol{c} \in \mathbb{Z}^n$ if and only if $I = \langle \boldsymbol{c}(x) \rangle$, i.e. I is principal. □

Corollary 5.4.4. *A full-rank sublattice $L \subseteq \mathbb{Z}^n$ is simple cyclic if and only if $L = \phi(\langle \boldsymbol{c}(x) \rangle)$ where $\boldsymbol{c}(x) \in R_n$ is not a zero-divisor.*

Proof. Combine Lemmas 5.4.2 and 5.4.3. □

Remark 5.4.1. Recall that

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

where $\Phi_d(x)$ stands for d-th cyclotomic polynomial. Then it follows from [61] (Theorem A combined with Theorem 1.2) that the number of ideals in R_n (hence the

number of cyclic sublattices of $\mathbb{Z}^n$) with index $\leq T$ grows like $O\left(T(\log T)^{\tau(n)-1}\right)$ as $T \to \infty$, where $\tau(n)$ is the number of divisors of n (see also Theorem 2.3 of [33] for a convenient formulation). Simple cyclic sublattices of full rank correspond to principal ideals of finite index, and hence their number also grows like $O\left(T(\log T)^{\tau(n)-1}\right)$. This follows from the proof of Theorem 2.3 of [33], since every ideal class in R_n contributes equally to the total number of ideals of bounded index.[1]

5.5 Cyclic representation of root lattices

In this section we focus on the cyclic properties of the standard root lattices, in particular proving Theorem 5.1.3.

Lemma 5.5.1. *The root lattice*

$$A_n = \left\{ \boldsymbol{x} \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0 \right\}$$

and its dual A_n^* are simple cyclic lattices of rank n in $\mathbb{R}^{n+1}$ for each $n \geq 2$.

Proof. Write $\sum(\boldsymbol{x})$ for the sum of all the coordinates of the vector $\boldsymbol{x}$, and notice that $\sum(\boldsymbol{x}) = \sum(\rho(\boldsymbol{x}))$ for any vector $\boldsymbol{x} \in \mathbb{R}^n$ for any $n \geq 1$. Then the lattice A_n is closed under $\rho : \mathbb{R}^{n+1} \to \mathbb{R}^{n+1}$, and hence is a cyclic lattice of rank n in $\mathbb{R}^{n+1}$. In fact,

$$A_n = \operatorname{span}_{\mathbb{Z}} \left\{ \boldsymbol{a}, \rho(\boldsymbol{a}), \ldots, \rho^{n-1}(\boldsymbol{a}) \right\}$$

for the vector $\boldsymbol{a} = (1, -1, 0, \ldots, 0)^\top$, hence it is simple cyclic.

Let us write $\mathbf{1}_{n+1}$ for the vector in $\mathbb{R}^{n+1}$ with all the coordinates equal to 1 and $\mathbf{1}_{n+1}^\perp$ for the co-dimension one subspace of $\mathbb{R}^{n+1}$ orthogonal to $\mathbf{1}_{n+1}$. Then $A_n = \mathbf{1}_{n+1}^\perp \cap \mathbb{Z}^{n+1}$ and A_n^* is the orthogonal projection of $\mathbb{Z}^{n+1}$ onto $\mathbf{1}_{n+1}^\perp$. As described in

[1] This observation is due to Stefan Kühnlein.

Proposition 4.2.3 of [49], A_n^* is generated by the vectors

$$\boldsymbol{y}_i = \frac{1}{n+1}\left((n+1)\boldsymbol{e}_i - \mathbf{1}_{n+1}\right),\ 1 \le i \le n+1,$$

which are rotation shifts of $\boldsymbol{y}_1$. Hence A_n^* is also simple cyclic in $\mathbb{R}^{n+1}$. □

Lemma 5.5.2. *The root lattice*

$$D_n = \left\{ \boldsymbol{x} \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \equiv 0 \pmod 2 \right\}$$

is cyclic in $\mathbb{R}^n$ for each $n \ge 2$. It is simple cyclic if and only if n is odd.

Proof. Since $\sum(\boldsymbol{x}) = \sum(\rho(\boldsymbol{x}))$ for any $\boldsymbol{x} \in \mathbb{R}^n$, we see that D_n is cyclic. Let $n \ge 3$ be odd, and take $\boldsymbol{c} = (1, 1, 0, \ldots, 0)^\top \in D_n$. We will show that $D_n = \mathrm{P}(\boldsymbol{c})^\top \mathbb{Z}^n$. Recall that $\det D_n = 2$, hence it is sufficient to show that $\det \mathrm{P}(\boldsymbol{c})^\top = \pm 2$. Notice that

$$\mathrm{P}(\boldsymbol{c})^\top = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 1 \\ 1 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 0 \\ 0 & 0 & 0 & \ldots & 1 & 1 \end{pmatrix}.$$

Performing the Laplace expansion along the first row and keeping in mind that n is odd, we see that $\det \mathrm{P}(\boldsymbol{c})^\top = 2$, and hence $D_n = \Lambda(\boldsymbol{c})$.

Now suppose $n \ge 2$ is even. Arguing toward a contradiction, suppose that there exists some $\boldsymbol{c} \in D_n$ such that $D_n = \Lambda(\boldsymbol{c})$. Let $\boldsymbol{c}(x)$ be as in (5.11), then by (5.12),

$$\det \mathrm{P}(\boldsymbol{c}) = \prod_{j=1}^{n} \boldsymbol{c}(\omega_n^j) = \pm \det D_n = \pm 2.$$

In particular, $1 = \omega_n^n$ and $-1 = \omega_n^{n/2}$ are both n-th roots of unity, and so $\boldsymbol{c}(1)\boldsymbol{c}(-1)$ is a nonzero integer. Then the remaining product

$$\prod_{j=1,\ j\neq\frac{n}{2}}^{n-1} \boldsymbol{c}(\omega_n^j) = \pm\frac{2}{\boldsymbol{c}(1)\boldsymbol{c}(-1)} \in \mathbb{Q},$$

but this product is also an algebraic integer, hence it is in $\mathbb{Z}$. This means that $|\boldsymbol{c}(1)\boldsymbol{c}(-1)| \leq 2$. On the other hand, $\boldsymbol{c}(1) = \sum_{i=1}^{n} c_i$ is even, since $\boldsymbol{c} \in D_n$, thus $\boldsymbol{c}(1) = \pm 2$ and so $\boldsymbol{c}(-1) = \pm 1$. Let α be the sum of coefficients of $\boldsymbol{c}(x)$ in front of even powers of x and β be the sum of coefficients in front of odd powers of x, then

$$2 \mid \boldsymbol{c}(1) = \alpha + \beta,\ 2 \nmid \boldsymbol{c}(-1) = \alpha - \beta,$$

implying that $2 \nmid \boldsymbol{c}(1) + \boldsymbol{c}(-1) = 2\alpha$. This is a contradiction, and hence D_n is not simple cyclic. □

Remark 5.5.1. The cyclic lattice A_n can be constructed from the ideal $\langle x - 1\rangle$ of rank n in $R_{n+1} = \mathbb{Z}[x]/\langle x^{n+1} - 1\rangle$ and D_n from an ideal of full rank in $R_n = \mathbb{Z}[x]/\langle x^n - 1\rangle$, as we discussed in Section 5.4. The lattices A_n (in $\mathbb{R}^{n+1}$) and D_n for odd n are simple cyclic; the latter one can also be easily obtained from the ideal $\langle x + 1\rangle$ in R_n (see also Propositions 4.5 and 4.2 of [22]). However, D_n for even n is of full rank but not simple cyclic, and hence cannot come from a principal ideal in R_n, by Lemma 5.4.3. In fact, it can easily be seen as the image under ϕ of the ideal

$$I = \langle 2, x + 1\rangle = \left\langle x^{n-1} + x^{n-2}, -x^{n-1} + 1\right\rangle \subset R_n.$$

This can be compared to Proposition 4.4 of [22], where D_n for even $n \geq 4$ is obtained as the image of the principal ideal $\langle x + 1\rangle$ in $\mathbb{Z}[x]/\langle x^n + 1\rangle$ under the same kind of coefficient embedding into $\mathbb{Z}^n$.

Lemma 5.5.3. *The lattice E_8 is cyclic, but not simple cyclic. The lattices E_6 and E_7 are not cyclic.*

Proof. Recall that the lattice E_8 can be defined as

$$E_8 = D_8 \cup \left(\frac{1}{2}\mathbf{1}_8 + D_8\right).$$

Notice that the vector $\mathbf{1}_8$ is invariant under ρ, and hence $\frac{1}{2}\mathbf{1}_8 + D_8$ is closed under ρ, as is D_8. This means that E_8 is cyclic. On the other hand, if $\boldsymbol{c} \in E_8$, then either $\boldsymbol{c} \in D_8$ or $\boldsymbol{c} \in \frac{1}{2}\mathbf{1}_8 + D_8$. If $\boldsymbol{c} \in D_8$, then $\Lambda(\boldsymbol{c}) \subseteq D_8$, so $\Lambda(\boldsymbol{c}) \neq E_8$. We now argue similarly to our proof of Lemma 5.5.2 above. Suppose that $\boldsymbol{c} \in \frac{1}{2}\mathbf{1}_8 + D_8$ is such that $\Lambda(\boldsymbol{c}) = E_8$, then $\boldsymbol{c} = \frac{1}{2}\mathbf{1}_8 + \boldsymbol{c}'$ for some $\boldsymbol{c}' \in D_8$, and

$$\prod_{j=1}^{8} \boldsymbol{c}(\omega_8^j) = \pm \det E_8 = \pm 1. \tag{5.13}$$

Notice that

$$\boldsymbol{c}(x) = \frac{1}{2}\sum_{k=0}^{7} x^k + \boldsymbol{c}'(x) = \frac{x^8 - 1}{2(x-1)} + \boldsymbol{c}'(x),$$

for all $x \neq 1$, and so $\boldsymbol{c}(\omega_8^j) = \boldsymbol{c}'(\omega_8^j) \in \mathbb{Z}$ for every $1 \leq j \leq 7$ and $\boldsymbol{c}(1) = 4 + \boldsymbol{c}'(1)$. In order for (5.13) to hold, we must in particular have

$$\boldsymbol{c}(1)\boldsymbol{c}(-1) = (4 + \boldsymbol{c}'(1))\boldsymbol{c}'(-1) = \pm 1.$$

However, $\boldsymbol{c}'(1)$ and $\boldsymbol{c}'(-1)$ must both be even, since $\boldsymbol{c}' \in D_8$. This is a contradiction, and hence E_8 is not simple cyclic.

The root lattices E_7 and E_6 can be described as sublattices of E_8 orthogonal to the vector $\boldsymbol{e}_7 + \boldsymbol{e}_8$ and to the pair of vectors $\boldsymbol{e}_7 + \boldsymbol{e}_8$, $\boldsymbol{e}_6 + \boldsymbol{e}_8$, respectively. These

lattices are not cyclic, since the spaces

$$\mathrm{span}_{\mathbb{R}}\{\boldsymbol{e}_7 + \boldsymbol{e}_8\},\ \mathrm{span}_{\mathbb{R}}\{\boldsymbol{e}_7 + \boldsymbol{e}_8, \boldsymbol{e}_6 + \boldsymbol{e}_8\}$$

are not closed under ρ. For instance, $\boldsymbol{x} = \boldsymbol{e}_4 + \boldsymbol{e}_5 \in E_7 \cap E_6$, however $\rho(\boldsymbol{x}) \notin E_6$ and $\rho^2(\boldsymbol{x}) \notin E_7$. □

Proof of Theorem 5.1.3. The theorem follows by combining Lemmas 5.5.1, 5.5.2, and 5.5.3 with Lemma 5.4.1. □

A family of lattices heavily related to A_n, the Coxeter lattices A_n^r, are also simple cyclic for certain values of r, as observed by Martinet:

Lemma 5.5.4. *Let $r = \frac{n+1}{2}$ with odd $n \geq 5$. Then A_n^r is simple cyclic.*

Proof. See [49], proposition 5.2.3 (iv). □

5.6 Number field lattices

Yet another important class of lattices comes from rings of integers of number fields. In this section we classify those of them that are cyclic, proving Theorem 5.1.4. As in Section 5.3, let K be a number field of degree $d = r_1 + 2r_2$ with embeddings

$$\sigma_1, \ldots, \sigma_d : K \hookrightarrow \mathbb{C},$$

where r_1 of them are real and $2r_2$ are complex, split into conjugate pairs. Then $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ can be viewed as a subspace of $\mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} \subseteq \mathbb{C}^d$, given by (up to a permutation of the coordinates)

$$\left\{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{2r_2} : y_{r_2+j} = \bar{y}_j \ \forall\ 1 \leq j \leq r_2\right\} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \subseteq \mathbb{C}^d.$$

Notice that in this last containment, we identify each copy of $\mathbb{R}$ with the real part of the corresponding copy of $\mathbb{C}$. It is a Euclidean space with respect to the bilinear form induced by the trace-form $\langle \alpha, \beta \rangle$ on the number field K:

$$\langle \alpha, \beta \rangle := \mathrm{Tr}_K(\alpha\bar{\beta}) \in \mathbb{R} \tag{5.14}$$

for any $\alpha, \beta \in K$, where Tr_K stands for the usual trace map on the number field K. We can define the embedding

$$\Sigma_K = (\sigma_1, \ldots, \sigma_d) : K \hookrightarrow K_{\mathbb{R}}$$

of K into $K_{\mathbb{R}}$. The ring of integers $\mathcal{O}_K$ becomes a lattice of full rank in $K_{\mathbb{R}}$ under this embedding, and we write Λ_K for the image $\Sigma_K(\mathcal{O}_K)$. An equivalent description of Λ_K is as a free $\mathbb{Z}$-module $\mathcal{O}_K$ equipped with the bilinear form $\langle \cdot, \cdot \rangle$ we defined in (5.14). It is easy to verify that $\langle \alpha, \beta \rangle$ is equal to the usual dot product of the vectors $\Sigma_K(\alpha)$ and $\Sigma_K(\beta)$ in $K_{\mathbb{R}}$. We write $\mathrm{Aut}(\Lambda_K)$ for the automorphism group of the lattice Λ_K, i.e. the group of isometries of this trace-induced bilinear form.

Lemma 5.6.1. *Suppose $K/\mathbb{Q}$ is a Galois extension with the Galois group G. Then $G \leq \mathrm{Aut}(\Lambda_K)$.*

Proof. Notice that all the embeddings of K are precisely the elements of G, and for every $\tau \in G$ and $\alpha, \beta \in \mathcal{O}_K$,

$$\begin{aligned} \langle \tau(\alpha), \tau(\beta) \rangle &= \mathrm{Tr}_K(\tau(\alpha\bar{\beta})) = \sum_{\sigma \in G} \sigma\tau(\alpha\bar{\beta}) \\ &= \sum_{\sigma \in G} \sigma(\alpha\bar{\beta}) = \mathrm{Tr}_K(\alpha\bar{\beta}) = \langle \alpha, \beta \rangle , \end{aligned}$$

since right-multiplication by τ simply permutes elements of G. Therefore G is a subgroup of $\mathrm{Aut}(\Lambda_K)$. □

Notice, however, that $\mathrm{Aut}(\Lambda_K)$ can be quite a bit larger than the Galois group of $K/\mathbb{Q}$. For example, $\Lambda_{\mathbb{Q}(i)}$ is similar to $\mathbb{Z}^2$, which has automorphism group of order 8, and $\Lambda_{\mathbb{Q}(\sqrt{-3})}$ is similar to the hexagonal lattice, which has automorphism group of order 12; in both cases, Galois groups of the quadratic fields have order 2. Hence there are often automorphisms of the lattice that do not come from the Galois action. This observation raises a question: if Λ_K is cyclic, does the cyclic shift operator ρ necessarily come from the Galois action? In the next lemma we answer this question in the affirmative. To avoid ambiguity, in this section we view lattices as cyclic under the rotational shift operator ρ as in (5.1) but on $\mathbb{C}^d$.

Lemma 5.6.2. *Suppose $K/\mathbb{Q}$ is a Galois extension with Galois group G. Then Λ_K is cyclic (for an appropriate ordering of the embeddings) if and only if $K/\mathbb{Q}$ is a cyclic extension with $G = \langle\sigma\rangle$, where the automorphism $\sigma : K \to K$ is such that*

$$\rho\left(\Sigma_K(\alpha)\right) = \Sigma_K(\sigma(\alpha)), \tag{5.15}$$

for every $\alpha \in \mathcal{O}_K$.

Proof. Suppose first that Λ_K is cyclic, then for any $\alpha \in \mathcal{O}_K$,

$$\rho\left(\sigma_1(\alpha), \ldots, \sigma_d(\alpha)\right) = \left(\sigma_d(\alpha), \sigma_1(\alpha), \ldots, \sigma_{d-1}(\alpha)\right) \in \Lambda_K.$$

This means that $\sigma_d(\alpha) \in \mathcal{O}_K$ and

$$\sigma_1\sigma_d(\alpha) = \sigma_d(\alpha), \sigma_2\sigma_d(\alpha) = \sigma_1(\alpha), \ldots, \sigma_d^2(\alpha) = \sigma_{d-1}(\alpha),$$

for all $\alpha \in \mathcal{O}_K$. Then σ_1 is the identity map, and

$$\sigma_2\sigma_d = \sigma_1, \sigma_3\sigma_d = \sigma_2, \sigma_4\sigma_d = \sigma_3, \ldots, \sigma_d^2 = \sigma_{d-1}.$$

This implies that

$$\sigma_j = \sigma_d^{d-j+1},\ \forall\ 1 \leq j \leq d-1,$$

and the action of ρ on Λ_K is given by the action of σ_d on $\mathcal{O}_K$ as specified in (5.15).

On the other hand, suppose that $K/\mathbb{Q}$ is cyclic with Galois group $G = \langle\sigma\rangle$ so that the embeddings are ordered as

$$\sigma_j = \sigma^{d-j+1},\ \forall\ 1 \leq j \leq d-1. \tag{5.16}$$

Then for any $\Sigma(\alpha) \in \Lambda_K$, we have

$$\begin{aligned} \rho\left(\alpha, \sigma^{d-1}(\alpha), \sigma^{d-2}(\alpha), \ldots, \sigma(\alpha)\right) &= \left(\sigma(\alpha), \alpha, \sigma^{d-1}(\alpha), \ldots, \sigma^2(\alpha)\right) \\ &= \Sigma_K(\sigma(\alpha)) \in \Lambda_K, \end{aligned}$$

and so Λ_K is closed under ρ, hence is cyclic. □

In fact, one can also ask which of these cyclic lattices of the form Λ_K are simple cyclic. We discuss this next. A normal basis for a Galois number field K is a basis consisting of all conjugates of one algebraic number, and a normal integral basis for K is a $\mathbb{Z}$-basis like this for $\mathcal{O}_K$. The normal basis theorem guarantees that every number field has a normal basis. However, having a normal integral basis is a much more delicate property. The finite Galois extension $K/\mathbb{Q}$ is called tamely ramified if all the ramification indices for every rational prime p are relatively prime with p. The Hilbert-Speiser theorem asserts that an abelian number field (i.e. Galois number field with abelian Galois group) has a normal integral basis if and only if it is tamely ramified (see, for instance, Chapter 9 of [45] for the details).

Lemma 5.6.3. *Let K be a cyclic Galois number field. Then the lattice Λ_K is simple cyclic (for an appropriate ordering of the embeddings) if and only if $K/\mathbb{Q}$ is tamely ramified.*

Proof. Let $d = [K : \mathbb{Q}]$ and $G = \langle \sigma \rangle$ be the Galois group of $K/\mathbb{Q}$. Let $\sigma_1, \ldots, \sigma_d$ be the embeddings of K, ordered as in (5.16). By the Hilbert-Speiser theorem $K/\mathbb{Q}$ is tamely ramified if and only if K has a normal integral basis. First assume that such a basis exists, i.e. $\sigma_1(\theta), \ldots, \sigma_d(\theta)$ form a $\mathbb{Z}$-basis for $\mathcal{O}_K$ for some $\theta \in \mathcal{O}_K$. Notice that

$$\Sigma(\sigma_1(\theta)), \ldots, \Sigma(\sigma_d(\theta))$$

forms a basis for Λ_K. Now for each $1 \leq j \leq d$,

$$\begin{aligned} \Sigma_K(\sigma_j(\theta)) &= \Sigma_K(\sigma^{d-j+1}(\theta)) = \rho(\Sigma_K(\sigma^{d-j}(\theta))) \\ &= \rho^2(\Sigma_K(\sigma^{d-j-1}(\theta))) = \cdots = \rho^{d-j}(\Sigma_K(\sigma(\theta))) = \rho^{d-j+1}(\Sigma_K(\theta)), \end{aligned}$$

by recursive application of (5.15). Therefore Λ_K is spanned by the basis

$$\Sigma_K(\theta), \rho(\Sigma_K(\theta)) \ldots, \rho^{d-1}(\Sigma_K(\theta)),$$

and hence it is simple cyclic.

Next suppose Λ_K is simple cyclic, then

$$\Lambda_K = \mathrm{span}_{\mathbb{Z}}\{\boldsymbol{x}, \rho(\boldsymbol{x}), \ldots, \rho^{d-1}(\boldsymbol{x})\}$$

for some $\boldsymbol{x} \in \Lambda_K$. Let $\theta \in \mathcal{O}_K$ be such that $\Sigma_K(\theta) = \boldsymbol{x}$, then

$$\Sigma_K(\theta), \rho(\Sigma_K(\theta)) \ldots, \rho^{d-1}(\Sigma_K(\theta))$$

is a basis for Λ_K, where for each $1 \leq j \leq d$,

$$\Sigma_K(\sigma_j(\theta)) = \rho^{d-j+1}(\Sigma_K(\theta)),$$

as we derived above. Therefore $\sigma_1(\theta), \ldots, \sigma_d(\theta)$ form a $\mathbb{Z}$-basis for $\mathcal{O}_K$, i.e. K has a normal integral basis. $\square$

An example of a family of such number fields comes from the cyclotomic fields.

Corollary 5.6.4. *Let $K = \mathbb{Q}(\zeta_n)$ be n-th cyclotomic field. There exists an ordering of the embeddings*

$$\sigma_1, \ldots, \sigma_{\phi(n)} : K \hookrightarrow \mathbb{C},$$

for which the lattice $\Lambda_K = \Sigma_K(\mathcal{O}_K)$ is cyclic if and only if $n = 2, 4, p^k$, or $2p^k$ for some odd prime p and positive integer k. Further, the cyclotomic lattice Λ_K is simple cyclic if and only if $n = 2, p$, or $2p$ for an odd prime p.

Proof. Recall that $K/\mathbb{Q}$ is Galois with the Galois group $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$, which is cyclic if and only if $n = 2, 4, p^k$, or $2p^k$ for some odd prime p and positive integer k: these are precisely the values of n for which primitive roots modulo n exist. If $G = \langle\sigma\rangle$ is cyclic, order the embeddings as in (5.16), and the first statement follows from Lemma 5.6.2. Further, the cyclotomic field $K = \mathbb{Q}(\zeta_n)$ is tamely ramified if and only if n is squarefree. Thus for K to be cyclic *and* tamely ramified, n must be equal to $2, p$, or $2p$ for an odd prime p. The second assertion then follows by Lemma 5.6.3. $\square$

Proof of Theorem 5.1.4. The theorem now follows from Lemmas 5.6.2, 5.6.3 and Corollary 5.6.4. $\square$

Remark 5.6.1. It is known that the lattice Λ_K is well-rounded if and only if K is a cyclotomic field: this was proved in [36] for a slightly different embedding, but the argument is identical for our embedding Σ_K (see also Lemma 7.1.5 of [40]). Hence the only cyclic well-rounded lattices of the form Λ_K are those characterized in Corollary 5.6.4, while there are also other cyclic lattices Λ_K (from non-cyclotomic cyclic extensions) that are not well-rounded. Indeed, consider for example the real quadratic

(hence cyclic) extension $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$. It is tamely ramified, and hence has a normal integral basis

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

Thus Λ_K is simple cyclic by Lemma 5.6.3. However, it is not well-rounded: its only minimal vectors are $\pm \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ (on the other hand, it is stable). In fact, any quadratic number field $\mathbb{Q}(\sqrt{D})$ for squarefree D is cyclic, and thus (when $D \neq -1, -3$) gives rise to a non-well-rounded cyclic lattice (although not necessarily simple cyclic like in the example above, e.g. if $D \not\equiv 1 \pmod 4$ then $\mathbb{Q}(\sqrt{D})$ is not tamely ramified).

BIBLIOGRAPHY

[1] A. Ash. On Eutactic Forms. *Canad. J. Math.*, 29(5):1040–1054, Oct. 1977.

[2] A. Ash and R. Gross. Lattice-Packing by Spheres and Eutactic Forms. *Exp. Math.*, pages 1–7, June 2019.

[3] M. Baake, R. Scharlau, and P. Zeiner. Well-rounded sublattices of planar lattices. *Acta Arith.*, 166(4):301–334, 2014.

[4] W. U. Bajwa, R. Calderbank, and S. Jafarpour. Why Gabor frames? Two fundamental measures of coherence and their role in model selection. *J. Commun. Netw.*, 12(4):289–307, Aug. 2010.

[5] W. U. Bajwa, R. Calderbank, and D. G. Mixon. Two are better than one: Fundamental parameters of frame coherence. *Appl. Comput. Harmon. Anal.*, 33(1):58–78, July 2012.

[6] E. S. Barnes and G. E. Wall. Some extreme forms defined in terms of Abelian groups. *J. Aust. Math. Soc.*, 1(1):47–63, Aug. 1959.

[7] E. Bayer-Fluckiger. Cyclotomic modular lattices. *J. Théor. Nombres Bordeaux*, 12(2):273–280, 2000.

[8] E. Bayer-Fluckiger. Ideal Lattices. In G. Wüstholz, editor, *A Panorama of Number Theory or The View from Baker's Garden*, pages 168–184. Cambridge University Press, 1st edition, Sept. 2002.

[9] Z. I. Borevič and I. R. Šafarevič. *Number theory*. Academic Press, Orlando, 2nd edition, 1987.

[10] A. Böttcher, L. Fukshansky, S. R. Garcia, H. Maharaj, and D. Needell. Lattices from equiangular tight frames. *Linear Algebra Appl.*, 510:395–420, Dec. 2016.

[11] B. Casselman. Stability of Lattices and the Partition of Arithmetic Quotients. *Asian J. Math.*, 8(4):607–638, Dec. 2004.

[12] T. F. Chan. An Optimal Circulant Preconditioner for Toeplitz Systems. *SIAM J. Sci. and Stat. Comput.*, 9(4):766–771, July 1988.

[13] Y. Chen, G. Hu, R. Liu, Y. Pan, and S. Shang. Relations Between Minkowski-Reduced Basis and θ-orthogonal Basis of Lattice. In Y.-J. Zhang, editor, *Image and Graphics*, Lecture Notes in Computer Science, pages 169–179, Cham, 2015. Springer International Publishing.

[14] M. T. Chu and R. J. Plemmons. Real-Valued, Low Rank, Circulant Approximation. *SIAM J. Matrix Anal. Appl.*, 24(3):645–659, Jan. 2003.

[15] H. Cohn and A. Kumar. Optimality and uniqueness of the Leech lattice among lattices. *Ann. of Math. (2)*, 170(3):1003–1050, Nov. 2009.

[16] H. Cohn, A. Kumar, S. Miller, D. Radchenko, and M. Viazovska. The sphere packing problem in dimension 24. *Ann. of Math. (2)*, 185(3), May 2017.

[17] J. H. Conway and N. J. A. Sloane. Laminated Lattices. *Ann. of Math. (2)*, 116(3):593–620, 1982.

[18] J. H. Conway and N. J. A. Sloane. A lattice without a basis of minimal vectors. *Mathematika*, 42(1):175–177, June 1995.

[19] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices, and groups*. Springer-Verlag, New York, 3rd edition, 1999.

[20] R. Coulangeon and G. Nebe. The unreasonable effectiveness of the tensor product. *arXiv:1201.1832 [math]*, Jan. 2012. arXiv: 1201.1832.

[21] M. Craig. Extreme forms and cyclotomy. *Mathematika*, 25(1):44–56, 1978.

[22] A. J. Ferrari and A. A. de Andrade. Algebraic lattices via polynomial rings. *Comp. Appl. Math.*, 38(4):163, Oct. 2019.

[23] L. Fukshansky. On distribution of well-rounded sublattices of Z2. *J. Number Theory*, 128(8):2359–2393, Aug. 2008.

[24] L. Fukshansky. On similarity classes of well-rounded sublattices of Z2. *J. Number Theory*, 129(10):2530–2556, Oct. 2009.

[25] L. Fukshansky. Revisiting the hexagonal lattice: on optimal lattice circle packing. *Elem. Math.*, pages 1–9, 2011.

[26] L. Fukshansky. Well-rounded zeta-function of planar arithmetic lattices. *Proc. Amer. Math. Soc.*, 142(2):369–380, Oct. 2013.

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

[28] L. Fukshansky, P. Guerzhoy, and F. Luca. On arithmetic lattices in the plane. *Proc. Amer. Math. Soc.*, 145(4):1453–1465, Oct. 2016.

[29] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead. On Integral Well-rounded Lattices in the Plane. *Discrete Comput. Geom.*, 48(3):735–748, Oct. 2012.

[30] L. Fukshansky and D. Kogan. On average coherence of cyclotomic lattices. *arXiv:2012.07807 [math]*, Apr. 2021. arXiv: 2012.07807.

[31] L. Fukshansky and D. Kogan. On the geometry of nearly orthogonal lattices. *Linear Algebra Appl.*, 629:112–137, Nov. 2021.

[32] L. Fukshansky and D. Kogan. Cyclic and well-rounded lattices. *Mosc. J. Comb. Number Theory*, 11(1):79–96, Mar. 2022.

[33] L. Fukshansky, S. Kühnlein, and R. Schwerdt. Counting ideals in polynomial rings. *arXiv:1701.04633 [math]*, Jan. 2017. arXiv: 1701.04633.

[34] L. Fukshansky, D. Moore, R. Andrew Ohana, and W. Zeldow. On well-rounded sublattices of the hexagonal lattice. *Discrete Math.*, 310(23):3287–3302, Dec. 2010.

[35] L. Fukshansky, D. Needell, J. Park, and Y. Xin. Lattices From Tight Frames and Vertex Transitive Graphs. *Electron. J. Combin.*, 26(3):P3.49, Sept. 2019.

[36] L. Fukshansky and K. Petersen. On well-rounded ideal lattices. *Int. J. Number Theory*, 08(01):189–206, Feb. 2012.

[37] G. H. Hardy, E. M. Wright, D. R. Heath-Brown, and J. H. Silverman. *An introduction to the theory of numbers*. Oxford University Press, Oxford, 6th edition, 2008.

[38] R. B. Holmes and V. I. Paulsen. Optimal frames for erasures. *Linear Algebra Appl.*, 377:31–51, Jan. 2004.

[39] M. Kalecki. On certain sums extended over primes or prime factors. *Prace Mat.*, 8:121–129, 1963.

[40] Y. Kitaoka. *Arithmetic of quadratic forms*. Cambridge University Press, Cambridge ; New York, 1st pbk. ed. (with corrections) edition, 1999.

[41] A. Korkine and G. Zolotareff. Sur les formes quadratiques positives. *Math. Ann.*, 11(2):242–292, June 1877.

[42] S. Kühnlein. Well-rounded Sublattices. *Int. J. Number Theory*, 08(05):1133–1144, 2012.

[43] V. I. Levenshtein. On bounds for packing in n-dimensional Euclidean space. *Dokl. Akad. Nauk*, 20:417–421, 1979.

[44] T. Loher and D. Masser. Uniformly counting points of bounded height. *Acta Arith.*, 111:277–297, Jan. 2004.

[45] R. L. Long. *Algebraic number theory*. M. Dekker, New York, 1977.

[46] V. Lyubashevsky and D. Micciancio. Generalized Compact Knapsacks Are Collision Resistant. In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, editors, *Automata, Languages and Programming*, Lecture Notes in Computer Science, pages 144–155, Berlin, Heidelberg, 2006. Springer.

[47] D. A. Marcus. *Number Fields*. Springer, Cham, 2018.

[48] J. Martinet. Sur l'indice d un sous-réseau. In J. Martinet, editor, *Réseaux euclidiens, designs sphériques et formes modulaires*, pages 163–211. L'Enseignement Mathématique, Genève, 2001.

[49] J. Martinet. *Perfect lattices in Euclidean spaces*. Springer-Verlag, Berlin; New York, 2003.

[50] J. Martinet and A. Schürmann. Bases of minimal vectors in lattices, iii. *Int. J. Number Theory*, 8(2):551–567, Mar. 2012.

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

[52] D. Micciancio. Generalized Compact Knapsacks, Cyclic Lattices, and Efficient One-Way Functions. *Comput. Complexity*, 16(4):365–411, Dec. 2007.

[53] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems*. Springer US, Boston, MA, 2002.

[54] J. W. Milnor and D. Husemöller. *Symmetric bilinear forms*. Springer-Verlag, Berlin, New York, 1973.

[55] O. Musin. The kissing number in four dimensions. *Ann. of Math. (2)*, 168(1):1–32, July 2008.

[56] R. Neelamani, S. Dash, and R. G. Baraniuk. On Nearly Orthogonal Lattice Bases and Random Lattices. *SIAM J. Discrete Math.*, 21(1):199–219, Jan. 2007.

[57] D. G. Northcott. Periodic Points on an Algebraic Variety. *Ann. of Math. (2)*, 51(1):167, Jan. 1950.

[58] A. M. Odlyzko and N. J. A. Sloane. New bounds on the number of unit spheres that can touch a unit sphere in n dimensions. *J. Combin. Theory Ser. A*, 26(2):210–214, Mar. 1979.

[59] C. Peikert and A. Rosen. Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices. In *Theory of Cryptography*, volume 3876, pages 145–166. Springer, Berlin, Heidelberg, 2006.

[60] M. Pohst. On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications. *SIGSAM Bull.*, 15(1):37–44, Feb. 1981.

[61] T. Rossmann. Enumerating submodules invariant under an endomorphism. *Math. Ann.*, 368(1):391–417, June 2017.

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

[63] A. Södergren. On the distribution of angles between the N shortest vectors in a random lattice. *J. Lond. Math. Soc. (2)*, 84(3):749–764, 2011.

[64] M. A. Tsfasman and S. G. Vlăduț. *Algebraic-geometric codes*. Kluwer Academic Publishers, Dordrecht; Boston, 1991.

[65] M. Viazovska. The sphere packing problem in dimension 8. *Ann. of Math. (2)*, 185(3):991–1015, May 2017.

[66] G. Voronoi. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs. *J. Reine Angew. Math.*, 134:198–287, 1908.

[67] B. L. v. d. Waerden and K. Schütte. Das Problem der 13 Kugeln. *Math. Ann.*, 125:325–334, 1952.

[68] S. F. D. Waldron. *An Introduction to Finite Tight Frames*. Birkhäuser/Springer, New York, 2018.