Aalto University
School of Science
Master's Programme in Mathematics and Operations Research

Niklas Miller

Algebraic number theory: On generic well-rounded lattices

Master's Thesis
Espoo, December 30, 2020

Supervisor: Professor Camilla Hollanti
Advisor: Professor Guillermo Mantilla-Soler

Aalto University
School of Science
Master's Programme in Mathematics and Operations Research

ABSTRACT OF MASTER'S THESIS

Author:	Niklas Miller		
Title:	Algebraic number theory: On generic well-rounded lattices		
Date:	December 30, 2020	**Pages:**	76
Major:	Mathematics	**Code:**	SCI3054
Supervisor:	Professor Camilla Hollanti		
Advisor:	Professor Guillermo Mantilla-Soler		

Recently, well-rounded (WR) lattices and in particular, well-rounded lattices with high sphere packing density and a low kissing number, have been proposed as good candidates for lattices used in lattice coset codes in wiretap channels. Generic well-rounded (GWR) lattices are WR lattices with minimal kissing number, and thus potential options for lattice coset codes.

In this work, we explore Lagrangian lattices, which emerge from certain types of number fields, and their sublattices, which interestingly turn out to be GWR under some assumptions about their parameters. We develop bounds for the center density, a common measure of sphere packing density, of a WR sublattice of a Lagrangian lattice, and further, characterize when a sublattice is equivalent to either the orthogonal lattice $\mathbb{Z}^n$ or the root lattice A_n.

We present new constructions of so-called deformed lattices – we call these D_n^α and E_8^α, which are an attempt to capture the good packing density of the lattices D_n and E_8, while being GWR. We investigate the center densities of these lattices and develop conditions under which scaled variants of these lattices are sublattices of $\mathbb{Z}^n$.

Keywords:	Well-rounded lattices, Generic well-rounded lattices, Algebraic number theory, Lagrangian lattices, Deformed lattices
Language:	English

Aalto-universitetet
Högskolan för teknikvetenskaper

Aalto-universitetet
Högskolan för teknikvetenskaper
Magisterprogrammet i matematik och operationsanalys

SAMMANDRAG AV
DIPLOMARBETET

Utfört av:	Niklas Miller		
Arbetets namn:	Algebraisk talteori: Om generiska välrundade gitter		
Datum:	Den 30 december 2020	**Sidantal:**	76
Huvudämne:	Matematik	**Kod:**	SCI3054
Övervakare:	Professor Camilla Hollanti		
Handledare:	Professor Guillermo Mantilla-Soler		

Nyligen har välrundade (VR) gitter, och i synnerhet välrundade gitter med hög packningstäthet och ett lågt kysstal, visat sig vara goda kandidater för koder som baserar sig på gittersidoklasser, som används i avlyssningskanaler. Generiska välrundade (GVR) gitter är VR gitter med ett möjligast lågt kysstal, och därmed potentiella alternativ för dessa typers koder.

I detta arbete undersöker vi Lagrangian gitter, som uppkommer ur vissa slags algebraiska talkroppar, samt deras undergitter, som intressant nog visar sig vara GVR under vissa antaganden gällande deras parametrar. Vi utvecklar gränser för centerdensiteten, ett vanligt mått på packningstätheten, för ett VR undergitter av ett Lagrangian gitter och vidare, karakteriserar när undergittret är ekvivalent med antingen det ortogonala gittret $\mathbb{Z}^n$ eller gittret A_n.

Vi presenterar nya konstruktioner av så kallade deformerade gitter – vi kallar dessa D_n^α och E_8^α. Dessa deformerade gitter har god packningstäthet så som D_n^α och E_8^α, medan de är GVR. Vi undersöker centerdensiteten för dessa gitter och utvecklar villkor under vilka skalade versioner av dem är undergitter av $\mathbb{Z}^n$.

Nyckelord:	Välrundade gitter, Generiska välrundade gitter, Algebraisk talteori, Lagrangian gitter, Deformerade gitter
Språk:	Engelska

Acknowledgements

I would like to thank Professors Camilla Hollanti and Guillermo Mantilla-Soler for providing me an interesting topic to work on, as well as giving me advice, corrections and ideas throughout the process of writing this thesis.

Espoo, December 30, 2020

Niklas Miller

Contents

Chapter 1

Introduction

Suppose that a person wants to reliably transfer messages to another person via a noisy channel, under the presence of an eavesdropper. Encoding at the transmitter's end and decoding at the receiver's end is allowed. Further, the eavesdropper has knowledge about the codes used. This setting is sometimes called a wiretap channel, first introduced by Wyner [33]. The designer of the coding scheme has multiple objectives, such as maximizing the probability of the receiver decoding correctly, achieving a high rate of information, and perhaps most importantly, minimizing the probability of the eavesdropper decoding correctly and minimizing the mutual information between the message and what is received by the eavesdropper. One possible way to achieve the latter goals is to add redundancy to the messages by adding random bits, a method called coset coding [26].

Lattice coset coding [3], [24] utilizes the idea of coset coding: briefly, the coding setup consists of a lattice Λ_B and a sublattice $\Lambda_E \subset \Lambda_B$. The message, a string of bits, that the transmitter wants to send to the receiver, is first encoded – the message is injectively mapped to a coset $S \in \Lambda_B/\Lambda_E$. Randomness is then introduced by choosing a random coset representative in S. Thus, the transmitted lattice vector $\mathbf{x} \in \Lambda_B$ contains both data and randomness. Although the setting is quite simple, choosing a pair of lattices (Λ_B, Λ_E) which minimizes the probability of the eavesdropper decoding correctly, at a given signal-to-noise ratio, is all but trivial.

The development of design criteria for lattice coset codes have lead to the study of well-rounded (WR) lattices. In particular, well-rounded lattices with high sphere packing density and a low kissing number have been shown to perform well (measured in the probability of the eavesdropper decoding

correctly at a given signal-to-noise ratio) in actual wiretap simulations [8], [9], [13], [14]. This motivates the study and construction of generic well-rounded (GWR) lattices – the subset of well-rounded lattices with minimal kissing number. Thus, our main goal in this thesis is to examine GWR lattices and characterize their sphere packing densities. The lattices we encounter are interesting in their own right, motivating their study on a theoretical level.

We begin by introducing the main concepts in lattice theory in Chapter 2. Then, in Chapter 3 we give a brief introduction to algebraic number theory, and show how lattices can be constructed from number fields. In Chapter 4, we illustrate how certain types of number fields give rise to an interesting lattice type, a Lagrangian lattice. Under some conditions, specific sublattices of a Lagrangian lattice are well-rounded, and moreover, possess a basis of shortest vectors [10]. In fact, we will show that under some extra assumptions, the sublattices are actually GWR. Having established this, we proceed to investigate the center densities of the sublattices. In particular, we show that the center densities of the sublattices are upper bounded by the center density of the A_n lattice, the densest lattice packing in dimensions 1–3. Moreover, we present conditions under which a WR sublattice is equivalent to A_n, or the orthogonal lattice $\mathbb{Z}^n$, respectively. We take a closer look at the dual lattice of a Lagrangian lattice, and its sublattices. Specifically, we show that the dual of a Lagrangian lattice is Lagrangian, and that the dual of a sublattice of a Lagrangian lattice has a certain shape, under some assumptions.

In Chapter 5, we take a different approach and start with dense lattice packings, and then deform the lattices by slightly changing the coordinates of the basis vectors, in a way that renders the lattices GWR. We construct a deformed version of the D_n lattice, which we call D_n^α, where α is a parameter describing how much the basis vectors of the D_n lattices are perturbed. We prove that the D_n^α lattices are GWR, which shows the existence of GWR lattices with a packing density arbitrarily close to the optimal packing density in dimensions 4 and 5. Furthermore, we give conditions under which a scaled version of the D_n^α lattice is a sublattice of $\mathbb{Z}^n$. Finally, we construct a GWR variant of the E_8 lattice; we call this the E_8^α lattice. We perform similar analysis to this lattice – in particular, we develop conditions under which we get a scaled version of E_8^α as a sublattice of $\mathbb{Z}^n$.

Chapter 2

Lattice theory

In this chapter, we give an overview of lattice theory. We take a closer look at the sphere packing and kissing number problems, and present some known bounds for the sphere packing density and kissing number of a lattice packing. For an extensive treatment of lattices, we refer the reader to the book [7] by Conway and Sloane.

2.1 The basics

Definition 2.1. *A lattice Λ is a discrete subgroup of the additive group $(\mathbb{R}^n, +)$. Equivalently, it is a set*

$$\Lambda = \left\{ \sum_{i=1}^{m} u_i \mathbf{b}_i : u_i \in \mathbb{Z} \right\},$$

where $\mathcal{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m\}$ is a set of linearly independent vectors in $\mathbb{R}^n$ called a basis of Λ, and m is called the rank of Λ. If $m = n$, then Λ is said to be full rank.

In this thesis, we are mainly interested in full rank lattices. Therefore, with the term lattice we mean a full rank lattice, if not explicitly stated otherwise. The matrix $M \in \mathbb{R}^{n \times n}$ whose columns consist of vectors $\mathbf{b}_i$, $1 \leq i \leq n$, is called a generator matrix of the lattice Λ. One can use the compact notation $\Lambda = M\mathbb{Z}^n = \{M\mathbf{u} : \mathbf{u} \in \mathbb{Z}^n\}$ to represent a lattice generated by the matrix M. It is worth noting that the generator matrix of a lattice is not unique, as the following proposition shows.

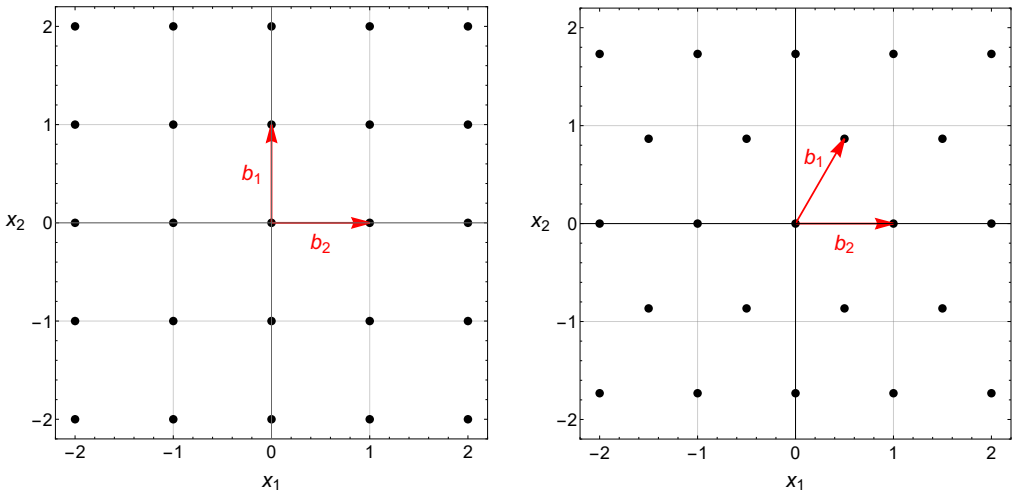
Proposition 2.1. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice with generator matrix M. A matrix M' generates the same lattice Λ if and only if $M' = MU$ for some matrix $U \in \mathbb{Z}^{n\times n}$ with $\det(U) = \pm 1$.*

We call a matrix $U \in \mathbb{Z}^{n\times n}$ satisfying $\det(U) = \pm 1$ a unimodular matrix – it is easily verified that the set of unimodular matrices $\mathrm{GL}_n(\mathbb{Z})$ is a group under matrix multiplication. We give the following well-known examples of lattices:

Example 2.1. *The orthogonal lattice $\mathbb{Z}^n$ for $n \geq 1$ is a lattice with a generator matrix I_n, where $I_n \in \mathbb{R}^{n\times n}$ is the identity matrix. Proposition 2.1 shows that any $U \in GL_n(\mathbb{Z})$ will serve as a generator matrix for $\mathbb{Z}^n$.*

Example 2.2. *The lattice $A_n := \left\{(x_1, \ldots, x_{n+1})^T \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0\right\}$ is a rank n lattice defined in $\mathbb{R}^{n+1}$. A basis is given by the vectors $\mathbf{v}_i = \mathbf{e}_i - \mathbf{e}_{i+1}$ for $1 \leq i \leq n$, where $\mathbf{e}_1, \ldots, \mathbf{e}_{n+1}$ are the standard basis vectors in $\mathbb{R}^{n+1}$. The lattice A_2 is equivalent (see Definition 2.7) to the hexagonal lattice A_h illustrated in Figure 2.1(b).*

Example 2.3. *The Checkerboard lattice $D_n := \{(x_1, \ldots, x_n)^T \in \mathbb{Z}^n : \sum_{i=1}^{n} x_i \equiv 0 \pmod 2\}$.*



(a) $\mathbb{Z}^2$ (b) A_h

Figure 2.1: Two planar lattices, the orthogonal lattice $\mathbb{Z}^2$ and the hexagonal lattice A_h. A basis $\{\mathbf{b}_1, \mathbf{b}_2\}$ for each lattice is illustrated with red arrows.

Throughout this thesis, let $\langle \cdot, \cdot \rangle$ denote the standard inner product in $\mathbb{R}^n$,

which induces the standard Euclidean norm, which we will denote by $\|\cdot\|$. If we use this norm to define the lengths of vectors in a lattice, we see that the squared norm of any lattice vector $\mathbf{x} = M\mathbf{u} \in \Lambda$, where $\mathbf{u} \in \mathbb{Z}^n$, takes the form

$$\|\mathbf{x}\|^2 = \langle \mathbf{x}, \mathbf{x} \rangle = \langle M\mathbf{u}, M\mathbf{u} \rangle = (M\mathbf{u})^T (M\mathbf{u}) = \mathbf{u}^T M^T M \mathbf{u}.$$

We can immediately recognize the importance of the matrix $M^T M$, which encodes information about the inner products of the basis vectors of the lattice. This matrix deserves its own definition.

Definition 2.2. *The Gram matrix of a lattice $\Lambda \subset \mathbb{R}^n$ with a generator matrix M is the symmetric and positive definite matrix defined as*

$$G := M^T M = (\mathbf{b}_i^T \mathbf{b}_j)_{1 \leq i,j \leq n}.$$

Remark that if M and M' are two generator matrices for Λ, then by Proposition 2.1, they are related by $M' = MU$ for some unimodular matrix U, and in particular, the corresponding Gram matrices are related by $G' = U^T G U$. This shows that the Gram matrix for a lattice is not unique. We define two related concepts which in some sense measure the scale of a lattice.

Definition 2.3. *The determinant of a lattice Λ with Gram matrix G is defined as*

$$\det(\Lambda) := \det(G).$$

If Λ is full rank, then its determinant is guaranteed to be positive, as G is positive definite in this case.

Definition 2.4. *The volume of a lattice Λ is defined as*

$$\mathrm{vol}(\Lambda) := \sqrt{\det(\Lambda)}.$$

For a full rank lattice Λ, the volume reduces to $\mathrm{vol}(\Lambda) = |\det(M)|$. Further, the volume is independent of the choice of basis. Many of the lattices we study are integral lattices, which we define as:

Definition 2.5. *A lattice is called integral, if its Gram matrix has entries in $\mathbb{Z}$.*

An equivalent definition to the above is that $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all $\mathbf{x}, \mathbf{y} \in \Lambda$. An integral lattice is called even, if $\langle \mathbf{x}, \mathbf{x} \rangle \in 2\mathbb{Z}$ for every $\mathbf{x} \in \Lambda$, otherwise it is called odd. An integral lattice of unit volume is called a unimodular lattice.

2.2 Sublattices and equivalent lattices

Sometimes we are interested in finding a lattice which is a subset of another lattice. This is the case, for instance, in lattice coset coding, where we seek lattices inside another lattices having certain properties. It is also useful to recognize when two lattices are isometric, *i.e.*, one can be obtained from the other by rotation, reflection and scaling.

Definition 2.6. *Let Λ be a lattice. A subset $\Lambda' \subseteq \Lambda$ which itself is a lattice is called a sublattice of Λ.*

As Λ' and Λ have the structure of abelian groups, it makes sense to consider the quotient group $\Lambda/\Lambda' = \{\mathbf{x}+\Lambda' : \mathbf{x} \in \Lambda\}$. The cardinality of Λ/Λ' is called the index of the sublattice Λ' in Λ, denoted $[\Lambda : \Lambda']$. For lattices $\Lambda' \subseteq \Lambda$ of the same rank, we have:

$$[\Lambda : \Lambda'] = \frac{\mathrm{vol}(\Lambda')}{\mathrm{vol}(\Lambda)}.$$

Example 2.4. *Let $m, n > 0$ be integers. The lattice $m\mathbb{Z}^n$ is a sublattice of $\mathbb{Z}^n$ with*

$$[\mathbb{Z}^n : m\mathbb{Z}^n] = \frac{\mathrm{vol}(m\mathbb{Z}^n)}{\mathrm{vol}(\mathbb{Z}^n)} = \frac{m^n}{1} = m^n.$$

Next we define an important equivalence relation on the set of lattices.

Definition 2.7. *Two lattices Λ and Λ' with generator matrices M and M', respectively, are said to be equivalent, denoted $\Lambda \sim \Lambda'$, if $M' = \alpha BMU$ for some $\alpha > 0$, a real orthogonal matrix B and a unimodular matrix U.*

If $\alpha = 1$, we say that Λ and Λ' are congruent and denote it by $\Lambda \cong \Lambda'$. Remark that two lattices are equivalent if and only if one is obtained from the other by rotation, reflection and scaling. The following remark gives the relationship between the Gram matrices of equivalent lattices:

Remark 2.1. As a consequence of Definition 2.7, the Gram matrices G and G' of equivalent lattices are related by

$$\begin{aligned} G' &= (\alpha BMU)^T(\alpha BMU) && (2.1)\\ &= \alpha^2 U^T M^T B^T BMU && (2.2)\\ &= \alpha^2 U^T M^T MU && (2.3)\\ &= \alpha^2 U^T GU. && (2.4) \end{aligned}$$

In particular, the Gram matrices of congruent lattices are related by $G' = U^T GU$.

The following lemma gives the relationship between the volumes of equivalent lattices.

Lemma 2.1. *Suppose that Λ, $\Lambda' \subset \mathbb{R}^n$ are equivalent lattices with generator matrices M and M', respectively, related by $M' = \alpha BMU$, where $\alpha > 0$, B is a real orthogonal matrix and U is a unimodular matrix. Then* $\mathrm{vol}(\Lambda') = \alpha^n \mathrm{vol}(\Lambda)$.

Proof. Since orthogonal and unimodular matrices have determinant ± 1,

$$\begin{aligned} \mathrm{vol}(\Lambda') &= |\det(\alpha BMU)| && (2.5)\\ &= |\det(\alpha I_n)\det(B)\det(M)\det(U)| && (2.6)\\ &= \alpha^n |\det(M)| && (2.7)\\ &= \alpha^n \mathrm{vol}(\Lambda). && (2.8) \end{aligned}$$

□

A direct consequence of the above lemma is that the lattice $\alpha\Lambda$, where $\alpha := \mathrm{vol}(\Lambda)^{-\frac{1}{n}}$, has unit volume.

2.3 Dual lattices

A useful concept in lattice theory is that of the dual lattice, which in some sense is the same to a lattice as what the dual space is to a vector space. The geometry of the dual lattice is related to the primal, which allows one to deduce information about the primal lattice by studying the dual lattice. The definition goes as follows.

Definition 2.8. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Its dual lattice Λ^* is defined by*

$$\Lambda^* := \{\mathbf{v} \in \mathbb{R}^n : \langle \mathbf{v}, \mathbf{x} \rangle \in \mathbb{Z} \text{ for any } \mathbf{x} \in \Lambda\}.$$

The connection to the dual space of a vector space is the following. Suppose that V is a real vector space. The dual space V^* is defined as the set of linear functions $\phi : V \to \mathbb{R}$. It is a vector space itself, and if V has finite dimension, then V^* has the same dimension. In fact, if $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is a basis for V, then a dual basis is given by the linear functions $\{\phi_1, \ldots, \phi_n\}$, where $\phi_i(\mathbf{e}_j) = \delta_{i,j}$. If $V \subseteq \mathbb{R}^n$ is a Euclidean vector space, then each linear map $\phi : V \to \mathbb{R}$ can be identified with a vector $\mathbf{v} \in V$, by the relation $\phi(\mathbf{x}) = \langle \mathbf{v}, \mathbf{x} \rangle$. Such a vector is $\mathbf{v} = (\phi(\mathbf{e}_1), \ldots, \phi(\mathbf{e}_n))^T$.

Lattices are not vector spaces, but they are modules over the ring $\mathbb{Z}$, and modules over rings can be thought of as generalizations of vector spaces.

Therefore, if we replace $\mathbb{R}$ with $\mathbb{Z}$ and consider the $\mathbb{Z}$-linear maps $\phi : \Lambda \to \mathbb{Z}$, we end up with the notion of a dual lattice. In particular, any $\mathbb{Z}$-linear map $\phi : \Lambda \to \mathbb{Z}$ can be identified with a vector $\mathbf{v} \in \mathbb{R}^n$ by the relation $\phi(\mathbf{x}) = \langle \mathbf{v}, \mathbf{x} \rangle$, where we require that $\phi(\Lambda) \subseteq \mathbb{Z}$. By the dual lattice we mean the vectors that identify the linear maps, instead of the linear maps themselves.

We can explicitly describe a generator matrix of the dual lattice if we know a generator matrix of the primal lattice, as Proposition 2.2 shows.

Proposition 2.2. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice with a generator matrix M. Then Λ^* has a generator matrix $(M^T)^{-1}$.*

Proof. Let $\mathbf{x} = M\mathbf{u} = \sum_{i=1}^{n} u_i \mathbf{b}_i \in \Lambda$ where $\mathbf{b}_i$'s are the columns of M and $\mathbf{u} \in \mathbb{Z}^n$. Then for any $\mathbf{v} \in \mathbb{R}^n$,

$$\langle \mathbf{v}, \mathbf{x} \rangle = \sum_{i=1}^{n} u_i \langle \mathbf{v}, \mathbf{b}_i \rangle .$$

Therefore, $\mathbf{v} \in \Lambda^*$ if and only if $\langle \mathbf{v}, \mathbf{b}_i \rangle \in \mathbb{Z}$ for every $i \in \{1, \ldots, n\}$, or equivalently, $M^T\mathbf{v} \in \mathbb{Z}^n$, *i.e.*, $\mathbf{v} \in (M^T)^{-1}\mathbb{Z}^n$. □

The above proposition implies that $(\Lambda^*)^* = \Lambda$. Further, we have the following.

Remark 2.2. If G is a Gram matrix for the primal lattice, then G^{-1} is a Gram matrix for the dual lattice. To see this, let $G = M^T M$ be the Gram matrix for the primal lattice with respect to the generator matrix M. Then

$$G^{-1} = (M^T M)^{-1} = M^{-1}(M^T)^{-1} = ((M^T)^{-1})^T (M^T)^{-1}$$

is the Gram matrix for the dual lattice with respect to the generator matrix $(M^T)^{-1}$.

We present some basic results for dual lattices.

Lemma 2.2. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice and $\alpha > 0$ a scalar. Then*

$$(\alpha\Lambda)^* = \frac{1}{\alpha}\Lambda^*.$$

Lemma 2.3. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Then*

$$\mathrm{vol}(\Lambda^*) = \frac{1}{\mathrm{vol}(\Lambda)}.$$

The latter lemma says that the scale of the dual lattice is the inverse of the scale of the primal lattice. If $\Lambda = \Lambda^*$, then we say that Λ is self-dual. In particular, if Λ is integral and self-dual, then it is necessarily unimodular. A standard example of a self-dual lattice is $\mathbb{Z}^n$.

2.4 Successive minima and kissing number

In this section, we define the concept of lattice successive minima, and briefly discuss the kissing number problem. We give some known bounds on the maximum kissing number in a given dimension.

Definition 2.9. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Define the i:th successive minimum of the lattice Λ, for $i \in \{1, 2, \ldots, n\}$, as*

$$\lambda_i(\Lambda) := \inf \left\{ r > 0 : \dim(\mathrm{span}_{\mathbb{R}}(\Lambda \cap \overline{B}(\mathbf{0}, r)) \geq i \right\},$$

where $\overline{B}(\mathbf{0}, r) = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq r\}$ is the closed origin-centered ball of radius r.

In other words, $\lambda_i(\Lambda)$ describes the minimum radius r, such that all lattice vectors at distance at most r from the origin span a subspace of $\mathbb{R}^n$ of dimension at least i. We have the bounds $0 < \lambda_1(\Lambda) \leq \lambda_2(\Lambda) \leq \cdots \leq \lambda_n(\Lambda) < \infty$, where $0 < \lambda_1(\Lambda)$ follows from the discreteness of the lattice. The constant $\lambda_1(\Lambda)$ is an important lattice constant deserving its own definition, which is equivalent to Definition 2.9 for $i = 1$.

Definition 2.10. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Define the shortest vector length, or minimum, of Λ as*

$$\lambda_1(\Lambda) := \min_{0 \neq \mathbf{x} \in \Lambda} \|\mathbf{x}\|.$$

Equivalently, $\lambda_1(\Lambda)$ is the minimum distance between any two lattice vectors. We will later see that $\lambda_1(\Lambda)$ is related to the sphere packing density of a lattice, and that maximizing $\lambda_1(\Lambda)$ over volume 1 lattices is equivalent to maximizing the packing density over all lattices. The set of lattice vectors having length $\lambda_1(\Lambda)$ is particularly important, motivating the following definition.

Definition 2.11. *Let Λ be a lattice. The set $S(\Lambda) = \{\mathbf{x} \in \Lambda : \|\mathbf{x}\| = \lambda_1(\Lambda)\}$ is called the set of minimal vectors of Λ. Its cardinality $\kappa(\Lambda) = |S(\Lambda)|$ is called the kissing number of the lattice.*

The kissing number has the following interpretation. If we place identical spheres with maximum radius centered at the lattice points such that the

spheres are allowed to barely kiss each other, then the kissing number is the number of spheres touching the sphere centered at the origin. We denote by κ_n the maximum kissing number of a lattice in dimension n. The more general kissing number problem asks for the maximum number of identical spheres that one can fit around a central one such that the spheres do not overlap, but the spheres are not required to be centered at lattice points. We will denote the non-lattice maximum kissing number in dimension n by κ'_n. The kissing number problem has its origins in a late 17th century debate between Isaac Newton and David Gregory on how many spheres one could fit around a central one, in dimension 3. Newton believed that the answer is 12, whereas Gregory thought 13 spheres would be possible. Newton was right, but this was not proved until the late 19th century by Schütte and van der Waerden [27].

The exact maximum kissing number (non-lattice and lattice) is only known in dimensions 1, 2, 3, 4, 8 and 24. Kabatiansky and Levenshtein [16] proved in 1978 that the non-lattice maximum kissing number has the asymptotic upper bound

$$\kappa'_n \leq 2^{0.401n(1+o(1))}. \tag{2.9}$$

Further, Wyner [34] showed that the non-lattice maximum kissing number has an asymptotic lower bound given by

$$\kappa'_n \geq 2^{0.2075n(1+o(1))}. \tag{2.10}$$

These results imply that κ'_n increases exponentially as dimension grows. However, no exponential lower bound for the lattice maximum kissing number κ_n was known until recently, when Vlăduţ [31] gave the asymptotic lower bound

$$\kappa_n \geq 2^{0.0219n(1+o(1))}. \tag{2.11}$$

Figure 2.2 shows the kissing numbers of certain standard lattices, and the currently best known bounds for the non-lattice maximum kissing number κ'_n in dimensions 1-24. The bounds are based on the numerical computations in [20], where the authors use a method by Bachoc and Vallentin [1] to develop bounds for the non-lattice kissing number.

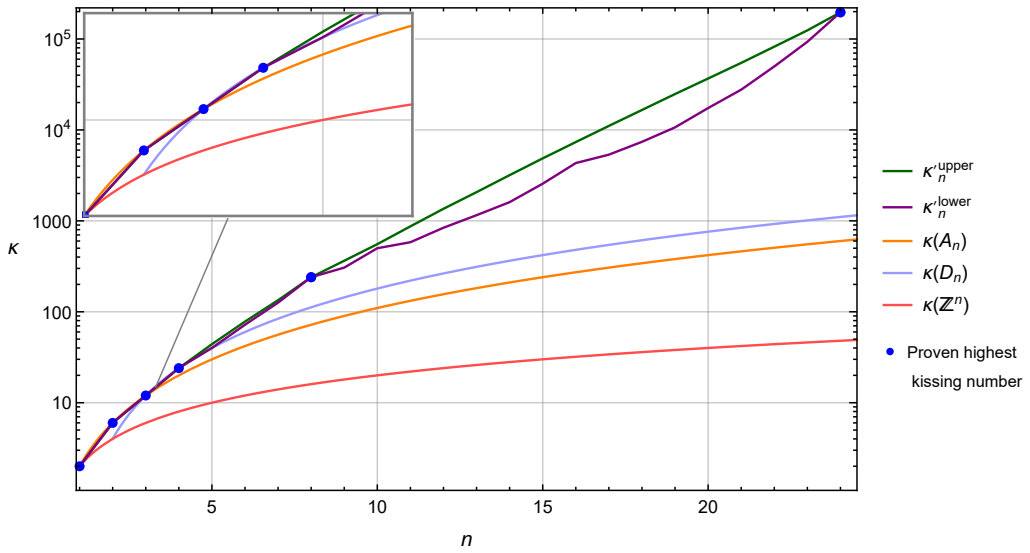


Figure 2.2: Kissing numbers for various lattices, and bounds for κ'_n. Proven largest kissing numbers are also shown. Notice the logarithmic scaling of the vertical axis.

2.5 Lattice packings and density

The problem of finding the densest arrangement of non-overlapping equal spheres in a given dimension is called the sphere packing problem. With the density of a sphere packing we mean the proportion of space occupied by the spheres, or rather, the limit of the proportion of spheres inside a finite region such as an origin-centered ball, when the radius of the ball approaches infinity. We distinguish lattice packings, in which the spheres are required to be centered at lattice points, from more general sphere packings where the centers of the spheres do not have to be centered at lattice points.

In dimension one, the answer to the sphere packing problem is trivial: take the lattice $\mathbb{Z}$ and place spheres of radius $\frac{1}{2}$ centered at the lattice points. In dimension two, the answer is still quite intuitive: take the hexagonal packing, where each sphere (circle) kisses six other spheres. The first to give a proof of the optimality of the hexagonal packing was Thue [30] in 1892. In dimension three, the problem is more involved – 17th century mathematician and astronomer Kepler conjectured that the maximum packing density in three dimensional space is $\frac{\pi}{3\sqrt{2}} \approx 0.74$, achieved by the face-centered cubic lattice packing. Although intuitive, it took considerable effort to prove the conjecture: a proof involving computer calculations was announced by

mathematician Thomas Hales in 1998 – a more detailed one was published in 2005 [15]. In higher dimensions, the optimal packing density is known only in a handful of dimensions.

Besides being fundamentally interesting, dense packings of spheres have practical applications, especially in communications. The idea of representing signals as points in $\mathbb{R}^n$ dates back to Shannon [28]. To illustrate how the sphere packing problem is related to the seemingly unrelated problem of choosing a signal set for communication via a noisy channel, consider the following scenario. Suppose that signals are represented as points in a bounded subset $A \subset \mathbb{R}^n$, such as a ball centered at the origin. Our goal is to choose a finite set of signals $S \subset A$, which we want to transmit over a noisy channel to a receiver. Each signal $\mathbf{x} \in S$ is received as a point $\mathbf{y} \in \mathbb{R}^n$, where in general $\mathbf{x} \neq \mathbf{y}$. In a simplistic noise model, we may assume that $\|\mathbf{x} - \mathbf{y}\| < \eta$ always holds, for some small $\eta > 0$. The receiver decodes $\mathbf{y}$ to the closest point $\mathbf{x} \in S$. Thus, to make decoding at the receiver unambiguous, one has to ensure that $B(\mathbf{x}_1, \eta) \cap B(\mathbf{x}_2, \eta) = \emptyset$ for every $\mathbf{x}_1, \mathbf{x}_2 \in S$. As we want to increase the information rate, we want to maximize the number of points in S. Equivalently, we want to pack as many spheres with radius η inside A. When A becomes larger, this problem becomes the same problem as the sphere packing problem.

Let us for a moment focus on lattice packings. These have a simple formula for the density, and as we will see, the shortest vector length of the lattice is related to the density of the corresponding lattice packing.

Definition 2.12. *The density of a lattice $\Lambda \subset \mathbb{R}^n$ is defined as*

$$\Delta(\Lambda) := \frac{V_n \rho^n}{\mathrm{vol}(\Lambda)},$$

where $\rho := \frac{\lambda_1(\Lambda)}{2}$ is the packing radius of the lattice and V_n is the volume of a unit sphere in dimension n.

We denote by Δ_n the maximum lattice density, and by Δ'_n the maximum packing density (not necessarily lattice packing), in dimension n. Motivated by the fact that V_n is just a constant for a given n, we define the center density of a lattice.

Definition 2.13. *The center density of a lattice $\Lambda \subset \mathbb{R}^n$ is defined as*

$$\delta(\Lambda) := \frac{\Delta(\Lambda)}{V_n} = \frac{\lambda_1(\Lambda)^n}{2^n \,\mathrm{vol}(\Lambda)}.$$

We define δ_n as the maximum center density of any lattice in dimension n. The center density is invariant under rotation, reflection and scaling, as the next lemma shows.

Lemma 2.4. *Suppose that $\Lambda \sim \Lambda'$. Then $\delta(\Lambda) = \delta(\Lambda')$.*

Proof. Suppose that M and M' are generator matrices of Λ and Λ', respectively. By definition, we have $M' = \alpha BMU$ where $\alpha > 0$, B is a real orthogonal matrix and U is a unimodular matrix. By Lemma 2.1,

$$\delta(\Lambda') = \frac{\lambda_1(\Lambda')^n}{2^n \operatorname{vol}(\Lambda')} \tag{2.12}$$

$$= \frac{\alpha^n \lambda_1(\Lambda)^n}{2^n \alpha^n \operatorname{vol}(\Lambda)} \tag{2.13}$$

$$= \delta(\Lambda). \tag{2.14}$$

□

In particular, if $\delta(\Lambda) \neq \delta(\Lambda')$, then we can conclude that Λ and Λ' are non-equivalent. The previous lemma shows that when maximizing the center density for a given dimension, one only has to consider volume 1 lattices. Therefore, by Definition 2.13, maximizing $\delta(\Lambda)$ is the same problem as maximizing $\lambda_1(\Lambda)$ over the space of volume 1 lattices.

Definition 2.14. *Define*

$$\mathcal{L}_n := \{\Lambda \subset \mathbb{R}^n : \Lambda \text{ is a lattice such that } \operatorname{vol}(\Lambda) = 1\}.$$

Let us denote by $\lambda_{1,n}$ the maximum shortest vector length of any rank n lattice of volume 1, that is $\lambda_{1,n} := \max_{\Lambda \in \mathcal{L}_n} \lambda_1(\Lambda)$. We define yet another constant, which is called the Hermite constant.

Definition 2.15. *The Hermite constant γ_n in dimension $n \geq 1$ is defined as*

$$\gamma_n := \lambda_{1,n}^2.$$

Equivalently, one has $\gamma_n = 4\delta_n^{2/n} = 4\left(\frac{\Delta_n}{V_n}\right)^{2/n}$. The exact value of the Hermite constant is known only in dimensions 1–8 and 24. However, we have the following bounds, where the lower bound is due to Ball [2] and the upper bound is due to Blichfeldt [4].

Proposition 2.3. *Let $n \geq 2$ be an integer. The Hermite constant γ_n satisfies*

$$\left(\frac{2(n-1)\zeta(n)}{V_n}\right)^{\frac{2}{n}} \leq \gamma_n \leq \left(\frac{2}{\pi}\right)\Gamma\left(2+\frac{n}{2}\right)^{\frac{2}{n}}, \tag{2.15}$$

where ζ is the Riemann zeta function and Γ is the gamma function.

Remark 2.3. Dividing (2.15) by n and taking the limits of the lower and upper bounds as $n \to \infty$, we get that for any $\epsilon > 0$ and sufficiently large n, the linear bounds

$$\frac{1}{2\pi e} - \epsilon \leq \frac{\gamma_n}{n} \leq \frac{1}{\pi e} + \epsilon$$

hold. In [7], the authors assert the even stronger asymptotic bounds

$$\frac{1}{2\pi e} \lesssim \frac{\gamma_n}{n} \lesssim \frac{1.744}{2\pi e}.$$

Figures 2.3 and 2.4 summarize what is known about the shortest vector lengths and center densities of certain standard lattices, and the best known lattice packings. For a list of densest known lattice (and non-lattice) packings in dimensions up to 128, see [7] and [22].

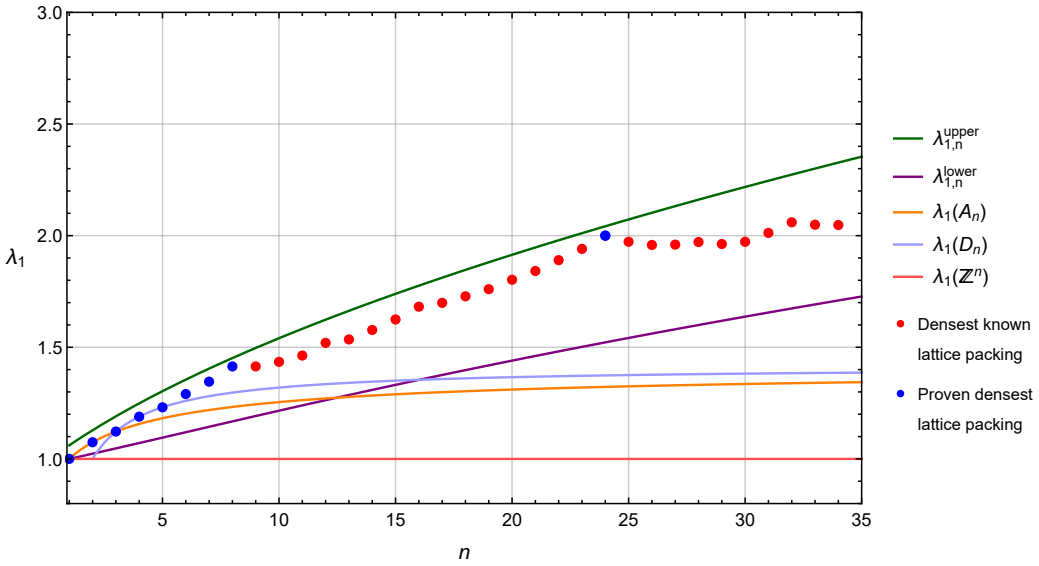


Figure 2.3: Shortest vector lengths for various lattices, and the largest known shortest vector lengths, plotted against dimension. The bounds for $\lambda_{1,n}$ derived from (2.15) are also plotted. The lattices are assumed to have unit volume.

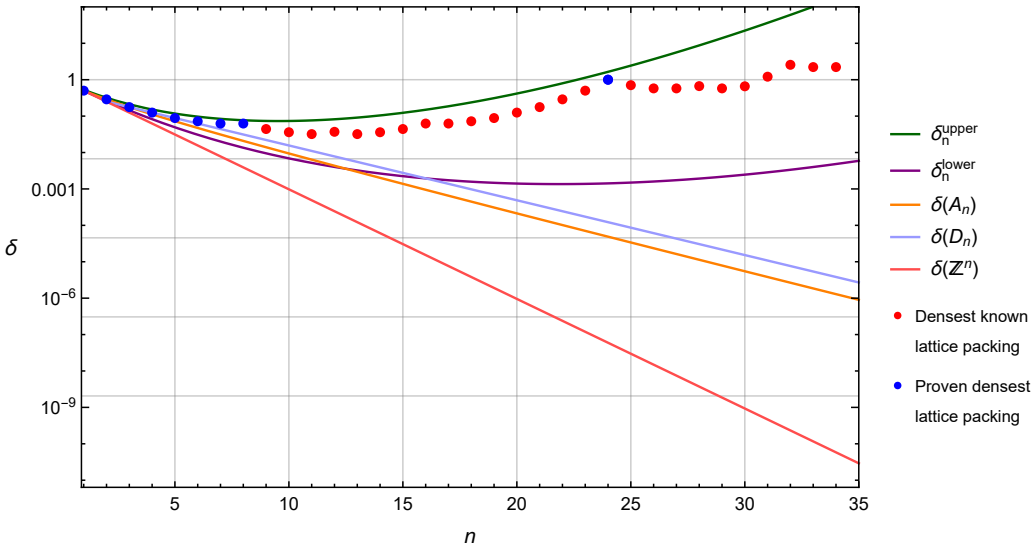


Figure 2.4: Center densities for various lattices, and the largest known center densities, plotted against dimension. The bounds for δ_n derived from (2.15) are also plotted. Notice the logarithmic scaling of the vertical axis.

2.6 Well-rounded lattices

The main focus in this thesis will be on well-rounded lattices. These are characterized by the fact that their set of minimal vectors span the ambient space. Well-rounded lattices are important in applications such as discrete optimization and secure wireless communication. In particular, they have been proposed as good candidates for lattices used in coset codes in wiretap channels [8], [9], [13], [14]. The densest lattice packings are all well-rounded: this follows from the fact that the lattice density function defined on the space of all lattices attains its local extrema at perfect and eutactic lattices, and perfect lattices are always well-rounded [32].

Definition 2.16. *A lattice* $\Lambda \subset \mathbb{R}^n$

(i) is called well-rounded (abbreviated WR) if the $\mathbb{R}$*-span of* $S(\Lambda)$ *is* $\mathbb{R}^n$*.*

(ii) is called strongly well-rounded (abbreviated SWR) if the $\mathbb{Z}$*-span of* $S(\Lambda)$ *is* Λ*.*

(iii) has a basis of minimal vectors if the $\mathbb{Z}$*-span of the linearly independent set* $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq S(\Lambda)$ *is* Λ*.*

An equivalent definition to (i) is the following:

(i') $\Lambda \subset \mathbb{R}^n$ *is well-rounded if and only if* $\lambda_1(\Lambda) = \cdots = \lambda_n(\Lambda)$.

Note that (iii) $\Longrightarrow$ (ii) $\Longrightarrow$ (i). In [17], Martinet proved that all conditions (i), (ii) and (iii) are equivalent in dimension $n \leq 4$, but as the counterexample in [10, pp. 3] shows, when $n \geq 5$, conditions (i) and (ii) are no longer equivalent. In [18], Martinet and Schürmann showed that (ii) $\Longrightarrow$ (iii) in dimension $n \leq 9$, and that in general, (ii) $\not\Longrightarrow$ (iii) in dimension $n \geq 10$.

Note that WR lattices have at least $2n$ shortest vectors, which come in pairs $\pm\mathbf{v} \in S(\Lambda)$. An interesting subset of WR lattices are generic WR lattices, which we define as:

Definition 2.17. *A lattice* $\Lambda \subset \mathbb{R}^n$ *is said to be generic well-rounded (abbreviated GWR), if it is well-rounded and has kissing number* $\kappa(\Lambda) = 2n$.

In other words, GWR lattices are well-rounded lattices with minimal kissing number. A prototypical example of such lattice is the orthogonal lattice $\mathbb{Z}^n$. We will construct some families of GWR lattices in Chapter 5.

Chapter 3

Algebraic number theory

In this chapter, we give a brief introduction to algebraic number theory and introduce lattices constructed from the rings of integers of number fields, and their $\mathbb{Z}$-modules. For an in-depth treatment of algebraic number theory, see for instance Neukirch's book [23] and Milne's notes [19]. Regarding field extensions and Galois theory, Stewart's book [29] serves as a great reference. For a review of the central topics in algebraic number theory, algebraic lattices and lattice code design for wireless communication needs, see *e.g.* [25].

3.1 Field extensions

Definition 3.1. *Let K and L be fields such that $K \subseteq L$. We say that L is a field extension of K and denote it by L/K. We call K the small field and L the large field.*

If L/K is a field extension and $S \subseteq L$, then we denote by $K(S)$ the smallest subfield of L containing $K \cup S$. We say that $K(S)$ is obtained from K by adjoining the set S. If S consists of only one element s, then we say that $K(s)/K$ is a simple extension and call s a primitive element of the extension.

Given a field extension L/K, the larger field L has the structure of a K-vector space, with scalar multiplication defined by

$$(\alpha, x) \mapsto \alpha x \quad \forall \alpha \in K,\ \forall x \in L$$

and vector addition defined by

$$(x, y) \mapsto x + y \quad \forall x, y \in L.$$

Thus, it makes sense to consider the dimension of L as a K-vector space.

Definition 3.2. *Let L/K be a field extension. The dimension of L as a K-vector space is called the degree of the extension, denoted by $[L : K]$.*

If $[L : K] < \infty$, we say that the extension is finite, otherwise we say that it is infinite. If $[L : K] = 1$, then $L = K$ and the extension is said to be trivial. In the special cases $[L : K] = 2$ or 3 we say that L/K is a quadratic or cubic extension, respectively. We are particularly interested in the case $K = \mathbb{Q}$:

Definition 3.3. *A finite extension of $\mathbb{Q}$ is called a number field.*

Sometimes we will say that K is a number field, when in fact we mean that the extension $K/\mathbb{Q}$ is a number field.

Example 3.1. *Consider the number field $K = \mathbb{Q}(i, \sqrt{2})$, obtained from $\mathbb{Q}$ by adjoining $i, \sqrt{2} \in \mathbb{C}$ to it. In this case, any element $\alpha \in K$ can be represented as*

$$\alpha = a_0 + a_1 i + a_2\sqrt{2} + a_3 i\sqrt{2},$$

where the a_i's are in $\mathbb{Q}$. Consequently, a basis for K over $\mathbb{Q}$ is given by $\left\{1, i, \sqrt{2}, i\sqrt{2}\right\}$ and thus, $[K : \mathbb{Q}] = 4$.

It may not be obvious that the extension in the above example is simple, but this is indeed the case: $K = \mathbb{Q}(\theta)$, where $\theta = i + \sqrt{2}$. The inclusion $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(i, \sqrt{2})$ follows from $i + \sqrt{2} \in \mathbb{Q}(i, \sqrt{2})$. For the reverse inclusion, note that $\theta^3 + \theta = 6i$ from which it follows that $i \in \mathbb{Q}(\theta)$. Then $\sqrt{2} = \theta - i \in \mathbb{Q}(\theta)$ as well, proving the equality. In fact, any number field can be represented as a simple extension, as we will see later. Let us first introduce the concept of an algebraic number.

Definition 3.4. *Let L/K be a field extension and $\alpha \in L$. Suppose that there is a non-zero polynomial $p \in K[x]$ such that $p(\alpha) = 0$. Then we say that α is algebraic over K. Otherwise, we say that α is transcendental over K.*

If every element in L is algebraic, we say that L/K is an algebraic extension. For instance, $\sqrt{3}$ is algebraic over $\mathbb{Q}$, since it is a root of $p(x) = x^2 - 3$, a polynomial with coefficients in $\mathbb{Q}$. Given an algebraic $\alpha \in L$, the unique monic polynomial in $K[x]$ of smallest degree satisfying $p(\alpha) = 0$ is called the minimal polynomial of α over K. As an example, consider the number field in Example 3.1. The element $\theta = i + \sqrt{2}$ is a root of the monic and irreducible polynomial $p(x) = x^4 - 2x^2 + 9$, which must be the minimal polynomial of θ over $\mathbb{Q}$.

It can be shown that given an algebraic simple extension $K(\theta)/K$, the degree n of the extension over K is equal to the degree of the minimal polynomial

of θ over K. In this case, a basis is given by $\{1, \theta, \ldots, \theta^{n-1}\}$. The following theorem, which is a special case of the primitive element theorem, shows that any number field is a simple extension.

Theorem 3.1. *Let K be a number field. Then $K = \mathbb{Q}(\theta)$ for some $\theta \in K$ algebraic over $\mathbb{Q}$.*

Let us define the concept of an algebraic integer, which we will need later when defining the ring of integers of a number field.

Definition 3.5. *Let $\alpha \in \mathbb{C}$. If $p(\alpha) = 0$ for some monic non-zero polynomial $p \in \mathbb{Z}[x]$, then we say that α is an algebraic integer.*

Recall the extension in Example 3.1. The element θ is an algebraic integer, since it is the root of a monic polynomial $p(x) = x^4 - 2x^2 + 9$ with integer coefficients.

3.2 Embeddings of a number field into $\mathbb{C}$

The goal in this section is to show how one can embed a number field into the complex numbers. This will be useful when we later define the Minkowski embedding, which we use to injectively map elements of a number field to lattice points in $\mathbb{R}^n$. Let us recall the definition of a field homomorphism.

Definition 3.6. *Let F and K be fields. We call $\psi : F \to K$ a field homomorphism, if it satisfies*

1. *$\psi(x + y) = \psi(x) + \psi(y)$ for all $x, y \in F$*
2. *$\psi(x \cdot y) = \psi(x) \cdot \psi(y)$ for all $x, y \in F$*
3. *$\psi(1_F) = 1_K$ and $\psi(0_F) = 0_K$.*

In particular, it can be shown that a field homomorphism is injective. If K is a number field and $\psi : K \to \mathbb{C}$ is a field homomorphism, then it is not difficult to see that ψ fixes $\mathbb{Q}$.

Definition 3.7. *Let K be a number field. A field homomorphism $\sigma : K \hookrightarrow \mathbb{C}$ is called an embedding of K into $\mathbb{C}$.*

If $K = \mathbb{Q}(\theta)$ is a number field of degree n over $\mathbb{Q}$, then there are exactly n distinct embeddings of K into $\mathbb{C}$, which we denote by $\sigma_1, \ldots, \sigma_n$. Further, each embedding is determined by $\sigma_i(\theta) = \theta_i$, where $\theta_1, \ldots, \theta_n$ are the distinct zeros of the minimal polynomial of θ over $\mathbb{Q}$. To see that σ_i is uniquely determined by $\sigma_i(\theta)$, note that if $\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} \in K$ is

arbitrary, then, due to the properties of a field homomorphism,

$$\sigma_i(\alpha) = a_0 + a_1\sigma_i(\theta) + \cdots + a_{n-1}\sigma_i(\theta)^{n-1}.$$

This shows that $\sigma_i(\theta)$ uniquely determines σ_i. Now suppose that $p_\theta \in \mathbb{Q}[x]$ is the minimal polynomial of θ over $\mathbb{Q}$. Again, due to the properties of a field homomorphism, we have that

$$0 = \sigma_i(0) = \sigma_i(p_\theta(\theta)) = p_\theta(\sigma_i(\theta)) = p_\theta(\theta_i),$$

which shows that θ_i is a root of p_θ. The elements $\theta_1, \ldots, \theta_n$ need not belong to K. Indeed, this is the case for the number field $K = \mathbb{Q}(\sqrt[3]{2})$: the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ is $p(x) = x^3 - 2$, which contains roots in $\mathbb{C} \setminus \mathbb{R}$, but $K \subseteq \mathbb{R}$. If the elements $\theta_1, \ldots, \theta_n$ belong to K, then we say that the extension $K/\mathbb{Q}$ is normal – in the context of field extensions inside $\mathbb{C}$, this is equivalent to say that it is Galois. In this case, we call the θ_i's the Galois conjugates of θ. The embeddings σ_i form a group under function composition – this group is the Galois group, denoted by $\mathrm{Gal}(K/\mathbb{Q})$. If the Galois group is isomorphic to a group G, we say that $K/\mathbb{Q}$ is a G-number field. In particular, if G is abelian or cyclic, we say that $K/\mathbb{Q}$ is an abelian, respectively cyclic, number field.

We will make the distinction between real embeddings, which have image inside $\mathbb{R}$, and complex embeddings, whose image is strictly larger than $\mathbb{R}$. It is worth noting that the complex embeddings come in pairs: if τ is a complex embedding, then so is $\overline{\tau}$. This gives rise to the following definition.

Definition 3.8. *Let K be a degree n number field, and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Let r_1 be the number of real embeddings and r_2 the number of pairs of complex embeddings. Then $n = r_1 + 2r_2$ and (r_1, r_2) is called the signature of K.*

If $r_2 = 0$, then K is called a totally real number field and if $r_1 = 0$, then it is called a totally imaginary number field. Two important notions regarding number fields are the trace and norm of an element.

Definition 3.9. *Let K be a number field and $\alpha \in K$. We define the trace and norm of α, respectively, as*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \cdots + \sigma_n(\alpha)$$

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdots \sigma_n(\alpha).$$

It can be shown that $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha), \mathrm{N}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Q}$ for every $\alpha \in K$.

Example 3.2. *Let us illustrate the concepts defined in this section. Consider the Gaussian rational field $K = \mathbb{Q}(i)$, a quadratic extension over the rationals. There are two embeddings of K into $\mathbb{C}$, defined by $\sigma_1(i) = i$ and $\sigma_2(i) = -i$, where $\pm i$ are the roots of the minimal polynomial of i over $\mathbb{Q}$; namely $p(x) = x^2 + 1$. It is clear that σ_1 is the identity and σ_2 is complex conjugation, so the Galois group is $Gal(K/\mathbb{Q}) = \{id, \sigma_2\} \cong \mathbb{Z}/2\mathbb{Z}$. Given an element $\alpha = p + qi \in K$, we have*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = (p + qi) + (p - qi) = 2p,$$

$$\mathrm{N}_{K/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) \cdot \sigma_2(\alpha) = (p + qi) \cdot (p - qi) = p^2 + q^2.$$

3.3 Rings of integers and their ideals

Recall the definition of an algebraic integer (Definition 3.5). The subset of algebraic integers of a number field forms a ring, which motivates the following definition.

Definition 3.10. *The ring of integers of a number field K is defined as*

$$\mathcal{O}_K := \{\alpha \in K : \alpha \text{ is an algebraic integer}\}.$$

It is not immediate from the definition that $\mathcal{O}_K$ is indeed a ring, but this is not that difficult to prove. It is a fact that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, and therefore, $\mathbb{Z} \subseteq \mathcal{O}_K$ for any number field K. Suppose that K is a number field of degree n over $\mathbb{Q}$. Then, as an abelian group, $K \cong \mathbb{Q}^n$. Similarly, it can be proved that $\mathcal{O}_K \cong \mathbb{Z}^n$ as an abelian group. In particular, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n – there exists a basis $\{\omega_1, \ldots, \omega_n\}$ such that $\mathcal{O}_K$ is the $\mathbb{Z}$-span of this basis. Such a basis is called an integral basis of K. A special kind of an integral basis is a normal integral basis, where the ω_i's are Galois conjugates of each other.

Definition 3.11. *Let $K/\mathbb{Q}$ be a Galois number field and let $G := Gal(K/\mathbb{Q})$ denote its Galois group. If there exists $\omega \in \mathcal{O}_K$ such that $\{g(\omega) : g \in G\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$, we say that $\{g(\omega) : g \in G\}$ is a normal integral basis for K.*

The concept of a normal integral basis will be important when we discuss Lagrangian lattices. A fundamentally important constant of a number field is the discriminant:

Definition 3.12. *Let K be a number field and let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for K. The discriminant of K is defined as $d_K := \det((\sigma_i(\omega_j))_{i,j=1}^n)^2$.*

Equivalently, one can define the discriminant to be

$$d_K := \det((\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i\omega_j))_{i,j=1}^n).$$

The discriminant is an invariant of a number field – it is independent of the choice of an integral basis.

The ring of integers has the important property that non-zero proper ideals factor uniquely as the product of prime ideals. This gives the important Theorem 3.2 presented below. Let us recall that the product of two ideals I and J in a ring R is defined as

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J, n \in \mathbb{N} \right\}.$$

Theorem 3.2. *Let $p \in \mathbb{Z}$ be a prime. The ideal $p\mathcal{O}_K$ factors uniquely as*

$$p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

where $\mathfrak{P}_i$ are prime ideals and $e_i \geq 1$.

If $e_i > 1$ for some i, then we say that p ramifies in K, otherwise p is said to be unramified in K. If $g = 1$ and $e_1 = 1$, then p is said to be inert in K: the ideal $p\mathcal{O}_K$ is prime itself. Finally, if $g = [K : \mathbb{Q}]$ and $e_i = 1$ for all i, we say that p is split in K. A further distinction is made between the cases where p is relatively prime to e_i for all i and when this is not the case. In the former case, we say that p is tamely ramified, and in the latter case we say that it is wildly ramified. If every prime which is ramified is tamely ramified, then K is said to be a tame number field. The reason why we care about tame number fields in this thesis is the following result, which we will use in the context of Lagrangian lattices in Chapter 4.

Proposition 3.1. *Suppose that K is a tame number field. Then*

$$\mathrm{Tr}_{K/\mathbb{Q}} : \mathcal{O}_K \to \mathbb{Z}$$

is a surjection.

For a proof of the proposition, see [21]. The connection between primes ramifying in a number field and its discriminant is given by the following theorem.

Theorem 3.3. *A prime $p \in \mathbb{Z}$ ramifies in a number field K if and only if $p \mid d_K$.*

Let us illustrate the concepts defined in this section.

Example 3.3. *Consider the quadratic number field $K = \mathbb{Q}(i)$ from Example 3.2. The ring of integers of K is the Gaussian integers, $\mathcal{O}_K = \mathbb{Z}[i]$. An integral basis for K is $\{\omega_1, \omega_2\} = \{1, i\}$ and the discriminant of K can be computed as*

$$d_K = \begin{bmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(\omega_1^2) & \mathrm{Tr}_{K/\mathbb{Q}}(\omega_1\omega_2) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\omega_2\omega_1) & \mathrm{Tr}_{K/\mathbb{Q}}(\omega_2^2) \end{bmatrix} = \begin{bmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(1) & \mathrm{Tr}_{K/\mathbb{Q}}(i) \\ \mathrm{Tr}_{K/\mathbb{Q}}(i) & \mathrm{Tr}_{K/\mathbb{Q}}(-1) \end{bmatrix} = -4,$$

where we used the result $\mathrm{Tr}_{K/\mathbb{Q}}(p + qi) = 2p$ for all $p + qi \in K$.

Since $2 \mid d_K$, the prime $p = 2$ is ramified in K by Theorem 3.3. Indeed,

$$\langle 2 \rangle = \langle 1 + i \rangle^2 .$$

On the other hand, $p = 5$ is split in K, since

$$\langle 5 \rangle = \langle 1 + 2i \rangle \langle 1 - 2i \rangle .$$

3.4 Lattices from number fields

Our goal is to represent elements of a number field K, with degree n over $\mathbb{Q}$, as lattice points in $\mathbb{R}^n$. To do this, we need a certain embedding of K into $\mathbb{R}^n$, called the Minkowski embedding.

Definition 3.13. *Let K be a number field of degree n and let $\{\sigma_1, \ldots, \sigma_{r_1}\}$ be the real embeddings of K into $\mathbb{C}$ and let $\{\sigma_{r_1+i}, \sigma_{r_1+r_2+i}\}$ for $1 \leq i \leq r_2$ be the pairs of complex embeddings of K into $\mathbb{C}$. The Minkowski embedding $\sigma : K \to \mathbb{R}^n$ is defined as*

$$x \mapsto (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x))^T.$$

Now we are ready to present how one can construct a lattice from the ring of integers of a number field using the Minkowski embedding.

Theorem 3.4. *Let K be a degree n number field and let $\mathcal{O}_K$ be its ring of integers. Let $\sigma : K \to \mathbb{R}^n$ be the Minkowski embedding. Then $\Lambda_K := \sigma(\mathcal{O}_K)$ is a full rank lattice in $\mathbb{R}^n$. Further, if $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for K, then a basis for Λ_K is given by $\{\sigma(\omega_1), \ldots, \sigma(\omega_n)\}$.*

Proof. The vectors $\sigma(\omega_1), \ldots, \sigma(\omega_n)$ are linearly independent. To see this, define $B := (\sigma(\omega_1), \cdots, \sigma(\omega_n)) \in \mathbb{R}^{n \times n}$ and note that $|\det(B)| =$

$2^{-r_2}\sqrt{|d_K|} \neq 0$. We can write $\mathcal{O}_K = \{\sum_{i=1}^{n} a_i\omega_i : a_i \in \mathbb{Z}\}$. Then since σ is $\mathbb{Z}$-linear,

$$\Lambda_K = \sigma(\mathcal{O}_K) = \left\{ \sum_{i=1}^{n} a_i\sigma(\omega_i) : a_i \in \mathbb{Z} \right\},$$

which is full rank lattice in $\mathbb{R}^n$ with a basis $\{\sigma(\omega_1), \ldots, \sigma(\omega_n)\}$. □

The theorem above applies not only to $\mathcal{O}_K$, but any $\mathbb{Z}$-module M of full rank in $\mathcal{O}_K$. Further, if M is a free $\mathbb{Z}$-module with a basis $\{\gamma_1, \ldots, \gamma_n\}$, then $\Lambda_M := \sigma(M)$ is a full rank lattice in $\mathbb{R}^n$ with basis vectors $\sigma(\gamma_1), \ldots, \sigma(\gamma_n)$. It is well-known that non-zero ideals of rings of integers satisfy this property: they are isomorphic to $\mathbb{Z}^n$ as abelian groups. Thus, we have the notion of an ideal lattice, which we denote by $\Lambda_I := \sigma(I)$.

The usefulness of constructing lattices from number fields is that many of the properties of the lattice, such as volume, diversity (minimum number of non-zero components in a non-zero lattice vector) and vector lengths are easily computed using the properties of the number field. For instance, consider a totally real number field K and a $\mathbb{Z}$-module $M \subseteq \mathcal{O}_K$ of full rank. If we want to compute the inner product of lattice vectors $\mathbf{x} = \sigma(\alpha), \mathbf{y} = \sigma(\beta) \in \Lambda_M$ for some $\alpha, \beta \in M$, we can just compute

$$\langle \mathbf{x}, \mathbf{y} \rangle = \langle \sigma(\alpha), \sigma(\beta) \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\beta).$$

In particular, $\|\mathbf{x}\|^2 = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2)$ and $\lambda_1^2(\Lambda_M) = \min_{\alpha \in M \setminus \{0\}} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^2)$. If K is totally imaginary, then $\|\mathbf{x}\|^2 = \frac{1}{2}\,\mathrm{Tr}_{K/\mathbb{Q}}(\alpha\overline{\alpha})$.

Let us end this chapter by giving an example of a lattice constructed from the ring of integers of a number field.

Example 3.4. *Consider the totally imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-3})$. It is well-known that K has an integral basis $\{\omega_1, \omega_2\} = \left\{1, \frac{1+\sqrt{-3}}{2}\right\}$. The embeddings $K \hookrightarrow \mathbb{C}$ consist of the identity map and complex conjugation. Thus, given $x \in K$, we have $\sigma(x) = (\Re(x), \Im(x))$. A generator matrix for Λ_K is given by*

$$M = \begin{bmatrix} \Re(\omega_1) & \Re(\omega_2) \\ \Im(\omega_1) & \Im(\omega_2) \end{bmatrix} = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{bmatrix},$$

which is a generator matrix for the hexagonal lattice Λ_h (see Figure 2.1(b)).

It has been shown (see [12]) that Λ_K is WR if and only if K is a cyclotomic extension. In the example above, $\Lambda_K = \Lambda_h$ is WR. Indeed, $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive third root of unity.

Chapter 4

Lagrangian lattices

In this chapter, we take a look at a certain family of lattices called Lagrangian lattices, and their sublattices. Lagrangian lattices arise naturally from specific types of number fields via the Minkowski embedding. In fact, the term Lagrangian basis is used in [6, pp. 193] to describe a normal integral basis $\{\omega_1, \ldots, \omega_n\}$ of a tame, cyclic number field $K/\mathbb{Q}$ of odd prime degree, such that $\mathrm{Tr}_{K/\mathbb{Q}}(\omega_1) = -1$ and the matrix

$$G := (\mathrm{Tr}_{K/\mathbb{Q}}(\omega_i \omega_j))_{i,j=1}^{n} \tag{4.1}$$

has a certain shape.

When K is totally real, the matrix (4.1) can be recognized as a Gram matrix of the lattice $\Lambda_K = \sigma(\mathcal{O}_K)$, where σ is the Minkowski embedding. Thus, it makes sense to study the lattice we obtain from a Lagrangian basis of a number field. The authors in [10] use the term Lagrangian lattice to describe such a lattice (the precise definition is given later).

In addition to capturing key properties of certain number fields, Lagrangian lattices are interesting in their own right. Moreover, they are useful for constructing sublattices possessing a basis of minimal vectors and thus being (strongly) well-rounded. In [10], the authors show how one can construct sublattices of a Lagrangian lattice via a certain linear transformation, and further give a condition involving the parameters of the sublattice and the Lagrangian lattice, such that when the condition is satisfied, the sublattice is well-rounded and possesses a minimal basis.

We will see that the sublattices of a Lagrangian lattice are not only well-rounded but generic well-rounded, under a certain assumption. Further, we will show that the center density of a WR sublattice of a Lagrangian lattice

never exceeds that of the A_n lattice, and give conditions under which the sublattice is indeed equivalent to A_n or $\mathbb{Z}^n$. We give an explicit construction of A_n as a sublattice of a Lagrangian lattice in any dimension $n \geq 2$. Relaxing some of the conditions in the definition of a Lagrangian lattice, we are able to construct denser lattices. We will give examples of densest lattices in some particular dimensions constructed from certain linear maps. We also investigate the dual lattice of a Lagrangian lattice and its WR sublattices.

4.1 Motivation

We start by giving the definition of a Lagrangian lattice, as defined in [10]. This definition does not involve any algebraic number theory.

Definition 4.1. *Let $n \geq 1$ be an integer and $\mathcal{L} \subset \mathbb{R}^n$ a lattice. We call the lattice $\mathcal{L}$ Lagrangian if there exists a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of $\mathcal{L}$ and a non-zero vector $\mathbf{v}_1 \in \mathcal{L} \cap \mathcal{L}^*$ such that*

1. $\sum_{i=1}^{n} \mathbf{e}_i = \mathbf{v}_1$
2. $\langle \mathbf{e}_i, \mathbf{v}_1 \rangle = 1$ *for all* $1 \leq i \leq n$
3. $\langle \mathbf{e}_i, \mathbf{e}_i \rangle = a$ *for all* $1 \leq i \leq n$
4. $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = -h$ *for all* $1 \leq i \neq j \leq n$.

In this case, we call $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ a Lagrangian basis for $\mathcal{L}$.

Conditions 3 and 4 give an explicit expression for the Gram matrix of the Lagrangian lattice with respect to the basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$:

$$G = \begin{bmatrix} a & -h & \ldots & -h \\ -h & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & -h \\ -h & \ldots & -h & a \end{bmatrix}. \tag{4.2}$$

Moreover, the conditions imply that $a - h(n-1) = 1$. Indeed, substituting 1 into 2 gives

$$\langle \mathbf{e}_i, \mathbf{e}_1 + \cdots + \mathbf{e}_n \rangle = a - h(n-1) = 1,$$

for any $i \in \{1, \ldots, n\}$. Conversely, if $\Lambda \subset \mathbb{R}^n$ is a lattice with Gram matrix of the form (4.2) with respect to a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$, and $a - h(n-1) = 1$, then it is Lagrangian with a Lagrangian basis given by $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Indeed, conditions 3 and 4 are trivially satisfied, and taking $\mathbf{v}_1 = \mathbf{b}_1 + \cdots + \mathbf{b}_n \in \Lambda \cap \Lambda^*$ we find that conditions 1 and 2 are satisfied as well.

Given a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, the vector $\mathbf{v}_1 \in \mathcal{L} \cap \mathcal{L}^*$ is implicitly determined by condition 1. Thus, we will in the sequel omit writing it if clarity is not sacrificed.

Example 4.1. *The lattice $\mathbb{Z}^n$ is a standard example of a Lagrangian lattice, with $(a, h) = (1, 0)$. The planar hexagonal lattice Λ_h is another example of a Lagrangian lattice, with $(a, h) = (2, 1)$.*

The volume of a Lagrangian lattice takes a simple form, as we show next.

Lemma 4.1. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a Lagrangian lattice with a Lagrangian basis $\mathcal{B} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Let $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Then*

$$\mathrm{vol}(\mathcal{L}) = (a + h)^{\frac{n-1}{2}}.$$

Proof. The Lagrangian lattice $\mathcal{L}$ has the following Gram matrix with respect to the basis $\mathcal{B} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$:

$$G_{\mathcal{B}} = \begin{bmatrix} a & -h & \ldots & -h \\ -h & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & -h \\ -h & \ldots & -h & a \end{bmatrix},$$

which has the well-known determinant

$$\det(G_{\mathcal{B}}) = (a + h)^n - nh(a + h)^{n-1} = (a + h)^{n-1}(a + h(1 - n)).$$

We have $a + h(1 - n) = 1$ and thus,

$$\mathrm{vol}(\mathcal{L}) = \sqrt{\det(G_{\mathcal{B}})} = \sqrt{(a + h)^{n-1}} = (a + h)^{\frac{n-1}{2}},$$

as desired. □

Remark 4.1. If $\mathcal{L} \subset \mathbb{R}^n$ is a Lagrangian lattice, then its Gram matrix $G_{\mathcal{B}}$ is a positive definite matrix, and thus $\det(G_{\mathcal{B}}) = (a + h)^{n-1} > 0$ and in particular, the inequality $a + h > 0$ and equation $a + h(1 - n) = 1$ imply $a > \frac{1}{n}$ and $h > \frac{-1}{n}$.

Let us now see how Lagrangian lattices emerge from number fields. Recall the definition of a normal integral basis (Definition 3.11). A theorem by Hilbert and Speiser tells that an abelian number field possesses a normal integral basis if and only if it is tame. We will use this and the fact that a Galois number field of prime degree is always cyclic, in the following claim.

Claim 4.1. *Consider a tame, cubic number field K, Galois over $\mathbb{Q}$. Then $\Lambda_K = \sigma(\mathcal{O}_K)$ has a Lagrangian basis.*

Proof. Let $\mathrm{Gal}(K/\mathbb{Q}) = \{id, \theta, \theta^2\}$ be the Galois group of K over $\mathbb{Q}$ and $\{e_1, e_2, e_3\}$ a normal integral basis for K, where $e_2 = \theta(e_1)$ and $e_3 = \theta^2(e_1)$ are the Galois conjugates of e_1. By Lemma 3.1, the trace $\mathrm{Tr}_{K/\mathbb{Q}} : \mathcal{O}_K \to \mathbb{Z}$ is surjective. Therefore, $\mathrm{Tr}_{K/\mathbb{Q}}(e_1)$ must be a generator of $\mathbb{Z}$, hence, replacing $-e_1$ with e_1 if necessary,

$$\mathrm{Tr}_{K/\mathbb{Q}}(e_1) = e_1 + e_2 + e_3 = 1. \tag{4.3}$$

A basis for the lattice Λ_K corresponding to the basis $\{e_1, e_2, e_3\}$ is given by the vectors

$$\mathbf{b}_1 = (e_1, \theta(e_1), \theta^2(e_1))^T = (e_1, e_2, e_3)^T, \tag{4.4}$$
$$\mathbf{b}_2 = (e_2, \theta(e_2), \theta^2(e_2))^T = (e_2, e_3, e_1)^T, \tag{4.5}$$
$$\mathbf{b}_3 = (e_3, \theta(e_3), \theta^2(e_3))^T = (e_3, e_1, e_2)^T. \tag{4.6}$$

Thus, it is easily checked that $a := \|\mathbf{b}_i\|^2 = e_1^2 + e_2^2 + e_3^2$ and $-h := \langle \mathbf{b}_i, \mathbf{b}_j \rangle = e_1e_2 + e_2e_3 + e_1e_3$ for all $1 \leq i \neq j \leq 3$. The Gram matrix of Λ_K with respect to this basis takes the form

$$G = \begin{bmatrix} a & -h & -h \\ -h & a & -h \\ -h & -h & a \end{bmatrix},$$

which shows that conditions 3 and 4 of a Lagrangian lattice are met. For conditions 1 and 2, define $\mathbf{v}_1 := \sigma(1) = (1, 1, 1)^T \in \Lambda_K \cap \Lambda_K^*$ and note that by equation (4.3),

$$\mathbf{b}_1 + \mathbf{b}_2 + \mathbf{b}_3 = \mathbf{v}_1$$

and similarly, $\langle \mathbf{b}_i, \mathbf{v}_1 \rangle = 1$ for all $i = 1, 2, 3$. This proves that Λ_K is a Lagrangian lattice with a Lagrangian basis $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3\}$. □

Remark 4.2. Note that in the above claim, $a, h \in \mathbb{Z}$ since $\mathrm{Tr}_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$, so the lattice is integral. Moreover, $d_K = \det(G) = (a + h)^2$.

The above result is a special case of a more general theorem by Conner and Perlis [6], which states the following.

Theorem 4.1. *Let $K/\mathbb{Q}$ be a Galois number field of prime degree, which is tame. Then $\Lambda_K = \sigma(\mathcal{O}_K)$ is a Lagrangian lattice.*

The condition that K is tame is necessary, as the following example shows.

Claim 4.2. *Let ζ be a primitive ninth root of unity and let $L = \mathbb{Q}(\zeta)$ be the cyclotomic extension of degree $[L : \mathbb{Q}] = \phi(9) = 6$ over $\mathbb{Q}$. Let $K = \mathbb{Q}(\zeta+\zeta^{-1})$ be the maximal real subfield of L. Then K is a cubic Galois number field such that Λ_K does not have a Lagrangian basis.*

Proof. To see that $K/\mathbb{Q}$ is cubic, note that $p(x) = (x-\zeta)(x-\zeta^{-1}) = x^2-(\zeta+\zeta^{-1})x+1$ is the minimal polynomial of ζ over K, so that $[L : K] = 2$ and thus $[K : \mathbb{Q}] = 3$. One can compute the minimal polynomial of $\zeta + \zeta^{-1}$ over $\mathbb{Q}$; it is

$$f(x) = x^3 - 3x + 1,$$

the roots of which are given by $\alpha_1 = \zeta+\zeta^{-1}$, $\alpha_2 = \zeta^2+\zeta^{-2}$ and $\alpha_3 = \zeta^4+\zeta^{-4}$, all of which are in K. Thus, K is Galois, and the Galois group is cyclic.

The ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[\zeta + \zeta^{-1}]$, with a (non-normal) integral basis $\{1, \alpha_1, \alpha_2\}$. We have that $\mathrm{Tr}_{K/\mathbb{Q}}(1) = 3$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^2) = \sum_{i=1}^3 \alpha_i^2 = 6$ for $i = 1, 2$. Moreover, $\mathrm{Tr}_{K/\mathbb{Q}}(1 \cdot \alpha_i) = \sum_{i=1}^3 \alpha_i = 0$ for $i = 1, 2$ and $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_2) = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = -3$. Therefore, the discriminant of K is the determinant of the matrix

$$G = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & -3 \\ 0 & -3 & 6 \end{bmatrix},$$

which is $d_K = \det(G) = 3^4$. There cannot exist a Lagrangian basis for Λ_K, since otherwise there would exist a pair of integers a, h such that $d_K = (a+h)^2$ and $a - 2h = 1$, or

$$3^4 = d_K = (3h + 1)^2,$$

a contradiction. □

In the above example, the number field K is not tame since $3 \mid d_K$, and therefore, no normal integral basis for K exists.

4.2 Well-rounded sublattices

Now that we have seen how Lagrangian lattices can be constructed from number fields, let us proceed to investigate the Lagrangian lattices, and their sublattices, themselves. Our goal in this section is to build upon the results presented in [10]. We begin by introducing an important map which we will use often.

Definition 4.2. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice and $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$ a non-trivial linear map. Let r, s be integers, $\mathbf{v}_1 \in \mathcal{L} \setminus \ker \mathrm{T}$ and $m := r + s\,\mathrm{T}(\mathbf{v}_1)$. Define*

$\Phi_{(r,s)} : \mathcal{L} \to \mathcal{L}$ *to be the linear map*

$$\mathbf{x} \mapsto r\mathbf{x} + s\,\mathrm{T}(\mathbf{x})\mathbf{v}_1.$$

Define the lattice $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$ *to be the image of* $\mathcal{L}$ *under the map* $\Phi_{(r,s)}$*:*

$$\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1} := \Phi_{(r,s)}(\mathcal{L}).$$

In [10, Proposition 3.1], it is proven that if r and m are non-zero, then $\Phi_{(r,s)}$ is an injection. A direct consequence of this is the following lemma [10, Corollary 3.2].

Lemma 4.2. *Assume that* $\mathcal{L}$, T *and* $\mathbf{v}_1$ *are as in Definition 4.2 and* r, s *are integers such that* $0 < |r| < |\,\mathrm{T}(\mathbf{v}_1)|$*. Then* $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$ *is a full rank sublattice of* $\mathcal{L}$*.*

In particular, if the conditions in the above lemma are satisfied, then if $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is a basis for $\mathcal{L}$, then $\left\{\Phi_{(r,s)}(\mathbf{e}_1), \ldots, \Phi_{(r,s)}(\mathbf{e}_n)\right\}$ is a basis for $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$. We will be particularly interested in the following linear map:

$$\mathrm{T}_{\mathbf{v}_1} : \mathcal{L} \to \mathbb{Z}, \quad \mathrm{T}_{\mathbf{v}_1}(\mathbf{x}) = \langle \mathbf{x}, \mathbf{v}_1 \rangle,$$

where $0 \neq \mathbf{v}_1 \in \mathcal{L} \cap \mathcal{L}^*$. We define

$$\mathcal{L}^{(r,s)}_{\mathbf{v}_1} := \mathcal{L}^{(r,s)}_{\mathrm{T}_{\mathbf{v}_1},\mathbf{v}_1}.$$

We return later to the general T, but for now, we let $\mathrm{T} := \mathrm{T}_{\mathbf{v}_1}$.

From now on, we will consider the case when $\mathcal{L}$ is Lagrangian with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ such that $\mathbf{v}_1 = \sum_{i=1}^n \mathbf{e}_i$. It is worth noting that in this case, $\mathrm{T}(\mathbf{v}_1) = \|\mathbf{v}_1\|^2 = n$. The next theorem (Theorem 4.9 in [10]) gives a condition which tells when $\mathcal{L}^{(r,s)}_{\mathbf{v}_1}$ is WR.

Theorem 4.2. *Let* $n \geq 2$ *be an integer and* $\mathcal{L} \subset \mathbb{R}^n$ *a Lagrangian lattice with a Lagrangian basis* $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$*. Let* $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ *and* $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$*. Let* r, s *be integers such that* $0 \neq |r| < n$ *and let* $m = r + sn$*. Suppose that*

$$\frac{na-1}{n^2-1} \leq \left(\frac{m}{r}\right)^2 \leq \frac{(na-1)(n+1)}{n-1}. \tag{4.7}$$

Then $\mathcal{L}^{(r,s)}_{\mathbf{v}_1}$ *is a full rank sublattice of* $\mathcal{L}$ *of index* $|mr^{n-1}|$*, with minimum*

$$\lambda_1^2(\mathcal{L}^{(r,s)}_{\mathbf{v}_1}) = ar^2 + \frac{m^2 - r^2}{n}$$

and a basis of minimal vectors $\{r\mathbf{e}_1 + s\mathbf{v}_1, \ldots, r\mathbf{e}_n + s\mathbf{v}_1\}$*.*

The proof of the theorem in [10] shows actually more: the set of minimal vectors is $S(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \{\pm(r\mathbf{e}_i + s\mathbf{v}_1) : 1 \leq i \leq n\}$, *i.e.* $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is in fact GWR given that (4.7) holds with a strict inequality on the right-hand side. The proof follows almost directly from Theorem 4.6, Proposition 4.7 and Corollary 4.8 in [10], but for the sake of completeness, we give the proof here.

Theorem 4.3. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Let $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Let r, s be integers such that $0 \neq |r| < n$ and let $m = r + sn$. Suppose that*

$$\frac{na-1}{n^2-1} \leq \left(\frac{m}{r}\right)^2 < \frac{(na-1)(n+1)}{n-1}.$$

Then $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is GWR.

Proof. Define the function $f : \mathcal{L} \setminus \{0\} \to \mathbb{R}^+$ by $f(\alpha) = A\,\|\alpha\|^2 + B\,\mathrm{T}(\alpha)^2$, where $A = r^2$ and $B = \frac{m^2 - r^2}{n}$. As Proposition 3.10 in [10] shows, $f(\alpha) = \left\|\Phi_{(r,s)}(\alpha)\right\|^2$ for every $\alpha \in \mathcal{L}$. Theorem 4.2 tells that

$$\lambda_1^2(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \min_{\alpha \in \mathcal{L}\setminus\{0\}} f(\alpha) = Aa + B$$

and that the minimum of f is achieved by $\pm\mathbf{e}_i$, $1 \leq i \leq n$, a total of $2n$ vectors. Note that these vectors correspond to $\pm(r\mathbf{e}_i + s\mathbf{v}_1)$ in the lattice $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$. We need to prove that no other vector $\alpha \in \mathcal{L} \setminus \{0\}$ achieves the minimum. Consider the partition $\mathcal{L} = \cup_{d\in\mathbb{Z}} S_d$, where $S_d = \{\mathbf{x} \in \mathcal{L} : \mathrm{T}(\mathbf{x}) = d\}$, for each $d \in \mathbb{Z}$. We may write

$$\lambda_1^2(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \min_{d \geq 0} \left(\min_{\alpha \in S_d \setminus \{0\}} f(\alpha) \right).$$

Consider different values for d. If $d = 0$, then

$$\min_{\alpha \in S_0\setminus\{0\}} f(\alpha) = \min_{\alpha \in S_0\setminus\{0\}} A\,\|\alpha\|^2 = 2A(a+h)$$

as Corollary 3.20 in [10] shows. But since by assumption we have the strict inequality $Aa + B < 2A(a+h)$, no element in $S_0 \setminus \{0\}$ achieves the minimum.

Consider $d > 0$. Let k be the residue class of d modulo n and $c = (d-k)/n$. Theorem 4.4 in [10] gives that

$$\min_{\alpha \in S_d\setminus\{0\}} f(\alpha) = f(E_I) + c^2 f(\mathbf{v}_1) + 2ck(A + nB)$$

where $I \subseteq \{1, \ldots, n\}$ and $|I| = k$ and $E_I = \sum_{i \in I} \mathbf{e}_i$. In the case $c \neq 0$ we have

$$\min_{\alpha \in S_d \setminus \{0\}} f(\alpha) = f(E_I) + c^2 f(\mathbf{v}_1) + 2ck(A + nB) > f(\mathbf{v}_1) \geq Aa + B$$

where the last inequality is equivalent to the inequality $\frac{na-1}{n^2-1} \leq \left(\frac{m}{r}\right)^2$. So in this case, the minimum is not achieved. In the case $c = 0$ we have $k \neq 0$ and

$$\min_{\alpha \in S_d \setminus \{0\}} f(\alpha) = f(E_I).$$

By Proposition 4.7 in [10] we have $f(E_I) \geq Aa+B$ and since $f(E_I) > f(\mathbf{e}_i) = Aa + B$ when $|I| > 1$, equality holds if and only if $|I| = 1$. To conclude,

$$\lambda_1^2(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \min_{d \geq 0} \left(\min_{\alpha \in S_d \setminus \{0\}} f(\alpha) \right)$$

is achieved by $\pm \mathbf{e}_i \in \mathcal{L} \setminus \{0\}$, where $1 \leq i \leq n$, but by no other vectors in $\mathcal{L} \setminus \{0\}$ proving that $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is GWR. □

The interesting case is when the upper bound in (4.7) is achieved; then, $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is no longer GWR. Instead, $\kappa(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = n(n+1)$ as Theorem 4.4 tells.

Theorem 4.4. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Let $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Let r, s be integers such that $0 \neq |r| < n$ and let $m = r + sn$. Suppose that*

$$\left(\frac{m}{r}\right)^2 = \frac{(na-1)(n+1)}{n-1}.$$

Then $\kappa(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = n(n+1)$. In particular, $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is not GWR.

Proof. Note that $\lambda_1^2(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \min_{d \geq 0} \left(\min_{\alpha \in S_d \setminus \{0\}} f(\alpha)\right)$ is now achieved by the $2n$ elements $\pm \mathbf{e}_i$, for $1 \leq i \leq n$, in S_1 and also by the shortest vectors in $S_0 \cong \sqrt{a+h} A_{n-1}$ (see Theorem 3.19 in [10]). As the lattice A_{n-1} has kissing number $\kappa(A_{n-1}) = n(n-1)$, and the sets S_0 and S_1 are disjoint, we must have

$$\kappa(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = n(n-1) + 2n = n(n+1),$$

proving the claim. □

Since $\kappa(A_n) = n(n+1)$, the previous theorem says that $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ has the same kissing number as A_n, when the equality occurs.

4.3 Center density of sublattices

We know the kissing number and shortest vector length of a WR sublattice $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ of a Lagrangian lattice $\mathcal{L}$. The next natural question to ask is: what is the sphere packing density? Additionally, how large of a packing density can such a lattice have? These are questions that we answer in this section.

Proposition 4.1. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Let $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Let r, s be integers such that $0 \neq |r| < n$ and let $m = r + sn$. Suppose that*

$$\frac{na-1}{n^2-1} \leq \left(\frac{m}{r}\right)^2 \leq \frac{(na-1)(n+1)}{n-1}.$$

Then the center density of $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is given by

$$\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \frac{((na-1)r^2+m^2)^{n/2}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}|mr^{n-1}|}.$$

Proof. Note that by Lemma 4.1 and Theorem 4.2,

$$\operatorname{vol}(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \operatorname{vol}(\mathcal{L})[\mathcal{L} : \mathcal{L}_{\mathbf{v}_1}^{(r,s)}] = (a+h)^{\frac{n-1}{2}}|mr^{n-1}|.$$

Using the definition of center density and the expression for the shortest vector length of $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$, we get

$$\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \frac{\lambda_1^2(\mathcal{L}_{\mathbf{v}_1}^{(r,s)})^{n/2}}{2^n \operatorname{vol}(\mathcal{L}_{\mathbf{v}_1}^{(r,s)})} \tag{4.8}$$

$$= \frac{\left(ar^2 + \frac{m^2-r^2}{n}\right)^{n/2}}{2^n(a+h)^{\frac{n-1}{2}}|mr^{n-1}|} \tag{4.9}$$

$$= \frac{((na-1)r^2+m^2)^{n/2}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}|mr^{n-1}|} \tag{4.10}$$

as desired. □

Next we will derive bounds for the center density of a lattice of the form $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$, using elementary calculus. The following lemma will turn out useful.

Lemma 4.3. *Let $n \geq 2$ be an integer and let $a > \frac{1}{n}$. Define*

$$l := \frac{na-1}{n^2-1}, \tag{4.11}$$

$$u := \frac{(na-1)(n+1)}{n-1}. \tag{4.12}$$

Then the real-valued function $f : [l, u] \to \mathbb{R}$ defined by

$$f(x) = \frac{(na - 1 + x)^n}{x}$$

has a maximum point at $x = u$ and the maximum value is

$$f(u) = 2^n n^n (na - 1)^{n-1} (n - 1)^{1-n} (n + 1)^{-1}.$$

Further, f has a minimum point at $x = x_0 := \frac{na-1}{n-1}$ and the minimum value is

$$f(x_0) = n^n (na - 1)^{n-1} (n - 1)^{1-n}.$$

Proof. As a differentiable function, f achieves its extreme values at the endpoints of $[l, u]$ or at a point where f' vanishes. A simple calculation shows that

- $f(l) = n^{2n}(na - 1)^{n-1}(n^2 - 1)^{1-n}$
- $f(u) = 2^n n^n (na - 1)^{n-1} (n - 1)^{1-n} (n + 1)^{-1}$
- $f'(x) = \frac{(na+x-1)^{n-1}((n-1)x-na+1)}{x^2}$ and thus $f'(x) = 0$ if and only if

$$x = 1 - na \quad \text{or} \quad x = \frac{na - 1}{n - 1}.$$

The first equality is impossible since $na > 1$ by assumption, and negative solutions are not allowed since $l > 0$. This leaves us with a single zero for the derivative, $x_0 = \frac{na-1}{n-1} \in [l, u]$. The value of the function at this point is

$$f(x_0) = n^n (na - 1)^{n-1} (n - 1)^{1-n}.$$

Note that

$$\frac{f(u)}{f(l)} = \frac{2^n}{(n+1)^2} \left(1 + \frac{1}{n}\right)^n \geq \frac{2^2}{(2+1)^2} \left(1 + \frac{1}{2}\right)^2 = 1,$$

when $n \geq 2$. Similarly,

$$\frac{f(l)}{f(x_0)} = n^n (n + 1)^{1-n} \geq 2^2 (2 + 1)^{1-2} = \frac{4}{3} > 1,$$

when $n \geq 2$. Since f is positive, it follows that

$$f(x_0) < f(l) \leq f(u),$$

proving the lemma. □

The previous lemma allows us to derive bounds for the center density of $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$.

Proposition 4.2. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Let $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Let r, s be integers such that $0 \neq |r| < n$ and let $m = r + sn$. Suppose that*

$$\frac{na-1}{n^2-1} \leq \left(\frac{m}{r}\right)^2 \leq \frac{(na-1)(n+1)}{n-1}.$$

Then

$$\frac{1}{2^n} \leq \delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) \leq \frac{1}{2^{n/2}\sqrt{n+1}}.$$

Further, the lower bound is achieved when

$$\left(\frac{m}{r}\right)^2 = \frac{na-1}{n-1}$$

and the upper bound is achieved when

$$\left(\frac{m}{r}\right)^2 = \frac{(na-1)(n+1)}{n-1}.$$

Proof. Proposition 4.1 gives the center density as

$$\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \frac{((na-1)r^2 + m^2)^{n/2}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}|mr^{n-1}|} \tag{4.13}$$

$$= \frac{\left(na - 1 + \left(\frac{m}{r}\right)^2\right)^{n/2}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}\left|\frac{m}{r}\right|}. \tag{4.14}$$

The condition for $q := (m/r)^2$ is satisfied when $q \in [l, u]$, where l and u are defined as in Lemma 4.3. Note that we have

$$\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) = \frac{\sqrt{f(q)}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}}, \tag{4.15}$$

where $f : [l, u] \to \mathbb{R}$ is the function defined in Lemma 4.3. It follows from

the previous lemma, where $x_0 = \frac{na-1}{n-1}$, that

$$\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) \geq \frac{\sqrt{f(x_0)}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}} \tag{4.16}$$

$$= \frac{\sqrt{f(x_0)}}{2^n n^{n/2}(a+\frac{a-1}{n-1})^{\frac{n-1}{2}}} \tag{4.17}$$

$$= \frac{n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}}{2^n n^{n/2}(a+\frac{a-1}{n-1})^{\frac{n-1}{2}}} \tag{4.18}$$

$$= \frac{n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}}{2^n n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}} \tag{4.19}$$

$$= \frac{1}{2^n}, \tag{4.20}$$

and

$$\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) \leq \frac{\sqrt{f(u)}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}} \tag{4.21}$$

$$= \frac{\sqrt{f(u)}}{2^n n^{n/2}(a+\frac{a-1}{n-1})^{\frac{n-1}{2}}} \tag{4.22}$$

$$= \frac{2^{n/2} n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}(n+1)^{-1/2}}{2^n n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}} \tag{4.23}$$

$$= \frac{1}{2^{n/2}\sqrt{n+1}}, \tag{4.24}$$

proving the claim. □

Remark 4.3. Since $\delta(A_n) = \frac{1}{2^{n/2}\sqrt{n+1}}$ and $\delta(\mathbb{Z}^n) = 2^{-n}$, the previous proposition says that

$$\delta(\mathbb{Z}^n) \leq \delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) \leq \delta(A_n).$$

The next theorem shows that the lattice $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is equivalent to $\mathbb{Z}^n$ or A_n, respectively, in these extreme cases.

Theorem 4.5. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Let $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Let r, s be integers such that $0 \neq |r| < n$ and let $m = r + sn$. If*

(a)

$$\left(\frac{m}{r}\right)^2 = \frac{na-1}{n-1},$$

then $\mathcal{L}_{\mathbf{v}_1}^{(r,s)} \cong |r|\sqrt{\frac{na-1}{n-1}}\mathbb{Z}^n$.

(b)

$$\left(\frac{m}{r}\right)^2 = \frac{(na-1)(n+1)}{n-1},$$

then $\mathcal{L}_{\mathbf{v}_1}^{(r,s)} \cong |r|\sqrt{\frac{na-1}{n-1}}A_n$.

Proof. Theorem 4.2 gives a basis of minimal vectors

$$\mathcal{B} = \left\{\Phi_{(r,s)}(\mathbf{e}_i) : 1 \leq i \leq n\right\} = \{r\mathbf{e}_1 + s\mathbf{v}_1, \ldots, r\mathbf{e}_n + s\mathbf{v}_1\}$$

for the lattice $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$. A direct computation shows that

1. $\left\langle \Phi_{(r,s)}(\mathbf{e}_i), \Phi_{(r,s)}(\mathbf{e}_i)\right\rangle = ar^2 + \frac{m^2-r^2}{n}$ for all $1 \leq i \leq n$.
2. $\left\langle \Phi_{(r,s)}(\mathbf{e}_i), \Phi_{(r,s)}(\mathbf{e}_j)\right\rangle = -r^2h + \frac{m^2-r^2}{n}$ for all $1 \leq i \neq j \leq n$.

For (a), using the equations $a + h(1-n) = 1$ and $m^2 = r^2\frac{na-1}{n-1}$ we end up with

$$\left\langle \Phi_{(r,s)}(\mathbf{e}_i), \Phi_{(r,s)}(\mathbf{e}_j)\right\rangle = \begin{cases} \frac{(na-1)r^2}{n-1} & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

As a consequence, the Gram matrix of the lattice $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ with respect to the basis $\mathcal{B}$ is given by

$$G_{\mathcal{B}} = \frac{(na-1)r^2}{n-1}I_n.$$

Therefore, $\mathcal{L}_{\mathbf{v}_1}^{(r,s)} \cong |r|\sqrt{\frac{na-1}{n-1}}\mathbb{Z}^n$ proving (a). For (b), using the equations $a + h(1-n) = 1$ and $m^2 = r^2\frac{(na-1)(n+1)}{n-1}$ we end up with

$$\left\langle \Phi_{(r,s)}(\mathbf{e}_i), \Phi_{(r,s)}(\mathbf{e}_j)\right\rangle = \begin{cases} \frac{2(na-1)r^2}{n-1} & \text{if } i = j \\ \frac{(na-1)r^2}{n-1} & \text{if } i \neq j. \end{cases}$$

As a consequence, the Gram matrix for the lattice $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ with respect to the basis $\mathcal{B}$ is given by

$$G_{\mathcal{B}} = \frac{(na-1)r^2}{n-1}\begin{bmatrix} 2 & 1 & \ldots & 1 \\ 1 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \ldots & 1 & 2 \end{bmatrix} =: \frac{(na-1)r^2}{n-1}A.$$

Define the unimodular matrix

$$U := \begin{bmatrix} 1 & 0 & \dots & 0 \\ -1 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & -1 & 1 \end{bmatrix}.$$

Note that

$$\frac{n-1}{(na-1)r^2} U G_{\mathcal{B}} U^T = U A U^T = G$$

where

$$G = \begin{bmatrix} 2 & -1 & \dots & 0 \\ -1 & 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ 0 & \dots & -1 & 2 \end{bmatrix}$$

is a Gram matrix for A_n. Therefore, $\mathcal{L}_{\mathbf{v}_1}^{(r,s)} \cong |r|\sqrt{\frac{na-1}{n-1}} A_n$ proving (b). □

4.4 Construction of A_n

We know that a lattice of the form $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is equivalent to A_n if condition (b) in Theorem 4.5 holds. But the question remains, for which values of the parameter a for the Lagrangian superlattice does there exist a pair of integers (r, s) such that the condition is satisfied. If we take the orthogonal lattice, with $a = 1$, the condition can only be satisfied when $n+1$ is a square. But if we consider a Lagrangian lattice with $a = n$, then we can always find pairs (r, s) such that $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is equivalent to A_n. Propositions 4.3 and 4.4 show how one can construct a lattice equivalent to the A_n lattice as a sublattice of $\mathbb{Z}^n$ in the case that $n+1$ is a square, and as a sublattice of a specific Lagrangian lattice for a general n.

Proposition 4.3. *Suppose that $n + 1 = d^2$ for some integer $d > 1$. Let $\mathcal{L} = \mathbb{Z}^n$ be the Lagrangian lattice with $(a, h) = (1, 0)$ and a Lagrangian basis $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$, where the $\mathbf{e}_i$'s are the standard basis vectors in $\mathbb{R}^n$. Then $\mathcal{L}_{\mathbf{v}_1}^{(d+1,1)}$ is a sublattice of $\mathcal{L}$ such that $\mathcal{L}_{\mathbf{v}_1}^{(d+1,1)} \cong (d+1)A_n$.*

Proof. Let $(r, s) = (d+1, 1)$, and note that $0 < |r| = d+1 < (d+1)(d-1) = n$. Moreover,

$$\left(\frac{m}{r}\right)^2 = \left(\frac{r+sn}{r}\right)^2 = \left(1 + \frac{n}{r}\right)^2 = d^2 = n + 1 = \frac{(na-1)(n+1)}{n-1}.$$

By Theorem 4.5, part (b),

$$\mathcal{L}_{\mathbf{v}_1}^{(r,s)} \cong (d+1)A_n.$$

□

Proposition 4.4. *Let $n \geq 2$ be an integer and let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the standard basis vectors in $\mathbb{R}^n$. Let $\mathbf{v}_1 = (1, \ldots, 1)^T \in \mathbb{R}^n$ and define the vectors $\mathbf{e}'_i = \left(\frac{1-\sqrt{n+1}}{n}\right)\mathbf{v}_1 + \sqrt{n+1}\mathbf{e}_i$ for each $i = 1, \ldots, n$. Then the lattice $\mathcal{L} \subset \mathbb{R}^n$ with the basis $\{\mathbf{e}'_1, \ldots, \mathbf{e}'_n\}$ is Lagrangian with $(a, h) = (n, 1)$. Further, for any integer r such that $0 < |r| < n$, we have that $\mathcal{L}_{\mathbf{v}_1}^{(r,r)}$ is a sublattice of $\mathcal{L}$ such that $\mathcal{L}_{\mathbf{v}_1}^{(r,r)} \cong |r|\sqrt{n+1}A_n$.*

Proof. First we need to check that the vectors $\mathbf{e}'_i$ form a Lagrangian basis.

1. $\sum_{i=1}^n \mathbf{e}'_i = n\left(\frac{1-\sqrt{n+1}}{n}\right)\mathbf{v}_1 + \sqrt{n+1}\mathbf{v}_1 = \mathbf{v}_1$.
2. $\langle \mathbf{e}'_i, \mathbf{v}_1 \rangle = n\left(\frac{1-\sqrt{n+1}}{n}\right) + \sqrt{n+1} = 1$ for all $1 \leq i \leq n$.
3. $a = \langle \mathbf{e}'_i, \mathbf{e}'_i \rangle = (n-1)\left(\frac{1-\sqrt{n+1}}{n}\right)^2 + \left(\frac{1-\sqrt{n+1}}{n} + \sqrt{n+1}\right)^2 = n$ for all $1 \leq i \leq n$.
4. $-h = \langle \mathbf{e}'_i, \mathbf{e}'_j \rangle = (n-2)\left(\frac{1-\sqrt{n+1}}{n}\right)^2 + 2\left(\frac{1-\sqrt{n+1}}{n}\right)\left(\frac{1-\sqrt{n+1}}{n} + \sqrt{n+1}\right) = -1$ for all $1 \leq i \neq j \leq n$.

The conditions are satisfied, so $\mathcal{L}$ is Lagrangian with $(a, h) = (n, 1)$. For the second part, suppose that r is an integer such that $0 < |r| < n$. Let $s := r$, so that $m = r(1+n)$, and note that

$$\left(\frac{m}{r}\right)^2 = (1+n)^2 = \frac{(n^2-1)(n+1)}{n-1} = \frac{(na-1)(n+1)}{n-1}.$$

By Theorem 4.5, part (b),

$$\mathcal{L}_{\mathbf{v}_1}^{(r,r)} \cong |r|\sqrt{\frac{na-1}{n-1}}A_n = |r|\sqrt{n+1}A_n$$

and we are done. □

Remark 4.4. The lattice $\mathcal{L}_{\mathbf{v}_1}^{(r,r)} \subseteq \mathcal{L}$ in Proposition 4.4 has basis vectors

given by

$$\Phi_{(r,r)}(\mathbf{e}'_i) = r(\mathbf{e}'_i + \mathbf{v}_1) \tag{4.25}$$

$$= r\left(\frac{n+1-\sqrt{n+1}}{n}\right)\mathbf{v}_1 + \sqrt{n+1}r\mathbf{e}_i \tag{4.26}$$

$$= r\sqrt{n+1}\left(\frac{\sqrt{n+1}-1}{n}\mathbf{v}_1 + \mathbf{e}_i\right) \tag{4.27}$$

$$=: r\sqrt{n+1}\mathbf{b}_i. \tag{4.28}$$

We will henceforth denote by $\tilde{A}_n$ the full rank lattice generated by the vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Contrast this to A_n, which is a rank n lattice in $\mathbb{R}^{n+1}$. Note that $\tilde{A}_n \cong A_n$.

In Figure 4.1, we illustrate the Lagrangian lattice $\mathcal{L}$ from Proposition 4.4 and its sublattice $\mathcal{L}_{\mathbf{v}_1}^{(r,r)}$ for $r = 1$ and $n = 2$. In dimension 2, $\mathcal{L}$ is equivalent to A_n too.

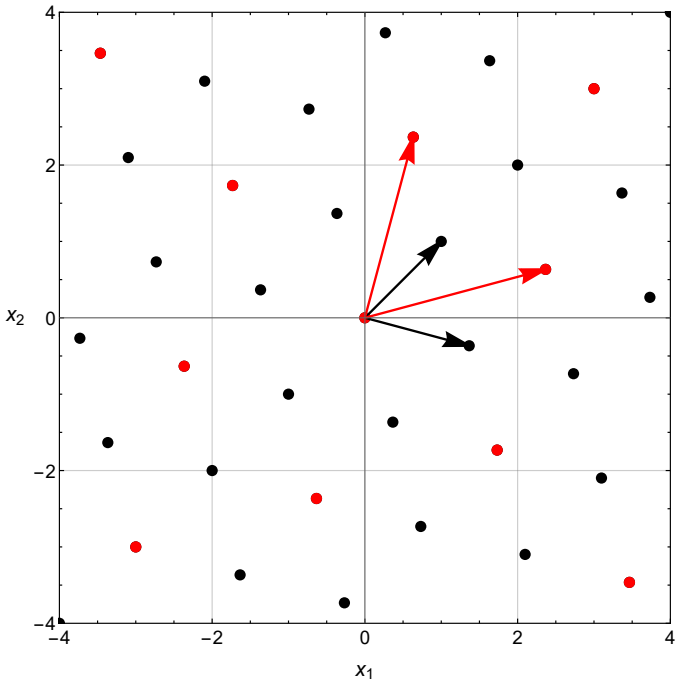


Figure 4.1: The Lagrangian lattice $\mathcal{L}$ from Proposition 4.4 (marked with black dots) and its sublattice $\mathcal{L}_{\mathbf{v}_1}^{(1,1)} = \sqrt{3}\tilde{A}_n$ (marked with red dots) where $n = 2$. Arrows represent basis vectors.

4.5 Dual lattices

We will now illustrate the concept of lattice duality by proving that the dual lattice of a lattice of the form $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is $\mathcal{L}$ scaled given that a certain condition holds. We also show that the dual lattice of a Lagrangian lattice is Lagrangian.

Proposition 4.5. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Let $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Let r, s be integers such that $0 \neq |r| < n$. Suppose that $s = rh$. Then the dual lattice of $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is $\frac{1}{r(a+h)}\mathcal{L}$.*

Proof. A basis for $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is given by the vectors $r\mathbf{e}_i + s\mathbf{v}_1$, for $i = 1, \ldots, n$. Let $c := \frac{1}{r(a+h)}$. Then a basis for $\frac{1}{r(a+h)}\mathcal{L}$ is given by the vectors $c\mathbf{e}_1, \ldots, c\mathbf{e}_n$. Note that for every $i, j \in \{1, \ldots, n\}$,

$$\langle r\mathbf{e}_i + s\mathbf{v}_1, c\mathbf{e}_j \rangle = \begin{cases} c(ra+s), & \text{if } i = j \\ c(s-rh), & \text{if } i \neq j, \end{cases}$$

where we used the fact that $\langle \mathbf{v}_1, \mathbf{e}_j \rangle = 1$ for all $1 \leq j \leq n$, and that $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = a$ if $i = j$ and $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = -h$ else. The assumption $s = rh$ and $c \neq 0$ give that

$$\langle r\mathbf{e}_i + s\mathbf{v}_1, c\mathbf{e}_j \rangle = c(ra+s)\delta_{ij} = cr(a+h)\delta_{ij} = \delta_{ij}$$

for all $1 \leq i \neq j \leq n$, proving that the generator matrices M and M' of $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ and $\frac{1}{r(a+h)}\mathcal{L}$, respectively, are related by $M^T M' = I_n$. The claim follows from Proposition 2.2. □

Example 4.2. *Recall the Lagrangian lattice $\mathcal{L} \subset \mathbb{R}^n$ with $(a, h) = (n, 1)$ from Proposition 4.4 and its sublattice $\mathcal{L}_{\mathbf{v}_1}^{(r,r)} = |r|\sqrt{n+1}\tilde{A}_n$, where $0 < |r| < n$. Since $s = r = rh$, the previous proposition and Lemma 2.2 give that*

$$\tilde{A}_n^* = \left(\frac{1}{|r|\sqrt{n+1}} \mathcal{L}_{\mathbf{v}_1}^{(r,r)} \right)^* = |r|\sqrt{n+1} \left(\mathcal{L}_{\mathbf{v}_1}^{(r,r)} \right)^* \tag{4.29}$$

$$= |r|\sqrt{n+1} \cdot \frac{1}{r(n+1)} \mathcal{L} = \frac{1}{\sqrt{n+1}} \mathcal{L}. \tag{4.30}$$

We will now show that if $\mathcal{L}$ is Lagrangian, then so is $\mathcal{L}^*$.

Lemma 4.4. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$. Let $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$ and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Then the dual lattice $\mathcal{L}^*$ is a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}'_1, \ldots, \mathbf{e}'_n\}$, such that $\tilde{a} := \langle \mathbf{e}'_1, \mathbf{e}'_1 \rangle = \frac{1+h}{a+h}$ and $\tilde{h} := -\langle \mathbf{e}'_1, \mathbf{e}'_2 \rangle = \frac{-h}{a+h}$.*

Proof. First note that

$$\tilde{a} - (n-1)\tilde{h} = \frac{1+h}{a+h} - (n-1)\left(\frac{-h}{a+h}\right) = \frac{1+hn}{a+h} = \frac{a+h}{a+h} = 1,$$

since $a - h(n-1) = 1$, *i.e.*, $1 + hn = a + h$, by the definition of a Lagrangian lattice. Furthermore,

$$\tilde{a} + \tilde{h} = \frac{1+h}{a+h} + \frac{-h}{a+h} = \frac{1}{a+h} > 0$$

since $a + h > 0$ by Remark 4.1. If we can show that $\mathcal{L}^*$ has a Gram matrix $\tilde{G}$ of the form

$$\tilde{G} = \begin{bmatrix} \tilde{a} & -\tilde{h} & \dots & -\tilde{h} \\ -\tilde{h} & \tilde{a} & \ddots & \vdots \\ \vdots & \ddots & \ddots & -\tilde{h} \\ -\tilde{h} & \dots & -\tilde{h} & \tilde{a} \end{bmatrix},$$

with respect to some basis $\{\mathbf{e}'_1, \dots, \mathbf{e}'_n\}$, then we have shown that $\mathcal{L}^*$ is a Lagrangian lattice with a Lagrangian basis $\{\mathbf{e}'_1, \dots, \mathbf{e}'_n\}$ such that $\tilde{a} = \langle \mathbf{e}'_1, \mathbf{e}'_1 \rangle = \frac{1+h}{a+h}$ and $\tilde{h} = -\langle \mathbf{e}'_1, \mathbf{e}'_2 \rangle = \frac{-h}{a+h}$. Denote by $\{\mathbf{b}_1, \dots, \mathbf{b}_n\}$ the rows of the Gram matrix G of the Lagrangian lattice $\mathcal{L}$, and by $\{\mathbf{d}_1, \dots, \mathbf{d}_n\}$ the columns of the matrix $\tilde{G}$. Let us compute the inner products $\langle \mathbf{b}_i, \mathbf{d}_j \rangle$ for all $i, j \in \{1, \dots, n\}$. For $i = j$, we obtain

$$\begin{aligned} \langle \mathbf{b}_i, \mathbf{d}_i \rangle &= (-h, \dots, a, \dots, -h)^T(-\tilde{h}, \dots, \tilde{a}, \dots, -\tilde{h}) && (4.31) \\ &= (n-1)h\tilde{h} + a\tilde{a} && (4.32) \\ &= (n-1)h\tilde{h} + a(1 + (n-1)\tilde{h}) && (4.33) \\ &= a + (n-1)\tilde{h}(a+h) && (4.34) \\ &= a + (n-1)\left(\frac{-h}{a+h}\right)(a+h) && (4.35) \\ &= a - h(n-1) = 1. && (4.36) \end{aligned}$$

For $i \neq j$, we have

$$\begin{aligned}
\langle \mathbf{b}_i, \mathbf{d}_j \rangle &= (-h, \ldots, a, -h \ldots, -h)^T (-\tilde{h}, \ldots, -\tilde{h}, \tilde{a}, \ldots, -\tilde{h}) && (4.37)\\
&= (n-2)h\tilde{h} - \tilde{a}h - a\tilde{h} && (4.38)\\
&= \tilde{h}((n-2)h - a) - \tilde{a}h && (4.39)\\
&= -\tilde{h}(a - h(n-1) + h) - \tilde{a}h && (4.40)\\
&= -\tilde{h}(1+h) - \tilde{a}h && (4.41)\\
&= \left(\frac{h}{a+h}\right)(1+h) - \frac{h(1+h)}{a+h} && (4.42)\\
&= 0. && (4.43)
\end{aligned}$$

This shows that G and $\tilde{G}$ are related by $G\tilde{G} = I_n$. But by Remark 2.2, $\tilde{G}$ must be a Gram matrix for the dual lattice $\mathcal{L}^*$. □

4.6 Construction of some dense lattices

We have seen that, under the assumptions made in Theorem 4.2, a well-rounded lattice of the form $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ has density less than or equal to the density of A_n. However, if we replace $\mathrm{T}_{\mathbf{v}_1}(\mathbf{x}) = \langle \mathbf{x}, \mathbf{v}_1 \rangle$ with a general $\mathbb{Z}$-linear map $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$, then we may get lattices with higher density. Indeed, in [10, Example 3.6], using the trace map $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$, $\mathrm{T}(\mathbf{x}) = \sum_{i=1}^{n} x_i$, the authors construct the lattice D_n as a lattice of the form $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$. The purpose of this section is to show how one can construct the densest known lattices in dimensions 8 and 9 as lattices $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$, when $\mathcal{L}$ is the Lagrangian lattice $\mathbb{Z}^n$. This shows that there are many different types of lattices that can be obtained from a Lagrangian lattice $\mathcal{L}$, using the linear map $\Phi_{(r,s)}$.

4.6.1 The E_8 lattice

The E_8 lattice is the densest lattice packing in dimension 8, with many intriguing properties. There are two equivalent versions of the lattice; the even (Γ_8) and odd (Γ_8') coordinate system version. Let us recall the definition of both.

Definition 4.3. *Define*

$$\Gamma_8 := \left\{ \mathbf{x} \in \mathbb{Z}^8 \cup \left(\mathbb{Z} + \frac{1}{2}\right)^2 : \sum_{i=1}^{8} x_i \in 2\mathbb{Z} \right\}, \tag{4.44}$$

$$\Gamma_8' := \left\{ \mathbf{x} \in \mathbb{Z}^8 : \sum_{i=1}^{8} x_i \in 2\mathbb{Z} \right\} \cup \left\{ \mathbf{x} \in \left(\mathbb{Z} + \frac{1}{2}\right)^8 : \sum_{i=1}^{8} x_i \in 2\mathbb{Z} + 1 \right\}. \tag{4.45}$$

We will only be interested in the Γ_8' lattice in this thesis. Before we proceed to construct a scaled variant of Γ_8', we need the following proposition, which gives the index of $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$ in $\mathcal{L}$.

Proposition 4.6. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice, $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$ a non-trivial linear map and $\mathbf{v}_1 \in \mathcal{L} \setminus \ker \mathrm{T}$. Let r, s be integers such that $0 \neq |r| < |\mathrm{T}(\mathbf{v}_1)|$ and let $m = r + s\,\mathrm{T}(\mathbf{v}_1)$. Then*

$$[\mathcal{L} : \mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}] = |mr^{n-1}|.$$

Proof. The case when $\mathcal{L}$ has a basis which is rigid with respect to T is proven in [10, Proposition 3.7], so let us prove that such a basis always exists. As an abelian group, $\mathcal{L} \cong \mathbb{Z}^n$. Then, as $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$ is a homomorphism between groups, the first isomorphism theorem states that $\ker \mathrm{T}$ is a subgroup of $\mathcal{L} \cong \mathbb{Z}^n$, and further, that $im(\mathrm{T}) \cong \mathcal{L}/\ker \mathrm{T}$. Now since $im(\mathrm{T}) \cong \mathbb{Z}$ and $\mathcal{L} \cong \mathbb{Z}^n$, we must have $\ker \mathrm{T} \cong \mathbb{Z}^{n-1}$. Suppose that $\{\mathbf{w}_1, \ldots, \mathbf{w}_{n-1}\}$ is a basis for $\ker \mathrm{T}$, and let $\mathbf{v} \in \mathcal{L} \setminus \ker \mathrm{T}$ be such that $\mathrm{T}(\mathbf{v})$ is a generator of the image $im(\mathrm{T})$. Then, $\{\mathbf{w}_1, \ldots, \mathbf{w}_{n-1}, \mathbf{v}\}$ is a basis for $\mathcal{L}$. Finally, consider the basis for $\mathcal{L}$ defined by $\mathbf{w}_i' = \mathbf{w}_i + \mathbf{v}$ for $1 \leq i \leq n-1$ and $\mathbf{w}_n' = \mathbf{v}$. Clearly, $\mathrm{T}(\mathbf{w}_i') = \mathrm{T}(\mathbf{v})$ for all $1 \leq i \leq n$, proving that $\mathcal{L}$ has a basis which is rigid with respect to T. □

Lemma 4.5. *Let $\mathcal{L} = \mathbb{Z}^8$ and $\mathbf{c} = (1, -1, 1, -1, 1, -1, 1, -1)^T$. Define the linear map $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$, $\mathrm{T}(\mathbf{x}) = \mathbf{c}^T\mathbf{x}$. Let $\mathbf{v}_1 = (-1, 1, -1, 1, 1, 1, 1, 1) \in \mathcal{L} \setminus \ker \mathrm{T}$, and $(r, s) = (2, 1)$. Then $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)} = 2\Gamma_8'$.*

Proof. First note that $0 \neq |r| = 2 < 4 = |\mathrm{T}(\mathbf{v}_1)|$, so Lemma 4.2 gives that $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$ is a full rank sublattice of $\mathcal{L}$. Let $m := r + s\,\mathrm{T}(\mathbf{v}_1) = 2 + (-4) = -2$. Let $\mathbf{e}_1, \ldots, \mathbf{e}_8$ be the standard basis vectors in $\mathbb{R}^8$. A basis for $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$ is given by the vectors

$$\Phi_{(r,s)}(\mathbf{e}_i) = r\mathbf{e}_i + s\,\mathrm{T}(\mathbf{e}_i)\mathbf{v}_1 = 2\mathbf{e}_i + c_i\mathbf{v}_1$$

producing the generator matrix

$$M = \begin{bmatrix} 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 3 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 3 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \end{bmatrix}.$$

If we add column i to column $i+1$ for every $i \in \{1, \dots, 7\}$, we get the following generator matrix:

$$M' = \begin{bmatrix} 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 2 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

Since the columns of M' are contained in $2\Gamma_8'$, we can conclude that $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)} \subseteq 2\Gamma_8'$. On the other hand, since $\det(\mathcal{L}) = 1$ and $[\mathcal{L} : \mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}] = |mr^{n-1}|$ by Proposition 4.6, we have

$$\det(\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}) = [\mathcal{L} : \mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}]^2 \det(\mathcal{L}) = |mr^{n-1}|^2 = |(-2) \cdot 2^{8-1}|^2 = 4^8 = \det(2\Gamma_8'),$$

proving $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)} = 2\Gamma_8'$. □

4.6.2 Densest known lattice in dimension 9

The largest known center density in dimension 9 is $\delta_9 = \frac{1}{16\sqrt{2}}$, achieved by the laminated lattice Λ_9 [22]. Here we show how we can construct a lattice $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$ with this center density.

Example 4.3. *Let* $\mathcal{L} = \mathbb{Z}^9$ *and* $\mathbf{c} = (1, -1, 1, -1, 1, -1, 1, -1, 1)^T$. *Define the linear map* $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$, $\mathrm{T}(\mathbf{x}) = \mathbf{c}^T\mathbf{x}$. *Let*

$$\mathbf{v}_1 = (-1, -1, -1, -1, -1, -1, -2, 1, -1) \in \mathcal{L} \setminus \ker \mathrm{T},$$

and $(r, s) = (2, 1)$. *Then* $\delta(\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}) = \frac{1}{16\sqrt{2}} = \delta_9$.

Proof. First note that $0 \neq |r| = 2 < 4 = |\operatorname{T}(\mathbf{v}_1)|$, so $\mathcal{L}_{\operatorname{T},\mathbf{v}_1}^{(r,s)}$ is a full rank sublattice of $\mathcal{L}$. Let $\mathbf{e}_1, \ldots, \mathbf{e}_9$ be the standard basis vectors in $\mathbb{R}^9$. A basis for $\mathcal{L}_{\operatorname{T},\mathbf{v}_1}^{(r,s)}$ is given by the vectors

$$\Phi_{(r,s)}(\mathbf{e}_i) = r\mathbf{e}_i + s\operatorname{T}(\mathbf{e}_i)\mathbf{v}_1 = 2\mathbf{e}_i + c_i\mathbf{v}_1.$$

Thus, a generator matrix for $\mathcal{L}_{\operatorname{T},\mathbf{v}_1}^{(r,s)}$ is given by

$$M = \begin{bmatrix} 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 3 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 3 & -1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 & -1 & 3 & -1 & 1 & -1 \\ -2 & 2 & -2 & 2 & -2 & 2 & 0 & 2 & -2 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \end{bmatrix}.$$

If we add column i to column $i+1$ for every $i \in \{1, \ldots, 8\}$, we get the generator matrix

$$M' = \begin{bmatrix} 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \\ -2 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{bmatrix}.$$

One can verify that $\lambda_1(\mathcal{L}_{\operatorname{T},\mathbf{v}_1}^{(r,s)}) = \sqrt{2^2 + 2^2} = \sqrt{8}$ and $\operatorname{vol}(\mathcal{L}_{\operatorname{T},\mathbf{v}_1}^{(r,s)}) = 2^9$. Therefore,

$$\delta(\mathcal{L}_{\operatorname{T},\mathbf{v}_1}^{(r,s)}) = \frac{\lambda_1(\mathcal{L}_{\operatorname{T},\mathbf{v}_1}^{(r,s)})^9}{2^9 \operatorname{vol}(\mathcal{L}_{\operatorname{T},\mathbf{v}_1}^{(r,s)})} = \frac{(\sqrt{8})^9}{2^9 \cdot 2^9} = \frac{2^9 \cdot (\sqrt{2})^9}{2^9 \cdot 2^9} = \frac{1}{16\sqrt{2}} = \delta_9.$$

□

Chapter 5

Generic well-rounded lattices

In this chapter, we deform dense lattices in a such a way that we obtain generic well-rounded lattices with high sphere packing density. In the previous section, we have showed that one can construct GWR lattices with center density as close as desired to the center density of the A_n lattice; this can be done using sublattices of Lagrangian lattices. However, the A_n lattice is the densest lattice packing only in dimensions 1–3. Thus, we would like to have generic well-rounded variants of the densest lattices in dimensions $n \geq 4$. As it is well-known, the D_n lattice has the greatest density of all lattices in dimension $n = 4, 5$. Therefore, in Section 5.2 we introduce a version of the D_n lattice, where the basis vectors are slightly deformed. This produces a GWR lattice which resembles D_n. Then, in Section 5.3 we do the same thing for the densest lattice packing in dimension 8, the E_8 lattice, to obtain a deformed version of the E_8 lattice which is GWR. We also investigate when the deformed lattices (scaled) are sublattices of $\mathbb{Z}^n$.

5.1 The planar case: Deformed hexagonal lattice

To motivate the idea behind the deformed lattices, we illustrate how the densest lattice packing in dimension 2, the hexagonal lattice, can be deformed to produce GWR lattices with density as close as wanted to the optimal density. In fact, we end up with a certain parametrization of representatives of equivalence classes of planar well-rounded lattices. The example is simple, but very illustrative.

Definition 5.1. *Let* $0 \leq \alpha \leq \frac{1}{2}$ *and* $\overline{\alpha} := \sqrt{1-\alpha^2}$. *Define* Λ_h^α *to be the*

planar lattice generated by the matrix

$$M_{\Lambda_h^\alpha} := \begin{bmatrix} 1 & \alpha \\ 0 & \overline{\alpha} \end{bmatrix}.$$

It is immediate from the definition that $\Lambda_h^{\frac{1}{2}} = \Lambda_h$, the hexagonal lattice, and $\Lambda_h^0 = \mathbb{Z}^2$, the orthogonal lattice. It is also immediate that

$$\mathrm{vol}(\Lambda_h^\alpha) = |\det(M_{\Lambda_h^\alpha})| = \overline{\alpha}.$$

It is a well-known fact that the planar WR lattices are fully determined, up to equivalence, by the angle θ between minimal basis vectors $\{\mathbf{b}_1, \mathbf{b}_2\}$, which can always be chosen such that $\theta \in [\frac{\pi}{3}, \frac{\pi}{2}]$ (see [11] for more details). Further, $\theta = \frac{\pi}{3}$ gives the hexagonal lattice with kissing number 6, and each $\theta \in (\frac{\pi}{3}, \frac{\pi}{2}]$ gives a (up to equivalence) unique GWR lattice.

Given the above characterization, it is clear that $\alpha \mapsto \Lambda_h^\alpha$, $\alpha \in [0, \frac{1}{2}]$ is a parametrization of representatives of the equivalence classes of WR lattices in the plane. To see this, note that the basis vectors of Λ_h^α corresponding to the generator matrix $M_{\Lambda_h^\alpha}$, call them $\mathbf{b}_1, \mathbf{b}_2$, have unit length and further, if θ is the (smaller) angle between $\mathbf{b}_1$ and $\mathbf{b}_2$, then

$$\cos(\theta) = \langle \mathbf{b}_1, \mathbf{b}_2 \rangle = \alpha \in [0, \tfrac{1}{2}],$$

which gives that θ must be in the range $[\frac{\pi}{3}, \frac{\pi}{2}]$. Thus, we have a bijection $[\frac{\pi}{3}, \frac{\pi}{2}] \to [0, \frac{1}{2}]$, $\theta \mapsto \cos(\theta) = \alpha$, showing that there is a one-to-one correspondence between the angles $\theta \in [\frac{\pi}{3}, \frac{\pi}{2}]$ and $\alpha \in [0, \frac{1}{2}]$.

The center density of Λ_h^α takes a very simple form:

$$\delta(\Lambda_h^\alpha) = \frac{\lambda_1(\Lambda_h^\alpha)^2}{2^2 \,\mathrm{vol}(\Lambda_h^\alpha)} = \frac{1}{4\overline{\alpha}}.$$

We have $\delta(\Lambda_h^{\frac{1}{2}}) = \frac{1}{4\sqrt{1-\left(\frac{1}{2}\right)^2}} = \frac{1}{2\sqrt{3}} = \delta(\Lambda_h)$ and $\delta(\Lambda_h^0) = \frac{1}{4} = \delta(\mathbb{Z}^2)$. The center density of Λ_h^α is illustrated in Figure 5.1 for all $\alpha \in [0, \frac{1}{2}]$.

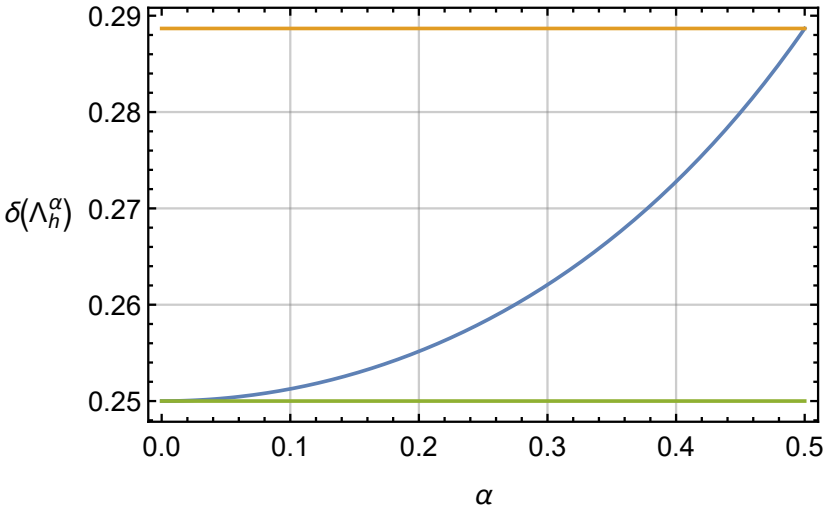


Figure 5.1: Center density of the deformed hexagonal lattice Λ_h^α as a function of α. The bottom line shows $\delta(\mathbb{Z}^2)$ and the upper line $\delta(\Lambda_h)$.

5.2 Deformed D_n lattices

Definition 5.2. *Let $1 \leq \alpha \leq \sqrt{2}$ and $\overline{\alpha} := \sqrt{2-\alpha^2}$. We define D_n^α, $n \geq 3$, to be the rank n lattice with generator matrix*

$$M_{D_n^\alpha} := \begin{bmatrix} \alpha & 0 & \overline{\alpha} & 0 & 0 & 0 & \dots & 0 \\ \overline{\alpha} & \alpha & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \overline{\alpha} & \alpha & \overline{\alpha} & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & -\alpha & \overline{\alpha} & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & -\alpha & \overline{\alpha} & \ddots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & 0 & -\alpha & \overline{\alpha} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\alpha \end{bmatrix}.$$

Remark that $0 \leq \overline{\alpha} \leq 1$ whenever $1 \leq \alpha \leq \sqrt{2}$, and that α and $\overline{\alpha}$ satisfy the equality $\alpha^2 + \overline{\alpha}^2 = 2$. Further, $D_n^1 = D_n$ (hence the notation) and $D_n^{\sqrt{2}} = \sqrt{2}\mathbb{Z}^n$. For other values of α, we get a lattice which in some sense is an intermediate form of these. Our main goal is to show that D_n^α is generic well-rounded for all parameters $1 < \alpha \leq \sqrt{2}$. We also show that when we decrease the value of α from $\sqrt{2}$ towards 1, we get generic well-rounded lattices of increasing density. In particular, we have then shown

that there exists generic well-rounded lattices of density arbitrarily close to the maximum in dimensions $n = 4, 5$.

The fact that D_n^α is a full rank lattice follows from the following proposition, which implies that the determinant of $M_{D_n^\alpha}$ is non-zero.

Proposition 5.1. *The volume of D_n^α is given by*

$$\mathrm{vol}(D_n^\alpha) = \alpha^{n-3}(\alpha^3 + \overline{\alpha}^3).$$

Proof. Notice that $M_{D_n^\alpha}$ has the form of an upper triangular block matrix. Therefore, the determinant is equal to the product of the determinants of the diagonal blocks;

$$\det(M_{D_n}^\alpha) = \begin{vmatrix} \alpha & 0 & \overline{\alpha} \\ \overline{\alpha} & \alpha & 0 \\ 0 & \overline{\alpha} & \alpha \end{vmatrix} \cdot (-\alpha)^{n-3} = (-1)^{n-3}(\alpha^3 + \overline{\alpha}^3)\alpha^{n-3}.$$

The claim follows from $\mathrm{vol}(D_n^\alpha) = |\det(M_{D_n^\alpha})|$. □

Note that in particular, $\mathrm{vol}(D_n^1) = 1^{n-3} \cdot (1^3 + 1^3) = 2 = \mathrm{vol}(D_n)$ and $\mathrm{vol}(D_n^{\sqrt{2}}) = (\sqrt{2})^{n-3} \cdot (\sqrt{2}^3 + 0^3) = 2^{n/2} = \mathrm{vol}(\sqrt{2}\mathbb{Z}^n)$, as expected.

The next theorem shows that D_n^α is generic well-rounded when $\alpha > 1$. Furthermore, it says that D_n^α has a basis of minimal vectors given by the columns of $M_{D_n^\alpha}$.

Theorem 5.1. *Let $1 < \alpha \leq \sqrt{2}$. Then D_n^α has a set of minimal vectors $S(D_n^\alpha) = \{\pm\mathbf{b}_1, \ldots, \pm\mathbf{b}_n\}$ where $\mathbf{b}_i$ is the i:th column of $M_{D_n^\alpha}$. In particular, D_n^α is GWR and $\lambda_1^2(D_n^\alpha) = 2$.*

Proof. The case $\alpha = \sqrt{2}$ is clear since $D_n^{\sqrt{2}} = \sqrt{2}\mathbb{Z}^n$. Let us therefore assume $1 < \alpha < \sqrt{2}$. Note that $\|\mathbf{b}_i\|^2 = \alpha^2 + \overline{\alpha}^2 = 2$ for all $1 \leq i \leq n$, which gives $\lambda_1^2(D_n^\alpha) \leq 2$. Now suppose that $\mathbf{x} \in S(D_n^\alpha)$; then $\|\mathbf{x}\|^2 \leq 2$. Write $\mathbf{x} = \sum_{i=1}^n c_i\mathbf{b}_i$, where $c_i \in \mathbb{Z}$ and not all c_i's are zero. Then

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ \vdots \\ x_{n-1} \\ x_n \end{bmatrix} = \begin{bmatrix} c_1\alpha + c_3\overline{\alpha} \\ c_1\overline{\alpha} + c_2\alpha \\ c_2\overline{\alpha} + c_3\alpha + c_4\overline{\alpha} \\ -c_4\alpha + c_5\overline{\alpha} \\ -c_5\alpha + c_6\overline{\alpha} \\ \vdots \\ -c_{n-1}\alpha + c_n\overline{\alpha} \\ -c_n\alpha \end{bmatrix}.$$

We have that $\|\mathbf{x}\|^2 \geq x_n^2 = c_n^2\alpha^2 > c_n^2$ and hence $|c_n| \leq 1$. If $c_n = 0$, then $\|\mathbf{x}\|^2 \geq x_{n-1}^2 = c_{n-1}^2\alpha^2 > c_{n-1}^2$ and so $|c_{n-1}| \leq 1$. Otherwise, if $|c_n| = 1$, then also $|c_{n-1}| \leq 1$. To see this, suppose that $|c_{n-1}| \geq 2$. Then $\|\mathbf{x}\|^2 \geq x_{n-1}^2 + x_n^2 \geq (2\alpha - \overline{\alpha})^2 + \alpha^2 > \alpha^2 + \alpha^2 > 2$, a contradiction. Inductively, we conclude $|c_i| \leq 1$ for $i = 4, 5, \ldots, n$.

Consider the coefficient c_4. We may without loss of generality assume that $c_4 \in \{0, 1\}$, since we can always replace $\mathbf{x}$ by $-\mathbf{x}$.

Case 1: $c_4 = 0$. We have

$$\|\mathbf{x}\|^2 \geq x_1^2 + x_2^2 + x_3^2 = (c_1\alpha + c_3\overline{\alpha})^2 + (c_1\overline{\alpha} + c_2\alpha)^2 + (c_2\overline{\alpha} + c_3\alpha)^2.$$

Note that c_1, c_2, c_3 cannot all be non-zero. If this was the case, then two of them, say c_i and c_j, would have the same sign and we would get the contradiction $\|\mathbf{x}\|^2 \geq (c_i\alpha + c_j\overline{\alpha})^2 \geq (\alpha + \overline{\alpha})^2 = 2 + 2\alpha\overline{\alpha} > 2$. Now suppose that $c_i = 0$ for some $i \in \{1, 2, 3\}$ and denote by c_j and c_k the other two coefficients. Then if both c_j and c_k are non-zero, we get

$$\|\mathbf{x}\|^2 \geq c_j^2\alpha^2 + c_k^2\overline{\alpha}^2 + (c_k\alpha + c_j\overline{\alpha})^2 > \alpha^2 + \overline{\alpha}^2 = 2,$$

since $(c_k\alpha + c_j\overline{\alpha})^2 > 0$ when $c_j, c_k \in \{\pm 1\}$. This is a contradiction. We conclude that either

(i) $|c_i| = 1$ for some $i \in \{1, 2, 3\}$ and $c_j = 0$ for $j \in \{1, 2, 3\} \setminus \{i\}$ or,

(ii) $c_i = 0$ for all $i \in \{1, 2, 3\}$.

In case (i),

$$\begin{aligned} \|\mathbf{x}\|^2 &= \alpha^2 + \overline{\alpha}^2 + x_4^2 + \cdots + x_n^2 && (5.1)\\ &= 2 + c_5^2\overline{\alpha}^2 + (-c_5\alpha + c_6\overline{\alpha})^2 + \cdots + (-c_{n-1}\alpha + c_n\overline{\alpha})^2 + c_n^2\alpha^2 && (5.2) \end{aligned}$$

and thus $c_5 = \cdots = c_n = 0$. In case (ii),

$$\|\mathbf{x}\|^2 = x_4^2 + \cdots + x_n^2 = c_5^2\overline{\alpha}^2 + (-c_5\alpha + c_6\overline{\alpha})^2 + \cdots + (-c_{n-1}\alpha + c_n\overline{\alpha})^2 + c_n^2\alpha^2.$$

Suppose that there are at least two non-zero coefficients c_i where $i \in \{5, \ldots, n\}$. Let c_j and c_k be two such coefficients, with j minimal and k maximal. Then

$$\|\mathbf{x}\|^2 = c_j^2\overline{\alpha}^2 + (-c_j\alpha + c_{j+1}\overline{\alpha})^2 + \cdots + (-c_{k-1}\alpha + c_k\overline{\alpha})^2 + c_k^2\alpha^2 > c_j^2\overline{\alpha}^2 + c_k^2\alpha^2 = 2,$$

a contradiction. We conclude that $|c_i| = 1$ for one $i \in \{5, \ldots, n\}$ and $c_i = 0$ else.

Case 2: $c_4 = 1$. Note that

$$x_1^2 + x_2^2 + x_3^2 = (c_1\alpha + c_3\overline{\alpha})^2 + (c_1\overline{\alpha} + c_2\alpha)^2 + ((c_2+1)\overline{\alpha} + c_3\alpha)^2$$

$$x_4^2 + \cdots + x_n^2 = (-\alpha + c_5\overline{\alpha})^2 + \cdots + (-c_{n-1}\alpha + c_n\overline{\alpha})^2 + c_n^2\alpha^2 \geq \alpha^2.$$

Suppose that c_1, c_2, c_3 are all non-zero. If c_1 and c_3 have the same sign or c_1 and c_2 have the same sign, we get a contradiction $\|\mathbf{x}\|^2 \geq x_1^2 + x_2^2 + x_3^2 \geq (\alpha + \overline{\alpha})^2 > 2$. On the other hand, if c_2 and c_3 have the same sign, then $x_3^2 \geq \alpha^2$ which implies $\|\mathbf{x}\|^2 \geq \alpha^2 + \alpha^2 > 2$, a contradiction. Therefore, $c_i = 0$ for some $i \in \{1, 2, 3\}$. If $c_1 = 0$ then

$$\|\mathbf{x}\|^2 \geq c_3^2\overline{\alpha}^2 + c_2^2\alpha^2 + ((c_2+1)\overline{\alpha} + c_3\alpha)^2 + \alpha^2$$

which implies $c_2 = 0$ and $c_3 = 0$. If $c_2 = 0$ then

$$\|\mathbf{x}\|^2 \geq (c_1\alpha + c_3\overline{\alpha})^2 + c_1^2\overline{\alpha}^2 + (\overline{\alpha} + c_3\alpha)^2 + \alpha^2$$

which implies $c_1 = 0$ and $c_3 = 0$. If $c_3 = 0$ then

$$\|\mathbf{x}\|^2 \geq c_1^2\alpha^2 + (c_1\overline{\alpha} + c_2\alpha)^2 + (c_2+1)^2\overline{\alpha}^2 + \alpha^2$$

which implies $c_1 = 0$ and $c_2 = 0$. In any case, $c_1 = c_2 = c_3 = 0$. Therefore, $x_1^2 + x_2^2 + x_3^2 = \overline{\alpha}^2$ and

$$\|\mathbf{x}\|^2 = \overline{\alpha}^2 + (-\alpha + c_5\overline{\alpha})^2 + \cdots + (-c_{n-1}\alpha + c_n\overline{\alpha})^2 + c_n^2\alpha^2 \geq 2$$

with equality holding if and only if $c_5 = c_6 = \cdots = c_n = 0$.

Cases 1 and 2 imply that $\mathbf{x} = \pm\mathbf{b}_i$ for some $i \in \{1, \ldots, n\}$. This shows that $S(D_n^\alpha) = \{\pm\mathbf{b}_1, \ldots, \pm\mathbf{b}_n\}$. To see that D_n^α is WR, note that $M_{D_n^\alpha}$ is non-singular and thus $S(D_n^\alpha)$ spans $\mathbb{R}^n$. Moreover, D_n^α is GWR since $\kappa(D_n^\alpha) = |S(D_n^\alpha)| = 2n$. □

Next we proceed to investigate the center density of the lattices D_n^α.

Corollary 5.1. *The center density of D_n^α is given by*

$$\delta(D_n^\alpha) = \frac{1}{2^{n/2}\alpha^{n-3}(\alpha^3 + \overline{\alpha}^3)}.$$

Proof. By Theorem 5.1, $\lambda_1^2(D_n^\alpha) = 2$. Thus, using Proposition 5.1,

$$\delta(D_n^\alpha) = \frac{\lambda_1(D_n^\alpha)^n}{2^n \operatorname{vol}(D_n^\alpha)} = \frac{1}{2^{n/2}\alpha^{n-3}(\alpha^3 + \overline{\alpha}^3)}.$$

□

From the above corollary, we recover the center densities $\delta(D_n^1) = \frac{1}{2^{n/2+1}} = \delta(D_n)$ and $\delta(D_n^{\sqrt{2}}) = \frac{1}{2^n} = \delta(\sqrt{2}\mathbb{Z}^n)$. A natural question to ask is if the center density of D_n^α is always between these two extreme values, and whether or not different values for α produce the same center density. To answer this question we need the following lemma.

Lemma 5.1. *Let $n \geq 3$ be an integer. Define the real-valued function*

$$f : [1, \sqrt{2}] \to \mathbb{R}, \quad f(x) = x^{n-3}(x^3 + (2 - x^2)^{3/2}).$$

Then f is strictly increasing on $[1, \sqrt{2}]$.

Proof. A direct computation shows that

$$f'(x) = x^{n-4}\left((n-3)\left(x^3 + \left(2 - x^2\right)^{3/2}\right) + 3\left(x - \sqrt{2 - x^2}\right)x^2\right) > 0$$

for all $x \in (1, \sqrt{2})$, since $(n-3)(x^3 + (2-x^2)^{3/2}) \geq 0$ and $x - \sqrt{2-x^2} > 0$ when $x \in (1, \sqrt{2})$. □

We can now assert the following proposition:

Proposition 5.2. *The center density of D_n^α satisfies*

$$\delta(\mathbb{Z}^n) \leq \delta(D_n^\alpha) \leq \delta(D_n),$$

and the upper bound is achieved when $\alpha = 1$ and the lower bound is achieved when $\alpha = \sqrt{2}$. Moreover, $\delta(D_n^\alpha)$ is strictly decreasing on $[1, \sqrt{2}]$.

Proof. Let f be the function defined in Lemma 5.1. Then $\delta(D_n^\alpha) = \frac{1}{2^{n/2} f(\alpha)}$ and in particular, by the previous lemma, $\delta(D_n^\alpha)$ is strictly decreasing on $[1, \sqrt{2}]$. Therefore,

$$\delta(D_n^\alpha) \leq \frac{1}{2^{n/2} f(1)} = \frac{1}{2^{n/2+1}} = \delta(D_n)$$

and

$$\delta(D_n^\alpha) \geq \frac{1}{2^{n/2} f(\sqrt{2})} = \frac{1}{2^n} = \delta(\mathbb{Z}^n).$$

□

5.2.1 Integral deformed D_n lattices

From a computational perspective, the deformed D_n lattices can be problematic, since the basis vectors might contain irrational entries, or entries close to 1 if we wanted to have a high center density. Moreover, often we are interested in finding GWR lattices as a sublattice of the orthogonal lattice $\mathbb{Z}^n$. These considerations motivate finding integral versions of D_n^α, and in particular, versions contained in $\mathbb{Z}^n$.

One way to obtain a lattice D_n^α such that cD_n^α for some $c \neq 0$ is a sublattice of $\mathbb{Z}^n$ is to ensure that $\alpha, \overline{\alpha} \in \mathbb{Q}$ and then scale the lattice D_n^α with the denominator of α. If we suppose that $\alpha = p/q$ for some positive and relatively prime $p, q \in \mathbb{Z}$ such that $1 \leq p/q < \sqrt{2}$, then $\overline{\alpha} = \frac{\sqrt{2q^2-p^2}}{q} \in \mathbb{Q}$ if and only if $2q^2 - p^2$ is a square. Equivalently, (p, q) is a solution to the generalized Pell's equation $2y^2 - x^2 = d^2$ for some $d \in \mathbb{Z}$. There exists algorithms for finding a solution to such an equation (in fact, infinitely many solutions), if a solution exists. We are particularly interested in solutions for which q is small, since this gives a small determinant for qD_n^α, and for which p/q is close to 1, since this gives a high center density. Thus, it suffices to check case by case all small pairs of integers (p, q) which have the desired properties. Table 5.1 shows some pairs of integers (p, q), and corresponding d, $\alpha = p/q$, center density and normalized squared lattice minimum, such that $2q^2 - p^2 = d^2$ for some $d \in \mathbb{Z}$ and consequently, $qD_n^\alpha \subseteq \mathbb{Z}^n$. We have excluded the trivial case $p = q$ which yields D_n.

Table 5.1: Pairs of integers (p, q) which produce a sublattice $qD_n^\alpha \subseteq \mathbb{Z}^n$. Here $D_n^{\alpha\prime}$ denotes the lattice cD_n^α where c is chosen such that $\mathrm{vol}(cD_n^\alpha) = 1$.

p	q	d	α	$\delta(D_n^\alpha)$	$\lambda_1^2(D_n^{\alpha\prime})$
7	5	1	1.4	$\frac{2^{-\frac{n}{2}-3}\cdot 5^n\cdot 7^{3-n}}{43}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-3}\cdot 5^n\cdot 7^{3-n}}{43}\right)^{\frac{2}{n}}$
17	13	7	1.30769	$\frac{2^{-\frac{n}{2}-3}\cdot 13^n\cdot 17^{3-n}}{657}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-3}\cdot 13^n\cdot 17^{3-n}}{657}\right)^{\frac{2}{n}}$
31	25	17	1.24	$\frac{2^{-\frac{n}{2}-4}\cdot 25^n\cdot 31^{3-n}}{2169}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-4}\cdot 25^n\cdot 31^{3-n}}{2169}\right)^{\frac{2}{n}}$
49	41	31	1.19512	$\frac{2^{-\frac{n}{2}-4}\cdot 41^n\cdot 49^{3-n}}{9215}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-4}\cdot 41^n\cdot 49^{3-n}}{9215}\right)^{\frac{2}{n}}$
71	61	49	1.16393	$\frac{2^{-\frac{n}{2}-3}\cdot 61^n\cdot 71^{3-n}}{59445}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-3}\cdot 61^n\cdot 71^{3-n}}{59445}\right)^{\frac{2}{n}}$
97	85	71	1.14118	$\frac{2^{-\frac{n}{2}-3}\cdot 85^n\cdot 97^{3-n}}{158823}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-3}\cdot 85^n\cdot 97^{3-n}}{158823}\right)^{\frac{2}{n}}$
127	113	97	1.12389	$\frac{2^{-\frac{n}{2}-5}\cdot 113^n\cdot 127^{3-n}}{92533}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-5}\cdot 113^n\cdot 127^{3-n}}{92533}\right)^{\frac{2}{n}}$
161	145	127	1.11034	$\frac{2^{-\frac{n}{2}-5}\cdot 145^n\cdot 161^{3-n}}{194427}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-5}\cdot 145^n\cdot 161^{3-n}}{194427}\right)^{\frac{2}{n}}$
199	181	161	1.09945	$\frac{2^{-\frac{n}{2}-3}\cdot 181^n\cdot 199^{3-n}}{1506735}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-3}\cdot 181^n\cdot 199^{3-n}}{1506735}\right)^{\frac{2}{n}}$
287	265	241	1.08302	$\frac{2^{-\frac{n}{2}-4}\cdot 265^n\cdot 287^{3-n}}{2352339}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-4}\cdot 265^n\cdot 287^{3-n}}{2352339}\right)^{\frac{2}{n}}$
391	365	337	1.07123	$\frac{2^{-\frac{n}{2}-3}\cdot 365^n\cdot 391^{3-n}}{12256153}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-3}\cdot 365^n\cdot 391^{3-n}}{12256153}\right)^{\frac{2}{n}}$
511	481	449	1.06237	$\frac{2^{-\frac{n}{2}-6}\cdot 481^n\cdot 511^{3-n}}{3499245}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-6}\cdot 481^n\cdot 511^{3-n}}{3499245}\right)^{\frac{2}{n}}$

We provide an example which illustrates how an integral scaled D_n^α lattice can be obtained.

Example 5.1. *Suppose that $n = 4$ and $(p, q) = (7, 5)$. Then $\alpha = \frac{p}{q} = \frac{7}{5}$ and $\overline{\alpha} = \frac{d}{q} = \frac{1}{5}$, as seen from Table 5.1. In this case, a generator matrix for qD_n^α is given by*

$$M_{qD_n^\alpha} = \begin{bmatrix} 7 & 0 & 1 & 0 \\ 1 & 7 & 0 & 0 \\ 0 & 1 & 7 & 1 \\ 0 & 0 & 0 & -7 \end{bmatrix}.$$

By Corollary 5.1, (or from Table 5.1),

$$\delta(D_n^\alpha) = \frac{1}{2^{n/2}\alpha^{n-3}(\alpha^3+\overline{\alpha}^3)} = \frac{1}{2^{4/2}\cdot\left(\frac{7}{5}\right)^{4-3}\cdot\left(\left(\frac{7}{5}\right)^3+\left(\frac{1}{5}\right)^3\right)} \approx 0.0648879.$$

5.3 Deformed E_8 lattice

We proceed to deform the densest lattice in dimension 8, the E_8 lattice. In particular, we construct a GWR variant of the odd coordinate system version of the E_8 lattice, the Γ_8' lattice (see Definition 4.3).

Definition 5.3. *Let $1 \le \alpha \le \sqrt{2}$ and $\overline{\alpha} := \sqrt{2-\alpha^2}$. We define E_8^α to be the rank 8 lattice with generator matrix*

$$M_{E_8^\alpha} := \frac{1}{2}\begin{bmatrix} 1 & 2\alpha & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2\overline{\alpha} & 2\alpha & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2\overline{\alpha} & 2\alpha & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2\overline{\alpha} & 2\alpha & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 2\overline{\alpha} & 2\alpha & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 2\overline{\alpha} & 2\alpha & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 2\overline{\alpha} & 2\alpha \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2\overline{\alpha} \end{bmatrix}.$$

Note that $\alpha^2+\overline{\alpha}^2 = 2$ and that $E_8^1 = \Gamma_8'$. This motivates the notation.

Lemma 5.2. *The volume of E_8^α is given by*

$$\mathrm{vol}(E_8^\alpha) = \frac{1}{2}\left(\overline{\alpha}^2(\alpha-\overline{\alpha})(\alpha^4+\alpha^2\overline{\alpha}^2+\overline{\alpha}^4)+\alpha^6(\alpha+\overline{\alpha})\right).$$

Proof. A direct computation shows that

$$\det(M_{E_8^\alpha}) = -\frac{1}{2}\left(\overline{\alpha}^2(\alpha-\overline{\alpha})(\alpha^4+\alpha^2\overline{\alpha}^2+\overline{\alpha}^4)+\alpha^6(\alpha+\overline{\alpha})\right).$$

The claim follows from $\mathrm{vol}(E_8^\alpha) = |\det(M_{E_8}^\alpha)|$. □

The above lemma implies that E_8^α is a full rank lattice for all $1 \le \alpha \le \sqrt{2}$, and as expected, $\mathrm{vol}(E_8^1) = 1 = \mathrm{vol}(\Gamma_8')$. The following theorem states that E_8^α is a GWR lattice for all parameter values $1 < \alpha \le \sqrt{2}$.

Theorem 5.2. *Let $1 < \alpha \le \sqrt{2}$. Then E_8^α has a set of minimal vectors $S(E_8^\alpha) = \{\pm\mathbf{b}_1, \ldots, \pm\mathbf{b}_8\}$, where $\mathbf{b}_i$ is the i:th column of $M_{E_8^\alpha}$. In particular, E_8^α is GWR and $\lambda_1^2(E_8^\alpha) = 2$.*

To make computations easier, consider the lattice $2E_8^\alpha$, generated by the vectors $\mathbf{w}_i = 2\mathbf{b}_i$ for $i = 1, \ldots, 8$. It is clear that $\|\mathbf{w}_i\|^2 = 8$ for all $i = 1, \ldots, 8$ and thus, $\lambda_1^2(2E_8^\alpha) \leq 8$. Let $\mathbf{x} = \sum_{i=1}^8 c_i \mathbf{w}_i \in S(2E_8^\alpha)$. Then in particular, $\|\mathbf{x}\|^2 \leq 8$. Our goal is to show that $\mathbf{x} = \pm\mathbf{w}_i$, *i.e.*, $c_i = \pm 1$ for some $i = 1, \ldots, 8$ and $c_i = 0$ else. Write

$$\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} c_1 + 2c_2\alpha \\ c_1 + 2c_2\overline{\alpha} + 2c_3\alpha \\ c_1 + 2c_3\overline{\alpha} + 2c_4\alpha \\ c_1 + 2c_4\overline{\alpha} + 2c_5\alpha \\ c_1 + 2c_5\overline{\alpha} + 2c_6\alpha \\ c_1 + 2c_6\overline{\alpha} + 2c_7\alpha \\ -c_1 + 2c_7\overline{\alpha} + 2c_8\alpha \\ c_1 + 2c_8\overline{\alpha} \end{bmatrix},$$

where not all c_i's are zero. We have that

$$\begin{aligned} \|\mathbf{x}\|^2 &= (c_1 + 2c_2\alpha)^2 + (c_1 + 2c_2\overline{\alpha} + 2c_3\alpha)^2 + (c_1 + 2c_3\overline{\alpha} + 2c_4\alpha)^2 && (5.3) \\ &+ (c_1 + 2c_4\overline{\alpha} + 2c_5\alpha)^2 + (c_1 + 2c_5\overline{\alpha} + 2c_6\alpha)^2 && (5.4) \\ &+ (c_1 + 2c_6\overline{\alpha} + 2c_7\alpha)^2 + (-c_1 + 2c_7\overline{\alpha} + 2c_8\alpha)^2 + (c_1 + 2c_8\overline{\alpha})^2. && (5.5) \end{aligned}$$

We may without loss of generality assume that $c_1 \geq 0$, since we can replace $\mathbf{x}$ by $-\mathbf{x}$ if necessary. Let us consider two cases separately: $c_1 = 0$ and $c_1 = k > 0$.

Case 1: $c_1 = 0$. The expression for $\|\mathbf{x}\|^2$ reduces to

$$\begin{aligned} \|\mathbf{x}\|^2 &= 4c_2^2\alpha^2 + (2c_2\overline{\alpha} + 2c_3\alpha)^2 + (2c_3\overline{\alpha} + 2c_4\alpha)^2 && (5.6) \\ &+ (2c_4\overline{\alpha} + 2c_5\alpha)^2 + (2c_5\overline{\alpha} + 2c_6\alpha)^2 + (2c_6\overline{\alpha} + 2c_7\alpha)^2 && (5.7) \\ &+ (2c_7\overline{\alpha} + 2c_8\alpha)^2 + 4c_8^2\overline{\alpha}^2. && (5.8) \end{aligned}$$

Suppose that $\mathbf{x}$ has at least two non-zero coefficients. Let c_j, c_k be two such coefficients, where $j, k \in \{2, \ldots, 8\}$ and j is minimal and k is maximal. Then

$$\begin{aligned} \|\mathbf{x}\|^2 &= 4c_j^2\alpha^2 + (2c_j\overline{\alpha} + 2c_{j+1}\alpha)^2 + \cdots + (2c_{k-1}\overline{\alpha} + 2c_k\alpha)^2 + 4c_k^2\overline{\alpha}^2 && (5.9) \\ &> 4c_j^2\alpha^2 + 4c_k^2\overline{\alpha}^2 \geq 4(\alpha^2 + \overline{\alpha}^2) = 8, && (5.10) \end{aligned}$$

since $c_i\overline{\alpha} + c_{i+1}\alpha \neq 0$ when $c_i, c_{i+1} \in \{\pm 1\}$, because $1 < \alpha \leq \sqrt{2}$. This contradicts $\mathbf{x} \in S(E_8^\alpha)$; therefore, only one coefficient can be non-zero. Now since $\|\mathbf{w}_i\|^2 = 8$, we must have $c_i = \pm 1$ for exactly one index $i \in \{2, \ldots, 8\}$.

Case 2: $c_1 = k > 0$. Our goal is to derive bounds $l_i \leq c_i \leq u_i$ for $i \in \{1, \ldots, 8\}$ and then simply check that for each combination of coefficients

within the bounds, $\|\mathbf{x}\|^2 > 8$ for all $\alpha \in (1, \sqrt{2}]$, except for the case $c_1 = 1$ and $c_i = 0$ for $i \in \{2, \ldots, 8\}$, where equality holds. We obtain the bounds by simply noticing that $\|\mathbf{x}\| \leq x_i^2 \leq 8$, and in particular, $|x_i| < 3$ for each i. We will need to use that $0 \leq \overline{\alpha} < 1 < \alpha \leq \sqrt{2}$ and that $0 \leq \frac{\overline{\alpha}}{\alpha} < 1$.

We first derive bounds for c_i, where $i \in \{2, \ldots, 8\}$, in terms of k, and then derive bounds for k. We begin with c_2. Note that

$$|x_1| < 3 \implies -3 < k + 2c_2\alpha < 3 \implies \frac{-3-k}{2\alpha} < c_2 < \frac{3-k}{2\alpha} < 1.$$

Using the above, we get a lower bound for c_3 by estimating x_2 from above and using the condition $-3 < x_2$, as follows:

$$x_2 = k + 2c_2\overline{\alpha} + 2c_3\alpha \leq k + 2c_3\alpha,$$

$$\implies -3 < k + 2c_3\alpha \implies \frac{-3-k}{2\alpha} < c_3.$$

Similarly, to get an upper bound on c_3,

$$x_2 = k + 2c_2\overline{\alpha} + 2c_3\alpha \geq k + 2\left(\frac{-3-k}{2\alpha}\right)\overline{\alpha} + 2c_3\alpha \geq -3 + 2c_3\alpha,$$

$$\implies -3 + 2c_3\alpha < 3 \implies c_3 < \frac{3}{\alpha}.$$

To get a lower bound for c_4,

$$x_3 = k + 2c_3\overline{\alpha} + 2c_4\alpha \leq k + 6 + 2c_4\alpha,$$

$$\implies -3 < k + 6 + 2c_4\alpha \implies \frac{-9-k}{2\alpha} < c_4.$$

Similarly, to get an upper bound for c_4,

$$x_3 = k + 2c_3\overline{\alpha} + 2c_4\alpha \geq k + 2\left(\frac{-3-k}{2\alpha}\right)\overline{\alpha} + 2c_4\alpha \geq -3 + 2c_4\alpha,$$

$$\implies -3 + 2c_4\alpha < 3 \implies c_4 < \frac{3}{\alpha}.$$

To derive a lower bound for c_5, note that

$$x_4 = k + 2c_4\overline{\alpha} + 2c_5\alpha \leq k + 6 + 2c_5\alpha,$$

$$\implies -3 < k + 6 + 2c_5\alpha \implies \frac{-9-k}{2\alpha} < c_5.$$

For the upper bound for c_5, note that

$$x_4 = k + 2c_4\overline{\alpha} + 2c_5\alpha \geq k + 2\left(\frac{-9-k}{2\alpha}\right)\overline{\alpha} + 2c_5\alpha \geq -9 + 2c_5\alpha,$$

$$\implies -9 + 2c_5\alpha < 3 \implies c_5 < \frac{6}{\alpha}.$$

To get a lower bound for c_6, note that

$$x_5 = k + 2c_5\overline{\alpha} + 2c_6\alpha \leq k + 12 + 2c_6\alpha,$$

$$\implies -3 < k + 12 + 2c_6\alpha \implies \frac{-15-k}{2\alpha} < c_6.$$

For the upper bound for c_6, note that

$$x_5 = k + 2c_5\overline{\alpha} + 2c_6\alpha \geq k + 2\left(\frac{-9-k}{2\alpha}\right)\overline{\alpha} + 2c_6\alpha \geq -9 + 2c_6\alpha,$$

$$\implies -9 + 2c_6\alpha < 3 \implies c_6 < \frac{6}{\alpha}.$$

Then for the lower bound for c_7,

$$x_6 = k + 2c_6\overline{\alpha} + 2c_7\alpha \leq k + 12 + 2c_7\alpha,$$

$$\implies -3 < k + 12 + 2c_7\alpha \implies \frac{-15-k}{2\alpha} < c_7.$$

We get an upper bound for c_7 by noting that

$$x_6 = k + 2c_6\overline{\alpha} + 2c_7\alpha \geq k + 2\left(\frac{-15-k}{2\alpha}\right)\overline{\alpha} + 2c_7\alpha \geq -15 + 2c_7\alpha,$$

$$\implies -15 + 2c_7\alpha < 3 \implies c_7 < \frac{9}{\alpha}.$$

Similarly for c_8, we get a lower bound by noting that

$$x_7 = -k + 2c_7\overline{\alpha} + 2c_8\alpha \leq -k + 18 + 2c_8\alpha,$$

$$\implies -3 < -k + 18 + 2c_8\alpha \implies \frac{-21+k}{2\alpha} < c_8,$$

and an upper bound by noticing that

$$x_7 = -k + 2c_7\overline{\alpha} + 2c_8\alpha \geq -k + 2\left(\frac{-15-k}{2\alpha}\right)\overline{\alpha} + 2c_8\alpha \geq -2k - 15 + 2c_8\alpha,$$

$$\implies -2k - 15 + 2c_8\alpha < 3 \implies c_8 < \frac{9+k}{\alpha}.$$

Finally, we have that

$$x_8 = k + 2c_8\overline{\alpha} \geq k + 2\left(\frac{-21+k}{2\alpha}\right)\overline{\alpha} \geq 2k - 21$$

when $k \leq 21$, and since we require $x_8 < 3$, we must have $k < 12$. If $k > 21$ then $x_8 > 21$ so certainly these values of k are not acceptable.

Let us collect the bounds that we have so far:

1. $l_1 = 1 \leq k \leq 11 = u_1$.
2. $l_2 = \frac{-3-k}{2} \leq \frac{-3-k}{2\alpha} < c_2 < \frac{3-k}{2\alpha} \leq \frac{3-k}{2\sqrt{2}} = u_2$. The last inequality is valid when $k \geq 3$, but since $c_2 \leq 0$, u_2 serves as an upper bound for all $k \geq 1$.
3. $l_3 = \frac{-3-k}{2} \leq \frac{-3-k}{2\alpha} < c_3 < \frac{3}{\alpha} \leq 3 = u_3$.
4. $l_4 = \frac{-9-k}{2} \leq \frac{-9-k}{2\alpha} < c_4 < \frac{3}{\alpha} \leq 3 = u_4$.
5. $l_5 = \frac{-9-k}{2} \leq \frac{-9-k}{2\alpha} < c_5 < \frac{6}{\alpha} \leq 6 = u_5$.
6. $l_6 = \frac{-15-k}{2} \leq \frac{-15-k}{2\alpha} < c_6 < \frac{6}{\alpha} \leq 6 = u_6$.
7. $l_7 = \frac{-15-k}{2} \leq \frac{-15-k}{2\alpha} < c_7 < \frac{9}{\alpha} \leq 9 = u_7$.
8. $l_8 = \frac{-21+k}{2} \leq \frac{-21+k}{2\alpha} < c_8 < \frac{9+k}{\alpha} < 9 + k = u_8$.

To summarize, for each $k \in \{1, \ldots, 11\}$ we have to compute the bounds l_i and u_i for every $i \in \{2, \ldots, 8\}$ and then for each combination of coefficients $(k, c_2, \ldots, c_8) \in \{1, \ldots, 11\} \times \{\lceil l_2 \rceil, \ldots, \lfloor u_2 \rfloor\} \times \cdots \times \{\lceil l_8 \rceil, \ldots, \lfloor u_8 \rfloor\}$ compute the resulting value of $\|\mathbf{x}\|^2$, which depends on α.

Instead of checking each combination by hand, we refer to the source code in Appendix A. The code, which is written with the Mathematica language, performs a nested for-loop where the coefficients $k, c_2, \ldots, c_8$ range between l_i and u_i for each $i \in \{1, \ldots, 8\}$. If at some iteration $\min_{\alpha \in [1,\sqrt{2}]} x_1^2 + \cdots + x_k^2 > 8$ for some $k \in \{1, \ldots, 8\}$, then the code does not check for further coefficients. Instead, it breaks out of the current for-loop. For those combinations of coefficients for which

$$m := \min_{\alpha \in [1,\sqrt{2}]} x_1^2 + \cdots + x_8^2 \leq 8,$$

the code outputs the value of m, the corresponding coefficients, as well as the values for α for which $\|\mathbf{x}\|^2 = m$.

It turns out that no combination of coefficients yields $m < 8$, and that 92 combinations of coefficients yield $m = 8$. In 91 cases, $m = 8$ is achieved by $\alpha = 1$ but not by any $\alpha \in (1, \sqrt{2}]$, and in one case, namely

$$(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8) = (1, 0, 0, 0, 0, 0, 0, 0),$$

$m = 8$ is achieved by all $\alpha \in [1, \sqrt{2}]$. This proves the theorem. □

Using the previous theorem, we are able to express the center density of E_8^α.

Proposition 5.3. *The center density of E_8^α is given by*

$$\delta(E_8^\alpha) = \frac{1}{8\left(\overline{\alpha}^2(\alpha - \overline{\alpha})(\alpha^4 + \alpha^2\overline{\alpha}^2 + \overline{\alpha}^4) + \alpha^6(\alpha + \overline{\alpha})\right)}.$$

Proof. By Lemma 5.2 and Theorem 5.2,

$$\begin{aligned}
\delta(E_8^\alpha) &= \frac{\lambda_1(E_8^\alpha)^8}{2^8 \operatorname{vol}(E_8^\alpha)} && (5.11)\\
&= \frac{2^4}{2^8 \cdot \frac{1}{2}\left(\overline{\alpha}^2(\alpha - \overline{\alpha})(\alpha^4 + \alpha^2\overline{\alpha}^2 + \overline{\alpha}^4) + \alpha^6(\alpha + \overline{\alpha})\right)} && (5.12)\\
&= \frac{1}{8\left(\overline{\alpha}^2(\alpha - \overline{\alpha})(\alpha^4 + \alpha^2\overline{\alpha}^2 + \overline{\alpha}^4) + \alpha^6(\alpha + \overline{\alpha})\right)}. && (5.13)
\end{aligned}$$

□

5.3.1 Integral deformed E_8 lattice

Our goal in this section is to find scaled variants of the E_8^α lattice as a sublattice of $\mathbb{Z}^8$. We apply the exact same strategy as with the D_n^α lattice. Let $\alpha = \frac{p}{q}$ for some relatively prime, positive $p, q \in \mathbb{Z}$ such that $1 \leq p/q < \sqrt{2}$. Then $\overline{\alpha} = \frac{\sqrt{2q^2 - p^2}}{q} \in \mathbb{Q}$ if and only if $2q^2 - p^2 = d^2$ for some $d \in \mathbb{Z}$. If this is the case, then $2qE_8^\alpha$ is a sublattice of $\mathbb{Z}^8$. We want to find small values for q to get a small determinant for $2qE_8^\alpha$, and a value of $\alpha = \frac{p}{q}$ which is close to 1 to maximize the center density. Table 5.2 shows some pairs of integers (p, q), and corresponding α, d, center density and squared lattice minimum, such that $2q^2 - p^2 = d^2$ for some $d \in \mathbb{Z}$ and thus, $2qE_8^\alpha \subseteq \mathbb{Z}^n$. As the table indicates, if we desire a high center density, we have to accept large values for q.

Table 5.2: Examples of pairs of integers (p, q) which produce a sublattice $2qE_8^\alpha \subseteq \mathbb{Z}^8$. Here $E_8^{\alpha\prime}$ denotes the lattice cE_8^α where c is chosen such that $\mathrm{vol}(cE_8^\alpha) = 1$.

p	q	d	α	$\delta(E_8^\alpha)$	$\lambda_1^2(E_8^{\alpha\prime})$
7	5	1	1.4	0.0102162	1.27169
17	13	7	1.30769	0.0124829	1.33702
31	25	17	1.24	0.0159616	1.42177
49	41	31	1.19512	0.0192763	1.49045
71	61	49	1.16393	0.0222471	1.54482
97	85	71	1.14118	0.0248757	1.58856
127	113	97	1.12389	0.0272007	1.62445
161	145	127	1.11034	0.0292647	1.65442
241	221	199	1.0905	0.0327571	1.70171
337	313	287	1.07668	0.0355924	1.7374
449	421	391	1.06651	0.0379372	1.76533
647	613	577	1.05546	0.0407789	1.7975
881	841	799	1.04756	0.0430324	1.82183
1249	1201	1151	1.03997	0.0453987	1.84638
1799	1741	1681	1.03331	0.0476548	1.8689
2591	2521	2449	1.02777	0.0496839	1.88849
4049	3961	3871	1.02222	0.0518646	1.90888
6727	6613	6497	1.01724	0.0539629	1.9279
30257	30013	29767	1.00813	0.0582025	1.9647
95047	94613	94177	1.00459	0.0600098	1.97977
301087	300313	299537	1.00258	0.0610791	1.98853

Chapter 6

Conclusion

In this work, we have explored Lagrangian lattices, and their well-rounded sublattices. We have seen that the sublattices are GWR under certain circumstances, and characterized the packing densities of said sublattices. We have also given a condition which tells when a well-rounded sublattice is equivalent to $\mathbb{Z}^n$ or A_n. The Lagrangian lattices can be constructed from tame, Galois number fields of prime degree, as a theorem (Theorem 4.1) by Conner and Perlis [6] shows. Recently, this theorem has been generalized to hold for tame, Galois, cyclic number fields of arbitrary degree [5]. This shows that the set of number fields giving rise to Lagrangian lattices can be quite large. An interesting, but perhaps a very difficult task would be to characterize all or most of the number fields whose ring of integers have a Lagrangian basis.

Our construction of the deformed lattices D_n^α and E_8^α provide a way to obtain GWR lattices with packing densities arbitrarily close to the optimal density in dimensions 3–5 and 8. The philosophy behind the deformed lattices is slightly different from the philosophy behind the Lagrangian sublattices. While the Lagrangian sublattices are obtained via an injective map $\Phi_{(r,s)} : \mathcal{L} \to \mathcal{L}$, the deformed lattices are obtained by, in essence, rotating the the basis vectors of a dense lattice in certain directions in space. The downside of the deformed lattices is that they rely on the existence of a dense (or the densest) lattice in a given dimension, and the densest lattices are known only in a handful of dimensions – even worse, the optimal packing density is known only in a few dimensions. Of course, one could start with the orthogonal lattice $\mathbb{Z}^n$ and then deform it, but it is not obvious how the basis vectors should be deformed in order to obtain a GWR lattice with good packing density.

The deformed lattices are an instance of a more general phenomenon, where a closed interval $I \subset \mathbb{R}$ is mapped to a subset of rank n lattices. If we identify a lattice with its generator matrix, which is unique up to multiplication by a unimodular matrix, the deformations can be seen as maps

$$\xi : I \to \mathrm{GL}_n(\mathbb{R}) / \mathrm{GL}_n(\mathbb{Z}).$$

Especially the case when ξ is injective seems interesting. The map

$$\xi : [1, \sqrt{2}] \to \mathrm{GL}_n(\mathbb{R}) / \mathrm{GL}_n(\mathbb{Z}), \quad \alpha \mapsto D_n^\alpha$$

is an example of such a map, with the property that $\xi(1) = D_n$ and $\xi(\sqrt{2}) = \sqrt{2}\mathbb{Z}^n$. These kinds of transformations could produce interesting lattices. A concrete future research task would be to construct GWR variants of E_6, E_7, Λ_{24} and other known optimal lattice packings.

We mentioned in the beginning of this thesis that the motivation to find GWR lattices with good packing density has its origins in secure wireless communications and in particular, lattice coset coding in wiretap channels. We have not addressed the coding theoretic aspects of lattice coset coding, nor have we described the various channel types that exist. Although the simulations in [8], [9], [13], [14] indicate that well-rounded lattices, and in particular, well-rounded lattices with a small kissing number and high packing density outperform other lattices, it is not known if GWR lattices with high packing density are the best ones. One thing to keep in mind with the deformed lattices D_n^α and E_8^α is that, for α-values close to 1, the lattices have lattice vectors of length very close to the lattice minimum.

Nevertheless, the integral deformed lattices presented in sections 5.2.1 and 5.3.1 are an attempt to construct lattices suitable for lattice coset codes, based on currently known criteria for good lattice coset codes. Whether or not these lattices are useful in practice, should be evaluated by simulations in actual wiretap channels. Figure 6.1 summarizes where some of the lattices studied in this thesis lie on the graph where the horizontal axis is the squared shortest vector length and the vertical axis is the kissing number. We chose dimension 8, partially because the lattices studied in this thesis are represented in this dimension, but also because this seems to be a popular choice of the dimension of lattices used in lattice coset codes.

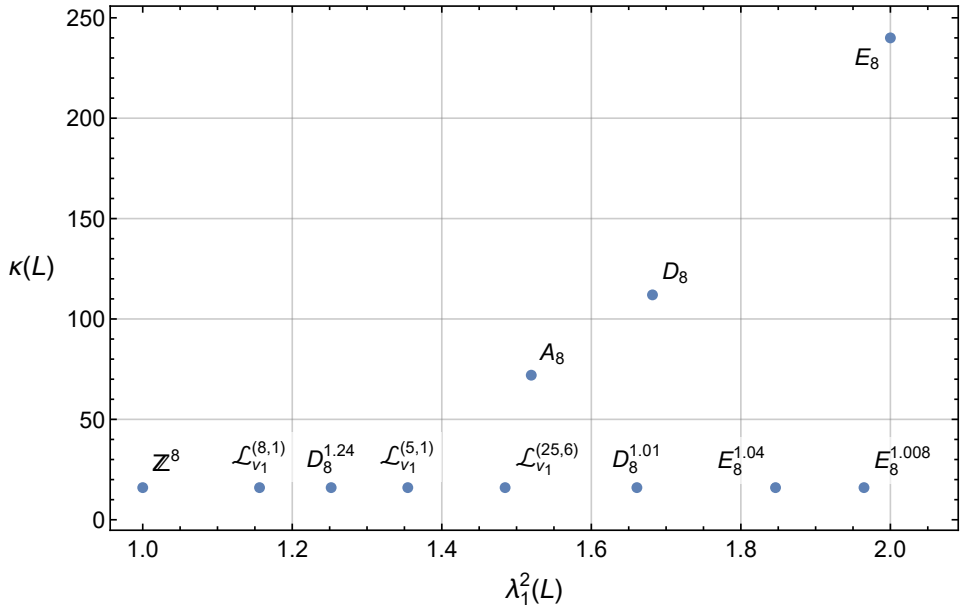


Figure 6.1: An overview of the kissing number versus squared lattice minimum of some 8-dimensional lattices constructed and studied in this thesis.

Appendix A

Source code for Theorem 5.2

```
In[1]:= (*Author: Niklas Miller, 1.12.2020*)
        g[a_] = Sqrt[2-a^2]; (*Conjugate of a*)
        sv = 0; (*Number of shortest vectors found*)
        For[k=1, k<=11, k++,
         For[c2=Ceiling[(-3-k)/2], c2<=Floor[(3-k)/(2 Sqrt[2])], c2++,
         x1[a_] = k + 2 c2*a;
         min1 = Minimize[{x1[a]^2, 1<=a<=Sqrt[2]}, a];
         For[c3=Ceiling[(-3-k)/2], c3<=3, c3++,
          If[min1[[1]] > 8, Break[]];
          x2[a_] = k + 2*c2*g[a] + 2*c3*a;
          min2 = Minimize[{x1[a]^2+x2[a]^2, 1<=a<=Sqrt[2]}, a];
          For[c4=Ceiling[(-9-k)/2], c4<=3, c4++,
           If[min2[[1]] > 8, Break[]];
           x3[a_] = k + 2*c3*g[a] + 2*c4*a;
           min3 = Minimize[{x1[a]^2+x2[a]^2+x3[a]^2,
                1<=a<=Sqrt[2]}, a];
           For[c5=Ceiling[(-9-k)/2], c5<=6, c5++,
            If[min3[[1]] > 8, Break[]];
            x4[a_] = k + 2*c4*g[a] + 2*c5*a;
            min4 = Minimize[{x1[a]^2+x2[a]^2+x3[a]^2+x4[a]^2,
                1<=a<=Sqrt[2]}, a];
            For[c6=Ceiling[(-15-k)/2], c6<=6, c6++,
             If[min4[[1]] > 8, Break[]];
             x5[a_] = k + 2*c5*g[a] + 2*c6*a;
             min5 = Minimize[{x1[a]^2+x2[a]^2+x3[a]^2+x4[a]^2+x5[a]^2,
                1<=a<=Sqrt[2]}, a];
             For[c7=Ceiling[(-15-k)/2], c7<=9, c7++,
              If[min5[[1]] > 8, Break[]];
              x6[a_] = k + 2*c6*g[a] + 2*c7*a;
```

In[2]:=

```
min6 = Minimize[{x1[a]^2+x2[a]^2+x3[a]^2
     +x4[a]^2+x5[a]^2+x6[a]^2, 1<=a<=Sqrt[2]}, a];
  For[c8=Ceiling[(-21+k)/2], c8<=9+k, c8++,
   If[min6[[1]] > 8, Break[]];
   x7[a_] = -k + 2*c7*g[a] + 2*c8*a;
   x8[a_] = k + 2*c8*g[a];
   f[a_] = x1[a]^2+x2[a]^2+x3[a]^2+x4[a]^2
   +x5[a]^2+x6[a]^2+x7[a]^2+x8[a]^2;
   min8 = Minimize[{f[a], 1<=a<=Sqrt[2]}, a];
   If[min8[[1]] <= 8,
     sv += 1;
     (*Print results. "Reduce" outputs for which
     1<=a<=sqrt(2) the squared norm is equal to
     the minimum value.*)
     Print["Number of shortest vectors found: ", sv,
     ". Coefficients (c1,c2,...,c8)=(", k, ",", c2, ",", c3,
     ",", c4, ",",  c5, ",", c6, ",", c7, ",", c8, "). ",
     "Squared norm ", FullSimplify[f[a]], " = ", min8[[1]],
     " at ", min8[[2]], ". Squared norm at a = 1.01: ",
     FullSimplify[f[1.01]], ". Squared norm = ", min8[[1]],
     " when ", Reduce[f[a] == min8[[1]] && 1<=a<=Sqrt[2]], "."
      ]
     ]
    ]
   ]
  ]
 ]
]
```

Bibliography

[1] Bachoc, C., and Vallentin, F. New upper bounds for kissing numbers from semidefinite programming. *Journal of the American Mathematical Society 21*, 3 (2008), 909–924.

[2] Ball, K. A lower bound for the optimal density of lattice packings. *International Mathematics Research Notices 1992*, 10 (1992), 217–221.

[3] Belfiore, J.-C., and Oggier, F. Lattice code design for the Rayleigh fading wiretap channel. In *2011 IEEE International Conference on Communications Workshops (ICC)* (2011), pp. 1–5.

[4] Blichfeldt, H. F. A new principle in the geometry of numbers, with some applications. *Transactions of the American Mathematical Society 15*, 3 (1914), 227–235.

[5] Bolaños, W., and Mantilla-Soler, G. The trace form over cyclic number fields. *Canadian Journal of Mathematics* (2020), 1–23.

[6] Conner, P. E., and Perlis, R. *A Survey Of Trace Forms Of Algebraic Number Fields*. World Scientific, 1984.

[7] Conway, J. H., and Sloane, N. J. A. *Sphere Packings, Lattices and Groups (3. ed.)*. New York: Springer, 1999.

[8] Damir, M. T., Gnilke, O., Amorós, L., and Hollanti, C. Analysis of some well-rounded lattices in wiretap channels. In *2018 IEEE 19th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)* (2018), IEEE, pp. 1–5.

[9] Damir, M. T., Karrila, A., Amorós, L., Gnilke, O., Karpuk, D., and Hollanti, C. Well-rounded lattices: Towards optimal coset codes for Gaussian and fading wiretap channels. *arXiv preprint arXiv:1609.07723v4* (2020).

[10] Damir, M. T., and Mantilla-Soler, G. Bases of minimal vectors in Lagrangian lattices. *arXiv preprint arXiv:2006.16794* (2020).

[11] Fukshansky, L. Revisiting the hexagonal lattice: on optimal lattice circle packing. *Elemente der Mathematik 66*, 1 (2011), 1–9.

[12] Fukshansky, L., and Petersen, K. On well-rounded ideal lattices. *International Journal of Number Theory 8*, 1 (2012), 189–206.

[13] Gnilke, O. W., Barreal, A., Karrila, A., Tran, H. T. N., Karpuk, D., and Hollanti, C. Well-rounded lattices for coset coding in MIMO wiretap channels. In *2016 26th International Telecommunication Networks and Applications Conference (ITNAC)* (2016), IEEE, pp. 289–294.

[14] Gnilke, O. W., Tran, H. T. N., Karrila, A., and Hollanti, C. Well-rounded lattices for reliability and security in Rayleigh fading SISO channels. In *2016 IEEE Information Theory Workshop (ITW)* (2016), IEEE, pp. 359–363.

[15] Hales, T. C. A proof of the Kepler conjecture. *Annals of mathematics 162*, 3 (2005), 1065–1185.

[16] Kabatiansky, G. A., and Levenshtein, V. I. On bounds for packings on a sphere and in space. *Problemy Peredači Informacii 14*, 1 (1978), 3–25.

[17] Martinet, J. Bases of minimal vectors in lattices, ii. *Archiv der Mathematik 89*, 6 (2007), 541–551.

[18] Martinet, J., and Schürmann, A. Bases of minimal vectors in lattices, iii. *International Journal of Number Theory 8*, 2 (2012), 551–567.

[19] Milne, J. S. Algebraic number theory (v3.08). Available: `www.jmilne.org/math/`, 2020. [Online; accessed 2020-10-28].

[20] Mittelmann, H. D., and Vallentin, F. High-accuracy semidefinite programming bounds for kissing numbers. *Experimental Mathematics 19*, 2 (2010), 175–179.

[21] Narkiewicz, W. *Elementary and analytic theory of algebraic numbers*. Springer, 2004.

[22] Nebe, G., and Sloane, N. J. A. Table of densest packings presently known. Available: `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/density.html`, 2012. [Online; accessed 2020-10-07].

[23] Neukirch, J. *Algebraic Number Theory*. Springer, 2010.

[24] Oggier, F., Sole, P., and Belfiore, J.-C. Lattice codes for the wiretap Gaussian channel: Construction and analysis. *IEEE Transactions on Information Theory 62*, 10 (2016), 5690–5708.

[25] Oggier, F., and Viterbo, E. Algebraic number theory and code design for Rayleigh fading channels. *Foundations and Trends in Communications and Information Theory 1*, 3 (2004), 333–415.

[26] Ozarow, L. H., and Wyner, A. D. Wire-tap channel ii. *AT&T Bell Laboratories technical journal 63*, 10 (1984), 2135–2157.

[27] Schütte, K., and van der Waerden, B. L. Das Problem der dreizehn Kugeln. *Mathematische Annalen 125*, 1 (1952), 325–334.

[28] Shannon, C. E. A mathematical theory of communication. *The Bell system technical journal 27*, 3 (1948), 379–423.

[29] Stewart, I. *Galois Theory, Third Edition*. Chapman Hall/CRC Mathematics Series. Taylor & Francis, 2003.

[30] Thue, A. Om nogle geometrisk-taltheoretiske Theoremer. *Forandlingerneved de Skandinaviske Naturforskeres 14* (1892), 352–353.

[31] Vladuts, S. Lattices with exponentially large kissing numbers. *arXiv preprint arXiv:1802.00886* (2018).

[32] Voronoi, G. Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs. *Journal für die reine und angewandte Mathematik (Crelles Journal) 1908*, 134 (1908), 198–287.

[33] Wyner, A. D. The wire-tap channel. *The Bell System Technical Journal 54*, 8 (1975), 1355–1387.

[34] Wyner, A. D. Capabilities of bounded discrepancy decoding. *The Bell System Technical Journal 44*, 6 (1965), 1061–1122.