Hollanti, Camilla; Mantilla-Soler, Guillermo; Miller, Niklas

Dense Generic Well-Rounded Lattices

Published in:
SIAM Journal on Applied Algebra and Geometry

DOI:
10.1137/22M1532779

Published: 01/01/2025

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Hollanti, C., Mantilla-Soler, G., & Miller, N. (2025). Dense Generic Well-Rounded Lattices. *SIAM Journal on Applied Algebra and Geometry*, *9*(1), 154-185. https://doi.org/10.1137/22M1532779

SIAM J. APPL. ALGEBRA GEOMETRY
Vol. 9, No. 1, pp. 154–185

Dense Generic Well-Rounded Lattices*

Camilla Hollanti†, Guillermo Mantilla-Soler‡, and Niklas Miller†

Abstract. It is well known that the densest lattice sphere packings also typically have large kissing numbers. The sphere packing density maximization problem is known to have a solution among well-rounded lattices, of which the integer lattice $\mathbb{Z}^n$ is the simplest example. The integer lattice is also an example of a generic well-rounded lattice, i.e., a well-rounded lattice with a minimal kissing number. However, the integer lattice has the worst density among well-rounded lattices. In this paper, the problem of constructing explicit generic well-rounded lattices with dense sphere packings is considered. To this end, so-called *tame* lattices recently introduced by Damir and Mantilla-Soler are utilized. Tame lattices came to be as a generalization of the ring of integers of certain abelian number fields. The sublattices of tame lattices constructed in this paper are shown to always result in either a generic well-rounded lattice or the lattice A_n, with density ranging between that of $\mathbb{Z}^n$ and A_n. In order to find generic well-rounded lattices with densities beyond that of A_n, explicit deformations of some known densest lattice packings are constructed, yielding a family of generic well-rounded lattices with densities arbitrarily close to the optimum. In addition to being an interesting mathematical problem in its own right, the constructions are also motivated from a more practical point of view. Namely, generic well-rounded lattices with high packing density make good candidates for lattice codes used in secure wireless communications.

Key words. dense lattice sphere packings, generic well-rounded lattices, kissing number, tame lattices, trace forms

MSC codes. 11H31, 11F27, 11P21, 11H71

DOI. 10.1137/22M1532779

1. Introduction.

Lattices are of broad interest both in mathematics and applications. *Well-rounded lattices* [22, 21] are a profound family of lattices, providing a sufficient source for various optimization problems. For instance, the known densest lattice sphere packings (e.g., the Gosset lattice E_8) arise from well-rounded lattices, and it has been shown that the lattice sphere packing problem can be restricted to the space of well-rounded lattices also in general. A prominent feature of well-rounded lattices is that the set of shortest vectors spans the ambient space. Previously, constructions of well-rounded lattices have been considered in, e.g., [16, 1, 19, 8, 2], and they also relate to the famous Minkowski and Woods conjectures [27].

*Received by the editors November 3, 2022; accepted for publication (in revised form) November 7, 2024; published electronically February 14, 2025.
https://doi.org/10.1137/22M1532779
Funding: This work was supported by Research Council of Finland grant 351271. The visiting professor funding from the Aalto Science Institute to the second author is also gratefully acknowledged.

†Department of Mathematics and Systems Analysis, Aalto University, Espoo, 00076, Finland (camilla.hollanti@aalto.fi, niklas.miller@aalto.fi).
‡Department of Mathematics, Universidad Nacional de Colombia sede Medellín, Columbia (gmantelia@gmail.com).

One way to describe a lattice Λ is via its theta series (see section 2 for a rigorous definition),

$$\Theta_\Lambda(q) := \sum_{\mathbf{x}\in\Lambda} q^{\|\mathbf{x}\|^2}, \quad |q| < 1,$$

which is also closely related to the so-called *flatness factor* utilized in wireless security [25] and the *smoothing parameter* in cryptography [28]. In [17], it was shown that well-rounded lattices yield promising candidates for lattice codes in wireless communications [32] and physical layer security [9]. This stems from the fact that certain optimization problems related to such code design can be restricted to the set of well-rounded lattices. This connection will be elaborated more in section 2.2. Here, let us just briefly mention that one such optimization problem is the minimization of the theta function [5, 17]. However, computing the value of a theta function is far from easy, which makes finding the minimum in general very hard. Indeed, the minimum is known only in few dimensions and is not always the densest lattice packing [29]. To this end, if we look at a simple truncation of the theta function corresponding to the first minimum, it becomes evident that the minimization problem in this case can be formulated as simultaneously maximizing the first minimum (i.e., the lattice packing density) and minimizing the number of shortest vectors (i.e., the kissing number). Unfortunately, there is no obvious tradeoff between these two goals. Namely, the densest packings tend to exhibit large kissing numbers. Hence, it is interesting to study dense *generic well-rounded (GWR) lattices* having minimal kissing numbers, as proposed in [17]. Naturally, the truncation approximation is coarse. In [3], a novel theta function approximation was derived, enabling efficient comparison of candidate lattice codes in the above light.

Motivated by these findings, *tame lattices* were introduced in [18], providing a source for constructing explicit well-rounded lattices. In the present paper, we take a step further and show that tame lattices also give rise to GWR lattices. Moreover, we show that by distorting some of the densest lattice packings, it is possible to construct lattices that simultaneously have a large minimum distance and a small kissing number. Such lattices should provide ideal solutions for reliable and secure communications. More specifically, our main contributions are the following:

- In Theorem 3.6, we state a stronger version of Theorem 4.9 in [18], namely, that a well-rounded lattice of the form $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ (see Definition 3.3) is GWR or similar to A_n.
- In Proposition 3.9, we prove that for the center densities it holds that

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

- In Theorem 3.10, we give two conditions which tell when a well-rounded lattice $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is similar to either $\mathbb{Z}^n$ or A_n. This is particularly interesting from an applications point of view, as discussed in section 5.
- In Theorem 3.15, we show that the dual of a lattice of the form $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$ is of the same type.
- In sections 4.2 and 4.3 we introduce *deformed* lattices D_n^α and E_8^α, where α is a real parameter, and in Theorems 4.4 and 4.10 we prove that these lattices are GWR if they are not similar to D_n and E_8, respectively. It is also shown that the center density can be brought arbitrarily close to the optimum.

Let us next provide some mathematical motivation for the concept of tame lattices.

Let p be an odd prime, and let K be a number field that is Galois over $\mathbb{Q}$ and such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}/p\mathbb{Z}$. In [11, section IV.8] Conner and Perlis showed that if K is tame, i.e., no rational prime has wild ramification, then there exists an integral basis for O_K, which they called the *Lagrangian basis,* such that the Gram matrix of the integral trace in such basis is a $p \times p$ matrix of the form

$$\begin{bmatrix} a & -h & \dots & -h \\ -h & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & -h \\ -h & \dots & -h & a \end{bmatrix}.$$

The values of a and h are given by

$$a = \frac{d(p-1)+1}{p}, \quad h = \frac{d-1}{p},$$

where d is the conductor of K, i.e., the smallest positive integer such that K is contained in the cyclotomic extension $\mathbb{Q}(\zeta_d)$. Since K is tame, d is also equal to the product of the primes that ramify in K. Based on this explicit description of the trace form over O_K, in [19] the authors have constructed families of well-rounded lattices that are sublattices of O_K. In [18], the notion of tame lattice is introduced by axiomatizing the key properties of the integral trace over degree p Galois extensions. For instance, notice that a and h satisfy $a - h(p-1) = 1$ and $a, h \geq 0$. In [18] these lattices are used to develop a procedure to construct well-rounded lattices, in fact strongly well rounded, for which the previous results on the Galois degree p number fields case is just a particular example. In the present paper we explore the construction of tame lattices further. For instance, one of the key elements in the construction of strongly well-rounded lattices in [18] is the construction of a family of sublattices of the form

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

for a given lattice $\mathcal{L}$; see Definition 3.3 for details. Such construction is inspired by the study of the trace form over real number fields, but its applications go beyond such fields. For instance, we show that several lattices, including A_n, D_n, E_8 and their duals, all arise as special cases of this construction. Furthermore we study the behavior of quantities such as the center density over such families, and we exhibit examples of lattices with large center density.

1.1. Organization. The rest of the paper is organized as follows. In section 2, we introduce the mathematical preliminaries needed in later sections and discuss application potential in secure wireless communications. In section 3 we study well-rounded sublattices of tame lattices. We give bounds for the center densities of such lattices and characterize them under certain conditions. In section 4 we define deformed lattices E_8^α and D_n^α, which are families of GWR lattices with density approaching the optimum as $\alpha \to 1$. In section 5, we conclude this work and give directions for future research.

2. Preliminaries. In this section we define some basic concepts that we will need later on, as well as discuss some connections to applications. Vectors will always be column vectors and will be denoted by boldface letters.

2.1. Lattices. A standard reference for the theory of lattices is the book [12].

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 $\{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m\}$ 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.

All lattices considered in this text are full rank. The nonsingular square matrix M whose columns consist of the basis vectors $\mathbf{b}_i$, $1 \le i \le n$, is called a *generator matrix* for the lattice Λ. The generator matrix is not unique: if M is a generator matrix for Λ and $U \in \mathbb{Z}^{n \times n}$ is a unimodular matrix, then $M' = MU$ is another generator matrix for Λ. We have the following two important examples of lattices frequently occurring in this article.

Example 1. The orthogonal lattice $\mathbb{Z}^n$ is a lattice with a generator matrix I_n, the identity matrix.

Example 2. The root lattice A_n is a rank n lattice in $\mathbb{R}^{n+1}$ defined by

$$A_n := \left\{ (x_1, \ldots, x_{n+1})^T \in \mathbb{Z}^{n+1} : \sum_{i=1}^{n+1} x_i = 0 \right\}.$$

Basis vectors are given by $\mathbf{v}_i = \mathbf{e}_i - \mathbf{e}_{i+1}$, for $1 \le i \le n$, where the $\mathbf{e}_i$ are standard basis vectors in $\mathbb{R}^{n+1}$. The lattice A_n can be embedded as a full rank lattice in $\mathbb{R}^n$ as follows: take the cyclic shifts of the vector $\mathbf{v}(x, y) = (x, y, y, \ldots, y) \in \mathbb{R}^n$, where $x = \frac{\sqrt{n+1}+(n-1)}{n}$ and $y = \frac{\sqrt{n+1}-1}{n}$. Then it is easy to check that the Gram matrix (defined below) of this lattice is of the form $I_n + J_n$, where I_n is the identity matrix and J_n is the matrix of all ones. This is the Gram matrix of the A_n lattice [12].

Information about the inner products between basis vectors of a lattice is encoded in the *Gram matrix,* which we define to be the symmetric and positive definite matrix

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

Since the generator matrix of a lattice is not unique, neither is the Gram matrix. Indeed, if M is a generator matrix for Λ and $M' = MU$ is another generator matrix for some unimodular U, then the corresponding Gram matrices are related by $G' = M'^T M' = (MU)^T MU = U^T G U$. It is, however, the case that $\det(G') = \det(G)$, motivating the definition of the *determinant* of a lattice, which we simply denote by $\det(\Lambda) := \det(G)$, where G is any Gram matrix of Λ. We define the *volume* (sometimes known as the *covolume*) of a lattice Λ to be the Lebesgue measure of a fundamental domain for the translation action of Λ on $\mathbb{R}^n$, or simply

$\mathrm{vol}(\Lambda) := \sqrt{\det(\Lambda)}$. For a full rank lattice this reduces to $\mathrm{vol}(\Lambda) = |\det(M)|$. If a lattice Λ has a Gram matrix G with integral entries, then the lattice is said to be *integral.*

We are interested in certain *sublattices* of tame lattices. What we mean by a sublattice of a lattice Λ is a lattice $\Lambda' \subseteq \Lambda$. If Λ' and Λ have the same rank, then we have the following formula for the index of Λ' in Λ:

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

Two lattices Λ and Λ' with generator matrices M and M', respectively, are said to be *similar,* denoted $\Lambda \sim \Lambda'$, if one is obtained from the other by a rotation and dilation: $M' = \alpha BMU$ for some $\alpha > 0$, a real orthogonal matrix B, and a unimodular matrix $U \in \mathbb{Z}^{n\times n}$. If $\alpha = 1$, we say that Λ and Λ' are *isometric* and denote it by $\Lambda \cong \Lambda'$. Hence, two lattices are similar if and only if one is obtained from the other by rotation, reflection, and scaling. The Gram matrices of similar lattices Λ and Λ', as above, are related by $G' = \alpha^2 U^T G U$. Consequently, the volumes of the lattices are related by $\mathrm{vol}(\Lambda') = \alpha^n \mathrm{vol}(\Lambda)$.

The *dual lattice* of $\Lambda \subseteq \mathbb{R}^n$ is the dual module $\mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$, which we view as a lattice in $\mathbb{R}^n$ as follows.

Definition 2.2. *Let $\Lambda \subset \mathbb{R}^n$ be a lattice. Its dual lattice Λ^* is defined as*

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

Remark 1. Given a basis $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of a lattice Λ, the dual lattice Λ^* is generated by $\{\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*\}$, where $\mathbf{b}_i^* \cdot \mathbf{b}_j = \delta_{ij}$ for all $1 \le i, j \le n$, where δ_{ij} denotes the Kronecker delta symbol. Thus, it is clear that the dual Λ^* is generated by the matrix $(M^T)^{-1}$, where M is any generator matrix for Λ. A Gram matrix for Λ^* is then given by G^{-1}, where G is any Gram matrix of Λ.

An important lattice invariant is the *shortest vector length,* or *first minimum.* Given a lattice $\Lambda \subset \mathbb{R}^n$, we define it to be the norm of the shortest nonzero lattice vector, i.e.,

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

Maximizing $\lambda_1(\Lambda)$ over the set of rank n lattices $\Lambda \subset \mathbb{R}^n$ of volume 1 is in general a hard problem: this problem is equivalent to finding the densest lattice packing of spheres, and the solution is known only in dimensions 1–8 and 24. A commonly used measure of sphere packing density of a lattice packing is the *center density,* which we define to be

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

The center density is invariant under lattice similarity. We can see from the very definition that $\delta(\Lambda) = 2^{-n}\lambda_1(\Lambda)^n$ for a volume 1 lattice Λ, showing that maximizing the center density is equivalent to maximizing the shortest vector length. We will denote by δ_n the largest known center density of a lattice in dimension n. The set $S(\Lambda) = \{\mathbf{x} \in \Lambda : \|\mathbf{x}\| = \lambda_1(\Lambda)\}$ is called the *set of minimal vectors* of Λ, and its cardinality $\kappa(\Lambda) := |S(\Lambda)|$ is called the *kissing number* of the lattice.

We will be concerned with specific types of lattices called *well-rounded* lattices.

Definition 2.3. *A lattice* $\Lambda \subset \mathbb{R}^n$
(i) *is called* well rounded *if the* $\mathbb{R}$*-span of* $S(\Lambda)$ *is* $\mathbb{R}^n$*;*
(ii) *is called* strongly well rounded *if the* $\mathbb{Z}$*-span of* $S(\Lambda)$ *is* Λ*;*
(iii) *has a* basis of minimal vectors *if there exists a set* $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\} \subseteq S(\Lambda)$ *whose* $\mathbb{Z}$*-span is* Λ*;*
(iv) *is called* generic well rounded (GWR) *if it is well rounded and has kissing number* $\kappa(\Lambda) = 2n$.

A common example of a GWR lattice is $\mathbb{Z}^n$.

The *theta series* of a lattice is defined as

$$\Theta_\Lambda(q) := \sum_{\mathbf{x}\in\Lambda} q^{\|\mathbf{x}\|^2}, \tag{2.1}$$

where $q = e^{i\pi\tau}$, and $\Im\tau > 0$. We are interested in the case $\tau = it$, i.e., when q is real. We can express the theta function equivalently as

$$\Theta_\Lambda(q) = 1 + k_1 q^{l_1^2} + k_2 q^{l_2^2} + \cdots,$$

where l_i, $i = 1, 2, \ldots$, is the length of the ith shortest vector in the lattice and $k_i := |\{\mathbf{x} \in \Lambda : \|\mathbf{x}\| = l_i\}|$. In particular, $l_1 = \lambda_1(\Lambda)$ and $k_1 = \kappa(\Lambda)$.

2.2. Secure wireless communications. In this section, we will provide a short practical motivation for the construction of generic well-rounded lattices with large packing densities. We refer the interested reader to [32, 4, 9, 13] and references therein for more details on reliable and secure wireless communications.

When communicating over a wireless channel, reliability and security of the transmission are natural concerns. Lattice codes have manifested themselves as a good design tool for this purpose. A *lattice code* is a finite collection of lattice vectors centered at the origin, often carved out by a hypersphere or a hypercube. The related design criteria may vary depending on the specific application and channel model. Over the wireless medium, the channel model can be described as

$$\mathbf{y} = H\mathbf{x} + \mathbf{n} \in \mathbb{R}^n,$$

where $\mathbf{x} \in \Lambda$ is the transmitted message, $\mathbf{n} \in \mathbb{R}^n$ is additive white Gaussian noise (AWGN), $H \in \mathbb{R}^{n\times n}$ is random fading following a certain (real, continuous) distribution, and $\mathbf{y}$ is the received distorted message. In the case of no fading, the channel is simply called an *AWGN channel* and $H = I_n$. Another typical model is the *Rayleigh fading channel,* which refers to the case where H is diagonal with Rayleigh distributed independent entries. Maximum-likelihood (ML) decoding with this model corresponds to (bounded distance) closest lattice point search.

If the communication channel can be expected to be of good quality, measured by *signal-to-noise ratio (SNR),* and we assume a Rayleigh fading channel, then reliability (under ML decoding) can be maximized by maximizing the *modulation diversity* L and *minimum product distance* of the lattice [32]. The former is defined as

$$L := \min_{0\neq\mathbf{x}\in\Lambda} |\{i : x_i \neq 0\}|,$$

the minimum number of nonzero coordinates in a nonzero lattice vector, and the latter is defined as

$$d_{p,min}(\Lambda) := \inf_{0 \neq \mathbf{x} \in \Lambda} \prod_{i=1}^{n} |x_i|$$

for a full diversity lattice with $L = n$. For a low signal quality, the minimum distance $\lambda_1(\Lambda)$ becomes crucial.

When considering security in addition to reliability, we choose a sublattice $\Lambda_s \subset \Lambda$, and the respective cosets represent our messages. In more detail, the lattice vector $\mathbf{m} \in \Lambda$ is "masked" by a randomly chosen sublattice vector r, and the message $\mathbf{x} = \mathbf{m} + \mathbf{r} \in \Lambda/\Lambda_s$ is sent through the channel. On this type of a *wiretap channel* [36, 33] we assume that the noise experienced by the eavesdropper is larger than that of the legitimate receiver. As a result, the legitimate receiver is able to decode the message with high probability, while the eavesdropper only gains negligible information. For more details on wiretap coset coding and illustrating examples, see [31].

The security of the aforementioned wiretap lattice coding can be measured by the information leaked to the eavesdropper or alternatively by the eavesdropper's correct decoding probability. Both of these measures have been shown [25, 26, 17] to be bounded from above by the *flatness factor*, which is defined by the deviation of the lattice Gaussian probability density function g_n from the uniform distribution on the Voronoi cell $\mathcal{V}(\Lambda)$. More rigorously, the flatness factor $\varepsilon_\Lambda(\sigma)$ is characterized by

$$\varepsilon_\Lambda(\sigma) := \max_{\mathbf{u} \in \mathbb{R}^n} \left| \frac{g_n(\Lambda + \mathbf{u}; \sigma)}{1/\operatorname{vol}(\Lambda)} - 1 \right|, \tag{2.2}$$

where we can maximize over $\mathbb{R}^n$ by periodicity. One can think of this as the measure of "how much better" an eavesdropper can do than just random guessing when trying to intercept (decode) the sent message. The "flatter" the channel, the closer it is to a uniform observation from the eavesdropper's perspective. Therefore, a reasonable design goal is to minimize the flatness factor. We have the following useful equalities:

$$\varepsilon_\Lambda(\sigma) = \operatorname{vol}(\Lambda) g_n(\Lambda; \sigma) - 1 = \frac{\operatorname{vol}(\Lambda)}{(\sqrt{2\pi}\sigma)^n} \Theta_\Lambda\left(e^{-1/2\sigma^2}\right) - 1 = \Theta_{\Lambda^*}\left(e^{-2\pi\sigma^2}\right) - 1. \tag{2.3}$$

Here, $\sigma^2 = \frac{1}{2\pi t}$ is the variance of the Gaussian distribution related to the channel noise.

It was proved in [17] that the minimizer of the flatness factor is a well-rounded lattice. Now, the benefit from well-rounded lattices is now manifold: they contain the maximizers of the minimum product distance, the densest lattice sphere packings, as well as the global minimizers of the flatness factor, which is closely related to the theta series as shown by (2.3). For more details, see [17, sect. VI], [34, 14, 20]. Hence, well-rounded lattices make an excellent candidate space for reliable and secure wireless communications.

As we mentioned, the minimization of the theta function is in general a very hard problem. Hence, we can aim at studying its truncations. The longer the shortest vector and the smaller the kissing number, the smaller the dominating term in the theta series becomes (see section 4 for more details). From this, the question of how to construct GWR lattices with good packing densities has a clear practical motivation and acts as the driving force for the findings of this paper.

3. Tame lattices. In this section, we define the concept of a *tame lattice,* which was introduced in [18], and expand on the results in [18] concerning well-rounded sublattices of tame lattices. We give conditions under which well-rounded sublattices of tame lattices are generic, and develop bounds for the center densities of said sublattices. We end up with two conditions which tell when a sublattice is similar to either $\mathbb{Z}^n$ or A_n. We also give an explicit construction of A_n as a sublattice of a tame lattice, and further show that the dual lattice of a tame lattice is tame.

The term *Lagrangian basis* was used by Conner and Perlis [11, p. 193] to describe a normal integral basis of a Galois, tame number field of odd prime degree, such that the Gram matrix of the lattice obtained from this basis via the Minkowski embedding has a certain form. Later, it has been proven that such bases exist in a larger set of number fields. Particularly, when the number field is tame and has a prime conductor, such a basis has been shown to exist [7]. The following definition is given in [18].

Definition 3.1. *Let $n \geq 1$ be an integer and $\mathcal{L} \subset \mathbb{R}^n$ a lattice. We call the lattice $\mathcal{L}$ tame if there exists a basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ of $\mathcal{L}$ and a nonzero 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 a tame lattice with respect to the basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$:

$$G = \begin{bmatrix} a & -h & \ldots & -h \\ -h & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & -h \\ -h & \ldots & -h & a \end{bmatrix}. \tag{3.1}$$

Moreover, the conditions imply that $a - h(n-1) = 1$. Conversely, a basis with a Gram matrix of the form (3.1) such that $a - h(n-1) = 1$ holds is Lagrangian. We can express the volume of a tame lattice using (3.1).

Lemma 3.2. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a tame lattice with a Lagrangian basis $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, $a := \langle \mathbf{e}_1, \mathbf{e}_1 \rangle$, and $h := -\langle \mathbf{e}_1, \mathbf{e}_2 \rangle$. Then*

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

Proof. Consider the matrix $M_n(x,y) = xI_n + yJ_n$, where $x, y \in \mathbb{R}$ and J_n is the matrix of all ones. If $\mathbf{v} \in \mathbb{R}^n \setminus \{0\}$ is an eigenvector for $M_n(x,y)$ with eigenvalue λ, then $M_n(x,y)\mathbf{v} = x\mathbf{v} + y\langle \mathbf{v}, \mathbf{u} \rangle \mathbf{u} = \lambda \mathbf{v}$, where $\mathbf{u}$ is the vector of all ones in the standard basis. This shows that either $\langle \mathbf{v}, \mathbf{u} \rangle = 0$ and $\lambda = x$ is an eigenvalue with multiplicity $n-1$ or $\mathbf{v}$ is parallel to $\mathbf{u}$ and $\lambda = x + yn$ is an eigenvalue with multiplicity one. Therefore, the determinant equals $\det(M_n(x,y)) = (x+yn)x^{n-1}$. If we plug in $x = a+h$ and $y = -h$, we obtain the determinant

of (3.1) as

$$\det(G) = (a+h)^{n-1}(a+h(1-n)).$$

Since $a+h(1-n)=1$,

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

as desired. ∎

Remark 2. If $\mathcal{L} \subset \mathbb{R}^n$ is a tame lattice with a Gram matrix G, then since G is a positive definite matrix, we have $\det(G) = (a+h)^{n-1} > 0$ and, in particular, the inequality $a+h>0$ and equation $a+h(1-n)=1$ imply $a > \frac{1}{n}$ and $h > -\frac{1}{n}$.

3.1. Well-rounded sublattices. In this section, we present some of the definitions and results in [18], since our goal is to expand on these results. We recall how one can produce full-rank sublattices, and particularly tame lattices, via a specific linear map. We also restate the main theorem presented in [18].

Remark 3. The motivation behind the following definition of $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1} := \Phi_{(r,s)}(\mathcal{L})$ comes from number theory. Let p be an odd prime and let K be a Galois degree p number field, where p is unramified. For an integer $m \equiv 1 \pmod{p}$ it turns out the ring of integers O_K, seen as a lattice via the Minkowski embedding, contains a sublattice O_m that has a minimal basis. Such a sublattice is a particular instance of $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$; in this case $\mathcal{L}$ is O_K, $\mathbf{v}_1 = 1$, T is the trace map, $r=1$, and $s = \frac{m-1}{p}$. For details, see section 1.1 and Lemma 3.8 in [18].

Definition 3.3. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice and $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$ a nontrivial linear map. Let r, s be integers, and let $\mathbf{v}_1 \in \mathcal{L} \setminus \ker \mathrm{T}$ 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 $\Phi_{(r,s)}$:

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

Remark 4. It is clear that $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$ is a sublattice of $\mathcal{L}$. Further, if r and m are nonzero, then $\Phi_{(r,s)}$ turns out to be an injection. This can be achieved, for instance, when $0 < |r| < |\,\mathrm{T}(\mathbf{v}_1)|$, whence we get the following result (Corollary 3.2 in [18]).

Lemma 3.4. *Assume that $\mathcal{L}$, T and $\mathbf{v}_1$ are as in Definition 3.3 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 $\mathcal{L}$.*

If the conditions in the above lemma are satisfied and if $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ is a basis for $\mathcal{L}$, then $\{\Phi_{(r,s)}(\mathbf{e}_1), \dots, \Phi_{(r,s)}(\mathbf{e}_n)\}$ 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

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

In [18], the authors give a condition which tells when $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is well rounded and, in fact, possesses a minimal basis. If the condition is met, then the index $[\mathcal{L}_{\mathbf{v}_1}^{(r,s)} : \mathcal{L}]$ and the lattice minimum of $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ are given. We state this more specifically in the following theorem.

Theorem 3.5 (see [18, Thm. 4.9]). *Let $n \geq 2$ be an integer and $\mathcal{L} \subset \mathbb{R}^n$ a tame 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*

$$\frac{na-1}{n^2-1} \leq \left(\frac{m}{r}\right)^2 \leq \frac{(na-1)(n+1)}{n-1}. \tag{3.2}$$

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

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

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

In fact a stronger result is true: if the upper bound in (3.2) is strict, then $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is GWR. Namely, in this case, [18, Cor. 4.8] shows that the vectors $\Phi_{(r,s)}(\mathbf{e}_i)$ have strictly smaller length than the vectors coming from the sublattice $\mathcal{L}^0$ of vectors of trace zero (since the upper bound is equivalent to $Aa+B \leq 2A(a+h)$). Moreover, [18, Prop. 4.7] shows that the vectors $\Phi_{(r,s)}(\mathbf{e}_i)$ also have smaller length than the vectors $\Phi_{(r,s)}(\mathbf{v})$, where $\mathbf{v} \in S_d = \{\mathbf{x} \in \mathcal{L} : T(\mathbf{x}) = d,\ d \neq 0\}$.

Theorem 3.6. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a tame 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.

An interesting observation is that when the upper bound in (3.2) is achieved, then $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ has the same kissing number as A_n, which is $n(n+1)$. In particular, $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is no longer GWR. Later (in Theorem 3.10) we will show that $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is actually similar to A_n in this case.

3.2. Center densities of sublattices of tame lattices. Our goal in this section is to characterize the center densities of the lattices $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ in Definition 3.3 and develop bounds for them. The following proposition gives an explicit formula for the center density.

Proposition 3.7. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a tame 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 3.2 and Theorem 3.5,

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

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

$$\begin{aligned}\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) &= \frac{\lambda_1^2(\mathcal{L}_{\mathbf{v}_1}^{(r,s)})^{n/2}}{2^n \,\mathrm{vol}(\mathcal{L}_{\mathbf{v}_1}^{(r,s)})} \\ &= \frac{\left(ar^2 + \frac{m^2-r^2}{n}\right)^{n/2}}{2^n(a+h)^{\frac{n-1}{2}}|mr^{n-1}|} \\ &= \frac{((na-1)r^2+m^2)^{n/2}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}|mr^{n-1}|},\end{aligned}$$

as desired. ∎

The following lemma will turn out to be useful when we maximize and minimize the expression for the center density derived in the previous proposition.

Lemma 3.8. *Let* $n \geq 2$ *be an integer and let* $a > \frac{1}{n}$. *Define*

$$\begin{aligned} l &:= \frac{na-1}{n^2-1}, \\ u &:= \frac{(na-1)(n+1)}{n-1}. \end{aligned}$$

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. ∎

We now have the ingredients to find bounds for $\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)})$.

Proposition 3.9. *Let $n\geq 2$ be an integer and let $\mathcal{L}\subset\mathbb{R}^n$ be a tame lattice with a Lagrangian basis $\{\mathbf{e}_1,\dots,\mathbf{e}_n\}$. 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 3.7 gives the center density of $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ as

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

The condition for $q := (m/r)^2$ is satisfied when $q \in [l,u]$, where l and u are defined as in Lemma 3.8. Note that we have

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

where $f : [l,u] \to \mathbb{R}$ is the function defined in Lemma 3.8. It follows from the previous lemma, where $x_0 = \frac{na-1}{n-1}$, that

$$\begin{aligned}\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) &\geq \frac{\sqrt{f(x_0)}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}} \\ &= \frac{\sqrt{f(x_0)}}{2^n n^{n/2}\left(a+\frac{a-1}{n-1}\right)^{\frac{n-1}{2}}} \\ &= \frac{n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}}{2^n n^{n/2}\left(a+\frac{a-1}{n-1}\right)^{\frac{n-1}{2}}} \\ &= \frac{n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}}{2^n n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}} \\ &= \frac{1}{2^n}\end{aligned}$$

and

$$\begin{aligned}\delta(\mathcal{L}_{\mathbf{v}_1}^{(r,s)}) &\leq \frac{\sqrt{f(u)}}{2^n n^{n/2}(a+h)^{\frac{n-1}{2}}} \\ &= \frac{\sqrt{f(u)}}{2^n n^{n/2}\left(a+\frac{a-1}{n-1}\right)^{\frac{n-1}{2}}} \\ &= \frac{2^{n/2}n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}(n+1)^{-1/2}}{2^n n^{n/2}(na-1)^{\frac{n-1}{2}}(n-1)^{\frac{1-n}{2}}} \\ &= \frac{1}{2^{n/2}\sqrt{n+1}},\end{aligned}$$

proving the claim. ∎

Remark 5. Since $\delta(A_n) = \frac{1}{2^{n/2}\sqrt{n+1}}$ and $\delta(\mathbb{Z}^n) = 2^{-n}$, the previous proposition says that

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

Note that under the assumptions made in Theorem 3.5, the family of lattices $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ do not have asymptotically good packing density. In section 3.5, we will see that under more general assumptions denser packings can be obtained from simple tame lattices. To complete our analysis, we give a characterization of $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ when the bounds of the previous proposition are achieved.

Theorem 3.10. *Let $n \ge 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a tame lattice with a Lagrangian basis $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$. 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 $0 \ne |r| < n$ and let $m = r + sn$.*

(a) *If*

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

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

(b) *If*

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

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

Proof. Theorem 3.5 gives a basis of minimal vectors

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

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 $1 \le i \le n$;
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 $1 \le i \ne j \le n$.

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

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

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

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

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

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

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

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

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). ∎

3.3. Construction of A_n. We know that a lattice of the form $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is similar to A_n if condition (b) in Theorem 3.10 holds. But the question remains, for which values of the parameter a for the tame 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 tame lattice with $a=n$, then we can always find pairs (r,s) such that $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is similar to A_n. Propositions 3.11 and 3.12 show how one can construct a lattice similar 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 tame lattice for a general n.

Proposition 3.11. *Suppose that $n+1=d^2$ for some integer $d>2$. Let $\mathcal{L}=\mathbb{Z}^n$ be the tame lattice with $(a,h)=(1,0)$ and a Lagrangian basis $\{\mathbf{e}_1,\dots,\mathbf{e}_n\}$, where the $\mathbf{e}_i$ 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 3.10, part (b),

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

∎

Proposition 3.12. *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 $\mathbf{e}'_i = (\frac{1-\sqrt{n+1}}{n})\mathbf{v}_1 + \sqrt{n+1}\mathbf{e}_i$ 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 tame 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. $\sum_{i=1}^n \mathbf{e}'_i = n(\frac{1-\sqrt{n+1}}{n})\mathbf{v}_1 + \sqrt{n+1}\mathbf{v}_1 = \mathbf{v}_1$.
2. $\langle \mathbf{e}'_i, \mathbf{v}_1 \rangle = n(\frac{1-\sqrt{n+1}}{n}) + \sqrt{n+1} = 1$ for all $1 \leq i \leq n$.
3. $a = \langle \mathbf{e}'_i, \mathbf{e}'_i \rangle = (n-1)(\frac{1-\sqrt{n+1}}{n})^2 + (\frac{1-\sqrt{n+1}}{n} + \sqrt{n+1})^2 = n$ for all $1 \leq i \leq n$.
4. $-h = \left\langle \mathbf{e}'_i, \mathbf{e}'_j \right\rangle = (n-2)(\frac{1-\sqrt{n+1}}{n})^2 + 2(\frac{1-\sqrt{n+1}}{n})(\frac{1-\sqrt{n+1}}{n} + \sqrt{n+1}) = -1$ for all $1 \leq i \neq j \leq n$.

The conditions are satisfied, so $\mathcal{L}$ is tame 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 3.10, 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. ∎

3.4. Dual lattices. In this section we show that the dual of a lattice of the form $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is a scaled version of $\mathcal{L}$ (Proposition 3.13), and that the dual of a tame lattice is also tame (Lemma 3.14). The most general result is Theorem 3.15, which says that lattices of the form $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$, with some conditions on the parameters r, s, are closed, modulo scaling, under duality.

Proposition 3.13. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a tame 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 $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = -h$ otherwise. The assumption $s = rh$ and $c \neq 0$ give us 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 $M^T M' = I_n$. Therefore, $\mathcal{L}_{\mathbf{v}_1}^{(r,s)}$ is the dual lattice of $\frac{1}{r(a+h)}\mathcal{L}$ by Remark 1. ∎

Lemma 3.14. *Let $n \geq 2$ be an integer and let $\mathcal{L} \subset \mathbb{R}^n$ be a tame 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 tame 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 tame 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 2. If we can show that $\mathcal{L}^*$ has a Gram matrix $\tilde{G}$ of the form

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

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

$$\begin{aligned} \langle \mathbf{b}_i, \mathbf{d}_i \rangle &= (-h, \ldots, a, \ldots, -h)^T (-\tilde{h}, \ldots, \tilde{a}, \ldots, -\tilde{h}) \\ &= (n-1)h\tilde{h} + a\tilde{a} \\ &= (n-1)h\tilde{h} + a(1 + (n-1)\tilde{h}) \\ &= a + (n-1)\tilde{h}(a+h) \\ &= a + (n-1)\left(\frac{-h}{a+h}\right)(a+h) \\ &= a - h(n-1) = 1. \end{aligned}$$

For $i \neq j$, we have

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

This shows that G and $\tilde{G}$ are related by $G\tilde{G} = I_n$, so $\tilde{G}$ must be a Gram matrix for the dual lattice $\mathcal{L}^*$ by Remark 1. ∎

More generally in the next theorem we give conditions under which the family of lattices of the form $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$ is closed, modulo scaling, under duality. Before doing so we recall the notion of dual map. Given two lattices Λ_1 and Λ_2, and a linear map between them, $\phi : \Lambda_1 \to \Lambda_2$, there exists a unique linear map $\phi^* : \Lambda_2^* \to \Lambda_1^*$ that is completely characterized by the following adjoint property: for every $l_1 \in \Lambda_1$ and $l_2^* \in \Lambda_2^*$ we have that

$$\langle \phi^*(l_2^*), l_1 \rangle_1 = \langle l_2^*, \phi(l_1) \rangle_2,$$

where $\langle\ ,\ \rangle_i$ denotes the inner product in the vector space $\Lambda_i \otimes \mathbb{R}$. If we pick bases for Λ_i, together with their respective dual basis, we can identify $\mathrm{Hom}(\Lambda_1, \Lambda_2)$ with $\mathrm{M}_{m,n}(\mathbb{Z})$. Under this choice of coordinates the map

$$\begin{aligned} \mathrm{Hom}(\Lambda_1, \Lambda_2) &\to \mathrm{Hom}(\Lambda_2^*, \Lambda_1^*) \\ \phi &\mapsto \phi^* \end{aligned}$$

is just transposition,

$$\begin{aligned} \mathrm{M}_{m,n}(\mathbb{Z}) &\to \mathrm{M}_{n,m}(\mathbb{Z}) \\ A &\mapsto A^T. \end{aligned}$$

Observe that in particular we have that the map $\phi \mapsto \phi^*$ is linear and that $(\phi \circ \psi)^* = \psi^* \circ \phi^*$.

Theorem 3.15. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a tame lattice, and let $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$ be a nontrivial linear map such that $\mathbf{v}_1 \in \mathcal{L} \setminus \ker \mathrm{T}$. Let r, s be integers such that $r \neq 0$ and $m := r + s\,\mathrm{T}(\mathbf{v}_1) \neq 0$. Suppose that $r + m = 0$. Then the dual lattice of $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$ is, up to scaling, of the same type. More explicitly, there exists a rank n tame lattice $\mathcal{L}_1$, a nontrivial linear map $\widetilde{\mathrm{T}} : \mathcal{L}_1 \to \mathbb{Z}$, and $\widetilde{\mathbf{v}}_1 \in \mathcal{L}_1 \setminus \ker \widetilde{\mathrm{T}}$, with $r + s\widetilde{\mathrm{T}}(\mathbf{v}_1) \neq 0$, such that $(\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1})^*$ is $\frac{1}{r^2}(\mathcal{L}_1)^{(r,s)}_{\widetilde{\mathrm{T}},\widetilde{\mathbf{v}}_1}$.*

Proof. By definition (see Remark 4), $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$ is the rank n lattice defined as the image of the map $\Phi_{(r,s)} : \mathcal{L} \to \mathcal{L};\ \mathbf{x} \mapsto r\phi_1(\mathbf{x}) + s\phi_2(\mathbf{x})$, where $\phi_1(\mathbf{x}) = \mathbf{x}$ and $\phi_2(\mathbf{x}) = \mathrm{T}(\mathbf{x})\mathbf{v}_1$. Since dualizing is a linear operator we see that $\Phi^*_{(r,s)} = r\phi_1^* + s\phi_2^*$. Notice that the map $\phi_2 : \mathcal{L} \to \mathcal{L};\ \phi_2(\mathbf{x}) = \mathrm{T}(\mathbf{x})\mathbf{v}_1$ can be written as the composition of the maps $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$ and $\mu_{\mathbf{v}_1} : \mathbb{Z} \to \mathcal{L};\ n \mapsto n\mathbf{v}_1$,

$$\phi_2 = \mu_{\mathbf{v}_1} \circ \mathrm{T}.$$

Hence,

$$\phi_2^* = \mathrm{T}^* \circ \mu^*_{\mathbf{v}_1}.$$

Let $\widetilde{\mathrm{T}} = \mu^*_{\mathbf{v}_1}$ and $\widetilde{\mathbf{v}}_1 := \mathrm{T}^*(1)$ (here we are using that $\mathbb{Z}^* = \mathbb{Z}$). The image of $\mathrm{T}^* : \mathbb{Z}^* \to \mathcal{L}^*$ is generated by $\widetilde{\mathbf{v}}_1$ so we can write, in a similar fashion to that above, $\mu_{\widetilde{\mathbf{v}}_1} := \mathrm{T}^*$ and obtain that

$$\phi_2^* = \mu_{\widetilde{\mathbf{v}}_1} \circ \widetilde{\mathrm{T}}.$$

It follows from this tha $\Phi^*_{(r,s)}(\mathbf{x}) = r\phi_1^*(\mathbf{x}) + s\phi_2^*(\mathbf{x}) = r\mathbf{x} + s\widetilde{\mathrm{T}}(\mathbf{x})\widetilde{\mathbf{v}}_1$. Thanks to Lemma 3.14 we have that $\mathcal{L}_1 := \mathcal{L}^*$ is a tame lattice, and since $\widetilde{\mathrm{T}}(\widetilde{\mathbf{v}}_1) = \mu^*_{\mathbf{v}_1} \circ \mathrm{T}^*(1) = (\mathrm{T} \circ \mu_{\mathbf{v}_1})^*(1) = \mathrm{T}(\mathbf{v}_1)$, we see that $r + s\widetilde{\mathrm{T}}(\widetilde{\mathbf{v}}_1) \neq 0$. In particular, $(\mathcal{L}_1)^{(r,s)}_{\widetilde{\mathrm{T}},\widetilde{\mathbf{v}}_1}$ is well-defined and it has, by definition, a $\mathbb{Z}$-basis of the form $\{\Phi^*_{(r,s)}(\mathbf{e}_1^*), \ldots, \Phi^*_{(r,s)}(\mathbf{e}_n^*)\}$, where $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{L}$. To finish the proof of the theorem we must show that $\langle \Phi_{(r,s)}(\mathbf{e}_i), \Phi^*_{(r,s)}(\mathbf{e}_j^*)\rangle = r^2\delta_{i,j}$ for some basis. Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ be a Lagrangian basis of $\mathcal{L}$ with $\mathbf{v}_1 = \mathbf{e}_1 + \cdots + \mathbf{e}_n$ and let $\{\mathbf{e}_1^*, \ldots, \mathbf{e}_n^*\}$ be its dual basis.

$$\begin{aligned}
\left\langle \Phi_{(r,s)}(\mathbf{e}_i), \Phi^*_{(r,s)}(\mathbf{e}_j^*) \right\rangle &= \left\langle r\mathbf{e}_i + s\mathbf{v}_1\,\mathrm{T}(\mathbf{e}_i), \Phi^*_{(r,s)}(\mathbf{e}_j^*) \right\rangle \\
&= r\left\langle \mathbf{e}_i, \Phi^*_{(r,s)}(\mathbf{e}_j^*) \right\rangle + s\,\mathrm{T}(\mathbf{e}_i)\left\langle \mathbf{v}_1, \Phi^*_{(r,s)}(\mathbf{e}_j^*) \right\rangle \\
&= r\left\langle \Phi_{(r,s)}(\mathbf{e}_i), \mathbf{e}_j^* \right\rangle + s\,\mathrm{T}(\mathbf{e}_i)\left\langle \Phi_{(r,s)}(\mathbf{v}_1), \mathbf{e}_j^* \right\rangle \\
&= r\left\langle \Phi_{(r,s)}(\mathbf{e}_i), \mathbf{e}_j^* \right\rangle + s\,\mathrm{T}(\mathbf{e}_i)\sum_{k=1}^{n}\left\langle \Phi_{(r,s)}(\mathbf{e}_k), \mathbf{e}_j^* \right\rangle \\
&= r\left\langle r\mathbf{e}_i + s\mathbf{v}_1\,\mathrm{T}(\mathbf{e}_i), \mathbf{e}_j^* \right\rangle + s\,\mathrm{T}(\mathbf{e}_i)\sum_{k=1}^{n}\left\langle \Phi_{(r,s)}(\mathbf{e}_k), \mathbf{e}_j^* \right\rangle \\
&= r\left\langle r\mathbf{e}_i + s\mathbf{v}_1\,\mathrm{T}(\mathbf{e}_i), \mathbf{e}_j^* \right\rangle + s\,\mathrm{T}(\mathbf{e}_i)\sum_{k=1}^{n}\left\langle r\mathbf{e}_k + s\mathbf{v}_1\,\mathrm{T}(\mathbf{e}_k), \mathbf{e}_j^* \right\rangle \\
&= r^2\delta_{i,j} + rs\,\mathrm{T}(\mathbf{e}_i) + s\,\mathrm{T}(\mathbf{e}_i)\left(r + s\sum_{k=1}^{n}\mathrm{T}(\mathbf{e}_k)\right) \\
&= r^2\delta_{i,j} + rs\,\mathrm{T}(\mathbf{e}_i) + s\,\mathrm{T}(\mathbf{e}_i)\,(r + s\,\mathrm{T}(\mathbf{v}_1)) \\
&= r^2\delta_{i,j} + rs\,\mathrm{T}(\mathbf{e}_i) + s\,\mathrm{T}(\mathbf{e}_i)m = r^2\delta_{i,j} + s\,\mathrm{T}(\mathbf{e}_i)(r+m) = r^2\delta_{i,j}.
\end{aligned}$$

■

3.5. Construction of some lattices with high center density. We have seen that under the assumptions made in Theorem 3.5, a well-rounded lattice of the form $\mathcal{L}^{(r,s)}_{\mathbf{v}_1}$ has center density less than or equal to the center 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 get lattices with higher center density. Indeed, in [18, Exam. 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 $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$. The purpose of this section is to show how one can construct the densest known lattices in dimensions 8 and 9 as lattices $\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}$, when $\mathcal{L}$ is the tame lattice $\mathbb{Z}^n$. This shows that there are many different types of lattices that can be obtained from a tame lattice $\mathcal{L}$, using the linear map $\Phi_{(r,s)}$.

3.5.1. The E_8 lattice. The E_8 lattice is the densest lattice packing in dimension 8. There are two equivalent versions of the lattice: the even (Γ_8) and odd (Γ_8') coordinate system version. Let us state the definitions of both.

Definition 3.16. *Define*

$$\Gamma_8 := \left\{ \mathbf{x} \in \mathbb{Z}^8 \cup \left(\mathbb{Z} + \frac{1}{2}\right)^8 : \sum_{i=1}^{8} x_i \in 2\mathbb{Z} \right\}, \tag{3.3}$$

$$\Gamma_8' := \left\{ \mathbf{x} \in \mathbb{Z}^8 : \sum_{i=1}^{8} x_i \in 2\mathbb{Z} \right\} \cup \left\{ \mathbf{x} \in \left(\mathbb{Z} + \frac{1}{2}\right)^8 : \sum_{i=1}^{8} x_i \in 2\mathbb{Z} + 1 \right\}. \tag{3.4}$$

Proposition 3.17 gives the index of $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$ in $\mathcal{L}$; this result will become useful in Lemma 3.18.

Proposition 3.17. *Let $\mathcal{L} \subset \mathbb{R}^n$ be a lattice, $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$ a nontrivial 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 [18, Prop. 3.7], so let us prove that such a basis always exists. Since $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$ is nontrivial there is $\mathbf{v} \in \mathcal{L}$ such that $\mathrm{Im}(\mathrm{T})$ is generated by $\mathrm{T}(\mathbf{v})$; moreover, by the additivity of the rank $\ker \mathrm{T}$ is a sublattice of $\mathcal{L}$ of rank $n-1$. Let $\{\mathbf{w}_1, \ldots, \mathbf{w}_{n-1}\}$ be a basis for $\ker \mathrm{T}$. Notice that $\{\mathbf{w}_1, \ldots, \mathbf{w}_{n-1}, \mathbf{v}\}$ is a basis for $\mathcal{L}$. Thus, $\{\mathbf{w}_1 + \mathbf{v}, \ldots, \mathbf{w}_{n-1} + \mathbf{v}, \mathbf{v}\}$ is a basis for $\mathcal{L}$ and it is rigid with respect to T since T takes the value of $\mathrm{T}(\mathbf{v})$ at every element in the set. ∎

Lemma 3.18. *Let $\mathcal{L} = \mathbb{Z}^8$ and $\mathbf{c} = (1, -1, 1, -1, 1, -1, 1, -1)$ in the standard basis. Define the linear map $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$, $\mathrm{T}(\mathbf{x}) = \langle \mathbf{c}, \mathbf{x} \rangle$. Let $\mathbf{v}_1 = (-1, 1, -1, 1, 1, 1, 1, 1) \in \mathcal{L} \setminus \ker \mathrm{T}$ in the standard basis, 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 3.4 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 3.17, 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 $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)} = 2\Gamma_8'$. ∎

3.5.2. Densest known lattice packing in dimension 9. The largest known center density of a lattice packing in dimension 9 is $\delta_9 = \frac{1}{16\sqrt{2}}$, achieved by the laminated lattice Λ_9 [30]. Here we show how we can construct a lattice $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$ with this center density.

Lemma 3.19. *Let $\mathcal{L} = \mathbb{Z}^9$ and $\mathbf{c} = (1,-1,1,-1,1,-1,1,-1,1)$ in the standard basis. Define the linear map $\mathrm{T} : \mathcal{L} \to \mathbb{Z}$, $\mathrm{T}(\mathbf{x}) = \mathbf{c}^T\mathbf{x}$. Let*

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

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

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

Thus, a generator matrix for $\mathcal{L}_{\mathrm{T},\mathbf{v}_1}^{(r,s)}$ 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 $i \in \{1,\dots,8\}$, 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 $\lambda_1(\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}) = \sqrt{2^2+2^2} = \sqrt{8}$ and $\mathrm{vol}(\mathcal{L}^{(r,s)}_{\mathrm{T},\mathbf{v}_1}) = 2^9$. Therefore,

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

4. Generic well-rounded lattices. In the previous section we saw how to construct GWR sublattices of tame lattices with center density ranging from $\delta(\mathbb{Z}^n)$ to $\delta(A_n)$, so maximally dense lattice packings in dimensions 1–3. We proceed to construct GWR lattices which have a good packing density in higher dimensions. We deform basis vectors of the densest lattice packing in dimensions 3–5, D_n, and in dimension 8, E_8, to obtain lattices with good sphere packing density and minimal kissing number in these dimensions. We call these constructions D_n^α and E_8^α, where α is a parameter describing how much the basis vectors are distorted. We also investigate when it is possible to scale these deformed lattices to embed them as sublattices of $\mathbb{Z}^n$.

As mentioned earlier, one motivation for finding GWR lattices with high sphere packing density has to do with the theta series of a lattice (cf. (2.1)). Now if we approximate the series with

$$\Theta_\Lambda\left(q := e^{-\frac{1}{2\sigma^2}}\right) \approx 1 + k_1 q^{l_1^2} = 1 + \kappa(\Lambda) e^{-\frac{\lambda_1(\Lambda)^2}{2\sigma^2}},$$

we see that the kissing number and shortest vector length of a lattice play important roles in the theta series.

The minimization of the theta series for specific ranges for q is interesting in itself, but this problem has also real-life applications in contexts such as wireless communications (cf. section 2.2). The minimization of the theta series also has applications in physics, e.g., finding optimal arrangements of particles interacting under Gaussian potentials [6].

Densest lattice packings have a large kissing number in all dimensions for which the densest packings are known. Thus, a natural direction is to consider lattices with minimal kissing number but for which λ_1 is close to the maximum in that dimension. This is the motivation behind the deformed lattices. As we will see, however, this does not mean that the theta function of the deformed lattice will be smaller than those for the nondeformed lattices D_n and E_8. Indeed, it has been recently shown in [10] that in dimensions 8 and 24, minimizers

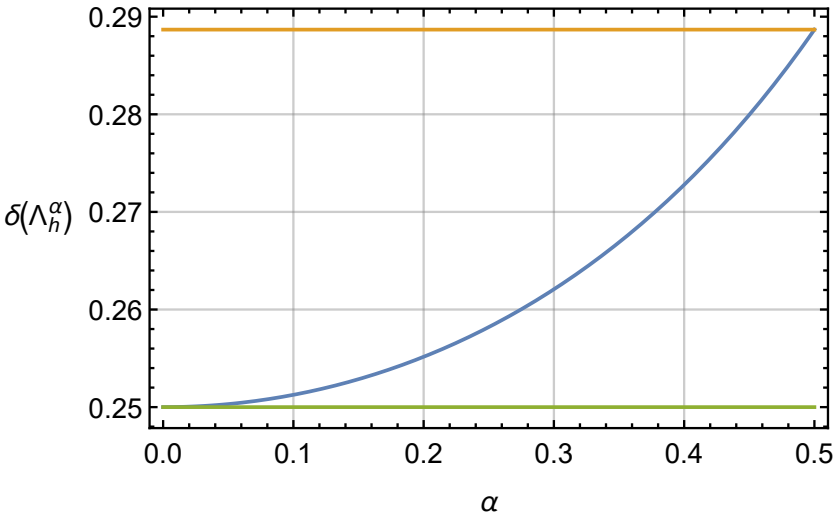

Figure 4.1. *Center density of the deformed hexagonal lattice Λ_h^α as a function of α. The bottom line shows $\delta(\mathbb{Z}^2)$ and the upper line $\delta(\Lambda_h)$.*

of the theta series in these dimensions are the E_8 and Leech lattice, respectively. Nevertheless, the construction of GWR lattices with arbitrary good packing density is something that, as far as we are aware, has not been done before. Further, such constructions provide good candidates for secure lattice codes according to [17] (see also the discussion in section 5).

4.1. The planar case. To highlight the idea behind the deformed lattices, we illustrate how the densest lattice packing in dimension 2, the hexagonal lattice $\Lambda_h \sim A_2$, can be deformed to produce GWR lattices with density as close as desired to the optimal density in dimension 2. In fact, we end up with a parametrization of representatives of equivalence classes of planar well-rounded lattices.

Definition 4.1. *Let $0 \le \alpha \le \frac{1}{2}$ 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 follows from the definition that $\Lambda_h^{\frac{1}{2}} = \Lambda_h$, the hexagonal lattice, and $\Lambda_h^0 = \mathbb{Z}^2$, the orthogonal lattice. For other values of α, Λ_h^α is a planar GWR lattice. The volume of Λ_h^α is given by $\mathrm{vol}(\Lambda_h^\alpha) = |\det(M_{\Lambda_h^\alpha})| = \overline{\alpha}$, and the center density is given by $\delta(\Lambda_h^\alpha) = \frac{\lambda_1(\Lambda_h^\alpha)^2}{2^2\,\mathrm{vol}(\Lambda_h^\alpha)} = \frac{1}{4\overline{\alpha}}$. In particular, $\alpha \mapsto \delta(\Lambda_h^\alpha)$ is an increasing function on $\left[0, \frac{1}{2}\right]$, as can be seen from Figure 4.1.

4.2. Deformed D_n. The checkerboard lattice, which is defined as

$$D_n := \left\{ (x_1, \ldots, x_n)^T \in \mathbb{Z}^n : \sum_{i=1}^n x_i \equiv 0 \pmod 2 \right\},$$

is a root lattice and the densest lattice packing in dimensions 3–5. D_3 is also known as the face-centered cubic lattice. It is easy to see that D_n has kissing number $2n(n-1)$; indeed, the shortest vectors are given by permutations of $(\pm 1, \pm 1, 0, \dots, 0)$.

Using the same strategy as with the hexagonal lattice, we distort the basis vectors of D_n to produce a family of GWR lattices $\{D_n^\alpha\}$, where $\alpha \in (1, \sqrt{2}]$, such that $\delta(D_n^\alpha) \to \delta(D_n)$ as $\alpha \to 1$.

Definition 4.2. *Let $1 \le \alpha \le \sqrt{2}$ and $\overline{\alpha} := \sqrt{2-\alpha^2}$. We define D_n^α, $n \ge 3$, 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 $0 \le \overline{\alpha} \le 1$ when $1 \le \alpha \le \sqrt{2}$ and $\alpha^2 + \overline{\alpha}^2 = 2$. Further, $D_n^1 = D_n$ (motivating the notation) and $D_n^{\sqrt{2}} = \sqrt{2}\mathbb{Z}^n$. For any $\alpha \in (1, \sqrt{2}]$ we get a GWR lattice D_n^α (Theorem 4.4) and further, $\alpha \mapsto \delta(D_n^\alpha)$ is strictly decreasing on $[1, \sqrt{2}]$ (Proposition 4.7). We start by deriving an expression for the volume of D_n^α.

Proposition 4.3. *The volume of D_n^α is given by*

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

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 $\operatorname{vol}(D_n^\alpha) = |\det(M_{D_n^\alpha})|$. ∎

Theorem 4.4. *Let $1 < \alpha \le \sqrt{2}$. Then D_n^α has the set of minimal vectors $S(D_n^\alpha) = \{\pm \mathbf{b}_1, \dots, \pm \mathbf{b}_n\}$ where $\mathbf{b}_i$ is the ith column of $M_{D_n^\alpha}$. In particular, D_n^α is GWR and $\lambda_1^2(D_n^\alpha) = 2$.*

Proof. See the appendix A.1. ∎

Knowing the volume and shortest vector length of D_n^α, we are able to compute its center density.

Corollary 4.5. *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 4.4, $\lambda_1^2(D_n^\alpha) = 2$. Thus, using Proposition 4.3,

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

■

Next we will show that the center density $\delta(D_n^\alpha)$ is a strictly decreasing function on $[1, \sqrt{2}]$. This implies that no two lattices in the family $\{D_n^\alpha\}$ are similar. Lemma 4.6 will be used to prove this fact.

Lemma 4.6. *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 $x \in (1, \sqrt{2})$. ■

Proposition 4.7. *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 4.6. 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,

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

■

4.2.1. Integral deformed D_n. From a computational perspective, the lattices D_n^α 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, in the context of lattice coset coding, one often looks for GWR lattices which are sublattices of the orthogonal lattice $\mathbb{Z}^n$. Since scaling does not change the center density of a lattice, and GWR lattices are closed under scaling, the aforementioned considerations motivate finding lattices $cD_n^\alpha \subseteq \mathbb{Z}^n$, where c is a constant.

One way to obtain a lattice $cD_n^\alpha \subseteq \mathbb{Z}^n$ is to ensure that $\alpha, \overline{\alpha} \in \mathbb{Q}$ and then scale 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 exist 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 4.1 shows some pairs of integers (p, q), and corresponding

Table 4.1

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	$\frac{2^{-\frac{n}{2}-6}\cdot 481^n\cdot 511^{3-n}}{3499245}$	$4\cdot\left(\frac{2^{-\frac{n}{2}-6}\cdot 481^n\cdot 511^{3-n}}{3499245}\right)^{\frac{2}{n}}$

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.

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

Example 3. 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 4.1. 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 4.5 (or from Table 4.1),

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

4.3. Deformed E_8. Recall the definition of the E_8 lattice (Definition 3.16), the densest lattice packing in dimension 8, with a center density of 0.0625. Our goal in this section is to deform the basis vectors of the lattice Γ_8' (the odd coordinate system version of E_8) in the

same way that we did with the D_n lattice, to obtain GWR lattices with good packing density in dimension 8.

Definition 4.8. *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 4.9. *The volume of E_8^α is given by*

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

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 $\operatorname{vol}(E_8^\alpha) = |\det(M_{E_8}^\alpha)|$. ∎

The following theorem states that E_8^α is GWR for all $1 < \alpha \le \sqrt{2}$. This means that, in particular, $\{E_8^\alpha\}$ is a family of GWR lattices with center density approaching $\delta_8 = 0.0625$ as $\alpha \to 1$.

Theorem 4.10. *Let $1 < \alpha \le \sqrt{2}$. Then E_8^α has the set of minimal vectors $S(E_8^\alpha) = \{\pm\mathbf{b}_1, \dots, \pm\mathbf{b}_8\}$, where $\mathbf{b}_i$ is the ith column of $M_{E_8^\alpha}$. In particular, E_8^α is GWR and $\lambda_1^2(E_8^\alpha) = 2$.*

Proof. The proof is similar to the proof of Theorem 4.4 (see the appendix A.1), but even longer and relies on a computer program, so we simply omit it here. ∎

We can now compute the center density of the lattice E_8^α.

Proposition 4.11. *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 4.9 and Theorem 4.10,

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

∎

Table 4.2

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

4.3.1. 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 4.2 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 $2q{E_8}^\alpha \subseteq \mathbb{Z}^n$. As the table indicates, if we desire a high center density, we have to accept large values for q.

5. Conclusions and future work. Motivated by the attempt to construct lattices suitable for lattice coset codes for the fading wiretap channel as well as by the mathematical question itself, we have in this paper explored different constructions of generic well-rounded lattices: sublattices of tame lattices and deformed dense lattices. The task of finding GWR lattices with good sphere packing density was motivated by the findings in, e.g., [15, 23, 24, 17], where it was demonstrated, using fading wiretap channel simulations, that having a small kissing number and a high packing density for the eavesdropper's lattice can lower the correct decoding probability of the eavesdropper.

Furthermore, as discussed in section 2.2, when the communication channel is of good quality, the performance of a lattice code is dictated by its diversity and minimum product distance, which both should be maximized. The deformed lattices D_n^α and E_8^α defined in this

paper are clearly not full diversity. However, a natural way to obtain full diversity variants of the integral deformed lattices discussed in sections 4.2.1 and 4.3.1 is to apply orthogonal transformations which maximize modulation diversity and minimum product distance for the lattice $\mathbb{Z}^n$. Then, since the integral deformed lattices are sublattices of $\mathbb{Z}^n$, if we apply the same orthogonal transformation, the obtained lattices must also have full diversity and minimum product distance lower bounded by the minimum product distance of the optimally rotated $\mathbb{Z}^n$ lattice. For some currently best known rotations, maximizing the minimum product distance of $\mathbb{Z}^n$, see [35]. Let us also note that in scenarios where the channel quality is constantly low (e.g., due to long communication distance, high speed, physical obstacles, or low transmission power), non-full-diversity lattices can be of great interest.

As for more applied future work, it is left to evaluate how well the constructed lattices perform in actual wiretap channel simulations. As mentioned earlier, one design criterion for the fading wiretap channel is to minimize the flatness factor of the sublattice, which is equivalent to minimizing the theta series. However, at least in dimension 8, the deformed lattices E_8^α cannot be minimizers of the theta function, since E_8 is the unique minimizer. Still, the theta series of E_8^α approaches that of the E_8 lattice as the parameter α approaches 1.

In this paper, we also demonstrated the fact that, at least in dimensions less than 5 and in dimension 8, there exist GWR lattices with density arbitrarily close to the optimal density. One would expect this to hold for other dimensions as well. As far as we know, the research on GWR lattices is rather scarce, even though GWR lattices are widely represented in the set of well-rounded lattices. For instance, in dimension 1, all well-rounded lattices are GWR, and in dimension 2, all well-rounded lattices except for the hexagonal lattice are GWR.

Appendix A. Proof of Theorem 4.4.

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 $1 \le i \le n$, which gives $\lambda_1^2(D_n^\alpha) \le 2$. Now suppose that $\mathbf{x} \in S(D_n^\alpha)$; then $\|\mathbf{x}\|^2 \le 2$. 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 $\|\mathbf{x}\|^2 \ge x_n^2 = c_n^2\alpha^2 > c_n^2$ and hence $|c_n| \le 1$. If $c_n = 0$, then $\|\mathbf{x}\|^2 \ge x_{n-1}^2 = c_{n-1}^2\alpha^2 > c_{n-1}^2$ and so $|c_{n-1}| \le 1$. Otherwise, if $|c_n| = 1$, then also $|c_{n-1}| \le 1$. To see this, suppose that $|c_{n-1}| \ge 2$. Then $\|\mathbf{x}\|^2 \ge x_{n-1}^2 + x_n^2 \ge (2\alpha - \overline{\alpha})^2 + \alpha^2 > \alpha^2 + \alpha^2 > 2$, a contradiction. Inductively, we conclude $|c_i| \le 1$ 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 nonzero. 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 nonzero, 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),

$$\|\mathbf{x}\|^2 = \alpha^2 + \overline{\alpha}^2 + x_4^2 + \cdots + x_n^2 \tag{A.1}$$

$$= 2 + c_5^2\overline{\alpha}^2 + (-c_5\alpha + c_6\overline{\alpha})^2 + \cdots + (-c_{n-1}\alpha + c_n\overline{\alpha})^2 + c_n^2\alpha^2, \tag{A.2}$$

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 nonzero 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 $c_i = 0$ otherwise.

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 nonzero. 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 well rounded, note that $M_{D_n^\alpha}$ is nonsingular and thus $S(D_n^\alpha)$ spans $\mathbb{R}^n$. Moreover, D_n^α is GWR since $\kappa(D_n^\alpha) = |S(D_n^\alpha)| = 2n$. ∎

REFERENCES

[1] C. Alves, W. L. da Silva Pinto, and A. A. de Andrade, *Well-Rounded Lattices via Polynomials*, CoRR preprint, abs/1904.03510, 2019, http://arxiv.org/abs/1904.03510, 2019.

[2] R. Bacher, *Constructions of some perfect integral lattices with minimum* 4, J. Théor. Nombres Bordeaux, 27 (2015), pp. 655–687.

[3] A. Barreal, M. T. Damir, R. Freij-Hollanti, and C. Hollanti, *An approximation of theta functions with applications to communications*, SIAM J. Appl. Algebra Geom., 4 (2020), pp. 471–501, https://doi.org/10.1137/19M1275334.

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

[5] J.-C. Belfiore and F. E. Oggier, *Secrecy gain: A wiretap lattice code design*, in 2010 International Symposium On Information Theory & Its Applications, IEEE, 2010, pp. 174–178.

[6] X. Blanc and M. Lewin, *The crystallization conjecture: A review*, EMS Surv. Math. Sci., 2 (2015), pp. 255–306.

[7] W. Bolaños and G. Mantilla-Soler, *The trace form over cyclic number fields*, Canad. J. Math., (2020), pp. 1–23.

[8] A. Böttcher, L. Fukshansky, S. R. Garcia, and H. Maharaj, *On lattices generated by finite abelian groups*, SIAM J. Discrete Math., 29 (2015), pp. 382–404, https://doi.org/10.1137/140982520.

[9] A. Chorti, C. Hollanti, J. Belfiore, and H. Poor, *Physical Layer Security: A Paradigm Shift in Data Confidentiality*, Springer Lect. Notes Elect. Engrg. 358, Springer, 2016, pp. 1–15.

[10] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska, *Universal optimality of the E_8 and Leech lattices and interpolation formulas*, Ann. of Math. (2), 196 (2022), pp. 983–1082.

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

[12] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer, New York, 1999.

[13] S. I. Costa, F. Oggier, A. Campello, J.-C. Belfiore, and E. Viterbo, *Lattices Applied to Coding for Reliable and Secure Communications*, Springer, 2017.

[14] R. Coulangeon, *Spherical designs and zeta functions of lattices*, Int. Math. Res. Not., 2006 (2006), 49620, https://doi.org/10.1155/IMRN/2006/49620.

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

[16] M. T. Damir and D. Karpuk, *Well-rounded twists of ideal lattices from real quadratic fields*, J. Number Theory, 196 (2019), pp. 168–196, https://doi.org/10.1016/j.jnt.2018.09.017.

[17] M. T. Damir, A. Karrila, L. Amorós, O. W. Gnilke, D. Karpuk, and C. Hollanti, *Well-rounded lattices: Towards optimal coset codes for Gaussian and fading wiretap channels*, IEEE Trans. Inform. Theory, 67 (2021), pp. 3645–3663, https://doi.org/10.1109/TIT.2021.3059749.

[18] M. T. Damir and G. Mantilla-Soler, *Bases of minimal vectors in tame lattices*, Acta Arith., 205 (2022), pp. 265–285, https://doi.org/10.4064/aa220408-18-8.

[19] R. R. de Araujo and S. I. Costa, *Well-rounded algebraic lattices in odd prime dimension*, Arch. Math., 112 (2019), pp. 139–148, https://doi.org/10.1007/s00013-018-1232-7.
[20] B. N. Delone and S. S. Ryshkov, *A contribution to the theory of the extrema of a multi-dimensional ζ-function*, Dokl. Akad. Nauk, 173 (1967), pp. 991–994.
[21] L. Fukshansky, G. Henshaw, P. Liao, M. Prince, X. Sun, and S. Whitehead, *On well-rounded ideal lattices* II, Int. J. Number Theory, 9 (2013), pp. 139–154, https://doi.org/10.1142/S1793042112501291.
[22] L. Fukshansky and K. Petersen, *On well-rounded ideal lattices*, Int. J. Number Theory, 8 (2012), pp. 189–206, https://doi.org/10.1142/S179304211250011X.
[23] O. W. Gnilke, A. Barreal, A. Karrila, H. T. N. Tran, D. A. Karpuk, and C. Hollanti, *Well-rounded lattices for coset coding in MIMO wiretap channels*, in Proceedings of the IEEE International Telecommunication Networks and Applications Conference, 2016, pp. 289–294.
[24] O. W. Gnilke, H. T. N. Tran, A. Karrila, and C. Hollanti, *Well-rounded lattices for reliability and security in Rayleigh fading SISO channels*, in Proceedings IEEE Information Theory Workshop, 2016, pp. 359–363.
[25] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, *Semantically secure lattice codes for the Gaussian wiretap channel*, IEEE Trans. Inform. Theory, 60 (2014), pp. 6399–6416, https://doi.org/10.1109/TIT.2014.2343226.
[26] L. Luzzi, R. Vehkalahti, and C. Ling, *Almost universal codes for fading wiretap channels*, in IEEE Int. Symp. Inf. Theory, 2016, pp. 3082–3086.
[27] C. McMullen, *Minkowski's conjecture, well-rounded lattices and topological dimension*, J. Amer. Math. Soc., 18 (2005), pp. 711–734, https://doi.org/10.1090/S0894-0347-05-00483-2.
[28] D. Micciancio and O. Regev, *Worst-case to average-case reductions based on Gaussian measures*, SIAM J. Comput., 37 (2007), pp. 267–302, https://doi.org/10.1137/S0097539705447360.
[29] H. L. Montgomery, *Minimal theta functions*, Glasgow Math. J., 30 (1988), pp. 75–85, https://doi.org/10.1017/S0017089500007047.
[30] G. Nebe and N. J. A. Sloane, *Table of Densest Packings Presently Known*, 2012, http://www.math.rwth-aachen.de/∼Gabriele.Nebe/LATTICES/density.html.
[31] F. Oggier, P. Solé, and J. Belfiore, *Lattice codes for the wiretap Gaussian channel*, Construction Anal., 62 (2016), pp. 5690–5708.
[32] F. Oggier and E. Viterbo, *Algebraic Number Theory and Code Design for Rayleigh Fading Channels*, Foundations Trends Commun. Inform. Theory 1, Now Publisher, 2004.
[33] L. H. Ozarow and A. D. Wyner, *Wire-tap channel* II, At&T Lab. Tech. J., 63 (1984), pp. 2135–2157, https://doi.org/10.1002/j.1538-7305.1984.tb00072.x.
[34] P. Sarnak and A. Strömbergsson, *Minima of Epstein's zeta function and heights of flat tori*, Invent. Math., 165 (2006), pp. 115–151, https://doi.org/10.1007/s00222-005-0488-2.
[35] E. Viterbo and F. E. Oggier, *Full Diversity Rotations*, 2005, http://www.ecse.monash.edu.au/staff/eviterbo/rotations/rotations.html.
[36] A. D. Wyner, *The wiretap channel*, Bell Syst. Tech. J., 54 (1975), pp. 1355–1387.