Configurations of sublattices and Dirichlet-Voronoi cells of periodic point sets

Dissertation
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)

Der Fakultät für Mathematik der
Technischen Universität Dortmund
vorgelegt von

Dipl.-Math. Marc Christian Zimmermann

am 14. August 2017

Dissertation

Configurations of sublattices and Dirichlet-Voronoi cells of periodic point sets

Fakultät für Mathematik
Technische Universität Dortmund

Erstgutachter: Prof. Dr. Rudolf Scharlau

Zweitgutachter: Prof. Dr. Achill Schürmann

Tag der mündlichen Prüfung: 22.09.2017

Contents

Introduction

"The world is full of nasty numbers..."

— J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices and groups, p.56*

WHAT THIS THESIS IS ABOUT. AND WHY.

The study of lattices and geometric properties of point sets in Euclidean space are brought together in a vast amount of mathematical research. The more prominent problems, such as the sphere packing problem and the sphere covering problem, are both classical and still current subjects of research. But there is another geometric problem involving Euclidean lattices, which has received less attention, at least from the mathematical community:

the lattice quantizer problem.

We will handle lattice quantization from a purely mathematical point of view. For an detailed account of its history in information theory as well as a collection of some of the most important results up to its publication, we refer the interested reader to [GN98]. For a textbook introduction to lattice quantization, also written from an information theoretic point of view, we refer the interested reader to [Zam14]. A resource from mathematics that we wish to mention is [Hem04], a Ph.D. thesis which shows where the mathematical reception of the problem stood around 2004. Since then, not to much has happened on the mathematical side of this problem[1].

Lattice quantization emerged as a subject of research in its own right as a special case of general vector quantization. The underlying principle is easy: suppose you have to deal with arbitrary real numbers, produced in some way and yours to handle. Maybe these are descriptions of analog phenomena like speech, or video. In any case, it might be reasonable to ask how to efficiently get a discretized, possibly finite, description of real numbers, that albeit loses only as much "information" as is unavoidable. This is the basic question of quantization: Given a source that produces real numbers x, choose a discrete (and for practical purposes finite) subset of the real line and provide a rule to assign one of those values to a number produced by that source. Or to quote: "A quantizer [...] is a device for converting nasty

[1] There is one notable exception in form of [DSSV09]. There, among other things, the explicit value of the quantizer constant of certain highly symmetrical lattices is derived.

numbers into nice numbers" (cf. Chapter 2, 3.1 in [CS98]). The easiest example one can possibly think of is to use the set $\mathbb{Z}$ and simply round a real number to the integer nearest to it.

Now a vector quantizer is based on the idea that it might be beneficial to not quantize, or round, each real number for itself, but rather to collect, say, n of them and find a way to quantize the so obtained vector. Before we talk about how to do so, we should be allowed to ask: why do we do so? The answer is that it pays off. The idea is to assign a performance measure to a quantizer and ask for such structures that optimize performance with respect to said measure. A crucial insight is that using higher-dimensional structures allows to reduce the margin of error. We will give a short account of this for lattice quantizers later on (cf. Chapter 5).

In this thesis we deal with two mathematical problems that arose from this general setup. We will discuss them in two separate parts.

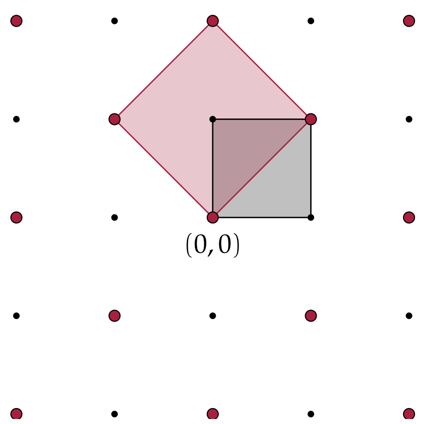
Similar sublattices and finite quadratic modules

The main goal of this part is to

enumerate similar sublattices of integral lattices.

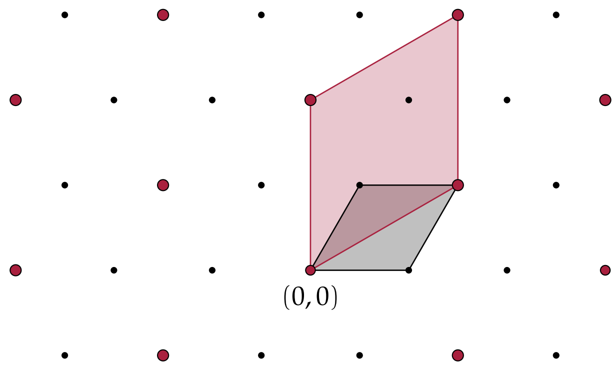
More recently several authors discussed the idea to assign multiple descriptions to each quantized vector, rather than to just take the output of the quantizer as a final result. The idea here is that if certain of these descriptions would get lost, say, after sending the information over a channel, the received subset of descriptions could be used to at least get a (good) approximation of the initial code word. While we will not include a discussion of such schemes in this thesis, this was the starting point for the investigations regarding similar sublattices: the multiple-description lattice quantization schemes all use similar sublattices in the construction of the descriptions (cf. [SVS99], [KGK00], [VSS01], [DSV02], [AS10], and [AS12]).

A sublattice of a lattice L is called similar if it is the image L under an isometry followed by a scaling operation $\lambda \,\mathrm{id}$. Below we depict examples for similar sublattices of the standard lattice $\mathbb{Z}^2$ and the Hexagonal lattice A_2. The superlattice consists of all points shown (black and red), while the sublattice consists of the red points only. For $\mathbb{Z}^2$ we show a similar sublattice with scale factor 2, it is obtained by a 45-degree rotation and followed by $2\,\mathrm{id}$:



We also show fundamental parallelotopes for the super- and the sublattice, from which one can visually read off that the scale factor is in fact 2.

For A_2 we provide an example of a similar sublattice that is obtained by a 30-degree rotation followed by $3\,\mathrm{id}$. We depict A_2 with lattice basis $(1,0), (1/2, \sqrt{3}/2)$:



Again, it is easy to verify the scale factor to be 3. At this point we should wonder in which way the shown sublattices are special. Could we have found similar sublattices for an arbitrary scale factor? Is there just this one, or are there more? Both questions can be answered for these special lattices, but in higher dimensions both problems become increasingly difficult.

However, the extent in which the mathematical literature deals with this geometric problem is rather small. What can be found in the literature, is a criterion for the existence of similar sublattices of rational lattices (cf. [CRS99]) and some results on the number of similar sublattices of certain lattices in dimensions 2 and 4 (cf. [BSZ11], [BM99], and [BHM08]). But these works often rely on certain structural assumptions that are quite special and their methods are not likely to be applicable in higher dimensions.

We use an arithmetical approach to obtain results on the number of similar sublattices (under certain conditions). At least in theory this approach provides a method to explicitly construct similar sublattices with the use of a computer algebra system. The main results for this part are presented in Chapter 2, where we classify and count maximal totally isotropic submodules of regular quadratic modules over finite rings, and in Chapter 3, where we relate the study of similar sublattices to the results of Chapter 2.

If we consider a slightly generalized situation, namely that of sublattices of an integral lattice L that are similar to some lattice in the genus of L, rather than only to L itself, the full strength of the arithmetic approach becomes visible. For certain well-behaved classes of lattices, most prominently even unimodular lattices, our approach gives a full answer to the related counting problem: for a given scale factor, or equivalently index, how many sublattices similar to a lattice in the genus of L do exist? Given L there might be a finite number of exceptions, where we cannot predict this number, the case of scale factors not coprime to the determinant of L. However, for unimodular lattices this is without consequence.

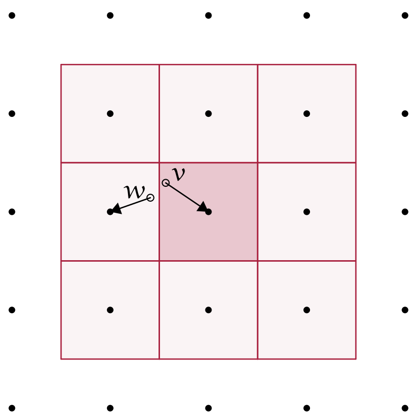
A locally explicit formula for the quantizer constant in monohedral periodic vector quantization

The main goal of this part is to

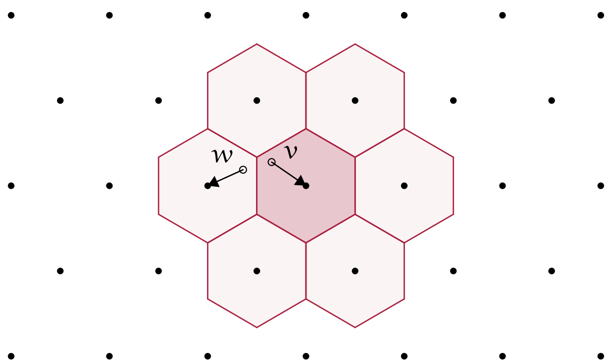
> *systematically investigate the quantizer constant and its minimal values for monohedral periodic sets.*

We take a set of points in $\mathbb{R}^n$, use their Dirichlet-Voronoi tiling of $\mathbb{R}^n$ and associate to an $x \in \mathbb{R}^n$ the Dirichlet-Voronoi cell it is contained in[2]. This defines a vector quantizer.

If the points form the standard lattice $\mathbb{Z}^n$, this is just component wise rounding:



Here the black dots are the lattice points and we depict the Dirichlet-Voronoi cell of the origin in a darker red shade. We see that the other Dirichlet-Voronoi cells of this lattice are all translates, by lattice points, of this fundamental cell. We depict some of them in a lighter red shade. As an example for quantization take a look at the points v, w. They lie in distinct Dirichlet-Voronoi cells and v would be quantized by $(0,0)$ and w would be quantized by $(-1,0)$. Another example, where it is still easy to see how to quantize, is the Hexagonal lattice A_2. We depict it with lattice basis $(1,0), (1/2, \sqrt{3}/2)$:



the above remarks hold in a literal manner.

[2]If x is contained in several Dirichlet-Voronoi cells, which can happen if and only if it lies on their boundary, the tie can be broken arbitrarily.

A good reason why to use lattices instead of dealing with arbitrary point sets is lies in the hardness of the closest vector problem. It surely is hard for lattices, but it is much harder for arbitrary unstructured sets. We utilize the squared Euclidean distance as a measure of performance and ask to minimize the mean error of quantization. For a lattice this amounts to a minimization of the quantity

$$G(L) = \frac{1}{n} \frac{1}{\det(L)^{1/2+1/n}} \int_{DV(L)} \|x\| dx.$$

We contribute to the problem of finding and identifying the best lattices for this measure of quality, by utilizing a reduction theory of Voronoi. This will allow us to reduce the general problem of evaluating the integral above for arbitrary lattices, to a finite number of easier problems. To be precise we will be able to express this integral as the quotient of a polynomial by a power of $\det(L)$ in Corollary 6.3.9. This expression also will show that the problem of finding the best lattice in a fixed dimension can be translated into a finite number of polynomial optimization problems in Theorem 6.3.7. But beware, their number explodes from dimension 6 onwards.

The methods utilized do not depend on the underlying point set to be a lattice. More generally they work for periodic sets and, in particular, for periodic sets for which all Dirichlet-Voronoi cells are congruent to one another. This latter property is commonly asked for in quantization, following a conjecture of Gersho [Ger79]. We thus chose to derive all results directly in the case of monohedral periodic sets, including lattices as a special case.

The approach to obtain an explicit formula for the quantizer constant in this way is not new, it was first used in [BS83] to prove that the lattice $A_3^\# \cong D_3^\#$ is a global minimum for the lattice quantizer problem in dimension 3, and that it is in fact the only local minimum in this dimension. We provide a systematic treatment of this approach and find that both $A_4^\#$ and $D_4^\#$ are local minima in dimension 4 in Theorems 6.4.3 and 6.4.4.

STRUCTURE OF THE THESIS

This thesis is divided into two parts, which are almost independent of each other, only Part II uses some of the notation provided in Chapter 1 of Part I to reduce redundancy. This is done on purpose to make the main results of each part easier to access if one is only interested in this particular problem. We described above how these parts are connected and that, in fact, they started out from a single question:

what can mathematics contribute to the vector quantizer problem?

Part I starts off with an introductory chapter on quadratic forms and lattices (cf. Chapter 1). We then present some results on maximal totally isotropic submodules of regular quadratic modules over finite rings (cf. Chapter 2). The first part is concluded by an arithmetic approach to the enumeration of (genus-)similar sublattices of integral lattices (cf. Chapter 3).

Part II starts off with an introductory chapter on point sets and tilings in Euclidean space (cf. Chapter 4). Here we continue with a short introduction to, or survey of, vector quantization (cf. Chapter 5). The second part is concluded by the application of Voronoi 's second reduction theory to the quantizer problem for monohedral periodic sets and local optimality of lattices in dimension 4 (cf. Chapter 6).

MAIN RESULTS

We present a list of what we deem to be our main results, by parts. They are presented in their order of appearance.

Part I:

- Theorem 2.4.4, achieving the full classification of maximal totally isotropic submodules of regular quadratic modules over finite local rings.
- 2.6, presenting the explicit numbers of maximal totally isotropic submodules of regular quadratic modules over finite local principal ideal rings, in low dimensional cases. Those are of importance for the application to the enumeration of similar sublattices.
- Theorem 3.3.13, the most general result we derive on the validity of the arithmetic approach to enumerate (genus-)similar sublattices of integral maximal lattices.

Part II:

- Theorem 6.3.7, showing that the quantizer problem for suitable periodic sets is equivalent to a finite number of polynomial optimization problems.
- Corollary 6.3.9, providing an explicit expression for the quantizer constant for lattices.
- Theorems 6.4.3 and 6.4.4, proving local optimality of the root lattices $D_4^\#$ and $A_4^\#$ for the lattice quantizer problem in dimension 4.

USE OF COMPUTER ALGEBRA SYSTEMS

We used the computer algebra systems MAGMA [BCP97] (V2.22-7) and MAPLE[3] (2015.0) [Map] to obtain the computational results of this thesis. Wherever results depend on the usage of said systems, an indication is given.

[3]Maple is a trademark of Waterloo Maple Inc.

List of notations

We provide a list of symbolic notations used throughout this thesis. The symbolic notation is grouped according to the chapter it is introduced in and sorted in order of appearance.

Chapter 1

$\mathfrak{b}_q$	1.1.1	*the associated bilinear form of the quadratic form* q.
$[\cdot]$, $\langle\cdot\rangle$		*matrix notations for free quadratic modules.*
$O(E,\mathfrak{b})$, $O(E,q)$	1.1.2	*isometry group of the* $(E,\mathfrak{b})$ (E,q).
$\cong$		*isometry of quadratic and bilinear modules.*
$G_{\mathcal{B}}(E,\mathfrak{b})$, $G_{\mathcal{B}}(E,q)$	1.1.3	*gram matrix of* $(E,\mathfrak{b})$, (E,q).
$d(E,\mathfrak{b})$, $d(E,q)$		*determinant of* $(E,\mathfrak{b})$, (E,q).
$G_{\mathcal{B}}(E,\mathfrak{b})$, $G_{\mathcal{B}}(E,q)$	1.1.3	*gram matrix of* $(E,\mathfrak{b})$, (E,q).
$\perp$	1.1.4	*as operator: orthogonal sum; as exponent: orthogonal module.*
$E*$	1.1.5	*the dual module of* E, $E* := \mathrm{Hom}_R(E,R)$.
$\hat{\mathfrak{b}}$		$\mathfrak{b}$ *on* E*:* $\hat{\mathfrak{b}} : E \to E^*;\ y \mapsto \hat{\mathfrak{b}}(y)$.
$\hat{\mathfrak{b}}(y)$		$\mathfrak{b}$ *on* E*:* $\hat{\mathfrak{b}}(y) : E \to R;\ x \mapsto \mathfrak{b}(x,y)$.
$\mathbb{H}$	1.1.6	*the hyperbolic plane.*
$\mathbb{Q}_p$, $\mathbb{Z}_p$	1.2.1	*the field (ring) of* p*-adic rational numbers (integers).*
$\mathbb{Q}_\infty$, $\mathbb{Z}_\infty$		*the Archimedean completion of* $\mathbb{Q}$, $\mathbb{Z}$.
S_p	1.2.2	*the Hasse-symbol.*
$\mathfrak{s}L$, $\mathfrak{n}L$, $\mathfrak{v}L$	1.3.2	*the scale, norm, volume ideal of the lattice L.*
${}^{\alpha}L$		*the lattice* L *with its quadratic (bilinear) form scaled by* α.
$L^{\#}$		*the dual lattice of* L, $L^{\#} := \{x \in KL \mid \mathfrak{b}(x,L) \subset \mathfrak{o}\}$.
$L^{p,\#}$		*the* p*-partial dual lattice of* L, $L^{p,\#} := \frac{1}{p} \cap L^{\#}$.
L_p		*the localization of* L *at* p.
$\mathrm{gen}(L)$		*the genus of* L.
$\mathfrak{g}L$	1.3.4	*the norm group of* L.

Chapter 2

We abbreviate: mtis. ≙ maximal totally isotropic submodule(s)

$\operatorname{spec}(R)$	2.2.1	*the spectrum of a ring.*
$\mathfrak{m}$		*a maximal ideal of a local ring.*
$R_{\mathfrak{m}}$		*localization of a ring at* $\mathfrak{m}$.
$\overline{}, \overline{}^{[k]}$	2.2.4	*reduction modulo* $\mathfrak{m}$, $\mathfrak{m}^k$.
W		*non-hyperbolic module of rank* $1, 2$.
$\nu_{\mathfrak{m}}(v)$	2.3.1	$\mathfrak{m}$*-order of* v, $\nu_{\mathfrak{m}}(v) := \max\left\{ k \in \mathbb{N}_0 \mid \mathfrak{m}^{r-k}v = 0 \right\}$.
$V_{(k)}, V^{pr}_{(k)}$	2.3.1	*set of elements of* $\mathfrak{m}$*-order* $\geqslant, = k$.
$S(V), S^*(V)$	2.3.2	*the sets of isotropic, primitive isotropic elements of* V.
$s(V), s^*(V)$	2.3.2	*cardinalities of the sets* $S(V), S^*(V)$
$s^*(V)_k$		*number of isotropic elements with* $\mathfrak{m}$*-order* k.
ν_M	2.4.2	M *submodule,* $\left\{ \nu_{\mathfrak{m}}(m) \mid m \in M: q(m) = 0 \right\}$.
$H_{e,f}(k), \mathbb{H}_{e,f}(k)$		*mtis of hyperbolic planes.*
$\mathbf{t}$		*a type.*
$m(V), m(V, t)$		*number of mtis, such of type* $\mathbf{t}$.
$s^*(\mathbf{t})_k$		*number of isotropic elements with* $\mathfrak{m}$*-order* k *in a mtis of type* $\mathbf{t}$.

Chapter 3

$\Sigma(L)$	3.1	*the set of similarities of* L.
$\operatorname{SSL}(L)$		*the set of similar sublattices of* L.
$s_L, \operatorname{ssl}_L$		*counting functions for similarities, similar sublattices.*
$\Sigma^g(L)$		*the set of genus similarities of* L.
$\operatorname{SSL}^g(L)$		*the set of genus-similar sublattices of* L.
$s^g_L, \operatorname{ssl}^g_L$		*counting functions for genus similarities, genus-similar sublattices.*

Chapter 4

We abbreviate: D-V ≙ Dirichlet-Voronoi

$\mathcal{F}_{\mathcal{B}}(L)$	4.1	*the fundamental parallelotope of* L *with respect to the basis* $\mathcal{B}$.
$\Lambda_{\mathbf{t}}$		*standard periodic set* $\Lambda_{\mathbf{t}} := \bigcup_{i=1}^{n} t_i + \mathbb{Z}^n$.
vol_b	4.1.1	*volume with respect to an inner product* b.
$\operatorname{vol}(L, b)$		$\operatorname{vol}(L, b) := \operatorname{vol}_b(F_{\mathcal{B}}(L)) = \sqrt{\det(L, b)}$.
$\mathbf{t}$	4.1.2	*a collection of translation vectors.*
$\operatorname{GL}^{\mathbf{t}}_n(\mathbb{Z})$		$\{U \in \operatorname{GL}_n(\mathbb{Z}) \mid U\Lambda_{\mathbf{t}} = \Lambda_{\mathbf{t}}\}$.
$\mathcal{S}^n_{>0}$	4.1.3	*the cone of positive-definite symmetric quadratic matrices.*
$\mathcal{S}^{n,m}_{>0}$	4.1.5	*set of positive definite periodic forms.*
$(Q, \mathbf{t})$		*a periodic form.*

$\mathrm{star}(v, \mathcal{C})$	4.2.1	*the star of* v *in the polytopal complex* $\mathcal{C}$.
$\mathcal{C}(P), \mathcal{C}(\partial P)$		*trivial subdivision of a polytope* P, *its boundary complex.*
$\mathrm{vert}(\mathcal{C})$		*the vertices of the polytopal complex* $\mathcal{C}$.
$p_v^-(\mathcal{C})$		*pulling refinement of a polytopal complex.*
$\mathrm{DV}_{\mathcal{P},\Vert\cdot\Vert}(p)$	4.3.3	*D-V cell of* p *in* $\mathcal{P}$ *with respect to* $\Vert \cdot \Vert$.
$\mathrm{DV}_{\mathcal{P}}(\Vert \cdot \Vert)$		*D-V subdivision of* $\mathcal{P}$ *with respect to* $\Vert \cdot \Vert$.
$\mathrm{DV}(L), \mathrm{DV}(\Lambda)$		*the D-V cell of a lattice* L, *periodic set* Λ.
$\mathrm{DV}(Q)$		*the D-V cell of the lattice* $(\mathbb{Z}^n, Q)$.
$\mathrm{Del}_{\mathcal{P}}(\Vert \cdot \Vert)$	4.3.4	*the Delone subdivision of* $\mathcal{P}$ *with respect to* $\Vert \cdot \Vert$.
$\mathrm{DV}(Q, P)$	4.3.13	*the D-V polytope for the Delone polytope* P, *quadratic form* Q.

Chapter 5

$G(L)$	5.1	*the normalized second moment/ quantizer constant of a lattice* L.
$G_b(L)$		*the normalized second moment/ quantizer constant of a lattice* (L, b).

Chapter 6

T	6.1.1	*linear subspace of* $\mathcal{S}^n_{>0}$.
$\Delta_T(\mathcal{D})$		*the* T*-secondary cone of* $\mathcal{D}$.
$M(S)$	6.2.1	*the matrix whose* i*-th row is* $(s_i - s_0)^T$, $s_i \in \mathrm{vert}(S)$, S *a simplex.*
$G(Q)$	6.3	$G(Q) := G(L, Q)$.
$G_\Delta(Q)$		*the quantizer polynomial (in* Q*) for the secondary cone* Δ.
$c(Q)$	6.4.1	*conic parameter of* Q.
F^c		*a function* F *in conic parameters.*
$\mathcal{V}^n$		*the Delone triangulation for Voronoi's principal domain of the first type.*
$\overline{\Delta(\mathcal{V}^n)}$		*Voronoi's principal domain of the first type.*

Part I

Similar sublattices and finite quadratic modules

CHAPTER

1 Quadratic modules and lattices

In this first introductory chapter we collect basic algebraic and arithmetic notions and results of the theory of quadratic forms.

We first discuss the abstract theory of quadratic forms over rings and fields in 1.1. This includes the notions of regularity, duality and isometry.

Basic facts about the localizations of $\mathbb{Q}$ and $\mathbb{Z}$ in 1.2 are followed by a discussion of lattices over $\mathbb{Z}$ and its localizations in 1.3. In particular, we provide an overview of the arithmetic theory of integral lattices and their localizations, including the notion of a genus of a lattice and the classification of unimodular and maximal $\mathbb{Z}_p$-lattices.

1.1 QUADRATIC FORMS OVER RINGS AND FIELDS

We follow the exposition in [Kne02]. Let R be a commutative ring with 1 and let E be an R-module. Furthermore let S be a ring extension of R, i.e., there exists a monomorphism of rings $\iota : R \hookrightarrow S$.

1.1.1 Quadratic and bilinear forms

An S-valued **quadratic form** on E is a map $q : E \to S$ which satisfies

$$q(\lambda x) = \lambda^2 q(x) \text{ for all } \lambda \in R, x \in E,$$
$$q(x+y) = q(x) + q(y) + b_q(x,y),$$

where b_q is a symmetric bilinear form, the **associated bilinear form** to q. The pair (E, q) is then called a **quadratic module**. If R is a field, E is a vector space and we use the term **quadratic space**. Accordingly we speak of a **bilinear module** (E, b), whenever b is a symmetric bilinear form on E.

Directly from the definition we obtain that $2q(x) = b_q(x,x)$, thus if 2 is not a zero-divisor in R, a quadratic form is uniquely determined by the associated bilinear form b_q, if $2 \in R^\times$, we obtain $q(x) = \frac{1}{2} b_q(x,x)$. In this case only little distinction is necessary between (E, q) and (E, b_q).

If E is a finitely generated projective[1] R module of rank n, we can find a not necessarily symmetric bilinear form $a : E \times E \to R$ for which $q(x) = a(x, x)$. We can do so by choice of a basis $(x_1, \ldots, x_n)$ for a free module $G = E \oplus E'$ enveloping E, using

$$q(\sum_{i=1}^{n} \lambda_i x_i) = \sum_{i=1}^{n} q(x_i)\lambda_i^2 + \sum_{1 \leqslant i < j \leqslant n} b_q(x_i, x_j)\lambda_i \lambda_j,$$

and setting $a(x_i, x_i) := q(x_i)$, $a(x_i, x_j) := b_q(x_i, x_j)$ for $i < j$ and $a(x_i, x_j) := 0$ for $i > j$. We silently used the extension of q to G where $q(x) = 0$ for all $x \in E'$. In any case, a bilinear form a will always lead to a quadratic form $q(x) := a(x, x)$, with associated bilinear form $b_q(x, y) = a(x, y) + a(y, x)$.

This also shows that free quadratic modules are in correspondence to homogeneous polynomials with coefficients in R of degree 2 in n indeterminates, which is the more classical definition of a quadratic form.

To describe a free quadratic module of rank n we may write

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ & a_{22} & & \\ & & \ddots & \\ & & & a_{nn} \end{bmatrix} = \begin{bmatrix} q(x_1) & b_q(x_1, x_2) & \ldots & b_q(x_1, x_n) \\ & q(x_2) & & \\ & & \ddots & \\ & & & q(x_n) \end{bmatrix},$$

where all entries below the diagonal are zero. If the matrix is diagonal we write $[q(x_1), \ldots, q_(x_n)]$. If 2 is not a zero divisor we write

$$\left\langle \begin{matrix} b_{11} & \ldots & b_{1n} \\ \vdots & \vdots & \\ b_{n1} & \ldots & b_{nn} \end{matrix} \right\rangle = \left\langle \begin{matrix} b_q(x_1, x_1) & \ldots & b_q(x_1, x_n) \\ \vdots & \vdots & \\ b_q(x_n, x_1) & \ldots & b_q(x_n, x_n) \end{matrix} \right\rangle$$

and accordingly $\langle b_q(x_1, x_1), \ldots, b_q(x_n, x_n) \rangle$.

1.1.2 Isometries

An **isometry** of quadratic modules $(E, q), (E', q')$ is an injective module-homomorphism $\phi : E \to E'$ such that

$$q'(\phi(x)) = q(x), \; \forall x \in E.$$

If there is a bijective isometry, we say that (E, q) and (E', q') are **isometric** and write $(E, q) \cong (E', q')$.

The collection of all isometries $(E, q) \to (E, q)$ is the **isometry group** of (E, q), we write $O(E, q)$.

Similarly an **isometry** of bilinear modules $(E, b), (E', b')$ is an injective module-homomorphism $\phi : E \to E'$ such that

$$b'(\phi(x), \phi(y)) = b(x, y), \; \forall x, y \in E.$$

If there is a bijective isometry, we say that (E, b) and (E', b') are **isometric** and write $(E, b) \cong (E', b')$.

[1] A module is (finitely generated) projective if and only if it is a direct summand of a free module (of finite rank), cf. Proposition 3.10 and its Corollary in [Jac09].

The collection of all isometries $(E, b) \to (E, b)$ is the **isometry group** of (E, b), we write $O(E, b)$.

It is readily checked that each isometry of quadratic modules is also an isometry for the associated bilinear forms.

1.1.3 Gram matrices and determinants of free modules

If (E, b) is a free bilinear module of rank n and $\mathcal{B} = (x_1, \dots, x_n)$ is a basis, the matrix $G_{\mathcal{B}}(E, b) := (b(x_i, x_j))_{i,j=1,\dots,n}$ is the **Gram** matrix of (E, b) with respect to the basis $\mathcal{B}$. If $\mathcal{B}'$ is another basis there is an element $T \in GL_n(R)$ such that $G_{\mathcal{B}'}(E, b) = T^T G_{\mathcal{B}}(E, b)T$. To any Gram matrix we associate its determinant in the usual way and observe that $\det(G_{\mathcal{B}'}(E, b)) = \det(T)^2 \det(G_{\mathcal{B}}(E, b))$. Therefore we define the **determinant** of a free bilinear module as the class of the determinant of any Gram matrix in $R/R^{\times 2}$. We denote this square class by $d(E, b)$, or in short dE.

We associate a **determinant** to any free quadratic module (E, q) by $d(E, q) := d(E, b_q)$.

1.1.4 Orthogonality

Elements $x, y \in E$ are **orthogonal** with respect to some symmetric bilinear form $b : E \times E \to R$ if $b(x, y) = 0$. For any $F \subset E$ we have an **orthogonal submodule** $F^\perp := \{y \in E \mid b(F, y) = 0\}$. We say that E is the **(internal) orthogonal sum** of submodules $E_1, \dots, E_m$ if $E = \bigoplus_{i=1}^m E_i$ and $b(E_i, E_j) = 0$ for all $i \neq j$, and write $E = E_1 \perp \dots \perp E_m$.

The **(external) orthogonal sum** of bilinear modules (E, b), (E', b') is their exterior direct sum, together with the bilinear form $b \perp b' : E \oplus E' \times E \oplus E' \to R;\ (x + x', y + y') \mapsto b(x, y) + b'(x', y')$. It is denoted by $(E \perp E', b \perp b')$.

For a quadratic module (E, q) we use the above terms if they hold for the associated bilinear form b_q.

1.1.5 Duality and regularity

We denote the **dual module** of any R-module E by $E^* := \mathrm{Hom}_R(E, R)$. Assume that E is equipped with a bilinear form b. We define a module homomorphism $\hat{b} : E \to E^*$, where the value of $\hat{b}$ on $y \in E$ is given by the linear form

$$\hat{b}(y) :\ E \to R;\ \ x \mapsto b(x, y).$$

To any submodule $F \subset E$ we write $\hat{b}_F$ for the map $\hat{b}$ followed by the restriction map from E^* to F^*, that is, the value of $\hat{b}$ on $y \in E$ is given by the linear form

$$\hat{b}_F(y) :\ F \to R;\ \ x \mapsto b(x, y).$$

It is clear that $\ker(\hat{b}_F) = F^\perp$. For a submodule $F \subset E$ we therefore have $E = F \perp F^\perp$ if and only if $\hat{b}_F$ induces a bijection of F on $\hat{b}_F(E)$, that is if $\hat{b}_F(E) = \hat{b}_F(F)$ and $F \cap F^\perp = \{0\}$. We write $\hat{b} = \hat{b}_E$.

We say that a bilinear form b on E is **non-degenerate** if $\hat{b}$ is injective, and **regular** if $\hat{b}$ is bijective and E is finitely generated projective.

A submodule F of a module E is **primitive** if F is a direct summand of E. If b is a bilinear form on E, F is b-**primitive** if F is finitely generated projective and if $\widehat{b_F}(E) = F^*$. In this situation, a regular submodule is b-primitive and a b-primitive submodule is primitive.

For a quadratic module (E, q) we use the above terms if they hold for the associated bilinear form b_q.

1.1.6 Isotropy and hyperbolic modules

Let (E, q) be a quadratic module. $x \in E$ is called **isotropic** if $q(x) = 0$, otherwise it is called **anisotropic**. A submodule $F \subset E$ is called **isotropic** if it contains an isotropic $x \neq 0$, it is called **anisotropic** if it does not contain non-zero isotropic elements. It is called **totally isotropic** if every element is isotropic.

For a free R-module E set $\mathbb{H}(E) := E \oplus E^*$ and equip it with the quadratic form $q(x, y) := < x, y >= y(x)$. This defines a free regular quadratic module. We say that a free quadratic module (E, q) is **hyperbolic** if there exists some free R-module F such that $E \cong \mathbb{H}(F)$. If $(E, q) \cong \mathbb{H}(R)$ we say that (E, q) is a **hyperbolic plane**.

A hyperbolic plane can be written as $Re + Rf$, with $q(e) = q(f) = 0$ and $b_q(e, f) = 1$, we then refer to such a basis (e, f) as **hyperbolic pair**. In the above matrix notation this is expressed by

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \text{ and } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

whenever applicable.

1.2 LOCAL NOTIONS

References for the subsequent discussion should be found in almost all introductory texts on algebraic number theory and the arithmetic of quadratic forms, for example Kapitel 2 in [Neu06] and Section 15 in [Kne02].

1.2.1 Localizations of $\mathbb{Q}$ and $\mathbb{Z}$

Every valuation on $\mathbb{Q}$ is equivalent to either a p-adic valuation, where p runs through the primes of $\mathbb{Z}$, or to the usual absolute value (cf. 12.1 in [O'M73]). It is common to say that a p-adic valuation is introduced by the finite (or non-Archimedean, or prime) **spot** p (or rather $\mathfrak{p} = (p) = p\mathbb{Z}$) and the absolute value is induced by the infinite (or Archimedean) **spot** ∞. We will denote spots on $\mathbb{Z}$ by p, including the case $p = \infty$.

If p is a prime of $\mathbb{Z}$, we denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ in the topology induced by the p-adic valuation, and refer to it as the **localization** of $\mathbb{Q}$ at p, it therefore is a complete local field. Similarly we write $\mathbb{Z}_p$ for the completion of $\mathbb{Z}$ under the above topology and refer to this as the **localization** of $\mathbb{Z}$ at p. In this situation $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$ and $\mathbb{Z}_p$ is the valuation ring and topological closure of $\mathbb{Z}$ in $\mathbb{Q}_p$, both with respect to the p-adic valuation. We refer to elements of $\mathbb{Z}_p$ as the **integers** of $\mathbb{Q}_p$. For a fractional ideal $\mathfrak{a}$ of $\mathbb{Z}$ we can define $\mathfrak{a}_p$ as the topological closure of $\mathfrak{a}$ in $\mathbb{Z}_p$ (cf. 81 : 13 in [O'M73]). Note that $\mathbb{Z}_p$ is a discrete valuation ring and therefore a principal ideal domain.

If p is the Archimedean spot ∞ the situation becomes even simpler, we set $\mathbb{Q}_\infty = \mathbb{R}$, the completion of $\mathbb{Q}$ with respect to the usual absolute value. We then write $\mathbb{Z}_\infty = \mathbb{Q}_\infty = \mathbb{R}$.

1.2.2 Local invariants for quadratic spaces

We define the **Hilbert-symbol** for $\mathbb{Q}$ and primes $p \in \mathbb{Z}$ to be

$$(a,b)_p := \begin{cases} +1, & \exists x,y \in \mathbb{Q}_p : \; ax^2 + by^2 = 1, \\ -1, & \text{else.} \end{cases}$$

Clearly the Hilbert-symbol is invariant under distinct representatives of a square class in each argument, thus we will allow for the arguments to be square classes of field elements.

If $V \cong <\alpha_1> \perp \ldots \perp <\alpha_n>$ is a non-degenerate quadratic space of dimension n over $\mathbb{Q}_p$ we also have the **Hasse-symbol**

$$S_p V = \prod_{1 \leqslant i \leqslant n} (\alpha_i, \prod_{1 \leqslant j \leqslant i} \alpha_j)_p.$$

This definition does not depend on the chosen orthogonal splitting of V. Furthermore if p is a prime spot and V' is another $\mathbb{Q}_p$ space of dimension n, then $V \cong V'$ if and only if $S_p V = S_p V'$ (cf. §63B. in [O'M73]).

The only invariant we need for quadratic spaces over $\mathbb{Q}_\infty$ is the usual notion of the signature over the real numbers.

1.3 LATTICES OVER $\mathbb{Z}$ AND ITS LOCALIZATIONS

We now gather aspects of the theory of lattices over the ring $\mathbb{Z}$ or one of its completions and clarify the notation used. A general reference for this is [O'M73] and we follow closely the notation of this book and only indicate certain spots of interest more clearly with a direct reference to this book.

Let K be one of the fields $\mathbb{R}, \mathbb{Q}, \mathbb{Q}_p, \mathbb{Q}_\infty$, where p is a prime. Let $\mathfrak{o} = \mathbb{Z}$ if $K \in \{\mathbb{R}, \mathbb{Q}\}$ and let $\mathfrak{o}$ be the localization of $\mathbb{Z}$ in K if $K = \mathbb{Q}_p$ for a prime p or $K = \mathbb{Q}_\infty = \mathbb{R}$.

1.3.1 Lattices

An $\mathfrak{o}$-**lattice** in a K vector space V is a finitely generated $\mathfrak{o}$-submodule of V, it is **on** V if $KL = V$. For any lattice in V we can find a **basis** $\mathcal{B}$, by which we understand a vector space basis $\mathcal{B} = (v_1, \ldots, v_m)$ of $KL \subset V$, such that

$$L = \mathfrak{o}v_1 + \ldots + \mathfrak{o}v_m.$$

The number $m = \dim(KL) = \mathrm{rk}(L)$ is the rank of L as $\mathfrak{o}$-module and is referred to as the **rank** of the lattice L. All of the above lattices are free modules, because we assume $\mathfrak{o}$ to be a principal ideal ring.

A subset $L' \subset L$ that is itself a lattice, is called a **sublattice** of L.

1.3.2 Lattices on bilinear and quadratic spaces

Let (V, b) is a bilinear space with associated quadratic form q defined by $q(x) = b(x,x)$[2] for $x \in V$. Let L be a lattice on V[3]. If $\mathcal{B} = (v_1, \ldots, v_n)$ is a lattice basis, the **Gram matrix** of L with respect to $\mathcal{B}$ is the

[2] That is, $b = \frac{1}{2} b_q$.

[3] It is not hard to see that we in fact could start with some finitely generated torsion-free quadratic or bilinear $\mathfrak{o}$-module L and embed it into the K vector space $V := K \otimes_{\mathfrak{o}} L$ such that L is a lattice on V. This shows that the actual object of interest is given by the pair (L, b), resp. (L, q).

Gram matrix of the quadratic $\mathfrak{o}$-module (L, q)

$$G_{\mathcal{B}}(L, b) := G_{\mathcal{B}}(V, b) = (b(v_i, v_j))_{i,j=1,\dots,n}.$$

The **volume ideal** of L is the ideal $\mathfrak{v}L = \det(G_{\mathcal{B}}(L, b))\mathfrak{o}$, this definition does not depend on the chosen basis: the determinants of different Gram matrices differ by the square of a unit. The **determinant** of L is the determinant of the quadratic $\mathfrak{o}$-module (L, q), thus $\mathfrak{v}L$ is the ideal generated by any representative of the determinant of L. If $\mathfrak{o} = \mathbb{Z}$, 1 is the only square of a unit in $\mathbb{Z}$. We therefore interpret $\det(L, q)$ as an integer and obtain $\mathfrak{v}L = (\det(L))$.

For a lattice L a Gram matrix of V with respect to any lattice basis $\mathcal{B}$ is also called a **Gram matrix** of L, we write $G_{\mathcal{B}}(L, b)$.

If $\alpha \in K$ and L is in (V, b), we write ${}^{\alpha}L$ for the lattice L in $(V, \alpha b)$, which we abbreviate to ${}^{\alpha}V$ if the bilinear form is clear from context. We say that we **scale** L (respectively V, or b) by α in that case.

To L we associate the **scale ideal** $\mathfrak{s}L$, the $\mathfrak{o}$-ideal generated by the set $b(L, L) = \{b(x, y) \mid x, y \in L\}$, and the **norm ideal** $\mathfrak{n}L$, the $\mathfrak{o}$-ideal generated by the set $q(L) = \{b(x, x) \mid x \in L\}$. Then (cf. §82E. in [O'M73])

$$2\mathfrak{s}L \subset \mathfrak{n}L \subset \mathfrak{s}L, \text{ and } \mathfrak{v}L \subset (\mathfrak{s}L)^n.$$

Furthermore for $\alpha \in K$ we immediately obtain

$$\mathfrak{s}^{\alpha}L = \alpha\mathfrak{s}L, \ \mathfrak{n}^{\alpha}L = \alpha\mathfrak{n}L, \ \mathfrak{v}^{\alpha}L = \alpha^n\mathfrak{v}L.$$

Let L be a $\mathbb{Z}$-lattice over $K \in \{\mathbb{Q}, \mathbb{R}\}$ and let L' be a sublattice of L. Then

$$\det(L') = [L : L']^2 \det(L),$$

this is sometimes called the **determinant-index formula** (cf. 81 : 11 and 82 : 11 in [O'M73]).

A non-zero lattice on a non-degenerate quadratic space (V, b) is called **$\mathfrak{a}$-maximal**, for some fractional ideal $\mathfrak{a}$, if $\mathfrak{n}L \subset \mathfrak{a}$ and for every lattice L' on V, for which $L \subset L'$ and $\mathfrak{n}L' \subset \mathfrak{a}$ are satisfied, the equality $L = L'$ holds. For $\alpha \in K$ we immediately obtain that if L is $\mathfrak{a}$-maximal on V, then ${}^{\alpha}L$ is $\alpha\mathfrak{a}$-maximal on ${}^{\alpha}V$.

We can adapt the notions of isometry and isometry groups to lattices in a literal manner from 1.1.2. This induces an equivalence relation on the set of lattices on V and the equivalence class of a lattice L is called **isometry class** of L, denoted by $\mathrm{cls}(L)$. The isometry group of a lattice is often called its **orthogonal group** if $\mathfrak{o} = \mathbb{Z}$ and $K \in \{\mathbb{Q}, \mathbb{R}\}$. The **automorphism group** of L is $\mathrm{Aut}(L) = \{\phi \in GL(V) \mid \phi(L) = L\}$, thus $O(L, b) = \mathrm{Aut}(L) \cap O(V, b)$. If the bilinear form or quadratic form is clear from context we also abbreviate $O(L)$ for $O(L, b)$ or $(O(L, q))$. For $\alpha \in K$ we immediately obtain

$$O(L) = O({}^{\alpha}L), \text{ and } \mathrm{cls}(L) = \mathrm{cls}({}^{\alpha}L).$$

The **dual lattice** of L in (V, b) is given by $L^{\#} := \{x \in KL \mid b(x, L) \subset \mathfrak{o}\}$. If $\mathcal{B} = (v_1, \dots, v_m)$ is a basis for L in which

$$L = \mathfrak{o}v_1 + \dots + \mathfrak{o}v_m,$$

then

$$L = \mathfrak{o}v_1^\# + \ldots + \mathfrak{o}v_m^\#,$$

where $\mathcal{B}^\# = (v_1^\#, \ldots, v_m^\#)$ is the **dual basis** of $\mathcal{B}$ with respect to b, that is $b(v_i, v_j^\#) = \delta_{ij}$.

Let L be an integral $\mathbb{Z}$-lattice over $\mathbb{Q}$ or $\mathbb{R}$. We associate to any integer $p \mid \det(L)$ the p**-partial dual** $L^{p,\#} := \frac{1}{p}L \cap L^\#$ and for any co-prime integers p, q such that $\det(L) = pq$ we immediately derive

$$L^\# = L^{p,\#} \cap L^{q,\#}. \tag{1.1}$$

A lattice is called $\mathfrak{a}$**-modular** for some fractional ideal $\mathfrak{a}$ if $\mathfrak{s}L = \mathfrak{a}$ and $\mathfrak{v}L = \mathfrak{a}^n$. For $\alpha \in K$ we say that L is α-modular if L is $(\alpha) = \alpha\mathfrak{o}$-modular. L is **unimodular** if it is $\mathfrak{o}$-modular. If (L, b) is non-degenerate then L is unimodular if and only if $L = L^\#$.

1.3.3 Localizations and the genus of an integral lattice

Let p be a prime of $\mathbb{Z}$. We can localize a vector space V over $\mathbb{Q}$ and a $\mathbb{Z}$-lattice L in V. We set $V_p := \mathbb{Q}_p V$ and $L_p = \mathbb{Z}_p L$ for the **localization**. In addition, $\mathbb{Q}_\infty = \mathbb{R}$ and $\mathbb{Z}_\infty = \mathbb{R}$. Then L_p is a lattice on V_p, and in fact L_p is the $\mathbb{Z}_p$-submodule generated by L in V_p. If $\mathcal{B}$ is a basis of L, then

$$L_\mathfrak{p} = \mathbb{Z}_p v_1 + \ldots + \mathbb{Z}_p v_m.$$

In particular $\mathfrak{s}(L_p) = (\mathfrak{s}L)_p$, $\mathfrak{n}(L_p) = (\mathfrak{n}L)_p$, $\mathfrak{v}(L_p) = (\mathfrak{v}L)_p$, and L is $\mathfrak{a}$-maximal if and only if L_p is $\mathfrak{a}_p$-maximal (cf. §82K. [O'M73]).

It is the well-known Hasse-Minkowski Theorem (cf. 66 : 4 in [O'M73]) that relates non-degenerate quadratic spaces and their localizations: non-degenerate quadratic $\mathbb{Q}$-spaces V, V' are isometric if and only if $V_p \cong V'_p$ for all primes p of $\mathbb{Z}$ and $V_\infty \cong V'_\infty$. Therefore, two non-degenerate $\mathbb{Q}$-spaces V, V' are isometric if and only if $V_p \cong V'_p$ for all prime numbers and if the signature of $\mathbb{R}V$ and $\mathbb{R}V'$ are identical.

Now for lattices on a non-degenerate quadratic space V the Hasse-Minkowski Theorem fails in general: there might be non-isometric lattices L, L' such that $L_p \cong L'_p$ for all spots p (including primes and ∞) of $\mathbb{Z}$. Thus the set

$$\operatorname{gen}(L) := \{L' \text{ lattice on } V \mid L'_p \cong L_p \text{ for all spots } \mathfrak{p} \text{ of } \mathbb{Z}\}$$

will in general be a disjoint union of several distinct isometry classes of lattices on V. We call this set the **genus** of L. The number of distinct isometry classes in gen(L) is the **class number** of L and we say that L is **unigeneric** if this number is equal to 1.

1.3.4 Unimodular lattices over local fields

Let L be a $\mathbb{Z}_p$-lattice over $\mathbb{Q}_p$, where p is a prime of $\mathbb{Z}$. In this situation, for any dimension n, the classification of unimodular lattices divides into two cases. We have to handle the case that $p \mid 2$, the so called **dyadic** case and the case that $2 \in \mathbb{Z}_p^*$, the so called **non-dyadic** case, separately

In the non-dyadic case there are two classes of non-isometric non-degenerate quadratic spaces over $\mathbb{Q}_p$ on which a unimodular lattice can exist, and on each of those there exists exactly one isometry class of unimodular lattices. In particular, this implies that if L, L' are on V and both are unimodular at $\mathfrak{p}$, then $L_\mathfrak{p} \cong L'_\mathfrak{p}$ (cf. §92. in [O'M73]).

In the dyadic case this becomes more difficult. We need an additional invariant, the **norm group** of a lattice

$$\mathfrak{g}L := q(L) + 2\mathfrak{s}L.$$

This group in fact generates the norm ideal, but might provide more information as

$$2\mathfrak{s}L \subset \mathfrak{g}L \subset \mathfrak{n}L.$$

And in fact: unimodular lattices L, L' on the same space over $\mathbb{Q}_p$ are isometric if and only if $\mathfrak{g}L = \mathfrak{g}L'$ (cf. Theorem 93 : 16 in [O'M73]).

For unimodular lattices over $\mathbb{Z}_2$ this implies that $\mathfrak{g}(L) = \mathbb{Z}_2$ or $\mathfrak{g}(L) = 2\mathbb{Z}_2$, the odd and even case.

1.3.5 Maximal lattices over local fields

Another well-behaved class of lattices over the fields $\mathbb{Q}_p$ is that of maximal lattices. If V is a regular quadratic space over $\mathbb{Q}_p$ and if $\mathfrak{a}$ is a fractional ideal of its ring of integers, then $L \cong L'$ for all $\mathfrak{a}$-maximal lattices L, L' on V (cf. 91 : 2 in [O'M73]).

Chapter

2 Maximal totally isotropic submodules of regular quadratic modules over finite rings

This chapter contains some of the main results of this thesis. We provide a local-global principle for quadratic forms over finite rings, classify maximal totally isotropic submodules of regular quadratic modules over finite rings, and count their number over finite principal ideal rings.

We start by recalling some basic results for quadratic forms over special rings. This includes splitting off hyperbolic planes, Witt's Theorem over local rings, and basic facts regarding quadratic forms over finite fields.

This is followed by a discussion of quadratic forms over finite rings, where we derive a local-global principle for finite quadratic forms in Theorem 2.2.2.

Using a variant of Hensel's Lemma we relate regular quadratic modules over finite local rings to regular quadratic spaces over their residue fields. As a consequence, we can divide regular quadratic modules over finite local rings into 3 cases (cf. Proposition 2.2.5). For each case we can derive a formula for the order of the orthogonal group (cf. 2.2.8).

Together with a construction we refer to as slicing (cf. 2.3.1), this enables us to give explicit formulae for the number of isotropic elements of given order (cf. Propositions 2.3.8 and 2.3.9).

We then focus on the classification of maximal totally isotropic submodules of regular quadratic modules over finite rings (cf. 2.4). This classification is one of the main results of this thesis and achieved in Theorem 2.4.4. Its proof is subdivided into a number of Lemmata and presented in 2.4.3. The classification is based on the new notion of type of a maximal totally isotropic submodule, explicit examples of such submodules, for every type, are collected in Example 2.4.3.

Combining the results of 2.3 and 2.4, we provide a way to count the number of maximal totally isotropic submodules of regular quadratic modules over finite principal ideal rings. The main case is that the ring is also local, then Proposition 2.5.5 gives the number of maximal totally isotropic submodules of a fixed type. The general case can be reduced to the local case by the local-global principle established earlier (cf. Proposition 2.5.1).

We conclude this chapter with some explicit numbers of maximal totally isotropic submodules of regular quadratic modules of even rank over finite local principal ideal rings (cf. 2.6). In particular, these results apply to modules over $\mathbb{Z}/p^r\mathbb{Z}$ (and by multiplicativity to modules over $\mathbb{Z}/c\mathbb{Z}$). By Theorem 3.3.12) we find that (2.9) provides the number of similar sublattices of E_8 of norm p^r. These were not known before, this application to the counting of similar sublattices was the main motivation for the subsequent research.

2.1 Generalities

2.1.1 Quadratic modules split off hyperbolic planes

For the sake of readability we collect some basic results for quadratic modules over commutative rings with 1.

PROPOSITION 2.1.1 (CF. (1.6) IN [KNE02]). *Let (V, q) be a quadratic module. If $U \subset V$ is a regular submodule then U splits V: $V = U \perp U^{\perp}$.*

As in the case of fields, a free regular totally isotropic submodule of a quadratic module can be embedded in a hyperbolic submodule. A bit more is actually true.

PROPOSITION 2.1.2 (CF. (2.22) IN [KNE02]). *Let U be a $\mathfrak{b}_q$-primitive free totally isotropic submodule of a quadratic module (V, q). Then there exists a hyperbolic submodule $W \subset V$ such that $U \subset W$.*

In the case of primitive isotropic elements of regular modules, we obtain the well known process of splitting off an hyperbolic plane.

COROLLARY 2.1.3. *Let (V, q) be a quadratic module. Let $v \in V$ be $\mathfrak{b}_q$-primitive isotropic. Then there exists a hyperbolic plane H and a submodule $W \subset V$ such that $V = H \perp W$*

2.1.2 Witt's Theorem for quadratic forms over local rings

Let R be a local ring with maximal ideal $\mathfrak{m}$. We start by recalling in which way a quadratic module over a local ring can be described as an orthogonal sum of submodules.

PROPOSITION 2.1.4 ((CF. (4.1) IN [KNE02]). *Let V be an finitely generated R-module with symmetric bilinear form $\mathfrak{b}$. Then V can be decomposed orthogonally into regular submodules of rank 1 or 2, and a module W such that $\mathfrak{b}(W, W) \subset \mathfrak{m}$. V is regular if and only if $W = \{0\}$.*

There is a version of Witt's theorem which holds over local rings:

THEOREM 2.1.5 (CF. (4.3) IN [KNE02]). *Let (V, q) be a quadratic R-module with associated bilinear form $\mathfrak{b} = \mathfrak{b}_q$, X, Y, Z submodules, where X, Y are free and of finite rank and let*

$$\hat{\mathfrak{b}}_X(Z) = X^*,\ \hat{\mathfrak{b}}_Y(Z) = Y^*$$

be satisfied. Let $\phi : X \to Y$ be an isomorphism satisfying $\phi(x) \equiv_Z x$ for all $x \in X$. Then there is an extension of ϕ to an automorphism of V, satisfying $\phi(v) \equiv_Z v$ for all $v \in V$, while fixing every $z \in Z^{\perp}$.

This implies the validity of Witt's cancellation Theorem for local rings.

COROLLARY 2.1.6. *Let* (V, q) *be a quadratic module over a local ring* R. *Let* $\phi' : X \to Y$ *be an isometry of* b_q*-primitive submodules of* V. *Then there is an isometry* $\phi : V \to V$ *such that* $\phi_{|X} = \phi'$.

COROLLARY 2.1.7. *Let* $(X_1, q_1), (X_2, q_2), (Y_1, q_1), (Y_2, q_2)$ *be quadratic modules over a local ring* R, *where* X_1, X_2 *are regular. Then*

$$X_1 \perp Y_1 \cong X_2 \perp Y_2 \text{ and } X_1 \cong X_2 \Longrightarrow Y_1 \cong Y_2.$$

COROLLARY 2.1.8. *Let* (V, q) *be a quadratic* R*-module. Then* $\mathrm{rk}(M_1) = \mathrm{rk}(M_2)$ *for any* b_q*-primitive maximal totally isotropic submodules* M_1, M_2 *of* V.

We will write $\mathrm{ind}((V, q)) := \mathrm{rk}(M)$ for any b_q-primitive maximal totally isotropic submodule of a quadratic module (V, q) and refer to this as the **Witt index** of (V, q), which is well-defined by the above result.

2.1.3 Facts on quadratic forms over finite fields

Let (V, q) be a regular quadratic space with $\mathrm{ind}(V) = m$ over $\mathbb{F}_q$. The following facts can be found in §12 Klassifikation and §13 Anzahlbestimmungen in [Kne02].

FACT 2.1.9. *Let* V *be a regular quadratic* $\mathbb{F}_q$*-space with* $\mathrm{ind}(V) = m$. *Then* V *decomposes as*

$$V \cong \mathbb{H} \perp \ldots \perp \mathbb{H} \perp W,$$

with W *anisotropic, where we distinguish* 3 *cases:*

I) $\dim(V) = 2m$, $\dim(W) = 0$ *and* V *is hyperbolic.*

II.1) $\dim(V) = 2m + 1$, $\dim(W) = 1$ *and* V *is non-hyperbolic of odd rank,*

II.2) $\dim(V) = 2m + 2$, $\dim(W) = 2$ *and* V *is non-hyperbolic of even rank.*

In cases I *and* II.2 *the decomposition determines the isometry class of* V. *In case* II.1 *and* $\mathrm{char}(\mathbb{F}_q) \neq 2$, *there are* 2 *distinct isometry classes. In all these cases the spaces are regular. If* $\mathrm{char}(\mathbb{F}_q) = 2$ *there exist no regular quadratic spaces of odd dimension.*

In the case of $\mathrm{char}(\mathbb{F}_q) \neq 2$ this can be reformulated in terms of orthogonal bases.

FACT 2.1.10. *Let* (V, q) *be a regular quadratic* $\mathbb{F}_q$*-space where* $\mathrm{char}(\mathbb{F}_q) \neq 2$. *Then* $V \cong < 1, \ldots, 1, \det(q) >$, *and there are two distinct isometry classes of given dimension.*

FACT 2.1.11. *Let* V *be a regular quadratic* $\mathbb{F}_q$*-space with* $\mathrm{ind}(V) = m$. *The order of the corresponding orthogonal groups are*

$$\text{I)}\ |O(V)| = 2 \cdot q^{n(n-1)/2} \cdot (1 - q^{-m}) \cdot \prod_{2i<n} (1 - q^{-2i}),$$
$$\text{II.1)}\ |O(V)| = c \cdot q^{n(n-1)/2} \cdot \prod_{2i<n} (1 - q^{-2i}),$$
$$\text{II.2)}\ |O(V)| = 2 \cdot q^{n(n-1)/2} \cdot (1 + q^{-m-1}) \cdot \prod_{2i<n} (1 - q^{-2i}),$$

where $c = 1$ *if* $\mathrm{char}(\mathbb{F}_q) = 2$ *and* $c = 2$ *else.*

FACT 2.1.12. *Let* V *be a regular quadratic* $\mathbb{F}_q$*-space with* $\operatorname{ind}(V) = m$*. The number of primitive isotropic vectors is given by*

$$\begin{aligned} \text{I)}\ s^*(V) &= (q^m - 1)(q^{m-1} + 1), \\ \text{II.1)}\ s^*(V) &= q^{2m} - 1, \\ \text{II.2)}\ s^*(V) &= (q^{m+1} + 1)(q^m - 1). \end{aligned}$$

FACT 2.1.13. *For regular quadratic spaces* V *and* W*, both hyperbolic or both non-hyperbolic, with* $\dim(W) = \dim(V) - 2$*:*

$$|O(V)| = s^*(V) \cdot q^{n-2} \cdot |O(W)|.$$

2.2 REGULAR QUADRATIC FORMS OVER FINITE RINGS

2.2.1 Artinian rings

A commutative ring R, with unity, is **artinian** if it satisfies the descending chain condition for ideals, that is, if for every descending chain

$$I_1 \supset I_2 \supset \dots$$

of ideals of R, there exists an $r \in \mathbb{N}$ such that

$$I_1 \supset I_2 \supset \dots \supset I_r = I_{r+1} = \dots,$$

we say that the chain becomes stable. In particular,

$$\forall I < R\ \exists r \in \mathbb{N}:\ I \supset I^2 \supset \dots \supset I^r = I^{r+1}. \tag{2.1}$$

Let $\operatorname{spec} R$ denote the **spectrum** of R, that is, the set of all prime ideals of R. If R is artinian, every prime ideal is already maximal (cf. Proposition 8.1 in [AM94]) and $\operatorname{spec} R$ is finite (cf. Proposition 8.3 in [AM94]). The intersection $\mathfrak{N}(R) := \bigcap_{\mathfrak{m} \in \operatorname{spec} R} \mathfrak{m}$ is the **nilradical** and it is nilpotent (cf. Proposition 8.4 in [AM94]).

Let $\mathfrak{m} \in \operatorname{spec} R$, and let r be minimal in (2.1). Then we get the localization $R_\mathfrak{m} \cong R/\mathfrak{m}^r$ of R at $\mathfrak{m}$ (cf. proof of Theorem 8.7 in [AM94]).

If R is artin local with maximal ideal $\mathfrak{m}$, then $\mathfrak{m} = \mathfrak{N}(R)$ and thus nilpotent. In this case the minimal r in (2.1) is the nilpotency index of $\mathfrak{m}$ in R.

THEOREM 2.2.1 (CF. THEOREM 8.7 IN [AM94]). *Let* R *be artinian and let* r *be the nilpotency index of* $\mathfrak{N}(R)$*. Then* R *is a finite direct product of artin local rings:*

$$R \cong \prod_{\mathfrak{m} \in \operatorname{spec} R} R_\mathfrak{m} \cong \prod_{\mathfrak{m} \in \operatorname{spec} R} R/\mathfrak{m}^r.$$

For a local artinian ring R the quotients $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ are $R/\mathfrak{m}$-vector spaces. Since artinian rings are noetherian, the dimension of these $R/\mathfrak{m}$-spaces is finite. Furthermore, R is a principal ideal ring if and only if $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \leqslant 1$.

2.2.2 Finite rings

Every finite ring R is both artinian and noetherian and thus Theorem 2.2.1 is applicable.

Let R be finite local, with maximal ideal $\mathfrak{m}$. Then $R/\mathfrak{m}$ is a finite field, and thus there exists a prime p and a power $q = p^k$ such that $R/\mathfrak{m} \cong \mathbb{F}_q$. Then there exists $s \in \mathbb{N}$, such that $|R| = q^s$, in fact, $|R| = \prod_{i=1}^{r} |\mathfrak{m}^{i-1}/\mathfrak{m}^i|$ and as we noted each $\mathfrak{m}^{i-1}/\mathfrak{m}^i$ is a $\mathbb{F}_q$-vector space, thus all cardinalities appearing are powers of q. But then $q = |R/\mathfrak{m}| = [R : \mathfrak{m}] = \frac{|R|}{\mathfrak{m}}$ and thus $|\mathfrak{m}| = q^{s-1}$.

R is a principal ideal ring if and only if $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \leqslant 1$. We distinguish the two possible cases. Either $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) = 0$ and $\mathfrak{m} = \mathfrak{m}^2 = \{0\}$, so R is a field, or $|\mathfrak{m}^k| = |\mathfrak{m}|^k = q^k$ for all $0 \leqslant k \leqslant r$ and, in particular, $r = s$.

2.2.3 A local-global principle for quadratic forms over finite rings

Let R be finite, let $\operatorname{spec} R = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_l\}$. By Theorem 2.2.1

$$R \cong \prod_{i=1}^{l} R_{\mathfrak{m}_i} \cong \prod_{i=1}^{l} R/\mathfrak{m}_i^{r_i}, \tag{2.2}$$

where r_i is minimal in (2.1) for $\mathfrak{m}_i$. Let V be a finitely generated R module. Then this implies that

$$V \cong \prod_{i=1}^{l} V_{\mathfrak{m}_i} \cong \prod_{i=1}^{l} V/\mathfrak{m}_i^{r_i},$$

where $V_{\mathfrak{m}_i} := R_{\mathfrak{m}_i} \otimes_R V$. If V carries a quadratic form q, we can localize q as well: $q_{\mathfrak{m}_i} : V_{\mathfrak{m}_i} \to R_{\mathfrak{m}_i}$ defined by $q_{\mathfrak{m}_i}(\alpha \otimes v) := \alpha \otimes q(v)$. The associated bilinear form $q_{\mathfrak{m}_i}$ is then the localization of the associated bilinear form of q.

Now each $R_{\mathfrak{m}_i}$ is a **flat** R-module, that is, tensoring with $R_{\mathfrak{m}_i}$ preserves exact sequences (cf. p. 16 and Theorem (3.11) in [Rei75]). This property is quite useful, as the next result will show.

THEOREM 2.2.2 (LOCAL-GLOBAL PRINCIPLE FOR FINITE QUADRATIC FORMS). *Let* R *be a finite ring.*

i. A quadratic module (V, q) *is regular over* R *if and only if* $(V_\mathfrak{m}, q_\mathfrak{m})$ *is regular for all* $\mathfrak{m} \in \operatorname{spec} R$.

ii. For R*-modules* $(V, q), (V', q')$*, we have* $(V, q) \cong_R (V', q')$ *if and only if* $(V_\mathfrak{m}, q_\mathfrak{m}) \cong (V'_\mathfrak{m}, q'_\mathfrak{m})$ *for all* $\mathfrak{m} \in \operatorname{spec} R$.

PROOF. Ad (i): We consider the dual module of V first. Let $\mathfrak{m} \in \operatorname{spec} R$:

$$\begin{aligned}(\operatorname{Hom}_R(V, R))_{\mathfrak{m}_i} &= R_{\mathfrak{m}_i} \otimes_R \operatorname{Hom}_R(V, R)\\ &\cong \operatorname{Hom}_{R_{\mathfrak{m}_i}}(V_{\mathfrak{m}_i}, R_{\mathfrak{m}_i})\\ &\cong \operatorname{Hom}_{R/\mathfrak{m}_i^{k_i}}(V/\mathfrak{m}_i^{k_i}, R/\mathfrak{m}_i^{k_i}),\end{aligned}$$

where the first isomorphy comes from Theorem 3.18 in [Rei75] if we note that V is clearly finitely presented.

Taking this isomorphy and the decomposition of R, V, and V^* as direct products, we see that (V, q) is regular if and only if

$$\hat{b}_q : V \to \operatorname{Hom}_R(V, R)$$

is an isomorphism if and only if

$$\hat{b}_{q_{\mathfrak{m}}} : V_{\mathfrak{m}} \to (\mathrm{Hom}_R(V, R))_{\mathfrak{m}} \cong \mathrm{Hom}_{R_{\mathfrak{m}}}(V_{\mathfrak{m}}, R_{\mathfrak{m}})$$

is an isomorphism for all $\mathfrak{m} \in \operatorname{spec} R$ if and only if $(V_{\mathfrak{m}}, q_{\mathfrak{m}})$ is regular for all $\mathfrak{m} \in \operatorname{spec} R$.

Ad (ii): Write $\operatorname{spec} R = \{\mathfrak{m}_1, \dots, \mathfrak{m}_l\}$ and to each $\mathfrak{m}_i$ let r_i be as in (2.2). Clearly $q(v) = q'(v')$ if and only if $\Phi(q(v)) = \Phi(q(v'))$ under the isomorphism

$$\Phi : \ R \to \prod_{i=1}^{l} R/\mathfrak{m}_i^{r_i}.$$

Let π_i be the projection of the direct product onto $R/\mathfrak{m}_i^{r_i}$, and ι_i its injection. Then given a map $\phi : V \to V'$ we obtain a map $\Phi(\phi) : \prod_{i=1}^{l} V/\mathfrak{m}_i^{r_i} \to \prod_{i=1}^{l} R/\mathfrak{m}_i^{r_i}$ in the natural way.

Thus, by directness of the product, we derive that $\phi : V \to V'$ is an isometry if and only if $\Phi(\phi)$ is if and only if $\pi_i \circ \Phi(\phi) \circ \iota_i : \ V/\mathfrak{m}_i^{r_i} \to R/\mathfrak{m}_i^{r_i}$ is. □

2.2.4 Isometry classes over finite local rings

We now restrict ourselves to the case that R is a finite local ring with maximal ideal $\mathfrak{m}$ of nilpotency index r. For a quadratic R-module V we set $\overline{V} := V/\mathfrak{m}$, $\overline{q}(\overline{v}) := \overline{q(v)}$ for the quadratic $R/\mathfrak{m}$ space $(\overline{V}, \overline{q})$ that is induced from V. More generally for $1 \leqslant k \leqslant r$ we set $\overline{V}^{[k]} := V/\mathfrak{m}^k$, $\overline{q}^{[k]}(\overline{v}^{[k]})$ to refer to the projection modulo the ideal $\mathfrak{m}^k$ of R, where $\overline{V}^{[1]} = \overline{V}$ and $\overline{V}^{[r]} \cong V$.

We restrict our interest to finitely generated projective modules V, which then are free since R is assumed to be a commutative local ring (cf. [Theorem 7.7] [Jac09], also true for arbitrary projective modules over local rings, (cf. [Kap58, Theorem 2]).

Since R local, so is R/I for any ideal $I < R$. In particular, $\mathfrak{m}/I$ is the maximal ideal of R/I. It is easily seen that if V is regular over R, then V/I is regular over R/I: in fact, since V is free, regularity is equivalent to $dV = \varepsilon R^{\times 2}$, with $\varepsilon \in R^\times$. Now if $v_1, \dots, v_n$ is a basis of V, then $v_1 + IV, \dots, v_n + IV$ is a basis for V/I, thus $dV/I = (\varepsilon + I)(R/I)^{\times 2}$. Thus $\varepsilon \in R^\times = R \backslash \mathfrak{m}$ implies that $\varepsilon + I \in (R/I)^\times = R/I \backslash \mathfrak{m}/I$, so that the claim on regularity follows.

LEMMA 2.2.3. *Let $(V, q), (W, q')$ be regular quadratic R-modules of rank n.*

$$V \cong W \Leftrightarrow \overline{V} \cong \overline{W}.$$

If R is a principal ideal ring, each isometry $\overline{V} \to \overline{W}$ lifts to $|\mathfrak{m}|^{n \cdot (n-1)/2}$ distinct isometries of V onto W.

PROOF. This is basically a finite version of Hensel's Lemma (cf. (15.3) in [Kne02]). Let r be minimal with $\mathfrak{m}^r = \{0\}$.

First of all, if $\overline{V} \cong \overline{W}$, there is some R-linear map $\phi : V \to W$, for which $\overline{\phi} : \overline{V} \cong \overline{W}$ is an isometry. This can be obtained by choice of bases $x_1, \dots, x_n$ of V and $y_1, \dots, y_n$ of W for which $\overline{\phi}(\overline{x_i}) = \overline{y_i}$ holds, simply set $\phi(x_i) := y_i$ in that case.

We denote $\phi_1 := \phi$ for one such map and proceed iteratively.

Given ϕ_{j-1}, satisfying $q'(\phi_{j-1}(v)) \equiv_{\mathfrak{m}^{j-1}} q(v)$ for all $v \in V$, we construct ϕ_j satisfying $q'(\phi_j(v)) \equiv_{\mathfrak{m}^j} q(v)$. Of course, once we reach $j = r$, that is after $r-1$ steps, we have constructed the desired isometry $\phi' := \phi_r : V \to W$.

Since $q'(\phi_{j-1}(v)) \equiv_{\mathfrak{m}^{j-1}} q(v)$, we see that the quadratic form $q_j(v) := q'(\phi_{j-1}(v)) - q(v)$ satisfies $q_j(V) \subset \mathfrak{m}^{j-1}$. Let a be a bilinear form (not necessarily symmetric) such that $q_j(v) = a(v,v)$, note that also $a(V,V) \subset \mathfrak{m}^{j-1}$ (cf. 1.1.1).

Make the ansatz $\phi_j(v) = \phi_{j-1}(v) + \psi(v)$, with some linear map $\psi : V \to \mathfrak{m}^{j-1}W$. Then

$$\begin{aligned} q'(\phi_j(v)) &= q'(\phi_{j-1}(v)) + q'(\psi(v)) + b_{q'}(\phi_{j-1}(v), \psi(v)) \\ &\equiv_{\mathfrak{m}^j} q'(\phi_{j-1}(v)) + b_{q'}(\phi_{j-1}(v), \psi(v)) \end{aligned}$$

This shows that for ϕ_j as such, by definition of q_j, the congruences

$$q'(\phi_j(v)) \equiv_{\mathfrak{m}^j} q(v) \quad \text{for all } v \in V,$$

are equivalent to

$$b_{q'}(\phi_{j-1}(v), \psi(v)) \equiv_{\mathfrak{m}^j} -q_j(v) = -a(v,v) \quad \text{for all } v \in V. \tag{2.3}$$

We now claim that we can choose ψ in such a way, that more generally the following holds:

$$b_{q'}(\phi_{j-1}(w), \psi(v)) \equiv_{\mathfrak{m}^j} -a(w,v), \quad \text{for all } w \in V.$$

To see this, fix a basis $v_1, \dots, v_n$ of V. For all $v_i + \mathfrak{m}^j$ we find an element $z_i + \mathfrak{m}^j \in V/\mathfrak{m}^j$ such that

$$b_{q'}(\phi_{j-1}(w + \mathfrak{m}^j), z_i + \mathfrak{m}^j) + \mathfrak{m}^j = -a(w + \mathfrak{m}^j, v_i + \mathfrak{m}^j) + \mathfrak{m}^j, \quad \text{for all } w + \mathfrak{m}^j \in V/\mathfrak{m}^j, \tag{2.4}$$

simply by regularity of the reduction of $b_{q'}$ modulo $\mathfrak{m}^j$. Thus we can define a map ψ by the conditions $v_i \mapsto z_i$. It remains to show that $\psi(V) \subset \mathfrak{m}^{j-1}W$, but this follows from the fact that $z_i \in \mathfrak{m}^{j-1}W$ for $i \in \{1, \dots, n\}$: The reduction of $b_{q'}$ modulo $\mathfrak{m}^{j-1}$ is regular, so the congruence

$$b_{q'}(\phi_{j-1}(w), z_i) \equiv_{\mathfrak{m}^j} -a(w, v_i) \equiv_{\mathfrak{m}^{j-1}} 0$$

holds for all $\phi_{j-1}(w) + \mathfrak{m}^{j-1}$, where $w \in V$. But the reduction of ϕ_{j-1} modulo $\mathfrak{m}^{j-1}$ is an isometry $V/\mathfrak{m}^{j-1} \to W/\mathfrak{m}^{j-1}$, thus $x + \mathfrak{m}^{j-1} \mapsto b_{q'}(x + \mathfrak{m}^{j-1}, z_i + \mathfrak{m}^{j-1}) + \mathfrak{m}^{j-1}$ is the zero map, which implies $z_i \in \mathfrak{m}^{j-1}$.

It remains to count the number of extensions of every isometry over the residue field to isometries over R in the case that $\mathfrak{m} \neq \{0\}$ is a principal ideal. We have to check which $z_i + \mathfrak{m}^j \in \mathfrak{m}^{j-1}/\mathfrak{m}^j$ are solutions to the congruence equation (2.4). There is a total of $|\mathfrak{m}^{j-1}/\mathfrak{m}^j|$ choices of z_i for each i, thus in combination we have $|\mathfrak{m}^{j-1}/\mathfrak{m}^j|^{n \cdot n}$ possible choices for ψ modulo $\mathfrak{m}^j$. But each $\psi : V \to \mathfrak{m}^{j-1}W$ generates one of the $|\mathfrak{m}^{j-1}/\mathfrak{m}^j|^{n\cdot(n+1)/2}$ quadratic forms on the $R/\mathfrak{m}$-vector space $\mathfrak{m}^{j-1}W/\mathfrak{m}^j \cong \left(\mathfrak{m}^{j-1}/\mathfrak{m}^j\right)^n$. Conversely each such quadratic form on $\left(\mathfrak{m}^{j-1}/\mathfrak{m}^j\right)^n$ can be obtained this way, and each one of them is constructed the same number of times. This in particular implies that every quadratic form on $\left(\mathfrak{m}^{j-1}/\mathfrak{m}^j\right)^n$ is the image of exactly $|\mathfrak{m}^{j-1}/\mathfrak{m}^j|^{n\cdot(n-1)/2} = |\mathfrak{m}^{j-1}/\mathfrak{m}^j|^{n\cdot n - n\cdot(n+1)/2}$ linear maps $V \to \left(\mathfrak{m}^{j-1}/\mathfrak{m}^j\right)^n$.

So at each step above there are precisely $|\mathfrak{m}^{j-1}/\mathfrak{m}^j|^{n\cdot(n-1)/2}$ linear maps $V \to \left(\mathfrak{m}^{j-1}/\mathfrak{m}^j\right)^n$, such that condition (2.3) is satisfied for the quadratic form $a(v,v)$. Completing all $r-1$ steps we arrive at

$$\prod_{j=2}^{r} |\mathfrak{m}^{j-1}/\mathfrak{m}^j|^{n\cdot(n-1)/2} = \left(\frac{|\mathfrak{m}|}{|\mathfrak{m}^r|}\right)^{n\cdot(n-1)/2} = |\mathfrak{m}|^{n\cdot(n-1)/2}$$

distinct lifts to isometries $V \to W$. □

REMARK 2.2.4. We have pursued the counting of lifts only in the case that $\mathfrak{m}$ is a principal ideal. The proof is intendedly written in such a way that it can be directly generalized to the non-principal case, but more variables come in to play: as is evident from the proof, it is the dimension of the $R/\mathfrak{m}$ vector space $\mathfrak{m}^{j-1}/\mathfrak{m}^j$ that brings in new degrees of freedom once $\mathfrak{m}$ is not principal. One has to evaluate this dimension at each step and the resulting quantity will not posses a closed form as simple as in the principal ideal case. ■

Lemma 2.2.3 provides a very important result, which allows us to explicitly describe the possible Witt-decompositions of regular quadratic modules (V, q) over R, just as in the case of finite fields.

PROPOSITION 2.2.5. *Let V be a regular quadratic module over R. Then*

$$V \cong \mathbb{H} \perp \ldots \perp \mathbb{H} \perp W,$$

where W is the (unique up to isometry) non-hyperbolic quadratic R-module of rank 0 (case I), 1 (case II.1), or 2 (case II.2).

As with finite fields, in the case of $\mathrm{char}(\overline{R}) \neq 2$ we can reformulate this in terms of orthogonal bases.

PROPOSITION 2.2.6. *Let (V, q) be a regular quadratic R-module where $\mathrm{char}(\overline{R}) \neq 2$. Then*

$$q \cong \langle 1, \ldots, 1, \det(q) \rangle$$

and there are two distinct isometry classes of given rank.

PROOF. This follows from 2.2.3 and the well-known classification of regular quadratic modules over finite fields (cf. (12.5) in [Kne02] and 2.1.10). □

REMARK 2.2.7. The non-hyperbolic regular module W of rank 1 or 2 is not anisotropic if $r > 1$, though it cannot contain primitive isotropic elements, it certainly will contain isotropic elements, namely those of the submodule $\mathfrak{m}^{\lceil r/2 \rceil} W$, which is totally isotropic (cf. Lemma 2.4.10). ■

By the above, it is possible to compute the orthogonal groups of regular quadratic modules over R by computation of the lifting homomorphisms used in the proof of Lemma 2.2.3, this can be of use for the construction of similar sublattices in certain cases (cf. Remark 3.3.14). In any case, we can derive the orders of the associated orthogonal groups of such modules.

COROLLARY 2.2.8. *Let R be a principal ideal ring. Let (V, q) be a regular quadratic R-module of cardinality q^s. Then*

$$| \mathrm{O}(V, q) | = |\mathfrak{m}|^{n(n-1)/2} \cdot | \mathrm{O}(\overline{V}, \overline{q}) | .$$

That is, if V is hyperbolic

$$| \mathrm{O}(V, q) | = 2 \cdot (q^s)^{n(n-1)/2} \cdot (1 - q^{-n/2}) \cdot \prod_{2i<n} (1 - q^{-2i}),$$

if V is non-hyperbolic of odd rank

$$| \mathrm{O}(V, q) | = c \cdot (q^s)^{n(n-1)/2} \cdot \prod_{2i<n} (1 - q^{-2i}),$$

where $c = 1$ if $\mathrm{char}(\mathbb{F}_q) = 2$ and $c = 2$ else, and if V is non-hyperbolic of even rank

$$| \mathrm{O}(V, q) | = 2 \cdot (q^s)^{n(n-1)/2} \cdot (1 + q^{-n/2}) \cdot \prod_{2i<n} (1 - q^{-2i}).$$

2.2.5 Isometry classes over finite rings

Let R be a finite ring. From Theorem 2.2.2 we immediately derive that the isometry classes of a regular quadratic module over R are in bijection with all direct products of isometry classes of regular quadratic spaces over its localizations. There are no regular quadratic modules over R if $2 \mid |R|$ and the rank of the localization at the maximal ideal containing 2 is odd (cf. 2.1.9).

2.3 COUNTING ISOTROPIC ELEMENTS IN REGULAR QUADRATIC MODULES OVER FINITE LOCAL PRINCIPAL IDEAL RINGS

Throughout this section R is a finite local principal ideal ring with maximal ideal $\mathfrak{m}$ and corresponding nilpotency index r. Note that if $|R| = q^s$ then $s = r$ for such rings. There are a few results which hold in greater generality, these are clearly marked to hold for rings that are not necessarily principal ideal rings.

A direct approach to count the isotropic elements of given $\mathfrak{m}$-order, comparable to 13 Anzahlbestimmungen in [Kne02] seems to lead to a messy inductive calculation involving a range of representation numbers once R is not a field. We relate isotropic elements of fixed $\mathfrak{m}$-order $k < 2r$ to primitive isotropic elements of a related regular quadratic module over the ring $R/\mathfrak{m}^{r-2k}$. Counting primitive isotropic elements of a regular quadratic R-module can be reduced to the counting of primitive isotropic elements over the residue field of R, combining both we obtain the number of isotropic elements of arbitrary $\mathfrak{m}$-order.

2.3.1 Slicing of regular quadratic modules

Let (V, q) be a regular quadratic R-module. Let $v \in V$, we denote by $\nu_\mathfrak{m}(v)$ the $\mathfrak{m}$-**order** of v, that is $\nu_\mathfrak{m}(v) := \max\left\{ k \in \mathbb{N}_0 \;\middle|\; \mathfrak{m}^{r-k} v = 0 \right\}$. We sort the elements of V into layers comprised of those elements with identical $\mathfrak{m}$-order. The union of all such layers, starting at any $0 \leqslant k \leqslant r$, will then be a submodule. We ultimately will count the number of isotropic elements for each layer separately; to do so we proceed by giving a description of all isotropic elements with $\mathfrak{m}$-order equal to k below.

DEFINITION 2.3.1. Let V be a regular quadratic space over R, and let $0 \leqslant k \leqslant r$.

$$V_{(k)} := \left\{ v \in V \;\middle|\; \nu_\mathfrak{m}(v) \geqslant k \right\},$$
$$V_{(k)}^{\mathrm{pr}} := \left\{ v \in V \;\middle|\; \nu_\mathfrak{m}(v) = k \right\}.$$

◆

LEMMA 2.3.2. *Let* V *be a free regular quadratic space over* R, *and let* $0 \leqslant k \leqslant r$. *Then*

$$V_{(k)} = \mathfrak{m}^k V,$$
$$V_{(k)}^{\mathrm{pr}} = \mathfrak{m}^k V^{\mathrm{pr}}.$$

In particular for $v \in V$, $\nu_\mathfrak{m}(v) \geqslant k$ *if and only if there is a* v' *such that* $v = \mu^k v'$, *and* $\nu_\mathfrak{m}(v) = k$ *if and only if there is a primitive* v' *such that* $v = \mu^k v'$ *for some* $\mu \in \mathfrak{m}$.

PROOF. Since V is free we can identify elements of V with the vector of their coefficients λ_i, with respect to some basis. Let $v \in V_{(k)}$, that is $\mathfrak{m}^{r-k} v = 0$ and it follows that for each coefficient λ_i we have $\mathfrak{m}^{r-k} v_i = 0$. But this implies that $\nu_\mathfrak{m}(\lambda_i) \geqslant k$, and $\lambda_i \in \mathfrak{m}^k$, therefore $V_{(k)} \subset \mathfrak{m}^k V$, the other inclusion is obvious.

Now assume $\nu_\mu(v) = k$. Then $\nu_\mu(v') = \nu_\mu(v) - k = k - k = 0$ shows that v' is primitive. □

We want to use the fact that every element of $V_{(k)}$ therefore "essentially is divisible by $\mathfrak{m}^k$".

Since $V_{(k)}$ is annihilated by $\mathfrak{m}^{r-k}$, we see that $V_{(k)}$ has a structure as $R/\mathfrak{m}^{r-k}$-module. If $2k < r$, we make $V_{(k)}$ a quadratic $R/\mathfrak{m}^{r-k}$-module by defining a quadratic form $q_{(k)}$ on $V_{(k)}$, that is "essentially the form q divided by $\mathfrak{m}^{2k}$". Let $v_1, \dots, v_n$ be a basis of V. Without loss of generality we assume that the basis is chosen such that with respect to this basis

i. for $2 \nmid \operatorname{char}(R)$ we have $q = \langle 1, \dots, 1, \delta \rangle$ where $\delta = \det(q)$ (cf. Proposition 2.2.6);

ii. for $2 \mid \operatorname{char}(R)$ we have a decomposition

$$V = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}^{\operatorname{ind}(V)} \perp W,$$

where

$$W = \begin{cases} \{0\} & \text{if } n = 2\operatorname{ind}(V), \\ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} & \text{if } n = 2\operatorname{ind}(V) + 2, \end{cases}$$

If $2k < r$, we fix the basis of the $R/\mathfrak{m}^{r-k}$-module $V_{(k)}$ that is obtained by the images of $v_1, \dots, v_n$ under the structure transport discussed above. By the values on this basis we define a form $q_{(k)}$ on $V_{(k)}$ as follows:

i. if $p \neq 2$ we define $(V_{(k)}, q_{(k)})$ to be the quadratic $R/\mathfrak{m}^{r-k}$-module

$$V_{(k)} = \langle 1, \dots, 1, \overline{\delta}^{[r-k]} \rangle,$$

where $\overline{\delta}^{[r-k]}$ is the canonical image of $\det(q)$ embedded in $R/\mathfrak{m}^{r-k}$ and the diagonal form is written with respect to the above fixed basis of $V_{(k)}$;

ii. if $p = 2$ we define $(V_{(k)}, q_{(k)})$ to be the quadratic $R/\mathfrak{m}^{r-k}$-module

$$V_{(k)} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}^{\operatorname{ind}(V)} \perp W_{(k)},$$

where

$$W_{(k)} = \begin{cases} \{0\} & \text{if } n = 2\operatorname{ind}(V), \\ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} & \text{if } n = 2\operatorname{ind}(V) + 2, \end{cases}$$

with respect to the above fixed basis of $V_{(k)}$.

LEMMA 2.3.3. *Let V be a regular quadratic R-module and let $2k < r$. With the above definition of $q_{(k)}$ we obtain a regular quadratic $R/\mathfrak{m}^{r-k}$-module $(V_{(k)}, q_{(k)})$. In particular, $(V_{(k)}, q_{(k)})$ is hyperbolic (resp. non-hyperbolic) if and only if (V, q) is hyperbolic (resp. non-hyperbolic).*

By reduction of $(V_{(k)}, q_{(k)})$ modulo $\mathfrak{m}^{r-2k}/\mathfrak{m}^{r-k}$ we obtain a regular quadratic $R/\mathfrak{m}^{r-2k}$ module, which characterizes the isotropic elements of $\mathfrak{m}$-order k.

LEMMA 2.3.4. *Let (V, q) be a regular quadratic R-module and let $2k < r$. The following are regular quadratic modules of the same rank. One of the three is hyperbolic if and only if all of them are.*

i. (V, q) *as* R*-module,*

ii. $(V_{(k)}, q_{(k)})$ *as* $R/\mathfrak{m}^{r-k}$*-module,*

iii. $\left(\overline{V_{(k)}}^{[r-2k]}, \overline{q_{(k)}}^{[r-2k]}\right)$ *as* $R/\mathfrak{m}^{r-2k}$*-module.*

An element $v \in V_{(k)}$ is q-isotropic if and only if $\nu_{\mathfrak{m}}(q_{(k)}(v)) \geqslant r - 2k$ if and only if $\overline{v}^{[r-2k]}$ is $\overline{q_{(k)}}$ isotropic.

If $2k \geqslant r$, then $(V_{(k)}, q_{(k)})$ is a totally isotropic quadratic $R/\mathfrak{m}^{r-k}$-module and therefore every element is isotropic.

Combining this we obtain the desired description of isotropic elements of $\mathfrak{m}$-order k.

LEMMA 2.3.5. *In the above notation: For $v \in V$ with $0 \leqslant \nu_{\mathfrak{m}}(v) = k \leqslant \lfloor \frac{r}{2} \rfloor$*

$$q(v) = 0 \Leftrightarrow \overline{q_{(k)}}^{[r-2k]}(\overline{v}^{[r-2k]}) = 0.$$

In addition, every $v \in V$ with $\nu_{\mathfrak{m}}(v) \geqslant \lceil \frac{r}{2} \rceil$ is isotropic.

2.3.2 Counting elements

DEFINITION 2.3.6. Let V be a regular quadratic module over R.

$$\begin{aligned} S(V) &:= \{\ v \in V\backslash\{0\} \mid q(v) = 0\ \} \\ s(V) &:= |S(V)| \\ S^*(V) &:= \{\ v \in V\backslash\{0\} \mid q(v) = 0,\ v \text{ primitive}\ \} \\ s^*(V) &:= |S^*(V)| \end{aligned}$$

◆

We compute $s^*(V)$ and $s(V)$. The next Lemma shows that $s^*(V) = |\operatorname{O}(V)|/|\operatorname{stab}_{\operatorname{O}(V)}|$. Then it will suffice to compute $|\operatorname{stab}_{\operatorname{O}(V)}(v)|$ for an arbitrary primitive isotropic v, since we can get the value of $|\operatorname{O}(V)|$ from Corollary 2.2.8.

LEMMA 2.3.7. *Let (V, q) be a regular quadratic R module, R not necessarily a principal ideal ring. $\operatorname{O}(V)$ acts transitively on $S^*(V)$.*

PROOF. We fix some $v_0 \in S^*(V)$, thus v_0 is a primitive isotropic element of V and we can find some hyperbolic plane $\mathbb{H}_0$ that contains v and write $V = \mathbb{H}_0 \perp W$ (cf. Corollary 2.1.3). Now for an arbitrary $v \in S^*(V)$ the same is true and we obtain a decomposition $V = \mathbb{H} \perp W'$ where $v \in \mathbb{H}$. Clearly, there exists an isometry $\mathbb{H}_0 \to \mathbb{H}$ that sends v_0 to v. In addition, $\mathbb{H}_0$ and $\mathbb{H}$ are b_q -primitive because they are regular submodules. Thus Corollary 2.1.6) assures the existence of an isometry $V \to V$ sending v_0 to v. □

Since Rv is contained in a hyperbolic plane $\mathbb{H} = Rv + Rv'$, we split this plane from V and obtain $V = \mathbb{H} \perp W$. For $\phi \in O(V)$ to be in $\mathrm{stab}_{O(V)}(v)$, it is necessary and sufficient to satisfy $\phi(v) = v, q(\phi(v')) = 0, b(v, \phi(v')) = 1$. By Witt's Theorem on the extension of isometries (cf. Corollary 2.1.6) we can choose any $u \in V$ satisfying these conditions and find $\phi \in O(V)$ with $\phi(v) = v$, $\phi(v') = u$. Write $u = \lambda v + \mu v' + w$, then $q(u) = q(w) + \lambda\mu b(v, v') = q(w) + \lambda\mu$ as well as $1 = b(v, u) = b(v, \mu v') = \mu b(v, b') = \mu$. Putting this together we arrive at $0 = q(w) + \lambda$. For each $w \in W$ this necessitates $\lambda = -q(w)$. Therefore, we obtain $q^{s(n-2)}$ distinct such u and conclude:

$$\begin{aligned} |\,\mathrm{stab}_{O(V)}(v)| &= |\left\{ \; u \in V \;\middle|\; q(u) = 0, b(v, u) = 1 \; \right\}| \cdot |\,O(W)| \\ &= q^{s(n-2)} \cdot |\,O(W)|. \end{aligned}$$

PROPOSITION 2.3.8. *Let* V *be a regular quadratic* R*-module of rank* n *and with* $\mathrm{ind}(V) = m$. *Then* $s^*(V)$ *is as follows:*

$$\begin{aligned} \text{I) } s^*(V) &= q^{(s-1)(n-1)} \cdot (q^m - 1)(q^{m-1} + 1), \\ \text{II.1) } s^*(V) &= q^{(s-1)(n-1)} \cdot (q^{2m} - 1), \\ \text{II.2) } s^*(V) &= q^{(s-1)(n-1)} \cdot (q^{m+1} + 1)(q^m - 1). \end{aligned}$$

PROOF. From

$$s^*(V) = |O(V)|/|\,\mathrm{stab}_{O(V)}(v)|,$$

where v is an arbitrary primitive isotropic vector, and the above discussion we find

$$|\,\mathrm{stab}_{O(V)}(v)| = q^{s(n-2)} \cdot |\,O(W)|,$$

where $\dim(W) = \dim(V) - 2$ and W hyperbolic if and only if V hyperbolic. Therefore,

$$\begin{aligned} s^*(V) &= q^{-s(n-2)} \cdot \frac{|\,O(V)|}{|\,O(W)|} \\ &= q^{-s(n-2)} \cdot q^{(s-1)(2n-3)} \cdot \frac{|\,O(\overline{V})|}{|\,O(\overline{W})|} \\ &= q^{-s(n-2)} \cdot q^{(s-1)(2n-3)} \cdot q^{n-2} \cdot s^*(\overline{V}) \\ &= q^{(s-1)(n-1)} \cdot s^*(\overline{V}), \end{aligned}$$

where $\overline{V}, \overline{W}$ are the corresponding reductions modulo $\mathfrak{m}$. The second equality follows from Corollary 2.2.8 and the third equality follows from Fact 2.1.13. Filling in the quantities $s^*(\overline{V})$ from Fact 2.1.12 we arrive at the claim. □

We proceed with $s(V)$. We use the above introduced (cf. 2.3.1) slicing of V.

PROPOSITION 2.3.9. *Let* V *be a regular quadratic* R*-module of rank* n *and with* $\mathrm{ind}(V) = m$. *If* V *is hyperbolic*

$$s_k^*(V) = \begin{cases} (q^m - 1)(q^{m-1} + 1) \cdot q^{kn} \cdot q^{((s-2k)-1)(n-1)} & k < s/2 \\ q^{(s-k-1)n}(q^n - 1) & k \geqslant s/2, \end{cases}$$

$$s(V) = (q^m - 1)(q^{m-1} + 1) \cdot \left(\sum_{k=0}^{\lceil s/2 \rceil - 1} q^{nk} \cdot q^{((s-2k)-1)(n-1)} \right) + q^{(s-\lceil s/2 \rceil)n},$$

if V *is non-hyperbolic of odd rank*

$$s_k^*(V) = \begin{cases} (q^{2m}-1)\cdot q^{kn}\cdot q^{((s-2k)-1)(n-1)} & k < s/2 \\ q^{(s-k-1)n}(q^n-1) & k \geqslant s/2, \end{cases}$$

$$s(V) = (q^{2m}-1)\cdot\left(\sum_{k=0}^{\lceil s/2\rceil-1} q^{nk}\cdot q^{((s-2k)-1)(n-1)}\right) + q^{(s-\lceil s/2\rceil)n},$$

and if V *is non-hyperbolic of even rank*

$$s_k^*(V) = \begin{cases} (q^{m+1}+1)(q^m-1)\cdot q^{kn}\cdot q^{((s-2k)-1)(n-1)} & k < s/2 \\ q^{(s-k-1)n}(q^n-1) & k \geqslant s/2, \end{cases}$$

$$s(V) = (q^{m+1}+1)(q^m-1)\cdot\left(\sum_{k=0}^{\lceil s/2\rceil-1} q^{nk}\cdot q^{((s-2k)-1)(n-1)}\right) + q^{(s-\lceil s/2\rceil)n}.$$

PROOF. We fix $t := \lceil s/2\rceil$. Write $V = \bigcup_{k=0}^{s} V_{(k)}^*$.

First of all we have seen that for $2k \geqslant s$ each of the $q^{(s-k)n}$ distinct elements of $V_{(k)}$ is isotropic (cf. Lemma 2.3.5). Because of $V_{(t)} = \bigcup_{s/2\leqslant k\leqslant s} V_{(k)}^{pr}$, we write $V = \bigcup_{k=0}^{t} V_{(k)}^{pr} \cup V_{(t)}$. This decomposition is disjoint, so we find $s(V) = \sum_{k=0}^{t} s^*(V_{(k)}^{pr}) + s(V_{(t)}) = \sum_{k=0}^{t} s^*(V_{(k)}^{pr}) + q^{(s-t)n}$.

Following Lemma 2.3.5, in the case $2k < s$ a vector $v \in V_{(k)}^*$ is isotropic if and only if the corresponding $\overline{v} \in \overline{V_{(k)}}$ satisfies $\overline{q}(\overline{v}) = 0$ (here we work with the reduction modulo $\mathfrak{m}^{r-2k}/\mathfrak{m}^{r-k}$).

By construction of $\overline{V_{(k)}}$, each primitive isotropic vector in $\overline{V_{(k)}}$ represents $q^{(s-k)n}/q^{(s-2k)n} = q^{kn}$ distinct isotropic elements in $V_{(k)}^{pr}$. This states that there are $q^{kn}\cdot s^*(\overline{V_{(k)}})$ isotropic vectors in $V_{(k)}^{pr}$. But $\overline{V_{(k)}}$ is regular, as noted after its construction, so we already know the quantities $s^*(\overline{V_{(k)}})$ by Proposition 2.3.8.

Since $\overline{V_{(k)}}$ is hyperbolic if and only if $V_{(k)}$ is hyperbolic if and only if V is hyperbolic, we arrive at

$$s(V) = s^*(\overline{V})\cdot\left(\sum_{k=0}^{t-1} q^{kn}\cdot q^{((s-2k)-1)(n-1)}\right) + q^{(s-t)n}. \qquad \square$$

2.4 A CLASSIFICATION OF MAXIMAL TOTALLY ISOTROPIC SUBMODULES OF REGULAR QUADRATIC MODULES OVER FINITE LOCAL RINGS

Throughout this Section R will be a finite local ring of cardinality s, with maximal ideal $\mathfrak{m}$ and corresponding nilpotency index r, if not specified otherwise.

2.4.1 Reduction of the general case

As in the case of isometry above, the problem of identifying maximal totally isotropic submodules obeys to the local-global principle of Theorem 2.2.2.

PROPOSITION 2.4.1. *Let* R *be a finite ring with spectrum* $\operatorname{spec} R = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_l\}$. *Let* (V, q) *be a quadratic* R*-module, and let* M *be a submodule. Then*

$$M \cong \prod_{i=1}^{l} M_{\mathfrak{m}_i} \cong \prod_{i=1}^{l} M/\mathfrak{m}_i.$$

M *is (maximal) totally isotropic if and only if* $M_{\mathfrak{m}}$ *is (maximal) totally isotropic in* $(V_{\mathfrak{m}}, q_{\mathfrak{m}})$ *for all* $\mathfrak{m} \in \operatorname{spec} R$.

PROOF. The decomposition of M into local factors and quotient rings is clear since it holds for all finitely generated modules over R. Since a module (M, q) is totally isotropic if and only if it is isometric to $(M, 0)$, where 0 is the trivial quadratic form, and since $(M, 0)_{\mathfrak{m}} = (M_{\mathfrak{m}}, 0)$ for all maximal ideals, the assertion of the Proposition follows by *ii.* of Theorem 2.2.2. □

2.4.2 A structure theorem for maximal totally isotropic submodules of regular modules over finite rings

We achieve a complete classification of maximal totally isotropic submodules of regular modules over the finite ring R by a structural decomposition of any such submodule M into blocks that are supported on a rank 2 submodule. This is the main result of this Chapter and its proof will be given in quite some detail.

We fix some notation: Let M be a maximal totally isotropic submodule of V. We let

$$\nu_M := \min\left\{ \ \nu_{\mathfrak{m}}(m) \ \middle| \ m \in M : \ q(m) = 0 \ \right\}$$

denote the minimal $\mathfrak{m}$-order of an isotropic element in M.

DEFINITION 2.4.2. Let $H = Re + Rf \cong \mathbb{H}$ be a hyperbolic plane over R, where (e, f) is a hyperbolic pair. Then $M = \mathfrak{m}^k e + \mathfrak{m}^{r-k} f$ is a maximal totally isotropic submodule. We write $H_{e,f}(k) = H_{e,f}(\nu_M)$ for this submodule. If we are interested in a representative of an M as such up to isometry, we will use the notation $\mathbb{H}(k)$. ◆

EXAMPLE 2.4.3. Let (V, q) be a regular free quadratic module. We can construct examples of maximal totally isotropic submodules from rank-two building blocks.

i. Let $V = H_1 \perp \ldots \perp H_m$, with $H_i = Re_i + Rf_i \cong \mathbb{H}$ and (e_i, f_i) hyperbolic pairings. Let $0 \leqslant k_1, \ldots, k_m \leqslant \lceil \frac{r}{2} \rceil$ be integers. Then $M := H_{1\,e_1,f_1}(k_1) \perp \ldots \perp H_{m\,e_m,f_m}(k_m)$ is a maximal totally isotropic submodule.
ii. Let $V = H_1 \perp \ldots \perp H_m \perp W$, with $H_i = Re_i + Rf_i \cong \mathbb{H}$ and e_i, f_i hyperbolic pairings, W non-hyperbolic, free regular of rank 1 or 2. Let $0 \leqslant k_1, \ldots, k_m \leqslant \lceil \frac{r}{2} \rceil$ be integers. Then $M := H_{1\,e_1,f_1}(k_1) \perp \ldots \perp H_{m\,e_m,f_m}(k_m) \perp \mathfrak{m}^{\lceil r/2 \rceil} W$ is a maximal totally isotropic submodule.

We will not dwell on providing a proof, for the maximality of the submodules above, here. This will be proven along the lines of the proof of the structural decomposition Theorem in 2.4.3. ■

This example already contains a representative for each isometry class of maximal totally isotropic submodules of free regular quadratic modules over R. This is made precise in the main Theorem of this Chapter, which gives a structural decomposition of any maximal totally isotropic submodule, which looks as the examples above.

THEOREM 2.4.4 (STRUCTURAL DECOMPOSITION FOR MAXIMAL TOTALLY ISOTROPIC SUBMODULES). *Let* R *be a finite local ring with maximal ideal* $\mathfrak{m}$ *and corresponding nilpotency index* r. *Let* V *be a free regular quadratic module over* R, *with* $\operatorname{ind}(V) = m$. *Let* M *be a maximal totally isotropic submodule of* V. *Then there exists a (unique) sequence* $\nu_M = k_1 \leqslant \ldots \leqslant k_m \leqslant \lceil \frac{r}{2} \rceil$ *together with a decomposition of* V *into hyperbolic planes* $H_i = Re_i + Rf_i$, *and possibly some non-hyperbolic module* W *of rank* 1 *or* 2, *such that:*

I) V *is hyperbolic* ($\operatorname{rk}(V) = 2m$) *and*

$$V = H_1 \perp \ldots \perp H_m$$
$$M = H_{1\,e_1,f_1}(k_1) \perp \ldots \perp H_{m\,e_m,f_m}(k_m),$$

II) V *is non-hyperbolic* ($\operatorname{rk}(V) = 2m+1$ *or* $\operatorname{rk}(V) = 2m+2$) *and*

$$V = H_1 \perp \ldots \perp H_m \perp W$$
$$M = H_{1\,e_1,f_1}(k_1) \perp \ldots \perp H_{m\,e_m,f_m}(k_m) \perp \mathfrak{m}^{\lceil r/2 \rceil} W.$$

DEFINITION 2.4.5. Let V be a free regular quadratic module over R and $M \subset V$ be a maximal totally isotropic submodule. We define the **type** of M to be the sequence

$$[k_1, \ldots, k_m], \text{ if } V \text{ is hyperbolic,}$$

or

$$[k_1, \ldots, k_m, \lceil r/2 \rceil], \text{ if } V \text{ is non-hyperbolic,}$$

where the integers $\nu_M = k_1 \leqslant \ldots \leqslant k_m \leqslant \lceil \frac{r}{2} \rceil$ are those obtained from Theorem 2.4.4. ◆

REMARK 2.4.6. It is quite clear that the notion of type as defined above is well-defined. For if

$$M \cong \mathbb{H}(k_1) \perp \ldots \perp \mathbb{H}(k_m) \perp W'$$

and $M \cong \mathbb{H}(l_1) \perp \ldots \perp \mathbb{H}(l_m) \perp W'$ for admissible sequences $[k_1, \ldots, k_m]$, $[l_1, \ldots, l_m]$, the equality $[k_1, \ldots, k_m] = [l_1, \ldots, l_m]$ is inevitable. To see this consider the first index j from the left where $k_j \neq l_j$, w.l.o.g. we assume $k_j > l_j$. Then it is easy to see that the number of elements with $\mathfrak{m}$-order k_j in $\mathbb{H}(k_1) \perp \ldots \perp \mathbb{H}(k_m) \perp W'$ would be strictly larger than the number of such elements in $\mathbb{H}(l_1) \perp \ldots \perp \mathbb{H}(l_m) \perp W'$, while both are isometric to M. This is absurd. ■

The discussion of the examples in 2.4.3 and the structural decomposition Theorem 2.4.4 immediately characterizes the set of possible types of a given free regular quadratic module V over R.

COROLLARY 2.4.7. *Let* V *be a regular quadratic module over* R *with* $\operatorname{ind}(V) = m$.

i) If V *is hyperbolic, a sequence* $[\nu_1, \ldots, \nu_m]$ *is the type of a maximal totally isotropic submodule of* V *if and only if* $\nu_i \in \{0, \ldots, \lceil r/2 \rceil\}$ *is a non decreasing sequence.*

ii) If V *is non-hyperbolic, a sequence* $[\nu_1, \ldots, \nu_m, \lceil \nu_{m+1} \rceil]$ *is the type of a maximal totally isotropic submodule of* V *if and only if* $\nu_{m+1} = \lceil r/2 \rceil$ *and* $\nu_i \in \{0, \ldots, \lceil r/2 \rceil\}$ *is a non decreasing sequence.*

As mentioned before, the case of primitive maximal totally isotropic submodules over local rings is not much different from the situation over fields. In particular, their rank is an invariant (cf. Corollary 2.1.8), equal to $\operatorname{ind}(V)$.

COROLLARY 2.4.8. *Let* V *be a regular quadratic module over a finite local principal ideal ring* R*, and let* M *be a maximal totally isotropic submodule of type* $\mathbf{t}$.

i. If r *is even, then* $|M| = q^{r(n/2)}$.

ii. If r *is odd, then*

II.1) $|M| = q^{(r-1)/2} \cdot q^{r(n-1/2)}$,

II.2) $|M| = q^{(r-1)} \cdot q^{r((n/2)-1)}$.

In particular $|M| = q^{s(n/2)}$ *if and only if* r *is even or if* M *is hyperbolic.*

Furthermore, it is an easy consequence of the fact that $O(V)$ acts transitively on the set of primitive isotropic elements (cf. Lemma 2.3.7) that all primitive maximal totally isotropic submodules lie in one orbit under the action of $O(V)$. This situation generalizes to non-primitive maximal totally isotropic submodules.

COROLLARY 2.4.9. *Let* V *be a regular quadratic module over* R *and let* $\mathbf{t}$ *be a type of* V*. Then for any maximal totally isotropic submodules* M, M' *of type* $\mathbf{t}$ *there exists* $\phi \in O(V)$ *such that* $\phi(M) = M'$.

2.4.3 The proof of the structural decomposition Theorem

We will work through the proof of the structural decomposition Theorem in several steps. We start with the description of the maximal totally isotropic submodules of the regular free non-hyperbolic and hyperbolic modules of rank 1 and 2 in Lemmata 2.4.10 and 2.4.11. The general situation will then be reduced to these. To do so, Lemma 2.4.14 provides a way to split off some $\mathbb{H}(k)$ from a given M. This can be done in such a way that $M \cong \mathbb{H}(k) \perp M'$, where M' is a maximal totally isotropic submodule of a free regular quadratic module V', which is Witt-equivalent to V and satisfies $\mathrm{rk}(V') = \mathrm{rk}(V) - 2$.

LEMMA 2.4.10. *Let* W *be a non-hyperbolic regular quadratic module of rank* 1 *or* 2 *over* R*. Then*

i. $w \in W$ *is isotropic if and only if* $\nu_{\mathfrak{m}}(w) \geqslant \lceil r/2 \rceil$*, that is,* $w \in \mathfrak{m}^{\lceil r/2 \rceil}W$.

ii. $\mathfrak{m}^{\lceil r/2 \rceil}W$ *is the unique maximal totally isotropic submodule of* W.

PROOF. It is clear that W has no primitive isotropic elements, for those would project to primitive isotropic elements of $\overline{W}$, which itself is an anisotropic space. Along the same lines we conclude that $q(w) \in R^\times$ for all primitive $w \in W$; if $w \in W$ with $q(w) \in R\backslash R^\times = \mathfrak{m}$, then w is isotropic modulo $\mathfrak{m}$ and therefore $\overline{w}$ is the zero element of $\overline{W}$, thus w cannot be primitive.

If $w \in \mathfrak{m}^k W$ is isotropic, we write $w = \mu^k w'$ with w' primitive and $\mu \in \mathfrak{m}\backslash\mathfrak{m}^2$. Then $q(w) = \mu^{2k} q(w')$. Since $q(w') \in R^\times$ we have $\nu_{\mathfrak{m}}(q(w)) = 2k$. So necessarily $k \geqslant r/2$ if $q(w) = 0$.

Clearly $\mathfrak{m}^{\lceil r/2 \rceil}W$ is a totally isotropic subspace and, by the above, there are no isotropic elements in $W\backslash\mathfrak{m}^{\lceil r/2 \rceil}W$. This completes the proof. □

Having settled the non-hyperbolic case of rank 1 and 2, we deal with the second basic building block, hyperbolic planes.

LEMMA 2.4.11. *Let $\mathbb{H}$ be a hyperbolic plane over* R*. Let* M *be a maximal totally isotropic submodule of* M *and let $x \in M$ be such that $k := \nu_{\mathfrak{m}}(x) = \nu_M$. Then there exists a hyperbolic pair (e, f) such that*

i. $\mathbb{H} = Re + Rf$,

ii. $M = \mathbb{H}_{e,f}(k) = \mathfrak{m}^k e + \mathfrak{m}^{r-k} f$.

PROOF. Let x' be primitive in $\mathbb{H}$, so that $x = \lambda x'$ for $\lambda \in \mathfrak{m}^k$.

Given x' (not necessarily isotropic itself), there exists some primitive isotropic element $f \in \mathbb{H}$, such that $b(x', f) = 1$. For if we choose any isotropic basis h_1, h_2 of $\mathbb{H}$, non-existence of an f as proposed would mean that $b(f, h_i) \in \mathfrak{m}$, a contradiction to the regularity of $\mathbb{H}$.

We now show that $M = \mathfrak{m}^k x' + \mathfrak{m}^{r-k} f$. If $k = 0$ this is clear since every primitive isotropic element x of $\mathbb{H}$ is contained in a uniquely determined maximal totally isotropic submodule Rx, as in the case of a field.

If $k > 0$, we see that $\alpha x' \notin M$ for all $\alpha \in R \backslash \mathfrak{m}^k$, since $\nu_{\mathfrak{m}}(\alpha x') = \nu_{\mathfrak{m}}(\alpha) < k = \nu_{\mathfrak{m}}(M)$ would be a contradiction. Now the submodule $Rx \subsetneq M$, because Rx is not maximal totally isotropic. In fact let $\alpha \in \mathfrak{m}^k$, $\beta \in \mathfrak{m}^{r-k}$, then $q(\beta f) = 0$, and $q(\alpha x' + \beta f) = \alpha\beta \in \mathfrak{m}^r = \{0\}$, showing $Rx = \mathfrak{m}^k x' \subsetneq \mathfrak{m}^k x' + \mathfrak{m}^{r-k} f$, where the latter submodule is totally isotropic. Therefore, there exists $y \in M \backslash Rx$. Write $y = \alpha x' + \beta f$. Since $\nu_{\mathfrak{m}}(M) = k$, it follows that $\alpha, \beta \in \mathfrak{m}^k$. But then $\beta f = y - \alpha x' \in M$ and therefore $\mathfrak{m}^k x' + R\beta f \subset M$. In particular, for some $\mu \in \mathfrak{m} \backslash \mathfrak{m}^2$ we set $z := \mu^k x' + \beta f \in M$ and obtain $q(z) = \mu^k \beta = 0$, showing $\beta \in \mathfrak{m}^{r-k}$. Therefore $y \in \mathfrak{m}^k x' + \mathfrak{m}^{r-k} f$ and thus $M \subset \mathfrak{m}^k x' + \mathfrak{m}^{r-k} f$. But since the latter is a totally isotropic subspace and M is a maximal totally isotropic subspace it follows that equality holds.

We now show that there is a hyperbolic pair (e, f) such that $M = \mathfrak{m}^k x' + \mathfrak{m}^{r-k} f = \mathfrak{m}^k e + \mathfrak{m}^k f$. Suppose that x' is not isotropic itself, otherwise $e := x'$ and f are a basis as desired. Since x', f are a basis of $\mathbb{H}$, so is $x' + \beta f, f$, for $\beta \in R$. Then

$$q(x' + \beta f) = q(x') + \beta^2 q(f) + \beta \cdot b_q(x', f) = q(x') + 0 + \beta \cdot 1 = q(x') + \beta$$

implies, that with $e := x' - q(x')f$, we arrive at a hyperbolic pair (e, f). We claim that $\lambda e \in M$. To see this note that $q(x') \in \mathfrak{m}^{r-2k}$ because otherwise

$$\nu_{\mathfrak{m}}(q(x)) = \nu_{\mathfrak{m}}(q(\lambda x')) = \nu_{\mathfrak{m}}(\lambda^2) + \nu_{\mathfrak{m}}(q(x')) < 2k + r - 2k = r,$$

contradicting $q(x) = 0$. Thus $\lambda e = \lambda x' - (\lambda q(x'))f \in \mathfrak{m}^k x' + \mathfrak{m}^{r-k} f = M$, since $\nu_{\mathfrak{m}}(\lambda q(x')) \geqslant k + r - 2k = r - k$. It now follows that $\mathfrak{m}^k e + \mathfrak{m}^{r-k} f = \mathfrak{m}^k x' + \mathfrak{m}^{r-k} f = M$. □

This settles the problem for the rank 1 and 2 modules. We proceed by a reduction of the general situation to the rank 1 and 2 case.

LEMMA 2.4.12. *Let* V *be a regular quadratic module over* R*, such that* $\mathrm{rk}(V) \geqslant 3$*. Then there exists a basis consisting of isotropic elements.*

PROOF. This clearly is true if V is hyperbolic. So assume that V is not hyperbolic and write $n := \mathrm{rk}(V)$ and $V = \mathbb{H}_1 \perp \ldots \perp \mathbb{H}_s \perp W$, where W is a regular non-hyperbolic quadratic module of rank 1 or 2. We concatenate a basis $h_1, \ldots, h_{n-2}$ of the hyperbolic part and a basis of W, to obtain a basis derived from the decomposition in an obvious way. W.l.o.g. we can assume that $q(h_i) = 0$ for all indices i. By assumption at least one hyperbolic plane splits V, and by its universality we can, for each w in a basis of W, choose some $h_w \in \mathbb{H}$ such that $q(h_w) = -q(w)$. Replacing w by $w + h_w$ in the above basis we arrive at a basis composed of isotropic elements. □

LEMMA 2.4.13. *Let* V *be a regular quadratic module over* R*, such that* $\mathrm{rk}(V) \geqslant 3$*. Let* $x \in V$ *be primitive, such that* λx *is isotropic for some* λ *with* $\nu_{\mathfrak{m}}(\lambda) < \frac{r}{2}$*. Then there exists a submodule* $H = Rx + Rv$ *that splits* V*, such that* $H \cong \mathbb{H}$*,* $x \in H$*,* $b_q(x, v) = 1$*, and* $q(v) = 0$ *are satisfied.*

PROOF. Choose some primitive isotropic $v \in V$ that satisfies $b_q(x, v) = 1$. Such an element has to exist, since there is some isotropic basis of V by Lemma 2.4.12 and the regularity of V does not allow that $b_q(x, v) \in \mathfrak{m}$ for all v in such a basis.

Set $H := Rx + Rv$. This is a regular submodule, where the regularity can be checked by computing the determinant of H to be equal to -1. A regular quadratic module of rank 2, which by assumption contains the isotropic element $\lambda x \in H$ with $\nu_{\mathfrak{m}}(\lambda x) < \frac{r}{2}$, can not be non-hyperbolic as noted in Lemma 2.4.10. Therefore, $H \cong \mathbb{H}$ and H splits V. □

LEMMA 2.4.14. *Let* V *be a regular quadratic module over* R*, such that* $\mathrm{rk}(V) \geqslant 3$*. Let* M *be a maximal totally isotropic submodule of* V*. Then there exists some hyperbolic plane* $H \subset V$*, with corresponding splitting* $V = H \perp V'$*, such that*

i. $M = H' \perp M'$*, where* $H' \subset H$ *and* $M' \subset V'$*.*

ii. $H' = M \cap H$ *is a maximal totally isotropic submodule of* H *and* $\nu_{M \cap H} = \nu_M$*,*

iii. $M' = M \cap V'$ *is a maximal totally isotropic submodule of* V' *and* $\nu_{M \cap V'} \leqslant \nu_M$*.*

PROOF. Assume that $\nu_M < \frac{r}{2}$, because otherwise $M \subset \mathfrak{m}^{\lceil r/2 \rceil} V$, where the latter is totally isotropic, thus implying equality and the claim holds by Witt decomposition of V.

If $k := \nu_M < \frac{r}{2}$, there is some $x \in M$ with $\nu_{\mathfrak{m}}(x) = \nu_M = k < \frac{r}{2}$, so there exist a $\lambda \in R$ and a primitive $x' \in V$ with $\nu_{\mathfrak{m}}(\lambda) = k < \frac{r}{2}$ such that $x = \lambda x'$. Using Lemma 2.4.13 we find $H = Rx' + Rv \subset V$ hyperbolic such that $x' \in H$, v is isotropic and $V = H \perp V'$.

STEP 1: We show that $\mathfrak{m}^k V \cap x^\perp = H' \perp \mathfrak{m}^k V'$, where $H' = \mathfrak{m}^k x' + \mathfrak{m}^{r-k} v$ is a maximal totally isotropic submodule of H.

Since $\mathfrak{m}^k V' \subset \mathfrak{m}^k V \cap x^\perp$, we can write $\mathfrak{m}^k V \cap x^\perp = \mathfrak{m}^k H \cap x^\perp \perp \mathfrak{m}^k V'$. We are left to show that $\mathfrak{m}^k H \cap x^\perp = \mathfrak{m}^k x' + \mathfrak{m}^{r-k} v$, where the "$\supset$" inclusion is straightforward.

Towards the "$\subset$" inclusion we choose $y \in \mathfrak{m}^k H = \mathfrak{m}^k x' + \mathfrak{m}^k v$ with $b_q(x, y) = 0$. We can write $y = \alpha\mu_1 x' + \beta\mu_2 v$ with $\mu_1, \mu_2 \in \mathfrak{m}^k \backslash \mathfrak{m}^{k+1}$, whence

$$0 = b_q(x, y) = b_q(\lambda x', \alpha\mu_1 x' + \beta\mu_2 v) = \alpha b_q(\lambda x', \mu_1 x') + \lambda\beta\mu_2 b(x', v) = \lambda\mu_2\beta.$$

Only the last equality needs some justification: by choice of x we have $b_q(x, x) = 2q(x) = 0$. Now $b_q(x, x) = b_q(\lambda x', \lambda x')$ and for this to equal 0 necessarily $\nu_{\mathfrak{m}}(b_q(x', x')) \geqslant r - 2\nu_{\mathfrak{m}}(\lambda) = r - 2k$ has to hold, so $b_q(x', x') \in \mathfrak{m}^{r-2k}$. But then also $b_q(\lambda x', \mu_1 x') = \lambda\mu_1 b(x', x') \in \mathfrak{m}^k \cdot \mathfrak{m}^k \cdot \mathfrak{m}^{r-2k} = \{0\}$. Furthermore $b_q(x', v) = 1$ by construction of H (cf. Lemma 2.4.13). Having justified this, we observe that clearly $\lambda\mu_1\beta = 0$ if and only if $\beta \in \mathfrak{m}^{r-2k}$ if and only if $\beta\mu_1 \in \mathfrak{m}^{r-k}$. Maximality of H' follows from the classification made in Lemma 2.4.11. This concludes the first step.

STEP 2: We show that $M \subset H' \perp \mathfrak{m}^k V'$.

It is clear that $M \subset x^\perp$, and by assumption $M \subset \mathfrak{m}^k V$. Thus $M \subset \mathfrak{m}^k V \cap x^\perp$. By the identity

$$\mathfrak{m}^k V \cap x^\perp = H' \perp \mathfrak{m}^k V',$$

which was proved in STEP 1, we therefore obtain $M \subset H' \perp \mathfrak{m}^k V'$. This concludes the second step.

STEP 3: We show that $H' \subset M$.

For $y \in H'$ we find $M \subset Ry + M$. We claim that $Ry + M$ is totally isotropic, which then implies equality by the maximality of M. Take any element $\alpha y + m$ where $m \in M$ can be written as $m = h + v$ with $h \in H'$ and $v \in \mathfrak{m}^k V'$. Then

$$q(\alpha y + m) = b_q(\alpha y, m) = b_q(\alpha y, h + v) = b_q(\alpha y, h) + b_q(\alpha y, v) = q(\alpha y + h) = 0,$$

where $b_q(\alpha y, v) = 0$ by the orthogonality of H' and V'. Furthermore, $\alpha y, h \in H'$, so $\alpha y + h \in H'$ and $0 = q(\alpha y + h) = b(\alpha y, h)$ by the total isotropy of H'. This concludes the third step.

STEP 4: We show that $M = H' \perp M'$, where $M' := M \cap \mathfrak{m}^k V' \subset V'$ is a maximal totally isotropic submodule of V'.

By step 2 we can write an $m \in M$ as $m = h + v$ with $h \in H'$ and $v \in \mathfrak{m}^k V'$. By the inclusion $H' \subset M$ of step 3 then also $v = m - h \in M$. With $M' := M \cap \mathfrak{m}^k V' \subset V'$ we obtain $M = H' \perp M'$. H' is maximal totally isotropic in H by step 1. Furthermore M' is totally isotropic with $\nu_{M'} \geqslant \nu_M$, and in fact, M' is a maximal totally isotropic submodule of V', because for totally isotropic $M'' \subset V'$ with $M' \subset M''$ we have $M \subset H' + M''$, where the maximality of M forces equality and shows $M' = M''$. This concludes the fourth step.

Conclusion of the proof:

We just established that $M = H' \perp M'$ with $H' = M \cap H \subset H$ maximal totally isotropic by step 1 and $M' = M \cap V' \subset V'$ maximal totally isotropic by step 5. This concludes the proof. □

Before we go on to put all pieces together and give a proof of Theorem 2.4.4, we formulate a Corollary to the preceding Lemma which will be of use later on (cf. Lemma 2.5.2).

COROLLARY 2.4.15. *Let V be a regular quadratic module over R and let M be a maximal totally isotropic submodule. Let $x \in M$, such that $\nu_m(x) = \nu_M$ and that there exists a hyperbolic plane H containing x. Then $V = H \perp V'$ with V, V' Witt-equivalent, and $M = H(\nu_M) \perp M'$, where M' is a maximal totally isotropic submodule of V'.*

PROOF OF THEOREM 2.4.4. We start with the existence of a decomposition as claimed. If $\mathrm{rk}(V) \leqslant 2$ this is covered by the Lemmata 2.4.10 and 2.4.11.

If $\mathrm{rk}(V) \geqslant 3$ we proceed by induction with Lemma 2.4.14: We write $V = H \perp V'$ and see that $M = M \cap H \perp M \cap V'$ where $H' = M \cap H$ and $M' = M \cap V'$ are maximal totally isotropic subspaces of H and V'. By Lemma 2.4.11, $H' = H(\nu_M) \cong \mathbb{H}(\nu_M)$. Furthermore since V and V' are Witt-equivalent and since $\mathrm{rk}(V') = \mathrm{rk}(V) - 2$ we inductively get

$$M' = H_2(k_2) \perp \ldots \perp H_m(k_m), \text{ or}$$
$$M' = H_2(k_2) \perp \ldots \perp H_m(k_m) \perp \mathfrak{m}^{\lceil r/2 \rceil} W,$$

depending on V being hyperbolic or not.

Uniqueness of a decomposition as such, up to isometry, was already discussed in Remark 2.4.6. □

2.5 COUNTING MAXIMAL TOTALLY ISOTROPIC SUBMODULES OF QUADRATIC MODULES OVER FINITE PRINCIPAL IDEAL RINGS

Let R be a finite principal ideal ring. Let $M(V)$ denote the set of all maximal totally isotropic submodules of V and let $M(V, \mathbf{t})$ denote the set of maximal totally isotropic submodules of V, that are of type $\mathbf{t}$. We set $m(V) := |M(V)|$ and $m(V, \mathbf{t}) := |M(V, \mathbf{t})|$.

2.5.1 Reduction of the general case

Employing the results on the decomposition of modules over finite rings, we immediately derive the following multiplicativity result.

PROPOSITION 2.5.1. *Let (V, q) be a regular quadratic module over R. Then*

$$m((V, q)) = \prod_{\mathfrak{m} \in \operatorname{spec} R} m((V_\mathfrak{m}, q_\mathfrak{m})),$$

where $m((V_\mathfrak{m}, q_\mathfrak{m}))$ is the number of maximal totally isotropic submodules of the regular quadratic $R_\mathfrak{m}$-module $(V_\mathfrak{m}, q_\mathfrak{m})$.

PROOF. This follows directly from Proposition 2.4.1. □

2.5.2 The case of a finite local principal ideal ring

Let R be local in addition to the assumptions already made. Let $\mathfrak{m}$ be the maximal ideal of R. Then if $|R| = q^s$, we find that $s = r$, where r is the nilpotency index of $\mathfrak{m}$. To compute the number of maximal totally isotropic submodules of regular quadratic modules over R we compute the number of maximal totally isotropic submodules of a given type, followed by summation over all different types.

Let $s^*_{t_1}(V)$ denote the number of isotropic elements of V with $\mathfrak{m}$-order $t_1 = \nu_1$, and let $s^*_{t_1}(\mathbf{t})$ denote the number of isotropic elements with $\mathfrak{m}$-order t_1 in a maximal totally isotropic submodule of type $\mathbf{t}$.

LEMMA 2.5.2. *Let V be a regular quadratic module over R and let $\mathbf{t}$ be a type. Let M be of type $\mathbf{t}$ and write $V = H \perp V'$, $M = H(t_1) \perp M'$ as in Lemma 2.4.14. The number of maximal totally isotropic subspaces of type $\mathbf{t}$ obeys to the recursion*

$$m(V, \mathbf{t}) = \frac{s^*_{t_1}(V)}{s^*_{t_1}(\mathbf{t})} \cdot m(V', \mathbf{t}'),$$

where $\mathbf{t}'$ is the type of M'.

PROOF. Let $x \in S^*_{\nu_1}(V)$, and let H be any hyperbolic plane in V that contains x (as is given by Lemma 2.4.13) and write $V = H \perp V'$. Let $N \subset M(V, \mathbf{t})$ be composed of those maximal totally isotropic spaces of type $\mathbf{t}$ that contain x. By Corollary 2.4.15 we can write any $M \in N$ as $M = H(\nu_1) \perp M'$ where M' is a maximal totally isotropic submodule of V'. Then M' is of type $\mathbf{t}' := [t_2, \ldots, t_{n/2}]$ by the uniqueness of type (cf. Theorem 2.4.4). So there are exactly $m(V', \mathbf{t}')$ distinct elements of $M(V, \mathbf{t})$ that contain x.

Of course $m(V', \mathbf{t}')$ does not depend on V' itself, but only on the Witt-equivalence class of V' and its rank.

If we do so for all of the $s^*_{t_1}(V)$ elements of $S^*_{t_1}(V)$, we meet each element $M \in M(V, \mathbf{t})$ exactly $s^*_{t_1}(\mathbf{t})$ times: Once for each isotropic element $x \in M$ with $\nu(x) = t_1$, of which there are $s^*_{t_1}$ by definition of this quantity.

But this translates to $m(V, \mathbf{t}) \cdot s^*_{t_1}(\mathbf{t}) = s^*_{t_1}(V) \cdot m(V', \mathbf{t}')$ and therefore proves the claim. □

So we are left with the need to compute the quantities $s^*_{t_1}(\mathbf{t})$ and $s^*_{t_1}(V)$, in order to be able to compute $m(V, \mathbf{t})$. The latter one is given in Proposition 2.3.9, the former one is calculated below.

We fix some notation. Given a type $\mathbf{t} = [t_1, \ldots, t_{n/2}]$ for some V with $\operatorname{ind}(V) = m$, let $(s_1, \ldots, s_a)$ be the sequence of numbers that indicate how many consecutive entries of $\mathbf{t}$ are equal before each increment that does not reach $\frac{r}{2}$ and let $s = s_1 + \ldots + s_a$. That is,

$$t_1 = \ldots = t_{s_1} < t_{s_1+1} = \ldots = t_{s_1+s_2} < \ldots < t_{s_1+\ldots s_{a-1}+1} = \ldots = t_s < \frac{r}{2}.$$

Then we have that $s \leqslant m$ and $m' := \lceil n/2 \rceil - s$ is exactly the number of entries of t equal to $\lceil \frac{r}{2} \rceil$. Furthermore, we set $t^{(j)} := t_{s_1+\ldots+s_{j-1}+1}$, that is, $t^{(j)}$ picks out the j-th smallest value of $\mathbf{t}$.

REMARK 2.5.3. For a type $\mathbf{t}$ of a regular quadratic R-module V certain restrictions apply for the numbers s, m'. These are:

i. V hyperbolic, r odd: $s = m$, $m' = 0$;
ii. V hyperbolic, r even: $0 \leqslant s \leqslant m$, $0 \leqslant m' \leqslant m$, such that $s + m' = m$;
iii. V non-hyperbolic, r odd: $s = m$, $m' = 1$;
iv. V non-hyperbolic, r even: $0 \leqslant s \leqslant m$, $1 \leqslant m' \leqslant m+1$, such that $s + m' = m + 1$.

■

LEMMA 2.5.4. *Let V be a regular quadratic module over R, and let $\mathbf{t}$ be a type of V. Then if $t_1 < \lceil \frac{r}{2} \rceil$:*

$$\text{I) } s^*_{t_1}(\mathbf{t}) = q^{rm}(1 - q^{-s_1}),$$
$$\text{II.1) } s^*_{t_1}(\mathbf{t}) = q^{rm}(1 - q^{-s_1}) \cdot q^{\lfloor r/2 \rfloor},$$
$$\text{II.2) } s^*_{t_1}(\mathbf{t}) = q^{rm}(1 - q^{-s_1}) \cdot q^{2\lfloor r/2 \rfloor}.$$

If $t_1 = \lceil \frac{r}{2} \rceil$, then $M = \mathfrak{m}^{\lceil r/2 \rceil} V$ and therefore $s^*_{t_1}(\mathbf{t}) = s^*_{\lceil r/2 \rceil}(V)$.

PROOF. Let $M \subset V$ be a maximal totally isotropic subspace of type $\mathbf{t}$, and let $m = \operatorname{ind}(V)$. We use Theorem 2.4.4 to obtain a decomposition $V = H_1 \perp \ldots \perp H_s \perp V'$, where $V' \cap M = \mathfrak{m}^{\lceil r/2 \rceil} V'$ and we write $n' = \operatorname{rk}(V') = n - 2s$. Therefore, we can find a basis $e_1, f_1, \ldots, e_s, f_s, v_1, \ldots, v_{n'}$ of V (each $Re_i + Rf_i \cong \mathbb{H}$, $V' = Rv_1 \oplus \ldots \oplus Rv_{n'}$) in which

$$M = M_{s_1} \perp M_{s-s_1} \perp M_{m'}$$

where

$$\begin{aligned} M_{s_1} &= \mathfrak{m}^{t(1)}e_1 + \mathfrak{m}^{r-t(1)}f_1 + \ldots + \mathfrak{m}^{t(s_1)}e_{s_1} + \mathfrak{m}^{r-t(s_1)}f_{s_1}, \\ M_{s-s_1} &= \mathfrak{m}^{t(s_1+1)}e_{s_1+1} + \mathfrak{m}^{r-t(s_1+1)}f_{s_1+1} \ldots + \mathfrak{m}^{t(s)}e_s + \mathfrak{m}^{r-t(s)}f_s, \\ M_{m'} &= \mathfrak{m}^{\lceil r/2 \rceil}V'. \end{aligned}$$

For $x \in M$ we accordingly write $x = x_{s_1} + x_{s-s_1} + x_{m'}$. Such x is primitive relative to M, i.e., a member of $S^*_{t_1}(\mathbf{t})$, if and only if x_{s_1} is primitive relative to M, i.e., if and only if

$$x_{s_1} = \alpha_1 \mu_{e_1}^{t_1} e_1 + \beta_1 \mu_{f_1}^{r-t_1} f_1 + \ldots + \alpha_{s_1} \mu_{e_{s_1}}^{t_{s_1}} e_1 + \beta_{s_1} \mu_{f_{s_1}}^{r-t_{s_1}} f_{s_1},$$

where $\mu_{e_i}, \mu_{f_i} \in \mathfrak{m} \backslash \mathfrak{m}^2$, with at least one $\alpha_i \in R^\times$.

There is a total of $q^{(r-1)s_1}$ elements of M_{s_1} that are not primitive relative to M. This follows from the observation that for the s_1 hyperbolic pairs (e_i, f_i) that span M_{s_1} we may not use a unit α_i. This leaves us with $q^{(r-1)}$ different possibilities to choose $\alpha \in R \backslash R^\times = \mathfrak{m}$. These scalars then amount to $q^{(r-1)-t_1}$ distinct elements $\alpha \mu_{e_i}^{t_1} e_i$ for each primitive e_i. To such an α_i we can choose an arbitrary $\beta \in R$, giving q^{t_1} distinct elements $\beta \mu_{f_i}^{t_1} f_i$ for each primitive f_i. In total, each pair (e_i, f_i) thus contributes to $q^{(r-1)-t_1} \cdot q^{t_1} = q^{r-1}$ different elements of M_{s_1} not primitive relative to M.

Since in the above decomposition of x, the summands x_{s-s_1} and $x_{m'}$ can be chosen arbitrarily and since $|M_{s-s_1}| = q^{r(s-s_1)}$, $|M_{m'}| = q^{n' \lfloor r/2 \rfloor}$, we have a total of

$$\left(q^{rs_1} - q^{(r-1)s_1}\right) \cdot q^{r(s-s_1)} \cdot q^{n' \lfloor r/2 \rfloor}$$

elements in $S^*_{t_1}(\mathbf{t})$. Depending on the parity of r and whether $n' = 2m'$ or $n' = 2m' - 1$ this can be simplified to the formulation in the Lemma. $\square$

We now can compute $m(V, \mathbf{t})$ for given V and $\mathbf{t}$.

PROPOSITION 2.5.5. *Let V be a regular quadratic module over R, with $\operatorname{ind}(V) = m$. Then:*

if V is hyperbolic

$$\begin{aligned} m(\mathbb{H}^m, \mathbf{t}) =& q^{(r-2)(ms - s(s+1)/2)} q^{-s} \cdot \prod_{i=1}^{s} (q^{(m-i+1)} - 1)(q^{(m-i)} + 1) \\ & \cdot \prod_{i=1}^{s_1} q^i (q^i - 1)^{-1} \cdot \ldots \cdot \prod_{i=1}^{s_r} q^i (q^i - 1)^{-1} \\ & \cdot \prod_{i=1}^{s_1} q^{-2(m-i)t^{(1)}} \cdot \ldots \cdot \prod_{i=s_1+\ldots+s_{a-1}+1}^{s} q^{-2(m-i)t^{(a)}}, \end{aligned}$$

if V is non-hyperbolic of odd rank

$$\begin{aligned} m(\mathbb{H}^m \perp W, \mathbf{t}) =& q^{(r-2)((m+1)s - s(s+1)/2)} q^{-s\lfloor r/2 \rfloor} \cdot \prod_{i=1}^{s} (q^{2(m-i+1)} - 1) \\ & \cdot \prod_{i=1}^{s_1} q^i (q^i - 1)^{-1} \cdot \ldots \cdot \prod_{i=1}^{s_r} q^i (q^i - 1)^{-1} \\ & \cdot \prod_{i=1}^{s_1} q^{-(2(m-i+1)-1)t^{(1)}} \cdot \ldots \cdot \prod_{i=s_1+\ldots+s_{a-1}+1}^{s} q^{-(2(m-i+1)-1)t^{(a)}}, \end{aligned}$$

and if V is non-hyperbolic of even rank

$$
\begin{aligned}
m(\mathbb{H}^m \perp W, \mathbf{t}) =& q^{(r-2)((m+1)s-s(s+1)/2)} q^{-s(r+1 \mod 2)} \cdot \prod_{i=1}^{s} (q^{(m-i+2)}+1)(q^{(m-i+1)}-1) \\
&\cdot \prod_{i=1}^{s_1} q^i (q^i-1)^{-1} \cdot \ldots \cdot \prod_{i=1}^{s_r} q^i (q^i-1)^{-1} \\
&\cdot \prod_{i=1}^{s_1} q^{-2(m-i+1)t^{(1)}} \cdot \ldots \cdot \prod_{i=s_1+\ldots+s_{a-1}+1}^{s} q^{-2(m-i+1)t^{(a)}}.
\end{aligned}
$$

PROOF. By Lemma 2.5.4 we recursively obtain

$$
m(\mathbb{H}^m, \mathbf{t}) = \prod_{i=1}^{s} \frac{s^*_{t_i}(\mathbb{H}^{(m-i+1)})}{s^*_{t_i}(\mathbf{t}_{[i-1]})},
$$

and

$$
m(\mathbb{H}^m \perp W, \mathbf{t}) = \prod_{i=1}^{s} \frac{s^*_{t_i}(\mathbb{H}^{(m-i+1)} \perp W)}{s^*_{t_i}(\mathbf{t}_{[i-1]})},
$$

where $\mathbf{t}_{[j]} = [t_{j+1}, \ldots, t_m]$ is the type obtained from $\mathbf{t}$ by omitting the first j entries.

We write $s_{(\leqslant l)} = s_1 + \ldots + s_l$. Using Proposition 2.3.9 and Lemma 2.5.4 we get for $t_i = t^{(l)} < \frac{r}{2}$, that is, for $i \in [s_{(\leqslant l-1)} + 1, \ldots, s_{(\leqslant l)}]$: for V hyperbolic

$$
\begin{aligned}
\frac{s^*_{t_i}(\mathbb{H}^{m-i+1})}{s^*_{t_i}(\mathbf{t}_{[i-1]})} &= (q^{m-i+1}-1)(q^{m-i}+1)q^{(r-2)(m-i)}q^{-1} \\
&\cdot q^{-2(m-i)t^{(l)}} q^{s_{(\leqslant l)}-i+1}(q^{s_{(\leqslant l)}-i+1}-1)^{-1},
\end{aligned}
$$

for V non-hyperbolic of odd rank

$$
\begin{aligned}
\frac{s^*_{t_i}(\mathbb{H}^{m-i+1} \perp W)}{s^*_{t_i}(\mathbf{t}_{[i-1]})} &= (q^{2m-i+1}-1)q^{(r-2)(m-i+1)}q^{-\lfloor r/2 \rfloor} \\
&\cdot q^{-(2(m-i+1)-1)t^{(l)}} q^{s_{(\leqslant l)}-i+1}(q^{s_{(\leqslant l)}-i+1}-1)^{-1},
\end{aligned}
$$

and for V non-hyperbolic of even rank

$$
\begin{aligned}
\frac{s^*_{t_i}(\mathbb{H}^{m-i+1} \perp W)}{s^*_{t_i}(\mathbf{t}_{[i-1]})} &= (q^{m-i+2}+1)(q^{m-i+1}-1)q^{(r-2)(m-i+1)}q^{-(r+1 \mod 2)} \\
&\cdot q^{-2(m-i+1)t^{(l)}} q^{s_{(\leqslant l)}-i+1}(q^{s_{(\leqslant l)}-i+1}-1)^{-1}.
\end{aligned}
$$

Substituting these values we get for V hyperbolic

$$
\begin{aligned}
m(\mathbb{H}^m, \mathbf{t}) =& \prod_{l=1}^{a} \prod_{i=1}^{s_l} (q^{m-s_{(\leqslant l-1)}-i+1}-1)(q^{m-s_{(\leqslant l-1)}-i}+1)q^{(r-2)(m-s_{(\leqslant l-1)}-i)} \\
&\cdot q^{-1} q^{-2(m-s_{(\leqslant l-1)}-i)t^{(l)}} q^{s_l-i+1}(q^{s_l-i+1}-1)^{-1},
\end{aligned}
$$

for V non-hyperbolic of odd rank

$$
\begin{aligned}
m(\mathbb{H}^m \perp W, \mathbf{t}) =& \prod_{l=1}^{a} \prod_{i=1}^{s_l} (q^{2(m-s_{(\leqslant l-1)}-i+1)}-1)q^{(r-2)(m-s_{(\leqslant l-1)}-i+1)} \\
&\cdot q^{-\lfloor r/2 \rfloor} q^{-(2(m-s_{(\leqslant l-1)}-i+1)-1)t^{(l)}} q^{s_l-i+1}(q^{s_l-i+1}-1)^{-1}
\end{aligned}
$$

and for V non-hyperbolic of even rank

$$m(\mathbb{H}^m \perp W, \mathbf{t}) = \prod_{l=1}^{a}\prod_{i=1}^{s_l}(q^{m-s_{(\leqslant l-1)}-i+2}-1)(q^{m-s_{(\leqslant l-1)}-i+1}+1)q^{(r-2)(m-s_{(\leqslant l-1)}-i+1)} \cdot q^{-(r+1 \mod 2)}q^{-2(m-s_{(\leqslant l-1)}-i+1)t^{(l)}}q^{s_l-i+1}(q^{s_l-i+1}-1)^{-1}$$

respectively.

After some term rewriting, we finally arrive at the formulae given in the statement of the Lemma. □

2.6 Low rank cases over finite principal ideal rings

For certain low rank cases we provide a formula for the number of maximal totally isotropic submodules of regular quadratic modules over R. The results for modules over non-local finite rings then are obtained by the multiplicativity statement of Proposition 2.5.1. We used MAPLE for the computations presented below.

We only present the results for modules of even rank here. We include the hyperbolic and non-hyperbolic case (for even r) up to rank 6 and the hyperbolic case of rank 8. This selection stems from the main application of these results to the problem of counting similar sublattices of integral lattices, where only such maximal totally isotropic submodules with cardinality $q^{rn/2}$ are of interest (cf. Corollary 2.4.8 and Theorem 3.3.12). All results are in particular valid for modules over $\mathbb{Z}/p^r\mathbb{Z}$ (with $q = p$).

We will make use of an abbreviated form of $m(V, \mathbf{t})$ for explicit types. Suppose $\mathbf{t}$ is a type for which, in the terminology introduced before Lemma 2.5.4, we have distinct entries $j_1 < \ldots < j_a$ for which j_i occurs a total of s_i times. We then identify $m(V, \mathbf{t})$ with

$$m_{\underbrace{j_1\ldots j_1}_{s_1}\ldots\underbrace{j_a\ldots j_a}_{s_a}}(V).$$

We ignore any entry of the form $\lceil \frac{r}{2}\rceil$ thus for example $m(V, [j_1, j_2, j_2, \frac{r}{2}, \frac{r}{2}])$ (for some even r) in a module of rank 5 would be encoded by $m_{j_1 j_2 j_2}(V)$. If the module V is clear from context, we allow ourselves to drop it from the notation.

2.6.1 Rank 2

It is straightforward that the types in the hyperbolic case are of the form [j] with $j \leqslant \frac{r}{2}$, whereas in the non-hyperbolic case there is only the type $[\lceil \frac{r}{2}\rceil]$. Using Proposition 2.5.5 we see

$$m(\mathbb{H}, [j]) = \begin{cases} \frac{2\cdot q^{r-1}(\Phi_1(q))}{q^{r-1}(q-1)} = 2 & j < \frac{r}{2} \\ 0 & j = \frac{r}{2}, \end{cases}$$

$$m(\mathbb{A}, [j]) = \begin{cases} 0 & j < \frac{r}{2} \\ 1 & j = \lceil \frac{r}{2}\rceil, \end{cases}$$

and therefore

$$m(\mathbb{H}) = r + 1,$$
$$m(\mathbb{A}) = 1.$$

2.6.2 Rank 4

We handle the hyperbolic and non-hyperbolic cases separately.

The hyperbolic case

There are up to 4 distinct classes of types to be considered. The types are given by $[j_1, j_2], [j_1, j_1]$ in the case of r odd and additionally $[j_1, \frac{r}{2}], [\frac{r}{2}, \frac{r}{2}]$ for r even, as long as the restrictions $j_i < j_{i+1}$ and $j_i < \frac{r}{2}$ apply for every occurrence.

For these we compute using Proposition 2.5.5

$$\begin{aligned} m_{j_1 j_2} &= 2\, q^{r-2} \cdot \Phi_2(q)^2 \cdot q^{-2j_1}, \\ m_{j_1 j_1} &= 2\, q^{r-2} \cdot \Phi_2(q) \cdot q \cdot q^{-2j_1}, \\ m_{j_1} &= q^{r-2} \cdot \Phi_2(q)^2 \cdot q^{-2j_1}, \end{aligned}$$

We notice that $m_{j_1 j_2}$ does not depend on the value of j_2.

Thus for odd r and $l := \frac{r-1}{2}$:

$$m(\mathbb{H}^2) = \sum_{j_1=0}^{l-1} \sum_{j_2=j_1+1}^{l} m_{j_1 j_2} + \sum_{j_1=0}^{l} m_{j_1 j_1}.$$

This is essentially a geometric sum, which we simplify using the symbolic engine of MAPLE to

$$m(\mathbb{H}^2) = \frac{q^r \cdot \big((r+1)(q^2-1) - 2q\big) + 2}{(q-1)^2}. \tag{2.5}$$

For even r we have to add the contribution from the types which include $\frac{r}{2}$, we fix $l = \frac{r}{2} - 1$:

$$m(\mathbb{H}^2) = \sum_{j_1=0}^{l-1} \sum_{j_2=j_1+1}^{l} m_{j_1 j_2} + \sum_{j_1=0}^{l} (m_{j_1 j_1} + m_{j_1}) + 1,$$

Explicit evaluation of the above then shows that the formula in (2.5) is also valid for even r.

The non-hyperbolic case

For the following we assume that r is even. There are up to 2 distinct classes of types to be considered. The types are given by $[j_1, \frac{r}{2}]$ and $[\frac{r}{2}, \frac{r}{2}]$, as long as the restriction $j_1 < \frac{r}{2}$ applies for every occurrence.

For these we compute using Proposition 2.5.5

$$m_{j_1} = q^{r-2} \cdot \Phi_4(q) \cdot q^{-2j_1}.$$

Thus with $l := \frac{r}{2} - 1$ we obtain:

$$m(\mathbb{H} \perp W) = \sum_{j=0}^{l} m_{j_1} + 1 = \frac{q^r \cdot \Phi_4(q) - 2}{q^2 - 1}. \tag{2.6}$$

2.6.3 Rank 6

We handle the hyperbolic and non-hyperbolic cases separately.

The hyperbolic case
There are up to 8 distinct classes of types to be considered. The types are given by

$$[j_1, j_2, j_3], [j_1, j_2, j_2], [j_1, j_1, j_2], [j_1, j_1, j_1]$$

in the case of odd r and additionally

$$[j_1, j_2, \tfrac{r}{2}], [j_1, j_1, \tfrac{r}{2}], [j_1, \tfrac{r}{2}], [\tfrac{r}{2}, \tfrac{r}{2}, \tfrac{r}{2}]$$

for even r, as long as the restrictions $j_i < j_{i+1}$ and $j_i < \frac{r}{2}$ apply for every occurrence.

Applying Proposition 2.5.5, we compute

$$\begin{aligned}
m_{j_1j_2j_3} &= 2\, q^{3(r-2)} \cdot \Phi_2(q)^2 \cdot \Phi_3(q) \cdot \Phi_4(q) \cdot q^{-4j_1} \cdot q^{-2j_2},\\
m_{j_1j_2j_2} &= 2\, q^{3(r-2)} \cdot \Phi_2(q) \cdot \Phi_3(q) \cdot \Phi_4(q) \cdot q \cdot q^{-4\,j_1} \cdot q^{-2\,j_2},\\
m_{j_1j_1j_2} &= 2\, q^{3(r-2)} \cdot \Phi_2(q) \cdot \Phi_3(q) \cdot \Phi_4(q) \cdot q \cdot q^{-6\,j_1},\\
m_{j_1j_1j_1} &= 2\, q^{3(r-2)} \cdot \Phi_2(q) \cdot \Phi_4(q) \cdot q^3 \cdot q^{-6\,j_1},\\
m_{j_1j_2} &= q^{3(r-2)} \cdot \Phi_2(q)^2 \cdot \Phi_3(q) \cdot \Phi_4(q) \cdot q^{-4\,j_1} \cdot q^{-2\,j_2},\\
m_{j_1j_1} &= q^{3(r-2)} \cdot \Phi_2(q) \cdot \Phi_3(q) \cdot \Phi_4(q) \cdot q \cdot q^{-6\,j_1},\\
m_{j_1} &= q^{2(r-2)} \cdot \Phi_3(q) \cdot \Phi_4(q) \cdot q^{-4\,j_1}.
\end{aligned}$$

We notice that $m_{j_1j_2j_3}$ does not depend on the value of j_3 and that $m_{j_1j_1j_2}$ does not depend on the value of j_2.

Thus for odd r and $l := \frac{r-1}{2}$:

$$m(\mathbb{H}^3) = \sum_{j_1=0}^{l-2} \sum_{j_2=j_1+1}^{l-1} \sum_{j_3=j_2+1}^{l} m_{j_1j_2j_3} + \sum_{j_1=0}^{l-1} \sum_{j_2=j_1+1}^{l} (m_{j_1j_2j_2} + m_{j_1j_1j_2}) + \sum_{j_1=0}^{l} m_{j_1j_1j_1}.$$

This is essentially a cascade of geometric sums, which we simplify using the symbolic engine of MAPLE and some additional work by hand. This gives

$$m(\mathbb{H}^3) = \frac{q^{3r} \cdot a_{3r} + q^{2r} \cdot a_{2r} + a_0}{(q^3-1)\,(q^2-1)\,(q-1)}, \tag{2.7}$$

where

$$\begin{aligned}
a_{3r} &= \big((r+1)(q^3-1) - 2q \cdot \Phi_2(q)\big) \cdot \Phi_2(q) \cdot \Phi_4(q),\\
a_{2r} &= 2 \cdot \Phi_3(q)^2,\\
a_0 &= -2.
\end{aligned}$$

For even r we have to add the contribution from the types which include $\frac{r}{2}$, we fix $l = \frac{r}{2} - 1$:

$$\begin{aligned}
m(\mathbb{H}^3) = &\sum_{j_1=0}^{l-2} \sum_{j_2=j_1+1}^{l-1} \sum_{j_3=j_2+1}^{l} m_{j_1j_2j_3} + \sum_{j_1=0}^{l-1} \sum_{j_2=j_1+1}^{l} (m_{j_1j_2j_2} + m_{j_1j_1j_2} + m_{j_1j_2})\\
&+ \sum_{j_1=0}^{l} (m_{j_1j_1j_1} + m_{j_1j_1} + m_{j_1}) + 1.
\end{aligned}$$

Explicit evaluation of the above then shows that the formula in (2.7) is also valid for even r.

The non-hyperbolic case

For the following we assume that r is even. There are up to 4 distinct classes of types to be considered. The types are given by

$$[j_1, j_2, \tfrac{r}{2}], [j_1, j_1, \tfrac{r}{2}], [j_1, \tfrac{r}{2}, \tfrac{r}{2}], [\tfrac{r}{2}, \tfrac{r}{2}, \tfrac{r}{2}],$$

as long as the restrictions $j_i < j_{i+1}$ and $j_i < \frac{r}{2}$ apply for every occurrence.

Applying Proposition 2.5.5, we compute

$$\begin{aligned} m_{j_1,j_2} &= q^{3(r-2)} \cdot (q^3+1) \cdot \Phi_2(q) \cdot \Phi_4(q) \cdot q^{-4j_1} \cdot q^{-2j_2}, \\ m_{j_1,j_1} &= q^{3(r-2)} \cdot (q^3+1) \cdot \Phi_4(q) \cdot q \cdot q^{-6j_1}, \\ m_{j_1} &= q^{2(r-2)} \cdot (q^3+1) \cdot \Phi_2(q) \cdot q^{-4j_1}. \end{aligned}$$

Thus with $l := \frac{r}{2} - 1$ we obtain:

$$m(\mathbb{H} \perp W) = \sum_{j_1=0}^{l-1} \sum_{j_2=j_1+1}^{l} m_{j_1,j_2} + \sum_{j_1=0}^{l} (m_{j_1,j_1} + m_{j_1}) + 1,$$

which simplifies to

$$m(\mathbb{H}^2 \perp W) = \frac{q^{3r} \cdot b_{3r} + q^{2r} \cdot b_{2r} + b_0}{(q^3-1)(q-1)(q^2+1)}, \tag{2.8}$$

where

$$\begin{aligned} b_{3r} &= \Phi_4(q)^2 \cdot \Phi_6(q), \\ b_{2r} &= -2 \cdot \Phi_3(q) \cdot \Phi_6(q), \\ b_0 &= -(q^4 - 2q - 1) \cdot \Phi_6(q). \end{aligned}$$

2.6.4 Rank 8

We restrict our investigation to the hyperbolic case. There are up to 16 distinct classes of types to be considered. The types are given by

$$\begin{gathered} [j_1, j_2, j_3, j_4], [j_1, j_2, j_3, j_3], [j_1, j_2, j_2, j_3], [j_1, j_2, j_2, j_2], \\ [j_1, j_1, j_2, j_3], [j_1, j_1, j_2, j_2], [j_1, j_1, j_1, j_2], [j_1, j_1, j_1, j_1] \end{gathered}$$

in the case of odd r and additionally

$$\begin{gathered} [j_1, j_2, j_3, \tfrac{r}{2}], [j_1, j_2, j_2, \tfrac{r}{2}], [j_1, j_1, j_2, \tfrac{r}{2}], [j_1, j_1, j_1, \tfrac{r}{2}], \\ [j_1, j_2, \tfrac{r}{2}, \tfrac{r}{2}], [j_1, j_1, \tfrac{r}{2}, \tfrac{r}{2}], [j_1, \tfrac{r}{2}, \tfrac{r}{2}, \tfrac{r}{2}], [\tfrac{r}{2}, \tfrac{r}{2}, \tfrac{r}{2}, \tfrac{r}{2}] \end{gathered}$$

for even r, as long as the restrictions $j_i < j_{i+1}$ and $j_i < \frac{r}{2}$ apply for every occurrence.

Applying Proposition 2.5.5, we compute

$$
\begin{aligned}
m_{j_1j_1j_1j_1} &= 2\,q^{6(r-2)} \cdot \Phi_2(q)^2 \cdot \Phi_4(q) \cdot \Phi_6(q) \cdot q^6 \cdot q^{-12j_1},\\
m_{j_1j_1j_1j_2} &= 2\,q^{6(r-2)} \cdot \Phi_2(q)^3 \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q^3 \cdot q^{-12j_1},\\
m_{j_1j_1j_2j_2} &= 2\,q^{6(r-2)} \cdot \Phi_2(q)^2 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q^2 \cdot q^{-10j_1} \cdot q^{-2j_2},\\
m_{j_1j_1j_2j_3} &= 2\,q^{6(r-2)} \cdot \Phi_2(q)^3 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q \cdot q^{-10j_1} \cdot q^{-2j_2},\\
m_{j_1j_2j_2j_2} &= 2\,q^{6(r-2)} \cdot \Phi_2(q)^3 \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q^3 \cdot q^{-6j_1} \cdot q^{-6j_2},\\
m_{j_1j_2j_2j_3} &= 2\,q^{6(r-2)} \cdot \Phi_2(q)^3 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q \cdot q^{-6j_1} \cdot q^{-6j_2},\\
m_{j_1j_2j_3j_3} &= 2\,q^{6(r-2)} \cdot \Phi_2(q)^3 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q \cdot q^{-6j_1} \cdot q^{-4j_2} \cdot q^{-2j_3},\\
m_{j_1j_2j_3j_4} &= 2\,q^{6(r-2)} \cdot \Phi_2(q)^4 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q^{-6j_1} \cdot q^{-4j_2} \cdot q^{-2j_3},\\
m_{j_1j_2j_3} &= q^{6(r-2)} \cdot \Phi_2(q)^4 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q^{-6j_1} \cdot q^{-4j_2} \cdot q^{-2j_3},\\
m_{j_1j_2j_2} &= q^{6(r-2)} \cdot \Phi_2(q)^3 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q \cdot q^{-6j_1} \cdot q^{-6j_2},\\
m_{j_1j_1j_2} &= q^{6(r-2)} \cdot \Phi_2(q)^3 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q \cdot q^{-10j_1} \cdot q^{-2j_2},\\
m_{j_1j_1j_1} &= q^{6(r-2)} \cdot \Phi_2(q)^3 \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q^3 \cdot q^{-12j_1},\\
m_{j_1j_2} &= q^{5(r-2)} \cdot \Phi_2(q)^2 \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q^{-6j_1} \cdot q^{-4j_2},\\
m_{j_1j_1} &= q^{5(r-2)} \cdot \Phi_2(q) \cdot \Phi_3(q) \cdot \Phi_4(q)^2 \cdot \Phi_6(q) \cdot q \cdot q^{-10j_1},\\
m_{j_1} &= q^{3(r-2)} \cdot \Phi_2(q)^2 \cdot \Phi_4(q) \cdot \Phi_6(q) \cdot q^{-6j_1}.
\end{aligned}
$$

We notice that m_{j_1,j_2,j_3,j_4} does not depend on the value of j_4, that m_{j_1,j_2,j_2,j_3} and m_{j_1,j_1,j_2,j_3} do not depend on the value of j_3 and that m_{j_1,j_1,j_1,j_2} does not depend on the value of j_2.

Thus for odd r and $l := \frac{r-1}{2}$:

$$
\begin{aligned}
m(\mathbb{H}^4) = &\sum_{j_1=0}^{l-3} \sum_{j_2=j_1+1}^{l-2} \sum_{j_3=j_2+1}^{l-1} \sum_{j_4=j_3+1}^{l} m_{j_1j_2j_3j_4}\\
&+ \sum_{j_1=0}^{l-2} \sum_{j_2=j_1+1}^{l-1} \sum_{j_3=j_2+1}^{l} m_{j_1j_2j_3j_3} + m_{j_1j_2j_2j_3} + m_{j_1j_1j_2j_3}\\
&+ \sum_{j_1=0}^{l-1} \sum_{j_2=j_1+1}^{l} m_{j_1j_2j_2j_2} + m_{j_1j_1j_2j_2} + m_{j_1j_1j_1j_2}\\
&+ \sum_{j_1=0}^{l} m_{j_1j_1j_1j_1}.
\end{aligned}
$$

This is essentially a cascade of geometric sums, which we simplify using the symbolic engine of MAPLE and some additional work by hand. This gives

$$
m(\mathbb{H}^4) = \frac{q^{6r} a_{6r} + q^{5r} a_{5r} + q^{3r} a_{3r} + a_0}{(q^5-1)(q^3-1)^2(q-1)}, \tag{2.9}
$$

where

$$\begin{aligned}
a_{6r} &= ((r+1)(q^4-1) - 2q \cdot \Phi_3(q)) \cdot \Phi_3(q) \cdot \Phi_5(q) \cdot \Phi_6(q),\\
a_{5r} &= 2 \cdot \Phi_3(q)^3 \cdot \Phi_4(q) \cdot \Phi_6(q),\\
a_{3r} &= -2 \cdot \Phi_4(q) \cdot \Phi_5(q),\\
a_0 &= 2.
\end{aligned}$$

For even r we have to add the contribution from the types which include $\frac{r}{2}$, we fix $l = \frac{r}{2} - 1$:

$$\begin{aligned}
m(\mathbb{H}^4) = &\sum_{j_1=0}^{l-3} \sum_{j_2=j_1+1}^{l-2} \sum_{j_3=j_2+1}^{l-1} \sum_{j_4=j_3+1}^{l} m_{j_1 j_2 j_3 j_4}\\
&+ \sum_{j_1=0}^{l-2} \sum_{j_2=j_1+1}^{l-1} \sum_{j_3=j_2+1}^{l} m_{j_1 j_2 j_3 j_3} + m_{j_1 j_2 j_2 j_3} + m_{j_1 j_1 j_2 j_3} + m_{j_1 j_2 j_3}\\
&+ \sum_{j_1=0}^{l-1} \sum_{j_2=j_1+1}^{l} m_{j_1 j_2 j_2 j_2} + m_{j_1 j_1 j_2 j_2} + m_{j_1 j_1 j_1 j_2} + m_{j_1 j_2 j_2} + m_{j_1 j_1 j_2} + m_{j_1 j_2}\\
&+ \left(\sum_{j_1=0}^{l} m_{j_1 j_1 j_1 j_1} + m_{j_1 j_1 j_1} + m_{j_1 j_1} + m_{j_1} \right) + 1.
\end{aligned}$$

Explicit evaluation of the above then shows that the formula in (2.9) is also valid for even r.

CHAPTER

3 Similar sublattices

This chapter contains some of the main results of this thesis. We use the arithmetic theory of integral lattices to relate similar sublattices of maximal integral lattices and maximal totally isotropic submodules of regular quadratic modules over the rings $\mathbb{Z}/c\mathbb{Z}$.

We start by recalling basic facts about similarities of Euclidean lattices. We discuss elementary results about the structure of the set of all similarities and similar sublattices and introduce the arithmetic function ssl counting the number of similar sublattices by their index. These notions are generalized to include sublattices of a lattice L, not necessarily similar to L itself, but rather to any lattice in $\text{gen}(L)$.

We then recall basic features of the defined arithmetic functions, in particular, we discuss their super-multiplicativity and provide an example for the failure of multiplicativity in general. Furthermore we discuss a result of Conway, Rains and Sloane which was the first result to give necessary and sometimes sufficient conditions regarding the existence of similar sublattices of rational lattices.

In 3.3.3 we introduce a novel approach to the problem of the enumeration of similar sublattices of maximal integral lattices. Here we find a bijective correspondence (cf. Lemmata 3.3.9, 3.3.10) between c-genus-similar sublattices of a lattice L and maximal totally isotropic submodules of L/cL, with a canonically induced regular quadratic form (cf. Lemmata 3.3.6 and 3.3.7), provided that L is maximal and integral and that $\gcd(\det(L), c)$ if L is even, and $\gcd(2\det(L), c)$ if L is odd.

This then implies the main results of this chapter, Theorem 3.3.12 which combines the results of the preceding Lemmata and of chapter 2 to show that under the above assumptions, the arithmetic counting function ssl is multiplicative and that its value on sublattices of index $m = c^{n/2}$ is given by the number of maximal totally isotropic submodules of L/cL with a suitable quadratic form. In addition, we obtain Theorem 3.3.13, the analog to Theorem 3.3.12 for genus similar sublattices.

We conclude this chapter with 3.4, a short discussion of Dirichlet series and Zeta functions for the cases where the above defined arithmetic function ssl^g is multiplicative. The lattice E_8 satisfies $\text{ssl}_{E_8} = \text{ssl}^g_{E_8}$ and is an important special case of the general result. We provide the Dirichlet series for E_8 and show that it satisfies a local functional equation.

3.1 SIMILAR SUBLATTICES OF LATTICES

Let $c \in \mathbb{R}_{>0}$. A **c-similarity**, or **similarity** of **norm** c, of (V, b) is a linear map $\sigma : V \to V$ satisfying

$$b(\sigma(x), \sigma(y)) = cb(x, y)$$

for all $x, y \in V$. We write $\Sigma(V, b)$ for the set of all similarities of (V, b). Any similarity is bijective by the above formula and the non-degeneracy of b. Clearly, $\Sigma(V, b)$ is a subgroup of $GL(V)$. Furthermore, the **norm map** $N : \Sigma(V, b) \to \mathbb{R}_{>0};\ \sigma \mapsto c$ associating to a similarity σ its norm is a surjective (cf. Section 3.3.) homomorphism of groups with kernel $O(V, b)$. In fact if σ, σ' are c-similarities then there exists $\phi, \phi' \in O(V)$ such that $\sigma = \phi \circ \sigma' = \sigma' \circ \phi$. In particular, the set $\Sigma(V, b; c) := \{\sigma \in \Sigma(V, b) \mid N(\sigma) = c\}$, the fiber of the value c under the norm map N, is a right and left coset of $O(V, b)$.

DEFINITION 3.1.1. Let (L, b) be a Euclidean lattice. A **c-similarity**, or **similarity** of **norm** c, of L, is a c-similarity σ of $(\mathbb{R}L, b)$ such that $\sigma(L) \subset L$. ◆

We introduce notation for the set of similarities and similar sublattices of a Euclidean lattice.

DEFINITION 3.1.2. Let (L, b) be a Euclidean lattice.

i. The set of similarities is

$$\Sigma(L, b) := \{\sigma \in \Sigma(\mathbb{R}L, b) \mid \sigma(L) = L\}.$$

The **index** of a similarity σ is the index $[L : \sigma(L)]$.

ii. A sublattice $L' \subset L$ is a **(self)-similar sublattice**, short **SSL**, if there exists a similarity σ such that $L' = \sigma(L)$. The **norm** of L' is the norm of σ. We set

$$SSL(L, b) := \{\sigma(L) \subset L \mid \sigma \in \Sigma(L, b)\}.$$ ◆

We will subsequently count similarities and similar sublattices in terms of their index, this will align nicely into some existing framework regarding Zeta functions. Note that rewriting the counting process in terms of their norms is easily done, as we will see now.

LEMMA 3.1.3. *Let σ be a c-similarity of L and write $n = \dim(L)$, then*

$$[L : \sigma(L)] = c^{n/2}.$$

We define two counting functions.

DEFINITION 3.1.4. Let (L, b) be a Euclidean lattice. We associate to (L, b) the similarity counting function

$$s_{(L,b)} : \mathbb{N} \to \mathbb{N};\ a \mapsto |\Sigma(L, b; a)|.$$

where

$$\Sigma(L, b; a) := \{\sigma \in \Sigma(L, b) \mid [L : \sigma(L)] = a\},$$

and the similar sublattice counting function

$$ssl_{(L,b)} : \mathbb{N} \to \mathbb{N};\ a \mapsto |SSL(L, b; a)|,$$

where

$$\mathrm{SSL}(L, b; a) := \{L' \in \mathrm{SSL}(L, b) \mid [L : L'] = a\}.$$

◆

For the notations introduced above we will as usual sometimes abbreviate (L, b) to L if the inner product is clear from context.

Having notation and vocabulary at hand, we now delve into the discussion of the most basic properties and connections of the objects in question. We first discuss invariance under scaling of a lattice.

LEMMA 3.1.5. *Let* (L, b) *be a Euclidean lattice. Let* $\lambda \in \mathbb{R}_{>0}$. *Then*

i. $\Sigma(L, b) = \Sigma(L, \lambda b)$;

ii. $\Sigma(L, b; a) = \Sigma(L, \lambda b; a)$;

iii. $s_{(L,b)} = s_{(L,\lambda b)}$;

iv. $\mathrm{ssl}_{(L,b)} = \mathrm{ssl}_{(L,\lambda b)}$.

That is, the occurring norms and indexes of similarities and similar sublattices, as well as the number of such, do not change under scaling.

We collect some facts on the structure of the sets of similarities and and similar sublattices.

LEMMA 3.1.6. *Let* (L, b) *be a Euclidean lattice.*

i. $\Sigma(L) \subset \Sigma(\mathbb{R}L)$ *is a monoid, but not a group.*

ii. $O(L) = \Sigma(L; 1) \subset \Sigma(L)$.

iii. $\Sigma(L; c)$ *is finite for all* $c \in S_L$.

PROOF. The claims are quite obvious. Towards (i) we have seen that there always is a similarity of norm greater than 1, and the inverse of this map can clearly not map into L. (ii) is clear by definition and towards (iii) we can apply a standard proof for the finiteness of $O(L)$, which of course is a special case of the claim. The idea is to fix a basis $\mathcal{B}$ of L. Let $\lambda := \max\{b(v, v) \mid v \in \mathcal{B}\}$. Then if σ is a c-similarity, σ can map the elements of $\mathcal{B}$ only to elements in $L \cap B_{c\lambda}(0)$, those elements in L of length at most $c\lambda$. But since L is discrete and a ball is compact, this set is finite. Thus there can only be finitely many c-similarities. □

The sets $\Sigma(L)$ (resp. $\Sigma(L; c)$) and $\mathrm{SSL}(L)$ (resp. $\mathrm{SSL}(L; c)$) are connected to each other through an action by the orthogonal group of the lattice L:

LEMMA 3.1.7. *Let* (L, b) *be a Euclidean lattice. For the right action of* $O(L)$ *on the sets* $\Sigma(L)$, $\Sigma(L; c)$, *for* $c \in S_L$ *we obtain:*

i. If similarities $\sigma, \sigma' \in \Sigma(L)$ *are in the same* $O(L)$*-orbit, their norms agree.*

ii. *Similarities* $\sigma, \sigma' \in \Sigma(L; c)$ *are in the same* $O(L)$*-orbit if and only if* $\sigma(L) = \sigma'(L)$.

iii. *The* $O(L)$*-orbits on* $\Sigma(L)$ *are of the form* $\Sigma(L)_{L'} = \{\sigma \in \Sigma(L) \mid \sigma(L) = L'\}$*, where* $L' \in SSL(L)$*. Thus* $SSL(L)$ *is a set of representatives*[1] *of the above action and in particular* $SSL(L; c)$ *is a set of representatives for the* $O(L)$*-action on* $\Sigma(L; c)$.

iv. $s_L(c) = ssl_L(c) \cdot |O(L)|$.

v. *There exist* $r := ssl_L(c)$ *distinct* c*-similarities* $\sigma_1, \dots, \sigma_r$ *such that*

$$\Sigma(L; c) = \dot{\bigcup}_{i=1}^{r} \sigma_i\, O(L).$$

PROOF. (i) is clear. Towards (ii) the assumption $\sigma(L) = \sigma'(L)$ implies that $\sigma^{-1} \circ \sigma'(L) = L$ and thus $\sigma' = \sigma \circ \phi$ for some $\phi \in O(L)$. On the other hand if such ϕ exists, clearly $\sigma'(L) = \sigma \circ \phi(L) = \sigma(L)$. The remaining claims follow immediately. □

3.2 GENUS-SIMILAR SUBLATTICES OF LATTICES

All of this generalizes to sublattices of a given lattice L that are not necessarily similar to L, but similar to a lattice in the genus of L. Though this may seem artificial at the moment, it is the natural environment of the arithmetic method which we apply to the problem of enumerating similar sublattices. This point of view is, in particular, natural in the theory of representations of a lattice by another one. In the framework of the arithmetic theory of quadratic forms (with the notation of Chapter X in [Kne02]), the numbers $ssl_L(c^{n/2})$ and $ssl_L^g(c^{n/2})$ can be related to the representation numbers

$$\frac{a(L, {}^{c^{-1}}L)}{O(L)} \text{ and } \sum_{i=1}^{k} \frac{a(M_i, {}^{c^{-1}}L)}{O(M_i)},$$

where $\{M_1, \dots, M_k\}$ is a set of representatives of $\operatorname{gen}(L)$.

DEFINITION 3.2.1. Let (L, b) be a Euclidean lattice and let $M_1, \dots, M_h \subset \mathbb{R}L$ be a set of representatives for the ($\mathbb{Q}$-)isometry classes in $\operatorname{gen}(L)$.

i. The set of genus similarities is

$$\Sigma^g(L, b) := \{\sigma \in \Sigma(\mathbb{R}L, b) \mid \sigma(M) = L \text{ for } M \in \{M_1, \dots, M_h\}\}.$$

The **index** of a similarity σ is the index $[L : \sigma(L)]$.

ii. A sublattice $L' \subset L$ is a **genus-similar sublattice**, short **GSSL**, if there exists a similarity σ such that $L' = \sigma(M)$ for some $M \in \operatorname{gen}(L)$. We say that the **norm** of L' is the norm of σ. We set

$$SSL^g(L, b) := \{\sigma(L) \mid \sigma \in \Sigma^g(\mathbb{R}L, b)\}.$$ ◆

DEFINITION 3.2.2. Let (L, b) be a Euclidean lattice. We associate to (L, b) the genus similarity counting function

$$s^g_{(L,b)} : \mathbb{N} \to \mathbb{N};\ a \mapsto |\Sigma^g(L, b; a)|.$$

[1] We allow to refer to any set, that is in a one-to-one correspondence with the equivalence classes of some equivalence relation, as a set of representatives, rather than considering only subsets of the set the relation is defined on.

where

$$\Sigma^g(L, b; a) := \{\sigma \in \Sigma^g(L, b) \mid [L : \sigma(L)] = a\},$$

and the similar sublattice counting function

$$\mathrm{ssl}^g_{(L,b)} : \mathbb{N} \to \mathbb{N};\ a \mapsto |\,\mathrm{SSL}^g(L, b; a)|,$$

where

$$\mathrm{SSL}^g(L, b; a) := \{L' \in \mathrm{SSL}^g(L, b) \mid [L : L'] = a\}.$$

◆

The choice of which representatives $M_1, \ldots, M_h$ we choose does affect the above definitions of $\Sigma^g(L)$ and $\Sigma^g(L; c)$, but only in the following sense: If $M'_1, \ldots, M'_h$ is another set of representatives the associated sets would be in bijection, induced by the isometries of $M_1 \cong M'_1, \ldots, M_h \cong M'_h$ (which we can assume by appropriate choice of labeling). However, the function s^g_L is well-defined. In any case, as we make the transition to the associated sets of sublattices of L this ambiguity vanishes entirely.

Now the results of Lemma 3.1.7 do not generalize directly to the case of genus-similar sublattices. This is for the fact that now we cannot let $O(L)$ act from the right, since in general $O(L)$ will not stabilize another lattice in the genus of L. We can however let each $O(M)$ act on the right on those similarities $\sigma \in \Sigma^g(L)$ that map M into L. But this will only show that $|\Sigma^g(L)| = \sum_{i=1}^h a_i |O(M)|$, where we let a_i denote the number of elements of $\Sigma^g(L; c)$ that map M into L (in accordance with the discussion above, $a_i = \frac{a(M, c^{-1}L)}{O(M)}$).

3.3 EXISTENCE AND ENUMERATION OF SIMILAR SUBLATTICES

3.3.1 Properties of the counting function ssl

Clearly, $\mathrm{ssl}_{(L,b)}(1) = 1$, it thus is an arithmetic function and we should ask whether it is multiplicative or not.

It is not always multiplicative as the following example shows.

EXAMPLE 3.3.1. On page 1392 of [BHM08] the lattice $L = 2e_1\mathbb{Z} + 3e_2\mathbb{Z}$, together with the standard inner product, is named as an example for the failure of multiplicativity . Explicitly the first non-trivial norms of similar sublattices are 4 and 9, and these norms provide a counterexample by

$$\mathrm{ssl}_L(36) = 2 > 1 \cdot 1 = \mathrm{ssl}_L(4) \cdot \mathrm{ssl}_L(9).$$

■

PROPOSITION 3.3.2. *Let* (L, b) *be a Euclidean lattice.* $\mathrm{ssl}_{(L,b)}$ *and* $\mathrm{ssl}^g_{(L,b)}$ *are* ***super-multiplicative****, that is, for* a, a' *coprime*

$$\mathrm{ssl}_{(L,b)}(aa') \geqslant \mathrm{ssl}_{(L,b)}(a)\,\mathrm{ssl}_{(L,b)}(a'),$$
$$\mathrm{ssl}^g_{(L,b)}(aa') \geqslant \mathrm{ssl}^g_{(L,b)}(a)\,\mathrm{ssl}^g_{(L,b)}(a').$$

A proof of this can for example be found in Theorem 2.6 of [Heu10], we present the proof for convenience.

PROOF. Let M_1, M_2 be genus-similar sublattices of index a of L and let N_1, N_2 be genus similar sublattices of index a' of M_1, M_2 respectively. In particular N_1, N_2 are genus-similar sublattices of index aa' of L. If we assert that

$$N_1 = N_2 =: N \Rightarrow M_1 = M_2,$$

the Proposition is proven.

In order to do so, we write

$$a' = [M_i : N] = [M_i : M_1 \cap M_2] \cdot [M_1 \cap M_2 : N],$$
$$a = [L : M_i] = [L : M_1 + M_2] \cdot [M_1 + M_2 : M_i].$$

Since then

$$[M_1 + M_2 : M_i] = [M_i : M_1 \cap M_2].$$

is a common divisor of a and a', this index equals 1. But this shows $M_1 = M_2$. □

3.3.2 Similarities of rational quadratic spaces and an existence theorem for similarities of rational lattices

In the case of a Euclidean space the question of existence and even a full description of all similarities of a given norm c has a straightforward answer. For any $c \in \mathbb{R}_{>0}$ the map $\sigma_c : V \to V;\ x \mapsto \sqrt{c}x$ clearly is a similarity of norm c and thus the norm map is surjective. The set of all such similarities is then given as an $O(V)$-coset $\Sigma(V; c) = \sigma_c\, O(V)$.

The situation already becomes more difficult by considering rational spaces with an inner product. Let (V, b) be a positive definite quadratic $\mathbb{Q}$-space. All of the above definitions for real spaces can be applied to this situation also, where clearly the codomain of the norm map then is $\mathbb{Q}_{>0}$. It is still true that the fibers of the norm map are cosets of $O(V)$, but surjectivity can fail.

PROPOSITION 3.3.3. *Let (V, b) be quadratic $\mathbb{Q}$-space of dimension n. Then*

$$N(\Sigma(V, b)) = \{c \in \mathbb{Q}_{>0} \mid (c, (-1)^{n(n+1)/2} dV)_p = 1 \textit{ for all primes } p \mid 2c \cdot dV\}.$$

PROOF. Observe that $c \in N(\Sigma(V, b))$ if and only if ${}^cV \cong V$ since any such isometry $\phi : {}^cV \to V$ satisfies

$$cb(x, y) = b(\phi(x), \phi(y))\ \forall x, y \in V,$$

and thus the underlying linear map $\phi : V \to V$ is a c-similarity.

But now $V \cong {}^cV$ if and only if $V_p \cong {}^cV_p$ for all primes $p \in \mathbb{Z}$, by the Hasse-Minkowski Theorem (cf. 66 : 4 in [O'M73] or the discussion in 1.3.3). We can dismiss the real spot since scaling by a positive number clearly does not affect the signature.

Thus we have to check the Hasse-symbol of both spaces. These are related by (cf. p. 167 in [O'M73]):

$$S_p{}^cV = (c, (-1)^{n(n+1)/2} \cdot dV^{n+1})_p S_p V.$$

If p is odd and does not divide either c or dV both arguments are units and thus the symbol computes to 1 in any case (cf. 63 : 12 in [O'M73]). Thus we are left to check that it equals 1 in the remaining cases, and the thus set of $c \in Q_{>0}$ for which this is the case is precisely the set of norms of similarities. □

This proof is one half of the proof of the next Theorem, and was given by Conway, Rains and Sloane in their 1999 work [CRS99].

THEOREM 3.3.4 (THEOREM 1 [CRS99]). *A necessary condition for a rational* $2k$*-dimensional lattice* L *to have a similar sublattice of norm* c *is that the Hilbert symbol*

$$\left(c, (-1)^k \det L\right)_p = 1$$

for all primes p dividing $2c \det L$. *If* L *is unigeneric and* $r\mathbb{Z}$*-maximal for some* $r \in \mathbb{Q}$ *then this condition is also sufficient.*

PROOF. The necessity of the condition is covered by Proposition 3.3.3. On the other hand if c satisfies the condition in the Theorem, the lattice $\sqrt{c}L$ is rationally equivalent to L ($\mathbb{Q}\sqrt{c}L \cong \mathbb{Q}L$) and thus there is an isometry ϕ of the spaces. Furthermore, $\phi(\sqrt{c}L)$ is contained in an $r\mathbb{Z}$-maximal lattice and there is only one such genus on each space (cf. 102 : 3 in [O'M73]). Since L is assumed to be $r\mathbb{Z}$-maximal and unigeneric $\phi(\sqrt{c}L)$ is a sublattice of L and it is by construction c-similar to L. □

3.3.3 Enumeration of similar sublattices of integral lattices using finite quadratic modules

Lemma 3.1.5 showed that the of enumeration of similar sublattices of Euclidean lattice does not depend on how that lattice is scaled. Therefore it suffices to consider integral lattices instead of rational lattices. Furthermore, we can assume that $\mathfrak{s}(L) = \mathbb{Z}$.

LEMMA 3.3.5. *Let* (L, b) *be an integral lattice. Then the norm of any similarity, or similar sublattice, is an integer.*

PROOF. Without loss of generality we assume that $\mathfrak{s}(L) = \mathbb{Z}$. Let σ be a similarity of norm c. Then $[L : \sigma(L)] = c^{n/2} \in \mathbb{N}$ by Lemma 3.1.3. By assumption there are $x, y \in L$ with $b(x, y) = 1$. Then

$$c = c \cdot b(x, y) = b(\sigma(x), \sigma(y)) \in \mathbb{Z},$$

since $\sigma(L)$ is integral as a sublattice of an integral lattice. □

The above allows to argue for the counting functions to be indexed by the norm rather than the index. However, we stick with the way we introduced them, as functions of the index.

The proof, as well as the condition, of Theorem 3.3.4 clearly has a local flavor. In the subsequent we will describe a method which relates such sublattices to maximal totally isotropic submodules of free regular quadratic modules over rings of the form $\mathbb{Z}/p^r\mathbb{Z}$, with p a prime. This method is subject to two constraints: It restricts to similarity factors c which satisfy $\gcd(c, \det(L)) = 1$ and enumerates sublattices which are similar to a lattice in the genus of L, rather than to L itself.

If, however, L is unigeneric, we get sublattices necessarily similar to L. In addition we can show that ssl_L and ssl_L^g behave multiplicatively if the above constraints are satisfied. This method was developed by Rudolf Scharlau, the subsequent discussion is based on a manuscript [Sch11a], which was made available to the author. Publicly available slides of a talk given on this subject can be found online [Sch11b].

In particular, the subsequent results include the previously unsettled case of the root lattice E_8. In addition, for all similarity factors coprime to the respective determinants we can reproduce results about the root lattices A_4, D_4 (cf. [BM99], [BHM08]); it should be noted that the aforementioned results include the cases of similarity factors that are not coprime to the respective determinants and thus are of greater generality for these specific cases.

Given an integral lattice (L, b). We define a quadratic form q as follows: if L is even, set $q(x) := \frac{1}{2}b(x, x)$ for all $x \in L$, otherwise set $q(x) := b(x, x)$ for all $x \in L$. In any case we obtain a quadratic $\mathbb{Z}$-module with values in $\mathbb{Z}$. Let $c \in \mathbb{N}$ and let $^{-}$ denote reduction modulo c, where we assume that the modulus is clear from context. Furthermore, let $\pi : L \to L/cL$ be the canonical projection. Then we associate to the quadratic $\mathbb{Z}$-module (L, q) the free finite quadratic $\mathbb{Z}/c\mathbb{Z}$ - module $(L/cL, \overline{q})$, where $\overline{q} : L/cL \to \mathbb{Z}/c\mathbb{Z}$ is the quadratic form induced by q.

LEMMA 3.3.6. *Let* (L, b) *be an integral lattice.* $(L/cL, \overline{q})$ *is a regular quadratic* $\mathbb{Z}/c\mathbb{Z}$*-module if*

$$\gcd(c, \det(L)) = 1 \text{ if } L \text{ is even}$$
$$\text{or } \gcd(c, 2\det(L)) = 1 \text{ if } L \text{ is odd.}$$

PROOF. In the case that L is even, $q(x) = \frac{1}{2}b(x, x)$, thus $b_q = b$ and the claim follows since $\overline{\det(L)} \in \mathbb{Z}/c\mathbb{Z}^*$ is a representative for $d(L/cL, \overline{q}) = d(L/cL, \overline{b_q})$ and we assumed $\gcd(c, \det(L)) = 1$.

In the case that L is odd, $q(x) = b(x, x)$, thus $b_q = 2b$. But $\overline{\det(L, b)} \in \mathbb{Z}/c\mathbb{Z}^*$ if and only if $\overline{\det(L, 2b)} \in \mathbb{Z}/c\mathbb{Z}^*$,by the additional assumption $2 \nmid c$. □

We use this quadratic module to characterize sublattices that are c-similar to lattices in the genus of L.

LEMMA 3.3.7. *Let* L *be an integral lattice,* σ *be a similarity of norm* c*, and* $M = \sigma(L')$ *be a sublattice similar to some lattice* $L' \in \text{gen}(L)$*. If* $\gcd(c, \det(L)) = 1$*, then* $cL \subset M$ *and therefore* $M/cL \subset L/cL$*.*

PROOF. By assuming $\gcd(c, \det(L)) = 1$ and the fact that $[L : M] = c^{n/2}$ it follows that $M^\# = M^{c^n,\#} \cap M^{\det(L),\#}$, since $\det(M) = [L : M]^2 \det(L) = c^n \det(L)$ (cf. (1.1)).

We claim that $M^{c^n,\#} = M^{c,\#} = \frac{1}{c}M$ and that $L/M \subset \frac{1}{c}M/M$. Then $cL/M \subset M/M$, or equivalently, $cL \subset M$ holds.

To prove the claimed equality $M^{c^n,\#} = M^{c,\#} = \frac{1}{c}M$, we make a comparison of orders: Clearly, $|M^{c^n,\#}| = c^n$ by the above. Furthermore, $M^{c,\#} \subset M^{c^n,\#}$ by definition. Now $M^{c,\#} = \frac{1}{c}M \cap M^\#$ and since $M = \sigma(L')$, we find $b(x, y) = b(\sigma(x'), \sigma(y')) = c \cdot b(x', y') \in c\mathbb{Z}$ with $x', y' \in L'$, for arbitrary $x, y \in M$. But then $b(\frac{1}{c}x, y) \in \mathbb{Z}$, or equivalently $\frac{1}{c}x \in M^\#$. Thus $M^{c,\#} = \frac{1}{c}M$. Finally, $|\frac{1}{c}M/M| = |M/cM| = c^n = |M^{c^n,\#}|$ and this completes the proof of the claim. □

If the condition $\gcd(c, \det(L)) = 1$ is violated, this can be wrong:

EXAMPLE 3.3.8. Using MAGMA, we can compute similar sublattices via backtracking. We found a similarity σ of norm 3 of the Coxeter-Todd lattice K_{12}, for which $3K_{12} \not\subset \sigma(K_{12})$. However, $9K_{12} \subset \sigma(K_{12})$. ■

LEMMA 3.3.9. *Let* L *be an integral lattice and let* $c \in \mathbb{N}$ *with* $\gcd(c, \det(L)) = 1$*. If* $M \subset L$ *is* c*-similar to some lattice in the genus of* L*, then* $\pi(M) \subset L/cL$ *is a maximal totally isotropic submodule of cardinality* $c^{n/2}$ *of the free regular quadratic module* $(L/cL, \overline{q})$*.*

PROOF. Let $M \subset L$ be a similar sublattice of norm c. By Lemma 3.3.7 $\mathcal{M} := \pi(M) = M/cL \subset L/cL$ is a submodule of the free regular quadratic module $(L/cL, \overline{q})$. Since $q(x)$ is divisible by c for all $x \in M$, we have $\overline{q}(\mathcal{M}) = \{0\}$, thus $\mathcal{M}$ is totally isotropic. Furthermore, $|\mathcal{M}| = [L : M] = c^{n/2}$. With the classification of maximal totally isotropic submodules of free regular quadratic modules over $\mathbb{Z}/p^r\mathbb{Z}$ we deduce that $\mathcal{M}$ is maximal (cf Corollary 2.4.8). □

LEMMA 3.3.10. *Let L be a $r\mathbb{Z}$-maximal integral lattice, and let $c \in \mathbb{N}$ be such that $\gcd(c, 2\det(L)) = 1$ if L is odd and $\gcd(c, \det(L)) = 1$ if L is even. If ${}^c(\mathbb{Q}L) \cong \mathbb{Q}L$, then for every totally isotropic $\mathcal{M} \subset (L/cL, \overline{q})$ with $|\mathcal{M}| = c^{n/2}$ the sublattice $M := \pi^{-1}(\mathcal{M})$ is c-similar to a lattice in the genus of L.*

PROOF. If $\mathcal{M} \subset L/cL$ is a totally isotropic submodule of cardinality $c^{n/2}$. $M = \pi^{-1}(\mathcal{M})$ is integral and $b(M, M) \subset c\mathbb{Z}$ since $b(x, y) = q(x + y) - q(x) - q(y) \in c\mathbb{Z}$ for all $x, y \in M$ by isotropy of $\mathcal{M}$.

The lattice $M' := {}^{c^{-1}}M$ is on ${}^{c^{-1}}\mathbb{Q}L \cong {}^c\mathbb{Q}L \cong \mathbb{Q}L$, since M is on $\mathbb{Q}L$. This implies that we can replace M' by some lattice on the same space as L, in particular, this holds for all localizations. However, by abuse of language, we stick to the name M'. Since there is a c-similarity from M' to M, we are left to show that $M' \in \text{gen}(L)$.

We show that there is an isometry $M'_p \cong L_p$ at every prime p, which suffices because L and M' are positive definite. We distinguish 2 cases:

i. $p \nmid c$, which implies that $c \in \mathbb{Z}_p^*$;
ii. $p \mid c$, which implies that $p \nmid \det(L)$.

Ad i.: Write $M = TL$ where T is the representation matrix of a base change from L to M. T is integral by definition and $\det(T) = [L : M] = c^{n/2}$. Therefore T_p is in $GL_n(\mathbb{Z}_p)$, since $c \in \mathbb{Z}_p^*$. Thus $M_p = T_pL_p = L_p$. Then

$$\begin{aligned} L \text{ is } r\mathbb{Z}\text{-maximal} &\Rightarrow L_p \text{ is } r\mathbb{Z}_p\text{-maximal} \\ &\Rightarrow M_p \text{ is } r\mathbb{Z}_p\text{-maximal} \\ &\Rightarrow M'_p = {}^{c^{-1}}M_p \text{ is } c^{-1}r\mathbb{Z}_p\text{-maximal} \\ &\Rightarrow M'_p \text{ is } r\mathbb{Z}_p\text{-maximal,} \end{aligned}$$

where for the last implication we again use $c \in \mathbb{Z}_p^*$ (cf. 1.3.3). M'_p and L_p are on the same $\mathbb{Q}_p$-space and up to isometry there is only one $r\mathbb{Z}_p$-maximal lattice on this space (cf. 1.3.5, or 91 : 2 in [O'M73]). Thus $L_p \cong M'_p$, for all $p \nmid c$.

Ad ii.: Since $\det(L) = \det(M')$ and $p \nmid \det(L)$, we obtain that L_p, M'_p are both unimodular. But by assumption ${}^c\mathbb{Q}L \cong \mathbb{Q}L$, thus we can assume that M' is on $\mathbb{Q}L$ as well.

As noted before, L_p, M'_p are unimodular lattices on the $\mathbb{Q}_p$-space $\mathbb{Q}_pL$. For $p \neq 2$ we are in the non-dyadic case, this directly implies $L_p \cong M'_p$ (cf. 1.3.4, or 92 : 2b. in [O'M73]). If $p = 2$, the dyadic case, L is even, since we assumed $2 \nmid c$ for odd lattices. Thus, to obtain an isometry, we have to assure for L_p and M'_p to have identical norm groups (cf. 1.3.4, or Theorem 93 : 16 in [O'M73]).

Let $Q(x) := b(x, x) = 2q(x)$ for all $x \in L$. Then $\mathfrak{g}(L_2) = Q(L_2) + 2\mathfrak{s}L_p$. Now $\mathbb{Z}_2 \subset \mathfrak{g}(L_2) \subset 2\mathbb{Z}_2$ because L_2 is unimodular. Exactly one equality holds: $\mathfrak{g}(L_2) = Q(L_2) + 2\mathfrak{s}L = 2\mathbb{Z}_2$, since $Q(L) \subset 2\mathbb{Z}$ (L is even) implies $Q(L_2) \subset 2\mathbb{Z}_2$. All of this shows, that $\mathfrak{g}(L_2) = 2\mathbb{Z}_2$ for all even lattices L, such that L_2 is unimodular. But M' is also even: $q(x) = \frac{1}{2}b(x,x) \in c\mathbb{Z}$ for all $x \in M$ by construction, thus $Q(M) \subset 2c\mathbb{Z}$ and after rescaling, $c^{-1}Q(M) \subset 2\mathbb{Z}$ implies that M' is even. Therefore the same reasoning as above gives $\mathfrak{g}(M'_2) = 2\mathbb{Z}_2 = \mathfrak{g}(L_2)$. Thus $L_p \cong M'_p$, for all $p \mid c$.

We conclude: $L_p \cong M'_p$ for all primes p and $p = \infty$, thus $M' \in \text{gen}(L)$. □

This culminates in another criterion for the existence of c-similar sublattices of an integral lattice (cf. Theorem 3.3.4). Recall that in the case of odd dimension c has to be a square and that for all squares c a similar sublattice of norm c exists. We thus focus on even dimensional lattices.

THEOREM 3.3.11. *Let* L *be maximal integral lattice of rank* $n = 2k$ *and let* $c \in \mathbb{N}$ *such that* $c = \prod_{i=1}^{t} p_i^{r_i}$ *is the factorization of* c *in pairwise distinct primes* p_i. *A necessary condition for* L *to have a sublattice* M *that is* c*-similar to* L*, is that the* $\mathbb{F}_{p_i}$*-space* $(L/p_iL, \overline{q})$ *is hyperbolic for all* p_i*, for which* r_i *is odd.*

PROOF. This follows from Lemma 3.3.10 together with Corollary 2.4.8. □

Putting all of the above together we arrive at the main result of this section.

THEOREM 3.3.12. *Let* L *be an unigeneric maximal integral lattice and* $c \in \mathbb{N}$ *such that* $\gcd(c, 2\det(L)) = 1$ *if* L *is odd and* $\gcd(c, \det(L)) = 1$ *if* L *is even. If there is at least one similar sublattice of* L *with norm* c*, there is a one-to-one correspondence between sublattices* M *that are* c*-similar to* L *and maximal totally isotropic submodules of* $(L/cL, \overline{q})$*. The function* ssl_L *is multiplicative on all* c *satisfying the above conditions.*

PROOF. Lemmata 3.3.9 and 3.3.10 provide the one-to-one correspondence. Multiplicativity follows by Proposition 2.5.1. □

This can be slightly generalized without altering the prove, the previous Lemmata have already been formulated in accordance.

THEOREM 3.3.13. *Let* L *be an integral maximal lattice and* $c \in \mathbb{N}$ *such that* $\gcd(c, 2\det(L)) = 1$ *if* L *is odd and* $\gcd(c, \det(L)) = 1$ *if* L *is even. If there is at least one sublattice of* L *which is* c*-similar to a lattice in* $\text{gen}(L)$*, there is a one-to-one correspondence between sublattices* M *which are* c*-similar to a lattice in* $\text{gen}(L)$ *and maximal totally isotropic submodules of* $(L/cL, \overline{q})$*. The function* ssl_L^g *is multiplicative on all* c *satisfying the above conditions.*

REMARK 3.3.14. The above discussion shows one more thing. If L and c fulfill the assumptions of Theorem 3.3.12 or Theorem 3.3.13, we cannot only count (genus-)similar sublattices of norm c of L, but we can compute them explicitly using the results of Chapter 2, for example with MAGMA. To do so we could compute the orthogonal group $O(L/cL, \overline{q})$, compute a representation of $(L/cL, \overline{q})$ in a basis according to a Witt decomposition as in Proposition 2.2.5, and compute the orbits of $O(L/cL, \overline{q})$ on a representative set of maximal totally isotropic submodules as in Example 2.4.3. Then Theorem 2.4.4 and Corollary 2.4.9 assure that we have computed all such submodules. It is now a standard problem, which MAGMA is capable of intrinsically, to convert these submodules of L/cL to sublattices.

At the time of writing this thesis, MAGMA unfortunately does not handle quadratic modules over arbitrary finite rings, or even local finite rings of the form $\mathbb{Z}/p^r\mathbb{Z}$, intrinsically. A package to overcome this gap, recall that we depend on the orthogonal group of modules over such rings in the above approach, is in preparation and planned to be made available by the author. ∎

3.4 A GLANCE TOWARDS ZETA FUNCTIONS FOR COUNTING (GENUS-)SIMILAR SUBLATTICES

Let $L = (L, b)$ be a Euclidean lattice for which we assume that ssl_L, or ssl_L^g are multiplicative. By the above results this is true for ssl_{E_8}, since E_8 is unigeneric, and more generally for ssl_L^g for all even unimodular lattices.

In this case it makes sense to define a Dirichlet series as a generating function of ssl_L, or ssl_L^g:

$$D_L(s) := \sum_{m=1}^{\infty} \frac{\mathrm{ssl}_L(m)}{m^s} = \sum_{L' \in \mathrm{SSL}(L)} \frac{1}{[L : L']^s}, \tag{3.1}$$

$$D_L^g(s) := \sum_{m=1}^{\infty} \frac{\mathrm{ssl}_L^g(m)}{m^s} = \sum_{L' \in \mathrm{SSL}^g(L)} \frac{1}{[L : L']^s}. \tag{3.2}$$

Examples of Dirichlet series related to similar sublattices of certain low dimensional lattices can be found in [BM99], [BHM08], and [BSZ11].

In the latter formulation of (3.1) and (3.2) we see a very general way of assigning Zeta functions to algebraic structures. Particular well known cases are Zeta functions of algebraic number fields, where for such a field K

$$\zeta_K(s) = \sum_{\mathfrak{a} \leqslant \mathfrak{o}_K} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} = \sum_{\mathfrak{a} \leqslant \mathfrak{o}_K} \frac{1}{[\mathfrak{o}_K : \mathfrak{a}]^s}.$$

This makes sense since the norm of ideals is multiplicative for Dedekind rings, and this can be rewritten in the form

$$\zeta_K(s) = \sum_{m=1}^{\infty} \frac{a_m}{m^s},$$

where $a_m = |\{\mathfrak{a} \leqslant \mathfrak{o}_K \mid \mathfrak{N}(\mathfrak{a}) = m\}$.

This is also true of ssl_L and ssl_L^g if these functions are multiplicative. We treat these Dirichlet series as formal sums and do not dwell on questions regarding their convergence here.

By the multiplicativity result of the Theorems 3.3.12 and 3.3.13 we write

$$D_L(s) = \prod_p^{\infty} \sum_{r=0}^{\infty} \frac{\mathrm{ssl}_L(p^r)}{p^{rs}}, \tag{3.3}$$

$$D_L^g(s) = \prod_p^{\infty} \sum_{r=0}^{\infty} \frac{\mathrm{ssl}_L^g(p^r)}{(p^r)^s}. \tag{3.4}$$

For ssl_L^g we can use the results of 2.6 to make this decomposition into Euler factors more explicit.

EXAMPLE 3.4.1 (A ZETA FUNCTION FOR SIMILAR SUBLATTICES OF $\mathbb{E}_8$). The (even) root lattice E_8 has similar sublattices of arbitrary norm $c \in \mathbb{N}$ (cf. Theorem 3.3.4). The index of a similar sublattice of norm c is given by c^4 by Lemma 3.1.3. With Theorem 3.3.12 we find

$$\mathrm{ssl}_{E_8}(c^4) = m(\mathbb{H}^4),$$

where $\mathbb{H}^4$ is the hyperbolic module of rank 8 over the appropriate ring $\mathbb{Z}/c\mathbb{Z}$. If we apply this to the Dirichlet series (3.3) we find

$$\sum_{r=0}^{\infty} \frac{\mathrm{ssl}_L^g(p^{4r})}{(p^{4r})^s} = \frac{W(p, p^{-s})}{(1-p^{-s})(1+p^{-s})(1+p^{-2s})(1-p^{3-4s})(1-p^{5-4s})(1-p^{3-2s})^2(1+p^{3-2s})^2},$$

where

$$\begin{aligned} W(X,Y) &= (X^3Y^4+1)(X^5Y^2+X^5Y+2X^4Y+2X^3Y+2X^2Y+2XY+Y+1) \\ &= X^8Y^{12}+X^8Y^8+2X^7Y^8+2X^6Y^8+3X^5Y^8+2X^4Y^8+X^3Y^8 \\ &\quad +X^5Y^4+2X^4Y^4+3X^3Y^4+2X^2Y^4+2XY^4+Y^4+1. \end{aligned}$$

Note that the factors in the denominator belong to the Euler factors of zeta functions or their quotients (cf. the example to Theorem 11.7 in [Apo13]):

$$\begin{aligned} \zeta(s) &= \prod_p \frac{1}{1-p^{-s}}, \\ \frac{\zeta(2s)}{\zeta(s)} &= \prod_p \frac{1}{1+p^{-s}}. \end{aligned}$$

If we write $Z(s) := \prod_p W(p, p^-s)$ we therefore can write

$$D_{E_8}(s) = \zeta(4s) \cdot \zeta(4s-3) \cdot \zeta(4s-5) \cdot \zeta(4s-6)^2 \cdot Z(s).$$

An interesting observation is, that the Euler factors satisfy a functional equation. Write $D_{E_8,p}$ for the complete Euler factor of D_{E_8} at the prime p. Then

$$D_{E_8,p}|_{p\to p^{-1}} = -p^{12-8s} \cdot D_{E_8 p}. \tag{3.5}$$

■

Observations like (3.5) are a common motive in the theory of Zeta functions of groups and rings, the interested reader is referred to [DSW08] for information on this topic. We will only add the closing remark that it should be of interest to fit the Dirichlet series obtained from the (genus)-similar sublattice counting functions into the more general framework of Zeta functions of groups and rings, the above cited book deals in some detail with Zeta functions of rings that are not necessarily associative, but additively isomorphic to $\mathbb{Z}^n$, just as lattices are.

Part II

A locally explicit formula for the quantizer constant in monohedral periodic vector quantization

CHAPTER

4 Geometric foreplay

This introductory chapter starts with 4.1, a collection of some basic notions about lattices and periodic point sets in Euclidean space. Here we exclude the contents of Chapter 1 from the discussion, wherever they can be spared. This is concluded by a discussion of suitable parameter spaces for lattices and periodic sets.

In 4.2 we recall some facts and notions about polyhedral complexes and triangulations.

Finally 4.3 covers Dirichlet-Voronoi and Delone subdivisions induced by Delone sets, in particular, by lattices and periodic sets. Duality of those polytopal complexes is discussed with the help of the more abstract notion of Dirichlet-Voronoi polytopes in dual space.

4.1 Lattices and periodic sets

Recall from 1.3 that a ($\mathbb{Z}$-)**lattice** L in $\mathbb{R}^n$ is a finitely generated $\mathbb{Z}$-submodule of $\mathbb{R}^n$. So $L \subset \mathbb{R}^n$ is a lattice in $\mathbb{R}^n$ if and only if there are linearly independent vectors $v_1, \dots, v_m$ of $\mathbb{R}^n$ such that $L \cong \bigoplus_{i=1}^m v_i\mathbb{Z}$.

If L is on $\mathbb{R}^n$ with basis $\mathcal{B} = (v_1, \dots, v_n)$ and if we write B for the matrix whose columns are given by $v_1, \dots, v_n$ (in that order) we obtain $L = B\mathbb{Z}^n$, and in this way any $B \in GL_n(\mathbb{R})$ determines a lattice on $\mathbb{R}^n$, a matrix as such is called **basis matrix** of the lattice L. The lattice $\mathbb{Z}^n$ is called the **standard lattice** on $\mathbb{R}^n$.

Let L be on $\mathbb{R}^n$ and let $\mathcal{B} = (v_1, \dots, v_n)$ be a lattice basis of L. The **fundamental parallelotope**

$$\mathcal{F}_{\mathcal{B}}(L) = \left\{ \sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in [0,1], \text{for } i \in \{1, \dots, n\} \right\}$$

is a fundamental domain of L. That is, $\operatorname{int}(x + F_{\mathcal{B}}(L)) \cap \operatorname{int}(y + F_{\mathcal{B}}(L)) = \varnothing$ for any $x, y \in L$ and $\bigcup_{f \in F_{\mathcal{B}}(L)} f + L$ covers $\mathbb{R}^n$.

A **periodic set** Λ in $\mathbb{R}^n$ is a finite union of translates of a lattice L in $\mathbb{R}^n$, thus it is a set of the form $\Lambda = \bigcup_{i=1}^m t_i + L$, for some $\mathbf{t} = (t_1, \dots, t_m) \in (\mathbb{R}^n)^m$. We say that L is a **translation lattice** for Λ and that

Λ is **m-periodic** for L, or an **m-periodic set** for L, if none of $t_1, \dots, t_m$ is a translate of another by some element of L, that is, if the above union is disjoint. We say that m is the **period** of Λ for L. If $L = \mathbb{Z}^n$ and $\mathbf{t} = (t_1, \dots, t_m) \in (\mathbb{R}^n)^m$ we write $\Lambda_{\mathbf{t}} := \bigcup_{i=1}^n t_i + \mathbb{Z}^n$ and refer to this as a **standard periodic set**. In particular lattices are special cases of periodic sets.

If Λ is a periodic set, there always exists a unique **maximal translation lattice**

$$L_\Lambda = \{v \in \mathbb{R}^n \mid \forall\, x \in \Lambda : \; x + v \in \Lambda\}.$$

Let m_Λ be denote the period of Λ for L_Λ, then it is the unique smallest period of Λ, the **minimal period** of Λ.

For $\Lambda = \bigcup_{i=1}^m t_i + L$, a fundamental domain of L will be called an **L-fundamental domain** of Λ. It then is a fundamental domain of Λ under the action of the translation lattice L.

4.1.1 Euclidean lattices

If $\mathbb{R}^n$ is equipped with an inner product b we can associate certain geometric notions to any lattice. To make clear which inner product is used, we will write (L, b) instead of L, whenever b is not clear from context. If we want to emphasize the existence of a inner product we speak of a **Euclidean lattice**.

We write vol for the Lebesgue-volume on the standard Euclidean space and vol_b for the volume on $(\mathbb{R}^n, b)$. By use of the formulae

$$\mathrm{vol}_b = \sqrt{\det(G(b))}\,\mathrm{vol},$$

and

$$\mathrm{vol}(F_{\mathcal{B}}(L)) = |\det(B)| = \sqrt{\det(G_{\mathcal{B}}(L, b))}$$

we observe that each fundamental parallelotope has the same volume and we call this number the **volume** of L:

$$\mathrm{vol}(L, b) := \mathrm{vol}_b(\mathcal{F}_{\mathcal{B}}(L)) = \sqrt{\det(L, b)}.$$

4.1.2 Isometries of Euclidean lattices and periodic sets

The notion of isometry (cf. 1.1.2 and 1.3.2) can be applied to periodic sets in Euclidean space too. Let $\Lambda = \bigcup_{i=1}^m t_i + L$, where w.l.o.g. $t_1 = 0$ and L is on $\mathbb{R}^n$, be a periodic set in $(\mathbb{R}^n, b)$. We set

$$\mathrm{GL}(\Lambda) := \{U \in \mathrm{GL}_n(\mathbb{Z}) \mid U\Lambda = \Lambda\},$$

a subgroup of $\mathrm{GL}_n(\mathbb{R})$, which is conjugate to $\mathrm{GL}_n^{\mathbf{t}}(\mathbb{Z}) := \mathrm{GL}(\Lambda_{\mathbf{t}})$, and its **orthogonal group**

$$O(\Lambda, b) := \{U \in \mathrm{GL}(\Lambda) \mid b(Ux, Uy) = b(x, y)\ \forall x, y \in \Lambda\}.$$

It is a well-known and important fact that the orthogonal group of any Euclidean lattice is finite (cf. Lemma 3.1.6) and by $O(\Lambda, b) \subset O(L_\Lambda, b)$, where L_Λ is the maximal translation lattice for Λ, this also is true for periodic sets.

4.1.3 Euclidean lattices and quadratic forms

We will often prefer to work with the notion of a (positive definite) quadratic form instead of that of an inner product. If Q is any real positive definite quadratic form we obtain an inner product $b_Q(x, y) = Q(x + y) - Q(x) - Q(y)$, which is the associated bilinear form. The other way around, if b is an inner product, we obtain a quadratic form Q by the relation $Q(x) = b(x, x)$ for all $x \in \mathbb{R}^n$ and $b = \frac{1}{2} b_Q$.

Thus we will identify the Euclidean space $(\mathbb{R}^n, \frac{1}{2} b_Q)$ with the quadratic space $(\mathbb{R}^n, Q)$ in any such situation and all of the above stays valid.

Since real positive definite quadratic forms are, by choice of basis and their associated Gram matrices, in bijection with the cone of positive definite symmetric matrices $\mathcal{S}^n_{>0}$ over $\mathbb{R}$. We will also use the above notation for matrices $Q \in \mathcal{S}^n_{>0}$.

4.1.4 Parameter spaces for lattices

If L is any lattice on $(\mathbb{R}^n, b)$ we can use the Cholesky decomposition of the Gram matrix $Q \in \mathcal{S}^n_{>0}$ of b with respect to the standard basis $\mathcal{E}$ (or by slight modification any basis) $Q = G_{\mathcal{E}}(b) = A^T A$ and any basis matrix B of L to construct a lattice $L' := (AB)\mathbb{Z}^n$ in n-dimensional Euclidean standard space, that is isometric to L.

We note that if $L = B\mathbb{Z}^n$, $L' = B'\mathbb{Z}^n$ are lattices in Euclidean standard space $\mathbb{R}^n$, they are

i. equal, if and only if there exists a $U \in GL_n(\mathbb{Z})$ such that $B' = B \cdot U$;

ii. isometric, if and only if there exists a $U \in O_n(\mathbb{R})$ such that $B' = U \cdot B$.

Thus we obtain parameter spaces (up to isometry) for

$$\text{lattices on } \mathbb{R}^n \longleftrightarrow GL_n(\mathbb{R})/GL_n(\mathbb{Z})$$
$$\text{isometry classes of lattices on } \mathbb{R}^n \longleftrightarrow O_n(\mathbb{R})\backslash GL_n(\mathbb{R})/GL_n(\mathbb{Z}).$$

Similarly the lattice $\mathbb{Z}^n$ in $(\mathbb{R}^n, Q')$, with $Q'(x) := Q(Bx)$, is isometric to L, thus $G_{\mathcal{E}}(Q') = G_{\mathcal{B}}(L, Q)$. Since real positive definite quadratic forms are in bijection to $\mathcal{S}^n_{>0}$, the cone of real positive definite symmetric $n \times n$-matrices, we identify a real positive definite quadratic form with its Gram matrix with respect to the standard basis.

We note that $(\mathbb{Z}^n, Q) \cong (\mathbb{Z}^n, Q')$ if and only if Q, Q' are conjugate under the action of $GL_n(\mathbb{Z})$. Thus we obtain parameter spaces for

$$\text{bases up to orthogonal transformations of } \mathbb{R}^n \longleftrightarrow \mathcal{S}^n_{>0}$$
$$\text{isometry classes of lattices on } \mathbb{R}^n \longleftrightarrow \mathcal{S}^n_{>0}/GL_n(\mathbb{Z}).$$

PROPOSITION AND DEFINITION 4.1.1 (COORDINATE REPRESENTATION OF A EUCLIDEAN LATTICE). *Let* L *be a Euclidean lattice on* $(\mathbb{R}^n, Q)$. *We can associate to* L *and any basis* $\mathcal{B}$ *of* L *the Euclidean lattice*

$$(\mathbb{Z}^n, G_{\mathcal{B}}((L, Q))).$$

This lattice is called the ***coordinate representation*** *of* L *with respect to* $\mathcal{B}$. *Furthermore* *i.* $(\mathbb{Z}^n, G_{\mathcal{B}}((L, Q))) \cong (L, Q)$,

ii. *the coordinate representations of isometric lattices are conjugate under the action of* $\mathrm{GL}_n(\mathbb{Z})$,

iii. *coordinate representation induces a bijection between* $\mathcal{S}^n_{>0}/\mathrm{GL}_n(\mathbb{Z})$ *and the set of isometry classes of Euclidean lattices on* $\mathbb{R}^n$.

4.1.5 Parameter spaces for periodic sets

To extend the above parameter spaces for lattices to periodic sets in general, we will accept some redundancy. We are interested in questions regarding periodic sets only up to isometry. So it is no loss of generality to confine our parameter spaces to comprise of periodic sets for which we assume that $t_1 = 0$. Furthermore we will not parametrize all periodic sets at once, but give one parameter space for each $m \in \mathbb{N}$ that comprises only those that are at most m-periodic.

That said, we use the parameter spaces for lattices above, leading to a basis parameter space

$$O_n(\mathbb{R})\backslash \mathrm{GL}_n(\mathbb{R})/\mathrm{GL}_n(\mathbb{Z}) \times (\mathbb{R}^n)^{m-1},$$

and a **coordinate parameter space**

$$\mathcal{S}^{n,m}_{>0} := \mathcal{S}^n_{>0}/\mathrm{GL}_n(\mathbb{Z}) \times (\mathbb{R}^n)^{m-1},$$

contained in

$$\mathcal{S}^{n,m} := \mathcal{S}^n/\mathrm{GL}_n(\mathbb{Z}) \times (\mathbb{R}^n)^{m-1}.$$

While we refer to elements Q of $\mathcal{S}^n$ as quadratic forms, we will refer to elements $(Q, \mathbf{t})$ of $\mathcal{S}^{n,m}$ as **periodic forms** (cf. section 3.2.1 in [Sch09]).

We should recall that the above parameter spaces do not give systems of representatives of isometry classes, as was the case for lattices. A periodic set may have several distinct representations of the above forms, since simply replacing $\mathbf{t}$ by some $\mathbf{t}'$ where the t_i' are translates of the t_i by some lattice vectors, or are a permutation of the t_i gives us a wealth of unequal representations.

We say that Λ is **representable** by $\Lambda_{\mathbf{t}}$, or **t-representable** if and only if there is a $\mathbb{R}^n$-isomorphism that maps Λ to $\Lambda_{\mathbf{t}}$. If Λ is $\mathbf{t}$-representable, we can associate to any (Λ, Q'), for $Q' \in \mathcal{S}^n_{>0}$, some isometric $(\Lambda_{\mathbf{t}}, Q)$, with $Q \in \mathcal{S}^n_{>0}$, similar to the case of lattices. A periodic form $(Q, \mathbf{t})$ and a periodic set $(\Lambda_{\mathbf{t}}, Q)$ can be thought of being essentially the same object, we therefore also say that (Λ, Q') is **represented** by $(Q, \mathbf{t})$, in the above scenario.

Clearly, if $Q \in \mathcal{S}^n_{>0}$, then $(\Lambda_{\mathbf{t}}, Q)$ is a $\mathbf{t}$-representable periodic set, and if $U \in \mathrm{GL}^{\mathbf{t}}_n$, then $(\Lambda_{\mathbf{t}}, Q)$ and $(\Lambda_{\mathbf{t}}, U^T Q U)$ are isometric.

PROPOSITION AND DEFINITION 4.1.2 (**t**-COORDINATE REPRESENTATION OF A PERIODIC SET).
Let $\mathbf{t} \in (\mathbb{R}^n)^{m-1}$. *Let* (Λ, Q') *be a* $\mathbf{t}$*-representable Euclidean periodic set on* $\mathbb{R}^n$. *For any* $Q \in \mathcal{S}^n_{>0}$ *for which* (Λ, Q') *is represented by* $(Q, \mathbf{t})$, *we say that the periodic set* $(\Lambda_{\mathbf{t}}, Q)$ *is a* ***t-coordinate representation*** *of* (Λ, Q'). *This construction implies that there is a surjection between* $\mathcal{S}^n_{>0}/\mathrm{GL}^{\mathbf{t}}_n(\mathbb{Z})$ *and the set of isometry classes of* $\mathbf{t}$*-representable periodic sets on* $\mathbb{R}^n$.

REMARK 4.1.3. The book [Sch09] covers periodic sets and forms with respect to the packing and covering problem. The above presentation relies on the notation used there. ■

4.2 POLYTOPES

4.2.1 Polytopes and polytopal complexes

This section follows the treatment in [Zie95].

The **dimension** of a polytope is the dimension of its affine hull. If a face has dimension k, then we say it is a **k-face**. For a polytope of dimension n we, as usual, refer to 0-faces as vertices and $n-1$-faces as facets.

A **polytopal complex** is a set $\mathcal{C}$ of polytopes in $\mathbb{R}^n$ such that $\varnothing \in \mathcal{C}$, for $P \in \mathcal{C}$ every facet of P is in $\mathcal{C}$, and for $P, Q \in \mathcal{C}$, $P \cap Q$ is a face of both P and Q. Its **underlying set** is $|\mathcal{C}| := \bigcup_{P \in \mathcal{C}} P$. If $\mathcal{C}' \subset \mathcal{C}$ is a polytopal complex, we call it a subcomplex of $\mathcal{C}$. If v is a vertex of the polytopal complex $\mathcal{C}$ then the **star** of v in $\mathcal{P}$ is $\operatorname{star}(v, \mathcal{C}) := \{F \in \mathcal{C} \mid v \in F\}$, the subcomplex containing all faces of $\mathcal{C}$ which contain v.

The **face lattice** of a polytope P is the partially ordered set (poset) of all faces of P, ordered by inclusion. It is a **lattice** in the order-theoretic sense: it is a bounded poset in which every two elements have a unique upper and lower bound (cf. Definition 2.5 in [Zie95]). It is defined analogously for a polytopal complex.

Each polytope P gives rise to a complex $\mathcal{C}(P)$, the complex of all faces of P. The subcomplex $\mathcal{C}(\partial P)$ formed by all proper faces of P is called the **boundary complex** of P, and we have $|\mathcal{C}(\partial P)| = \partial P$. For a polytopal complex $\mathcal{C}$ we fix the abbreviations $\mathcal{C}^{(k)}$ for the subset consisting of k-faces of $\mathcal{C}$. We write $\operatorname{vert}(\mathcal{C}) = \mathcal{C}^{(0)}$.

A **polytopal subdivision** of a set M is a polytopal complex $\mathcal{C}$ such that $|\mathcal{C}| = M$. A **triangulation** of a set M is a polytopal subdivision $\mathcal{T}$ of M such that each $S \in \mathcal{C}$ is a simplex. A triangulation is **pyramidal** if all of its full dimensional simplices have a point in common, which then is called the apex of the triangulation. We say that $\mathcal{C}(P)$ is the **trivial subdivision** of P.

Let $\mathcal{T}$ be a pyramidal triangulation of a polytope P, such that the apex 0 of $\mathcal{T}$ is in the interior of P, $\mathcal{T}^{(0)} = \operatorname{vert}(P) \cup \{0\}$, and $\mathcal{T} \cap F$ is a triangulation without new vertices of F for every $F \in \mathcal{C}(P)^{(\dim(P)-1)}$. A pyramidal triangulation $\mathcal{T}$ of a polytope P is essentially identifiable with a triangulation of the boundary complex of P, that does not contain points besides the vertices of P. They can be identified by the process of taking the complex of pyramids over 0 in the one direction and removing the faces that do contain 0 in the other.

A way to obtain a triangulation without new vertices is by **pulling refinements**[1]: let $\mathcal{C}$ be a polytopal subdivision and let $v \in \operatorname{vert}(\mathcal{C})$. Define $p_v^-(\mathcal{C})$ by

$$p_v^-(\mathcal{C}) := \bigcup_{\substack{F \subset C \in \mathcal{C} \\ \dim(F) = \dim(C)-1 \\ v \in C,\ v \notin F}} \mathcal{C}(\operatorname{conv}(F \cup \{v\})) \;\cup\; \bigcup_{\substack{C \in \mathcal{C} \\ v \notin C}} \mathcal{C}(C), \tag{4.1}$$

that is, $p_v^-(\mathcal{C})$ is obtained from $\mathcal{C}$ by the following rules: for $C \in \mathcal{C}$

i. If $v \notin C$ then $C \in p_v^-(\mathcal{C})$.

ii. If $v \in C$ then for all facets F of C: $\mathcal{C}(\operatorname{conv}(F \cup \{v\})) \subset p_{v_0}^-(\mathcal{C})$.

[1] There are other triangulations that would work as well, the so called lexicographic triangulations, cf. 4.3 in [DRS10]

Discussions of pulling, and more generally, lexicographic triangulations, can be found in both [DRS10] (Definition 4.3.7), and [Lee90]. Our presentation follows the latter source. It seems that the pulling triangulation was first described in [HS69], Lemma 1.4. All of the succeeding can be formulated accordingly for general lexicographic triangulations.

LEMMA 4.2.1. *Let* P *be a polytope.*

i. Let $\mathcal{C}$ *be a polytopal subdivision of* P*, and let* $v \in P$*. Then the above defined* $p_v^-(\mathcal{C})$ *is a refinement of* $\mathcal{C}$*.*

ii. Let $\mathcal{C}(P)$ *be the trivial subdivision of* P*, and let* $\text{vert}(P) \subset V \subset P$ *such that* V *is finite and labeled*[2] *in* $\{1, \dots, k\}$*. Then the subdivision*

$$p_{v_k}^- \dots p_{v_1}^-(\mathcal{C}(P))$$

is in fact a triangulation of P *with vertices in* V*.*

iii. If in the above case $V = \{v_1, \dots, v_k\} \cup \{v_0\}$*, where* $\text{vert}(P) = \{v_1, \dots, v_k\}$ *is labeled in* $\{1, \dots, k\}$ *and* 0 *labels a point* v_0 *inside* P*, the triangulation*

$$p_{v_k}^- \dots p_{v_1}^- p_{v_0}^-(\mathcal{C}(P))$$

is pyramidal with apex v_0*.*

Any such triangulation (resp. subdivision) obtained by a labeling J as above will be referred to as the **pulling triangulation** (resp. subdivision) with respect to the labeling J.

PROOF. (i) and (ii) are dealt with in the sources referred to above.

Ad (iii): The first refinement $p_{v_0}^-(\mathcal{C}(P))$ consists of two classes of polytopes by the above rules. Firstly, all faces of P, since $v_0 \notin F$ for all faces F of P. Secondly, all pyramids of faces of P over v_0, since $v_0 \in P$, but $v_0 \notin F$ for all facets F of P, which implies that all elements of $\mathcal{C}(\text{conv}(F \cup \{v_0\}))$ are added for all facets F. Note that only the second step is actually required here. The claim then follows by (i). □

It is clear from this definition of the pulling triangulation that it can be read off the from face lattice of the polytope; that is, if we have a polytope P with k vertices labeled in some ordered set I of cardinality k, we can compute a pulling triangulation of it simply in terms of the image of the face lattice of P in 2^I: all the necessary information, which is of purely combinatorial nature, is accessible from there. In this sense we allow to speak of the pulling triangulation of an abstract lattice $\mathcal{F}$, that is (isomorphic to) the face lattice of some polytope: Given a lattice $\mathcal{F} \in 2^I$, at the i-th refinement step (for $i \in I$) we run through all $F \in \mathcal{F}$ and check whether $i \notin F$ to keep F part of the refinement or else replace F by the collection of sets $F' \cup \{i\}$ for each maximal subset $F' \subset F \backslash \{i\}$. Again this can easily be extended to arbitrary lexicographic triangulations.

LEMMA 4.2.2. *Let* S *be any set of combinatorially equivalent polytopal complexes with* k *vertices and let* I *be an ordered set of cardinality* k*. Let* $\mathcal{F}$ *be a representative of their face lattices in* 2^I*. For each* $\mathcal{C} \in S$ *fix an isomorphism from* $\mathcal{F}$ *to the face lattice* $\mathcal{F}_P$ *of* P*. Then*

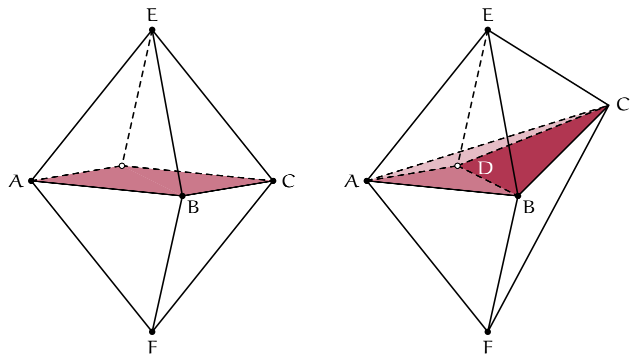
[2] By a labeling by some ordered set J we mean to express that there is some bijective map from J to V. This is depicted by enumerating the vertices in the above.

i. I *is a labeling for the vertices of* P,

ii. *for every abstract pulling (lexicographic) triangulation* $\mathcal{T}$ *of* $\mathcal{F}$, *the image* $\mathcal{T}_P$ *of* $\mathcal{T}$ *under the extension of* ϕ_P *defined on* $\mathcal{T}$ *is a pulling triangulation of* P.

This Lemma includes the case (iii) of Lemma 4.2.1. This construction will be applied later on (cf. Proposition 6.2.1).

Remark 4.2.3. A little note on the side: If P and P' are combinatorially equivalent polytopes, for which we fix a labeling of the vertices, in general it will not be true that a triangulation of P, given in terms of the labels, also gives a triangulation of P'. An example can be given by two octahedra:



In the right octahedron the complex generated by the 3-simplices

$$\operatorname{conv}\{A,B,C,D\}, \operatorname{conv}\{A,C,D,E\}, \operatorname{conv}\{A,B,C,E\}, \operatorname{conv}\{A,B,D,F\}, \text{ and } \operatorname{conv}\{B,C,D,F\}$$

is a triangulation. The translation of this triangulation in terms of the labels to the left octahedron fails to be a subdivision, in particular, it is not a triangulation: in the right octahedron $\operatorname{conv}\{A,B,C,D\}$ (the red one) is a simplex, it is not full dimensional in the left octahedron. Even if we would omit this polytope we would not obtain a subdivision of the left octahedron, the intersection of 3-simplices on different sides of $\operatorname{conv}\{A,B,C,D\}$ is never a common face of both.

However, if P and P' are equivalent in a stronger sense, namely if they have the same oriented matroid, then all triangulations can be translated (cf. Corollary 4.1.44. in [DRS10]). In our applications later on we will not be lucky enough to consider families of polytopes that are equivalent in this stronger sense. The mentioned defect of the polytope $\operatorname{conv}\{A,B,C,D\}$ not being of the same dimension in both octahedra is actually a proof of the inequivalence their oriented matroids.

But as stated above: not all hope is lost. If P and P' are combinatorially equivalent, then at least the lexicographic triangulations can be translated and we can even do so for polytopes with an interior point, used in a pyramidal triangulation. ■

4.3 Point sets and tilings in Euclidean space

In the subsequent (V,b) is an n-dimensional Euclidean space with norm $\|x\| := \sqrt{b(x,x)}$ and affine isometry group

$$\operatorname{Iso}(V,b) = \{\phi \in \operatorname{AGL}(V) \mid \forall x,y \in V: \ \|\phi(x)-\phi(y)\| = \|x-y\|\}.$$

4.3.1 Tilings

A **polytopal tiling** of V is a set $\mathcal{T}$ of full dimensional polytopes, such that $\bigcup_{P \in \mathcal{T}} P = V$, where for arbitrary $P, P' \in T$ the intersection $P \cap P'$ is a polytope of at most dimension $n-1$. Thus it is a covering and packing of space by polytopes. A tiling is **face-to-face** if for arbitrary $P, P' \in T$ the intersection $P \cap P'$ is a face (possibly empty) of both P and P', that is, if and only if T is the set of full dimensional polytopes of a polyhedral complex. A tiling is **facet-to-facet** if for $P, P' \in T$ with $n-1$-dimensional intersection $P \cap P'$, this intersection is a facet of both P and P'. A tiling is **locally finite** if each bounded set in V intersects only finitely many elements of $\mathcal{T}$.

If $\mathcal{T}$ is a locally finite polytopal tiling, it is face-to-face if and only if it is facet-to-facet (cf. [GR89]). In this case $\mathcal{T}$ induces a subdivision of the embedding space.

A tiling $\mathcal{T}$ for which all tiles are congruent to one another is called it is called **monohedral**. An isometry of a tiling $\mathcal{T}$ in a Euclidean space V is an affine isometry ϕ of V that fixes $\mathcal{T}$ under the induced action, that is for all $P \in \mathcal{T}$ also $\phi(P) \in \mathcal{T}$. If the isometry group of a tiling $\mathcal{T}$ operates transitively, the tiling is called **isohedral** (cf. [Eng93]).

4.3.2 Delone sets

A set $\Lambda \subset V$ is called **discrete** if and only if for each $v \in \Lambda$ there is some $\|\cdot\|$-ball $B_\varepsilon(v) \subset V$ such that $B_\varepsilon(v) \cap \Lambda = \{v\}$. A discrete set $\mathcal{P} \subset V$ is a **Delone set** or (r, R)**-system** if $B_r(p) \cap \mathcal{P} = \{p\}$ for all $p \in \mathcal{P}$ and if $B_R(x) \cap \mathcal{P} \neq \emptyset$ for all $x \in V$. Thus $\mathcal{P}$ is a Delone set if and only if the distance of arbitrary points $p, p' \in \mathcal{P}$ is at least r and from each point $x \in V$ there is a point $p \in \mathcal{P}$ of distance at most R. A vertex set having these properties is referred to as being **uniformly discrete** and **relatively dense** respectively.

A Delone set $\mathcal{P}$ is said to be **symmetric** if the (affine) isometry group

$$\mathrm{Iso}(\mathcal{P}, b) := \{\phi \in \mathrm{Iso}(V, b) \mid \phi(\mathcal{P}) = \mathcal{P}\},$$

of $\mathcal{P}$ acts transitive on $\mathcal{P}$.

An important example of Delone sets are Euclidean lattices and periodic sets. Furthermore lattices are always symmetric Delone sets.

4.3.3 Dirichlet-Voronoi cells and tilings of Delone sets

We will now meet the main object of interest of this Part:

DEFINITION 4.3.1 (DIRICHLET-VORONOI CELL). Let (V, b) be a Euclidean space with norm $\|\cdot\|$, and let $\mathcal{P} \subset V$ be discrete. The **Dirichlet-Voronoi cell** (or **DV-cell**) of an element $p \in \mathcal{P}$ relative to $\mathcal{P}$ and $\|\cdot\|$ is the set

$$\mathrm{DV}_{\mathcal{P},\|\cdot\|}(p) := \left\{ x \in V \;\middle|\; \|x - p\| \leqslant \|x - q\|, \;\; \forall q \in \mathcal{P} \right\}.$$

◆

Since the Dirichlet-Voronoi cell of a point of a discrete set $\mathcal{P}$ is defined as an intersection of half-spaces, it is natural to wonder if a finite number of half-spaces suffice and thus if it is a polyhedron in fact. Now $\mathcal{P}$ being discrete does not suffice to ensure this: there exist infinite discrete vertex sets such that there are non-polyhedral cells (cf., Example 2.1 in [Voi08a], also available as Beispiel 3.2.1 in [Voi08b]). However if $\mathcal{P}$ is finite (obviously), or a Delone set this can not happen, in such a case every Dirichlet-Voronoi cell is a polytope (cf. Theorem 2.2 in [Eng93] for the latter). In any case, the Dirichlet-Voronoi cells of discrete $\mathcal{P}$ will be **generalized polyhedra**, that is every intersection of such a cell with a polytope is itself a polytope (cf. Proposition 32.1 in [Gru07]).

Even though all Dirichlet-Voronoi cells we will deal with will be polytopes, we prefer the name "cell". At a later point (Definition 4.3.13 below) we will define another object, closely related to the notion of Dirichlet-Voronoi cell. This new object will be called a Dirichlet-Voronoi polytope, so some care in handling these objects is in order.

Of direct interest to us is the collection of all Dirichlet-Voronoi cells of points in $\mathcal{P}$ with respect to the norm $\|\cdot\|$:

$$\mathrm{DV}_{\mathcal{P}}(\|\cdot\|) := \left\{ \mathrm{DV}(p) \;\middle|\; p \in \mathcal{P} \right\}.$$

PROPOSITION 4.3.2. *Let $\mathcal{P}$ be a Delone set in Euclidean space (V, b) with norm $\|\cdot\|$. Then $\mathrm{DV}_{\mathcal{P}}(\|\cdot\|)$ is the set of full dimensional cells of a polytopal subdivision of V.*

The statement of the Proposition is well-known, cf., Corollary 32.1 in [Gru07] (being facet-to-facet) and Theorem 2.2 in [Eng93] (being polytopal).

The polytopal subdivision generated by $\mathrm{DV}_{\mathcal{P}}(\|\cdot\|)$ is called the **Dirichlet-Voronoi subdivision** of (V, b) relative to $\mathcal{P}$.

If $\mathcal{P}$ is a Delone set, such that $\mathrm{DV}_{\mathcal{P}}(\|\cdot\|)$ is monohedral (isohedral), we will by abuse of language call $\mathcal{P}$ itself **monohedral (isohedral)**.

REMARK 4.3.3. Note that the notion of a Dirichlet-Voronoi cell and tiling still make sense if we use a positive semi-definite bilinear or quadratic space. However, Dirichlet-Voronoi cells might be unbounded polyhedrons. ■

PROPOSITION 4.3.4. *Let $\mathcal{P}$ be a discrete set. If ϕ is an affine isometry of $\mathcal{P}$, then*

$$\mathrm{DV}_{\mathcal{P},Q}(\phi(x)) = \phi\left(\mathrm{DV}_{\mathcal{P},Q}(x)\right).$$

PROOF. By definition: $v \in \mathrm{DV}_{\mathcal{P},Q}(\phi(x)) \Leftrightarrow \|\phi(x) - v\|_Q \leqslant \|p - v\|_Q \;\forall p \in \mathcal{P}$. Since ϕ is an isometry, this is equivalent to $\|x - \phi^{-1}(v)\|_Q \leqslant \|\phi^{-1}(p) - \phi^{-1}(v)\|_Q \;\forall p \in \mathcal{P}$ which by $\phi(\mathcal{P}) = \mathcal{P}$ can be expressed as $\|x - \phi^{-1}(v)\|_Q \leqslant \|p - \phi^{-1}(v)\|_Q \;\forall p \in \mathcal{P}$. The latter clearly is equivalent to $\phi^{-1}(v) \in \mathrm{DV}_{\mathcal{P},Q}(x)$, as was claimed. □

COROLLARY 4.3.5. *Let $\mathcal{P} \subset V$ be a symmetric Delone set. Then $\mathrm{DV}_{\mathcal{P}}(\|\cdot\|)$ is an isohedral polytopal tiling of V. In particular, a symmetric periodic set is a monohedral periodic set.*

PROOF. If $p, p' \in \mathcal{P}$, there is an isometry of $\mathcal{P}$ mapping p to p' since $\mathcal{P}$ is symmetric. The Proposition above showed that any such isometry gives rise to an isometry of $\mathrm{DV}_{\mathcal{P}}(Q)$, mapping $\mathrm{DV}_{\mathcal{P},Q}(p)$ to $\mathrm{DV}_{\mathcal{P},Q}(p')$. Thus already the set of these isometries of $\mathrm{DV}_{\mathcal{P}}(Q)$ acts transitive. □

The above Corollary holds in particular in the case of a lattice (L, Q), where already the translations by lattice elements operate transitive on the set of all Dirichlet-Voronoi cells and $\mathrm{DV}_{L,Q}(x) = x + \mathrm{DV}_{L,Q}(0)$.

We will usually abbreviate $\mathrm{DV}(L,Q) = \mathrm{DV}_{L,Q}(0)$, as is common in the literature on lattices. If we deal with a coordinate representation $(\mathbb{Z}^n, Q)$ of a lattice, we might further abbreviate $\mathrm{DV}(Q) = \mathrm{DV}(\mathbb{Z}^n, Q)$; similarly we write $\mathrm{DV}(L) = \mathrm{DV}(L, \langle,\rangle) = \mathrm{DV}(L, I_n)$ if L is a basis representation in Euclidean standard space.

More generally, assume that $\mathcal{P}$ is a symmetric Delone set in (V,Q) and that $0 \in \mathcal{P}$. We will write $\mathrm{DV}(\mathcal{P}, Q) := \mathrm{DV}_{\mathcal{P}}(0)$ and refer to it as the Dirichlet-Voronoi cell $\mathcal{P}$, which seems justifiable by virtue of the transitive operation of $\mathrm{Iso}(\mathcal{P}, Q)$. If $Q = I_n$, i.e., $\mathcal{P}$ is in Euclidean standard space, we abbreviate further and write $\mathrm{DV}(\mathcal{P})$. In the case $\mathcal{P} = \Lambda_t$ on (V,Q), we write $\mathrm{DV}(Q, \mathbf{t})$ in resemblance of the above definition for lattices.

We give another example of symmetric Delone sets.

LEMMA 4.3.6. *Let* L *be a lattice and* $v \notin L$. *Then* $\Lambda := L \mathbin{\dot\cup} v + L$ *is a symmetric periodic set. In fact, if* $T(L)$ *denotes the group of translations by elements of* L *and* $\phi_{\frac{1}{2}v}$ *denotes the point reflection with center* $\frac{1}{2}v$, *then* $T(L) \rtimes \langle \phi_{\frac{1}{2}v} \rangle < \mathrm{Iso}(\Lambda)$ *acts transitively on* Λ.

PROOF. Let τ_x denote the translation by x. Then $\phi_{\frac{1}{2}v}$ is given by $-\mathrm{id} \circ \tau_{-v} = \tau_{\frac{1}{2}v} \circ -\mathrm{id} \circ \tau_{-\frac{1}{2}v}$, it is an isometry, and interchanges L and $v + L$:

$$\begin{cases} -\mathrm{id} \circ \tau_{-v}(x) \in v + L & \text{for } x \in L, \\ -\mathrm{id} \circ \tau_{-v}(x) \in v & \text{for } x \in v + L. \end{cases}$$

Since $T(G)$ acts transitively on L the claim follows immediately. □

For monohedral periodic sets, in particular for lattices, the volume of a Dirichlet-Voronoi cell and the determinant of a translation lattice are closely related.

LEMMA 4.3.7. *Let* Λ *be a monohedral periodic set in* $(\mathbb{R}^n, b)$, *which is* m*-periodic for a translation lattice* L. *Then*

$$\mathrm{vol}_b(\mathrm{DV}(\Lambda)) = \frac{\mathrm{vol}(L,b)}{m} = \frac{\sqrt{\det(L,b)}}{m}.$$

PROOF. The lattice case first: $\mathrm{DV}(L)$ is a fundamental domain of L (cf. 4.3.2), therefore $\mathrm{vol}_b(\mathrm{DV}(L)) = \mathrm{vol}_b(\mathcal{F}_{\mathcal{B}}(L)) = \mathrm{vol}(L,b)$.

If Λ is as above, then $\mathcal{F} := \bigcup_{i=1}^{m} \mathrm{DV}_{\Lambda}(t_i)$ is a fundamental domain for L. Thus

$$\mathrm{vol}_b(\mathrm{DV}(\Lambda)) = \frac{1}{m}\mathrm{vol}_b(\mathcal{F}) = \frac{1}{m}\mathrm{vol}_b(\mathcal{F}_{\mathcal{B}}(L)) = \frac{\mathrm{vol}(L,b)}{m}.$$ □

So in the case of monohedral periodic sets it makes sense to speak of the **volume** of such a set if we understand that this is the volume of its Dirichlet-Voronoi cell.

4.3.4 Delone polytopes of point sets

Though we are ultimately interested in Dirichlet-Voronoi cells, Delone polytopes and subdivisions will play a crucial role.

DEFINITION 4.3.8 (DELONE POLYTOPE). Let $\mathcal{P}$ be a discrete vertex set and let $P \subset V$ be a polyhedron with vertex set $\mathrm{vert}(P) \subset \mathcal{P}$. P is a **Delone polyhedron** (with respect to $\mathcal{P}$ and $\|\cdot\|$) if there exists $c \in V$ and $r \in \mathbb{R}$ with $\|c - p\| \geqslant r$ for all $p \in \mathcal{P}$, where $\|c - p\| = r$ if and only if $p \in \mathrm{vert}(P)$. ◆

The definition above is equivalent to P satisfying the **empty-sphere property**: P is a Delone polyhedron if and only if there exists a $\|\cdot\|$-ball $B = B_r(c) \subset V$ such that $B \cap \mathcal{P} = \mathrm{vert}(P)$.

In general, an arbitrary discrete set in a Euclidean space does not have to admit Delone polyhedra. However if $\mathcal{P} \subset V$ is a Delone set, they exist and are polytopes due to the definiteness of b and discreteness of $\mathcal{P}$. Even better: they make up a polytopal subdivision of the enveloping space. This can be seen as follows: for any sphere S in (V, b) that contains no point of $\mathcal{P}$ we construct the polytope $P := \mathrm{conv}(S \cap \mathcal{P})$. Then P is a Delone polytope, we say that it is constructed by the **empty-sphere method**. It is full-dimensional if the intersection of $\mathcal{P}$ and S contains an affine basis.

PROPOSITION 4.3.9. *Let $\mathcal{P}$ be a Delone set in (V, b) with norm $\|\cdot\|$. Then the set of polytopes constructed by the empty-sphere method is the polyhedral complex generated by the full-dimensional Delone polytopes.*

PROOF. This is the combination of Proposition 32.2 and Theorem 32.1 in [Gru07], there stated as Corollary 32.1 for Delone triangulations, though valid for arbitrary Delone subdivisions. □

DEFINITION 4.3.10. Let $\mathcal{P}$ be a Delone set in (V, b). The polytopal complex of Proposition 4.3.9 is called the **Delone subdivision** of (V, b) relative to $\mathcal{P}$. We write $\mathrm{Del}_{\mathcal{P}}(\|\cdot\|)$ for this subdivision. ◆

There is an alternative way of constructing the Delone subdivision of a Delone set, by a lifting construction, which we mention very briefly. Let $\mathcal{P} \subset V$ be a Delone set and let $\omega : V \to V \times \mathbb{R};\ x \mapsto (x, \|x\|^2)$. Then $\mathrm{conv}(\omega(\mathcal{P}))$ is a generalized polyhedron. All faces of this generalized polyhedron are lower in the following sense: if F is a face of P and $x \in F$, then for all $\varepsilon > 0$ the point $x + \varepsilon(0, -1) \in V \times \mathbb{R}$ is not contained in P. Now one can check that the projection of the (lower) faces of P back to V (i.e., forgetting the last coordinate) gives a polytopal complex, which is in fact the Delone subdivision of V (cf. 32.1 in [Gru07]).

We are mostly interested in the case where $\mathcal{P}$ is a periodic vertex set embedded in a quadratic space (V, Q). In this case we write $\mathrm{Del}_{\mathcal{P}}(Q)$ for $\mathrm{Del}_{\mathcal{P}}(\|\cdot\|_Q)$.

REMARK 4.3.11. Note that the above Definitions and Proposition also make sense if we consider a positive-definite bilinear space. What changes is that now there can be unbounded Delone polyhedra. But they are still constructible by the empty-sphere method and make up a polyhedral complex, which we will then also refer to as Delone subdivision (cf. (1.7) in [Nam76]) or 2.1 in [Val03]). ■

REMARK 4.3.12. It is also possible to define Delone and Dirichlet-Voronoi subdivisions by a lifting construction, we refer the interested reader to Chapter 32 in [Gru07]. ■

4.3.5 Dirichlet-Voronoi polytopes in dual space

We will now define what we understand to be a Dirichlet-Voronoi polytope. These objects are closely related to Dirichlet-Voronoi cells, but have certain advantages for us, in particular when dealing with coordinate representations of Euclidean lattices $L = (\mathbb{Z}^n, Q)$. This definition is, in its generality, due to [Nam76] in the case of $\mathcal{P} = \mathbb{Z}^n$, but all of the properties we are interested in here also hold for the case of an arbitrary Delone set. Namikawas definition resembles Voronoi's original approach to what is now called a Dirichlet-Voronoi cell (cf. Equation (10) in [Vor08]). The usefulness of this Definition in a similar context can already be seen in [Val03], where the main application is the lattice covering problem. In particular we adapt the modern notation used by Vallentin.

DEFINITION 4.3.13 (DIRICHLET-VORONOI POLYTOPE). Let (V, b) be a Euclidean space with norm $\|\cdot\|$ and quadratic form $Q \in \mathcal{S}^n_{>0}$ with associated bilinear form $b = b_Q$. Let $\mathcal{P} \subset V$ be a Delone set and $P = \operatorname{conv}\{p_1, p_2, \dots\}$ be a Delone polyhedron of Q in $\mathcal{P}$. The polytope

$$\operatorname{DV}(Q, P) := \left\{ \ \hat{b}(x) \in V^* \ \middle| \ \|x - p_i\| \leqslant \|x - p\|, \ \forall p \in \mathcal{P} \ \right\}$$

is called the **Dirichlet-Voronoi polytope** of Q corresponding to P with respect to $\mathcal{P}$. ◆

The object defined above actually is a bounded polyhedron, thus a polytope, even if we apply the above definition to the case of a positive-semidefinite quadratic form (cf. (1.7) in [Nam76]).

Recall that the map $\hat{b} : V \to V^*$ is given by $\hat{b}(x) = b(x, \cdot)$ (cf 1.1.5).

Now if $Q \in \mathcal{S}^n_{>0}$, it is the quadratic form associated to the Euclidean space $(\mathbb{R}^n, \frac{1}{2}b_Q)$. Since b_Q and $\frac{1}{2}b_Q$ are just scaled versions of one another, it actually does not make a difference which of the two bilinear forms we use for the definition. In particular $\operatorname{DV}(Q, P) = \operatorname{DV}(\lambda Q, P)$ for all $\lambda \in \mathbb{R}_{>0}$.

The concept of Dirichlet-Voronoi cell and polytope are closely related, we state it as a Lemma.

LEMMA 4.3.14. *Let $\mathcal{P}$ be a Delone set and $Q \in \mathcal{S}^n_{>0}$ with associated bilinear form $b = b_Q$. Then for $p \in \mathcal{P}$*

$$\operatorname{DV}_{\mathcal{P}}(Q, \{p\}) = \hat{b}(\operatorname{DV}_{\mathcal{P},Q}(p)).$$

In particular $\operatorname{DV}_{\mathcal{P},Q}(p)$ and $\operatorname{DV}_{\mathcal{P}}(Q, \{p\})$ are affinely isomorphic. □

In particular for the case of a lattice (L, Q) we obtain that

$$\operatorname{DV}_L(Q, \{0\}) = \hat{b}(\operatorname{DV}(L, Q)).$$

Analogously for an m-periodic set Λ with translation vectors $t_1, \dots, t_m$

$$\operatorname{DV}_\Lambda(Q, \{t_i\}) = \hat{b}(\operatorname{DV}_{\Lambda,Q}(t_i)).$$

4.3.6 Duality of Dirichlet-Voronoi and Delone subdivisions

Dirichlet-Voronoi and Delone subdivisions are combinatorially dual objects. This becomes even more apparent if we switch Dirichlet-Voronoi cells with the associated Dirichlet-Voronoi polytopes.

The following properties of Delone and Dirichlet-Voronoi polytopes will be useful, they can be found as part of (1.4) in [Nam76] if we replace $\mathbb{Z}^n$ by $\mathcal{P}$.

PROPOSITION 4.3.15. *Let $Q \in \mathcal{S}^n_{>0}$, $\mathcal{P}$ be a Delone set.*

i. For $P, P' \in \operatorname{Del}_{\mathcal{P}}(Q)$ we have that P is a face of P' if and only if $\operatorname{DV}(Q, P')$ is a face of $\operatorname{DV}(Q, P)$.

ii. For $P \in \operatorname{Del}_{\mathcal{P}}(Q)$ we have $\dim(P) + \dim(\operatorname{DV}(Q, P)) = n$.

By identifying $\mathbb{R}^n$ with $\mathbb{R}^{n*}$ by means of the standard inner product, it is easy to derive the following Lemma.

LEMMA 4.3.16. *Let $\mathcal{P}$ be a Delone set. For $Q, Q' \in \mathcal{S}^n_{>0}$ with $\mathrm{Del}_{\mathcal{P}}(Q) = \mathrm{Del}_{\mathcal{P}}(Q')$, the normal fans of the Dirichlet-Voronoi polytopes $\mathrm{DV}(Q, P)$ and $\mathrm{DV}(Q', P)$ coincide.*

SKETCH OF PROOF. Represent $\mathrm{DV}(Q, P)$ by elements of the form Qx of $\mathbb{R}^n$. Then all (not necessarily relevant) defining inequalities of this polytope look like

$$2(p_i - p)^T Qx \geqslant \|p_i\|_Q^2 - \|p\|_Q^2,$$

for suitable $p \in \mathcal{P}$ and $p_i \in \mathrm{vert}(P)$. In particular this holds for those inequalities relevant to a given face. In any case this implies that for Q, Q' as assumed, the polytopes are described by a system $Ax \geqslant b$ and $Ax \geqslant b'$ respectively (where the i-th row of A is a suitable $2(p_i - p)^T$), but this implies the claim.□

This in particular implies that the facet normals are characterized completely by $\Delta_{\mathcal{P}}(Q)$ and coincide for quadratic forms that induce the same Delone subdivision.

The duality of the Delone and Dirichlet-Voronoi subdivision of a space (V, Q) implies a straightforward characterization of the vertices of the Dirichlet-Voronoi cell of a point by its star in the Delone subdivision:

LEMMA 4.3.17. *Let $\mathcal{P}$ be a Delone set in a quadratic space (V, Q) with norm $\|\cdot\|_Q$. Then*

$$\mathrm{vert}(\mathrm{DV}_{\mathcal{P},Q}(p)) = \{\mathrm{centroid}_Q(D) \mid D \in \mathrm{star}(p, \mathcal{D}),\ \dim(D) = n\},$$

where $\mathrm{centroid}_Q(D)$ is the center of the $\|\cdot\|_Q$-circumsphere of D.

Chapter

5 Periodic vector quantization

This chapter contains a brief presentation of some of the main notions regarding vector quantization. It is included for the sole purpose of providing a self-contained overview about the main notions of vector quantization for a reader not yet familiar with this subject. We try to make a case for the importance of the quantizer constant within this problem. For a more detailed accounts we refer to [GG12] and [Zam14], the subsequent discussion is strongly based on these sources.

5.1 The normalized second moment and the quantizer constant

Given a body[1] $P \subset \mathbb{R}^n$ and a point $\hat{x}$ we define the **second moment** of P about $\hat{x}$ by

$$U(P) := \int_P \|x - \hat{x}\|^2 dx,$$

the **normalized second moment**

$$I(P) := \frac{U(P)}{\mathrm{vol}(P)},$$

and finally the **dimensionless normalized second moment**

$$G(P) := \frac{1}{n} \frac{U(P)}{\mathrm{vol}(P)^{1+2/n}} = \frac{1}{n} \frac{I(P)}{\mathrm{vol}(P)^{2/n}}.$$

We use the notation that is more common in the mathematical literature, as used by Conway and Sloane, cf. [CS98, Chapter 21]. However one should note that in much of the literature in information or coding theory, the name second moment is used for what we call the dimensionless second moment, denoted $\sigma^2(P) = \frac{1}{n}U(P)$, and the term normalized second moment is as well understood to be dimensionless, cf. [Zam14].

We now use the notation of Chapter 6 concerning Dirichlet-Voronoi cells. For a lattice L we set

$$G(L) := G(DV(L))$$

[1] We do not get into technicalities here: we only need this notion for convex polytopes and ellipsoids in the remainder. For such objects the notions discussed here clearly make sense.

and for any periodic set Λ with congruent Dirichlet-Voronoi cells we also abbreviate

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

The use of lattices and periodic sets in quantization motivates another name for $G(\Lambda)$, it is sometimes referred to as the **quantizer constant** of Λ. We will usually use this nomenclature from here on.

Thus for a lattice L in Euclidean standard space

$$G(L) = \frac{1}{n} \frac{1}{\det(L)^{1/2+1/n}} \int_{DV(L)} \|x\|^2 dx,$$

and for an m-periodic set $\Lambda = \bigcup_{i=1}^m t_i + L$ in Euclidean standard space, for which all Dirichlet-Voronoi cells are congruent

$$G(\Lambda) = \frac{1}{n} \frac{m^{1+2/n}}{\det(L)^{1/2+1/n}} \int_{DV(\Lambda)} \|x\|^2 dx,$$

by relating the volume of a Dirichlet-Voronoi cell to the determinant of the lattice involved (cf. Chapter 6, Lemma 4.3.7).

If we are in the more general situation of a Euclidean space $(\mathbb{R}, b)$, where Q is the Gram matrix of some inner product b, we find for a lattice

$$G_b(L) = \frac{1}{n} \frac{1}{(\det(Q)^{1/2} \det(L))^{1/2+1/n}} \int_{DV(L,Q)} \|x\|_Q^2 dx,$$

and for an m-periodic set $\Lambda = \bigcup_{i=1}^m t_i + L$ in Euclidean standard space, for which all Dirichlet-Voronoi cells are congruent

$$G_b(\Lambda) = \frac{1}{n} \frac{m^{1+2/n}}{(\det(Q)^{1/2} \det(L))^{1/2+1/n}} \int_{DV(\Lambda,Q)} \|x\|_Q^2 dx.$$

In this situation we also think of $G_b(\Lambda)$ as "a quantizer constant", but now referring to a different distortion measure. This will be elaborated on in 5.2.2 and 5.2.4 below.

5.2 VECTOR QUANTIZATION

5.2.1 General notions for vector quantization

In information and coding theory a (finite) **vector quantizer** of dimension or block length n and size N is given by specification of a finite set $\mathcal{C}$ of cardinality N and a map $\mathcal{Q} : \mathbb{R}^n \to \mathcal{C}$, where $\mathcal{C}$ is called the **codebook**, its elements the **codewords** or **code vectors**, and $\mathcal{Q}$ is known as the **quantization rule**. We assume that the elements of $\mathcal{C}$ are indexed by $\{1, \dots, N\}$. An associated quantity is the **resolution** $r := (\log_2 N)/n$, also called **code rate**. To each $c \in \mathcal{C}$ there is associated a **quantizer cell** $\mathcal{Q}^{-1}(c) = \{x \in \mathbb{R}^n \mid \mathcal{Q}(x) = c\}$, and the collection of all cells gives a partition of $\mathbb{R}^n$. We divide cells into two types, either they are bounded and called **granular** cell, or they are unbounded and called **overload** cell. The collection of either of those is then refered to granular and overload region respectively. A vector quantizer is called **regular** if all of its cells are convex, and it is called **polytopal** if each cell is a polyhedron.

To describe and analyze the application of vector quantizers in source coding it is usually decomposed into two seperate objects. On the one hand we have the **encoder** $\mathcal{E} : \mathbb{R}^n \to \{1, \dots, N\}$ and on the other hand the **decoder** $\mathcal{D} : \{1, \dots, N\} \to \mathbb{R}^n$. We do not wish to go into detail here and refer to [GG12, section 10.1]. The idea of encoding is that the encoder first chooses a suitable $c \in \mathcal{C}$ by finding the cell that contains a given source vector and then determines the index of said cell. Both tasks can become arbitrarily difficult, but can be dealt with for certain structured vector quantizers as we will elaborate on in a bit.

5.2.2 The performance of a vector quantizer

Let $\mathbf{X}$ be continuously distributed random vector in $\mathbb{R}^n$ with probability density function $f_{\mathbf{X}}$. Let d be a distortion measure, that is, a nonnegative function of $\mathbf{X}$ and its reproduction $\mathcal{Q}(\mathbf{X})$ under quantization. We assume that $f_{\mathbf{X}}$ is a joint probability density function for the components of $\mathbf{X}$. Let $\{\mathbf{X}_t\}$ be a (discrete time) random process constituted of random vectors, we assume from here on that it is independent and identically distributed (abbreviated by i.i.d.). If this process is stationary and ergodic we find, that with probability one the limit on the left side exists and satisfies

$$\lim_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} d(\mathbf{X}, \mathcal{Q}(\mathbf{X})) = \mathbb{E}(d(\mathbf{X}, \mathcal{Q}(\mathbf{X}))).$$

Here $\lim_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} d(\mathbf{X}, \mathcal{Q}(\mathbf{X}))$ is the **time average** of the distortion and $D = \mathbb{E}(d(\mathbf{X}, \mathcal{Q}(\mathbf{X})))$ is the **average distortion** of the coding scheme (cf. 10.3 in [GG12]). For the vector quantization scheme this can then be expressed by

$$D = \int d(x, \mathcal{Q}(x)) f_{\mathbf{X}}(x) dx \tag{5.1}$$

or with the partition of $\mathbb{R}^n$ given by the quantizer cells as

$$D = \sum_{c\in\mathcal{C}} P_c \mathbb{E}[d(x, c) \mid \mathbf{X} \in \mathcal{Q}^{-1}(c)]$$

where for $c \in \mathcal{C}$ we set $P_c = P(\mathbf{X} \in \mathcal{Q}^{-1}(c))$ to be the probability of $\mathbf{X}$ lying in the cell associated to c.

Of particular interest is the **squared error** distortion measure given by the squared Euclidean distance of x and its reproduction $Q(x)$

$$d(x, Q(x)) = \|x - Q(x)\|^2.$$

The reason behind this choice lies rather in the mathematical tractability of this measure, than its actual performance for various media. In any case, it can be interpreted as the energy of power of an error, which gives it some physical significance (cf. 2.4 in [Gra12]).

We also want to introduce the **weighted squared error** measure given by some positive definite bilinear form b through $d(x, \mathcal{Q}(x)) = b(x-y, x-y) = \|x-y\|_b^2$, where the **Mahalanobis distortion measure** is a special case, with b chosen in such a way that the Gram matrix of b with respect to the standard basis is given by the covariance matrix of the source vector $\mathbf{X}$. In the case of an i.i.d. Gaussian source with unit variance and zero mean the Mahalanobis distortion measure and the squared error coincide.

The squared error distortion measure also falls into the realm of **single letter** distortion measures of the form $d(\mathbf{X}, \hat{\mathbf{X}}) = \sum_{i=1}^{n} d_m(X_i, \hat{X}_i)$, where d_m is a scalar distortion measure, the **per-letter** distortion measure.

Two well-known optimality criteria in vector quantization are the **nearest neighbor** condition and the **centroid** condition. The nearest neighbor condition states that given a codebook $\mathcal{C}$ and a distortion measure d the optimal choice of the quantizer rule, and thus cell decomposition of $\mathbb{R}^n$ associated to $\mathcal{Q}$, has to satisfy

$$\mathcal{Q}(x) = c \Rightarrow d(x, c) = \min\{d(x, c') \mid c' \in \mathcal{C}\}.$$

It is not an "if and only if" statement because the codeword c minimizing the right hand side might not be unique. Therefore the quantizer cells have to lie between the interior and closure of the Dirichlet-Voronoi cells of the codewords with respect to the chosen distortion measure. If on the other hand the cell decomposition $\{C_1, \ldots, C_N\}$ of $\mathbb{R}^n$ is given and the codebook has to be chosen, the centroid condition states that the optimal choice of $\mathcal{C} = \{c_1, \ldots, c_N\}$ has to satisfy

$$c_i = \text{centroid}_d(C_i) \text{ for all } i \in \{1, \ldots, N\},$$

where $\text{centroid}_d(C) = \arg\min\{\mathbb{E}[d(\mathbf{X}, c) \mid \mathbf{X} \in C]\}$. The easy proofs may for example be found in [GG12, 11.2].

5.2.3 Periodic vector quantization with the squared error distortion measure

We now turn our attention to quantizers whose codebooks come from a (monohedral) periodic set $\Lambda \subset \mathbb{R}^n$ - which is assumed to generate $\mathbb{R}^n$. Before focusing on how to quantize, we want to quickly point out that there are two ways to cope with the infinite size of Λ. One approach is to chose a finite subset $\mathcal{C}$, the other idea is to work with the, infinite, periodic set as codebook, but applying some sort of entropy coding to obtain a notion of coding-rate that is finite. The book [Zam14] offers a quite recent and rather detailed introduction and discussion of these information theoretic aspects of vector quantization. Let us only briefly mention, without discussion of the results, that the below rough estimation of the quality of a quantizer in terms of the quantizer constant is completely justified by taking a closer look on the results of information theory: it is always the quantizer constant which has to be as small as possible for a quantization scheme to work well.

We concentrate our attention to distortion measures coming from Euclidean geometry, that is in most cases the squared Euclidean distance, but we should also keep the weighted squared error measure in mind. However, as discussed above, it is no restriction of generality to assume that d is the standard squared error distortion measure.

There is a widely known and widely accepted conjecture of Gersho regarding vector quantization: the optimal quantizer will have cells that are all congruent to some polytope. This is discussed in his 1979 work [Ger79]. We will therefore restrict our attention to monohedral periodic sets, so that all Dirichlet-Voronoi cells are congruent. We will call the resulting quantizer a **monohedral periodic quantizer**. Mathematically rather well tractable special cases of monohedral periodic sets are symmetric periodic and, above all, lattices.

If Λ is in fact a lattice, we will refer to the resulting quantizer as **lattice quantizer**.

The basic idea is similar in both cases. Let $\mathcal{C} \subset \Lambda$ be the codebook chosen from Λ. Respecting the optimality criteria presented above we start with the Dirichlet-Voronoi subdivision (cf. Definition 4.3.3) of $\mathbb{R}^n$ induced by $\mathcal{C}$, and map an element $x \in \mathbb{R}^n$ to the centroid of the Dirichlet-Voronoi cell it is contained in, or to any one of those centroids of such cells if x is contained in more than one, where a tie may be broken in an arbitrary way.

The easiest example, which indeed is a lattice quantizer, that albeit captures the mathematical essence of this idea, is that of rounding, which we can interpret as using the lattice $\mathbb{Z} \subset \mathbb{R}$ with $Q(x) = [x]$. Thus the quantizer cells are given by the half-open intervals of the form $[z - 1/2, z + 1/2)$ for $z \in \mathbb{Z}$.

Now given a symmetric periodic set $\Lambda \subset \mathbb{R}^n$ and the squared error distortion measure $d(x, y) = \|x - y\|^2$ the above summarizes in taking the quantization rule to be given by

$$Q : \mathbb{R}^n \to \Lambda;\ x \mapsto \arg\min_{\lambda \in \Lambda} \|x - \lambda\|$$

where ties might be broken in an arbitrary way. The quantizer cell of a given $\lambda \in \Lambda$ is then essentially given by its Dirichlet-Voronoi cell $DV_\Lambda(\lambda) = \{x \in \mathbb{R}^n \mid \|x - \lambda\| \leqslant \|x - \lambda'\|, \text{ for all } \lambda' \in \Lambda\}$. This is a bit imprecise however, as noted before. To obtain a well-defined map Q we were in need to break ties, that is a point $x \in \mathbb{R}^n$ lying on the boundary of $DV_\Lambda(\lambda)$ may not satisfy $Q(x) = \lambda$. This fortunately is not a problem in the analysis or design of such quantizers since $DV_\Lambda(\lambda)^o \subset Q(\lambda)^{-1} \subset DV_\Lambda(\lambda)$, implying that $DV_\Lambda(\lambda) \backslash Q(\lambda)^{-1}$ is a null set, regardless of the way a tie is broken. For the sake of analysis we will therefore assume that equality on the right hand side holds, and by abuse of language we will therefore sometimes refer to $DV_\Lambda(\lambda)$ as the quantizer cell of λ.

Assuming squared euclidean distance we now focus on the average distortion, which we will refer to as **mean squared error**. The easiest case would be that of a uniform source of finite support $\mathcal{S}$, where $\mathcal{C} = \Lambda \cap \mathcal{S}$. Then the integral in (5.1) becomes

$$D = \int_{\mathcal{S}} \|x - Q(x)\|^2 dx = \int_{\mathcal{S}_G} \|x - Q(x)\|^2 dx + \int_{\mathcal{S}_O} \|x - Q(x)\|^2 dx$$

where $\mathcal{S}_G$ and $\mathcal{S}_O$ shall denote the intersection of the granular and overload region with $\mathcal{S}$ respectively.

For more complicated and possibly unbounded sources lattice quantization is often used under the assumption of high, but finite, resolution. We will formulate the analysis for periodic quantizers and then return to the special case of lattices in a moment. To keep this discussion brief we restrict ourselves to say that under the high resolution assumption we assume that the rate grows so large that the source distribution among each cell becomes approximately uniform (cf. [GG12, 10.6]). We therefore can approximate the average distortion

$$D \approx \sum_{\lambda \in \mathcal{C}} f(\lambda) \int_{DV_\Lambda(\lambda)} \|x - \lambda\|^2 dx,$$

where we assume that $f_{\mathbf{X}}(v) \approx f(\lambda)$ for all $v \in DV_\Lambda(\lambda)$. With $P_\lambda := \Pr(\mathbf{X} \in DV_\Lambda(\lambda)) \approx f(\lambda) \cdot \mathrm{vol}(DV_\Lambda(\lambda))$ we get

$$D \approx \sum_{\lambda \in \mathcal{C}} \frac{P_\lambda}{\mathrm{vol}(DV_\Lambda(\lambda))} \int_{DV_\Lambda(\lambda)} \|x - \lambda\|^2 dx.$$

This analysis refines when Λ is a monohedral periodic set, since then all Dirichlet-Voronoi cells in the granular region are congruent (cf. 4.3.3)). Therefore in such a case we can approximate the granular contribution to the average distortion by

$$D_G \approx \frac{1}{\mathrm{vol}(DV(\Lambda))} \int_{DV(\Lambda)} \|x\|^2 dx \tag{5.2}$$

where we assume that almost all inputs fall into the granular region. Under the high resolution assumption one usually assumes furthermore that D_O is neglectable compared to D_G, so that (5.2) becomes a good approximation of the average distortion itself.

If we follow these lines we can express the distortion through the dimensionless normalized second moment of $DV(\Lambda)$ by

$$D \approx N \cdot I(DV(\Lambda)) = N \cdot n \cdot \mathrm{vol}(DV(\Lambda))^{1+2/n} \cdot G(DV(\Lambda)).$$

For a lattice L this simplifies to

$$D \approx N \cdot I(DV(L)) = N \cdot n \cdot \det(L)^{1/2+1/n} \cdot G(L),$$

since $\mathrm{vol}(DV(L)) = \sqrt{\det(L)}$ in this case.

It is this relation (and in more sophisticated schemes certain similar relations, cf. [Zam14] for a recent textbook treatment) that justify to call $G(\Lambda)$ quantizer constant.

5.2.4 Periodic vector quantization with the weighted squared error case distortion measure

Surely, if b is some positive definite bilinear form and we consider the euclidean space $(\mathbb{R}^n, b)$, and if Q is the gram matrix of b with respect to the standard basis, there is an isometry of this space to Euclidean standard space by mapping the standard basis in $\mathbb{R}^n$ to any basis that consist of the columns of any matrix A that satisfies $Q = A^T A$. Such a matrix always exists as is well-known, i.e., per Cholesky decomposition. This can be utilized to reduce the more general case of weighted squared error to the case of standard squared error. Clearly if one follows through the above arguments for the squared error distortion measure one obtains similar formulae for the distortion with G_b replacing G. But

$$G_b(\Lambda) = \det(A)^{-1} G(A\Lambda),$$

as is seen by invoking the formula for change of variables in integration (cf. the reasoning in Lemma 6.3.2). If b is fixed, then this shows that finding the minimal value of G_b is equivalent to finding the minimal value for G.

Chapter

6 Dirichlet-Voronoi cells and their normalised second moments

This chapter contains some of the main results of this thesis. We aim at contributing to certain mathematical facets of the quantizer problem, given that the codebook is a periodic set. In particular, the most prominent case of lattice codebooks lies at the very center of the subsequent investigations. We derive polynomial optimization problems related to the quantizer problem, a piecewise explicit expression for the quantizer constant of suitable periodic sets, and prove that $A_4^\#$ and $D_4^\#$ are local minima in the class of 4-dimensional lattices.

We will recall some well-known notation and results of Voronoi's second reduction theory, which we use as a main tool in our investigations. We then apply this theory to start a systematic investigation of the quantizer constant for (monohedral) periodic sets. This generalizes the special result that the root lattice $A_3^\# \cong D_3^\#$ is the sole local and thus global minimum of the lattice quantizer problem in dimension 3 (cf. [BS83]).

We fix a rational standard periodic set $\Lambda_\mathbf{t}$ and take a look at all periodic forms $(Q, \mathbf{t})$, or equivalently all periodic sets $(\Lambda_\mathbf{t}, Q)$. We can utilize Voronoi's second reduction theory to obtain a finite partition of $\mathcal{S}^n_{>0} \times \{t\}/\mathrm{GL}^\mathbf{t}_n(\mathbb{Z})$. This leads to a finite number of local quantizer problems in each dimension for the chosen standard periodic set. Unfortunately, even for lattices, the number of distinct local quantizer problems grows to be inaccessible beyond dimension 5.

From this we derive the main results of this part: the general problem of finding the optimal quantizer, with respect to a periodic codebook satisfying certain conditions (cf. Assumption 6.3.1), can be split into a finite number of polynomial optimization problems (cf. 6.3.7). A particular class of periodic sets that satisfy Assumption 6.3.1 without further ado, is the class of lattices. We furthermore show that for the partition of $\mathcal{S}^n_{>0}$ into secondary cones, there exists a piecewise explicit expression of the quantizer constant, viewed as a function $\mathcal{S}^n_{>0} \to \mathbb{R}_{>0}$. The restriction of this function to each secondary cone can be written as the quotient of a polynomial in Q, depending only on the secondary cone, and a power of $\det(Q)$ (cf. 6.3.9). For the three inequivalent secondary cones in dimension 4 we compute these explicit expressions (cf. 6.4.3, in particular, (6.10), (6.11), and (6.12)). We conclude this part with an application of the result to local optimality of lattices in dimension 4 (cf. 6.4.4).

6.1 VORONOI'S SECOND REDUCTION THEORY

We sketch out the basic notions of this theory, following the treatment in [Sch09] and [Val03], to keep this thesis as self contained as possible.

From now on we will restrict to discrete vertex sets that are periodic, including the classical case of lattices.

6.1.1 Secondary cones of Delone triangulations and subdivisions

Let $\Lambda = \Lambda_{\mathbf{t}}$ be a standard discrete periodic vertex set $\Lambda_{\mathbf{t}} = \bigcup_{i=1}^{m} t_i + \mathbb{Z}^n$ and T be a linear subspace of $\mathcal{S}^n$.

We ultimately are interested in classifying all essentially different Delone triangulations of Λ that occur by varying the quadratic form defining the geometry in $\mathcal{S}^n_{>0} \cap T$. From a technical point of view it is more appropriate to work in the larger set $\tilde{\mathcal{S}}^n_{\geqslant 0} \cap T = \text{cone}\{xx^T \mid x \in \mathbb{Z}^n\} \cap T$, which is the rational closure of $\mathcal{S}^n_{>0} \cap T$ (cf. Proposition 4.2 in [Sch09]).

Suppose $Q \in \mathcal{S}^n_{>0}$. Then we can construct Delone polytopes for Λ as follows: take $n+1$ affinely independent elements of Λ, construct the circumsphere of the simplex they define. If there are points of Λ inside the associated ball, there is no Delone polytope which contains the chosen elements as vertices; if there are no points of Λ inside this ball, the convex hull of the set of all elements of Λ, which lie on the boundary of the constructed ball, is a Delone polytope by construction. This is the empty-sphere method (cf. Section 4.3.4).

This does not work for an arbitrary $Q \in \mathcal{S}^n_{\geqslant 0}$. However, by the reasoning above it can bee seen to hold for such $Q \in \mathcal{S}_{\geqslant 0}$ for which there exists a $U \in GL_n\, Z)$ such that

$$U^T Q U = \begin{pmatrix} 0 & 0 \\ 0 & Q' \end{pmatrix},$$

with $Q' \in \mathcal{S}^n_{>0}$. In this case the Delone subdivision will contain unbounded polyhedra. As it turns out this is it, a form $Q \in \mathcal{S}^n_{\geqslant 0}$ admits Delone polyhedra with respect to Λ if and only if $Q \in \tilde{\mathcal{S}}^n_{\geqslant 0}$ (cf. [Sch09, 4.1, 4.2], [Nam76, §2.1]).

Let $\mathcal{D}$ be any Delone subdivision of Λ, then we define the T-**secondary cone** of $\mathcal{D}$ with respect to Λ to be

$$\Delta_T(\mathcal{D}) = \left\{ \; Q \in \tilde{\mathcal{S}}^n_{\geqslant 0} \cap T \;\middle|\; \text{Del}_\Lambda(Q) = \mathcal{D} \; \right\}.$$

In the classical case $T = \mathcal{S}^n$ we simply speak of secondary cones.

Delone triangulations are of primary interest, since the broader class of general Delone subdivisions is closely related to them, by the observation that if $\mathcal{D}$ is a Delone subdivision, which is not already a triangulation, there is a Delone triangulation D', such that $\overline{\Delta_T(\mathcal{D})}$ is a face of $\overline{\Delta_T(D')}$ (cf. Section 2.6. in [Val03]).

Now we let $GL^{\mathbf{t}}_n(\mathbb{Z})$ (cf. 4.1.2) act on the set of T-secondary cones by $U.\Delta := U^T \Delta U$. We call two T-secondary cones Δ, Δ' $(T, \mathbf{t})$-**equivalent** if there is $U \in GL^{\mathbf{t}}_n(\mathbb{Z})$ such that $U^T \Delta U = \Delta'$ and $U^T T U = T$. If Λ is a lattice we simply speak of T-equivalence, if $T = \mathcal{S}^n$ we simply speak of $\mathbf{t}$-equivalence or $GL^{\mathbf{t}}_n(\mathbb{Z})$-equivalence.

A special class of subspaces T of $\mathcal{S}^n$ are those that are of the form $T = T_G$, where G is a finite subgroup of $GL_n^{\mathbf{t}}(\mathbb{Z})$ and $T_G := \{Q \in \mathcal{S}^n \mid U^T Q U = Q \ \forall U \in G\}$. In this case we will use the notation of $(G, \mathbf{t})$-equivalence synonymous for $(T_G, \mathbf{t})$-equivalence and G-secondary cone synonymous for T_G-secondary cone.

Two Delone subdivisions $\mathcal{D}, \mathcal{D}'$ are referred to as **bistellar neighbors** if their corresponding $(T, \mathbf{t})$-secondary cones are **contiguous**, that is if $\mathcal{F} := \overline{\Delta_T(\mathcal{D})} \cap \overline{\Delta_T(\mathcal{D}')}$ is facet. The transition from $\mathcal{D}$ to $\mathcal{D}'$ is then called a T-**flip**.

6.1.2 A polyhedral description of secondary cones

The classical case of Voronoi's second reduction theory for lattices was generalized to consider linear subspaces $T \subset \mathcal{S}^n$ (cf. [DSSV08]) and to cover periodic sets (cf. [Sch09], this source also discusses the result on linear subspaces). We recall the polyhedral description of T-secondary cones as given in [Sch09, Chapter 4]. This combines Theorems 4.3, 4.5 and 4.7 of the aforementioned work.

To an element $w \in \mathbb{R}^n$ and an affine basis $V \subset \mathbb{R}^n$ of $\mathbb{R}^n$ we associate the quadratic form

$$N_{V,w} := ww^T - \sum_{v \in V} \alpha_v vv^T,$$

with α_v being the affine coordinates of w with respect to the basis V. If $V = \{v_1, \dots, v_{n+1}\}$ is the vertex set of a Delone simplex D, and w is such that $D' = \operatorname{conv}\{v_2, \dots, v_{n+1}, w\}$ is another Delone simplex adjacent (facet-sharing) to D, we write $N_{D,D'}$ instead of $N_{V,w}$.

Let $\mathcal{D}$ be a polyhedral subdivision of $\mathbb{R}^n$, such that $\Lambda := \operatorname{vert}(\mathcal{D})$ is a standard periodic vertex set (e.g. a Delone subdivision of any standard periodic vertex set).

Let $\mathcal{E}$ denote the system of linear equations of the form

$$\langle N_{V,w}, Q \rangle = 0,$$

where for each n-polytope $D \in \mathcal{D}$ we choose the vertex set $V \subset \operatorname{vert}(D)$ of an arbitrary n-simplex S in D and for all $w \in \operatorname{vert}(D)$ obtain an equation of the above form. Note that the above equations are trivially satisfied for all $Q \in \widetilde{S}^n_{\geqslant 0}$ whenever $D \in \mathcal{D}$ is itself a simplex (or more generally if $w \in V$), and are therefore redundant in this case.

Let U denote the null space of the system $\mathcal{E}$ on $\widetilde{S}^n_{\geqslant 0}$. Then the last comment in particular implies that if $\mathcal{D}$ is a triangulation, $U = \widetilde{S}^n_{\geqslant 0}$. Since $N_{V+v,w+v} = N_{V,w}$ for all $v \in \mathbb{R}^n$, and by periodicity of Λ, there are only finitely many such equalities.

Furthermore let $\mathcal{I}$ denote the system of linear inequalities of the form

$$\langle N_{V \cup w, w'}, Q \rangle > 0,$$

where for every facet F of the complex $\mathcal{D}$ and its adjacent n-polytopes $D, D' \in \mathcal{D}$ with $F = D \cap D'$ we choose the vertex set $V \subset \operatorname{vert}(F)$ of an arbitrary $n-1$-simplex S in F and for arbitrary $w \in \operatorname{vert}(D \backslash F)$, $w' \in \operatorname{vert}(D' \backslash F)$ we obtain one inequality as above. The definition of U implies that the orthogonal projection $\pi_U(N_{V \cup w, w'})$ does not depend on the choice of V, w, w' satisfying the above restrictions. Again we see that there are only finitely many distinct inequalities.

The main theorem of Voronoi's second reduction theory can than be formulated as follows.

THEOREM 6.1.1. *Let $\mathcal{D}$ be a polyhedral subdivision of $\mathbb{R}^n$, such that $\Lambda := \mathrm{vert}(\mathcal{D})$ is a standard periodic vertex set and let* T *be a subspace of* $\mathcal{S}^n$.

i. The closure $\overline{\Delta_T(\mathcal{D})}$ is a polyhedral cone in $\widetilde{\mathcal{S}}^n_{\geqslant 0} \cap T$ and

$$\Delta_T(\mathcal{D}) = \{Q \in U \cap T \mid Q \text{ satisfies the system } \mathcal{I}\}.$$

The system $\mathcal{I}$ and the number of defining equalities for U *are finite.*

ii. The map $\mathcal{D} \mapsto \overline{\Delta_T(\mathcal{D})}$ gives an isomorphism between the poset of Delone subdivisions of Λ ordered by coarsening and the poset of closures of T*-secondary cones ordered by inclusion. The closures of all* T*-secondary cones if Delone subdivisions form a polyhedral subdivision of $\widetilde{\mathcal{S}}^n_{\geqslant 0} \cap T$.*

PROOF. This is an amalgamation of Theorems 4.5, 4.7, 4.13 in [Sch09]. □

REMARK 6.1.2. The classical case of lattices goes back to Voronoi (cf. [Vor08]), the generalization to periodic sets is due to Schürmann (cf. [Sch09, Chapter 4]). We have used the language of the latter to formulate these results. ■

There are several finiteness results, that ensure the existence of a fundamental domain for the action of $\mathrm{GL}(\Lambda) = \mathrm{GL}^{\mathbf{t}}_n(\mathbb{Z})$, that is a finite union of secondary cones, if Λ is a periodic vertex set. We will briefly collect these here.

THEOREM 6.1.3 (VORONOI'S SECOND REDUCTION THEORY). *Let $\Lambda = \bigcup_{t \in \mathbf{t}} t + \mathbb{Z}^n$ be a standard periodic vertex set and* G *be a finite subgroup of* $\mathrm{GL}(\Lambda)$.

i. The topological closures of $(G, \mathbf{t})$ secondary cones give a polyhedral subdivision of $\widetilde{\mathcal{S}}^n_{\geqslant 0} \cap T_G$. The closures of two secondary cones have a common facet if and only if they are bistellar neighbors.

ii. If Λ is rational, there are only finitely many $(G, \mathbf{t})$-inequivalent G*-secondary cones.*

PROOF. This is an amalgamation of Theorems 4.7, 4.13, 4.19 in [Sch09]. □

REMARK 6.1.4. This includes the classical case with $\mathbf{t} = (\mathbf{0})$ and G being trivial. This can be made into an algorithm as described in [Sch09, Chapter 4], cf. [SVG] for an implementation of the lattice case. ■

6.1.3 Representatives of low-dimensional Delone triangulations of $\mathbb{Z}^n$

There has been a great deal of work done on the classification of inequivalent Delone triangulations and subdivisions. This includes Voronoi's classification of all inequivalent Delone triangulations up to dimension 4 (cf. [Vor08]). The classification of the 222 inequivalent Delone triangulations in dimension 5 was then settled by Engel and Grishukhin in 2002 (cf. [EG02]), building up on work of Ryshkov and Baranovskii (cf. [BR73], [RB78]) who already found 221 inequivalent Delone triangulations and work of Engel (cf. [Eng98]) who found the missing triangulation.

6.2 ON THE DV-CELL OF A MONOHEDRAL PERIODIC SET

Within this section (Λ, Q) will be a monohedral periodic set on (V, Q), and without loss of generality we assume that $0 \in \Lambda$. It then suffices to study one particular Dirichlet-Voronoi cell for geometrical insight. We will work with $\mathrm{DV}(\Lambda, Q) := \mathrm{DV}_{\Lambda,Q}(0)$.

To compute the explicit quantizer constant of a given lattice, we need knowledge about the geometry of its DV-cell. There are some rather classical results on the computation of Dirichlet-Voronoi cells and the quantizer constant (cf. [CS82], or Chapter 21 in [CS98]), and there is a more recent algorithm for these problems, which can handle higher dimensional lattices, provided a large enough amount of symmetry (cf. [DSSV09]).

We will work towards a description the Dirichlet-Voronoi cell of a symmetric periodic set, including the case of lattices, which is suited quite well to find at least locally an explicit expression for the quantizer constant. The main obstacle to overcome is to handle the geometry of classes of periodic sets at once, we will now show how Voronoi's second reduction theory aids to this cause.

6.2.1 The vertices of the DV-cell of a monohedral periodic set

We argued earlier that we can replace an arbitrary periodic set by a coordinate representation through periodic forms (cf. Propositions 4.1.1 and 4.1.2). Of course this reduces to the case of quadratic forms in the case of lattices.

So fix a standard periodic point set $\Lambda_t \subset \mathbb{R}^n$. Let $Q \in \mathcal{S}^n_{>0}$ and denote $\mathcal{D} = \mathrm{Del}_{\Lambda_t}(Q)$. Then the DV polytope of $\{0\}$ with respect to Λ_t and Q is determined through $\mathrm{star}(0, \mathcal{D})$ by means of its vertices as we noted in Lemma 4.3.17.

Therefore knowledge about the induced Delone subdivision of a periodic form yields a possibility to explicitly compute its DV-cell: recall that for an n-simplex $S \subset \mathbb{R}^n$ with $\mathrm{vert}(D) = \{s_0, \dots, s_n\}$ its centroid with respect to Q is the unique solution to the system of linear equalities given by $|x - s_i|_Q = |x - s_0|_Q$, where $i \in \{1, \dots, n\}$. If $M(S)$ denotes the matrix whose i-th row is given by $(s_i - s_0)^T$, we obtain:

$$(x - s_i)^T Q (x - s_i) = (x - s_0)^T Q (x - s_0)$$
$$\Leftrightarrow (s_i - s_0)^T Q x = \frac{1}{2}(|s_i|_Q^2 - |s_0|_Q^2).$$

Let a be the vector whose i-th entry is $\frac{1}{2}|s_i - s_0|_Q^2$, that is, the vector of halves of squared norms of rows in $M(S)$ and let b be the vector whose i-th entry is given by $\frac{1}{2}(|s_i|_Q^2 - |s_0|_Q^2)$. With this notation

$$c = s_0 + Q^{-1} M(S)^{-1} a = Q^{-1} M(S)^{-1} b \tag{6.1}$$

is the solution of the above system and thus the centroid of S. Now if $D \in \mathrm{star}(0, \mathcal{D})$ is not a simplex, we can choose any $n + 1$ affinely independent vertices of D and compute the centroid of the simplex obtained in this way. Since D is a Delone polytope this actually is the centroid of D.

6.2.2 On a triangulation for Dirichlet-Voronoi polytopes

We are interested in triangulations of Dirichlet-Voronoi cells of monohedral periodic sets, that do only depend on the associated secondary cone and are pyramidal with apex 0. Furthermore we would like a triangulation as such to add no new vertices, like for example the barycentric triangulation would do. This latter condition is posed to reduce the complexity of computations, by reducing the number of vertices involved. This of course comes with a trade-off: the barycentric triangulation might allow to exploit symmetries of the Dirichlet-Voronoi cell for later applications in computing, for example, the quantizer constant. For single lattices, opposed to secondary cones, exploiting symmetry by using a barycentric triangulation, lead to certain precise estimations of the quantizer constant of well-known lattices, that were inaccessible before (cf. [DSSV09]).

The isomorphy given by Lemma 4.3.14 implies that it suffices to find a triangulation as such for the Dirichlet-Voronoi polytope corresponding to the Delone polytope $\{0\}$. We use the duality between Dirichlet-Voronoi and Delone subdivisions to define a triangulation, for which the vertices of the simplices involved can be labeled by a fixed enumeration of the elements of the star of $\{0\}$. Then a triangulation through pulling (cf. Lemma 4.2.1) does the trick.

Let $\mathcal{P}$ be a Delone set with corresponding secondary cone Δ and with Delone subdivision $\mathcal{D}$. Fix an ordering of the full dimensional Delone polytopes in $\operatorname{star}(p, \mathcal{D})$, say $(D_1, \dots, D_k)$. Let $p \in \mathcal{P}$. We define a lattice (order-theoretic) in $2^{\{0,1,\dots,k\}}$ as follows:

i. $\operatorname{star}(p, \mathcal{D})$ gives rise to a poset dual to the face lattice $\mathcal{F}_Q$ for $\mathrm{DV}_{\mathcal{P},Q}(p)$ for arbitrary $Q \in \Delta^o$: we identify an element of $\operatorname{star}(p, \mathcal{D})$ by the n-dimensional Delone polytopes it is a common face of. Since the n-dimensional Delone polytopes are in bijection with their labels, we can therefore express any face by a subset of $\{1, \dots, k\}$. Inclusion of faces in $\operatorname{star}(p, \mathcal{D})$ then induces an ordering relation on the so obtained subset of $2^{\{1,\dots,k\}}$, which is ordinary inclusion. By Proposition 4.3.15 we immediately see that this is in fact a lattice and that it is dual to the face lattice of $\mathrm{DV}_{\mathcal{P}}(Q, \{p\})$ and thus to $\mathrm{DV}_{\mathcal{P},Q}(p)$, since they are affinely isomorphic (by Lemma 4.3.14).

ii. Since $\mathcal{F}_Q = \mathcal{F}_{Q'}$ for all $Q, Q' \in \Delta^o$, we simply write $\mathcal{F}$, it is the face lattice of a realizable convex polytope.

iii. $\mathcal{F}$ and the ordering $(D_1, \dots, D_k)$ induce the pulling triangulation

$$\mathcal{T} = \mathcal{T}(\mathcal{D}, (D_1, \dots, D_k), p) := p_k^- \dots p_1^- p_0^- (\partial \mathcal{F}),$$

cf. Lemma 4.2.2.

PROPOSITION 6.2.1. *Let $\mathcal{P}$ be a Delone set with corresponding secondary cone Δ and with Delone subdivision $\mathcal{D}$. Fix an ordering of the full dimensional Delone polytopes in* $\operatorname{star}(p, \mathcal{D})$, *say* $(D_1, \dots, D_k)$. *Let* $p \in \mathcal{P}$, *and let* $\mathcal{T} = \mathcal{T}(\mathcal{D}, (D_1, \dots, D_k), p)$ *be as above. Define a map* σ_Q *by*

$$t \mapsto \begin{cases} \operatorname{conv}(\{\operatorname{centroid}_Q(D_i) \mid i \in t\}) & 0 \notin t \\ \operatorname{conv}(\{p\} \cup \{\operatorname{centroid}_Q(D_i) \mid 0 \neq i \in t\}) & 0 \in t. \end{cases}$$

Then

i. $\sigma_Q(\mathcal{T})$ *is a pyramidal triangulation with apex* p *of* $\mathrm{DV}_{\mathcal{P}}(p)$.

ii. $|t| - 1$ *is equal to the rank of* $\sigma_Q(t)$ *for all* $t \in \mathcal{T}(\mathcal{D}, (D_1, \dots, D_k), p)$ *if and only if* $Q \in \Delta^o$.

PROOF. Ad (i): We have seen in (iii) of Lemma 4.2.2, that for every polytope that realizes $\mathcal{F}$, we obtain a triangulation, pyramidal with apex p, as desired. This proofs the claim for all $Q \in \Delta^o$. If $Q \in \partial\Delta$

nothing to bad happens: $\sigma_Q(\mathcal{T})$ still is a triangulation of $DV_{\mathcal{P},Q}(p)$, we only lose injectivity of the map σ_Q, non-maximal simplices in $\sigma_Q(\mathcal{T})$ might have distinct preimages in $\mathcal{T}$.

Ad (ii): Let $Q \in \Delta^o$ and let t be an element of $\mathcal{T}(\mathcal{D}, (D_1, \ldots, D_k), p)$. By construction $\sigma_Q(t)$ is a simplex. Assume that $0 \notin t$, thus $p \notin \sigma_Q(t)$. Let there be any labels $i \neq j$, for which $v_i, v_j \in \sigma_Q(t)$. By definition v_i, v_j are centroids of Delone polytopes $D_i \neq D_j$ in $\mathcal{D}$ thus implying $v_i \neq v_j$. Therefore $\sigma_Q(t)$ is a simplex with $|t|$ different vertices, therefore its rank is $|t| - 1$.

If $0 \in t$, the same is true by switching to $t\backslash\{0\}$, since for all D_i, the centroid v_i is distinct from p.

If on the other hand $Q \in \partial\Delta$ we have that $\mathrm{Del}_{\mathcal{P}}(Q)$ is a coarsening of $\mathcal{D}$ and we therefore find a set of labels $i_1, \ldots, i_r$ such that each D_{i_j} no longer is a Delone polytope, but their join is. Any t containing at least two of the above labels therefore maps to the convex hull of at most $|t| - 1$ different vertices of $DV_{\mathcal{P},Q}(0)$, therefore the rank of $\sigma_Q(t)$ is at most $|t| - 2$. □

In the implementation used for purposes of this thesis we chose to compute a pulling triangulation of $\mathcal{C}(\partial P)$ first and then build the pyramids over 0, this was done to decrease the dimension of polytopes on which the triangulation algorithm has to work on.

ALGORITHM 6.2.2 (LOCAL VORONOI TRIANGULATION).

i. Initialize $\mathcal{D}_0$ and fix an ordering $(D_1, \ldots, D_k)$ of its elements.

ii. Compute the incidence poset of $\mathrm{star}(0, \mathcal{D})$ under the chosen labeling as in the proof of Proposition 6.2.1 and dualize it. Denote the dualized poset by $\mathcal{F}$.

iii. For every facet $F \in \mathcal{F}$ obtain the face lattice $\mathcal{F}_{|F}$ of F by restriction of $\mathcal{F}$ and compute the pulling triangulation $p_k^- \ldots p_1^-(\mathcal{F}_{|F})$.

iv. For each of the obtained triangulations build the pyramids over 0.

v. The set of all of the above obtained pyramids gives an abstract triangulation $\mathcal{T}(\mathcal{D}, (D_1, \ldots, D_k))$ as was proposed by Proposition 6.2.1.

Another thing we will need to deal with is the orientation of the simplices in a triangulation of $DV_{\mathcal{P},Q}(0)$ induced by some $\mathcal{T}$ as in Proposition 6.2.1. The good news is: given $Q, Q' \in \Delta^o$ corresponding simplices $\sigma_Q(t), \sigma_{Q'}(t)$ for $t \subset \mathcal{T}$ are equally oriented.

LEMMA 6.2.3. *Let $\mathcal{P}$ be a Delone set, $p \in \mathcal{P}$ and $\mathcal{T} = \mathcal{T}(\mathcal{D}, (D_1, \ldots, D_k), p)$ be as in Proposition 6.2.1. Let $\epsilon \in \{\pm 1\}$, $Q \in \Delta^o$ and let $\sigma_Q(t)$ with $t \in \mathcal{T}^{(n)}$ be ϵ-oriented. Then $\sigma_{Q'}(t)$ is ϵ-oriented for all $Q' \in \Delta^o$ and for those $Q' \in \partial\Delta$ where it is full dimensional.*

PROOF. We show this for the case $p = 0$, the general case follows by application of a suitable isometry.

Write $S_Q = \sigma_Q(t)$ and $S_{Q'} = \sigma_{Q'}(t)$. Consider the map $\Sigma : \Delta \to \mathbb{R}^{n \times n}$ given by $Q \mapsto M(S_Q)$, where $M(S_Q)$ is the n by n matrix whose j-th column is given by the j-th vertex of S_Q (excluding the zeroth vertex 0). This map is entrywise polynomial in the entries of Q and thus continuous, as is easily seen by invoking the explicit term (6.1) for these vertices, which by construction are centroids of a Delone simplex. Each of these centroids depends continuously on a change in Q, as Q^{-1} and the norms $\|\cdot\|_Q$ do. Therefore the map $\det \circ \Sigma : \Delta \to \mathbb{R}$ is continuous.

Now S_Q is ϵ-oriented if and only if $\text{sign}(\det(M(S_Q))) = \epsilon$, that is, by definition, if $\text{sign}(\det \circ \Sigma(Q)) = \epsilon$. If $Q' \in \Delta$, we can move from Q to Q' along the line segment $\overline{QQ'} = \{\lambda Q + (1-\lambda)Q' \mid \lambda \in [0,1]\}$ as Δ is convex. Now we claim that for arbitrary $\widetilde{Q} \in \overline{QQ'} \backslash Q'$ we have that $S_{\widetilde{Q}}$ is ϵ-oriented.

In any case, $\overline{QQ'} \backslash Q' \subset \Delta^o$. Therefore, for any $\widetilde{Q} \in \overline{QQ'} \backslash Q'$ we have that $S_{\widetilde{Q}}$ is full dimensional (cf. Proposition 6.2.1, (ii)) and $\det \circ \Sigma(\widetilde{Q}) \neq 0$. By continuity of $\det \circ \Sigma$ it follows that $\text{sign}(\det \circ \Sigma(\widetilde{Q})) = \epsilon$. Since Q' is the limit of a sequence in $\overline{QQ'}$ we get $\text{sign}(\det \circ \Sigma(\widetilde{Q})) \in \{0, \epsilon\}$.

If $Q' \in \Delta^o$ and therefore $S_{Q'}$ is full dimensional we obtain that Q' is ϵ-oriented. If $Q' \in \partial\Delta$ and $S_{Q'}$ is full dimensional the above argument remains valid. □

6.2.3 Classical results on DV-cells of lattices

For sake of completeness we state some of the above mentioned classical results.

DEFINITION 6.2.4 (RELEVANT POINT). A point $q \in \mathcal{P}$ is called **Dirichlet-Voronoi-relevant** (**DV-relevant** or just **relevant**) for $p \in \mathcal{P}$ (or for $DV(p)$), if the hyperplane between p and q contains a facet of $DV(p)$. ◆

In the case of a lattice L we will call a lattice point **relevant** if it is a relevant point of $DV(L)$.

The following Theorem is due to Voronoi, and characterizes the relevant points of any lattice L.

THEOREM 6.2.5 ([CS98], CH. 21, THEOREM 10). *A point $0 \neq v \in L$ is relevant if and only if $\pm v$ are the only shortest vectors in the coset $v + 2L$.*

It is not surprising that the following lemma holds:

LEMMA 6.2.6 (MINIMAL VECTORS ARE RELEVANT). *If $v \in \text{Min}(L)$, then v is relevant.*

PROOF. We have to assure that $\pm v$ are the only vectors of length $\|v\|^2$ in $v + 2L$. Therefore let $v \neq u \in v + 2L$: $u = v + 2w$, $w \in L$. Then

$$\|u\|^2 = \|v\|^2 + 4\|w\|^2 + 4b(v, w)$$

If $\|u\|^2 = \|v\|^2$, this leads to $-b(u, w) = \|w\|^2$. By the Cauchy-Schwarz inequality we have $b(v, w)^2 \leqslant \|v\|^2 \cdot \|w\|^2$ with equality only if v, w are linearly dependent. In that case we obtain $\|v\|^2 = \|w\|^2$ which only is possible for $w = -v$, therefore $u = -v$. If v, w are linearly independent we have $\|w\|^2 < \|v\|^2$, which would contradict $v \in \text{Min}(L)$. □

6.3 A LOCALLY EXACT FORMULA AND A CONSTRAINED POLYNOMIAL OPTIMIZATION PROGRAM FOR THE LATTICE VECTOR QUANTIZER PROBLEM

The quantization problem is a minimization problem, where the objective function does not come in a handy way to employ standard optimization theory, such as linear or semi-definite programming. We will turn the problem of finding the optimal lattice quantizer of a given dimension n into a collection of constrained minimization problems, for each of which the objective function, as well as the constraints are polynomial functions. This is done with the help of Voronoi's second reduction theory, the same approach was used in [SV06] for the lattice covering and lattice covering packing problem.

We now assume to be in a more restricted version of the setup of Theorem 6.1.3. This will be the general assumption on periodic sets for the application of Voronoi's second reduction theory to the periodic quantizer problem.

ASSUMPTION 6.3.1. We assume that $\Lambda_{\mathbf{t}}$ is a rational standard periodic vertex set such that there exists a finite $G < GL(\Lambda) = GL_n^{\mathbf{t}}(\mathbb{Z})$ for which $(\Lambda_{\mathbf{t}}, Q)$ is monohedral for all $Q \in \mathcal{Q} \in \mathcal{S}^n_{>0} \cap T_G$. ■

An example for non-lattices that satisfy Assumption 6.3.1 are periodic sets that are the join of 2 translates of a lattice (cf. Lemma 4.3.6).

The general periodic quantizer problem is a problem of periodic sets in Euclidean standard space, but every such set is isometric to a coordinate representation, as we noted in Proposition and Definition 4.1.2.

In particular, we identify lattices with positive definite quadratic forms by fixing the set of lattice points to be the standard vertex set $\mathbb{Z}^n$ (Proposition and Definition 4.1.1). For lattices the group G above can be chosen to be trivial, lattices are symmetric by virtue of the action of translations and thus regardless of the involved quadratic form.

Let $L \subset \mathbb{R}^n$ be a lattice with respect to the standard inner product and associated coordinate lattice $(\mathbb{Z}^n, Q)$. We are interested in minimizing $G(L) = \det(L)^{-1/2-1/n} \int_{DV(L)} \|x\|^2 dx$. Since we prefer to work with the coordinate representation of L by $(\mathbb{Z}^n, Q)$, we reformulate this expression in terms of Q. We, more generally, derive this for periodic sets.

LEMMA 6.3.2. *Let $\Lambda = A\Lambda_{\mathbf{t}} \subset \mathbb{R}^n$ be a symmetric m-periodic set with respect to the standard inner product and associated coordinate representation $(\Lambda_{\mathbf{t}}, Q)$, that is $Q = A^T A$. Then*

$$G(\Lambda) = G(Q, \mathbf{t}),$$

where $G(Q, \mathbf{t}) := \frac{m^{1+2/n}}{n} \det(Q)^{-1/n} \int_{DV(Q,\mathbf{t})} \|x\|_Q^2 dx$.

PROOF. This becomes evident by application of the formula of change of variables for integrals

$$\begin{aligned}\int_{DV(\Lambda_{\mathbf{t}},Q)} \|x\|_Q^2 dx &= \int_{DV(\Lambda_{\mathbf{t}},Q)} \|Ax\|^2 dx \\ &= \det(A)^{-1} \int_{A\,DV(\Lambda_{\mathbf{t}},Q)} \|x\|^2 dx = \det(A)^{-1} \int_{DV(\Lambda)} \|x\|^2 dx,\end{aligned}$$

as $DV(\Lambda) = A\, DV_{\Lambda_{\mathbf{t}}}(Q)$ (recall that $DV(Q, \mathbf{t}) = DV(\Lambda_{\mathbf{t}}, Q)$). □

A standard technique to compute $\int_{DV(\Lambda)} \|x\|^2 dx$ is to find a triangulation $\mathcal{T}$ of $DV(\Lambda)$ and compute $\int_{DV(\Lambda)} \|x\|^2 dx = \sum_{\substack{S \subset \mathcal{T} \\ \dim(S)=n}} \int_S \|x\|^2 dx$ via the following formula.

THEOREM 6.3.3 ([CS98], CH. 21, THEOREM 2.). *Let V be the Euclidean standard space of dimension n, and let $S \subset V$ be a simplex with vertices $s_0, \dots, s_n$ and barycenter $\hat{s} = \frac{1}{n+1} \sum_{i=0}^n s_i$. Then*

$$\int_S \|x\|^2 dx = \frac{\mathrm{vol}(S)}{(n+1)(n+2)} \cdot \left(\|(n+1)\hat{s}\|^2 + \sum_{i=0}^n \|s_i\|^2 \right).$$

This then applies to $\int_{DV_{\mathbb{Z}^n}(Q)} \|x\|_Q^2 dx$ as follows.

COROLLARY 6.3.4. *Let* (V, Q) *be a quadratic space of dimension* n *with norm* $\|\cdot\|_Q$*, and let* $S \subset V$ *be a simplex with vertices* $s_0, \dots, s_n$ *and barycenter* $\hat{s} = \frac{1}{n+1}\sum_{i=0}^{n} s_i$*. Then*

$$\int_S \|x\|_Q^2 dx = \frac{\mathrm{vol}_Q(S)}{\sqrt{\det(Q)}} \frac{1}{(n+1)(n+2)} \cdot \left(\|(n+1)\hat{s}\|_Q^2 + \sum_{i=0}^{n} \|s_i\|_Q^2 \right)$$
$$= \frac{\mathrm{vol}(S)}{(n+1)(n+2)} \cdot \left(\|(n+1)\hat{s}\|_Q^2 + \sum_{i=0}^{n} \|s_i\|_Q^2 \right).$$

PROOF. Write $Q = A^T A$ (Cholesky decomposition). Now by the formula for the change of variables for integrals we have:

$$\int_S \|x\|_Q^2 dx = \int_S \|Ax\|^2 dx = \frac{1}{\det(A)} \int_{AS} \|x\|^2 dx$$
$$= \frac{1}{\det(A)} \cdot \frac{\mathrm{vol}(AS)}{(n+1)(n+2)} \cdot \left(\|(n+1)A\hat{s}\|^2 + \sum_{i=0}^{n} \|As_i\|^2 \right),$$

where $\mathrm{vol}(AS) = \det(A) \cdot \mathrm{vol}(S)$ and $\mathrm{vol}_Q(S) = \sqrt{\det(Q)} \cdot \mathrm{vol}(S)$, so that the claim is proven. □

Employing Voronoi's second reduction theory we obtain the knowledge needed about $DV_{\Lambda_t}(Q)$: with respect to the rational standard periodic vertex set Λ_t we choose a representative set of secondary cones, which is finite by Theorem 6.1.3. For each of these secondary cones we will formulate a local quantizer problem, since we can simultaneously triangulate the Dirichlet-Voronoi cells associated to quadratic forms in a fixed secondary cone:

Under the Assumption 6.3.1, the **Δ-local quantizer problem** is given by

$$\min G(Q, \mathbf{t})$$
$$\text{s. t. } Q \in \Delta.$$

From now on we fix a secondary cone Δ. Employing Lemma 4.3.17 we can compute the DV-cell of any monohedral periodic set (Λ_t, Q) for $Q \in \Delta$ in a general way. Using Proposition 6.2.1 we can find a triangulation for each of these lattices that can be described entirely by the means of Δ itself.

LEMMA 6.3.5. *Let* $S_1, \dots, S_n \subset \mathbb{R}^n$ *be simplices and denote the centroid of* S_i *by* c_i*. Suppose the simplex* $S := \mathrm{conv}\{0, c_1, \dots, c_n\}$ *is full dimensional. Let* $Q \in \mathcal{S}_{>0}^n$ *and let* $\widetilde{Q}$ *be the adjoint of* Q*, that is,* $Q\widetilde{Q} = \det(Q) I_n$*.*

i. The quantity $\det(Q)\|c_i\|_Q^2 = \|Qc_i\|_{\widetilde{Q}}^2$ *is polynomial in the entries of* Q*.*

ii. For $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ *the quantity* $\det(Q)\|\sum_{i=1}^{n} \lambda_i c_i\|_Q^2 = \|\sum_{i=1}^{n} \lambda_i Q c_i\|_{\widetilde{Q}}^2$ *is polynomial in the entries of* Q*.*

For the polynomial expressions above, the coefficients are determined solely by $S_1, \dots, S_n$*.*

PROOF. We have already seen that for $Q \in \mathcal{S}_{>0}^n$ and $S \subset \mathbb{R}^n$ a simplex, its centroid is given by $c = Q^{-1}M(S)^{-1}b$. Thus

$$\|c\|_Q^2 = (Q^{-1}M(S)^{-1}b)^T Q (Q^{-1}M(S)^{-1}b) = b^T (A^{-1})^T Q^{-1} M(S)^{-1} b$$
$$= \frac{1}{\det(Q)} b^T (M(S)^{-1})^T \widetilde{Q} M(S)^{-1} b = \frac{1}{\det(Q)} \|Qc\|_{\widetilde{Q}}^2,$$

where the entries of b (and therefore $Qc = M(S)^{-1}b$) are (linear) polynomials in the entries of Q, and the entries of $\widetilde{Q}$ are polynomial of degree $n-1$ in the entries of Q since each entry is a first minor of Q.

Thus $\|c\|_Q^2$ is rational in the entries of Q and $\det(Q)\|c\|_Q^2$ is polynomial in the entries of Q, both are of degree $n+1$. This proves the first assumption.

For $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ and $\sum_{i=1}^n \lambda_i c_i = Q^{-1}\sum_{i=1}^n \lambda_i A_i^{-1} b_i$ analogously $\det(Q)\|\sum_{i=1}^n \lambda_i c_i\|_Q^2$ is polynomial of degree $n+1$. □

This shows that if $S \subset \mathcal{T}$ is a simplex in a triangulation of $DV_{\Lambda_t}(Q)$, the norms of its vertices s_i are given by rational expressions in the entries of Q, as is the norm of their barycenter $\hat{s}$. To be precise we have: $\|s_i\|_Q^2 = \frac{1}{\det(Q)}\|Qs_i\|_{\widetilde{Q}}^2$ and $\|\hat{s}\|_Q^2 = \frac{1}{\det(Q)}\|Q\hat{s}\|_{\widetilde{Q}}^2$, where $\|Qs_i\|_{\widetilde{Q}}^2$ and $\|Q\hat{s}\|_{\widetilde{Q}}^2$ are polynomial in the entries of Q.

The volume of a n-simplex $S \subset \mathbb{R}^n$ can be calculated in different ways, rather then employing Cayley-Menger determinants, we use the volume of a related parallelepiped.

LEMMA 6.3.6. *Let $\Delta = \Delta(\mathcal{D})$ be a fixed secondary cone and fix an ordering $(D_1, \dots, D_k)$ for the elements of $\mathrm{star}(0, \mathcal{D})$. Let $\mathcal{T} = \mathcal{T}(\mathcal{D}, (D_1, \dots, D_k), 0)$ be a triangulation as obtained by Proposition 6.2.1. For an n-simplex $S \subset \mathbb{R}^n$ with $\mathrm{vert}(S) = \{s_0, s_1 \dots, s_n\}$ let $M(S)$ be the matrix whose j-th column is $s_j - s_0$.*

Let $t \in \mathcal{T}$ be maximal element. Then there exists $\epsilon = \epsilon(t) \in \{\pm 1\}$ such that for arbitrary $Q \in \Delta$

$$\mathrm{vol}_Q(\sigma_Q(t)) = \epsilon \frac{1}{n!} \det(Q)^{1/2} \det(M(\sigma_Q(t))),$$

and

$$\mathrm{vol}(\sigma_Q(t)) = \epsilon \frac{1}{n!} \det(M(\sigma_Q(t))),$$

where $\det(Q)^{1/2} \cdot \mathrm{vol}_Q(\sigma_Q(t))$ and $\det(Q) \cdot \mathrm{vol}(\sigma_Q(t))$ are polynomial in the entries of Q.

PROOF. Note that from the construction of the triangulation, $M(\sigma_Q)$ composes of the nontrivial vertices of σ_Q, since the zeroth vertex always is 0. Then

$$\mathrm{vol}(\sigma_Q(t)) = \left|\frac{1}{n}\det(M(\sigma_Q(t)))\right| = \epsilon\frac{1}{n}\det(M(\sigma_Q(t))) = \epsilon\frac{1}{n}\det(Q)^{-1}\det(Q \cdot M(\sigma_Q(t))),$$

where ϵ is the orientation of $\sigma_Q(t)$, but this only depends on t and Δ and not on the choice of Q in Δ, as we proved in Lemma 6.2.3.

The vertices s_i of $\sigma_Q(t)$ are of the form $s_i = Q^{-1}A_i^{-1}b_i$, where s_i is the centroid of a Delone simplex $D_i \in \mathrm{star}(0, \mathcal{D})$. Now $\det(Q \cdot M(\sigma_Q(t)))$ is a polynomial in the entries of Q, as we already noted in the proof of Lemma 6.2.3. Thus the volume of $\sigma_Q(t)$ is rational in the entries of Q where the denominator $\det(Q)$ comes from the factor $\det(Q)^{-1}$ in $\mathrm{vol}(\sigma_Q(t)) = \epsilon\frac{1}{n}\det(Q)^{-1}\det(Q \cdot M(\sigma_Q(t)))$. □

Now we are prepared to find an objective function that is polynomial in the entries of Q and can be used to solve the quantizer problem at least Δ-locally for each secondary cone Δ. The constraints we need are $Q \in \Delta$ which can be expressed by linear (and therefore polynomial) inequalities (cf. Theorem 6.1.1) and $\det(Q) \geqslant 1$. The latter one is of course polynomial in the entries of Q and is needed to avoid the remainder $\det(Q)^e$ that comes from the norms of the vertices, as well as the volume of the simplices in $\mathcal{D}_0$.

THEOREM 6.3.7. *Let $\Lambda_{\mathbf{t}}$ satisfy Assumption 6.3.1. Let Δ be a secondary cone for $\Lambda_{\mathbf{t}}$. The Δ-local quantizer problem*

$$\begin{aligned} &\min G(Q, \mathbf{t}) \\ &\text{s. t. } Q \in \Delta \end{aligned}$$

is equivalent to

$$\begin{aligned} &\min G_\Delta(Q) \\ &\text{s. t. } Q \in \Delta \\ &\text{s. t. } \det(Q) \geqslant 1 \end{aligned}$$

where $G_\Delta(Q)$ is a polynomial in the entries of Q. That is, the Δ-local quantizer problem is equivalent to a polynomial optimization problem with convex constraints; the constraint $Q \in \Delta$ can be replaced by a finite system of linear inequalities.

PROOF. We have

$$\int_{DV_{\mathbb{Z}^n}(Q)} \|x\|_Q^2 \, dx = \sum_{\substack{S \subset \mathcal{T}(Q) \\ \dim(S)=n}} \int_S \|x\|_Q^2 \, dx.$$

Using Corollary 6.3.4 the previous Lemmata 6.3.5 and 6.3.6 show that each of the righthand side summands is the quotient of a polynomial in Q by $\det(Q)^2$:

$$\begin{aligned} \det(Q)^2 \cdot \int_S \|x\|_Q^2 \, dx &= \det(Q)^2 \cdot \frac{\operatorname{vol}(S)}{(n+1)(n+2)} \cdot \left(\|(n+1)\hat{s}\|_Q^2 + \sum_{s \in \operatorname{vert} S} \|s\|_Q^2 \right) \\ &= \epsilon(\overline{S}) \cdot \frac{\det(Q) \cdot \det(M(S))}{(n+2)!} \cdot \left(\|(n+1)Q\hat{s}\|_{\tilde{Q}}^2 + \sum_{s \in \operatorname{vert} S} \|Qs\|_{\tilde{Q}}^2 \right). \end{aligned}$$

Substituting this we obtain

$$\begin{aligned} G(Q) &= \frac{1}{n} \det(Q)^{-1/n} \int_{DV\,\mathbb{Z}^n(Q)} \|x\|_Q^2 \, dx \\ &= \det(Q)^{-1/n-2} \cdot G_\Delta(Q), \end{aligned}$$

where

$$G_\Delta(Q) := \frac{1}{n(n+2)!} \sum_{\substack{S \subset \mathcal{T}(Q) \\ \dim(S)=n}} \epsilon(\overline{S}) \cdot \det(Q) \cdot \det(M(S)) \cdot \left(\|(n+1)Q\hat{s}\|_{\tilde{Q}}^2 + \sum_{s \in \operatorname{vert} S} \|Qs\|_{\tilde{Q}}^2 \right)$$

is polynomial in the entries of Q.

Since the quantizer constant is invariant to scaling we can assume that $\det(Q) = 1$ is fixed without missing an optimal solution, thus we get rid of the denominator. The relaxation $\det(Q) \geqslant 1$ poses no threat to finding optimal solutions, since $G_\Delta(\lambda Q) = \lambda^{(1+2n)} G_\Delta(Q)$ and therefore replacing a Q with $\det(Q) > 1$ by λQ such that $\det(\lambda Q) = 1$ results in $G_\Delta(\lambda Q) < G_\Delta(Q)$.

Finiteness of the involved system of linear inequalities was observed in Theorem 6.1.1. □

REMARK 6.3.8. We chose to drop $\mathbf{t}$ from the notation for G_Δ, it is implicitly involved since Δ is, by assumption, a secondary cone for Λ_t. ■

We state the following as a Corollary to have an explicit formula for the quantizer constant of a lattice at hand whenever needed.

COROLLARY 6.3.9. *Let* $Q \in \mathcal{S}^n_{>0}$, *and let* Δ *be the secondary cone of* $\mathrm{Del}_{\mathbb{Z}^n}(Q)$. *Then*

$$G(Q) = \frac{G_\Delta(Q)}{\det(Q)^{1/n+2}},$$

where $G_\Delta(Q)$ *is a polynomial in the coefficients of* Q. *The coefficients of* $G_\Delta(Q)$ *depend only on* Δ.

REMARK 6.3.10. In the subsequent we will provide the quantizer polynomials for lattices up to dimension 4. In all of these cases it turns out that $G_\Delta(Q)$ is a multiple of $\det(Q)$ (the determinant of an abstract matrix $Q \in \Delta$ as a polynomial in its entries). This is an effect that occurs only for the full DV-cell, for an simplex the corresponding summand will in general not be divisible by $\det(Q)$, as can be readily checked using the MAPLE-code described in Appendix B. ■

6.4 ON THE LATTICE QUANTIZER PROBLEM IN LOW DIMENSIONS

6.4.1 Introductory remarks

Conic parameters for quadratic forms

If we fix a secondary cone Δ we know that each $Q \in \Delta$ can be written as a conic combination $Q = \sum_k \lambda_k(Q) R^{(k)}$ where the $R^{(k)}$ are the extreme rays of Δ. for a given Q we set $c(Q) := (\lambda_1(Q), \ldots, \lambda_m(Q))$ to be the vector of **conic parameters**.

Now evidently we can transform any quantity F, which is given explicitly in the entries of Q, into a quantity which is given in the conic parameters of Q, simply by substituting $q_{ij} = \sum_k \lambda_k(Q) r^{(k)}_{ij}$. We denote such a transformation by $F^{(c)}$.

There is another similar kind of parameters for quadratic forms, the Selling parameters:

Let $Q = (q_{ij})^n_{i,j=1}$. We write $q_{ij} := e_i^T Q e_j$ for $i, j \in \{1, \ldots, n+1\}$, where $e_{n+1} = -\sum_{i=1}^{n} e_i$. Then $\sum_{j=1}^{n+1} q_{ij} = 0$, and therefore $q_{ii} = -\sum_{i \neq j=1}^{n+1} q_{ij}$.

Then we call the parameters q_{ij}, for $i, j \in \{1, \ldots, n+1\}$, $i \neq j$, the **Selling parameters** of Q. Below we will discuss their relation to the conical parameters in a special case.

Voronoi's principal domain of the first type

A common example of a Delone triangulation in dimension n is given by **Voronoi's principal domain of the first type**, given by $\overline{\Delta(\mathcal{V}^n)}$:

Let $Q \in \mathcal{S}^n_{>0}$ be given by $q_{ii} = n$, $q_{ij} = -1$ for all $i, j \in \{1, \ldots, n\}$, $i \neq j$. The lattice $(\mathbb{Z}^n, Q)$ is then isometric to $A^{\#}_n$. We find

$$\mathcal{V}^n := \mathrm{Del}_{\mathbb{Z}^n}(Q) = \{D_\sigma + v \mid \sigma \in S_{n+1},\ v \in \mathbb{Z}^n\},$$

where

$$D_\sigma = \operatorname{conv}\{e_{\sigma(1)}, e_{\sigma(1)} + e_{\sigma(2)}, e_{\sigma(1)} + \ldots + e_{\sigma(n+1)}\},$$

with the convention $e_{n+1} = -\sum_{i=1}^{n} e_i$. The automorphism group of $\mathcal{V}^n$ is isomorphic to S_{n+1}.

We will use the **snake notation** of Ryshkov, to write simplices as D_σ above in a more condensed way:

$$\langle v_1, \ldots, v_n \rangle = \operatorname{conv}\{v_1, v_1 + v_2, \ldots, v_1 + \ldots + v_n\}. \tag{6.2}$$

Thus

$$D_\sigma = \langle e_{\sigma(1)}, \ldots, e_{\sigma(n+1)} \rangle.$$

One finds (cf. §102 − 104 in [Vor08])

$$\Delta(\mathcal{V}^n) = \{Q \in \mathcal{S}^n \mid q_{ij} < 0 \text{ for } i \neq j \text{ and } \sum_{i=1}^{n} q_{ij} > 0 \text{ for } i \in \{1, \ldots, n\}\}.$$

The extreme rays of this cone are the matrices E_{0i} for $1 \leqslant i \leqslant n$ and E_{ij} for $1 \leqslant i < j \leqslant n$. Here E_{0i} is such that the entry at position (i,i) is equal to 1, while all other are equal to 0 and E_{ij} is such that the entries at positions $(i,i), (j,j)$ are equal to 1, the entries at positions $(i,j), (j,i)$ are equal to -1, and all other entries are equal to 0. If $Q \in \Delta$, we write λ_{0i} for the coefficient of E_{0i} and λ_{ij} for the coefficient of E_{ij}.

The Selling parameters and conical parameters of $Q \in \mathcal{V}^2$ satisfy the following relation:

$$q_{ij} = \begin{cases} -\lambda_{ij} & \text{for } i,j \leqslant n, \\ -\lambda_{0i} & \text{for } i \leqslant n,\ j = n+1. \end{cases}$$

6.4.2 Lattice quantizer polynomials and globally optimal solutions in dimensions 2 and 3

Dimension 2

We use this case to give a more detailed example of how to compute the quantizer polynomial, everything of importance can be seen here already, while the presentation of the discussion is quite simple.

There is only one equivalence class of Delone triangulations in dimension 2, this was already settled by Voronoi (cf. [Vor08]), it can be checked by computer using the algorithm sketched in the book [Sch09], cf. [SVG]. A representative is given by Voronoi's principal domain of the first type (cf. 6.4.1). The secondary cone $\Delta = \Delta(\mathcal{V}^2)$ can then be described as follows:

$$\begin{aligned} \Delta := \Delta(\mathcal{V}^2) &= \left\{ \ Q \in \mathcal{S}^2 \ \middle|\ q_{ij} < 0 \text{ for } i \neq j \text{ and } \textstyle\sum_{i=1}^{2} q_{ij} > 0 \text{ for } j = 1,2 \ \right\} \\ &= \left\{ \ Q \in \mathcal{S}^2 \ \middle|\ q_{12} < 0 \text{ and } q_{11} + q_{21} > 0 \text{ and } q_{21} + q_{22} > 0 \ \right\}. \end{aligned}$$

Those maximal cells of the triangulation $\mathcal{V}^2$, that contain the origin 0, are given by $\operatorname{star}(\mathcal{V}^2, 0)$. In hindsight of our wish to fix a lattice in $2^{\{0,1,\ldots,6\}}$ which produces a simultaneous triangulation of any corresponding Dirichlet-Voronoi cell, we fix an order on the elements of $\mathcal{V}_0^2$. Since we can index these elements by elements of the symmetric group S_3 it seems rather natural to start from there. A seemingly natural way to numerate the elements of S_3 is to index them by the order in which the Steinhaus-Johnson-Trotter algorithm produces them. For S_3 this amounts to $1 \mathrel{\widehat{=}} \mathrm{id}, 2 \mathrel{\widehat{=}} (23), 3 \mathrel{\widehat{=}} (132), 4 \mathrel{\widehat{=}} (13), 5 \mathrel{\widehat{=}} (123), 6 \mathrel{\widehat{=}} (12)$. Then

$$\mathrm{star}(\mathcal{V}^2, 0)^{(2)} = \{D_1, \dots, D_6\},$$

where

$$\begin{aligned} D_1 = D_{\mathrm{id}} &= \mathrm{conv}\{0, e_1, e_1 + e_2\}, \\ D_2 = D_{(23)} &= \mathrm{conv}\{0, e_1, -e_2\}, \\ D_3 = D_{(132)} &= \mathrm{conv}\{0, -e_2, -e_1 - e_2\}, \end{aligned}$$

and $D_4 = -D_1, D_5 = -D_2, D_6 = -D_3$.

Now Lemma 4.3.17 shows that the vertex set of the Voronoi cell of an arbitrary $Q \in \overline{\Delta} \cap S^2_{>0}$ can be read of from $\mathcal{V}^2_0$ by $v_i = \mathrm{centroid}_Q(D_i)$. However, we should note that for Q on the boundary of $\overline{\Delta}$ certain of these points v_i will coincide, this is a consequence of the fact that there are usually more inequivalent Delone subdivisions than triangulations, but those appear as the limiting cases of them. Here an example would be the standard form, where $v_1 = v_2$ and $v_4 = v_5$.

In the case of a $Q \in \Delta^0$ we have that $\mathrm{DV}_{\mathbb{Z}^n}(Q)$ is a permutahedron of order 3.

The pulling triangulation that we described in Algorithm 6.2.2 coming from the labeling of elements of $\mathcal{D}_0$ as above leads to an polynomial expression in the entries of Q for the quantizer constant that computes to

$$G(Q) = \frac{1}{24} \cdot \frac{q_{11}^2 q_{22} + q_{11} q_{22}^2 - 2q_{11} q_{12}^2 - 2q_{22} q_{12}^2 - 2q_{12}^3}{(q_{11} q_{22} - q_{12}^2)^{3/2}}. \tag{6.3}$$

Since

$$\Delta = \mathrm{cone}\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \right\}$$

we can parametrize an arbitrary $Q \in \Delta$ by $\lambda_{01}, \lambda_{02}, \lambda_{12} \in \mathbb{R}_{\geqslant 0}$ (cf. 6.4.1), the coefficients of Q as a conic combination of the extreme rays of Δ. This parametrization is closely related to the selling parameters of Q, they differ from one another by a change of sign, as noted above.

Now as described in general above we can transform the quantity $G(Q)$ to be an expression in $c(Q)$ by substituting $q_{11} = \lambda_{01} + \lambda_{12}$, $q_{22} = \lambda_{02} + \lambda_{12}$ and $q_{12} = -\lambda_{12}$, this computes to

$$G^{(c)}(c(Q)) = \frac{1}{24} \cdot \frac{\lambda_{01}^2\lambda_{02} + \lambda_{01}^2\lambda_{12} + \lambda_{01}\lambda_{02}^2 + \lambda_{01}\lambda_{12}^2 + \lambda_{02}^2\lambda_{12} + \lambda_{02}\lambda_{12}^2 + 4\lambda_{01}\lambda_{02}\lambda_{12}}{(\lambda_{01}\lambda_{02} + \lambda_{01}\lambda_{12} + \lambda_{02}\lambda_{12})^{3/2}}. \tag{6.4}$$

The related quantizer polynomial is given by

$$\begin{aligned} G^{(c)}_{\Delta}(c(Q)) = & \frac{\lambda_{01}\lambda_{02} + \lambda_{01}\lambda_{12} + \lambda_{02}\lambda_{12}}{24} \\ & \cdot (\lambda_{01}^2\lambda_{02} + \lambda_{01}^2\lambda_{12} + \lambda_{01}\lambda_{02}^2 + \lambda_{01}\lambda_{12}^2 + \lambda_{02}^2\lambda_{12} + \lambda_{02}\lambda_{12}^2 + 4\lambda_{01}\lambda_{02}\lambda_{12}). \end{aligned}$$

THEOREM 6.4.1 (CF. P. 81 IN [FT53], P. 60 IN [CS98]). *The optimal (lattice) quantizer in dimension 2 is given by any lattice arithmetically equivalent to the hexagonal lattice $A_2 \cong A_2^{\#}$, the optimal value is $G(A_2) = \frac{5}{108}\sqrt{3}$. This is the only local minimum of the lattice quantizer problem in dimension 2.*

Dimension 3

As in dimension 2, there is only one equivalence class of Delone triangulations in dimension 3, a representative is given by Voronoi's principal domain of the first type (cf. 6.4.1). The secondary cone Δ can then be described as follows:

$$\Delta := \Delta(\mathcal{V}^3) = \left\{ \; Q \in \mathcal{S}^3 \;\middle|\; q_{ij} < 0 \text{ for } i \neq j \text{ and } \textstyle\sum_{i=1}^{3} q_{ij} > 0 \text{ for } j = 1,2,3 \; \right\}$$

that is the set of forms $Q \in \mathcal{S}^3$ such that the coefficients satisfy

$$\begin{aligned} &q_{12} < 0, q_{13} < 0, q_{23} < 0 \\ &q_{11} + q_{21} + q_{31} > 0 \\ &q_{12} + q_{22} + q_{32} > 0 \\ &q_{13} + q_{23} + q_{33} > 0. \end{aligned}$$

Those maximal cells of the triangulation $\mathcal{V}^3$, that contain the origin 0, are given by star$(\mathcal{V}^3, 0)$:

$$\text{star}(\mathcal{V}^3, 0)^{(3)} = \{D_1, \ldots, D_{24}\},$$

where again we numerate the elements of $\mathcal{V}_0^3$ by associating an permutation in S_4 to the position it has in the list the Steinhaus-Johnson-Trotter algorithm produces.

If $Q \in \Delta^o$ we know that $\mathrm{DV}_{\mathbb{Z}^3}(Q)$ is a permutahedron of order 4, i.e., a truncated octahedron. There are two combinatorially different types of facets appearing: 4-gons and 6-gons. A pulling triangulation as described in Algorithm 6.2.2 corresponding to the above ordering of vertices can be obtained by pulling each facet individually and building the pyramids with apex 0 above each simplex won by this. To be precise it suffices to execute simply one pulling refinement by the vertex with lowest index. If the facet is a 4-gon we obtain two simplices, if it is a 6-gon we obtain 4 simplices. It is possible to obtain the polynomial $G_\Delta^{(c)}(c(Q))$ directly from this combinatorial description, cf. [BS83].

This leads to the a polynomial expression in the entries of Q for the quantizer constant that computes to

$$G(Q) = \frac{G_\Delta(Q)}{\det(Q)^{7/3}} \tag{6.5}$$

with

$$\begin{aligned} G_\Delta(Q) = \frac{\det(Q)}{36} \cdot \big(&q_{11}^2 q_{22} q_{33} - q_{11}^2 q_{23}^2 - 2q_{11} q_{12}^2 q_{33} + 4q_{11} q_{12} q_{13} q_{23} \\ &-2q_{11} q_{13}^2 q_{22} + q_{11} q_{22}^2 q_{33} - 2q_{11} q_{22} q_{23}^2 + q_{11} q_{22} q_{33}^2 \\ &-2q_{11} q_{23}^3 - 2q_{11} q_{23}^2 q_{33} - 2q_{12}^3 q_{33} + 2q_{12}^2 q_{13}^2 + 6q_{12}^2 q_{13} q_{23} \\ &-2q_{12}^2 q_{22} q_{33} + 2q_{12}^2 q_{23}^2 - q_{12}^2 q_{33}^2 + 6q_{12} q_{13}^2 q_{23} \\ &+4q_{12} q_{13} q_{22} q_{23} + 6q_{12} q_{13} q_{23}^2 + 4q_{12} q_{13} q_{23} q_{33} - 2q_{13}^3 q_{22} \\ &-q_{13}^2 q_{22}^2 - 2q_{13}^2 q_{22} q_{33} + 2q_{13}^2 q_{23}^2 \big) \end{aligned}$$

Since

$$\Delta = \text{cone}\left\{ \begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0\\0&1&0\\0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0\\0&0&0\\0&0&1\end{pmatrix}, \right.$$
$$\left. \begin{pmatrix}1&-1&0\\-1&1&0\\0&0&0\end{pmatrix}, \begin{pmatrix}1&0&-1\\0&0&0\\-1&0&1\end{pmatrix}, \begin{pmatrix}0&0&0\\0&1&-1\\0&-1&1\end{pmatrix} \right\},$$

we can parametrize an arbitrary $Q \in \Delta$ by $\lambda_{01}, \lambda_{02}, \lambda_{03}, \lambda_{12}, \lambda_{13}, \lambda_{23} \in \mathbb{R}_{\geqslant 0}$, the coefficients of Q as a conic combination of the extreme rays of Δ. This parametrization is closely related to the selling parameters of Q, they differ from one another by a change of sign.

Now as described in general above, and laid out for dimension 2 we can transform the quantity $G_\Delta(Q)$ to be an expression in $c(Q)$, this computes to

$$G_\Delta^{(c)}(c(Q)) = \frac{\det^{(c)}}{36} \cdot \left(\det^{(c)} \cdot \Sigma_1 + 2 \cdot \Sigma_2 + \Sigma_3\right), \tag{6.6}$$

where

$$\Sigma_1 = \sum^{(6)} \lambda_{01},$$
$$\Sigma_2 = \sum^{(3)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{23},$$

and

$$\det^{(c)} = \sum^{(12)} \lambda_{01}\lambda_{02}\lambda_{13} + \sum^{(4)} \lambda_{01}\lambda_{02}\lambda_{03}.$$

THEOREM 6.4.2 (THEOREM 1 IN [BS83]). *The optimal lattice quantizer in dimension* 3 *is given by any lattice arithmetically equivalent to the lattice* $A_3^\# \cong D_3^\#$*, the optimal value is* $G(A_3^\#) = 19/(96\sqrt[3]{16})$. *This is the only local minimum of the lattice quantizer problem in dimension* 3.

6.4.3 The lattice quantizer polynomials in dimension 4

There are 3 inequivalent secondary cones that represent the three inequivalent Delone triangulations in dimension 4. We use the description found in [Val03, 4.4.1]. From there we read off that we can describe those cones with the following positive semi-definite forms $E_{01}, \ldots, E_{04}, E_{12}, E_{13}, \ldots, E_{34}$ together with

$$E_a := \begin{pmatrix}2&1&-1&-1\\&2&-1&-1\\&&2&0\\&&&2\end{pmatrix}, E_b := \begin{pmatrix}1&1&-1&-1\\&1&-1&-1\\&&1&1\\&&&1\end{pmatrix}$$

where E_{0i} shall be the all zero matrix except that the i-th diagonal entry is equal to 1 and E_{ij} shall be the all zero matrix except that the i-th and j-th diagonal entries equal 1 and the entries at positions ij and ji equal -1. Note that E_a represents the root lattice D_4.

We set

$$\Delta_1 = \Delta(\mathrm{Del}(Q_1)) = \mathrm{int}\,(\mathrm{cone}\,\{E_{01}, \ldots, E_{04}, E_{12}, E_{13}, \ldots, E_{34}\}) \tag{6.7}$$
$$\Delta_2 = \Delta(\mathrm{Del}(Q_2)) = \mathrm{int}\,(\mathrm{cone}\,\{E_{01}, \ldots, E_{04}, E_{13}, \ldots, E_{34}, E_a\}) \tag{6.8}$$
$$\Delta_3 = \Delta(\mathrm{Del}(Q_3)) = \mathrm{int}\,(\mathrm{cone}\,\{E_{01}, \ldots, E_{04}, E_{13}, \ldots, E_{24}, E_a, E_b\}), \tag{6.9}$$

where

$$Q_1 = \begin{pmatrix} 4 & -1 & -1 & -1 \\ & 4 & -1 & -1 \\ & & 4 & -1 \\ & & & 4 \end{pmatrix}, Q_2 = \begin{pmatrix} 5 & 1 & -2 & -2 \\ & 5 & -2 & -2 \\ & & 6 & -1 \\ & & & 6 \end{pmatrix}, Q_3 = \begin{pmatrix} 6 & 2 & -3 & -3 \\ & 6 & -3 & -3 \\ & & 6 & 1 \\ & & & 6 \end{pmatrix}.$$

In particular $\Delta_1 = \Delta(\mathcal{V}^4)$.

From this we can read of any data we need. The remaining 49 inequivalent Delone subdivisions (that are not triangulations) correspond to the faces of the closures of these cones, we therefore can compute their secondary cones from the representations in (6.7),(6.8),(6.9) above. From another look into [Val03, 4.4.1] we obtain that Δ_1 shares each of its facets, and therefore each of its faces, with a $GL_4(\mathbb{Z})$ translate of Δ_2 and Δ_3 shares but one of its facets with a $GL_4(\mathbb{Z})$ translate of Δ_2, where its remaining facet is shared with a $GL_4(\mathbb{Z})$ translate of itself. This comes from the fact that the corresponding Delone triangulations are bistellar neighbors of one another in exactly the same pattern.

Therefore we can proceed by finding a $GL_4(\mathbb{Z})$ representative set of facets (and then on of faces of them) of Δ_2 to cover the majority of cases. The remaining work then is to evaluate Δ_1 itself, Δ_3 itself and the remaining facet of Δ_3 (and of course its faces).

The 52 inequivalent secondary cones

This classification has been achieved quite a few times, we refer to [Val03, 4.4.4 to 4.4.6] for an expository treatment.

Though one can read off the 52 inequivalent secondary cones from a table in 4.4.6 of the above cited source, we go ahead and compute them ourselves by directly computing the rays of each of the representatives. We collect the data in a table; for more information we again refer to [Val03, 4.4.6].

Using this information it is possible to derive the remaining 49 quantizer polynomials from those given for the three inequivalent Delone triangulations in dimension 4, below.

The local quantizer polynomial for $\Delta(\mathcal{V}^4)$:

We start with the rational closure $\overline{\Delta_1}$ of the secondary cone of the Delone triangulation $\mathcal{V}^4$ of Voronoi's principal form of the first type.

Those maximal cells of the triangulation $\mathcal{V}^4$, that contain the origin 0, are given by the star of $\mathcal{V}^4$ around 0. We set $D_1^1 :=< e_1, e_2, e_3, e_4, e_5 >$ written in the snake notation of Ryshkov (cf. (6.2)), where $e_5 = -e_1 - e_2 - e_3 - e_4$. Then $\mathcal{V}_0^4$ is given by the S_5 orbit of D_1^1 where S_5 is supposed to act on the subscripts of the vectors. This in particular implies that the automorphism group of $\mathcal{V}^4$ is isomorphic to S_5. Thus

$$\text{star}(\mathcal{V}^4, 0)^{(4)} = \{D_1^1, \dots, D_{120}^1\},$$

where we numerate the elements of $\text{star}(\mathcal{V}^4, 0)^{(4)}$ by associating an permutation in S_5 to the position it has in the list the Steinhaus-Johnson-Trotter algorithm produces.

By the same reasoning as above we can read off the Dirichlet-Voronoi cell of $Q \in \mathcal{S}_{>0}^4$ from $\mathcal{V}_0^4$. If $Q \in \Delta_1^o$ we know that $DV_{\mathbb{Z}^4}(Q)$ is a permutahedron of order 5.

Table 6.1: Representative vectors of the 52 inequivalent secondary cones in dimension 4.

dim	Representative vector
1	$(0,0,0,0,0,0,0,0,0,0,1,0)$
2	$(1,0,0,0,0,0,0,0,0,0,1,0)$
3	$(1,1,0,0,0,0,0,0,0,0,1,0)$
3	$(1,0,1,0,0,0,0,0,0,0,1,0)$
4	$(1,1,1,1,0,0,0,0,0,0,0,0)$
4	$(1,1,1,0,0,0,0,0,0,0,1,0)$
4	$(1,0,1,1,0,0,0,0,0,0,1,0)$
4	$(1,0,1,0,0,1,0,0,0,0,1,0)$
4	$(0,0,0,1,0,1,0,1,0,0,1,0)$
5	$(1,1,1,1,1,0,0,0,0,0,0,0)$
5	$(0,1,1,1,1,1,0,0,0,0,0,0)$
5	$(0,0,1,1,1,0,1,1,0,0,0,0)$
5	$(1,1,1,1,0,0,0,0,0,0,1,0)$
5	$(1,1,1,0,0,1,0,0,0,0,1,0)$
5	$(1,1,0,1,0,1,0,0,0,0,1,0)$
5	$(0,0,1,1,0,1,1,0,0,0,1,0)$
5	$(1,0,0,1,0,1,0,1,0,0,1,0)$
6	$(1,1,1,1,1,1,0,0,0,0,0,0)$
6	$(0,1,1,1,1,1,1,0,0,0,0,0)$
6	$(1,1,1,1,0,0,1,1,0,0,0,0)$
6	$(1,0,1,1,1,0,1,1,0,0,0,0)$
6	$(1,1,1,1,0,1,0,0,0,0,1,0)$
6	$(1,0,1,1,0,1,1,0,0,0,1,0)$
6	$(0,1,1,1,0,1,1,0,0,0,1,0)$
6	$(1,1,0,1,0,1,0,1,0,0,1,0)$
6	$(1,0,1,1,0,1,0,1,0,0,1,0)$
6	$(0,1,0,1,0,1,1,1,0,0,1,0)$

dim	Representative vector
7	$(1,1,1,1,1,1,1,0,0,0,0,0)$
7	$(1,1,1,1,1,1,0,1,0,0,0,0)$
7	$(1,1,1,1,1,0,1,1,0,0,0,0)$
7	$(0,1,1,1,1,1,1,1,0,0,0,0)$
7	$(1,1,1,1,0,1,1,0,0,0,1,0)$
7	$(1,1,1,1,0,1,0,1,0,0,1,0)$
7	$(1,1,1,1,0,0,1,1,0,0,1,0)$
7	$(1,1,0,1,0,1,1,1,0,0,1,0)$
7	$(1,1,0,0,0,1,1,1,1,0,1,0)$
7	$(0,0,1,1,0,1,1,1,1,0,1,0)$
7	$(1,0,1,1,0,1,1,0,0,1,1,0)$
8	$(1,1,1,1,1,1,1,1,0,0,0,0)$
8	$(1,1,1,1,0,1,1,1,1,0,0,0)$
8	$(1,1,1,1,0,1,1,1,0,0,1,0)$
8	$(1,1,1,0,0,1,1,1,1,0,1,0)$
8	$(1,0,1,1,0,1,1,1,1,0,1,0)$
8	$(1,1,1,1,0,1,1,0,0,1,1,0)$
8	$(1,1,1,1,0,1,0,1,0,1,1,0)$
9	$(1,1,1,1,1,1,1,1,1,0,0,0)$
9	$(1,1,1,1,0,1,1,1,1,0,1,0)$
9	$(1,1,1,1,0,1,1,1,0,1,1,0)$
9	$(1,1,1,1,0,1,1,1,1,0,0,1)$
10	$(1,1,1,1,1,1,1,1,1,1,0,0)$
10	$(1,1,1,1,0,1,1,1,1,1,1,0)$
10	$(1,1,1,1,0,1,1,1,1,0,1,1)$

Recall that

$$\Delta_1 = \text{cone}\left\{E_{01}, \ldots, E_{04}, E_{12}, E_{13}, \ldots, E_{34}\right\},$$

so for $i = 1, \ldots, 4$ we denote by $\lambda_{0i} = \lambda_{0i}(Q)$ the coefficient of E_{0i} in a conic representation of $Q \in \Delta_1$, and for $i = 1, \ldots, 3, i < j \leqslant 4$ with $\lambda_{ij} = \lambda_{ij}(Q)$ the coefficient of E_{ij}.

S_5 leaves G invariant by acting on the indices[1] of the conical parameters, for if $\rho \in S_5$ we have that

$$\lambda_{ab}(\rho(Q)) = \lambda_{\rho(a)\rho(b)}(Q).$$

by choice of labeling. This explains our choice in naming the extreme rays and it allows to write up $G^{(c)}_{\Delta_1}$ in a condensed form, which we chose to resemble the one for the three dimensional case $\mathcal{V}^3$:

$$G^{(c)}_{\Delta_1}(c(Q)) = \frac{\det^{(c)}}{48} \cdot \left(\det^{(c)} \cdot \Sigma_1 + \Sigma_2 + 3 \cdot \Sigma_3 + \Sigma_4\right), \tag{6.10}$$

[1]We assume that the permutation acts on the unordered set of subscripts, these of course uniquely determine the parameter.

where

$$\Sigma_1 = \sum^{(10)} \lambda_{01},$$
$$\Sigma_2 = \sum^{(60)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{12}\lambda_{14} + \sum^{(60)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{12}\lambda_{34} + 2 \cdot \sum^{(60)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14}\lambda_{24},$$
$$\Sigma_3 = \sum^{(12)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{24}\lambda_{34},$$
$$\Sigma_4 = \sum^{(30)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04}\lambda_{12},$$

and finally

$$\det{}^{(c)} = \sum^{(5)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04} + \sum^{(60)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14} + \sum^{(60)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{24}.$$

The local quantizer polynomial for Δ_2:

We continue with the rational closure $\overline{\Delta_2}$, let $\mathcal{D}^2$ denote its associated delone triangulation.

Those maximal cells of the triangulation $\mathcal{D}^2$, that contain the origin 0, are given by the star of $\mathcal{D}^2$ around 0. Following [Val03, 8.4.2] we set

$$\begin{array}{lll lll}
D^2_{I} & := & < e_1, e_2 - e_1, e_1 + e_5, e_4, e_3 > & D^2_{VIII} & := & < e_1, e_5, e_2, e_4, e_3 > \\
D^2_{II} & := & < e_1, e_2 - e_1, e_1 + e_3, e_4, e_5 > & D^2_{XI} & := & < e_1, e_3, e_2, e_5, e_4 > \\
D^2_{V} & := & < e_1, e_2 - e_1, e_1 + e_5, e_3, e_4 > & D^2_{IV} & := & < e_1, e_5, e_2, e_3, e_4 > \\
D^2_{VI} & := & < e_1, e_2 - e_1, e_1 + e_4, e_3, e_5 > & D^2_{XII} & := & < e_1, e_4, e_2, e_3, e_5 > \\
D^2_{IX} & := & < e_1, e_2 - e_1, e_1 + e_4, e_5, e_3 > & D^2_{VII} & := & < e_1, e_4, e_2, e_5, e_3 > \\
D^2_{X} & := & < e_1, e_2 - e_1, e_1 + e_3, e_5, e_4 > & D^2_{III} & := & < e_1, e_3, e_2, e_5, e_4 >
\end{array}$$

which follows Voronois numeration (cf. p. 169 in [Vor08]). Again we use the snake notation of Ryshkov (cf. (6.2)), where $e_5 = -e_1 - e_2 - e_3 - e_4$. If D is any of the above simplices we denote its image under $-\operatorname{id}$ by the roman numeral that corresponds to $12 + i$ where i is the value of the roman numeral of D. $\operatorname{star}(0, \mathcal{D}^2)^{(4)}$ then consists of the translates of the above numbered 24 simplices by their vertices. This amounts to a total of 120 elements. Thus

$$\operatorname{star}(0, \mathcal{D}^2)^{(4)} = \{D^2_1, \dots, D^2_{120}\},$$

where we numerate the elements of $\operatorname{star}(0, \mathcal{D}^3)^{(4)}$ by starting with, say, $D^2_1 := D^2_I$, followed by its translates $D^2_2, \dots, D^2_5$ and continuing with D^2_6 being D^2_{II} and so on.

We compute $\operatorname{Aut}(\Delta_2) \cong \mathrm{Di}_6$ to be isomorphic to the dihedral group of order 12. In fact we compute the matrix group fixing E_a, which is isomorphic to $\operatorname{Aut}(D_4)$ and afterwards the subgroup fixing Δ_2. This matrix group is isomorphic to the direct product of the dihedral group of order 12 and a cyclic group of order 2 acting on the extreme rays with the cyclic factor being the kernel of the operation. $\operatorname{Aut}(\Delta_2)$ acts on the conical parameters if we write it as subgroup of S_5, to be explicit we use the subgroup generated by (03),(04), and (12). By abuse of language we will also refer to this group as $\operatorname{Aut}(\Delta_2)$.

Doing this we can derive a "compressed" expression for $G^{(c)}_{\Delta_2}$, however it is unfortunately still quite messy:

$$G^{(c)}_{\Delta_2} = \frac{\det^{(c)}}{240} \cdot \left(\sum_{i=0}^{5} \lambda^i_a \cdot \Sigma_i \right), \tag{6.11}$$

where

$$
\begin{aligned}
\Sigma_5 =\ & 104,\\
\Sigma_4 =\ & 130\cdot\Big(\sum\nolimits^{(6)}\lambda_{01}+\sum\nolimits^{(3)}\lambda_{03}\Big),\\
\Sigma_3 =\ & 20\cdot\Big(\sum\nolimits^{(6)}\lambda_{01}^2+\sum\nolimits^{(3)}\lambda_{03}^2\Big)\\
&+130\cdot\Big(\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{13}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{23}+\sum\nolimits^{(3)}\lambda_{03}\lambda_{04}\Big)\\
&+160\cdot\Big(\sum\nolimits^{(6)}\lambda_{01}\lambda_{34}+\sum\nolimits^{(3)}\lambda_{01}\lambda_{02}\Big),\\
\Sigma_2 =\ & 15\cdot\Big(\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{13}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{23}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}^2+\sum\nolimits^{(6)}\lambda_{03}^2\lambda_{04}\Big)\\
&+\ 20\cdot\Big(\sum\nolimits^{(6)}\lambda_{01}^2\lambda_{02}+\sum\nolimits^{(6)}\lambda_{03}^2\lambda_{14}+\sum\nolimits^{(6)}\lambda_{01}^2\lambda_{34}\Big)\\
&+\ 60\cdot\Big(\sum\nolimits^{(6)}\lambda_{01}\lambda_{03}\lambda_{13}+\sum\nolimits^{(1)}\lambda_{03}\lambda_{04}\lambda_{34}\Big)\\
&+110\cdot\Big(\sum\nolimits^{(6)}\lambda_{01}\lambda_{03}\lambda_{04}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{03}\lambda_{23}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{23}\lambda_{14}+\sum\nolimits^{(2)}\lambda_{01}\lambda_{13}\lambda_{14}\Big)\\
&+120\cdot\Big(\sum\nolimits^{(12)}\lambda_{01}\lambda_{02}\lambda_{13}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}\lambda_{14}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}\lambda_{24}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}\lambda_{34}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{02}\lambda_{03}\Big)\\
&+200\cdot\Big(\sum\nolimits^{(3)}\lambda_{01}\lambda_{02}\lambda_{34}\Big),\\
\Sigma_1 =\ & 10\cdot\Big(\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{03}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{13}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{23}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{14}\\
&+\ \sum\nolimits^{(12)}\lambda_{03}^2\lambda_{24}\lambda_{34}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}^2\lambda_{34}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{34}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{23}\\
&+\ \sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{24}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{13}\lambda_{23}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{13}\lambda_{24}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{13}\lambda_{34}\\
&+\ \sum\nolimits^{(12)}\lambda_{01}^2\lambda_{23}\lambda_{34}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}^2\lambda_{04}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}^2\lambda_{14}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}^2\lambda_{24}\\
&+\ \sum\nolimits^{(6)}\lambda_{01}^2\lambda_{03}\lambda_{04}+\sum\nolimits^{(6)}\lambda_{01}^2\lambda_{13}\lambda_{14}+\sum\nolimits^{(6)}\lambda_{01}^2\lambda_{23}\lambda_{24}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{02}\lambda_{03}^2+\sum\nolimits^{(6)}\lambda_{01}\lambda_{03}^2\lambda_{23}\Big)\\
&+\ 20\cdot\Big(\sum\nolimits^{(6)}\lambda_{01}^2\lambda_{02}\lambda_{34}+\sum\nolimits^{(3)}\lambda_{03}^2\lambda_{14}\lambda_{24}\Big)\\
&+\ 40\cdot\Big(\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}\lambda_{04}\lambda_{13}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{13}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{03}\lambda_{04}\lambda_{34}\\
&+\ \sum\nolimits^{(6)}\lambda_{01}\lambda_{03}\lambda_{13}\lambda_{14}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{03}\lambda_{13}\lambda_{24}\Big)\\
&+\ 60\cdot\Big(\sum\nolimits^{(6)}\lambda_{01}\lambda_{03}\lambda_{14}\lambda_{34}\sum\nolimits^{(3)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{23}\Big)\\
&+\ 80\cdot\Big(\sum\nolimits^{(12)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}\lambda_{04}\lambda_{23}+\sum\nolimits^{(12)}\lambda_{01}\lambda_{03}\lambda_{14}\lambda_{23}\\
&+\ \sum\nolimits^{(6)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{14}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{24}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{03}\lambda_{24}\lambda_{34}+\sum\nolimits^{(3)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04}\Big)\\
&+100\cdot\Big(\sum\nolimits^{(12)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{34}+\sum\nolimits^{(6)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{34}\Big),\\
\Sigma_0 =\ & 5\cdot\Big(\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{03}\lambda_{14}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{03}\lambda_{24}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{03}\lambda_{34}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{13}\lambda_{24}\\
&+\ \sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{14}\lambda_{23}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{02}\lambda_{23}\lambda_{34}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{04}\lambda_{23}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{14}\lambda_{23}\\
&+\ \sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{14}\lambda_{24}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{23}\lambda_{24}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{23}\lambda_{34}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{03}\lambda_{24}\lambda_{34}\\
&+\ \sum\nolimits^{(12)}\lambda_{01}^2\lambda_{13}\lambda_{14}\lambda_{23}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{13}\lambda_{23}\lambda_{24}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{13}\lambda_{23}\lambda_{34}+\sum\nolimits^{(12)}\lambda_{01}^2\lambda_{13}\lambda_{24}\lambda_{34}
\end{aligned}
$$

$$
\begin{aligned}
+ \quad & \sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{03}^2\lambda_{14} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}^2\lambda_{14}\lambda_{24} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}^2\lambda_{04}\lambda_{23} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}^2\lambda_{04}\lambda_{24} \\
+ \quad & \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}^2\lambda_{14}\lambda_{23} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}^2\lambda_{24}\lambda_{34} + \sum\nolimits^{(6)} \lambda_{01}^2\lambda_{02}\lambda_{03}\lambda_{04} + \sum\nolimits^{(6)} \lambda_{01}^2\lambda_{02}\lambda_{13}\lambda_{14} \\
+ \quad & \sum\nolimits^{(6)} \lambda_{01}^2\lambda_{02}\lambda_{23}\lambda_{24} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{03}^2\lambda_{34} + \sum\nolimits^{(6)} \lambda_{03}^2\lambda_{04}\lambda_{14}\lambda_{24} \Big) \\
+ \quad 20 \cdot & \Big(\sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04}\lambda_{13} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{13}\lambda_{14} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{13}\lambda_{24} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{13}\lambda_{34} \\
+ \quad & \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}\lambda_{04}\lambda_{13}\lambda_{24} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{14}\lambda_{34} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{03}\lambda_{04}\lambda_{23}\lambda_{34} + \sum\nolimits^{(3)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04}\lambda_{34} \Big) \\
+ \quad 30 \cdot & \Big(\sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14}\lambda_{34} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14}\lambda_{24} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{14}\lambda_{23} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{03}\lambda_{04}\lambda_{23}\lambda_{24} \Big) \\
+ \quad 40 \cdot & \Big(\sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{24}\lambda_{34} \Big).
\end{aligned}
$$

In addition we find for the determinant

$$\det{}^{(c)} = \sum\nolimits_{i=0}^{4} \lambda_a^i \cdot \Sigma_{di},$$

where

$$
\begin{aligned}
\Sigma_{d0} = \quad & \sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{34} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}\lambda_{04}\lambda_{23} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}\lambda_{14}\lambda_{23} \\
+ \quad & \sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{34} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{14} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{13}\lambda_{24} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{03}\lambda_{24}\lambda_{34} \\
+ \quad & \sum\nolimits^{(3)} \lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04}, \\
\Sigma_{d1} = 2 \cdot & \Big(\sum\nolimits^{(12)} \lambda_{01}\lambda_{02}\lambda_{13} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}\lambda_{14} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}\lambda_{24} + \sum\nolimits^{(12)} \lambda_{01}\lambda_{03}\lambda_{34} \\
+ \quad & \sum\nolimits^{(6)} \lambda_{01}\lambda_{02}\lambda_{03} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{03}\lambda_{04} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{03}\lambda_{23} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{13}\lambda_{24} + \sum\nolimits^{(2)} \lambda_{01}\lambda_{13}\lambda_{14} \Big) \\
+ 4 \cdot & \Big(\sum\nolimits^{(3)} \lambda_{01}\lambda_{02}\lambda_{34} \Big), \\
\Sigma_{d2} = 3 \cdot & \Big(\sum\nolimits^{(12)} \lambda_{01}\lambda_{03} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{13} + \sum\nolimits^{(6)} \lambda_{01}\lambda_{23} + \sum\nolimits^{(3)} \lambda_{03}\lambda_{04} \Big) \\
+ 4 \cdot & \Big(\sum\nolimits^{(6)} \lambda_{01}\lambda_{34} + \sum\nolimits^{(3)} \lambda_{01}\lambda_{02} \Big), \\
\Sigma_{d3} = 4 \cdot & \Big(\sum\nolimits^{(6)} \lambda_{01} + \sum\nolimits^{(3)} \lambda_{03} \Big), \\
\Sigma_{d4} = \; & 4.
\end{aligned}
$$

The local quantizer polynomial for Δ_3:

We continue with the rational closure $\overline{\Delta_3}$, let $\mathcal{D}^3$ denote its associated Delone triangulation.

Those maximal cells of the triangulation $\mathcal{D}^3$, that contain the origin 0, are given by the star of $\mathcal{D}^3$ around 0. Following [Val03, 8.4.2] we set

$$
\begin{array}{lll}
D^3_{I} & := & < e_4, e_3 - e_4, e_2 + e_4, e_1 - e_2, e_2 + e_5 > \\
D^3_{II} & := & < e_4, e_2 + e_3, e_1 - e_2, e_2, e_5 > \\
D^3_{III} & := & < e_2, e_3, e_1, e_4, e_5 > \\
D^3_{IV} & := & < e_1 + e_4, e_3 - e_4, e_4, e_2, e_5 > \\
D^3_{V} & := & < e_1 - e_2, e_2, e_4, e_3 - e_4, e_2 + e_4 + e_5 > \\
D^3_{VI} & := & < e_2, e_1 - e_2, e_2 + e_4, e_3, e_5 > \\
D^3_{VII} & := & < e_3, e_1, e_4, e_2, e_5 > \\
D^3_{VIII} & := & < e_2 + e_4, e_3 - e_4, e_4, e_1, e_5 > \\
D^3_{IX} & := & < e_2 + e_4, e_1 - e_2, e_2, e_3, e_5 > \\
D^3_{X} & := & < e_2 + e_3, e_1 - e_2, e_2, e_4, e_5 > \\
D^3_{XI} & := & < e_1, e_3, e_2, e_4, e_5 > \\
D^3_{III} & := & < e_1, e_4, e_2, e_3, e_5 >
\end{array}
$$

which follows Voronois numeration (cf. p. 173 in [Vor08]). Again we use the snake notation of Ryshkov (cf. (6.2)), where $e_5 = -e_1 - e_2 - e_3 - e_4$. If D is any of the above simplices we denote its image under $-\mathrm{id}$ by the roman numeral that corresponds to $12 + i$ where i is the value of the roman numeral of D. $\mathcal{D}_0^2$ then consists of the translates of the above numbered 24 simplices by their vertices. This amounts to a total of 120 elements. Thus

$$\mathrm{star}(0, \mathcal{D}^3)^{(4)} = \{D_1^3, \ldots, D_{120}^3\},$$

where we numerate the elements of $\mathrm{star}(0, \mathcal{D}^3)^{(4)}$ by starting with, say, $D_1^3 := D_{\mathrm{I}}^3$, followed by its translates $D_2^3, \ldots, D_5^3$ and continuing with D_6^3 being D_{II}^3 and so on.

We compute $\mathrm{Aut}(\Delta_3)$ to be the subgroup of S_9, acting on the set $\{01, 02, 03, 04, 13, 14, 23, 24, b\}$ of indices of the extreme rays, that is generated by

$$\begin{aligned}
\sigma_1 &= (01, 03, 23, b, 24, 04)(02, 14, 13),\\
\sigma_2 &= (01, 23)(02, 13)(04, b),\\
\sigma_3 &= (01, 04, 14)(02, 23, 03)(13, 24, b).
\end{aligned}$$

This group has order 36 and is available as entry $< 36, 10 >$ in the small group database via GAP or MAGMA (cf. [BE99]). In fact we compute the matrix group fixing E_a, which is isomorphic to $\mathrm{Aut}(D_4)$ and afterwards the subgroup fixing Δ_3. $\mathrm{Aut}(\Delta_3)$ does unfortunately not act naturally on the conical parameters given the above explicit generators. Let us express our understanding that it is quite unfortunate that we did not find a nicer description of this action, as was possible in the cases of Δ_1 and Δ_2.

Doing this we can derive a "compressed" expression for $G_{\Delta_2}^{(c)}$, however it is unfortunately not as compressed as the one for $G_{\Delta_1}^{(c)}$, but fortunately nicer than the one for $G_{\Delta_2}^{(c)}$.

$$G_{\Delta_3}^{(c)} = \frac{\det^{(c)}}{240} \cdot \left(5 \cdot \det^{(c)} \cdot \Sigma_d + \sum_{i=0}^{5} \lambda_a^i \cdot \Sigma_i\right), \tag{6.12}$$

where

$$\det^{(c)} = \sum\nolimits_{i=0}^{4} \lambda_a^i \cdot \Sigma_{di},$$

where

$$\begin{aligned}
\Sigma_5 =&\ 104,\\
\Sigma_4 =&\ 130 \cdot \left(\sum\nolimits^{(9)} \lambda_{01}\right),\\
\Sigma_3 =&\ 20 \cdot \left(\sum\nolimits^{(9)} \lambda_{01}^2\right) + 130 \cdot \left(\sum\nolimits^{(18)} \lambda_{01}\lambda_{03} + \sum\nolimits^{(9)} \lambda_{01}\lambda_{23}\right) + 160 \cdot \left(\sum\nolimits^{(9)} \lambda_{01}\lambda_{02}\right),\\
\Sigma_2 =&\ 15 \cdot \left(\sum\nolimits^{(36)} \lambda_{01}^2\lambda_{03} + \sum\nolimits^{(18)} \lambda_{01}^2\lambda_{23}\right) + 20 \cdot \left(\sum\nolimits^{(18)} \lambda_{01}^2\lambda_{02}\right) + 60 \cdot \left(\sum\nolimits^{(6)} \lambda_{01}\lambda_{03}\lambda_{13}\right)\\
&+ 110 \cdot \left(\sum\nolimits^{(18)} \lambda_{01}\lambda_{03}\lambda_{04} + \sum\nolimits^{(3)} \lambda_{01}\lambda_{23}\lambda_{24}\right) + 120 \cdot \left(\sum\nolimits^{(36)} \lambda_{01}\lambda_{02}\lambda_{13} + \sum\nolimits^{(18)} \lambda_{01}\lambda_{02}\lambda_{03}\right)\\
&+ 200 \cdot \left(\sum\nolimits^{(3)} \lambda_{01}\lambda_{02}\lambda_b\right),\\
\Sigma_1 =&\ 10 \cdot \left(\sum\nolimits^{(36)} \lambda_{01}^2\lambda_{02}\lambda_{03} + \sum\nolimits^{(36)} \lambda_{01}^2\lambda_{02}\lambda_{14} + \sum\nolimits^{(36)} \lambda_{01}^2\lambda_{02}\lambda_{23} + \sum\nolimits^{(36)} \lambda_{01}^2\lambda_{03}\lambda_{23} + \sum\nolimits^{(36)} \lambda_{01}^2\lambda_{03}\lambda_{24}\right.\\
+&\ \left.\sum\nolimits^{(18)} \lambda_{01}^2\lambda_{03}\lambda_{04} + \sum\nolimits^{(18)} \lambda_{01}^2\lambda_{03}\lambda_{14} + \sum\nolimits^{(9)} \lambda_{01}^2\lambda_{23}\lambda_{24}\right) + 20 \cdot \left(\sum\nolimits^{(9)} \lambda_{01}^2\lambda_{02}\lambda_b\right)
\end{aligned}$$

$$
\begin{aligned}
&+\ 40\cdot\Big(\sum\nolimits^{(36)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{13}\Big)+60\cdot\Big(\sum\nolimits^{(9)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{23}\Big)\\
&+\ 80\cdot\Big(\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{14}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{24}+\sum\nolimits^{(9)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04}\Big)\\
&+100\cdot\Big(\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{b}\Big),\\
\Sigma_0 =\ &\ 5\cdot\Big(\sum\nolimits^{(36)}\lambda_{01}^2\lambda_{02}\lambda_{03}\lambda_{14}+\sum\nolimits^{(36)}\lambda_{01}^2\lambda_{02}\lambda_{03}\lambda_{24}+\sum\nolimits^{(36)}\lambda_{01}^2\lambda_{02}\lambda_{03}\lambda_{b}+\sum\nolimits^{(36)}\lambda_{01}^2\lambda_{02}\lambda_{13}\lambda_{24}\\
&+\ \sum\nolimits^{(36)}\lambda_{01}^2\lambda_{03}\lambda_{04}\lambda_{23}+\sum\nolimits^{(36)}\lambda_{01}^2\lambda_{03}\lambda_{23}\lambda_{24}+\sum\nolimits^{(18)}\lambda_{01}^2\lambda_{02}\lambda_{03}\lambda_{04}+\sum\nolimits^{(18)}\lambda_{01}^2\lambda_{02}\lambda_{13}\lambda_{14}\\
&+\ \sum\nolimits^{(18)}\lambda_{01}^2\lambda_{02}\lambda_{23}\lambda_{24}+\sum\nolimits^{(18)}\lambda_{01}^2\lambda_{02}\lambda_{23}\lambda_{b}+\sum\nolimits^{(18)}\lambda_{01}^2\lambda_{03}\lambda_{14}\lambda_{23}+\sum\nolimits^{(18)}\lambda_{01}^2\lambda_{03}\lambda_{14}\lambda_{24}\Big)\\
&+\ 20\cdot\Big(\sum\nolimits^{(36)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04}\lambda_{13}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{13}\lambda_{14}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{13}\lambda_{b}\Big)\\
&+\ 30\cdot\Big(\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14}\lambda_{24}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{14}\lambda_{23}\Big)\\
&+\ 40\cdot\Big(\sum\nolimits^{(9)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04}\lambda_{b}\Big).
\end{aligned}
$$

In addition we find for the determinant

$$\det{}^{(c)}=\sum\nolimits_{i=0}^{4}\lambda_a^i\cdot\Sigma_{di},$$

where

$$
\begin{aligned}
\Sigma_{d0} =\ &\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{14}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{b}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{14}\\
+\ &\sum\nolimits^{(18)}\lambda_{01}\lambda_{02}\lambda_{13}\lambda_{24}+\sum\nolimits^{(9)}\lambda_{01}\lambda_{02}\lambda_{03}\lambda_{04},\\
\Sigma_{d1} =\ &2\cdot\Big(\sum\nolimits^{(36)}\lambda_{01}\lambda_{02}\lambda_{13}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{03}\lambda_{02}+\sum\nolimits^{(18)}\lambda_{01}\lambda_{03}\lambda_{04}+\sum\nolimits^{(3)}\lambda_{01}\lambda_{23}\lambda_{24}\Big)\\
&+4\cdot\Big(\sum\nolimits^{(3)}\lambda_{01}\lambda_{02}\lambda_{b}\Big),\\
\Sigma_{d2} =\ &3\cdot\Big(\sum\nolimits^{(18)}\lambda_{01}\lambda_{03}+\sum\nolimits^{(9)}\lambda_{01}\lambda_{23}\Big)\\
&+4\cdot\Big(\sum\nolimits^{(9)}\lambda_{01}\lambda_{02}\Big),\\
\Sigma_{d3} =\ &4\cdot\Big(\sum\nolimits^{(9)}\lambda_{01}\Big),\\
\Sigma_{d4} =\ &4.
\end{aligned}
$$

6.4.4 Results on local optimality in dimension 4

We have already seen that there is only one local, and therefore global, optimum of the quantizer problem in dimensions 2 and 3.

For dimensions larger than 3 we can take a look on certain well-known lattices and check them for local optimality for the lattice quantizer problem, by use of the explicit formula for the quantizer constant given in Corollary 6.3.9. Given a lattice L we compute a coordinate representation $(\mathbb{Z}^n, Q)$. We can then compute $\Delta(\mathrm{Del}_{\mathbb{Z}^n}(Q))$ and then all secondary cones of triangulations that refine $\mathrm{Del}_{\mathbb{Z}^n}(Q)$. For each secondary cone of a triangulation we then compute the explicit term for $G_{(c)}$. In fact, since the conic parameters are homogeneous it is possible to assume that one of them is equal to 1, without any loss of generality, leading to a term $G'_{(c)}$. Next we compute the gradient and hessian of the altered explicit term $G'_{(c)}$ using the symbolic engine of MAPLE.

We do so for dimension 4.

THEOREM 6.4.3. *The lattice $D_4 \cong D_4^\#$ is a local minimum for the lattice quantizer problem in Dimension 4.*

PROOF. For D_4 we have to consider Δ_2 and Δ^3, the lattice corresponds to the extreme ray E_a which both cones share. In Δ^2 we assume that $G'_{(c)}$ comes from $\lambda_a = 1$ and find D_4 to be represented by $[0,0,0,0,0,0,0,0,0,1]$ and $\nabla G'_{(c)}$ vanishes at the truncated point. In Δ^3we assume that $G'_{(c)}$ comes from $\lambda_a = 1$ and find D_4 to be represented by $[0,0,0,0,0,0,0,0,1,0]$ and $\nabla G'_{(c)}$ vanishes at the truncated point. The hessian, evaluated at this point, is

$$\frac{4^{3/4}}{1536} \cdot \begin{pmatrix} 3 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ -1 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 3 & 0 & 0 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 3 & -1 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 3 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 3 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & -1 & 0 & 3 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & -1 & 0 & 3 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

regardless of the cone. This matrix is positive definite, where the integral part has eigenvalues 1 and 4 of multiplicities 3 and 6 respectively. □

THEOREM 6.4.4. *The lattice $A_4^\#$ is a local minimum for the lattice quantizer problem in Dimension 4.*

PROOF. For $A_4^\#$ we only have to consider Δ_1. We assume that $G'_{(c)}$ comes from $\lambda_{01} = 1$. $A_4^\#$ is represented by $[1,1,1,1,1,1,1,1,1,1]$ and $\nabla G'_{(c)}$ vanishes at the truncated point. The hessian, evaluated at this point, is

$$\frac{5^{1/4}}{150000} \cdot \begin{pmatrix} 111 & 14 & 14 & 14 & -65 & -65 & 14 & 14 & -65 \\ 14 & 111 & 14 & -65 & 14 & -65 & 14 & -65 & 14 \\ 14 & 14 & 111 & -65 & -65 & 14 & -65 & 14 & 14 \\ 14 & -65 & -65 & 111 & 14 & 14 & 14 & 14 & -65 \\ -65 & 14 & -65 & 14 & 111 & 14 & 14 & -65 & 14 \\ -65 & -65 & 14 & 14 & 14 & 111 & -65 & 14 & 14 \\ 14 & 14 & -65 & 14 & 14 & -65 & 111 & 14 & 14 \\ 14 & -65 & 14 & 14 & -65 & 14 & 14 & 111 & 14 \\ -65 & 14 & 14 & -65 & 14 & 14 & 14 & 14 & 111 \end{pmatrix}.$$

This matrix is positive definite, where the integral part has eigenvalues $81 + 3\sqrt{678}$, $81 + 3\sqrt{678}$, 255, and 18 of multiplicities 1, 1, 3, and 4 respectively. □

THEOREM 6.4.5. *The lattice A_4 is not a local minimum of the lattice quantizer problem in Dimension 4, it is, however, a saddle point.*

PROOF. For A_4 we only have to consider Δ_1. We assume that $G'_{(c)}$ comes from $\lambda_{01} = 1$. A_4 is represented by $[1,0,0,1,1,0,0,1,0,1]$ and $\nabla G'_{(c)}$ vanishes at the truncated point. The hessian, evaluated at this point, is

$$\frac{5^{3/4}}{6000} \cdot \begin{pmatrix} -3 & -3 & -2 & 3 & 2 & 2 & -2 & -3 & -2 \\ -3 & -3 & 3 & -2 & -3 & 2 & -2 & 2 & 3 \\ -2 & 3 & 12 & -3 & -2 & 3 & -3 & -2 & -3 \\ 3 & -2 & -3 & 12 & 3 & -2 & -3 & -2 & -3 \\ 2 & -3 & -2 & 3 & -3 & -3 & 3 & 2 & -2 \\ 2 & 2 & 3 & -2 & -3 & -3 & -2 & -3 & -2 \\ -2 & -2 & -3 & -3 & 3 & -2 & 12 & 3 & -3 \\ -3 & 2 & -2 & -2 & 2 & -3 & 3 & -3 & 3 \\ -2 & 3 & -3 & -3 & -2 & -2 & -3 & 3 & 12 \end{pmatrix}.$$

This matrix is regular, but indefinite. □

Appendix

A Table of quantizer constants

We present an overview of some explicit values of the quantizer constant for low dimensions. The table contains the currently known best monohedral periodic quantizers in dimensions 1 to 10 as well as those in dimensions 12 and 16, which are lattices with the exception of dimension 7 and 9.

The explicit values for $A_3^\# \cong D_3^\#$ appears on p.378 in [Ger79]. Explicit formulae for the quantizer constant of the root lattice families $A_n, A_n^\#$ (for $n \geqslant 1$) and $D_n, D_n^\#$ (for $n \geqslant 3$) as well as the explicit values for the exceptional lattices E_6, E_7, E_8 can be found in Chapter 21 of [CS98], cf. [CS82]. The approximate value of BW_{16} is from 2.3, Chapter 2 in [CS98], cf. [CS84]. The exact formulae for $E_6^\#, E_7^\#$ can be found in [Wor87], [Wor88]. The approximate values for D_7^+, D_9^+ are from Table IV [AE98]. The explicit values for D_{10}^+ and K_{12} are from Table 5 in [DSSV09]..

Dimension	Quantizer	Normalized second moment	source
1	$\mathbb{Z}$	$\frac{1}{12} \approx 0.83333$	[CS98]
2	$A_2^\# \cong A_2$	$\frac{5}{36} \cdot 3^{-1/2} \approx 0.080188$	[CS98]
3	$A_3^\# \cong D_3^\#$	$\frac{19}{192} \cdot 2^{-1/3} \approx 0.078543$	[CS98]
	$A_3 \cong D_3$	$2^{-11/3} \approx 0.078745$	[CS98]
4	$D_4^\# \cong D_4$	$\frac{13}{120} \cdot 2^{-1/2} \approx 0.076603$	[CS98]
	$A_4^\#$	$\frac{389}{1500} \cdot 5^{-3/4} \approx 0.077559$	[CS98]
	A_4	$\frac{7}{60} \cdot 5^{-1/4} \approx 0.078020$	[CS98]
5	$D_5^\#$	$\frac{2641}{23040} \cdot 2^{-3/5} \approx 0.075625$	[CS98]
	D_5	$\frac{1}{10} \cdot 2^{-2/5} \approx 0.075786$	[CS98]
	$A_5^\#$	$\frac{209}{648} \cdot 6^{-4/5} \approx 0.076922$	[CS98]
	A_5	$\frac{1}{9} \cdot 6^{-1/5} \approx 0.077647$	[CS98]

Dimension	Quantizer	Normalized second moment	source
6	$E_6^{\#}$	$\frac{12619}{204129} \cdot 3^{1/6} \approx 0.074244$	[Wor87]
	E_6	$\frac{5}{56} \cdot 3^{-1/6} 0.074347$	[CS98]
7	D_7^{+}	0.072734 ± 0.000003	[AE98]
	$E_7^{\#}$	$\frac{21361}{322560} \cdot 2^{1/7} 0.073116$	[Wor88]
	E_7	$\frac{163}{2016} \cdot 2^{-1/7} \approx 0.073231$	[CS98]
8	$E_8^{\#} \cong E_8$	$\frac{929}{12960} \approx 0.071682$	[CS98]
9	D_9^{+}	0.071103 ± 0.000003	[AE98]
10	D_{10}^{+}	$\frac{4568341}{64512000} \approx 0.070813$	[DSSV09]
12	K_{12}	$\frac{797361941}{6567561000} \cdot 3^{-1/2} \approx 0.070095$	[DSSV09]
16	$\Lambda_{16} \cong BW_{16}$	0.068299 ± 0.000027	[CS98]

APPENDIX

B Documentation of computations

B.1 METHOD OF COMPUTATION

To find the explicit expression for the quantizer constant, as proposed by Corollary 6.3.9, in the cases depicted in 6.4, we used the following approach involving the computer algebra systems MAGMA [BCP97] and MAPLE [Map].

Let $\Delta(\mathcal{D})$ be the secondary cone of the Delone subdivision $\mathcal{D}$ for which we are interested in an explicit formula.

i. Choose a labeling I for the full dimensional Delone polytopes in $\mathrm{star}(\mathcal{D}, 0)$.

ii. Choose $Q_0 \in \Delta$ and compute the vertices of its Dirichlet-Voronoi cell in order of the labeling I.

iii. In MAGMA: The intrinsic command `Polytope` computes the Dirichlet-Voronoi cell of Q_0 in terms of the labeling I, the intrinsic command `Faces` computes the full face lattice `FL`.

iv. In MAPLE: Convert `FL` into suitable input `FaceLatt` for the command `face_to_polytope` (cf. B.2).

v. In MAPLE: For all elements `F` of `FaceLatt` compute the pulling triangulation (in the inherent vertex order of the labeling) of `face_to_polytope(FaceLatt,F)`, using the command `pulling_triangulation` (cf. B.2).

vi. In MAPLE: The command `quantizerformula` (cf. B.2) computes the sought after expression.

We quickly explain what a suitable input for the command `pulling_triangulation` looks like. An n-polytope P, which we know in terms of its face lattice $\mathcal{F}$, is converted in the following way: for $0 \leqslant k < n$, a k-face of P, given in terms of the labels of the vertices as $[i_1, \ldots, i_j]$, is converted to $[k, \{i_1, \ldots, i_k\}]$, that is, for each face of P we store its dimension and its vertices. This produces a representation $\overline{\mathcal{F}}$.

The command `face_to_polytope` will take $\overline{\mathcal{F}}$ and an element $F \in \overline{\mathcal{F}}$ as input and compute an analogously representation of F, given in terms of its faces $[k', \{i_{j_1}, \ldots, i_{j_{l'}}\}]$.

B.2 Overview of routines

centroid(S,Q)

Returns the centroid of the simplex with vertices in the list S with respect to the quadratic form given by a matrix Q.

q_centroid(S,Q)

Returns Q times the centroid of the simplex with vertices in the list S with respect to the quadratic form given by a matrix Q.

simplexvolume(S)

Returns the volume of the simplex with vertices in the list S with respect to the standard inner product.

adj_norm(v,G)

Returns the squared norm of a vector v (can also be the list of coefficients) with respect to the adjoint of the matrix G.

simplexsummand(S,Q,S_0)

Returns the quantizer summand (cf. Corollary 6.3.4) belonging to the simplex with vertices in the list S cat [0]. S_0 has to be a list of vertices of an explicit realization of S in the same order as S, it is used to determine the sign of the orientation (cf. 6.3.6).

quantizerformula(Del,VorTriangulation,Q)

S - list; VorTriangulation - list; Q - matrix; Returns the quotient for the quantizer constant. The input has to be: Del - a list of the full dimensional Delone polytopes containing 0; VorTriangulation - a list containing an abstract triangulation of the Dirichlet-Voronoi cell; Q - a matrix representing an element of the interior of the associated secondary cone.

pyramid(P,v)

Returns the pyramid of v (given as a list) over P.

vertices(P)

Returns all vertices of P.

face_to_polytope(P.F)

Returns the face F of P as a polytope.

pull(L,v)

> *Returns the pulling refinement of L by pulling v (cf. 4.1).*

pulling_triangulation(P)

> *Returns the pulling triangulation of P corresponding to the vertex order in which P is given (cf. Lemma 4.2.1).*

SJT_alg(n)

> *Returns the symmetric group on n symbols in the order produced by the Steinhaus-Johnson-Trotter algorithm.*

use_sym_binary(sigma,M)

> *Returns the result of the operation of sigma on the binary symbols in M.*

use_sym_unary(sigma,M)

> *Returns the result of the operation of sigma on the unary symbols in M.*

sym_orbit_sum_red_binary(M,Sym)

> *Returns the polynomial in l that is the sum of the monomials indexed by sigma(M) for sigma in Sym, M a list of binary indices. Multiplicities are removed.*

sym_orbit_sum_red_unary(M,Sym)

> *Returns the polynomial in l that is the sum of the monomials indexed by sigma(M) for sigma in Sym, M a list of unary indices. Multiplicities are removed.*

expand_snake(S)

> *Returns a list of the vertices of the Simplex described by vertices in the list S, which is interpreted to be in snake notation (cf. 6.2).*

B.3 WORKSHEETS

The routines presented in B.2 are available online at

`https://marcchristianzimmermann.wordpress.com/`

The computations for dimension 4 (cf. 6.4.3, 6.4.4) are also available at the above address: for each of the three Delone triangulations we provide a text file containing a MAPLE script intended to be a check and documentation of the involved computations.

Index

Bibliography

[AE98] E. Agrell and T. Eriksson, *Optimization of lattices for quantization*, Information Theory, IEEE Transactions on **44** (1998), no. 5, 1814–1828.

[AM94] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley series in mathematics, Avalon Publishing, 1994.

[Apo13] T. M. Apostol, *Introduction to analytic number theory*, Springer Science & Business Media, 2013.

[AS10] E. Akhtarkavan and M. F. M. Salleh, *Multiple description lattice vector quantization using coinciding similar lattices of* A_4, Industrial Electronics Applications (ISIEA), 2010 IEEE Symposium on, oct. 2010, pp. 716 –721.

[AS12] E. Akhtarkavan and M. F. M. Salleh, *Multiple descriptions coinciding lattice vector quantizer for wavelet image coding*, Trans. Img. Proc. **21** (2012), no. 2, 653–661.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The magma algebra system* I*: The user language*, Journal of Symbolic Computation **24** (1997), no. 3-4, 235 – 265.

[BE99] H. U. Besche and B. Eick, *The groups of order at most 1000 except 512 and 768*, Journal of Symbolic Computation **27** (1999), no. 4, 405–413.

[BHM08] M. Baake, M. Heuer, and R. V. Moody, *Similar sublattices of the root lattice* A_4, Journal of Algebra **320** (2008), no. 4, 1391 – 1408.

[BM99] M. Baake and R. V. Moody, *Similarity submodules and root system in four dimensions*, Canad. J. Math. **51** (1999), 1258 – 1276.

[BR73] E. P. Baranovskii and S. S. Ryshkov, *Primitive five-dimensional parallelohedra*, Soviet Math. Dokl, vol. 14, 1973, pp. 1391–1395.

[BS83] E. S. Barnes and N. J. A. Sloane, *The optimal lattice quantizer in three dimensions*, SIAM Journal on Algebraic Discrete Methods **4** (1983), no. 1, 30–41.

[BSZ11] M. Baake, R. Scharlau, and P. Zeiner, *Similar sublattices of planar lattices*, Canad. J. Math. **63** (2011), 1220–1237.

[CRS99] J. H. Conway, E. M. Rains, and N. J. A. Sloane, *On the existence of similar sublattices*, Canad. J. Math. **51** (1999), no. 6, 1300–1306.

[CS82] J. H. Conway and N. J. A. Sloane, *Voronoi regions of lattices, second moments of polytopes, and quantization*, Information Theory, IEEE Transactions on **28** (1982), no. 2, 211–226.

[CS84] ———, *On the voronoi regions of certain lattices*, SIAM Journal on Algebraic Discrete Methods **5** (1984), no. 3, 294–305.

[CS98] ———, *Sphere packings, lattices and groups*, third edition ed., Springer, 1998.

[DRS10] J. A. DeLoera, J. Rambau, and F. Santos, *Triangulations: Structures for algorithms and applications*, Algorithms and computation in mathematics, Springer, 2010.

[DSGSW15] M. Dutour Sikirić, A. Garber, A. Schürmann, and C. Waldmann, *The complete classification of five-dimensional Dirichlet-Voronoi polyhedra of translational lattices*, arXiv preprint arXiv:1507.00238 (2015).

[DSSV08] M. Dutour Sikirić, A. Schürmann, and F. Vallentin, *A generalization of Voronoi's reduction theory and its application*, Duke Mathematical Journal **142** (2008), no. 1, 127–164.

[DSSV09] ———, *Complexity and algorithms for computing voronoi cells of lattices*, Mathematics of computation **78** (2009), no. 267, 1713–1731.

[DSV02] S. N. Diggavi, N. J. A. Sloane, and V. A. Vaishampayan, *Asymmetric multiple description lattice vector quantizers*, Information Theory, IEEE Transactions on **48** (2002), no. 1, 174–191.

[DSW08] M. Du Sautoy and L. Woodward, *Zeta functions of groups and rings*, Springer, 2008.

[EG02] P. Engel and V. Grishukhin, *There are exactly 222 L-typesvof primitive five-dimensional lattices*, European Journal of Combinatorics **23** (2002), no. 3, 275–279.

[Eng93] P. Engel, *Geometric crystallography*, Handbook of Convex Geometry (P. M. Gruber and J. M. Wills, eds.), vol. B, Elsevier, 1993, pp. 989–1041.

[Eng98] ———, *Investigations of parallelohedra in* $\mathbb{R}^d$, Voronoi's impact on Modern Science, P. Engel and H. Syta (eds), Institute of Mathematics **2** (1998), 22–60.

[FT53] L. Fejes Tóth, *Lagerungen in der Ebene auf der Kugel und im Raum*, Springer-Verlag, 1953.

[Ger79] A. Gersho, *Asymptotically optimal block quantization*, IEEE Transactions on information theory **25** (1979), no. 4, 373–380.

[GG12] A. Gersho and R. M. Gray, *Vector quantization and signal compression*, vol. 159, Springer Science & Business Media, 2012.

[GN98] R. M. Gray and D. L. Neuhoff, *Quantization*, Information Theory, IEEE Transactions on **44** (1998), no. 6, 2325–2383.

[GR89] P. M. Gruber and S. S. Ryshkov, *Facet-to-facet implies face-to-face*, European Journal of Combinatorics **10** (1989), no. 1, 83 – 84.

[Gra12] R. M. Gray, *Source coding theory*, vol. 83, Springer Science & Business Media, 2012.

[Gru07] P. M. Gruber, *Convex and discrete geometry*, vol. 336, Springer Science & Business Media, 2007.

[Hem04] B. Hemkemeier, *Algorithmische Konstruktionen von Gittern*, Ph.D. thesis, Technische Universität Dortmund, 2004.

[Heu10] M. Heuer, *Combinatorial aspects of root lattices and words*, Ph.D. thesis, The Open University, Milton Keynes, 2010.

[HS69] J. F. P. Hudson and J. L. Shaneson, *Piecewise linear topology*, vol. 11, WA Benjamin New York, 1969.

[Jac09] N. Jacobson, *Basic algebra* II*: Second edition*, Dover Publications, 2009.

[Kap58] I. Kaplansky, *Projective modules*, Annals of Mathematics (1958), 372–377.

[KGK00] J. A. Kelner, V. K. Goyal, and J. Kovacevic, *Multiple description lattice vector quantization: Variations and extensions*, Data Compression Conference, 2000. Proceedings. DCC 2000, IEEE, 2000, pp. 480–489.

[Kne02] M. Kneser, *Quadratische Formen*, Springer, 2002.

[Lee90] C. W. Lee, *Regular Triangulations of Convex Polytopes*, Tech. report, DIMACS, 1990.

[Map] Maplesoft, *Maple 2015.0*, Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

[Nam76] Y. Namikawa, *A new compactification of the Siegel space and degeneration of abelian varieties.* I, Mathematische Annalen **221** (1976), no. 2, 97–141.

[Neu06] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Lehrbuch Masterclass, Springer Berlin Heidelberg, 2006.

[O'M73] O. T. O'Meara, *Introduction to quadratic forms*, Springer, 1973.

[RB78] S. S. Ryshkov and E. P. Baranovskiĭ, *C-types of n-dimensional lattices and 5-dimensional primitive parallelohedra: With application to the theory of coverings*, Proc. Steklov Inst. Math., American Mathematical Soc., 1978.

[Rei75] I. Reiner, *Maximal orders*, vol. 38, Academic press London, 1975.

[Sch09] A. Schürmann, *Computational geometry of positive definite quadratic forms*, University Lecture Series **49** (2009).

[Sch11a] R. Scharlau, *Similar sublattices of Euclidean lattices*, personal communication, 2011.

[Sch11b] ———, *Similar sublattices of higher dimensional lattices*, `https://www.mathematik.tu-dortmund.de/~scharlau/research/talks/2011_scharlau_wien_similar.pdf`, 2011, Slides of a talk at the Erwin Schrödinger International Institute for Mathematical Physics, Vienna, Austria.

[SV06] A. Schürmann and F. Vallentin, *Computational approaches to lattice packing and covering problems*, Discrete & Computational Geometry **35** (2006), no. 1, 73–116.

[SVG] A. Schürmann, A. Vallentin, and A. Garber, *secondary cone cruiser*, `http://www.math.uni-rostock.de/~achill/SCC-2.0/HTML/scc2.html`, ver. 2.0.

[SVS99] S. D. Servetto, V. A. Vaishampayan, and N. J. A. Sloane, *Multiple description lattice vector quantization*, Data Compression Conference, 1999. Proceedings. DCC'99, IEEE, 1999, pp. 13–22.

[Val03] F. Vallentin, *Sphere coverings, lattices, and tilings (in low dimensions)*, Ph.D. thesis, Phd. Thesis, Technische Universität München, 2003.

[Voi08a] I. K. Voigt, *Voronoi cells of discrete point sets*, arXiv preprint arXiv:0811.1525 (2008).

[Voi08b] ———, *Voronoizellen diskreter Punktmengen*, Ph.D. thesis, Technische Universität Dortmund, 2008.

[Vor08] G. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques. deuxième mémoire. recherches sur les parallélloèdres primitifs.*, Journal für die reine und angewandte Mathematik **134** (1908), 198–287.

[VSS01] V. A. Vaishampayan, N. J. A. Sloane, and S. D. Servetto, *Multiple-description vector quantization with lattice codebooks: Design and analysis*, IEEE Transactions on Information Theory **47** (2001), no. 5, 1718–1734.

[Wor87] R. T. Worley, *The Voronoi region of* E_6^*, Journal of the Australian Mathematical Society **43** (1987), no. 2, 268–278.

[Wor88] ———, *The Voronoi region of* E_7^*, SIAM journal on discrete mathematics **1** (1988), no. 1, 134–141.

[Zam14] R. Zamir, *Lattice coding for signals and networks: A structured coding approach to quantization, modulation, and multiuser information theory*, Cambridge University Press, 2014.

[Zie95] G. M. Ziegler, *Lectures on polytopes*, vol. 152, Springer Science & Business Media, 1995.