Lattices, Codes, and Radon Transforms

ACADEMISCH PROEFSCHRIFT

ten verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. J.J.M. Franse
ten overstaan van een door het college voor promoties
ingestelde commissie, in het openbaar te verdedigen
in de Aula der Universiteit
op woensdag 23 juni 1999 te 14 uur

door

Mikhail Igorevitch Boguslavsky
geboren te Moskou

Samenstelling van de promotiecommissie:

promotor	:	Prof. dr. G.B.M. van der Geer
overige leden	:	Prof. dr. R.H. Dijkgraaf
		Prof. dr. T.H. Koornwinder
		Prof. dr. M.A. Tsfasman
		Dr. G.R. Pellikaan

Korteweg–de Vries Instituut voor Wiskunde
Faculteit der Wiskunde, Informatica, Natuukunde en Sterrenkunde

ISBN 90-5776-025-8

Cover: Albrecht Dürer, Melencolia I, 1514. In the upper right corner you can see a latin square. It is related to Radon transforms over a finite field (see a footnote on page 23.)

Contents

Introduction **1**

1 Codes and Lattices **7**
1.1 Codes and Lattices: the Classical Theory 7
1.1.1 Basic Notions 7
1.1.2 Duality 9
1.1.3 Spectra 11
1.2 Generalized weights 12
1.2.1 Definitions 12
1.2.2 Duality 13
1.2.3 Generalized Spectra 13
1.2.4 Generalized Spectra and Tensor Products 16
1.2.5 Bounds 16
1.3 Interpretations of Generalized Hermite Parameters . . . 19
1.3.1 Adelic Interpretation 19
1.3.2 Systoles of Riemann Manifolds 20

2 Homogeneous spaces in duality **21**
2.1 General Theory 21
2.2 A Duality Between Vectors and $(n-1)$-sublattices . . . 24
2.3 Weight/Multiplicity Duality for Projective Multisets . . . 26
2.4 Generalized Plotkin Bound 29
2.5 Generalized Minkowski–Hlawka Theorem 30

3 Projective codes and bounds on the second Hermite parameter **35**
3.1 Grassmannians as metric spaces 35
3.2 Bounds on the second generalized Hermite parameter . . 39

3.3 Examples 41

4 Number of Points on Algebraic Sets **43**
4.1 Introduction 43
4.2 Conjectures 46
4.3 Two equations 49
4.4 Generalized weights 54
Bibiliography **57**
Curriculum Vitae **65**
Nederlandse Samenvatting **66**

Introduction

In this thesis, generalized Hamming weights of codes and generalized Hermite parameters of lattices in Euclidean space are studied. Generalized Hamming weights, also called *dimension/length profile*, *minimum support sizes*, or *weight hierarchy*, are relatively new parameters of a linear code. They are being intensively studied since early 1990s. Generalized weights of a code are closely connected with the trellis complexity, decoding, and the performance of the code when used in a cryptographic channel of a special type. Besides that, generalized weights are used to classify the codes, to construct curves over finite fields with many points, and for other problems.

Generalized Hermite parameters of lattices are analogues of generalized Hamming weights. They were first introduced by Rankin [Ran1] in 1953 as natural invariants of a quadratic form; intensive research in this field started just several years ago. Generalized Hermite parameters are also connected with the trellis complexity and with decoding of Euclidean codes. They are the systoles of flat tori, so their study is important from the point of view of Riemann geometry. Recently, a nice adelic interpretation and generalization of generalized Hermite parameters was discovered.

There exists a noticeable amount of results about generalized Hamming weights; generalized Hermite parameters are much less studied; in particular, few bounds are known. In this thesis, we obtain several new bounds.

Many results from the coding theory have natural analogues in the theory of lattice sphere packings. In many cases, there exist general constructions, so that the results about codes and lattices can be regarded as special cases of one general theorem. For example, the Poisson sum-

mation formula implies the functional equations for the Θ-functions of lattices as well as the MacWilliams identities for weight enumerators. We describe a new construction of this type which is useful in the study of generalized Hamming weights and generalized Hermite parameters. Namely, we construct a Radon transform in spaces connected with codes and lattices and demonstrate several applications of this transform.

An interesting topic in modern algebraic coding theory is the study of algebraic-geometric codes obtained from algebraic varieties of dimension greater than one. There is but few results in this direction ([HTV], [Nog1], [Nog2].) The calculation of generalized Hamming weights for these codes leads to interesting and important geometric problems. In this thesis, we consider the problem of computation of generalized weights for projective Reed-Muller codes. This is equivalent to the computation of the maximum possible number of solutions to a polynomial system of a given rank over a finite field.

We obtain the following new results in this thesis. The notion of *the T-functions* of lattice is introduced. These functions are a generalization of the classical Θ-function and analogues of the generalized MacWilliams weight enumerators. Several identities for these functions are proved. We derive from the Plancherel formula for Radon transforms in various spaces identities for weight enumerators and proofs of a bound on generalized Hamming weights and of the generalized Minkowski–Hlawka theorem. The last proof is based on our generalization of Siegel mean value theorem which is also proved. The inversion formula for a Radon transform gives a new interpretation of the weight/multiplicity duality for projective multisets.

From the known bounds on spherical codes, packings in Grassmannians and in projective spaces, we obtain new bounds for generalized Hermite parameters of lattices with several minimal vectors. For many classical families of lattices these bounds are far better than the previously known ones. In particular, we obtain upper bounds on the (unknown) second generalized Hermite parameter of the dual root lattices A_n^* and D_n^*. These bounds are approximately 1.3 times higher than the known lower bounds.

We obtain a bound on the maximal number of points over a finite

field on an algebraic set of given dimension and degree. Another similar problem is to determine the maximum possible number of solutions to a polynomial system consisting of r linearly independent equations of the same degree d in a projective space over a finite field. We solve the problem for $r = 2$ and propose conjectures about the general case. The problem is equivalent to the computation of generalized Hamming weights for projective Reed-Muller codes.

This thesis is organized as follows. In **Chapter 1**, we give the necessary definitions and mention some known results. In In §1.1 we give the definition of a linear code and of a lattice and describe the connection between a code and its projective multiset. Consider an n-dimensional vector space $\mathbb{F}_q^n$ over a finite field $\mathbb{F}_q$ with the standard basis. We can introduce there the following metric: the distance between two vectors equals the number of distinct coordinates of these vectors. This distance is called *the Hamming distance*; it induces on $\mathbb{F}_q^n$ a structure of a metric vector space. An $[n, k, d]_q$*-code* C is a k-dimensional subspace in $\mathbb{F}_q^n$ such that the minimum distance between any two distinct vectors from C equals d. A code may be considered as a packing of q^k non-intersecting open balls of radius $d/2$ in $\mathbb{F}_q^n$. From any $[n, k, d]_q$-code one can construct *a projective multiset*. It is an n-point multiset in a $(k-1)$-dimensional projective space over $\mathbb{F}_q$. A code can be reconstructed from a multiset up to an isometry. The sets of $\mathbb{F}_q$-points of algebraic varieties are an ample source of good projective multisets. The corresponding codes are called *algebraic-geometric (AG) codes*.

A *lattice* L is a discrete subgroup of $\mathbb{R}^n$, that is the set of all integer linear combinations of the elements of a certain basis in $\mathbb{R}^n$. Let $r(L)$ denote the length of the shortest non-zero lattice vector. Open balls of radius $r(L)/2$ with the centers in lattice vectors do not intersect each other. The density of such packing is an important parameter of the lattice. On of the ways to measure this density is *the Hermite parameter* $\gamma(L) = r^2(L)/\operatorname{vol}^{2/n} L$, where $\operatorname{vol} L$ is the volume of the fundamental domain of L. Another interesting parameter of a lattice is *the kissing number* $\tau(L)$ equal to the number of vectors of length $r(L)$ in L.

In §1.2 we define generalized Hamming weights of linear codes and their analogues for lattices – generalized Hermite parameters. An r-*subcode* is a linear dimension r subspace of a code. *The support* of a

subset $D \subset \mathbb{F}_q^n$ is the set of coordinate positions such that there exists an element of D with a nonzero coordinate at this position. Define *the r-th generalized Hamming weight* $d_r(C)$ of a code C as the minimum support size of an r-subcode. It is clear that $d_1(C) = d(C)$ and that $d_k(C) = n$ provided that there is no position which is zero for all vectors from C. Generalized weights have a natural interpretation for projective multisets, and, in particular, for AG-codes: the r generalized weight is equal to the minimal number of points outside a section of the multiset by a linear space of codimension r.

Let $\mathrm{vol}_m(L)$ denote the minimum volume of a sublattice $M \subset L$ of rank m. Norming this parameters on the volume of the lattice, one gets *the generalized Hermite parameters*$\gamma_r(L)$ of L. Like the Θ-function enumerates the norms of lattice vectors, *the r-th T-function* $r = 1, \ldots, n$ enumerates the norms of r-sublattices. These functions satisfy duality relations; the first T-function is connected with the Θ-function by the means of a Moebius transform.

Further, we describe various relations and bounds on generalized Hermite parameters: generalized Mordell inequality, Coulangeon bound, bounds from packings, and generalized Minkowsky–Hlawka theorem.

The chapter is concluded by a description of two situations where lattices and their generalized Hermite parameters appear as special cases: adelic geometry after Thunder and systoles of Riemann manifolds after Gromov.

Chapter 2 describes applications of the theory of homogeneous spaces in duality ([Hel1],[Hel2]) to codes and lattices. In §2.1 we give a short overview of this theory. The classical example of such an object is the pair of spaces (points in $\mathbb{R}^n$, hyperplanes in $\mathbb{R}^n$) connected by the standard *incidence relation*, that is, a point x is incident to a hyperplane ξ (we denote it by $x \bowtie \xi$) iff $x \in \xi$. In the general case, a pair of homogeneous spaces in duality is a pair of factors of the same locally compact group by two "nice" subgroups. Given a pair (X,Ξ) of homogeneous spaces in duality, to any "nice" function $f(x) : X \to \mathbb{C}$ corresponds *the Radon transform* of this function $\hat{f}(\xi) : \Xi \to \mathbb{C}$. In

the discrete case, the function $\hat{f}(\xi)$ is defined by

$$\hat{f}(\xi) := \sum_{x \bowtie \xi} f(x).$$

Similarly, one defines *the dual Radon transform* defined on "nice" functions $\phi(\xi) : \Xi \to \mathbb{C}$. An important identity is *the Plancherel formula*

$$\sum_{x \in X} f(x)\check{\phi}(x) = \sum_{\xi \in \Xi} \hat{f}(\xi)\phi(\xi). \tag{1}$$

In §2.2 we give a representation of the sublattice spaces $L^{[r]}$ as homogeneous spaces in duality and derive from the Plancherel formula (1) identities on T- and Θ-functions.

In §2.3 we construct a Radon transform in a projective space over a finite field and obtain inversion formulas for it. These formulas have a nice interpretation in the terms of weight/multiplicity duality for projective multisets.

In §2.4 and §2.5 we give two more applications of the Plancherel formula for Radon transforms: a proof of an known Plotkin–type upper bound for generalized Hamming weights and a proof of a nonconstructive lower bound for generalized Hermite parameters (a generalized Minkowski–Hlawka theorem.)

In **Chapter 3**, we prove a number of bounds on the second generalized Hermite parameter. The main idea is the following: if a lattice L has several minimal vectors and a big second generalized Hermite parameter $\gamma_2(L)$, then the configuration of the minimal vectors gives rise to sphere packings and packings in projective space which are "too good to exist." Various known bounds on these packings lead to upper bounds on the ratio $\gamma_2(L)/\gamma_1^2(L)$ in terms of the dimension n and the kissing number $\tau(L)$.

These bounds can be applied to estimate the second generalized Hermite parameter of classical lattices. In some cases the second generalized Hermite parameter is known; our bounds are often approximately 1.3 times higher, than the true value. For some other lattices, second generalized Hermite parameter is unknown; it is interesting, that in these cases our bound differs from the lower bound (generalized Mordell inequality) also approximately in 1.3 times.

In **Chapter 4**, we study the following problem. Consider the m-dimensional projective space $\mathbb{P}^m$ over a finite field $\mathbb{F}_q$ with q elements and a system of r linearly independent homogeneous polynomials of the same degree d. The problem is to find the maximum possible number of solutions in $\mathbb{P}^m$ to such a system. For $r = 1$ this problem was solved by J.-P. Serre [Ser] who proved a conjecture by Tsfasman. We solve this problem for $r = 2$ and state several conjectures about the general case. For the affine space this problem was solved by Heijnen and Pellikaan [HP]. The answer is similar, but the methods they used are quite different and it is not clear how they can be extended to the projective case.

Another similar problem is to determine the maximum possible number $|X|$ of $\mathbb{F}_q$-points on an algebraic set X in $\mathbb{P}^m$ of given dimension s and degree d. This problem was addressed by several researchers in last 40 years ([Nis],[Sch],[Lac].) We prove that

$$|X| \leq dp_s,$$

where $p_s = (q^{s+1} - 1)/(q - 1)$ is the number of points in a projective space of dimension s. Previously, this inequality was proven only under various restrictions on d, q, m, and s.

The first problem is equivalent to the calculation of the maximum possible number of points on a section of codimension r of a Veronese variety, and, thus, to the calculation of the generalized Hamming weights of the corresponding AG-code. These codes are called *degree d projective q-ary Reed-Muller codes* and are interesting from the theoretical point of view (they are in a certain sense a *universal* family of codes.)

Proofs of our results are based on construction, which is equivalent to the use of the Plancherel formula for a Radon transform in $\mathbb{P}^m$.

I would like to express my deep gratitude to my advisors Gerard van der Geer and Michael Tsfasman for their attention and help, and also to Leonid Bassalygo, Tom Koornwinder, Alexander Kuznetsov, Oscar Lemmers, Vladimir Levenshtein, Riccardo Re, Pyotr Sergeev, Georgij Shabat, and Vassily Shabat for valuable discussions and help.

Chapter 1

Codes and Lattices

In this chapter, we give an overview of the theory of lattice sphere packings in Euclidean space, and of the theory of linear block codes. We start with the classical theory in Section 1.1. These topics are covered in detail in books [SPLAG] and [McWS]. In Section 1.2, we describe the current state of knowledge on generalized Hermite parameters and generalized Hamming weights. In the description of generalized weights, we use the excellent review papers [Wei2], [TV2], and [HKYL]. The author is unaware of any detailed review on generalized Hermite parameters.

1.1 Codes and Lattices: the Classical Theory

1.1.1 Basic Notions

In an n–dimensional vector space $\mathbb{F}_q^n$ over a finite field $\mathbb{F}_q$, one may introduce *the Hamming metric*

$$d(u,v) := \text{“the number of distinct coordinate positions in } u \text{ and } v''.$$

A *linear* $[n,k,d]_q$*-code* C is a k-dimensional subspace of $\mathbb{F}_q^n$ such that the distance between any two distinct vectors from C is at least d. Any linear subspace $D \in C$ is called a *subcode* of C. The vectors from C are also called the *codewords* of C. The distance from a codeword c to the

all-zero vector is called *the (Hamming) weight* of the codeword and is denoted by $\mathrm{wt}(c)$.

The codewords of a linear $[n,k,d]_q$-code can be considered as a packing of q^k open non-overlapping spheres of radius $[d/2]$ in the metric space $\mathbb{F}_q^n$.

A *lattice* is a discrete subgroup in the Euclidean space $\mathbb{R}^n$. As a group, any lattice is isomorphic to $\mathbb{Z}^m$, $m \leq n$. Given a subset $M \subset \mathbb{R}^n$, by $\langle M \rangle_{\mathbb{R}}$ we denote the linear subspace generated by M. If not explicitly stated otherwise, lattices will be assumed to be of *full rank*, i.e. $\langle L \rangle_{\mathbb{R}} = \mathbb{R}^n$,

Fix a scalar product in $\mathbb{R}^n$. Then, besides the rank, any lattices gets metric invariants. The most important are *the length of the minimal vector*

$$r(L) := min_{v \in L \setminus \{0\}} |v|,$$

and *the volume* $\mathrm{vol}\, L$ *of the fundamental domain* $\mathbb{R}^n/L$. This volume is also called the *volume*[1] *of* L. We shall mostly use the square of this volume which is called *the determinant of* L and is denoted by $\det L$,

$$\det L := \mathrm{vol}^2(\mathbb{R}^n/L).$$

If $(e_1, \ldots, e_n)$ is a $\mathbb{Z}$-basis of L, then $\det L$ equals the determinant of the Gram matrixof $(e_1, \ldots, e_n)$. Another interesting invariant of a lattice is the *kissing number* $\tau(L)$ — the number of lattice vectors with the length $r(L)$.

A *geometric invariant* of a lattice is a parameter invariant under the standard action of the orthogonal group $O(n)$ and under scalings $v \mapsto \lambda v$, $\lambda \in \mathbb{R}^*$. Neither $r(L)$ nor $\det L$ are geometric invariants of L. However, one can combine them to get a geometric invariant. The usual way to do so is to consider *the Hermite parameter* (also called *the coding gain*) of L

$$\gamma(L) := \frac{r^2(L)}{\det^{1/n} L}. \tag{1.1}$$

Obviously, the kissing number is also a geometric invariant.

[1]Perhaps, it is more appropriate to call it *the covolume* of L

An r-sublattice is a rank r subgroup of a lattice. The following proposition is evident.

Proposition 1.1 *The following three properties of a sublattice $M \subset L$ are equivalent:*

1. *the $\mathbb{R}$-hull of M intersects with L by M: $\langle M \rangle_{\mathbb{R}} \cap L = M$;*
2. *M is not strictly contained in any sublattice of the same rank as M;*
3. *any basis of M may be completed to a basis of L.*

A sublattice $M \subset L$ satisfying any of the three equivalent properties of Proposition 1.1 is called *primitive*.

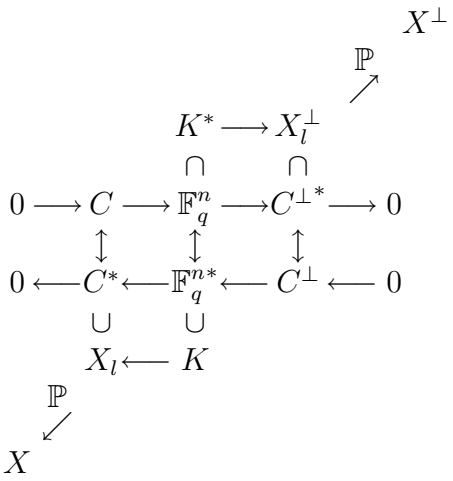
A lattice L may be considered as a packing of spheres of radius $r(L)/2$. The density of this packing is determined by $r(L)$ and $\det L$. There exist many (equivalent) ways to measure the density. Most widely used are the following three (by V_n we denote the volume of a unit ball in $\mathbb{R}^n$: $V_n = \frac{\pi^{n/2}}{\Gamma(n/2+1)}$ and $\rho = r(L)/2$ is the packing radius):

packing density	$\Delta(L) = \frac{V_n \cdot \rho^n}{(\det^{1/2} L)}$
central density	$\delta(L) = \rho^n / \det^{1/2} L$
Hermite parameter	$\gamma(L) = r(L)^2 / \det^{1/n} L = 4 \cdot \delta^{2/n}$

1.1.2 Duality

For a given linear code C there exist at least two objects which are in some sense dual to C: the *dual code* $C^\perp$ and the projective multiset $X(C)$. For an $[n,k,d]_q$-code C the *dual code* is a code $C^\perp \subset \mathbb{F}_q^n$ such that for any codewords $y \in C^\perp$ and $x \in C$ the scalar product (x,y) equals zero. The restrictions to C of n coordinates in $\mathbb{F}_q^n$ are the elements of the linear space C^* dual to C. The image of these n elements under projectivization $C^* \to \mathbb{P}^{k-1}$ is called *the projective multiset $X(C)$* of a code C. Let K be the standard basis in $\mathbb{F}_q^{n*}$ and let K^* be the dual basis of $\mathbb{F}_q^n$. From the definiton of the dual code it follows that the embeddings $C \hookrightarrow \mathbb{F}_q^n$ and $C^\perp \hookrightarrow \mathbb{F}_q^{n*}$ can be completed to short exact sequences (see the commutative diagram below.) These completions

deliver the image X_l of K on C^* and the image $X_l^\perp$ of K^* in $C^{\perp *}$. The image of X_l under the projectivization $C^* \to \mathbb{P}C^*$ is the projective multiset X of code C; the image of $X_l^\perp$ under the projectivization $C^{\perp *} \to \mathbb{P}C^{\perp *}$ is the projective multiset $X^\perp$ of the dual code code $C^\perp$.



An interesting (unsolved) problem is to reconstruct $X^\perp$ from X.

The projective multiset may be also considered as the restriction of the Hamming metric in $\mathbb{F}_q^n$ on C. Tsfasman and Vlăduţ [TV1] have shown that most problems about codes can be naturally reformulated in the terms of projective multisets.

The dual code can be defined in a more general way. Consider a code C as a subgroup of $\mathbb{F}_q^n$ and define the dual code $C^\perp$ as the group of C-invariant characters on $\mathbb{F}_q^n$. The MacWilliams identities (1.3) stated below are then a corollary of the general Poisson summation formula. This formula states that for a locally compact group G and a closed subgroup $H \subset G$ the integral of a function f over H equals the integral of the Fourier transform $\tilde{f}$ over h-invariant characters:

$$\int_H f(x)\,dx = \int_{\widehat{G/H}} \tilde{f}(\alpha)\,d\alpha. \tag{1.2}$$

For a lattice L, the *dual lattice* $L^\perp$ may be also defined as the group of L-invariant characters on $\mathbb{R}^n$. A scalar product in $\mathbb{R}^n$ allows then to

identify $L^\perp$ with the set $\{y \in \mathbb{R}^n : \ \forall x \in L \ (x,y) \in \mathbb{Z}\}$. The Poisson summation fromula implies the functional equation (1.5).

Instead of a discrete group with an embedding to $\mathbb{R}^n$ we can consider a free $\mathbb{Z}$-module of rank n equipped with a positive quadratic form. Thus, any statement about lattices may be easily reformulated in the language of quadratic forms. This language will be sometimes convenient to us in Chapter 2.

1.1.3 Spectra

Let $A_j(C)$ denote the number of the codewords of weight j in a code C. The ordered set $\{A_j(C)\}$, $j = 0, \ldots, n$, is called the *weight spectrum* of C. It is convenient to represent the spectrum by *the weight enumerator* $W_C(x,y) := \sum_{j=0}^n A_j x^{n-j} y^j$.

The spectrum of an $[n,k,d]_q$-code C and of the dual code $C^\perp$ satisfy the MacWilliams identities

$$W_{C^\perp}(x,y) = \frac{1}{q^k} W_C(x + (q-1)y, x-y). \tag{1.3}$$

The spectrum of a lattice is the distribution of length of lattice vectors. The analogue of the weight enumerator is *the* Θ*-function* of a lattice:

$$\Theta_L(q) := \sum_{v \in L} q^{\|v\|} = \sum_k N_k q^k, \tag{1.4}$$

where N_k is the number of lattice vectors with the norm k. It is easy to show that for any lattice $N_k = 0$ for all k not in a certain discrete set. It is often convenient to replace the argument q of Θ by z, $q = e^{\pi i z}$.

The analogue of the MacWilliams identities (1.3) is the functional equation for Θ-functions:

$$\Theta_{L^\perp}(z) = (\det L)^{1/2} \left(\frac{i}{z}\right)^{n/2} \Theta_L\left(-\frac{1}{z}\right). \tag{1.5}$$

As well as the the MacWilliams identities (1.3), this equation is a corollary of the Poisson summation formula (1.2).

1.2 Generalized weights

1.2.1 Definitions

Generalized Hamming weights of linear codes were first introduced by Helleseth, Kløve, and Mykkeltveit [HKM] in 1977. The are also called *the weight hierarchy*, *minimum support sizes*, or *the dimension/length profile*. Let C be a linear $[n,k,d]_q$-code. *The support* $\operatorname{supp}(D) \subset \{1,\dots,n\}$ of a subset $D \subset C$ is the set of coordinate positions such that there exists a codeword $c \in D$ with a non-zero component in this position. Let $C^{[r]}$ denote the set of all r-subcodes of C. Define *the r-th generalized Hamming weight* $d_r(C)$, $r = 1,\dots,k$ by

$$d_r(C) := \min_{D \in C^{[r]}} \#\operatorname{supp}(D).$$

The set $\{d_1, d_2, \dots, d_r\}$ is called *the weight hierarchy* of C. The properties of generalized weights are described in reviews [Wei2], [HKYL], and [TV2].

An analogue of generalized weights for lattices was introduced by R. Rankin [Ran1] in 1953.

Let $\operatorname{vol}_m(L)$, $m = 1, 2, \dots, n$, denote the minimal volume of an m-sublattice of a lattice L:

$$\operatorname{vol}_m(L) := \min_{M \subset L,\ \operatorname{rk} M = m} \operatorname{vol} M. \tag{1.6}$$

It is clear that $\operatorname{vol}_1(L) = r(L)$ and $\operatorname{vol}_n(L) = \operatorname{vol}(L)$. It is not hard to check that the minimum in Eq. (1.6) is reached at a certain sublattice. The numbers $\operatorname{vol}_m(L)$ are not geometric invariants of a lattice: they are not preserved under scaling. We can normalize them on $\det L$. Thus we get *the generalized Hermite parameters* of L

$$\gamma_m(L) := \operatorname{vol}_m^2(L)/\det{}^{m/n} L.$$

They are also called *Rankin m-invariants*.

Note. From some points of view better analogues of generalized Hamming weights are *the normalized logarithmic densities* introduced by Forney [For2]

$$\kappa'_m(L) := -\log(\operatorname{vol}_m(L)/\operatorname{vol}(L)^{m/n}) = -\frac{1}{2}\log\gamma_m(L).$$

Rankin proved that *the generalized true Hermite constants*

$$\gamma_{n,m} = \max_{\mathrm{rk}(L)=n} \gamma_m(L)$$

exist and that the maximum is reached at a certain lattice L.

1.2.2 Duality

Wei [Wei1] proved that generalized Hamming weights of a code C are determined by the generalized Hamming weights of the dual code $C^\perp$.

Rankin proved the following duality relation for generalized Hermite parameters:

Proposition 1.2 ([Ran1],[For2]) *For any $1 \le m < n$ and for any lattice $L \in \mathbb{R}^n$*

$$\gamma_m(L) = \gamma_{n-m}(L^\perp) \tag{1.7}$$
$$\gamma_{n,m} = \gamma_{n,n-m}\,. \tag{1.8}$$

Sketch of the proof. Without loss of generality we can assume that $\det L = 1$. Then for any m-sublattice $M \subset L$ there exists an $(n-m)$-sublattice $K \subset L^\perp$ with $\mathrm{vol}\, M = \mathrm{vol}\, K$ (see [Ran1]; this is a generalization of Kramer matrix inversion formula.) This proves Eq. (1.7). Taking the minimum in Eq. (1.7) over all sublattices of rank n we obtain Eq. (1.8) $\triangle$

1.2.3 Generalized Spectra

The generalized spectrum $(A_i^r(C))$, $r = 0, \ldots, k$; $i = 0, \ldots, n$ of a code is the distribution of subcode support sizes:

$$A_i^r(C) := \#\{D \in C^{[r]} |\ \mathrm{supp}\, D = i\}.$$

Let $\begin{bmatrix} a \\ b \end{bmatrix}_q$ denote the Gaussian binomial coefficient

$$\begin{bmatrix} a \\ b \end{bmatrix}_q := \frac{(q^a-1)(q^{a-1}-1)\ldots(q^{a-b+1}-1)}{(q^b-1)(q^{b-1}-1)\ldots(q-1)}.$$

The generalized spectrum $(A_i^r)$of an $[n,k]_q$-code C and the generalized spectrum $(\tilde{A}_v^u)$ of the dual $[n,n-k]_q$-code $C^\perp$ are related by *generalized MacWilliams identities* (see [Klo], [Sim])

$$\sum_{i=0}^{j} \binom{n-i}{n-j} A_i^r = \sum_{u=0}^{r+k-j} q^{u(j-k+u-r)} \begin{bmatrix} j-k \\ r-u \end{bmatrix}_q \sum_{v=0}^{n-j} \binom{n-v}{j} \tilde{A}_v^u,$$
$$r = 0, \ldots, k, \quad j = 0, \ldots, n. \tag{1.9}$$

Let $L^{[r]}$ denote the set of all primitive r-sublattices of a lattice L and $\overline{L^{[r]}}$ denote the set of all shifts of r-sublattices by lattice vectors. The "size" of a sublattice ξ is measured by $\det \xi$. In this section, we shall sometimes write $\|\xi\|$ instead of $\det \xi$. It is convenient to represent the distribution of r-sublattice sizes by the *r-th T-function* of a lattice: $(r = 1, \ldots, n)$:

$$T_L^r(q) := \sum_{\xi \in L^{[r]}} q^{\|\xi\|}. \tag{1.10}$$

The first T-function $T_L^1(q)$ does not coincide with the Θ-function of L; however, they are closely related and determined by each other. Let $\mu : \mathbb{N} \mapsto \mathbb{N}$ denote the Moebius μ-function: $\mu(k)$ is zero whenever k is not square-free; otherwise, $\mu(k)$ equals the oddity of the number of prime divisors of k.

Proposition 1.3 *For any lattice L*

$$\Theta_L(q) - 1 = 2 \sum_{m=1}^{\infty} T_L^1(q^{m^2}) =; \tag{1.11}$$

$$2T_L^1(q) = \sum_{k=1}^{\infty} \mu(k) \left(\Theta_L(q^{k^2}) - 1 \right). \tag{1.12}$$

Proof. To any primitive 1-sublattice $M \subset L$ corresponds a pair of primitive vectors $(p_M, -p_M)$ such that $M = \mathbb{Z}p_M$. Any vector $v \in L$ can be uniquely written as $v = mp_M$, where p_M is a primitive vector and $m \in \mathbb{Z}$. Thus,

$$\Theta_L(q) - 1 = 2 \sum_{v \in L} q^{\|v\|} = 2 \sum_{M \in L^{[1]}} \sum_{m=1}^{\infty} q^{\|mp_M\|} = 2 \sum_{m=1}^{\infty} T_L^1(q^{m^2}).$$

Eq. (1.12) can be obtained from Eq. (1.11) by a standard Moebius inversion. $\triangle$

Θ-function of a lattice can be also expressed via the summation over primitive 1-sublattices and the third Jacobi θ-function:

$$\begin{aligned}\Theta_L(q) - 1 &= \sum_{v\in L\setminus\{0\}} q^{\|v\|} = \\ &= 2\left(\sum_{v\in L^{[1]}} q^{\|v\|} + \sum_{v/2\in L^{[1]}} q^{\|v\|} + \ldots + \sum_{v/k\in L^{[1]}} q^{\|v\|} + \ldots\right) = \\ &= 2\sum_{v\in L^{[1]}}\sum_{m=1}^{\infty} q^{m^2\|v\|} = 2\sum_{v\in L^{[1]}} \theta_3(q^{\|v\|}). \qquad (1.13)\end{aligned}$$

Similarly to the duality relations (1.7) one can prove the following proposition.

Proposition 1.4 *For any lattice L*

$$T_L^r(q) = T_{L^\perp}^{n-r}(q^{\det L}). \qquad (1.14)$$

An interesting problem is to determine the lattice analogue of generalized MacWilliams identities (1.9). Proposition 1.4 gives n relations on generalzied spectra. Since we have $(k+1)(n+1)$ generalized MacWilliams identity, one could expect to have more relations on T-functions. Propositions 1.3 and 1.4 combined with the functional equation (1.5) for the Θ-function imply two more such relations. Consider the following objects: a lattice L, its dual $L^\perp$, and the sets $L^{[1]}$, $L^{[n-1]}$, $L^{\perp[1]}$, $L^{\perp[n-1]}$ of their primitive sublattices of ranks 1 and $n-1$. Let $\leftrightarrow$ mean that the spectrum of one object is determined by the spectrum of another. We have the following diagram.

$$\begin{array}{ccc} L^{[1]} & \overset{(1.14)}{\longleftrightarrow} & L^{\perp[n-1]} \\ \updownarrow{\scriptstyle (1.12)} & & \\ L & \overset{(1.5)}{\longleftrightarrow} & L^\perp \\ & & \updownarrow{\scriptstyle (1.12)} \\ L^{[n-1]} & \overset{(1.14)}{\longleftrightarrow} & L^{\perp[1]} \end{array}$$

Traveling along this "snake" we see that the spectrum of $L^{[1]}$ is determined by the spectrum of $L^{[n-1]}$ and that the same is true for $L^{\perp}$. Unfortunately, the author failed to write explicitly these relations in a nice form.

1.2.4 Generalized Spectra and Tensor Products

Kløve [Klo] proved generalized MacWilliams identities (1.9) by the following argument. For a given code C consider the code $C^{(s)} := C \otimes \mathbb{F}_{q^s}$ over the degree s extension $\mathbb{F}_{q^s}$ of $\mathbb{F}_q$. Codewords of $C^{(s)}$ can be represented by $s \times n$-matrices over $\mathbb{F}_q$; the rows of these matrices are codewords of C. The weight of a codeword $c \in C^{(s)}$ equals the support size of a subcode $D \in C$ generated by the rows of c. Thus, the generalized spectrum of C can be expressed via the usual spectra of $C^{(s)}$, $s = 1, \ldots, k$. The MacWilliams identities for $C^{(s)}$ imply then Eqs. (1.9). Note that instead of $\mathbb{F}_{q^s}$ one could use an arbitrary free $\mathbb{F}_q$-module of rank s.

It seems that generalized Hermite parameters of lattices can not be expressed via the usual parameters of any simple tensor object. On the other hand, the minimum norm of the tensor power $L^{\otimes m} = L \otimes L \otimes \ldots \otimes L$ is a lower bound on the minimum norm of m-sublattices of L. However, $L^{\otimes m}$ contains also non-split elements. Coulangeon [Cou2] proved that there exist lattices such that the minimum norm in $L^{\otimes m}$ is reached on a non-split element.

1.2.5 Bounds

Bounds on generalized weights are given in [TV2] and [HKYL].

The bounds on generalized Hermite parameters of lattices can be divided into the following three groups:

- Upper bounds;
- Lower bounds;
- Relations between various generalized Hermite parameters and other invariants.

In the theory of packings, one usually calls *upper bounds* the statements of the form

$$\gamma_{n,m} < C(n,m) \qquad \text{for any } n.$$

An upper bound for generalized Hermite parameters was obtained by Coulangeon (see Eq. (1.19) below.)

A lower bound is usually a statement of the form "for any n there exists a lattice $L \subset \mathbb{R}^n$ with $\gamma_m(L) > C(n,m)$." Obviously any infinite family of lattices with growing rank produces a lower bound. However, as in most other cases in the theory of packings, these *constructive* lower bounds are worse than the *nonconstructive* lower bounds, i.e. the lower bounds obtained by a certain averaging argument. A good nonconstructive lower bound is given by the generalized Minkowski–Hlawka theorem (Eq. (1.18).)

Besides upper and lower bounds, we have also relations (1.15), (1.16) between different generalized Hermite parameters and relations (1.20), (1.21), (3.11), (3.12) between them and other invariants of lattices.

A) Generalized Mordell Inequality [Ran1]. For any n-lattice L and any m and r such that $1 \le m < r < n$ we have

$$\gamma_m(L) \le \gamma_{r,m}(\gamma_r(L))^{m/r}, \tag{1.15}$$

and

$$\gamma_{n,m} \le \gamma_{r,m}(\gamma_{n,r})^{m/r}. \tag{1.16}$$

Rankin proved (1.16); his argument also proves Eq. (1.15) although he did not state it explicitly.

Independently, Forney [For2] proved a special case of Eq. (1.15). Substituting $m = 1$ to Eq. (1.15) we get the inequality

$$\gamma_r(L) \ge \gamma_1(L)/\gamma_r^r, \tag{1.17}$$

which is equivalent to Forney bound $\kappa_r(L) \le (r/2)\log(\gamma_r/\gamma_1(L))$.

A lattice L meets bound (1.17) iff it has the densest r-dimensional lattice as a sublattice with the same minimum norm as L. For example, for the laminated lattice Λ_n we have $\gamma_r(\Lambda_n) = \gamma(\Lambda_n)/\gamma_r^r$ at least for $r = 1, \dots, 8$ and any n. It is often convenient to use inequality (1.17) combined with lower bounds on γ_r as a lower bound on $\gamma_r(L)$.

B) Lower bound on $\gamma_{n,m}$ (generalized Minkowski–Hlawka theorem.) This is a non-constructive lower bound. It was first proved by Thunder [Thu1] in a more general adelic context. In Chapter 2 we shall give a simpler proof of this theorem as a corollary of the Plancherel formula for a suitable Radon transform. The theorem states that for any $m < n$ there exists a lattice $L \subset \mathbb{R}^n$ such that

$$\gamma_m(L) \geq \left(n \frac{\prod_{j=n-m+1}^{n} Z(j)}{\prod_{j=2}^{m} Z(j)} \right)^{2/n}, \tag{1.18}$$

where $Z(j) = \zeta(j)\Gamma(j/2)/\pi^{j/2}$, and $\zeta(j) = \sum_{k=1}^{\infty} k^{-j}$ is the Riemann ζ-function.

C) Coulangeon [Cou1] proved the following **upper bound on $\gamma_{n,r}$**

$$\gamma_{n,r} \leq \gamma_n^r. \tag{1.19}$$

This result is essentially a corollary of Minkowski studies on consecutive minima of a quadratic form. It allows to apply various upper bounds on the classical Hermite constant to generalized Hermite constants.

D) Bounds on $\gamma_2(L)$ via packings in projective spaces. Suppose L has $\tau(L) \geq 4$ minimal vectors. Then

$$\gamma_2(L) \leq \frac{n-1}{n} \times \frac{\tau(L)}{\tau(L)-2} \times \gamma_1(L)^2. \tag{1.20}$$

If $\tau(L) > n(n+1)$ then (1.20) may be improved and

$$\gamma_2(L) \leq \frac{n-1}{n} \times \gamma_1(L)^2. \tag{1.21}$$

We shall prove these bounds and several others of the same form in Chapter 3.

Note that combining bounds (1.18) and (1.19) we get that for any fixed m

$$\log \gamma_{n,m} = m \log n + O(1)$$

as $n \to \infty$. The implied constant depends on m and is unknown even for the classical case $m = 1$.

1.3 Interpretations of Generalized Hermite Parameters

1.3.1 Adelic Interpretation

J. Thunder [Thu1], [Thu2] proposed an adelic generalization of the Hermite parameter; our generalized Hermite parameters are a special case of this generalization.

Let K be a number field and let $K_{\mathbb{A}}$ be the ring of adeles of K. For a vector $x \in K^n$ and a place v of K let $\|x\|_v$ be the norm of x defined by

$$\|x\|_v = \begin{cases} \max_{1\le i\le n} \{|x_i|_v\} & \text{if } v \text{ is finite} \\ \left(\sum_{i=1}^n |x_i|_v^2\right)^{1/2} & \text{if } v \text{ is real} \\ \sum_{i=1}^n |x_i|_v & \text{if } v \text{ is complex.} \end{cases}$$

For $x \in K^n$ and $A = \{A_v\} \in GL_n(K_{\mathbb{A}})$ define *the twisted height* $H_A(x)$ by

$$H_A(x) = \left(\prod_v \|A_v(x)\|_v\right)^{1/\deg K}.$$

From the product formula for valuations it follows that $H_A(x)$ is preserved by the scalings of x, so it is a height on the projective space $\mathbb{P}^{n-1}(K)$. If A is the identity matrix $E_n \in GL_n(K_{\mathbb{A}})$, then we get the usual absolute multiplicative Weil height.

This height can be extended to a Grassmannian $\mathcal{G}(n,m)$ using the exterior products. For a linear subspace $V \in \mathcal{G}(n,m)$ the height $H_A(V)$ can be defined as the height of the m-th external power $\wedge^m V \in \mathbb{P}^{\binom{n}{m}-1}(K)$.

Define now *the generalized Hermite constant* $\gamma_{n,m}(K)$ as

$$\gamma_{n,m}(K) = \sup_A \inf_V \left(H_A(V)\right)^2 \Big/ (\det A)^{\frac{2m}{n \deg K}}.$$

Thunder has shown that for $K = \mathbb{Q}$ this definition coincides with our definition of generalized Hermite constants. He also proved the generalized Mordell inequality (1.16), Coulangeon upper bound (1.19), and generalized Minkowski–Hlawka theorem (1.18) for arbitrary K.

1.3.2 Systoles of Riemann Manifolds

Another point of view on generalized Hermite parameters is given in [Gro]. Let $\mathcal{M}$ be a Riemann manifold of dimension n. *The m-th homological systole* $\mathrm{syst}_m(\mathcal{M}, H_m(\mathbb{Z}))$ of $\mathcal{M}$ is defined as the minimal volume of a non-homological to zero m-cycle in $\mathcal{M}$. We denote this systole also by by $\mathrm{syst}_m(\mathcal{M})$. Similarly, one may define systoles with the coefficients in other groups. The volume of a smallest non-contractible m-cycle in $\mathcal{M}$ is called *the m-th homotopical systole* of $\mathcal{M}$ and is denoted by $\mathrm{syst}_m(\mathcal{M}, \pi_1)$. One may also use the homologies of $\mathcal{M}$ with the coefficients in a domain other than $\mathbb{Z}$. For example, $\mathrm{syst}_m(\mathcal{M}, H_m(\mathbb{Z}/2\mathbb{Z}))$ is the volume of a smallest non-homological to zero modulo 2 cycle in $\mathcal{M}$. It is clear that

$$\mathrm{syst}_m(\mathcal{M}, \pi_1) \leq \mathrm{syst}_m(\mathcal{M}, H_m(\mathbb{Z})) \leq \mathrm{syst}_m(\mathcal{M}, H_m(\mathbb{Z}/2\mathbb{Z})).$$

The notion of the m-th systole was introduced by M. Berger [Ber1], [Ber2] in 1972 following the ideas and works by Loewner, Pu [Pu], and Accola [Acc]. See also [BS], [Bav] and [BM] for the discussions of systoles for special families of lattices and manifolds.

When $\mathcal{M}$ is a flat tori (that is a factor of $\mathbb{R}^n$ by a full rank lattice L with the induced metric), then the m-th systole $\mathrm{syst}_m(\mathcal{M}, H_m(\mathbb{Z}))$ coincides with the generalized Hermite parameter $\gamma_m(L)$.

For $\dim \mathcal{M} = 2$ Loewner proved the following theorem.

Theorem 1.1 ([Gro]) *Let $\mathcal{M}$ be a topological 2-torus with a Riemann metric normalized so that* $\mathrm{vol}(\mathcal{M}) = 1$. *Then*

$$\mathrm{syst}_1(\mathcal{M}) \leq \left(\frac{2}{\sqrt{3}}\right)^{1/2}.$$

The proof of the theorem is based on **the uniformization theorem for tori** (see [Apa]) which states that for every $\mathcal{M}$ there exists a flat tori $\mathcal{M}'$ with a conformal diffeomorphism $\phi : \mathcal{M}' \to \mathcal{M}$. This theorem means that the systole of a topological flat torus does not exceed the systole of the flat torus corresponding to the densest 2-dimensional lattice. No similar results are known for higher dimensions.

Chapter 2

Homogeneous spaces in duality

In this chapter, we mention first some notions from the theory of homogeneous spaces in duality as developed in [Hel1] and [Hel2]. This theory delivers a unified point of view on many dualities arising in coding and lattices theories. We prove relations on T-functions, two known bounds on generalized Hamming weights and generalized Hermite parameters, and give a new interpretation of Nogin weight/multiplicity duality. It seems to us that many other applications of these technique are possible. For example, in proofs of Theorems 4.1, 4.2, and 4.3 in Chapter 4, the key step is equivalent to the use of the Plancherel formula for a suitable Radon transform in $\mathbb{P}^m(\mathbb{F}_q)$.

2.1 General Theory

In this section, we follow the books [Hel1] and [Hel2].

Let G be a locally compact group, X and Ξ two (left) coset spaces $X = G/H_X$ and $\Xi = G/H_\Xi$, where H_X and H_Ξ are two closed subgroups of G. Let K be the intersection $X \cap \Xi$. Let us make the following assumptions:
(i) The groups G, H_X, H_Ξ, $H_X \cap H_\Xi$ are unimodular (i.e. the left-invariant Haar measures are right-invariant);
(ii) For any $h_X \in H_X$ the inclusion $h_X H_\Xi \subset H_\Xi H_X$ implies $h_X \in H_\Xi$;

for any $h_\Xi \in H_\Xi$ the inclusion $h_\Xi H_X \subset H_X H_\Xi$ implies $h_\Xi \in H_X$;
(iii) The set $H_X H_\Xi$ is closed.

Homogeneous spaces X and Ξ are called *homogeneous spaces in duality*. We shall say that $x \in X$ and $\xi \in \Xi$ are *incident* and denote it by $x \bowtie \xi$ if the cosets xH_X and ξH_Ξ are not disjoint. The classical example of the homogenous spaces in duality is the pair (points in $\mathbb{R}^n$, hyperplanes in $\mathbb{R}^n$) with the incidence relation $(x \bowtie \xi) \Leftrightarrow (x \in \xi)$.

Other examples are the pair of real Grassmanians $(\mathcal{G}(n,m), \mathcal{G}(n, n-m-1))$, ([Hel1]), symmetric spaces, complex spaces, and quadrics in $\mathbb{C}^4$ ([GGV]), The transform considered in §2.3 can be regarded as the $\mathbb{F}_q$-analogue of the real *X-ray transform* widely applied in radiology and tomography [LS].

We put

$$\check{x} = \{\xi \in \Xi : x \bowtie \xi\} \subset \Xi, \quad \hat{\xi} = \{x \in X : \xi \bowtie x\} \subset X.$$

The factor G/K may be identified with the set $\{(x,\xi) \in X \times \Xi : x \bowtie \xi\}$.

The maps $x \mapsto \check{x}$ and $\xi \mapsto \hat{\xi}$ can be also described via the double filtration

$$\begin{array}{ccc} & G/K & \\ p \swarrow & & \searrow \pi \\ X = G/H_X & & \Xi = G/H_\Xi \end{array}, \tag{2.1}$$

where $p(gH_x \cap H_\Xi) = gH_X$ and $\pi(gH_X \cap H_\Xi) = gH_\Xi$. Namely,

$$\check{x} = \pi\left(p^{-1}(x)\right), \hat{\xi} = p\left(\pi^{-1}(\xi)\right).$$

Given Haar measures that satisfy (i) we may construct nice G-invariant measures $m(x)$ on each $\hat{\xi}$ and $\mu(\xi)$ on each $\check{x}$ (cf. [Hel1, p. 143].)

The *Radon transform* $\hat{f} : \Xi \to \mathbb{C}$ of a function $f : X \to \mathbb{C}$ is defined by

$$\hat{f}(\xi) = \int_{\hat{\xi}} f(x)\, dm(x); \tag{2.2}$$

the *dual Radon transform* $\check{\phi} : X \to \mathbb{C}$ of a function $\phi : \Xi \to \mathbb{C}$ is defined by

$$\check{\phi}(x) = \int_{\check{x}} \phi(\xi)\, d\mu(\xi). \tag{2.3}$$

Lemma 2.1 *(***[Hel1], Plancherel formula.)** *Let $f : X \to \mathbb{C}$ and $\phi : \Xi \to \mathbb{C}$ be continuous compact support functions. Then $\hat{f}$ and $\check{\xi}$ are continuous and*

$$\int_X f(x)\check{\phi}(x)\,dx = \int_\Xi \hat{f}(\xi)\phi(\xi)\,d\xi. \tag{2.4}$$

Note. For a discrete group G the formal equalities

$$\sum_{x\in X} f(x)\check{\phi}(x) = \sum_{(x,\xi)\in X\times\Xi:\ x\bowtie\xi} f(x)\phi(\xi) = \sum_{\xi\in\Xi} \hat{f}(\xi)\phi(\xi) \tag{2.5}$$

show that Eq. (2.4) holds also for any functions f and ϕ such that all series in (2.5) converge absolutely. The proof for the general case is similar but requires some additional facts about measures and groups.

Actually, equality (2.4) holds in a more general case of a double filtration like (2.1) than that of conditions (i)-(iii). However, the existence of a nice group structure is often useful and helps to choose the right homogeneous space representation.

The problem of the *inversion* of a Radon transform (2.2) and of the dual transform (2.3), is, in general, rather complicated[1], and there is no general inversion formula. In some special cases this problem was solved. For the classical case of the pair ($\mathbb{R}^n$, hyperplanes in $\mathbb{R}^n$) this problem was solved by J. Radon [Rad]. The inversion formulas are quite different in the cases of the even and odd dimensions. For a pair of real Grassmannians, the Radon transform was inverted by Helgason [Hel1]. We did not find an inversion formula for lattice spaces being investigated in the next section. The case of codes is simpler and an inversion formula for a Radon transform in a projective space over a finite field is obtained in Section 2.3. An equivalent result was proved by Nogin [Nog3] in connection with one problem about projective multisets.

[1] A Radon transform often maps some "non–essential" functions to the all-zero function (see [GGV].) In the case of a vector space over a finite field these "non–essential" functions are somewhat similar to latin squares (see the cover.) Indeed, take the rows and the columns of a latin square as one space Ξ , and the cells as the other space X. The numbers in cells define a certain function on X and the Radon tranform of this function is constant on Ξ.

2.2 A Duality Between Vectors and $(n-1)$-sublattices

Let $A(n)$ denote the group of integer $n \times n$ matrices with the determinant ± 1:

$$A(n) := \{M \in GL_n(\mathbb{Z}) : \quad |\det M| = 1\} \simeq SL_n(\mathbb{Z}) \times \{\pm 1\}.$$

The subset $G = R(n) \subset GL_{n+1}(\mathbb{Z})$ defined by

$$G = R(n) := \begin{pmatrix} A(n) & \mathbb{Z}^n \\ 0 & 1 \end{pmatrix} \tag{2.6}$$

is a group with the respect to the usual matrix multiplication. The map $x \mapsto Mx = M'x + v, \quad M = \begin{pmatrix} M' & v \\ 0 & 1 \end{pmatrix} \in R(n), x \in \mathbb{Z}^n$ defines an action of $R(n)$ on $\mathbb{Z}^n$. Note that this is also a transitive action of $R(n)$ on the set of all shifts of bases of $\mathbb{Z}^n$.

Let H_X denote the stabilizer of the point 0:

$$H_X = St(0) \simeq A(n); \tag{2.7}$$

let Π be a shift of an $(n-1)$-sublattice of $\mathbb{Z}^n$ and let H_Ξ denote the stabilizer of Π. Assume now that Π is the sublattice $\Pi_0 \subset \mathbb{Z}^n$ spanned by the first $n-1$ base vectors; then

$$H_\Xi = St(\Pi_0) = St\langle v_1, v_2, \ldots, v_{n-1}\rangle \simeq R(n-1) \times \{\pm 1\}. \tag{2.8}$$

Lemma 2.2 *The spaces $X = G/H_X$ and $\Xi = G/H_\Xi$ defined by Eq. (2.6), (2.7) and (2.8) satisfy conditions (i), (ii) and (iii).*

Proof. Conditions (i) and (iii) are obvious. Let us check condition (ii). We need to prove that if $h_X \in H_X$ is such that for any $h_\Xi \in H_\Xi$ there exist $g_X \in H_X$ and $g_\Xi \in H_\Xi$ satisfying

$$h_X h_\Xi = g_\Xi g_x \tag{2.9}$$

then $h_X \in H_\Xi$. Applying the right and the left hand sides of (2.9) to the origin, we get

$$h_X\,(h_\Xi\, 0) = g_\Xi\,(g_X\, 0)\,. \tag{2.10}$$

Since $g_X 0 = 0$, the right hand side of (2.10) belongs to Π_0. It is clear that H_Ξ acts transitively on Π_0, so $h_\Xi 0$ runs through Π_0 as h_Ξ runs through H_Ξ. Thus, $h_X(p) \in \Pi_0$ for any $p \in \Pi_0$, i.e. $h_X \in H_\Xi$. The dual statement of (ii) is proved similarly. $\triangle$

Recall that by $L^{[m]}$ we denote the set of all primitive m-sublattices of a lattice L and denote by $\overline{L^{[m]}}$ *the set of all shifts of primitive m-sublattices of L by vectors of L.*

The intersection of H_X with H_Ξ is

$$K := H_X \cap H_\Xi = \begin{pmatrix} A(n-1) & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \simeq A(n-1) \times \{\pm 1\}.$$

The factorspace $X = G/H_X$ can be identified with $\mathbb{Z}^n$, and the factorspace $\Xi = G/H_\Xi$ can be identified with the set $\overline{(\mathbb{Z}^n)^{[n-1]}}$ of all integer shifts of primitive $(n-1)$-sublattices in $\mathbb{Z}^n$. It can be checked that with our choice of Π_0 a point $x \in X$ is incident with a shift of sublattice $\xi \in \Xi$ iff $x \in \xi$.

Note. A different choice of Π_0 in (2.8) will give a different incidence relation; for example, when H_Ξ stabilizes

$$\Pi = \Pi_\lambda = \langle v_1, v_2, \ldots, v_{n-1} \rangle + \lambda v_n, \ \lambda \in \mathbb{Z},$$

we get the incidence relation $x \overset{\lambda}{\bowtie} \xi \Leftrightarrow \mathrm{ind}_{\mathbb{Z}^n}(x, \xi) = \lambda$.

The Plancherel formula (2.4) gives

$$\sum_{x \in \mathbb{Z}^n} f(x) \check{\phi}(x) = \sum_{\xi \in \overline{\left(\mathbb{Z}^n\right)^{[n-1]}}} \hat{f}(\xi) \phi(\xi) \tag{2.11}$$

for any $f : L \to \mathbb{C}$ and $\phi : L^{[n-1]} \to \mathbb{C}$ such that both series converge absolutely.

Theorem 2.1 *For any lattice L of rank n*

$$\Theta_L(q) \cdot T_L^{n-1}(p) = \sum_{\xi \in \overline{L^{[n-1]}}} p^{\|\xi\|} \Theta_\xi(q). \tag{2.12}$$

PROOF. Let us apply Eq. (2.11) to $f(x) = q^{\|x\|}$ and $\phi(\xi) = p^{\|\xi\|}$, where the norms $\|\cdot\|$ are given by the positive quadratic form associated to L. By the definitions,

$$\begin{aligned}\Theta_L(q) \cdot T_L^{n-1}(p) &= \left(\sum_{x\in\mathbb{Z}^n} q^{\|x\|}\right)\left(\sum_{\xi\in(\mathbb{Z}^n)^{[n-1]}} p^{\|\xi\|}\right) = \\ &= \sum_{x\in\mathbb{Z}^n}\left(q^{\|x\|}\sum_{\xi\in(\mathbb{Z}^n)^{[n-1]}} p^{\|\xi\|}\right).\end{aligned}$$

Shift a sublattice $\xi \in L^{[n-1]}$ by a vector x. We can replace now a summation over all $\xi \in L^{[n-1]}$ by a summation over all $\xi_x = \xi + x \in \overline{L^{[n-1]}}$, $\|\xi_x\| = \|\xi\|$ and apply then the Plancherel formula (2.11):

$$\begin{aligned}&\sum_{x\in\mathbb{Z}^n}\left(q^{\|x\|}\sum_{\xi\in\Xi} p^{\|\xi\|}\right) = \sum_{x\in\mathbb{Z}^n} q^{\|x\|}\left(\sum_{\xi_x\in\Xi:\ x\in\xi_x} p^{\|\xi_x\|}\right) = \\ &= \sum_{x\in\mathbb{Z}^n}\sum_{\xi\rhd\lhd x} q^{\|x\|}p^{\|\xi\|} \overset{(2.11)}{=} \sum_{\xi\in\Xi}\sum_{x\rhd\lhd\xi} q^{\|x\|}p^{\|\xi\|} = \sum_{\xi\in\Xi} p^{\|\xi\|}\Theta_\xi(q).\end{aligned}$$

$\triangle$

Thus, we proved that the product of the Θ-function of a lattice with the T^{n-1}-function equals the weighted sum of shifted sublattice Θ-functions.

Applying the duality relations (1.7), (1.14) we get the following corollary

Corollary 2.1 *For any lattice $L \subset \mathbb{R}^n$ holds*

$$\Theta_L(q) \cdot T^1_{L^\perp}(p^{\det L}) = \sum_{\xi\in\overline{L^{[n-1]}}} p^{\|\xi\|}\Theta_\xi(q). \tag{2.13}$$

2.3 Weight/Multiplicity Duality for Projective Multisets

Nogin [Nog3] proposed the following construction of new linear codes from the known ones.

The projective multiset Y_C of a linear $[n,k,d]_q$-code C (see §1.1.2) can be considered as a multiset of n hyperplanes with multiplicities $\nu(H)$ in the projectivization $\mathbb{P}C$ of the code C. Assign multiplicity zero to any hyperplane not in the multiset. The weight of a 1-subcode $c \in \mathbb{P}C$ equals

$$\mathrm{wt}(c) = \sum_{H \not\supset c} \nu(H). \tag{2.14}$$

A natural problem is to invert relations (2.14), i.e. given the set of weights $\{\mathrm{wt}(c) | c \in \mathbb{P}C\}$ one wants to reconstruct the multiplicities $\{\nu(H)\}$. Nogin proved the following inversion formula for (2.14):

$$\nu(H) = \frac{\sum_{c \in \mathbb{P}C} \mathrm{wt}(c) - q \sum_{c \in H} \mathrm{wt}(c)}{q^{k-1}}. \tag{2.15}$$

Now, for any given function $\widetilde{\mathrm{wt}} : \mathbb{P}^{k-1} \to \mathbb{Z}$ one can reconstruct a set of "multiplicities". These "multiplicities" do not necessarily correspond to an actual set of multiplicities of a projective multiset. However, they can be corrected to an actual set of multiplicities by a linear transform (see [Nog3]). Nogin used this inversion to construct new long linear codes: one can take a "small" code C_1, construct from it in a certain way a set of "weights", apply Eq. (2.15) to obtain a set of "multiplicities" and correct them to a set of multiplicities of a projective multiset. The code C_2 corresponding to this multiset is much longer than C_1 and its spectrum is determined by the spectrum of C_1.

This construction has a natural interpretation via a Radon transform. Consider the group $G := PGL(k-1, \mathbb{F}_q)$ with the standard action on $\mathbb{P}C$ and subgroups $H_X := St(P)$ and $H_\Xi := St(H)$, where P is an arbitrary but fixed point in $\mathbb{P}C$, and H is a hyperplane containing P. The conditions (i)–(iii) (see page 21) can be easily checked, so the pair $(X = G/H_X, \Xi = G/H_\Xi)$ is a pair of homogeneous spaces in duality. The incidence relation is

$$x \bowtie \xi \Leftrightarrow x \in \xi,$$

the Radon transform and the dual are given by

$$\hat{f}(\xi) = \sum_{x \in \xi} f(x), \tag{2.16}$$

$$\check{\phi}(x) = \sum_{\xi \ni x} \phi(\xi). \tag{2.17}$$

These transform can be inverted in the following way. Consider a function $f : X \to \mathbb{R}$. We want to express f via its Radon transform $\hat{f}$. Let p_m denote the number of points in an m-dimensional projective space over $\mathbb{F}_q$, $p_m = \frac{q^{m+1}-1}{q-1}$. Let us introduce the following functionals $s(\phi)$, $\sigma(f)$ and operators $D\phi$, Δf defined on the function spaces $\{\phi : \Xi \to \mathbb{C}\}$ $\{f : X \to \mathbb{C}\}$ by

$$s(\phi) := \sum_{\xi \in \Xi} \phi(\xi) \qquad \sigma(f) := \sum_{x \in X} f(x)$$
$$D\phi(\xi) := \phi(\xi) - \frac{p_{m-2}}{p_{m-1}^2} s(\phi) \qquad \Delta f(x) := f(x) - \frac{p_{m-2}}{p_{m-1}^2} \sigma(f).$$

Theorem 2.2 *The Radon transform (2.16) and the dual Radon transform (2.17) are inverted by the formulas*

$$f(x) = \frac{1}{q^{m-1}} \left(D\hat{f}\right)^{\vee}(x) \qquad \phi(\xi) = \frac{1}{q^{m-1}} \left(\Delta\check{\phi}\right)^{\wedge}(x). \tag{2.18}$$

Proof. It is sufficient to prove Eq. (2.18) for the indicator function of the one-point set $\{P\}$, i.e. for the function

$$I_P(x) = \begin{cases} 1, & x = P \\ 0, & x \neq P \end{cases}$$

The result can be then extended to arbitrary functions by the linearity of the Radon transform. For $I_P(x)$ it is clear that

$$\widehat{I_P}(\xi) = \begin{cases} 1, & \xi \ni P \\ 0, & \xi \not\ni P \end{cases};$$

$s(\widehat{I_P}) = p_{m-1}$ so

$$D\widehat{I_P}(\xi) = \begin{cases} 1, & \xi \ni P \\ 0, & \xi \not\ni P \end{cases}.$$

$\triangle$

Note that Eq. (2.14) can be rewritten as

$$\mathrm{wt}(c) = n - \check{\nu}(c).$$

Using the inversion formula (2.18) for the function $\nu(c)$ we get Eq. (2.15).

2.4 Generalized Plotkin Bound

In this section, we prove a lower bound for generalized Hamming weights (see [TV2] and [HKYL].) We show that this bound can be regarded as a corollary of the Plancherel formula.

We use the following lemma, which is due to van der Geer and van der Vlugt:

Lemma 2.3 ([GV1]) *For any r-subcode D holds*

$$\mathrm{wt}(D) = \frac{1}{q^r - q^{r-1}} \sum_{c \in D} \mathrm{wt}(c). \tag{2.19}$$

Let the incidence relation between r-subcodes of a code C be given by

$$c \bowtie D \Leftrightarrow c \in D,$$

where $c \in C$ is a codeword and $D \subset C$ is an r-subcode.

Theorem 2.3 *For any linear $[n, k, d]_q$-code C and for any $r = 1, \ldots, k$ the following holds*

$$\sum_{D \in C^{[r]}} \mathrm{wt}(D) = \frac{nq^{k-r}}{q^k - 1} \begin{bmatrix} k \\ r \end{bmatrix}_q .$$

Proof. We use twice Eq. (2.19) (lemma 2.3) and once Eq. (2.4) (lemma 2.1):

$$\begin{aligned}
\sum_{D \in C^{[r]}} \mathrm{wt}(D) &\overset{(2.19)}{=} \frac{1}{q^r - q^{r-1}} \sum_{D \in C^{[r]}} \sum_{c \bowtie D} \mathrm{wt}(c) \overset{(2.4)}{=} \frac{1}{q^r - q^{r-1}} \sum_{c \in C} \sum_{D \bowtie c} \mathrm{wt}(c) = \\
&= \frac{1}{q^r - q^{r-1}} \sum_{c \in C} \#\{D \in C^{[r]} | c \in D\} \, \mathrm{wt}(c) = \\
&= \frac{1}{q^r - q^{r-1}} \begin{bmatrix} k \\ r \end{bmatrix}_q \sum_{c \in C} \mathrm{wt}(c) \overset{(2.19)}{=} \\
&\overset{(2.19)}{=} \frac{1}{q^r - q^{r-1}} \begin{bmatrix} k \\ r \end{bmatrix}_q (q^k - q^{k-1}) \, \mathrm{wt}(C) = \\
&= \frac{nq^{k-r}}{q^k - 1} \begin{bmatrix} k \\ r \end{bmatrix}_q .
\end{aligned}$$

$\triangle$

An easy corollary of this theorem is the following bound on d_r (this is Theorem 1.1 from [TV2].)

Corollary 2.2 ([TV2]) *The r-h generalized Hamming weight $d_r(C)$ of an $[n,k,d]_q$-code C satisfies*

$$d_r(C) \le \frac{n(q^r-1)q^{k-r}}{q^k-1}.$$

2.5 Generalized Minkowski–Hlawka Theorem

This theorem is a nonconstructive lower bound on $\gamma_{n,m}$. It was first proved by Thunder [Thu1] in greater generality (see §1.3.1.) We give a shorter and simpler proof of this theorem based on the Plancherel formula.

Let $Z(j) = \zeta(j)\Gamma(j/2)/\pi^{j/2}$, where $\zeta(j)$ is the Riemann ζ-function $\zeta(j) = \sum_{n=1}^{\infty} n^{-j}$.

Theorem 2.4 (Generalized Minkowski–Hlawka Theorem) *For any $m < n$ there exists a lattice $L \subset \mathbb{R}^n$ with*

$$\gamma_m(L) \ge \left(n \frac{\prod_{j=n-m+1}^{n} Z(j)}{\prod_{j=2}^{m} Z(j)} \right)^{2/n}. \tag{2.20}$$

For $m = 1$ we get the classical Minkowski–Hlawka theorem. The idea of our proof is the same as in Siegel's proof of Minkowsi-Hlawka theorem [Sie]. The main ingredient of that proof is Siegel mean value theorem, which states that for a compactly supported continous function $\phi : \mathbb{R}^n \to \mathbb{R}$,

$$\int_{\mathbb{R}^n} \phi(x)\,dx = \zeta(n) \int_{\mathcal{L}_n} \sum_{z \in P} \phi(gz)\; dg, \tag{2.21}$$

where $\mathcal{L}_n$ is the factorspace $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ with the Haar measure dg scaled so that $\mathrm{vol}(SL_n(\mathbb{R})/SL_n(\mathbb{Z})) = 1$ and P is the set of primitive

integer vectors in $\mathbb{R}^n$. We shall prove a generalization of this mean value theorem is a corollary of the Plancherel formula for the pair of homogenous spaces in duality $(\mathcal{L}_n, \mathcal{R}_m)$, where $\mathcal{R}_m$ is the space of all m-lattices in $\mathbb{R}^n$, and the incidence relation is

$$\bowtie M \Leftrightarrow \text{“}M \text{ is a primitive sublattice of } L\text{”}. \tag{2.22}$$

The standard way to represent $\mathcal{L}_n$ as a homogenous space is to identify it with $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$. However, it is more convenient for us to identify it with the factorspace of real unitary matrices by the integer unitary matrices. Let $U_n(\mathbb{R}) \simeq SL_n(\mathbb{R}) \times \{\pm 1\}$ be the subgroup of $GL_n(\mathbb{R})$ consisting of all matrices A with $|\det A| = 1$ and let $U_n(\mathbb{Z}) \simeq SL_n(\mathbb{Z}) \times \{\pm 1\}$ be the subgroup of all integer matrices in $U_n(\mathbb{R})$. It is clear that

$$\mathcal{L}_n = U_n(\mathbb{R})/U_n(\mathbb{Z}) \tag{2.23}$$

and that $U_n(\mathbb{R})$ acts transitively on the set $\mathcal{R}_m$. Thus,

$$\mathcal{R}_m = U_n(\mathbb{R})/St(M_0), \tag{2.24}$$

where M_0 is any fixed m-lattice in $\mathbb{R}^n$. In coordinates, when M_0 is spanned by the first m basis vectors we have

$$St(M_0) = \begin{pmatrix} U_n(\mathbb{Z}) & * \\ 0 & U_{n-m}(\mathbb{R}) \end{pmatrix}.$$

In the sequel, the integrations over $\mathcal{L}_n$ and $\mathcal{R}_m$ are assumed to be with the respect to the measures induced by the Haar measure on $U_n(\mathbb{R})$ scaled so that $\operatorname{vol} \mathcal{L}_n = 1$. One can check that the pair of spaces $(\mathcal{L}_n, \mathcal{R}_m)$ is a pair of homogenous spaces of duality in the sense of conditions (i)–(iii) on page 21with the incidence relation (2.22).

Theorem 2.5 (Generalized Siegel mean value theorem) *Let $\phi(\cdot)$ be a compactly supported function on $\mathcal{R}_m$. Then*

$$C \int_{\mathcal{L}_n} \sum_{M \bowtie L} \phi(M)\, dL = \int_{\mathcal{R}_m} \phi(M)\, dM, \tag{2.25}$$

where

$$C = \frac{\pi^{n/2}}{\Gamma(n/2+1)} n^m \left(\frac{\prod_{j=n-m+1}^{n} Z(j)}{\prod_{j=2}^{m} Z(j)} \right)^m.$$

Note. For $m = 1$ we have $C = 2\zeta(n)$ and not $\zeta(n)$ as in in (2.21) because our space $\mathcal{R}_1$ does not coincide with $\mathbb{R}^n$ but is in fact the factor $\mathbb{R}^n/\{\pm 1\}$.

PROOF. We should simply use the Plancherel formula (2.4) for the pair $(\mathcal{L}_n, \mathcal{R}_m)$ of homogenous spaces in duality defined by (2.23) and (2.24). It is easy to check that $M \in \mathcal{R}_m$ is incident to $L \in \mathcal{L}_n$ iff M is a primitive m-sublattice of L.

Take $\phi(\cdot)$ as the function on $\mathcal{R}_m$ and $f(L) \equiv 1$ as the function on $\mathcal{L}_n$. We have

$$\int_{\mathcal{L}_n} f(L)\widehat{\phi}(L)\, dL = \int_{\mathcal{R}_m} \phi(M)\check{f}(M)\, dM.$$

Substituting $f(L) \equiv 1$ and using the definitions we get

$$\int_{\mathcal{L}_n} \sum_{M \bowtie L} \phi(M)\, dL = \int_{\mathcal{R}_m} \mathrm{vol}(\check{M})\phi(M)\, dM.$$

It is clear that $\mathrm{vol}(\check{M})$ is independent of M. In fact, it equals the volume of the space of all n-lattices with a fixed m-sublattice. Define the constant C by $1/C = \mathrm{vol}(\check{M})$. Thus

$$C \int_{\mathcal{L}_n} \sum_{M \bowtie L} \phi(M)\, dL = \int_{\mathcal{R}_m} \phi(M)\, dM.$$

Similarly to Siegel's argument, one computes now the value of C via a rather technical inductive calculation in the space of matrices. $\triangle$

Theorem 2.4 follows now by the standard argument: let $B_R \subset \mathcal{R}_m$ be the ball $B_R = \{M \,|\, \det M < R^2\}$ of radius R and let $\phi(M)$ be the indicator function of this ball. The right hand side of Eq. (2.25) equals $\mathrm{vol}(B_R)$. So if R is such that $\mathrm{vol}\, B_R < C$, then $\sum_{M \bowtie L} \phi(M) < 1$ for at least one $L \in \mathcal{L}_n$. Thus, any m-sublattice of L is outside B_R, so

$$\gamma_m(L) > R^2.$$

This completes the proof of Theorem 2.4. $\triangle$

The bound of this theorem is asymptotically good, that is, it differs from the lower bound (1.19) just by a multiplicative constant.

Note that a similar bound for generalized Hamming weights of codes (generalized Gilbert–Varshamov bound, see [TV2]) can be proved similarly, by using the Placherel formula for the pair of homogenous spaces in duality

$$([n,k]_q - \text{codes}, [n,r]_q - \text{codes}).$$

Chapter 3

Projective codes and bounds on the second Hermite parameter

Generalized Hermite parameters measure the minimal "size" of a sublattice of the given lattice. The *Grassmann variety* $\mathcal{G}(n,m)$ is the real analogue of the space of all sublattices and the packings in $\mathcal{G}(n,m)$ are in some instances similar to the sets of sublattices. In this chapter, we deduce upper bounds on the second generalized Hermite parameter of lattices with at least four minimal vectors from known bounds on packings in projective spaces and Grassmannians.

3.1 Grassmannians as metric spaces

Consider the set of all m-dimensional subspaces in an n-dimensional real vector space. The *Plücker coordinates* induce on this set the structure of a smooth compact Riemann manifold of dimension $m(n-m)$ (see, for example [GH]). This manifold is called a *Grassmann manifold* or a *Grassmannian* and is denoted by $\mathcal{G}(n,m)$. Note that $\mathcal{G}(n,m)$ is a homogeneous space isomorphic, for example, to $O(n)/O(k)\times O(n-k)$.

Although the Grassmannians are being studied for more than a century, the problem of packings in Grassmannians did not attract much attention (except for some particular cases) before the paper [CHS] by

Conway, Hardy, and Sloane. Our exposition of the theory of packings in Grassmannians is based on this paper.

Fix a scalar product in $\mathbb{R}^n$. To any $R \in \mathcal{G}(n,m)$ corresponds the set $\operatorname{Ann} R$ of all vectors orthogonal to R. This gives a bijection between $\mathcal{G}(n,m)$ and $\mathcal{G}(n-m,m)$. This bijection is also an isomorphism of Riemann manifilds. Thus, without loss of generality we may assume that $m \leq n/2$. In this chapter, E_n denotes the identity $n \times n$-matrix.

A special case ($m = 1$) of packings in Grassmannians are the packings in a projective space $\mathbb{P}^n$ with the metric $d(l_1, l_2) = |\sin(l_1 l_2)|$, where $l_1, l_2 \in \mathbb{P}^n$ are two lines and $\sin(l_1, l_2)$ is the sinus of the angle between them. Tthis metric is a special case of the metric on a Grassmannian which will be introduced below. Kabatiansky and Levenstein [KL] noticed that this is equivalent to an association scheme (see [Del]) on the unit sphere S^{n-1} with the "distance" $d(x,y) = |(x,y)|$. They also prove several linear programming bounds on the maximum cardinality $M(n,s)$ of packings in $\mathbb{P}^n$ with the given minimum distance s. We shall use these bounds in the sequel.

Let us introduce now a metric in $\mathcal{G}(n,m)$. Fix a scalar product in $\mathbb{R}^n$ and consider two linear subspaces R and S of dimension m in $\mathbb{R}^n$. We can associate to R and S the set of *principal angles* $(\theta_1, \theta_2, \ldots, \theta_m)$ in the following way. Choose unit vectors $u_1 \in R$ and $v_1 \in S$ so that the angle between them is the minimal possible. Inductively, choose unit vectors $u_j \in R$ and $v_j \in S$, $j = 2, \ldots, m$, such that

$$(u_j, u_i) = (v_j, v_i) = (u_j, v_i) = (u_i, v_j) = 0$$

for all $i = 1, \ldots, j-1$ and the angle between u_j is v_j the minimal possible. The vectors u_j and v_j, $j = 1, \ldots, m$, are called *principal vectors* for the pair (R, S). The angles $\theta_i := \arccos(u_i, v_i)$, $i = 1, \ldots, m$, are called *the principal angles* between R and S. The principal angles do not depend on the choice of principal vectors; the set of principal angles is an $O(n)$-invariant of the pair (R, S).

Since $\mathcal{G}(n,m)$ has a natural structure of a Riemann manifold, one of the ways to introduce a metric on the set $\mathcal{G}(n,m)$ is to take *the geodesic distance* between the points of the manifold. One can prove ([Won]), that the geodesic distance $d_g(R,S)$ can be expressed via the principal

angles in the following way:

$$d_g(R,S) = \sqrt{\theta_1^2 + \theta_2^2 + \ldots + \theta_n^2}.$$

A drawback of the geodesic distance is that its square is not an everywhere differentiable function on $\mathcal{G}(n,m) \times \mathcal{G}(n,m)$.

One can introduce another distance on $\mathcal{G}(n,m)$. Define the *chordal distance* $d_c(R,S)$ between linear subspaces R and S by

$$d_c(R,S) := \sqrt{\sin^2\theta_1 + \sin^2\theta_2 + \ldots + \sin^2\theta_m}. \tag{3.1}$$

the square of the chordal distance is a smooth function on $\mathcal{G}(n,m)$. The use of the word "chordal" will be clear after we explain the connection between this distance and the projection operators.

Associate to each m-plane R the operator of the orthogonal projection P_R onto this plane. In coordinates, given m orthogonal unit vectors $w_1, \ldots, w_m$ that span R define *the generator matrix* A_R by $A_R := (w_1, \ldots, w_m)$. Then A_R is an $n \times m$-matrix with orthogonal columns. The symmetric $n \times n$-matrix $P_R := {}^tA_R A_R$ is then the matrix of the orthogonal projection onto R.

For any pair (R,S) of m-planes there exists an orthonormal basis in $\mathbb{R}^n$ such that the generator matrices are

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

$$A_S = \begin{pmatrix} \cos\theta_1 & 0 & \ldots & 0 & \sin\theta_1 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \cos\theta_2 & \ldots & 0 & 0 & \sin\theta_2 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & \cos\theta_m & 0 & 0 & 0 & \sin\theta_m & 0 & \ldots & 0 \end{pmatrix}. \tag{3.2}$$

In particular, from (3.2) it follows that $\operatorname{trace} P_R = m$. Thus, the correspondence $R \mapsto P_R$ gives an embedding of the topological space $\mathcal{G}(n,m)$ into $\mathbb{R}^D$, $\quad D = \binom{n+1}{2} - 1$. Let $\|\cdot\|$ denote the L_2-norm in a matrix space:

$$\|\,(M_{ij})\,\| := \sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} M_{ij}^2} = \sqrt{\operatorname{trace} {}^tM M}. \tag{3.3}$$

Substituting into Eq. (3.3) the matrices (3.2) and the definition (3.1) we get

$$\begin{aligned} d_c^2(R,S) &= n - \left(\cos^2\theta_1 + \ldots + \cos^2\theta_m\right) = \\ &= n - \operatorname{trace} A_R{}^t A_R A_S{}^t A_S = \frac{1}{2}\|P_R - P_S\|^2. \end{aligned}$$

Let us consider now the map

$$R \mapsto \frac{1}{\sqrt{2}}\overline{P_R}, \qquad \overline{P_R} := P_R - (n/m)E_n. \tag{3.4}$$

Since $\|\overline{P_R}\|^2 = m(n-m)/n$, the correspondence (3.4) is an isometric embedding of the metric space $\mathcal{G}(n,m)$ with the chordal distance into a sphere in $\mathbb{R}^D$ of radius $\sqrt{m(n-m)/2n}$. Thus, we proved the following result (this is Theorem 5.1 from [CHS].)

Theorem 3.1 ([CHS]) *The map (3.4) isometrically embeds $\mathcal{G}(n,m)$ with the chordal distance (3.1) into a sphere of radius $\sqrt{m(n-m)/2n}$ in $\mathbb{R}^D$, $D = \binom{n+1}{2} - 1$.*

This construction allows to apply many known upper bounds on spherical codes to the packings in Grassmannians. Thus, applying Rankin bounds [Ran2], [SPLAG] on the cardinality $A(n,\phi)$ of a spherical code with the angular separation ϕ

$$\begin{aligned} A(n,\phi) &= n+1, \qquad \text{for } \phi \in (\arccos(-\frac{1}{n}), \frac{\pi}{2}]; \\ A(n,\frac{\pi}{2}) &= 2n \end{aligned}$$

one gets the following two lemmas.

Lemma 3.1 ([CHS]) *For a packing of N planes in $\mathcal{G}(n,m)$,*

$$d_c^2 \le \frac{m(n-m)}{n}\frac{N}{N-1}\,. \tag{3.5}$$

Equality requires $N \le D+1 = \binom{n+1}{2}$, and occurs if and only if the N points in $\mathbb{R}^D$ corresponding to the planes form a regular equatorial simplex.

Lemma 3.2 ([CHS]) *For* $N \geq \binom{n+1}{2}$,

$$d_c^2 \leq \frac{m(n-m)}{n}\,. \tag{3.6}$$

Equality requires $N \leq 2D = (n-1)(n+2)$, *and occurs if the* N *points in* $\mathbb{R}^D$ *form a subset of the* $2D$ *vertices of a regular orthoplex. If* $N = 2D$ *this condition is also necessary.*

Only special cases of these two lemmas ($m = 1$) will be used to derive bounds on the second generalized Hermite parameter. Note that bound (3.5) for $m = 1$ coincides with a linear programming bound with a linear polynomial on a packing in $\mathbb{P}^n$ from [KL]. Among other bounds, Kabatiansky and Levenstein [KL] proved a linear programming bound with a quadratic polynomial, which is equivalent to

$$d_c^2 \leq \frac{n-1}{n+2}\frac{N}{N-n}, \tag{3.7}$$

and a bound equivalent to

$$d_c^2 \leq 1 - \sqrt[k]{\frac{Ng(k,n)-1}{N-1}}, \qquad \text{where } k \text{ is any natural number,} \tag{3.8}$$

and

$$g(k,n) := \frac{\Gamma(k-\frac{1}{2}+1)}{\Gamma(k+n/2)}\frac{\Gamma(n/2)}{\Gamma(\frac{1}{2})} = \frac{1}{2^k}\frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2k-1)}{(\frac{n}{2}+k-1)(\frac{n}{2}+k-2)\ldots(\frac{n}{2}-1)}.$$

3.2 Bounds on the second generalized Hermite parameter

We give a construction, which for any upper bound on spherical codes or packings in $\mathcal{G}(n,1)$ delivers an upper bound on $\gamma_2(L)/\gamma_1^2(L)$ that depends on the kissing number $\tau(L)$ and the dimension n. The basic idea is the following: if a lattice L has a big $\gamma_2(L)$, and L also has linearly independent minimal vectors (i.e. $\tau(L) > 2$), then the minimal vectors of L form an antipodal spherical code of the cardinality $\tau(L)$

with a big angular separation; from such a code we get a packing in $\mathcal{G}(n,1)$ of cardinality and a big minimum distance; now we can either apply to this packing an upper bound, or use Theorem 3.1 to get a spherical code of cardinality $\tau(L)/2$ and with the angular separation ϕ lower bounded, as we shall see, by

$$\sin^2\frac{\phi}{2} \geq \frac{\gamma_2(L)}{2\gamma_1(L)^2}\frac{n}{n-1},$$

and apply then upper bounds to this spherical code.

Let us prove first a corollary of lemmas 3.1 and 3.2.

Theorem 3.2 *Let L be a lattice in $\mathbb{R}^n$ with the kissing number $\tau(L) > 2$; then*

$$\frac{\gamma_2(L)}{\gamma_1(L)^2} \leq \frac{n-1}{n}\frac{\tau(L)}{\tau(L)-2}; \tag{3.9}$$

if $\tau(L) > n(n+1)$, then

$$\frac{\gamma_2(L)}{\gamma_1(L)^2} \leq \frac{n-1}{n}. \tag{3.10}$$

Proof. Without loss of generality we may assume that $r(L) = 1$. Take linearly independent minimal vectors $v_1 \in L$ and $v_2 \in L$. Let $\theta(v_1, v_2)$ denote the angle between v_1 and v_2. It is clear that

$$\mathrm{vol}_2(L) \leq \sin\theta(v_1,v_2)|v_1|\,|v_2| = \sin\theta(v_1,v_2).$$

Let θ be the minimal angle between any two distinct minimal vectors. The set of all minimal vectors of L is a spherical code $\mathcal{S}$ of cardinality $\tau(L)$ with the angular separation θ. This code is antipodal, i.e. with any vector v the code contains also $-v$. The set of lines $\mathbb{R}v$ forms a packing in $\mathcal{G}(n,1)$ with the minimum distance $\sin\theta$. Applying lemmas 3.1 and 3.2 to this packing we get Eqs. 3.9 and 3.10.

Note that we could apply various bounds on spherical code to the code $\mathcal{S}$, but since antipodal codes are worse than general spherical codes, the results would be weaker.

△

Note. There exist many upper bounds on spherical codes that lead to bounds on packings in Grassmannians (see, for example, [BDB] and [Lev]), but they do not yield any significant improvement over the results of Theorem 3.2.

Similarly to the proof of Theorem 3.2 we can use bounds on packings in $\mathbb{P}^n$ by Kabatiansky and Levenstein to get the following theorem.

Theorem 3.3 *Let L be a lattice in $\mathbb{R}^n$ with the kissing number $\tau(L) > 2n$; then*

$$\frac{\gamma_2(L)}{\gamma_1(L)^2} \le \frac{n-1}{n+2}\frac{\tau(L)}{\tau(L)-2n}; \tag{3.11}$$

and for any natural k

$$\frac{\gamma_2(L)}{\gamma_1(L)^2} \le 1 - \sqrt[k]{\frac{\tau(L)g(k,n)-2}{\tau(L)-2}}, \tag{3.12}$$

where

$$g(k,n) := \frac{\Gamma(k-\frac{1}{2}+1)}{\Gamma(k+n/2)}\frac{\Gamma(n/2)}{\Gamma(\frac{1}{2})} = \frac{1}{2^k}\frac{1\cdot 3\cdot 5\cdot \ldots \cdot (2k-1)}{(\frac{n}{2}+k-1)(\frac{n}{2}+k-2)\ldots(\frac{n}{2}-1)}.$$

Bound (3.11) is better then both bounds of Theorem 3.2 if and only if $\tau(L) > n(n+2)$.

3.3 Examples

In this section, we apply Theorems 3.2 and 3.3 to several classical families of lattices. We use the same notation and the same versions of lattices as [SPLAG]. The parameters of lattices are from [NS].

Cubic lattice $\mathbb{Z}^n$. It is clear that $\gamma_m(\mathbb{Z}^n) = 1$, $m = 1, \ldots, n$, and $\tau(\mathbb{Z}^n) = 2n$. Thus inequality (3.9) is an equality for these lattices.

Root lattice $\mathbf{A}_n$. We have $\det \mathbf{A}_n = n+1$, $r^2 = 2$, $\tau = n(n+1)$. Since $\mathbf{A}_n$ contains a hexagonal 2-sublattice generated by minimal vectors, we have

$$\gamma_2(\mathbf{A}_n) = \frac{3}{(n+1)^{2/n}},$$

while (3.9) implies that $\gamma_2(\mathbf{A}_n) \le \frac{4}{3}\frac{n+1}{n+2}\frac{3}{(n+1)^{2/n}}$.

Dual root lattice $\mathbf{A}_n^*$. We have $\det(\mathbf{A}_n^*) = \frac{1}{n+1}$, $r^2 = \frac{n}{n+1}$, $\tau = 2n+2$ ($n \ge 2$) and $\gamma_1(\mathbf{A}_n^*) = \frac{n}{(n+1)^{(n-1)/n}}$. Thus,

$$\gamma_2(\mathbf{A}_n^*) \le (n-1)(n+1)^{\frac{2}{n}-1}.$$

Combined with Eq. (1.17) this gives

$$\frac{3}{4}n^2(n+1)^{\frac{2}{n}-2} \le \gamma_2(\mathbf{A}_n^*) \le ((n-1)(n+1))\,(n+1)^{\frac{2}{n}-2}. \qquad (3.13)$$

From the duality (1.7) it follows that $\gamma_{n-2}(\mathbf{A}_n)$ also satisfies inequalities (3.13).

Root lattice $\mathbf{D}_n$. We have $\det(\mathbf{D}_n) = 4$, $r^2 = 2$, $\tau = 2n(n+1) > n(n+1)$, and $\gamma_1(\mathbf{D}_n) = 2^{(n-2)/n}$. This lattice has a hexagonal 2-sublattice generated by minimal vectors, so $\gamma_2(\mathbf{D}_n) = 3 \cdot 2^{-4/n}$, while Eq. (3.11) implies

$$\gamma_2(\mathbf{D}_n) \le 4\frac{n-1}{n}\frac{n+1}{n+2}2^{-4/n}.$$

Dual root lattice $\mathbf{D}_n^*$. We have $\det(\mathbf{D}_n^*) = 1/4$, $r^2 = 1$, $\tau = 2n$ ($n \ge 5$) and $\gamma_1(\mathbf{D}_n^*) = 4^{1/n}$. Thus,

$$\gamma_2(\mathbf{D}_n^*) \le 4^{2/n}.$$

Combining this with bound (1.17) we get

$$\frac{3}{4}4^{2/n} \le \gamma_2(\mathbf{D}_n^*) \le 4^{2/n}. \qquad (3.14)$$

From the duality (1.7) it follows that $\gamma_{n-2}(\mathbf{D}_n)$ also satisfies inequalities (3.14).

The exact values of $\gamma_2(\mathbf{D}_n^*)$, $\gamma_2(\mathbf{A}_n^*)$, $\gamma_{n-2}(\mathbf{A}_n)$ and $\gamma_{n-2}(\mathbf{D}_n)$ are unknown to the author. Inequalities (3.13) and (3.14) give lower and upper bounds on them; the ration of the upper bound to the lower is in both cases slightly less than $\frac{4}{3}$.

Laminated lattice Λ_n. It is clear that $\gamma_m(\Lambda_n) = \gamma_1(\Lambda_n)/\gamma_m^m$, $m = 1, \dots, 8$. For example, for Λ_{40} we get $\gamma_2(\Lambda_{40}) = 3 \cdot 2^{14/5}$, while $\tau = 531120$ (see [NS]) is large enough to use (3.10), so $\gamma_2(\Lambda_{40}) \le \frac{13}{10} \cdot 3 \cdot 2^{14/5}$. Since $\tau > n(n+2)$,the bound (3.11) is better and gives $\gamma_2(\Lambda_{40}) \le \frac{39}{42} \cdot \frac{531120}{531040} \cdot 2^{24/5} \approx 1.238281754\ldots \cdot 3 \cdot 2^{14/5}$.

Chapter 4

Number of Points on Algebraic Sets

In this chapter, we prove two upper bounds on the number of points on algebraic sets over finite fields. We give also several conjectures about more general bounds of this kind. As a corollary, we obtain some results about generalized Hamming weights of q-ary projective Reed–Muller codes.

4.1 Introduction

Consider a system of polynomial equations

$$\begin{cases} F_1(x_0 : x_1 : \ldots : x_m) &= 0 \\ F_2(x_0 : x_1 : \ldots : x_m) &= 0 \\ \qquad\qquad \ldots & \\ F_r(x_0 : x_1 : \ldots : x_m) &= 0 \end{cases} \tag{4.1}$$

where F_i are linearly independent homogeneous polynomials in $m+1$ variables over a finite field $\mathbb{F}_q$ with q elements. Suppose all F_i have degree d. The main purpose of this paper is to determine the maximal possible number of solutions of system (4.1) in m-dimensional projective space $\mathbb{P}^m(\mathbb{F}_q)$.

In this chapter, q is fixed, $|X|$ denotes the number of $\mathbb{F}_q$-points of an algebraic set X, $p_m = |\mathbb{P}^m| = \frac{q^{m+1}-1}{q-1}$.

The case of one equation ($r = 1$) was considered a few years ago. M.Tsfasman constructed for each $d \leq q + 1$ a polynomial F of degree d with $dq^{m-1} + p_{m-2}$ zeroes and made a conjecture that this is the maximal possible value. This was proved by J.-P. Serre [Ser] and by Sørensen [Sor1], [Sor2].

Theorem 4.1 *Let $F(x_0 : x_1 : \ldots : x_m)$ be a homogeneous polynomial in $m + 1$ variable with coefficients in $\mathbb{F}_q$ and of degree d. The number of zeroes of $F(x_0 : x_1 : \ldots : x_m)$ in $\mathbb{P}^m(\mathbb{F}_q)$ is less than or equal to $dq^{m-1} + p_{m-2}$.*

Serre used the induction on the dimension m to prove that the number of zeroes of Tsfasman's polynomial F is the maximal possible. F is a reducible polynomial. The zero set X of this polynomial is a union of d hyperplanes passing through one common linear space of codimension 2.

Thus the bound given by Theorem 4.1 is exact for $d \leq q+1$. When $d = q + 1$ the theorem gives the upper bound p_m. For $d \geq q + 1$ there exist polynomials with p_m zeroes.

One can study the same problem from another point of view. Let us consider the Veronese embedding of degree d

$$\mathcal{V}_d : \mathbb{P}^m \to \mathbb{P}^{\binom{d+m}{m}-1}.$$

For $i_0+i_1+\ldots+i_m = d$ denote the homogeneous coordinates in $\mathbb{P}^{\binom{d+m}{m}-1}$ by $(u_{i_0 i_1 \ldots i_m})$, and let $x_0, \ldots, x_m$ be the homogeneous coordinates in $\mathbb{P}^m$. The Veronese embedding is the map given by $u_{i_0 i_1 \ldots i_m} = x_0^{i_0} x_1^{i_1} \ldots x_m^{i_m}$. The image of $\mathbb{P}^m$ under this map is called a Veronese variety. Any hyperplane section of a Veronese variety is a 1-1 image of an effective divisor of degree d in $\mathbb{P}^m$. Therefore any section of a Veronese variety by a linear subspace of codimension r is a 1-1 image of an intersection of r independent effective divisors of degree d in $\mathbb{P}^m$. Thus the study of solutions of system (4.1) is equivalent to the study of linear sections of Veronese varieties.

Suppose $r = 2$. Then system (4.1) consists of two equations. In section 4.3, we prove the following theorem.

Theorem 4.2 *Let $F_1(x_0 : x_1 : \ldots : x_m)$ and $F_2(x_0 : x_1 : \ldots : x_m)$ be homogeneous polynomials in $m+1$ variables of degree d. Suppose they are linearly independent and $d < q-1$; then the maximal possible number of their common zeroes in $\mathbb{P}^m(\mathbb{F}_q)$ equals $(d-1)q^{m-1} + p_{m-2} + q^{m-2}$.*

Theorem 4.2 is a direct modification of Theorem 4.1 to the case $r = 2$. The proof uses similar ideas.

To prove Theorem 4.2 we need the following Theorem 4.3, which can be also considered as a bound for the number of solutions of system (4.1) when polynomials F_i are supposed to have no common proper divisors.

Theorem 4.3 *Let $X \subset \mathbb{P}^m$ be an algebraic set of degree δ and dimension s. Then*

$$|X| \leq \delta p_s.$$

For $\delta \leq q$ Theorem 4.3 was proven by Lachaud [Lac]. This bound is far better than the bounds of Schmidt (see [Sch], Lemma 4,) and Nisnevich [Nis].

Now we give some definitions. The set of solutions of system (4.1) is called an (r, m, d)-*configuration*, corresponding to system (4.1). An (r, m, d)-configuration is always an algebraic subset in $\mathbb{P}^m$ whose image under the Veronese embedding of degree d lies in a linear subspace of codimension r.

Note that a given subset of $\mathbb{P}^m$ can be an (r, m, d)-configuration for many different r and d.

An (r, m, d)-configuration is called *maximal* if it contains the maximum possible number of $\mathbb{F}_q$-points (for given r, m, d and q.)

An (r, m, d)-configuration X is called *linear* if all $\mathbb{F}_q$-points lie on linear components of X. Note that there can be non-linear components which contribute no extra $\mathbb{F}_q$-points.

A linear (r, m, d)-configuration is called *dim-maximal* , if it contains the maximal possible number of components of high dimension (a strict definition is given in the next section.)

In section 4.3, we construct a maximal $(2, m, d)$-configuration, which consists of a maximal $(1, m, d-1)$-configuration plus an additional linear subspace of codimension two. This configuration as well as a

maximal $(1, m, d)$-configuration is linear and dim-maximal. We make a conjecture that a maximal (r, m, d)-configuration is also linear and dim-maximal. This will be discussed in section 4.2. In section 4.3, we prove Theorems 4.2 and 4.3. Applications to the coding theory are given in section 4.4.

4.2 Conjectures

We know that in the affine case all maximal $(1, m, d)$-configurations are linear (see [McWS] for the binary case and [DGM] for an arbitrary q.)

The following conjecture was stated by M.Tsfasman.

Conjecture 4.1 *There exists a maximal (r, m, d)-configuration which is linear.*

By Theorems 4.1 and 4.2, this conjecture is true for $r = 1, 2$.

Now we introduce the notion of a dim-maximal linear (r, m, d)-configuration.

Let us consider linear (r, m, d)-configurations from the point of view of dimensions of their components. We shall say that $(\nu_1, \nu_2, \ldots, \nu_m)$ is the *dim-type* of a linear (r, m, d)-configuration X if for all $i = 1, \ldots, m$, X contains ν_i components of codimension i not contained in components of smaller codimensions.

The lexicographical order on the dim-types induces a linear order on the set of all linear (r, m, d)-configurations: a configuration containing ν_i components defined over $\mathbb{F}_q$ for all $i = 1, \ldots, m$ is greater than a configuration containing μ_i components of codimension i for all $i = 1, \ldots, m$, if and only if there exists b such that $\nu_i = \mu_i$ for any $i < b$ and $\nu_b > \mu_b$.

An (r, m, d)-configuration that is maximal with the respect to this order is called *dim-maximal*.

The following conjecture looks also plausible to us.

Conjecture 4.2 *Let $x_1^{\nu_1} x_2^{\nu_2} \ldots x_{m+1}^{\nu_{m+1}}$ be the r-th in lexicographical order monomial of degree d in $m + 1$ variable. Then the dim-type of a dim-maximal (r, m, d)-configuration is $(\nu_1, \nu_2, \ldots, \nu_m)$.*

Note that for an arbitrary configuration the sum $\sum_i \nu_i$ can exceed d.

Now we shall give another expression for the set $\{\nu_i(r), i = 1 \dots m+1\}$. Let $x_1^{\nu_1} x_2^{\nu_2} \dots x_{m+1}^{\nu_{m+1}}$ be the r-th monomial. For each j_1 ($\nu_1 < j_1 \le d$) there exist $\binom{d-j_1+m-1}{m-1}$ monomials starting with $x_1^{j_1}$. All these monomials precede $x_1^{\nu_1} x_2^{\nu_2} \dots x_{m+1}^{\nu_{m+1}}$. Further, for each j_2 ($\nu_2 < j_2 \le d - \nu_1$) there exist $\binom{d-\nu_1-j_2+m-2}{m-2}$ monomials starting with $x_1^{\nu_1} x_2^{j_2}$. They also precede $x_1^{\nu_1} x_2^{\nu_2} \dots x_{m+1}^{\nu_{m+1}}$. Similarly, for each i ($1 \le i \le m+1$) and for each j_i ($\nu_i < j_i \le d - \sum_{l=1}^{i-1} \nu_l$) there exist $\binom{d-\sum_{l=1}^{i-1}\nu_l - j_i + m - i}{m-i}$ monomials that start with $x_1^{\nu_1} x_2^{\nu_2} \dots x_i^{j_i}$ and precede the monomial $x_1^{\nu_1} x_2^{\nu_2} \dots x_{m+1}^{\nu_{m+1}}$. Therefore

$$r = \sum_{i=1}^{m+1} \sum_{j=\nu_i+1}^{d-\sum_{l=1}^{i-1}\nu_l} \binom{d - \sum_{l=1}^{i-1}\nu_l - j + m - i}{m-1}. \tag{4.2}$$

Lemma 4.1 *There exists a union of d_i linear subspaces of $\mathbb{P}^m$ of codimension i ($i = 1, \dots, m$) that contains*

$$\sum_{i=j}^{m} d_i (p_{m-i} - p_{m-i-j}) + p_{m-2j}$$

$\mathbb{F}_q$-points, where j is the smallest integer such that $d_j \neq 0$. This is the maximum possible number of points on a union of d_i linear subspaces of codimension i ($i = 1, \dots, m$).

Proof. We compute the maximal possible number of $\mathbb{F}_q$-points on a union X of d_1 linear subspaces Π_ℓ^{m-1} ($\ell = 1, \dots, d_1$) of codimension one, d_2 linear subspaces Π_ℓ^{m-2} ($\ell = 1, \dots, d_2$) of codimension two, …, d_m linear subspaces Π_ℓ^0 ($\ell = 1, \dots, d_m$) of codimension m. We have

$$|X| = \sum_i d_i p_{m-i} - |I|,$$

where I is a set of points (with multiplicities) that were counted more than once; a point P belongs to I with multiplicity t iff P belongs exactly to $t+1$ linear subspaces Π_ℓ^i. A configuration with the maximal

number of points is a configuration with the minimal number of points in I.

Let j be the smallest integer such that $d_j > 0$. Fix a linear subspace Π_1^{m-j}. Each linear subspace of codimension i intersects with Π_1^{m-j} at least by a space of codimension $i+j$. Thus,

$$|I| \geq (d_j - 1)p_{m-j} + \sum_{i=j+1}^{m} d_i p_{m-i-j} = \sum_{i=j}^{m} d_i p_{m-i-j} - p_{m-2j}.$$

Now we prove that there exists a configuration with $|I| = \sum_{i=j}^{m} d_i p_{m-i-j} - p_{m-2j}$. Put all components of minimal codimension j so that they intersect by one common linear subspace M of codimension $2j$ in $\mathbb{P}^m$. Since $d_j \leq q$, we can put all components of codimension $j+1$ so that they do not intersect with any of Π_ℓ^{m-j} outside M, $\Pi_i^{m-j-1} \cap \Pi_\ell^{m-j-1} \subset M$ $(i \neq \ell)$, and the dimensions of intersections $\Pi_i^{m-j-1} \cap \Pi_\ell^{m-j-1}$ and $\Pi_i^{m-j-1} \cap \Pi_\ell^{m-j}$ are maximal. Since $d_{j+1} \leq q$, we can put all components of codimension $j+2$ so that all intersections $\Pi_i^{m-j-2} \cap \Pi_\ell^{m-j}$, $\Pi_i^{m-j-2} \cap \Pi_\ell^{m-j-1}$ and $\Pi_i^{m-j-2} \cap \Pi_\ell^{m-j-2}$ $(i \neq \ell)$ have maximum dimensions and are contained in M, etc. Finally, put all linear subspaces of codimension m (points) outside all other components. It is easy to check that I contains exactly $\sum_{i=j}^{m} d_i p_{m-i-j} - p_{m-2j}$ points. Therefore the configuration contains the maximal number of points. $\triangle$

We propose the following

Conjecture 4.3 *There exists a maximal (r, m, d)-configuration that is dim-maximal.*

We know that this conjecture is true for $r = 1, 2$ and for the plane case ($m = 2$). Clearly, a dim-maximal (1,m,d)-configuration contains d hyperplanes, so the maximal (1,m,d)-configuration described in section 4.1 is dim-maximal. In the proof of Lemma 4.2 , we construct a maximal (2,m,d)-configuration. It contains $d-1$ hyperplanes and one linear subvariety of $\mathbb{P}^m$ of codimension two outside these hyperplanes. It is readily seen that this configuration is also dim-maximal.

The problem for the affine case is solved in [HP]. The maximal affine configuration is similar to the configuration from Conjecture 4.3. The method of the proof is quite different and it is not clear how it can be extended to the projective case.

From Lemma 4.1 easily follows the

Corollary 4.1 *Suppose Conjecture 4.3 holds, then the maximum possible number of points on an (r, m, d)-configuration equals*

$$\sum_{i=j}^{m} \nu_i (p_{m-i} - p_{m-i-j}) + p_{m-2j},$$

where ν_i are such that $x_1^{\nu_1} x_2^{\nu_2} \dots x_{m+1}^{\nu_{m+1}}$ is the r-th (in lexicographical order) monomial of degree d in $m+1$ variables and j is the smallest integer such that $\nu_j \neq 0$.

In 1995, Lachaud proposed the following conjecture.

Conjecture 4.4 *Under the conditions of Theorem 4.3 suppose that $s \geq m/2$ and $d \leq q+1$. Then*

$$|X| \leq \delta p_s - (\delta - 1) p_{2s-m}.$$

For relevant δ and s this conjecture is stronger than Theorem 4.3. By Lemma 4.1, this conjecture holds for a union of linear subvarieties. Moreover, Lemma 4.1 implies that if this conjecture is true then its bound is exact.

4.3 Two equations

In this section we prove Theorems 4.2 and 4.3. Let R and S denote divisors of zeroes of functions F_1 and F_2 respectively. Let us show first that the bound of Theorem 4.2 can not be improved.

Lemma 4.2 *There exist effective divisors R and S of degree d such that*

$$|R \cap S| = (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

PROOF. Let $H_1, \dots, H_{d-1}$ be $d-1$ hyperplanes with a common linear space M of codimension 2. Let N be a linear subspace of codimension 2 such that N intersects M by a linear subspace of codimension 3 and

is not contained in any of H_i. Then N doesn't intersect any of H_i outside M. Let H_d and H'_d be any pair of hyperplanes intersecting by N. Let $R = H_1 + H_2 + \ldots + H_d$ and $S = H_1 + H_2 + \ldots + +H_{d-1} + H'_d$. Obviously,

$$|R \cap S| = (d-1)|H_1 \backslash M| + |N \backslash M| + |M| = (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

$\triangle$

Theorem 4.3 gives a bound on the number of $\mathbb{F}_q$-points in an algebraic set X of dimension s and degree δ in $\mathbb{P}^m$. The bound does not depend on m. This topic was discussed by Lachaud in [Lac]. Lachaud proved that if $\delta \leq q$ then there exists a linear subspace of dimension $m-s-1$ in $\mathbb{P}^m$ defined over $\mathbb{F}_q$ that doesn't intersect X, the projection of X from this subspace is a δ-sheeted covering of $\mathbb{P}^s$ defined over $\mathbb{F}_q$, so

$$|X| \leq \delta p_s. \tag{4.3}$$

This bound can be easily improved when $\delta \geq p_m/p_s$: the number of $\mathbb{F}_q$-points on X can not exceed p_m. It is not clear whether the bound of Theorem 4.3 is exact for $\delta < p_m/p_s$ (see, however, Conjecture 4.4 on page 49.)

Proof of Theorem 4.3.

The proof is by induction on m. For $m = 1$ we have $\dim X = 0$ and $|X| \leq \deg X = \delta$. Suppose we proved the theorem for the dimension $m-1$.

First we consider the case (i) when X is irreducible and not contained in a hyperplane. Secondly we consider the case (ii) when X is contained in a hyperplane. Finally (iii), we deduce from (i) and (ii) the bound for an arbitrary X.

(i) Suppose X is irreducible and X is not contained in any hyperplane. Thus, $X \cap H$ is an algebraic set of dimension $s-1$ and degree δ in $H \simeq \mathbb{P}^{m-1}$ for any hyperplane H. By the induction hypothesis, $|X \cap H| \leq \delta p_{s-1}$.

Now we use a construction, similar to one Serre used to prove Theorem 4.1. Consider the set in $\mathbb{P}^{m*} \times \mathbb{P}^m$ consisting of all pairs (H, P), where H is a hyperplane and P a point of $\mathbb{P}^m$, both defined over $\mathbb{F}_q$,

such that $P \in H \cap X$. We compute the number of $\mathbb{F}_q$-points in this set by two different ways.

We have $|X|$ ways of selecting a point $P \in X$ and for each P we have p_{m-1} ways of selecting H. On the other hand, we can first select one of p_m hyperplanes in $\mathbb{P}^m$ and then select one of points on the intersection $H \cap X$. So,

$$|X|p_{m-1} = \sum_H |H \cap X| \tag{4.4}$$

Combining this with

$$|H \cap X| \leq \delta p_{s-1},$$

we get

$$|X|p_{m-1} \leq p_m \delta p_{s-1}.$$

Thus,

$$|X| \leq \delta p_s \frac{p_{s-1}p_m}{p_s p_{m-1}}.$$

It is easy to prove that $(p_{s-1}p_m)/(p_s p_{m-1}) < 1$ for $s < m$ so

$$|X| < \delta p_s. \tag{4.5}$$

(II) Suppose X is contained in a hyperplane H. Then X is an algebraic set of dimension s in $H \simeq \mathbb{P}^{m-1}$ and of degree δ. By the induction hypothesis,

$$|X| \leq \delta p_s. \tag{4.6}$$

(III) Let X be an arbitrary algebraic set of dimension s. X can be decomposed into the sum of (absolutely) irreducible components $X = X_1 + X_2 + \ldots + X_k$ of degrees $\delta_1, \delta_2 \ldots \delta_k$; $\sum_{i=1}^k \delta_i = \delta$. If X_i is not contained in a hyperplane then $|X_i| \leq \delta_i p_s$ by inequality (4.5). If X_i is contained in a hyperplane the same is true by inequality (4.6). Note that some of X_i may be not defined over $\mathbb{F}_q$, some of them may have dimension less than s; in both cases we have the same bound.

Thus,

$$|X| \leq \sum_{i=1}^k |X_i| \leq (\sum_{i=1}^k \delta_i) p_s = \delta p_s.$$

$\triangle$

Note that the argument that led to Eq. (4.4) can be seen as an application of the Plancherel formula for a suitable Radon transform (see Chapter 2.) Take the standard action of $PGL(m, \mathbb{F}_q)$ on $\mathbb{P}^m$ and the homogenous spaces in duality (hyperplanes in $\mathbb{P}^m$, points in $\mathbb{P}^m$) with the trivial incidence relation

$$(H \bowtie P) \Leftrightarrow (H \ni P).$$

Eq. (4.4) is obtained by applying the Plancherel formula (2.4) to the indicator function $f(P) = I_X(P)$ and $\phi(H) \equiv 1$. A similar argument will be used in the proof of Theorem 4.2 with $f(P)$ being the indicator function of the Veronese variety.

Now we prove Theorem 4.2. Let $M_q(2, m, d)$ denote the number of points on the configuration from Lemma 4.2:

$$M_q(2, m, d) = (d-1)q^{m-1} + q^{m-2} + p_{m-2}.$$

We show that for any two effective divisors R and S of degree d in $\mathbb{P}^m$

$$|R \cap S| \leq M_q(2, m, d).$$

Proof of Theorem 4.2.

(i) Let X be the intersection $R \cap S$ and let Y be the maximal divisor such that $R - Y \geq 0$ and $S - Y \geq 0$. Let X' be $(R - Y) \cap (S - Y)$. Then $X = Y \cup X'$. Let $b = \deg Y$. Then $0 \leq b \leq d - 1$. By Theorem 4.1, $|Y| \leq bq^{m-1} + p_{m-2}$. X' is an algebraic set of codimension 2 and degree $\delta = (d-b)^2$. By Theorem 4.3, $|X'| \leq (d-b)^2 p_{m-2}$.

(ii) Suppose $b = 0$, then $X = X'$ and $|X| \leq d^2 p_{m-2}$. It can be easily checked that

$$|X| - M_q(2, m, d) \leq \frac{d-1}{q-1}\left(-q^m + (d+2)q^{m-1} - (d+1)\right) - q^{m-2}.$$

For $d < q - 1$ the last expression is negative, so $|X| \leq M_q(2, m, d)$.

(iii) Suppose $b > 0$. We have

$$|X| \leq |Y| + |X'| \leq bq^{m-1} + p_{m-2} + (d-b)^2 p_{m-2}.$$

After some calculations we get

$$|X|-M_q(2,m,d) \le -\frac{1}{q-1}\left(q^{m-1}\left(d-b-1\right)\left(q-(d-b+2)\right)+(d-b)^2-q^{m-2}\right) \tag{4.7}$$

The sign of the right hand side of (4.7) is the same as the sign of

$$\theta = -q^{m-1}\left(d-b-1\right)\left(q-(d-b+2)\right)-(d-b)^2+q^{m-2}.$$

(IV) Suppose $0 < b < d-1$. If $(d-b-1)(q-(d-b+2)) > 0$ then

$$q^{m-1}\left(d-b-1\right)\left(q-(d-b+2)\right) \ge q^{m-1}$$

and $\theta < 0$. We have $d-b-1 > 0$, $d-b \le d-1$. Combining this with the assumption $d < q-1$ we get $d-b < q-2$ and $(d-b-1)(q-(d-b+2)) > 0$.

Thus, $\theta < 0$ and $|X| \le M_q(2,m,d)$.

(V) Now we consider the last case $b = d-1$. We have $\deg X' = 1$, so X' is a linear subspace of codimension 2. We can not apply Theorem 4.1 directly, since we would get

$$|X| \le |Y|+|X'| \le (d-1)q^{m-1}+p_{m-2}+p_{m-2} > (d-1)q^{m-1}+q^{m-2}+p_{m-2}.$$

If Y contains an $\mathbb{F}_q$-hyperplane H then $H \cap X'$ contains a linear subspace of dimension $m-3$, whence

$$\begin{aligned} |X| &\le |Y|+|X'|-p_{m-3} \le (d-1)q^{m-1}+p_{m-2}+p_{m-2}-p_{m-3} = \\ &= (d-1)q^{m-1}+q^{m-2}+p_{m-2}. \end{aligned}$$

Suppose Y does not contain an $\mathbb{F}_q$-hyperplane, i.e. for any H the intersection $Y \cap H$ is a divisor on H. As in the proof of Theorem 4.3, we use the induction on the dimension m and Serre's construction.

The case $m = 1$ is trivial. Now suppose we proved the proposition for the dimension $m-1$. If $Y(\mathbb{F}_q) \subset X'$ then the proposition is evident. Otherwise fix an $\mathbb{F}_q$-point $Q \in (Y \backslash X')$. There exists a unique hyperplane H_0 passing through Q and X'. The intersection $H_0 \cap Y$ is a divisor of degree $d-1$ in $H \simeq \mathbb{P}^{m-1}$, $H_0 \cap X' = X'$. We have

$$|H_0 \cap X| \le |H_0 \cap Y|+|X'| \le (d-1)q^{m-2}+p_{m-3}+p_{m-2}.$$

For any other hyperplane $H \neq H_0$ passing through Q the intersection $H \cap X$ is an algebraic set in $H \simeq \mathbb{P}^{m-1}$ consisting of an effective divisor $H \cap Y$ of degree $d-1$ and of a linear subspace $H \cap X'$ of codimension 2 in H. By the induction hypothesis,

$$|H \cap X| \leq M_q(2, m-1, d).$$

Consider the set in $\mathbb{P}^{m*} \times \mathbb{P}^m$ consisting of all pairs (H, P), where H is a hyperplane and P a point of $\mathbb{P}^m$, both defined over $\mathbb{F}_q$, such that $Q \in H$, $P \in H \cap X$, $P \neq Q$. We compute the number of $\mathbb{F}_q$-points in this set by two different ways.

We have $|X| - 1$ ways of selecting a point $P \in X$ such that $P \neq Q$ and for each P we have p_{m-2} ways of selecting H passing through P and Q. On the other hand, we can first select one of p_{m-1} hyperplanes in $\mathbb{P}^m$ passing through Q and then select one of points in $(H \cap X) \backslash Q$.

Thus,

$$\begin{aligned}(|X|-1)p_{m-2} &= \sum_{H \neq H_0} (|H \cap X| - 1) + |H_0 \cap X| - 1 \quad \leq \\ &\leq p_{m-1}\left(M_q(2, m-1, d) - 1\right) + p_{m-2} - q^{m-3}.\end{aligned}$$

Therefore,

$$\begin{aligned}|X| &\leq 1 + \frac{p_{m-1}}{p_{m-2}}\left(M_q(2, m-1, d) - 1\right) + \frac{p_{m-2} - q^{m-3}}{p_{m-2}} \\ &= M_q(2, m, d) + \frac{1}{p_{m-2}}\left(q^{m-2}(d-1-q) + p_{m-3}\right).\end{aligned}$$

We have $d \leq q$; thus, $q^{m-2}(d-1-q) + p_{m-3} < 0$ and $|X| < M_q(2, m, d)$.

This completes the proof of the theorem. $\triangle$

4.4 Generalized weights

In this section we discuss applications of our results to coding theory. Re4call that a linear k-dimensional subspace C of $\mathbb{F}_q^n$ is called a *linear* $[n, k]_q$*-code*. Elements of this subspace are called *codewords* and n is

called the *length* of C. The most important parameters of a linear code C are n, k and the *minimum Hamming distance* d.

Definition. The *support* $\chi(D)$ of a code D is defined as

$$\chi(D) = \{i : \exists(x_1, x_2, \ldots, x_n) \in D : x_i \neq 0\}.$$

The r-th *generalized Hamming weight* of a linear code C is the minimal support size of a r-dimensional subcode of C:

$$d_r(C) = min\{|\chi(D)| : D \subset C, \dim D = r\}.$$

Generalized weights of a linear $[n, k, d]_q$-code are a monotone set of integers $d_1 = d \leq d_2 \leq \ldots \leq d_{k-1} \leq d_k = n$. The set of all generalized weights $\{d_1, d_2, \ldots, d_k\}$ is called the *weight hierarchy* of a code.

Hirschfeld, Tsfasman and Vlăduţ [HTV] presented a geometric interpretation of generalized weights. It is well known [TV1] that the study of linear $[n, k]_q$-codes can be reduced to the study of projective systems, that is of n-point subsets of a $(k-1)$-dimensional projective space over $\mathbb{F}_q$.

The minimum distance equals the minimal number of points of a projective system lying outside a hyperplane and the r-th generalized weight equals the minimal number of points outside a linear subspace of codimension r:

$$d_r = \min(|X| - |X \cap H|), . \tag{4.8}$$

The linear subspaces that reach the minimum in Eq.(4.8) contain the maximal possible number of points of the projective system X and are called the *maximal sections* of X.

Sets of $\mathbb{F}_q$-points of algebraic varieties are a good source of projective systems (see [TV1]). Codes, corresponding to algebraic varieties, are called algebraic-geometric codes.

Generalized weights for codes on several classes of algebraic varieties have been computed (see [HTV], [Nog1], [Nog2], [Bog0] and [TV2] for more references.)

Veronese varieties correspond to q-ary projective Reed-Muller codes. These codes are one of natural generalizations of binary Reed-Muller codes. The minimal distance for these codes was computed in [Sor1], [Sor2].

In his paper [Wei1], V.Wei computed the weight hierarchy for binary Reed-Muller codes. He implemented a strong result from the extremal set theory, namely the Kruskal-Katona theorem. Note that our results concern the case $d < q$ and $q > 2$.

Heijnen and Pellikaan [HP] computed the weight hierarchy for affine q-ary Reed-Muller codes. The answer is similar to Corollary 4.3.

The following is a straightforward consequence of Theorem 4.2.

Corollary 4.2 *The second generalized Hamming weight of a projective q-ary Reed-Muller code of order $d < q-1$ is equal to $p_m - (d-1)q^{m-1} - p_{m-2} - q^{m-2}$.*

From Corollary 4.1 follows

Corollary 4.3 *Suppose Conjecture 4.3 holds, then the weight hierarchy of a projective q-ary Reed-Muller code of order $d < q$ is given by*

$$d_r = p_m - \sum_{i=j}^{m} \nu_i (p_{m-i} - p_{m-i-j}) + p_{m-2j},$$

where ν_i are such that $x_1^{\nu_1} x_2^{\nu_2} \dots x_{m+1}^{\nu_{m+1}}$ is the r-th (in lexicographical order) monomial of degree d in $m+1$ variables, and j is the smallest integer such that $\nu_j \neq 0$.

Bibliography

[Acc] R.D.M. Accola, 'Differential and extremal lengths on Riemannian surfaces,' *Proc. Nat. Acad. Sci. USA,* **46**, (1960), 540–543.

[Apa] B. Apanasov, *Discrete groups in space and uniformization problems*, Mathematics and its Applications (Soviet Series), **40**, Kluwer, Dordrecht, (1991).

[Bav] C. Bavard, 'Systole et invariant d'Hermite,' *J. Reine Angew. Math.,* **482**, (1997), 93–120.

[BM] A.-M. Bergé and J. Martinet, "Densité dans des famillies des réseaux, Application aux réseaux isoduaux," *Enseign. Math*, **41** (1995), 335–365.

[Ber1] M. Berger, 'Du côté de chez Pu,' *Ann. Scient. Ec. Norm. Sup,* 4^e serie, **5**, (1972), 1–44.

[Ber2] M. Berger, 'A l'ombre de Loewner,' *Ann. Scient. Ec. Norm. Sup,* 4^e serie, **5**, (1972), 241–260.

[BDB] P. Boyalenkov, D. Danev, and S. Bumova, 'Upper bounds on the minimum distance of spherical codes,' *IEEE Trans. Inform. Theory*, **42**, (1996), no. 5, 1576–1581.

[Bog0] M. Boguslavsky, 'Sections of the del Pezzo surfaces, and generalized weights', *Problems Inform. Transmission* **34** (1998), no. 1, 14–24 .

[Bog1] M. Boguslavsky, 'On the number of points in an algebraic set', *Proceedings of the Fifth International Workshop "Algebraic and Combinatorial Coding Theory,"* Sozopol, Bulgaria, June 1996, 54–58.

[Bog2] M. Boguslavsky, 'On the number of solutions of polynomial systems', *Finite Fields and their Applications*, **3**, (1997), 287–299.

[Bog3] M. Boguslavsky, 'Generalized Hermitian constants and kissing numbers', *Proceedings of the Sixth International Workshop "Algebraic and Combinatorial Coding Theory,"* Pskov, Russia, September 1998, 46–51.

[Bog4] M. Boguslavsky, 'Lattices, Codes, and Radon transforms,' *Proceedings of the Workshop on coding and Cryptography'99*, INRIA, Paris, February 1999.

[BS] P. Buser and P. Sarnak, 'On the period matrix of a Riemann surface of large genus', *Invent. Math.*, **117**, no. 1, (1994), 27–56.

[CHS] J. Conway, R. Hardin, and N. Sloane, 'Packing lines, planes, etc.: packings in Grassmannian spaces,' *Experimental Mathematics*, **5** (1996), no. 2, 139–159.

[Cou1] R. Coulangeon, 'Réseaux k-extrêmes,' *Proc. London Math. Soc. (3)*, **73** (1996), no. 3, 555–574.

[Cou2] R. Coulangeon, 'Minimal vectors in the second exterior power of a lattice', *J. Algebra*, **194**, (1997), no. 2, 467–476.

[Del] P.Delsarte, 'The associations schemes in coding theory,' *Combinatorics. Proc. NATO Advanced Study Inst., Breukelen, Part 1: Theory of designs, finite geometry, and coding theory*, (1974), pp. 139–157.

[DGM] P.Delsarte, J.-M.Goethals, and F.J.MacWilliams, 'On generalized Reed-Muller codes their relatives,' *Inform. and Control,* **16**, (1974), 423–442.

[Elk] N. Elkies, 'Mordell–Weil lattices in characteristic 2. I.," *Int. Math. Res. Notes,* **8**, (1994), 343–361.

[For1] G. Forney, Jr, 'Dimension/length profiles and trellis complexity of linear block codes,' *IEEE Trans. Inform. Theory*, **40**, (1994), no. 6, 1741–1752.

[For2] G. Forney, Jr, 'Density/length profiles and trellis complexity of lattices,' *IEEE Trans. Inform. Theory*, **40**, (1994), no. 6, 1753–1772.

[GV1] G. van der Geer and M. van der Vlugt, 'How to construct curves over finite fields', alg-geom/9511005.

[GV2] G. van der Geer and M. van der Vlugt, 'Quadratic forms, generalized Hamming weights and curves over finite fields with many points', J. of Number Theory, **59**, (1996), 20–36.

[GV3] G. van der Geer and M. van der Vlugt, 'Generalized Reed–Muller codes and curves with many points', alg-geom/9710016.

[GV4] G. van der Geer and M. van der Vlugt, 'Curves over finite fields of characteristic 2 with many rational points,' *C. R. Acad. Sci. Paris,* vol. 317, ser. I, (1993), 593–597.

[GGV] I.M. Gelfand, M.I. Graev,and N.Ya. Vilenkin, *Generalized functions. Vol. 5. Integral geometry and representation theory*, Academic Press, New York-London, (1966) [1977].

[Gop] V.D. Goppa, 'Algebraic-geometric codes', (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.*, **46** (1982), no. 4, 762–781, 896.

[GH] P. Griffiths, and J. Harris, *Principles of algebraic geometry*, Wiley-Interscience, New York, (1978).

[Gro] M. Gromov, 'Systoles and intersystolic inequalities', preprint IHES/M/92/98, (1992).

[HP] P. Heijnen and R. Pelikaan 'Generalized Hamming weights of q-ary Reed-Muller codes,' *IEEE Trans. Inform. Theory*, **44** (1998), no. 1, 181–196.

[Hel1] S. Helgason, *Groups and Geometric Analysis. Integral geometry, invariant differential operators, and spherical functions*, Academic press, (1984).

[Hel2] S. Helgason, *Geometric Analysis on Symmetric Spaces*, AMS, (1994).

[HKM] T. Helleseth, T. Kløve, and J. Mykkeltveit, 'The weight distribution of irreducible cyclic codes with block length $n_1\left(\left(q^l-1\right)/N\right)$,' *Discr. Math.*, **18**, (1977), 179–211.

[HKYL] T. Helleseth, T. Kløve, O. Ytrehus, and V. Levenshtein, 'Bounds on the minimum support weights,' *IEEE Trans. Inform. Theory,* **41**, (1995), 432–440.

[HTV] J.W.P. Hirschfeld, M.A. Tsfasman and S.G. Vlăduţ, 'The weight hierarchy of higher-dimensional Hermitian codes', *IEEE Trans. Inform. Theory*, **40**, (1994), 275–279.

[KL] G. Kabatjanskij and V. Levenstein, 'Bounds for packings on the sphere and in space', (Russian) *Problemy Peredach Informacii*, **14** (1978), no. 1, 3–25

[KTFL] T. Kasami, T. Tanaka, T. Fujiwara and S. Lin, 'On complexity of trellis structure of linear block codes,' *IEEE Trans. Inform. Theory,* **39**, (1993), 1057–1064.

[Klo] T. Kløve, 'Support weight distribution of linear codes', Discrete Math., **106/107**, (1992), 311-313.

[Lac] G. Lachaud, 'Number of points of plane sections and linear codes defined by forms on algebraic varieties,', in *"Arithmetic, Geometry and Coding Theory",* Walter de Gruyter, Berlin, (1996), 77–104.

[LS] M. Lavrentjev and L. Saveljev, *Linear operators and ill-posed problems. With a supplement by A. L. Bukhgeim*, Consultants Bureau, New York; (1995).

[Lev] V. Levenshtein, 'Universal bounds for codes and designs,' *Handbook of Coding Theory*, Elsevier, Amsterdam, (1998).

[McWS] F.J. MacWilliams N.J.A. Sloane, *"The Theory of Error-correcting Codes,"* Elsevier, Amsterdam, (1977).

[NS] G. Nebe and N. Sloane, *The electronic catalogue of lattices*, http://www.research.att.com/~njas/lattices.

[Nis] L.B. Nisnevich,'On the number of points of an algebraic manifold over a prime field,' *Dokl. Acad. Nauk SSSR (N.S.)*, **99**, 1954, 17–20.

[Nog1] D. Nogin, 'Generalized Hamming weights for codes on multidimensional quadrics,' *Problems Inform. Transmission* , **29**, (1993), no. 3, 218–227

[Nog2] D. Nogin, 'Codes associated to Grassmanians', in *Arithmetic, Geometry and Coding Theory,* Walter de Gruyter, Berlin, (1996), 145–154.

[Nog3] D. Nogin, 'Weight/multiplicity duality', *Proceedings of the Sixth International Workshop "Algebraic and Combinatorial Coding Theory,"* Pskov, Russia, September 1998, 195–198.

[Pu] P.M. Pu, "Some inequalities in certain nonorientable Riemannian manifolds," *Pacific J. Math*, **2**, (1952), 55–71.

[Rad] J. Radon, 'Über die Bestimmung von Funktionen durch ihre Integralwärte längs gewisser Männigfretigkeiten', *Ber. Verh. Sčhs. Akad.* ,**69** (1917), 262-277.

[Ran1] R. Rankin, 'On positive definite quadratic forms,' *J. London Math. Soc.*, **28**, (1953), 309–314.

[Ran2] R. Rankin, 'The closest packing of spherical cups in n dimensions,' *Proc. Glasgow Math. Assoc.,* **2**, (1955), 139–144.

[Sch] W. Schmidt 'A lower bound for the number of solutions of equations over finite fields,' *J. of Number Theory*, **6**, (1976), 448–480.

[Ser] J.-P.Serre, 'Lettre à M. Tsfasman', in *Journées Arithmètiques de Luminy (1989)*, *Astèrisque* **198-199-200** (1991), 149–156.

[Sie] K.L. Siegel, 'A mean value theorem in geometry of numbers,", *Annals of Mathematics,* **46**, (1945), 340–347.

[Sim] J. Simonis, 'The effective length of subcodes', *Applicable Algebra in Engineering, Communication and Computing*, **5**, (1994), 371–377.

[Sor1] A.B. Sørensen, 'Rational points on hypersurfaces, Reed-Muller codes and algebraic-geometric codes,' Ph. D. Thesis, Aarhus, (1991).

[Sor2] A.B. Sørensen, 'Projective Reed-Muller codes,' *IEEE Trans. Inform. Theory*, **37**, (1991), 1567–1576.

[SPLAG] J.H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups.*, Third edition. Springer-Verlag, New York, (1999).

[Thu1] J. Thunder, 'Higher-dimensional analogs of Hermite's constant,' *Michigan Math. J. ,* **45** (1998), no. 2, 301–314.

[Thu2] J. Thunder, 'An adelic Minkowski-Hlawka theorem and an application to Siegel's lemma,' *J. Reine Angew. Math.,* **475** (1996), 167–185.

[TV1] M. Tsfasman and S. Vlăduţ, *Algebraic - Geometric Codes.* Dordrecht: Kluwer Academic Publishers, (1991).

[TV2] M. Tsfasman and S. Vlăduţ, 'Geometric approach to higher weights'. *IEEE Trans. Info. Theory,* **41** (1995), 1564–1588.

[Wan] Z. Wan, 'Weight hierarchies of the projective codes from non-degenerated quadrics,' *Codes, Designs and Cryptography*, Walter de Gruyter, Berlin, (1996).

[Wei1] V.K. Wei, 'Generalized Hamming weights for linear codes', *IEEE Trans. Inform. Theory*, **38**, (1992), 1125-1130.

[Wei2] V.K. Wei, 'Generalized Hamming weights; Fundamental open problems in coding theory', ijn *"Arithmetic, Geometry and Coding Theory,"* Walter de Gruyter, Berlin, (1996), 269–281.

[Won] Y.-C. Wong, 'Differential geometry of Grassmann manifolds', *Proc. Nat. Acad. Sci. USA*, **47** (1967), 589–594.

Curriculum Vitae

Op 17 maart 1974 ben ik geboren in Moskou, Rusland. Na het behalen van mijn middelbare schooldiploma aan School 57 te Moskou, begon ik in 1990 met de studie Wiskunde aan de Universiteit van Moskou. In juni 1995 studeerde ik cum laude af en sinds augustus van dat jaar ben ik werkzaam als onderzoeker in opleiding bij het Instituut voor Informatie Transmissie Problemen, Russische Academie van Wetenschappen en sinds mei 1997 ben ik werkzaam als bursaal bij de vakgroep Wiskunde van de Universiteit van Amsterdam.

Nederlandse Samenvatting

Roosters, Codes en Radon Transformaties

In dit proefschrift worden gegeneraliseerde Hamming–gewichten van codes en gegeneraliseerde parameters van roosters in de Euclidische ruimte bestudeerd. Gegeneraliseerde Hamminggewichten zijn relatief nieuwe parameters van een lineaire code. Zij worden intensief bestudeerd sinds de aanvang der jaren negentij. Gegeneraliseerde gewichten van een code hangen nauw samen met de trellis–complexiteit, ontcijfering, en de prestatie van de code wanneer zij gebruikt wordt in een cryptografisch kanaal van een speciaal type. Verder worden gegeneraliseerde gewichten gebruikt om codes te classificeren, om krommen met vele punten over eindige lichamen te construeren, en voor tal van andere problemen.

Gegeneraliseerde Hermite–parameters van roosters zijn analoog aan de gegeneraliseerde Hamming–gewichten. Zij werden door Rankin in 1953 ingevoerd als natuurlijke invarianten van een kwadratische vorm; intensief onderzoek in deze richting startte echter pas enige jaren geleden. Gegeneraliseerde Hermite–parameters zijn ook verbonden met de trellis complexiteit en met het ontcijferen van Euclidische codes. Zij zijn de systolen van vlakke tori, dus het is belangrijk hen te bestuderen vanuit meetkundig oogpunt. Onlangs werd een mooie adelische interpretatie en generalisatie van gegeneraliseerde Hermite parameters gevonden.

Er bestaat een aanzienlijke hoeveelheid van resultaten betreffende gegeneraliseerde Hamming gewichten; gegeneraliseerde Hermite parameters worden veel minder bestudeerd; in het bijzonder zijn weinig grenzen bekend. In dit proefschrift worden verscheidene nieuwe grenzen verkregen.

Veel resultaten van coderingstheorie hebben natuurlijke analogieen in de theorie van bolpakkingen (verkregen via roosters). In veel gevallen bestaan algemene constructies, zodat de resultaten over codes en roosters beschouwd kunnen worden als speciale gevallen van een algemene stelling. Om een voorbeeld te geven : de Poisson sommatieformule impliceert zowel de functionaalvergelijkingen voor de Θ-functies van roosters als de MacWilliams–identiteiten voor gewichtstellers. We beschrijven een nieuwe constructie van dit type dat nuttig is bij het bestuderen

van gegeneraliseerde Hamming–gewichten en gegeneraliseerde Hermite–parameters. Dit doen we door een Radon–transformatie te construeren in ruimten verbonden met codes in roosters, en we laten verschillende toepassingen van deze transformatie zien, waaronder een bewijs van een gegeneraliseerde Minkowski-Hlawka stelling.

Een interessant onderwerp in de moderne algebraïsche coderingstheorie is de studie van algebraïsche variëteiten van dimensie groter dan een. Er zijn slechts weinig resultaten bekend in deze richting. De berekening van gegeneraliseerde Hamming–gewichten voor deze codes leidt tot interessante en belangrijke meetkundige problemen. In dit proefschrift beschouwen we het probleem der berekening van gegeneraliseerde gewichten voor projectieve Reed-Muller codes. Dit is equivalent met de berekening van het maximale aantal mogelijke oplossingen van een polynomiaal systeem van een gegeven rang over een eindig lichaam.