Radon Transforms and Packings

Michael I. Boguslavsky[*]

November 1999

Abstract

We use some basic results and ideas from the integral geometry to study certain properties of group codes. The properties being studied are generalized weights and spectra of linear block codes over a finite field and their analogues for lattice sphere packings in Euclidean space. We do not obtain any new results about linear codes, although several short and simple proofs for known results are given. As to the lattices, we introduce a generalization of lattice Θ-functions, prove several identities on these functions, and prove generalizations of Siegel mean value and Minkowski–Hlawka theorems.

1 Introduction

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 summation 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 kind which is useful in the study of generalized Hamming weights and their lattice analogues, generalized Hermite parameters. Namely, we construct a Radon transform in spaces connected with codes and lattices and demonstrate several applications of this transform.

We introduce the notion of *the T-functions* of lattice. 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

[*] Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow; e-mail: mic@iitp.ru. This work has been supported in part by Russian Fund for Fundamental Research (RFFI) and is based on a part of author's Ph.D. thesis defended in June, 1999 at the University of Amsterdam under the joint supervision of Prof. Gerard van der Geer and Prof. Michael Tsfasman.

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.

This paper is organized as follows. In the next section we give the necessary definitions and mention some notions from the integral geometry. In section 3 we study the properies of T-functions, and in section 4 we prove a bound for generalized Hermite parameters of lattices (see the definition below.)

I would like to thank Gerard van der Geer, Michael Tsfasman, and Vladimir Levenstein for many valuable discussions.

2 Basic Notions

2.1 Codes and Lattices

Let us mention first necessary definitons and results from coding theory and theory of lattice sphere packings. Most of these facts can be found, for example, in [CS]. In an n–dimensional fixed basis vector space $\mathbb{F}_q^n$ over a finite field $\mathbb{F}_q$, one may introduce *the Hamming metric* defining the distance $d(u,v)$ between vectors u and v by

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

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 r-dimensional subspace $D \in C$ is called an r*-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 matrix of $(e_1,\ldots,e_n)$.

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

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

An r-sublattice is a rank r subgroup of a lattice. The following proposition is obvious and well-known, although the author is unable to provide a reference for it.

Proposition 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 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; the Hermite parameter $\gamma(L)$ is one of them – the bigger $\gamma(L)$ is, the denser is the corresponding sphere packing.

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 $\mathbb{F}_q^n$. Since the vector space $\mathbb{F}_q^n$ has fixed basis, it has also the standard scalar product $(x, y) = \sum_{i=1}^n x_i y_i$. This scalar product yields a natural embedding of the dual code to the same space $\mathbb{F}_q^n$; under this embedding, codewords of $C^{\perp}$ correspond to vectors $y \in \mathbb{F}_q^n$ such that $(x, y) = 0$ for any $x \in C$.

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

$$W_{C^{\perp}}(x, y) = \frac{1}{q^k} W_C(x + (q-1)y, x - y). \tag{2}$$

MacWilliams identities (2) are 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:

$$\int_H f(x)\, dx = \int_{\widehat{G/H}} \tilde{f}(\alpha)\, d\alpha. \tag{3}$$

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 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:

$$\Theta_L(q) := \sum_{v\in L} q^{\|v\|} = \sum_k N_k q^k, \tag{4}$$

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 (2) is the functional equation for Θ-functions:

$$\Theta_{L^\perp}(z) = (\det L)^{1/2} \left(\frac{i}{z}\right)^{n/2} \Theta_L\left(-\frac{1}{z}\right). \tag{5}$$

As well as the MacWilliams identities (2), this equation is a corollary of the Poisson summation formula (3).

2.2 Generalized weights and spectra

2.2.1 Generalized Hamming weights

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 [TV]. Generalized weights describe the performance of a code when used in certain encryption schemes; they are connected to trellis complexity and can be used for code classification and other purposes.

2.2.2 Generalized Hermite Parameters

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:

$$\operatorname{vol}_m(L) := \min_{M\subset L,\ \operatorname{rk} M = m} \operatorname{vol} M. \tag{6}$$

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. (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

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

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]

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

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.

Generalized Hermite parameters are related to trellis complexity in the same way as generalized Hamming weights; they appear naturally in many areas of mathematics where lattices do, for example, in adelic geometry [Thu1], [Thu2], or as the k-systoles of Riemann manifolds [Gro] and Abelian varieties [BuSa].

2.2.3 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 2 ([Ran1],[For2]) *For any $1 \le m < n$ and for any lattice $L \in \mathbb{R}^n$*

$$\gamma_m(L) = \gamma_{n-m}(L^\perp) \qquad (7)$$

$$\gamma_{n,m} = \gamma_{n,n-m}\,. \qquad (8)$$

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. (7). Taking the minimum in Eq. (7) over all sublattices of rank n we obtain Eq. (8) $\triangle$

2.2.4 Generalized Spectra

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

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

Let $\left[{a \atop b} \right]_q$ denote the Gaussian binomial coefficient

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

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])

$$\sum_{i=0}^{j} \binom{n-i}{n-j} A_i^r = \sum_{u=0}^{r+k-j} q^{u(j-k+u-r)} \begin{bmatrix} j-k \\ r-u \end{bmatrix}_q \sum_{v=0}^{n-j} \binom{n-v}{j} \tilde{A}_v^u,$$
$$r=0,\dots,k, \quad j=0,\dots,n. \tag{9}$$

Kløve [Klo] proved generalized MacWilliams identities (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 $C^{(s)}$, $s=1,\dots,k$. The MacWilliams identities for $C^{(s)}$ imply then Eqs. (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 $L^{\otimes m} = L \otimes L \otimes \dots \otimes L$ 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.

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 primitive 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: $(r=1,\dots,n)$:

$$T_L^r(q) := \sum_{\xi \in L^{[r]}} q^{\|\xi\|}. \tag{10}$$

We shall study the properties of these functions in section 3.

2.2.5 Bounds

Many known bounds on generalized Hamming weights are listed in [TV] and [HKYL]. We give here the known bounds on generalized Hermite parameters.

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

$$\gamma_m(L) \le \gamma_{r,m}(\gamma_r(L))^{m/r}, \tag{11}$$

and

$$\gamma_{n,m} \leq \gamma_{r,m}(\gamma_{n,r})^{m/r}. \tag{12}$$

Rankin proved (12); his argument also proves Eq. (11) although he did not state it explicitly.

Independently, Forney [For2] proved a special case of Eq. (11). Substituting $m = 1$ to Eq. (11) we get the inequality

$$\gamma_r(L) \geq \gamma_1(L)/\gamma_r^r, \tag{13}$$

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

A lattice L meets bound (13) 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 $r = 1, \ldots, 8$ and any n. It is often convenient to use inequality (13) 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 subsection 4.2 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

$$\gamma_m(L) \geq \left(n \frac{\prod_{j=n-m+1}^{n} Z(j)}{\prod_{j=2}^{m} Z(j)} \right)^{2/n}, \tag{14}$$

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 $\gamma_{n,r}$**

$$\gamma_{n,r} \leq \gamma_n^r. \tag{15}$$

This result is essentially a corollary of Minkowski studies on succesive 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

$$\gamma_2(L) \leq \frac{n-1}{n} \times \frac{\tau(L)}{\tau(L)-2} \times \gamma_1(L)^2. \tag{16}$$

If $\tau(L) > n(n+1)$ then (16) may be improved and

$$\gamma_2(L) \leq \frac{n-1}{n} \times \gamma_1(L)^2. \tag{17}$$

These bounds were proved in [Bog1] and [Bog3] using a reduction to packings in projective spaces and spherical codes.

2.3 Homogenous spaces in duality

Let us describe first few basic results 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 that many other applications of these technique are possible. For example, in proofs of bounds on the number of points on algebraic sets in [Bog2] the key step is equivalent to the use of the Plancherel formula for a suitable Radon transform in $\mathbb{P}^m(\mathbb{F}_q)$.

2.3.1 General Theory

In this subsection, 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 §2.3.2 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

$$\begin{tikzcd} & G/K \arrow[dl, "p"'] \arrow[dr, "\pi"] & \\ X = G/H_X & & \Xi = G/H_\Xi \end{tikzcd} \quad , \tag{18}$$

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

$$\hat{f}(\xi) = \int_{\hat{\xi}} f(x)\, dm(x); \tag{19}$$

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

$$\check{\phi}(x) = \int_{\check{x}} \phi(\xi)\, d\mu(\xi). \tag{20}$$

Lemma 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*

$$\int_X f(x)\check{\phi}(x)\, dx = \int_\Xi \hat{f}(\xi)\phi(\xi)\, d\xi. \tag{21}$$

Note. For a discrete group G the formal equalities

$$\sum_{x \in X} f(x)\check{\phi}(x) = \sum_{(x,\xi)\in X\times\Xi:\ x \bowtie \xi} f(x)\phi(\xi) = \sum_{\xi\in\Xi} \hat{f}(\xi)\phi(\xi) \tag{22}$$

show that Eq. (21) holds also for any functions f and ϕ such that all series in (22) converge absolutely. The proof for the general case is similar but requires some additional facts about measures and groups.

Actually, equality (21) holds in a more general case of a double filtration like (18) 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 (19) and of the dual transform (20), is, in general, rather complicated, 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 the next subsection. An equivalent result was proved by Nogin [Nog] in connection with one problem about projective multisets.

2.3.2 Weight/Multiplicity Duality for Projective Multisets

Nogin [Nog] 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 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

$$\mathrm{wt}(c) = \sum_{H \not\ni c} \nu(H). \tag{23}$$

A natural problem is to invert relations (23), 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 (23):

$$\nu(H) = \frac{\sum_{c \in \mathbb{P}C} \mathrm{wt}(c) - q \sum_{c \in H} \mathrm{wt}(c)}{q^{k-1}}. \tag{24}$$

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 [Nog]). 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. (24) to obtain a set of "multiplicities" and correct them to a set of multiplicities of a projective multiset. The spectrum of the code C_2 corresponding to this multiset 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 subsection 2.3.1) 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

$$\hat{f}(\xi) = \sum_{x \in \xi} f(x), \tag{25}$$

$$\check{\phi}(x) = \sum_{\xi \ni x} \phi(\xi). \tag{26}$$

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 $\{\phi : \Xi \to \mathbb{C}\}$ and $\{f : X \to \mathbb{C}\}$ 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 1 *The Radon transform (25) and the dual Radon transform (26) are inverted by the formulas*

$$f(x) = \frac{1}{q^{m-1}} \left(D\hat{f} \right)^{\vee} (x) \qquad \phi(\xi) = \frac{1}{q^{m-1}} \left(\Delta\check{\phi} \right)^{\wedge} (x). \tag{27}$$

Proof. It is sufficient to prove Eq. (27) 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

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

△

Note that Eq. (23) can be rewritten as

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

Using the inversion formula (27) for the function $\nu(c)$ we get Eq. (24).

3 T-functions

In this section we study the properties of the *lattice T-functions*

$$T_L^r(q) := \sum_{\xi \in L^{[r]}} q^{\det \xi}, \qquad r = 1, \ldots, n.$$

These functions can be considered as generalizations of the classical Θ-function of a lattice

$$\Theta_L(q) := \sum_{v \in L} q^{\|v\|}.$$

3.1 Main Properties

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 3 *For any lattice L*

$$\Theta_L(q) - 1 = 2 \sum_{m=1}^{\infty} T_L^1(q^{m^2}); \tag{28}$$

$$2T_L^1(q) = \sum_{k=1}^{\infty} \mu(k) \left(\Theta_L(q^{k^2}) - 1 \right). \tag{29}$$

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 nonzero vector $v \in L$ can be uniquely written as $v = mp_M$, where p_M is a primitive vector and $m \in \mathbb{N}$. Thus,

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

Eq. (29) can be obtained from Eq. (28) by a standard Moebius inversion. △

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

$$\begin{aligned} \Theta_L(q) - 1 &= \sum_{v \in L\backslash\{0\}} q^{\|v\|} = \\ &= 2\left(\sum_{v \in L^{[1]}} q^{\|v\|} + \sum_{v/2 \in L^{[1]}} q^{\|v\|} + \ldots + \sum_{v/k \in L^{[1]}} q^{\|v\|} + \ldots \right) = \\ &= 2 \sum_{v \in L^{[1]}} \sum_{m=1}^{\infty} q^{m^2\|v\|} = 2 \sum_{v \in L^{[1]}} \theta_3(q^{\|v\|}). \end{aligned} \tag{30}$$

Similarly to the duality relations (7) one can prove the following proposition.

Proposition 4 *For any lattice L*

$$T_L^r(q) = T_{L^\perp}^{n-r}(q^{\det L}). \tag{31}$$

An interesting problem is to determine the lattice analogue of generalized MacWilliams identities (9). Proposition 4 gives n relations on generalized spectra. Since we have $(k+1)(n+1)$ generalized MacWilliams identities, one could expect to have more relations on T-functions. Propositions 3 and 4 combined with the functional equation (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 ↔ mean that the spectrum of one object is determined by the spectrum of another. We have the following diagram.

$$\begin{tikzcd}
L^{[1]} \arrow[r, leftrightarrow, "(31)"] \arrow[d, leftrightarrow, "(29)"] & L^{\perp[n-1]} \\
L \arrow[r, leftrightarrow, "(5)"] & L^{\perp} \arrow[d, leftrightarrow, "(29)"] \\
L^{[n-1]} \arrow[r, leftrightarrow, "(31)"] & L^{\perp[1]}
\end{tikzcd}$$

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 $L^\perp$.

In the next subsection we shall use the Plancherel formula to obtain another relation between T_L^1 and T_L^{n-1}. This relation expresses their product via a weighted sum of shifted sublattice Θ-functions.

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

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

$$A(n) := \{M \in M_n(\mathbb{Z}) : \quad |\det M| = 1\}.$$

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

$$G = R(n) := \begin{pmatrix} A(n) & \mathbb{Z}^n \\ 0 & 1 \end{pmatrix} \tag{32}$$

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:

$$H_X = St(0) \simeq A(n); \tag{33}$$

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

$$H_\Xi = St(\Pi_0) = St\langle v_1, v_2, \ldots, v_{n-1}\rangle. \tag{34}$$

Lemma 2 *The spaces $X = G/H_X$ and $\Xi = G/H_\Xi$ defined by Eq. (32), (33) and (34) 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

$$h_X h_\Xi = g_\Xi g_X \tag{35}$$

then $h_X \in H_\Xi$. Applying the right and the left hand sides of (35) to the origin, we get

$$h_X\,(h_\Xi\,0) = g_\Xi\,(g_X\,0)\,. \tag{36}$$

Since $g_X 0 = 0$, the right hand side of (36) 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. △

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

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

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 (34) 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 (21) gives

$$\sum_{x \in \mathbb{Z}^n} f(x)\check{\phi}(x) = \sum_{\xi \in \overline{(\mathbb{Z}^n)^{[n-1]}}} \hat{f}(\xi)\phi(\xi) \tag{37}$$

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

Let $p^{\|\xi\|}$ denote the determinant of a lattice ξ.

Theorem 2 *For any lattice L of rank n*

$$\Theta_L(q) \cdot T_L^{n-1}(p) = \sum_{\xi \in \overline{L^{[n-1]}}} p^{\|\xi\|}\Theta_\xi(q). \tag{38}$$

Proof. Let us apply Eq. (37) 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 (37):

$$\begin{aligned}&\sum_{x \in \mathbb{Z}^n}\left(q^{\|x\|}\sum_{\xi \in \Xi} p^{\|\xi\|}\right) = \sum_{x \in \mathbb{Z}^n} q^{\|x\|}\left(\sum_{\xi_x \in \Xi:\ x \in \xi_x} p^{\|\xi_x\|}\right) = \\ &= \sum_{x \in \mathbb{Z}^n}\sum_{\xi \bowtie x} q^{\|x\|}p^{\|\xi\|} \overset{(37)}{=} \sum_{\xi \in \Xi}\sum_{x \bowtie \xi} q^{\|x\|}p^{\|\xi\|} = \sum_{\xi \in \Xi} p^{\|\xi\|}\Theta_\xi(q).\end{aligned}$$

$\triangle$

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 (7), (31) we get the following corollary

Corollary 1 *For any lattice $L \subset \mathbb{R}^n$ holds*

$$\Theta_L(q) \cdot T^1_{L^\perp}(p^{\det L}) = \sum_{\xi \in \overline{L^{[n-1]}}} p^{\|\xi\|}\Theta_\xi(q). \tag{39}$$

4 Bounds

4.1 Generalized Plotkin Bound

In this section, we prove a lower bound for generalized Hamming weights (see [TV] 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 3 ([GV]) *For any r-subcode D holds*

$$\mathrm{wt}(D) = \frac{1}{q^r - q^{r-1}} \sum_{c \in D} \mathrm{wt}(c). \tag{40}$$

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 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. (40) (lemma 3) and once Eq. (21) (lemma 1):

$$\begin{aligned}
\sum_{D \in C^{[r]}} \mathrm{wt}(D) &\overset{(40)}{=} \frac{1}{q^r - q^{r-1}} \sum_{D \in C^{[r]}} \sum_{c \bowtie D} \mathrm{wt}(c) \overset{(21)}{=} \frac{1}{q^r - q^{r-1}} \sum_{c \in C} \sum_{D \bowtie c} \mathrm{wt}(c) = \\
&= \frac{1}{q^r - q^{r-1}} \sum_{c \in C} \#\{D \in C^{[r]} | c \in D\} \, \mathrm{wt}(c) = \\
&= \frac{1}{q^r - q^{r-1}} \begin{bmatrix} k \\ r \end{bmatrix}_q \sum_{c \in C} \mathrm{wt}(c) \overset{(40)}{=} \\
&\overset{(40)}{=} \frac{1}{q^r - q^{r-1}} \begin{bmatrix} k \\ r \end{bmatrix}_q (q^k - q^{k-1}) \, \mathrm{wt}(C) = \\
&= \frac{nq^{k-r}}{q^k - 1} \begin{bmatrix} k \\ r \end{bmatrix}_q .
\end{aligned}$$

△

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

Corollary 2 ([TV]) *The r-h generalized Hamming weight $d_r(C)$ of an $[n,k,d]_q$-code C satisfies*

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

4.2 Generalized Minkowski–Hlawka Theorem

This theorem is a non constructive lower bound on $\gamma_{n,m}$. It was first proved by Thunder [Thu1] in greater generality. 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 4 (Generalized Minkowski–Hlawka Theorem) *For any $m < n$ there exists a lattice $L \subset \mathbb{R}^n$ with*

$$\gamma_m(L) \geq \left(n \frac{\prod_{j=n-m+1}^{n} Z(j)}{\prod_{j=2}^{m} Z(j)} \right)^{2/n}. \tag{41}$$

For $m = 1$ we get the classical Minkowski–Hlawka theorem. The latter is a famous result conjectured first by Minkowski and proved many years later by Hlawka and then by Siegel. It is a non constructive lower bound on Hermite constant γ_n. Asymptotically, Minkowski–Hlawka theorem yields

$$\log \gamma_n \geq \log n + O(1) \tag{42}$$

as $n \to \infty$. All the subsequent improvements of this result concern only the $O(1)$ term; in fact, combining (42) with known upper bounds one gets

$$\log \gamma_n = \log n + O(1).$$

Our generalized Minkowski–Hlawka theorem combined with bound (15) gives

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

The implied constant depends on m and is unknown even for the classical case $m = 1$.

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

$$\int_{\mathbb{R}^n} \phi(x)\, dx = \zeta(n) \int_{\mathcal{L}_n} \sum_{z \in P} \phi(gz)\, dg, \tag{43}$$

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 as 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

$$L \bowtie M \Leftrightarrow \text{“}M \text{ is a primitive sublattice of } L\text{”}. \tag{44}$$

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 $U_n(\mathbb{R})$ 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

$$\mathcal{L}_n = U_n(\mathbb{R})/U_n(\mathbb{Z}) \tag{45}$$

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

$$\mathcal{R}_m = U_n(\mathbb{R})/St(M_0), \tag{46}$$

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) (see subsection 2.3.1) with the incidence relation (44).

Theorem 5 (Generalized Siegel mean value theorem) *Let $\phi(\cdot)$ be a compactly supported function on $\mathcal{R}_m$. Then*

$$C \int_{\mathcal{L}_n} \sum_{M \bowtie L} \phi(M)\, dL = \int_{\mathcal{R}_m} \phi(M)\, dM, \tag{47}$$

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 (43) 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 (21) for the pair $(\mathcal{L}_n, \mathcal{R}_m)$ of homogenous spaces in duality defined by (45) and (46). 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

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

It is clear that $\operatorname{vol}(\check{M})$ 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 $1/C = \operatorname{vol}(\check{M})$. 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 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. (47) 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 4. $\triangle$

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

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

References

[Bog1] M. Boguslavsky, *Lattices, Codes, and Radon Transforms*, Ph.D. thesis, Korteweg–de Vries Institute for Mathematics, University of Amsterdam, (1999).

[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.

[BuSa] 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.

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

[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.

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

[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].

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

[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, Ø. Ytrehus, and V. Levenshtein, 'Bounds on the minimum support weights,' *IEEE Trans. Inform. Theory,* **41**, (1995), 432–440.

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

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

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

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

[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.

[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.

[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.

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

[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.