PDMI PREPRINT — 27/1998

CODING THEORY AND UNIFORM DISTRIBUTIONS

M. M. Skriganov

Russian Academy of Sciences
Steklov Mathematical Institute
St. Petersburg Department
Fontanka 27, St. Petersburg 191011, Russia

E-mail:skrig @ pdmi.ras.ru

December 4, 1998

ABSTRACT

In the present paper we introduce and study finite point subsets of a special kind, called optimum distributions, in the n-dimensional unit cube. Such distributions are close related with known (δ, s, n)-nets of low discrepancy.

It turns out that optimum distributions have a rich combinatorial structure. Namely, we show that optimum distributions can be characterized completely as maximum distance separable codes with respect to a non-Hamming metric. Weight spectra of such codes can be evaluated precisely.

We also consider linear codes and distributions and study their general properties including the duality with respect to a suitable inner product. The corresponding generalized MacWilliams identies for weight enumerators are brifly discussed.

Broad classes of linear maximum distance separable codes and linear optimum distributions are explicitly constructed in the paper by the Hermite interpolations over finite fields.

1991 *Mathematics Subject Classification.* 11K38, 11T71, 94B60

Key words and phrases. Combinatorial structure of uniform distributions, non-Hamming metrics on q-ary codes

The work was partially supported by Russian Fund for Fundamental Research (Project No. 96-01-00856).

Typeset by $\mathcal{AMS}$-TEX

Contents

1. Introduction
2. Distributions and codes
3. Weight spectra
4. Linear codes and distributions
5. Constructions of linear MDS codes and optimum distributions
6. Reconstructions of codes and distributions
References

1. Introduction

The present paper deals with a combinatorial structure of point sets uniformly distributed in the n-dimensional unit cube. We introduce point sets of a special kind, called optimum distributions, which are close related with known distributions, so-called (δ, s, n)-nets, of low discrepancy. It turns out that optimum distributions have a rich interior combinatorial structure, namely, they can be characterized completely as maximum distance separable codes over finite fields with respect to a non-Hamming metric. Moreover, it is found that weight spectra of such codes can be evaluated precisely.

We also study linear codes and distributions. In this case new good codes and distributions can be obtained from given ones by duality with respect to a suitable inner product. The corresponding MacWilliams identities for weight enumerators in the non-Hamming metric are also brifly discussed in the paper. Notice that broad classes of linear maximum distance separable codes and linear optimum distributions can be explicitly given by interpolations over finite fields.

We emhasize that the specifying of a new non-Hamming metric on the space of codes and distributions is of crucial importance for our study. As soon as such the metric is introduced, the basic concepts and methods of the modern coding theory may be applied to uniform distributions. In the present paper this approach is illustrated by several general results.

Conceivable theory of uniform distributions may also work for error-correcting codes. Further studies of intimate linkages between the coding theory and uniform distributions should be exceptionally intriguing.

The reader interested in the fundamental aspects of the coding theory is refered to the encyclopaedic book MacWilliams and Sloane [17] and references therein.

We recall basic facts in theory of uniform distributions. For necessary details we refer to Beck and Chen [4], Kuipers and Niederreiter [12], and a recent book Matoušek [18].

Let $D \subset U^n$ be a distribution of finitely many points in the n-dimensional unit cube $U^n = [0,1)^n$. The L_∞-discrepancy $\mathcal{L}[D]$ is defined by

$$\mathcal{L}[D] = \sup_{Y \in U^n} |\#\{D \cap B(Y)\} - \#\{D\} \operatorname{vol} B(Y)|, \tag{1.1}$$

where $B(Y) = [0, y_1) \dots [0, y_n)$, $Y = (y_1, \dots, y_n) \in U^n$, are rectangular boxes in U^n, and $\operatorname{vol} B(Y) = y_1 \dots y_n$.

A main problem in theory of uniform distributions is the construction of distributions with minimal discrepancies (1.1). It is known that for each $N \geq 2$ there exist distributions $D_N \subset U^n$ consisting of N points with

$$\mathcal{L}[D_N] = O((\log N)^{n-1}), \tag{1.2}$$

where the implied constant depends only on n.

By a theorem of Roth for any distribution D_N of $N \geq 2$ points one has the following lower bound

$$\mathcal{L}[D_N] > c_n (\log N)^{\frac{1}{2}(n-1)}, \tag{1.3}$$

and by a theorem of Schmidt in two dimensions the bound (1.3) admits the following improvements

$$\mathcal{L}[D_N] > c \log N. \tag{1.4}$$

In (1.3) and (1.4) c_n and c are positive absolute constants independent of N.

Thus, in two dimensions the bound (1.2) is best possible. In dimensions $n > 2$ an exact minimal order of the discrepancy (1.1) still remains inaccessible. By [4, Sections 1.1 and 9.2] this is a "Great open problem" in theory of uniform distributions. See also Baker [2] and Beck [3] where certain improvements of the lower bound (1.3) for the discrepancy (1.1) are given in dimensions $n > 2$.

One of known approachs to the construction of distributions of low discrepancy can be outlined as follows. Fix a prime p and a prime power $q = p^e$, $e \in \mathbb{N}$. We write $\mathbb{N}$ for the set of natural numbers and $\mathbb{N}_0$ for the set of all non-negative integers. Introduce elementary boxes Δ_A^M by setting

$$\Delta_A^M = \left[\frac{m_1}{q^{a_1}}, \frac{m_1+1}{q^{a_1}}\right) \dots \left[\frac{m_n}{q^{a_n}}, \frac{m_n+1}{q^{a_n}}\right), \tag{1.5}$$

where $A = (a_1, \dots, a_n)$, $M = (m_1, \dots, m_n) \in \mathbb{N}_0^n$, and $m_j \in [0, q^{a_j})$, $1 \leq j \leq n$. We write $\mathbb{N}_0^n$ for the set of all vectors in $\mathbb{R}^n$ with non-negative integer coordinates. Notice that boxes (1.5) have volume

$$\operatorname{vol} \Delta_A^M = q^{-a_1 - \dots - a_n}. \tag{1.6}$$

Definition 1.1. *Given integers $0 \leq \delta \leq s$. A subset $D \subset U^n$ consisting of q^s points is called a (δ, s, n)-net of deficiency δ in base q if each elementary box Δ_A^M of volume $q^{\delta - s}$ contains exactly q^δ points of D.*

Obviously (δ, s, n)-nets fill out the unit cube U^n very uniformly. It is easily shown (cf. [4, Section 3.2] and [19, Section 3]) that the discrepancy $\mathcal{L}[D]$ of a (δ, s, n)-net D satisfies the bound

$$\mathcal{L}[D] = O(q^\delta s^{n-1}) = O(q^\delta (\log N)^{n-1}), \tag{1.7}$$

where $N = \#\{D\} = q^s$, and the implied contants in (1.7) depend only on n and q. Hence (δ, s, n)-nets of bounded deficiency δ satisfy the relation (1.2).

We mention the following simple corollary of definition 1.1 (cf. [22, Lemma 9]) which shows that the base p^e of a given net can be always reduced to p at the cost of an increase in deficiency.

Lemma 1.1. *Every (δ, s, n)-net in base p^e is a (δ', es, n)-net of deficiency $\delta' = e\delta + (e-1)(n-1)$ in base p.*

The first constructions of (δ, s, n)-nets were given by Sobol [28, 29] and Faure [11]. Namely, in an arbitrary dimension n for any $s \in \mathbb{N}$ (δ, s, n)-nets of deficiency $\delta = O(n \log n)$ in base 2 were constructed in [28, 29], and $(0, s, n)$-nets of zeroth deficiency in arbitrary prime base $p \geq n - 1$ were given in [11].

A systematic study of (δ, s, n)-nets (including nets in arbitrary integer bases $b \in \mathbb{N}$) was started by Niederreiter [19], see also a book [20] and a recent survey [21]. Among other things the following impressive result was recently obtained within the context of these studies. Niederreiter and Xing [22, 23] discovered that very good (δ, s, n)-nets of deficiency $\delta = O(n)$ can be constructed in terms of algebraic curves over finite fields. Moreover, for a given base q the bound $\delta = O(n)$ turns to be best possible as $n \to \infty$.

It was observed in Adams and Shader [1], Clayman and Mullen [8], Edel and Bierbrauer [10], and Lawrence *et al.* [13] that properties of (δ, s, n)-nets can be improved in some instances by error-correcting codes with large Hamining weights. The corresponding details and further references can also be found in the survey [23, Section 6].

It should be noted that (δ, s, n)-nets can be used to construct new remarkable classes of uniform distributions. For example, probabilistic variations of (δ, s, n)-nets were used in Chen [6] (see also [4, Section 3.4]) to determine exact minimal orders of the L_W-discrepancies for all $0 < W < \infty$.

Concerning alternative constructions of distributions of low discrepancy, we should mention the author's paper [24] (see also [25]) where methods of the geometry of numbers had been used. In a sense the approach given in the present paper is based on similar geometric ideas adapted for finite fields.

Main concepts of the geometry of numbers (like sphere packings, homogeneous and inhomogeneous minima, etc.) arranged for finite fields can be found in Conway and Sloane [9]. For general facts on geometry of vector spaces over finite fields we refer to Lang [14] and Lidl and Niederreiter [15].

In the present paper we study point sets of a special kind which are defined as follows. Introduce the following collection of elementary boxes (1.5)

$$\mathfrak{E}_s = \mathfrak{E}_s(q, n) = \{\Delta_A^M : A = (a_1, \dots, a_n),\ 0 \le a_j \le s,\ 1 \le j \le n\}. \tag{1.8}$$

Definition 1.2. *Given an integer $0 \le k \le n$. A subset $D \subset U^n$ consisting of q^{ks} points is called an optimum $[n, k, s]$-distribution in base q if each elementary box $\Delta_A^M \in \mathfrak{E}_s(q, n)$ of volume q^{-ks} contains exactly one point of D.*

A meaning of Definition 1.2 is to settle on a relation between the number of points in a given distribution and the magnitude of denominators in the definition of elementary boxes (1.5).

In the sequel an arbitrary subset $D \subset U^n$ consisting of q^{ks} points is conveniently said to be an *$[n, k, s]$-distribution in base q*.

The following result is a simple corollary of Definition 1.2.

Lemma 1.2. *Let $D \subset U^n$ be an optimum $[n, k, s]$ – distribution in base q. Then,*

(i) *Each elementary box $\Delta_A^M \in \mathfrak{E}_s(q, n)$ contains exactly $q^{ks - a_1 - \dots - a_n}$ points of D, provided that $a_1 + \dots + a_n \le ks$.*

(ii) *Each elementary box $\Delta_A^M \in \mathfrak{E}_s(q, n)$ contains at most one point of D, provided that $a_1 + \dots + a_n > ks$.*

Proof. (i) Choose integers $c_1, \dots, c_n$ to satisfy the relations $c_1 + \dots + c_n = ks - a_1 - \dots - a_n$, $0 \le c_j \le s$, $1 \le j \le n$. Let $b_j = a_j + c_j$, $1 \le j \le n$, then from (1.5) we obtain that

$$\Delta_A^M = \left[\frac{q^{c_1} m_1}{q^{b_1}}, \frac{q^{c_1} m_1 + q^{c_1}}{q^{b_1}}\right) \dots \left[\frac{q^{c_n} m_n}{q^{b_n}}, \frac{q^{c_n} m_n + q^{c_n}}{q^{b_n}}\right).$$

Hence, the box Δ_A^M is a union of disjoint elementary boxes $\Delta_B^T \in \mathfrak{E}_s(q, n)$ of volume q^{-ks}, and (i) follows from Definition 1.2.

(ii) It suffices to notice that each elementary box $\Delta_A^M \in \mathfrak{E}_s(q, n)$ with $a_1 + \dots + a_n > ks$ is contained in a bigger elementary box $\Delta_B^T \in \mathfrak{E}_s(q, n)$ of volume q^{-ks}, and (ii) follows from Definition 1.2. □

Now a linkage between optimum distributions and nets can be described as follows.

Proposition 1.1. *An optimum $[n,k,s]$-distribution is a $((k-1)s, ks, n)$-net in the same base q.*

Proof. It suffices to compare Lemma 1.2 (i) with Definition 1.1 and take into account that any elementary box Δ_A^M of volume q^{-s} belongs to the collection $\mathfrak{E}_s(q,n)$. □

From Proposition 1.1 and the bound (1.7) we conclude that the discrepancy $\mathcal{L}[D]$ of an optimum $[n,k,s]$-distribution D satisfies the bound

$$\mathcal{L}[D] = O(q^{(k-1)s}s^{n-1}) = O(N^{1-\frac{1}{k}}(\log N)^{n-1}), \tag{1.9}$$

where $N = \#\{D\} = q^{ks}$. Thus, optimum $[n,1,s]$ – distributions coinside with $(0,s,n)$-nets of zeroth deficiency and they satisfy the relation (1.2).

At first glance the foregoing implies that only optimum distributions with $k=1$ are of interest to theory of uniform distributions. However, such is not the case, and distributions with $k>1$ can also be used to construct new ones which already satisfy the relation (1.2). More precisely, from a given optimum $[gn,g,s]$-distribution $D \subset U^{gn}$, $g \in \mathbb{N}$, we can obtain a new optimum $[n,1,gs]$-distribution $\pi_{g,n}D \subset U^n$ by a mapping $\pi_{g,n} : U^{gn} \to U^n$ which is merely the known Peano's bijection between points of the unit cubes U^{gn} and U^n. Moreover, it turns out that the distributions $\pi_{g,n}D$ have additional intriguing properties. Concerning Peano's mappings, the reader is refered to any text-book on the elementary set theory.

The study of optimum $[n,k,s]$-distributions is a main goal of the present paper. Previously a part of our results was given in the author's paper [26].

The paper is organized as follows. Section 2 contains general results on distributions and their q-ary codes. Our main concepts of a non-Hamming metric ρ and maximum distance separable (or brifly MDS) codes in the metric ρ are introduced in Sec. 2.2 and Sec. 2.3, corresponding. Notice that by definition MDS codes consist of the most widely spaces code words.

A general theory of MDS codes in the Hamming metric $\varkappa$ is given in [16, Chapter 11]. Metrics different from the Hamming one, say, the Lee metric, are known in the coding theory and its applications (see [16]). It is an interesting question whether the non-Hamming metric ρ can be practically applied in concrete communication systems. Some artificial examples could be given at once. However, we do not consider this question in the paper, especially as the author does not hope to be an expert in the communication engineering.

In Sec. 2.3 optimum distributions are characterized completely in terms of their q-ary codes. We show that a given distribution is an optimum distribution if and only if its code is an MDS code in the metric ρ (see Theorem 2.1).

Section 3 contains explicit formulas for weight spectra of optimum distributions and MDS codes in the metric ρ (see Theorem 3.1). We emphasize that such formulas are fully inspired by the coding theory where similar results are well known for MDS codes in the Hamming metric (cf. [16, Chapter 11, Theorem 6]).

Explicit formulas for weight spectra are proved in Section 3 for arbitrary (linear or non-linear) MDS codes and optimum distributions. Furthermore, such formulas imply certain necessary conditions for the existence of MDS codes and optimum distributions (see Proposition 3.1).

Section 4 contains results on linear codes and distributions. An additional group structure of these subjects allows to apply the Fourier analysis on Abelian groups to study linear codes and distributions. Here this approach is illustrated by several results of a general character.

We define the duality with respect to an inner product on the space of codes and distributions (see Definition 4.2), and show that the dual subjects to linear MDS $[n,k,s]$-codes and optimum $[n,k,s]$-distributions are linear MDS $[n,n-k,s]$-codes, and correspondingly, optimum $[n,n-k,s]$-distributions (see Theorem 4.1).

In particular, linear optimum $[n, 1, s]$- and $[n, n-1, s]$-distributions are mutually dual. By the way, this confirms once more that the consideration of optimum $[n, k, s]$-distributions with $k > 1$ is of interest to us. It turns out that linear (δ, s, n)-nets can also be characterized completely in terms of weights of their dual subjects (see Theorem 4.2).

Furthermore, in Sec. 4.4 we shall take a quick look at generalized MacWilliams relations for weight enumerators in the metric ρ. However, an extended discussion of this matter is beyond the scope of the paper.

Section 5 contains explicit examples of linear MDS codes in the metric ρ and linear optimum distributions constructed by the Hermite interpolations over finite fields. A general theory of the Hermite interpolation problem over the field of complex numbers $\mathbb{C}$ can be found in Berezin and Zhidkov [5, Chapter 2, Section 11]. It should be pointed out that in the problem over finite fields we replace the usual formal derivatives by hyperderivatives introduced by Hasse and Teichmüller (see [15] and references therein). Such approach turns to be very convenient for calculations in fields of finite characteristic.

Constructions of MDS codes in the Hamming metric by interpolations are also known in the coding theory (see Mandelbaum [17]). From this standpoint our constructions of MDS codes in the metric ρ can be regarded as a suitable generalization of the known Reed–Solomon codes, or more generally, the redundant residue codes (see [16, Chapter 10]).

It was mentioned above that new algebraic-geometric constructions of very good (δ, s, n)-nets had been given by Niderreiter and Xing [22, 23]. In the spirit of our discussion of parallels between the coding theory and uniform distributions these constructions should be interpreted as the known Goppa codes adapted for the non-Hamming metric ρ. Concerning the Goppa codes and related topics we refer to [16, Chapter 2], Stichtenoth [29], and Tsfasman and Vlăduts [30]. Unfortunately, in the present paper we have to leave aside these extremely interesting questions.

Section 6 contains more specific results. Here we study the behavior of distributions under Peano's bijection $\pi_{g,n} : U^{gn} \to U^n$. It is worth noting that the reconstruction of codes and distributions by the mapping $\pi_{g,n}$ is also inspired by the coding theory, where reconstructions of a similar kind are known, say, for the so-called concatenated codes (cf. [16, Chapter 10]).

We show that for a given optimum $[gn, gk, s]$-distribution $D \subset U^{gn}$, $g \in \mathbb{N}$, the image $\pi_{g,n} D \subset U^n$ is an optimum $[n, k, gs]$-distributions. It turns out that the distribution $\pi_{g,n} D$ also has a large weight in the usual Hamming metric $\varkappa$ (see Propositions 6.1 and 6.3). We give explicit examples of codes and distributions with large weights simultaneously in both metrics ρ and $\varkappa$ (see Theorems 6.1 and 6.2). These questions are close related with a recent joint work of Chen and the author [7]. Conceivably the treatment of codes and distributions simultaneously in several different (or even in all possible) metrics should be of much interest to clarify the structure of these subjects.

The author hopes that the foregoing discussion could show the benefits of interactions between the coding theory and theory of uniform distributions.

Acknowledgments. I would like to express my sincere thanks to W. W. L. Chen, S. T. Dougherty, J. Matoušek, and H. Niederreiter for numerous discussions and valuable suggestions on the matter of the present paper.

2. Distributions and codes

2.1 Preliminaries.

Consider the q-ary representation of a point $x \in [0, 1)$,

$$x = \sum_{i \geq 1} \eta_i(x) q^{-i}, \quad \eta_i(x) \in \{0, 1, \ldots, q-1\}. \tag{2.1}$$

The representation (2.1) is uniquely defined if we argee that the series (2.1) is finite for rational q-ary points $x = \frac{m}{q^a}$, $a \in \mathbb{N}$, $m \in \{0, 1, \ldots, q^a - 1\}$. We write $\mathbb{Q}(q^s)$, $s \in \mathbb{N}$, for the set of all points $x = \frac{m}{q^a} \in [0, 1)$ with $a \leq s$, and $\mathbb{Q}^n(q^s)$ for the set of all points $X = (x_1, \ldots, x_n)^T \in U^n$ with coordinates $x_j \in \mathbb{Q}(q^s)$, $1 \leq j \leq s$. Here $(.)^T$ denotes the transpose of a matrix $(.)$.

For each $x \in [0, 1)$ we define a projection $\tau_s x$ onto $\mathbb{Q}(q^s)$ by

$$\tau_s x = \sum_{i=1}^{s} \eta_i(x) q^{-i}. \tag{2.2}$$

Obviously, we have

$$x - \tau_s x = \sum_{i \geq s+1} \eta_i(x) q^{-i} \in [0, q^{-s}). \tag{2.3}$$

Similarly, for each point $X = (x_1, \ldots, x_n)^T \in U^n$ we define a projection $\tau_s X$ onto $\mathbb{Q}^n(q^s)$ by

$$\tau_s X = (\tau_s x_1, \ldots, \tau_s x_n)^T. \tag{2.4}$$

Lemma 2.1. *Let $D \subset U^n$ be an optimum $[n, k, s]$-distribution, then its projection $\tau_s D \subset \mathbb{Q}^n(q^s)$ is also an optimum $[n, k, s]$-distribution.*

Proof. From the relations (2.2), (2.3), and (2.4) we conclude that a point X falls into an elementary box $\Delta_A^M \in \mathfrak{E}_s(q, n)$ if and only if its projection $\tau_s X$ does, and Lemma 2.1 follows at once from Definition 2.1. $\square$

Thus, without loss of generality, we may consider in the sequel only optimum $[n, k, s]$-distribution which are subsets in $\mathbb{Q}^n(q^s)$.

The representation (2.1) is convenient to write down in the form

$$x = \sum_{i=1}^{s} \xi_i(x) q^{i-s-1}, \tag{2.5}$$

where $\xi_i(x) = \eta_{s+1-i}(x)$.

The coefficients $\xi_i(x)$ in (2.5) can be identified with elements of a finite field. Let $\mathbb{F}_q$ be a finite field with $q = p^e$ elements. Fix a basis in $\mathbb{F}_q$ over $\mathbb{F}_p$, and represent elements $\mu = (\mu^{(1)}, \ldots, \mu^{(e)}) \in \mathbb{F}_q$ as e-term sets of elements $\mu^{(i)} \in \mathbb{F}_p$. In so doing, elements of the field $\mathbb{F}_p$ are thought of as reduced residues $\{0, 1, \ldots, p-1\}$ modulo p (see [15] for details). With these conventions we have the following bijection between elements $\mu \in \mathbb{F}_q$ and integers $m \in \{0, 1, \ldots, q-1\}$:

$$\mathbb{F}_q \ni \mu = (\mu^{(1)}, \ldots, \mu^{(e)}) \rightleftarrows m = \sum_{i=1}^{e} \mu^{(i)} p^{i-1} \in \{0, 1, \ldots, p-1\}. \tag{2.6}$$

By the use of the bijection (2.6), the coefficients $\xi_i(x)$ in (2.5) may be regarded as elements of the field $\mathbb{F}_q$, and therefore, a point $x \in \mathbb{Q}(q^s)$ can be identified with the following row matrix

$$\omega\langle x \rangle = \omega_q\langle x \rangle = (\xi_1(x), \ldots, \xi_s(x)) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q). \tag{2.7}$$

We write $\mathrm{Mat}_{n,s}(k)$ for the linear space of all matrices with n rows and s columns over a field k.

Using (2.7), we identify each point $X \in \mathbb{Q}^n(q^s)$ with the following matrix, the *code word* of X,

$$\Omega\langle X\rangle = (\omega(x_1), \dots , \omega(x_n))^T \in \mathrm{Mat}_{\,n,s}(\mathbb{F}_q). \tag{2.8}$$

For a given distribution $D \subset \mathbb{Q}^n(q^s)$ we define its code $\mathcal{C}\langle D\rangle \subset \mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$ as the following array of the corresponding code words (2.8):

$$\mathcal{C}\langle D\rangle = \{\Omega(X), X \in D\}. \tag{2.9}$$

Obviously, each subset $\mathcal{C} \subset \mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$ is the code (2.8) for a distribution $D = D\langle \mathcal{C}\rangle \subset \mathbb{Q}^n(q^s)$.

By the relations (2.5), (2.7), and (2.8) a structure of the vector space $\mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$ can be transfered onto the set of all rational q-ary points $\mathbb{Q}^n(q^s)$. Namely, for any two points $X = (x_1, \dots , x_n)^T$ and $Y = (y_1, \dots , y_n)^T \in \mathbb{Q}^n(q^s)$ and two elements α and $\beta \in \mathbb{F}_q$ we define a linear combination $\alpha X \oplus \beta Y = (\alpha x_1 \oplus \beta y_1, \dots , \alpha x_n \oplus \beta y_n)^T \in \mathbb{Q}^n(q^s)$ by setting

$$\xi_i(\alpha x_j \oplus \beta y_j) = \alpha\xi_i(x_j) + \beta\xi_i(y_i), \quad 1 \le i \le s, \quad 1 \le j \le n, \tag{2.10}$$

where $\xi_i(x) \in \mathbb{F}_q$ are coefficients in the representation (2.5).

With respect to the arithmetic operations (2.10) the set $\mathbb{Q}^n(q^s)$ is a vector space of dimension ns over $\mathbb{F}_q$.

We need to describe special affine subspaces (cf. [15, Chapter 3, Sec. 4]) in $\mathbb{Q}^n(q^s)$ associated with elementary boxes (1.5).

Lemma 2.2. *For each elementary box $\Delta^M_A \in \mathfrak{E}_s(q, n)$ the intersection $V^M_A = \mathbb{Q}^n(q^s) \cap \Delta^M_A$ is an affine subspace in $\mathbb{Q}^n(q^s)$ of dimension $ns-a_1-\dots-a_n$ parallel to the subspace $V^0_A = \mathbb{Q}^n(q^s) \cap \Delta^0_A$, that is, $V^M_A = V^0_A \oplus Y^M_A$, where a vector $Y^M_A \in \mathbb{Q}^n(q^s)$ is defined uniquely up to translations along V^0_A; in particular one may take $Y^M_A = \left(\frac{m_1}{q^{a_1}}, \dots , \frac{m_n}{q^{a_n}}\right)^T$.*

More precisely, the affine subspace V^M_A consists of points $X = (x_1, \dots , x_n)^T \in \mathbb{Q}^n(q^s)$ which satisfy the following system of $a_1 + \dots + a_n$ linear independent equations

$$\xi_i(x_j) = \xi_i\left(\frac{m_j}{q^{a_j}}\right), \quad s \ge i \ge s + 1 - a_j, \quad 1 \le j \le n, \tag{2.11}$$

where $\xi_i(.)$ are coefficients in the q-ary representation (2.5).

Proof. From the representation (2.1) we easily conclude that a point $x \in \mathbb{Q}(q^s)$ falls into an interval $\left[\frac{m}{q^a}, \frac{m+1}{q^a}\right)$, $a \in \mathbb{N}_0$, $0 \le a \le s$, $m \in \{0, 1, \dots , q^a - 1\}$, if and only if $\eta_i(x) = \eta_i\left(\frac{m}{q^a}\right)$ for $1 \le i \le a$. Writing these equations in terms of coefficients $\xi_i(.)$ in (2.5), and using the definition (1.8), we obtain (2.11). It is evident that the equations (2.11) imply all the other statements of Lemma 2.2. $\Box$

2.2. Definition of a non-Hamming metric.

We introduce the following non-Hamming *weight* ρ on the space $\mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$. At first, let $n = 1$ and $\omega = (\xi_1, \dots , \xi_s) \in \mathrm{Mat}_{\,1,s}(\mathbb{F}_q)$. Then we put $\rho(0) = 0$, and

$$\rho(\omega) = \rho_q(\omega) = \max\{j : \xi_j \ne 0\} \tag{2.12}$$

for $\omega \ne 0$.

Notice that in the sequel the base q is usually assumed to be fixed, and we drop it from our notation. Only in Sec. 6.4 we shall need to indicate the dependence on q in order to treat the variation of q from p^e to p.

It is obvious that $\rho(\omega) > 0$ for $\omega \neq 0$, $\rho(\alpha\omega) = \rho(\omega)$ for $\alpha \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, and

$$\rho(\omega + \omega') \leq \max\{\rho(\omega), \rho(\omega')\} \leq \rho(\omega) + \rho(\omega')$$

for all $\omega, \omega' \in \operatorname{Mat}_{1,s}(\mathbb{F}_q)$. Moreover, we have trivially that

$$\rho(\omega) \leq s \tag{2.13}$$

for all $\omega \in \operatorname{Mat}_{1,s}(\mathbb{F}_q)$.

Let $\Omega = (\omega^{(1)}, \dots, \omega^{(n)})^T \in \operatorname{Mat}_{n,s}(\mathbb{F}_q)$, $\omega^{(j)} \in \operatorname{Mat}_{1,s}(\mathbb{F}_q)$, $1 \leq j \leq n$. Then we put

$$\rho(\Omega) = \rho_q(\Omega) = \sum_{j=1}^{n} \rho(\omega^{(j)}). \tag{2.14}$$

For example, let $n = 2$, $s = 3$, and $\Omega = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, then $\rho(\Omega) = \rho((1\,1\,0)) + \rho((0\,0\,1)) = 2 + 3 = 5$.

Obviously, $\rho(\Omega) > 0$ for $\Omega \neq 0$, $\rho(\alpha\Omega) = \rho(\Omega)$ for $\alpha \in \mathbb{F}_q^*$, and

$$\rho(\Omega + \Omega') \leq \rho(\Omega) + \rho(\Omega')$$

for all Ω, $\Omega' \in \operatorname{Mat}_{n,s}(\mathbb{F}_q)$. Thus, $\rho(\Omega - \Omega')$ is a *metric* (or a *distance*) on the space $\operatorname{Mat}_{n,s}(\mathbb{F}_q)$.

Recall that by definition the *Hamming weight* $\varkappa(\Omega) = \varkappa_q(\Omega)$, $\Omega \in \operatorname{Mat}_{n,s}(\mathbb{F}_q)$ is equal to the number of non-zeroth entries in the matrix Ω (cf. [16]). It is easily seen that the weights $\varkappa$ and ρ are related by

$$\varkappa(\Omega) \leq \rho(\Omega) \leq s\varkappa(\Omega), \tag{2.15}$$

and these inequalities can not be improved on the whole space $\operatorname{Mat}_{n,s}(\mathbb{F}_q)$. In this sense the metric ρ is stronger than $\varkappa$ for large s.

Remark 2.1. In the special of $s = 1$ the metrics ρ and $\varkappa$ coinside. Hence, the results and methods of the present paper contain those for the Hamming metric $\varkappa$ as a specific case.

Remark 2.2. It should be of interest to determine all transformations preserving the metric ρ. Obviously, arbitrary permutations of rows of a matrix $\Omega \in \operatorname{Mat}_{n,s}(\mathbb{F}_q)$ preserve the weight $\rho(\Omega)$ (and the weight $\varkappa(\Omega)$ as well). Examples of another kind can be given as follows. Let $\omega = (\xi_1, \dots, \xi_s) \in \operatorname{Mat}_{1,s}(\mathbb{F}_q)$ and v be an arbitrary lower triangular s by s matrix over $\mathbb{F}_q$ with $\det v \neq 0$, then it is readily seen that $\rho(\omega v) = \rho(\omega)$. However, this is still a question whether or not the above transformations generate a full group of linear transformations preserving the weight ρ.

2.3. MDS codes in the metric ρ.

Given an arbitrary metric λ on the space $\operatorname{Mat}_{n,s}(\mathbb{F}_q)$. Using the relations (2.5), (2.7), and (2.8), the metric λ can be transfered onto the set of all rational q-ary points $\mathbb{Q}^n(q^s)$ by setting

$$\lambda(X) = \lambda(\Omega\langle X\rangle) \tag{2.16}$$

for the λ-weight of a point $X \in \mathbb{Q}^n(q^s)$, and

$$\lambda(X \ominus X') = \lambda(\Omega\langle X\rangle - \Omega\langle X'\rangle) \tag{2.17}$$

for the λ-distance between two points $X, X' \in \mathbb{Q}^n(q^s)$. In (2.17) the symbol $\ominus$ denotes the subtraction with respect to the addition $\oplus$, which was defined in (2.10).

For each code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, which is assumed to contain at least two elements, its *weight* $\lambda(\mathcal{C})$ is defined by

$$\lambda(\mathcal{C}) = \min\{\lambda(\Omega - \Omega') : \Omega, \Omega' \in \mathcal{C}, \Omega \neq \Omega'\} \tag{2.18}$$

Similarly, for each distribution $D \subset \mathbb{Q}^n(q^s)$, which contains at least two points, its *weight* $\lambda(D)$ is defined by

$$\lambda(D) = \min\{\lambda(X \ominus X') : X, X' \in D, X \neq X'\}. \tag{2.19}$$

It is obvious that $\lambda(D) = \lambda(\mathcal{C}\langle D\rangle)$ and $\lambda(\mathcal{C}) = \lambda(D\langle\mathcal{C}\rangle)$.

In the sequel λ is equal to either $\varkappa$ or ρ. So that, we write $\varkappa(\mathcal{C})$ and $\rho(\mathcal{C})$, and correspondingly $\varkappa(D)$ and $\rho(D)$, for the Hamming and non-Hamming weights of codes $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ and distributions $D \subset \mathbb{Q}^n(q^s)$.

The relations (2.15) imply the similar inequality for weights

$$\varkappa(C) \le \rho(C) \le s\varkappa(C), \quad \varkappa(D) \le \rho(D) \le s\varkappa(D). \tag{2.20}$$

Notice also that if a code or a distribution coincides with the whole space, then

$$\rho(\mathrm{Mat}_{n,s}(\mathbb{F}_q)) = \rho(\mathbb{Q}^n(q^s)) = 1. \tag{2.21}$$

These relations follow at once from the definitions (2.12), (2.14), and (2.18), (2.19).

Given an integer $1 \le k \le n$. An arbitrary code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ consisting of q^{ks} elements is conveniently said to be an $[n, k, s]$-*code*.

Proposition 2.1. *Every* $[n, k, s]$*-code satisfies the bound* $\rho(\mathcal{C}) \le (n-k)s + 1$.

Proof. For each integer $1 \le k \le n$ and $\Omega \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ we denote by $P_k\Omega$ a matrix whose first k rows coinside with first k rows of Ω and last $n-k$ rows are zeros. We have $\Omega = P_k\Omega + \Xi_k$ with a matrix Ξ_k whose first k rows are zeros, and the definition (2.14) implies

$$\rho(\Omega) = \rho(P_k\Omega) + \rho(\Xi_k). \tag{2.22}$$

From (2.13) and (2.14) we conclude that $\rho(\Xi_k) \le (n-k)s$. Hence, using (2.17) and (2.22), we obtain the inequality

$$\rho(\mathcal{C}) \le (n-k)s + \min\{\rho(P_k\Omega - P_k\Omega') : \Omega, \Omega' \in \mathcal{C}, \Omega \neq \Omega'\}. \tag{2.23}$$

Now we observe that cardinalities of the code $\mathcal{C}$ and the space $P_k\mathrm{Mat}_{n,s}(\mathbb{F}_q) = \mathrm{Mat}_{k,s}(\mathbb{F}_q)$ coinside and are equal to q^{ks}. Therefore, there are only two opportunities: either $P_k\Omega = P_k\Omega'$ for two distinct matrices $\Omega, \Omega' \in \mathcal{C}$, and in this case the second term at the right side of (2.23) is equal to 0, or $P_k\mathcal{C} = \mathrm{Mat}_{k,s}(\mathbb{F}_q)$, and in such case the second term at the right side of (2.24) is equal to 1 (cf. (2.21)). In both cases the bound in question holds. □

Proposition 2.1 leads immediately to the following.

Definition 2.1. *An $[n,k,s]$-code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ is called a maximum distance separable (or brifly MDS) $[n,k,s]$-code in the metric ρ if its weight $\rho(\mathcal{C}) = (n-k)s + 1$.*

It should be noted (cf. Remark 2.1) that for $s = 1$ Definition 2.1 coincides with a known definition of MDS codes in the Hamming metric (cf. [16, Chapter 11]).

2.4. Optimum distributions and MDS codes in the metric ρ.

Our first result on optimum distributions can be stated as follows.

Theorem 2.1. *Let $D \subset \mathbb{Q}^n(q^s)$ be a distribution and $\mathcal{C}\langle D\rangle \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ be its code* (2.9). *Then the following two statements are equivalent:*

(i) *D is an optimum $[n,k,s]$-distribution,*

(ii) *$\mathcal{C}\langle D\rangle$ is an MDS $[n,k,s]$-code in the metric ρ.*

For the proof of Theorem 2.1 we need the following.

Lemma 2.3. (i) *A given point $X \in \mathbb{Q}^n(q^s)$ falls into an elementary box $\Delta^0_A \in \mathfrak{E}_s(q,n)$ of volume q^{-ks} if and only if the weight $\rho(X) \le (n-k)s$.*

(ii) *Two given points $X, X' \in \mathbb{Q}^n(q^s)$ fall simultaneously into an elementary box $\Delta^M_A \in \mathfrak{E}_s(q,n)$ of volume q^{-ks} if and only if the distance $\rho(X \ominus X') \le (n-k)s$.*

Proof. First of all, we notice that the definition (2.11) and the representation (2.5) imply the inequality

$$x = \sum_{i=1}^{\rho(x)} \xi_i(x) q^{i-s-1} \le (q-1) \sum_{i=1}^{\rho(x)} q^{i-s-1} < q^{\rho(x)-s} \tag{2.24}$$

for all $x \in \mathbb{Q}(q^s)$ and the inequiality

$$x = \sum_{i=1}^{\rho(x)} \xi_i(x) q^{i-s-1} \ge q^{\rho(x)-s-1} \tag{2.25}$$

for $x > 0$, $x \in \mathbb{Q}(q^s)$.

(i) Let $\rho(X) \le (n-k)s$. Writing the inequality (2.24) for all coordinates of the point $X = (x_1, \dots, x_n)^T \in \mathbb{Q}^n(q^s)$ and using the definition (1.5), we conclude that $X \in \Delta^0_{A(X)}$ with $A(X) = (a_1(x_1), \dots, a_n(x_n))$ where $a_j(x_j) = s - \rho(x_j)$, $1 \le j \le n$. Therefore, we have (cf. (2.14), (2.17))

$$a_1(x_1) + \ldots + a_n(x_n) = ns - \rho(X) \ge ks,$$

and $0 \le a_j(x_j) \le s$, $1 \le j \le n$. Hence (cf. (1.6), (1.8)), there exists an elementary box $\Delta^0_A \in \mathfrak{E}_s(q,n)$ of volume q^{-ks} such that $\Delta^0_A \supseteq A^0_{A(X)} \ni X$.

Let $\rho(X) > (n-k)s$. Writing the inequality (2.25) for all non-zeroth coordinates of the point $X = (x_1, \dots, x_n)^T \in \mathbb{Q}^n(q^s)$ and using the definitions (1.5) and (1.8), we observe the following: if the point X falls into an elementary box $\Delta^0_A \in \mathfrak{E}_s(q,n)$ with $A = (a_1, \dots, a_n)$, then $0 \le a_j \le s - \rho(x_j)$ for $x_j > 0$ and $0 \le a_j \le s$ for $x_j = 0$, $1 \le j \le n$. Since $\rho(0) = 0$, we have

$$a_1 + \ldots + a_n \le ns - \rho(x_1) - \ldots - \rho(x_n) = ns - \rho(X) < ks.$$

Hence (cf. (1.6)), the elementary box $\Delta^0_A \in \mathfrak{E}_s(q,n)$ has volume strictly bigger than q^{-ks}.

The proof of the statement (i) is complete.

(ii) Since the distance $\rho(X \ominus X')$ is invariant under translations $X \to X \oplus Y$, $X' \to X' \oplus Y$, $Y \in \mathbb{Q}^n(q^s)$, the statement (ii) follows at once from the statement (i) with the help of Lemma 2.2. $\square$

Proof of Theorem 2.1. (i) Let D be an optimum $[n,k,s]$-distribution. Then, by Definition 1.2, each elementary box $\Delta_A^M \in \mathfrak{E}_s(q,n)$ of volume q^{-ks} contains exactly one point of D, and by Lemma 2.3 (ii), the distance $\rho(X \ominus X') > (n-k)s$ for any pair of distinct points X, $X' \in D$. Therefore, by Definition 2.1, $\mathcal{C}\langle D\rangle$ is an MDS $[n,k,s]$-code in the metric ρ.

(ii) Let $\mathcal{C}\langle D\rangle$ be an MDS $[n,k,s]$-code in the metric ρ. Then, by Definition 2.1, the distance $\rho(X \ominus X') > (n-k)s$ for any pair of distinct points $X, X' \in D$, and by Lemma 2.3 (ii), each elementary box $\Delta_A^M \in \mathfrak{E}_s(q,n)$ of volume q^{-ks} contains at most one point of D. Now we observe that for a given $A = (a_1, \dots, a_n) \in \mathbb{N}_0^n$ with $a_1 + \ldots + a_n = ks$ and $0 \le a_j \le s$, $1 \le j \le n$, the number of the corresponding elementary boxes $\Delta_A^M \in \mathfrak{E}_s(q,n)$ with $M = (m_1, \dots, m_n) \in \mathbb{N}_0^n$, $m_j \in \{0, 1, \dots, q^{a_j} - 1\}$, $1 \le j \le n$, is equal to q^{ks}, that coinsides with the cardinality of D. Therefore, each of these elementary boxes $\Delta_A^M \in \mathfrak{E}_s(q,n)$ of volume q^{-ks} contains exactly one point of D. Thus, D is an optimum $[n,k,s]$-distribution. $\square$

3. Weight spectra

3.1. Spheres and balls in the metric ρ.

Definition 3.1. *Given a code $\mathcal{C} \subset \operatorname{Mat}_{n,s}(\mathbb{F}_q)$. The following set of ns non-negative integers*

$$w_r(\Omega') = w_r(\mathcal{C}; \Omega') = \#\{\Omega \in \mathcal{C} : \rho(\Omega - \Omega') = r\}, \quad r \in \mathbb{N}_0, \quad 0 \le r \le ns, \tag{3.1}$$

is called the weight spectrum of the code $\mathcal{C}$ relatively to an element $\Omega' \in \mathcal{C}$. Similarly, for a distribution $D \subset \mathbb{Q}^n(q^s)$ the set of non-negative integers

$$w_r(X') = w_r(D; X') = \#\{X \in D : \rho(X \ominus X') = r\}, \quad r \in \mathbb{N}_0, \quad 0 \le r \le ns, \tag{3.2}$$

is called the weight spectrum of the distribution D relatively to a point $X' \in D$.

It is obvious that weight spectra of distributions and the corresponding codes coinside: $w_r(D; X') = w_r(\mathcal{C}\langle D\rangle; \Omega(X'))$.

A remarkable thing is that weight spectra of all MDS codes in the metric ρ as well as optimum distributions can be evaluated precisely. For MDS codes in the Hamming metric such results are well known in the coding theory (see [16, Chapter 11]).

Clearly, the weights (3.1) and (3.2) are equal to the number of elements $\Omega \in \mathcal{C}$ or points $X \in D$ lying on spheres in the metric ρ. Hence, we need to consider these geometric subjects closer. Here we consider only the space $\mathbb{Q}^n(q^s)$. Certainly, the corresponding definitions and results for the space $\operatorname{Mat}_{n,s}(\mathbb{F}_q)$ can easily be given as well.

Let

$$\mathfrak{S}(r) = \{X \in \mathbb{Q}^n(q^s) : \rho(X) = r\}, \quad 0 \le r \le ns, \tag{3.3}$$

be a sphere of radius $r \in \mathbb{N}_0$ in the metric ρ on the space $\mathbb{Q}^n(q^s)$.

Split the unit interval into union of the following $s+1$ subintervals

$$[0,1) = \bigcup_{0 \le b \le s} g_b, \tag{3.4}$$

where $g_0 = [0, q^{-s})$, $g_1 = [q^{-s}, q^{-s+1}), \dots, g_s = [q^{-1}, 1]$. Then, the unit cube splits into a union of the following $(s+1)^n$ disjoint boxes

$$U^n = \bigcup_B G_B, \quad G_B = \prod_{j=1}^n g_{b_j}, \tag{3.5}$$

where $B = (b_1, \dots, b_n) \in \mathbb{N}_0^n$, $0 \le b_j \le s$, $1 \le j \le n$. The boxes G_B are said to be *fragments*.

Lemma 3.1. *Each sphere* (3.3) *is a disjoint union of the following fragments*

$$\mathfrak{S}(r) = \bigcup_{b_1+\ldots+b_n=r} G_B. \tag{3.6}$$

Proof. Comparing the q-ary representation (2.5) with the definitions of the ρ-weight (2.11) and subintervals g_b in (3.4), we observe the following: a point $x \in \mathbb{Q}(q^s)$ belongs to a subinterval g_b if and obly if its weight $\rho(x) = b$. Thus, a point $X = (x_1, \ldots, x_n)^T \in \mathbb{Q}^n(q^s)$ falls into a sphere $\mathfrak{S}(r)$ if and only if X belongs to one of fragments G_B with $b_1 + \ldots + b_n = r$. □

For a given integer vector $B = (b_1, \ldots, b_n) \in \mathbb{N}_0^n$ we denote by $\varkappa(B)$ the number of non-zero coordinates b_j, $1 \leq j \leq n$, thus, $\varkappa(B)$ is equal to the Hamming weight of the vector B. Consider a subset $\mathfrak{S}_l(r) \subset \mathfrak{S}(r)$ consistings of fragments $G_B \subset \mathfrak{S}(r)$ with $\varkappa(B) = l$,

$$\mathfrak{S}_l(r) = \bigcup_{\substack{b_1+\ldots+b_n=r,\\ \varkappa(B)=l}} G_B, \quad l \in \mathbb{N}_0, \quad 0 \leq l \leq ns. \tag{3.7}$$

From (3.6) and (3.7) we obtain that

$$\mathfrak{S}(r) = \bigcup_{0 \leq l \leq n} \mathfrak{S}_l(r). \tag{3.8}$$

Certainly, some of subsets $\mathfrak{S}_l(r)$ in (3.8) may be empty.

We introduce non-negative integers $\sigma_s(l, r)$, $r \in \mathbb{N}_0$, $l \in \mathbb{N}_0$, $0 \leq l \leq ns$, by setting

$$\sigma_s(l, r) = \#\{A = (a_1, \ldots, a_l) \in \mathbb{N}^l : a_1 + \ldots + a_l = r, \, 0 < a_j \leq s, 1 \leq j \leq l\} \tag{3.9}$$

for $l \geq 1$, for $l = 0$ we put $\sigma_s(0, 0) = 1$ and $\sigma_s(0, r) = 0$ for $r \geq 1$. In particular, for $s = 1$ we have

$$\sigma_1(l, r) = \delta_{l,r}, \tag{3.10}$$

where $\delta_{l,r}$ is the Kronecker symbol.

Moreover, by elementary arguments from the lattice point counting, we obtain the following asymptotics

$$\sigma_s(l, st + c) = \sqrt{l}\, v(l, t) s^{l-1} + O(s^{l-2}) \tag{3.11}$$

as $s \to \infty$. In (3.11) $1 \leq t \leq l-1$, $c \in \mathbb{N}$ are integers, and $v(l, t)$ is the $(l-1)$-dimensional volume of a section of the l-dimensional unit cube U^l by the hyperplane $x_1 + \ldots + x_l = t$. It is evident that $v(l, t) > 0$.

We write $\binom{n}{i}$ for the usual binomial coeffcients, moreover, $\binom{n}{i} = 0$ for $i > n$.

Lemma 3.2. *For each subset* $\mathfrak{S}_l(r)$ *the number of fragments* G_B *in the union* (3.7) *is equal to* $\binom{n}{l} \sigma_s(l, r)$.

Proof. Let $l = 0$. Then, there is only one fragment $G_B = G_0 = [0, q^{-s})^n$ with $\varkappa(B) = 0$. It is obvious that the fragment G_0 is present in the union (3.7) only for $t = 0$. This proves Lemma 3.2 for $l = 0$.

Let $l \geq 1$. Consider one of $\binom{n}{l}$ possible choices of l indices $J = \{j_1, \dots, j_l\} \subset \{1, \dots, n\}$. It is obvious (cf. Lemma 3.1) that the numbers of fragments $G_B \subset \mathfrak{S}_l(r)$ with such B that $0 < b_j \leq s$ for $j \in J$ and $b_j = 0$ for $j \notin J$ is equal to $\sigma_s(l, t)$. This prives Lemma 3.2 for $l \geq 1$. $\square$

Using Lemma 3.2 and the representations (3.7) and (3.8), we can easily evaluate the number of points $X \in \mathbb{Q}^n(q^s)$ lying on a sphere $\mathfrak{S}(r)$. First of all, we notice that

$$\#\{\mathbb{Q}(q^s) \cap g_i\} = \begin{cases} 1 & \text{if} \quad i = 0, \\ (q-1)q^{i-1} & \text{if} \quad i = 1, \dots, s. \end{cases}$$

Now, from (3.5) we conclude that

$$\#\{\mathbb{Q}^n(q^s) \cap G_B\} = (q-1)^{\varkappa(B)} q^{b_1 + \ldots + b_n - \varkappa(B)}.$$

Therefore, using Lemma 3.2 and (3.7), (3.8), we obtain the relation

$$\#\{\mathbb{Q}^n(q^s) \cap \mathfrak{S}(r)\} = \sum_{l=0}^{n} \binom{n}{l} \sigma_s(l, r)(q-1)^l q^{r-l}. \tag{3.12}$$

Notice that the terms with $l > r$ are absent in (3.10), because $\sigma_s(l, r) = 0$ if $l > r$ (cf. (3.9)).

Let

$$\mathfrak{B}(t) = \{X \in \mathbb{Q}^n(q^s) : \rho(X) \leq t\} \tag{3.13}$$

be a ball of radius $t \in \mathbb{N}_0$ in the metric ρ. It is obvious that

$$\mathfrak{B}(t) = \bigcup_{0 \leq r \leq t} \mathfrak{S}(r). \tag{3.14}$$

Let $D \subset \mathbb{Q}^n(q^s)$ be a distribution of N points. Assume that its weight $\rho(D) \geq 2t + 1$, $t \in \mathbb{N}_0$ (see (2.20)). Then the balls $\{\mathfrak{B}(t) \oplus X, X \in D\}$ are pairwise disjoint. This observation together with the relations (3.12), (3.13), and (3.14) implies the following *ball packing bound*

$$N \sum_{r=0}^{t} \sum_{l=0}^{n} \binom{n}{l} \sigma_s(l, t)(q-1)^l q^{t-l} \leq q^{ns}. \tag{3.15}$$

In view of (3.10) the relation (3.15) for $s = 1$ coinsides with the well know Hamming bound for usual codes (cf. [9, 15, 16]). In a similar spirit known results of the coding theory (like the Elias and Plotkin bounds) can be also given with respect to the metric ρ. In connection with this, we should mention a very interesting combinatorial problem on the description of *perfect distributions* $D \subset \mathbb{Q}^n(q^s)$ (and the corresponding *perfect codes* $\mathcal{C}\langle D\rangle \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$) in metric ρ which provide exact close-packings (without gaps and overlappings) of the space $\mathbb{Q}^n(q^s)$ by balls $\{\mathfrak{B}(t) \oplus X, X \in D\}$ or spheres $\{\mathfrak{S}(r) \oplus X, X \in D\}$. However, in the present paper we shall not consider these questions closer.

The following result gives a description of balls (3.13) in terms of elementary boxes (1.5).

Lemma 3.3. *Each ball* (3.13) *is a union of the following elementary boxes* (1.5) *from the collection* (1.8)

$$\mathfrak{B}(t) = \bigcup_{a_1+\ldots+a_n=t} \Delta^0_{A^*}, \tag{3.16}$$

where $A^* = (a_1^*, \ldots, a_n^*)$ *with* $a_j^* = s - a_j$, $0 \le a_j \le s$, $1 \le j \le n$.

Proof. Our arguments here are quite similar to those in the proof of Lemma 2.3. Let $X \in \mathfrak{B}(t)$. Writing the inequality (2.24) for all coordinates of the point X, we conclude that $X \in \Delta^0_{A(X)}$ with $A(X) = (a_1(x_1), \ldots, a_n(x_n))$ where $a_j(x_j) = s - \rho(x_j)$, $1 \le j \le n$, and $\rho(x_1) + \ldots + \rho(x_n) = \rho(X) \le t$. Hence, there exists an elementary box Δ^0_A in the union (3.16) such that $\Delta^0_A \supseteq \Delta^0_{A(X)} \ni X$.

Let $X \notin \mathfrak{B}(t)$, that is, $\rho(X) > t$. Writing the inequalities (2.13) and (2.25) correspondingly for zeroth and non-zeroth coordinates of the point X, we observe the following: if the point X falls into an elementary box $\Delta^0_{A^*} \in \mathfrak{E}_s(q, n)$ with $A^* = (a_1^*, \ldots, a_n^*)$ and $a_j^* = s - a_j$, $0 \le a_j \le s$, $1 \le j \le n$, then $\rho(x_j) \le a_j \le s$, $1 \le j \le n$. Therefore, we have $a_1 + \ldots + a_n \ge \rho(X) > t$, and hence, the elementary box $\Delta^0_{A^*}$ does not belong to the union (3.16). $\square$

3.2. Weight spectra of MDS codes and optimum distributions.

Our main result on weight spectra can be stated as follows.

Theorem 3.1. *Let* $D \subset \mathbb{Q}^n(q^s)$ *be an optimum* $[n, k, s]$*-distribution and* $\mathcal{C} = C\langle D\rangle$ *the corresponding MDS* $[n, k, s]$*-code in the metric* ρ. *Then weights* (3.1) *and* (3.2) *are independent of elements* $\Omega' \in \mathcal{C}$ *and points* $X' \in D$, *and* $w_r = w_r(\Omega') = w_r(X')$ *are given by*

$$w_0 = 1, \quad w_r = 0 \tag{3.17}$$

for $0 \le r < \rho(\mathcal{C}) = (n-k)s + 1$, *and*

$$w_r = \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l, r) \sum_{t=0}^{r-\rho(\mathcal{C})} (-1)^t \binom{l}{t} (q^{r-\rho(\mathcal{C})+1-t} - 1)$$

$$= (q-1) \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l, r) \sum_{t=0}^{r-\rho(\mathcal{C})} (-1)^t \binom{l-1}{t} q^{r-\rho(\mathcal{C})-t} \tag{3.18}$$

for $\rho(\mathcal{C}) \le t \le ns$.

We wish to discuss some corollaries of Theorem 3.1. First of all, we notice that in view of (3.10) the relations (3.18) for $s = 1$ imply

$$w_r = \sum_{t=0}^{r-\rho(\mathcal{C})} (-1)^t \binom{l}{t} (q^{r-\rho(\mathcal{C})+1-t} - 1)$$

$$= (q-1) \sum_{t=0}^{r-\rho(\mathcal{C})} (-1)^t \binom{l-1}{t} q^{r-\rho(\mathcal{C})-t}.$$

These relations coinside with known identities (cf. [16, Chapter 11, Theorem 6]) for weight spectra of MDS codes in the Hamming metric (see Remark 2.1).

Now we consider the special case of $k = 1$. Introduce the following positive integers

$$\tilde{\sigma}_s(n, r) = \#\{A = (a_1, \ldots, a_n) \in \mathbb{N}_0^n : a_1 + \ldots + a_n = r,\ 0 \le a_j \le s,\ 1 \le j \le n\}. \tag{3.19}$$

Comparing the definitions (3.9) and (3.19), we immediately obtain the relation

$$\tilde{\sigma}_s(n, r) = \sum_{l=1}^{n} \binom{n}{l} \sigma_s(l, r), \quad r \ge 1. \tag{3.20}$$

Theorem 3.1 implies the following result.

Theorem 3.2. *Let D be an optimum $[n, 1, s]$-distribution or, that is the same (cf. Proposition 1.1), a $(0, s, n)$-net. Then weights (3.2) are given by*

$$w_0 = 1, \quad w_r = 0 \tag{3.21}$$

for $0 \le r < \rho(D) = (n-1)s + 1$, and

$$\begin{aligned} w_r &= \tilde{\sigma}_s(n, r) \sum_{t=0}^{r-\rho(D)} (-1)^t \binom{n}{t} (q^{r-\rho(D)+1-t} - 1) \\ &= \tilde{\sigma}_s(n, r)(q-1) \sum_{t=0}^{r-\rho(D)} (1-1)^t \binom{n-1}{t} q^{r-\rho(D)-t} \end{aligned} \tag{3.22}$$

for $\rho(D) \le r \le ns$. In particular,

$$w_r = \tilde{\sigma}_s(n, r)(q-1)^n q^{r-\rho(D)-n+1} \tag{3.23}$$

for $\rho(D) + n - 1 \le r \le ns$.

Proof. Evidently, the relations (3.17) imply (3.21). Let $\rho(D) = (n-1)s + 1 \le r \le ns$, then $\sigma_s(l, r) = 0$ for $1 \le l \le n-1$ and $\sigma_s(n, r) = \tilde{\sigma}_s(n, r)$ (see (3.9), (3.19), and (3.20)). Hence, the relations (3.18) imply (3.22). Finally, the relations (3.23) follow at once from (3.22), because, for $\rho(D) + n - 1 \le r \le ns$ the summation in (3.22) is taken over all indeces $0 \le t \le n-1$. □

By definition weights (3.1) and (3.2) are non-negative. Together with Theorem 3.1 and 3.2 this leads to a series of necessary conditions for the existence of optimum distributions and MDS codes. From the relation (3.17) we find first non-trivial terms in the weight spectrum

$$w_{\rho(D)} = \tilde{\sigma}_s(n, \rho(D))(q-1), \tag{3.24}$$

and

$$w_{\rho(D)+1} = (q-1) \sum_{l=1}^{n} \binom{n}{l} (q+1-l) \sigma_s(l, \rho(D)+1). \tag{3.25}$$

Notice that the relation (3.20) has been used in (3.24). Moreover, writing the relation (3.25), we assume that $\rho(D) + 1 \le ns$; this means that $s > 1$ if $k = 1$.

For $k = 1$ the relation (3.25) takes the form

$$w_{\rho(D)+1} = (q-1)\sigma_s(\rho(D)+1)(q-n+1). \tag{3.26}$$

Since the weight (3.26) is non-negative, we obtain the following necessary condition for the existence of $[n, 1, s]$-optimum distributions:

$$q \ge n - 1. \tag{3.27}$$

For $(0, n, s)$-nets the condition (3.27) is well known (cf. [4, Lemma 3.28] and [19, Corollary 5.11]). The above arguments can be considered as an interpretation of the condition (3.27) in terms of weight spectra.

From the relation (3.25) we can also derive the following general result.

Proposition 3.1. *Suppose that for given $1 \leq k \leq n-1$ and an infinite sequence of $s \in \mathbb{N}$ there exist optimum $[n,k,s]$-distributions or, that is the same, MDS $[n,k,s]$-codes in the metric ρ. Then the condition* (3.27) *holds.*

Proof. Substituting the asymptotics (3.11) to the relation (3.25), we find that

$$(q-1)(q+1-n)\sqrt{n}\, v(n,n-k)s^{n-1} + O(s^{n-2}) \geq 0, \quad s \to \infty,$$

with the constant $v(n,n-k) > 0$, and the inequality (3.27) follows. □

Remark 3.1. For given $1 \leq k \leq n-1$, $q \geq n-1$ and arbitrary $s \in \mathbb{N}$ optimum $[n,k,s]$-distributions will be explicitly constructed in Section 5 (see Theorem 5.2 below). Hence, the condition (3.27) is actually necessary and sufficient for the existence of infinite sequences of optimum distributions and MDS codes.

3.3. Proof of Theorem 3.1.

First of all, we notice that Theorem 3.1 may be proved only for optimum distribution, because a given MDS $[n,k,s]$-code $= \mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ can be identified with the corresponding optimum $[n,k,s]$-distribution $D = D\langle\mathcal{C}\rangle \subset \mathbb{Q}^n(q^s)$ by Theorem 2.1.

Next, from Definition 2.1 and Theorem 2.1 we conclude that if $D \subset \mathbb{Q}^n(q^s)$ is an optimum $[n,k,s]$-distribution, then so is any distribution $D \oplus X'$ shifted by an arbitrary vector $X' \in \mathbb{Q}^n(q^s)$. Thus, without loss of generality, in proving of Theorem 3.1 we may assume that $0 \in D$ and consider the weight spectrum (3.2) only relatively to the origin $X' = 0$. In so doing, we put $w_r = w_r(0)$.

Notice also that the relations (3.17) hold trivially, in view of Definition 2.1 and Theorem 2.1. Thus, we have to consider only weights w_r with $r \geq \rho(D) = (n-k)s+1$.

With the above conventions we turn to the proof of the relations (3.18). From Lemma 3.1 we obtain the relation

$$w_r = \#\{D \cap \mathfrak{S}(r)\} = \sum_{b_1+\ldots+b_n=r} \#\{D \cap G_B\}. \tag{3.28}$$

Consider a fragment G_B, $B = (b_1,\ldots,b_n)$, in (3.28) with $\varkappa(B) = l \geq 1$. Notice that a fragment G_B with $\varkappa(B) = 0$ is absent in (3.28) since $r > 0$. Suppose that $b_j \neq 0$ $(0 < b_j \leq s)$ for $j \in J$ and $b_j = 0$ for $j \notin J$, where $J = \{j_1,\ldots,j_l\} =\subseteq \{1,\ldots,n\}$ is a subset of l undices. Using (3.4), (3.5), we conclude that the fragment G_B has the following representations in terms of elementary boxes (1.5)

$$G_B = \Delta^0_{A_0} \setminus \bigcup_{i\in J} \Delta^0_{A_i}, \tag{3.29}$$

where $A_0 = (a_1^{(0)},\ldots,a_n^{(0)})$ with

$$a_j = s - b_j, \quad 1 \leq j \leq n, \tag{3.30}$$

and $A_i = (a_1^{(i)},\ldots,a_n^{(i)})$ with

$$a_j^{(i)} = \begin{cases} s & \text{if} \quad j \notin J, \\ s - b_j & \text{if} \quad j \in J \quad \text{and} \quad j \neq i, \\ s - b_i + 1 & \text{if} \quad j \in J \quad \text{and} \quad j = i. \end{cases} \tag{3.31}$$

Obviously, we have the equality

$$a_1^{(0)} + \ldots + a_n^{(0)} = ns - b_1 - \ldots - b_n = ns - r. \tag{3.32}$$

Let $I = \{i_1, \ldots, i_t\} \subset J = \{j_1, \ldots, j_l\}$ be a subset of t indices. Then,

$$\Delta^0_{A_{i_1}} \cap \ldots \cap \Delta^0_{A_{i_t}} = \Delta^0_{A_I}, \tag{33}$$

where $A_I = (a_1^{(I)}, \ldots, a_n^{(I)})$ with

$$a_j^{(I)} = \max\{a_j^{(i_1)}, \ldots, a_j^{(i_t)}\} = \begin{cases} s - b_j & \text{if} \quad j \notin I, \\ s - b_j + 1 & \text{if} \quad j \in I. \end{cases} \tag{3.34}$$

Notice that the relations (3.31) have been used in (3.34). Obviously, we have the equality

$$a_1^{(I)} + \ldots + a_n^{(I)} = ns - r + l. \tag{3.35}$$

Applying the principle of inclusion and exclusion to the summand $\#\{D \cap G_B\}$ in (3.28), and using the relations (3.29), (3.32), we obtain the formula

$$\#\{D \cap G_B\} = \{D \cap \Delta^0_{A_0}\} - \sum_{t=1}^{l} \sum_{\substack{I \subset J, \\ \#\{I\}=t}} (-1)^t \#\{D \cap \Delta^0_{A_I}\}, \tag{3.36}$$

where the inner sum is taken over all $\binom{l}{t}$ subsets $I = \{i_1, \ldots, i_t\} \subseteq J = \{j_1, \ldots, j_l\}$ of t indices.

From the relations (3.30) and (3.34) we conclude that all elementary boxes $\Delta^0_{A_0}$ and $\Delta^0_{A_I}$ in (3.36) belong to the collection (1.8). Now we observe the following. Let an elementary box $A^0_A \in \mathfrak{E}_s(q, n)$, then

$$\#\{D \cap \Delta^0_A\} = \begin{cases} q^{s-a_1-\ldots-a_n} & \text{if} \quad a_1 + \ldots + a_n < ks, \\ 1 & \text{if} \quad a_1 + \ldots + a_n \geq ks. \end{cases} \tag{3.37}$$

The first equality in (3.37) follows from Lemma 1.2 (i), and the second follows from Lemma 1.2 (ii) and the above assumption that $0 \in D$.

Substituting (3.37) to (3.36), and using (3.32) and (3.35), we find that

$$\#\{D \cap G_B\} = \sum_{t=0}^{r-(n-k)s-1} (-1)^t \binom{l}{t} q^{r-(n-k)s-t} + \sum_{t=r-(n-k)s}^{l} (-1)^t \binom{l}{t}$$

$$= \sum_{t=0}^{r-\rho(D)} (-1)^T \binom{l}{t} (q^{r-\rho(D)+1-t} - 1) = (q-1) \sum_{t=0}^{r-\rho(D)} (-1)^t \binom{l-1}{t} q^{r-\rho(D)-t}. \tag{3.38}$$

Notice that the well know identities for binomial coefficients $\sum_{t=0}^{l} (-1)^t \binom{l}{t} = 0$ and $\binom{l}{t} = \binom{l-1}{t} + \binom{l-1}{t-1}$ have been used in the calculation (3.38).

The relation (3.28) can be written down in the form

$$w_r = \sum_{l=1}^{n} \sum_{B:\varkappa(B)=l} \#\{D \cap G_B\}, \tag{3.39}$$

where the inner sum is taken over all fragments $G_B \subset \mathfrak{S}(r)$ with $\varkappa(B) = l$. The number of such fragments is equal to $\binom{l}{t} \sigma_s(l, r)$ by Lemma 3.2.

Substituting (3.38) to (3.39), we obtain the relation in question (3.28).

The proof of Theorem 3.1 is complete. □

4. Linear codes and distributions

4.1. Duality for codes and distributions.

Definition 4.1. *A subset $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ is called a linear code if $\mathcal{C}$ is a subspace in $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Similarly, a subset $D \subset \mathbb{Q}^n(q^s)$ is called a linear distribution if D is a subspace in the vector space $\mathbb{Q}^n(q^s)$ over $\mathbb{F}_q$ with respect to the arithmetic operations* (2.10).

For linear codes and distributions the definitions of their weights (2.17) and (2.18) take the form

$$\lambda(\mathcal{C}) = \min\{\lambda(\Omega) : \Omega \in \mathcal{C} \setminus \{0\}\}, \quad \lambda(D) = \min\{\lambda(X) : X \in D \setminus \{0\}\}, \tag{4.1}$$

where λ is one of the metrices $\varkappa$ or ρ.

Notice that the relations (4.1) are quite similar to the known definition of the homogeneous minimum of a lattice in Euclidean spaces (cf. [9] and [16]).

We introduce the following *inner product* $\langle \cdot, \cdot \rangle$ on the space $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. At first, let $n = 1$ and $\omega_1 = (\xi'_1, \dots, \xi'_s)$, $\omega_2 = (\xi''_1, \dots, \xi''_s) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, then we put

$$\langle \omega_1, \omega_2 \rangle = \langle \omega_2, \omega_1 \rangle = \sum_{i=1}^{s} \xi'_i \xi''_{s+1-i}. \tag{4.2}$$

Now, let $\Omega_i = (\omega_i^{(1)}, \dots, \omega_i^{(n)})^T \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, $i = 1, 2$, where $\omega_i^{(j)} \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, $1 \le j \le n$. Then we put

$$\langle \Omega_1, \Omega_2 \rangle = \langle \Omega_2, \Omega_1 \rangle = \sum_{j=1}^{n} \langle \omega_1^{(j)}, \omega_2^{(j)} \rangle. \tag{4.3}$$

Certainly, instead of (4.2) we should write the inner product in a common form $(\omega_1, \omega_2) = \xi'_1 \xi''_1 + \ldots + \xi'_s \xi''_s$. In doing so, $(\omega_1, \omega_2) = \langle \omega_1, \Phi_0 \omega_2 \rangle$ with a non-singular s by s matrix Φ_0 over $\mathbb{F}_q$. Recall that an arbitrary non-singular bilinear form $\Phi(\omega_1, \omega_2) = \langle \omega_1, \Phi\omega_2 \rangle$, $\det \Phi \neq 0$, could be used as an appropriate inner product on the space $\mathrm{Mat}_{1,n}(\mathbb{F}_q) \simeq \mathbb{F}_q^n$ (cf. [14, Chapters 13, 14]). The definition (4.2) is preferable here, because otherwise, the matrix Φ would be involved in all subsequent considerations.

Using the relation (2.8), we can transfer the inner product (4.3) onto the vector space of rational q-ary points $\mathbb{Q}^n(q^s)$ by setting

$$\langle X_1, X_2 \rangle = \langle \Omega(X_1), \Omega(X_2) \rangle, \quad X_1, X_2 \in \mathbb{Q}^n(q^s). \tag{4.4}$$

Definition 4.2. *Given a linear code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Then the dual code $\mathcal{C}^{\perp} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ is defined by*

$$\mathcal{C}^{\perp} = \{\Omega_2 \in \mathrm{Mat}_{n,s}(\mathbb{F}_q) : \langle \Omega_1, \Omega_2 \rangle = 0 \quad \textit{for all} \quad \Omega_1 \in \mathcal{C}\}. \tag{4.5}$$

Similarly, for a given linear distribution $D \subset \mathbb{Q}^n(q^s)$ the dual distribution $D^{\perp} \subset \mathbb{Q}^n(q^s)$ is defined by

$$D^{\perp} = \{X_2 \in \mathbb{Q}^n(q^s) : \langle X_1, X_2 \rangle = 0 \quad \textit{for all} \quad X_1 \in D\}. \tag{4.6}$$

The following simple corollaries of Definition 4.2 should be mentioned. Dual codes (4.5) and distributions (4.6) are also linear subspaces. Moreover,

$$(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}, \quad (D^{\perp})^{\perp} = D, \tag{4.7}$$

and (cf. (2.9))

$$\mathcal{C}\langle D^{\perp}\rangle = (\mathcal{C}\langle D\rangle)^{\perp}, \quad D\langle \mathcal{C}^{\perp}\rangle = (D\langle \mathcal{C}\rangle)^{\perp}. \tag{4.8}$$

Thus, in view of (4.7), linear codes $C, C^{\perp} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ and distributions $D, D^{\perp} \subset \mathbb{Q}^n(q^s)$ are pairs of mutually dual subspaces.

Let $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ and $D \subset \mathbb{Q}^n(q^s)$ be subspaces of dimension d, then $\mathcal{C}^{\perp}$ and $D^{\perp}$ are subspaces of dimention $d^{\perp} = ns - d$. This implies in passing the following relations for their cardinalities

$$\#\{\mathcal{C}\} = \#\{D\} = q^d, \quad \#\{\mathcal{C}^{\perp}\} = \#\{D^{\perp}\} = q^{d^{\perp}}, \tag{4.9}$$

and

$$\#\{\mathcal{C}\}\#\{\mathcal{C}^{\perp}\} = \#\{D\}\#\{D^{\perp}\} = q^{ns}. \tag{4.10}$$

Furthermore, let $\mathcal{C}$ and D be linear an $[n,k,s]$-code and, correspondingly, an $[n,k,s]$-distribution, then $\mathcal{C}^{\perp}$ and $D^{\perp}$ are linear an $[n, n-k, s]$-code and, correspondingly, $[n, n-k, s]$-distribution.

Our results on metric properties of mutually dual codes and distributions can be stated as follows.

Theorem 4.1. (i) *Let $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ be a linear MDS $[n,k,s]$-code in the metric ρ. Then $\mathcal{C}^{\perp}$ is a linear MDS $[n, n-k, s]$-code in the metric ρ.*

(ii) *Let $D \subset \mathbb{Q}^n(q^s)$ be a linear optimum $[n,k,s]$-distribution. Then $D^{\perp}$ is a linear optimum $[n, n-k, s]$-distribution.*

It is notable that linear (δ, n, s)-nets (cf. Definition 1.1) can also be characterized completely in terms of their dual distributions.

Theorem 4.2. *Let D, $D^{\perp} \subset \mathbb{Q}^n)q^s)$ be mutually dual distributions. Then the following two statements are equivalent:*

(i) *D is a (δ, n, s)-net of deficiency δ,*

(ii) *$D^{\perp}$ has a weight $\rho(D^{\perp}) \geq (n-1)s + 1 - \delta$.*

It should be noted that the statements of Theorem 4.1 for $k = 1$ and Theorem 4.2 for $\delta = 0$ actually coincide (cf. Proposition 1.1 and Theorem 2.1).

For the proof of Theorems 4.1 and 4.2 we need to recall some known facts about the Fourier transform on vector spaces over finite fields. For details we refer to [15] and [16]. Notice also that the necessary facts are given here in the form adapted to the vector spaces $\mathbb{Q}^n(q^s)$.

4.2. Fourier transform on the space of distributions.

Introduce a function $\Psi(X_1, X_2)$, $X_1, X_2 \in \mathbb{Q}^n(q^s)$, by setting

$$\Psi(X_1, X_2) = \exp\left(2\pi\sqrt{-1}\frac{1}{p}\operatorname{Tr}\langle X_1, X_2\rangle\right), \tag{4.11}$$

where we write $\operatorname{Tr}\xi = \xi + \xi^p + \xi^{p^2} + \ldots + \xi^{p^{e-1}}$ for the trace of an element $\xi \in \mathbb{F}_q$, $q = p^e$, over $\mathbb{F}_p$.

It is obvious that the function (4.11) satisfies the relation

$$\Psi(X, X_1 \oplus X_2) = \Psi(X, X_1)\Psi(X, X_2). \tag{4.12}$$

Hence, for a given X the function $\Psi(X, \cdot)$ is an additive character on the vector space $\mathbb{Q}^n(q^s)$. One can show (cf. [15, Section 5.1]) that each character of the additive group of $\mathbb{Q}^n(q^s)$ coincides with $\Psi(X, \cdot)$ for a suitable X.

The Fourier transform $\tilde{f}$ of a complex-valued function $f : \mathbb{Q}^n(q^s) \to \mathbb{C}$ is defined by

$$\tilde{f}(Y) = \sum_{X \in \mathbb{Q}^n(q^s)} \Psi(Y, X) f(X). \tag{4.13}$$

The following results are well known in theory of Abelian groups (see, for example, [15, Chapters 5, 9] and [16, Chapter 5]).

Lemma 4.1. *Let D, $D^\perp \subset \mathbb{Q}^n(q^s)$ be mutually dual linear distributions. Then,*

(i) *One has the relation*

$$\sum_{X \in D} \Psi(Y, X) = \begin{cases} \#\{D\} & \text{if } \; Y \in D^\perp, \\ 0 & \text{if } \; Y \notin D^\perp. \end{cases} \tag{4.14}$$

(ii) *One has the Poisson summation formula*

$$\sum_{X \in D} f(X) = q^{-ns}\#\{D\} \sum_{Y \in D^\perp} \tilde{f}(Y) \tag{4.15}$$

for an arbitrary function f.

Consider affine subspaces $V_A^M = \mathbb{Q}^n(q^s) \cap \Delta_A^M$, $\Delta_A^M \in \mathfrak{E}_s(q, n)$ as distributions in $\mathbb{Q}^n(q^s)$ (see Lemma 2.2). We write $\chi_A^M(\cdot)$ for the indicator function of V_A^M, that is,

$$\chi_A^M(X) = \begin{cases} 1 & \text{if } \; X \in V_A^M, \\ 0 & \text{if } \; X \notin V_A^M. \end{cases}$$

Since $V_A^M = V_A^0 \oplus Y_A^M$ with $Y_A^M = \left(\frac{m_1}{q^{a_1}}, \ldots, \frac{m_n}{q^{a_n}}\right)^T \in \mathbb{Q}^n(q^s)$, we have

$$\chi_A^M(X) = \chi_A^0(X \ominus Y_A^M). \tag{4.16}$$

We wish to find out distributions $(V_A^0)^\perp$ dual to subspaces V_A^0 and evaluate the Fourier transform $\tilde{\chi}_A^M(\cdot)$ of $\chi_A^M(\cdot)$.

Notice that in view of (4.12), (4.13), and (4.16) we have the relation

$$\tilde{\chi}_A^M(Y) = \Psi(Y, Y_A^M)\tilde{\chi}_A^0(Y). \tag{4.17}$$

Lemma 4.2. *Let, for a given $A = (a_1, \dots, a_n) \in \mathbb{N}_0^n$, $0 \le a_j \le s$, the vector $A^* = (a_1^*, \dots, a_n^*) \in \mathbb{N}_0^n$, $0 \le a_j^* \le s$, $1 \le j \le n$, be defined by $a_j^* = s - a_j$, $1 \le j \le n$. Then one has the relations*

$$(V_A^0)^\perp = V_{A^*}^0, \tag{4.18}$$

and

$$\tilde{\chi}_A^0(Y) = q^{ns-a_1-\dots-a_n} \chi_{A^*}^0(Y). \tag{4.19}$$

Proof. From Lemma 2.2 we derive that the subspace V_A^0 consists of points $X = (x_1, \dots, x_n)^T \in \mathbb{Q}^n(q^s)$ with coordinates

$$x_j = \sum_{i=1}^{s-a_j} \xi_i(x_j) q^{i-s-1}, \quad 1 \le j \le n,$$

where $\xi_i(x_j)$ are arbitrary elements of the field $\mathbb{F}_q$. Using the definitions (4.2), (4.3), (4.4), and (4.6), we conclude that the dual subspace $(V_A^0)^\perp$ consists of points $Y = (y_1, \dots, y_n)^T \in \mathbb{Q}^n(q^s)$ which satisfy the equations

$$\xi_{s+1-i}(y_j) = 0 \quad \text{for} \quad 1 \le i \le s - a_j, \quad 1 \le j \le n,$$

or in an equivalent form

$$\xi_i(y_j) = 0 \quad \text{for} \quad s \ge i \ge s + 1 - a_j^*, \quad 1 \le j \le n.$$

By Lemma 2.2 this implies the relation (4.18).

The relation (4.19) follows at once from (4.18). It suffices to write the relation (4.14) for $D = V_A^0$ and take into account that $\#\{V_A^0\} = q^{ns-a_1-\dots-a_n}$ (cf. the relation (4.9) and Lemma 2.2). $\square$

Lemma 4.3. *Let D, $D^\perp \subset \mathbb{Q}^n(q^s)$ be mutually dual linear distributions. Then for each elementary box $\Delta_A^M \in \mathfrak{E}_s(q,n)$ one has the relation*

$$\#\{D \cap \Delta_A^M\} = q^{-a_1-\dots-a_n} \#\{D\} \sum_{Y \in D^\perp} \Psi(Y, Y_A^M) \chi_{A^*}^0(Y). \tag{4.20}$$

In particular,

$$\#\{D \cap \Delta_A^0\} = q^{-a_1-\dots-a_n} \#\{D\} \#\{D^\perp \cap \Delta_{A^*}^0\}. \tag{4.21}$$

Proof. It suffices to substitute (4.17) and (4.19) to the Poisson summation formula (4.15) and use the relation

$$\#\{D \cap \Delta_A^M\} = \sum_{X \in D} \chi_A^M(X). \quad \square$$

4.3. Proof of Theorems 4.1 and 4.2.

Theorems 4.1 and 4.2 are direct corollaries of the following general result.

Proposition 4.1. *Let D, $D^\perp \subset \mathbb{Q}^n(q^s)$ be mutually dual linear distributions of dimensions d and $d^\perp = ns - d$, correspondingly. Then for a given integer $0 \le \delta \le d$ the following two statements are equivalent:*

(i) *Each elementary box $\Delta_A^M \in \mathfrak{E}_s(q,n)$ of volume $q^{-d+\delta}$ contains exactly q^δ points of D.*

(ii) *$D^\perp$ has a weight $\rho(D^\perp) \ge ns - d^\perp - \delta + 1 = d - \delta + 1$.*

By the relation (4.8) the statement (i) and (ii) of Theorem 4.1 are equivalent. At the sume time Theorem 4.1 (ii) follows at once from Proposition 4.1 for $d = ks$ and $\delta = 0$. Similarly, Theorem 4.2 follows from Definition 1.1 and Proposition 4.1 for $d = s$ and δ equal to the deficients of the corresponding net.

The proof of Theorems 4.1 and 4.2 is complete. $\square$

Proof of Proposition 4.1. (i) Let the statement (i) be held. Then, writing the equality (4.21) for an elementary box $\Delta_A^0 \in \mathfrak{E}_s(q,n)$ of volume $q^{-d+\delta}$, and using the relations (1.6) and (4.9), we conclude that $\#\{D^\perp \cap \Delta_{A^*}^0\} = 1$ for an arbitrary elementary box $\Delta_{A^*}^0 \in \mathfrak{E}_s(q,n)$ with $a_1^* + \ldots + a_n^* = ns - d + \delta = d^\perp + \delta$. Hence each indicated elementary boxes $\Delta_{A^*}^0$ contains a single point $Y = 0$ belonging to $D^\perp$. By Lemma 3.3 this means that the ball $\mathfrak{B}(t) \subset \mathbb{Q}^n(q^s)$ of radius $t = ns - d^\perp - \delta = d - \delta$ does not contain points of $D^\perp$ other than the origin $Y = 0$. Therefore $\rho(D^\perp) \ge ns - d^\perp - \delta + 1 = d - \delta + 1$ (cf. the definition (4.1)).

(ii) Let the statement (ii) be held. Then, by Lemma 3.3 each elementary box $\Delta_{A^*}^0 \in \mathfrak{E}_s(q,n)$ with $a_1^* + \ldots + a_n^* = d^\perp + \delta = ns - d + \delta$ contains a single point $Y = 0$ belonging to $D^\perp$. Writing the equality (4.20) for the indicated boxes $\Delta_{A^*}^0$, we find that $\#\{D \cap \Delta_A^M\} = q^\delta$ for each elementary box $\Delta_A^M \in \mathfrak{E}_s(q,n)$ of volume $q^{-d+\delta}$. $\square$

4.4. Enumerators of mutually dual distributions.

The relations (4.21) can be expressed in terms of the corresponding generating functions. For a given distribution $D \subset \mathbb{Q}^n(q^s)$ we define its *box enumerator* $\varphi(D; z_1, \ldots, z_n)$, $(z_1, \ldots, z_n) \in \mathbb{C}^n$, by

$$\varphi(D; z_1, \ldots, z_n) = \sum_{\substack{0 \le a_j \le s, \\ 1 \le j \le n}} \#\{D \cap \Delta_A^0\} z_1^{a_1} \ldots z_n^{a_n}$$

$$\sum_{X \in D} \sum_{\substack{0 \le a_j \le s, \\ 1 \le j \le n}} \chi_A^0(X) z_1^{a_1} \ldots z_n^{a_n}. \tag{4.22}$$

The expression (4.22) is a polynomial of degree s in each complex variable z_j.

Substituting the relation (4.21) to (4.22), we immediately obtain the following.

Theorem 4.3. *Let D and $D^\perp \subset \mathbb{Q}^n(q^s)$ be linear mutually dual distributions. Then, one has the relation*

$$\varphi(D; z_1, \ldots, z_n) = \#\{D\} \left(\frac{z_1 \ldots z_n}{q^n} \right)^s \varphi\left(D^\perp; \frac{1}{qz_1}, \ldots, \frac{1}{qz_n} \right). \tag{4.23}$$

For a given linear distribution $D \subset \mathbb{Q}^n(q^s)$ we can also introduce its *weight enumerator* $\mathcal{W}(D; z)$, $z \in \mathbb{C}$, by

$$\mathcal{W}(D; z) = \sum_{r=0}^{ns} w_r(D)\, z^r = \sum_{r=0}^{ns} \#\{D \cap \mathfrak{S}(r)\} z^r, \tag{4.24}$$

where $w_0(D) = 1, w_1(D), \ldots, w_{ns}(D)$ is the weight spectrum of D in the metric ρ (cf (4.1)), and $\mathfrak{S}(r)$ is the sphere (3.3).

In the Hamming metric weight enumerators of mutually dual codes are related by the known MacWilliams identity (see [16, Chapter 5, Theorem 13]). Is there an extension of such identities to the metric ρ? Unfortunately, within the limits of the present paper we can not treat this question in detail. Here we consider only the special case of $n = 1$. The author hopes to return to this matter elsewhere.

Theorem 4.4. (i) *For every linear distribution $D \subset \mathbb{Q}(q^s)$ its box and weight enumerators $\varphi(D; z)$ and $\mathcal{W}(D; z)$ are related by*

$$\mathcal{W}(D; z) = z^s(1-z)\varphi\left(D; \frac{1}{z}\right) + \#\{D\}z^{s+1}. \tag{4.25}$$

(ii) *For linear mutually dual distributions D and $D^\perp \subset \mathbb{Q}(q^s)$ one has the identity*

$$(qz-1)\mathcal{W}(D; z) + 1 - z = \#\{D\}z^{s+1}\left(q(1-z)\mathcal{W}\left(D^\perp; \frac{1}{qz}\right) + qz - 1\right), \tag{4.26}$$

or more symmetrically,

$$v(D; z) = \#\{D\}q\, z^{s+2}v\left(D^\perp, \frac{1}{qz}\right), \tag{4.27}$$

where $v(D; z) = (qz-1)\mathcal{W}(D; z) + 1 - z$.

Proof. Be Lemma 3.1 every sphere $\mathfrak{S}(r) \subset \mathbb{Q}(q^s)$ consists of a single fragment g_r. Precisely, the spheres have the following structure: $\mathfrak{S}(0) = [0, q^{-s}) = \Delta^0_s$, and

$$\mathfrak{S}(r) = [q^{-s+r-1}, q^{-s+r}) = \Delta^0_{s-r} \setminus \Delta^0_{s-r+1}, 1 \le r \le s,$$

where $\Delta^0_a = [0, q^{-a})$, $0 \le a \le s$, are elementary boxes (1.5) for $n = 1$. Notice also that $\#\{D \cap \Delta^0_0\} = \#\{D\}$, and $\#\{D \cap \Delta^0_s\} = 1$, since D is a linear distribution.

Substituting the foregoing relations to (4.24), we find that

$$\mathcal{W}(D, z) = 1 + \sum_{r=1}^{s}(\#\{D \cap \Delta^0_{s-r}\} - \#\{D \cap \Delta^0_{s-r+1}\})z^r$$

$$= 1 + \sum_{a=0}^{s}\#\{D \cap \Delta^0_a\}z^{s-a} - \sum_{a=0}^{s}\#\{D \cap \Delta^0_a\}z^{s+1-a}$$

$$-\#\{D \cap \Delta^0_s\} + \#\{D \cap \Delta^0_0\}z^{s+1} = \varphi\left(D; \frac{1}{z}\right)z^s - \varphi\left(D; \frac{1}{z}\right)z^{s+1} + \#\{D\}z^{s+1}.$$

This proves the relation (4.25).

(ii) The identities (4.26) and (4.27) follow from the relations (4.23) and (4.25) by a direct calculation. □

5.1 Hermite interpolations over finite fields.

Let $\mathbb{F}_q[z]$, $q = p^e$, be the ring of polynomials

$$f(z) = \sum_{i=0}^{t-1} f_i\, z^i \tag{5.1}$$

with coefficients $f_i \in \mathbb{F}_q$, $t = \deg f + 1$. For a given polynomial (5.1) its j^{th} hyperderivative $\partial^j f \in \mathbb{F}_q[z]$ is defined by

$$\partial^j f(z) = \sum_{i=0}^{t-1} \binom{i}{j} f_i\, z^{i-j}, \tag{5.2}$$

(cf. [15, Section 6.4]). Hereinafter we write $\binom{i}{j}$ for binomial coefficients modulo p, moreover, as it usually is, $\binom{i}{j} = 0$ for $j > i$.

In particular, the definition (5.2) implies

$$\partial^j (z-\beta)^i = \binom{i}{j} (z-\beta)^{i-j} \tag{5.3}$$

for each $\beta \in \mathbb{F}_q$. Using (5.2) and (5.3), it is easy to check the following expansion

$$f(z) = \sum_{j=0}^{t-1} \partial^j f(\beta)(z-\beta)^j, \tag{5.4}$$

where $\partial^j f(\beta)$ denotes the value of $\partial^j f(z)$ at $\beta \in \mathbb{F}_q$.

It should be noted that for $j < p$ the hyperderivative (5.2) and the usual j^{th} formal derivative $f^{(j)}(z)$ are related by

$$\partial^j f(z) = \frac{1}{j!}\, f^{(j)}(z). \tag{5.5}$$

Certainly, in the ring of polynomials over a field of infinite characteristic the relation (5.5) holds for all $j \in \mathbb{N}_0$.

We can formally add a point ∞ to $\mathbb{F}_q$. In so doing, all arithmetic operations (except $0 \cdot \infty$) may be defined in the obvious way on the set $\mathbb{F}_q \cup \infty$ of $q+1$ elements. For a polynomial (5.1) of degree $t-1$ we put by definition

$$\partial^j f(\infty) = \begin{cases} f_{t-1-j} & 0 \le j \le t-1, \\ 0 & \text{if} \quad j > t-1. \end{cases} \tag{5.6}$$

Obviously, $\partial^j f(\infty) = \partial^j \check{f}(0)$, where $\check{f}(z) = z^{t-1} f\left(\frac{1}{z}\right) = f_{t-1} + f_{t-2} z + \ldots + f_0 z^{t-1}$ is a polynomial receprocal to $f(z)$.

Let $\mathbb{M}^t \subset \mathbb{F}_q[z]$ denote a set of all polynomials (5.1) of degree less than t, $t \in \mathbb{N}_0$, then $\mathbb{M}^t$ is a vector space of dimension t over $\mathbb{F}_q$. Consider the following *Hermite interpolation problem*: Find a polynomial $f \in \mathbb{M}^t$ which satisfies the equations

$$\partial^j f(\beta_i) = a_i^{(j)}, \quad j = 0, \ldots, t_i - 1, \quad 1 \le i \le l, \tag{5.7}$$

where l distinct elements $\beta_1, \ldots, \beta_l \in \mathbb{F}_q \cup \infty$ (interpolation nodes) are fixed, and integers $t_i \in \mathbb{N}$ and coefficients $a_i^{(j)} \in \mathbb{F}_q$ are given. Certainly, we assume here that $q \ge l - 1$.

Proposition 5.1. (i) *The Hermite interpolation problem* (5.7) *has a unique solution* $f \in \mathbb{M}^t$, *provided that* $t_1 + \ldots + t_l = t$.

(ii) *The homogeneous Hermite interpolation problem* (5.7) *with all coefficients* $a_i^{(j)} = 0$ *has a unique solution* $f = 0$ *in the space* $\mathbb{M}^t$, *provided that* $t_1 + \ldots + t_l \geq t$.

Proof. (i) At first, we suppose that all interpolation nodes $\beta_i \in \mathbb{F}_q$, $1 \leq i \leq l$. Consider the polynomials

$$r_i(z) = \sum_{j=0}^{t_i-1} a_i^{(j)}(z - \beta_i)^j, \quad 1 \leq i \leq l. \tag{5.8}$$

From the relations (5.3), (5.4), and (5.8) we conclude that the equations (5.7) are equivalent to the following congruences in the ring $\mathbb{F}_q[z]$

$$f(z) = r_i(z) \mod (z - \beta_i)^{t_i}, \quad 1 \leq i \leq l. \tag{5.9}$$

In (5.9) the polynomials $(z-\beta_i)^{t_i}$, $1 \leq i \leq l$, are pairwise coprime. Therefore, the congruences (5.9) have a unique solution $f \in \mathbb{M}^t$, $t = t_1 + \ldots + t_l$ by the Chinese remainder theorem in the ring $\mathbb{F}_q[z]$ (see [16, Section 10.9, Theorem 5]).

Now, let one of interpolation nodes, say β_l, coinsides with ∞. Then, using (5.6), we put

$$f(z) = g(z) + r_l(z), \tag{5.10}$$

where

$$r_l(z) = \sum_{j=t-t_l}^{t-1} a_l^{(j)} z^j,$$

and $g(z)$ is a polynomial of degree less than $t - t_l$.

Substituting (5.10) to first $l-1$ equations (5.7), we find that the polynomial $g \in \mathbb{M}^{t-t_l}$ is a solution of the following Hermite interpolation problem with $l-1$ nodes $\beta_1, \ldots, \beta_{l-1} \in \mathbb{F}_q$

$$\partial^j g(\beta_i) = b_i^{(j)}, \quad j = 0, \ldots, t_i - 1, \quad 1 \leq i \leq l-1,$$

where $b_i^{(j)} = a_i^{(j)} - \partial^j r(\beta_i)$, and $t_1 + \ldots + t_{l-1} = t - t_l$. This problem has a unique solution by the above arguments.

(ii) This statement follows at once from (i) because we may choose integers $t_i' \in \mathbb{N}$, $t_i' \leq t_i$, to satisfy the equality $t_1' + \ldots + t_l' = t$. $\square$

Remark 5.1. The Hermite interpolations may be treated as a confluent Lagrange interpolation problem (cf. [5, Chapter 2, Section 11]). This leads to another proof of Proposition 5.1. Substituting the relations (5.2) for a polynomial $f \in \mathbb{M}^t$ to (5.7), we obtain a system of $t_1 + \ldots + t_l$ linear equations for t unknown coefficients f_i. If $t_1 + \ldots + t_l = t$, then the system has a unique solution, since the corresponding t by t matrix turns to be a confluent Vandermonde matrix, and Proposition 1.1 should follow. However, the above arguments based on the Chinese remainder theorem seem to be the most readily even in the case of the Hermite interpolations over the field of complex numbers.

5.1. Explicit constructions.

Henceforward we assume that $q \geq n-1$. Fix n distinct elements $\beta_1, \dots, \beta_n \in \mathbb{F}_q \cup \infty$, and define a linear mapping $\Gamma_{n,s} : \mathbb{F}_q[z] \to \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ by setting

$$\Gamma_{n,s} : \mathbb{F}_q[z] \ni f \to \Gamma_{n,s} f = (\partial^{s-1-j} f(\beta_i)) \in \mathrm{Mat}_{n,s}(\mathbb{F}_q), \tag{5.11}$$

where $0 \leq j \leq s-1$ and $1 \leq i \leq n$.

Thus, for each polynomial $f \in \mathbb{F}_q[z]$ the matrix $\Gamma_{n,s} f = (\omega_f^{(1)}, \dots, \omega_f^{(n)})^T \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ consists of n rows of the form

$$\omega_f^{(i)} = (\partial^{s-1} f(\beta_i), \dots, \partial f(\beta_i), f(\beta_i)) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q), \quad 1 \leq i \leq n. \tag{5.12}$$

Lemma 5.1. *For $t \leq ns$ the image $\Gamma_{n,s}\mathbb{M}^t \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ of the vector space $\mathbb{M}^t \subset \mathbb{F}_q[z]$ under the mapping* (5.11) *is a subspace of dimension t.*

Proof. It suffices to prove that $\Gamma_{n,s}\mathbb{M}^{ns} = \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, since $\mathbb{M}^t \subset \mathbb{M}^{ns}$ for $t \leq ns$ and the cardinalities of $\mathbb{M}^{ns}$ and $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ coinside. Let $f \in \mathbb{M}^{ns}$ and $\Gamma_{n,s} f = 0$, then from (5.11) we conclude that f is a solution of a homogeneous Hermite interpolation problem (5.7) with $l = n$, $t = ns$, $t_1 = \ldots = t_n = s$. Therefore $f = 0$ by Proposition 5.1. □

Theorem 5.1. *For each integer $1 \leq k \leq n$ the subspace $\Gamma_{n,s}\mathbb{M}^{ks} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ is an MDS $[n,k,s]$-code in the metric ρ.*

Proof. By Definition 2.1 and the relations (4.1) it sufficies to show that $\rho(\Gamma_{n,s} f) \geq (n-k)s + 1$ for all $f \in \mathbb{M}^{ks} \setminus \{0\}$. Suppose on the contrary that there is a non-zeroth polynomial $f \in \mathbb{M}^{ks}$ such that $\rho(\Gamma_{n,s} f) \leq (n-k)s$. By the definitions (2.14), and (5.11), (5.12) this yields

$$\rho(\Gamma_{n,s} f) = \rho(\omega_f^{(1)}) + \ldots + \rho(\omega_f^{(n)}) \leq (n-k)s. \tag{5.13}$$

From (5.13) we conclude that the strict inequality

$$\rho(\omega_f^{(i)}) < s \tag{5.14}$$

holds at least for k distinct indices i. Without loss of generality, we may assume that the inequality (5.14) holds for $i = 1, \dots, l$ with $l \geq k$ and $\rho(\omega_f^{(i)}) = s$ for $i = l+1, \dots, n$.

Using (5.11), (5.12), and (5.14), we find that the polynomial $f \in \mathbb{M}^{ks}$ is a solution of the following homogeneous Hermite interpolation problem (5.7)

$$\partial^j f(\beta_i) = 0, \quad j = 0, \dots, t_i - 1, \quad 1 \leq i \leq l,$$

where $t_i = s - \rho(\omega_f^{(i)}) \in \mathbb{N}$.

It is easy to check that $t_1 + \ldots + t_l = ns - \rho(\Gamma_{n,s} f)$. Therefore, $t_1 + \ldots + t_l \geq ks$ and $f = 0$ by Proposition 1.1, a contradiction. □

Theorem 5.1 gives broad classes of linear MDS $[n,k,s]$-codes in the metric ρ with arbitrary values of the parameters n, k, and s. By Theorem 2.1 such MDS codes correspond to linear optimum $[n,k,s]$-distributions, which can be explicitly described as follows. Introduce a linear mapping $\gamma_{n,s} : \mathbb{F}_q[z] \to \mathbb{Q}^n(q^s)$ by setting

$$\gamma_{n,s} : \mathbb{F}_q[z] \ni f \to \gamma_{n,s} f = X = (x_1, \dots, x_n)^T \in \mathbb{Q}^n(q^s), \tag{5.15}$$

where coordinates x_i of the point X are given by

$$x_i = \sum_{j=1}^{s} \partial^{j-1} f(\beta_i) q^{-j}. \tag{5.16}$$

Using (5.1), (5.2), and (5.6), we can write the coefficients $\partial^{j-1} f(\beta_i)$ in the form

$$\partial^{j-1} f(\beta_i) = \sum_{l=0}^{t-1} \binom{j-1}{l} \beta_i^{l+1-j} f_l \tag{5.17}$$

for $\beta_i \in \mathbb{F}_q$, and

$$\partial^{j-1} f(\beta_i) = f_{t-j} \tag{5.18}$$

for $\beta_i = \infty$.

Theorem 5.2. *For each integer $1 \leq k \leq n$ the subspace $\gamma_{n,s}\mathbb{M}^{ks} \subset \mathbb{Q}^n(q^s)$ is an optimum $[n, k, s]$-distribution.*

Proof. It suffices to compare the relations (5.15), (5.16) with (5.11), (5.12), and use Theorems 5.1 and 2.1. □

In the special case of $k = 1$ an optimum $[n, 1, s]$-distribution $\gamma_{n,s}\mathbb{M}^s$ (defined by the relations from (5.15) to (5.18)) coinsides with a $(0, s, n)$-net of zeroth deficiency (cf. Proposition 1.1) which was given previously in [11] and [19].

6. Reconstructions of codes and distributions

6.1. Peano's bijection.

As usually, for a matrix $\Omega \in \mathrm{Mat}_{g,s}(\mathbb{F}_q)$ we write $\Omega = (\omega_1, \ldots, \omega_g)^T$ where $\omega_j = (\xi_1^{(j)}, \ldots, \xi_s^{(j)}) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$. Introduce a mapping π_g from $\mathrm{Mat}_{g,s}(\mathbb{F}_q)$ to $\mathrm{Mat}_{1,gs}(\mathbb{F}_q)$ by

$$\pi_g : \mathrm{Mat}_{g,s}(\mathbb{F}_q) \ni \Omega \to \pi_g\Omega = (\xi_1^{(1)}, \ldots, \xi_1^{(g)}, \ldots, \xi_s^{(1)}, \ldots, \xi_s^{(g)}) \in \mathrm{Mat}_{1,gs}(\mathbb{F}_q). \tag{6.1}$$

It is obvious that the mapping (6.1) is an isomorphism of vector spaces $\mathrm{Mat}_{g,s}(\mathbb{F}_q)$ and $\mathrm{Mat}_{1,gs}(\mathbb{F}_q)$.

By the relations (2.4), (2.5), and (2.6) the mapping (6.1) can be considered as an isomorphism of vector spaces $\mathbb{Q}^g(q^s)$ and $\mathbb{Q}(q^{gs})$. In this case π_g coinsides with a well know Peano's mapping (restricted on $\mathbb{Q}^g(q^s)$) which gives a bijection between points of the unit cube U^g and the unit segment $[0, 1)$.

More generally, we introduce an isomorphism $\pi_{g,n}$ of vector spaces $\mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ and $\mathrm{Mat}_{n,gs}(\mathbb{F}_q)$ as follows. For a matrix $\Omega \in \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ we write $\Omega = (\Omega_1, \ldots, \Omega_n)^T$ where $\Omega_j \in \mathrm{Mat}_{g,s}(\mathbb{F}_q)$, $1 \leq j \leq n$. Now we put

$$\pi_{g,n} : \mathrm{Mat}_{gn,s}(\mathbb{F}_q) \ni \Omega \to \pi_{g,n}\Omega = (\pi_g\Omega_1, \ldots, \pi_g\Omega_n)^T \in \mathrm{Mat}_{n,gs}(\mathbb{F}_q). \tag{6.2}$$

In other words, we split gn rows of a matrix $\Omega \in \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ into n subsets $\Omega_1, \ldots, \Omega_n$, each of which consists of successive g rows; and subsequently by π_g, we map first g rows Ω_1 to the first row of the matrix $\pi_{g,n}\Omega \in \mathrm{Mat}_{n,gs}(\mathbb{F}_q)$, second g rows Ω_2 to the second row of $\pi_{g,n}\Omega$, and so on, last g rows Ω_n are mapped to the n^{th} row of $\pi_{g,n}\Omega$.

Using the relations (2.8) and (6.2), we define an isomorphism

$$\pi_{g,n} : \mathbb{Q}^{gn}(q^s) \ni X \to \pi_{g,n} X \in \mathbb{Q}^n(q^{gs}) \tag{6.3}$$

of vector spaces $\mathbb{Q}^{gn}(q^s)$ and $\mathbb{Q}^n(q^{gs})$ by setting

$$\Omega\langle \pi_{g,n} X\rangle = \pi_{g,n}\Omega\langle X\rangle. \tag{6.4}$$

It is obvious that the mapping (6.3), (6.4) is a restriction on $\mathbb{Q}^{gn}(q^s)$ and $\mathbb{Q}^n(q^{gs})$ of the well known Peano's bijection between points of the unit cubes U^{gn} and U^n.

The foregoing implies the following.

Lemma 6.1. (i) *Let $\mathcal{C} \subset \mathrm{Mat}_{\,gn,s}(\mathbb{F}_q)$ be a $[gn, gk, s]$-code and $D \subset \mathbb{Q}^{gn}(q^s)$ be a $[gn, gk, s]$-distribution, then $\pi_{g,n}\mathcal{C} \subset \mathrm{Mat}_{\,n,gs}(\mathbb{F}_q)$ is a $[n, k, gs]$-code and $\pi_{g,n}D \subset \mathbb{Q}^n(q^{gs})$ is a $[n, k, gs]$-distribution.*

(ii) *If a code $\mathcal{C} \subset \mathrm{Mat}_{\,gn,s}(\mathbb{F}_q)$ and a distribution $D \subset \mathbb{Q}^{gn}(q^s)$ are linear, then the code $\pi_{g,n} \subset \mathrm{Mat}_{\,n,gs}(\mathbb{F}_q)$ and the distribution $\pi_{g,n}D \subset \mathbb{Q}^n(q^{gs})$ are also linear.*

Now our concern is with the behavior of the Hamming and non-Hamming weights $\varkappa$ and ρ under the mappings (6.2) and (6.3).

Lemma 6.2. (i) *For arbitrary matrices $\Omega \in \mathrm{Mat}_{\,gn,s}(\mathbb{F}_q)$ and points $X \in \mathbb{Q}^{gn}(q^s)$ one has the relations*

$$\varkappa(\pi_{g,n}\Omega) = \varkappa(\Omega), \quad \varkappa(\pi_{g,n}X) = \varkappa(X), \tag{6.5}$$

and

$$\rho(\pi_{g,n}\Omega) \geq \rho(\Omega), \quad \rho(\pi_{g,n}X) \geq \rho(X). \tag{6.6}$$

(ii) *For arbitrary codes $\mathcal{C} \subset \mathrm{Mat}_{\,gn,s}(\mathbb{F}_q)$ and distributions $D \subset \mathbb{Q}^{gn}(q^s)$ one has the relations*

$$\varkappa(\pi_{g,n}\mathcal{C}) = \varkappa(\mathcal{C}), \quad \varkappa(\pi_{g,n}D) = \varkappa(D) \tag{6.7}$$

and

$$\rho(\pi_{g,n}\mathcal{C}) \geq \rho(\mathcal{C}), \quad \rho(\pi_{g,n}D) \geq \rho(D). \tag{6.8}$$

Proof. (i) It suffices to prove (6.5) and (6.6) only for matrices $\Omega \in \mathrm{Mat}_{\,gn,s}(\mathbb{F}_q)$.

To prove (6.5) we simply notice that the matrix $\pi_{g,n}\Omega$ is obtained by a reordering (see (6.1), (6.2)) of elements of Ω. Therefore, the matrices $\pi_{g,n}\Omega$ and Ω have the same number of non-zeroth entries.

To prove (6.6) we first consider the behavior of the ρ-weight under the mapping (6.1). We wish to prove that for an arbitrary matrix $\Omega \in \mathrm{Mat}_{\,g,s}(\mathbb{F}_q)$ one has the inequality

$$\rho(\pi_g\Omega) \geq \rho(\Omega). \tag{6.9}$$

Since (6.9) holds trivially for $\Omega = 0$, we suppose that $\Omega \neq 0$. Let $\Omega = (\omega_1, \dots, \omega_g)^T$ where $\omega_j \in \mathrm{Mat}_{\,1,s}(\mathbb{F}_q)$, $1 \leq j \leq g$. Introduce an integer l, $1 \leq l \leq g$, by setting

$$l = l(\Omega) = \max\{j : \rho(\omega_j) \neq 0\}. \tag{6.10}$$

Comparing the definitions (2.12) and (6.1), we conclude that

$$\rho(\pi_g\Omega) = \rho(\omega_l) + (l-1)s. \tag{6.11}$$

Moreover, the definition (2.14) implies

$$\rho(\Omega) = \sum_{j=1}^{l} \rho(\omega_j). \tag{6.12}$$

Using the relations (2.13), (6.11), and (6.12), we find that

$$\rho(\Omega) = \rho(\omega_l) + \sum_{j=1}^{l-1} \rho(\omega_j) \le \rho(\omega_l) + (l-1)s = \rho(\pi_g \Omega).$$

The proof of the inequality (6.9) is complete.

Now, let an arbitrary matrix $\Omega \in \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ be given. Then $\Omega = (\Omega_1, \dots, \Omega_n)^T$ where $\Omega_j \in \mathrm{Mat}_{g,s}(\mathbb{F}_q)$, $1 \le j \le n$. Comparing the distributions (2.14) and (6.2), we conclude that

$$\rho(\Omega) = \sum_{j=1}^{n} \rho(\Omega_j), \quad \rho(\pi_{g,n}\Omega) = \sum_{j=1}^{n} \rho(\pi_g \Omega_j). \tag{6.13}$$

Substituting the inequality (6.9) to (6.13), we obtain the inequality (6.6).

(ii) The proposition (ii) follows at once from (i) and the definitions (2.18), (2.19) of weights $\varkappa$ and ρ. $\square$

Proposition 6.1. *Let $\mathcal{C} \subset \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ be an MDS $[gn, gk, s]$-code in the metric ρ and $D \subset \mathbb{Q}^{gn}(q^s)$ be an optimum $[gn, gk, s]$-distribution. Then,*

$$\rho(\pi_{g,n}\mathcal{C}) = (n-k)gs + 1, \quad \rho(\pi_{g,n}D) = (n-k)gs + 1, \tag{6.14}$$

so that, $\pi_{g,n}\mathcal{C} \subset \mathrm{Mat}_{n,gs}(\mathbb{F}_q)$ is an MDS $[n, k, gs]$-code in the metric ρ and $\pi_{g,n}D \subset \mathbb{Q}^n(g^{gs})$ is an optimum $[n, k, gs]$-distribution.

Furthermore, the corresponding Hamming weights satisfy the following inequalities

$$\varkappa(\pi_{g,n}\mathcal{C}) \ge (n-k)g + 1, \quad \varkappa(\pi_{g,n}D) \ge (n-k)g + 1. \tag{6.15}$$

Proof. It suffices to prove the relations (6.14) and (6.15) obnly for codes.

To prove (6.14) we notice that $\rho(\pi_{g,n}\mathcal{C}) \ge (n-k)gs + 1$ by Definition 2.1 and the inequality (6.8). It remains to refer to Proposition 2.1.

To prove (6.15) we notice that

$$\varkappa(\mathcal{C}) \ge s^{-1}\rho(\mathcal{C}) = (n-k)g + s^{-1}$$

by the inequality (2.19) and Definition 2.1. Therefore $\varkappa(\mathcal{C}) \ge (n-k)g + 1$, since the weight $\varkappa(\mathcal{C})$ is an integer. It remains to refer to the equality (6.7). $\square$

6.2. Duality and Peano's bijection.

We wish to consider the behavior of the inner products (4.2) and (4.3) under the mappings (6.1) and (6.2). We introduce an isomorphism J_g of the space $\mathrm{Mat}_{g,s}(\mathbb{F}_q)$ by setting

$$J_g : \mathrm{Mat}_{g,s}(\mathbb{F}_q) \ni \Omega = (\omega_1, \dots, \omega_g)^T \to J_g\Omega = (\omega_g, \dots, \omega_1)^T \in \mathrm{Mat}_{g,s}(\mathbb{F}_q), \tag{6.16}$$

where $\omega_j \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, $1 \leq j \leq g$. Thus, J_g is merely a permutation of rows in inverse order.

By a direct calculation from the definitions (4.2), (4.3) and (6.1), (6.16) we derive the identity

$$\langle \pi_g \Omega_1, \pi_g \Omega_2 \rangle = \langle J_g \Omega_1, \Omega_2 \rangle = \langle \Omega_1, J_g \Omega_2 \rangle \tag{6.17}$$

for all Ω_1, $\Omega_2 \mathrm{Mat}_{g,s}(\mathbb{F}_q)$.

Now we introduce an isomorphism $J_{g,n}$ of the space $\mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ by setting

$$J_{g,n} : \mathrm{Mat}_{gn,s}(\mathbb{F}_q) \ni \Omega = (\Omega_1, \dots, \Omega_n)^T \to J_{g,n}\Omega = (J_g\Omega_1, \dots, J_g\Omega_n)^T \in \mathrm{Mat}_{gn,s}, \tag{6.18}$$

where $\Omega_j \in \mathrm{Mat}_{g,s}(\mathbb{F}_q)$.

Using the definitions (4.2), (4.3), (6.1), (6.2), and the relation (6.17), we obtain the identity

$$\langle \pi_{g,n} \Omega_1, \pi_{g,n} \Omega_2 \rangle = \langle J_{g,n} \Omega_1, \Omega_2 \rangle = \langle \Omega_1, J_{g,n} \Omega_2 \rangle \tag{6.19}$$

for all Ω_1, $\Omega_2 \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$.

Proposition 6.2. *Given a linear code $\mathcal{C} \subset \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ and its image $\pi_{g,n}\mathcal{C} \subset \mathrm{Mat}_{n,gs}(\mathbb{F}_q)$ under the mapping* (6.2). *Then the dual codes $\mathcal{C}^\perp$ and $(\pi_{g,n}\mathcal{C})^\perp$ are related by*

$$(\pi_{g,n}\mathcal{C})^\perp = \pi_{g,n}(J_{g,n}\mathcal{C}^\perp). \tag{6.20}$$

Proof. Since the mapping (6.2) is a bijection, we can write $(\pi_{g,n}\mathcal{C})^\perp = \pi_{g,n}\mathcal{C}_1$ with a linear code $\mathcal{C}_1 \subset \mathrm{Mat}_{n,gs}(\mathbb{F}_q)$. Using Definition 4.1 and the relation (6.19), we conclude that $J_{g,n}\mathcal{C}_1 = \mathcal{C}^\perp$. Therefore, $\mathcal{C}_1 = J_{g,n}\mathcal{C}^\perp$, because $J_{g,n}^2$ is the identity, and the relation (6.20) follows. □

For linear codes and distributions Proposition 6.1 can be supplemented with the following result.

Proposition 6.3. *Let $\mathcal{C} \subset \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ be a linear MDS $[gn, gk, s]$-code in the metric ρ and $D \subset \mathbb{Q}^{gn}(q^s)$ be a linear optimum $[gn, gk, s]$-distribution. Then, the Hamming and non-Hamming weights of the dual subjects $(\pi_{g,n}\mathcal{C})^\perp$ and $(\pi_{g,n}D)^\perp$ satisfy the following relations*

$$\rho((\pi_{g,n}\mathcal{C})^\perp) = (n-k)gs + 1, \quad \rho((\pi_{g,n}D)^\perp) = (n-k)gs + 1$$

and

$$\varkappa((\pi_{g,n}\mathcal{C})^\perp) \geq kg + 1, \quad \varkappa((\pi_{g,n}D)^\perp) \geq kg + 1.$$

Proof. It suffices to prove Proposition 6.3 only for codes.

First of all, we notice that

$$\rho(J_{g,n}\mathcal{C}_1) = \rho(\mathcal{C}_1) \tag{6.21}$$

and

$$\varkappa(J_{g,n}\mathcal{C}_1) = \varkappa(\mathcal{C}_1) \tag{6.22}$$

for an arbitrary code $\mathcal{C} \subset \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$, because the mapping $J_{g,n}$ is nothing but a permutation of rows of the corresponding code words, that preserves both weights ρ and $\varkappa$ (cf. Remark 2.2).

Now let $\mathcal{C} \subset \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ be a linear MDS $[gn, gk, s]$-code in the metric ρ. Then, by Theorem 4.1 (i), $\mathcal{C}^\perp \subset \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ is an MDS $[gn, g(n-k), s]$-code in the metric ρ. Therefore, the relations (6.7), (6.15) (where k is replaced by $n-k$), (6.20), and (6.21), (6.22) imply

$$\rho((\pi_{g,n}C)^\perp) = \rho(\pi_{g,n}(J_{g,n}C^\perp)) = \rho(J_{g,n}C^\perp) = \rho(C^\perp) = (n-k)gs + 1,$$

and similarly,

$$\varkappa((\pi_{g,n}C)^\perp) = \varkappa(\pi_{g,n}(J_{g,n}C^\perp)) = \varkappa(J_{g,n}C^\perp) = \varkappa(C^\perp) \geq kg + 1. \ \square$$

6.3. Codes and distributions with large ρ- and $\varkappa$-weights.

Now we can give explicit constructions of codes and distributions with large weights simultaneously in both metrics ρ and $\varkappa$.

Given an arbitrary integer $g \in \mathbb{N}$. Define a linear $[gn, gk, s]$-code $\mathcal{C}_g \subset \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ and a linear $[gn, gk, s]$-distribution $D_g \subset \mathbb{Q}^{gn}(q^s)$ by

$$\mathcal{C}_g = \Gamma_{gn,s}\mathbb{M}^{gks}, \quad D_g = \gamma_{gn,s}\mathbb{M}^{gks}, \tag{6.23}$$

where the mappings $\Gamma_{gn,s}$ and $\gamma_{gn,s}$ are given in (5.11). Certainly, we assume here that

$$q = p^e \geq gn - 1. \tag{6.24}$$

Next, we introduce an $[n, k, gs]$-code $\pi_{g,n}\mathcal{C}_g \subset \mathrm{Mat}_{n,gs}(\mathbb{F}_q)$ and an $[n, k, gs]$-distribution $\pi_{g,n}D_g \subset \mathbb{Q}^n(q^{gs})$, where $\pi_{g,n}$ are Peano's bijections (6.2) and (6.3). We consider also the dual $[n, n-k, gs]$-code $(\pi_{g,n}\mathcal{C}_g)^\perp \subset \mathrm{Mat}_{n,gs}(\mathbb{F}_q)$ and $[n, n-k, gs]$-distribution $(\pi_{g,n}D_g)^\perp \subset \mathbb{Q}^n(q^{gs})$.

Theorem 6.1. *With the above notation one has the following relations for the corresponding Hamming and non-Hamming weights*

$$\begin{aligned} \rho(\pi_{g,n}\mathcal{C}_g) &= (n-k)gs + 1, & \rho(\pi_{g,n}D_g) &= (n-k)gs + 1, \\ \varkappa(\pi_{g,n}\mathcal{C}_g) &\geq (n-k)g + 1, & \varkappa(\pi_{g,n}D_g) &\geq (n-k)g + 1, \end{aligned} \tag{6.25}$$

and

$$\begin{aligned} \rho((\pi_{g,n}\mathcal{C}_g)^\perp) &= kgs + 1, & \rho((\pi_{g,n}D_g)^\perp) &= kgs + 1, \\ \varkappa((\pi_{g,n}\mathcal{C}_g)^\perp) &\geq kg + 1, & \varkappa((\pi_{g,n}D_g)^\perp) &\geq kg + 1, \end{aligned} \tag{6.26}$$

Proof. As usually, we prove Theorem 6.1 only for codes. By Theorem 5.1 $C_g \subset \mathrm{Mat}_{gn,s}(\mathbb{F}_q)$ given in (6.23) is a linear MDS $[gn, gk, s]$-code in the metric ρ. This implies the relations (6.25) by Proposition 6.1 and the relations (6.26) by Proposition 6.3. □

6.4. Variations of the base q.

Every distribution in the space $\mathbb{Q}^n(q^s)$, $q = p^e$, can be treated as a distribution in the space $\mathbb{Q}^n(p^{es})$ (cf. Lemma 1.1). We wish to find out what happens to metric properties of a given distribution $D \subset \mathbb{Q}^n(q^s)$ when the base q varies from p^e to p.

In what follows we write $\varkappa_q$, ρ_q for the corresponding Hamming and non-Hamming weights on the space $\mathbb{Q}^n(q^s)$, $q = p^e$, and $\varkappa_p$, ρ_p for those on the space $\mathbb{Q}^n(p^{es})$ (cf. Sec. 2.2).

Let $x \in \mathbb{Q}(q^s)$. Consider the representation (2.5) in bases q and p,

$$x = \sum_{i=1}^{s} \xi_i(x) q^{i-s-1} = \sum_{j=1}^{es} \theta_j(x) p^{j-es-1}, \tag{6.27}$$

where $\xi_i(x) = \xi_i = \mu_i^{(1)} + \mu_i^{(2)} p + \ldots + \mu_i^{(e)} p^{e-1}$, and $\mu_i^{(e)} = \mu_i^{(e)}(x) \in \{0, 1, \ldots, p-1\}$ (cf. (2.6)). The coefficients $\theta_j = \theta_j(x)$ in (6.27) are determined by the following rule for the corresponding code words:

$$\begin{aligned} \mathrm{Mat}_{1,s}(\mathbb{F}_q) \ni \omega_q\langle x \rangle &= (\xi_1, \ldots, \xi_s) = (\mu_1^{(1)}, \ldots, \mu_1^{(e)}, \mu_2^{(1)}, \ldots, \mu_2^{(e)}, \ldots, \mu_s^{(1)}, \ldots, \mu_s^{(e)}) \\ &= (\theta_1, \ldots, \theta_{es}) = \omega_p\langle x \rangle \in \mathrm{Mat}_{1,es}(\mathbb{F}_p). \end{aligned} \tag{6.28}$$

It is obvious that $\rho_q(0) = \rho_p(0) = 0$. So, we consider $x \neq 0$. With the above notation the definition (2.12) takes the form

$$\rho_q(x) = \max\{i : \xi_i \neq 0\}, \quad \rho_p(x) = \max\{j : \theta_j \neq 0\}. \tag{6.29}$$

Suppose that $\rho_q(x) = r$, $r \in \mathbb{N}$, then using (6.28) and (6.29), we conclude that $\theta_j = 0$ for all $j > er$ and there is an element $\theta_j \neq 0$ with $e(r-1)+1 \leq j \leq er$. Therefore,

$$e(\rho_q(x) - 1) + 1 \leq \rho_p(x) \leq e\rho_q(x). \tag{6.30}$$

Combining the inequality (6.32) with the definition (2.14), we find the following

$$e(\rho_q(X) - 1) + 1 - (e-1)(n-1) \leq \rho_p(X) \leq e\rho_q(X) \tag{6.31}$$

where $X \in \mathbb{Q}^n(q^s)$ is an arbitrary point. Cerntainly, the left side of (6.30) and (6.31) is informative only for sufficiently large weights ρ_q.

Similarly, using the rule (6.28), we obtain the following inequality for the Hamming weights

$$\varkappa_q(X) \leq \varkappa_p(X) \leq e\varkappa_q(X), \tag{6.32}$$

where $X \in \mathbb{Q}^n(q^s)$ is an arbitrary point. Notice that bounds of such kind are well known in the coding theory (cf. [16, Section 7.7]).

The foregoing immediately implies the following result

Proposition 6.4. *Given a distribution $D \subset \mathbb{Q}^n(q^s)$, $q = p^e$. Then, its Hamming and non-Hamming weights $\varkappa(D)$ and $\rho(D)$ in bases q and p are related by*

$$e(\rho_q(D) - 1) + 1 - (e-1)(n-1) \leq \rho_p(D) \leq e\rho_q(D) \tag{6.33}$$

and

$$\varkappa_q(D) \leq \varkappa_p(D) \leq e\varkappa_q(D). \tag{6.34}$$

In particular, if $D \subset \mathbb{Q}^n(q^s)$ is an optimum $[n,k,s]$-distribution in base q then its weight $\rho_p(D)$ in base p satisfies the inequality

$$\rho_p(D) \geq (n-k)es + 1 - (e-1)(n-1). \tag{6.35}$$

Proof. The inequalities (6.33), (6.34) follow from (6.31), (6.32), and the definition (2.18). If $D \subset \mathbb{Q}^n(q^s)$ is an optimum $[n,k,s]$-distribution, then $\rho_q(D) = (n-k)s + 1$ by Theorem 2.1, and the inequality (6.35) follows from (6.33). $\square$

We return to the $[n,k,s]$-distribution $\pi_{g,n}D_g \subset \mathbb{Q}^n(q^{gs})$ and the dual $[n, n-k, s]$-distribution $(\pi_{g,n}D_g)^\perp \subset \mathbb{Q}^n(q^{gs})$ which were introduced in Sec. 6.3. The bounds for their Hamming and non-Hamming weights $\varkappa = \varkappa_q$ and $\rho = \rho_q$ in base q are given in Theorem 6.1. Now we wish to estimate the corresponding weights $\varkappa_p$ and ρ_p in base p.

Theorem 6.2. *With the notation of Sec. 6.3 one has the following relations for the corresponding Hamming and non-Hamming weights in base p*

$$\begin{gathered}\rho_p(\pi_{g,n}D_g) \geq (n-k)egs + 1 - (e-1)(n-1), \\ \varkappa_p(\pi_{g,n}D_g) \geq (n-k)g + 1,\end{gathered} \tag{6.36}$$

and

$$\begin{gathered}\rho_p((\pi_{g,n}D_g)^{\perp}) \geq k\, egs + 1 - (e-1)(n-1), \\ \varkappa_p((\pi_{g,n}D_g)^{\perp}) \geq k\, eg + 1,\end{gathered} \tag{6.37}$$

where integers e, $g \in \mathbb{N}$ and the prime p are related by (6.24).

Proof. It suffices to compare Theorem 6.1 and Proposition 6.4; in so doing the inequalities (6.36) and (6.37) follow from the inequalities (6.25) and (6.26), correspondingly. □

Thus, we have constructed explicitly the distributions $\pi_{g,n}D_g$ and $(\pi_{g,n}D_g)^{\perp}$ with large weights simulteneously in metrics ρ_p and $\varkappa_p$. As mentiones in Introduction distributions with such metric properties are of crucial importance for further applications (see [7]).

References

1. M. J. Adams, B. L. Shader, "A construction for (t, m, s)-nets in base q," *SIAM J. Discrete Math.*, **10** (1997), 460–468.
2. R. C. Baker, "On irregularities of distribution. II," *J. London Math. Soc.* (to appear).
3. J. Beck, "A two-dimensional van Aardenne–Ehrenfest theorem in irregularities of distributions," *Composito Math.*, **72** (1989), 269–339.
4. J. Beck, W. W. L. Chen, *Irregularities of Distributions*, Cambridge Univ. Press, Cambridge (1987).
5. I. S. Berezin, N. P. Zhidkov, *Computing Methodes*, vol. 1, Addison–Wesley, Reading Mass. (1965).
6. W. W. L. Chen, "On irregularities of distributions. II," *Quart. J. Math. Oxford* (2), **34** (1983), 257–279.
7. W. W. L. Chen, M. M. Skriganov, "Explicit constructions of point sets with a minimal order of the L_2-discrepancy," in preparation.
8. A. T. Clayman, G. L. Mullen, "Improved (t, m, s)-net parameters from the Gilbert–Varshamov bound," *Applicable Algebra Engrg. Comm. Comp.* **8** (1997), 491–496.
9. J. H. Conway, N. J. Sloane, *Sphere Packings, Lattices and Groups*, Springer, New York (1988).
10. Y. Edel, J. Bierbrauer, "Construction of digital nets from BCH-codes," In: *Monte Carlo and Quasi – Monte Carlo Methods 1996 (H. Niederreiter et. al., eds.). Lecture Notes in Statistics*, Vol. 127, pp. 221–231, Springer, New York (1997).
11. H. Faure, "Descrépance de suites associées à un systme̋ de numération (en dimension s)," *Acta Arith.*, **41** (1982), 337–351.
12. L. Kuipers, H. Niederreiter, *Uniform Distribution of Sequences*, John Wiley & Sons, New York etc. (1974).
13. K. M. Lawrence, A. Mahalanabis, G. L. Mullen, W. Ch. Schmid, "Construction of digital (t, m, s)-nets from linear codes," in: *Finite Fields and Applications* (S. Cohen and H. Niederreiter, eds.) *London Math. Soc. Lecture Note Series*, Vol. 233, pp. 189–208, Cambridge Univ. Press, Cambridge (1996).
14. S. Lang, *Algebra*, Addison–Wesley, Reading, Mass. (1971).
15. R. Lidl, H. Niederreiter, *Finite Fields*, Addison–Wesley, London etc. (1983).
16. F. J. MacWilliams, N. J. A. Sloane, *The Theory of error-correcting codes*, North-Holland, Amsterdam (1977).
17. D. M. Mandelbaum, "Construction of error-correcting codes by interpolation," *IEEE Trans. Inf. Theor.*, **IT-25** (1979), 27–35.
18. J. Matoušek, *Geometric discrepancy (an illustrated guide)*, Springer, Berlin (1998).
19. H. Niederreiter, "Point sets and sequences with small discrepancy," *Monatsh. Math.*, **104** (1987), 273–337.
20. H. Niederreiter, *Random Number Generation and Quasi – Monte Carlo Methods*, SIAM, Philadelphia (1992).
21. H. Niederreiter, "Nets, (t, s)-sequences, and algebraic curves over finite fields with many rational points," *International Congress of Mathematicians in Berlin, Documenta Mathematica*, Extra Volume III (1998), 377–386.
22. H. Niederreiter, C. P. Xing, "Low-discrepancy sequences and global function fields with many rational places," *Finite Fields Appl.*, **2** (1996), 241–273.

23. H. Niederreiter, C. P. Xing, "Nets, (t, s)-sequences, and algebraic geometry," In: *Pseudo- and Quasi-Random Point Sets* (P. Hellekalek and G. Larcher, eds.), *Lectures Notes in Statistics*, Vol. 138, Springer, New York (1998).
24. M. M. Skriganov, "Constructions of uniform distributions in terms of geometry of numbers," *Algebra Analiz*, **6**, No. 3 (1994), 200–230; Reprinted in St. Petersburg Math. J., **6** (1995), 635–664.
25. M. M. Skriganov, "Ergodic theory on $SL(n)$, diophantine approximations, and anomalies in the lattice point problem," *Invent. Math.*, **132** (1998), 1–72.
26. M. M. Skriganov, "Uniform distributions, error-correcting codes, and interpolations over finite fields," *Steklov Math. Inst. at St. Petersburg*, Preprint (1998).
27. I. M. Sobol, "On the distribution of points in a cube and the approximate evaluation of integrals, *Ž. Vyčisl. Mat. Mat. Fiz.*, **7** (1967), 784–802; English transl.: *U.S.S.R. Comp. Math. and Math. Phys.*, **7** (1967), 86–112.
28. I. M. Sobol, *Multi-Dimensional Quadrature Formulas and Haar Functions* [in Russian], Nauka, Moscow (1969).
29. H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin (1993).
30. M. A. Tsfasman, S. G. Vlăduts, *Algevraic-Geometric Codes*, Kluwer, Dordrecht (1991).