PDMI PREPRINT — 16/1998

UNIFORM DISTRIBUTIONS, ERROR-CORRECTING CODES, AND INTERPOLATIONS OVER FINITE FIELDS

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

August 28, 1998

ABSTRACT

In the present paper we consider finite point sets of a special kind, q-optimum distributions, which fill out the n-dimensional unit cube very uniformly. It turns out that such point sets have a rather rich combinatorial structure, namely, we show that q-optimum distributions can be characterized as maximum distance codes with respect to a non-Hamming metric. Broad classes of such codes and distributions are explicity constructed by Hermite interpolations over finite fields. In addition, weight spectra of maximum distance codes are also evaluated precisely in the paper.

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

1. Optimum distributions

Fix a prime p and a prime power $q = p^e$, $e \in \mathbb{N}$. We denote by $\mathbb{N}$ the set of natural numbers, and by $\mathbb{N}_0$ the set of all non-negative integers.

Let $U^n = [0,1)^n$ be the n-dimensional unit cube. We introduce elementary q-boxes $\Delta_A^M(q) \subset U^n$ by setting

$$\Delta_A^M(q) = \left[\frac{m_1}{q^{a_1}}, \frac{m_1+1}{q^{a_1}}\right) \cdots \left[\frac{m_n}{q^{a_n}}, \frac{m_n+1}{q^{a_n}}\right), \tag{1.1}$$

where $A = (a_1, \dots, a_n)$, $M = (m_1, \dots, m_n) \in \mathbb{N}_0^n$, and $m_j \in \{0, 1, \dots, q^{a_j} - 1\}$, $1 \le j \le n$. We denote by $\mathbb{N}_0^n$ the set of all vectors in $\mathbb{R}^n$ with non-negative integer coordinates. Notice that q-boxes (1.1) have volume

$$\operatorname{vol} \Delta_A^M(q) = q^{-a_1-\dots-a_n}. \tag{1.2}$$

Definition 1.1. *A subset $D \subset U^n$ consisting of q^s, $s \in \mathbb{N}_0$, points is called the q-optimum distribution if each elementary q-box $\Delta_A^M(q)$ of volume q^{-s} contains exactly one point of D.*

Optimum distributions have extremly low discrepancies (cf. [1, Sec. 3.2]). Actually, such point sets are most uniformly distributed in the unit cube. However, in the present paper we will mainly study only geometric and combinatorial aspects of optimum distributions.

The paper is organized as follows. In the present section we give basic definitions and their elementary corollaries. Relations between distributions and codes are described in Sec. 2.

In Sec. 3 we introduce a non-Hamming metric on the space of codes, and in Sec. 4 we show that q-optimum distributions can be characterized as maximum distance codes with respect to this metric. In Sec. 5 we consider Hermite interpolations over finite fields. These interpolations are applied in Sec. 6 to construct explicitly maximum distance codes and q-optimum distributions. Moreover, weight spectra of maximum distance codes are evaluated precisely in Sec. 7.

It should be noting that q-optimum distributions consisting of q^s, $s > 1$, points do not exist if $q < n - 1$ (see Theorem 7.2 below). At the same time, for each a prime power q,

$$q \ge n - 1, \tag{1.3}$$

we construct q-optimum distributions of q^s points with arbitrary $s \in \mathbb{N}$. Among other things, this implies that the condition (1.3) is necessary and sufficient for the existence of non-trivial q-optimum distributions.

Concerning to general concepts and know results in theory of uniform distributions and the coding theory, we refer to [1, 4] and respectively to [5, 6].

In addition to q-boxes (1.1) we introduce elementary p-boxes $\Delta_B^L(p)$ by setting

$$\Delta_B^L(p) = \left[\frac{l_1}{p^{b_1}}, \frac{l_1+1}{p^{b_1}}\right) \cdots \left[\frac{l_n}{p^{b_n}}, \frac{l_n+1}{p^{b_n}}\right), \tag{1.4}$$

where $B = (b_1, \dots, b_n)$, $L = (l_1, \dots, l_n) \in \mathbb{N}_0^n$, and $l_j \in \{0, 1, \dots, p^{b_j} - 1\}$, $1 \le j \le n$. p-boxes (1.4) have volume

$$\operatorname{vol} \Delta_B^L(p) = p^{-b_1-\dots-b_n}. \tag{1.5}$$

Our concern is with the behavior of a q-optimum distribution with respect to p-boxes (1.4). Such questions naturally arise in computing applications, as for instance, in multi-dimensional quadrature formulas where points of a q-optimum distribution, say with $q = 2^e$, can be used as nodes of integration (cf. [2, 4, 7]).

The following is a variation of Definition 1.1.

Definition 1.2. *For a given $\delta \in \mathbb{N}_0$ a distribution $D \subset U^n$ consisting of p^v, $v \in \mathbb{N}_0$, $v \geq \delta$, points is called the p-optimum distribution of deficient δ if each elementary p-box $\Delta_B^L(p)$ of volume $p^{\delta-v}$ contains exactly p^δ points of D.*

The above question can be answered as follows.

Proposition 1.1. *Each q-optimum distribution consisting of $q^s = p^{es}$, $s \geq \frac{n(e-1)}{e}$, points is a p-optimum distribution of deficientce $\delta = n(e-1)$.*

For the proof of Proposition 1.1 we need a simple corollary of Definition 1.1.

Lemma 1.1. *Let $D \subset U^n$ be a q-optimum distribution consisting of q^s points. Then each elementary q-box $\Delta_A^M(q)$ contains exactly $q^{s-a_1-\ldots-a_n}$ points of D, provided that*

$$a_1 + \ldots + a_n \leq s. \tag{1.6}$$

It is worth noting that, in general, the number of points of D falling into a q-box $\Delta_A^M(q)$ with $a_1 + \ldots + a_n > s$ can not be precisely controled, this number is equal to 0 or 1 accidentally.

Proof. Since $a_1, \ldots, a_n$ satisfy (1.6), we may choose non-negative integers $c_1, \ldots, c_n$ to satisfy the quation $c_1 + \ldots + c_n = s - a_1 - \ldots - a_n$. Put $a_j = b_j - c_j$, $1 \leq j \leq n$, where $b_1 + \ldots + b_n = s$, then from (1.1) we obtain

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

Therefore, the q-box $\Delta_A^m(q)$ is a union of $q^{c_1+\ldots+c_n}$ disjoint q-boxes $\Delta_B^L(q)$, $B = (b_1, \ldots, b_n)$, of volume q^{-s}, and Lemma 1.1 follows from Definition 1.1. □

Proof of Proposition 1.1. Given an elementary p-box $\Delta_B^L(p)$ of volume $p^{n(e-1)-es}$. Put

$$b_j = ea_j - c_j, \qquad 0 \leq c_j \leq e - 1, \qquad 1 \leq j \leq n. \tag{1.7}$$

Since $b_1 + \ldots + b_n = es - n(e-1)$ (see (1.5)), we have

$$e(a_1 + \ldots + a_n) = es + c_1 + \ldots + c_n - n(e-1) \leq es. \tag{1.8}$$

Substituting (1.7) to (1.4), we find that

$$\Delta_B^L(p) = \left[\frac{p^{c_1} l_1}{q^{a_1}}, \frac{p^{c_1} l_1 + p^{c_1}}{q^{a_1}}\right) \ldots \left[\frac{p^{c_n} l_n}{q^{a_n}}, \frac{p^{c_n} l_n + p^{c_n}}{q^{a_n}}\right).$$

Therefore, the p-box $\Delta_B^L(p)$ is a union of $p^{c_1+\ldots+c_n}$ disjoint elementary q-boxes $\Delta_A^M(q)$, each of which has volume $q^{-a_1-\ldots-a_n}$ and in view of (1.8), contains exactly $q^{s-a_1-\ldots-a_n}$ points of D by Lemma 1.1. Hence the p-box $\Delta_B^L(p)$ contains exactly

$$p^{c_1+\ldots+c_n} q^{s-a_1-\ldots-a_n} = p^{es-b_1-\ldots-b_n} = p^{n(e-1)} = p^\delta$$

points of the distribution D. □

2. Distributions and codes

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

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

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

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

Moreover, we obviously 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 $X = (x_1, \dots, x_n)^T \in U^n$ we define its projection $\tau_s X$ onto $\mathbb{Q}^n(q^s)$ by setting

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

From the relations (2.2)–(2.4) we conclude that a point X falls into an elementary q-box $\Delta_A^M(q)$ of volume q^{-s} if and only if so does its projection $\tau_s X$. Thus, without loss of generality, we may further consider only q-optimum distributions which are subsets in $\mathbb{Q}^n(q^s)$.

For $x \in \mathbb{Q}(q^s)$ we will write the representation (1.3) also in the form

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

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

Let $\mathbb{F}_q$ be a finite field of $q = p^e$ elements. Fix a basis in $\mathbb{F}_q$ over $\mathbb{F}_p$, and represent elements $\mu = (\mu^{(1)}, \dots, \mu^{(e)}) \in \mathbb{F}_q$ as e-term sets of elements $\mu^{(i)} \in \mathbb{F}_p$ (cf. [5]). In so doing, elements of the field $\mathbb{F}_p$ are thought of as reduced residues $\{0, 1, \dots, p-1\}$ modulo p. With these conventions we have the following one-to-one correspondence between elements $\mu \in \mathbb{F}_q$ and integers $m \in \{0, 1, \dots, q-1\}$

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

By the use of the correspondence (2.6), the coefficients $\omega_i(x)$ 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

$$\boldsymbol{\omega}(x) = (\omega_1(x), \dots, \omega_n(x)) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q). \tag{2.7}$$

We denote by $\mathrm{Mat}_{n,s}(k)$ 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,

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

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 (2.9) for a distribution $D \subset \mathbb{Q}^n(q^s)$. In Sec. 4 we will see how q-optimum distributions can be characterized by their codes.

It might be well to mention that the structure of the vector space $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ can be transfered by (2.5), (2.7), and (2.8) 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

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

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

Remark 2.1. With respect to the arithmetic operations (2.10) $\mathbb{Q}^n(q^s)$ is a vector space of dimension ns over $\mathbb{F}_q$. Moreover, for each elementary q-box $\Delta_A^M(q)$, $A = (a_1, \dots, a_n)$, $0 \le a_j \le s$, $1 \le j \le n$, the intersection $V_A^M = \mathbb{Q}^n(q^s) \cap \Delta_A^M(q)$ is an affine subspace in $\mathbb{Q}^n(q^s)$ of dimension $ns - a_1 - \ldots - a_n$ parallel to the subspace $V_A^0 = \mathbb{Q}^n(q^s) \cap \Delta_A^0(q)$, that is $V_A^M = V_A^0 \oplus Y_A^M$, where a vector $Y_A^M \in \mathbb{Q}^N(q^s)$ is defined uniquely up to translations along the subspace V_A^0. We refer to [5] concerning geometry of vector spaces over finite fields.

3. A non-Hamming metric on the space $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$

We introduce the following non-Hamming *weight* ρ on the space $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Let $\boldsymbol{\omega} = (\omega_1, \dots, \omega_s) \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$. We put $\rho(0) = 0$, and

$$\rho(\boldsymbol{\omega}) = \max\{j : \omega_j \ne 0\} \tag{3.1}$$

for $\boldsymbol{\omega} \ne 0$. Obviously, $\rho(\boldsymbol{\omega}) > 0$ for $\boldsymbol{\omega} \ne 0$, $\rho(\alpha\boldsymbol{\omega}) = \rho(\boldsymbol{\omega})$ for $\alpha \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$, and

$$\rho(\boldsymbol{\omega} + \boldsymbol{\omega}') \le \max\{\rho(\boldsymbol{\omega}), \rho(\boldsymbol{\omega}')\} \le \rho(\boldsymbol{\omega}) + \rho(\boldsymbol{\omega}') \tag{3.2}$$

for all $\boldsymbol{\omega}$, $\boldsymbol{\omega}' \in \mathrm{Mat}_{a,s}(\mathbb{F}_q)$. Moreover, we have trivially

$$\rho(\boldsymbol{\omega}) \le s \tag{3.3}$$

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

Let $\Omega = (\boldsymbol{\omega}^{(1)}, \dots, \boldsymbol{\omega}^{(n)})^T \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$, $\boldsymbol{\omega}^{(j)} \in \mathrm{Mat}_{1,s}(\mathbb{F}_q)$, $1 \le j \le n$. We put

$$\rho(\Omega) = \sum_{j=1}^{n} \rho(\boldsymbol{\omega}^{(j)}). \tag{3.4}$$

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

$$\rho(\Omega + \Omega') \leq \rho(\Omega) + \rho(\Omega') \tag{3.5}$$

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

Recall that the Hamming weight $\varkappa(\Omega)$, $\Omega \in \mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$, is equal, by definition (cf. [5, 6]), to the number of non-zero entries in the matrix Ω. It is easily seen that the weights $\varkappa$ and ρ are related by

$$\varkappa(\Omega) \leq \rho(\Omega) \leq s\,\varkappa(\Omega), \tag{3.6}$$

and these inequalities can not be improved on the whole space $\mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$. In this sense the metric ρ is stronger than $\varkappa$ for large s. Certainly, in a special case of $s=1$ metrics ρ and $\varkappa$ coinside.

Using the relations (2.5), (2.7), and (2.8), the ρ-weight and ρ-metric can be transfered onto the set of all rational q-ary points $\mathbb{Q}^n(q^s)$ by setting

$$\rho(X) = \rho(\Omega(X)) \tag{3.7}$$

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

$$\rho(X \ominus X') = \rho(\Omega(X) - \Omega(X')) \tag{3.8}$$

for the ρ-distance between two points $X,\ X' \in \mathbb{Q}^n(q^s)$. In (3.8) 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 $\rho(\mathcal{C})$ is defined by

$$\rho(\mathcal{C}) = \min\{\rho(\Omega - \Omega')\ :\ \Omega,\ \Omega' \in C, \Omega \neq \Omega'\}. \tag{3.9}$$

Notice that if a code coinsides with the whole space, then

$$\rho(\mathrm{Mat}_{\,n,s}(\mathbb{F}_q)) = 1, \tag{3.10}$$

that follows at once from the definitions (3.1), (3.4), and (3.9).

Proposition 3.1. *Let $\mathcal{C} \subset \mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$ be a code consisting of q^{ks}, $1 \leq k \leq n$, elements, then*

$$\rho(\mathcal{C}) \leq (n-k)s + 1. \tag{3.11}$$

Proof. For each $1 \leq k \leq n$ and $\Omega \in \mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$ we denote by $\pi_k\Omega$ a matrix whose first k rows coinside with first k rows of Ω and last $n-k$ rows are zeros. We have $\Omega = \pi_k\Omega + \Xi_k$ with a matrix Ξ_k whose first k rows are zeros, and the definition (3.4) implies

$$\rho(\Omega) = \rho(\pi_k\Omega) + \rho(\Xi_k). \tag{3.12}$$

From (3.1) and (3.3) we conclude that $\rho(\Xi_k) \leq (n-k)s$. Hence, using (3.9) and (3.12), we obtain the inequality

$$\rho(\mathcal{C}) \leq (n-k)s + \min\{\rho(\pi_k\Omega - \pi_k\Omega') : \Omega,\ \Omega' \in \mathcal{C}, \Omega \neq \Omega'\}. \tag{3.13}$$

Now we observe that the cardinalities of the code $\mathcal{C}$ and the space $\pi_k\mathrm{Mat}_{\,n,s}(\mathbb{F}_q) = \mathrm{Mat}_{\,k,s}(\mathbb{F}_q)$ coinside and are equal to q^{ks}. Therefore, there are only two opportunities: either $\pi_k\Omega = \pi_k\Omega'$ for two distinct matrices $\Omega, \Omega' \in \mathcal{C}$, and in this case the second term at the right side of (3.13) is equal to 0, or $\pi_k C = \mathrm{Mat}_{\,n,s}(\mathbb{F}_q)$, and in such case the second term at the right side of (3.13) is equal to 1 (cf. (3.10)). In both cases the bound (3.11) holds. □

Proposition 3.1 naturally leads to the following.

Definition 3.1. *A code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ consisting of q^{ks}, $1 \le k \le n$, points is called the maximum distance code if its weight $\rho(\mathcal{C}) = (n-k)s + 1$.*

4. Optimum distributions and maximum distance codes

Our first result on optimum distributions is the following observation.

Theorem 4.1. *Let $D \subset \mathbb{Q}^n(q^s)$ be a distribution consisting of q^s points 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 a q-optimum distribution.*
(ii) *$\mathcal{C}\langle D\rangle$ is a maximum distance code.*

For the proof of Theorem 4.1 we need the following.

Lemma 4.1. (i) *A given point $X \in \mathbb{Q}^n(q^s)$ falls into an elementary q-box $\Delta^0_A(q)$ of volume q^{-s} if and only if the weight $\rho(X) \le (n-1)s$.*

(ii) *Two given points X and $X' \in \mathbb{Q}^n(q^s)$ fall simultaneously into an elementary q-box $\Delta^M_A(q)$ of volume q^{-s} if and only if the distance $\rho(X \ominus X') \le (n-1)s$.*

Proof. First of all we notice that the definition (2.1) and the representation (1.5) imply the inequality

$$x = \sum_{i=1}^{\rho(x)} \omega_i(x) q^{i-s-1} \le (q-1) \sum_{i=1}^{\rho(x)} q^{i-s-1} < q^{\rho(x)-s} \tag{4.1}$$

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

$$x = \sum_{i=1}^{\rho(x)} \omega_i(x) q^{i-s-1} \ge q^{\rho(x)-s-1} \tag{4.2}$$

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

(i) Let $\rho(X) \le (n-1)s$. Writing the inequality (4.1) for all coordinates of the point $X = (x_1, \dots, x_n)^T \in \mathbb{Q}^n(q^s)$ and using the definition (1.1), we conclude that $X \in \Delta^0_{A(X)}(q)$ 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

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

Hence, there exists an elementary q-box Δ^0_A of volume q^{-s}, such that $A^0_A \supset \Delta^0_{A(X)} \ni X$.

Let $\rho(X) > (n-1)s$. Writing the inequality (4.1) for all non-zero coordinates of the point $X = (x_1, \dots, x_n)^T \in \mathbb{Q}^n(q^s)$ and using the definition (1.1), we observe the following: if the point X falls into an elementary q-box $\Delta^0_A(q)$, $A = (a_1, \dots, a_n)$, then $a_j \le s - \rho(x_j)$ for $x_j > 0$ and $a_j \le s$ for $x_j = 0$. Since $\rho(0) = 0$, we have

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

Hence, by (1.2), the box $\Delta^0_A(q)$ has volume greater than q^{-s}.

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 Remark 2.1. □

Proof of Theorem 4.1. (i) Let D be a q-optimum distribution. Then, by Definition 1.1, each elementary q-box $\Delta_A^M(q)$ of volume q^{-s} contains exactly one point of D, and by the statement (ii) of Lemma 4.1, the distance $\rho(X \ominus X') > (n-1)s$ for any pair of distinct points X and $X' \in D$. Therefore, by and Definition 3.1, $\mathcal{C}\langle D\rangle$ is a maximum distance code.

(ii) Let $\mathcal{C}\langle D\rangle$ be a maximum distance code consisting of q^s elements. Then, by Definition 3.1, the distance $\rho(X \ominus X') > (n-1)s$ for any pair of distinct points X and $X' \in D$, and by the statement (ii) of Lemma 4.1, each elementary q-box $\Delta_A^M(q)$ of volume q^{-s} 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 $a_1 + \dots + a_n = s$ the number of the corresponding q-boxes $\Delta_A^M(q)$, $M = (m_1, \dots, m_n) \in \mathbb{N}_0^n$, $m_j \in \{0, 1, \dots, q^{a_j} - 1\}$, $1 \le j \le n$, is equal to q^s, that coinsides with the cardinality of D. Therefore, each elementary q-box $\Delta_A^M(q)$ of volume q^{-s} contains exactly one point of D. Thus, D is a q-optimum distribution.
$\square$

It should be emphasize that maximum distance codes $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ consisting of q^{ks} elements with $k > 1$ can not generate distributions with very low discrepancies. Raughly speaking, denominators of the order q^s in (2.5) are too small to provide a well distribution of the corresponding q^{ks} points. Here we state only one result on such distributions.

Introduce the following subset of elementary q-boxes (1.1)

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

Theorem 4.2. *Let $D \subset \mathbb{Q}^n(q^s)$ be a distribution consisting of q^{ks}, $1 \le k \le n$, points 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) *Each elementary q-box $\Delta_A^M(q) \in \mathfrak{E}_s$ of volume q^{-ks} contains exactly one point of D.*

(ii) *$\mathcal{C}\langle D\rangle$ is a maximum distance code.*

The proof of Theorem 4.2 is quite similar to the proof of Theorem 4.1 and is not given here.

5. Hermite interpolations over finite fields

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

$$f(z) = \sum_{i=0}^{d} f_i z^i \tag{5.1}$$

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

$$\partial^j f(z) = \sum_{i=0}^{d} \binom{i}{j} f_j z^{i-j} \tag{5.2}$$

where $\binom{i}{j}$ are binomial coefficients modulo p, moreover, as it usually is, $\binom{i}{j} = 0$ for $j > i$ (cf. [5, Sec. 6.4]). In particulary,

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

for each $\beta \in \mathbb{F}_q$.

Using (5.2) and (5.3), it is easy check the following expansion

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

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

It should be noting 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, for polynomials over a field of infinite characteristic the relation (5.5) should hold for all $j \in \mathbb{N}_0$.

We can formally add a point ∞ to $\mathbb{F}_q$. In so doing, all the 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 d we put by definition

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

Obviously, $\partial^j f(\infty) = \partial^j \tilde{f}(0)$, where $\tilde{f}(z) = z^d f(\frac{1}{z}) = f_d + f_{d-1}z + \ldots + f_0 z^d$ is a polynomial receprocal to $f(z)$.

Let $\mathbb{M}^t \subset \mathbb{F}_q[z]$ denote a set of all polynomials of degree less than t, $\mathbb{M}^t$ is a vector space of dimension t over $\mathbb{F}_q$.

Henceforward we assume that

$$q \ge n - 1. \tag{5.7}$$

Consider the following *Hermite interpolation problem*: I there a polynomial $f \in \mathbb{M}^t$ which satisfies the equations

$$\partial^j f(\beta_i) = a_i^{(j)}, \quad j = 0, \ldots, t_i - 1, \quad i = 1, \ldots, l, \quad 1 \le l \le n, \tag{5.8}$$

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?

Concerning the usual Hermite interpolations over the fields of real and complex numbers we refer to [2, Chap. 2, Sec. 11].

Proposition 5.1. (i) *The Hermite interpolation problem* (5.8) *has a unique solution* $f \in \mathbb{M}^t$, *provided that* $t_1 + \ldots + t_l = t$.

(ii) *The homogeneous Hermite interpolation problem* (5.8) *with all coefficients* $a_i^{(j)} = 0$ *has a unique solution* $f = 0$ *in the space* $\mathbb{M}^t$, *provided that* $t_1 + \ldots + t_l \ge t$.

Proof. (i) First, we suppose that $\beta_i \in \mathbb{F}_q$, $1 \le i \le l$, that is, no one of interpolation nodes coinsides with ∞. We introduce the polynomials

$$r_i(z) = \sum_{j=0}^{t_i - 1} a_i^{(j)} (z - \beta_i)^j, \quad 1 \le i \le l. \tag{5.9}$$

Using (5.3), (5.4), and (5.9), we observe that the equation (5.7) are equivalent to the following congruences in the ring $\mathbb{F}_q[z]$

$$f(z) = r_i(z) \bmod (z - \beta_i)^{t_i}, \quad 1 \le i \le l. \tag{5.10}$$

In (5.10) the polynomials $(z - \beta_i)^{t_i}$, $1 \le i \le l$, are pairwise coprime. Therefore, the congrunces (5.10) 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, e.g., [6, Sec. 10.9, Theorem 5]).

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

$$f(z) = g(z) + r_l(z), \tag{5.11}$$

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 (5.11) 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 $\beta_1, \ldots, \beta_{l-1} \in \mathbb{F}_q$

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

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 $t_i' \in \mathbb{N}$, $t_i' \le t_i$ to satisfy the equality $t_1' + \ldots + t_l' = t$. □

6. Explicit constructions of maximum distance codes and optimum distributions

Fix n distinct elements $\beta_1, \ldots, \beta_n \in \mathbb{F}_q \cup \infty$ (cf. (5.7)), and define a linear mapping $\Gamma : \mathbb{M}^t \to \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ by setting

$$\Gamma : \mathbb{M}^t \ni f \to \Gamma f = (\partial^{s-1-j} f(\beta_i))_{\substack{0 \le j \le s-1 \\ 1 \le i \le n}} \in \mathrm{Mat}_{n,s}(\mathbb{F}_q). \tag{6.1}$$

Thus, for each polynomial $f \in \mathbb{M}^t$ the matrix $\Gamma f = (\boldsymbol{\omega}_f^{(1)}, \ldots, \boldsymbol{\omega}_f^{(n)})^T \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ consists of n rows of the form

$$\boldsymbol{\omega}_f^{(i)} = (\partial^{s-1} f(\beta_i), \ldots, \partial f(\beta_i), f(\beta_i)) \in \mathrm{Mat}_{n,s}(\mathbb{F}_q), \quad 1 \le i \le n. \tag{6.2}$$

Lemma 6.1. *For $t \le ns$, the image $\Gamma(\mathbb{M}^t)$ of the vector space $\mathbb{M}^t$ under the mapping* (6.1) *is a subspace of dimension t in* $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$.

Proof. Since $\mathbb{M}^t \subset \mathbb{M}^{ns}$ for $t \le ns$, it sufficies to show that $\Gamma(\mathbb{M}^{ns}) = \mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Let $f \in \mathbb{M}^{ns}$ and $\Gamma f = 0$, then from (5.1) we conclude that f is a solution of a homogeneous Hermite interpolation problem (5.8) with $l = n$, $t = ns$ and $t_1 = m_1 = t_n = s$. Therefore, $f = 0$ by Proposition 5.1. □

Now we can describe our explicit constructions of maximum distance codes and optimum distributions.

Theorem 6.1. *For each $1 \leq k \leq n$ the subspace $\Gamma(\mathbb{M}^{ks}) \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ is a maximum distance code consisting of q^{ks} elements.*

Codes $\mathcal{C}$ which are subspaces in $\mathrm{Mat}_{n,s}(\mathbb{F}_q)$ are said to be *linear codes* (cf. [5, 6]). Notice that for a linear code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ the formula (3.9) for the weight $\rho(\mathcal{C})$ takes the form

$$\rho(\mathcal{C}) = \min\{\rho(\Omega) : \Omega \in \mathcal{C} \setminus \{0\}\}. \tag{6.3}$$

Proof of Theorem 6.1. By Definition 3.1 and the relations (6.3), it suffices to show that $\rho(\Gamma f) \geq (n-k)s + 1$ for all $f \in \mathbb{M}^{ks} \setminus \{0\}$. Suppose on the contrary that there is a non-zero polynomial $f \in \mathbb{M}^{ks}$ such that $\rho(\Gamma f) \leq (n-k)s$. By (3.4) and (6.1), (6.2), this yields

$$\rho(\Gamma f) = \rho(\boldsymbol{\omega}_f^{(1)}) + \ldots + \rho(\boldsymbol{\omega}_f^{(n)}) \leq (n-k)s. \tag{6.4}$$

From (6.4) we conclude that the following strict inequality

$$\rho(\boldsymbol{\omega}_f^{(i)}) < s \tag{6.5}$$

holds at last for k distinct indices i. Without loss of generality, we may assume that the inequality (6.5) holds for $i = 1, \ldots, l$ with $l \geq k$ and $\rho(\boldsymbol{\omega}_f^{(i)}) = s$ for $i = l+1, \ldots, n$.

Using (6.1), (6.2) and (6.5), we observe the polynomial $f \in \mathbb{M}^{ks}$ is a solution of the following homogeneous Hermite interpolation problem (5.8):

$$\partial^j f(\beta_i) = 0, \quad j = 0, \ldots, t_i - 1, \quad i = 1, \ldots, l, \tag{6.6}$$

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

It is easy to check that $t_1 + \ldots + t_l = ns - \rho(\Gamma f)$. Therefore, $t_1 + \ldots + t_l \geq ks$ and $f = 0$ by Proposition 5.1, a contradiction. $\square$

Thus, we have constructed a broad class of linear maximum distance codes in the metric ρ.

For $k = 1$ Theorem 6.1 gives a maximum distance code $\Gamma(\mathbb{M}^s) \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ which, by Theorem 4.1, is the code (2.9) of a q-optimum distribution. Precisely, we define a distribution $\mathfrak{D} \subset \mathbb{Q}^n(q^s)$ consisting of q^s points by

$$\mathcal{C}\langle\mathfrak{D}\rangle = \Gamma(\mathbb{M}^s) \tag{6.7}$$

From (6.1), (6.2) and (2.5), (2.8), (2.9), we find that coordinates of a point $X = (x_1, \ldots, x_n)^T \in \mathbb{D}$ are given by

$$x_i = \sum_{j=1}^{s} \partial^j f(\beta_i) q^{-j}, \tag{6.8}$$

where $f(z) = f_0 + f_1 z + \ldots + f_{s-1} z^{s-1} \in \mathbb{M}^s$.

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

$$\partial^j f(\beta_i) = \sum_{l=0}^{d} \binom{j}{l} (\beta_i)^{l-j} f_l \tag{6.9}$$

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

$$\partial^j f(\beta_i) = f_{s-1-j} \tag{6.10}$$

for $\beta_i = \infty$.

Comparing Theorems 4.1, 6.1 and Proposition 1.1, we immediately obtain the following.

Theorem 6.2. *Let $q = p^e \geq n-1$, and $\mathfrak{D} \subset \mathbb{Q}^n(q^s)$ be the distribution of q^s points defined by (6.7). Then,*

(i) *$\mathfrak{D}$ is a q-optimum distribution.*

(ii) *$\mathfrak{D}$ is a p-optimum distribution of deficient $\delta = n(e-1)$.*

Thus, for a given prime p, say $p = 2$, in any dimension n a minimal $e \in \mathbb{N}$ should be chosen to satisfy the inequality $p^e \geq n-1$, and the corresponding distribution $\mathfrak{D}$, given by (6.7)–(6.10), will be a p-optimum distribution of deficient $\delta = n(e-1) = O_p(n \log n)$. Moreover, in practice, points of the distribution $\mathfrak{D}$ can be easily produced with the help of the relations (6.8)–(6.10).

It must be emphasized that 2-optimum distributions of deficient $\delta = O(n \log n)$ were first given by Sobol [7] and for $q = p \geq n-1$ the p-optimum distributions $\mathfrak{D}$ were first constructed by Faure [3].

7. Weight spectra

In this section we give additional results which show a parallelism between uniform distributions and error-correcting codes.

Definition 7.1. *Given a code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$. The following sequence of non-negative integers*

$$w_t(\Omega') = \#\{\Omega \in \mathcal{C} : \rho(\Omega - \Omega') = t\}, \quad 0 \leq t \leq ns, \tag{7.1}$$

is called the weight spectrum of the code $\mathcal{C}$ relatively to an element $\Omega' \in \mathcal{C}$.

A remarkable thing is that weight spectra of all maximum distance codes can be precisely given. A similar phenomenon is well known in the coding theory for the Hamming metric (see [6, Chapter 11]).

We introduce a sequence of natural numbers $\sigma(t)$, $t \in \mathbb{N}$, $0 \leq t \leq ns$, by setting

$$\sigma(t) = \{A = (a_1, \ldots, a_n) \in \mathbb{N}^n : a_1 + \ldots + a_n = t,\ 0 \leq a_j \leq s,\ 1 \leq j \leq n\}. \tag{7.2}$$

In the following, $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ are the usual binomial coefficients, moreover $\binom{n}{i} = 0$ for $i > n$.

Theorem 7.1. *Let $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ be a maximum distance code consisting of q^s elements. Then weights (7.1) are independent of the element $\Omega' \in \mathcal{C}$, and $w_t = w_t(\Omega')$ are given by*

$$w_0 = 1, \quad w_t = 0 \tag{7.3}$$

for $0 < t < \rho(\mathcal{C}) = (n-1)s + 1$,

$$\begin{aligned} w_t &= \sigma(t) \sum_{i=0}^{t-\rho(\mathcal{C})} (-1)^i \binom{n}{i} (q^{t-\rho(\mathcal{C})+1-i} - 1) \\ &= \sigma(t)(q-1) \sum_{i=0}^{t-\rho(\mathcal{C})} (-1)^i \binom{n-1}{i} q^{t-\rho(\mathcal{C})-i}, \end{aligned} \tag{7.4}$$

for $\rho(\mathcal{C}) \leq t \leq ns$. In particular,

$$w_t = \sigma(t)(q-1)^n q^{t-\rho(\mathcal{C})-n+1} \tag{7.5}$$

for $\rho(\mathcal{C})+n-1 \le t \le ns$.

Here we do not consider maximum distance codes $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ consisting of q^{ks}, $k>1$, elements because the corresponding explicit formulas for weight spectra are much more complicated.

From the relation (7.3) we find first non-trivial terms in the weight spectrum

$$w_{\rho(\mathcal{C})} = \sigma(\rho(\mathcal{C}))(q-1), \tag{7.6}$$

and

$$w_{\rho(\mathcal{C})+1} = \sigma(\rho(\mathcal{C})+1)(q-1)(q-n+1) \tag{7.7}$$

Certainly, writing the relation (7.7), we assume that $\rho(\mathcal{C})+1 \le ns$, this means that $s>1$. Obviously, the quantity (7.7) has to be non-negative. This observation together with Theorem 4.1 implies the following corollary.

Theorem 7.2. *Let* $q < n-1$ *and* $s>1$. *Then there exist neither maximum distance codes* $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ *consisting of* q^s *elements nor* q*-optimum distributions* $D \subset \mathbb{Q}^n(q^s)$ *consisting of* q^s *points.*

It is worth to mention that a direct proof of Theorem 7.2, independing of the consideration of weight spectra, can be also given (cf. [1, Lemma 3.27]).

For the proof of Theorem 7.1 we need to consider the structure of spheres in the metric ρ. In the following, it is convenient to deal with distributions instead of their codes. Let

$$\Sigma_t = \{X \in \mathbb{Q}^n(q^s) : \rho(X) = t\}, \quad 0 \le t \le ns \tag{7.8}$$

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

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

$$[0,1) = \bigcup_{0 \le b \le s} g_b, \tag{7.9}$$

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

$$U^n = \bigcup_B G_B, \quad G_B = \prod_{j=1}^n g_{b_j}, \tag{7.10}$$

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 7.1. *Each sphere* (7.8) *is a union of the following fragments*

$$\Sigma_t = \bigcup_{b_1+\ldots+b_n=t} G_B. \tag{7.11}$$

The number of fragments in the union (7.11) *is equal to* $\sigma(t)$ *(see* (7.2)*).*

Proof. Comparing the q-ary representation (2.5) with the definition of the ρ-weight (3.1) and subintervals g_b in (7.9), we observe the following: a point $x \in \mathbb{Q}(q^s)$ belongs to a subinterval g_b

if and only 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 Σ_t if and only if X belongs to one of fragments G_B with $b_1 + \ldots + b_n = t$. □

Proof of Theorem 7.1. First of all, from Definition 3.1 we conclude that if $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ is a maximum distance code, then so is any code $\mathcal{C} + \Omega'$ shifted by an arbitrary element $\Omega' \in \mathrm{Mat}_{n,s}(\mathbb{F}_q)$. Thus, without loss of generality, in proving of the relations (7.3), (7.4), (7.5), we may assume that $0 \in \mathcal{C}$ and consider the weight spectrum (7.1) only relatively to the element $\Omega' = 0$. To simplify the notations we put $w_t = w_t(0)$.

Notice also that the relations (7.3) hold trivially, in view of Definition 3.1. Thus, we have to consider only weights w_t with $t \geq \rho(C) = (n-1)s + 1$.

By Theorem 4.1 we can identify a given maximum distance code $\mathcal{C} \subset \mathrm{Mat}_{n,s}(\mathbb{F}_q)$ with the corresponding q-optimum distribution $D \subset \mathbb{Q}^n(q^s)$, $\mathcal{C} = \mathcal{C}\langle D\rangle$, and we can consider the distribution D instead of the code $\mathcal{C}$. In so doing, we assume that the origin $0 \in D$.

From Lemma 7.1 we obtain the relation

$$w_t = \#\{D \cap \Sigma_t\} = \sum_{b_1+\ldots+b_n=t} \#\{D \cap G_B\}. \tag{7.12}$$

Notice that in (7.12) no one of the b_j, $1 \leq j \leq n$, is equal to zero, because $b_1 + \ldots + b_n = t \geq (n-1)s + 1$ and $0 \leq b_j \leq s$. Hence, the boxes G_B involved in (7.12) have the following representation in terms of elementary q-boxes (1.1)

$$G_B = \Delta^0_{A_0}(q) \setminus \bigcup_{1 \leq i \leq n} \Delta^0_{A_i}(q), \tag{7.13}$$

where $A_0 = (a_1^{(0)}, \ldots, a_n^{(0)})$ with $a_j^{(0)} = s - b_j$, and $A_i = (a_1^{(i)}, \ldots, a_n^{(i)})$ with $a_j^{(i)} = s - b_j$ if $j \neq i$ and $a_i^{(i)} = s - b_i + 1$. Moreover, we have the equality

$$a_1^{(0)} + \ldots + a_n^{(0)} = ns - b_1 - \ldots - b_n = ns - t. \tag{7.14}$$

Let $I = \{i_1, \ldots, i_l\} \subset \{1, \ldots, n\}$ be a subset of l distinct indices, then

$$\Delta^0_{A_{i_1}}(q) \cap \ldots \cap \Delta^0_{A_{i_l}}(q) = \Delta^0_{A_I}(q), \tag{7.15}$$

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

$$a_j^{(I)} = \max\{a_j^{(i_1)}, \ldots, a_j^{(i_l)}\} = \begin{cases} s - b_j & \text{if } j \neq i_1, \ldots, i_l, \\ s - b_j + 1 & \text{if } j = i_1, \ldots, i_l. \end{cases}$$

Moreover, we have the equality

$$a_1^{(I)} + \ldots + a_n^{(I)} = ns - t + l. \tag{7.16}$$

Applying the principle of inclusion and exclusion to the summand $\#\{D \cap G_B\}$ in (7.12), and using the relations (7.13), (7.15), we obtain the formula

$$\#\{D \cap G_B\} = \#\{D \cap \Delta^0_{A_0}(q)\} - \sum_{l=1}^{n} \sum_{I:\#\{I\}=l} (-1)^l \#\{D \cap \Delta^0_{A_I}(q)\}, \tag{7.17}$$

where the inner sum is taken over all $\binom{n}{l}$ subsets $I = \{i_1, \dots, i_l\} \subset \{1, \dots, n\}$.

Now, we observe the following: Let $\Delta^0_A(q)$ be an elementary q-box (1.1) with an arbitrary $A = (a_1, \dots, a_n) \in \mathbb{N}^n_0$, then

$$\#\{D \cap \Delta^0_A(q)\} = \begin{cases} q^{s-a_1-\dots-a_n} & \text{if } a_1 + \dots + a_n < s, \\ 1 & \text{if } a_1 + \dots + a_n \geq s. \end{cases} \tag{7.18}$$

The first equality (7.18) follows from Lemma 1.1, and the second follows from the proposition (i) of Lemma 4.1 and the above assumption that $0 \in D$.

Substituting (7.18) to (7.17), and using (7.14), (7.16), we find that

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

$$= \sum_{i=0}^{t-\rho(\mathcal{C})} (-1)^i \binom{n}{i} (q^{t-\rho(\mathcal{C})+1-i} - 1) = (q-1) \sum_{i=0}^{t-\rho(\mathcal{C})} (-1)^i \binom{n-1}{i} q^{t-\rho(\mathcal{C})-i}. \tag{7.19}$$

Notice that in the calculation (7.19) we used well known identities for binomial coefficients, as for instance, $\sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$ and $\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1}$

Substituting (7.19) to (7.12), and using (7.2), we obtain the relations (7.4). $\square$

An acknowledgment. I wish to express my sincere thanks to William Chen for numerous valuable discussions on the matter of uniform distributions.

References

[1] J. Beck, W. W. L. Chen, *Irregularities of distributions*, Cambridge Univ. Press, 1987.

[2] I. S. Berezin, N. P. Zhidkov, *Computing methodes*, vol. 1, Nauka, Moscow, 1962; English transl.: Addison-Wesley, Reading Mass., 1965.

[3] H. Faure, *Descrépance de suites associées à un systme de numération (en dimension s)*, Acta Arith., **41** (1982), 337–351.

[4] L. Kuipers, H. Niederreiter, *Uniform distribution of sequences*, John Wiley & Sons, New York etc., 1974.

[5] R. Lidl, H. Niederreiter, *Finite fields*, Addison-Wesley, London etc., 1983.

[6] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[7] I. M. Sobol, *On the distribution of points in a cube and the approximate evaluation of integrals*, Ž. Vyčisl. Mat. i Mat. Fiz. **7** (1967), 784–802; English transl. in U.S.S.R. Comp. Math. and Math. Phys., **7** (1967), 86–112.