ISSN 0032-9460, Problems of Information Transmission, 2022, Vol. 58, No. 4, pp. 352–371. © Pleiades Publishing, Inc., 2022.
Russian Text © The Author(s), 2022, published in Problemy Peredachi Informatsii, 2022, Vol. 58, No. 4, pp. 62–83.

CODING THEORY

On Codes with Distances d and n

P. Boyvalenkov[a,*], **K. Delchev**[a,**], **V. A. Zinoviev**[b,***], **and D. V. Zinoviev**[b,****]

[a] *Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria*
[b] *Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia*
e-mail: *peter@math.bas.bg, **kdelchev@math.bas.bg, ***vazinov@iitp.ru, ****dzinov@iitp.ru

Received November 14, 2022; revised November 25, 2022; accepted November 28, 2022

Abstract—We enumerate all q-ary additive (in particular, linear) block codes of length n and cardinality $N \geq q^2$ with exactly two distances: d and n. For arbitrary codes of length n with distances d and n, we obtain upper bounds on the cardinality via linear programming and using relationships to 2-distance sets on a Euclidean sphere.

Key words: two-distance code, two-weight code, linear two-weight code, difference matrix, maximal arc, Latin square, orthogonal array, bounds for codes, linear programming bounds, spherical code.

DOI: 10.1134/S0032946022040068

1. INTRODUCTION

We consider q-ary block codes of length n with only two distances, d and n. Codes with two distances are a classical object in algebraic coding theory for more than 55 years. A comprehensive survey of such codes can be found in [1]. The construction of new families of such codes, as well as the description of some existing classes of such codes, remain to be important open problems in algebraic coding theory (see, e.g., [2] and references therein). In spite of many known infinite classes of two-weight codes, a complete classification of linear two-weight codes is far from being completed. Even in the case of codes with distances d and n, we could not say before this paper that all such codes are known.

In two previous papers [3,4], we classified such codes for the special case where the two distances are d and $d + 1$ and showed that all such codes come from equidistant codes in two ways: by either adding one arbitrary coordinate position (so that to preserve the linearity of the code) to all codewords or deleting one arbitrary position from all codewords. Then in [5,6] we considered arbitrary linear and nonlinear codes with two weights d and $d + \delta$ and strengthened the known results of Delsarte [7,8] on necessary conditions for the existence of such projective codes. We should also refer to [9], where by characterizing arcs in projective geometry $\mathrm{PG}(r, q)$ with multiplicities of hyperplanes w, $w + 1$, and $w + 2$, all q-ary linear codes with distances d, $d + 1$, and $d + 2$ were classified.

The main goal in this paper is to enumerate additive and nonadditive (including distance invariant) block codes of length n with exactly two distances for a very special case where these distances are d and n. It is interesting that linear such codes have generator matrices related to generator matrices of equidistant linear codes (they are obtained from the latter by adding the all-zero column and then the all-one row). This phenomenon was described in [10] in terms of completely regular codes with covering radius $\rho = 2$. We give necessary and sufficient conditions for the existence of such codes and obtain simple descriptions of these codes. Some new upper bounds on the cardinality of arbitrary (unrestricted) such codes with exactly two distances d and n are also obtained. One of them is a linear programming bound, and another one comes from spherical codes with exactly two Euclidean distances.

2. PRELIMINARY RESULTS

Let $q \geq 2$ be a positive integer, and for the rest of the paper let $Q = \{0, 1, \ldots, q-1\}$ be an additive abelian group with a neutral element 0. Any subset $C \subseteq Q^n$ is a code of length n, cardinality $N = |C|$, and minimum (Hamming) distance d (i.e., $d = \min\{d(x, y) : x, y \in C, x \neq y\}$), where

$$d(x, y) = |\{i\} : x_i \neq y_i,\ i = 1, \ldots, n\}|, \quad \text{for } x = (x_1, \ldots, x_n) \text{ and } y = (y_1, \ldots, y_n);$$

such a code is denoted by $(n, N, d)_q$. If q is a prime power, then Q is the set of elements of the Galois field $\mathbb{F}_q$, which we also denote by $0, 1, \ldots, q-1$ though perform operations in $\mathbb{F}_q$. If an $(n, N, d)_q$ code C is a k-dimensional subspace of the linear space Q^n, then we use for C the standard notation $[n, k, d]_q$, where $N = q^k$. For the binary case, i.e., when $q = 2$, we omit q and use the notation (n, N, d) and $[n, k, d]$, respectively. Here by an *additive* code we mean a code which is an abelian subgroup in the abelian group Q^n under the additive componentwise operation in Q (thus, these codes include also linear codes).

Denote by $(n, N, \{d, n\})_q$ and $(n, N, d)_q$ a code $C \subset Q^n$ with the following property: for any two distinct codewords x and y of C, the Hamming distance $d(x, y)$ equals either d or n. Unless otherwise stated, we always assume that both distances d and n are realized in such a code.

We are interested in existence, construction, and classification results and also in upper bounds on the maximum possible size of an arbitrary such code.

We do not consider trivial cases like, for example, repetitions of two (or more) $(n_1, N, \{d_1, n_1\})_q$ and $(n_2, N, \{d_2, n_2\})_q$ codes with the same or different parameters, equidistant codes, codes with trivial (i.e., constant) positions, etc.

Definition 1. Let G be an abelian group of order q written additively. A square matrix D of order $q\mu$ with elements from G is called a difference matrix and is denoted by $D(q, \mu)$ if the componentwise difference of any two different rows of D contains every element of G exactly μ times.

Clearly, the matrix D is invariant under adding a constant vector $(a, a, \ldots, a)$, where $a \in G$, to any row or column of D. By performing such operations, we can always obtain a *normalized* difference matrix which has the zero first row and zero first column. Furthermore, unless otherwise stated, we always assume without loss of generality that a difference matrix is represented in normalized form.

From [11] (see also [12]) we have the following result.

Lemma 1. *For any prime power q and any positive integers ℓ and h there exists a difference matrix $D(q^\ell, q^h)$.*

We briefly describe the construction of all such difference matrices $D(q^\ell, q^h)$ from [12]. For any integer $m \geq 1$, fix a one-to-one correspondence between the elements of $\mathbb{F}_{p^m}$ and of the vector space $\mathbb{F}_p^m$. For any positive integers ℓ and h, denote $u = \ell + h$. For the Galois field $\mathbb{F}_{q^u}$ with elements $\{f_0 = 0,\ f_1 = 1,\ f_2,\ \ldots,\ f_{p^u-1}\}$, denote by $F = [f_{i,j}]$ the matrix of size $q^u \times q^u$ whose rows and columns are indexed by the elements of $\mathbb{F}_{q^u}$, where $f_{i,j} = f_i f_j$; i.e., F is the multiplication table for the elements of $\mathbb{F}_{q^u}$. Define the operator $\Phi = \Phi_{u\to\ell}$ which maps elements $x = (x_1, \ldots, x_u)$ of $\mathbb{F}_q^u$ to elements $x^{(\ell)} = (x_1, \ldots, x_\ell)$ of $\mathbb{F}_q^\ell$ by cutting the last (rightmost) $u - \ell$ positions of vectors from $\mathbb{F}_q^u$:

$$\Phi_{u\to\ell}(x_1, \ldots, x_\ell, \ldots, x_u) = (x_1, \ldots, x_\ell).$$

Denote by $F^{[\ell]}$ the matrix obtained from F by applying the operator Φ to all elements of F:

$$F^{[\ell]} = \left[f_{i,j}^{[\ell]}\right]: \quad f_{i,j}^{[\ell]} = \Phi_{u\to\ell}(f_{i,j}).$$

Now we obtain the following fact [11] (see also [12]).

Lemma 2. *For any prime power q and any positive integers ℓ and h, the matrix $F^{[\ell]}$ is an additive difference matrix $D = D(q^\ell, q^h)$. If ℓ divides h, i.e., $N = q^{h/\ell+1}$, then $F^{[\ell]}$ is a vector space, implying that the difference matrix D is linear.*

Let us explain the construction of the $(n, N, \{d, n\})_q$ code based on the difference matrix $D(q, \mu)$ over G. In the case at hand we have $G = \mathbb{F}_q$. Assume that the first row of D consists of zeros. Denote by $D^{(g)}$ the matrix obtained from D by adding the element $g \in G$ to all elements of D; i.e., if $D = [d_{i,j}]$, then $D^{(g)} = [d_{i,j} + g]$ for all i and j (recall that the addition is in G). By the definition of D, the matrix $D^{(g)}$ is a difference matrix $D(q, \mu)$. It follows also that for any two rows, $\boldsymbol{r}$ from D and $\boldsymbol{r}^{(g)}$ from $D^{(g)}$, the following property is valid [12]:

$$d(\boldsymbol{r}, \boldsymbol{r}^{(g)}) = \begin{cases} q\mu & \text{if } \boldsymbol{r}^{(g)} = \boldsymbol{r} + (g, g, \ldots, g), \\ (q-1)\mu & \text{if } \boldsymbol{r}^{(g)} \neq \boldsymbol{r} + (g, g, \ldots, g). \end{cases} \tag{1}$$

Clearly, the matrix $D(q, \mu)$ induces an equidistant $(q\mu - 1, q\mu, \mu(q-1))_q$ code which is optimal with respect to the Plotkin upper bound

$$N \le \frac{qd}{qd - (q-1)n} \tag{2}$$

provided that the denominator is positive. To see this, firstly, we have to transform D to the form which has the zero first column and, secondly, delete this trivial column. From (1) we obtain the following result.

Lemma 3 [12]. *Rows of the $N \times n$ matrix $\left[D^{(0)} \mid \ldots \mid D^{(q-1)}\right]^t$ form a two-weight $(n, N, \{d, n\})_q$ code with parameters*

$$n = q\mu, \qquad N = q^2\mu, \qquad d = \mu(q-1). \tag{3}$$

The code C based on a difference matrix D (as described above) is called a *difference matrix code*, or, for short, a *DM code*. Any $(n, N, \{d, n\})_q$ code whose parameters satisfy (3) is called a *pseudo difference matrix code*, or, for short, a *PDM code*. Below we will see that an additive PDM code is a DM code. These codes are optimal with respect to a q-ary analog of the Gray–Rankin bound [13], which they meet with exact equality. Any q-ary $(n, N, \{d, n\})_q$ code which can be partitioned into trivial $(n, q, n)_q$ subcodes (referred to as *simplexes*) satisfies this bound [13]

$$\frac{N}{q} \le \frac{q(qd - (q-2)n)(n-d)}{n - ((q-1)n - qd)^2} \tag{4}$$

provided that $n - ((q-1)n - qd)^2 > 0$.

We also recall the linear programming bound on the cardinality N of a code C in which the maximum distance between codewords is bounded, say by D; see [14] for the first case $D = n$ of this bound and [15] for the general case. For $D = n$ this bound looks as follows:

$$N \le \frac{q^2 d}{dq - (q-1)(n-1)}, \tag{5}$$

provided that the denominator is positive. Note that an $(n, N, \{d, n\})_q$ PDM code also meets this bound with equality.

As we have already mentioned, we consider not only additive but also nonadditive codes, in particular, *distance invariant* codes, i.e., codes whose weight spectrum does not depend on the choice of a zero codeword.

Recall that a q-ary $N \times n$ matrix M is called an *orthogonal array* of strength t, index $\lambda = N/q^t$, and n constraints and is denoted by $\mathrm{OA}(N, n, q, t)$ if every its $N \times t$ submatrix contains every q-ary vector of length t as a row exactly λ times [16].

We say that an $(n+1, N, d+1)_q$ code C^* is obtained by extension of an $(n, N, d)_q$ code C if to all codewords of C we add the overall parity-checking position, i.e.,

$$C^* = \{(c_1, \ldots, c_n, c_{n+1}) : (c_1, \ldots, c_n) \in C\}, \quad \text{where} \quad c_{n+1} = \sum_{i=1}^{n+1} c_i.$$

The following result is well known and can be found, e.g., in [17]. For a given q and a positive integer m, we use the notation $n_m = (q^m - 1)/(q - 1)$.

Lemma 4. *Let $\mathcal{H}_m$ be an $[n_m, k, 3]_q$ Hamming code. Then the extended code $\mathcal{H}_m^*$ has minimum distance 4 if and only if*

(i) *$q = 2$ and $m \geq 2$, or*

(ii) *$q = 2^r \geq 4$ and $m = 2$, i.e., $n_m + 1 = q + 2$ and $k = q - 1$.*

For an arbitrary $(n, N, d)_q$ code C, define its *covering radius* $\rho = \rho_C$ to be the smallest integer such that all spheres of radius ρ drawn around all codewords of C (centered at these codewords) cover the whole space Q^n.

3. NECESSARY CONDITIONS

A natural question on the existence of a q-ary two-weight $(n, N, \{d, d+\delta\})_q$ code is the question of under which conditions such a code exists. Here we answer this question for the case where $d+\delta = n$ and the code satisfies some regularity properties. We need some known facts on projective two-weight codes; see [1, 7, 8] and references therein. Let $\mathrm{PG}(n, q)$ denote the n-dimensional projective space over the field $\mathbb{F}_q$. An *m-arc* of points in $\mathrm{PG}(n, q)$, where $m \geq n+1$ and $n \geq 2$, is a set M of m points such that no $n+1$ points of M belong to a hyperplane in $\mathrm{PG}(n, q)$. A $(q+1)$-arc in $\mathrm{PG}(2, q)$ is called an *oval*, and a $(q+2)$-arc in $\mathrm{PG}(2, q)$, q even, is called a *complete oval* or a *hyperoval* (see, e.g., [18–20]).

A linear code C is said to be *projective* if its dual code $C^\perp$ has minimum distance $d^\perp \geq 3$ (i.e., any generator matrix of C does not contain two columns that are scalar multiples of each other). For projective $[n, k, d]_q$ codes C, one can introduce the notion of its *complementary code* C_c (see, e.g., [1, 7]). Let $[C]$ denote the matrix formed by all codewords of C (i.e., the rows of $[C]$ are the codewords of C). A code C_c is called the complementary of C if the matrix $[[C] \,|\, [C_c]]$ is a linear equidistant code and C_c has the minimum possible length giving this property. For a given $[n, k, d]_q$ code C with parity-check matrix H, its *complementary* $[n_{n-k} - n, k, d_c]$ code C_c has parity-check matrix H_c obtained from H_{n-k} by removing all columns of H and multiples of them. Recall an important property of a complementary code: *to any codeword of weight w in an $[n, k, d]_q$ code C there corresponds a codeword of weight $w_c = q^{k-1} - w$ in the complementary code C_c*. As a consequence of this simple fact, we have the following lemma.

Lemma 5 [7]. *A linear $[n, k, d]_q$ code C with covering radius $\rho = 2$ which is not the dual of a DM code exists simultaneously with its complementary projective code C_c having the same covering radius $\rho_c = 2$.*

An extension of this well-known concept to arbitrary linear two-weight $[n, k, \{d, d+\delta\}]_q$ codes was obtained in [5, 6]. Here we give a variant of this result for the case of $[n, k, \{d, n\}]_q$ codes.

For any code C with parity-check matrix H, denote by s the maximum number of occurrences of any column in H counted with its multiples, i.e, columns obtained by multiplying it by a nonzero element of $\mathbb{F}_q$.

Lemma 6 [5, 6]. *Let C be a q-ary linear nontrivial two-weight $[n,k,\{d,n\}]_q$ code which is not the dual of an s-times repetition of a DM code, and let μ_1 and μ_2 denote the number of codewords of weights d and n, respectively. Then there exists a complementary linear two-weight $[n_c,k_c,\{d_c,d_c+\delta\}]_q$ code C_c with*

$$n+n_c = s\frac{q^k-1}{q-1}, \quad d+d_c+\delta = sq^{k-1}, \quad n=d+\delta, \quad s=1,2,\ldots,$$

such that C_c contains μ_1 codewords of weight $d_c+\delta$ and μ_2 codewords of weight d_c and, moreover, C_c is of the minimum possible length n_c such that the matrix $[[C]\,|\,[C_c]]$ is an equidistant $[s(q^k-1)/(q-1),k,sq^{k-1}]_q$ code.

Note that the integer s in Lemma 6 is the maximal size of a collection of columns in the generator matrix of C which are scalar multiples of one column. For projective two-weight $[n,k,\{d,n\}]_q$ codes (i.e., for the case of $s=1$), the following results are known.

Lemma 7 [8]. *Let C be a two-weight projective $[n,k,\{w,n\}]_q$ code over $\mathbb{F}_q$, where $q=p^m$ and p is a prime. Then there exist two integers $u\ge 0$ and $h\ge 1$ such that*

$$w = hp^u, \qquad n=(h+1)p^u.$$

For the case of projective codes, we recall the following result (which directly follows from the MacWilliams identities taking into account that the dual code $C^\perp$ has minimum distance $d^\perp \ge 3$); see [8].

Lemma 8. *Let C be a two-weight projective $[n,k,\{w,n\}]_q$ code C over $\mathbb{F}_q$, where $q=p^m$ and p is a prime. Denote by μ_1 and μ_2 the number of codewords of C of weights w and n, respectively. Then*

$$\begin{cases} w\mu_1+n\mu_2 = n(q-1)q^{k-1},\\ w^2\mu_1+n^2\mu_2 = n(q-1)(n(q-1)+1)q^{k-2}. \end{cases} \tag{6}$$

In [5, 6] (see also [4] for the special case $n-d=1$), we derived integrality conditions similar to the conditions obtained by Delsarte in [8] (see also [1]) for projective two-weight codes using simple combinatorial arguments that are not related to eigenvalues of strongly regular graphs. For the case of arbitrary two-weight $(n,N,\{d,n\})_q$ codes with distances d and n, those conditions reduce to the following result. As in [8] and [1], we consider here only two-weight $(n,N,\{d,n\})_q$ codes with cardinality $N\ge q^2$. There are many trivial and nontrivial examples of such codes with $N\le q^2$; below we mention some of them. We regard such codes as being of little interest, since their cardinality is not always optimal, i.e., does not meet upper bounds. Recall that by trivial codes we also mean two-weight codes that can be represented as a direct sum (or repetition) of two or more $(n_i,N,\{d_i,n_i\})_q$ codes.

Theorem 1. *Let Q be any alphabet of size q, and let C be an arbitrary nontrivial q-ary two-weight $(n,N,\{d,n\})_q$ code, where $N\ge q^2$. Then*

(i) *The cardinality N of the code C lies in the range*

$$(q-1)n+1 \le N \le \frac{q^2d}{qd-(q-1)(n-1)} \tag{7}$$

provided that $qd-(q-1)(n-1)>0$;

(ii) *The right-hand inequality in* (7) *turns into equality if and only if the matrix* $[C]$ *formed by all codewords of* C *is an orthogonal array of strength* $t \geq 2$;

(iii) *If the right-hand inequality in* (7) *is an equality, then the length* n *and distance* d *of* C *are as follows*:

$$n = \frac{N(q(d+1)-1) - q^2 d}{N(q-1)} \tag{8}$$

and

$$d = (n-1)\frac{(q-1)N}{q(N-q)}; \tag{9}$$

(iv) *The left-hand inequality in* (7) *turns into equality if and only if* C *is an equidistant* $(n, N, d)_q$ *code*;

(v) *If the right-hand inequality in* (7) *is an equality, then* N *divides* $q^2 d$ *and* $q-1$ *divides* $(N-1)d$.

Proof. (i) For the case where C is an arbitrary q-ary two-weight $(n, N, \{d, n\})_q$ code, this directly follows from the linear programming bound for such codes, which we present in Section 5.1. For the case where C is an orthogonal array of strength $t \geq 2$, this result comes from arguments similar to those used in [6]. Here we provide a simple proof for the general case where C is an arbitrary distance-invariant $(n, N, \{d, n\})_q$ code of cardinality $N \geq q^2$; we will also need these arguments below.

Assume that C contains the all-zero codeword and μ codewords of weight d. Let C^* consist of codewords of weight d only, and let $[C^*]$ be a $\mu \times n$ matrix whose rows are codewords of C^*.

First we compute the total number of zeros (which we denote by Σ_0) in the matrix $[C^*]$ in two different (though obvious) ways. Indeed, by the definition we have

$$\Sigma_0 = \mu(n-d) = (N/q - 1)n.$$

Next, since C is distance invariant and therefore each column contains the same number of zeros, namely $N/q = \mu(n-d)/n + 1$, we obtain that

$$\mu = \frac{n(N-q)}{q(n-d)}. \tag{10}$$

Now we compute the total number $\Sigma_{(0,0)}$ of pairs of coordinate positions containing zero elements $(0,0)$ which occur in all the $n(n-1)/2$ pairs of positions in the rows of $[C^*]$. Denote by $s(i,j)$ the number of such zero pairs $(0,0)$ occurring in the ith and jth columns of $[C^*]$. We obviously obtain

$$\left(\frac{N}{q^2} - 1\right) n(n-1) \leq \Sigma_{(0,0)} = \sum_{1 \leq i < j = n} s(i,j) = \mu(n-d)(n-d-1). \tag{11}$$

Using the expression for μ from (10) in (11), we obtain the following inequality:

$$N\left(qd - (q-1)(n-1)\right) \leq q^2 d. \tag{12}$$

This gives the right-hand inequality in (7), since we have the condition

$$qd - (q-1)(n-1) > 0.$$

Now consider the left-hand inequality in (7). The right-hand inequality in (7) (which holds for an arbitrary two-weight $(n, N, \{d, n\})_q$ code) implies the following upper bound on d:

$$d \leq (n-1)\frac{N(q-1)}{q(N-q)}.$$

But the values of d for an $(n, N, \{d, n\})_q$ code cannot be greater than the quantity (which we denote by $d^{(p)}$) guaranteed by the Plotkin upper bound (2), which is tight for an equidistant code (indeed, the average estimate over all distances is always greater than the minimum distance of a code with several distances). Hence, from the inequality

$$d \le (n-1)\frac{N(q-1)}{q(N-q)} \le d^{(p)} = n\frac{(q-1)N}{q(N-1)}$$

we obtain that

$$(n-1)(N-1) \le n(N-q),$$

which implies the left-hand inequality for N in (7).

(ii) The right-hand inequality in (7) turns into equality if and only if (11) is an equality. This happens when the code C satisfies the following condition: *the quantity $s_0(i,j) = s(i,j)$ is constant for any chosen code positions i and j*. We claim that this is possible only if the matrix $[C]$ is an orthogonal array of strength $t \ge 2$. Assume the contrary: let for some $a \in Q$ the quantity $s_a(i,j)$ be not the same for all i and j. Then define a new code $C^{(a)}$ obtained from C by interchanging the elements 0 and a of the alphabet in all codewords of C. Making the same computations for the new code, we arrive at a contradiction. Since $s_a(i,j)$ is not constant in (7), we obtain a strict inequality, contradicting the condition of the claim. Hence, we conclude that $[C]$ is an orthogonal array. But if $[C]$ is an orthogonal array, then $s_0(i,j) = s(i,j)$ is constant for all i and j, equation (11) is an equality, and therefore the right-hand inequality in (7) is an equality.

(iii) If the right-hand inequality (7) is an equality, this means that (11) is also an equality, which can be rewritten as follows:

$$(N - q^2)n(n-1) = qn(N-q)(n-d-1). \tag{13}$$

Therefore, we can rewrite the expression for n as a function of q, d, and N, thus obtaining (8), and the expression for d as a function of q, n, and N, obtaining (9).

(iv) The condition $N = (q-1)n + 1$ corresponds to the case of equidistant codes, which was considered in [21] in detail (in this case the matrix $[C]$ is also an orthogonal array of strength $t = 2$).

(v) Since n is a natural number, we deduce from (13) that d must be a multiple of N/q^2. From the same equality, taking into account that

$$N(q(d+1)-1) - q^2 d = (q-1)\left(N(d+1) - d(q+1)\right) + d(N-1),$$

we conclude that $d(N-1)$ is a multiple of $q-1$. △

The next result shows that the existence of an additive two-weight $(n, N, \{d, n\})_q$ code C over an alphabet Q which is an abelian group, imposes a very strong condition on this group. The order q and the structure of the group Q are by far not arbitrary. Recall that for an additive abelian group Q, the order of an element x, denoted by $\operatorname{ord}(x)$, is the smallest number t such that $tx = \underbrace{x + x + \ldots + x}_{t \text{ times}} = 0$.

Theorem 2. *Let Q be an abelian group of order q, and let C be an additive nontrivial q-ary two-weight $(n, N, \{d, n\})_q$ code C over the alphabet Q containing the all-zero codeword. Then we have the following*:

(i) *All elements of Q have the same order*, *i.e.*, $\operatorname{ord}(x) = \operatorname{ord}(y)$ *for any pair of nonzero elements* $x, y \in Q^*$;

(ii) *The group Q is a direct sum of m cyclic groups $\mathbb{Z}_p$*:

$$Q = \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p;$$

(iii) *The number q is of the form $q = p^m$, where p is a prime and m a positive integer*;
(iv) *The code C contains at least $q-1$ words of weight n.*

Proof. It is obvious that any permutation π of elements of Q such that $\pi(0) = 0$, being applied to any position of the code C, preserves the property of a code to be a two-weight $(n, N, \{d, n\})_q$ code with the all-zero codeword. Denote by π a permutation preserving the additivity property of C, so that

$$x - y = \pi(x) - \pi(y) = \pi(x - y).$$

(i) For a given pair of alphabet elements $x, y \in Q^* = Q \setminus \{0\}$ and for a codeword $c = (x_1, x_2, \ldots, x_n) \in C$ of weight n, choose some permutations $\pi_1, \ldots, \pi_n$ of elements of Q satisfying the condition $\pi_i(0) = 0$ and such that by applying them to all coordinate positions of c we obtain a codeword $c' = (x, y, \ldots, y)$ of an additive code (indeed, applying such permutations π_i to all coordinates preserves the additivity property of the code). Assume that $t = \mathrm{ord}(x) \neq \mathrm{ord}(y)$. Then the sum $c' + \ldots + c'$ of t copies of c' is a codeword $(0, ty, \ldots, ty)$ of weight $n-1$, since by the assumption we have $ty \neq 0$. Thus, we arrive at a contradiction, and therefore all nonzero elements of the alphabet are of the same order.

(ii) This directly follows from (i). Indeed, it is well known that any abelian group is a direct sum (direct product) of cyclic groups. On the other hand, any cyclic group $\mathbb{Z}_{p_1p_2}$ has elements of orders p_1, p_2, and p_1p_2, which contradicts (i) and proves the claim.

(iii) From (ii) it follows that all p_i are the same, whence we obtain the claim.

(iv) Since the code is additive, we conclude that $N \geq qn$. Fix a coordinate position, say the first one. Partition all codewords into cosets according to their elements in the first positions. Every coset is an equidistant code of cardinality at least n [21] (whence the above inequality follows). Since the code is a group, it is clear that we can translate the coset with zero at the first position to any other coset. This also implies that every element of the alphabet occurs in a column the same number of times.

Let μ_1 and μ_2 denote the number of codeword of C of weights d and n, respectively. First consider the case of $N = qn$. Let $\mu = n - d$. Then we can compute the total number of nonzero positions in C. We have the following two expressions:

$$\begin{cases} \mu_1 + \mu_2 = N - 1, \\ d\mu_1 + n\mu_2 = nN\Big(1 - \dfrac{1}{q}\Big). \end{cases} \tag{14}$$

Using the expression for μ_1 from the first equation in the second one and taking into account that $N = nq$, we reduce it to the form

$$d(N - 1 - \mu_2) + n\mu_2 = nN\left(1 - \frac{1}{q}\right) = n^2(q-1).$$

Taking into account that $\mu = n - d$, we obtain

$$d(qn - 1 - \mu_2) + n\mu_2 = d(qn-1) + (n-d)\mu_2 = (n-\mu)(qn-1) + \mu\mu_2 = n^2(q-1).$$

Thus, we arrive at the equation

$$\mu\mu_2 = n(q\mu - n) + n - \mu. \tag{15}$$

Since each of its two sides is a positive integer, we conclude that $q\mu - n \geq 0$. Therefore, we may put

$$q\mu = n + \lambda,$$

where $\lambda \geq 0$ is an integer. Equation (15) can be rewritten in the following form (with μ carried to the left-hand side):

$$\begin{cases} q\mu = n + \lambda, \\ \mu(\mu_2 + 1) = (\lambda + 1)n. \end{cases} \tag{16}$$

Since $(\lambda + 1)n \geq n + \lambda$, this implies

$$\mu(\mu_2 + 1) \geq q\mu,$$

or equivalently $\mu_2 + 1 \geq q$. Hence, we obtain that $\mu_2 \geq q - 1$. For the case of $N > qn$, the proof is the same. △

In the next statement we formulate a variant of Theorem 2 from [6] for the case of nontrivial $[n, k, \{d, n\}]_q$ codes, so this statement does not need a proof. Here we assume that $q = p^m$, where $m \geq 1$ and p is a prime. For a given $q = p^m$ and an arbitrary natural number a, denote by $\gamma_a \geq 0$ the largest integer such that p^{γ_a} is a divisor of a, i.e., $a = p^{\gamma_a} h$ with h and p coprime. Define the numbers γ_d, γ_δ, and γ_c in a similar way for d, δ, and d_c, respectively. Recall that (a, b) denotes the greatest common divisor of integers a and b.

Theorem 3. *Let $q = p^m$, where $m \geq 1$ and p is a prime number. Let C be a q-ary linear* (*two-weight*) *$[n, k, \{d, n\}]_q$ code of dimension $k \geq 2$, and let C_c be its complementary two-weight $[n_c, k, \{d_c, d_c + \delta\}]_q$ code, where*

$$d + \delta = n \qquad \textit{and} \qquad d + d_c + \delta = sq^{k-1}, \quad s \geq 1.$$

(i) *If $s = 1$ and $k \geq 4$, i.e., C and therefore C_c are projective codes, then the following two equalities hold*:

$$(q, d) = (q, \delta) \qquad \textit{and} \qquad (q, d_c) = (q, \delta); \tag{17}$$

(ii) *If $s = 1$ and $k = 3$, then both equalities in* (17) *hold if one of the following two conditions is satisfied*:

$$(d, q)^2 \leq q(n(n-1), q) \qquad \textit{or} \qquad (d + \delta, q)^2 > q(n_c(n_c - 1), q);$$

(iii) *If $s = 1$ and $k \geq 2$, then at least one of the following two equalities is satisfied*:

$$\gamma_d = \gamma_\delta \qquad \textit{or} \qquad \gamma_c = \gamma_\delta; \tag{18}$$

(iv) *If $s \geq 1$ and $k \geq 3$, then at least one of the two equalities in* (18) (*respectively, in* (17)) *is valid.*

4. KNOWN $(n, N, \{d, n\})_q$ CODES

Here, we enumerate all known nontrivial additive $(n, N, \{d, n\})_q$ codes. Most of these two-weight codes can be found in a comprehensive survey of such codes in [1].

We start with a statement which is a reformulation of the corresponding result from [10], where all known completely regular linear codes with covering radius 2 whose dual codes are antipodal (i.e., contain words of weight n) were presented. In [10] this theorem was stated and proved for the case of linear codes. We formulate a similar result for arbitrary additive codes.

Theorem 4. *Let C be a nontrivial additive $(n, N, \{d, n\})_q$ code of cardinality $N \geq q^2$ over Q. The code C can be reduced by equivalent transformations to a code C^* such that the following conditions hold*:

(i) *For every nonzero codeword $\boldsymbol{v} \in C^*$ of weight d, every element $a \in Q$ that occurs in a coordinate position of this word $\boldsymbol{v}$ occurs in this word exactly $n - d$ times*;

(ii) *Every nonzero codeword $\boldsymbol{v} \in C^*$ of weight n either satisfies property* (i) *or is of the form $\boldsymbol{v} = (a, a, \ldots, a)$, where $a \in Q$*;

(iii) *The length n of the code C^** (*and therefore of C*) *is a multiple of $n - d$.*

Recall that in Section 2, following [13], we called a trivial $(n, q, n)_q$ code a *simplex*. Recall also that a q-ary distance invariant code of length n is a *simplex code* if it contains as a subcode a simplex, i.e., an $(n, q, n)_q$ code. Clearly, an additive $(n, N, \{d, n\})_q$ code containing a simplex is a distance invariant simplex code. The following result can be found in [13].

Proposition 1. *Assume that a q-ary code C of length n with minimum distance $d = \dfrac{(q-1)n}{q}$ has cardinality $N = qn$. Then C can be represented as a union of disjoint simplexes.*

A natural question arises: *What are the conditions for a simplex code given in Proposition* 1 *to be a PDM or DM code*? The following theorem gives a partial answer to this question.

Theorem 5. *Let C be a distance invariant simplex code with parameters $(n, N, \{d, n\})_q$. Then we have the following*:

(i) *The code C can be partitioned into disjoint subcodes as follows*:

$$C = \bigcup_{i=1}^{N/q} C_i,$$

where C_i for every i is a simplex and the cardinality N is a multiple of q;

(ii) *For any codeword $\boldsymbol{c} \in C$ other than words of the form $(a, a, \ldots, a)$, $a \in Q$, every symbol $\alpha \in Q$ that occurs in a coordinate position of $\boldsymbol{c}$ occurs in this position exactly μ times*, *where $\mu = n - d$ and n is a multiple of μ*;

(iii) *The distance d of C satisfies the inequality*

$$d \le n\frac{q-1}{q}; \tag{19}$$

(iv) *If* (19) *turns into equality and $N = qn$*, *then C is a PDM code with parameters*

$$n = \mu q, \qquad N = \mu q^2, \qquad d = \mu(q-1), \qquad \mu = n - d;$$

(v) *If the code C in* (iv) *is additive*, *then it is a DM code.*

Proof. (i) Since C contains as a subcode a simplex code with the zero codeword $\mathbf{0}$, we can choose $q-1$ codewords of weight n of the form $\boldsymbol{a} = (a, a, \ldots, a)$, where $a \in \{1, \ldots, q-1\}$, if there are such codewords in C. Otherwise, we can obtain such codewords from codewords of weight n by permuting alphabet elements. Since C is distance invariant, this is valid for any choice of a zero codeword. For any such choice we obtain as a subcode a simplex containing $q-1$ codewords of weight n. In this way we obtain a partition of C into subcodes where every subcode is a simplex. Clearly, any codeword of C will belong to some simplex. It remains to show that any two distinct simplexes cannot have a common codeword. Indeed, we can translate one of such simplexes to a simplex containing codewords of the form $\boldsymbol{a} = (a, a, \ldots, a)$; none of such words can belong to another simplex, since all codewords from other simplexes are at distance d from this simplex. We conclude that C is partitioned into disjoint subcodes of cardinality q; therefore, N must be a multiple of q.

(ii) Denote by C_0 the simplex code which contains the zero codeword and $q-1$ codewords of the form $\boldsymbol{a} = (a, a, \ldots, a)$. Consider any codeword $\boldsymbol{c}$ which does not belong to C_0. Clearly, every element a which occurs in a coordinate position of $\boldsymbol{c}$ must occur (in order to be at distance exactly d from q codewords of C_0) exactly $n-d$ times. This implies, first, that every element that occurs in positions of $\boldsymbol{c}$ occurs exactly $\mu = n - d$ times, and second, that n must be a multiple of $n - d$.

(iii) Since there are at most q different elements at positions of any codeword $\boldsymbol{c}$, the following obvious inequality must be valid: $n \le q(n-d)$. This implies (19).

(iv) The equality in (19) implies that n can be expressed as $n = q\mu$, where $\mu = n - d$, and hence $d = \mu(q-1)$. For these values of n and d we obtain from (4) that $N \le q^2\mu$. If $N = qn$, then $N = q^2\mu$, and according to [13] C is a PDM code, which proves (iv).

(v) From (iv) we have that C is a PDM code. Now we show that an additive PDM code is a DM code. Since C is additive, a sum of any two rows, say $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$, belongs to C and contains every element of the alphabet in the coordinate positions μ times (Theorem 4). From the code C, we construct a $q\mu \times q\mu$ matrix D containing all codewords with zero in the first position, where $\mu = n - d$. This is clearly possible, since C is an additive code.

Now any nonzero row of D contains any element of Q exactly μ times (Theorem 4), and for any two distinct rows $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ of D their componentwise difference $\boldsymbol{c}_1 - \boldsymbol{c}_2$ also belongs to D (by the definition, words of D have 0 at the first position). Any codeword $\boldsymbol{c} \in C$ with the first nonzero position $a \in Q$ is obtained from D by adding the vector $(a, a, \ldots, a)$, which exists in C, since C is a simplex code. We conclude that D is a difference matrix $D(q, n-d)$, and C is an $(n, qn, \{d, n\})_q$ DM code. $\triangle$

Remark 1. The conditions $n = q(n-d)$ and $N = qn$ in (iv) and (v) cannot be removed, as is shown by the following example. Consider the matrix $[C] = [D^{(0)} \mid \cdots \mid D^{(q-1)}]^t$ formed by translates $D^{(i)}$ of a difference matrix $D = D(q, \mu)$, where C is an $(n, N, \{d, n\})_q$ DM code. If we remove one or more such matrices $D^{(i)}$ from the matrix $[C]$, we obtain a distance invariant simplex code of some cardinality $N^* < qn$, i.e., a nonlinear two-weight $(n, N^*, \{d, n\})_q$ code satisfying the conditions of the theorem. Similarly, we cannot remove the condition $N = qn$ in (iv) and (v). For example, a linear Bose–Bush code (see below) has length $n < q(n-d)$. Similarly, an additive $(n, N, \{d, n\})_q$ code need not necessarily be of cardinality q^k. For example, the difference matrix $D(4, 2)$ induces an optimal additive $(8, 32, \{6, 8\})_4$ code of cardinality $N \ne 4^k$.

Remark 2. The case of codes of cardinality $N = q^2$ is also quite specific. A well-known result guarantees that $r-2$ mutually orthogonal Latin squares of order q induce a $(r, q^2, \{r-1, r\})_q$ code. For the case where q is a prime power, there exist $q-1$ mutually orthogonal Latin squares inducing a linear equidistant $[q+1, 2, q]_q$ code (the converse is also valid for any length r and is well known). Using these codes with corresponding values of r, we can construct as a direct sum (using partitions into simplexes) an $(n, 2, \{d, n\})_q$ code for any natural $d = n - s$ and $n = r_1 + \ldots + r_s$ by considering the direct sum of s initial $(r_i, q^2, \{r_i - 1, r_i\})_q$ Latin square codes. Therefore, we have excluded (as in [1,8]) all these trivial codes except for $(r, q^2, \{r-1, r\})_q$ codes of length $r \le q$ induced by $r-2$ mutually orthogonal Latin squares of order q. Besides, of course, there are also $[q+2, 2, \{q+1, q+2\}]_q$ codes obtained from equidistant $[q+1, 2, q]_q$ codes by adding one position (see [4]).

Now we can present all known families of nontrivial additive $(n, N, \{d, n\})_q$ codes, which were given in the survey [1] (and also in [10] for the linear case). If we exclude codes induced by Latin squares, then all known $(n, N, \{d, n\})_q$ codes are divided into two large classes of codes: $(n = q\mu, N = qn, \{(q-1)\mu, q\mu\})_q$ difference matrix codes, whose length n is a multiple of q, and $[n, k, \{d, n\}]_q$ Denniston codes of length n such that $n-1$ is a multiple of $(q^{k-1}-1)/(q-1)$.

Difference matrix codes (DM codes). These are $(q\mu, q^2\mu, \{(q-1)\mu, q\mu\})_q$ codes [12] induced by difference matrices. Lemma 1 describes the construction of such codes for $q = p^h$ and $\mu = p^\ell$, where p is a prime and h and ℓ are arbitrary natural numbers.

It should be noted that these codes include (binary) $(4m, 8m, \{2m, 4m\})$ *Hadamard codes.* Indeed, a binary (i.e., consisting of elements 0 and 1) Hadamard matrix is a difference matrix $D(2, 2m)$.

Denniston codes. These are $[n = 1 + (q+1)(h-1), 3, \{q(h-1), n\}]_q$ codes, where $1 < h < q$ and h divides q, for $q = 2^r \ge 4$ (see the TF2 family in [1]). In Theorem 1 this case corresponds to the distance $d = n - h + 1 = (n-1)q/(q+1)$, implying that $N = q^3$. For the case of $h = 2$, we obtain $[n = q+2, 3, \{q, n\}]_q$ Bose–Bush codes (see the TF1 family in [1]), constructed in 1952 [11], which are induced by hyperovals in $\mathrm{PG}(3, q)$. To the value $h = q/2$ there correspond $[n = q(q-1)/2, 3, \{q(q-2)/2, n\}]_q$ Delsarte codes [7] (see the TF1^d family in [1]), independently constructed in 1971, which are projectively dual to the Bose–Bush codes [1].

The Dennistion codes are induced by maximal arcs in projective plains [18] (see also [19, 20]). Let us briefly explain how to construct such codes for an arbitrary $q = 2^m \geq 4$ and a natural $h \geq 2$ dividing q, i.e., $h = 2^u \leq q/2$. For a given $\mathbb{F}_q$, let H denote the subgroup of order h of the additive group of $\mathbb{F}_q$. Let $\varphi(x, y) = ax^2 + bxy + cy^2$ be an irreducible quadratic form over $\mathbb{F}_q$. Then the $[n, 3, \{d, n\}]_q$ Denniston code is generated by the following $(3 \times n)$ matrix:

$$G_d = \begin{bmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{bmatrix}, \tag{20}$$

where $n = (q+1)(h-1)+1$, $d = n-h$, and (x_i, y_i) are all ordered pairs of elements of $\mathbb{F}_q$ that are mapped to H, i.e., $\varphi(x_i, y_i) \in H$.

Let us also present generator matrices for Bose–Bush codes and for Delsarte codes, since they can be given explicitly. Let G be a matrix of the form

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 1 & 0 & x_0 & x_1 & \dots & x_i & \dots & x_{q-2} \\ 0 & 0 & 1 & y_0 & y_1 & \dots & y_i & \dots & y_{q-2} \end{bmatrix}, \tag{21}$$

where x_i and y_i run over all nonzero elements of $\mathbb{F}_q$. Then, if $y_i = x_i^2$, the matrix G generates a Bose–Bush code. If x_i and y_i run over all pairs (x_i, y_i) of nonzero elements (the number of different such pairs being, obviously, $(q-1) \times q/2$, i.e., the length of the Delsarte codes) such that $\mathrm{Tr}(x_i y_i) = 1$, where $\mathrm{Tr}(x)$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_2$, i.e.,

$$\mathrm{Tr}(x) = x + x^2 + x^4 + \ldots + x^{q/2},$$

then the matrix G generates a Delsarte code.

Theorem 6. *Let C be an additive nontrivial $(n, N, \{d, n\})_q$ code, where $q = p^m$, p is an arbitrary prime, and $m = 1, 2, \ldots$. Assume that $N \geq q^2$ and $n > 2$. Then the parameters of this code coincide with the parameters of some code belonging to one of the code families described above.*

Proof. Since C is a nontrivial additive code, it has cardinality $N = q^2\mu \geq q^2$.

We start with the case $N = q^2$. For any natural q, the existence of r pairwise orthogonal Latin squares implies the existence of an $(r+2, q^2, \{r+1, r+2\})_q$ MDS code (see Remark 2). These codes include the shortest nontrivial $(q, q^2, \{q-1, q\})_q$ PM codes, which exist for any prime power q and coincide with the Latin square codes. We again emphasis that there exists many trivial additive two-weight $(n, q^2, \{d, n\})_q$ codes mentioned in the remarks above, which we do not consider. Recall also that since C is additive, all PDM codes are DM codes by Theorem 5.

Now we have to prove that for the case $N = q^2\mu$, where $2 \leq \mu < q$, a nontrivial additive $(n, N, \{d, n\})_q$ code C is nothing else but a $(q\mu, q^2\mu, \{(q-1)\mu, n\})_q$ PDM or DM code. The following argument was used in [13] (see also [21]), where q new codes C_j were defined, $j = \{0, 1, \ldots, q-1\}$, obtained from C by taking all codewords of C that have the element j at the first position and then removing this first position. One can easily see [13] that every code C_j has only one distance, namely d. Hence, C_j is an equidistant $(n_0, N_0, d_0)_q = (n-1, q\mu, d)_q$ code of cardinality $N_0 = q\mu$. Moreover, the parameters of this code meet the Plotkin upper bound (2) with an exact integer equality; hence, every symbol i of the alphabet $\{0, 1, \ldots, q-1\}$ occurs at every position of all codewords of C_j the same number (namely μ) of times [21]. Now we apply Theorem 4, which states that every codeword $\boldsymbol{c}$ of C_j contains all alphabet elements $i \neq j$ as coordinate elements exactly μ times and contains the element j exactly $\mu - 1$ times.

Since C is an additive code, its subcode C_0 is also an additive code satisfying the following property: any nonzero word of C_0 contains every nonzero element of the alphabet exactly μ times. We conclude therefore that by Theorem 5, C_0 becomes a difference matrix if we append zero positions to all codewords of C_0. By additivity, any subcode C_j is a translate of C_0. Thus, C is a DM code.

Now consider the case $N = q^3$. First we show that for Denniston codes h must divide q. From Theorem 5 we conclude that n is a multiple of $n - d$. Hence, n can be represented as $n = (n - d)\ell$ for some natural number ℓ. Therefore, $d = n(\ell - 1)/\ell$, and from (19) we obtain

$$d = n\frac{\ell - 1}{\ell} \leq n\frac{q - 1}{q},$$

whence it follows that $\ell \leq q$. But the case $\ell = q$ gives a DM code. We conclude therefore that $\ell < q$. Now assume that

$$n = 1 + (q + 1)(h - 1) \qquad \text{and} \qquad d = q(h - 1)$$

for some natural number $h \geq 2$. This means that

$$n = q(h - 1) + h = d + h.$$

Thus, combining the equalities

$$n = 1 + (q + 1)(h - 1) \qquad \text{and} \qquad d = q(h - 1) = n\frac{\ell - 1}{\ell},$$

we obtain

$$q(h - 1) = (q(h - 1) + h)\frac{\ell - 1}{\ell},$$

which implies that $h(\ell - 1) = q(h - 1)$. Since $h \geq 2$ and, hence, h and $h - 1$ are coprime, we conclude that h divides q, whence it follows that we obtain a code with the parameters of a Denniston code.

The case $N > q^3$ can be excluded by similar arguments. First we consider the case $N = q^3\mu$, where $2 \leq \mu < q$. Recall that $q = p^m$. We argue that in this case we can obtain DM codes only. Indeed, for any value of $\mu = p^r$, where $0 < r < m$, there exists a $(q^2\mu, q^3\mu, \{q(q-1)\mu, n\})_q$ DM code. In Section 2 we have described the construction of all such codes (see the text after Lemma 1), which can be found in [12]. Let us see why these are the only possible cases. By dividing both sides of (8) by $q^3\mu$, we obtain that $d = n(q - 1)/q$, so this must be a difference matrix. Hence, for the case where $d \neq n(q - 1)/q$, which (for the case of $q^3\mu$) is equivalent to the condition $d = q(q - 1)\mu$, we cannot have an integer equality in (8). Since a repetition of s copies of a DM code does not change the equality $d = n(q - 1)/q$, we conclude that the above nontrivial DM code is the only nontrivial code for these values of N.

Now consider the case $N = q^4$, which gives linear difference-matrix codes [12]. Indeed, having got such an $[n, 4, \{d, n\}]_q$ code C, we can construct (as we have done above, for example, in Theorem 5) a code C_0 which is a linear equidistant $[n - 1, 3, d]_q$ code of length $n - 1 = (q^4 - 1)/(q - 1)$ with distance $d = q^3$ whose dual is a q-ary perfect Hamming code.

Now we show that for the case $N = q^4$ there are no Denniston-type codes. By Theorem 4, the length of a Denniston-type code must be of the form $n = s(q^3 - 1)/(q - 1) + 1$. Since n is a multiple of $n-d$ (see Theorem 4 again), this expression takes the form $n = d\ell/(\ell-1)$ for some natural $\ell \le q$. Taking into account that $d = sq^2$, we obtain

$$n = s\frac{q^3-1}{q-1} + 1 = d\frac{\ell}{\ell-1} = sq^2\frac{\ell}{\ell-1}. \tag{22}$$

Now we need to consider the cases $(s, q-1) = 1$ and $(s, q-1) \ge 2$ separately.

First, let $(s, q-1) = 1$. Then we see that the expression for n on the left-hand side of (22) is divisible by neither s nor q, while the right-hand side is divisible by both of these numbers. Hence, we conclude that codes of this type do not exist.

Next, consider the case $(s, q-1) \ge 2$. For the case $s = q-1$ we obtain that $n = q^3$, and since $N = q^4$, i.e., $N = qn$, we conclude that C is a DM code.

Assume now that $s = u(q-1)$ with $u \ge 2$. Using this s in (22), we arrive at the equality

$$u(q-1)\frac{q^3-1}{q-1} + 1 = u(q-1)q^2\frac{\ell}{\ell-1};$$

simplifying it and multiplying both sides by $(\ell-1)$, we obtain

$$(\ell-1)(u(q^3-1)+1) = \ell u(q^3-q^2).$$

By simple algebra and since $2 \le \ell \le q$ and $u \ge 2$, we come to the inequality

$$0 \le uq^2(q-\ell) = -u\ell + (u+\ell) - 1 \le -1,$$

which is impossible; this completes consideration of the case $N = q^4$.

The case $q^4 < N < q^5$ can be considered similarly. Here, we have only additive DM codes for the values $n = q^4\mu$, where μ runs over all powers of p and $q = p^m$.

The case $N = q^k$ for $k \ge 5$ can be considered similarly, and we omit it to avoid repeating the same arguments.

Now we have to make some comments on the case where q is a power of an odd prime. In 1952, Bush proved in [22] the nonexistence of $[q+2, 3, q]_q$ codes for an odd q, which implies the nonexistence of $[q(q-1)/2, 3, \{q(q-2)/2, q(q-1)/2\}]_q$ Delsarte codes. Then, in 1997, the nonexistence of maximal arcs in Desarguesian planes of an odd order was proved in [23], which automatically implies the nonexistence of all Denniston codes for odd values of q. $\triangle$

5. UPPER BOUNDS

Here we consider upper bounds on the quantity

$$A_q(n; \{d, n\}) = \max\{N : \exists \text{ an } (n, N, \{d, n\}) \text{ code}\},$$

i.e., bounds on the maximum possible cardinality of a code in Q_q^n with two distances d and n.

5.1. Linear Programming Bounds

We performed extensive investigation of the linear programming (LP) bound on $A_q(n; \{d, n\})$ using the Delsarte LP bound in the following form. Define Krawtchouk polynomials as

$$Q_i^{(n,q)}(t) = \frac{1}{r_i} K_i^{(n,q)}(z), \quad z = \frac{n(1-t)}{2}, \quad r_i = (q-1)^i \binom{n}{i},$$

where

$$K_i^{(n,q)}(z) = \sum_{j=0}^{i}(-1)^j(q-1)^{i-j}\binom{z}{j}\binom{n-z}{i-j}$$

are the (standard) Krawtchouk polynomials. For a real polynomial $f(t)$ of degree at most n, consider its expansion

$$f(t) = \sum_{i=0}^{n} f_i Q_i^{(n,q)}(t) \tag{23}$$

in Krawtchouk polynomials.

Theorem 7. *Let $n \geq q \geq 2$, and let $f(t) \in \mathbb{R}[t]$ be a polynomial of degree at most n such that*:
(A1) $f(-1) \leq 0$ *and* $f(1-2d/n) \leq 0$;
(A2) *The coefficients in expansion* (23) *satisfy the conditions $f_0 > 0$ and $f_i \geq 0$ for every $i \geq 1$.*
Then $A_q(n;\{d,n\}) \leq f(1)/f_0$. If an $(n,N,\{d,n\})_q$ code C meets this bound with some $f(t)$, then $f(1-2d/n) = f(-1) = 0$ and $f_i M_i(C) = 0$ for every $i \geq 1$, where

$$M_i(C) = \sum_{x,y\in C} Q_i^{(n,q)}(1-2d(x,y)/n). \tag{24}$$

The linear programming bound from our paper [6] (equation (40)), which was derived for $\delta = n-d$, gives in our case the bound (5) (which is precisely the upper bound in (7)). This yields a simple proof of the necessary condition in part (ii) of Theorem 4.

The second proof of part (ii) of Theorem 1. The upper bound in (5) is obtained by Theorem 1 with the use of the second-degree polynomial $f(t) = (t-1+2d/n)(t+1)$. If this bound is attained by an $(n,N,\{d,n\})_q$ code C, then from the conditions of Theorem 7 it follows that $M_1(C) = M_2(C) = 0$, since $f_1 > 0$ and $f_2 > 0$. This means that the code C is an orthogonal array of strength 2. Then, clearly, we conclude that the cardinality N of the code C, i.e.,

$$N = \frac{dq^2}{qd-(q-1)(n-1)},$$

is divisible by q^2 and that d is divisible by $qd-(q-1)(n-1)$. △

Numerical results suggest several general LP bounds for special cases of families of parameters q, n, and d. We present one of them here (the other seem to be weaker). This bound is a special case of the bound recently obtained in [24] for values just outside the Plotkin bound range.

Theorem 8. *For every positive integer $m \geq 2$, we have the inequality*

$$A_2(4m+1,\{2m,4m+1\}) \leq 4m+2. \tag{25}$$

Proof. Apply Theorem 7 for the length $n = 4m+1$ and distance $d = 2m$ with the polynomial

$$f(t) = 1 + 2mQ_2^{(4m+1,2)}(t) + (2m+1)Q_{4m-1}^{(4m+1,2)}(t). \tag{26}$$

Condition (A2) is obviously satisfied. Let us prove that condition (A1) holds with equalities.

From $Q_i^{(n,2)}(-1) = (-1)$ we have $f(-1) = 0$. Since $1-2d/n = 1/(4m+1)$, consider

$$f\left(\frac{1}{4m+1}\right) = 1 + \frac{2m}{\binom{4m+1}{2}}\sum_{j=0}^{2}(-1)^j\binom{2m}{j}\binom{2m+1}{2-j}$$
$$+\frac{2m+1}{\binom{4m+1}{4m-1}}\sum_{j=0}^{4m-1}(-1)^j\binom{2m}{j}\binom{2m+1}{4m-1-j}.$$

Table 1. Optimal polynomials with one nonzero coefficient, $q = 3$.

n	d	f_3	$\mathrm{sb}_3(n,d)$	n	d	f_3	$\mathrm{sb}_3(n,d)$
4	1	8	9	4	2	8	9
5	2	8	9	9	4	28	29
10	5	32	33	12	6	44	45
16	8	80	81	20	10	152	153
22	11	224	225				

The first sum can be computed directly, and it equals $-2m/(4m+1)$. For the second sum, we notice that the only values of j for which both binomial coefficients in the sum are nonzero are $2m-2 \le j \le 2m$. This leads to $f(1/(4m+1)) = 0$.

The computation of the corresponding moments $M_i(C)$, which are defined in (24), gives $M_2(C) = M_{4m-1}(C) = 0$ (since $f_2 > 0$ and $f_{2m+1} > 0$) for any $(4m+1, 4m+2, \{2m, 4m+1\})$ code attaining the bound. △

5.2. Numerical Computation of Linear Programming Upper Bounds

In this section, we present LP bounds for $A_q(n, \{d, n\})$ obtained through direct calculation of the LP bound through the simplex method, implemented in Maple 19. We have applied the algorithm for every $q \le 5$ and $n \le 50$. There are numerous cases in which the best bounds are obtained by polynomials of degrees 1 and 2, which lead to already existing bounds, so we have omitted all such cases, preferring to explore bounds obtained by polynomials of degree 3 or higher. Furthermore, we have omitted bounds on all trivial codes with cardinality 4 or less, the bound obtained in (5), and bounds whose values are not positive integers. Finally, we have also omitted the cases for which the bound obtained through spherical codes (see Section 5.3 below) is better, as well as those falling into the case of Theorem 8.

We normalize our LP by $f_0 = 1$, so the bound given by an admissible polynomial f is therefore

$$A_q(n, \{d, n\}) \le 1 + f_1 + f_2 + \ldots + f_n,$$

just as in the classical Delsarte LP setting. In all interesting cases, only one or two coefficients f_i are nonzero. Note that due to the nature of the LP bound, we do not expect many nonzero coefficients, and in fact we have not observed a case with three or more.

We denote by $\mathrm{sb}_q(n, d)$ the best numerical result for $A_q(n, \{d, n\})$ obtained in the aforementioned way. Since all cases for $q = 2$ are covered by the above-mentioned exceptions and the results from [24], we start our review of the interesting LP bound with $q = 3$.

Results for $q = 3$. Similarly to the binary case, for $q = 3$ we observe numerous parameter sets where the only nonzero coefficient (apart from $f_0 = 1$) in the Krawtchouk expansion of the optimal polynomial is f_3, i.e., the LP polynomial is $f(t) = 1 + f_3 Q_3^{(n,3)}(t)$. All but one of them have d close to $n/2$. We systematize them in Table 1.

The rest of the cases that we have found have two nonzero coefficients apart from the obligatory $f_0 = 1$; they are presented in Table 2.

Finally, we report two cases with

$$f(t) = 1 + f_5 Q_5^{(n,3)}(t),$$

for $(n, d) = (46, 23)$ and $(48, 24)$, giving

$$\mathrm{sb}_3(46, 23) = 2753 \qquad \text{and} \qquad \mathrm{sb}_3(48, 24) = 3009,$$

respectively.

Table 2. Optimal polynomials with two nonzero coefficients, $q = 3$.

n	d	Nonzero coefficients	$\mathrm{sb}_3(n,d)$	n	d	Nonzero coefficients	$\mathrm{sb}_3(n,d)$
7	4	$f_2 = 6,\ f_3 = 20$	27	10	6	$f_2 = 12,\ f_3 = 20$	45
24	12	$f_3 = 113,\ f_4 = 210$	324	28	14	$f_3 = 208,\ f_4 = 400$	609
30	15	$f_3 = 320,\ f_4 = 624$	945	7	2	$f_3 = 4,\ f_5 = 16$	21

Table 3. Optimal polynomials for $q = 4$.

n	d	Nonzero coefficients	$\mathrm{sb}_4(n,d)$	n	d	Nonzero coefficients	$\mathrm{sb}_4(n,d)$
5	2	$f_1 = 3/4,\ f_3 = 81/4$	22	5	3	$f_3 = 27$	28
6	3	$f_1 = 1/2,\ f_3 = 45/2$	24	9	6	$f_2 = 12,\ f_3 = 63$	76
10	5	$f_3 = 81$	82	18	12	$f_2 = 33,\ f_3 = 126$	160
24	16	$f_2 = 57,\ f_3 = 198$	256	42	28	$f_3 = 615$	616

Results for $q = 4$. For $q = 4$ we have found optimal polynomials almost entirely of the third degree, in a total of eight cases, as shown in Table 3.

The only case other than those in Table 3 was the fifth-degree polynomial

$$f(t) = 1 + 75Q_4^{(18,4)}(t) + 468Q_5^{(18,4)}(t),$$

giving

$$\mathrm{sb}_4(18,9) = 544.$$

Results for $q = 5$. For the case $q = 5$ we found optimal polynomials only of the third and fourth degree, as shown in Table 4.

5.3. Upper Bounds via Spherical Codes

The relationship between two-distance codes in Q_q^n and spherical two-distance codes on the Euclidean sphere $\mathbb{S}^{n-1}$ (described, for example, in [6, Section 4.3]) implies that every $(n, N, \{d, n\})_q$ code $C \subset Q_q^n$ corresponds to a spherical two-distance code $W \subset \mathbb{S}^{(q-1)n-1}$. The squared distances between points of W are $2dq/(q-1)n$ and $2q/(q-1)$. Using the classical result of [25] and the results of [6], we find that either

$$d = \frac{(k-1)n}{k} \tag{27}$$

for some positive integer $k \in \big[2, (\sqrt{2(q-1)n} + 1)/2\big]$ (and n is obviously divisible by k), or the cardinality N is bounded from above by $N \le 2(q-1)n + 1$.

For a general $q \ge 3$, relation (27) with $k > q$ implies that $d > (q-1)n/q$; i.e., d is in the range of the Plotkin bound. Plugging in the Plotkin bound, we obtain that it can be written as $N \le (k-1)q/(k-q)$. These observations are summarized as follows.

Theorem 9. *If C is an $(n, N, \{d, n\})_q$ code, then either*

$$N \le 2(q-1)n + 1$$

or

$$d = (k-1)n/k,$$

where $k \in \big[2, (\sqrt{2(q-1)n} + 1)/2\big]$ is a positive integer; moreover,

$$N \le \frac{(k-1)q}{k-q}$$

for $q \ge 3$ and $q < k \le (\sqrt{2(q-1)n} + 1)/2$.

Table 4. Optimal polynomials for $q = 5$.

n	d	Nonzero coefficients	$\mathrm{sb}_5(n,d)$	n	d	Nonzero coefficients	$\mathrm{sb}_5(n,d)$
6	3	$f_1 = 4/3,\ f_3 = 128/3$	45	6	4	$f_3 = 64$	65
7	4	$f_1 = 1,\ f_3 = 48$	50	16	12	$f_2 = 40,\ f_3 = 224$	265
21	14	$f_3 = 304$	305	27	18	$f_3 = 624,$	625
32	24	$f_2 = 92,\ f_3 = 432$	525	33	22	$f_3 = 1984$	1985
44	33	$f_2 = 152,\ f_3 = 672$	825	36	24	$f_3 = 32,\ f_4 = 2272$	2405
42	28	$f_3 = 1696,\ f_4 = 6528$	8225				

Further set of bounds (to be applied in different regimes for d and n) can be extracted from the results on spherical two-distance sets described and used in [26]. We note that the paper [26] deals with binary codes only; however, specifically, Lemma 3.3 and Theorem 3.5 from that paper can be applied for $q \geq 3$ as well. Though we proceed with the case of distances d and n, other cases also follow from these results. In what follows we assume that $q \geq 3$.

At this point it is convenient to switch to inner products for points of spherical codes. It is easy to see that the inner products α and β, $-1 < \alpha < \beta < 1$, for points of W are

$$\alpha = -\frac{1}{q-1}, \qquad \beta = \frac{n(q-1) - dq}{n(q-1)}.$$

Now [26, Lemma 3.3] implies that if $d > n(q-2)/q$ (this is equivalent to $\alpha + \beta < 0$), then

$$A_q(n, \{d, n\}) \leq \binom{n(q-1)}{2}$$

except (possibly) in the cases $n(q-1) = \gamma^2 - 2$ and $n(q-1) = \gamma^2 - 3$, where $\gamma := (n-d)q/n(q-1)$ is an odd integer. Similarly, [26, Theorem 3.5] (originally obtained in [27]) gives the bound

$$A_q(n, \{d, n\}) \leq \frac{n(q-1) + 2}{1 - (n(q-1) - 1)(q-1)^2/dq},$$

which is valid when $dq > (n(q-1) - 1)(q-1)^2$.

FUNDING

The research of P. Boyvalenkov was supported in part by the Bulgarian National Science Foundation, project no. KP-06-Russia/33-2020.

The research of K. Delchev was supported in part by the Bulgarian National Science Foundation, project no. KP-06-N32/2-2019.

The research of V.A. Zinoviev and D.V. Zinoviev was carried out at the Institute for Information Transmission Problems of the Russian Academy of Sciences within the program of fundamental research on the topic "Mathematical Foundations of the Theory of Error-Correcting Codes" and was also supported by the National Science Foundation of Bulgaria under project no. 20-51-18002.

REFERENCES

1. Calderbank, R. and Kantor, W.M., The Geometry of Two-Weight Codes, *Bull. London Math. Soc.*, 1986, vol. 18, no. 2, pp. 97–122. https://doi.org/10.1112/blms/18.2.97
2. Shi, M., Guan, Y., and Solé, P., Two New Families of Two-Weight Codes, *IEEE Trans. Inform. Theory*, 2017, vol. 63, no. 10, pp. 6240–6246. https://doi.org/10.1109/TIT.2017.2742499

3. Boyvalenkov, P., Delchev, K., Zinoviev, D.V., and Zinoviev, V.A., Codes with Two Distances: d and $d+1$, in *Proc. 16th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT-XVI), Svetlogorsk, Kaliningrad region, Russia, Sept. 2–8, 2018*, pp. 40–45. Available at `https://www.dropbox.com/s/h7u89lh8vyirww9/Proceedings\%20final.pdf?dl=0`.

4. Boyvalenkov, P., Delchev, K., Zinoviev, D.V., and Zinoviev V.A., On q-ary Codes with Two Distances d and $d+1$, *Probl. Peredachi Inf.*, 2020, vol. 56, no. 1, pp. 38–50 [*Probl. Inf. Transm.* (Engl. Transl.), 2020, vol. 56, no. 1, pp. 33–44]. `https://doi.org/10.1134/S0032946020010044`

5. Boyvalenkov, P., Delchev, K., Zinoviev, D.V., and Zinoviev, V.A., On Two-Weight (Linear and Nonlinear) Codes, in *Proc. 17th Int. Workshop on Algebraic and Combinatorial Coding Theory (ACCT'2020), on-line, Bulgaria, Oct. 11–17, 2020*, pp. 11–17. `https://doi.org/10.1109/ACCT51235.2020.9383353`

6. Boyvalenkov, P., Delchev, K., Zinoviev, D.V., and Zinoviev, V.A., On Two-Weight Codes, *Discrete Math.*, 2021, vol. 344, no. 5, Paper No. 112318 (15 pp.). `https://doi.org/10.1016/j.disc.2021.112318`

7. Delsarte, P., Two-Weight Linear Codes and Strongly Regular Graphs, *MBLE Res. Lab. Report*, Brussels, Belgium, 1971, no. R160.

8. Delsarte, P., Weights of Linear Codes and Strongly Regular Normed Spaces, *Discrete Math.*, 1972, vol. 3, no. 1–3, pp. 47–64. `https://doi.org/10.1016/0012-365X(72)90024-6`

9. Landjev, I., Rousseva, A., and Storme, L., On Linear Codes of Almost Constant Weight and the Related Arcs, *C. R. Acad. Bulgare Sci.*, 2019, vol. 72, no. 12, pp. 1626–1633. `https://doi.org/10.7546/CRABS.2019.12.04`

10. Borges, J., Rifà, J., and Zinoviev, V.A., On q-ary Linear Completely Regular Codes with $\rho = 2$ and Antipodal Dual, *Adv. Math. Commun.*, 2010, vol. 4, no. 4, pp. 567–578. `https://doi.org/10.3934/amc.2010.4.567`

11. Bose, R.C. and Bush, K.A., Orthogonal Arrays of Strength Two and Three, *Ann. Math. Statist.*, 1952, vol. 23, no. 4, pp. 508–524. `https://doi.org/10.1214/aoms/1177729331`

12. Semakov, N.V., Zinoviev, V.A., and Zaitsev, G.V., A Class of Maximum Equidistant Codes, *Probl. Peredachi Inf.*, 1969, vol. 5, no. 2, pp. 84–87 [*Probl. Inf. Transm.* (Engl. Transl.), 1969, vol. 5, no. 2, pp. 65–68]. `http://mi.mathnet.ru/eng/ppi1804`

13. Bassalygo, L.A., Dodunekov, S.M., Zinoviev, V.A., and Helleseth, T., The Grey–Rankin Bound for Nonbinary Codes, *Probl. Peredachi Inf.*, 2006, vol. 42, no. 3, pp. 37–44 [*Probl. Inf. Transm.* (Engl. Transl.), 2006, vol. 42, no. 3, pp. 197–203]. `https://doi.org/10.1134/S0032946006030033`

14. Helleseth, T., Kløve, T., and Levenshtein, V.I., A Bound for Codes with Given Minimum and Maximum Distances, in *Proc. 2006 IEEE Int. Symp. on Information Theory (ISIT'2006), Seattle, WA, USA, July 9–14, 2006*, pp. 292–296. `https://doi.org/10.1109/ISIT.2006.261600`

15. Boyvalenkov, P.G., Dragnev, P.D., Hardin, D.P., Saff, E.B., and Stoyanova, M.M., Universal Bounds for Size and Energy of Codes of Given Minimum and Maximum Distances, *IEEE Trans. Inform. Theory*, 2021, vol. 67, no. 6, pp. 3569–3584. `https://doi.org/10.1109/TIT.2021.3056319`

16. Beth, T., Jungnickel, D., and Lenz, H., *Design Theory*, Cambridge, UK: Cambridge Univ. Press, 1986.

17. MacWilliams, F.J. and Sloane, N.J.A., *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1977. Translated under the title *Teoriya kodov, ispravlyayushchikh oshibki*, Moscow: Svyaz', 1979.

18. Denniston, R.H.F., Some Maximal Arcs in Finite Projective Planes, *J. Combin. Theory*, 1969, vol. 6, no. 3, pp. 317–319. `https://doi.org/10.1016/S0021-9800(69)80095-5`

19. Thas, J.A., Construction of Maximal Arcs and Partial Geometry, *Geom. Dedicata*, 1974, vol. 3, no. 1, pp. 61–64. `https://doi.org/10.1007/BF00181361`

20. Thas, J.A., Projective Geometry over a Finite Field, Ch. 7 of *Handbook of Incidence Geometry: Buildings and Foundations*, Buekenhout, F., Ed., Amsterdam: Elsevier, 1995, pp. 295–347. `https://doi.org/10.1016/B978-044488355-1/50009-8`

21. Semakov, N.V. and Zinoviev, V.A., Equidistant q-ary Codes with Maximal Distance and Resolvable Balanced Incomplete Block Designs, *Probl. Peredachi Inf.*, 1968, vol. 4, no. 2, pp. 3–10 [*Probl. Inf. Transm.* (Engl. Transl.), 1968, vol. 4, no. 2, pp. 1–7]. http://mi.mathnet.ru/eng/ppi1845

22. Bush, K.A., Orthogonal Arrays of Index Unity, *Ann. Math. Statist.*, 1952, vol. 23, no. 3, pp. 426–434. https://doi.org/10.1214/aoms/1177729387

23. Ball, S., Blokhuis, A., and Mazzocca, F., Maximal Arcs in Desarguesian Planes of Odd Order Do Not Exist, *Combinatorica*, 1997, vol. 17, no. 1, pp. 31–41. https://doi.org/10.1007/BF01196129

24. Landjev, I., Rousseva, A., and Vorobev, K., Constructions of Binary Codes with Two Distances, *Preprint*, 2022.

25. Larman, D.G., Rogers, C.A., and Seidel, J.J., On Two-Distance Sets in Euclidean Space, *Bull. London Math. Soc.*, 1977, vol. 9, no. 3, pp. 261–267. https://doi.org/10.1112/blms/9.3.261

26. Barg, A., Glazyrin, A., Kao, W.-J., Lai, C.-Y., Tseng, P.-C., and Yu, W.-H., On the Size of Maximal Binary Codes with 2, 3, and 4 Distances, https://arXiv.org/abs/2210.07496 [math.CO], 2022.

27. Glazyrin, A. and Yu, W.-H., Upper Bounds for s-Distance Sets and Equiangular Lines, *Adv. Math.*, 2018, vol. 330, pp. 810–833. https://doi.org/10.1016/j.aim.2018.03.024