On the weight distribution of some minimal codes

Bartoli, Daniele; Bonini, Matteo; Timpanella, Marco

Published in:
Designs, Codes, and Cryptography

DOI (link to publication from Publisher):
10.1007/s10623-020-00826-8

Publication date:
2021

Document Version
Accepted author manuscript, peer reviewed version

ON THE WEIGHT DISTRIBUTION OF SOME MINIMAL CODES

DANIELE BARTOLI, MATTEO BONINI, AND MARCO TIMPANELLA

Abstract. Minimal codes are a class of linear codes which gained interest in the last years, thanks to their connections to secret sharing schemes. In this paper we provide the weight distributions and the parameters of families of minimal codes recently introduced by C. Tang, Y. Qiu, Q. Liao, Z. Zhou, answering some open questions.

Keyword: Linear code, minimal code, weight distribution.
2010 MSC: 94B05, 94A62

1. Introduction

A codeword c in a linear code $\mathcal{C}$ is called *minimal* if its support (i.e., the set of nonzero coordinates of c) does not contain the support of any other independent codeword. A minimal code is a linear code whose nonzero codewords are minimal. Minimal codewords and minimal codes in general have interesting connections to linear code-based secret sharing schemes (SSS); see [22, 23].

A secret sharing scheme is a method to distribute shares of a secret to each of the participants $\mathcal{P}$ in such a way that only the authorized subsets of $\mathcal{P}$ could reconstruct the secret; see [4, 24].

In [22, 23] Massey considered the use of linear codes for realizing a perfect (i.e. all authorized sets of participants can recover the secret while unauthorized sets of participants cannot determine any shares of the secret) and ideal (i.e. the shares of all participants are of the same size as that of the secret) SSS. It turns out that the access structure of the secret-sharing scheme corresponding to an $[n, k]_q$-code $\mathcal{C}$ is specified by the support of minimal codewords in the dual code $\mathcal{C}^\perp$ having 1 as the first component.

In general, it is quite hard to find the whole set of minimal codewords of a given linear code; see [3, 9]. For this reason, minimal codes have been widely investigated in the last years; see for instance [11, 25]. Most of the known families of minimal codes are in characteristic two.

A sufficient criterion for a linear code to be minimal is given by Ashikhmin and Barg in [2].

Lemma 1.1. *A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is minimal if*

$$\frac{w_{min}}{w_{max}} > \frac{q-1}{q}, \tag{1.1}$$

where w_{min} and w_{max} denote the minimum and maximum nonzero Hamming weights in $\mathcal{C}$, respectively.

Families of minimal linear codes satisfying Condition (1.1) have been considered in several papers; e.g. see [13, 14, 16, 27]. However, Condition (1.1) is not necessary and examples of minimal codes not satisfying Condition (1.1) have been constructed in i.e. [1, 5–7, 10, 12, 15, 19, 26].

In this paper we provide the weight distribution and the parameters of families of minimal codes recently introduced in [26], answering to some open questions.

The constructions of minimal codes presented in [26] can be described in a geometrical way, thanks to connections of minimal codes with cutting blocking sets. The characterization of minimal codes using cutting blocking sets was also provided by [1] independently. Consider the affine space $\mathrm{AG}(k,q) \simeq \mathbb{F}_q^k$ of dimension k over the finite field $\mathbb{F}_q$, q a prime power.

Let $D = \{P_1, \ldots, P_n\}$ be a multiset of points in $\mathrm{AG}(k,q)$ corresponding to the columns of a generator matrix of an $[n,k]_q$ linear code C_D. For a hyperplane $H : \alpha_1 x_1 + \cdots + \alpha_k x_k = 0$ through the origin of $\mathrm{AG}(k,q)$ and a point $P = (\overline{x}_1, \ldots, \overline{x}_k) \in \mathrm{AG}(k,q)$, $H(P)$ denotes $\alpha_1\overline{x}_1 + \cdots + \alpha_k\overline{x}_k$.

With this notation,

$$\mathrm{C}_D := \{(H(P_1), \ldots, H(P_n)) : H \text{ is an hyperplane of } AG(k,q) \text{ through the origin}\}.$$

The authors of [26], following [17,18], call D the defining set of C_D. They also presented an interesting machinery which provides new minimal codes from old ones; see [26, Theorem 43], where they make use of the concept of vectorial cutting blocking set [7].

Theorem 1.2. *Let $k \geq 2$. Let M_1 and M_2 be two vectorial cutting blocking sets in $AG(k,q)$ such that $M_1 = a \cdot M_1$ for any $a \in \mathbb{F}_q^*$. Consider the following subset of $AG(k+1,q)$*

$$\widetilde{[M_1, M_2]} := \{(\mathbf{x}, 1) \in AG(k+1,q) : \mathbf{x} \in M_1\} \bigcup \{(\mathbf{x}, 0) \in AG(k+1,q) : \mathbf{x} \in M_2\}.$$

Then, $\widetilde{[M_1, M_2]}$ is a vectorial cutting blocking set in $AG(k+1,q)$. In particular, $\mathrm{C}_{\widetilde{[M_1,M_2]}}$ is a minimal code of length $(\#M_1 + \#M_2)$ and dimension $(k+1)$.

In [26] the authors constructed several families of minimal codes not satisfying Condition (1.1). They left the determination of the weight distribution of some of them as open problems. In general, the computation of the weight distribution or of the weight spectrum (i.e. the set of its nonzero weights) of codes could be a challenging task. On the other hand, this computation provides important information, since for instance the weight distribution of a code allows the computation of the probability of error detection and correction with respect to some error detection and error correction algorithms; see [21] for more details.

Therefore our aim is to provide the weight spectrum or the weight distribution of specific minimal codes constructed in [26]. In particular, we consider the following families of defining sets.

(1) **Family 1.**

$$D_1 = \left\{ (x_1, \ldots, x_k) \in AG(k,q) \setminus \{\overline{0}\} : \left(\sum_{i=1}^{h} x_i \right) \prod_{i=1}^{h} x_i = 0 \right\},$$

where $4 \leq h \leq k$; see [26, Open Problem 37].

(2) **Family 2.**

$$D_2 = \left\{ (x_1, \ldots, x_k) \in AG(k,q) \setminus \{\overline{0}\} : \prod_{1 \leq i < j \leq h} (x_i + x_j) = 0 \right\},$$

where $3 \leq h \leq k$; see [26, Open Problem 38].

(3) **Family 3.**

$$D_3 = \left\{ (x_1, \ldots, x_k) \in AG(k,q) \setminus \{\overline{0}\} : \prod_{i=1}^{h} x_i \prod_{1 \leq i < j \leq h} (x_i + x_j) = 0 \right\},$$

where $3 \leq h \leq k$; see [26, Open Problem 39].

(4) **Family 4.**

$$D_4 = \left\{ (x_1, \ldots, x_k) \in AG(k,q) \setminus \{\overline{0}\} : \prod_{i=1}^{h} x_i = 0 \right\},$$

where $3 \leq h \leq k$; see [26, Open Problem 48].

We determine the weight distribution of C_{D_1}, $\mathrm{C}_{\widetilde{[D_1, D_1]}}$, and $\mathrm{C}_{\widetilde{[D_4, D_4]}}$, and the parameters of the codes C_{D_2} and C_{D_3}.

Remark 1.3. Our computations also show that the Singleton defect of these families of minimal codes is large. This is not uncommon since usually minimal codes are not optimal from an error-correction point of view.

2. Preliminaries

Throughout this paper $AG(k,q)$ denotes the affine space of dimension k over the Galois field $\mathbb{F}_q$, where $q = p^r$ is a prime power. We recall in this section some basic definitions from coding theory; for a detailed exposition see [20].

Definition 2.1. Let C be a k-dimensional vector subspace of $(\mathbb{F}_q)^n$. Then C is an $\mathbb{F}_q$-*linear code* of dimension k and length n. An element of C is called a *codeword*.

Definition 2.2. For any two vectors $x, y \in (\mathbb{F}_q)^n$, the *Hamming distance* of x and y, denoted by $d(x,y)$, is the number of coordinates where the two vectors differ. Also, the

Hamming weight $\mathrm{w}(x)$ of $x \in (\mathbb{F}_q)^n$ is defined as the Hamming distance of x and the null vector of $(\mathbb{F}_q)^n$.

Definition 2.3. The *minimum distance of a linear code* C (or simply *distance*) is the minimum Hamming distance between any two different codewords of C.

If C is an $\mathbb{F}_q$-linear code with length n, dimension k and minimum distance d, we say that C is an $[n,k,d]_q$ linear code.

Definition 2.4. For an $[n,k,d]_q$ linear code C, we denote by A_i the number of codewords of weight i. The set $\{A_i\}_{i=1,\dots,n}$ is also called the *weight distribution* of C, whereas the A_i's are also called the *weight elements* of C. The set $\{i \mid A_i \neq 0\}$ is called the *weight spectrum* of C.

3. Family 1

By [26, Theorem 23] it is readily seen that the dimension of C_{D_1} is k. By [26, Lemma 32] and [26, Theorem 33], C_D is a minimal code of length

$$n = q^{k-h-1}(q^{h+1} - (q-1)^{h+1} + (-1)^h(q-1)) - 1.$$

In order to compute the weight distribution of C_D it is useful to consider the following integers

$$\begin{aligned}
\psi_s &:= \#\left\{(x_1,\dots,x_s) \in AG(s,q) : \sum_{i=1}^{s} x_i = 0 \text{ and } x_i \neq 0 \text{ for any } i = 1,\dots,s\right\},\\
\varphi_s &:= \#\left\{(x_1,\dots,x_s) \in AG(s,q) : \sum_{i=1}^{s} x_i = 1 \text{ and } x_i \neq 0 \text{ for any } i = 1,\dots,s\right\}.
\end{aligned}$$

As generalization of [26, Lemma 31], we have

$$\psi_s = \frac{(q-1)^s + (-1)^s(q-1)}{q}, \qquad \varphi_s = \frac{(q-1)^s - \psi_s}{q-1}.$$

In particular note that $\psi_0 = 1$ and $\varphi_0 = 0$.

Consider now $a_1,\dots,a_s \in \mathbb{F}_q^*$. It is readily seen that

$$\begin{aligned}
\psi_s &= \#\left\{(x_1,\dots,x_s) \in AG(s,q) : \sum_{i=1}^{s} a_i x_i = 0 \text{ and } x_i \neq 0 \text{ for any } i = 1,\dots,s\right\},\\
\varphi_s &= \#\left\{(x_1,\dots,x_s) \in AG(s,q) : \sum_{i=1}^{s} a_i x_i = 1 \text{ and } x_i \neq 0 \text{ for any } i = 1,\dots,s\right\}.
\end{aligned}$$

Let π be the hyperplane of $AG(k,q)$ through the origin with affine equation

$$a_{i_1}x_{i_1} + \ldots + a_{i_s}x_{i_s} + b_{j_1}x_{j_1} + \ldots + b_{j_r}x_{j_r} = 0, \tag{3.1}$$

where $s \geq 0$, $r \geq 0$, $a_{i_1}, \ldots, a_{i_s}, b_{j_1}, \ldots, b_{j_r} \in \mathbb{F}_q^*$, $i_1, \ldots, i_s \in \{1, \ldots, h\}$ and $j_1, \ldots, j_r \in \{h+1, \ldots, k\}$.

For the weight distribution of C_{D_1}, we need to investigate the number of solutions Λ of the system

$$\begin{cases} a_{i_1}x_{i_1} + \ldots + a_{i_s}x_{i_s} + b_{j_1}x_{j_1} + \ldots + b_{j_r}x_{j_r} = 0 \\ (x_1 + \ldots + x_h)x_1 \cdot \ldots \cdot x_h = 0 \end{cases} . \tag{3.2}$$

Indeed, the weight of the codeword induced by π is $n - \Lambda + 1$.

Proposition 3.1. *Let $r \geq 1$. Then*

$$\Lambda = q^{k-1} - q^{k-h-1}(q-1)^h + \psi_h q^{k-h-1} = q^{k-h-1}(q^h + \psi_h - (q-1)^h).$$

Proof. An easy computation shows that the number of solutions of the system

$$\begin{cases} a_{i_1}x_{i_1} + \ldots + a_{i_s}x_{i_s} + b_{j_1}x_{j_1} + \ldots + b_{j_r}x_{j_r} = 0 \\ x_1 \cdot \ldots \cdot x_h = 0 \end{cases}$$

is $q^{k-1} - q^{k-h-1}(q-1)^h$. Therefore it remains to compute the number of solutions of

$$\begin{cases} a_{i_1}x_{i_1} + \ldots + a_{i_s}x_{i_s} + b_{j_1}x_{j_1} + \ldots + b_{j_r}x_{j_r} = 0 \\ x_1 + \ldots + x_h = 0 \\ x_1 \cdot \ldots \cdot x_h \neq 0. \end{cases} \tag{3.3}$$

The above system (3.3) is equivalent to

$$\begin{cases} x_{j_1} = -\alpha_{i_1}x_{i_1} - \ldots - \alpha_{i_s}x_{i_s} - \beta_{j_2}x_{j_2} - \ldots - \beta_{j_r}x_{j_r} \\ x_1 + \ldots + x_h = 0 \\ x_1 \cdot \ldots \cdot x_h \neq 0, \end{cases} \tag{3.4}$$

with $\alpha_{i_l} = a_{i_l}/b_{j_1}$ and $\beta_{j_l} = b_{j_l}/b_{j_1}$. Since the number of solutions of (3.4) is $\psi_h q^{k-h-1}$, we obtain $\Lambda = q^{k-1} - q^{k-h-1}(q-1)^h + \psi_h q^{k-h-1} = q^{k-h-1}(q^h + \psi_h - (q-1)^h)$. □

Proposition 3.2. *Let $l \geq 1$, $r_1, \ldots, r_l \geq 1$, and consider l pairwise distinct nonzero elements $\alpha_1, \ldots, \alpha_l$ of $\mathbb{F}_q$. Let $A_{r_1,\ldots,r_l}$ be the number of solutions of the system*

$$S_{r_1,\ldots,r_l}(\gamma): \begin{cases} x_1^{(1)} + \ldots + x_{r_1}^{(1)} + x_1^{(2)} + \ldots + x_{r_2}^{(2)} + \cdots + x_1^{(l)} + \ldots + x_{r_l}^{(l)} = \gamma \\ \alpha_1(x_1^{(1)} + \ldots + x_{r_1}^{(1)}) + \alpha_2(x_1^{(2)} + \ldots + x_{r_2}^{(2)}) + \cdots + \alpha_l(x_1^{(l)} + \ldots + x_{r_l}^{(l)}) = 0 \\ \prod_{i,j} x_j^{(i)} \neq 0, \end{cases} \tag{3.5}$$

Then, for $l = 1$, $A_{r_1} = \psi_{r_1}$ if $\gamma = 0$ and $A_{r_1} = 0$ otherwise, and for $l > 1$

$$\begin{cases} A_{r_1,\ldots,r_l} = \psi_{r_1+\cdots+r_{l-1}}\varphi_{r_l} + (-1)^{r_l}A_{r_1,\ldots,r_{l-1}}, & \text{if } \gamma = 0; \\ (\psi_{r_1+\cdots+r_l} - A_{r_1,\ldots,r_l})/(q-1), & \text{if } \gamma \neq 0. \end{cases} \tag{3.6}$$

Proof. We proceed by induction on l and we also show that the number of solutions does not depend on the values $\alpha_1, \ldots, \alpha_l$. If $\ell = 1$, it is clear that if $\gamma \neq 0$ then the number of solutions is 0. Also, if $\gamma = 0$, this number is precisely ψ_{r_1}. Clearly, this does not depend on the value α_1.

Suppose that Formula (3.6) holds for $\ell \geq 1$ and that the number of solutions does not depend on the values $\alpha_1, \ldots, \alpha_l$. Consider $\ell + 1$. We first deal with $\gamma = 0$. The system $S_{r_1,\ldots,r_l,r_{l+1}}(0)$ can be written as

$$S'_{r_1,\ldots,r_l,r_{l+1}}(0): \begin{cases} x_1^{(1)} + \ldots + x_{r_1}^{(1)} + x_1^{(2)} + \ldots + x_{r_2}^{(2)} + \cdots + x_1^{(l+1)} + \ldots + x_{r_{l+1}}^{(l+1)} = 0 \\ (\alpha_1 - \alpha_{l+1})(x_1^{(1)} + \ldots + x_{r_1}^{(1)}) + (\alpha_2 - \alpha_{l+1})(x_1^{(2)} + \ldots + x_{r_2}^{(2)}) \\ \qquad + \cdots + (\alpha_l - \alpha_{l+1})(x_1^{(l)} + \ldots + x_{r_l}^{(l)}) = 0 \\ \prod_{i,j} x_j^{(i)} \neq 0. \end{cases}$$

Each solution of $S'_{r_1,\ldots,r_l,r_{l+1}}(0)$ is a solution of precisely one of the following systems

$$S''_{r_1,\ldots,r_l,r_{l+1}}(\gamma): \begin{cases} x_1^{(1)} + \ldots + x_{r_1}^{(1)} + x_1^{(2)} + \ldots + x_{r_2}^{(2)} + \cdots + x_1^{(l)} + \ldots + x_{r_l}^{(l)} = \gamma \\ x_1^{(l+1)} + \ldots + x_{r_{l+1}}^{(l+1)} = -\gamma \\ (\alpha_1 - \alpha_{l+1})(x_1^{(1)} + \ldots + x_{r_1}^{(1)}) + (\alpha_2 - \alpha_{l+1})(x_1^{(2)} + \ldots + x_{r_2}^{(2)}) \\ \qquad + \cdots + (\alpha_l - \alpha_{l+1})(x_1^{(l)} + \ldots + x_{r_l}^{(l)}) = 0 \\ \prod_{i,j} x_j^{(i)} \neq 0. \end{cases}$$

Viceversa, each solution of a particular $S''_{r_1,\ldots,r_l,r_{l+1}}(\gamma)$ is a solution of $S'_{r_1,\ldots,r_l,r_{l+1}}(0)$.

The number of solutions of $S''_{r_1,\ldots,r_l,r_{l+1}}(\gamma)$ is $A_{r_1,\ldots,r_l}\psi_{r_{l+1}}$ if $\gamma = 0$, and

$$\frac{\psi_{r_1+\cdots+r_l} - A_{r_1,\ldots,r_l}}{q-1}\varphi_{r_{l+1}}$$

otherwise. By hypothesis these numbers do not depend on the choice of $\alpha_1 - \alpha_{l+1}, \ldots, \alpha_l - \alpha_{l+1}$. Summing up, the number of solutions of $S_{r_1,\ldots,r_l,r_{l+1}}(0)$ is

$$\begin{aligned} A_{r_1,\ldots,r_l}\psi_{r_{l+1}} + (q-1)\frac{(\psi_{r_1+\cdots+r_l} - A_{r_1,\ldots,r_l})}{q-1}\varphi_{r_{l+1}} &= \psi_{r_1+\cdots+r_l}\varphi_{r_{l+1}} + A_{r_1,\ldots,r_l}(\psi_{r_{l+1}} - \varphi_{r_{l+1}}) \\ &= \psi_{r_1+\cdots+r_l}\varphi_{r_{l+1}} + (-1)^{r_{l+1}}A_{r_1,\ldots,r_l}. \end{aligned}$$

It is readily seen that the number of solutions of $S_{r_1,\ldots,r_l,r_{l+1}}(\gamma) = S_{r_1,\ldots,r_l,r_{l+1}}(\delta)$ for any non-zero $\gamma, \delta \in \mathbb{F}_q$. The claim follows. □

Remark 3.3. From Proposition (3.2) it follows that

$$A_{r_1,\ldots,r_l} = \psi_{r_1+\cdots+r_{l-1}}\varphi_{r_l} + (-1)^{r_2+\cdots+r_l}\psi_{r_1} + \sum_{i=1}^{l-2}(-1)^{r_{l-i+1}+\cdots+r_l}\psi_{r_1+\cdots+r_{l-i-1}}\varphi_{r_{l-i}}.$$

As a notation, for $r_1, \ldots, r_l$ all distinct from 0, we denote by $A_{r_1,\ldots,r_l,0}$ the integer $A_{r_1,\ldots,r_l}$.

Proposition 3.4. *Let $r = 0$. Then the number of solutions of (3.2) is*

$$\Lambda = q^{k-1} - (q-1)^{h-s}q^{k-h}\psi_s + q^{k-h}A_{r_1,\dots,r_l,h-s}.$$

Proof. Without loss of generality we can assume $(i_1, \dots, i_s) = (1, \dots, s)$. As in Proposition 3.1 we count the number of solutions of two different systems, namely

$$\begin{cases} a_1x_1 + \ldots + a_sx_s = 0 \\ x_1 \cdot \ldots \cdot x_h = 0 \end{cases} \tag{3.7}$$

and

$$\begin{cases} x_1 + \ldots + x_h = 0 \\ a_1x_1 + \ldots + a_sx_s = 0 \\ x_1 \cdot \ldots \cdot x_h \neq 0. \end{cases} \tag{3.8}$$

In order to count the number of solutions of (3.7), we consider

$$\begin{cases} a_1x_1 + \ldots + a_sx_s = 0 \\ x_1 \cdot \ldots \cdot x_h \neq 0. \end{cases}$$

Here, we have $(q-1)^{h-s}q^{k-h}$ choices for $x_{s+1}, \dots, x_k$, while for the remaining coordinates we have ψ_s possibilities: in total $(q-1)^{h-s}q^{k-h}\psi_s$ solutions.

This shows that System (3.7) has $q^{k-1} - (q-1)^{h-s}q^{k-h}\psi_s$ solutions.

We now deal with System (3.8).

We write (3.8) (up to a permutation of $(1, \dots, s)$) in blocks of proportionality as

$$\begin{cases} x_1 + \ldots + x_s + x_{s+1} + \ldots + x_h = 0 \\ \alpha_1(x_1 + \ldots + x_{r_1}) + \ldots + \alpha_l(x_{s-r_l+1} + \ldots + x_s) = 0 \\ x_1 \cdot \ldots \cdot x_s \cdot x_{s+1} \ldots \cdot x_h \neq 0 \end{cases}, \tag{3.9}$$

for some $l \geq 1$, $r_1, \dots, r_l \geq 1$ such that $r_1 + \ldots + r_l = s$, α_i pairwise distinct and nonzero.

Note that if $s = h$ then the number of solutions of (3.9) is $q^{k-h}A_{r_1,\dots,r_l} = q^{k-h}\psi_0 A_{r_1,\dots,r_l} = q^{k-h}\psi_0 A_{r_1,\dots,r_l,0}$.

Suppose now $s < h$. Each solution of (3.9) is a solution of a certain

$$S_\gamma : \begin{cases} x_1 + \ldots + x_s = \gamma \\ x_{s+1} + \ldots + x_h = -\gamma \\ \alpha_1(x_1 + \ldots + x_{r_1}) + \ldots + \alpha_l(x_{s-r_l+1} + \ldots + x_s) = 0 \\ x_1 \cdot \ldots \cdot x_s \cdot x_{s+1} \ldots \cdot x_h \neq 0. \end{cases} \tag{3.10}$$

By Proposition 3.2, for $\gamma = 0$ System (3.10) has $q^{k-h}\psi_{h-s}A_{r_1,\dots,r_l}$ solutions, whereas for $\gamma \neq 0$, the number of solutions is $q^{k-h}\varphi_{h-s}(\psi_{r_1+\cdots+r_l} - A_{r_1,\dots,r_l})/(q-1)$. Summing up, the number of solutions of (3.8) is

$$\begin{aligned} q^{k-h}\psi_{h-s}A_{r_1,\dots,r_l} + q^{k-h}\varphi_{h-s}(\psi_{r_1+\cdots+r_l} - A_{r_1,\dots,r_l}) &= q^{k-h}(\psi_{r_1+\cdots+r_l}\varphi_{h-s} + (-1)^{h-s}A_{r_1,\dots,r_l}) \\ &= q^{k-h}A_{r_1,\dots,r_l,h-s} \end{aligned}$$

The claim follows. □

Finally, we provide the weight spectrum and the weight distribution of the code C_{D_1} answering to [26, Open Problem 37].

For an l-tuple $r_1, \dots, r_l$, we say that it is of type $(i_1, \dots, i_j)$ if there are j distinct values among $r_1, \dots, r_l$ and they are repeated $i_1, \dots, i_j$ times.

Theorem 3.5. *The weight spectrum of the minimal code* C_{D_1} *is*

$$\left\{n - q^{k-h-1}(q^h + \psi_h - (q-1)^h) + 1, n - q^{k-1} - (q-1)^{h-s}q^{k-h}\psi_s + q^{k-h}A_{r_1,\dots,r_l,h-s} + 1\right\},$$

where s *ranges in* $1, \dots, h$ *and* $r_1 + \cdots + r_l = s$. *Moreover, the number* B_i *of codewords of weight* i *is*

(i) $q^k - q^h$, *if* $i = n - q^{k-h-1}(q^h + \psi_h - (q-1)^h) + 1$;
(ii) $\binom{h}{s}\binom{s}{r_1;\dots;r_l}\binom{l}{i_1;\dots;i_j}\binom{q-1}{l}$, *if* $i = n - q^{k-1} - (q-1)^{h-s}q^{k-h}\psi_s + q^{k-h}A_{r_1,\dots,r_l,h-s} + 1$ *and* $r_1, \dots, r_l$ *is of type* $(i_1, \dots, i_j)$.

Proof. The claim on the weight spectrum follows from Propositions 3.1 and 3.4.

Let $\bar{i} = n - q^{k-h-1}(q^h + \psi_h - (q-1)^h) + 1$. By Proposition 3.1, every hyperplane $H : \alpha_1 x_1 + \ldots + \alpha_k x_k = 0$ with $(\alpha_{h+1}, \dots, \alpha_k) \neq (0, \dots, 0)$ induces a codeword of weight $\bar{i}$, whence $B_{\bar{i}} = q^k - q^h$.

Assume now $\bar{i} = n - q^{k-1} - (q-1)^{h-s}q^{k-h}\psi_s + q^{k-h}A_{r_1,\dots,r_l,h-s} + 1$ for a partition $(r_1, \dots, r_l)$ of s, $s \in [1, \dots, h]$, $l \geq 1$, of type $i_1, \dots, i_j$. We count the number of k-tuples of $(\mathbb{F}_q)^k$ such that the last $k-h$ entries are zero and that admit, among the first h entries, l distinct nonzero values and $h - s$ zeros.

The $h - s$ zero entries can be chosen in $\binom{h}{s}$ ways among the first h entries. The possible l-tuples of nonzero elements of $\mathbb{F}_q$ are $\binom{q-1}{l}$. Finally for any chosen l-tuple $\alpha_1 \dots, \alpha_l$, $\binom{s}{r_1;\dots;r_l}\binom{l}{i_1;\dots;i_j}$ counts the number s-uples where $\alpha_1, \dots, \alpha_l$ appear exactly $r_1, \dots, r_l$ times.

Each hyperplane H corresponding to such a k-tuple induces, by Proposition 3.4, a codeword of weight $\bar{i}$.

□

Remark 3.6. The weights in Theorem 3.5 (ii) are not all distinct. For instance, let $h = 4$ and $k \geq h$. Then the weights corresponding to the choices $s = 4$, $r_1 = 3$, $r_2 = 1$ and $s = 2$, $r_1 = 1$, $r_2 = 1$ are equal.

We end this section with explicit tables showing the weight distributions of the codes C_{D_1}.

TABLE 1. Weight Distribution of C_{D_1} for $q = 3$, $h = 4$, and $k = 5$

Weight i	0	132	138	142	144	150
B_i	1	10	30	162	20	20

TABLE 2. Weight Distribution of C_{D_1} for $q = 5$, $h = 4$, and $k = 5$

Weight i	0	1480	1660	1680	1684	1700	1720	1740
B_i	1	20	180	240	2500	24	40	120

TABLE 3. Weight Distribution of C_{D_1} for $q = 7$, $h = 4$, and $k = 5$

Weight i	0	6636	7686	7728	7746	7770	7896	7938
B_i	1	30	450	1200	14406	360	60	300

Remark 3.7. The weight distribution of codes C_{D_1} can be determined using a MAGMA program [8]. For the sake of completeness we include here an example. It can be used to check the correctness of our results. After specifying q, k, and h one can run the following program. Similar programs can be easily obtained for the other codes considered in this paper.

```
V:=VectorSpace(GF(q),k);
P:=PolynomialRing(GF(q),k);
fp:=0;
fm:=1;
for i in [1..h] do
    fp+:=P.i;
    fm*:=P.i;
end for;
f:=fp*fm;
DS:=[v: v in V| Evaluate(f,ElementToSequence(v)) eq 0 and v ne 0];
WeightDistribution(LinearCode(Transpose(Matrix(GF(q),#DS,k,DS))));
```

4. FAMILY 2

By [26, Theorem 23] it is readily seen that the dimension of C_{D_2} is k.

Proposition 4.1. *Let*

$$\Gamma(h,q) := \sum_{s=1}^{\min(h,(q-1)/2)} \frac{(q-1)(q-3)\cdots(q-2s+1)}{s!}\mathcal{S}(h,s),$$

where $\mathcal{S}(x,y)$ is the number of surjective functions from a set of size x to a set of size $y \leq x$.

The code C_{D_2} has length

$$\begin{cases} q^{k-h}\left(q^h - q(q-1)\cdots(q-h+1)\right) - 1, & \text{if } p = 2 \text{ and } h \leq q; \\ q^k - 1, & \text{if } p = 2 \text{ and } h > q; \\ q^{k-h}\left(q^h - \Gamma(h,q) - h\Gamma(h-1,q)\right) - 1, & \text{if } p > 2. \end{cases}$$

Proof. First, we count the number of h-tuples for which

$$\text{no pairs of entries } (x_i, x_j), 1 \leq i < j \leq h, \text{ satisfy } x_i + x_j = 0. \tag{4.1}$$

Assume $p = 2$. In this case the number of h-tuples for which at least one pair of entries (x_i, x_j), $1 \leq i < j \leq h$, satisfies $x_i + x_j = 0$ is $q^h - q(q-1)\cdots(q-h+1)$ (in particular it is q^h if $h > q$).

From now on, let us consider the case $p > 2$. We distinguish two cases.

(1) All entries are nonzero. Suppose that the h entries assume exactly s distinct values $\alpha_1, \ldots, \alpha_s$ of $\mathbb{F}_q^*$. Since $\alpha_i \neq \pm\alpha_j$ for any $i \neq j$, s can be at most $(q-1)/2$. For a given chosen number $s \in \{1, \ldots, \min\{h, (q-1)/2\}\}$, there are $(q-1)(q-3)\cdots(q-2s+1)/s!$ possible choices for the set $\{\alpha_1, \ldots, \alpha_s\}$. In fact α_1 can be chosen in $q-1$ ways, $\alpha_2 \neq \pm\alpha_1$, $\alpha_3 \notin \{\pm\alpha_1, \pm\alpha_2\}$ and so on. Now, when the set $\{\alpha_1, \ldots, \alpha_s\}$ is fixed, the h entries can assume only values $\{\alpha_1, \ldots, \alpha_s\}$. The number of possible h-tuples equals the number $\mathcal{S}(h,s)$ of surjective functions from $\{1, \ldots, h\}$ to $\{\alpha_1, \ldots, \alpha_s\}$. The number of h-tuples satisfying (4.1) is $\Gamma(h,q)$.
(2) One entry is 0. In this case, any other entry is nonzero. To the other $h-1$ entries we can apply the same argument as above. Since the unique 0 entry can appear in h different positions, in this case the number of h-tuples satisfying (4.1) is $h\Gamma(h-1,q)$.

Summing up, there are in total $\Gamma(h,q) + h\Gamma(h-1,q)$ h-tuples satisfying (4.1): the number of h-tuples for which at least one pair of entries (x_i, x_j), $1 \leq i < j \leq h$, satisfies $x_i + x_j = 0$ is $q^h - \Gamma(h,q) - h\Gamma(h-1,q)$. The length of the code C_{D_2} is given by the number of k-tuples in $\mathbb{F}_q$ for which the first h entries can be chosen in $q^h - \Gamma(h,q) - h\Gamma(h-1,q)$ ways.

□

Proposition 4.2. *Let $q > 5$ and $p > 2$. Then the minimum weight in C_{D_2} is realized by the hyperplanes $x_i + x_j = 0$, $1 \leq i < j \leq h$.*

Proof. It is readily seen that all the hyperplanes $x_i + x_j = 0$, $1 \le i < j \le h$, contain $q^{k-1} - 1$ points of D_2 and therefore they correspond to minimum weight codewords. Let H be an hyperplane different from $x_i + x_j = 0$, $1 \le i < j \le h$.

- If $H : x_i + \alpha x_j = 0$ for some $i \neq j$ and $\alpha \neq 1$ then the point
$$(1, \dots, 1, \underbrace{-\alpha}_{i}, 1, \dots, 1) \in H \setminus (D_2 \cup \{0\})$$
and therefore $w(c_H) > n - q^{k-1} + 1$, where n is the length of C_{D_2}.
- Suppose now that $H : x_i = \beta x_l + \sum_{j \in J} \alpha_j x_j$, with $\#J \ge 1$, $\beta \neq 0, -1$, $l \notin J$. Let $\lambda \in \mathbb{F}_q \setminus \{-1, -(\sum_{j\in J} \alpha_j)/(\beta+1), -(1+\sum_{j\in J}\alpha_j)/\beta\}$. Then the point
$$(1, \dots, 1, \underbrace{\lambda}_{l}, 1, \dots, 1, \underbrace{\lambda\beta + \sum_{j\in J} \alpha_j}_{i}, 1, \dots, 1) \in H \setminus (D_2 \cup \{0\})$$
therefore $w(c_H) > n - q^{k-1} + 1$.
- Consider now the case $H : x_i = -x_l - x_s - \sum_{j\in J} x_j$, with $\#J \ge 0$. Let $\lambda \in \mathbb{F}_q \setminus \{-1, -\#J\}$, $\mu \in \mathbb{F}_q \setminus \{-1, -\lambda, -\#J, 1 - \lambda - \#J\}$. Then the point
$$(1, \dots, 1, \underbrace{\lambda}_{l}, 1, \dots, 1, \underbrace{\mu}_{s}, 1, \dots, 1, \underbrace{-\lambda - \mu - \#J}_{i}, 1, \dots, 1) \in H \setminus (D_2 \cup \{0\})$$
therefore $w(c_H) > n - q^{k-1} + 1$.

□

5. Family 3

By [26, Theorem 23] it is readily seen that the dimension of C_{D_3} is k.

Proposition 5.1. *Let $\Gamma(h, q)$ be defined as in Proposition 4.1. The code C_{D_3} has length*

$$\begin{cases} q^{k-h}\left(q^h - (q-1)\cdots(q-h)\right) - 1, & \text{if } p = 2 \text{ and } h < q; \\ q^k - 1, & \text{if } p = 2 \text{ and } h \ge q; \\ q^{k-h}\left(q^h - \Gamma(h,q)\right) - 1, & \text{if } p > 2. \end{cases}$$

Proof. First, we investigate the number of h-tuples for which

(5.1) no coordinates are zero and no pairs $(x_i, x_j), 1 \le i < j \le h,$ satisfy $x_i + x_j = 0$.

Assume first $p > 2$. By the proof of Proposition 4.1 (case (1)) the number of h-tuples satisfying (5.1) equals $\Gamma(h, q)$. Therefore the number of h-tuples for which one coordinate is zero or at least one pair of entries (x_i, x_j), $1 \le i < j \le h$, satisfies $x_i + x_j = 0$ is $q^h - \Gamma(h, q)$. The length of the code C_{D_3} is given by the number of k-tuples in $\mathbb{F}_q$ for which the first h entries are chosen in such $q^h - \Gamma(h, q)$ ways.

Assume now $p = 2$. In this case the number of h-tuples for which one coordinate is zero or at least one pair of entries (x_i, x_j), $1 \le i < j \le h$, satisfies $x_i + x_j = 0$ is $q^h - (q-1)\cdots(q-h)$ (in particular it is q^h if $h \ge q$). The claim follows. □

Proposition 5.2. *Let $q > 5$ and $p > 2$. Then the minimum weight in C_{D_3} is realized by the hyperplanes $x_i + x_j = 0$ and $x_i = 0$, $1 \le i < j \le h$.*

Proof. Clearly, for $1 \le i < j \le h$, any hyperplane $x_i + x_j = 0$ or $x_i = 0$ contains $q^{k-1} - 1$ points of D_3 and hence such hyperplanes correspond to minimum weight codewords. We will show that if H is an hyperplane (through the origin) different from $x_i + x_j = 0$, $1 \le i < j \le h$, and $x_i = 0$, $1 \le i \le h$, then there exists a point $P \in H \setminus D_3$. We argue as in the proof of Proposition 4.2, the only difference being that P must not have zero coordinates.

- If $H : x_i + \alpha x_j = 0$ for some $i \ne j$ and $\alpha \ne 0, 1$ then the point
$$(1, \dots, 1, \underbrace{-\alpha}_{i}, 1, \dots, 1) \in H \setminus (D_3 \cup \{0\})$$
and therefore $w(c_H) > n - q^{k-1} + 1$, where n is the length of C_{D3}.
- Suppose now that $H : x_i = \beta x_l + \sum_{j \in J} \alpha_j x_j$, with $\#J \ge 1$, $\beta \ne 0, -1$, $l \notin J$. Let $\lambda \in \mathbb{F}_q \setminus \{0, -1, -(\sum_{j\in J}\alpha_j)/(\beta+1), -(\sum_{j\in J}\alpha_j)/\beta, -(1+\sum_{j\in J}\alpha_j)/\beta\}$. Then the point
$$(1, \dots, 1, \underbrace{\lambda}_{l}, 1, \dots, 1, \underbrace{\lambda\beta + \sum_{j\in J}\alpha_j}_{i}, 1, \dots, 1) \in H \setminus (D_3 \cup \{0\})$$
therefore $w(c_H) > n - q^{k-1} + 1$.
- Consider now the case $H : x_i = -x_l - x_s - \sum_{j\in J} x_j$, with $\#J \ge 0$. Let $\lambda \in \mathbb{F}_q \setminus \{0, -1, -\#J\}$, $\mu \in \mathbb{F}_q \setminus \{0, -1, -\lambda, -\#J, -\lambda - \#J, 1 - \lambda - \#J\}$. Then the point
$$(1, \dots, 1, \underbrace{\lambda}_{l}, 1, \dots, 1, \underbrace{\mu}_{s}, 1, \dots, 1, \underbrace{-\lambda - \mu - \#J}_{i}, 1, \dots, 1) \in H \setminus (D_3 \cup \{0\})$$
therefore $w(c_H) > n - q^{k-1} + 1$.

□

6. Family 4

In this Section we deal with codes $\mathrm{C}_{\widetilde{[D,D]}}$ as defined in Theorem 1.2. Note that if D is a subset of $\mathrm{AG}(k, q)$ such that $aD = D$ for every $a \in \mathbb{F}_q^*$ and $\#D = n$, then
$$D = \mathbb{F}_q^* P_1 \cup \mathbb{F}_q^* P_2 \cup \cdots \cup \mathbb{F}_q^* P_{n/(q-1)},$$

for some $P_1, \ldots, P_{n/(q-1)} \in D$. Also observe that the weight of any codeword of $\mathrm{C}_{\widetilde{[D,D]}}$ is divisible by $q-1$.

Since the defining set of $\mathrm{C}_{\widetilde{[D,D]}}$ is

$$\{(x_1, \ldots, x_k, 0) : (x_1, \ldots, x_k) \in D\} \cup \{(x_1, \ldots, x_k, 1) : (x_1, \ldots, x_k) \in D\} \subset \mathrm{AG}(k+1, q),$$

it follows that for any hyperplane $H \subset \mathrm{AG}(k+1, q)$ through the origin, the corresponding codeword $c_H \in \mathrm{C}_{\widetilde{[D,D]}}$ can be written as $(c_{H,0}, c_{H,1})$ where

$$c_{H,0} = (H(x_1, \ldots, x_k, 0))_{x \in (\mathbb{F}_q^k)^*} \qquad \text{and} \qquad c_{H,1} = (H(x_1, \ldots, x_k, 1))_{x \in (\mathbb{F}_q^k)^*}.$$

Clearly, $\mathrm{w}(c_H) = \mathrm{w}(c_{H,0}) + \mathrm{w}(c_{H,1})$.

Proposition 6.1. *For $H : \alpha_1 x_1 + \cdots + \alpha_k x_k + \alpha_{k+1} x_{k+1} = 0$, let $\widetilde{H} : \alpha_1 x_1 + \cdots + \alpha_k x_k = 0$. If $c_H \in \mathrm{C}_{\widetilde{[D,D]}}$ and $c_{\widetilde{H}} \in \mathrm{C}_D$ are the codewords corresponding to H and $\widetilde{H}$ respectively, then*

(i) *If $\alpha_{k+1} = 0$ then $\mathrm{w}(c_{H,1}) = \mathrm{w}(c_{H,0})$ and $\mathrm{w}(c_H) = 2\mathrm{w}(c_{\widetilde{H}})$.*
(ii) *If $\alpha_{k+1} \neq 0$ then $\mathrm{w}(c_H) = n + \frac{q-2}{q-1}\mathrm{w}(c_{\widetilde{H}})$.*

Proof. Point (i) is clear.

Suppose now that $\alpha_{k+1} \neq 0$. From the assumptions on D, for each $P = (x_1, \ldots, x_k) \in D$ and $a \in \mathbb{F}_q^*$, the point aP is in D. We distinguish two cases:

(a) If $\widetilde{H}(P) = 0$ then $\widetilde{H}(Q) = 0$ for any $Q \in \mathbb{F}_q^* P$. In this case the entries corresponding to $\mathbb{F}_q^* P$ in $c_{H,0}$ are 0, whereas those in $c_{H,1}$ are nonzero.
(b) If $\widetilde{H}(P) \neq 0$ then there exists a unique value $a \in \mathbb{F}_q^*$ such that $H((ax_1, \ldots, ax_k, 1)) = \widetilde{H}(aP) + \alpha_{k+1} = 0$. In this case no entry corresponding to $\mathbb{F}_q^* P$ in $c_{H,0}$ is 0, whereas exactly one in $c_{H,1}$ vanishes.

Therefore

$$\mathrm{w}(c_{H,1}) = n - \frac{\mathrm{w}(c_{\widetilde{H}})}{q-1}$$

and

$$\mathrm{w}(c_{H,1}) + \mathrm{w}(c_{H,0}) = n - \frac{\mathrm{w}(c_{\widetilde{H}})}{q-1} + \mathrm{w}(c_{\widetilde{H}}) = n + \frac{(q-2)\mathrm{w}(c_{\widetilde{H}})}{q-1}.$$

□

Proposition 6.1 shows that the weight distribution of $\mathrm{C}_{\widetilde{[D,D]}}$ is uniquely determined by the weight distribution of C_D. As a corollary of Proposition 6.1 the following holds.

Corollary 6.2. *Let A_i be the number of codewords of weight i in C_D. Then the weight spectrum of $\mathrm{C}_{\widetilde{[D,D]}}$ is*

$$\bigcup_{i=1}^{n} \left\{ 2i, n + \frac{q-2}{q-1} i : A_i \neq 0 \right\}.$$

Moreover, if B_i denotes the number of codewords of weight i in $\mathrm{C}_{\widetilde{[D,D]}}$, then

$$B_i = \eta_{\frac{i}{2}} A_{\frac{i}{2}} + (q-1)\eta_{(i-n)\frac{q-1}{q-2}} A_{(i-n)\frac{q-1}{q-2}} \tag{6.1}$$

where

$$\eta_s = \begin{cases} 1, & \text{if } s \in \mathbb{Z}; \\ 0, & \text{otherwise.} \end{cases}$$

In what follows we will focus on the computation of the weight distribution of the code $\mathrm{C}_{\widetilde{[D_4,D_4]}}$, where $D_4 = \left\{(x_1,\dots,x_k) \in AG(k,q) \setminus \{\overline{0}\} : \prod_{i=1}^{h} x_i = 0\right\}$. First, we report some information on C_{D_4} proved in [26, Theorem 23].

Proposition 6.3. *C_{D_4} is a $\left[n,\, k\,, n-q^{k-1}+1\right]_q$-code, where $n = q^{k-h}(q^h-(q-1)^h)-1$. Moreover,*

- *C_{D_4} has weight spectrum*
$$\left\{n-q^{k-1}+q^{k-h-1}(q-1)^h+1, n-q^{k-1}+q^{k-h}(q-1)^{h-s}\psi_s+1\right\},$$
where $s = 1,\dots,h$.
- *If A_i denotes the number of codewords of C_{D_4} of weight i, then*
$$A_i = \begin{cases} q^k - q^h, & \text{if } i = n-q^{k-1}+q^{k-h-1}(q-1)^h+1; \\ \binom{h}{s}(q-1)^s, & \text{if } i = n-q^{k-1}+q^{k-h}(q-1)^{h-s}\psi_s+1. \end{cases}$$

As a notation, let

$$\begin{aligned} w_s &= n-q^{k-1}+q^{k-h}(q-1)^{h-s}\psi_s+1, \\ w &= n-q^{k-1}+q^{k-h-1}(q-1)^h+1. \end{aligned}$$

Note that if $h=k$, $A_w = 0$.

We are now in position to address [26, Open Problem 48], providing the parameters and the weight distribution of the code $\mathrm{C}_{\widetilde{[D_4,D_4]}}$.

Proposition 6.4. *$\mathrm{C}_{\widetilde{[D_4,D_4]}}$ is a $[2n,k+1,n]_q$-code, where n is the lenght of C_{D_4}. Moreover, the weight spectrum of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ is*

- *for $k > h$*
$$\left\{0, n, 2w_s, n+w_s\frac{q-2}{q-1}, 2w, n+w\frac{q-2}{q-1}\right\}_{s=1,\dots,h};$$
- *for $k = h$*
$$\left\{0, n, 2w_s, n+w_s\frac{q-2}{q-1}\right\}_{s=1,\dots,h}.$$

Proof. The claim on the weight spectrum is a consequence of Propositions 6.1 and 6.3. We only need to prove that the minimum weight of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ equals n. By Proposition

6.1, the only candidates as minimum weights are those arising from the minimum weight codewords in C_{D_4} and from the null word of C_{D_4} . Therefore, the minimum distance of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ is

$$\min\left(n, 2(n-q^{k-1}+1), (n-q^{k-1}+1)\frac{q-2}{q-1}\right) = n.$$

□

Clearly there may be collisions between two weights in the weight spectrum of Proposition 6.4. In the next proposition we provide a deeper analysis of the weight distribution of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$.

Proposition 6.5. *Let B_i be the number of codewords of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ of weight i. If $q > 3$ the weight distribution of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ is given in Table 4.*

TABLE 4. Weight Distribution of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ for $q > 3$

Weight i	B_i
0	1
n	$q-1$
$2w_s$, *for* $s = 1, \ldots, h$	$\binom{h}{s}(q-1)^s$
$n + w_s\frac{q-2}{q-1}$, *for* $s = 1, \ldots, h$	$\binom{h}{s}(q-1)^{s+1}$
$2w$	$q^k - q^h$
$n + w\frac{q-2}{q-1}$	$(q^k - q^h)(q-1)$

Proof. The claim follows by Corollary 6.2 and Proposition 6.4, after proving that there are no collisions between two weights in the weight spectrum of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$. First, observe that while w and w_s are divisible by $q-1$, they are not divisible by $(q-1)^2$ (possibly with the only exception of w_h). Indeed,

$$\frac{w}{q-1} \equiv \frac{w_s}{q-1} \equiv \frac{q^k-1}{q-1} - \frac{q^{k-1}-1}{q-1} \equiv q^{k-1} \not\equiv 0 \mod q-1 \tag{6.2}$$

for $s = 1, \ldots, h-1$, while if $s = h$

$$\frac{w_h}{q-1} \equiv q^{k-h-1}(q^h + (-1)^h) \mod q-1. \tag{6.3}$$

We now consider all the possibile cases of collision between two weights.

- If $k > h+1$ it is readily seen that $n \neq 2w_s$ and $n \neq 2w$, since $n \equiv -1 \mod q$ whereas $w, w_s \equiv 0 \mod q$. If $k = h+1$ or $k = h$, a direct computation shows that $n < \min\{2w, 2w_s\}$. Indeed,

$$\begin{aligned} 2w_s - n &= n - 2q^{k-1} + 2q^{k-h}(q-1)^{h-s}\psi_s + 2 \\ &> n - 2q^{k-1} + 1 = q^k - q^{k-h}(q-1)^h - 2q^{k-1} > 0, \end{aligned}$$

for $q > 3$. The same argument yields $n < 2w$.

- $n = n + w\frac{q-2}{q-1}$ or $n = n + w_s\frac{q-2}{q-1}$ cannot occur for $q > 3$.
- $w_s = w$ (which yields $2w_s = 2w$ and $n + w_s\frac{q-2}{q-1} = n + w\frac{q-2}{q-1}$) implies

$$(q-1)^{h-s}q^{k-h}\psi_s = (q-1)^h q^{k-h-1}$$

that is

$$q\psi_s = (q-1)^s$$

a contradiction.

- As observed above, since $(q-1)$ divides w and w_s but $(q-1)^2$ does not (except possibly for w_h), we have

$$2w_s \neq n + \frac{q-2}{q-1}w$$

for $s = 1, \ldots, h$, and

$$2w \neq n + \frac{q-2}{q-1}w_s$$

for $s = 1, \ldots, h-1$.

It remains to check if it is possible that $2w = n + \frac{q-2}{q-1}w_h$. Note first that if h is odd then $\frac{w_h}{q-1} \not\equiv 0 \mod q-1$, whence the same argument as above applies and $2w \neq n + \frac{q-2}{q-1}w_h$. Assume now h even. Then $2w = n + \frac{q-2}{q-1}w_h$ reads

$$2(n - q^{k-1} + q^{k-h-1}(q-1)^h + 1) = n + (q-2)(q^{k-h-1}(q^h - (q-1)^h) + q^{k-h-1}),$$

that is

$$n = q^k - q^{k-h}(q-1)^h + q^{k-h} - 2q^{k-h-1} - 2, \tag{6.4}$$

a contradiction to $n \equiv -1 \mod q$.

- If $w_s = w_{s'}$ for some $s, s' \in \{1, \ldots, h\}$ with $s' > s$, then

$$(-1)^{s'}(q-1)^{h-s'+1} = (-1)^s(q-1)^{h-s+1}$$

that is

$$(-1)^{s-s'}(q-1)^{s'-s} = 1,$$

a contradiction to $q > 3$.

- If $2w = n + w\frac{q-2}{q-1}$, then $(q-1)n = qw$; a contradiction, since n is not divisible by q. The same argument also shows that $2w_s \neq n + w_s\frac{q-2}{q-1}$.

□

Remark 6.6. If $q = 3$, almost the same argument in Proposition 6.5 applies: the only difference arises from Equation (6.4) when $k = h+1$. Indeed, in this case, $2w = n + \frac{q-2}{q-1}w_h$. Table 5 shows the weight distribution of $\mathrm{C}_{\widetilde{[D_4, D_4]}}$ for $q = 3$ and $k = h + 1$.

The following tables show the weight distributions of $\mathrm{C}_{\widetilde{[D_4, D_4]}}$ for $h = 4$, $k = 5$ and $q = 3, 5$.

TABLE 5. Weight Distribution of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ for $q=3$ and $k=h+1$

Weight i	B_i
0	1
n	2
$2w_s$, for $s=1,\ldots,k-1$	$\binom{k-1}{s}2^s$
$n+w_s/2$, for $s=1,\ldots,k-2$	$\binom{k-1}{s}2^{s+1}$
$2w$	3^k-3^{k-1}
$n+w/2$	$2(3^k-3^{k-1})$

TABLE 6. Weight Distribution of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ for $q=3$, $h=4$, and $k=5$

Weight i	0	194	228	251	252	257	259	260	263	264	276
B_i	1	2	8	16	32	64	324	194	48	16	24

TABLE 7. Weight Distribution of $\mathrm{C}_{\widetilde{[D_4,D_4]}}$ for $q=5$, $h=4$, and $k=5$

Weight i	0	1844	2440	2759	2920	2939	2951	2952	2954	2960	2999	3080
B_i	1	4	16	64	256	1024	10000	2500	1024	256	384	96

As an application of Proposition 6.1 we provide the weight distribution of the code $\mathrm{C}_{\widetilde{|D_1,D_1|}}$. In this case we will not deal with possible collisions of two weights (since this problem is already hard to study for the weight distribution of C_{D_1}).

Proposition 6.7. *With the same notation as in Theorem 3.5, the weight distribution of* $\mathrm{C}_{\widetilde{[D_1,D_1]}}$ *is given in Table 8.*

TABLE 8. Weight Distribution of $\mathrm{C}_{\widetilde{[D_1,D_1]}}$

Weight i	B_i
0	1
n	$q-1$
$2(n-q^{k-h-1}(q^h+\psi_h-(q-1)^h)+1)$	q^k-q^h
$n+(n-q^{k-h-1}(q^h+\psi_h-(q-1)^h)+1)\frac{q-2}{q-1}$	$(q-1)(q^k-q^h)$
$2(n-q^{k-1}-(q-1)^{h-s}q^{k-h}\psi_s+q^{k-h}A_{r_1,\ldots,r_l,h-s}+1)$	$\binom{h}{s}\binom{s}{r_1;\ldots;r_l}\binom{l}{i_1;\ldots;i_j}\binom{q-1}{l}$
$n+(n-q^{k-1}-(q-1)^{h-s}q^{k-h}\psi_s+q^{k-h}A_{r_1,\ldots,r_l,h-s}+1)\frac{q-2}{q-1}$	$(q-1)\left(\binom{h}{s}\binom{s}{r_1;\ldots;r_l}\binom{l}{i_1;\ldots;i_j}\binom{q-1}{l}\right)$
$n+(n-q^{k-1}-(q-1)^{h-s}q^{k-h}\psi_s+q^{k-h}A_{r_1,\ldots,r_l,h-s}+1)\frac{q-2}{q-1}$	$(q-1)\left(\binom{h}{s}\binom{s}{r_1;\ldots;r_l}\binom{l}{i_1;\ldots;i_j}\binom{q-1}{l}\right)$

The following table shows the weight distribution of $\mathrm{C}_{\widetilde{[D_1,D_1]}}$ for $h=4$, $k=5$ and $q=3$.

Finally, we present the following open problems.

TABLE 9. Weight Distribution of $\mathrm{C}_{\widetilde{[D_1,D_1]}}$ for $q=3$, $h=4$ and $k=5$

Weight i	0	212	264	276	278	281	283	284	287	288	300
B_i	1	2	10	30	20	60	324	202	40	20	20

Open Problem 6.8. Determine the weight distribution (without collisions) of C_{D_1} and $\mathrm{C}_{\widetilde{[D_1,D_1]}}$.

Open Problem 6.9. Determine the weight distribution of C_{D_2} and C_{D_3}.

7. Acknowledgments*

The research of D. Bartoli, M. Bonini, and M. Timpanella was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

References

[1] G. N. Alfarano, M. Borello, A. Neri. A geometric characterization of minimal codes and their asymptotic performance. arXiv:1911.11738 (2019).

[2] A. Ashikhmin, A. Barg. Minimal vectors in linear codes. *IEEE Trans. Inf. Theory* **44**(5), 2010–2017 (1998).

[3] E. R Berlekamp, R. J. McEliece, H. C. A. van Tilborg. On the Inherent Intractability of Certain Coding Problems. *IEEE Trans. Inform. Theory* **24**(3), 384–386 (1978).

[4] G. R. Blakley. Safeguarding cryptographic keys. In: *Proc. of AFIPS National Computer Conference*, New York, USA, pp. 313–317 (1979).

[5] D. Bartoli, M. Bonini. Minimal linear codes in odd characteristic. *IEEE Trans. Inf. Theory* **65**(7), 4152–4155 (2019).

[6] D. Bartoli, M. Bonini, B. Gűnes. An inductive construction of minimal codes. arXiv:1911.09093 (2019).

[7] M. Bonini, M. Borello. Minimal linear codes arising from blocking sets. *Journal of Algebraic Combinatorics*. https://link.springer.com/article/10.1007/s10801-019-00930-6.

[8] Bosma, W., Cannon, J., and Playoust, C. 1997. The Magma algebra system. I. The user language. *J. Symb. Comput.*, **24**, 235–265.

[9] J. Bruck, M. Naor. The Hardness of Decoding Linear Codes with Preprocessing. *IEEE Trans. Inform. Theory* **36**(2), 381–385 (1990).

[10] S. Chang, J. Y. Hyun. Linear codes from simplicial complexes. *Des. Codes Cryptogr.* **86**(10), 2167–2181 (2018).

[11] H. Chabanne, G. Cohen, A. Patey. Towards secure two-party computation from the wire-tap channel. In: *Information Security and Cryptology – ICISC 2013*, Heidelberg, Germany, 2014, pp. 34–46.

[12] G. D. Cohen, S. Mesnager, A. Patey. On minimal and quasi-minimal linear codes. In: *IMACC 2013*, Heidelberg, Germany, 2013, pp. 85–98.

[13] C. Carlet, C. Ding, J. Yuan. Linear codes from highly nonlinear functions and their secret sharing schemes. *IEEE Trans. Inf. Theory* **51**(6), 2089–2102 (2005).

[14] C. Ding. Linear codes from some 2-designs. *IEEE Trans. Inf. Theory* **60**(6), 3265–3275 (2015).

[15] C. Ding, Z. Heng, Z. Zhou. Minimal binary linear codes. *IEEE Trans. Inf. Theory* 64(10), 6536–6545 (2018).
[16] C. Ding, N. Li, C. Li, Z. Zhou. Three-weight cyclic codes and their weight distributions. *Discrete Math.* **339**(2), 415–427 (2016).
[17] C. Ding, J. Luo, H. Niederreiter. Two weight codes punctured from irreducible cyclic codes. In: Li, Y., Ling, S., Niederreiter, H., Wang, H., Xing, C., Zhang, S. (Eds.) Proc. of the First InternationalWorkshop on Coding Theory and Cryptography, pp. 119–124. Singapore,World Scientific, (2008).
[18] C. Ding, H. Niederreiter. Cyclotomic linear codes of order 3. *IEEE Trans. Inf. Theory* **53**, 2274–2277 (2007).
[19] Z. Heng, C. Ding, Z. Zhou. Minimal linear codes over finite fields. *Finite Fields Appl.* **54**, 176–196 (2018).
[20] W.C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.
[21] T. Kløve. Codes for Error Detection. Singapore: World Scientific, 2007.
[22] J. L. Massey. Minimal codewords and secret sharing. In: Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory, Sweden, pp. 276–279 (1993).
[23] J. L. Massey. Some applications of coding theory in cryptography. In: Codes and Cyphers: Cryptography and Coding IV, Esses, England, pp. 33–47 (1995).
[24] A. Shamir. How to share a secret. *Commun. ACM* **22**(11), 612–613 (1979).
[25] Y. Song, Z. Li, Y. M. Li. Secret sharing with a class of minimal linear codes. Acta Electronic Sinica **41**, 220–226 (2013).
[26] C. Tang, Y. Qiu, Q. Liao, Z. Zhou. Full Characterization of Minimal Linear Codes as Cutting Blocking Sets. arXiv:1911.09867 (2019)
[27] J. Yuan, C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Trans. Inf. Theory* **52**(1), 206–212 (2006).

Dipartimento di Matematica e Informatica, Università degli Studi di Perugia

Email address: daniele.bartoli@unipg.it

Dipartimento di Matematica, Università di Trento

Email address: matteo.bonini@unitn.it

Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata

Email address: marco.timpanella@unibas.it