On the minimum number of minimal codewords

Romar dela Cruz[1], Michael Kiermaier[2], Sascha Kurz[2] and Alfred Wassermann[2]

[1]Institute of Mathematics, University of the Philippines Diliman, Philippines
[2]Mathematisches Institut, University of Bayreuth, Germany

Abstract

We study the minimum number of minimal codewords in linear codes using techniques from projective geometry. Minimal codewords have been used in decoding algorithms and cryptographic protocols. First, we derive a new lower bound on the number of minimal codewords. Then we give a formula for the minimum number of minimal codewords of linear codes for certain lengths and dimensions. We also determine the exact value of the minimum for a range of values of the length and dimension. As an application, we completed a table of the minimum number of minimal codewords for codes of length up to 15. Finally, we discuss an extension of the geometric approach to minimal subcode supports.

1 Introduction

The support of a vector is the set of its nonzero coordinate positions. In a linear code, a nonzero codeword is said to be *minimal* if its support does not properly contain the support of another nonzero codeword. Minimal codewords can be viewed as circuits in matroids and also as cycles in graphs (see for instance [3, 4, 5, 10, 14, 15, 18]). In coding theory, minimal codewords were first used in decoding algorithms [1, 2, 17]. The number of minimal codewords in a linear code gives a lower bound on the complexity of these algorithms. They were reintroduced by Massey [22] in the context of secret sharing schemes where it was shown that the access structure of code-based schemes can be described by the minimal codewords of the dual code.

General properties of minimal codewords were presented in [1, 2, 7, 17]. The main question concerning minimal codewords is to completely determine them for a given linear code. A general algorithm was given by Agrell in [1] that uses the generator matrix or the parity-check matrix of the code. However, the method is highly inefficient when the size of the code is large. For some linear codes, the minimal codewords were determined by exploiting special properties of those codes, for instance see [1, 7, 9, 12, 23, 27].

Another line of research is the construction of codes with special properties that lead to a complete description of the minimal codewords. A major example are the so-called *minimal linear codes*, that is, linear codes whose nonzero codewords are all minimal. These codes were first studied in [7, 13] and were also used in the protocol for secure two-party computation proposed in [11].

The authors in [3, 4, 5] initiated a new research direction by studying the maximum and minimum number of minimal codewords in binary linear codes. Given the length and dimension, bounds and some exact values were presented. These can be seen as a coding-theoretic analogue of studies on the number of circuits in matroids [14] and on the number of cycles in graphs [15].

In this work, we present new results on the minimum number of minimal codewords using techniques from projective geometry. We derive a lower bound on the number of minimal codewords of a linear code using a geometric characterization of minimal (and non-minimal) codewords. As a consequence, we obtain exact values of the minimum number of minimal codewords of linear codes of certain lengths and dimensions. The geometric approach can also be extended to minimal subcode supports. We also complete the table presented in [3] showing the minimum number of minimal codewords for small lengths and dimensions.

One of the key ideas we used to obtain our results is the correspondence between a minimal codeword and a hyperplane with the property that it has a basis contained in the set of projective points associated with the code. This geometric characterization of minimal codewords was first noted in a different form by Agrell in [2]. Some recent papers [8, 6, 21, 24] on minimal linear codes also utilized this geometric view but in a way that is different from the one used in this work. Those papers use it to study the constructions and properties of minimal codes while this work applies it to the problem of finding the minimum number of minimal codewords in linear codes (not necessarily minimal codes).

2 Theoretical background

Let $\mathbb{F}_q$ be the finite field with q elements where q is a power of a prime. A q-ary $[n,k]_q$ *linear code* C is a k-dimensional subspace of the n-dimensional vector space $\mathbb{F}_q^n$. Elements $c \in C$ are called *codewords* and n is called the *length* of the code. The *support* of a codeword c is the set of coordinates with a non-zero entry, i.e., $\operatorname{supp}(c) = \{i \in \{1,\ldots,n\} : c_i \neq 0\}$. The *Hamming weight* $\operatorname{wt}(c)$ of a codeword is the cardinality $|\operatorname{supp}(c)|$ of its support. We define $\operatorname{supp}(C) = \cup_{c\in C} \operatorname{supp}(c)$ and call $|\operatorname{supp}(C)|$ the *effective length* of C. We call a code C *non-trivial* if its dimension $\dim(C) = k$ is at least 1. Here we assume that all codes are non-trivial and that the effective length equals the length n (or $n(C)$ to be more precise). A matrix G with the property that the linear span of its rows generate the code C, is a *generator matrix* of C.

Consider the projective space $PG(\mathbb{F}_q^k)$ and recall that its points are the 1-dimensional subspaces, its lines are the 2-dimensional subspaces and its hyperplanes are the $(k-1)$-dimensional subspaces of $\mathbb{F}_q^k$. We use the abbreviation $\begin{bmatrix}k\\1\end{bmatrix}_q = \frac{q^k-1}{q-1}$ for the number of points in $PG(\mathbb{F}_q^k)$. The number of hyperplanes is also given by $\begin{bmatrix}k\\1\end{bmatrix}_q$.

Let G_i, $1 \leq i \leq n$, be the ith column of a generator matrix G of C. To each $[n,k]_q$ code C, we can assign a multiset $\mathcal{P}$ of points in $PG(\mathbb{F}_q^k)$ by considering $\langle G_i \rangle$, the span of G_i. For convenience of notation, we let $\mathcal{P} = \{\langle G_1\rangle, \langle G_2\rangle, \ldots, \langle G_n\rangle\}$. Technically, a multiset of points can be described by a characteristic function χ mapping each point of $PG(\mathbb{F}_q^k)$ to a non-negative integer. With this, the cardinality $|\mathcal{P}|$ is just the sum over $\chi(P)$ for all points P. By construction, $|\mathcal{P}|$ equals the effective length of C.

Each non-zero codeword $c \in C$ corresponds to a hyperplane H in $PG(\mathbb{F}_q^k)$ such that the set of zero coordinates of c corresponds to $\mathcal{P} \cap H$. In other words, $i \in \operatorname{supp}(c)$ if and only if $G_i \in PG(\mathbb{F}_q^k) \setminus (\mathcal{P} \cap H)$. Hence, $\operatorname{wt}(c) = |\mathcal{P}| - |\mathcal{P} \cap H|$. We call two codewords *equivalent* if they arise by a multiplication with a nonzero field element, so that equivalent codewords correspond to the same hyperplane.

A codeword of $C\backslash\{\mathbf{0}\}$ is called *minimal* if its support does not properly contain the support of another nonzero codeword. General properties of minimal codewords are discussed in [7]. We denote by $M(C)$ the number of non-equivalent minimal codewords in C, so that $M(C) \leq \begin{bmatrix} k \\ 1 \end{bmatrix}_q$. If G is a generator matrix of C and C' is the code that arises if we remove all zero-columns and all duplicated columns from G, then $M(C) = M(C')$. A code without zero- and duplicated columns in a generator matrix is called *projective.* In geometric terms this means that the multiset $\mathcal{P}$ is indeed a set.

We denote by $m_q(n,k)$ the minimum of $M(C)$ for all projective $[n,k]_q$ codes C so that $m_q(n,k)$ is undefined if $n < k$ or $n > \begin{bmatrix} k \\ 1 \end{bmatrix}_q$. Obviously, we have $m_q(k,k) = k$, $m_q\left(\begin{bmatrix} k \\ 1 \end{bmatrix}_q, k\right) = \begin{bmatrix} k \\ 1 \end{bmatrix}_q$, and $m_q(n,k) \leq m_q(n',k)$ for $k \leq n \leq n' \leq \begin{bmatrix} k \\ 1 \end{bmatrix}_q$.

Similarly, we define $M_q(n,k)$ to be the maximum of $M(C)$ for all projective $[n,k]_q$ codes C. This quantity was studied in [4, 5] for the case of binary codes. The focus of this work is on $m_q(n,k)$ and it is interesting to note that finding the minimum of $M(C)$ is one of the problems raised in [17], the paper that introduced the concept of minimal codewords.

Kashyap showed that $m_2(n,k) \geq n$ and that the only binary codes that meet this bound are the direct sum of Simplex codes [19]. An alternative proof of the aforementioned lower bound was given in [3]. The authors in [3] also showed that $m_2(n,n-1) = n, m_2(n,n-2) = n$ for $n \geq 6$, and computed bounds or exact values of $m_2(n,k)$ for $1 \leq k \leq n \leq 15$. They also determined the exact values of $m_2(n,k)$ restricted to the cycle codes from graphs for $1 \leq k \leq n \leq 15$.

3 A geometric approach to minimal codewords

Let C be a projective $[n,k]_q$ code and let $\mathcal{P}$ be the corresponding set of points in $PG(\mathbb{F}_q^k)$. For a codeword $c \in C$, we denote by H_c the corresponding hyperplane in $PG(\mathbb{F}_q^k)$. Suppose c is not minimal. Then there exists a non-zero codeword c' such that $\operatorname{supp}(c') \subset \operatorname{supp}(c)$. Equivalently, $(\mathcal{P} \cap H_c) \subset (\mathcal{P} \cap H_{c'})$. Thus, we have the following geometric characterization of minimal codewords:

Lemma 3.1. *A non-zero codeword c in an $[n,k]_q$ code C is minimal if and only if $\langle \mathcal{P} \cap H_c \rangle = H_c$ or, equivalently, $\dim(\langle \mathcal{P} \cap H_c \rangle) = k-1$.*

We note that an equivalent characterization in terms of the generator matrix was obtained by Agrell [2]. We can deduce from Lemma 3.1 that if $c \in C$ is a minimal codeword then $d \leq \operatorname{wt}(c) \leq n-k+1$ where d is the minimum Hamming weight of C. This is a known property of minimal codewords, see [17].

Another well-known result that can be obtained from Lemma 3.1 concerns $M_q(n,k)$. Since the dimension of a hyperplane is $k-1$ then we have $M_q(n,k) \leq \binom{n}{k-1}$. This result was first proved in [14] for matroids, and an alternative proof was given in [4] for binary codes. We have equality if and only if each $(k-1)$-subset of $\mathcal{P}$ spans a distinct hyperplane. This means that $\mathcal{P}$ is an n-arc in $PG(\mathbb{F}_q^k)$ or, equivalently, C is an MDS code.

It follows that for each non-zero non-minimal codeword c, there exists a subspace $U_c \leq H_c$ of dimension $k-2$, i.e., co-dimension 2, with $\langle \{x : x \in \mathcal{P} \cap H_c\} \rangle \leq U_c$. Note that there may be several such subspaces U_c and the existence of at least one such subspace U_c implies that c is a non-minimal codeword.

We now present a lower bound on $M(C)$, the number of non-equivalent minimal codewords in C. We recall that $M(C) \leq \begin{bmatrix} k \\ 1 \end{bmatrix}_q$. Let $\alpha_q(k,r)$ denote the minimum cardinality of a point set

$\mathcal{S} \subseteq PG(\mathbb{F}_q^k)$ such that there exist r different hyperplanes $H_1, \dots, H_r$ and r subspaces $U_1, \dots, U_r$ of co-dimension 2 with $U_i \le H_i$ for all $1 \le i \le r$ and $\cup_{i=1}^r (H_i \backslash U_i) \subseteq \mathcal{S}$. For $k = 2$, we define $\alpha_q(2, r) = r$ and for $r = 0$, we define $\alpha_q(k, 0) = 0$.

Proposition 3.2. *Let C be a projective $[n, k]_q$ code and $1 \le r \le {k \brack 1}_q$ be an integer. If $n > {k \brack 1}_q - \alpha_q(k, r)$ then $M(C) > {k \brack 1}_q - r$.*

Proof. If $M(C) \le {k \brack 1}_q - r$, then C contains at least r non-minimal codewords. These imply the existence of r different hyperplanes $H_1, \dots, H_r$ and r subspaces $U_1, \dots, U_r$ of co-dimension 2 with $U_i \le H_i$ for all $1 \le i \le r$ and $\mathcal{P} \cap (\cup_{i=1}^r (H_i \backslash U_i)) = \emptyset$. Thus, $n = |\mathcal{P}| \le {k \brack 1}_q - \alpha_q(k, r)$. □

The values of $\alpha_q(k, r)$ are easy to determine analytically if r is small. First, we have $\alpha_q(k, 1) = q^{k-2}$ since $|H \backslash U| = q^{k-2}$ for any hyperplane H and subspace $U \le H$ of co-dimension 2.

Proposition 3.3. *$\alpha_q(k, 2) = 2q^{k-2} - q^{k-3}$ for $k \ge 3$.*

Proof. We consider $\mathcal{S} = (H_1 \backslash U_1) \cup (H_2 \backslash U_2)$ for two distinct hyperplanes H_1 and H_2, so that $\dim(H_1 \cap H_2) = k - 2$. We have $|\mathcal{S}| = 2q^{k-2} - |(H_1 \backslash U_1) \cap (H_2 \backslash U_2)|$. If $H_1 \cap H_2 = U_1$ or $H_1 \cap H_2 = U_2$ then $|\mathcal{S}| = 2q^{k-2}$. Otherwise, we have $|(H_1 \backslash U_1) \cap (H_2 \backslash U_2)| = q^{k-3}$ or $q^{k-3} - q^{k-4}$ (if $k \ge 4$). Therefore, $\alpha_q(k, 2) = 2q^{k-2} - q^{k-3}$ for $k \ge 3$. □

A *κ-arc* in $PG(\mathbb{F}_q^3)$ is a set of κ points in $PG(\mathbb{F}_q^3)$ no three of which are collinear. A *dual κ-arc* in $PG(\mathbb{F}_q^3)$ is a set of κ lines in $PG(\mathbb{F}_q^3)$ no three of which have a common point. The maximum possible κ such that a κ-arc in $PG(\mathbb{F}_q^3)$ exists is well known. It is $q + 2$ if the field size q is even and $q + 1$ otherwise, see e.g. [16].

Proposition 3.4. *Let $r \ge 3$ and $k \ge 3$. We have $\alpha_q(k, r) = r \cdot q^{k-2} - \binom{r}{2} \cdot q^{k-3}$ if q is odd and $r \le q$ or if q is even and $r \le q + 1$.*

Proof. First we note that $\alpha_q(k, r) \ge r \cdot q^{k-2} - \binom{r}{2} q^{k-3}$ for $k \ge 3$ and $r \ge 1$, see the analysis in the proof of Proposition 3.3. We will show that this lower bound is also tight if r is not too large.

Fix a subspace X of co-dimension 3. All subspaces H_i and U_i, $i = 1, 2, 3$, to be constructed will contain X, thus we can describe the setting in the quotient space $\overline{V} := \mathbb{F}_q^k / X \cong \mathbb{F}_q^3$, which may be considered geometrically as a projective plane. In $\overline{V}$ we choose dual $(r + 1)$-arc $L_1, \dots, L_{r+1}$, which is possible due to the assumed upper bound on r. By construction, the intersections of the L_i are pairwise disjoint. For $1 \le i \le r$ let $P_i = L_i \cap L_{r+1}$, i.e., the intersection point of the lines L_i and L_{r+1}. With this, we set $H_i = \langle L_i, X \rangle$ and $U_i = \langle P_i, X \rangle$ for $1 \le i \le r$.

Let $\mathcal{S} = \cup_{i=1}^r (H_i \backslash U_i)$. Since $|H_i \backslash U_i| = q^{k-2}$ for $1 \le i \le r$, $|(H_i \backslash U_i) \cap (H_j \backslash U_j)| = q^{k-3}$ for $1 \le i < j \le r$, and $\cap_{i \in I} (H_i \backslash U_i) = \emptyset$ (note that $\cap_{i \in I} H_i = \cap_{i \in I} U_i = X$) for all $I \subseteq \{1, \dots, r\}$ with $|I| \ge 3$, we have $|\mathcal{S}| = r \cdot q^{k-2} - \binom{r}{2} \cdot q^{k-3}$. □

To turn the bound of Proposition 3.2 into a statement on exact values for $m_q(n, k)$ is slightly more technical:

Proposition 3.5. *For a given field size q, let n and k be positive integers with $2 \le k \le n \le {k \brack 1}_q$. Let $1 \le r \le {k \brack 1}_q$ be an integer with $n > {k \brack 1}_q - \alpha_q(k, r)$ and $n \le {k \brack 1}_q - \alpha_q(k, r - 1)$. Then $m_q(n, k) = {k \brack 1}_q - r + 1$.*

Proof. From Proposition 3.2 we directly conclude $m_q(n,k) \geq \begin{bmatrix} k \\ 1 \end{bmatrix}_q - r + 1$. Let $\mathcal{S}$ be a set of points in $PG(\mathbb{F}_q^k)$ attaining $\alpha_q(k, r-1)$ and C be the linear code corresponding to the complement of $\mathcal{S}$. Then, C has effective length $n' = \begin{bmatrix} k \\ 1 \end{bmatrix}_q - \alpha_q(k, r-1) \geq n$ and at least $r-1$ non-minimal codewords. If C has at least r non-minimal codewords, then $\alpha_q(k,r) \leq \alpha_q(k, r-1)$, i.e., $\alpha_q(k,r) = \alpha_q(k,r-1)$, which is impossible due to our assumption on n. Thus, C has exactly $r-1$ non-minimal codewords. Since $n' \geq n$ we have $m_q(n,k) \leq m_q(n',k) \leq \begin{bmatrix} k \\ 1 \end{bmatrix}_q - r + 1$. □

Corollary 3.6. *For $k \geq 2$, we have $m_q(n,k) = \begin{bmatrix} k \\ 1 \end{bmatrix}_q$ if and only if $\begin{bmatrix} k \\ 1 \end{bmatrix}_q - q^{k-2} < n \leq \begin{bmatrix} k \\ 1 \end{bmatrix}_q$.*

Proof. Setting $r = 1$ in Proposition 3.5, we obtain that for $k \geq 2$, if $\begin{bmatrix} k \\ 1 \end{bmatrix}_q - q^{k-2} < n \leq \begin{bmatrix} k \\ 1 \end{bmatrix}_q$ then $m_q(n,k) = \begin{bmatrix} k \\ 1 \end{bmatrix}_q$. Next we show that $m_q\left(\begin{bmatrix} k \\ 1 \end{bmatrix}_q - q^{k-2}, k\right) < \begin{bmatrix} k \\ 1 \end{bmatrix}_q$. Let H be a hyperplane and $U \leq H$ a subspace of co-dimension 2. Consider the code C whose point set $\mathcal{P} = PG(\mathbb{F}_q^k) \backslash (H \backslash U)$. Note that $|\mathcal{P}| = \begin{bmatrix} k \\ 1 \end{bmatrix}_q - q^{k-2}$. Then C has at least one non-minimal codeword (the one associated with H). □

Since $m_q(n,k)$ attains the maximum possible value for $M(C)$ then all codes in this range are minimal linear codes. If C is an $[n,k]_q$ minimal code then it was shown in [6, 21, 24] that the length satisfies $n \geq (k-1)q + 1$. The case of $r = 1$ above gives a tight lower bound for projective $[n,k]_q$ minimal codes as $n \geq \begin{bmatrix} k \\ 1 \end{bmatrix}_q - q^{k-2} + 1$.

When $r = 2$ in Proposition 3.5, we get: for $k \geq 3$, if $\begin{bmatrix} k \\ 1 \end{bmatrix}_q - 2q^{k-2} + q^{k-3} < n \leq \begin{bmatrix} k \\ 1 \end{bmatrix}_q - q^{k-2}$ then $m_q(n,k) = \begin{bmatrix} k \\ 1 \end{bmatrix}_q - 1$. For this range of k and n, the value of $m_q(n,k)$ is the maximum possible value. Hence, we can say that each code C in this range has $M(C) = \begin{bmatrix} k \\ 1 \end{bmatrix}_q - 1$, i.e. has exactly one non-minimal codeword.

We can apply the above discussion to update the tables given in [3]. For example, we have $m_2(6,3) = 7$ and $m_2(n,4) = 15$ for $n = 12, 13, 14, 15$. For the remaining entries of Table 1 we consider an exhaustive enumeration of linear codes. First note that if a linear code C contains a codeword of weight 1 then removing the corresponding coordinate yields a code C' with $n(C') = n(C) - 1$ and $M(C') = M(C) - 1$. Thus it is sufficient to consider all projective $[n,k]_2$ codes with minimum distance at least 2. These can be generated easily and for each code we can simply count the number of minimal codewords. To this end we have applied the algorithm from [20].

4 Minimal subcode supports

The geometric approach used in the previous section can be extended to subcode supports. Let C be a projective $[n,k]_q$ code and let D be an l-dimensional subcode of C. The *support of* D, denoted by $\operatorname{supp}(D)$, is the union of the supports of all the codewords in D and the *weight of* D, denoted by $\operatorname{wt}(D)$, is the cardinality of its support. The l-th *generalized Hamming weight* d_l of C is the minimum among the weights of the r-dimensional subcodes of C [26]. In short,

$$\begin{aligned} \operatorname{supp}(D) &= \{i \in \{1, \ldots, n\} \ : \ \exists\, v \in D \text{ with } v_i \neq 0\} \\ \operatorname{wt}(D) &= |\operatorname{supp}(D)| \\ d_l &= \min\{\operatorname{wt}(D) \ : \ D \leq C, \dim(D) = l\}. \end{aligned}$$

n/k	2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	3	3												
4		4	4											
5		6	5	5										
6		7	6	6	6									
7		7	8	7	7	7								
8			8	9	8	8	8							
9			12	9	9	9	9	9						
10			14	10	10	10	10	10	10					
11			14	15	11	11	11	11	11	11				
12			15	15	13	12	12	12	12	12	12			
13			15	16	14	13	13	13	13	13	13	13		
14			15	16	14	15	14	14	14	14	14	14	14	
15			15	16	17	15	16	15	15	15	15	15	15	15

Table 1: $m_2(n,k)$ for $3 \leq n \leq 15, 1 \leq k \leq 9$

For a given subcode D with $\dim(D) = l$, we can associate a subspace in $PG(\mathbb{F}_q^k)$ of codimension l. Let G be a generator matrix for C. Then there exists an $l \times k$ matrix M such that the rows of MG form a basis for D. The nullspace W of M is a subspace in $PG(\mathbb{F}_q^k)$ of co-dimension l. In fact, there is a one-to-one correspondence between the subcodes of C of dimension l and subspaces of $PG(\mathbb{F}_q^k)$ of co-dimension l (for more details, see [18, 25]).

Let $\mathcal{P} \subseteq PG(\mathbb{F}_q^k)$ be the set of points associated with C. Let D be an l-dimensional subcode of C. Then D corresponds to a subspace W in $PG(\mathbb{F}_q^k)$ of co-dimension l. From [18], we have $\operatorname{supp}(D) = PG(\mathbb{F}_q^k)\backslash(\mathcal{P} \cap W)$ and $wt(D) = n - |\mathcal{P} \cap W|$. The l-th generalized Hamming weight $d_l = n - \min\{|\mathcal{P} \cap W| \ : \ W$ subspace of co-dimension $l\}$. We say that D is a *support-minimal subcode* if there is no other l-dimensional subcode $D' \leq C$ such that $\operatorname{supp}(D') \subset \operatorname{supp}(D)$.

The following lemma extends the geometric characterization in the previous section to subcodes:

Lemma 4.1. *Let C be a projective $[n,k]_q$ code and $\mathcal{P}$ be the corresponding set of points in $PG(\mathbb{F}_q^k)$. Let D be an l-dimensional subcode of C and consider the associated subspace W_D in $PG(\mathbb{F}_q^k)$ of co-dimension l. Then $supp(D)$ is minimal if and only if $\langle \mathcal{P} \cap W_D \rangle = W_D$. Equivalently,* $\dim(\langle \mathcal{P} \cap W_D \rangle) = k - l$.

If D is a support-minimal subcode with $\dim(D) = l$ then $d_l \leq \operatorname{wt}(D) \leq n - k - l$, where d_l is the l-th generalized Hamming weight of C. Minimal subcode supports were studied as circuits of certain matroids in [10]. It was shown that the set of minimal subcode supports determines the multiset of subcode supports. For $1 \leq l' \leq l \leq k$, the set of minimal l'-dimensional subcode supports also determines the set of minimal l-dimensional subcode supports.

Example 4.1. *We look at some codes and their support-minimal subcodes.*

1. *Simplex codes. Let C be the k-th order q-ary Simplex code which has parameters $[(q^k-1)/(q-1), k, q^{k-1}]$. The columns of the generator matrix for C form a set of non-zero representatives of the 1-dimensional subspaces of $\mathbb{F}_q^k$. This means that the point set associated with C is $PG(\mathbb{F}_q^k)$. By Lemma 4.1, for a given $1 \leq l \leq k$, all the l-dimensional subcodes of C are support-minimal and have the same weight.*

2. *l-MDS codes. Let C be an l-MDS code, i.e. $d_l = n - k + l$. It follows that among the l-dimensional subcodes of C, the only support-minimal subcodes are those with weight equal to d_l. For an l-MDS code, we have $d'_l = n - k + l'$ for $l' \geq l$. Hence, among the l'-dimensional subcodes of C, the only support-minimal subcodes are those with weight equal to d'_l. In particular, if C is an MDS code then we can completely determine all the support-minimal subcodes for $1 \leq l \leq k$.*

For $1 \leq l \leq k$, we define $M^l(C)$ to be the number of support-minimal l-dimensional subcodes of C. When $l = 1$ we get $M^1(C) = (q-1)M(C)$. An upper bound for $M^l(C)$ is given by $M^l(C) \leq \begin{bmatrix} k \\ l \end{bmatrix}_q$ where

$$\begin{bmatrix} k \\ l \end{bmatrix}_q = \frac{(q^k - 1)(q^{k-1} - 1)\cdots(q^{k-l+1} - 1)}{(q^l - 1)(q^{l-1} - 1)\cdots(q-1)}$$

is the Gaussian binomial coefficient that gives the number of subspaces in $PG(\mathbb{F}_q^k)$ of co-dimension l.

From Lemma 4.1, a subcode D is not support-minimal if there exists a subspace $U_D \leq W_D$ of co-dimension $l+1$ such that $\langle \mathcal{P} \cap W_D \rangle \leq U_D$. For $1 \leq l \leq k$ and $1 \leq r \leq \begin{bmatrix} k \\ l \end{bmatrix}_q$, we define $\alpha_q^l(k, r)$ to be the minimum cardinality of a point set $\mathcal{S} \subseteq PG(\mathbb{F}_q^k)$ such that there exist r distinct subspaces $W_1, \ldots, W_r$ of co-dimension l and r subspaces $U_1, \ldots, U_r$ of co-dimension $l+1$ with $U_i \leq W_i$ and $\cup_{i=1}^r (W_i \backslash U_i) \subseteq \mathcal{S}$. The next proposition extends Proposition 3.2 to subcodes.

Proposition 4.2. *Let C be a projective $[n, k]_q$ code and consider integers l, r such that $1 \leq l \leq k$ and $1 \leq r \leq \begin{bmatrix} k \\ l \end{bmatrix}_q$. If $n > \begin{bmatrix} k \\ l \end{bmatrix}_q - \alpha_q^l(k, r)$ then $M^l(C) > \begin{bmatrix} k \\ l \end{bmatrix}_q - r$.*

Proof. The proof is similar to 3.2. □

5 Concluding remarks

We considered the minimum number of minimal codewords of linear codes given the length and dimension. A new lower bound is obtained on the number of minimal codewords of a linear code. We presented a formula for the minimum number of minimal codewords and the determined the exact value of the minimum in many cases that were not known before. We also completely updated the table of exact values presented in [3] and studied subcodes with minimal supports. An open problem is to determine the unknown values of $\alpha_q(r, k)$ for $r \geq 3$. Another interesting topic of research is to try to apply the techniques used in this paper to the problem of finding the maximum number of minimal codewords.

Acknowledgments

Romar dela Cruz gratefully acknowledges the support of the Alexander von Humboldt Foundation through the Georg Forster Research Fellowship and the Mathematisches Institut, University of Bayreuth.

References

[1] E. Agrell. Voronoi Regions for Binary Linear Block Codes. *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 310-316, 1998.

[2] E. Agrell. On the Voronoi neighbor ratio for binary linear codes. *IEEE Transactions on Information Theory*, vol. 44, no. 7, pp. 3064-3072, 1998.

[3] A. Alahmadi, R.E.L. Aldred, R. dela Cruz, S. Ok, P. Solé and C. Thomassen. The minimum number of minimal codewords in an $[n, k]$-code. *Discrete Applied Mathematics*, vol. 184, pp. 32-39, 2015.

[4] A. Alahmadi, R.E.L. Aldred, R. dela Cruz, P. Solé and C. Thomassen. The maximum number of minimal codewords in an $[n, k]$-code. *Discrete Mathematics*, vol. 313, issue 15, pp. 1569-1574, 2013.

[5] A. Alahmadi, R.E.L. Aldred, R. dela Cruz, P. Solé and C. Thomassen. The maximum number of minimal codewords in long codes. *Discrete Applied Mathematics*, vol. 161, issue 3, pp. 424-429, 2013.

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

[7] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 2010-2017, 1998.

[8] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *Journal of Algebraic Combinatorics*, 2020.

[9] Y. Borissov and N. Manev. Minimal codewords in linear codes. *Serdica Mathematical Journal*, vol. 30, pp. 303-324, 2004.

[10] T. Britz. Higher support matroids. *Discrete Mathematics*, vol. 307, issue 1718, pp. 2300-2308, 2007.

[11] H. Chabanne, G. Cohen and A. Patey. Towards Secure Two-Party Computation from the Wire-Tap Channel. In *Proc. Information Security and Cryptology ICISC 2013*, LNCS, vol. 8565, pp. 34-46.

[12] C. Ding, D. Kohel and S. Ling. Secret-sharing with a class of ternary codes. *Theoretical Computer Science*, vol. 246, issues 1-2, pp. 285-298, 2000.

[13] C. Ding and J. Yuan. Covering and secret sharing with linear codes. In *Proc. 4th Int. Conf. on Discrete Mathematics and Theoretical Computer Science*, Dijon, France, pp. 11-25, 2003.

[14] G. Y. Dosa, I. Szalkai and C. Laflamme. The maximum and minimum number of circuits and bases of matroids. *Pure Mathematics and Applications*, vol. 15, no. 4, pp. 383-392, 2004.

[15] R. Entringer and P. Slater. On the maximum number of cycles in a graph. *Ars Combinatoria*, vol. 11, pp. 289-294, 1981.

[16] J. W. P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory and finite projective spaces. *Journal of Statistical Planning and Inference*, vol. 72, pp. 355-380, 1998.

[17] T.-Y. Hwang. Decoding linear block codes for minimizing word error rate. *IEEE Transactions on Information Theory*, vol. IT-25, pp. 733-737, 1979.

[18] R. Jurrius. Weight enumeration of codes from finite spaces. *Designs, Codes and Cryptography*, vol. 63, issue 3, pp. 321-330, 2012.

[19] N. Kashyap. On the convex geometry of binary linear codes. preprint. http://ita.ucsd.edu/workshop/06/papers/82.pdf.

[20] S. Kurz. LinCode - computer classification of linear codes. arXiv preprint 1912.09357, 2019.

[21] W. Lu X. Wu and X. Cao. The Parameters of Minimal Linear Codes. arXiv preprint 1911.07648, 2019.

[22] J. L. Massey. Minimal codewords and secret sharing. In *Proc. 6th Joint Swedish-Russian Workshop on Information Theory*, Molle, Sweden, pp. 276-279, 1993.

[23] J. Schillewaert, L. Storme and J. A. Thas. Minimal codewords in Reed-Muller codes. *Designs, Codes and Cryptography*, vol. 54, issue 3, pp. 273-286, 2010.

[24] C. Tang, Y. Qiu, Q. Liao, and Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. arXiv preprint 1911.09867, 2019.

[25] M. Tsfasman and S. Vladut. Geometric approach to higher weights. *IEEE Transactions on Information Theory*, vol. 41, issue 6, pp. 1564-1588, 1995.

[26] V. Wei. Generalized Hamming weights for linear codes. *IEEE Transactions on Information Theory*, vol. 37, issue 5, pp. 1412-1418, 1991.

[27] K. Yasunaga and T. Fujiwara. Determination of the Local Weight Distribution of Binary Linear Block Codes. *IEEE Transactions on Information Theory*, vol. 52, issue 10, pp. 4444-4454, 2006.