On the maximum number of minimal codewords

Romar dela Cruz[1] and Sascha Kurz[2]

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

Abstract

Minimal codewords have applications in decoding linear codes and in cryptography. We study the maximum number of minimal codewords in binary linear codes of a given length and dimension. Improved lower and upper bounds on the maximum number are presented. We determine the exact values for the case of linear codes of dimension k and length $k+2$ and for small values of the length and dimension. We also give a formula for the number of minimal codewords of linear codes of dimension k and length $k+3$.

1 Introduction

The minimal codewords of a linear code are those whose supports, i.e., the set of nonzero coordinates, do not properly contain the supports of other nonzero codewords. They are equivalent to circuits in matroids and cycles in graphs. In coding theory, minimal codewords were first used in decoding algorithms [1, 2, 7, 15]. They have also found applications in cryptography: in secret sharing schemes [19] and in secure two-party computation [9].

The set of minimal codewords is only known for a few classes of codes (see [1, 6, 7, 8, 11, 12, 18, 20, 21, 22]) and, in general, it is a very hard problem to determine this set. In this work, we consider the following question: what is the maximum number of minimal codewords of linear codes of a given length and dimension? This problem is already studied in the case of cycles in graphs [14]. In the matroid setting, the maximum number of circuits was first addressed in [13]. The study of the maximum and minimum number of minimal codewords of linear codes was initiated in [3, 4, 5, 10].

The results in this paper are described as follows. We determine the maximum number of minimal codewords for binary linear codes of dimension k and length $k+2$. We also give a formula for the number of minimal codewords for the case of dimension k and length $k+3$. A general construction of linear codes with a relatively large number of minimal codewords is also presented. This gives a lower bound that is asymptotically close to the matroid upper bound. An upper bound that is better than the matroid upper bound is also derived. The key idea is to use the systematic generator matrix for a linear code and analyze the properties of the subsets of rows that produce minimal codewords. We also compute the exact values of the for maximum number of minimal codewords small values of length and dimension (completing the table in [4]).

2 Preliminaries

Let q be a power of a prime p and $\mathbb{F}_q$ be the finite field of order q. An $[n,k]_q$ linear code C is a k-dimensional subspace of $\mathbb{F}_q^n$. Given a vector $x \in \mathbb{F}_q^n$, the support of x is defined as $\operatorname{supp}(x) =$

$\{i : x_i \neq 0, 1 \leq i \leq n\}$. A $k \times n$ matrix G whose rows form a basis for C is called a generator matrix. If $G = [I_k|A]$, where I_k is the $k \times k$ identity matrix, then we say that G is systematic or in standard form.

A nonzero codeword $c \in C$ is minimal if there does not exist a nonzero codeword c' such that $\mathrm{supp}(c') \subset\neq \mathrm{supp}(c)$. Otherwise (including the case $c = \mathbf{0}$), we call the codeword c non-minimal. General properties of minimal codewords can be found in [7]. Note that a codeword and its nonzero scalar multiples have the same support. We say that two codewords are equivalent if one is a scalar multiple of the other. We use the notation $M(C)$ for the number of non-equivalent minimal codewords of C. Let $M_q(n, k)$ be the maximum of $M(C)$ for all $[n, k]_q$ codes C. Since C has $q^k - 1$ nonzero codewords, we have

$$M_q(n, k) \leq \frac{q^k - 1}{q - 1}.$$

Bounds for $M_q(n, k)$ and some exact values can be found in [2, 4, 7, 5, 10, 13]. In the setting of matroids, it was shown in [13], that

$$M_q(n, k) \leq \binom{n}{k - 1}. \tag{1}$$

This is bound is also called the matroid upper bound. Alternative proofs were given in [5]. Inequality (1) is satisfied with equality for MDS codes. Another upper bound was derived by Agrell in [2] for binary codes with high rate: for $\frac{k-1}{n} > \frac{1}{2}$, we have

$$M_2(n, k) \leq \frac{2^k}{4n\left(\dfrac{k-1}{n} - \dfrac{1}{2}\right)}.$$

Based on random coding, the lower bound

$$M_q(n, k) \geq \sum_{j=0}^{n-k+1} \binom{n}{j} \frac{(q-1)^j}{q^{n-k}} \prod_{i=0}^{j-2} \left[1 - q^{-(n-k-i)}\right]$$

was given in [7].

It is clear that we have $M_q(n, 1) = 1$ and $M_q(k, k) = k$ for all $k \geq 1$. In [4], it was shown that $M_2(k + 1, k) = \binom{k+1}{2}$ for $k \geq 2$. For small values of k and n, the authors in [4] presented some exact values and bounds on $M_2(n, k)$. In addition, exact values for the case of cycle codes were obtained.

3 Relations between minimal codewords and the rows of a systematic generator matrix

Let C be a linear $[k + t, k]_2$, i.e. binary, code with systematic generator matrix G. By g^i we denote the ith row of G, where $1 \leq i \leq k$. For each subset $S \subseteq \{1, \ldots, k\}$ let c^S denote the sum of the rows of G with indices in S, i.e., $c^S = \sum_{i \in S} g^i \in C$. For each codeword $c \in C$ let $c_S \in \mathbb{F}_2^k$ denote the systematic part of c, i.e., the restriction of c to the first k coordinates $c_1, \ldots, c_k$. Similarly, for each codeword $c \in C$ let $c_I \in \mathbb{F}_2^t$ denote the information bits, i.e., the restriction of c to the last t coordinates $c_{k+1}, \ldots, c_{k+t}$. Some of the subsequent observations can also be found in [18].

Lemma 3.1. *Let $\emptyset \neq S \subseteq \{1, \ldots, k\}$. If there exists a subset $\emptyset \neq T \subsetneq S$ with $c_I^T = \mathbf{0}$, then c^S is non-minimal.*

Proof. Since $\operatorname{supp}\left(c_I^{S\setminus T}\right) = \operatorname{supp}\left(c_I^S\right)$ and $\operatorname{supp}\left(c_S^{S\setminus T}\right) \subsetneq \operatorname{supp}\left(c_S^S\right)$, we have $\operatorname{supp}\left(c^{S\setminus T}\right) \subsetneq \operatorname{supp}\left(c^S\right)$. □

Lemma 3.2. *Let $\emptyset \neq S \subseteq \{1, \ldots, k\}$. The codeword c^S is non-minimal iff there exists a subset $\emptyset \neq T \subsetneq S$ with* $\operatorname{supp}(c_I^T) \subseteq \operatorname{supp}(c_I^S)$.

Proof. Since $S \neq \emptyset$ we have $c^S \neq \mathbf{0}$. Thus, if c^S is non-minimal, there exists a subset $\emptyset \neq T \subsetneq S$ with $\operatorname{supp}(c^T) \subsetneq \operatorname{supp}(c^S)$, so that $\operatorname{supp}(c_I^T) \subseteq \operatorname{supp}(c_I^S)$. For the other direction let $\emptyset \neq T \subsetneq S$ with $\operatorname{supp}(c_I^T) \subseteq \operatorname{supp}(c_I^S)$. If $\operatorname{supp}(c_I^T) \neq \operatorname{supp}(c_I^S)$, then $\operatorname{supp}(c_I^T) \subsetneq \operatorname{supp}(c^S)$ implies $\operatorname{supp}(c^T) \subsetneq \operatorname{supp}(c_I^S)$ so that c^S is non-minimal by definition. If $\operatorname{supp}(c_I^T) = \operatorname{supp}(c_I^S)$, then $c_I^{S\setminus T} = \mathbf{0}$ and we can apply Lemma 3.1. □

Corollary 3.3. *Let c^S be a minimal codeword. Then, we have $1 \leq \#S \leq t+1$. Moreover, if $\#S = t+1$, then $c_I^S = \mathbf{0}$.*

Proof. The largest cardinality of a set of linearly independent vectors in $\mathbb{F}_2^t$ is t. Thus, if $\#S \geq t+1$, then there exists a subset $T \subseteq S$ with $c_I^T = \mathbf{0}$ and $\#T \leq t+1$. We finally apply Lemma 3.1 to conclude $\#S \leq t+1$. □

As a direct consequence we conclude

$$M_2(k+t, k) \leq \sum_{i=1}^{t+1} \binom{k+t}{i},$$

which asymptotically tends to $\binom{k+t}{t+1}$ for a fixed value of t (if k tends to infinity). In Proposition 4.3 we will present a strict improvement over the matroid upper bound $\binom{n}{k-1} = \binom{k+t}{t+1}$, see (1), provided that k is large enough.

Lemma 3.4. *Let $\emptyset \neq S \subseteq \{1, \ldots, k\}$ be a subset such that $c_I^S = \mathbf{0}$. Then, c^S is minimal iff $c_I^T \neq \mathbf{0}$ for all $\emptyset \neq T \subsetneq S$.*

Proof. Since $S \neq \emptyset$ we have $c^S \neq \mathbf{0}$. If c^S is non-minimal, then there exists a subset $\emptyset \neq T \subsetneq S$ with $\operatorname{supp}(c^T) \subsetneq \operatorname{supp}(c^S)$. Since $c_I^S = \mathbf{0}$ this implies $c_I^T = \mathbf{0}$. For the other direction we apply Lemma 3.1. □

Lemma 3.5. *Let G be a systematic generator matrix of an $[k+t, k]_2$ code C and $1 \leq i \leq k$ be an index with $g_I^i = \mathbf{0}$. By G' we denote the matrix that arises from G by removing the ith row g^i and by G'' the matrix if we additionally remove the ith column. Let C' and C'' be the linear codes generated by G' and G'', respectively. Then C' is $[k+t, k-1]_2$ code, C'' a $[k+t-1, k-1]_2$ codes, and we have $M(C) = M(C') + 1 = M(C'') + 1$.*

Proof. The stated lengths and the dimensions of the codes C' and C'' directly follow from their construction. Since removing a zero column in a generator matrix does not change the number of minimal codewords, we have $M(C') = M(C'')$, so that it remains to show $M(C) = M(C') + 1$. The codeword g^i itself is minimal in C and not contained in C'. For any subset $\{i\} \subsetneq S \subseteq \{1, \ldots, k\}$

the codeword c^S is non-minimal due to Lemma 3.1 (choosing $T = \{i\}$). It remains to show that for subsets $\emptyset \neq S \subseteq \{1, \ldots, k\} \backslash \{i\}$ the codeword $c^S \in C' \le C$ is minimal in C' iff it is minimal in C. Since C' is a subcode of C we only need to consider the case where c^S is non-minimal in C. Then, there exists a subset $\emptyset \neq T \subsetneq S$ with $\operatorname{supp}(c^T) \subsetneq \operatorname{supp}(c^S)$. Since $g_I^i = \mathbf{0}$ we can assume $i \notin T$, so that $c^T \in C'$ and c^S is also non-minimal in C'. □

So, in the following we may assume $c_I^S \neq \mathbf{0}$ whenever needed and we mention the implication $M_2(k, k) = k$ for all $k \geq 1$.

Definition 3.1. *Let C and especially t be given. By $\mathcal{T}$ we denote the set of the 2^t elements of $\mathbb{F}_2^t$. For each $\tau \in \mathcal{T}$ we set $a_\tau = \#\left\{1 \le i \le k \,:\, r_I^i = \tau\right\}$. The counting vector of all a_τ is denoted by $\mathbf{a}$. More precisely, we write $a_\tau(C)$ and $\mathbf{a}(C)$ whenever the code C is not clear from the context.*

Since column and row permutations of a generator matrix do not change the number of minimal codewords, we have:

Lemma 3.6. *Let C and C' be two $[k+t, k]_2$ codes. If $\mathbf{a}(C) = \mathbf{a}(C')$, then $M(C) = M(C')$.*

For the case $t = 1$ we can easily determine $M(C)$ given the vector $\mathbf{a}(C) = (a_0, a_1)$.

Lemma 3.7. *Let C be a $[k+1, k]_2$ code. Then, $M(C) = k + \binom{a_1}{2}$.*

Proof. For all subsets $S \subseteq \{1, \ldots, k\}$ of cardinality 1, the codeword c^S is minimal, which give k minimal codewords. Due to Corollary 3.3 is suffices to consider codewords of the form c^S with $\emptyset \subseteq S \subseteq \{1, \ldots, k\}$ and $\#S \le 2$, so that it remains to consider the cases with $\#S = 2$. Due to Lemma 3.1, Corollary 3.3, and Lemma 3.4 the codeword $c^{\{i,j\}}$ is minimal iff $i \neq j$ and $g_I^i = g_I^j = 1$. □

Corollary 3.8. *$M_2(k+1, k) = \binom{k+1}{2} = (k+1)k/2$.*

The same result was also obtained in [4]. Not that the matroid upper bound $M_2(n, k) \le \binom{n}{k-1} = \binom{k+t}{k-1} = \binom{k+t}{t+1}$, see (1), is matched with equality. We remark that the unique code attaining this upper bound is the so-called projective base (of $\mathbb{F}_2^k$) given by a generator matrix consisting of the k unit vectors and the all-1-vector as columns.

In Lemma 3.4 we have characterized whether c^S is minimal for the special case when $c_I^S = \mathbf{0}$ using the information bits of g^i, where $i \in S$, only. This can be generalized and formalized as follows.

Definition 3.2. *Let C be a $[k+t, k]_2$ code and $\emptyset \neq S \subseteq \{1, \ldots, k\}$ a subset. With this, we set*

$$\overline{C^S} := \left\langle \{g_I^i \,:\, i \in S\} \right\rangle .$$

We call $\overline{C^S}$ the reduced code of C with respect to S.

Lemma 3.9. *Let C be a $[k+t, k]_2$ code and $\emptyset \neq S \subseteq \{1, \ldots, k\}$ a subset. The codeword c^S is minimal in C iff c_I^S is either minimal in $\overline{C^S}$ or $c_I^S = \mathbf{0}$ and $c_I^T \neq \mathbf{0}$ for all $\emptyset \neq T \subsetneq S$.*

Proof. Assume that c^S is non-minimal. Since $S \neq \emptyset$ we have $c^S \neq \mathbf{0}$, so that there exists a subset $\emptyset \neq T \subsetneq S$ with $\operatorname{supp}\left(c^T\right) \subsetneq \operatorname{supp}\left(c^S\right)$. Thus, we have $\operatorname{supp}\left(c_I^T\right) \subseteq \operatorname{supp}\left(c_I^S\right)$. If $\operatorname{supp}\left(c_I^T\right) \neq \operatorname{supp}\left(c_I^S\right)$, then $\operatorname{supp}\left(c_I^T\right) \subsetneq \operatorname{supp}\left(c_I^S\right)$ and c_I^S is non-minimal in $\overline{C^S}$. If $\operatorname{supp}\left(c_I^T\right) = \operatorname{supp}\left(c_I^S\right)$, then $c_I^{S \backslash T} = \mathbf{0}$. So, either $c_I^S \neq \mathbf{0}$ and $\mathbf{0} = c_I^{S \backslash T} \subsetneq c_I^S$ or $c_I^S = \mathbf{0}$ and $c_I^{S \backslash T} = \mathbf{0}$, where $\emptyset \neq S \backslash T \subsetneq S$.

For the other direction we first assume that c_I^S is non-minimal in $\overline{C^S}$ and $c_I^S \neq \mathbf{0}$. Here, there exists a subset $\emptyset \neq T \subsetneq S$ with $\operatorname{supp}\big(c_I^T\big) \subsetneq \operatorname{supp}\big(c_I^S\big)$, which implies $\operatorname{supp}\big(c^T\big) \subsetneq \operatorname{supp}\big(c^S\big)$, i.e., c^S is non-minimal in C. In the other case we assume $c_I^S = \mathbf{0}$ and the existence of a subset $\emptyset \neq T \subsetneq S$ with $c_I^T = \mathbf{0}$. Here we have $\operatorname{supp}\big(c^T\big) \subsetneq \operatorname{supp}\big(c^S\big)$, i.e., c^S is non-minimal. □

Definition 3.3. *We call a subset $\hat{S} \subseteq \mathbb{F}_2^t$ minimal generating if $\sum_{x \in \hat{S}} x$ is minimal in $\langle \hat{S} \rangle$ or $\sum_{x \in \hat{S}} x = \mathbf{0}$ and $\sum_{x \in \hat{T}} x \neq \mathbf{0}$ for all $\emptyset \neq \hat{T} \subsetneq \hat{S}$.*

Note that no minimal generating set of cardinality at least two can contain the zero vector.

Theorem 3.10. *Let C be a linear $[k+t,k]_2$ code and $\mathbf{a}$ its corresponding vector counting the multiplicities of the occurring information vectors. With this, we have*

$$M(C) = k + \sum_{\tau \in \mathbb{F}_2^t \backslash \{\mathbf{0}\}} \binom{a_\tau}{2} + \sum_{\hat{S} \subseteq \mathbb{F}_2^t \,:\, \hat{S} \text{ is minimal generating and } 2 \le \#\hat{S} \le t+1} \; \prod_{\tau \in \hat{S}} a_\tau .$$

Proof. Let c^S be a minimal codeword in C for a subset $S \subseteq \{1,\dots,k\}$. Since $c^S \neq \mathbf{0}$ we have $S \neq \emptyset$. If $\#S = 1$, then c^S is minimal in all cases, which gives k possibilities. If S contains two different elements i and j with $g_I^i = g_I^j$, then we deduce $\#S = 2$ from Lemma 3.1 and Lemma 3.4. Since $i \neq j$ the codeword $c^{\{i,j\}}$ is indeed minimal, iff $g_I^i = g_I^j \neq \mathbf{0}$, which yields $\sum_{\tau \in \mathbb{F}_2^t \backslash \{\mathbf{0}\}} \binom{a_\tau}{2}$ further possibilities. In the remaining cases we have $2 \le \#S \le t+1$, see Corollary 3.3 for the upper bound, and $g_I^i \neq g_I^j$ for all different $i,j \in S$. In other words $\hat{S} := \big\{g_I^i \,:\, i \in S\big\}$ has cardinality $\#S$. Due to Lemma 3.9 and Definition 3.3 c^S is minimal iff $\hat{S}$ is minimal generating. Given $\hat{S}$, the number of choices for S are $\prod_{\tau \in \hat{S}} a_\tau$. □

In some cases it is possible to concretely describe the minimal generating sets in the formula of Theorem 3.10:

Proposition 3.11. *Let C be a linear $[k+t,k]_2$ code and $\mathbf{a}$ its corresponding vector counting the multiplicities of the occurring information vectors. If $a_\tau > 0$ implies $\tau \in \mathcal{T} := \{e_1,\dots,e_t,\mathbf{1}\}$, where $\mathbf{1} = e_1 + \dots + e_t$, then we have*

$$M(C) = k + \sum_{\tau \in \mathcal{T}} \binom{a_\tau}{2} + \sum_{\mathbf{1} \subsetneq \hat{S} \subseteq \mathcal{T}} \prod_{\tau \in \hat{S}} a_\tau .$$

Proof. Due to Theorem 3.10 it suffices to check which subsets of $\mathcal{T}$ are minimal generating. If $\mathbf{1} \notin \hat{S}$, then $\sum_{x \in \hat{S}} x$ is clearly not minimal within $\hat{S}$. In all other cases $\hat{S}$ is minimal generating, which easily follows from Lemma 3.9. □

As an example let $k \ge 2t$ be integers and A be the $k \times t$ matrix whose rows consist of 2 copies each of the unit vectors $e_1,\dots,e_t$ and $k-2t$ copies of the zero vector. Consider the $[k+t,k]$ linear code C with generator matrix $G = [I_k \,|\, A]$. Note that C is projective and

$$M(C) = k + \sum_{\tau \in \{e_1,\dots,e_t\}} \binom{a_\tau}{2} = k + t.$$

In [16, Lemma 5.1] it is shown that each projective $[k+t,k]_2$ code C satisfies $M(C) \ge k+t$.

4 Bounds for the maximum number of minimal codewords

A projective base can also be used to construct linear $[k+t,k]_2$ codes with a relatively large number of minimal codewords. To this end, let e_i denote the ith unit vector and $\mathbf{1}$ denote the all-1-vector (in $\mathbb{F}_2^t$).

Proposition 4.1.

$$M_2(k+t,k) \ge \left\lfloor \frac{k}{t+1} \right\rfloor^{t+1}$$

Proof. W.l.o.g. we assume $k \ge t+1$. Let C be a linear $[k+t,k]_2$ code with systematic generator matrix G such that $a_\tau(C) = 0$ if $\tau \notin \{e_1,\dots,e_t,\mathbf{1}\}$ and $a_\tau \ge \left\lfloor \frac{k}{t+1} \right\rfloor$ if $\tau \in \{e_1,\dots,e_t,\mathbf{1}\}$ for all $\tau \in \mathbb{F}_2^t$. Since $(t+1)\cdot \left\lfloor \frac{k}{t+1} \right\rfloor \le k$, the construction is possible. Now we consider all subsets $S \subseteq \{1,\dots,k\}$ with cardinality $\#S = t+1$ such that $\#\left\{c_I^i : i \in S\right\} = t+1$, i.e., each possible vector of information bits occurs exactly once. Note that there are

$$a_{e_1} \cdot \ldots a_{e_t} \cdot a_{\mathbf{1}} \ge \left\lfloor \frac{k}{t+1} \right\rfloor^{t+1}$$

choices. Since $\sum_{i=1}^t e_i = \mathbf{1}$ and no proper subset of $\{e_1,\dots,e_t,\mathbf{1}\}$ sums to zero we can apply Lemma 3.4 to deduce that those c^S are minimal codewords. □

The essential property of $\{e_1,\dots,e_t,\mathbf{1}\}$ used in the above proof is that of a projective basis. The explicit choice of vectors is called canonical basis in that context. We remark that it is also possible to precisely determine $M(C)$ if $a_\tau(C) \ne 0$ implies $\tau \in \{e_1,\dots,e_t,\mathbf{1}\}$ and those a_τ are given, see Proposition 3.11. The codes constructed in Proposition 4.1 show that the matroid upper bound $M_2(n,k) \le \binom{n}{k-1} = \binom{k+t}{t+1}$ is, up to a constant, asymptotically tight for every fixed value of t.

Our next aim is to conclude an upper bound for $M_2(k+t,k)$ from Theorem 3.10. To this end, we will utilize an optimization problem[1]:

Lemma 4.2. *Let s, r, and m be positive integers with $s \le r$ and $f\colon \mathbb{R}_{\ge 0}^r \to \mathbb{R}_{\ge 0}$ a function defined by*

$$f(x_1,\dots,x_r) = \sum_{S \subseteq \{1,\dots,r\}\,:\,\#S=s} \prod_{i\in S} x_i.$$

Then, the optimization problem $\max f(x_1,\dots,x_r)$ *subject to the constraint $\sum_{i=1}^r x_i = m$ has the unique optimal solution $x_i = \frac{m}{r}$ for all $1 \le i \le r$ with target value $\binom{r}{s}\cdot\left(\frac{m}{r}\right)^s$. If we additionally require that the x_i have to be integers, then an optimal solution is given by $x_i = \left\lfloor \frac{m+i-1}{r} \right\rfloor$ for $1 \le i \le r$.*

Proof. For $r = 1$ the statements are obvious, so that we assume $r \ge 2$ in the following. Assume that for a given optimal solution of the real-valued optimization problem stated above, there are indices $1 \le i,j \le r$ with $x_i \ne x_j$. From the given vector $\mathbf{x} = (x_1,\dots,x_r)$ we construct a vector $\bar{\mathbf{x}}$

[1] We are pretty sure that this problem has been studied in the literature before. However, since we were not able to find a reference, we give a self-contained proof here.

by replacing the ith and the jth component of $\mathbf{x}$ both by $\frac{x_i+x_j}{2}$. Now we want to compare $f(\mathbf{x})$ and $f(\bar{\mathbf{x}})$. Clearly, we have

$$\sum_{S\subseteq\{1,\dots,r\}\backslash\{i,j\}\,:\,\#S=s}\ \prod_{h\in S}\bar{x}_h=\sum_{S\subseteq\{1,\dots,r\}\backslash\{i,j\}\,:\,\#S=s}\ \prod_{h\in S}x_h.$$

For the cases where the subset S intersects $\{i,j\}$ in exactly one element we compute

$$\begin{aligned}
&\sum_{S\subseteq\{1,\dots,r\}\,:\,\#S=s,\#S\cap\{i,j\}=1}\ \prod_{h\in S}\bar{x}_h\\
=&\sum_{\bar{S}\subseteq\{1,\dots,r\}\backslash\{i,j\}\,:\,\#\bar{S}=s-1}(\bar{x}_i+\bar{x}_j)\cdot\prod_{h\in\bar{S}}\bar{x}_h\\
=&\sum_{\bar{S}\subseteq\{1,\dots,r\}\backslash\{i,j\}\,:\,\#\bar{S}=s-1}(x_i+x_j)\cdot\prod_{h\in\bar{S}}x_h\\
=&\sum_{S\subseteq\{1,\dots,r\}\,:\,\#S=s,\#S\cap\{i,j\}=1}\ \prod_{h\in S}x_h,
\end{aligned}$$

i.e., again there is no difference. If S contains both i and j, then we can write $S=\bar{S}\cup\{i,j\}$ with a subset $\bar{S}\subseteq\{1,\dots,r\}\backslash\{i,j\}$ and compute

$$\begin{aligned}
&\sum_{\bar{S}\in\{1,\dots,r\}\backslash\{i,j\}\,:\,\#\bar{S}=s-2}\bar{x}_i\cdot\bar{x}_j\cdot\prod_{h\in\bar{S}}\bar{x}_h\\
=&\sum_{\bar{S}\in\{1,\dots,r\}\backslash\{i,j\}\,:\,\#\bar{S}=s-2}\left(x_ix_j+\left(\frac{x_i-x_j}{2}\right)^2\right)\cdot\prod_{h\in\bar{S}}x_h\\
\ge&\sum_{\bar{S}\in\{1,\dots,r\}\backslash\{i,j\}\,:\,\#\bar{S}=s-2}x_i\cdot x_j\cdot\prod_{h\in\bar{S}}x_h.
\end{aligned}$$

Thus, we have $f(\bar{\mathbf{x}})\ge f(\mathbf{x})$. Next we remark that we have equality iff $\prod_{h\in\bar{S}}x_h=0$ for all subsets $\bar{S}\in\{1,\dots,r\}\backslash\{i,j\}\,:\,\#\bar{S}=s-2$, i.e., there are most $s-3$ indices $h\in\{1,\dots,r\}\backslash\{i,j\}$ with $x_h\neq 0$, so that $f(\mathbf{x})=0$, which clearly is not an optimal solution. Thus, in an optimal solution $\mathbf{x}$ all entries have to be equal. Since $\sum_{i=1}^r x_i=m$ we obtain $x_i=\frac{m}{r}$ and the stated target value is a direct conclusion.

For the case with integral variables we assume that $\mathbf{x}=(x_1,\dots,x_r)$ is an optimal solution such that there exist indices $1\le i,j\le r$ with $x_i-x_j\ge 2$. Now let $\bar{\mathbf{x}}$ arose from $\mathbf{x}$ by increasing x_j and decreasing x_i by one, respectively. Since $\mathbf{x}\in\mathbb{N}^r$ and $x_i-x_j\ge 2$, also $\bar{\mathbf{x}}\in\mathbb{N}^r$ and $\sum_{h=1}^r\bar{x}_h=\sum_{h=1}^r x_h=m$. Next we will show $f(\bar{\mathbf{x}})\ge f(\mathbf{x})$. To this end, we proceed as before and distinguish the summands in $\sum_{S\subseteq\{1,\dots,r\}\,:\,\#S=s}\prod_{i\in S}x_i$ and $\sum_{S\subseteq\{1,\dots,r\}\,:\,\#S=s}\prod_{i\in S}\bar{x}_i$ according to the cardinality of $S\cap\{i,j\}$. As before, for $\#S\cap\{i,j\}\le 1$ there is no difference if we compare the sum over all respective subsets S. For the cases $\#S\cap\{i,j\}=2$ we can utilize the inequality

$$(x_i-1)\cdot(x_j+1)\cdot z=x_ix_jz+(x_i-x_j-1)\cdot z\ge x_ix_jz$$

for $z\ge 0$ to conclude $f(\bar{\mathbf{x}})\ge f(\mathbf{x})$. Thus, there exists an optimal solution $\mathbf{x}$ with $|x_i-x_j|\le 1$ for all $1\le i,j\le r$. Due to symmetry we can assume $x_1\le\dots\le x_r$ w.l.o.g. Since $\sum_{i=1}^r x_i=m$, we obtain the stated formula $x_i=\left\lfloor\frac{m+i-1}{r}\right\rfloor$ for $1\le i\le r$. □

Proposition 4.3. *Let C be a linear $[k+t,k]_2$ code and* $\mathbf{a}$ *its corresponding vector counting the multiplicities of the occurring information vectors. With this, we have*

$$M(C) \le \frac{(k+1)k}{2} + \sum_{s=2}^{t+1} \binom{2^t-1}{s} \cdot \left(\frac{k}{2^t-1}\right)^s.$$

Proof. We want to apply Theorem 3.10 and remark that we clearly have

$$k + \sum_{\tau \in \mathbb{F}_2^t \backslash \{\mathbf{0}\}} \binom{a_\tau}{2} \le \frac{(k+1)k}{2}.$$

Since no minimal generating set of cardinality at least two contains the zero vector and the a_τ are non-negative, we conclude

$$\sum_{\hat{S} \subseteq \mathbb{F}_2^t \,:\, \hat{S} \text{ is minimal generating and } 2 \le \#\hat{S} \le t+1} \prod_{\tau \in \hat{S}} a_\tau \le \sum_{S \subseteq \mathbb{F}_2^t \backslash \{\mathbf{0}\} \,:\, 2 \le \#S \le t+1} \prod_{\tau \in S} a_\tau. \qquad (2)$$

Since $\sum_{\tau \in \mathbb{F}_2^t} a_\tau = k$ we can assume $a_{\mathbf{0}} = 0$ when maximizing the right-hand side of Inequality (2). Applying Lemma 4.2 onto the right-hand side of Inequality (2), with $s = \#S$, $r = 2^t - 1$, and $m = k$, gives the stated upper bound for $M(C)$. □

We remark that Proposition 4.3 improves upon the matroid upper bound $M_2(k+t,k) \le \binom{k+t}{t+1}$. As an example we state that Proposition 4.3 yields

$$\begin{aligned} M_2(k+2,k) &\le \frac{k^3}{27} + \mathcal{O}\big(k^2\big), \\ M_2(k+3,k) &\le \frac{5k^4}{343} + \mathcal{O}\big(k^3\big), \text{ and} \\ M_2(k+4,k) &\le \frac{1001k^5}{253125} + \mathcal{O}\big(k^4\big), \end{aligned}$$

while $\binom{k+2}{2+1} = \frac{k^3}{6} + \mathcal{O}\big(k^2\big)$, $\binom{k+3}{3+1} = \frac{k^4}{24} + \mathcal{O}\big(k^3\big)$, and $\binom{k+4}{4+1} = \frac{k^5}{120} + \mathcal{O}\big(k^4\big)$. Note however that the fraction between the coefficients of the leading terms tend to 1 as t tends to infinity. In order to obtain tighter bounds we need to study the properties of minimal generating sets.

Lemma 4.4. *For two different elements $a, b \in \mathbb{F}_2^t \backslash \{\mathbf{0}\}$ the set $\{a,b\}$ is minimal generating iff* $\operatorname{supp}(a) \cap \operatorname{supp}(b) \neq \emptyset$.

Proof. Note that we have $a + b \neq \mathbf{0}$. Since $b \neq \mathbf{0}$ the statement follows from the equivalence $\operatorname{supp}(a) \subseteq \operatorname{supp}(a+b)$ iff $\operatorname{supp}(a) \cap \operatorname{supp}(b) \neq \emptyset$. □

As an application of Theorem 3.10 we compute $M(C)$ in dependence of $\mathbf{a}$ for $t = 2$.

Proposition 4.5. *Let C be a linear $[k+2,k]_2$ code and* $\mathbf{a}$ *its corresponding vector counting the multiplicities of the occurring information vectors. With this, we have*

$$\begin{aligned} M(C) &= k + \frac{a_{10} \cdot (a_{10}-1)}{2} + \frac{a_{01} \cdot (a_{01}-1)}{2} + \frac{a_{11} \cdot (a_{11}-1)}{2} \\ &\quad + a_{10} \cdot a_{11} + a_{01} \cdot a_{11} + a_{10} \cdot a_{01} \cdot a_{11} \\ &= k + \frac{(k - a_{00}) \cdot (k - a_{00} - 1)}{2} - a_{10} \cdot a_{01} + a_{10} \cdot a_{01} \cdot a_{11}. \end{aligned}$$

Proof. Due to Lemma 4.4 the set $\{10, 01\}$ is the only subset of $\mathbb{F}_2^2\backslash\{\mathbf{0}\}$ that has cardinality 2 and is not minimal generating. The unique subset $\{01, 10, 11\}$ of $\mathbb{F}_2^2\backslash\{\mathbf{0}\}$ of cardinality 3 is indeed minimal generating. For the second equation note that $k = a_{00} + a_{01} + a_{10} + a_{11}$. □

Maximizing the formula from Proposition 4.5 we obtain:

Proposition 4.6. *We have*

$$M_2(k + 2, k) = k + k(k - 1)/2 + \lfloor (k - 1)/3\rfloor \cdot \lfloor k/3\rfloor \cdot \lfloor (k + 1)/3\rfloor$$

for all $k \ge 1$.

Proof. Let C be a $[k + 2, k]_2$ code. From the latter expression for $M(C)$ in Proposition 4.5 it is obvious that $a_{00} = 0$ and $a_{11} \ge 1$ in the maximum. Thus, it remains to maximize

$$f(a_{01}, a_{10}, a_{11}) = a_{10} \cdot a_{01} \cdot a_{11} - a_{10} \cdot a_{01} = a_{10} \cdot a_{01} \cdot (a_{11} - 1)$$

subject to $a_{01} + a_{10} + a_{11} = k$ and $a_{01}, a_{10}, a_{11} \in \mathbb{N}$. It is well known that f is maximized iff a_{01}, a_{10}, and $a_{11} - 1$ are as equal as possible while satisfying $a_{01} + a_{10} + (a_{11} - 1)$, c.f. Lemma 4.2. Thus, an optimal solution is given by $a_{01} = \left\lfloor \frac{k-1+2}{3} \right\rfloor$, $a_{10} = \left\lfloor \frac{k-1+1}{3} \right\rfloor$, and $a_{11} = \left\lfloor \frac{k-1}{3} \right\rfloor + 1$. Plugging into the formula in Proposition 4.5 gives the stated result. □

Proposition 4.7. *Let C be a linear $[k + 3, k]_2$ code and* **a** *its corresponding vector counting the multiplicities of the occurring information vectors. With this, we have*

$$\begin{aligned}
M(C) \quad = \quad & k + \sum_{\tau\in\mathbb{F}_2^3\backslash\{\mathbf{0}\}} \frac{a_\tau \cdot (a_\tau - 1)}{2} + a_{110} \cdot (a_{101} + a_{011} + a_{111}) + a_{101} \cdot (a_{011} + a_{111}) + a_{011} \cdot a_{111} \\
& + a_{100} \cdot (a_{110} + a_{101} + a_{111}) + a_{010} \cdot (a_{110} + a_{011} + a_{111}) + a_{001} \cdot (a_{011} + a_{101} + a_{111}) \\
& + a_{100}a_{010}a_{110} + a_{100}a_{001}a_{101} + a_{010}a_{001}a_{011} + a_{100}a_{010}a_{111} + a_{100}a_{001}a_{111} \\
& + a_{010}a_{001}a_{111} + a_{100}a_{110}a_{011} + a_{100}a_{011}a_{101} + a_{010}a_{110}a_{101} + a_{010}a_{101}a_{011} \\
& + a_{001}a_{110}a_{101} + a_{001}a_{110}a_{011} + a_{100}a_{011}a_{111} + a_{010}a_{101}a_{111} + a_{001}a_{110}a_{111} \\
& + a_{110}a_{101}a_{011} + a_{110}a_{101}a_{111} + a_{110}a_{011}a_{111} + a_{011}a_{101}a_{111} \\
& + a_{100}a_{010}a_{001}a_{111} + a_{100}a_{011}a_{110}a_{001} + a_{100}a_{101}a_{011}a_{010} + a_{100}a_{101}a_{110}a_{111} \\
& + a_{010}a_{110}a_{101}a_{001} + a_{010}a_{110}a_{011}a_{111} + a_{001}a_{011}a_{101}a_{111}
\end{aligned}$$

Proof. We apply Theorem 3.10. From the $\binom{7}{2} = 21$ 2-subsets of $\mathbb{F}_2^3\backslash\{\mathbf{0}\}$ only the six subsets

$$\{100, 010\}, \{100, 001\}, \{010, 001\}, \{100, 011\}, \{010, 101\}, \{001, 110\}$$

violate the condition from Lemma 4.4. The 15 other combinations are listed in the first two rows of the stated formula. It is a bit cumbersome to check by hand, but out of the $\binom{7}{3} = 35$ 3-subsets of $\mathbb{F}_2^3\backslash\{\mathbf{0}\}$ just those 19 listed in the rows three to six of the stated formula satisfy the criterion of Lemma 3.9. The sum over the 7 projective bases of $\mathbb{F}_2^3$ can be stated as

$$\sum_{\tau_3\in\mathbb{F}_2^3\backslash\{\mathbf{0},\tau_1,\tau_2,\tau_1+\tau_2\}} a_{\tau_1}a_{\tau_2}a_{\tau_3}a_{\tau_1+\tau_2+\tau_3},$$

see the subsequent Proposition 4.9, and also be spelled out as done in the last two rows of the formula in the statement of the proposition. □

The exact maximization of the formula of Proposition 4.7 might be a technical challenge, while it is easy to come up with a conjecture for large enough values of k:

Conjecture 4.8. *For $k \geq 4$ the exact value of $M_2(k+3,k)$ is given by the formula of Proposition 4.7 with $\mathbf{a} = (a_{000}, a_{100}, a_{010}, a_{001}, a_{110}, a_{101}, a_{011}, a_{111})$, where*

$$\mathbf{a} = \begin{cases} (l,l,l,l+1,l+1,l+1,l+1) & : \quad k = 4+7l, \\ (l,l,l,l+1,l+1,l+1,l+2) & : \quad k = 5+7l, \\ (l,l,l,l+1,l+1,l+2,l+2) & : \quad k = 6+7l, \\ (l,l,l,l+1,l+2,l+2,l+2) & : \quad k = 7+7l, \\ (l+1,l,l,l+2,l+2,l+1,l+2) & : \quad k = 8+7l, \\ (l+1,l,l,l+2,l+2,l+2,l+2) & : \quad k = 9+7l, \\ (l+1,l+1,l,l+2,l+2,l+2,l+2) & : \quad k = 10+7l \end{cases}$$

if $k \leq 26$ or

$$a_{000} = a_{001} = a_{110} = a_{111} = 0, a_{100} = \left\lfloor \frac{k}{4} \right\rfloor, a_{010} = \left\lfloor \frac{k+1}{4} \right\rfloor, a_{101} = \left\lfloor \frac{k+2}{4} \right\rfloor, \text{ and } a_{011} = \left\lfloor \frac{k+3}{4} \right\rfloor$$

if $k \not\equiv 0 \pmod 4$ and $k \geq 27$ or

$$a_{000} = a_{001} = a_{110} = a_{111} = 0, a_{100} = \frac{k}{4}, a_{010} = \frac{k}{4} - 1, a_{101} = \frac{k}{4} + 1, \text{ and } a_{011} = \frac{k}{4}$$

if $k \equiv 0 \pmod 4$ and $k \geq 27$.

We have computationally checked Conjecture 4.8 for all $k \leq 150$. For the leading term of $M_2(k+3,k)$, in terms of k, the situation is different to the one of Lemma 4.2, i.e., choosing $a_{000} = 0$ and $a_\tau = \frac{k}{7}$ for $\tau \in \mathbb{F}_2^3 \backslash \{\mathbf{0}\}$ just gives $M_2(k+3,k) \geq \frac{k^4}{343} + \mathcal{O}(k^3)$, while $a_{000} = a_{110} = a_{101} = a_{011} = 0$ and $a_{100} = a_{010} = a_{001} = a_{111} = \frac{k}{4}$ gives $M_2(k+3,k) \geq \frac{k^4}{256} + \mathcal{O}(k^3)$ (ignoring the rounding to integers, whose effect is in $\mathcal{O}(k^3)$). Conjecture 4.8 of course implies $M_2(k+3,k) = \frac{k^4}{256} + \mathcal{O}(k^3)$.

Next we focus on the leading term:

Proposition 4.9. *Let C be a linear $[k+t,k]_2$ code and $\mathbf{a}$ its corresponding vector counting the multiplicities of the occurring information vectors. If $t \geq 2$, then*

$$M(C) = \mathcal{O}(k^t) + \frac{1}{(t+1)!} \cdot \sum_{\tau_1 \in \mathcal{T}_1} \sum_{\tau_2 \in \mathcal{T}_2} \cdots \sum_{\tau_t \in \mathcal{T}_t} \left(\prod_{i=1}^{t} a_{\tau_i} \right) \cdot a_{\left(\sum_{i=1}^t \tau_i\right)},$$

where $\mathcal{T}_i = \mathbb{F}_2^t \backslash \langle \{\tau_j \,:\, 1 \leq j < i\} \rangle$ for $1 \leq i \leq t$.

Proof. We apply Theorem 3.10. If $t \geq 2$ then only the contributions of the minimal generating sets $\hat{S}$ of cardinality exactly $t+1$ are not covered by the $\mathcal{O}(k^t)$ term. Due to Corollary 3.3 we have $\sum_{x \in \hat{S}} x = \mathbf{0}$ in those remaining cases. By Lemma 3.4 we have to guarantee that no proper subset $\emptyset \neq \hat{T} \subsetneq \hat{S}$ satisfies $\sum_{x \in \hat{T}} x = \mathbf{0}$. Since there are $(t+1)!$ possible orders of the elements of $\hat{S}$ we obtain the stated summation formula (which mimics the construction or counting of projective bases of $\mathbb{F}_2^t$). □

We remark that the minimal generating sets of $\mathbb{F}_2^t$ of the maximum cardinality $t+1$ have a lot of equivalent descriptions. As mentioned before, they correspond to the projective bases of $\mathbb{F}_2^t$. Due to Corollary 3.3 and Lemma 3.4 they also correspond to minimal dual codewords (of the t-dimensional simplex code).

Conjecture 4.10. *Let $t \geq 2$ be an integer and $\mathcal{P} = \{e_1, \ldots, e_t, \mathbf{1}\}$. Then, the function*

$$\frac{1}{(t+1)!} \cdot \sum_{\tau_1 \in \mathcal{T}_1} \sum_{\tau_2 \in \mathcal{T}_2} \cdots \sum_{\tau_t \in \mathcal{T}_t} \left(\prod_{i=1}^{t} a_{\tau_i} \right) \cdot a_{\left(\sum_{i=1}^{t} \tau_i\right)},$$

where $\mathcal{T}_i = \mathbb{F}_2^t \backslash \langle \{\tau_j : 1 \leq j < i\} \rangle$ for $1 \leq i \leq t$, attains its maximum on $\mathbb{R}_{\geq 0}^{2^t - 1}$ subject to the constraint $\sum_{\tau \in \mathbb{F}_2^t \backslash \{\mathbf{0}\}} a_\tau = k$ at $a_\tau = \frac{k}{t+1}$ for all $\tau \in \mathcal{P}$ and $a_\tau = 0$ otherwise. If additionally $a_\tau \in \mathbb{N}$ is assumed, then the maximum is attained at the points where $|a_\tau - a_{\tau'}| \leq 1$ for all $\tau, \tau' \in \mathcal{P}$ and $a_\tau = 0$ otherwise.

A direct implication of this conjecture is $M_2(k+t, k) = \left(\frac{k}{t+1}\right)^{t+1} + \mathcal{O}\left(k^t\right)$. For $t = 2$ or $t = 3$, $k \leq 100$ Conjecture 4.10 is indeed true.

5 Exact values for small parameters

The aim of this subsection is to determine the exact value of $M_2(n, k)$ for cases with $1 \leq k \leq n \leq 15$. 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 $M(C') = M(C) - 1$. (In general we have $M(C) = M(C_1) + M(C_2)$ whenever $C = C_1 \oplus C_2$, i.e., it is sufficient to consider indecomposable codes.) Removing zero or duplicate columns from the generator matrix of a binary code (scalar multiples for $q > 2$) does not change the number of minimal codewords of the corresponding codes. 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 enumeration algorithm from [17], see Table 1 for the numerical results. In most cases we have verified the lower bounds from [4] to be exact and only improved the upper bounds. However, for $n = 15$ there are also some improvements for the lower bounds. We remark that the rather complicated structure of the formula of $M_2(k+3, k)$ for $k \leq 26$ in Conjecture 4.8 suggests that the exact determination of $M_2(k+t, k)$ might not admit an easy explicit solution when k is *small*.

Acknowledgments

Romar dela Cruz would like to thank the Alexander von Humboldt Foundation for the support through the Georg Forster Research Fellowship, and the Mathematical Institute at the University of Bayreuth. Both authors benefit from discussions with Michael Kiermaier and Alfred Wassermann. Especially, the basic idea for the construction in Proposition 4.1 is due to Michael Kiermaier.

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.

n/k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1														
2	1	2													
3	1	3	3												
4	1	3	6	4											
5	1	3	6	10	5										
6	1	3	7	11	15	6									
7	1	3	7	14	17	21	7								
8	1	3	7	14	22	25	28	8							
9	1	3	7	15	26	33	36	36	9						
10	1	3	7	15	30	42	48	48	45	10					
11	1	3	7	15	30	52	66	69	63	55	11				
12	1	3	7	15	30	54	90	103	95	82	66	12			
13	1	3	7	15	31	58	94	151	149	130	102	78	13		
14	1	3	7	15	31	62	106	159	245	217	175	126	91	14	
15	1	3	7	15	31	63	110	183	257	385	308	221	155	196	15

Table 1: $M_2(n,k)$ for $1 \leq n \leq 15, 1 \leq k \leq 15$

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

[9] 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.

[10] R. dela Cruz, M. Kiermaier, S. Kurz and A. Wassermann. On the minimum number of minimal codewords. arXiv preprint 1912.09357, 1912.09804.

[11] 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.

[12] 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.

[13] 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.

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

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

[16] N. Kashyap. On the convex geometry of binary linear codes. preprint. Proceedings of the *Inaugural UC San Diego Workshop on Information Theory and Applications*, 2006.

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

[18] S. Kurz. On the number of minimal codewords in codes generated by the adjacency matrix of a graph. arXiv preprint 2006.02975, 2020.

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

[20] 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.

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

[22] 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.