Three Combinatorial Perspectives on Minimal Codes

Gianira Alfarano, Martino Borello, Alessandro Neri, Alberto Ravagnani

Three Combinatorial Perspectives on Minimal Codes

Gianira N. Alfarano*[1], Martino Borello[2], Alessandro Neri†[3], and Alberto Ravagnani[4]

[1]Institute of Mathematics, University of Zurich, Switzerland
[2]Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, France
[3]Institute for Communication Engineering, Technical University of Munich, Germany
[4]Department of Mathematics and Computer Science, Eindhoven University of Technology, the Netherlands

Abstract

We develop three approaches of combinatorial flavour to study the structure of minimal codes and cutting blocking sets in finite geometry, each of which has a particular application. The first approach uses techniques from algebraic combinatorics, describing the supports in a linear code via the Alon-Füredi Theorem and the Combinatorial Nullstellensatz. The second approach combines methods from coding theory and statistics to compare the mean and variance of the nonzero weights in a minimal code. Finally, the third approach regards minimal codes as cutting blocking sets and studies these using the theory of spreads in finite geometry. Applying and combining these approaches with each other, we derive several new bounds and constraints on the parameters of minimal codes. Moreover, we obtain two new constructions of cutting blocking sets of small cardinality in finite projective spaces. In turn, these allow us to give explicit constructions of minimal codes having short length for the given field and dimension.

Introduction

In a linear code, a codeword is *minimal* if its support does not contain the support of any codeword other than its scalar multiples. A code is *minimal* if its codewords are all minimal.

Minimal codewords in linear codes were originally studied in connection with decoding algorithms [27] and have been used by Massey [31] to determine the access structure in his code-based secret sharing scheme. However, describing the minimal codewords of a linear code is in general a difficult problem, even for highly structured families of codes.

General properties of the minimal codewords of a code are studied in [4], where a sufficient condition for a code to be minimal is presented (often called the *Ashikhmin-Barg condition*).

The latter shows that a linear code in which the minimum and maximum weight are close enough to each other is necessarily minimal. Recently, estimates for the number of minimal codewords in a given code have been also found; see [20].

In the last decade, minimal codes have been the subject of intense mathematical research, yet their structural properties are far from being understood. First results on minimal codes were presented in [17], where the main motivation arises from secure two-party computation.

*Gianira N. Alfarano was supported by the Swiss National Science Foundation through grant no. 188430.
†Alessandro Neri was supported by the Swiss National Science Foundation through grant no. 187711.

Moreover, in the same paper an upper bound on the rate of a minimal code is established, which was recently improved in [1]. Other bounds on the minimum and maximum weight of minimal codes can be found in [18].

Various explicit constructions of minimal codes relying on the aforementioned Ashikhmin-Barg condition are known; see [16, 22] among many others. Constructions that exploit in other ways the minimal structure of the code are based, for example, on functions over finite fields [8, 14, 32, 33]. A geometric approach was proposed in [1, 30, 35], where minimal codes are characterized as cutting blocking sets.

A remarkable property of minimal codes is that they form an asymptotically good family [1, 18]. Since the proofs of [1, 18] are nonconstructive, this naturally poses the problem of *explicitly* constructing families of minimal codes of short length for a given dimension, which is equivalent to constructing small cutting blocking set in a given projective space. Problems of this type are very natural and yet wide open challenges in the realm of extremal combinatorial structures; see e.g. [5, 7, 13]. An important contribution in this direction is [23], where the authors construct small cutting blocking sets in $\mathrm{PG}(k-1,q)$, under the assumption that the characteristic of the field is strictly greater than $k-1$ and the field size is at least $2k-3$. Because of the constraints imposed on the field size, the construction of [23] is of limited applicability in coding theory and does not address the problem of constructing asymptotically good families of minimal codes (where q is fixed and k tends to infinity together with the code length). More recently, a construction of cutting blocking sets in $\mathrm{PG}(3,q)$ and $\mathrm{PG}(5,q)$, which are smaller that the previously known ones, has been given in [10]. This construction produces minimal codes of dimension respectively 4 and 6 over a finite field of arbitrary size.

Our contribution. In this paper, we propose three different approaches of strong combinatorial flavour to the study of minimal codes, each of which has a particular application. Most methods apply more generally to arbitrary linear codes, but give the best and most explicit results when combined with the minimality property of the underlying code.

The idea behind the first approach is to associate to a code a multivariate polynomial, which we call the *support polynomial*. This allows us to capture the combinatorics of the nonzero codewords of a code in an algebraic fashion, characterizing the inclusion relations among supports as the nonvanishing of a polynomial of bounded degree. We then study the support polynomial using tools from algebraic combinatorics, most notably the Alon-Füredi Theorem. As an application of this method, we obtain new lower bounds for both the minimum distance and the length of a minimal code. This improves on known results and excludes the existence of minimal codes for several new parameter sets.

The second approach uses instead ideas from statistics. More precisely, we regard the weight of a nonzero codeword as a discrete random variable and use Pless' equations, along with classical inequalities, to compare its mean and variance. All of this establishes inequalities between the maximum and minimum weight in a linear code, which are sharp for certain code families. In turn, these yield a new upper bound for the minimum distance of a minimal code and exclude the existence of such codes for yet other parameter sets.

Finally, the third approach is based on the correspondence between minimal codes and cutting blocking sets in finite geometry. We first reduce the problem of constructing short minimal codes to that of constructing cutting blocking sets of small cardinality. Then we show how to use the theory of *spreads* in projective spaces to obtain cutting blocking sets whose parameters can be computed explicitly. The applications of this geometric approach are twofold: On the one hand, we obtain new explicit constructions of short minimal codes; on the other hand, we establish a recursive upper bound for the least length of a minimal code over $\mathbb{F}_q$ having prescribed dimension.

For convenience of the reader we conclude the Introduction by listing the main contributions made by this paper, pointing to the corresponding statements.

— As an application of methods from algebraic combinatorics, in particular the Alon-Füredi Theorem and the Combinatorial Nullstellensatz:
    1. a lower bound on the minimum distance of a minimal code (Theorem 2.8);
    2. a structural result on the maximal codewords in a linear code (Theorem 2.13);
    3. a lower bound on the block length of a minimal code (Theorem 2.14).

— Combining ideas from coding theory and statistics with the algebraic combinatorial approach outlined above:
    4. an upper bound on the minimum distance of a minimal code and a constraint on its parameters (Corollary 3.7);
    5. a result connecting the relative difference between maximum and minimum weights in a linear code with its block length (Corollary 3.10).

— Using methods from projective geometry, most notably the theory of spreads:
    6. a construction of cutting blocking sets from spreads in finite geometry and of the corresponding minimal codes (Theorems 4.1 and 4.2);
    7. an inductive construction of cutting blocking sets of small cardinality and of the corresponding minimal codes (Proposition 4.5 and Theorem 4.6);
    8. two new general constructions of short minimal codes (Constructions A and B).

Outline. The paper is overall organized into four sections. Section 1 contains the preliminaries on minimal codes and illustrates their connection with cutting blocking sets. Each of the remaining three sections is devoted to a different approach to minimal codes, using algebraic combinatorics (Section 2), statistics (Section 3), and finite geometry (Section 4).

1 Preliminaries

In this section we establish the terminology for the remainder of the paper and state some preliminary results on the parameters of minimal codes. These will be applied in several instances in the sequel. All codes considered in this work are linear.

Notation 1.1. Throughout this paper, q is a prime power, $\mathbb{F}_q$ is the finite field with q elements, and n, k are integers with $n \geq k \geq 1$. For $i \in \mathbb{N} = \{0, 1, 2, \dots\}$ we let $[i] := \{j \in \mathbb{N} : 1 \leq j \leq i\}$. We only consider row-vectors and for any matrix $M \in \mathbb{F}^{a \times b}$ we denote by $\mathrm{rowsp}(M)$ the rowspace of M over $\mathbb{F}$, that is the $\mathbb{F}$-subspace of $\mathbb{F}^b$ generated by the rows of M. Finally, for $i \in \mathbb{N}_{\geq 1}$ we denote by e_i the i-th standard basis vector.

1.1 Minimal Codes

In this short subsection we define minimal codes and briefly survey some of their main properties. We will use them repeatedly throughout the paper.

Definition 1.2. The (**Hamming**) **support** of a vector $v \in \mathbb{F}_q^n$ is $\sigma(v) = \{i \mid v_i \neq 0\} \subseteq [n]$ and its (**Hamming**) **weight** is $\omega(v) = |\sigma(v)|$.

An $[n, k]_q$ **code** is a nonzero $\mathbb{F}_q$-linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$ of dimension k. Its elements are called **codewords**. The **minimum distance** of $\mathcal{C}$ is the integer $d(\mathcal{C}) = \min\{\omega(c) \mid c \in \mathcal{C},\, c \neq 0\}$ and its **maximum weight** is $\max\{\omega(c) \mid c \in \mathcal{C}\}$. If $d = d(\mathcal{C})$ is known, we say that $\mathcal{C}$ is an $[n, k, d]_q$ code. A **generator matrix** $G \in \mathbb{F}_q^{k \times n}$ of $\mathcal{C}$ is a matrix such that $\mathrm{rowsp}(G) = \mathcal{C}$.

Finally, codes $\mathcal{C}$ and $\mathcal{C}'$ are called (**monomially**) **equivalent** if there exists an $\mathbb{F}_q$-linear isometry $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $f(\mathcal{C}) = \mathcal{C}'$; see [26, page 24].

Recall that an $[n,k]_q$ code $\mathcal{C}$ is **nondegenerate** if there is no $i \in [n]$ with $c_i = 0$ for all $c \in \mathcal{C}$. Furthermore, $\mathcal{C}$ is called **projective** if in one (and thus in all) generator matrix G of $\mathcal{C}$ no two columns are proportional. Note that a projective code is necessarily nondegenerate.

In this paper we mostly concentrate on codes whose codewords are all minimal.

Definition 1.3. Let $\mathcal{C}$ be an $[n,k]_q$ code. A nonzero codeword $c \in \mathcal{C}$ is called **minimal** if every codeword $c' \in \mathcal{C}$ with $\sigma(c') \subseteq \sigma(c)$ is a multiple of c. We say that $\mathcal{C}$ is **minimal** if all its codewords are minimal.

Remark 1.4. Following the notation of Definition 1.3, in a minimal code $\mathcal{C}$ any nonzero codeword c is minimal, but also **maximal** (i.e., every other codeword $c' \in \mathcal{C}$ with $\sigma(c') \supseteq \sigma(c)$ is a multiple of c).

The following simple result states that every minimal codeword c in a $[n,k]_q$ code $\mathcal{C}$ has weight upper bounded by $n-k+1$. To see this, it suffices to puncture $\mathcal{C}$ on the nonzero positions of c, obtaining a new code whose length is $n-\omega(c)$ and whose dimension is $k-1$.

Proposition 1.5. Let $\mathcal{C}$ be an $[n,k]_q$ code. Every minimal codeword $c \in \mathcal{C}$ has $\omega(c) \leq n-k+1$.

The following result shows that minimal codes have relatively large length with respect to their dimension and field size; see also Remark 3.4.

Theorem 1.6 (see [1,30])**.** Let $\mathcal{C}$ be an $[n,k]_q$ minimal code with $k \geq 2$. We have $n \geq (k-1)q+1$.

The previous bound is not tight in general. More precisely, in [1] it was conjectured (and then proved in [35]) that the length n of an $[n,k]_q$ minimal code satisfies the following lower bound.

Theorem 1.7 (see [1,35])**.** Let $\mathcal{C}$ be an $[n,k]_q$ minimal code with $k \geq 2$. We have

$$n \geq (k-1)(q-1)+1+\sum_{i=1}^{k-1}\left\lceil \frac{(k-1)(q-1)+1}{q^i} \right\rceil .$$

In Section 2 we will further improve the bound in Theorem 1.7 using methods from algebraic combinatorics; see Theorem 2.14.

1.2 Minimal Codes and Cutting Blocking Sets

The concept of a *cutting blocking set* was introduced in [14] with the goal of constructing a family of minimal codes. The same objects were know earlier under various names and in different contexts. In [19] these are called *N-fold strong blocking set* and are used for constructing small saturating sets in projective spaces over finite fields. In [23], cutting blocking sets are referred to as *generator sets* and are constructed as union of disjoint lines. In [1] and [35] it was independently shown that cutting blocking sets are in one to one correspondence with minimal linear codes. In this subsection, we recall some properties of (cutting) blocking sets and known results about their size.

Consider the finite projective geometry of dimension N and order q, denoted by $\mathrm{PG}(N,q)$. Recall that

$$\mathrm{PG}(N,q) := \left(\mathbb{F}_q^{N+1} \setminus \{0\}\right)/_{\sim},$$

where $\sim$ denotes the proportionality relation, i.e., $u \sim v$ if and only if $u = \lambda v$ for some nonzero $\lambda \in \mathbb{F}_q$. A **d-flat** in $\mathrm{PG}(N,q)$ is a subspace Π isomorphic to $\mathrm{PG}(d,q)$. A 1-flat is a **line**, while a 2-flat is a **plane**. If $d = N-1$, then Π is called a **hyperplane**.

In our approach, projective systems are crucial geometric objects for the study of linear codes and their properties.

Definition 1.8. A **projective** $[n,k,d]_q$ **system** $\mathcal{P}$ is a finite set of n points (counted with multiplicity) of $\mathrm{PG}(k-1,q)$ that do not all lie on a hyperplane and such that

$$d = n - \max\{|H \cap \mathcal{P}| \,:\, H \subseteq \mathrm{PG}(k-1,q),\ \dim(H) = k-2\}.$$

Projective $[n,k,d]_q$ systems $\mathcal{P}$ and $\mathcal{P}'$ are **equivalent** if there exists a projective isomorphism ϕ of $\mathrm{PG}(k-1,q)$ mapping $\mathcal{P}$ to $\mathcal{P}'$ which preserves the multiplicities of the points.

There is a well-known correspondence between the (monomial) equivalence classes of non-degenerate $[n,k,d]_q$ linear codes and the equivalence classes of projective $[n,k,d]_q$ systems; see [36, Theorem 1.1.6]. More precisely, let G be a $k \times n$ generator matrix of an $[n,k]_q$ linear code. Consider the set $\mathcal{P}$ of one-dimensional subspaces of $\mathbb{F}_q^n$ spanned by the columns of G, which gives a set of points in $\mathrm{PG}(k-1,q)$. Conversely, let $\mathcal{P}$ be a projective $[n,k,d]_q$ system. Choose a representative for any point of $\mathcal{P}$ and consider the code generated by the matrix having these representatives as columns. Now observe that for any nonzero vector $u = (u_1, u_2, \ldots, u_k)$ in $\mathbb{F}_q^k$ the hyperplane

$$u_1x_1 + u_2x_2 + \cdots + u_kx_k = 0$$

contains $|\mathcal{P}| - w$ points of $\mathcal{P}$ if and only if the codeword uG has weight w.

Definition 1.9. Let t, r, N be positive integers with $r < N$. A t**-fold** r**-blocking set** in $\mathrm{PG}(N,q)$ is a set $\mathcal{M} \subseteq \mathrm{PG}(N,q)$ such that for every $(N-r)$-flat Λ of $\mathrm{PG}(N,q)$ we have $|\Lambda \cap \mathcal{M}| \geq t$. When $r = 1$, we will refer to $\mathcal{M}$ as a t**-fold blocking set**. When $t = 1$, we will refer to it as an r**-blocking set**. When $r = t = 1$, $\mathcal{M}$ is simply a **blocking set**.

Cutting blocking sets are defined as follows.

Definition 1.10. Let r, N be positive integers with $r < N$. An r-blocking set $\mathcal{M}$ in $\mathrm{PG}(N,q)$ is **cutting** if for every pair of $(N-r)$-flats Λ, Λ' of $\mathrm{PG}(N,q)$ we have

$$\mathcal{M} \cap \Lambda \subseteq \mathcal{M} \cap \Lambda' \iff \Lambda = \Lambda'.$$

Equivalently, an r-blocking set $\mathcal{M} \subseteq \mathrm{PG}(N,q)$ is cutting if and only if for every $(N-r)$-dimensional subspace Λ of $\mathrm{PG}(N,q)$ we have $\langle \mathcal{M} \cap \Lambda \rangle = \Lambda$; see [1].

It is shown in [1, 35] that the correspondence described above between projective $[n,k,d]_q$ systems and nondegenerate $[n,k,d]_q$ linear codes extends to a correspondence between equivalence classes of $[n,k,d]_q$ minimal codes and equivalence classes of projective $[n,k,d]_q$ systems that are cutting blocking sets. This geometric interpretation of minimal codes will be crucial in Section 4.

Remark 1.11. As already mentioned in the Introduction, we are particularly interested in finding lower bounds on the length of minimal codes or, equivalently, lower bounds on the size of cutting blocking sets in projective spaces. From this point of view, it is not restrictive to only consider projective codes, which correspond to projective systems in which all the points have multiplicity one.

It immediately follows from the definitions that a cutting blocking set $\mathcal{M}$ in $\mathrm{PG}(N,q)$ is necessarily an N-fold blocking set. The following theorem is obtained by combining a well-known result of Beutelspacher (which gives a lower bound on the cardinality of an N-fold blocking set in $\mathrm{PG}(N,q)$ when $N \leq q$) and the correspondence between minimal codes and cutting blocking sets.

Theorem 1.12 (see [11, Theorem 2])**.** Let $\mathcal{C}$ be an $[n,k]_q$ minimal code. If $k - 1 \leq q$, then $n \geq (q+1)(k-1)$.

The above results uses the fact that cutting blocking sets in $\mathrm{PG}(k-1,q)$ are in particular $(k-1)$-fold blocking sets. Beutelspacher also characterized $(k-1)$-fold blocking sets in $\mathrm{PG}(k-1,q)$ with cardinality $(q+1)(k-1)$, under the further assumption that $k \leq \sqrt{q}+2$. Recall that, when q is a square, a **Baer subspace** of $\mathrm{PG}(N,q)$ is a subgeometry isomorphic to $\mathrm{PG}(N,\sqrt{q})$.

Theorem 1.13 (see [11, Theorem 3])**.** Let $4 \leq k \leq \sqrt{q}+2$ and let $\mathcal{M}$ be a $(k-1)$-fold blocking set in $\mathrm{PG}(k-1,q)$. Then $|\mathcal{M}| \geq (q+1)(k-1)$. Moreover, equality holds if and only if one of the following scenarios occurs:

1. $\mathcal{M}$ is the set of points on $k-1$ mutually skew lines.
2. $k = \sqrt{q}+2$ and $\mathcal{M}$ is the point set of a 3-dimensional Baer subspace of $\mathrm{PG}(k-1,q)$.
3. $q=4$, $k=4$, and $\mathcal{M}$ is the complement of a hyperoval in a plane of $\mathrm{PG}(k-1,q)$, where an hyperoval is a set of $q+2$ points in a plane, no three of which are collinear.

In [1, Lemma 4.9] and in [35] it was observed that cutting blocking sets in $\mathrm{PG}(2,q)$ and 2-fold blocking sets are actually the same object. Moreover, in $\mathrm{PG}(2,q)$ one can always construct a 2-fold blocking set of size $3q$, or equivalently a $[3q,3]_q$ minimal code, by considering the union of three lines that do not intersect in the same point. When q is a square, one can construct a cutting blocking set as union of two disjoint Baer subplanes, producing a minimal code of length $2q+2\sqrt{q}+2$. We thus survey the known results on the cardinality of 2-fold blocking sets in $\mathrm{PG}(2,q)$, which turn out to be an accurate estimates also for the length of minimal codes of dimension 3.

Theorem 1.14 (see [6, Theorem 3.1])**.** Let $\mathcal{M}$ be a 2-fold blocking set in $\mathrm{PG}(2,q)$. The following hold.

1. If $q<9$, then $|\mathcal{M}| \geq 3q$.
2. If $q>4$ is a square, then $|\mathcal{M}| \geq 2q+2\sqrt{q}+2$.
3. If $q>19$, $q=p^{2d+1}$, then $|\mathcal{M}| \geq 2q+p^d\left\lceil \frac{(p^{d+1}+1)}{(p^d+1)} \right\rceil + 2$.
4. If $q=11,13,17,19$ is not a square, then $|\mathcal{M}| \geq \frac{(5q+7)}{2}$.

The bounds in Theorem 1.14, parts (3) and (4), are believed not to be sharp; see [6, page 133]. In particular, we are not aware of any construction of 2-fold blocking sets achieving these sizes.

Remark 1.15. In the literature, there are two *general* constructions of small cutting blocking sets we are aware of, which we briefly sketch in this remark.

The first one was proposed by Fancsali and Sziklai in [23] and it works as follows. One chooses any $2k-3$ distinct points on the rational normal curve in $\mathrm{PG}(k-1,q)$ and takes the union of the tangent lines at these points. The resulting set is a cutting blocking set, under the assumption that the characteristic of the field is at least k. We call this set the **rational normal tangent set**. The corresponding codes are minimal $[(2k-3)(q+1),k]_q$ codes whose minimum distance was proved to be at least kq in [10]. The drawback of this construction is the constraint on both the size (q) and the characteristic (p) of the underlying field, reading $q \geq 2k-3$ and $p \geq k$. For a fixed value of q, the approach of [23] constructs cutting blocking sets in $\mathrm{PG}(k-1,q)$ for only a finite number of values of k.

A second construction that instead works for every choice of the parameters k and q can be found in [1, 9, 30]. Consider k points $P_1,\dots,P_k$ in general position in $\mathrm{PG}(k-1,q)$ and let $\ell_{i,j} := \langle P_i, P_j \rangle$. Then the union of these lines gives a cutting blocking set. From this construction, called **tetrahedron**, one obtains a family of $[(q-1)\binom{k}{2}+k, k, (q-1)(k-1)+1]_q$ minimal codes. As a consequence of Theorem 1.14, when $k=3$ this construction provides a minimal 2-fold blocking set in $\mathrm{PG}(2,q)$ for any $q<9$.

2 Algebraic Combinatorial Approach

This section develops an algebraic combinatorial approach to study minimal codes. The method uses a generator matrix of a linear code to build a multivariate polynomial "machinery". This allows us to study the maximal codewords of a code by applying classical results on the number of roots of multivariate polynomials over finite grids. As an application of our method, with the aid of Alon's Combinatorial Nullstellensatz [2] and the Alon-Füredi Theorem [3], we improve known lower bounds on the minimum distance and the length of minimal codes.

It is interesting to observe that the results contained in this section are mainly exploiting the fact that in a minimal code all the codewords are *maximal*, as already observed in Remark 1.4. Although in a minimal code this code property is equivalent to all codewords being minimal, the focus on maximal codewords is crucial for deriving both the lower bound on the minimum distance (Theorem 2.8) and the lower bound on the length (Theorem 2.14) of minimal codes.

2.1 Combinatorial Nullstellensatz and Alon-Füredi Theorem

We start by surveying tools from algebraic combinatorics that will be applied repeatedly. Among these are Alon's Combinatorial Nullstellensatz and the Alon-Füredi Theorem.

Notation 2.1. We state the results of this subsection and of the next one for an arbitrary field $\mathbb{F}$. In Subsection 2.3 we will resume focusing on the case $\mathbb{F} = \mathbb{F}_q$ and on linear codes.

For a multivariate polynomial $p \in \mathbb{F}[x_1, \ldots, x_k]$ and a subset $A \subseteq \mathbb{F}^k$, denote by $V_A(p)$ the set of zeros of p in A, and by $U_A(p)$ the nonzeros of p in A, i.e.,

$$V_A(p) = \{v \in A \mid p(v) = 0\},$$
$$U_A(p) = \{u \in A \mid p(u) \neq 0\}.$$

The Alon–Füredi Theorem [3, Theorem 5] gives a lower bound on the cardinality of $U_A(p)$ when A is a finite grid and p is not identically zero on A. Equivalently, it provides an upper bound on the number of zeros of p. We recall it for convenience of the reader.

Theorem 2.2 (Alon–Füredi Theorem [3])**.** Let $A = A_1 \times \ldots \times A_k \subseteq \mathbb{F}^k$ be a finite grid with $A_i \subseteq \mathbb{F}$ and $|A_i| = n_i$, where $n_1 \geq n_2 \geq \ldots \geq n_k \geq 2$. Let $p \in \mathbb{F}[x_1, \ldots, x_k]$ be a polynomial that is not identically 0 on A, and let $\bar{p}$ be the polynomial p modulo the ideal $(f_1(x_1), \ldots, f_k(x_k))$, where $f_i(x_i) = \prod_{a \in A_i}(x_i - a)$. Then

$$|U_A(p)| \geq (n_s - \ell) \prod_{i=1}^{s-1} n_i,$$

where ℓ and s are the unique integers satisfying $\deg \bar{p} = \sum_{i=s+1}^{k}(n_i - 1) + \ell$, with $1 \leq s \leq k$ and $1 \leq \ell \leq n_s - 1$.

The above theorem relies on the fact that the polynomial p is not identically zero on the finite grid we are interested in. However, when dealing with polynomials that are not explicitly given, this property is not always easy to verify. In this direction, the celebrated Alon's Combinatorial Nullstellensatz helps determining a sufficient condition for a polynomial to be nonzero on a finite grid. We state it here for completeness.

Theorem 2.3 (Combinatorial Nullstellensatz [2])**.** Let $p \in \mathbb{F}[x_1, \ldots, x_k]$ and let $\deg p = \sum_{i=1}^{k} r_i$, for some $r_1, \ldots, r_k \in \mathbb{N}$. Suppose that the coefficient of the monomial $x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k}$ in p is nonzero. Let $A := A_1 \times \ldots \times A_k \subseteq \mathbb{F}^k$ be a grid with $|A_i| \geq r_i + 1$ for all $i \in [k]$. Then $U_A(p) \neq \emptyset$.

2.2 The Support Polynomials

We denote by $g^{(i)}$ the i-th column vector of a matrix $G \in \mathbb{F}^{k\times n}$. Moreover, we consider the vector $x = (x_1, \ldots, x_k)$ whose entries are algebraically independent variables over $\mathbb{F}$.

Definition 2.4. The **support polynomial** associated with a matrix $G \in \mathbb{F}^{k\times n}$ and a subset $I \subseteq [n]$ is

$$p_{G,I}(x) := \prod_{i\in I} x \cdot g^{(i)} \in \mathbb{F}[x_1, \ldots, x_k].$$

In our approach, support polynomials are crucial for the study of minimal codes (taking as G a generator matrix of an $[n, k, d]_q$ code and as I a subset of a codeword's support). However, for the moment we focus on general properties of support polynomials that do not necessarily arise from codes. The following result is straightforward and its proof is omitted.

Proposition 2.5. Let $G \in \mathbb{F}^{k\times n}$ and $I \subseteq [n]$.

1. For every $A \in \mathrm{GL}(k, \mathbb{F})$

   $$p_{AG,I}(x) = p_{G,I}(xA) = (p_{G,I} \circ L_A)(x),$$

   where L_A denotes the linear map associated to the matrix A, that is $v \longmapsto vA$.

2. For every $\tau \in \mathcal{S}_n$

   $$p_{G,\tau(I)}(x) = p_{GP_\tau,I}(x),$$

   where P_τ is the permutation matrix associated to τ, such that

   $$(v_1, \ldots, v_n)P_\tau = \left(v_{\tau(1)}, \ldots, v_{\tau(n)}\right).$$

3. For every $v \in \mathbb{F}^n$

   $$p_{GD_v,I}(x) = \Big(\prod_{i\in I} v_i\Big) p_{G,I}(x),$$

   where D_v denotes the diagonal matrix whose diagonal is v.

We now study a support polynomial in connection with the rowspace of the matrix $G \in \mathbb{F}^{k\times n}$ that defines it. We first show how the zeros and nonzeros of support polynomials are related when we choose matrices with the same rowspace.

Let $G_1, G_2 \in \mathbb{F}^{k\times n}$ be two matrices such that $\mathrm{rowsp}(G_1) = \mathrm{rowsp}(G_2)$. It is easy to see that there exists $A \in \mathrm{GL}(k, \mathbb{F})$ such that

$$U_{\mathbb{F}_q^k}(p_{G_1,I}) = U_{\mathbb{F}_q^k}(p_{G_2,I}) \cdot A := \left\{uA \mid u \in U_{\mathbb{F}_q^k}(p_{G_1,I})\right\},$$
$$V_{\mathbb{F}_q^k}(p_{G_1,I}) = V_{\mathbb{F}_q^k}(p_{G_2,I}) \cdot A := \left\{vA \mid v \in V_{\mathbb{F}_q^k}(p_{G_1,I})\right\}.$$

Indeed, any matrix A with $G_2 = AG_1$ satisfies the desired properties. Moreover, the nonzeros of a support polynomial are closely related to the support of vectors belonging to the rowspace of the defining matrix. This is shown by the following simple result, whose proof is omitted.

Lemma 2.6. Let $G \in \mathbb{F}^{k\times n}$ be a matrix. For all $I \subseteq [n]$ we have

$$U_{\mathbb{F}^k}(p_{G,I}) = \left\{u \in \mathbb{F}^k \mid \sigma(uG) \supseteq I\right\}.$$

In particular, $U_{\mathbb{F}^k}(p_{G,I}) \neq \emptyset$ if and only if there exists $c \in \mathrm{rowsp}(G)$ such that $\sigma(c) \supseteq I$.

2.3 Minimum Distance of Minimal Codes

In this subsection we investigate the support polynomials of generator matrices of linear codes and their set of zeros. As a corollary of our results, we establish[1] a conjecture from [1].

We start with the following lemma, whose proof directly follows from Lemma 2.6 and Remark 1.4.

Lemma 2.7. Let $G \in \mathbb{F}_q^{k\times n}$ be a generator matrix of an $[n,k]_q$ code $\mathcal{C}$. Let $c = uG$ be a maximal codeword of $\mathcal{C}$ and $I := \sigma(c)$. Then

$$U_{\mathbb{F}_q^k}(p_{G,I}) = \{\lambda u \mid \lambda \in \mathbb{F}_q^*\}.$$

In particular, if $\mathcal{C}$ is a minimal code then the above statement holds for every nonzero codeword.

Theorem 2.8. Let $\mathcal{C}$ be an $[n,k,d]_q$ code, and let c be a maximal codeword. Then $\omega(c) \geq (q-1)(k-1)+1$. In particular, if $\mathcal{C}$ is minimal then $d \geq (q-1)(k-1)+1$.

Proof. Let $c = (c_1,\ldots,c_n) \in \mathcal{C}$ be a maximal codeword of weight w and let $I := \sigma(c)$, i.e., $c_i \in \mathbb{F}_q^*$ if and only if $i \in I$. Take a generator matrix $G \in \mathbb{F}_q^{k\times n}$ for $\mathcal{C}$ and consider the polynomial $p_{G,I}(x) \in \mathbb{F}_q[x_1,\ldots,x_k]$. Observe that $p_{G,I}$ does not vanish identically on $\mathbb{F}_q^k$. Indeed, let $u \in \mathbb{F}_q^k$ be the vector such that $uG = c$. Then $p_{G,I}(u) = \prod_{i\in I} c_i \neq 0$. This also ensures that $\deg p_{G,I} = w$. Since c is a maximal codeword, by Lemma 2.7 we have $U_{\mathbb{F}_q^k}(p_{G,I}) = \{\alpha\lambda \mid \alpha \in \mathbb{F}_q^*\}$, which has cardinality $q-1$.

On the other hand, let $\bar{p}_{G,I}$ denote the reduction of the polynomial $p_{G,I}$ modulo the ideal $(\{x_i^q - x_i \mid i \in [k]\})$. By Theorem 2.2 we have

$$|U_{\mathbb{F}_q^k}(p_{G,I})| \geq (q-\ell)q^{s-1},$$

where ℓ and s are the unique integers satisfying $\deg \bar{p}_{G,I} = (q-1)(k-s)+\ell$, with $1 \leq s \leq k$ and $1 \leq \ell \leq q-1$.

Thus, combining this with the exact value of $|U_{\mathbb{F}_q^k}(p_{G,I})|$, we obtain $q-1 = |U_{\mathbb{F}_q^k}(p_{G,I})| \geq (q-\ell)q^{s-1}$, from which we deduce $s = 1$. Therefore,

$$w = \deg p_{G,I} \geq \deg \bar{p}_{G,I} = (q-1)(k-1)+\ell \geq (q-1)(k-1)+1. \qquad \square$$

Remark 2.9. The Alon-Füredi Theorem (Theorem 2.2) gives a lower bound on the number of nonzeros of a multivariate polynomial in a finite grid in terms of the degree of the polynomial and the size of the grid. This result has been used in coding theory for deriving the minimum distance of generalized Reed-Muller codes; see e.g. [24, 29]. It is interesting to observe that in our Theorem 2.8 the Alon-Füredi Theorem is applied in the "opposite" direction, i.e., we use it to derive a lower bound on the degree of the support polynomial associated to a maximal codeword, knowing the number of its nonzeros.

2.4 Maximal Codewords in Linear Codes

In this subsection we use support polynomials to study the structure of maximal codewords in a linear code $\mathcal{C}$. In particular, we show that for any maximal codeword $c \in \mathcal{C}$ there exist several codewords whose support contains a large subset of the support of c. This property will be crucial for deriving a lower bound on the length of minimal codes in Subsection 2.5.

[1] While preparing the final version of this manuscript, we realized that the same conjecture has been also established in a recent preprint [35], using different methods. The approach developed in this paper also serves to describe the structure of codes that are not necessarily minimal, proving general properties of their maximal codewords.

For $v = (v_1, \ldots, v_k) \in \mathbb{F}_q^k$, define

$$f_v(x) := \prod_{i=1}^{k} \Big(\prod_{s \in \mathbb{F}_q \setminus \{v_i\}} (x_i - s) \Big).$$

Next, consider the ideal $I_q := (x_1^q - x_1, \ldots, x_k^q - x_k)$ and denote by $\bar{f}$ the reduction of a polynomial $f \in \mathbb{F}_q[x_1, \ldots, x_k]$ modulo I_q. It is easy to check that for every $v \in \mathbb{F}_q^k$ we have $\bar{f_v} = f_v$. One can also easily prove that the set $\{f_v \mid v \in \mathbb{F}_q^k\}$ is an $\mathbb{F}_q$-basis for the space $\mathbb{F}_q[x_1, \ldots, x_k]/I_q$. Moreover, regarding the polynomials f_v's as maps from $\mathbb{F}_q^k$ to $\mathbb{F}_q$, the set $\{f_v \mid v \in \mathbb{F}_q^k\}$ is an $\mathbb{F}_q$-basis of $\{\varphi : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q\}$. This is due to the following well-known result.

Proposition 2.10. The evaluation map on $\mathbb{F}_q[x_1, \ldots, x_k]$ induces the isomorphism of $\mathbb{F}_q$-vector spaces

$$\mathbb{F}_q[x_1, \ldots, x_k]/I_q \cong \{\varphi : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q\}. \tag{2.1}$$

In particular, for every $p \in \mathbb{F}_q[x_1, \ldots, x_k]$ there exist unique $\mu_v \in \mathbb{F}_q$ for $v \in U_{\mathbb{F}_q^k}(p)$, such that

$$\bar{p} = \sum_{v \in U_{\mathbb{F}_q^k}(p)} \mu_v f_v.$$

Proposition 2.11. Let $\mathcal{C}$ be an $[n, k]_q$ code and let $c = (c_1, \ldots, c_n) \in \mathcal{C}$ be a maximal codeword of $\mathcal{C}$ with weight w and support $I := \sigma(c)$. Let w_1 be the unique integer in $[q-1]$ such that $w_1 \equiv w \mod (q-1)$. Then, for any $A \in \mathrm{GL}(k, q)$ such that the first row of $A^{-1}G$ is equal to c, we have $\bar{p}_{G,I}(x) = p_c(xA)$, where

$$p_c(x) = \Big(\prod_{i=1}^{w} c_i \Big) x_1^{w_1} \prod_{i=2}^{k} (1 - x_i^{q-1}).$$

Proof. We first prove the statement in the case where the first row of G is equal to c. Observe that $\bar{p}_c = p_c$, that is, the polynomial p_c is already reduced modulo I_q. Therefore, by the isomorphism given in (2.1), we only need to show that $p_{G,I}(v) = p_c(v)$ for every $v \in \mathbb{F}_q^k$. By definition of p_c we have

$$p_c(v) = \begin{cases} \lambda^{w_1} \prod_{i=1}^{w} c_i & \text{if } v = \lambda e_1, \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand, by the choice of G and Lemma 2.7 we have

$$p_{G,I}(\lambda e_1) = \prod_{i=1}^{w} (\lambda c_i) = \lambda^{w_1} \prod_{i=1}^{w} c_i,$$

where the last inequality follows using the identity $\lambda^q = \lambda$. Moreover, $p_{G,I}(v) = 0$ for every $v \notin \{\lambda e_1 \mid \lambda \in \mathbb{F}_q^*\}$.

The general case follows from the previous one. We first transform G into $A^{-1}G$, where the first row of $A^{-1}G$ is equal to c. This implies that $p_{A^{-1}G,I}(x) = p_c(x)$. Then, using Proposition 2.5, we find $p_{G,I}(x) = p_{A^{-1}G,I}(xA) = p_c(xA)$. ∎

Notation 2.12. In the remainder of the section we write $x = (x_1, \ldots, x_k)$ and for $\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{N}^k$ we denote by x^α the monomial $x_1^{\alpha_1} \cdots x_k^{\alpha_k}$. Moreover, we let $\|\alpha\| := \alpha_1 + \ldots + \alpha_k$. Finally, for a polynomial $p(x) \in \mathbb{F}_q[x_1, \ldots, x_k]$ and a monomial x^α, we denote by $[x^\alpha]p(x)$ the coefficient of the monomial $x^\alpha = x_1^{a_1} \cdots x_k^{a_k}$ in $p(x)$.

The following result on maximal codewords will be crucial in the next subsection for deriving a lower bound on the length of a minimal code.

Theorem 2.13. Let $\mathcal{C}$ be an $[n,k]_q$ code and let $c=(c_1,\dots,c_n)\in\mathcal{C}$ be a maximal codeword. For every $j\in\sigma(c)$ there exist $I_j\subseteq\sigma(c)\setminus\{j\}$ of cardinality $(q-1)(k-1)$ and a codeword $z\in\mathcal{C}$ such that $\sigma(z)\cap\sigma(c)\supseteq I_j$.

Proof. Let $c\in\mathcal{C}$ be a nonzero codeword with support $I:=\sigma(c)$ and weight $w=(q-1)(k-1)+w_1$. By Theorem 2.8 we have $w_1\geq 1$.

Assume first that $w\leq(q-1)k$, which implies $1\leq w_1\leq q-1$. We choose a generator matrix G for $\mathcal{C}$ whose first row is equal to c, and assume that $c_i=1$ for every $i\in I$. This can be done without loss of generality, up to replacing the code with an equivalent one. By Proposition 2.11 we have

$$\bar{p}_{G,I}(x)=p_c(x)=x_1^{w_1}\prod_{i=2}^{k}(1-x_i^{q-1}).$$

Let $j\in I$ and assume that the j-th column of G is $(1,0,\dots,0)^\top$. Define $\mathcal{L}_{I,j}:=\{L\subseteq I : j\notin L,\ |L|=(q-1)(k-1)\}$ and $\beta:=(w_1,q-1,q-1,\dots,q-1)$. We have

$$\begin{aligned}(-1)^{k-1}&=[x^\beta]\bar{p}_{G,I}(x)\\&=[x^\beta]p_{G,I}(x)\\&=\sum_{L\in\mathcal{L}_{I,j}}[x_2^{q-1}\cdots x_k^{q-1}]p_{G,L}(x).\end{aligned}$$

The first equality follows from direct inspection of $p_c(x)$. The second equality is due to the fact that the degree $p_{G,I}$ is equal to $(q-1)(k-1)+w_1$, which is also the degree of $\bar{p}_{G,I}$. The third equality follows from the fact that the coefficients of x_1 in the matrix G are all equal to 1. Therefore, there exists $I_j\in\mathcal{L}_{I,j}$ such that $[x_2^{q-1}\cdots x_k^{q-1}]p_{G,I_j}(x)\neq 0$. Let $x':=(x_2,\dots,x_k)$ and consider the polynomial $f(x'):=p_{G,I_j}(0,x_2,\dots,x_k)$. This polynomial has degree $|I_j|=(q-1)(k-1)$ and $[x_2^{q-1}\cdots x_k^{q-1}]f(x')=[x_2^{q-1}\cdots x_k^{q-1}]p_{G,I_j}(x)\neq 0$. Hence, by Theorem 2.3, there exists $v\in\mathbb{F}_q^{k-1}$ such that $f(v)=p_{G,I_j}(0,v)\neq 0$. By Lemma 2.6, this implies that the codeword $z:=(0,v)G\in\mathcal{C}$ satisfies $\sigma(z)\supseteq I_j$.

Now assume that $w>(q-1)k$, from which $w_1\geq q$. Let us write $w_1=a(q-1)+b$ with $1\leq b\leq q-1$. Since $w>(q-1)k$, we have $a\geq 1$. Denote the vector $\beta:=(b,q-1,q-1,\dots,q-1)$. Consider the set $T:=\{\alpha\in\mathbb{N}^k : \|\alpha\|=a(q-1),\alpha_i\equiv 0 \mod (q-1) \text{ for every } i\in[k]\}$. Then

$$\begin{aligned}(-1)^{k-1}&=[x^\beta]\bar{p}_{G,I}(x)\\&=\sum_{\alpha\in T}[x^{\beta+\alpha}]p_{G,I}(x).\end{aligned}$$

This means that there exists $\gamma\in T$ such that $[x^{\beta+\gamma}]p_{G,I}(x)\neq 0$. Define $\mathcal{L}_{I,j}^{(\gamma)}:=\{L\subseteq I : |L|=w-b-\gamma_1, j\notin L\}$, $\gamma':=(0,\gamma_2,\dots,\gamma_k)$, and $\beta':=(0,q-1,\dots,q-1)$. We have

$$[x^{\beta+\gamma}]p_{G,I}(x)=\sum_{L\in\mathcal{L}_{I,j}^{(\gamma)}}[x^{\beta'+\gamma'}]p_{G,L}(x)$$

and there exists $K\in\mathcal{L}_{I,j}^{(\gamma)}$ such that $[x^{\beta'+\gamma'}]p_{G,K}(x)\neq 0$. At this point we can consider the set $\mathcal{X}_K:=\{M\subseteq K : |M|=(q-1)(k-1)\}$ and write

$$[x^{\beta'+\gamma'}]p_{G,K}(x)=\sum_{M\in\mathcal{X}_K}\lambda_M\big([x^{\beta'}]p_{G,M}(x)\big)$$

for some $\lambda_M\in\mathbb{F}_q$. Since this sum is nonzero, there exists M such that $[x^{\beta'}]p_{G,M}(x)\neq 0$. As in the previous case, we use Theorem 2.3 and Lemma 2.6 to deduce that there exists a codeword $z\in\mathcal{C}$ such that $\sigma(z)\supseteq M$. ∎

2.5 The Length of Minimal Codes

As an application of Theorem 2.13, we derive the following lower bound on the length of a minimal code.

Theorem 2.14. Let $\mathcal{C}$ be an $[n,k,d]_q$ minimal code. We have $n \geq (q+1)(k-1)$.

Proof. Let $c \in \mathcal{C}$ be a codeword of minimum weight d with support $I := \sigma(c)$. Up to considering an equivalent code, we can assume $c_i = 1$ for every $i \in I$. Since c is in particular a maximal codeword of $\mathcal{C}$, by Theorem 2.13 there exists a codeword $z \in \mathcal{C}$ such that $|I \cap \sigma(z)| \geq (q-1)(k-1)$. Let $J := I \cap \sigma(z)$ and for every $\lambda \in \mathbb{F}_q^*$ define $J_\lambda := \{j \in J \mid z_j = \lambda\}$. Clearly, $J = \bigcup_{\lambda \in \mathbb{F}_q^*} J_\lambda$ and the union is disjoint. Thus by generalized pigeonhole principle there exists $\lambda' \in \mathbb{F}_q^*$ such that

$$|J_{\lambda'}| \geq \left\lceil \frac{|J|}{q-1} \right\rceil \geq k-1.$$

Now consider the codeword $z - \lambda' c$. Its support is $\sigma(z - \lambda' c) = (\sigma(c) \cup \sigma(z)) \setminus J_{\lambda'}$ and

$$\begin{aligned} \omega(z - \lambda' c) &= |\sigma(c)| + |\sigma(z)| - |J| - |J_{\lambda'}| \\ &\leq d + \omega(z) - q(k-1). \end{aligned}$$

Combining this with $\omega(z - \lambda' c) \geq d$ we obtain $\omega(z) \geq q(k-1)$. Furthermore, by Proposition 1.5 we have $\omega(z) \leq n - k + 1$, from which we finally obtain $n \geq (q+1)(k-1)$. □

Remark 2.15. The lower bound of Theorem 2.14 is an improvement on the bound in Theorem 1.7. Indeed, we have

$$(q+1)(k-1) \geq \sum_{i=0}^{k-1} \left\lceil \frac{(q-1)(k-1)+1}{q^i} \right\rceil. \tag{2.2}$$

We do not go into the details of the proof.

Remark 2.16. Observe that Theorem 2.14 is an improvement on the bound of Theorem 1.12, since it does not require the extra assumption that $k \leq q+1$.

We conclude this section with a detailed example building on [1, Example 5.11].

Example 2.17. We fix $q = 3$, $k = 4$ and take the minimal $[14,4,7]_3$ code $\mathcal{C}$ whose generator matrix is

$$G := \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1 \\ 0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Let $I := \{8, 9, \ldots, 14\}$ be the support of the codeword c given by the first row of G and let $x = (x_1, x_2, x_3, x_4)$. We compute the associated support polynomial

$$p_{G,I}(x) = x_1(x_3^2 - x_1^2)(x_1^2 - x_4^2)((x_4 - x_2)^2 - (x_3 - x_1)^2).$$

An easy calculation shows that the reduction of $p_{G,I}(x)$ modulo $I_3 = (x_1^3 - x_1, x_2^3 - x_2, x_3^3 - x_3, x_4^3 - x_4)$ is

$$\bar{p}_{G,I}(x) = x_1(1 - x_2^2)(1 - x_3^2)(1 - x_4^2) = p_c(x),$$

as we can also deduce from Proposition 2.11.

Moreover, since $\mathcal{C}$ is a minimal code, we can actually see that for every $j \in I$ there exists a codeword $z^{(j)} \in \mathcal{C}$ such that $\sigma(z^{(j)}) \supseteq I \setminus \{j\}$, as stated in Theorem 2.13. These 7 codewords (up to their nonzero scalar multiples) are

$$z^{(8)} = (0,0,0,0,2,1,2,0,1,1,1,1,1,2),$$

$$
\begin{aligned}
z^{(9)} &= (0,1,2,1,2,0,1,2,0,1,1,1,2,2),\\
z^{(10)} &= (1,2,0,1,2,0,1,1,1,0,1,2,1,2),\\
z^{(11)} &= (2,1,0,2,2,2,0,1,2,1,0,2,2,2),\\
z^{(12)} &= (1,2,0,1,1,1,0,1,2,1,2,0,2,1),\\
z^{(13)} &= (0,2,1,2,2,2,0,1,2,1,1,1,0,2),\\
z^{(14)} &= (0,1,2,1,1,1,0,1,2,1,1,1,1,0).
\end{aligned}
$$

Finally, note that, in order to derive the lower bound on the length of minimal codes given in Theorem 2.14, we use in its proof that each of the codewords $z^{(j)}$ has weight at least $q(k-1)=9$. However, in this case only $z^{(8)}$ has weight 9, while all the other codewords have weight 11.

Remark 2.18. It is natural to ask whether the bound of Theorem 2.14 is sharp or not. As stated in Subsection 1.2, minimal codes of dimension k over $\mathbb{F}_q$ correspond to cutting blocking sets in $\mathrm{PG}(k-1,q)$ and a cutting blocking set is in particular a $(k-1)$-fold blocking set. When we restrict to the case $4 \le k \le \sqrt{q}+2$, Theorem 1.13 characterizes a $(k-1)$-fold blocking set $\mathcal{M}$ in $\mathrm{PG}(k-1,q)$ of cardinality $(q+1)(k-1)$. This only happens in three cases.
Case I: $\mathcal{M}$ is the union of $k-1$ disjoint lines. In this case $\mathcal{M}$ cannot be a cutting blocking set. To see this, write $\mathcal{M} = \ell_1 \cup \ldots \cup \ell_{k-1}$. Pick $P_1 \in \ell_1, \ldots, P_{k-1} \in \ell_{k-1}$ and let $\Lambda := \langle P_1, \ldots, P_{k-1}\rangle$. If $\dim(\Lambda) \le k-3$, then Λ is contained in a $(k-3)$-flat Λ'. Consider the sheaf of hyperplanes containing Λ'. They are $q+1$ and only $k-1$ of them contain other points of $\mathcal{M}$ in addition to $P_1, \ldots, P_{k-1}$. Since $k-1 < q+1$ there is at least one hyperplane H such that $H \cap \mathcal{M} = \{P_1, \ldots, P_{k-1}\}$ and $\langle H \cap \mathcal{M}\rangle \subseteq \Lambda' \neq H$. This implies that, in this case, $\mathcal{M}$ is not a cutting blocking set. Suppose then that $\dim(\Lambda) = k-2$. Fix $P_1, \ldots, P_{k-3}$ and consider the flat $\Gamma := \langle P_1, \ldots, P_{k-3}, \ell_{k-2}\rangle$. If $\dim(\Gamma) < k-2$, then there exists $Q_{k-2} \in \ell_{k-2} \cap \langle P_1, \ldots, P_{k-3}\rangle$. Thus, if we replace P_{k-2} by Q_{k-2}, we get that $\dim(\Lambda) < k-2$, and we can conclude as done before that $\mathcal{M}$ is not cutting. Hence, assume $\dim(\Gamma) = k-2$. In this case $\Gamma \cap \ell_{k-1} \neq \emptyset$. Take $Q_{k-1} \in \Gamma \cap \ell_{k-1}$. If $Q_{k-1} \in \langle P_1, \ldots, P_{k-3}\rangle$, we substitute P_{k-1} with Q_{k-1} and get again $\dim(\Lambda) < k-2$, which implies $\mathcal{M}$ not being cutting. Therefore, assume that the space $\langle P_1, \ldots, P_{k-3}, Q_{k-1}\rangle$ is a hyperplane in Γ. Since Γ also contains ℓ_{k-2}, there exists $R_{k-2} \in \ell_{k-2} \cap \langle P_1, \ldots, P_{k-3}, Q_{k-1}\rangle$. Thus, replacing P_{k-1} with Q_{k-1} and P_{k-2} with R_{k-2}, we again obtain that $\dim(\Lambda) < k-2$ and $\mathcal{M}$ is not cutting.
Case II: $k = \sqrt{q}+2$ and $\mathcal{M}$ is a 3-dimensional Baer subspace. If $k \ge 5$, then $\langle \mathcal{M}\rangle \neq \mathrm{PG}(k-1,q)$, so $\mathcal{M}$ cannot be a cutting blocking set. For the remaining case, where $k = q = 4$, one can observe that for a (hyper)plane H in $\mathrm{PG}(3,q)$, H intersects $\mathcal{M}$ in a Baer subplane or in a Baer subline. In the latter case, one has $\langle \mathcal{M} \cap H\rangle \neq H$, and so $\mathcal{M}$ is not a cutting blocking set. The fact that for $k = q = 4$ a 3-dimensional Baer subspace $\mathcal{M}$ cannot be cutting could be also deduced from Example 3.8, since the cardinality of $\mathcal{M}$ is 15.
Case III: $q = k = 4$ and $\mathcal{M}$ is the complement of a hyperoval in a plane of $\mathrm{PG}(3,q)$. In this case $\langle \mathcal{M}\rangle \neq \mathrm{PG}(3,q)$ and $\mathcal{M}$ cannot be a cutting blocking set.

Therefore, when $4 \le k \le \sqrt{q}+2$, the bound in Theorem 2.14 is never sharp.

Corollary 2.19. Let $\mathcal{C}$ be a minimal $[n,k]_q$ code with $3 \le k \le \sqrt{q}+2$. Then $n \ge (q+1)(k-1)+1$, unless $q = 2$ and $k = 3$.

Proof. The case $k \ge 4$ has been discussed in Remark 2.18. When $k = 3$, cutting blocking sets are equivalent to 2-fold blocking set. Using Theorem 1.14, one can easily verify that the only case in which a 2-fold blocking set has cardinality $2q+2$ is when $q = 2$. □

3 Statistical Approach

Most bounds for minimal codes we are aware of involve either (q, n, k), or (q, k, d). Bounds involving all the four parameters (q, n, k, d) can in turn be obtained combining these with classical bounds for Hamming-metric codes, such as the Singleton or the Griesmer bound.

In this section, we develop a method to establish new inequalities that directly involve all the four parameters of a minimal code, namely (q, n, k, d). As an application, we obtain an upper bound for the minimum distance d of a minimal code in terms of (q, n, k). As we will see in the examples, this bound excludes the existence of minimal codes with parameter sets that do not violate any of the known bounds.

Our approach combines Theorem 2.8 with ideas from statistics, interpreting the weight of the codewords of a linear code as a discrete random variable and computing/estimating its mean and variance. As simple corollaries of our bounds, we recover classical results on constant-weight codes.

Throughout this section, $\mathcal{C}$ denotes a nondegenerate code. Our results can be made more precise when $\mathcal{C}$ is projective; see Section 1 for the definition.

3.1 Mean and Variance of the Nonzero Weights in a Linear Code

We start with an upper bound for the sum of the squares of the weights in a nondegenerate linear code. The proof uses one of the Pless' identities.

Lemma 3.1. Let $\mathcal{C}$ be a nondegenerate $[n, k]_q$ code. We have

$$\sum_{c\in\mathcal{C}} \omega(c)^2 \geq q^{k-2}\, n\,(q-1)\,[n(q-1)+1].$$

Moreover, equality holds if and only if $\mathcal{C}$ is projective.

Proof. For $i \in \{0, \dots, n\}$ we denote by $W_i(\mathcal{C}^\perp)$ the number of codewords of weight i in the dual code $\mathcal{C}^\perp$. Since $\mathcal{C}$ is nondegenerate, we have $W_1(\mathcal{C}^\perp) = 0$. Moreover, $\mathcal{C}$ is projective if and only if $W_2(\mathcal{C}^\perp) = 0$. Using Pless' identities [26, Theorem 7.2.3(P1)] we can write

$$\sum_{c\in\mathcal{C}} \omega(c)^2 = \sum_{\nu=0}^{2} \left(\nu!\, S(2,\nu)\, q^{k-\nu}(q-1)^\nu \binom{n}{n-\nu} \right) + 4W_2(\mathcal{C}^\perp) S(2,2) q^{k-2}, \tag{3.1}$$

where $S(a, b) \geq 0$ is the Stirling number of the second kind indexed by (a, b). Therefore

$$\sum_{c\in\mathcal{C}} \omega(c)^2 \geq \sum_{\nu=0}^{2} \left(\nu!\, S(2,\nu)\, q^{k-\nu}(q-1)^\nu \binom{n}{n-\nu} \right),$$

with equality if and only if $\mathcal{C}$ is projective. The lemma now follows from the fact that $S(2, 0) = 0$ and $S(2, 1) = S(2, 2) = 1$. □

The next step consists in defining the mean and variance of the nonzero weights in a linear code and to study the latter via Lemma 3.1.

Notation 3.2. For a code $\mathcal{C}$, let

$$\mathbb{E}(\mathcal{C}) := (q^k - 1)^{-1} \sum_{c\in\mathcal{C}} \omega(c),$$
$$\mathrm{Var}(\mathcal{C}) := (q^k - 1)^{-1} \sum_{c\in\mathcal{C}} \omega(c)^2 - \mathbb{E}(\mathcal{C})^2.$$

We now compute/estimate these two quantities.

Theorem 3.3. Let $\mathcal{C}$ be a nondegenerate $[n,k]_q$ code. Let $\ell = n(q-1)/(q^k-1)$. We have $\mathbb{E}(\mathcal{C}) = q^{k-1}\ell$ and $\mathrm{Var}(\mathcal{C}) \geq q^{k-2}\,\ell(1-\ell)$. Moreover, equality holds if and only if $\mathcal{C}$ is projective.

Proof. Since $\mathcal{C}$ is nondegenerate, we have

$$\mathbb{E}(\mathcal{C}) = (q^k-1)^{-1}\sum_{i=1}^{n}(q^k - q^{k-1}) = n(q^k-q^{k-1})/(q^k-1) = q^{k-1}\ell.$$

Combining this with Lemma 3.1 we obtain

$$\begin{aligned}\mathrm{Var}(\mathcal{C}) &\geq \frac{q^{k-2}n(q-1)[n(q-1)+1]}{q^k-1} - q^{2k-2}\,\frac{n^2(q-1)^2}{(q^k-1)^2}\\ &= q^{k-2}\ell[n(q-1)+1] - \ell^2 q^{2k-2}\\ &= q^{k-2}\ell(1-\ell),\end{aligned}$$

as desired. □

Remark 3.4. The quantity $\mathbb{E}(\mathcal{C})$ in Notation 3.2 expresses the **average weight** of $\mathcal{C}$ and can be used to extend Theorem 1.6 as follows. Suppose that $\mathcal{C}$ is a nondegenerate $[n,k]_q$ code with maximum weight w. Using $\mathbb{E}(\mathcal{C}) \leq w$ one obtains

$$n \geq \left\lceil (n-w)\,\frac{q^k-1}{q^{k-1}-1}\right\rceil \geq (n-w)q+1.$$

In particular, if $\mathcal{C}$ is minimal then $w \leq n-k+1$ by Proposition 1.5, from which Theorem 1.6 follows.

As an immediate consequence of Theorem 3.3 we obtain the well-known fact that constant-weight codes have large length; see e.g. [15].

Corollary 3.5. Let $\mathcal{C}$ be a constant-weight $[n,k,d]_q$ code. Then $n \geq (q^k-1)/(q-1)$. Moreover, if $\mathcal{C}$ is projective then $n = (q^k-1)/(q-1)$ and $d = q^{k-1}$.

Proof. Without loss of generality, $\mathcal{C}$ is nondegenerate. By Theorem 3.3 we have $0 \geq q^{k-2}\ell(1-\ell)$, from which $\ell \geq 1$. If $\mathcal{C}$ is projective then $\ell = 1$ and so $d = \mathbb{E}(\mathcal{C}) = q^{k-1}$, as claimed. □

3.2 Bounds

By applying the result of the previous subsection, we can finally derive an upper bound for the minimum distance of a code $\mathcal{C}$ as a function of q, n, k and the maximum weight in $\mathcal{C}$.

Theorem 3.6. Let $\mathcal{C}$ be a nondegenerate $[n,k,d]_q$ code of maximum weight $w > d$. Let $\ell = n(q-1)/(q^k-1)$. We have $w > n(q^k-q^{k-1})/(q^k-1)$ and

$$d \leq \left\lfloor q^{k-1}\ell - \frac{q^{k-2}\ell(1-\ell)}{w-q^{k-1}\ell}\right\rfloor. \tag{3.2}$$

Moreover, equality holds in (3.2) if and only if $\mathcal{C}$ is a projective two-weight code.

Proof. The first inequality follows from the fact that $w > \mathbb{E}(\mathcal{C})$, since $\mathcal{C}$ is not constant-weight. Using the inequality of Bhatia–Davis [12] we obtain

$$\mathrm{Var}(\mathcal{C}) \leq (w-\mathbb{E}(\mathcal{C}))(\mathbb{E}(\mathcal{C})-d).$$

Since $\mathcal{C}$ is nondegenerate and not constant-weight we have $\mathbb{E}(\mathcal{C}) = q^{k-1}\ell < w$. Therefore we conclude by Theorem 3.3.

The second part of the statement follows from the fact that the bound of Theorem 3.3 is sharp if and only if $\mathcal{C}$ is projective, and that the Bhatia–Davis inequality is met with equality if and only if the underlying distribution takes only two values; see [12, Proposition 1]. □

As an application of Theorem 3.6 we obtain the following bound for the minimum distance of a minimal code.

Corollary 3.7. Let $\mathcal{C}$ be a minimal nondegenerate $[n,k,d]_q$ code. If $\mathcal{C}$ is not constant-weight, then $n-k+1 > n(q^k-q^{k-1})/(q^k-1)$ and

$$d \leq \left\lfloor \frac{n(q-1)q^{k-2}[n-1-q(k-1)]}{n(q^{k-1}-1)-(k-1)(q^k-1)} \right\rfloor. \tag{3.3}$$

In particular, we have

$$q^{k-2}n^2 - Bn + C \geq 0, \tag{3.4}$$

where

$$\begin{cases} B = q^{k-2} + (k-1)(2q^{k-1}-1) + \dfrac{q^{k-1}-1}{q-1}, \\ C = (k-1)^2(q^k-1) + \dfrac{(k-1)(q^k-1)}{q-1}. \end{cases}$$

Proof. The maximum weight of $\mathcal{C}$ satisfies $w \leq n-k+1$ by Proposition 1.5. Combining this with Theorem 3.6 one gets $n-k+1 > n(q^k-q^{k-1})/(q^k-1)$ and

$$d \leq \left\lfloor q^{k-1}\ell - \frac{q^{k-2}\ell(1-\ell)}{n-k+1-q^{k-1}\ell} \right\rfloor, \tag{3.5}$$

where $\ell = n(q-1)/(q^k-1)$. Lengthy computations show that the RHS of (3.5) is equal to the RHS of (3.3). The second part of the statement follows by combining (3.3) with Theorem 2.8, after lengthy computations. □

Example 3.8. There is no minimal $[16,4]_4$ code. To see this, observe that if such a code existed, then (3.4) would give $-42 \geq 0$, a contradiction. So the minimum length of a minimal code of dimension 4 over $\mathbb{F}_4$ is at least 17.

Consider the parameters $(q,n,k) = (4,17,4)$ and suppose that there exists an $[17,4]_4$ nondegenerate minimal code $\mathcal{C}$. Since $n < (q^k-1)/(q-1)$, $\mathcal{C}$ cannot be constant weight by Corollary 3.5. Therefore by Corollary 3.7 we conclude that $d \leq 10$. The existence of a minimal nondegenerate $[17,4,11]_4$ code is therefore excluded by Corollary 3.7, but it is not excluded by any of the other known bounds for the parameters of minimal codes. Note moreover that, by Theorem 2.8, we have $d \geq 10$. Therefore the minimum distance of a putative $[17,4]_4$ nondegenerate minimal code is exactly 10 (when the largest minimum distance of an "unrestricted" $[17,4]_4$ linear code is instead known to be 12).

Remark 3.9. The constraints imposed by Corollary 3.7 and Theorem 2.14 are in general incomparable. More precisely, each of the two results excludes the existence of some minimal codes that are not excluded by the other.

One can see that Corollary 3.7 improves on Theorem 2.14 if and only if (3.4) is violated when specialized to $n = (q+1)(k-1)$. After lengthy computations, one sees that this happens if and only if

$$k < \frac{q^{k-1} + 2q^{k-2} - 2q^{k-3} + q - 2}{(q^{k-3}+1)(q-1)}.$$

Manipulating this inequality it can be checked that Corollary 3.7 improves on Theorem 2.14 for the parameter set $\{(k,q) \mid 3 \leq k \leq q+3,\ q \geq 3\}$. When q is at least 3, this is an improvement also on Corollary 2.19. On the other hand, Theorem 2.14 provides a strictly sharper estimate than Corollary 3.7 if and only if (3.4) is satisfied for $n = (q+1)(k-1)-1$. For instance, this happens for the parameter set $\{(k,q) : k \geq 2q\}$.

We include in Table 1 three collections of parameter sets that are excluded by Theorem 2.14 and Corollary 3.7. The first column contains parameters that are excluded by both results, while the other two contain parameters that are excluded by either Theorem 2.14 or Corollary 3.7 (and not by both).

Some parameters of minimal codes excluded by both Theorem 2.14 and Corollary 3.7	Some parameters of minimal codes excluded by Theorem 2.14 and not by Corollary 3.7	Some parameters of minimal codes excluded by Corollary 3.7 and not by Theorem 2.14
$[8,4]_2$	$[17,7]_2$	$[16,5]_3$
$[15,5]_3$	$[31,9]_3$	$[16,4]_4$
$[24,6]_4$	$[44,10]_4$	$[25,6]_4$
$[35,7]_5$	$[99,21]_4$	$[36,7]_5$
$[63,9]_7$	$[65,12]_5$	$[26,4]_7$

Table 1: Code parameters for which the existence of minimal codes is excluded by Theorem 2.14 and/or Corollary 3.7.

3.3 Other Applications

In this short subsection we illustrate how Theorem 3.6 can be applied to study codes that are not necessarily minimal. We start with a generalization of Corollary 3.5. More precisely, we show that the relative difference between the maximum and minimum weight of a code, $(w-d)/n$, gives a lower bound on the code's length. In other words, if the maximum and minimum weight of a code are relatively close to each other, then the code length is necessarily large.

Proposition 3.10. Let $\mathcal{C}$ be a nondegenerate $[n,k,d]_q$ code of maximum weight w. We have

$$\frac{1}{n} \leq \frac{q-1}{q^k-1} + \frac{1}{4}\left(\frac{w-d}{n}\right)^2 \frac{q^k-1}{q^{k-2}(q-1)}.$$

Note that in the extreme case where $w = d$ we recover Corollary 3.5.

Proof of Proposition 3.10. Using Popoviciu's inequality for the variance, along with Theorem 3.3, we find

$$q^{k-2}\ell(1-\ell) \leq \mathrm{Var}(\mathcal{C}) \leq \frac{1}{4}(w-d)^2,$$

where $\ell = n(q-1)/(q^k-1)$. Re-arranging the terms, after tedious computations one obtains the desired inequality. □

A second application of Theorem 3.6 consists in obtaining constraints on the parameters of a code having few weights. A classical result about these codes is the following theorem by Delsarte.

Theorem 3.11 (see [21])**.** Let $\mathcal{C}$ be an $[n,k]_q$ code and let $s = |\{\omega(c) \mid c \in \mathcal{C},\, c \neq 0\}|$. We have

$$q^k \leq \sum_{i=0}^{s} \binom{n}{i} (q-1)^i.$$

Specializing to $s = 2$, the previous theorem shows that, for example, any two-weight $[n,k]_q$ code satisfies

$$q^k \leq 1 + n(q-1) + \frac{n(n-1)}{2}(q-1)^2. \tag{3.6}$$

This result however does not take into account *which* values the weight distribution can take. Exploiting this information, Theorem 3.6 provides in general different constraints on n than those in (3.6). We illustrate this with an example.

Example 3.12. Following the notation of Theorem 3.6 and Theorem 3.11, let $(q, k, s, d, w) = (2, 8, 2, 16, 24)$. We look for a nondegenerate binary two-weight code $\mathcal{C}$ of dimension 8 having weights 16 and 24. The constraints imposed on n by Theorem 3.6 imply $34 \leq n \leq 45$, where the upper bound is met with equality if $\mathcal{C}$ is projective. The constraint imposed by (3.6) is instead $n \geq 23$. It is known that there exists a projective binary two-weight code of parameters $(n, k, d, w) = (45, 8, 16, 24)$.

4 Geometric Approach

As already illustrated in Subsection 1.2, minimal codes are in one-to-one correspondence with cutting blocking sets. In this section we focus on this point of view on minimal codes, exploiting their geometric characterization to construct new, general and infinite families of minimal codes. In particular, we provide a construction of cutting blocking sets derived from Desarguesian $(r-1)$-spreads of $\mathrm{PG}(rt-1, q)$. In turn, this leads to a an inductive construction of small cutting blocking sets or, equivalently, of minimal codes with short length. In contrast to previous approaches, our construction works over any (possibly very small) finite field.

4.1 Minimal Codes from Spreads

We start by recalling the definition of t-spread in $\mathrm{PG}(k-1, q)$, which we will use to obtain a new construction of minimal codes. A t-**spread** S of $\mathrm{PG}(k-1, q)$ is a partition of $\mathrm{PG}(k-1, q)$ in t-flats. It is well known that such a t-spread exists if and only if $t+1$ divides k; see [34]. In particular, a 1-spread of $\mathrm{PG}(k-1, q)$ is a partition of its points into disjoint lines and it is also called a **linespread**. It exists if and only if k is even.

An algebraic representation of an $(r-1)$-spread of $\mathrm{PG}(2r-1, q)$ can be obtained as follows. Let $\gamma \in \mathbb{F}_{q^r}$ be a primitive element and let $M \in \mathbb{F}_q^{r\times r}$ be the companion matrix of the minimal polynomial of γ over $\mathbb{F}_q$. It is well known that $\mathbb{F}_{q^r} \cong \mathbb{F}_q[\gamma] \cong \mathbb{F}_q[M] = \{0\} \cup \{M^i : 1 \leq i \leq q^r - 1\}$ as $\mathbb{F}_q$-algebras. For $i \in [q^r - 1]$ define $V_i := \{[x : xM^i] \mid x \in \mathrm{PG}(r-1, q)\}$, $V_0 := \{[x : 0] \mid x \in \mathrm{PG}(r-1, q)\}$ and $V_{q^r} := \{[0 : y] \mid y \in \mathrm{PG}(r-1, q)\}$. Then the set $\{V_0, \ldots, V_{q^r}\}$ is an $(r-1)$-spread of $\mathrm{PG}(2r-1, q)$.

Theorem 4.1. Let S be the $(r-1)$-spread of $\mathrm{PG}(2r-1, q)$ defined above and let $\mathcal{B} = V_0 \cup V_i \cup V_j \cup V_{q^r} \subseteq \mathrm{PG}(2r-1, q)$, with $0 < i < j < q^r$. Suppose that for every $s > 1$ dividing r we have $j - i \not\equiv 0 \mod \left(\frac{q^s-1}{q-1}\right)$. Then $\mathcal{B}$ is a cutting blocking set.

Proof. For ease of exposition we switch to vector notation, in which we represent V_0, V_i, V_j, V_{q^2} as elements of the Grassmannian $\mathrm{Gr}_q(r, 2r)$. In this representation we have $V_0 = \mathrm{rowsp}(I_r \mid 0)$, $V_{q^r} = \mathrm{rowsp}(0 \mid I_r)$, $V_i = \mathrm{rowsp}(I_r \mid M^i)$ and $V_j = \mathrm{rowsp}(I_r \mid M^j)$. Let H be a hyperplane in $\mathbb{F}_q^{2r}$. We want to show that $\langle H \cap \mathcal{B} \rangle = H$, or, equivalently, that $\langle H \cap \mathcal{B} \rangle = \langle H \cap V_0 \rangle + \langle H \cap V_{q^r} \rangle + \langle H \cap V_i \rangle + \langle H \cap V_j \rangle$ has dimension at least $2r-1$. Observe first that if H contains one among the V_ℓ's, say V_0, then there is nothing to prove, since $\langle H \cap V_0 \rangle + \langle H \cap V_i \rangle$ has already dimension (at least) $2r-1$. Hence we can assume that H intersect both V_0 and V_{q^r} in an $(r-1)$-dimensional subspace. Then the space $\langle H \cap V_0 \rangle + \langle H \cap V_{q^r} \rangle$ has dimension $2r-2$. We can write the intersection spaces as

$$\begin{array}{lcl@{\qquad\qquad}lcl} H \cap V_0 & = & \mathrm{rowsp}(\ X_1 \mid\ 0\ \ ), & H \cap V_i & = & \mathrm{rowsp}(X_2 \mid X_2M^i), \\ H \cap V_{q^r} & = & \mathrm{rowsp}(\ \ 0\ \ \mid X_3\ ), & H \cap V_j & = & \mathrm{rowsp}(X_4 \mid X_4M^j), \end{array}$$

for some $X_1, X_2, X_3, X_4 \in \mathbb{F}_q^{(r-1)\times r}$ of rank $r-1$.

Suppose by contradiction that $\langle H \cap \mathcal{B} \rangle$ has dimension exactly $2r-2$. This implies

$$\mathrm{rowsp}\begin{pmatrix} X_2 & X_2M^i \\ X_4 & X_4M^j \end{pmatrix} \subseteq \mathrm{rowsp}\begin{pmatrix} X_1 & 0 \\ 0 & X_3 \end{pmatrix},$$

which in turn implies $\mathrm{rowsp}(X_2) = \mathrm{rowsp}(X_4) = \mathrm{rowsp}(X_1)$ and $\mathrm{rowsp}(X_3) = \mathrm{rowsp}(X_2M^i) = \mathrm{rowsp}(X_4M^j)$. Without loss of generality, we can assume that $X_1 = X_2 = X_4 =: X$, which reduces the above condition to

$$\mathrm{rowsp}(X_3) = \mathrm{rowsp}(XM^i) = \mathrm{rowsp}(XM^j).$$

Thus, there exists a matrix $A \in \mathrm{GL}(r-1, q)$ such that

$$AX - XM^{j-i} = 0. \tag{4.1}$$

The matrix equation in (4.1), where the matrix X is the unknown, is a *Sylvester equation*. This is known to have a unique solution if the minimal polynomials of A and M^{j-i} are coprime; see e.g. [25, Theroem 2.4.4.1]. Observe that the minimal polynomial of M^{j-i} is irreducible of degree r, since M^{j-i} corresponds to the element γ^{j-i} and by the assumption on $j-i$ in the statement we have $\mathbb{F}_q[\gamma^{j-i}] = \mathbb{F}_{q^r}$. Moreover, the minimal polynomial of A has degree at most $r-1$, and hence it is coprime with the one of M^{j-i}'s. Therefore (4.1) has a unique solution, which is clearly $X = 0$. This leads to a contradiction and concludes the proof. □

We now concentrate on the more general case of $(r-1)$-spreads in $\mathrm{PG}(rt-1, q)$. These can be constructed using the so-called **field reduction**; see [28, 34]. This technique identifies points in $\mathrm{PG}(t-1, q^r)$ with $(r-1)$-flats in $\mathrm{PG}(rt-1, q)$. The idea is exactly the same as for the algebraic $(r-1)$-spread of $\mathrm{PG}(2r-1, q)$ described above. Let γ be a primitive element in $\mathbb{F}_{q^r}$ and let M be the companion matrix of the minimal polynomial of γ over $\mathbb{F}_q$. As already explained, there is an isomorphism $\mathbb{F}_{q^r} \cong \mathbb{F}_q[M] = \{0\} \cup \{M^i : 1 \le i \le q^r - 1\}$, which we call ϕ. We can then extend it to vectors in $\mathbb{F}_{q^r}^t$ componentwise, obtaining an injective map

$$\begin{array}{rcl} \varphi : \mathbb{F}_{q^r}^t & \longrightarrow & \mathbb{F}_q^{r \times rt} \\ (v_1, \ldots, v_t) & \longmapsto & (\phi(v_1) \mid \ldots \mid \phi(v_t)). \end{array}$$

This map can in turn be extended to a map $\bar{\varphi} : \mathrm{PG}(t-1, q^r) \longrightarrow \mathrm{Gr}_q(r, tr)$, the Grassmannian, defined by $P = [v] \longmapsto \mathrm{rowsp}(\varphi(v))$. Note that $\bar{\varphi}$ is well-defined since it does not depend on the choice of the representative v for the point P. Indeed, for a nonzero scalar multiple of v, say $\gamma^i v$, we have $\varphi(\gamma^i v) = M^i \varphi(v)$ and since M^i is invertible, $\mathrm{rowsp}(M^i\varphi(v)) = \mathrm{rowsp}(\varphi(v))$. It is then well-known that $\mathrm{Im}(\bar{\varphi})$ is a (vectorial) r-spread of $\mathbb{F}_q^{rt}$, which naturally gives rise to a projective $(r-1)$-spread of $\mathrm{PG}(rt-1, q)$. Such a spread is known as **Desarguesian spread**; see [34].

In the sequel we will need the following special points in $\mathrm{PG}(t-1, q^r)$: $P_\ell := [e_\ell]$ for $\ell \in [t]$ and $Q_{\ell,m,i} := [u_{\ell,m,i}]$, where $u_{\ell,m,i} := e_\ell + \gamma^i e_m$ for $1 \le \ell < m \le t$ and $i \in [q^r - 1]$. These will be used in the next result to extend the construction of Theorem 4.1 from two to t **blocks**.

Theorem 4.2. For each pair of integers (ℓ, m) such that $1 \le \ell < m \le t$, let $j_{\ell,m}, i_{\ell,m} \in [q^r - 1]$ be integers with the following property: for all $s > 1$ dividing r, $j_{\ell,m} - i_{\ell,m} \not\equiv 0 \mod \left(\frac{q^s-1}{q-1}\right)$. Define the set

$$\mathcal{T} := \left(\bigcup_{1 \le \ell \le t} \bar{\varphi}(P_\ell) \right) \cup \left(\bigcup_{1 \le \ell < m \le t} (\bar{\varphi}(Q_{\ell,m,i_{\ell,m}}) \cup \bar{\varphi}(Q_{\ell,m,j_{\ell,m}})) \right).$$

Then the projectivization of $\mathcal{T}$ is a cutting blocking set in $\mathrm{PG}(rt-1, q)$.

Proof. Once again we work in vector notation. Let H be a hyperplane in $\mathbb{F}_q^{rt}$. Let $a := |\{\ell : \bar{\varphi}(P_\ell) \subseteq H\}|$. Then $0 \le a \le t-1$ and $\dim(\langle H \cap \mathcal{T} \rangle) \ge ra + (r-1)(t-a)$. Without loss of generality assume that $\{\ell : \bar{\varphi}(P_\ell) \subseteq H\} = [a]$. Hence $\langle H \cap \mathcal{T} \rangle$ contains the span of the first $a \cdot r$ standard basis vectors. By taking the quotient on this span, we reduce ourselves to proving the same statement for $a = 0$, replacing t by $t - a$. Therefore we can also assume $a = 0$ without loss of generality.

We have that $\Lambda := \langle H \cap \left(\bigcup_\ell \bar{\varphi}(P_\ell)\right)\rangle$ has dimension $(r-1)t$. For all integers $1 \le \ell < m \le t$, define

$$\mathcal{S}_{\ell,m} := \bar{\varphi}(P_\ell) \cup \bar{\varphi}(P_m) \cup \bar{\varphi}(Q_{\ell,m,i_{\ell,m}}) \cup \bar{\varphi}(Q_{\ell,m,j_{\ell,m}}),$$
$$\Pi_{\ell,m} := \langle \bar{\varphi}(P_\ell) \cup \bar{\varphi}(P_m)\rangle = \langle e_i : (\ell-1)r+1 \le i \le \ell r, \text{ or } (m-1)r \le i \le mr\rangle.$$

Then $H \cap \Pi_{\ell,m}$ is a hyperplane in $\Pi_{\ell,m} \cong \mathbb{F}_q^{2r}$. Moreover, using the same argument as in the proof of Theorem 4.1, there exists a vector $v_{\ell,m} \in (H \cap \Pi_{\ell,m}) \cap \mathcal{S}_{\ell,m} \subseteq H \cap \mathcal{S}_{\ell,m}$ such that $v_{\ell,m} \notin \langle H \cap (\bar{\varphi}(P_\ell) \cup \bar{\varphi}(P_m))\rangle$. Observe that the support of $v_{\ell,m}$ is contained only in the ℓ-th and the m-th blocks and that we can write $v_{\ell,m} = w_{\ell,m}^{(\ell)} + w_{\ell,m}^{(m)}$, where $w_{\ell,m}^{(j)} \in \langle \bar{\varphi}(P_j)\rangle$, i.e., it has support contained only in the j-th block, for $j \in \{\ell, m\}$. Now consider the $t-1$ vectors $v_{1,2}, \dots, v_{1,t}$. Since $a = 0$, none of the $v_{1,i}$'s belongs to Λ. It is left to show that for each $i \ge 3$ we have $v_{1,i} \notin \Gamma_{i-1} := \Lambda + \langle v_{1,2}, \dots, v_{1,i-1}\rangle$. By contradiction, suppose that $v_{1,i} \in \Gamma_{i-1}$. Let $\rho_i : \mathbb{F}_q^{rt} \to \mathbb{F}_q^r$ denote the projection on the i-th block. We have

$$w_{1,i}^{(i)} = \rho_i(v_{1,i}) \in \rho_i(\Gamma_i) = \langle H \cap \bar{\varphi}(P_i)\rangle,$$

since, by construction, the i-th block of any vector in Γ_{i-1} is equal to the i-th block of some element in $\bar{\varphi}(P_i) \cap H$. Therefore, also the vector $w_{1,i}^{(1)} = v_{1,i} - w_{1,i}^{(i)}$ belongs to H. This means that $v_{1,i} \in H \cap (\bar{\varphi}(P_1) \cup \bar{\varphi}(P_i)) \subseteq \Lambda$, which leads to a contradiction. □

Remark 4.3. The construction of Theorem 4.2 for $r = t = 2$ (or, equivalently, the one of Theorem 4.1 for $r = 2$) coincides with the construction of cutting blocking sets of [19, Theorem 3.7], which consists of 4 disjoint lines in $\mathrm{PG}(3, q)$. Therefore, Theorem 4.2 can be viewed as a generalization of that result.

Example 4.4. We explicitly construct a cutting blocking set in $\mathrm{PG}(5, q)$ as explained in Theorem 4.2, with $r = 2$ and $t = 3$. We take as γ a primitive element of $\mathbb{F}_{q^2}$ whose minimal polynomial over $\mathbb{F}_q$ is $x^2 - p_1x - p_0$. We have $P_1 = [1:0:0]$, $P_2 = [0:1:0]$, $P_3 = [0:0:1]$ and choose the following points in $\mathrm{PG}(2, q^2)$: $Q_{1,2,q^2-1} = [1:1:0]$, $Q_{1,2,1} = [1:\gamma:0]$, $Q_{1,3,q^2-1} = [1:0:1]$, $Q_{1,3,1} = [1:0:\gamma]$, $Q_{2,3,q^2-1} = [0:1:1]$, $Q_{2,3,1} = [0:1:\gamma]$. Therefore the set $\mathcal{T}$ is

$$\begin{aligned}\mathcal{T} = &\{(x,y,0,0,0,0) : x,y \in \mathbb{F}_q\} \cup \{(0,0,x,y,0,0) : x,y \in \mathbb{F}_q\} \cup \{(0,0,0,0,x,y) : x,y \in \mathbb{F}_q\}\\
&\cup \{(x,y,x,y,0,0) : x,y \in \mathbb{F}_q\} \cup \{(x,y,y,p_0x+p_1y,0,0) : x,y \in \mathbb{F}_q\}\\
&\cup \{(x,y,0,0,x,y) : x,y \in \mathbb{F}_q\} \cup \{(x,y,0,0,y,p_0x+p_1y) : x,y \in \mathbb{F}_q\}\\
&\cup \{(0,0,x,y,x,y) : x,y \in \mathbb{F}_q\} \cup \{(0,0,x,y,y,p_0x+p_1y) : x,y \in \mathbb{F}_q\}.\end{aligned}$$

The projectivization of $\mathcal{T}$ gives the desired cutting blocking set in $\mathrm{PG}(5, q)$.

4.2 Inductive Constructions of Cutting Blocking Sets

As already observed in the Introduction, of particular interest is the study minimal codes of small length for a given dimension. Formally, for a fixed positive integer k and a prime power q, we are interested in determining the value of

$$m(k,q) := \min\{n \in \mathbb{N}_{\ge 1} \mid \text{ there exists a minimal } [n,k]_q \text{ code}\}.$$

This function has been explicitly studied in [30], where it was observed that $m(2,q) = q+1$ and that

$$q(k-1)+1 \le m(k,q) \le (q-1)\binom{k}{2} + k, \tag{4.2}$$

where the upper bound is *constructive* (the tetrahedron from page 6). The same results were independently obtained in [1], where shorter minimal codes are constructed for $k \in \{3,4,5\}$. In this notation, Theorem 2.14 improves on the lower bound in (4.2), reading

$$m(k,q) \geq (q+1)(k-1).$$

We already obtained improvements on this bound in Corollary 2.19 and Corollary 3.7, as shown in Table 1.

In [17] it has been shown that the upper bound on $m(k,q)$ in (4.2) is far from being tight. More precisely, one has

$$m(k,q) \leq \frac{2k}{\log_q\left(\frac{q^2}{q^2-q+1}\right)}, \tag{4.3}$$

indicating that, in principle, for a fixed q and k large enough one might construct much shorter minimal codes. In particular, a natural problem is that of finding, for a fixed q, an infinite family of minimal codes over $\mathbb{F}_q$ whose length is linear in k. This problem is naturally motivated by the goal of *explicitly* constructing asymptotically good minimal codes. Indeed, while these codes are known to be asymptotically good, the proofs in [1,18] are not constructive, as well as the bound in (4.3). We are currently unaware of any *explicit* general construction of minimal codes whose length is unbounded for a *fixed* q, and that are asymptotically shorter than the tetrahedron; see also the discussion in Remark 1.15.

In the sequel, we introduce two new families of minimal codes whose lengths are shorter than the one of the tetrahedron by a factor 2 and by a factor $\frac{9}{4}$, respectively. We start with a result that represents a first step towards inductive constructions of cutting blocking sets.

Proposition 4.5. Let $\mathcal{B} = \mathcal{B}_1 \cup \ldots \cup \mathcal{B}_r$ be a cutting blocking set in $\mathrm{PG}(N,q)$. For each $i \in [r]$, let $\Gamma_i := \langle \mathcal{B}_i \rangle \cong \mathrm{PG}(n_i,q)$ for some $n_i \leq N$ and let $\mathcal{B}'_i \subseteq \Gamma_i$ be the isomorphic image of a cutting blocking set in $\mathrm{PG}(n_i,q)$. Then $\mathcal{B}' := \mathcal{B}'_1 \cup \ldots \cup \mathcal{B}'_r$ is a cutting blocking set.

Proof. Let H be a hyperplane in $\mathrm{PG}(N,q)$. We want to show that $\langle H \cap \mathcal{B}' \rangle = H$. By hypothesis we have that

$$H = \langle H \cap \mathcal{B} \rangle = \langle H \cap \mathcal{B}_1 \rangle + \ldots + \langle H \cap \mathcal{B}_r \rangle.$$

Consider the spaces $\Lambda_i := H \cap \langle \mathcal{B}_i \rangle$, $i \in [r]$. Clearly, $\Lambda_i \supseteq \langle H \cap \mathcal{B}_i \rangle$ for all i. We now examine two cases separately.

Case I: $\Lambda_i = \langle \mathcal{B}_i \rangle$, that is, H contains $\langle \mathcal{B}_i \rangle$. In this case H also contains $\mathcal{B}'_i$ and $\langle H \cap \mathcal{B}'_i \rangle = \langle \mathcal{B}'_i \rangle = \langle \mathcal{B}_i \rangle = \Lambda_i$.

Case II: Λ_i is a hyperplane in $\langle \mathcal{B}_i \rangle$. By hypothesis, $\mathcal{B}'_i$ is a cutting blocking set in $\langle \mathcal{B}_i \rangle$, and hence $\langle H \cap \mathcal{B}'_i \rangle \supseteq \langle \Lambda_i \cap \mathcal{B}'_i \rangle = \Lambda_i$.

Therefore in both cases we have

$$\begin{aligned} \langle H \cap \mathcal{B}' \rangle &= \langle H \cap \mathcal{B}'_1 \rangle + \ldots + \langle H \cap \mathcal{B}'_r \rangle \supseteq \Lambda_1 + \ldots + \Lambda_r \\ &\supseteq \langle H \cap \mathcal{B}_1 \rangle + \ldots + \langle H \cap \mathcal{B}_r \rangle = H, \end{aligned}$$

concluding the proof. □

We are now ready to combine the above result with Theorem 4.2 and derive a recursive upper bound on $m(k,q)$.

Theorem 4.6. For all positive $a, b \in \mathbb{N}$,

$$m(ab,q) \leq a^2 m(b,q).$$

Proof. By Theorem 4.2 we know that we can construct a cutting blocking set in $\mathrm{PG}(ab-1,q)$ with the aid of a $(b-1)$-spread. More precisely, we only need to take a^2 disjoint $(b-1)$-flats $\Gamma_1,\dots,\Gamma_{a^2}\cong\mathrm{PG}(b-1,q)$ from the spread. By Proposition 4.5, for each of them we can take the isomorphic image of a cutting blocking set in $\mathrm{PG}(b-1,q)$ with minimum cardinality $m(b,q)$. Therefore, we finally obtain a cutting blocking set in $\mathrm{PG}(ab-1,q)$ of cardinality $a^2m(b,q)$. □

Observe that the proof of Theorem 4.6 gives an explicit way of constructing a minimal $[a^2m(b,q),ab]_q$ code, provided that there exists already a construction for an $[m(b,q),b]_q$ minimal code. We illustrate how this construction works with the following example.

Example 4.7. We fix $k=6=3\cdot 2$ and assume q to be a square. Observe that under these assumptions we know the exact values of $m(2,q)$ and $m(3,q)$; see Section 1.2. Namely, we have $m(2,q)=q+1$ and

$$m(3,q)=\begin{cases}3q & \text{if } q=4,\\ 2(q+\sqrt{q}+1) & \text{if } q\geq 9.\end{cases}$$

Now we can use Theorem 4.6 in two ways. On the one hand, we deduce that

$$m(6,q)\leq 9\cdot m(2,q)=9(q+1).$$

Such a construction is obtained by taking 9 lines from a linespread in $\mathrm{PG}(5,q)$ as explained also in Example 4.4. On the other hand, by interchanging the roles of 2 and 3 we obtain

$$m(6,q)\leq 4\cdot m(3,q)=\begin{cases}12(q+1) & \text{if } q=4,\\ 8(q+\sqrt{q}+1) & \text{if } q\geq 9.\end{cases}$$

The corresponding cutting blocking set is constructed by first selecting 4 planes in $\mathrm{PG}(5,q)$ via Theorem 4.1, and then by choosing, in each of these planes, a minimal 2-fold blocking set: when $q=4$, we take 3 lines not intersecting all in the same point; when $q\geq 9$, we choose 2 disjoint Baer subplanes. It is easy to check that for $q<64$ the cutting blocking set consisting of 9 lines is smaller, while for $q\geq 64$ the 8 Baer subplanes give rise to a cutting blocking set with smaller cardinality. Notice that both constructions produce a smaller cutting blocking set than the tetrahedron, which contains $15q-9$ points. For instance, let us consider the case $q=4$. The 9 lines give rise to a minimal $[45,6]_4$ code, the 8 Baer subplanes lead to a minimal $[56,6]_4$ code, while the tetrahedron provides a $[66,4]_4$ code. If we take $q=64$, then the three constructions produce minimal codes whose parameters are $[585,6]_{64}$, $[584,6]_{64}$ and $[966,6]_{64}$, respectively.

Remark 4.8. Very recently, a construction of cutting blocking sets in $\mathrm{PG}(5,q)$ as union of seven disjoint lines has been given in [10]. This gives an improvement on the known upper bound for $m(6,q)$. In the same work, a construction of a cutting blocking set in $\mathrm{PG}(3,q^3)$ of size $3(q^3+q^2+q+1)$ has been obtained as union of three suitable disjoint q-order subgeometries. These results together yield the following bounds:

$$m(4,q^3)\leq 3(q^3+q^2+q+1),$$
$$m(6,q)\leq 7(q+1).$$

The proof of Theorem 4.6, which constructs minimal codes of dimension $k=ab$, heavily relies on the existence of a smaller minimal code, whose dimension divides k. Clearly, this recursive construction does not cover all dimensions, as for instance it does not provide any nontrivial minimal code of prime dimension. While for $k=5$ one can rely on the construction provided in [1, Construction 2], which gives a $[8q-3,5]_q$ minimal code, for primes greater than 5 we are not (yet) able to construct any *short* minimal code different from the tetrahedron. Also, we are not (yet) able to construct short minimal codes of odd dimension, unless the latter is divisible by 3 and q is a square. When k is odd one can construct minimal codes taking several

$(r-1)$-flats in $\mathrm{PG}(k-1,q)$, where r is the smallest prime dividing k. However, when such a prime is big, the resulting code turns out to be quite long.

The discussion in the previous paragraph motivates us to look for alternative constructions of minimal codes, with the ultimate goal of covering a larger dimension range. Our next move in this direction is an inductive result that allows us to construct a cutting blocking set in $\mathrm{PG}(k,q)$ starting from a smaller one in $\mathrm{PG}(k-1,q)$. The following result has already been shown in [19, Construction A]. We include a proof for completeness.

Proposition 4.9 (see [19, Theorem 3.10])**.** Let $\mathcal{B}'$ be a cutting blocking set in $\mathrm{PG}(k-1,q)$. Fix a hyperplane $\Lambda \subseteq \mathrm{PG}(k,q)$ and take an isomorphic image $\mathcal{T}$ of $\mathcal{B}'$ in Λ. Moreover, select k points $P_1,\dots,P_k \in \langle \mathcal{T} \rangle$ not lying all in the same $(k-2)$-flat and a point $P \in \mathrm{PG}(k,q) \setminus \Lambda$. Define the lines $\ell_i := \langle P_i, P \rangle$. Then the set

$$\mathcal{B} := \mathcal{T} \cup \left(\bigcup_{i=1}^{k} \ell_i \setminus \{P_i\} \right)$$

is a cutting blocking set in $\mathrm{PG}(k,q)$. In particular, for every $k \in \mathbb{N}_{\geq 1}$ we have

$$m(k+1,q) \leq m(k,q) + (q-1)k + 1.$$

Proof. Let H be a hyperplane in $\mathrm{PG}(k,q)$. If $H = \Lambda$, then clearly $\langle H \cap \mathcal{B} \rangle = H$. If $H \neq \Lambda$, then we have that $\Lambda_0 := H \cap \Lambda$ is a hyperplane in Λ. Hence $\langle H \cap \mathcal{T} \rangle = \langle \Lambda_0 \cap \mathcal{T} \rangle = \Lambda_0$. Moreover, H meets each of the lines ℓ_i's in a point Q_i. Observe that not all of them can lie in Λ, because otherwise we would have $Q_i = P_i$ for every i and $H = \Lambda$. Therefore, there exists a point $Q_i \in (\ell_i \cap H) \setminus \langle \mathcal{T} \rangle$. This implies that $Q_i \in \langle H \cap \mathcal{B} \rangle \setminus \Lambda_0$ and we can conclude that $\langle H \cap \mathcal{B} \rangle = H$. □

Proposition 4.9 shows how to construct a cutting blocking set in $\mathrm{PG}(k,q)$ which contains a copy of a cutting blocking set $\mathcal{T}$ in $\mathrm{PG}(k-1,q)$. This is achieved by adding $(q-1)k+1$ points to $\mathcal{T}$. Moreover, among cutting blocking sets containing a copy of a smaller cutting blocking set (of codimension 1), the construction of Proposition 4.9 is optimal, as shown by the following result.

Proposition 4.10. Let $\mathcal{B} \subseteq \mathrm{PG}(k,q)$ be a cutting blocking set such that it contains (an isomorphic image of) a cutting blocking set $\mathcal{B}'$ of $\mathrm{PG}(k-1,q)$. Then

$$|\mathcal{B}| \geq |\mathcal{B}'| + (q-1)k + 1.$$

Proof. Let $\mathcal{B}$ be a cutting blocking set in $\mathrm{PG}(k,q)$ and suppose it contains a copy $\mathcal{B}'$ of a cutting blocking set in $\mathrm{PG}(k-1,q)$. Then $\mathcal{B}'$ is contained in a hyperplane H. By the correspondence between linear codes and projective systems (see page 5) we have

$$d \leq |\mathcal{B}| - |\mathcal{B} \cap H| \leq |\mathcal{B}| - |\mathcal{B}'|.$$

Combining this with Theorem 2.8 we obtain the desired inequality. □

Remark 4.11. Proposition 4.10 shows that the inductive construction from Proposition 4.9 gives rise to a cutting blocking set that is minimal among all the cutting blocking sets containing a given cutting blocking set of codimension 1. It is interesting to observe that starting from $\mathrm{PG}(1,q)$ and iterating this construction k times, one obtains the tetrahedron, which is, therefore, minimal among the cutting blocking sets in $\mathrm{PG}(k-1,q)$ containing an isomorphic copy of a cutting blocking set of $\mathrm{PG}(i,q)$ for each $i \leq k-2$. Note that its cardinality is $\sim \frac{1}{2}qk^2$ for k large.

All of this seems to suggest that in order to obtain cutting blocking sets in $\mathrm{PG}(k-1,q)$ of size $m(k,q)$ (or at least linear in k) one should look at sets that do not contain (isomorphic copies of) smaller cutting blocking sets.

4.3 Explicit Constructions of Short Minimal Codes

In this final subsection we combine the results obtained so far to construct minimal codes of short length. To our best knowledge, this constructions produce the shortest known minimal codes, for infinitely many dimensions and field sizes. In particular, the construction applies to all those pairs (k, q) for which the rational normal tangent set of [23] cannot be constructed in $\mathrm{PG}(k-1, q)$.

Construction A. Assume that $k = 2t$, for some $t \in \mathbb{N}_{\geq 1}$. We use the construction from Theorem 4.2, selecting $t^2 = \frac{k^2}{4}$ disjoint lines from a linespread. The union of these t^2 lines a cutting blocking set in $\mathrm{PG}(k-1, q)$, and we denote the corresponding code by $\mathcal{C}_{k,q}$.

Proposition 4.12. The code $\mathcal{C}_{k,q}$ of Construction A is a minimal $[(q+1)\frac{k^2}{2}, k, q(k-1)]_q$ code.

Proof. The minimality of $\mathcal{C}_{k,q}$ trivially follows from the fact that the associated projective system is a cutting blocking set; see Theorem 4.2. The length of the code $\mathcal{C}_{k,q}$ coincides with the cardinality of the cutting blocking set, which is $(q+1)\frac{k^2}{4}$. Therefore it remains to show that $d = q(k-1)$. By the correspondence between projective systems and linear codes and Definition 1.8, we have that $d = n - s = (q+1)t^2 - s$, where $k = 2t$ and

$$s := \max\{|\bar{H} \cap \bar{\mathcal{T}}| \,:\, \bar{H} \subseteq \mathrm{PG}(k-1, q),\, \dim(\bar{H}) = k-2\},$$

where $\bar{\mathcal{T}}$ is the projectivization of the set $\mathcal{T}$ defined in Theorem 4.2. We switch to vector notation and let $\mathcal{A}_{\ell,m} = \{\bar{\varphi}(P_\ell), \bar{\varphi}(P_m), \bar{\varphi}(Q_{\ell,m,i_{\ell,m}}), \bar{\varphi}(Q_{\ell,m,j_{\ell,m}})\}$ for all $1 \leq \ell < m \leq t$. Let H be a hyperplane of $\mathbb{F}_q^k = \mathbb{F}_q^{2t}$. Define the set $H_{\mathcal{T}} := \{i : \bar{\varphi}(P_i) \subseteq H\}$ and the integers $a := |H_{\mathcal{T}}|$ and $a_{\ell,m} := |\{A \in \mathcal{A}_{\ell,m} : A \subseteq H\}|$ for $1 \leq \ell < m \leq t$. Moreover, let b denote the number of lines forming $\bar{\mathcal{T}}$ that are fully contained in the projectivization $\bar{H}$ of H. Since each of the lines forming $\bar{\mathcal{T}}$ either intersects $\bar{H}$ in a point, or it is contained in $\bar{H}$, we have

$$s = (q+1)b + t^2 - b = qb + t^2. \tag{4.4}$$

Therefore, finding the maximum of s is the same as finding the maximum value of b. Now observe that a cannot be equal to t, as otherwise H would contain a basis of $\mathbb{F}_q^{2t}$. Moreover, we have that $a_{\ell,m} \in \{0, 1, 4\}$. Indeed, by construction, any two subspaces in $\mathcal{A}_{\ell,m}$ span the same 4-dimensional subspace, and if H contains two of them, then it contains all of them. It is readily seen that we have

$$\begin{aligned} b &= a + \sum_{\substack{\ell,m \in H_{\mathcal{T}},\\ \ell<m}} (a_{\ell,m} - 2) + \sum_{\substack{\ell \in H_{\mathcal{T}}, m \notin H_{\mathcal{T}},\\ \ell<m}} (a_{\ell,m} - 1) + \sum_{\substack{\ell \notin H_{\mathcal{T}}, m \in H_{\mathcal{T}},\\ \ell<m}} (a_{\ell,m} - 1) + \sum_{\substack{\ell,m \notin H_{\mathcal{T}},\\ \ell<m}} (a_{\ell,m}) \\ &= a + \sum_{\substack{\ell,m \in H_{\mathcal{T}},\\ \ell<m}} 2 + \sum_{\substack{\ell,m \notin H_{\mathcal{T}},\\ \ell<m}} (a_{\ell,m}) \leq a + \binom{a}{2} + \binom{t-a}{2} = a^2 + \binom{t-a}{2} =: f_t(a), \end{aligned}$$

where the second equality and the inequality both follow from the fact that $a_{\ell,m}$ can only be equal to $0, 1$ or 4. The function f_t is a quadratic polynomial in a with second derivative equal to $3 > 0$. Hence, the maximum in the interval $[0, t-1]$ is attained in one of the two interval extremes. One can see that this happens when $a = t-1$, from which $b \leq (t-1)^2$. Finally, combining this with (4.4) we have $s = qb + t^2 \leq q(t-1)^2 + t^2 = (q+1)t^2 - q(2t-1)$ and $d \geq (q+1)t^2 - s = q(2t-1) = q(k-1)$.

On the other hand, we can take any hyperplane H' containing $\bar{\varphi}(P_i)$, for each $i \in [t-1]$. The projectivization of such a hyperplane contains exactly $b = (t-1)^2$ lines forming $\bar{\mathcal{T}}$, and therefore $n - |\bar{H}' \cap \bar{\mathcal{T}}| = q(k-1)$. ∎

Example 4.13. Let $k = 6$ and take the cutting blocking set obtained in Example 4.4. This is a cutting blocking set arising from Construction A. When $q = 2$, we take γ to be a root of $x^2 + x + 1$ and obtain a minimal $[27, 6]_2$ code $\mathcal{C}_{6,2}$ whose generator matrix is

$$\begin{pmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0
\end{pmatrix}.$$

Our second construction combines Theorem 4.2 with the concept of a Baer subplane.

Construction B. Assume that $k = 3t$ for some $t \in \mathbb{N}$ and that q is a square. We first use the construction from Theorem 4.2 by selecting $t^2 = \frac{k^2}{9}$ disjoint planes from a 2-spread. Then we choose two disjoint Baer subplanes in each of these planes. The union of the selected $2t^2$ Baer subplanes is a cutting blocking set in $\mathrm{PG}(k-1, q)$, and we denote the corresponding code by $\mathcal{D}_{k,q}$.

Proposition 4.14. The code $\mathcal{D}_{k,q}$ of Construction B is a minimal $[(q+\sqrt{q}+1)\frac{2k^2}{9}, k, d]_q$ code, where $d \geq q\big(\frac{4}{3}k - 2\big)$.

Proof. The minimality of $\mathcal{D}_{k,q}$ trivially follows from the fact that the associated projective system $\mathcal{B}$ is a cutting blocking set (Theorem 4.2 and Proposition 4.5). The length of the code $\mathcal{D}_{k,q}$ coincides with the cardinality of the cutting blocking set, which is $(q+\sqrt{q}+1)\frac{2k^2}{9}$. We only need to prove that $d \geq q\big(\frac{4}{3}k - 2\big)$. We let $k = 3t$ and proceed as before, finding an upper bound on

$$s := \max\{|\bar{H} \cap \mathcal{B}| \,:\, \bar{H} \subseteq \mathrm{PG}(k-1, q),\, \dim(\bar{H}) = k-2\}.$$

Observe that $\mathcal{B}$ is obtained by first forming the cutting blocking set $\bar{\mathcal{T}}$ as in Theorem 4.2, which is the union of t^2 planes $\Lambda_1, \ldots, \Lambda_{t^2}$, and then selecting two disjoint Baer subplanes $\mathcal{B}_{i,1}, \mathcal{B}_{i,2}$ in each Λ_i. Let $\bar{H}$ be a hyperplane in $\mathrm{PG}(k-1, q)$ and let b denote the number of planes Λ_i that are fully contained in $\bar{H}$. With this notation, we have

$$\begin{aligned}
|\mathcal{B} \cap \bar{H}| &= 2b(q+\sqrt{q}+1) + \sum_{i\,:\,\Lambda_i \not\subseteq \bar{H}} |\mathcal{B}_{i,1} \cap \bar{H}| + |\mathcal{B}_{i,2} \cap \bar{H}| \\
&\leq 2(q+\sqrt{q}+1)b + 2(\sqrt{q}+1)(t^2 - b), \qquad (4.5)
\end{aligned}$$

where the last inequality follows from the fact that a hyperplane $\bar{H}$ meets a Baer subplane in either 1, $\sqrt{q}+1$ or $q+\sqrt{q}+1$ points. Moreover, arguing as in the proof of Proposition 4.12, one proves that $b \leq (t-1)^2$. Combining this with (4.5) we obtain that $s \leq 2(q+\sqrt{q}+1)t^2 - 2q(2t-1)$ and finally $d = n - s \geq q\big(\frac{4}{3}k - 2\big)$. □

We conclude with a remark that summarizes the code lengths obtained from the constructions and results of this section.

Remark 4.15. For every positive integer k and every prime power q, we have provided explicit constructions of minimal $[n_{k,q}, k]_q$ codes with

$$n_{k,q} = \begin{cases}
\frac{1}{4}(q+1)k^2 & \text{if } k \equiv 0 \mod 2, \\
\frac{2}{9}(q+\sqrt{q}+1)k^2 & \text{if } k \equiv 0 \mod 3 \text{ and } q \text{ is a square}, \\
\frac{2}{9}(q+\sqrt{q}+1)(k-1)^2 + (q-1)(k-1) + 1 & \text{if } k \equiv 1 \mod 3 \text{ and } q \text{ is a square}, \\
\frac{1}{4}(q+1)(k+1)^2 - (2k+q-2) & \text{otherwise.}
\end{cases}$$

The first length is given by Construction A, the second length is given by Construction B, and the last two lengths are obtained by combining Proposition 4.9 with these two constructions. It is easy to see that the minimum distance d of any code obtained using Proposition 4.9 meets the bound of Theorem 2.8 with equality, i.e., $d = (q-1)(k-1)+1$.

References

[1] G. N. Alfarano, M. Borello, and A. Neri. A geometric characterization of minimal codes and their asymptotic performance. *Adv. in Math. Commun.*, 2020.

[2] N. Alon. Combinatorial nullstellensatz. *Combin. Probab. Comput.*, 8(1-2):7–29, 2001.

[3] N. Alon and Z. Füredi. Covering the cube by affine hyperplanes. *European J. Combin.*, 14(2):79–83, 1993.

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

[5] S. Ball. Multiple blocking sets and arcs in finite planes. *J. London Math. Soc.*, 54(3):581–593, 1996.

[6] S. Ball and A. Blokhuis. On the size of a double blocking set in $\mathrm{PG}(2, q)$. *Finite Fields Appl.*, 2(2):125–137, 1996.

[7] J. Barát and L. Storme. Multiple blocking sets in $\mathrm{PG}(n, q), n \geq 3$. *Des. Codes Cryptogr.*, 33(1):5–21, 2004.

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

[9] D. Bartoli, M. Bonini, and B. Güneş. An inductive construction of minimal codes. *arXiv preprint arXiv:1911.09093*, 2019.

[10] D. Bartoli, A. Cossidente, G. Marino, and F. Pavese. On cutting blocking sets and their codes. *arXiv preprint arXiv:2011.11101*, 2020.

[11] A. Beutelspacher. On Baer subspaces of finite projective spaces. *Math. Z.*, 184(3):301–319, 1983.

[12] R. Bhatia and C. Davis. A better bound on the variance. *Amer. Math. Monthly*, 107(4):353–357, 2000.

[13] A. Blokhuis, P. Sziklai, and T. Szonyi. Blocking sets in projective spaces. In L. Storme and J. de Beule, editors, *Current research topics in Galois geometry*, pages 61–84. Nova Sci. Publ., New York, 2011.

[14] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *J. Algebraic Combin.*, pages 1–15, 2020.

[15] A. Bonisoli. Every equidistant linear code is a sequence of dual Hamming codes. *Ars Combin.*, 18:181–186, 1983.

[16] C. Carlet, C. Ding, and J. Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Trans. Inform. Theory*, 51(6):2089–2102, 2005.

[17] H. Chabanne, G. Cohen, and A. Patey. Towards secure two-party computation from the wire-tap channel. In *Information security and cryptology—ICISC 2013*, volume 8565 of *Lecture Notes in Comput. Sci.*, pages 34–46. Springer, Cham, 2014.

[18] G. D. Cohen, S. Mesnager, and A. Patey. On minimal and quasi-minimal linear codes. In *Cryptography and coding*, volume 8308 of *Lecture Notes in Comput. Sci.*, pages 85–98. Springer, Heidelberg, 2013.

[19] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. Linear nonbinary covering codes and saturating sets in projective spaces. *Adv. in Math. Commun.*, 5(1):119–147, 2011.

[20] R. dela Cruz, M. Kiermaier, S. Kurz, and A. Wassermann. On the minimum number of minimal codewords. *arXiv preprint 1912.09804*, 2019.

[21] P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Inform. and Control*, 23(5):407–438, 1973.

[22] C. Ding. Linear codes from some 2-designs. *IEEE Trans. Inform. Theory*, 61(6):3265–3275, 2015.

[23] S. Fancsali and P. Sziklai. Lines in higgledy-piggledy arrangement. *Electron. J. Comb.*, 21(2), 2014.

[24] O. Geil and C. Thomsen. Weighted Reed–Muller codes revisited. *Des. Codes Cryptogr.*, 66(1-3):195–220, 2013.

[25] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge University Press, 2013.

[26] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, 2010.

[27] T. Y. Hwang. Decoding linear block codes for minimizing word error rate. *IEEE Trans. Inform. Theory*, 25(6):733–737, 1979.

[28] M. Lavrauw and G. Van de Voorde. Field reduction and linear sets in finite geometry. *Topics in finite fields*, 632:271–293, 2015.

[29] H. H. López, C. Rentería-Márquez, and R. H. Villarreal. Affine cartesian codes. *Des. Codes Cryptogr.*, 71(1):5–19, 2014.

[30] W. Lu, X. Wu, and X. Cao. The parameters of minimal linear codes. *arXiv preprint arXiv:1911.07648*, 2019.

[31] J. L. Massey. Minimal codewords and secret sharing. *In Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279, 1993.

[32] S. Mesnager. Linear codes with few weights from weakly regular bent functions based on a generic construction. *Cryptogr. Commun.*, 9:71–84, 2017.

[33] S. Mesnager, F. Özbudak, and A. Sınak. Linear codes from weakly regular plateaued functions and their secret sharing schemes. *Des. Codes Cryptogr.*, 87(2-3):463–480, 2019.

[34] B. Segre. Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane. *Ann. Mat. Pura Appl.*, 64(1):1–76, 1964.

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

[36] M. A. Tsfasman and S. G. Vlăduţ. *Algebraic-geometric codes*, volume 58 of *Mathematics and its Applications (Soviet Series)*. Kluwer Academic Publishers Group, Dordrecht, 1991.