A geometric characterization of minimal codes and their asymptotic performance

Gianira Alfarano, Martino Borello, Alessandro Neri

▶ **To cite this version:**

Gianira Alfarano, Martino Borello, Alessandro Neri. A geometric characterization of minimal codes and their asymptotic performance. Advances in Mathematics of Communications, 2019, 16 (1), pp.115. 10.3934/amc.2020104 . hal-03852306

HAL Id: hal-03852306
https://hal.science/hal-03852306

Submitted on 14 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

arXiv:1911.11738v2 [cs.IT] 12 Dec 2019

A geometric characterization of minimal codes and their asymptotic performance

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

[1]University of Zurich, Switzerland
[2]LAGA, UMR 7539, CNRS, Université Paris 13 - Sorbonne Paris Cité, Université Paris 8, F-93526, Saint-Denis, France
[3]Inria Saclay Île-de-France, 91120 Palaiseau, France

December 13, 2019

Abstract

In this paper, we give a geometric characterization of minimal linear codes. In particular, we relate minimal linear codes to cutting blocking sets, introduced in a recent paper by Bonini and Borello. Using this characterization, we derive some bounds on the length and the distance of minimal codes, according to their dimension and the underlying field size. Furthermore, we show that the family of minimal codes is asymptotically good. Finally, we provide some geometrical constructions of minimal codes as cutting blocking sets.

1 Introduction

Let $\mathbb{F}_q$ be a finite field and $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code. A codeword $c \in \mathcal{C}$ is called *minimal* if its support $\{i \mid c_i \neq 0\}$ does not contain the support of another independent codeword. The study of the minimal codewords of a linear code finds application in combinatorics, in the analysis of the Voronoi region for decoding purposes [4, 1] and in secret sharing schemes [27, 28, 4].

Secret sharing schemes were introduced independently by Shamir and Blakley in 1979 [34, 11]. They are protocols used for distributing a secret among a certain number of participants. In particular, in its original framework, a secret sharing scheme works as follows: a dealer gives a share of a secret to n players in such a way that any subset of at least t players can reconstruct the secret, but no subset of less than t players can. This is also called (n, t)-threshold scheme protocol. A more general construction, based on

*G. N. Alfarano acknowledges the support of Swiss National Science Foundation grant n. 188430.
†A. Neri acknowledges the support of Swiss National Science Foundation grant n. 187711.

linear codes, was first investigated by McEliece and Sarwate in 1981 [29], where Reed-Solomon codes were used. Later, several authors used other linear error-correcting codes to construct the same protocol [26, 27, 28, 21].

The set of subsets of participants which are able to recover the secret is called *access structure*. It is common to consider only subsets which do not admit proper subsets of participants able to recover the secret: we may refer to their collection as *minimal access structure*. For example, in an (n, t)-threshold scheme protocol, the access structure is given by all subsets of at least t participants, whereas the minimal access structure is given by all subsets of exactly t participants.

In [27], Massey relates the secret sharing protocol to minimal codewords: in particular, the minimal access structure in his secret sharing protocol is given by the support of the minimal codewords of a linear code $\mathcal{C}$, having first coordinate equal to 1. However, finding the minimal codewords of a general linear code is a difficult task. For this reason, a special class of codes has been introduced: a linear code is said to be *minimal* if all its nonzero codewords are minimal.

In [4], Ashikhmin and Barg gave a sufficient condition for a linear code to be minimal.

Lemma 1.1. *Let $\mathcal{C}$ be an $[n, k]_q$ code, w_{min}, w_{max} be the minimum and the maximum Hamming weights in $\mathcal{C}$, respectively. Then $\mathcal{C}$ is minimal if*

$$\frac{w_{min}}{w_{max}} > \frac{q-1}{q}. \tag{AB}$$

The Ashikhmin-Barg Lemma gave rise to several works with the aim of constructing minimal codes, see for example [15, 39, 20, 22]. However, condition (AB) is only sufficient. Some constructions of families of minimal codes not satisfying the condition (AB) were first presented in [19, 17]. In [24], a necessary and sufficient condition for an $\mathbb{F}_q$-linear code to be minimal was given: an $[n, k]_q$ code $\mathcal{C}$ is minimal if and only if, for every pair of linearly independent codewords $a, b \in \mathcal{C}$, we have

$$\sum_{\lambda \in \mathbb{F}_q^*} \mathrm{wt}(a + \lambda b) \neq (q-1)\mathrm{wt}(a) - \mathrm{wt}(b).$$

In the same paper, the authors constructed an infinite family of minimal linear codes not satisfying the condition (AB). This construction was generalized to finite fields with odd characteristic by Bartoli and Bonini, in [8]. In [12], Bonini and Borello investigated the geometric generalization of the construction in [8], highlighting a first link between minimal codes and cutting blocking sets. Moreover, different types of recent constructions of minimal codes based on weakly regular bent plateaued functions have been also presented in [30, 31, 32].

In this paper, we give a characterization of minimal linear codes in terms of cutting blocking sets. We derive some bounds on the length and the distance of minimal codes, according to their dimension and the underlying field size. We then show that the family of minimal codes is asymptotically good and we provide some geometrical constructions and examples. The paper is organized as follows. In Section 2, we introduce some

basics about linear codes over finite fields. In particular, we focus on minimal codes and we introduce the notion of reduced minimal codes. After giving some background on projective systems, we explain how they are in one-to-one correspondence with linear codes. In Section 3, we relate minimal codes (reduced minimal code resp.) to cutting blocking sets (minimal cutting blocking sets resp.), by analyzing the correspondence given in Section 2. In Section 4, we derive bounds on the distance and on the length of minimal codes. One of the main results of this section is Theorem 4.8, in which we show that minimal codes are asymptotically good. Moreover, we find a correspondence between cutting blocking sets in $PG(2,q)$ and 2-fold blocking sets and we use this correspondence to derive upper and lower bounds on the length of reduced minimal codes of dimension 3. In Section 5, we provide a geometrical general construction of reduced minimal codes and we compute the weight distribution of these codes. For reduced minimal codes of dimension 4 and minimal codes of dimension 5, we exhibit a construction exploiting cutting blocking sets in $PG(3,q)$ and in $PG(4,q)$ (with smaller length than the ones derived with the general construction). We conclude with further remarks and open questions in Section 6, where we also propose a challenging conjecture on the minimum distance of minimal codes.

2 Preliminaries

2.1 Linear codes

We recall here some basic notions in coding theory which will be useful in the following.

Let q be a prime power, n be a positive integer and $\mathbb{F}_q$ be the finite field with q elements. In the vector space $\mathbb{F}_q^n$, the *support* of a vector $u = (u_1, \ldots, u_n) \in \mathbb{F}_q^n$ is the set $\mathrm{supp}(u) := \{i \mid u_i \neq 0\}$. The *Hamming distance* on $\mathbb{F}_q^n$ is defined as $d_H(u,v) = |\mathrm{supp}(u-v)|$, for every pair of vectors $u, v \in \mathbb{F}_q^n$. The *Hamming weight*, $w(u)$ of a vector $u \in \mathbb{F}_q^n$ is its distance from the all zero vector.

An $[n,k]_q$ *(linear) code* $\mathcal{C}$ is a k-dimensional subspace of $\mathbb{F}_q^n$ endowed with the Hamming distance and the elements of $\mathcal{C}$ are called *codewords*. Its *rate* is the number $R = k/n$. The *minimum distance* d of $\mathcal{C}$ is the quantity $d = \min\{d_H(u,v) \mid u, v \in \mathcal{C}, u \neq v\}$. If the minimum distance d of an $[n,k]_q$ code $\mathcal{C}$ is known, then $\mathcal{C}$ is denoted as $[n,k,d]_q$ code. The weight distribution of $\mathcal{C}$ is the sequence $A_0(\mathcal{C}), \ldots, A_n(\mathcal{C})$, where $A_i(\mathcal{C}) = |\{c \in C \mid w(c) = i\}|$.

An $[n,k]_q$ code $\mathcal{C}$ of dimension $k \geq 2$ is said to be *non-degenerate* if no coordinate position is identically zero. Unless specified otherwise, all codes discussed here are assumed to be non-degenerate.

An important notion for linear codes concerns the equivalence. Let $\mathcal{G}$ be the subgroup of the group of linear automorphisms of $\mathbb{F}_q^n$ generated by the permutations of coordinates and by the multiplication of the i-th coordinate by an element in $\mathbb{F}_q^*$. Two codes $\mathcal{C}$ and $\mathcal{C}'$ are *(monomially) equivalent* if there exists $\sigma \in \mathcal{G}$ such that $\mathcal{C}' = \sigma(\mathcal{C})$.

The central objects of this paper are minimal codes, which are defined as follows.

Definition 2.1. A linear code $\mathcal{C}$ is said to be *minimal* if, for every $c, c' \in \mathcal{C}$,

$$\mathrm{supp}(c) \subseteq \mathrm{supp}(c') \iff c = \lambda c' \text{ for some } \lambda \in \mathbb{F}_q.$$

Moreover, we introduce the notion of reduced minimal code, which will allow us to study the maximal rates of minimal codes.

Definition 2.2. An $[n,k]_q$ minimal code $\mathcal{C}$ is called *reduced* if for every $i \in \{1,\dots,n\}$, the code $\mathcal{C}_i$ obtained by puncturing $\mathcal{C}$ on the coordinate i (i.e. deleting the same coordinate i in each codeword) is not minimal.

2.2 Projective systems

In this section we consider linear codes from a geometrical view, as detailed in [37]. We first give some background of fundamentals of finite projective geometry. For a detailed introduction we refer to the recent book by Ball [6]. Let $PG(k,q)$ be the finite projective geometry of dimension k and order q. Due to a result of Veblen and Young [38], all finite projective spaces of dimension greater than two are isomorphic, and they correspond to Galois geometries. The space $PG(k,q)$ can be easily seen as the vector space of dimension $k+1$ over the finite field $\mathbb{F}_q$. In this representation, the one-dimensional subspaces correspond to the points, the two-dimensional subspaces correspond to the lines, etc. Formally, we have

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

where

$$u \sim v \text{ if and only if } u = \lambda v \text{ for some } \lambda \in \mathbb{F}_q.$$

It is not hard to show by elementary counting that the number of points of $PG(k,q)$ is given by

$$\theta_q(k) := \frac{q^{k+1}-1}{q-1}.$$

A *d-flat* Π in $PG(k,q)$ is a subspace isomorphic to $PG(d,q)$; if $d = k-1$, the subspace Π is called a *hyperplane*. It is clear that $\theta_q(k)$ is also the number of hyperplanes in $PG(k,q)$.

Recall that a *multiset* $(\mathcal{M}, m)$ *in* $PG(k-1,q)$ is a set of points $\mathcal{M} \subseteq PG(k-1,q)$ together with a weight function m, which associates a positive integer $m(P)$ to all the points $P \in \mathcal{M}$. A multiset $(\mathcal{M}, m)$ is said to be *finite* if $\sum_{P\in\mathcal{M}} m(P) < +\infty$.

Definition 2.3. Let $(\mathcal{M}, m)$ be a finite multiset in $\Pi = PG(k-1,q)$. We define the *character* function of $\mathcal{M}$, denoted $\mathrm{Char}_{\mathcal{M}}$, mapping the power set of Π to the non-negative integers:

$$\mathrm{Char}_{\mathcal{M}}(A) = \sum_{P\in A} m(P).$$

So $\mathrm{Char}_{\mathcal{M}}(A)$ is the number of points of $\mathcal{M}$ that belong also to A. With a slight abuse of notation, we will write $m(P) = \mathrm{Char}_{\mathcal{M}}(P)$, for any point P.

Central to the geometric point of view of linear codes is the idea of a projective system.

Definition 2.4. A *projective* $[n,k,d]_q$ *system* is a finite multiset $(\mathcal{M},m)$ in $PG(k-1,q)$, whose points do not lie all on a hyperplane, where $n=\sum_{P\in\mathcal{M}} m(P)$, and

$$d = n - \max\{\mathrm{Char}_{\mathcal{M}}(H) \mid H \subset PG(k-1,q), \dim(H) = k-2\}\,.$$

Two *projective* $[n,k,d]$ *systems* $(\mathcal{M},m)$ and $(\mathcal{M}',m')$ are said to be *equivalent* if there exists a projective isomorphism ϕ of $PG(k-1,q)$ mapping $\mathcal{M}$ to $\mathcal{M}'$ which preserves the multiplicities, i.e. such that $m(P)=m'(\phi(P))$ for every $P\in\mathcal{M}$.

Let $\mathcal{C}$ be an $[n,k]_q$ code with $k\times n$ generator matrix G. Note that multiplying any column of G by a nonzero field element yields a generator matrix for a code which is equivalent to $\mathcal{C}$. Consider the (multi)set of one-dimensional subspaces of $\mathbb{F}_q^n$ spanned by the columns of G. In this way the columns may be considered as a multiset $(\mathcal{M},m)$ of points in $PG(k-1,q)$, where the weight function m keeps track of how many times a certain column appears in the generator matrix, up to scalar multiple.

For any nonzero vector $v=(v_1,v_2,\ldots,v_k)$ in $\mathbb{F}_q^k$, it follows that the projective hyperplane

$$v_1x_1+v_2x_2+\cdots+v_kx_k=0$$

contains $|\mathcal{M}|-w$ points of $\mathcal{M}$ if and only if the codeword vG has weight w. Therefore, linear non-degenerate $[n,k,d]_q$ codes and projective $[n,k,d]_q$ systems are equivalent objects. Indeed, the procedure described above gives a correspondence between $[n,k,d]_q$ codes up to (monomial) equivalence and projective $[n,k,d]_q$ systems up to (projective) equivalence [37, Theorem 1.1.6]. This can be formally stated as follows. We denote by (Φ,Ψ) the correspondence

$$\{\text{ classes of non-deg. } [n,k,d]_q \text{ codes }\} \longleftrightarrow \{\text{ classes of projective } [n,k,d]_q \text{ systems }\}.$$

More specifically, for a class of non-degenerate $[n,k,d]_q$ code $[\mathcal{C}]$, $\Phi([C])$ is the (equivalence class of the) multiset obtained by taking the columns with multiplicities of any generator matrix of any representative of $[C]$, while Ψ is the functor that does the inverse operation. Given an equivalence class of multisets $[(\mathcal{M},m)]$ in $PG(k-1,q)$, it returns the class containing the code whose generator matrix has the points of $\mathcal{M}$, taken with multiplicities, as columns. It is not difficult to see that (Φ,Ψ) is an equivalence of the two categories (see [5] for a detailed discussion on the category of linear codes).

3 Cutting blocking sets and minimal codes

Cutting blocking sets have been introduced by Bonini and Borello in [12], for the construction of a particular family of minimal codes. However, we will show that minimal codes and cutting blocking sets are the same objects, under the equivalence (Φ,Ψ) between (non-degenerate) linear codes and projective systems.

First we recall some basic background on blocking sets.

Definition 3.1. Let t, r, N be positive integers with $r < N$. A *t-fold r-blocking set* in $PG(N,q)$ is a set $\mathcal{M} \subseteq PG(N,q)$ such that for every $(N-r)$-flat Λ of $PG(N,q)$ we have $|\Lambda \cap \mathcal{M}| \geq t$. When $r = 1$, we will refer to it as a *t-fold blocking set*. When $t = 1$, we will refer to it as an *r-blocking set*. Finally, *blocking sets* are the ones with $r = t = 1$.

Definition 3.2. Let r, N be positive integers with $r < N$. An r-blocking set $\mathcal{M}$ in $PG(N,q)$ is called *cutting* if for every pair of $(N-r)$-flats Λ, Λ' of $PG(N,q)$ we have

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

Moreover, a cutting r-blocking set $\mathcal{M}$ is called *minimal* if for every $P \in \mathcal{M}$, the set $\mathcal{M} \setminus \{P\}$ is not a cutting r-blocking set.

The following result gives a different characterization of cutting blocking sets. The result follows also from [12, Theorem 3.5].

Proposition 3.3. *A set $\mathcal{M} \subseteq PG(N,q)$ is a cutting r-blocking set if and only if for every $(N-r)$-flat Λ of $PG(N,q)$ we have $\langle \mathcal{M} \cap \Lambda \rangle = \Lambda$.*
In particular, a cutting r-blocking set in $PG(N,q)$ is an $(N-r+1)$-fold blocking set.

Proof. ($\Leftarrow$) Let Λ, Λ' be $(N-r)$-flats of $PG(N,q)$, such that $\mathcal{M} \cap \Lambda \subseteq \mathcal{M} \cap \Lambda'$. Then $\Lambda = \langle \mathcal{M} \cap \Lambda \rangle \subseteq \langle \mathcal{M} \cap \Lambda' \rangle = \Lambda'$, and since Λ and Λ' have the same dimension, we get $\Lambda = \Lambda'$, i.e. $\mathcal{M}$ is a cutting r-blocking set.

($\Rightarrow$) Suppose by contradiction that there exists an $(N-r)$-flat Λ such that $\langle \Lambda \cap \mathcal{M} \rangle = \Delta \subsetneq \Lambda$. Then, for every $(N-r)$-flat Λ' containing Δ we have $\Lambda' \cap \mathcal{M} \supseteq \Delta \cap \mathcal{M} = \Lambda \cap \mathcal{M}$. And therefore, $\mathcal{M}$ is not a cutting r-blocking set.

□

Theorem 3.4. *Equivalence classes of $[n,k,d]_q$ minimal codes are in correspondence with equivalence classes of projective $[n,k,d]_q$ systems $(\mathcal{M}, m)$ such that $\mathcal{M}$ is a cutting blocking set via (Φ, Ψ).*
Furthermore, via the same pair of functors (Φ, Ψ), equivalence classes of $[n,k,d]_q$ reduced minimal codes are in correspondence with projective $[n,k,d]_q$ systems $(\mathcal{M}, m)$ such that $\mathcal{M}$ is a minimal cutting blocking set and $m(P) = 1$ for every $P \in \mathcal{M}$.

Proof. The first statement follows from the definitions of the two objects. Hyperplanes $\langle v \rangle^\perp$ in $PG(k-1,q)$ correspond to linearly independent codewords vG of $\mathcal{C}$. For any pair of hyperplanes $H = \langle v \rangle^\perp$ and $H' = \langle v' \rangle^\perp$ we have $\mathcal{M} \cap H \subseteq \mathcal{M} \cap H'$ if and only if $\mathrm{supp}(vG) \supseteq \mathrm{supp}(v'G)$, where G is any generator matrix of $\mathcal{C}$ and $(\mathcal{M}, m)$ is the associated projective system.

Moreover, since puncturing on a coordinate of a code whose generator matrix is G coincides to removing the corresponding point from the multiset $(\mathcal{M}, m)$, we get the second statement. □

Observe that reduced minimal codes correspond to multisets $(\mathcal{M}, m)$ with no multiplicity, i.e. such that $m(P) = 1$ for every $P \in \mathcal{M}$. In particular, in order to construct

minimal codes, by Theorem 3.4 we only need to construct classical sets, without multiplicity. Therefore, from now on we will drop the multiplicity map from the notation when not necessary, and we will only talk about sets $\mathcal{M} \subseteq PG(N, q)$.

4 Bounds on length and distance of minimal codes

It is natural to ask for which values R we can produce minimal codes of rate R. It is in general easier to construct minimal codes with very small rate, such as symplex codes or related codes as in [8, 12]. However, a priori it is not clear if one can do it for arbitrary rates. In particular, for a given dimension k one would like to determine what is the smallest length n (and hence the largest rate $R = k/n$) such that an $[n, k]_q$ code exists. In this section we provide some partial answers to these questions, proving some bounds on the length and the minimum distance of a minimal code for a fixed dimension. The characterization given in Theorem 3.4 plays a crucial role in dealing with these problems.

Theorem 4.1. *Let $\mathcal{C}$ be an $[n, k]_q$ minimal code. Then*

$$n \geq (k-1)q + 1.$$

Proof. If $k = 1$ there is nothing to prove, hence we assume $k \geq 2$. Choose a generator matrix, and the corresponding projective $[n, k]_q$ system $(\mathcal{M}, m)$ in $\Pi = PG(k-1, q)$. Consider the set S of incident point-hyperplane pairs (P, Λ) in Π, where $P \in \mathcal{M}$. Summing over all the points of $\mathcal{M}$ we obtain

$$|S| = \sum_{P \in \mathcal{M}} m(P)\theta_q(k-2) = n\theta_q(k-2), \tag{1}$$

since $\theta_q(k-2)$ is the number of hyperplanes through a point.
On the other hand, summing over the set Γ of all the hyperplanes of Π we get

$$|S| = \sum_{H \in \Gamma} \mathrm{Char}_{\mathcal{M}}(H) \geq \sum_{H \in \Gamma} (k-1) = (k-1)\theta_q(k-1), \tag{2}$$

where the inequality follows from the fact that $(\mathcal{M}, m)$ is in particular a $(k-1)$-fold blocking set in Π, by Proposition 3.3. Combining (1) and (2), we obtain

$$n \geq \left\lceil (k-1)\frac{\theta_q(k-1)}{\theta_q(k-2)} \right\rceil,$$

We then conclude observing that $\left\lceil (k-1)\frac{\theta_q(k-1)}{\theta_q(k-2)} \right\rceil = (k-1)q + \left\lceil \frac{k-1}{\theta_q(k-2)} \right\rceil = (k-1)q+1$. □

As a consequence, we get an asymptotic improvement of a result by Chabanne, Cohen and Patey [16]. In that work, they showed that the rate R of an $[n, Rn]_q$ minimal code for n large enough satisfies $R \leq \log_q(2)$, calling this bound the *Maximal bound*.

Corollary 4.2. *If $\mathcal{C}$ is a minimal code of rate R, asymptotically it holds $R \leq \frac{1}{q}$.*

Proof. Let $\mathcal{C}$ be a minimal code of rate R. Then, by Theorem 4.1

$$R = \frac{k}{n} \leq \frac{n+q-1}{qn} \longrightarrow \frac{1}{q},$$

as n goes to infinity. □

We now prove an important result relating the minimum distance with the dimension of a minimal code and the size of the underlying field. We will give two different proofs of the theorem, to document further the interest of the geometric characterization.

Theorem 4.3. *Let $\mathcal{C}$ be an $[n,k,d]_q$ minimal code with $k \geq 2$. Then $d \geq k+q-2$.*

Proof. Consider the projective $[n,k,d]_q$ system $(\mathcal{M}, m)$ associated to $\mathcal{C}$. Without loss of generality we can assume that there are no multiplicities, i.e. that $\mathcal{M} = \{P_1, \ldots, P_n\}$ with the P_i's pairwise distinct. By Theorem 3.4, $\mathcal{M}$ is a cutting blocking set and there exists an hyperplane H such that $\{P_{d+1}, \ldots, P_n\} \subseteq H$ and $P_1, \ldots, P_d \notin H$. Consider the set $\mathcal{M}' := \{P_1, \ldots, P_d\}$. First we prove that $\mathcal{M}'$ is a projective system, i.e. that $P_1, \ldots, P_d$ do not belong to the same hyperplane. Indeed, suppose that there exists a hyperplane K such that $P_1, \ldots, P_d \in K$, then clearly $K \neq H$, and hence $\Lambda := H \cap K$ is a $(k-3)$-flat. Since there are $q+1$ hyperplanes containing Λ, there always exists a third hyperplane T different from H and K such that $\Lambda \subseteq T$. Moreover $P_1, \ldots, P_d \notin T$, otherwise we would have $T = K$. Thus, we get

$$\mathcal{M} \cap H = \{P_{d+1}, \ldots, P_n\} \supseteq \mathcal{M} \cap T,$$

which contradicts the fact that $\mathcal{M}$ is cutting. Therefore, $\mathcal{M}'$ is a projective $[d,k,d']_q$ system.

We show now that $d' \geq q-1$. Up to reordering the points, this means that there exists an hyperplane H' such that $P_1, \ldots, P_{d'} \notin H'$ and $P_{d'+1}, \ldots, P_d \in H'$. Consider the $(k-3)$-flat $\Lambda := H \cap H'$, and the sheaf of hyperplanes containing Λ. Except from H and H' there are $q-1$ hyperplanes left in this sheaf. Clearly $P_{d'+1}, \ldots, P_d \notin \Lambda$, and hence they do not belong to any of the remaining $q-1$ hyperplanes. Moreover, every point in $\{P_1, \ldots, P_{d'}\}$ can be in at most one hyperplane of the sheaf. Assume by contradiction that $d' \leq q-2$, then there exists at least a hyperplane $\tilde{H} \neq H$ such that $P_1, \ldots, P_d \notin \tilde{H}$. Hence

$$\mathcal{M} \cap H = \{P_{d+1}, \ldots, P_n\} \supseteq \mathcal{M} \cap \tilde{H},$$

which contradicts the fact that $\mathcal{M}$ is cutting. Thus, $\mathcal{M}'$ is a projective $[d,k,d']_q$ system, with $d' \geq q-1$. Combining it with the Singleton bound [35] we obtain

$$d \geq k + d' - 1 \geq k + q - 2.$$

□

An alternative proof, given from a coding theory point of view, is the following.

Second proof. Let c be a codeword of minimum weight d in $\mathcal{C}$. Then consider the code $\mathcal{C}'$ obtained by puncturing $\mathcal{C}$ in all the $n-d$ coordinates where c is 0. Observe that $\mathcal{C}'$ is a $[d,k]_q$ code. Indeed, if the dimension of $\mathcal{C}'$ is less than k, it means that there is at least one codeword w in $\mathcal{C}$ whose support is disjoint from the support of c. Hence $\mathrm{supp}(c+w)$ contains $\mathrm{supp}(c)$ and $\mathrm{supp}(w)$ and this contradicts the minimality of $\mathcal{C}$.

Now, observe that $\mathcal{C}'$ has distance $d' \geq q-1$. Indeed, consider $c' \in \mathcal{C}'$ that corresponds to c and has weight d, and let $u \in \mathcal{C}$ such that the corresponding $u' \in \mathcal{C}'$ is of minimum weight d' in $\mathcal{C}'$. Then, for any $\alpha \in \mathbb{F}_q^*$, consider the codeword $c' + \alpha u'$ in $\mathcal{C}'$. If $d' < q-1$, at least one of these codewords has weight d. The corresponding codeword in $\mathcal{C}$, then, has support containing $\mathrm{supp}(c)$, which yields a contradiction to the minimality of $\mathcal{C}$.

Finally, we apply the Singleton bound on $\mathcal{C}'$ and combine it with $d' \geq q-1$ to obtain the desired result:

$$d \geq d' + k - 1 \geq k + q - 2.$$

□

Remark 4.4. The bound in Theorem 4.3 is not sharp in general: considering the second proof, we remark that $d = k+q-2$ if and only if $\mathcal{C}'$ is a $[q+k-2, k, q-1]_q$ MDS code with exactly $q-1$ codewords of weight equal to the length (namely, all the nonzero multiples of c'). Weight enumerators of MDS codes are known (see for example [25, Ch. 11, §3, Theorem 6]), so that it is easy to prove that this may happen if and only if

$$\sum_{j=0}^{k-1} (-1)^j \cdot \binom{k-1+q-2}{j} \cdot q^{k-1-j} = 1$$

which is not true for $q \neq 2$ and $k \geq 3$. Moreover, one can also observe that assuming the MDS conjecture to be true (see [33]), a $[q+k-2, k, q-1]_q$ MDS code exists only for $k \leq 3$.

As a result, we can actually get new bounds on the length of a minimal code, combining Theorem 4.3 with known upper bounds on the minimum distance. It is easy to observe that using the Singleton bound does not improve on Theorem 4.1. However, if q is small, we can get better results using the Griesmer bound [23].

Corollary 4.5. *Let $\mathcal{C}$ be an $[n,k]_q$ minimal code. Then*

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{k+q-2}{q^i} \right\rceil.$$

Proof. It follows combining Theorem 4.3 with the Griesmer bound. □

Remark 4.6. Observe that for some sets of parameters Corollary 4.5 gives a better lower bound on the length of minimal codes than the one of Theorem 4.1, while for other sets of parameters the converse holds. For instance, it is easy to see that for $q = 2$, Corollary 4.5 is always better. Viceversa, when $q \geq k \geq 4$, Theorem 4.1 provides better results.

Furthermore, numerical results with MAGMA show that the bound in Corollary 4.5 is not sharp. For example, for $q = 2$ and $k = 4$, the minimum possible length of a minimal code is 9, while the above bound gives 8.

4.1 Asymptotic performance of minimal codes

We recall that there is an existence result that holds asymptotically, i.e. we can actually ensure the existence of minimal codes of arbitrary length n of a fixed rate R that only depends on q. This existence result is not constructive, and it was shown by Chabanne, Cohen and Patey [16].

Theorem 4.7 (Minimal Bound [16])**.** *For any rate $R = k/n$ such that*

$$0 \leq R \leq \frac{1}{2} \log_q \left(\frac{q^2}{q^2 - q + 1} \right),$$

there exists an infinite sequence of $[n, k]_q$ minimal codes.

The most important consequence of Theorem 4.3 is that it allows to show that minimal codes are asymptotically good. Let us recall that a family of codes is said *asymptotically good* if it contains a sequence $C = (\mathcal{C}_1, \mathcal{C}_2, \dots)$ of linear codes, where C_n is an $[n, k_n, d_n]_q$ code such that the rate R and the relative distance δ of C_n, that is

$$R := \liminf_{n \to \infty} \frac{k_n}{n} \qquad \text{and} \qquad \delta := \liminf_{n \to \infty} \frac{d_n}{n},$$

are both positive.

In general, we would like ideally both rate and relative distance of a code to be as large as possible, since the rate measures the number of information coordinates with respect to the length of the code and the relative distance measures the error correction capability of the code. Determining the rate and the relative distance for a class of codes is in general a difficult task. For example, it is still unknown if the family of cyclic codes is asymptotically good. However, some families of asymptotically good codes are known to exist. For example, codes that meet the Asymptotic Gilbert-Varshamov bound, binary quasi-cyclic codes [18, 2], self-dual codes [3], group codes [13].

A direct consequence of Theorem 4.3 and of the Minimal Bound of Theorem 4.7 is the following result.

Theorem 4.8. *Minimal codes are asymptotically good.*

4.2 Cutting blocking sets in the projective plane

In the projective plane, we can get better bounds on the cardinality of cutting blocking sets. This is due to the following result, which shows that we can reduce to study the cardinality of 2-fold blocking sets.

Lemma 4.9. *In $PG(2, q)$ a set $\mathcal{M}$ is a cutting blocking set if and only if it is a 2-fold blocking set.*

Proof. Clearly, a cutting blocking set is a 2-fold blocking set, as shown in Proposition 3.3. On the other hand, if $\mathcal{M}$ is a 2-fold blocking set, then for every line ℓ in $PG(2,q)$ $\langle \ell \cap \mathcal{M} \rangle = \ell$, since $|\ell \cap \mathcal{M}| \geq 2$. We conclude again by Proposition 3.3. □

Using this equivalence, we can give upper bounds on minimal cutting blocking sets and lower bounds on cutting blocking sets. Thanks to the correspondence of Theorem 3.4 between minimal codes and cutting blocking sets, we can regard these bounds as bounds on the length of minimal codes of dimension 3.

In particular, the following theorems follow directly from Lemma 4.9 and results in [7, 10].

Theorem 4.10 ([7])**.** *Let $\mathcal{C}$ be an $[n,3]_q$ minimal code.*

1. *If $q < 9$, then $n \geq 3q$.*
2. *If $q \in \{11, 13, 17, 19\}$, then $n \geq (5q+7)/2$.*
3. *If $q > 19$ and $q = p^{2d+1}$ for some p prime and $d \in \mathbb{N}$, then $n \geq p^d \left\lceil \frac{p^{d+1}+1}{p^d+1} \right\rceil + 2$.*
4. *If $q > 4$ and q is a square, then $n \geq 2q + 2\sqrt{q} + 2$.*

Theorem 4.11 ([10])**.** *Let $\mathcal{C}$ be an $[n,3]_q$ reduced minimal code. Then*

$$n \leq \frac{q}{2}\left(\sqrt{8q-7}+1\right)+2.$$

Remark 4.12. Observe that the minimal codes of Theorem 4.10 correspond to cutting blocking sets in $PG(2,q)$ and the reduced minimal codes of Theorem 4.11 correspond to minimal cutting blocking sets in $PG(2,q)$, via the correspondence (Φ, Ψ) of Theorem 3.4.

It would be interesting to have similar results for projective spaces of larger dimension, but in this case the equivalence of Lemma 4.9 does not hold.

5 Construction of minimal codes

In this section we provide a general construction of reduced minimal codes based on the geometric point of view. For this family of codes, we also determine the weight distribution, using basic combinatorial results in finite geometry.

We start with two auxiliary lemmas, based on avoiding results in finite projective spaces.

Lemma 5.1. *Let q be a prime power, k, r be integers such that $1 \leq r \leq k$. Let $P_1, \ldots, P_r \in PG(k-1,q)$ be points not on the same $(r-2)$-flat. Then, the number of hyperplanes H avoiding $P_1, \ldots, P_r$ is $q^{k-r}(q-1)^{r-1}$.*

Proof. It follows from a simple calculation using inclusion-exclusion principle. Since the number of hyperplanes is $\theta_q(k-1)$, and the number of hyperplanes containing at least i points among the P_j's is equal to $\theta_q(k-1-i)$, we get that the number of hyperplanes avoiding all the P_j's is

$$\begin{aligned}
&\theta_q(k-1) - \sum_{i=1}^{r} (-1)^{i-1} \binom{r}{i} \theta_q(k-1-i) \\
&= \frac{1}{q-1} \sum_{i=0}^{r} \binom{r}{i} (-1)^i (q^{k-i} - 1) \\
&= \frac{1}{q-1} \left(q^{k-r} \sum_{i=0}^{r} \binom{r}{i} (-1)^i q^{r-i} - \sum_{i=0}^{r} \binom{r}{i} (-1)^i \right) \\
&= q^{k-r}(q-1)^{r-1}.
\end{aligned}$$

□

Lemma 5.2. *Let $P_1, \ldots, P_k \in PG(k-1,q)$ be points in general position. Then, the number of hyperplanes containing $P_1, \ldots, P_s$ and avoiding $P_{s+1}, \ldots, P_k$ is $(q-1)^{k-s-1}$*

Proof. Let $\Lambda := \langle P_1, \ldots, P_s \rangle$, then the number of hyperplanes containing Λ and avoiding $P_{s+1}, \ldots, P_k$ is in correspondence with the number of hyperplanes in $PG(k-1)/\Lambda \cong PG(k-s,q)$ avoiding $P_{s+1}, \ldots, P_k$. Such number is, by Lemma 5.1, equal to $(q-1)^{k-s-1}$. □

Theorem 5.3. *Let $P_1, \ldots, P_k$ be points in general position in $PG(k-1,q)$. For $0 \leq i < j \leq k$, consider the line $\ell_{i,j} := \langle P_i, P_j \rangle$. Then, $\mathcal{M} := \bigcup_{i,j} \ell_{i,j}$ is a minimal cutting blocking set.*

Proof. Let H be a hyperplane in $PG(k-1,q)$. Since the points $P_1, \ldots, P_k$ are in general position, there exists at least one point among them, say P_1 that is not in H. Consider the intersection $H \cap \mathcal{M}$, which does not contain P_1. Hence H meets the lines $\ell_{1,j}$'s in $k-1$ distinct points $Q_2, \ldots Q_k$, i.e. $\{Q_j\} = H \cap \ell_{1,j}$ for $j \in \{2, \ldots, k\}$. Take the flat $\Lambda := \langle \mathcal{M} \cap H \rangle$, and observe that

$$\langle \Lambda, P_1 \rangle \supseteq \langle P_1, Q_j \rangle = \ell_{1,j},$$

However, $P_j \in \ell_{1,j}$ for every $j \in \{2, \ldots, k\}$, and this implies $\langle \Lambda, P_1 \rangle \supseteq \langle P_1, \ldots, P_k \rangle = PG(k-1,q)$. Hence, necessarily $\dim(\Lambda) = k-2$ and by Proposition 3.3, $\mathcal{M}$ is a cutting blocking set.

It is left to prove that $\mathcal{M}$ is minimal. Suppose we remove from $\mathcal{M}$ one of the points P_i's from $\mathcal{M}$, say P_1, getting $\tilde{\mathcal{M}} := \mathcal{M} \setminus \{P_1\}$. Take a $(k-3)$-flat $\Lambda \subseteq \langle P_2, \ldots, P_k \rangle$ avoiding the points $P_2, \ldots, P_k$. By Lemma 5.1 such an hyperplane always exists. Hence $H := \langle \Lambda, P_1 \rangle$ is an hyperplane such that $H \cap \tilde{\mathcal{M}} \subseteq \Lambda$, and by Proposition 3.3, $\tilde{M}$ is not minimal. Similarly, choose a point in $\mathcal{M} \setminus \{P_1, \ldots, P_k\}$ and remove it from $\mathcal{M}$. Without loss of generality, we can choose $Q_{1,2} \in \ell_{1,2} \setminus \{P_1, P_2\}$ and consider $\tilde{M} := \mathcal{M} \setminus \{Q_{1,2}\}$.

Take the space $H := \langle Q_{1,2}, P_3, \ldots, P_k \rangle$. It is easy to see that $\langle H, P_1 \rangle = \langle H, P_2 \rangle = PG(k-1, q)$, and hence H is an hyperplane. Moreover, $H \cap \mathcal{M} = \{Q_{1,2}, P_3, \ldots, P_k\}$, therefore $\dim(H \cap \tilde{\mathcal{M}}) = \dim(\langle P_3, \ldots, P_k \rangle) = k-3$, and by Proposition 3.3 $\tilde{\mathcal{M}}$ can not be a cutting blocking set. □

The next result analyzes the reduced minimal code obtained in Theorem 5.3, giving the full description of its weight distribution.

Theorem 5.4. *The code associated to the minimal cutting blocking set of Theorem 5.3 is a $[\binom{k}{2}(q-1)+k, k]_q$ reduced minimal code $\mathcal{C}$, whose weights are exactly*

$$f_{q,k}(r) := \frac{1}{2}(k-r)((k+r-1)q - 2k + 4),$$

for every $r \in \{0, \ldots, k-1\}$. Furthermore, the weight distribution of $\mathcal{C}$ is given by

$$A_i(\mathcal{C}) = \sum_{\{r | f_{q,k}(r) = i\}} \binom{k}{r} (q-1)^{k-r}.$$

Proof. By the equivalence (Φ, Ψ) between codes and projective systems, the dimension of the code obtained by $\mathcal{M}$ is clearly k and its length is $n = \binom{k}{2}(q-1)+k$. Now, for an hyperplane $H = \langle v \rangle^{\perp}$, the weight of its $q-1$ associated codewords (i.e. all the nonzero multiples of vG, where G is the generator matrix obtained from $\mathcal{M}$) is $n - |\mathcal{M} \cap H|$. Therefore, it is determined by $|H \cap \mathcal{M}|$. By the symmetric properties of $\mathcal{M}$, the quantity $|H \cap \mathcal{M}|$ only depends on the integer

$$r := |\{i \in \{1, \ldots, k\} \mid P_i \in H\}|.$$

In this case, without loss of generality we can assume that $P_1, \ldots, P_r \in H$, and $P_{r+1}, \ldots, P_{k-r} \notin H$. Hence, $\mathcal{M}$ contains all the lines $\ell_{i,j}$ for $0 \leq i < j \leq r$, and it intersects all the lines $\ell_{i,j}$ in $\{P_i\}$, for $0 \leq i \leq r < j \leq k$, and in $\{Q_{i,j}\}$ for $r+1 \leq i < j \leq k$. Moreover, observe that the points $Q_{i,j}$ are all pairwise distinct. Therefore, the weight of the codeword associated to H is equal to

$$\begin{aligned}
f_{q,k}(r) &= \binom{k}{2}(q-1) + k - |\mathcal{M} \cap H| \\
&= \binom{k}{2}(q-1) + k - \Big| \bigcup_{0 \leq i \leq r < j \leq k} \ell_{i,j} \Big| - \Big| \bigcup_{r+1 \leq i < j \leq k} \{Q_{i,j}\} \Big| \\
&= \binom{k}{2}(q-1) + k - \binom{r}{2}(q-1) - r + \binom{k-r}{2} \\
&= \frac{1}{2}(k-r)((k+r-1)q - 2k + 4).
\end{aligned}$$

The numbers $A_i(\mathcal{C})$ follow from Lemma 5.2, taking into account that for every hyperplane we need to count $q-1$ distinct codewords, which correspond to all the nonzero multiples. □

Example 5.5. We explain now in details the situation for $k = 3$. The construction of the minimal cutting blocking set of Theorem 5.4 corresponds to the union of three lines ℓ_1, ℓ_2, ℓ_3 in the projective plane $PG(2, q)$ with trivial intersection, that is $\ell_1 \cap \ell_2 \cap \ell_3 = \emptyset$. We write $\{P_{i,j}\} = \ell_i \cap \ell_j$ for $1 \leq i < j \leq 3$. Here hyperplanes are lines and for any line ℓ there are three possibilities: it can coincide with one of the lines ℓ_i's, it can contain one of the $P_{i,j}$'s, or none of them. The three cases give weights $f_{q,3}(2) = 2q-1$, $f_{q,3}(1) = 3q-2$ and $f_{q,3}(0) = 3q-3$. This code for $q \geq 3$ is a three-weight code with weight distribution $A_0 = 1$, $A_{2q-1} = 3(q-1)$, $A_{3q-3} = (q-1)^3$ and $A_{3q-2} = 3(q-1)^2$, and for $q = 2$ it is a two-weight code with weight distribution $A_0 = 1$, $A_3 = 4$ and $A_5 = 3$.

Remark 5.6. The family of codes described in Theorem 5.3 has been constructed independently also in [9]. However, in that paper the authors provided only the construction for $q \geq k + 2$ and they did not study the reducedness, nor find the weight distributions. This suggests that the geometric point of view allows to analyze better the properties of minimal codes.

Remark 5.7. The construction of Theorem 5.4 for dimension $k = 3$ gives rise to minimal codes of shortest possible length, whenever $q < 9$. This follows from Theorem 4.10. It is not clear, however, if this is true also when $q \geq 9$.

5.1 Minimal codes of dimension 4

Here we exhibit a special construction for minimal codes of dimension 4, using cutting blocking sets in $PG(3, q)$ which have size smaller than the ones provided in Theorem 5.3.

Construction 1. Let $P_1, P_2, P_3, P_4 \in PG(3, q)$ be points in general position. Up to change of coordinates, we can assume them to be the (representatives of the) standard basis vectors. Consider the lines $\ell_i = \langle P_i, P_{i+1} \rangle$ for $i \in \{1, 2, 3, 4\}$ and the indices taken modulo 4. For the line $m_1 := \langle P_1, P_3 \rangle$, consider the sheaf of planes $\{H_\alpha \mid \alpha \in \mathbb{F}_q^*\}$ containing it, given by $H_\alpha := \{[x, y, z, \alpha y] \mid [x, y, z] \in PG(2, q)\}$, where we have removed the planes $\langle \ell_1, \ell_2 \rangle$ and $\langle \ell_3, \ell_4 \rangle$. For the line $m_2 := \langle P_2, P_4 \rangle$, we do the same, and take the sheaf of planes $\{K_\alpha \mid \alpha \in \mathbb{F}_q^*\}$ containing it, given by $K_\alpha := \{[x, y, \alpha x, z] \mid [x, y, z] \in PG(2, q)\}$, where we have removed the planes $\langle \ell_1, \ell_4 \rangle$ and $\langle \ell_2, \ell_3 \rangle$. Now, for every $\alpha \in \mathbb{F}_q^*$ compute $H_\alpha \cap K_\alpha = \{[x, y, \alpha x, \alpha y] \mid [x, y] \in PG(1, q)\}$. We fix a $\beta \in \mathbb{F}_q^*$, and take the point

$$Q_{\beta,\alpha} := [1, \beta, \alpha, \beta\alpha].$$

Note that $Q_{\beta,\alpha} \in (H_\alpha \cap K_\alpha) \setminus (m_1 \cup m_2)$ for every $\alpha \in \mathbb{F}_q^*$. Moreover, the points $Q_{\beta,\alpha}$ are all on the line $\ell_\beta := \langle [1, \beta, 0, 0], [0, 0, 1, \beta] \rangle = \{[x, \beta x, y, \beta y] \mid [x, y] \in PG(1, q)\}$.

With this notation we define $\mathcal{M}_\beta$ to be the set

$$\mathcal{M}_\beta := \ell_1 \cup \ell_2 \cup \ell_3 \cup \ell_4 \cup \{Q_{\beta,\alpha} \mid \alpha \in \mathbb{F}_q^*\}.$$

Theorem 5.8. *The set $\mathcal{M}_\beta$ is a minimal cutting blocking set in $PG(3, q)$, for every $\beta \in \mathbb{F}_q^*$.*

Proof. Let H be a hyperplane of $PG(3,q)$, that is a plane. We call $\mathcal{N}$ the union of the four lines. First, it is easy to see that if H contains a line ℓ_i, then $\langle H \cap \mathcal{M} \rangle$ is an hyperplane, since it contains at least another point not on ℓ_i. Suppose that H meets a line ℓ_i in only one point R_i distinct from P_i and P_{i+1}. Without loss of generality, we can assume $i = 1$. Hence $\langle \mathcal{M}_\beta \cap H \rangle \supseteq \langle \mathcal{N} \cap H \rangle =: \Lambda$. Now, observe that $\langle \Lambda, P_1 \rangle$ contains at least the line ℓ_1, a point on ℓ_2 distinct from P_2 and another point on ℓ_4 different from P_1. Hence

$$\langle \Lambda, P_1 \rangle \supseteq \langle \ell_1, \ell_2, \ell_4 \rangle \supseteq \langle P_1, P_2, P_3, P_4 \rangle = PG(3,q),$$

which implies $\dim(\Lambda) = 2$. It remains to analyze the only case left, which is $\mathcal{N} \cap H = \{P_1, P_3\}$ (the case $\mathcal{N} \cap H = \{P_2, P_4\}$ is symmetric). In this case, necessarily $H = H_\alpha$, for some $\alpha \in \mathbb{F}_q^*$, and so $\langle H \cap \mathcal{M}_\beta \rangle = \langle P_1, P_3, Q_{\beta,\alpha} \rangle = H_\alpha = H$. This shows that $\mathcal{M}_\beta$ is a cutting blocking set.

It remains to prove that $\mathcal{M}_\beta$ is minimal. Clearly, we can not remove any of the points $Q_{\beta,\alpha}$'s, since $\mathcal{M}_\beta \setminus \{Q_{\beta,\alpha}\}$ meets H_α only in P_1 and P_3. The same happens if we remove one of the points P_i's. Indeed, $\mathcal{M}_\beta \setminus \{P_1\}$ meets H_α only in $\{P_3, Q_{\beta,\alpha}\}$, for every $\alpha \in \mathbb{F}_q^*$ (and symmetrically with $\mathcal{M}_\beta \setminus \{P_3\}$). The same happens with the hyperplanes K_α's if we remove P_2 or P_4. It is left to prove that if we remove a point R on one of the lines, say ℓ_1, the resulting set $\mathcal{M}_\beta \setminus \{R\}$ is not cutting. Take the point P_3 and consider the sheaf of planes containing the line $\langle P_3, R \rangle$. Every plane of this sheaf meets the line ℓ_4 in exactly one point. Hence, the sheaf is parametrized by the points on the line ℓ_4, and we can write it as $\{H_S \mid S \in \ell_4\}$, where clearly $H_S = \langle P_3, R, S \rangle$. Consider now the intersection between H_S and $\tilde{\mathcal{N}} := \mathcal{N} \setminus \{R\}$, i.e. the union of all the four lines without the point R. If $S = P_1$ then $H_{P_1} \cap \tilde{\mathcal{N}} = (\ell_1 \setminus \{R\}) \cup \{P_3\}$, which spans a hyperplane. It is not difficult to see that in all the remaining q cases it spans a line. However, every H_S meets the line ℓ_β in exactly a point. Hence it contains at most one of the $Q_{\beta,\alpha}$'s. However, we have q hyperplanes H_S and only $q-1$ points. Therefore, necessarily there exists $S \in \ell_4$ such that $H_S \cap \mathcal{M}_\beta = \{P_3, R, S\}$ and thus $\mathcal{M}_\beta \setminus \{R\}$ is not cutting. □

Corollary 5.9. *For every $\beta \in \mathbb{F}_q^*$, Construction 1 produces a $[5q-1, 4, 3q-2]_q$ reduced minimal code $\mathcal{C}_\beta$.*

Proof. Using the characterization result of Theorem 3.4, clearly the code obtained by the minimal cutting blocking set M_β via (Φ, Ψ) is a $[5q-1, 4]_q$ reduced minimal code. It is left to determine the minimum distance of $\mathcal{C}_\beta$, which corresponds via (Φ, Ψ) to the value $(5q-1) - \max\{|H \cap \mathcal{M}_\beta| : \dim(H) = 2\}$. Any hyperplane H can contain at most two of the lines ℓ_i's and ℓ_β, since every three of them span the whole space $PG(3,q)$. If it contains none of them, then $|\mathcal{M}_\beta \cap H| \leq 5$. If H contains only one of the ℓ_i's then $|\mathcal{M}_\beta \cap H| \leq q+3$. In the case H contains only ℓ_β we also have $|\mathcal{M}_\beta \cap H| \leq q+3$. Finally, the only case in which H contains a pair of lines is when $H = \langle \ell_i, \ell_{i+1} \rangle$, for $i \in \{1,2,3,4\}$ (where the indices are taken modulo 4). In this case, we can see that H does not contain any of the points $Q_{\alpha,\beta}$, and therefore, $|H \cap M_\beta| = 2q+1$. For every prime power q, the maximum among these values is given by $2q+1$, and this concludes the proof. □

We conclude this subsection with explanatory examples.

Example 5.10. According to Corollary 5.9, Construction 1 for $q = 2$ and $\beta = 1$ gives rise to a minimal $[9, 4, 4]_2$ code, whose generator matrix is

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

It was proved by computer search with MAGMA [14] that 9 is the shortest length that a minimal code of dimension 4 can have over $\mathbb{F}_2$. Moreover, always with MAGMA we observed that this is the unique $[9, 4]_2$ minimal code up to equivalence.

Example 5.11. For $q = 3$ and $\beta = 2$, Construction 1 gives the $[14, 4, 7]_3$ reduced minimal code $\mathcal{C}_2$ whose generator matrix is

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

5.2 Minimal codes of dimension 5

Here we show another special construction for minimal codes of dimension 5, using cutting blocking sets in $PG(4, q)$ whose size is smaller than the one provided in Theorem 5.3. When $q = 2$, we provide also an alternative construction for minimal codes of dimension 5 as minimal blocking sets in $PG(4, 2)$.

Construction 2. Let P_1, P_2, P_3, P_4, P_5 be five points in general position in $PG(4, 2)$. Without loss of generality, we can assume that they are the (representatives of the) standard basis vectors. Consider the lines $\ell_i = \langle P_i, P_{i+1} \rangle$ for $i \in \{1, 2, 3, 4, 5\}$, where the indices are taken modulo 5. Consider now for $i \in \{1, 2, 3, 4\}$ a point $Q_i \in \ell_i \setminus \{P_i, P_{i+1}\}$, and define the lines $m_1 := \langle Q_1, Q_3 \rangle$, $m_2 := \langle Q_2, Q_4 \rangle$ and $m_3 := \langle Q_1, Q_4 \rangle$.

With this notation, we define the set $\mathcal{M} := \ell_1 \cup \ell_2 \cup \ell_3 \cup \ell_4 \cup \ell_5 \cup m_1 \cup m_2 \cup m_3$. We will refer to the above construction also as the *pentagonal construction*.

Theorem 5.12. *The set $\mathcal{M}$ defined in Construction 2 is a cutting blocking set in $PG(4, q)$.*

Proof. We first write $\mathcal{N} = \ell_1 \cup \ell_2 \cup \ell_3 \cup \ell_4 \cup \ell_5$ and $\mathcal{N}' = m_1 \cup m_2 \cup m_3$. Let H be a hyperplane, define the spaces $\Lambda := \langle H \cap \mathcal{M} \rangle$ and $\Lambda_1 := \langle H \cap \mathcal{N} \rangle$ and consider the number r of the P_i's that are also in H. Clearly $r \in \{0, 1, 2, 3, 4\}$. If $r = 4$ it is clear that $\langle H \cap \mathcal{N} \rangle = H$. If $r = 0$, then it is easy to see that $\langle \Lambda_1, P_1 \rangle$ contains $\mathcal{N}$, and hence it is the whole $PG(4, q)$. Therefore $\dim(\Lambda_1) = \dim(\Lambda) = 3$. Also if $r = 1$, that is $P_1 \in H$, then $\langle \Lambda_1, P_2 \rangle$ turns out to be the whole space, hence $\dim(\Lambda) = 3$. Now assume

that $r = 3$. Then we have two possibilities for the indices of these points. They can be consecutive (modulo 5), say P_1, P_2, P_3, in which case H contains their span plus a point on ℓ_4. Clearly this implies $\dim(\Lambda) = \dim(\Lambda_1) = 3$. The second case is when the indices are of the form $i, i+1, i+3$, i.e. $\langle \ell_i, P_{i+3} \rangle \subseteq H$. Then H intersects at least one line $m_j = \langle Q_t, Q_s \rangle$ skew to ℓ_i in another point R distinct from Q_1, Q_2, Q_3, Q_4. Consider then $\langle \Lambda, Q_s \rangle \supseteq \langle \ell_i, m_j, P_{i+3} \rangle = PG(4, q)$. Hence also in this case $\dim(\Lambda) = 3$. It remains to show the case $r = 2$. If the indices of these two points are consecutive, then H contains a line ℓ_i and two more points, one on ℓ_{i+2} and one on ℓ_{i+3}. Clearly in this case $\langle \Lambda_1, P_{i+3} \rangle \supseteq \langle \ell_i, \ell_{i+2}, \ell_{i+3} \rangle = PG(4, q)$, and we conclude also in this case. Suppose now that the two points in H are P_i and P_{i+2}. Then H will also intersect the line ℓ_{i+3} in a point R, and at least a line $m_j = \langle Q_t, Q_s \rangle$ in a point S, which is different from Q_t and Q_s. Then it is easy to see that also in this case $\langle \Lambda, Q_s \rangle = PG(4, q)$, which finally shows that $\mathcal{M}$ is cutting. □

Corollary 5.13. *Construction 2 produces a* $[8q - 3, 5, 4q - 3]_q$ *minimal code.*

Proof. The fact that from Construction 2 we obtain a $[8q - 3, 5]_q$ minimal code, simply follows from the characterization result of Theorem 3.4. The minimum distance can be computed observing that a hyperplane H can contain at most 4 lines among the defining lines of $\mathcal{M}$, and this happens only in five cases: $H_1 = \langle \ell_1, \ell_2, m_2, m_3 \rangle$, $H_2 = \langle \ell_3, \ell_4, m_1, m_3 \rangle$, $H_3 = \langle \ell_1, \ell_2, \ell_3, m_1 \rangle$, $H_4 = \langle \ell_2, \ell_3, \ell_4, m_2 \rangle$ and $H_5 = \langle \ell_1, \ell_4, \ell_5, m_3 \rangle$. In these cases we have $|\mathcal{M} \cap H_i| = 4q$, and the weights of the associated codewords are $8q - 3 - 4q = 4q - 3$. In all the other cases, it is not difficult to see that any other hyperplane contains a smaller number of points of $\mathcal{M}$. Hence, the minimum distance of the code is $4q - 3$. □

In the binary case, the pentagonal construction gives the $[13, 5, 5]_2$ reduced minimal code whose generator matrix is

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

By MAGMA computations, we can observe that 13 is the shortest length for a binary minimal code of dimension 5.

For $q = 3$ the code obtained is $[21, 5, 9]_3$, but with the aid of MAGMA we found a $[20, 5, 9]_3$ minimal code. Hence, in general Construction 2 does not provide the smallest cutting blocking set in $PG(4, q)$.

In this sequel, we provide a construction of minimal codes of dimension 5 over $\mathbb{F}_2$, using cutting blocking sets in $PG(4, 2)$, different from the pentagonal construction. We will refer to it as the *hexagonal construction*.

Construction 3. Let $\{P_1, P_2, P_3, P_4, P_5, P_6\}$ be a projective frame in $PG(4, 2)$. Without loss of generality, we can assume P_1, P_2, P_3, P_4, P_5 to be the (representatives of the)

standard basis vectors and $P_6 = [1,1,1,1,1]$. Consider the lines $\ell_i = \langle P_i, P_{i+1} \rangle$ for $i \in \{1,2,3,4,5,6\}$, where the indices are taken modulo 6. Let $Q := [1,0,1,0,1]$.

The set $\mathcal{M} := \ell_1 \cup \ell_2 \cup \ell_3 \cup \ell_4 \cup \ell_5 \cup \ell_6 \cup \{Q\}$ is a minimal cutting blocking set in $PG(4,2)$. This is not difficult to verify by hand or computer search.

This construction produces the $[13,5,5]_2$ reduced minimal code generated by the following matrix:

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

With the aid of MAGMA we observed that the code constructed in this way and the one obtained from the pentagonal construction are the only two $[13,5,5]_2$ minimal codes up to equivalence.

The hexagonal construction can be adapted to $q = 3$. It gives a $[20,5,9]_3$ minimal codes, which is the shortest code that we could obtain. Unfortunately, it seems difficult to generalize it for minimal codes of dimension 5 over $\mathbb{F}_q$, for $q > 3$.

6 Conclusions and open problems

In this paper we characterized minimal linear codes from a geometrical point of view. Note that this characterization has been independently and simultaneously remarked also by Tang *et al.* in [36]. This geometric approach allowed to prove new bounds on the length and the minimum distance of minimal codes, depending on their dimension and on the cardinality of the underlying field. Moreover, we proved that the family of minimal linear codes is asymptotically good. However, calculations in MAGMA show that our lower bound on the length is not sharp, so that there is still room for improvement.

Problem 1. Is it possible to prove a sharp lower bound on the length of a minimal linear code?

The already cited existence result of Chabanne *et al.* of infinite sequences of minimal linear codes with fixed rate and growing length is unfortunately not constructive, and we are not aware of such a construction in the literature. The geometrical interpretation of minimal linear codes as cutting blocking sets should provide a way to construct codes with a length growing linearly in the dimension, by reducing as much as possible the number of points. However, in the construction by the tetrahedron of Theorem 5.3, the length grows as the square of the dimension, and the arguments in Subsection 5.1 do not seem generalizable to higher dimensions.

Problem 2. Is it possible to give an explicit construction of an infinite sequence of minimal linear codes whose lengths are growing linearly in the dimension?

Problem 3. How to generalize Construction 1 to dimension greater than 4?

Problem 4. How to generalize the pentagonal construction (Construction 2) to dimension greater than 5? How to generalize the hexagonal construction (Construction 3) to every prime power q and to dimension greater than 5?

Finally, in all our constructions of minimal codes, and in other constructions provided in [8, 9, 12, 36], we observed that the minimum distance satisfies $d \geq (k-1)(q-1)+1$, where this bound is met with equality in all our constructions of reduced minimal codes. Therefore, also motivated by Remark 4.4, where we observed that the bound of Theorem 4.3 is not sharp, we propose the following conjecture.

Conjecture. Let $\mathcal{C}$ be an $[n,k,d]_q$ minimal code. Then

$$d \geq (k-1)(q-1)+1.$$

If the above conjecture is true, then, combining it with the Griesmer bound, as we did for Corollary 4.5, we would get a new lower bound on the length of minimal codes, namely

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

It is easy to see that this lower bound would improve Theorem 4.1 for every set of parameters. This is not in contrast with our experimental results, which show that the bound of Theorem 4.1 is not sharp.

References

[1] E. Agrell. On the Voronoi neighbor ratio for binary linear block codes. *IEEE Transactions on Information Theory*, 44(7):3064–3072, 1998.

[2] A. Alahmadi, C. Güneri, H. Shoaib, and P. Solé. Long quasi-polycyclic t-CIS codes. *arXiv preprint arXiv:1703.03109*, 2017.

[3] A. Alahmadi, F. Özdemir, and P. Solé. On self-dual double circulant codes. *Designs, Codes and Cryptography*, 86(6):1257–1265, 2018.

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

[5] E. Assmus. The category of linear codes. *IEEE Transactions on information theory*, 44(2):612–629, 1998.

[6] S. Ball. *Finite geometry and combinatorial applications*, volume 82. Cambridge University Press, 2015.

[7] S. Ball and A. Blokhuis. On the size of a double blocking set in PG(2, q). *Finite Fields and their Applications*, 2(2):125–137, 1996.

[8] D. Bartoli and M. Bonini. Minimal linear codes in odd characteristic. *IEEE Transactions on Information 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] A. Bishnoi, S. Mattheus, and J. Schillewaert. Minimal multiple blocking sets. *The Electronic Journal of Combinatorics*, 25(4):4–66, 2018.

[11] G. R. Blakley. Safeguarding cryptographic keys. *Proceedings of the 1979 AFIPS National Computer Conference*, 48:313–317, 1979.

[12] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *arXiv preprint arXiv:1907.04626*, 2019.

[13] M. Borello and W. Willems. Group codes over fields are asymptotically good. *arXiv preprint arXiv:1904.10885*, 2019.

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

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

[16] H. Chabanne, G. Cohen, and A. Patey. Towards secure two-party computation from the wire-tap channel. In *International Conference on Information Security and Cryptology*, pages 34–46. Springer, 2013.

[17] S. Chang and J. Y. Hyun. Linear codes from simplicial complexes. *Designs, Codes and Cryptography*, 86(10):2167–2181, 2018.

[18] C. Chen, W. W. Peterson, and E. Weldon Jr. Some results on quasi-cyclic codes. *Information and Control*, 15(5):407–423, 1969.

[19] G. D. Cohen, S. Mesnager, and A. Patey. On minimal and quasi-minimal linear codes. In *IMA International Conference on Cryptography and Coding*, pages 85–98. Springer, 2013.

[20] C. Ding. Linear codes from some 2-designs. *IEEE Transactions on information theory*, 61(6):3265–3275, 2015.

[21] C. Ding, D. R. Kohel, and S. Ling. Secret-sharing with a class of ternary codes. *Theoretical Computer Science*, 246(1-2):285–298, 2000.

[22] C. Ding, C. Li, N. Li, and Z. Zhou. Three-weight cyclic codes and their weight distributions. *Discrete Mathematics*, 339(2):415–427, 2016.

[23] J. H. Griesmer. A bound for error-correcting codes. *IBM J. Research Develop.*, 4:532–542, 1960.

[24] Z. Heng, C. Ding, and Z. Zhou. Minimal linear codes over finite fields. *Finite Fields and Their Applications*, 54:176–196, 2018.

[25] W. C. Huffman and V. Pless. *Fundamentals of Error Correcting Codes*. Cambridge university press, 2010.

[26] E. Karnin, J. Greene, and M. Hellman. On secret sharing systems. *IEEE Transactions on Information Theory*, 29(1):35–41, 1983.

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

[28] J. L. Massey. Some applications of coding theory in cryptography. *Codes and Ciphers: Cryptography and Coding IV*, pages 33–47, 1995.

[29] R. J. McEliece and D. V. Sarwate. On sharing secrets and Reed-Solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

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

[31] 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.

[32] S. Mesnager and A. Sınak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Trans. Inf. Theory*, to appear.

[33] B. Segre. Curve razionali normali e k-archi negli spazi finiti. *Annali di Matematica Pura ed Applicata*, 39(1):357–379, 1955.

[34] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[35] R. C. Singleton. Maximum distance q-ary codes. *IEEE Transactions on Information Theory*, 10:116–118, 1964.

[36] C. Tang, Y. Qiu, Q. Liao, and Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. *arXiv preprint arXiv:1911.09867*, November 25th 2019.

[37] 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. Translated from the Russian by the authors.

[38] O. Veblen and J. W. Young. *Projective geometry. Vol. 1.* Blaisdell Publishing Co. Ginn and Co. New York-Toronto-London, 1965.

[39] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Transactions on Information Theory*, 52(1):206–212, 2005.