Small Strong Blocking Sets by Concatenation

Daniele Bartoli, Martino Borello

Small Strong Blocking Sets by Concatenation

Daniele Bartoli[1] and Martino Borello[2]

[1]Università degli Studi di Perugia, Italy
[2]Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, France

Abstract

Strong blocking sets and their counterparts, minimal codes, attracted lots of attention in the last years. Combining the concatenating construction of codes with a geometric insight into the minimality condition, we explicitly provide infinite families of small strong blocking sets, whose size is linear in the dimension of the ambient projective spaces. As a byproduct, small saturating sets are obtained.

Introduction

Nonlinear combinatorial objects, as arcs, saturating sets, blocking sets, have been broadly investigated in finite geometry not only for theoretical reasons but also for their deep connections with more applied areas of mathematics as coding theory and cryptography.

Denote by $\mathrm{PG}(N,q)$ the N-dimensional projective space over the finite field $\mathbb{F}_q$. A point set $\mathcal{B}$ is called a *blocking set* if any hyperplane of $\mathrm{PG}(N,q)$ contains at least one point of $\mathcal{B}$. A blocking set $\mathcal{B}$ is *strong* if any hyperplane section of $\mathcal{B}$ generates the hyperplane itself; see [10, 16, 19]. Although blocking sets were deeply investigated in the last decades (see for example [9] and references therein), much less is known about strong blocking sets.

Strong blocking sets are the geometrical counterpart of an important class of error correcting codes, the so-called minimal codes; see [1, 31]. A codeword is said to be *minimal* if its support does not contain the support of any other non-proportional nonzero codeword. A code for which every codeword is minimal is called *minimal*. The importance of minimal codes relies on their connection with cryptography and coding theory. In fact, minimal codewords in linear codes were used by Massey [26, 27] to determine the access structure in a code-based secret sharing scheme. Previously, minimal codewords were studied in connection with decoding algorithms [22]. For a given linear code, describing the whole set of minimal codewords can be a challenging task, even for special classes of linear codes. For this reason, in the last years, minimal codes attracted attention and many of the constructions are connected with few-weight codes (see e.g. [28–30]) or exploit the so-called Ashikhmin-Barg condition [4]. Bounds on the parameters of a minimal code were considered in [1, 2, 12, 14, 25]. Only recently, minimal codes were studied through their connection with strong blocking sets [1, 10, 25, 31]. It is worth mentioning that minimal codes form a class of asymptotically good codes [1, 14]. Families of short minimal codes (via their equivalence with strong blocking sets) were provided in [5, 21] also in connection with line spreads or sets of lines in higgledy-piggledy arrangement [19]. Apart from a few small dimensional cases, none of these constructions were effective. On the other hand, minimal codes whose length is quadratic in the dimension are constructed explicitly in [1, 2]. In a very recent work [3], minimal rank-metric codes are investigated, in connection with linear sets. As a byproduct, new constructions and perspectives on minimal codes are obtained.

One of the main open questions concerning strong blocking sets (in relation to the parameters of the associated minimal code) concerns the explicit constructions of infinite families of strong blocking sets whose size grows linearly with the dimension of the ambient projective space.

In this paper we exploit a machinery introduced in [14] to provide families of asymptotically good minimal codes via codes concatenation. We obtain explicit constructions of small strong blocking sets in projective spaces, whose size linearly depends on the dimension of the ambient space. It is worth mentioning that in some cases concatenation provides the smallest known strong blocking sets. As a byproduct, we obtain constructions of saturating sets for specific dimensions whose size is the smallest one can find in the literature.

The aim of this paper is two-fold. On the one hand we provide a more geometric insight of the concatenation method, discussing some relevant features of both outer and inner codes. On the other hand we show how explicit families of asymptotically good minimal codes and their corresponding small strong blocking sets can be obtained via this machinery.

Outline. The paper is organized into four sections. Section 1 contains the preliminaries on minimal codes, strong blocking sets and the known bounds on their size. In Section 2 we present a geometric interpretation of the well-known Ashikhmin-Barg condition, we introduce an analogue of the result of Ashkhmin and Barg in the context of concatenated codes – that we call Outer AB condition – and we present some explicit construction of small strong blocking sets. Section 3 is devoted to some asymptotic results, both theoretical and constructive. Finally, we apply some of the previous results to the study of ρ-saturating sets in Section 4.

1 Background

1.1 Minimal codes

For a vector $v \in \mathbb{F}_q^n$, the *Hamming weight* of v is $\mathrm{wt}(v) := |\sigma(v)|$, where $\sigma(v) := \{i \in \{1, \dots, n\} \mid v_i \neq 0\}$ is the Hamming support of v. An $[n, k, d]_q$ *linear code* $\mathcal{C}$ is a subspace of $\mathbb{F}_q^n$ of *dimension* k with *minimum weight*

$$d = d(\mathcal{C}) := \min\{\mathrm{wt}(c) \mid c \in \mathcal{C},\, c \neq 0\}$$

and its elements are called *codewords*. Normally, these are the fundamentals parameters for error correcting purposes, but in our context the *maximum weight* $w(\mathcal{C}) := \max\{\mathrm{wt}(c) \mid c \in \mathcal{C}\}$ will play a crucial role. A *generator matrix* G of $\mathcal{C}$ is a matrix whose rows form a basis for $\mathcal{C}$. A linear code $\mathcal{C}$ is called *projective* (resp. *non-degenerate*) if in one (and thus in all) generator matrix G of $\mathcal{C}$ no two columns are proportional (resp. no column is the zero vector). Two linear codes are said to be (monomially) *equivalent* if there is an a monomial transformation sending one into the other. A family of codes is said *asymptotically good* if it admits an infinite subfamily of increasing length with both dimension and minimum weight growing linearly in the length.

Definition 1.1. A nonzero codeword c of a code $\mathcal{C}$ over $\mathbb{F}_q$ is called *minimal* if every nonzero codeword c' in $\mathcal{C}$ with $\sigma(c') \subseteq \sigma(c)$ is λc for some nonzero $\lambda \in \mathbb{F}_q$. A linear code $\mathcal{C}$ is a *minimal code* if all its codewords are minimal.

Example 1.2. A *simplex code* $\mathcal{S}_q(k)$ of dimension k over $\mathbb{F}_q$ is a code defined up to equivalence as follows: its generator matrix is obtained by choosing as columns a nonzero vector from each 1-dimensional subspace of $\mathbb{F}_q^k$. It is easy to prove that its parameters are $[(q^k-1)/(q-1), k, q^{k-1}]_q$ and that all nonzero codewords have the same weight. This last property implies that $\mathcal{S}_q(k)$ is minimal.

In this paper, the *concatenation of codes*, a standard way of combining codes to obtain a code of larger length, plays a crucial role. To describe this process, let n, k be two integers such that $n \geq k$ and let $\pi : \mathbb{F}_{q^k} \to \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear injection. In the concatenation process, $\mathbb{F}_{q^k}$-linear codes in $\mathbb{F}_{q^k}^N$ are called *outer codes* and the $\mathbb{F}_q$-linear code $\mathcal{I} := \pi(\mathbb{F}_{q^k})$ is called *inner code*. If $\mathcal{C}$ is an $\mathbb{F}_{q^k}$-linear code of length N and $\mathbb{F}_{q^k}$-dimension K, then the $\mathbb{F}_q$-linear code

$$\mathcal{I} \square_\pi \mathcal{C} := \{(\pi(c_1), \ldots, \pi(c_n)) \mid (c_1, \ldots, c_n) \in \mathcal{C}\} \subseteq \mathbb{F}_q^{N \cdot n}$$

is called the concatenation of $\mathcal{C}$ with $\mathcal{I}$ by π, or simply the *concatenated code*. This last depends on the choice of π, but there are some of its properties independent of π. For example, $\mathcal{I} \square_\pi \mathcal{C}$ is an $[N \cdot n, K \cdot k, \geq d(\mathcal{I}) \cdot d(\mathcal{C})]_q$ for every choice of π (see for example [32, §1.2.3.]). If the properties in which we are interested do not depend on π, we will simply denote by $\mathcal{I} \square \mathcal{C}$ the concatenated code.

1.2 Strong blocking sets

For $k > 1$, the *finite projective geometry* of dimension $k-1$ and order q, denoted by $\mathrm{PG}(k-1, q)$ is

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

where $u \sim v$ if and only if $u = \lambda v$ for some nonzero $\lambda \in \mathbb{F}_q$. A *hyperplane* is a subspace $\mathcal{H} \subseteq \mathrm{PG}(k-1, q)$ of codimension 1. A *projective* $[n, k, d]_q$ *system* $\mathcal{P}$ is a finite set of n points (counted with multiplicity) of $\mathrm{PG}(r-1, q)$ not all lying on a hyperplane and such that

$$d = n - \max_{\mathcal{H} \text{ hyperplane}} \{|\mathcal{H} \cap \mathcal{P}|\}.$$

For an $[n, k, d]_q$ non-degenerate code $\mathcal{C}$ with generator matrix G, let $\mathcal{P}$ be set of columns of G, considered as points in $\mathrm{PG}(k-1, q)$. For $u = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$, $\mathrm{wt}(uG) = n - |\mathcal{H} \cap \mathcal{P}|$, where $\mathcal{H}$ is the hyperplane defined by the equation $u_1x_1 + \ldots + u_kx_k = 0$. So $\mathcal{P}$ is a projective $[n, k, d]_q$ system. For the same reason, from a projective $[n, k, d]_q$ system $\mathcal{P}$ one can obtain an $[n, k, d]_q$ code by choosing a representative for any point of $\mathcal{P}$ and considering the code generated by the matrix having these representatives as columns. This gives the well-known correspondence (see for example [32, Theorem 1.1.6]) between equivalence classes of non-degenerate $[n, k, d]_q$ linear codes and equivalence classes of projective $[n, k, d]_q$ systems.

Minimal codes correspond to $[n, k, d]_q$ systems with additional properties.

Definition 1.3 ([16])**.** A subset $\mathcal{M} \subseteq \mathrm{PG}(k-1, q)$ is called *strong blocking set* if for every hyperplane $\mathcal{H}$ of $\mathrm{PG}(k-1, q)$ we have $\langle \mathcal{M} \cap \mathcal{H} \rangle = \mathcal{H}$.

Example 1.4. The whole $\mathrm{PG}(k-1, q)$ is, clearly, a strong blocking set.

Strong blocking sets were introduced in [16]. In [19], strong blocking sets are referred to as generator sets and they are constructed as union of disjoint lines. In [10] they were reintroduced, with the name of *cutting blocking sets*, in order to construct a particular family of minimal codes. In [1] and [31] it was independently shown that strong blocking sets are the geometrical counterparts of minimal codes: the above correspondence between non-degenerate codes and projective systems restricts to a correspondence between equivalence classes of projective $[n, k, d]_q$ minimal codes and equivalence classes of subsets of $\mathrm{PG}(k-1, q)$ that are strong blocking sets (since in this paper we are interested in short minimal codes or, equivalently, in small strong blocking sets in projective spaces, it is not restrictive to narrow down to projective codes, which correspond to projective systems in which all the points have multiplicity one, that is subsets). Clearly, the simplex codes defined in Example 1.2 correspond to the strong blocking sets defined in Example 1.4.

1.3 Bounds on the size of strong blocking sets

Given the above equivalence between minimal codes and strong blocking sets, for the sake of brevity, in this section we will only state the bounds for the size of the latter, but clearly these bounds are also on the length of minimal codes.

For a given dimension and a base field, simplex codes are the longest projective minimal codes, as the whole projective space is the largest strong blocking set. Since from a given strong blocking set we can always obtain a larger one by adding any set of points, it is interesting to know how small a strong blocking set can be.

A $(k-1)$-*fold blocking set* in $\mathrm{PG}(k-1,q)$ is a subset $\mathcal{B}$ of points such that every hyperplane meets $\mathcal{B}$ in at least $k-1$ points. Clearly, a strong blocking set in $\mathrm{PG}(k-1,q)$ is a $(k-1)$-fold blocking set. By a well-known result of Beutelspacher on $(k-1)$-fold blocking sets (see [7, Theorem 2]), the size of a strong blocking set in $\mathrm{PG}(k-1,q)$, is at least $(q+1)(k-1)$, if $k \leq q+1$. The same result holds without restrictions on k:

Theorem 1.5 ([2])**.** The size of a strong blocking set in $\mathrm{PG}(k-1,q)$ is at least $(q+1)(k-1)$.

However, this lower bound is not sharp in general, as shown in [2].
There are many constructions of strong blocking sets of small size. One usual way to obtain them is to consider set of lines: a set of lines of $\mathrm{PG}(k-1,q)$ is in higgledy-piggledy arrangement if the union of their point sets is a strong blocking set of $\mathrm{PG}(k-1,q)$. Using higgledy-piggledy lines one can get strong blocking sets of size $(q+1)(2k-2)$ in $\mathrm{PG}(k-1,q)$, whenever $2k \leq q+2$ (see [19, Theorem 14]). Note that the above result cannot be used to obtain strong blocking sets for large dimensions. There are stronger results for small dimensions: see [16, 19] for $k=3,4$, [6] for $k=5$, and [5] for $k=6$.

The best bounds concerning the size of smallest strong blocking sets are summarized in the following theorem, which is a refinement of a result in [12].

Theorem 1.6 ([21])**.** The size of the smallest strong blocking sets in $\mathrm{PG}(k-1,q)$ is at most

$$\begin{cases} \frac{2k-1}{\log_2(4/3)}, & \text{if } q=2; \\ (q+1)\left\lceil \frac{2}{1+\frac{1}{(q+1)^2\ln q}}(k-1)\right\rceil, & \text{otherwise.} \end{cases}$$

The proof of the above theorem is probabilistic. Explicit small constructions can be found in [1, 2]: they are of size ck^2q, for some $c \geq 2/9$. However, from Theorem 1.5 and Theorem 1.6 we know that a construction where the size is linear in k (and q) does exist. Note that this would yield explicit construction of asymptotically good families of minimal codes, by the lower bounds on the minimum weight (see [2, Theorem 2.8]). In [15, §2.A] (for $q=2$) and [13, §2.4] (for all others cases), such a construction is sketched, and it employs the concatenation. However, these results seem to have gone unnoticed to date, in the context of both minimal codes and strong blocking sets. The main aim of this paper is to highlight the power of this approach by delving into it.

2 Strong blocking sets by concatenation

2.1 Geometric interpretation of the Ashikhmin-Barg condition

First, we provide an easy geometrical interpretation of part 3 of [4, Lemma 2.1], known as Ashikhmin-Barg condition, which provides a sufficient condition for a subset of points to be strong blocking set. Even if it is a direct consequence of the geometrical interpretation of minimal codes described above, we give a direct proof using only geometrical arguments.

Lemma 2.1 (Ashikhmin-Barg)**.** Let $\mathcal{B}$ be a subset of $\mathrm{PG}(k-1,q)$ of cardinality n and denote m (resp. M) the minimum (resp. the maximum) number of points of $\mathcal{B}$ contained in a hyperplane of $\mathrm{PG}(k-1,q)$. If

$$\frac{n-M}{n-m} > \frac{q-1}{q} \tag{1}$$

then $\mathcal{B}$ is a strong blocking set.

Proof. Suppose that $\mathcal{B} \subseteq \mathrm{PG}(k-1,q)$ is not a strong blocking set. Then there exists a hyperplane $\mathcal{H}$ such that $\mathcal{H} \cap \mathcal{B}$ is contained in a subspace $\mathcal{S}$ of codimension 2. Consider the q hyperplanes through $\mathcal{S}$ distinct from $\mathcal{H}$. If $x = |\mathcal{H} \cap \mathcal{B}|$, then

$$n = |\mathcal{B}| \leq x + q(M-x) = qM - (q-1)x \leq qM - (q-1)m.$$

□

In coding theoretical language, (1) reads as follows: let $\mathcal{C}$ be the (projective) linear code of length n associated with $\mathcal{B}$. If

$$\frac{d(\mathcal{C})}{w(\mathcal{C})} > \frac{q-1}{q} \tag{2}$$

then $\mathcal{C}$ is minimal. In the sequel, we will refer to (1) and (2) as AB condition.

2.2 Outer AB condition

The concatenation process allows to get strong blocking sets by imposing a similar but weaker condition on the outer codes.

Theorem 2.2 (Outer AB condition)**.** Let $\mathcal{C}$ be an $[N,K,D]_{q^k}$ code such that

$$\frac{D}{W} > \frac{q-1}{q},$$

where $W := w(\mathcal{C})$, and $\mathcal{I}$ be an $[n,k,d]_q$ minimal code. Then the concatenated code $\mathcal{I} \square_\pi \mathcal{C}$ is a minimal code of parameters $[Nn, Kk, \geq Dd]_q$. Equivalently, the corresponding set in $\mathrm{PG}(Kk-1,q)$ is a strong blocking set of size Nn.

Proof. Let x and x' be two nonzero codewords in $\mathcal{I} \square_\pi \mathcal{C}$ such that $\sigma(x') \subseteq \sigma(x)$. Let c and c' be the codewords in $\mathcal{C}$ such that $x = (\pi(c_1), \ldots, \pi(c_N))$ and $x' = (\pi(c'_1), \ldots, \pi(c'_N))$. Clearly $\sigma(c') \subseteq \sigma(c)$. Moreover, since $\mathcal{I}$ is minimal, it exists $\lambda_i \in \mathbb{F}_q^*$ such that $c_i = \lambda_i c'_i$ whenever $i \in \sigma(c')$. Since $|\sigma(c')| \geq D$, the scalars are equal to a certain $\lambda \in \mathbb{F}_q^*$ in at least $\left\lceil \frac{D}{q-1} \right\rceil$ coordinates. So, up to a multiplication by λ^{-1}, c and c' coincides in at least $\left\lceil \frac{D}{q-1} \right\rceil$ coordinates.

Now

$$D \leq |\sigma(c')| \leq |\sigma(c)| \leq W$$

and, since $D/W > (q-1)/q$,

$$W < \frac{q}{q-1} \cdot D = D + \frac{D}{q-1} \leq D + \left\lceil \frac{D}{q-1} \right\rceil.$$

Thus

$$|\sigma(c-c')| \leq W - \left\lceil \frac{D}{q-1} \right\rceil < D,$$

which yields $|\sigma(c-c')| = 0$ and $c = c'$. Hence $\mathcal{I} \square_\pi \mathcal{C}$ is minimal. □

Remark 2.3. As one can easily see from the proof of Theorem 2.2, we may get the same result by concatenating in each coordinate with a different minimal code.

It possible to provide a more geometrical interpretation of the concatenation process. In this geometrical description of concatenated codes, companion matrices play a crucial role. Let $p(x) = x^k + \sum_{i=0}^{k-1} p_i x^i \in \mathbb{F}_q[x]$ be an irreducible monic polynomial of positive degree k and define the companion matrix of $p(x)$ as

$$A := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -p_0 & -p_1 & -p_2 & \cdots & -p_{k-1} \end{pmatrix}.$$

The $\mathbb{F}_q$-algebra $\mathbb{F}_q[A]$ is a finite field with q^k elements (see [24, Chapter 2.5]). In particular, if α is a root of $p(x)$ and $v = v_0 + v_1\alpha + \ldots + v_{k-1}\alpha^{k-1}$ is a generic element of $\mathbb{F}_q[\alpha] \cong \mathbb{F}_{q^k}$ and $\phi : \mathbb{F}_q[\alpha] \to \mathbb{F}_q^k$ is the $\mathbb{F}_q$-linear isomorphism that sends v to $[v_0, \ldots, v_{k-1}]$, then $\phi(v)A = \phi(v\alpha)$.

Remark 2.4 (Geometric insight of Theorem 2.2)**.** Let $G_{\mathcal{I}} \in \mathbb{F}_q^{k\times n}$ be a generator matrix of the inner code $\mathcal{I}$ and let $\mathbb{F}_{q^k}^* = \langle\omega\rangle$. Denote by $A \in \mathbb{F}_q^{k\times k}$ the companion matrix of the minimal polynomial of ω. For an element $\alpha \in \mathbb{F}_{q^k}$ let

$$A(\alpha) := \begin{cases} A^r \in \mathbb{F}_q^{k\times k}, & \text{if } 0 \neq \alpha = \omega^r, \\ \mathbf{0} \in \mathbb{F}_q^{k\times k}, & \text{if } \alpha = 0. \end{cases}$$

Consider now a generator matrix $G_{\mathcal{C}} \in \mathbb{F}_{q^k}^{K\times N}$ of the outer code $\mathcal{C}$

$$G_{\mathcal{C}} = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} & \cdots & \alpha_{1,N} \\ \alpha_{2,1} & \alpha_{2,2} & \cdots & \alpha_{2,N} \\ \vdots & \vdots & & \vdots \\ \alpha_{K,1} & \alpha_{K,2} & \cdots & \alpha_{K,N} \end{pmatrix}.$$

A generator matrix of a concatenated code $\mathcal{I} \square \mathcal{C}$ can be chosen as follows

$$\begin{pmatrix} A(\alpha_{1,1})G_{\mathcal{I}} & A(\alpha_{1,2})G_{\mathcal{I}} & \cdots & A(\alpha_{1,N})G_{\mathcal{I}} \\ A(\alpha_{2,1})G_{\mathcal{I}} & A(\alpha_{2,2})G_{\mathcal{I}} & \cdots & A(\alpha_{2,N})G_{\mathcal{I}} \\ \vdots & \vdots & & \vdots \\ A(\alpha_{K,1})G_{\mathcal{I}} & A(\alpha_{K,2})G_{\mathcal{I}} & \cdots & A(\alpha_{K,N})G_{\mathcal{I}} \end{pmatrix} \in \mathbb{F}_q^{Kk\times Nn}. \tag{3}$$

Let

- $\mathcal{P} := \{P_{x+ny} \mid x \in \{1, \ldots, n\}, y \in \{0, \ldots, N-1\}\}$ be the set of points in $\mathrm{PG}(Kk-1, q)$ corresponding to the columns of (3);
- $\mathcal{Q} := \{Q_1, \ldots, Q_n\}$ be the set of points in $\mathrm{PG}(k-1, q)$ corresponding to the columns of $G_{\mathcal{I}}$;
- $\mathcal{R} := \{R_1, \ldots, R_N\}$ be the set of points in $\mathrm{PG}(K-1, q^k)$ corresponding to the columns of $G_{\mathcal{C}}$.

Let $\mathcal{H}$ and $\mathcal{H}'$ be two hyperplanes of $\mathrm{PG}(Kk-1, q)$ such that $\mathcal{P} \cap \mathcal{H} \subseteq \mathcal{P} \cap \mathcal{H}'$. We aim to prove that $\mathcal{H} = \mathcal{H}'$, which is equivalent to $\mathcal{P}$ being a strong blocking set (see for example [1, Proposition 3.3.])

Let v and v' be two vectors in $\mathbb{F}_q^{Kk}$ such that $\mathcal{H} = \langle v\rangle^\perp$ and $\mathcal{H}' = \langle v'\rangle^\perp$ and let

$$v = (v_1|\ldots|v_K), \quad v' = (v_1'|\ldots|v_K'),$$

with $v_i, v_i' \in \mathbb{F}_q^k$.

For $x \in \{1, \dots, n\}$ and $y \in \{0, \dots, N-1\}$,

$$\mathcal{H}(P_{x+ny}) = \sum_{i=1}^{K} \underbrace{v_i}_{\in \mathbb{F}_q^{1\times k}} \underbrace{A(\alpha_{i,y+1})}_{\in \mathbb{F}_q^{k\times k}} \underbrace{Q_x}_{\in \mathbb{F}_q^{k\times 1}} = \left(\sum_{i=1}^{K} v_i A(\alpha_{i,y+1}) \right) Q_x$$

and similarly

$$\mathcal{H}'(P_{x+ny}) = \sum_{i=1}^{K} \underbrace{v_i'}_{\in \mathbb{F}_q^{1\times k}} \underbrace{A(\alpha_{i,y+1})}_{\in \mathbb{F}_q^{k\times k}} \underbrace{Q_x}_{\in \mathbb{F}_q^{k\times 1}} = \left(\sum_{i=1}^{K} v_i' A(\alpha_{i,y+1}) \right) Q_x.$$

Recall that $\mathcal{Q}$ is a strong blocking set in $\mathrm{PG}(k-1, q)$. Now,

$$\left(\sum_{i=1}^{K} v_i A(\alpha_{i,y+1}) \right) \text{ and } \left(\sum_{i=1}^{K} v_i' A(\alpha_{i,y+1}) \right)$$

both correspond (if non-vanishing) to hyperplanes in $\mathrm{PG}(k-1, q)$ and therefore since $\mathcal{P} \cap \mathcal{H} \subseteq \mathcal{P} \cap \mathcal{H}'$, there exists $\lambda_i \in \mathbb{F}_q^*$ such that

$$\sum_{i=1}^{K} \eta_i \alpha_{i,y+1} = \sum_{i=1}^{K} (\lambda_i \eta_i') \alpha_{i,y+1},$$

where η_i and η_i' are the elements of $\mathbb{F}_{q^k}$ corresponding to v_i and v_i' respectively, by ϕ. Let $\overline{\mathcal{H}} = \langle \eta \rangle^\perp$ and $\overline{\mathcal{H}}' = \langle \eta' \rangle^\perp$ be the hyperplanes in $\mathrm{PG}(K-1, q^k)$ corresponding to η and η' respectively. Since $|\overline{\mathcal{H}}' \cap \mathcal{R}| \leq N - D$, λ_i is equal to some fixed $\lambda \in \mathbb{F}_q^*$ for at least $\left\lceil \frac{D}{q-1} \right\rceil$ values i. So, up to a multiplication by λ^{-1}, $\eta_i = \eta_i'$ for at least $\left\lceil \frac{D}{q-1} \right\rceil$ coordinates and the argument follows the proof of Theorem 2.2: we get that $\eta = \eta'$, so that also $\mathcal{H} = \mathcal{H}'$ and hence the set $\mathcal{P}$ is a strong blocking set.

Remark 2.5. We can reinterpret the construction in [2, Theorem 4.1.] in terms of concatenation. Actually, if ω is a primitive element of $\mathbb{F}_{q^k}$, that construction is the concatenation of a $[4, 2, 3]_{q^k}$ MDS code $\mathcal{C}$ with generator matrix

$$G_{\mathcal{C}} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & \omega^i & \omega^j & 1 \end{bmatrix},$$

where $0 < i < j < q^k$, with a simplex code $\mathcal{S}_q(k)$. Theorem 2.2 affirms that $\mathcal{S}_q(k) \square \mathcal{C}$ is minimal if $q < 4$. However, by [2, Theorem 4.1.] we have that $\mathcal{S}_q(k) \square \mathcal{C}$ is minimal whenever $i - j \not\equiv 0 \bmod \frac{q^s-1}{q-1}$ for every $s > 1$ dividing r. This provides an infinite family of minimal codes obtained with concatenation, where the outer codes do not satisfy the Outer AB condition.

2.3 Concatenation with MDS codes

In view of Theorem 2.2, it is important to have explicit constructions of codes satisfying the Outer AB condition. This is the case, for example, of some MDS codes, as the following result shows.

Corollary 2.6. Let k be an integer greater than 1. For $K \leq q^{k-1} + 1$ and $N := qK - (q-1)$, let $\mathcal{C}$ be an $[N, K, (q-1)(K-1)+1]_{q^k}$ MDS code and $\mathcal{I}$ be an $[n, k, d]_q$ minimal code. Then the concatenation $\mathcal{I} \square \mathcal{C}$ of $\mathcal{C}$ with $\mathcal{I}$ is a $[(qK - q + 1)n, Kk, \geq ((q-1)(K-1)+1)d]_q$ minimal code.

Thus, there exists a strong blocking set in $\mathrm{PG}(Kk-1, q)$ of size $nqK - qn + n$, for any $K \leq q^{k-1} + 1$.

Proof. It follows directly from Theorem 2.2, since, with the same notations as in Theorem 2.2,

$$\frac{D}{W} \geq \frac{D}{N} = \frac{(q-1)(K-1)+1}{N} > \frac{q-1}{q}.$$

□

Remark 2.7. We may concatenate MDS codes over $\mathbb{F}_{q^2}$ with simplex codes $\mathcal{S}_q(2)$, of parameters $[q+1, 2, q]_q$, which are the shortest of dimension 2. We get $[(qK-q+1)(q+1), 2K, \geq ((q-1)(K-1)+1)q]_q$ minimal codes. Those which are shorter than the upper bound of Theorem 1.6 have the following parameters: $[9,4]_2$, $[15,6]_2$, $[16,4]_3$, $[28,6]_3$, $[40,8]_3$, $[25,4]_4$, $[45,6]_4$, $[65,8]_4$, $[85,10]_4$.

Another possibility is to obtain short minimal codes by concatenating MDS codes over $\mathbb{F}_{q^3}$ with short minimal codes of dimension 3 over $\mathbb{F}_q$ (see [8] for an upper bound on their minimal lengths). We get minimal codes shorter than the upper bound of Theorem 1.6 for the following parameters: $[18,6]_2$, $[30,9]_2$, $[42,12]_2$, $[54,15]_2$, $[16,6]_3$, $[28,9]_3$.

Finally, let us remark that we use inner codes corresponding to the tetrahedron (see [1, Theorem 5.3.]) or some shorter ones constructed in [2], whose length is quadratic in the dimension. Even if we cannot get strong blocking sets smaller than those in [21], this construction has the great advantage of being explicit.

Example 2.8. We illustrate with a table some minimal codes that one can obtain by Corollary 2.6. Since we want to maximize the rate, we choose the inner code to have the shortest length. In the binary case, we know (see [1]) that the shortest minimal codes in dimensions ≤ 5 have parameters $[3,2,2]_2$, $[6,3,3]_2$, $[9,4,4]_2$, $[13,5,5]_2$. In the ternary case, the simplex $[4,2,3]_3$ code is the shortest minimal code of dimension 2 and we use a $[9,3,5]_3$ code with generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 0 & 0 & 2 & 2 \\ 0 & 1 & 0 & 0 & 0 & 1 & 2 & 1 & 2 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

which has the shortest length in dimension 3, by MAGMA exhaustive search. So we get Table 1 (in the last column we have the lower bound of Theorem 1.5 and the upper bound given by Theorem 1.6, unless otherwise specified).

Outer	Inner	Concatenated	Shortest length
$[3,2,2]_4$	$[3,2,2]_2$	$[9,4,4]_2$	Yes
$[5,3,3]_4$	$[3,2,2]_2$	$[15,6,6]_2$	Yes
$[3,2,2]_{16}$	$[9,4,4]_2$	$[27,8,8]_2$	$21 \leq n \leq 26$
$[5,3,3]_8$	$[6,3,3]_2$	$[30,9,9]_2$	$24 \leq n \leq 40$
$[3,2,2]_{32}$	$[13,5,5]_2$	$[39,10,10]_2$	$27 \leq n \leq 30$ (see [15])
$[7,4,4]_8$	$[6,3,3]_2$	$[42,12,12]_2$	$33 \leq n \leq 55$
$[9,5,5]_8$	$[6,3,3]_2$	$[54,15,15]_2$	$42 \leq n \leq 69$
$[7,4,4]_{16}$	$[9,4,4]_2$	$[63,16,16]_2$	$45 \leq n \leq 74$
$[3,2,2]_{512}$	$[30,9,9]_2$	$[90,18,18]_2$	$51 \leq n \leq 84$
$[9,5,5]_{16}$	$[9,4,4]_2$	$[81,20,20]_2$	$57 \leq n \leq 93$
$[4,2,3]_9$	$[4,2,3]_3$	$[16,4,9]_3$	$12 \leq n \leq 14$ (see [1])
$[7,3,5]_9$	$[4,2,3]_3$	$[28,6,15]_3$	$20 \leq n \leq 40$
$[10,4,7]_9$	$[4,2,3]_3$	$[40,8,21]_3$	$28 \leq n \leq 56$
$[7,3,5]_{27}$	$[9,3,5]_3$	$[63,9,26]_3$	$32 \leq n \leq 64$
$[10,4,7]_{27}$	$[9,3,5]_3$	$[90,12,35]_3$	$44 \leq n \leq 84$
$[13,5,9]_{27}$	$[9,3,5]_3$	$[117,15,45]_3$	$56 \leq n \leq 108$

Table 1: MDS concatenated with shortest minimal codes

We give here the generator matrix of the $[15, 6, 6]_2$ code obtained by the concatenation of the extended Reed-Solomon $[5, 3, 3]_4$ with the simplex $[3, 2, 2]_2$ code:

$$G := \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

The length of this code meets the bound in Theorem 1.5.

2.4 Concatenation with simplex codes

If one is interested in getting small strong blocking sets, the shorter the inner codes are, the better it is. On the other hand, concatenating with simplex codes has the great advantage that it is easy to get the weight distribution of the concatenated code. Actually, if $A_i(\mathcal{C}) = |\{c \in \mathcal{C} \mid \mathrm{wt}(c) = i\}|$, then

$$A_{q^{k-1}i}(\mathcal{S}_q(k) \,\square\, \mathcal{C}) = |\{c \in \mathcal{S}_q(k) \,\square\, \mathcal{C} \mid \mathrm{wt}(c) = q^{k-1}i\}| = A_i(\mathcal{C}),$$

and $A_j(\mathcal{S}_q(k) \,\square\, \mathcal{C}) = 0$ for all j which are not multiples of q^{k-1}.

Corollary 2.9. Let $\mathcal{C}$ be an $[N, K, D]_{q^k}$ linear code with maximum weight W. Suppose that $D/W > (q-1)/q$. Then there exists a minimal $[N(q^k-1)/(q-1), Kk, Dq^{k-1}]_q$ code $\mathcal{D}$. Equivalently, in $\mathrm{PG}(Kk-1, q)$ there exists a strong blocking set of size $N(q^k-1)/(q-1)$.

Proof. This is a straightforward consequence of Theorem 2.2, recalling that the simplex code of parameters $[(q^k-1)/(q-1), k, q^{k-1}]_q$ is in particular a minimal code. □

Example 2.10. We illustrate in Table 2.10 some minimal codes that one can obtain by Corollary 2.9. Since we want to maximize the rate, we choose the outer code to be the shortest code of a given dimension satisfying the Outer AB condition, in the library of codes with the best known minimum distance in Magma. Again, in the last column we have the lower bound of Theorem 1.5 and the upper bound given by Theorem 1.6.

Outer	Inner	Concatenated	Shortest length
$[9, 4, 5]_4$	$[3, 2, 2]_2$	$[27, 8, 10]_2$	$21 \le n \le 36$
$[11, 5, 6]_4$	$[3, 2, 2]_2$	$[33, 10, 12]_2$	$27 \le n \le 45$
$[15, 6, 8]_4$	$[3, 2, 2]_2$	$[45, 12, 16]_2$	$33 \le n \le 55$
$[21, 7, 11]_4$	$[3, 2, 2]_2$	$[63, 14, 22]_2$	$39 \le n \le 65$
$[23, 8, 12]_4$	$[3, 2, 2]_2$	$[69, 16, 24]_2$	$45 \le n \le 74$
$[16, 5, 11]_9$	$[4, 2, 3]_3$	$[64, 10, 33]_3$	$36 \le n \le 72$

Table 2: Best known linear codes satisfying Outer AB condition concatenated with simplex codes

Remark 2.11. When concatenating with a simplex code of dimension k, it is worth noting that the outer code in our construction is required have relative distance larger than $1 - 1/q$. Therefore its rate is smaller than $1/q + 1/n$ and thus the rate of the concatenated code is smaller than

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

The size of the corresponding strong blocking set is lower bounded by

$$\frac{q(q+1)}{2} \cdot k - q.$$

One can, in principle, search for outer codes having a slightly larger relative minimum weight, say $(1-1/q)^{1+\epsilon}$, and concatenate with an inner code with relative distance (or ratio between minimum and maximum weight) at least $(1-1/q)^{-\epsilon}$ and rate larger than $\frac{k(q-1)}{q^k-1}$. In this way one obtains constructions of shorter minimal codes and so of smaller strong blocking sets.

3 Asymptotic results

3.1 Non-constructive

By the Gilbert-Varshamov Bound (see [32, §1.3.2]), for any $0 \leq \delta \leq 1-1/q$ there exists a q-ary linear code of relative minimum weight δ and rate at least $1 - H_q(\delta)$, where

$$H_q(x) := x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x).$$

The following theorem shows that it is possible to construct for any q an infinite family of strong blocking sets of size linear in the dimension k and quadratic in q.

Theorem 3.1. For any $\epsilon \in (0,1]$ and any prime power q there exists an integer $k_{q,\epsilon}$ such that $\mathrm{PG}(k_{q,\epsilon}-1, q)$ possesses a strong blocking set of size

$$k_{q,\epsilon} \cdot \frac{q^{1+2\epsilon}(q+1)}{1-\epsilon}.$$

Proof. Fix $\delta = 1 - 1/q^{1+\epsilon} \leq 1 - 1/q^2$, for $\epsilon \in (0,1]$. By the Gilbert-Varshamov Bound there exists a q^2-ary linear code $\mathcal{C}$ of dimension $k_{q,\epsilon}$ with relative minimum weight δ and rate at least

$$\begin{aligned}
1 - H_{q^2}(\delta) &= 1 - \left(1 - \frac{1}{q^{1+\epsilon}}\right)\log_{q^2}\frac{q^2-1}{\left(1-\frac{1}{q^{1+\epsilon}}\right)} + \frac{1}{q^{1+\epsilon}}\log_{q^2}\left(\frac{1}{q^{1+\epsilon}}\right) \\
&= 1 - \left(1 - \frac{1}{q^{1+\epsilon}}\right)\left(1 + \frac{1}{2\ln q}\left(\frac{1}{q^{1+\epsilon}} - \frac{1}{q^2} + \frac{1}{2q^{2(1+\epsilon)}} - \frac{1}{2q^4}\cdots\right)\right) - \frac{1+\epsilon}{2q^{1+\epsilon}} \\
&\geq \frac{1-\epsilon}{2q^{1+\epsilon}} - \frac{1}{2\ln q}\left(\frac{1}{q^{1+\epsilon}} + \frac{1}{2q^{2(1+\epsilon)}} + \cdots\right) \geq \frac{1-\epsilon}{2q^{1+2\epsilon}}.
\end{aligned}$$

By Corollary 2.9, there exists a minimal q-ary code of rate at least

$$2 \cdot \frac{1-\epsilon}{2q^{1+2\epsilon}(q+1)} = \frac{1-\epsilon}{q^{1+2\epsilon}(q+1)}$$

and therefore a strong blocking set in $\mathrm{PG}(k_{q,\epsilon}-1, q)$ of size $k_{q,\epsilon} \cdot \frac{q^{1+2\epsilon}(q+1)}{1-\epsilon}$. □

3.2 Explicit constructions

As we have just seen, Corollary 2.9 and the Gilbert-Varshamov bound imply the existence of strong blocking set of size linear in the dimension and quadratic in size of the field. In this subsection, exploiting explicit constructions of asymptotically good AG codes, we provide constructions of families of asymptotically good minimal codes and therefore infinite families of small strong blocking sets.

Let $N_q(\mathcal{X})$ denote the number of degree 1 places of an $\mathbb{F}_q$-rational curve $\mathcal{X}$ and consider the Ihara's constant

$$A(q) = \limsup_{g\to\infty} \frac{\max\{\#N_q(\mathcal{X}) \mid \mathcal{X} \text{ has genus } g\}}{g}.$$

By the Drinfeld-Vladut Bound (see [32, Theorem 2.3.22]) we know that

$$A(q) \leq \sqrt{q} - 1.$$

If q is a square then the Drinfeld-Vladut Bound is actually attained, as shown by Ihara [23] and Tsfasman, Vladut and Zink [33], using the theory of modular curves.

We apply now Corollary 2.9 to the family of AG codes obtained by the curves considered in [20].

Theorem 3.2. Let q_0 be a prime power. Consider $h \geq 2$. Denote by

$$\begin{aligned} N_{h,n} &:= (q_0^{h(n+1)} - q_0^{hn} - 1); \\ \lambda_{h,n} &:= \begin{cases} (q_0^{nh/2} - 1)^2, & \text{if } 2 \mid n; \\ (q_0^{(n+1)h/2} - 1)(q_0^{(n-1)h/2} - 1), & \text{if } 2 \nmid n. \end{cases} \end{aligned}$$

There exists a family of good minimal codes $\mathcal{C}_{h,n}$ with parameters

$$\left[N_{h,n}\frac{q_0^{2h}-1}{q_0-1}, 2h\left(\left\lfloor \frac{N_{h,n}-1}{q_0} \right\rfloor - \lambda_{h,n} + 1\right), \geq q_0^{2h-1}N_{h,n}\left(1-\frac{1}{q_0}\right)\right]_{q_0}.$$

Proof. Denote $q = q_0^h > 2$. Consider the tower $\mathcal{T} = (T_1, T_2, T_3, \ldots)$ of function fields over $\mathbb{F}_{q^2}$ given by $T_n := \mathbb{F}_{q^2}(x_1, \ldots, x_n)$, with

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1}+1}, \text{ for } i \in \{1, \ldots, n-1\}.$$

By [20, Remark 3.8.], the genus of T_n is

$$g_n := g(T_n) = \begin{cases} (q^{n/2}-1)^2, & \text{if } n \equiv 0 \bmod 2; \\ (q^{(n+1)/2}-1)(q^{(n-1)/2}-1), & \text{if } n \equiv 1 \bmod 2. \end{cases}$$

Consider

$$\begin{aligned} \Omega &:= \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = 0\}; \\ S &:= \{R_\alpha \in \mathbb{P}(T_1) \mid \alpha \notin \Omega\}. \end{aligned}$$

By [20, Lemma 3.9], any $R \in S$ splits completely in all the extensions T_n/T_1. Let S_n be the places in T_n lying over the places in S. Since $[T_n : T_1] = q^{n-1}$, $\#S_n = \#S \cdot [T_n : T_1] = q^{n-1}(q^2-q)$. Let $n_n := \#S_n - 1 = q^{n-1}(q^2-q) - 1$.

Take a place $P_n \in S_n$ and the divisor $G_n := m_n P_n$ with $2g_n - 2 < m_n < n_n$. Since $q > 2$, such a value m_n exists. Then

$$k_n := \dim \mathcal{C}_n = \ell(G_n) = m_n - g_n + 1,$$

where the last equality is the celebrated Riemann-Roch Theorem (see [32, Chapter 2]).

In what follows we consider the AG code $\mathcal{C}_n := C\left(G_n, \sum_{P\in S_n\setminus\{P_n\}} P\right)$, which is an $[n_n, m_n - g_n + 1, d_n \geq n_n - m_n]_{q^2}$-code.

Note that

$$\frac{d_n}{w_n} \geq \frac{d_n}{n_n} \geq \frac{n_n - m_n}{n_m} = 1 - \frac{m_n}{n_n}.$$

Consider $m_n = \left\lfloor \frac{n_n - 1}{q_0} \right\rfloor$, so that $\frac{d_n}{w_n} \geq 1 - \frac{m_n}{n_n} > 1 - \frac{1}{q_0}$.

By Corollary 2.9 there exists a minimal $[n_n(q_0^{2h}-1)/(q_0-1), 2k_n h, \geq q_0^{2h-1} n_n (1-1/q_0)]_{q_0}$-code $\mathcal{D}_n$.

The family $\mathcal{D}_n$ is asymptotically good since the relative minimum weight and the rate are larger than

$$\frac{q_0^{2h-2}(q_0-1)^2 \cdot}{q_0^{2h}-1}$$

and

$$\begin{aligned} \frac{2h(q_0-1)\cdot(m_n - g_n + 1)}{(q_0^{2h}-1)\cdot n_n} &> \frac{2h(q_0-1)}{q_0^{2h}-1} \cdot \left(\frac{1}{q_0} - \frac{g_n}{n_n}\right) \\ &\geq \frac{2h(q_0-1)}{q_0^{2h}-1} \cdot \left(\frac{1}{q_0} - \frac{1}{q_0^h - 1}\right), \end{aligned}$$

whenever $n \geq 3$. Note that, the assumption $h \geq 2$ is necessary to have $\frac{1}{q_0} - \frac{1}{q_0^h - 1} > 0$. □

Corollary 3.3. Let $K_n := 4\left\lfloor \frac{N_{h,n}-1}{q_0} \right\rfloor - 4\lambda_{h,n} + 4$. In $\mathrm{PG}(K_n - 1, q_0)$ there exists a strong blocking sets of size at most

$$\left(\frac{q_0(q_0^4-1)(q_0+1)}{4(q_0^2-q_0+1)}\right) \cdot K_n \leq q_0 \cdot \frac{q_0^3 + 2q_0^2 + q_0 - 1}{4} \cdot K_n.$$

Proof. The claim follows considering $h = 2$ in Theorem 3.2.

□

Example 3.4. Let $q_0 = 2$ and $h = 3$, so that $q = 8$. We consider the function field $T = \mathbb{F}_{64}(x, y)$ with $y^2 + y = \frac{x^2}{x+1}$. The genus of T is 49. In this case the set S of points in T lying over the places that split completely in $T/\mathbb{F}_{64}(x)$ has cardinality 448. Take any $P \in S$. Consider $m = 223$, so that the divisor $G = 223P$ and $k = 223 - 49 + 1 = 175$ (but any k between 49 and 175 may also be chosen). The AG code $\mathcal{C} = C(G, \sum_{Q \in S \setminus \{P\}} Q)$ is a $[447, 175, \geq 224]_{64}$. Next, we concatenate with the $[7, 3, 4]_2$ simplex code, so that we obtain a minimal $[3129, 525, \geq 896]_2$ code.

Note that, following the proof of Theorem 3.2, it is readily seen that the sum of the rate and the relative distance of the concatenation of $\mathcal{C}_n$ with the simplex code is lower bounded by

$$1 - \frac{2}{q_0} + O\left(\frac{1}{q_0^2}\right), \tag{4}$$

In order to maximize it one can choose inner codes different from the simplex one, as shown in the next example.

Example 3.5. The RT4 in [11, Figure 1b] is a two weight code over $\mathbb{F}_{q_0}$ with parameters $\widetilde{n} = (q_0^5 - 1)(q_0^2 + 1)/(q_0 - 1)$, $h = 10$, $\widetilde{d} = q_0^6$, $\widetilde{w} = q_0^6 + q_0^4$. Also, $\frac{\widetilde{d}}{\widetilde{w}} = \frac{q_0^2}{q_0^2+1} = 1 - \frac{1}{q_0^2+1} > 1 - \frac{1}{q_0}$.

Now, choosing $m_n = \left\lfloor \frac{n_n(q_0^2 - q_0 + 1) - 1}{q_0^3} \right\rfloor$, one gets that the concatenation of $\mathcal{C}_n$ (as in Theorem 3.2) with the code RT4 is still minimal over q_0. Also, the rate of $\mathcal{D}_n$ is lower bounded by

$$\frac{h}{\widetilde{n}q} \cdot \left(\left(1 - \frac{\widetilde{w}}{\widetilde{d}} \frac{q_0 - 1}{q_0}\right)(q-1) - 1\right) = \frac{10(q_0-1)}{q_0^{10}(q_0^5-1)(q_0^2+1)}(q_0^7(q_0^2 - q_0 + 1) - 2) \simeq \frac{10}{q_0^7},$$

which is less than the corresponding value for the simplex code in dimension 10. Note that the relative minimum weight is larger than $\frac{q_0^3-q_0^2+q_0-1}{q_0^3}$, and

$$\frac{q_0^3-q_0^2+q_0-1}{q_0^3}+\frac{10}{q_0^7}=1-\frac{1}{q_0}+\frac{1}{q_0^2}+o(q_0^{-2})$$

which is larger than (4).

Remark 3.6. Example 3.5 shows that if one is interested in minimal codes maximizing the sum of the rate and the relative minimum weight the choice of the simplex code as inner code is not always the best.

Theorem 3.7. Suppose that there exists an $[\widetilde{n},2h,d]_{q_0}$ code $\mathcal{I}$, and denote by $\widetilde{D}:=\frac{d}{w}$. Let

$$0<\epsilon<1-\frac{1}{q_0^h-1}-\frac{1}{\widetilde{D}}\left(1-\frac{1}{q_0}\right).$$

Then there exists a family of minimal codes with rate at least $\frac{2h\epsilon}{\widetilde{n}}$.

Proof. Consider the code $\mathcal{C}_n$ as in Theorem 3.2. Choose n and m_n such that

$$\epsilon+\frac{1}{q_0^h-1}-\frac{1}{n_n}\leq\frac{m_n}{n_n}<1-\frac{1}{\widetilde{D}}\left(1-\frac{1}{q_0}\right).$$

By our assumption on $\widetilde{D}$, such a value m_n exists. Since

$$\left(1-\frac{m_n}{n_n}\right)\widetilde{D}>1-\frac{1}{q_0},$$

$\mathcal{I}\,\square\,\mathcal{C}_n$ is a minimal q_0-ary code by the AB condition.

Therefore,

$$\mathcal{R}(\mathcal{I}\,\square\,\mathcal{C}_n)\geq\frac{2h}{\widetilde{n}}\left(\frac{1}{n_n}+\frac{m_n}{n_n}-\frac{g_n}{n_n}\right)\geq\frac{2h\epsilon}{\widetilde{n}}.$$

□

Corollary 3.8. Suppose that there exists an $[\widetilde{n},2h,d]_{q_0}$ code $\mathcal{I}$, and denote by $\widetilde{D}:=\frac{d}{w}$. Let

$$0<\epsilon<1-\frac{1}{q_0^h-1}-\frac{1}{\widetilde{D}}\left(1-\frac{1}{q_0}\right).$$

Let

$$K_{h,n}:=\left\lfloor N_{h,n}\left(1-\frac{1}{\widetilde{D}}\left(1-\frac{1}{q_0}\right)\right)-1\right\rfloor.$$

In $\mathrm{PG}(K_{h,n}-1,q)$ there exists a strong blocking set of size at most $\frac{\widetilde{n}}{2h\epsilon}K_{h,n}$.

Remark 3.9. Corollary 3.8 provides an upper bound on the minimum size of strong blocking sets. Note that since $\widetilde{D}\geq 1$, $\epsilon<\frac{1}{q_0}-\frac{1}{q_0^h-1}$.

On the other hand, by [2, Corollary 3.7], since $\mathcal{I}$ is not a constant weight code,

$$\widetilde{n}\left(\frac{q_0^{2h-1}-1}{q_0^{2h}-1}\right)>2h-1\iff\frac{2h}{\widetilde{n}}<\frac{q_0^{2h-1}-1}{q_0^{2h}-1}+\frac{1}{\widetilde{n}}\iff\frac{\widetilde{n}}{2h}>\frac{\widetilde{n}(q_0^{2h}-1)}{\widetilde{n}(q_0^{2h-1}-1)+q_0^{2h}-1}.$$

The minimum for the upper bounds on minimal strong blocking set (considering also $\epsilon\simeq\frac{1}{2q_0}$) is roughly

$$\frac{\widetilde{n}(q_0^{2h}-1)q_0}{\widetilde{n}(q_0^{2h-1}-1)+q_0^{2h}-1}K_{h,n}\simeq q_0^2K_{h,n},$$

whenever $\widetilde{n}>>q_0$. This shows that in principle there is room for improvement in the bound provided by Corollary 3.3 if a suitable code $\mathcal{I}$ exists.

Remark 3.10. It would be interesting to search for $[n, 2h, d]_{q_0}$ codes $\mathcal{I}$ maximizing the quantity

$$\frac{2h}{n}\left(1-\frac{1}{q_0^h-1}-\frac{w}{d}\left(1-\frac{1}{q_0}\right)\right).$$

4 Application to ρ-saturating sets

As a byproduct of our constructions of short minimal codes, we present results on ρ-saturating sets of small size, which have deep connections with strong blocking sets [16].

Definition 4.1. A set $\mathcal{S} \subseteq \mathrm{PG}(k-1,q)$ is called *ρ-saturating* if for any point $Q \in \mathrm{PG}(k-1,q)\backslash\mathcal{S}$ there exist $\rho+1$ points $P_1,\dots,P_{\rho+1} \in \mathcal{S}$ such that $Q \in \langle P_1,\dots,P_{\rho+1}\rangle$ and ρ is the smallest value with this property. Let $s_q(k-1,\rho)$ denote the smallest size of a ρ-saturating set in $\mathrm{PG}(k-1,q)$.

Recall that the covering radius of an $[n, n-k]_q$ code is the least integer R such that the space $\mathbb{F}_q^n$ is covered by spheres of radius R centered on codewords. It is easy to prove (see [16]) that a linear $[n, n-k]_q$ code has covering radius R if every element of $\mathbb{F}_q^k$ is a linear combination of R columns of a generator matrix of the dual code (that is the orthogonal space with respect to the Euclidean inner product), and R is the smallest value with such a property. Thus the correspondence presented in Section 1.2 specializes to a correspondence between $(R-1)$-saturating sets of size n in $\mathrm{PG}(k-1,q)$ and the dual of $[n, n-k]_q$ codes of covering radius R.

A connection between strong blocking sets and ρ-saturating sets is the following.

Theorem 4.2 ([16])**.** Any strong blocking set in a subgeometry $\mathrm{PG}(k-1,q)$ of $\mathrm{PG}(k-1,q^{k-1})$ is a $(k-2)$-saturating set in $\mathrm{PG}(k-1,q^{k-1})$.

Recently, improvements on the upper bound on the minimum size of a ρ-saturating set have been obtained in [17, 18].

Theorem 4.3 ([18])**.** The following bound on the minimum size of a ρ-saturating in $\mathrm{PG}(k-1,q^{\rho+1})$ holds

$$\frac{\rho+1}{e}q^{k-1-\rho} \le s_{q^{\rho+1}}(k-1,\rho) \le \rho(\rho+1)\left(\frac{q^{k-1-\rho}}{2}+\frac{q^{k-1-\rho}-1}{q-1}\right).$$

In particular, for $\rho = k-2$,

$$s_{q^{k-1}}(k-1,k-2) \le q\binom{k-1}{2}+(k-1)(k-2). \tag{5}$$

The approach described in Section 3.2 yields an explicit construction of small saturating sets. We use the same notation:

- q_0 be a prime power and $h \ge 2$ an integer;
- $N_{h,n} := (q_0^{h(n+1)} - q_0^{hn} - 1)$;
- $\lambda_{h,n} := \begin{cases} (q_0^{nh/2}-1)^2, & \text{if } 2 \mid n; \\ (q_0^{(n+1)h/2}-1)(q_0^{(n-1)h/2}-1), & \text{if } 2 \nmid n; \end{cases}$
- $K_n := 4\left\lfloor \frac{N_{h,n}-1}{q_0} \right\rfloor - 4\lambda_{h,n} + 4$.

Theorem 4.4. In $\mathrm{PG}(K_n-1, q^{K_n-1})$ there exists an explicit construction of (K_n-2)-saturating set of size at most

$$\left(\frac{q_0(q_0^4-1)(q_0+1)}{4(q_0^2-q_0+1)}\right)\cdot K_n \le q_0 \cdot \frac{q_0^3+2q_0^2+q_0-1}{4}\cdot K_n \simeq \frac{q_0^4}{4}K_n. \tag{6}$$

Note that although Bound (6) is worse than the estimate in [21, Corollary 6.4], it provides the best explicit construction of small saturating sets for specific dimensions and it improves (5).

Acknowledgments

This work was started during the first author's stay at the LAGA at University Paris 8 as a Visiting Professor in 2021. The research of D. Bartoli was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

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] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Three combinatorial perspectives on minimal codes. *arXiv preprint arXiv:2010.16339*, 2020.

[3] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Linear cutting blocking sets and minimal codes in the rank metric. *arXiv preprint arXiv:2106.12465*, 2021.

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

[5] D. Bartoli, A. Cossidente, G. Marino, and F. Pavese. On cutting blocking sets and their codes. *arXiv preprint arXiv:2011.11101*, 11 2020.

[6] D. Bartoli, G. Kiss, S. Marcugini, and F. Pambianco. Resolving sets for higher dimensional projective spaces. *Finite Fields Appl.*, 67:101723, 14, 2020.

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

[8] A. Bishnoi, S. Mattheus, and J. Schillewaert. Minimal multiple blocking sets. *Electron. J. Combin.*, 25(4):Paper No. 4.66, 14, 2018.

[9] A. Blokhuis, P. Sziklai, and T. Szőnyi. Blocking sets in projective spaces. In *Current Research Topics in Galois Geometry* (De Beule, J. and Storme, L., eds), *Nova Academic*, pages 61–84, 2011.

[10] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *J. Algebraic Combin.*, 53(2):327–341, 2021.

[11] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, 18(2):97–122, 1986.

[12] H. Chabanne, G. Cohen, and A. Patey. Towards secure two-party computation from the wire-tap channel. In *Information Security and Cryptology – ICISC 2013*, pages 34–46. Springer International Publishing, 2014.

[13] G. Cohen and S. Mesnager. Variations on minimal linear codes. In *Coding theory and applications*, volume 3 of *CIM Ser. Math. Sci.*, pages 125–131. Springer, Cham, 2015.

[14] G. D. Cohen, S. Mesnager, and A. Patey. On minimal and quasi-minimal linear codes. In *Cryptography and Coding*, pages 85–98. Springer Berlin Heidelberg, 2013.

[15] G. D. Cohen and G. Zémor. Intersecting codes and independent families. *IEEE Transactions on Information Theory*, 40(6):1872–1881, 1994.

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

[17] A. A. Davydov, S. Marcugini, and F. Pambianco. New covering codes of radius R, codimension tR and $tR + \frac{R}{2}$, and saturating sets in projective spaces. *Des. Codes Cryptogr.*, 87(12):2771–2792, 2019.

[18] L. Denaux. Constructing saturating sets in projective spaces using subgeometries. *arXiv preprint arXiv:2008.13459*, 2020.

[19] S. L. Fancsali and P. Sziklai. Lines in higgledy-piggledy arrangement. *Electron. J. Comb.*, 21(2):research paper p2.56, 15, 2014.

[20] A. Garcia and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, 61(2):248–273, 1996.

[21] T. Héger and Z. L. Nagy. Short minimal codes and covering codes via strong blocking sets in projective spaces. *arXiv preprint arXiv:2103.07393*, 03 2021.

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

[23] Y. Ihara. Some remarks on the number of rational points of algebraic curves over finite fields. *J. Fac. Sci., Univ. Tokyo, Sect. I A*, 28:721–724, 1981.

[24] R. Lidl and H. Niederreiter. *Introduction to Finite Fields and their Applications*. Cambridge University Press, 2 edition, 1994.

[25] W. Lu, X. Wu, and X. Cao. The parameters of minimal linear codes. *Finite Fields Appl.*, 71:101799, 11, 2021.

[26] J. L. Massey. Minimal codewords and secret sharing. In *Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory*, pages 276–279, 1993.

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

[28] S. Mesnager and A. Sınak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Transactions on Information Theory*, 66(4):2296–2310, 2020.

[29] M. Shi and X. Li. Two classes of optimal p-ary few-weight codes from down-sets. *Discrete Appl. Math.*, 290:60–67, 2021.

[30] Z. Shi and F.-W. Fu. Several families of q-ary minimal linear codes with $w_{min}/w_{max} \leq (q-1)/q$. *Discrete Mathematics*, 343(6):111840, 2020.

[31] C. Tang, Y. Qiu, Q. Liao, and Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. *IEEE Trans. Inform. Theory*, 67(6):3690–3700, 2021.

[32] 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.

[33] M. A. Tsfasman, S. G. Vlădut, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.