A Collection of ELKH–ELTE GAC manuscripts

Tamás Héger, Zoltán Lóránt Nagy

Short minimal codes and covering codes via strong blocking sets in projective spaces

2021

ELKH–ELTE Geometric and Algebraic Combinatorics Research Group

successor of the MTA-ELTE GAC Research group of the Hungarian Academy of Sciences and the Eötvös University, Budapest

MANUSCRIPTS

Short minimal codes and covering codes via strong blocking sets in projective spaces

Tamás Héger[*], **Zoltán Lóránt Nagy**[†]

Abstract

Minimal linear codes are in one-to-one correspondence with special types of blocking sets of projective spaces over a finite field, which are called strong or cutting blocking sets. In this paper we prove an upper bound on the minimal length of minimal codes of dimension k over the q-element Galois field which is linear in both q and k, hence improve the previous superlinear bounds. This result determines the minimal length up to a small constant factor. We also improve the lower and upper bounds on the size of so called higgledy-piggledy line sets in projective spaces and apply these results to present improved bounds on the size of covering codes and saturating sets in projective spaces as well. The contributions rely on geometric and probabilistic arguments.

Keywords: minimal code, covering code, saturating set, strong blocking set, cutting blocking set, higgledy-piggledy line set, random construction, projective space

1 Introduction

Throughout this paper, q denotes a prime power and $\mathbb{F}_q$ denotes the Galois field with q elements, while p stands for the characteristics of $\mathbb{F}_q$. Let $\mathbb{F}_q^n$ be the n -dimensional vector space over $\mathbb{F}_q$. Denote by $[n, r]_q$ a q-ary linear code of length n and dimension r, which is the set of codewords (code vectors) of a subspace of $\mathbb{F}_q^n$ of dimension r. For a general introduction on codes we refer to [28].

Definition 1.1. *In a linear code, a codeword is* minimal *if its support does not contain the support of any codeword other than its scalar multiples. A code is* minimal *if its codewords are all minimal.*

Minimal codewords in linear codes were originally studied in connection with decoding algorithms [29] and have been used by Massey [34] to determine the access structure in his code-based secret sharing scheme. For a general overview on recent results in connection with minimal codes we refer to [1, 33]. The general problem is to determine the minimal length of a $[n, k]_q$ minimal code can have, provided that k and q are fixed.

[*]ELKH–ELTE Geometric and Algebraic Combinatorics Research Group, Eötvös Loránd University, Budapest, Hungary. The author is supported by the Hungarian Research Grant (NKFI) No. 124950. E-mail: heger.tamas@ttk.elte.hu

[†]ELKH–ELTE Geometric and Algebraic Combinatorics Research Group, Eötvös Loránd University, Budapest, Hungary. The author is supported by the Hungarian Research Grant (NKFI) No. K 120154, 124950, 134953. E-mail: nagyzoli@caesar.elte.hu

Definition 1.2 (Minimal length of a minimal code)**.** *Denote by $m(k,q)$ the minimal length of a $[n,k]_q$ minimal code with parameters k and q.*

The following bounds are due to Alfarano, Borello, Neri and Ravagnani [1]. We do not state the quadratic upper bound precisely, as it depends on some properties of q and k.

Theorem 1.3 ([1])**.** *Let $\mathcal{C}$ be an $[n,k]_q$ minimal code. We have*

$$(k-1)(q+1) \leq m(k,q) \leq ck^2q, \tag{1.1}$$

for some $c \geq 2/9$.

In [15] it has been shown by Chabanne, Cohen and Patey that the upper bound on $m(k,q)$ can be refined as follows.

Theorem 1.4 ([15])**.**

$$m(k,q) \leq \frac{2k}{\log_q\left(\frac{q^2}{q^2-q+1}\right)}. \tag{1.2}$$

Note that this bound is a non-constructive one and that $\lim_{q\to\infty} q\ln q \cdot \log_q\left(\frac{q^2}{q^2-q+1}\right) = 1$, hence for large q, it roughly says $m(k,q) \lesssim 2kq\ln(q)$. For $q=2$ it yields $m(k,2) \leq 2k/(\log_2(4/3))$.

Our contribution is a linear upper bound in both k and q. The two cases follow from Theorems 4.1 and 5.1.

Theorem 1.5. *If $q>2$, then*

$$m(k,q) \leq \left\lceil \frac{2}{1+\frac{1}{(q+1)^2\ln q}}(k-1)\right\rceil (q+1). \tag{1.3}$$

If $q=2$, then

$$m(k,2) \leq \frac{2k-1}{\log_2(\frac{4}{3})}. \tag{1.4}$$

The case $q>2$ will follow immediately from Theorem 4.1, which is based on a random construction of taking the point set of the union of less than $2k$ lines in a suitable projective space. From the proof it follows easily that with a positive probability (calculated therein), this provides a desired minimal code.

Note that to apply probabilistic arguments for problems in finite geometry is not at all new. Here we only mention the paper of Gács and Szőnyi [23] on various applications, the celebrated paper on complete arcs of Kim and Vu [31] which applies Rödl's nibble, and the paper of second author [35] on the topic of saturating sets of projective planes which we revisit later on.

As it was noticed recently by Alfarano, Borello and Neri [2] and independently by Tang, Qiu, Liao, and Zhou [37], minimal codes are in one-to-one correspondence with special types of blocking sets of projective spaces, which they called *cutting blocking sets* after the earlier paper of Bonini and Borello [12]. In fact, this concept has been investigated in connection with saturating sets and covering codes a decade earlier by Davydov, Giulietti, Marcugini and Pambianco [17] under the name *strong blocking sets* and in the paper of Fancsali and Sziklai [21] in connection with so-called higgledy-piggledy line arrangements under the name *generator set*.

Blocking sets and their generalisations are well-known concepts in finite geometry. For an introduction to finite geometries, blocking sets and various related topics we refer to [27, 32]. Let us give the corresponding definitions. We denote the finite projective geometry of dimension N and order q by $\mathrm{PG}(N,q)$.

Definition 1.6 (Blocking sets)**.** *Let t, r, N be positive integers with $r < N$. A t-fold r-blocking set in $\mathrm{PG}(N,q)$ is a set $\mathcal{B} \subseteq \mathrm{PG}(N,q)$ such that for every $(N-r)$-dimensional subspace Λ of $\mathrm{PG}(N,q)$ we have $|\Lambda \cap \mathcal{B}| \geq t$. When $r = 1$, we will refer to $\mathcal{B}$ as a t-*fold blocking set. When $t = 1$, we will refer to it as an *r-blocking set. When $r = t = 1$, $\mathcal{B}$ is simply a* blocking set.

Definition 1.7 (Strong blocking sets)**.** *A $(\varrho+1)$-fold strong blocking set of $\mathrm{PG}(N,q)$ is a point set that meets any ϱ-dimensional subspace Λ in a set of points spanning the whole subspace Λ. By a strong blocking set of $\mathrm{PG}(N,q)$ we always mean an N-fold strong blocking set of $\mathrm{PG}(N,q)$.*

An N-fold strong blocking set of $\mathrm{PG}(N,q)$ of size n corresponds to a minimal $[n, N+1]_q$ code (see [2, 37], and also Section 3). Thus, as short minimal codes are of interest, constructing small N-fold strong blocking sets of $\mathrm{PG}(N,q)$ is highly relevant.

N-fold strong blocking sets were also investigated by Héger, Patkós and Takáts [26] under the name hyperplane generating set. There it was proposed to construct such a set as the union of lines, and appropriate sets of lines were called line sets in *higgledy-piggledy arrangement.*

Definition 1.8. *A set of lines of $\mathrm{PG}(N,q)$ is in* higgledy-piggledy arrangement*, if the union of their point sets is a strong blocking set of $\mathrm{PG}(N,q)$. We may also refer to such line sets as higgledy-piggledy line sets for short.*

Such line sets of not necessarily finite projective spaces were studied in detail in [21] (see also [22] for a generalisation to higgledy-piggledy subspaces). Let us recall the three main results of Fancsali and Sziklai [21].

Theorem 1.9 (Fancsali, Sziklai, [21], Theorems 14, 24 and 26)**.** *Let $\mathbb{F}$ be an arbitrary field.*

i) If $|\mathbb{F}| \geq N + \lfloor N/2 \rfloor$, then every line set of $\mathrm{PG}(N,\mathbb{F})$ in higgledy-piggledy arrangement contains at least $N + \lfloor N/2 \rfloor$ lines.

ii) If $|\mathbb{F}| \geq 2N-1$, then there exist a line set of $\mathrm{PG}(N,\mathbb{F})$ in higgledy-piggledy arrangement containing $2N-1$ lines.

iii) If $\mathbb{F}$ is algebraically closed, then every line set of $\mathrm{PG}(N,\mathbb{F})$ in higgledy-piggledy arrangement contains at least $2N-1$ lines.

Note that for $2 \leq N \leq 5$, there are line sets in higgledy-piggledy arrangement in $\mathrm{PG}(N,q)$ of size $N + \lfloor N/2 \rfloor$, provided that q is large enough (see [21] and [17] for $2 \leq N \leq 3$, [9] for $N = 4$, and [6] for $N = 5$). The weakness of Theorem 1.9 is that it requires q to be large (both for the construction and for the lower bound), whereas the typical approach in coding theory is to fix q and let the length of the code vary. The only known construction of line sets in higgledy-piggledy arrangement that works for general N and q is the so-called tetrahedron: take $N+1$ points of $\mathrm{PG}(N,q)$ in general position, and then the $\binom{N+1}{2}$ lines joining these points are easily seen to be in higgledy-piggledy arrangement (see [2, 12, 17]). However, this construction is much larger than the expected minimum. Also, [17] gives a slightly smaller strong blocking set for general N and q.

Thus it is of interest to construct line sets in higgledy-piggledy arrangement in $\mathrm{PG}(N, q)$ of small size from two points of view. First, they give rise to short minimal codes. Second, to determine whether the lower bound remains valid for small q (and possibly large dimension) as well. The proof of our main result Theorem 1.5 relies on a probabilistic construction of higgledy-piggledy line arrangements in $\mathrm{PG}(N, q)$ containing less than $2N - 1$ lines (see Theorem 4.1), hence it improves Theorem 1.9 *ii)*. Furthermore, following this idea, a simple randomised computer search (see Section 5) provides examples of higgledy-piggledy line sets in $\mathrm{PG}(N, 2)$ of size less than $N + \lfloor N/2 \rfloor$ for particular small values of N, hence we obtain that the lower bound $N + \lfloor N/2 \rfloor$ (Theorem 1.9 *i)*) is not universally valid. On the other hand we show in Theorem 3.12 and Remark 3.13 that the assumption in Theorem 1.9 *i)* may be relaxed a bit. Let us also remark that the construction behind Theorem 1.9 and the ones mentioned after it are all based on careful selection of lines, and have an algebraic fashion. In contrast, in the proof of Theorem 4.1 we select lines of $\mathrm{PG}(N, q)$ randomly and prove that this results in a higgledy-piggledy line set of size smaller than $2N - 1$ with positive probability.

Let us mention that in $\mathrm{PG}(2, q)$, that is, projective planes, strong blocking sets coincide with *double blocking sets*. For lower bounds on the size of a double blocking set and constructions of the currently known smallest examples, we refer to [4, 11, 14, 19].

Finding short minimal codes, that is, small strong blocking sets, has relevance in another code theoretic aspect as well, since strong blocking sets are linked to *covering codes*. From a geometric perspective, these objects correspond to *saturating sets* in projective spaces. A point set $S \subset \mathrm{PG}(N, q)$ is ρ-saturating if for any point Q of $\mathrm{PG}(N, q) \setminus S$ there exist $\rho + 1$ points in S generating a subspace of $\mathrm{PG}(N, q)$ which contains Q, and ρ is the smallest value with this property. Equivalently, the subspaces of dimension ρ which are generated by the ρ-tuples of S must cover every point of the space. $s_q(N, \rho)$ denotes the smallest size of a ρ-saturating set in $\mathrm{PG}(N, q)$.

Definition 1.10 (Covering radius, covering code)**.** *The* covering radius *of an $[n, r]_q$ code is the least integer R such that the space $\mathbb{F}_q^n$ is covered by spheres of radius R centered on codewords. If a code $[n, r]_q$ has covering radius R then it is denoted as a $[n, r]_q R$ covering code.*

Note that we can apply the following equivalent description. A linear code of co-dimension r has *covering radius R* if every (column) vector of $\mathbb{F}_q^r$ is equal to a linear combination of R columns of a parity check matrix of the code, and R is the smallest value with this property.

The covering problem for codes is that of finding codes with small covering radius with respect to their lengths and dimensions. *Covering codes* are those codes which are investigated from the point of view of the above covering problem. Usually the parameters for the covering radius and the co-dimension are fixed and one seeks a good upper bound for the length of the corresponding covering codes. The length function $l_q(r, R)$ is the smallest length of a q-ary linear code of co-dimension r and covering radius R. There is a one-to-one correspondence between $[n, n - r]_q R$ codes and $(R - 1)$-saturating sets of size n in $\mathrm{PG}(r - 1, q)$. This implies $l_q(r, R) = s_q(r - 1, R - 1)$ [17, 18]. Applying a random construction based on point sets of subspaces in the spirit of higgledy-piggledy line sets (i.e. Theorem 4.1), we improve the known upper bounds when q is an Rth power and $R \geq r/2$. Let us note that these results are also related to *subspace designs*; references are given in Section 6.

Our paper is organised as follows. In Section 2, we introduce the main notation and recall some basic definitions and propositions. The following Section 3 is mainly devoted to provide simpler geometric arguments to known bounds on the length of minimal codes, that is, the size of strong blocking sets. Most of these results were obtained recently in the paper of Alfarano, Borello, Neri and Ravagnani [1]. We also derive some quick consequences on higgledy-piggledy line sets. We continue in Section 4 by a probabilistic argument which largely improves any previously known general upper bounds for strong blocking sets, minimal codes [1, 17] or higgledy-piggledy line sets [21]. Section 4 mainly deals with the cases where the underlying field has more than 2 elements while Section 5 is devoted to the $q = 2$ case. These results in turn imply improved results on covering codes and saturating sets as well that we present in Section 6.

2 Preliminaries

The Hamming distance $d(v, c)$ of vectors v and c in $\mathbb{F}_q^n$ is the number of positions in which v and c differ. The (Hamming) weight $w(c)$ of a vector c is the number of nonzero coordinates of c. The smallest Hamming distance between distinct code vectors is called the *minimum distance* of the code. An $[n, r]_q$ code with minimum distance d is denoted as an $[n, r, d]_q$ code. Note that for a linear code, the minimum distance is equal to the weight of a minimum weight codeword. The sphere of radius R with center c in $\mathbb{F}_q^n$ is the set $\{v : v \in \mathbb{F}_q^n,\ d(v, c) \leq R\}$.

$\begin{bmatrix} n \\ k \end{bmatrix}_q$ denotes the Gaussian binomial coefficient, whose value counts the number of subspaces of dimension k in a vector space of dimension n over a finite field with q elements, or likewise, number of subspaces of dimension $k-1$ in a projective space $\mathrm{PG}(n-1, q)$ of dimension $n-1$ over $\mathbb{F}_q$. More precisely,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{cases} \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q-1)(q^2-1)\cdots(q^k-1)} & k \leq n, \\ 0 & k > n. \end{cases}$$

θ_n denotes the number of points in $\mathrm{PG}(n, q)$, thus $\theta_n = \sum_{t=0}^{n} q^t = \begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q$.

Proposition 2.1. *The number of m-dimensional subspaces containing a given k-dimensional subspace in* $\mathrm{PG}(n, q)$ *equals* $\begin{bmatrix} n-k \\ n-m \end{bmatrix}_q$.

Lemma 2.2.
$\begin{bmatrix} n \\ k \end{bmatrix}_q < q^{(n-k)k} \cdot e^{1/(q-2)}$ *for* $q > 2$ *and*

$\begin{bmatrix} n \\ k \end{bmatrix}_2 < 2^{(n-k)k+1} \cdot e^{2/3}$ *for* $q = 2$.

For the special case $k = n - 2$, we have
$\begin{bmatrix} n \\ n-2 \end{bmatrix}_q < q^{2(n-2)} \cdot \frac{q}{q-1} \frac{q^2}{q^2-1}$ *for* $q \geq 2$.

Since this lemma is a simple but technical one, we opt to give a proof in the Appendix.

Definition 2.3. *An $[n, k]_q$ code $\mathcal{C}$ is* non-degenerate*, if there is no $i \in [n]$ such that $c_i = 0$ for all $c \in \mathcal{C}$. An $[n, k]_q$ code $\mathcal{C}$ is* projective*, if the coordinates of the codewords are linearly* *independent; that is, there exists no $i \neq j \in [n]$ and $\lambda \in \mathbb{F}_q^*$ such that $c_i = \lambda c_j$ for every codeword $c \in \mathcal{C}$.*

In terms of the generator matrix G of $\mathcal{C}$, non-degeneracy means that every column of G is nonzero, and projectivity means that no column of G is a scalar multiple of any other column of G.

Definition 2.4. *Let $\mathcal{C}$ be a code. The* support *$\sigma(c)$ of a codeword c is the set of nonzero coordinates of c; that is, $\sigma(c) = \{i \colon c_i \neq 0\}$. A codeword $c \in \mathcal{C}$ is* minimal *if for every $c' \in \mathcal{C}$ we have $\sigma(c') \subseteq \sigma(c)$ if and only if $c' = \lambda c$ for some $\lambda \in \mathbb{F}_q^*$. A codeword $c \in \mathcal{C}$ is* maximal *if for every $c' \in \mathcal{C}$ we have $\sigma(c') \supseteq \sigma(c)$ if and only if $c' = \lambda c$ for some $\lambda \in \mathbb{F}_q^*$.*

Note that for each codeword c, $|\sigma(c)| = w(c)$. A maximum (minimum) weight codeword may not be maximal (minimal) and, also, a maximal (minimal) codeword is not necessarily a maximum (minimum) weight codeword.

3 Geometrical arguments and higgledy-piggledy line sets

3.1 Geometrical arguments

In this section we aim to emphasise the geometrical interpretation of (minimal) codes in order to apply finite geometrical tools in their analysis. This was done in [1, 2, 37] as well, for example, but our intention is to use finite geometrical arguments much more transparently. Most results presented here are found in [1]; however, we believe that the usefulness of our approach is justified by the simplicity of the proofs.

A well-known and often exploited interpretation of linear codes is the following. Let G be a generator matrix of a non-degenerate $[n, k]_q$ code $\mathcal{C}$. Then the columns $G_1, \ldots, G_n$ of G may be interpreted as points of the projective space $\mathrm{PG}(k-1, q)$. Let $S(G) = \{G_1, \ldots, G_n\}$ denote the (multi)set of points in $\mathrm{PG}(k-1, q)$ corresponding to $\mathcal{C}$. Clearly, different generator matrices of $\mathcal{C}$ yield projectively equivalent (multi)sets of $\mathrm{PG}(k-1, q)$. From now on, we will always assume that a generator matrix G of a given code $\mathcal{C}$ is fixed, and it will not cause ambiguity to omit the references for the generator matrix G and, e.g., write only S. Note that S is a set if and only if $\mathcal{C}$ is projective.

Notation 3.1. *Let $u \in \mathbb{F}_q^k$. Then let $\Lambda_u = \{x \in \mathrm{PG}(k-1, q) \colon x \perp u\}$ be a hyperplane of $\mathrm{PG}(k-1, q)$. For a point set S of $\mathrm{PG}(k-1, q)$, S_u denotes $S \setminus \Lambda_u$. For a vector v over $\mathbb{F}_q$, let $\langle v \rangle = \{\lambda v \colon \lambda \in \mathbb{F}_q^*\}$.*

Each codeword $c \in \mathcal{C}$ can be uniquely obtained in the form uG for some $u \in \mathbb{F}_q^k$. Thus we may associate the hyperplane Λ_u to u. Note that $\Lambda_u = \Lambda_{u'}$ if and only if $\langle u \rangle = \langle u' \rangle$ if and only if $\langle uG \rangle = \langle u'G \rangle$; that is, each hyperplane of $\mathrm{PG}(k-1, q)$ corresponds to a set of $q-1$ (nonzero) codewords of $\mathcal{C}$, which form the nonzero vectors of a one-dimensional linear subspace of $\mathbb{F}_q^n$.

Lemma 3.2. *Let $\mathcal{C}$ be an $[n, k]_q$ code with generator matrix $G = (G_1, \ldots, G_n)$, and let $c = uG \in \mathcal{C}$, $u \in \mathbb{F}_q^k$. Let $S = \{G_1, \ldots, G_n\}$ be the corresponding point set of $\mathrm{PG}(k-1, q)$. Then*

- *c is a minimal codeword if and only if $\Lambda_u \cap S$ spans Λ_u in $\mathrm{PG}(k-1, q)$;*

- *c is a maximal codeword if and only if S_u intersects every hyperplane of* $\mathrm{PG}(k-1,q)$ *different from Λ_u; that is, S_u is an affine blocking set (with respect to hyperplanes) in* $\mathrm{PG}(k-1,q) \setminus \Lambda_u \simeq \mathrm{AG}(k-1,q)$.

Proof. For any two codewords $c = uG$ and $c' = u'G$, we clearly have $\sigma(u'G) \subseteq \sigma(uG)$ if and only if $S_{u'} \subseteq S_u$ if and only if $\Lambda_u \cap S \subseteq \Lambda_{u'} \cap S$.

Fix now $c = uG$. Suppose now that the span of $\Lambda_u \cap S$ is contained in a 2-codimensional subspace of $\mathrm{PG}(k-1,q)$. Consider a hyperplane $\Lambda_{u'} \neq \Lambda_u$ containing this subspace. Then, clearly, $\langle u \rangle \neq \langle u' \rangle$ and $S_{u'} \subseteq S_u$, so c is not minimal. On the other hand, if $\Lambda_u \cap S$ spans Λ_u, then $\sigma(u'G) \subseteq \sigma(uG)$ yields $\Lambda_u \cap S \subseteq \Lambda_{u'} \cap S$, whence $\langle u \rangle = \langle u' \rangle$, so u is minimal.

If for some $u' \in \mathbb{F}_q^k$ we have $\langle u \rangle \neq \langle u' \rangle$, then $\sigma(uG) \not\subseteq \sigma(u'G)$ is equivalent to $\Lambda_{u'} \cap S \not\subseteq \Lambda_u \cap S$ which holds if and only if $\Lambda_{u'}$ contains a point of $S \setminus \Lambda_u = S_u$. That is, $c = uG$ is maximal if and only if S_u is an affine blocking set in $\mathrm{PG}(k-1,q) \setminus \Lambda_u$. □

Corollary 3.3. *Let $\mathcal{C}$ be a non-degenerate $[n,k]_q$ code with generator matrix $G = (G_1, \ldots, G_n)$. Let $S = \{G_1, \ldots, G_n\}$ be the corresponding point set of* $\mathrm{PG}(k-1,q)$*. Then $\mathcal{C}$ is a minimal code if and only if S is a strong blocking set.*

Proof. This follows immediately from Definitions 1.1, 1.7 and Lemma 3.2. □

The above corollary was pointed out in [2] and [37] as well. Furthermore, as it was observed in [1], a code $\mathcal{C}$ is a minimal code if and only if each codeword of $\mathcal{C}$ is maximal. In terms of strong blocking sets, we get the following equivalent description.

Proposition 3.4. *S is a strong blocking set if and only if for any two distinct hyperplanes H_1 and H_2, $(H_1 \setminus H_2) \cap S \neq \emptyset$.*

Proof. The condition is clearly equivalent with $S \setminus H$ being an affine blocking set for each hyperplane H. □

Let us give yet another immediate but useful description of strong blocking sets with which one may also consider them as blocking sets of certain hypergraphs.

Proposition 3.5. *Let $\mathcal{P}$ denote the set of points of* $\mathrm{PG}(N,q)$*, and let*

$$\mathcal{H} = \{T \subseteq \mathcal{P} \mid \exists H, H' \textit{ subspaces s.t. } \dim H = N-1, \dim H' = N-2, H' \subset H, T = H \setminus H'\}.$$

Then S is a strong blocking set of $\mathrm{PG}(N,q)$ *if and only if $S \cap T \neq \emptyset$ for all $T \in \mathcal{H}$.*

Proof. This is just a reformulation of Proposition 3.4. □

As seen above, affine blocking sets are tightly connected to strong blocking sets, hence it is useful to recall a fundamental result on their sizes.

Theorem 3.6 (Jamison [30], Brouwer–Schrijver [13])**.** *Suppose that $\mathcal{B}$ is a blocking set of* $\mathrm{AG}(N,q)$*; that is, $\mathcal{B}$ is a set of points which intersects each hyperplane of* $\mathrm{AG}(N,q)$*. Then* $|\mathcal{B}| \geq N(q-1)+1$.

Next we reprove Theorem 2.8 of [1].

Theorem 3.7. *Let $\mathcal{C}$ be an $[n,k]_q$ code. If $c \in \mathcal{C}$ is maximal, then $w(c) \geq (k-1)(q-1)+1$. Thus the minimum weight of a minimal $[n,k]_q$ code is at least $(k-1)(q-1)+1$. In other words, if S is a strong blocking set of $\mathrm{PG}(N,q)$, then for each hyperplane H, $|S \setminus H| \geq N(q-1)+1$.*

Proof. Let $c = uG$. By Lemma 3.2, S_u is an affine blocking set in $\mathrm{PG}(k-1,q)\setminus\Lambda_u \simeq \mathrm{AG}(k-1,q)$. By Jamison's Theorem, $w(u) = |S_u| \geq (q-1)(k-1)+1$. □

Corollary 3.8 ([1, 2, 37])**.** *Let $\mathcal{C}$ be a minimal $[n,k]_q$ code. Then $n \geq q(k-1)+1$. In other words, a strong blocking set of $\mathrm{PG}(N,q)$ has at least $Nq+1$ points.*

Proof. Take a codeword $c = uG$ in $\mathcal{C}$. As c is maximal, $w(c) = |S_u| \geq (q-1)(k-1)+1$. As c is minimal, $\Lambda_u \cap S$ spans Λ_u, hence $|\Lambda_u \cap S| \geq k-1$. Thus $n = |S| \geq (q-1)(k-1)+1+(k-1)$. □

The proof of Theorem 3.7 in [1] uses the Alon-Füredi Theorem, while [37] also uses Jamison's theorem to derive Corollary 3.8. For connections among the Alon-Füredi Theorem, Jamison's Theorem and the (punctured) Combinatorial Nullstellensatz, we refer to [5].

The following two theorems were proved by Alfarano et al. [1].

Theorem 3.9 (Theorem 2.13 of [1])**.** *Let $\mathcal{C}$ be an $[n,k]_q$ code, and let $c \in \mathcal{C}$ be a maximal codeword. Then for every $i \in \sigma(c)$, there exists $c' \in \mathcal{C}$ such that $|\sigma(c') \cap (\sigma(c)\setminus\{i\})| \geq (q-1)(k-1)$. In other words, if S is a strong blocking set in $\mathrm{PG}(N,q)$, then for all hyperplane H and every point $P \in (S \setminus H)$ there exists a hyperplane H' such that $|S \setminus (H \cup H' \cup \{P\})| \geq (q-1)N$.*

Proof. Let $c = uG$. By Lemma 3.2, S_u is an affine blocking set in $\mathrm{PG}(k-1,q)\setminus\Lambda_u \simeq \mathrm{AG}(k-1,q)$. If $G_i \in S_u$ is an essential point for S_u (that is, $S_u \setminus \{G_i\}$ is not an affine blocking set), then there is a hyperplane Λ_v ($v \in \mathbb{F}_q^k$) such that $\Lambda_v \cap S_u = \{G_i\}$, hence $S_v \cap S_u \supseteq S_u \setminus \{G_i\}$; that is, $\sigma(vG) \supseteq (\sigma(uG) \setminus \{i\})$ and thus, by Theorem 3.7, $c' = vG$ is an appropriate choice.
If G_i is not essential for the affine blocking set S_u, then remove G_i and possibly some further points of S_u to obtain an affine blocking set for which every point is essential. By Jamison's theorem, this blocking set still has at least $(q-1)(k-1)+1$ points. As in the previous case, a tangent hyperplane to this affine blocking set corresponds to a proper codeword c'. □

The next proof is a direct geometric adaptation of the one in [1]; we include it for the sake of completeness.

Theorem 3.10 (Theorem 2.14 of [1])**.** *Let $\mathcal{C}$ be a minimal $[n,k]_q$ code. Then $n \geq (q+1)(k-1)$. In other words, a strong blocking set in $\mathrm{PG}(N,q)$ contains at least $N(q+1)$ points.*

Proof. Let $c = uG$ be a minimum weight codeword. Let $D = |H_u \cap S| = n - w(c)$. As $\mathcal{C}$ is minimal, c is a maximal codeword. By Theorem 3.9, there exists a codeword $c' = vG$ such that $|S_u \cap S_v| = |(S \setminus H_u) \setminus H_v| \geq (q-1)(k-1)|$. Let $H_{uv} = H_u \cap H_v$ be a 2-codimensional subspace. There are $q-1$ hyperplanes containing H_{uv} different from H_u and H_v, hence at least one of these contain at least $k-1$ points of $(S \setminus H_u) \setminus H_v$. Let H_z be such a hyperplane. Then, as $c = uG$ is a minimum weight codeword,

$$\begin{aligned} D \geq |H_z \cap S| &= |H_z \cap S_u| + |H_z \cap H_u \cap S| = |H_z \cap S_u| + |H_v \cap H_u \cap S| \\ &= |H_z \cap S_u| + |S \cap H_u| + |(S \setminus H_u) \setminus H_v| - |S \setminus H_v| \\ &\geq k-1+D+(q-1)(k-1)+|S \setminus H_v|, \end{aligned}$$

hence $|S \setminus H_v| \geq q(k-1)$. Since $c' = vG$ is a minimal codeword of $\mathcal{C}$, $S \cap H_v$ generates H_v and so it must contain at least $k-1$ points. Thus $n = |S| = |S \setminus H_v| + |S \cap H_v| \geq (q+1)(k-1)$. $\square$

3.2 Notes on higgledy-piggledy line sets

In the following, let us slightly strengthen Theorem 1.9 on the size of higgledy-piggledy line sets.

Lemma 3.11. *Let $\mathcal{L}$ be a higgledy-piggledy line set of* $\mathrm{PG}(N,q)$*, and suppose that a hyperplane H contains t lines of $\mathcal{L}$. Then $|\mathcal{L}| \geq N + t - \left\lfloor \frac{N-1}{q} \right\rfloor$.*

Proof. Since $S = \cup_{\ell \in \mathcal{L}} \ell$ is a strong blocking set, $S \setminus H$ is an affine blocking set, and thus it contains at least $N(q-1)+1$ points (see Jamison's Theorem 3.6). Since each line of $\mathcal{L}$ contains at most q points of $S \setminus H$, we need at least $\frac{|S \setminus H|}{q} \geq N - \frac{N-1}{q}$ lines to cover the points of $S \setminus H$. Together with the lines contained in H, this proves the assertion. $\square$

Theorem 3.12. *A line set of* $\mathrm{PG}(N,q)$ *in higgledy-piggledy arrangement contains at least $N + \left\lfloor \frac{N}{2} \right\rfloor - \left\lfloor \frac{N-1}{q} \right\rfloor$ elements.*

Proof. Let $\mathcal{L}$ be a higgledy-piggledy line set of $\mathrm{PG}(N,q)$, and let $S = \cup_{\ell \in \mathcal{L}} \ell$. As x lines of $\mathrm{PG}(N,q)$ span a subspace of dimension at most $2x-1$, we can find a hyperplane H which contains at least $\left\lfloor \frac{N}{2} \right\rfloor$ lines of $\mathcal{L}$ (we need that $|\mathcal{L}| \geq \left\lfloor \frac{N}{2} \right\rfloor$, but this is clear since $\mathcal{L}$ cannot be contained in a hyperplane). Apply Lemma 3.11 to finish the proof. $\square$

Remark 3.13. *Note that if $q \geq N$, the above result yields that a higgledy-piggledy line set contains at least $N + \left\lfloor \frac{N}{2} \right\rfloor$ lines. Comparing this to the assumption $q \geq N + \left\lfloor \frac{N}{2} \right\rfloor$ of Theorem 1.9, one can see that Theorem 3.12 gives a strengthening of the theorem of Fancsali and Sziklai.*

Fancsali and Sziklai prove that if there is no $(N-2)$-dimensional subspace intersecting every line of a line set in $\mathrm{PG}(N,q)$, then the line set is higgledy-piggledy [21, Theorem 11], and they also prove that if $q > |\mathcal{L}|$ for a higgledy-piggledy line set $\mathcal{L}$, then $\mathcal{L}$ has the aforementioned property [21, Lemma 12]. Thus they call this property 'almost equivalent' to being higgledy-piggledy. In the light of these considerations, it might be somewhat surprising that minimal higgledy-piggledy line sets *always* admit an $(N-2)$-dimensional subspace which intersects all but possibly one of their lines.

Proposition 3.14. *Suppose that $\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$ is a minimal set of higgeldy-piggledy lines in* $\mathrm{PG}(N,q)$ *(that is, $S = \cup_{i=1}^m \ell_i$ is a strong blocking set of* $\mathrm{PG}(N,q)$*, but for all $j \in \{1, \ldots, m\}$, $S_j := \cup_{\substack{i=1 \\ i \neq j}}^m \ell_i$ is not a strong blocking set). Then for all $j \in \{1, \ldots, m\}$, there exists a subspace Λ_j of co-dimension 2 which intersects ℓ_i for each $i \in \{1, \ldots, m\} \setminus \{j\}$. Moreover, there exists a hyperplane H_j containing Λ_j, which contains only those lines of $\mathcal{L} \setminus \{\ell_j\}$ that are contained in Λ_j.*

Proof. Fix $j \in \{1, \ldots, m\}$. Since S_j is not a strong blocking set, there exist a hyperplane H_1 for which the point set $S_j \setminus H_1$ is not an affine blocking set in $\mathrm{PG}(N,q) \setminus H_1$, that is, there exists another hyperplane H_2 such that $H_2 \cap (S_j \setminus H_1) = \emptyset$. As each line intersects H_2, this means that for each $i \in \{1, \ldots, m\} \setminus \{j\}$, $ell_i \cap H_2 \in H_1$. Thus the subspace $H_1 \cap H_2$ and the hyperplane H_2 are appropriate choices to prove the assertion. $\square$

Note that it might occur that a subspace of co-dimension 2 blocks every line of a higgledy-piggledy line set $\mathcal{L}$ of $\mathrm{PG}(N,q)$. In fact, this is the case whenever our line set has at most $N+\lfloor N/2\rfloor-1$ elements [21, Lemma 13], in which case $|\mathcal{L}|\geq q+1$ holds [21, Lemma 12]; but, if q is small compared to N, the latter conclusion is meaningless. In particular, when $q=2$, there exist examples of higgledy-piggledy line sets of $\mathrm{PG}(N,2)$ of size less than $N+\lfloor N/2\rfloor$, see Section 5. As seen, these must admit a subspace of dimension $(N-2)$ intersecting all their lines.

Let us point out that if q is small, then, by the pigeonhole principle, Proposition 3.14 yields that the $q+1$ hyperplanes passing through the $(N-2)$-dimensional subspace found therein behave unbalanced regarding the number of lines of $\mathcal{L}$ they contain.

4 Probabilistic approach

Theorem 4.1. *There exists a strong blocking set in* $\mathrm{PG}(N,q)$ *of size at most* $m(q+1)$*, which consists of the points of at most* m *lines, where*

$$m=\begin{cases}\left\lceil \frac{2}{1+\frac{1}{\ln(q)(q+1)^2}}N\right\rceil & \text{if } q>2,\\[2ex] \left\lceil \frac{\ln 8}{\ln 8/3}N\right\rceil & \text{if } q=2.\end{cases}$$

In other words, this theorem ensures the existence of m lines in higgledy-piggledy arrangement. Note that the multiplier of N for $q>2$ is strictly smaller than 2, while $\frac{\ln 8}{\ln 8/3}\approx 2.12$.

Proof. Let us take a projective space $\mathrm{PG}(N,q)$, and choose m lines, $\ell_1,\ell_2,\dots\ell_m$ uniformly at random. We denote this multiset by $\mathcal{L}=\{\ell_1,\ell_2,\dots\ell_m\}$.

Our aim is to bound from below the probability that the point set $\mathcal{B}=\bigcup_{i=1}^m\ell_i$ intersects every hyperplane Λ in a subset which spans Λ itself.

Clearly, by the definition of strong blocking sets,

$$\mathbb{P}(\mathcal{B}\text{ is a strong blocking set})=1-\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda=N-1,\ \langle\Lambda\cap\mathcal{B}\rangle\neq\Lambda).$$

Observe that for a hyperplane Λ, $\langle\Lambda\cap\mathcal{B}\rangle\neq\Lambda$ implies that $\dim\langle\Lambda\cap\mathcal{B}\rangle<N-1$. Since every ℓ_i intersects Λ, the intersections must be covered by a subspace of dimension at most $N-2$. Moreover, if the dimension of a covering subspace Λ' is $N-2$, then none of the lines ℓ_i intersects $\Lambda\setminus\Lambda'$. From this, we obtain the following bound.

$$\begin{aligned}\mathbb{P}(\mathcal{B}\text{ is a strong blocking set})\geq 1&-\sum_{d<N-2}\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda=d,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset)\\ &-\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda=N-2,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset,\ \bigcup_i\langle(\mathcal{B}\cap\Lambda)\cup\ell_i\rangle\neq\mathrm{PG}(N,q)).\end{aligned}\tag{4.1}$$

Firstly we give a bound to a term $\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda=d,\ \forall i\,\ell_i\cap\Lambda\neq\emptyset)$ with $d\leq N-2$ in Inequality (4.1).

$$\mathbb{P}(\exists\Lambda\colon\ \dim\Lambda = d,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset) \le \begin{bmatrix} N+1 \\ d+1 \end{bmatrix}_q \cdot \mathbb{P}(\ell_1\cap\Lambda\neq\emptyset)^m, \tag{4.2}$$

where the last probability is taken for a fixed d-dimensional subspace Λ and the line ℓ_1 chosen uniform randomly. Distinguishing the lines which are contained in Λ from those which intersect Λ in a single point, we get (for precise details, see the Appendix)

$$\begin{aligned} \mathbb{P}(\ell_1\cap\Lambda\neq\emptyset) &= \frac{\begin{bmatrix} d+1 \\ 2 \end{bmatrix}_q + \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q \cdot \frac{1}{q}\left(\begin{bmatrix} N+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q\right)}{\begin{bmatrix} N+1 \\ 2 \end{bmatrix}_q} \\ &< q^{d-N+1} + q^{d-N} - q^{2d-2N+1}. \end{aligned} \tag{4.3}$$

In the next step, we apply a simple upper bound $q^{d-N+1}(1+\frac{1}{q})$ for the probability above, while we will use the upper bound in its full strength later on when we consider the case $d = N-2$.

By combining Inequalities (4.2) and (4.3) with the upper bound of Lemma 2.2 on the Gaussian binomial coefficients, we get

$$\sum_{d<N-2}\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda = d,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset) < \sum_{d<N-2} q^{(N-d)(d+1)+(d-N+1)m}\cdot\left(1+\frac{1}{q}\right)^m\cdot\gamma(q), \tag{4.4}$$

where $\gamma(q) = e^{1/(q-2)}$ for $q>2$ and $\gamma(q) = 2e^{2/3}$ for $q=2$.

Here we may write (we may assume $m \ge N$)

$$\begin{aligned} \sum_{d=0}^{N-3} q^{(N-d)(d+1)+(d-N+1)m} &= \sum_{d=0}^{N-3} q^{(N-d)(d+1-m)+m} \\ &\le q^{3(N-2-m)+1+m} = q^{3N-2m-5}, \end{aligned}$$

which in turn implies

$$\sum_{d<N-2}\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda = d,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset) < q^{3N-2m-5}\cdot\left(1+\frac{1}{q}\right)^m\cdot\gamma(q). \tag{4.5}$$

It is easy to see that if $q\ge 3$, then $q^{3N-2m}\cdot\left(1+\frac{1}{q}\right)^m < 1$ holds for $m \ge 1.8N$, hence

$$p_{<N-2} := \sum_{d<N-2}\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda = d,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset) < q^{-5}\cdot\gamma(q) \tag{4.6}$$

in the case $q\ge 3$. Case $q=2$ only allows us to choose $m = \frac{\ln 8}{\ln 8/3}N \approx 2.12N$ in order to get $2^{3N-2m}\cdot\left(1+\frac{1}{2}\right)^m \le 1$, which implies Inequality (4.6) similarly for $q=2$. Let $\delta(q,N) = 1.8N$ for $q>2$ and $\delta(2,N) = \frac{\ln 8}{\ln 8/3}N$.

We continue by estimating the final summand, namely

$$\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda = N-2,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset,\ \bigcup_i\langle(\mathcal{B}\cap\Lambda)\cup\ell_i\rangle\neq \mathrm{PG}(N,q)).$$

Suppose now that every line of $\mathcal{L}$ intersects a fixed subspace Λ of dimension $N-2$. We have

$$\eta := \mathbb{P}(\ell\subseteq\Lambda\ \mid\ \ell\cap\Lambda\neq\emptyset) = \frac{\begin{bmatrix}N-1\\2\end{bmatrix}_q}{\begin{bmatrix}N-1\\2\end{bmatrix}_q + (q^{N-1}+q^{N-2})\begin{bmatrix}N-1\\1\end{bmatrix}_q} < \frac{1}{q^3+q^2-q}.$$

Observing that there are $q+1$ hyperplanes through Λ, the probability of the (bad) event that every line $\ell\in\mathcal{L}$ is either included in Λ or not included in a fixed hyperplane through Λ can be bounded above by the following formula:

$$\left(\eta+(1-\eta)\frac{q}{q+1}\right)^m < \left(\frac{1}{q^3+q^2-q}+\left(1-\frac{1}{q^3+q^2-q}\right)\frac{q}{q+1}\right)^m < \left(\frac{q}{q+1}+\frac{1}{q^3(q+1)}\right)^m.$$

Adding the probability of these events for every hyperplane through Λ, we obtain

$$\begin{aligned} p_{N-2} := \mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda = N-2,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset,\ \bigcup_i\langle(\mathcal{B}\cap\Lambda)\cup\ell_i\rangle\neq \mathrm{PG}(N,q)) \leq \\ \mathbb{P}\left(\exists\,\Lambda\colon\ \dim\Lambda = N-2,\ \forall i\ \ell_i\cap\Lambda\neq\emptyset\right)\cdot\left((q+1)\left(\frac{q}{q+1}+\frac{1}{q^3(q+1)}\right)^m\right) \end{aligned} \tag{4.7}$$

via conditional probability. We use Inequality (4.2), Lemma 2.2, and Inequality (4.3) with the more precise factor $\left(1+\frac{1}{q}-\frac{1}{q^2}\right)$ instead of $\left(1+\frac{1}{q}\right)$, and apply similar calculations to those in Inequalities (4.4) and (4.5) but with $d=N-2$. This provides

$$\begin{aligned} p_{N-2} \leq q^{2(N-1)-m}\cdot\frac{q}{q-1}\frac{q^2}{q^2-1}\left(1+\frac{1}{q}-\frac{1}{q^2}\right)^m\left((q+1)\cdot\left(\frac{q}{q+1}+\frac{1}{q^3(q+1)}\right)^m\right) \\ < \frac{q}{(q-1)^2}q^{2N-m}\left(1-\frac{1}{(q+1)^2}\right)^m. \end{aligned} \tag{4.8}$$

Putting all these estimates together, we get that if $m\geq\delta(q,N)$, then

$$\begin{aligned} \mathbb{P}(\mathcal{B}\text{ is a strong blocking set}) &\geq 1-p_{<N-2}-p_{N-2} \\ &> 1-q^{-5}\cdot\gamma(q)-\frac{q^{2N-m+1}}{(q-1)^2}\left(1-\frac{1}{(q+1)^2}\right)^m. \end{aligned}$$

This event is of positive probability for the point set of $m=\left\lceil\frac{2N}{1+\frac{1}{\ln(q)(q+1)^2}}\right\rceil$ randomly chosen lines for $q>2$. If $q=2$, then $p_{N-2}\leq\frac{1}{\sqrt{2}}$ suffice, and this can be attained if $2^{2N+1.5}\cdot 2^{-m}\cdot\frac{85}{96}^m=1$ via Inequality (4.8). This implies that the choice $m=\lceil 0.851\cdot(2N+1.5)\rceil > \left\lceil\frac{\ln 2}{\ln 2\cdot\frac{96}{85}}(2N+1.5)\right\rceil$ does the job, hence the proof is complete. □

5 Random constructions in $\mathrm{PG}(N, 2)$

When the order of the field is two, or in other words, in the case of binary minimal codes, we provide a better upper bound on the size of strong blocking sets than the one in Theorem 4.1. Let us mention that in this case, minimal codes coincide with the so-called intersecting codes. For more information about intersecting codes, we refer the reader to [15] and [16]. Recall that for $q = 2$, $\theta_i = 2^i + 2^{i-1} + \ldots + 1 = 2^{i+1} - 1$.

5.1 Uniform random point sets

Take a set S of x points of $\mathrm{PG}(N, 2)$ uniformly at random. By Proposition 3.5, S is a strong blocking set if and only if it intersects each element of

$$\mathcal{H} = \{T \subseteq \mathcal{P} \mid \exists H, H' \text{ subspaces s.t } \dim H = N-1, \dim H' = n-2, H' \subset H, T = H \setminus H'\},$$

where $\mathcal{P}$ denotes the point set of $\mathrm{PG}(N, q)$. Clearly, $|\mathcal{H}| = \theta_N \theta_{N-1}$, and for each $T \in \mathcal{H}$, $|T| = \theta_{N-1} - \theta_{N-2} = 2^{N-1}$. Consequently, the probability that a set $T \in \mathcal{H}$ is missed by S is $\left(\frac{\theta_N - 2^{N-1}}{\theta_N}\right)^x < (\frac{3}{4})^x$, which yields the following bound on the expected value of the number of elements of $\mathcal{H}$ not intersecting S:

$$\mathbb{E}(T \in \mathcal{H} \mid S \cap T = \emptyset) < 2^{2N+1} \left(\frac{3}{4}\right)^x.$$

The existence of a strong blocking set of size x follows if the latter formula is less than 1, thus $x = \left\lceil \frac{\log(2)}{\log(4/3)}(2N+1) \right\rceil \approx \lceil 2.41 \cdot (2N+1) \rceil$ suffices. Thus we have the following result.

Theorem 5.1. *In* $\mathrm{PG}(N, 2)$*, there exists a strong blocking set of size*

$$\left\lceil \frac{\log(2)}{\log(4/3)}(2N+1) \right\rceil.$$

Note that this random construction improves the bound of Theorem 1.4 by an additive constant.

Corollary 5.2.

$$m(k, 2) \leq \frac{2k-1}{\log_2(\frac{4}{3})}.$$

5.2 Explicit results for small N

We have utilised a computer to perform a simple Monte Carlo search. First we chose a set S of x points of uniform random distribution and then checked if the result was a strong blocking set of $\mathrm{PG}(N, q)$. We tried to decrease x as much as possible. The sizes of the smallest strong blocking sets found this way are found in the next table.

N	2	3	4	5	6	7	8	9	10
$\|S\|$	6	9	13	17	22	27	32	37	44

Doing the same in order to find m lines in higgledy-piggledy arrangement in $\mathrm{PG}(N,q)$, we obtained the results shown in the next table. For the sake of easy comparison with the bound $m \geq \lfloor 3N/2 \rfloor$ known to be valid for q large enough (cf. Theorem 1.9 and Remark 3.13), we inserted the value of $\lfloor 3N/2 \rfloor$ as well. Also, as the elements of a line set $\{\ell_1, \ldots, \ell_m\}$ in higgledy-piggledy arrangement are not necessarily disjoint, their union may be smaller than $m(q+1)$.

N	2	3	4	5	6	7	8	9	10
$\lfloor \frac{3N}{2} \rfloor$	3	4	6	7	9	10	12	13	15
m	3	4	5	6	8	9	11	13	14
$\lvert \cup_{i=1}^{m} \ell_i \rvert$	6	9	13	18	23	27	32	38	42

6 Covering codes and saturating sets

As we explained in detail in the Introduction, saturating sets and covering codes are corresponding objects, and bounding the size of a saturating set corresponds to bounding the length function $l_q(r, R)$ of the covering code. From now on, we use the geometric terminology. Let us recall the concept of ϱ–saturating sets of a projective plane $\mathrm{PG}(N,q)$.

Definition 6.1. *A set $\mathcal{S}$ of points of* $\mathrm{PG}(N,q)$ *is said to be* ϱ–saturating *if for any point $P \in \mathrm{PG}(N,q)$ there exist $\varrho+1$ points of $\mathcal{S}$ spanning a subspace of* $\mathrm{PG}(N,q)$ *containing P, and ϱ is the smallest value with such property.*

Davydov, Giulietti, Marcugini and Pambianco proved [17] a key connection between $(\varrho+1)$-fold strong (or cutting) blocking sets and ϱ-saturating sets.

Theorem 6.2 ([17], Theorem 3.2.)**.** *Any $(\varrho+1)$-fold strong blocking set in a subgeometry* $\mathrm{PG}(N,q) \subset \mathrm{PG}(N,q^{\varrho+1})$ *is a ϱ-saturating set in the space* $\mathrm{PG}(N,q^{\varrho+1})$.

Let $s_q(N,\varrho)$ denote the smallest size of a ϱ–saturating set of $\mathrm{PG}(N,q)$. For recent upper bounds on ϱ–saturating sets of $\mathrm{PG}(N,q)$ the reader is referred to [18, 20].

Theorem 6.3 (Denaux [20], Theorem 6.2.12.)**.** *Suppose that q is a prime power. Then*

$$\frac{\varrho+1}{e} q^{N-\varrho} < s_{q^{\varrho+1}}(N,\varrho) \leq \varrho(\varrho+1)\left(\frac{q^{N-\varrho}}{2} + \frac{q^{N-\varrho}-1}{q-1}\right).$$

The most well-studied case is $\varrho = 1$ where Theorem 6.2 provides an upper bound on saturating sets via the size of 2-fold strong blocking sets, while the other side of the spectrum, namely the case of N-fold strong blocking sets (that we called strong blocking sets for brevity) is also significant. Our probabilistic upper bound in Theorem 4.1 thus in turn gives the following corollary.

Corollary 6.4. *If $q > 2$, then* $s_{q^N}(N, N-1) \leq \left\lceil \frac{2N}{1+\frac{1}{\ln(q)(q+1)^2}} \right\rceil (q+1)$.

Note that the previously known general result in this direction was the tetrahedron construction, see [1] which provides a point set of size $\binom{N+1}{2}(q-1)+N+1$ for a cutting blocking set, and also for a saturating set in $\mathrm{PG}(N,q^2)$, and the very recent slight improvement of Denaux [20, Theorem 6.2.11.] gives $s_{q^N}(N,N-1) \leq \frac{N(N+1)}{2}q - \binom{N}{2}$.

It is easy to see that the larger ρ is, the larger is the gap between the lower and upper bounds of Theorem 6.3. Our main result in this section is Corollary 6.7 in which we get an upper bound close to the lower bound even if ϱ is large.

Following the proof of Theorem 4.1 on an upper bound of strong blocking sets, one can get a general result for t-fold strong blocking sets as well. The idea is analogous to that in Theorem 4.1: we construct a t-fold strong blocking set in $\mathrm{PG}(N,q)$ as the union of a small number of randomly chosen $(N-t+1)$-dimensional subspaces. Note that a set of subspaces of $\mathrm{PG}(N,q)$ of dimension $N-t+1$ whose union is a t-fold strong blocking set is also called a set of *higgledy-piggledy* $(N-t+1)$*-spaces* [22]. Similarly as in [21] for the case of higgledy-piggledy line sets (that is, $t=N$), Fancsali and Sziklai construct a set of higgledy-piggledy $(N-t+1)$-spaces in $\mathrm{PG}(N,q)$ of size $(N-t+2)(t-1)+1$, whenever $q>N+1$ [22, Subsection 3.4]. Our random construction reaches this size only asymptotically in q, but it does not require q to be large.

Theorem 6.5. *There is a strong t-fold blocking set $\mathcal{B}$ in $\mathrm{PG}(N,q)$ consisting of the points of m subspaces of dimension $N-t+1$ for*

$$m=\lceil (N-t+2)(t-1)c_1(q)+c_2(q)\rceil,$$

where the constants $c_1(q)$ and $c_2(q)$ are defined as

$$c_1(q)=\begin{cases}\frac{-\ln q}{\ln(1-e^{-\frac{1}{q-2}})} & \text{for } q>2,\\[2ex] \frac{-\ln 2}{\ln(1-0.5e^{-\frac{2}{3}})} & \text{for } q=2.\end{cases}\quad \text{and}\quad c_2(q)=\begin{cases}\frac{-1}{(q-2)\ln(1-e^{-\frac{1}{q-2}})} & \text{for } q>2,\\[2ex] \frac{-\ln(2e^{2/3})}{\ln(1-0.5e^{-\frac{2}{3}})} & \text{for } q=2.\end{cases}\tag{6.1}$$

In other words, the theorem above ensures the existence of a set of higgledy-piggledy $(N-t+1)$-spaces of size m. Note that $c_1(q)\to 1$ as q tends to infinity and $c_1(2)\approx 2.34$, whereas $c_2(q)\to 0$ as q tends to infinity and $c_2(2)\approx 4.58$, $c_2(3)\approx 2.18$, and $c_2(q)<1$ for $q\geq 4$.

Proof. The proof is again an application of the first moment method. Let us choose a (multi)set of m subspaces $\{H_1,\dots,H_m\}$ of dimension $N-t+1$ in $\mathrm{PG}(N,q)$ uniform randomly, and let $\mathcal{B}=\cup_{i=1}^m H_i$. First consider the following simple observation.

$$\mathbb{P}(\mathcal{B}\text{ is a } t\text{-fold strong blocking set})\geq 1-\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda=t-2,\ \forall i\ H_i\cap\Lambda\neq\emptyset)\tag{6.2}$$

Indeed, if there does not exists such a subspace, then the intersection with every $t-1$ dimensional subspace Λ must be a point set that cannot be covered by a single $t-2$ dimensional subspace, hence the intersection spans Λ itself. Here we may apply a rough estimate on the probability

$$\mathbb{P}(\exists\,\Lambda\colon\ \dim\Lambda=t-2,\ \forall i\ H_i\cap\Lambda\neq\emptyset)$$

by applying the following lemma.

Lemma 6.6. *Let H be a subspace of dimension $N-t+1$ chosen uniform randomly, and let Λ be a fixed $(t-2)$-dimensional subspace. Then*

$$\mathbb{P}(H\cap\Lambda\neq\emptyset)<\begin{cases}1-\frac{1}{e^{\frac{1}{q-2}}} & \text{for } q>2,\\[2ex] 1-\frac{1}{2e^{\frac{2}{3}}} & \text{for } q=2.\end{cases}\tag{6.3}$$

Proof. Let us consider $\mathrm{PG}(N,q)$ as an $(N+1)$-dimensional vector space over $\mathrm{GF}(q)$, and let us count the number A of $(N-t+2)$-dimensional subspaces that are disjoint from the given $(t-1)$-dimensional subspace Λ. We do this via counting the suitable bases for the $(N-t+2)$-dimensional subspace:

$$A = \frac{\prod_{i=0}^{N-t+1} (q^{N+1} - q^{t-1+i})}{\prod_{i=0}^{N-t+1} (q^{N-t+2} - q^i)} = \frac{\prod_{i=0}^{N-t+1} q^{t-1+i}}{\prod_{i=0}^{N-t+1} q^i} = q^{(t-1)(N-t+2)}.$$

Hence by taking into consideration the upper bound of Lemma 2.2 on Gaussian binomials, the probability that an $(N-t+2)$-dimensional subspace intersects Λ non-trivially is

$$1 - \frac{q^{(t-1)(N-t+2)}}{\begin{bmatrix} N+1 \\ N-t+2 \end{bmatrix}_q} < \begin{cases} 1 - \frac{1}{e^{\frac{1}{q-2}}} & \text{for } q > 2, \\ 1 - \frac{1}{2e^{\frac{2}{3}}} & \text{for } q = 2. \end{cases}$$

□

Clearly,

$$\mathbb{P}(\exists \Lambda\colon \dim \Lambda = t-2,\ \forall i\ H_i \cap \Lambda \neq \emptyset) \leq \begin{bmatrix} N+1 \\ t-1 \end{bmatrix}_q (\mathbb{P}(H_1 \cap \Lambda \neq \emptyset))^m .$$

From Lemma 2.2 on the Gaussian binomials and Lemma 6.6 we obtain

$$\mathbb{P}(\exists \Lambda\colon \dim \Lambda = t-2,\ \forall i\ H_i \cap \Lambda \neq \emptyset) \leq q^{(N-t+2)(t-1)} \cdot e^{1/(q-2)} \left(1 - e^{-\frac{1}{q-2}}\right)^m$$

for $q > 2$, and

$$\mathbb{P}(\exists \Lambda\colon \dim \Lambda = t-2,\ \forall i\ H_i \cap \Lambda \neq \emptyset) \leq q^{(N-t+2)(t-1)} \cdot 2e^{2/3} \left(1 - \frac{1}{2e^{\frac{2}{3}}}\right)^m$$

for $q = 2$.

It is easy to check that if we choose m as claimed, then the probability in view is strictly smaller than 1, completing the proof. □

This is turn provides a bound on ϱ-saturating sets via Theorem 6.2.

Corollary 6.7.

$$s_{q^{\varrho+1}}(N,\varrho) \leq \lceil c_1(q)(N-\varrho+1)\varrho + c_2(q) \rceil \frac{q^{N-\varrho+1}-1}{q-1}.$$

Note that this improves the bound of Denaux [20] if q and ϱ is large enough; more precisely for every $\varrho > N/2$ if q is large enough.

Let us also note that the aforementioned construction of Fancsali and Sziklai [22] yields

$$s_{q^{\varrho+1}}(N,\varrho) \leq \lceil (N-\varrho+1)\varrho \rceil \frac{q^{N-\varrho+1}-1}{q-1}$$

whenever $q > N+1$. Finally, let us mention that higgledy-piggledy lines and subspaces are also related to *uniform subspace designs.* For the definition and coding theoretic applications of subspace designs, we refer to the works of Guruswami and Kopparty [24], Guruswami, Resch, and Xing [25] and the references therein, whereas the relation of uniform subspace designs and higgledy-piggledy subspaces can be found in the work of Fancsali and Sziklai [22].

References

[1] G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani. Three Combinatorial Perspectives on Minimal Codes *Arxiv preprint.*, 2020. arXiv:2010.16339

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

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

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

[5] S. Ball and O. Serra. Punctured combinatorial Nullstellensätze. *Combinatorica*, 29:511–522, 2009.

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

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

[8] D. Bartoli, M. Bonini, and B. Güneş. An inductive construction of minimal codes. *Cryptogr. Commun.*, 2021.

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

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

[11] A. Blokhuis, L. Lovász, L. Storme, T. Szőnyi. On multiple blocking sets in Galois planes. *Adv. Geom.*, 7:39–53, 2007.

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

[13] A. E. Brouwer and A. Schrijver. The blocking number of an affine space. *J. Combin. Theory Ser. A*, 24:251–253, 1978.

[14] B. Csajbók, T. Héger. Double blocking sets of size $3q - 1$ in $\mathrm{PG}(2, q)$. *European Journal of Combinatorics* 78:73–89, 2019.

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

[16] G. Cohen, G., A. Lempel. Linear intersecting codes. *Discrete Mathematics*, 56(1), 35-43, 1985.

[17] A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco. Linear nonbinary covering codes and saturating sets in projective spaces. *Advances in Mathematics of Communications*, 5(1), 119–147, 2011.

[18] 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. Designs, Codes and Cryptography, 87(12), 2771–2792, 2019.

[19] J. De Beule, T. Héger, T. Szőnyi, G. Van de Voorde. Blocking and double blocking sets in finite planes. *Electronic J. Comb.*, 23(2), 2016.

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

[21] Sz. L. Fancsali, P. Sziklai. Lines in higgledy-piggledy arrangement. *Electron. J. Comb.*, 21(2):#P2.56, 2014.

[22] Sz. L. Fancsali, P. Sziklai. Higgledy-piggledy subspaces and uniform subspace designs. *Des. Codes Cryptogr.*, 79(3):625–645, 2016.

[23] A. Gács and T. Szőnyi. Random constructions and density results. *Designs, Codes and Cryptography*, 47(1-3), 267–287, (2008).

[24] V. Guruswami and S. Kopparty. Explicit subspace designs. *Combinatorica*, 36(2):161–185, 2016.

[25] V. Guruswami, N. Resch, and C. Xing. Lossless dimension expanders via linearized polynomials and subspace designs. *Combinatorica*, 2021. `https://doi.org/10.1007/s00493-020-4360-1`

[26] T. Héger, B. Patkós, M. Takáts. Search problems in vector spaces. *Designs, Codes and Cryptography*, 76(2), 207–216, 2015.

[27] J .W .P. Hirschfeld. Projective Geometries over Finite Fields. Oxford Mathematical Monographs, Oxford Science Publications, The Clarendon Press, Oxford University Press, New York (1998).

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

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

[30] R. E. Jamison. Covering finite fields with cosets of subspaces. *J. Comb. Th. Ser. A*, 22:253–266, 1977.

[31] J. H. Kim, and V. H. Vu. Small complete arcs in projective planes. *Combinatorica*, 23(2), 311–363, 2003.

[32] Gy. Kiss and T. Szőnyi. Finite Geometries (1st ed.). CRC Press, 2019.

[33] W. Lu, X. Wu, and X. Cao. The parameters of minimal linear codes. *Finite Fields and Their Applications,* 71, 101799. 2021.

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

[35] Z. L. Nagy. Saturating sets in projective planes and hypergraph covers. *Discrete Mathematics*, 341(4), 1078–1083, 2018.

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

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

7 Appendix

Lemma 2.2.

$\begin{bmatrix} n \\ k \end{bmatrix}_q < q^{(n-k)k} \cdot e^{1/(q-2)}$ for $q > 2$ and $k > 0$, and

$\begin{bmatrix} n \\ k \end{bmatrix}_2 < 2^{(n-k)k+1} \cdot e^{2/3}$ for $q = 2$ and $k > 0$.

$\begin{bmatrix} n \\ n-2 \end{bmatrix}_q < q^{2(n-2)} \cdot \frac{q}{q-1} \frac{q^2}{q^2-1}$ for $q \geq 2$.

Proof.

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)\cdots(q^2-1)(q-1)} < q^{(n-k)k} \cdot \prod_{t=1}^{k} \frac{q^t}{q^t-1}. \tag{7.1}$$

This gives the third statement as $\begin{bmatrix} n \\ n-2 \end{bmatrix}_q = \begin{bmatrix} n \\ 2 \end{bmatrix}_q$. Suppose now $q > 2$. Recall that $\left(1+\frac{1}{i}\right)^i$ is strictly increasing, whence $\left(1+\frac{1}{(q-1)^t}\right) \leq \left(1+\frac{1}{(q-1)^k}\right)^{(q-1)^{k-t}}$ follows for $t \leq k$. Thus we have

$$\begin{bmatrix} n \\ k \end{bmatrix}_q < q^{(n-k)k} \cdot \prod_{t=1}^{k} \frac{q^t}{q^t-1} \leq q^{(n-k)k} \prod_{t=1}^{k} \left(1+\frac{1}{(q-1)^t}\right) \leq q^{(n-k)k} \left(1+\frac{1}{(q-1)^k}\right)^{\sum_{t=1}^{k}(q-1)^{k-t}}$$

$$= q^{(n-k)k}\left(1+\frac{1}{(q-1)^k}\right)^{\frac{(q-1)^k-1}{q-2}} < q^{(n-k)k}\cdot e^{1/(q-2)}.$$

For $q=2$, (7.1) gives

$$\begin{bmatrix} n \\ k \end{bmatrix}_2 < 2^{(n-k)k}\cdot\prod_{i=1}^{k}\left(1+\frac{1}{2^t-1}\right) \le 2^{(n-k)k}\cdot 2\cdot\prod_{t=0}^{k-2}\left(1+\frac{1}{3\cdot 2^t}\right) < 2^{(n-k)k+1}\cdot\left(1+\frac{1}{3\cdot 2^{k-2}}\right)^{2^{k-1}},$$

which implies $\begin{bmatrix} n \\ k \end{bmatrix}_2 < 2^{(n-k)k+1}\cdot e^{2/3}$. □

Here comes the precise deduction of Inequality (4.3). We formulate a lemma first.

Lemma 7.1.

- *If* $0 \le a < b$, *then* $\frac{\theta_a+\frac{1}{q}}{\theta_b} \le q^{a-b} < \frac{\theta_a+1}{\theta_b}$.
- *If* $0 \le a \le b-2$, *then* $\frac{\theta_a+\theta_b}{q} > 2\theta_a+1$.
- $\begin{bmatrix} k+1 \\ 2 \end{bmatrix}_q = \frac{\theta_k\theta_{k-1}}{q+1}$.

Proof. The first assertion follows from $\theta_b = \theta_a(q^{b-a})+\theta_{b-a-1}$ and $q^{b-a-1} \le \theta_{b-a-1} < q^{b-a}$. As for the second, $b \ge a+2$ yields $\theta_b \ge q^2\theta_a+q+1$, whence $\theta_a+\theta_b \ge (q^2+1)\theta_a+q+1 > 2q\theta_a+q$, as asserted. $\begin{bmatrix} k+1 \\ 2 \end{bmatrix}_q$ is the number of lines in $\mathrm{PG}(k,q)$, which space has θ_k points, each incident with θ_{k-1} lines, all of which have $q+1$ points. □

Proof of Inequality (4.3). Recall that $d \le N-2$ is the dimension of a fixed subspace Λ, and ℓ_1 is a line chosen uniform randomly.

$$\mathbb{P}(\ell_1\cap\Lambda\ne\emptyset) = \frac{\begin{bmatrix} d+1 \\ 2 \end{bmatrix}_q + \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q\cdot\frac{1}{q}\left(\begin{bmatrix} N+1 \\ 1 \end{bmatrix}_q - \begin{bmatrix} d+1 \\ 1 \end{bmatrix}_q\right)}{\begin{bmatrix} N+1 \\ 2 \end{bmatrix}_q} = \frac{\frac{\theta_d\theta_{d-1}}{q+1}+\frac{\theta_d}{q}\left(\theta_N-\theta_d\right)}{\frac{\theta_N\theta_{N-1}}{q+1}} =$$

$$= \frac{\theta_d\theta_{d-1}+\left(1+\frac{1}{q}\right)\theta_d(\theta_N-\theta_d)}{\theta_N\theta_{N-1}} = \frac{\theta_d\theta_{d-1}+\left(\theta_d+\theta_{d-1}+\frac{1}{q}\right)(\theta_N-\theta_d)}{\theta_N\theta_{N-1}} =$$

$$= \frac{\theta_d+\theta_{d-1}+\frac{1}{q}}{\theta_{N-1}} - \frac{\theta_d^2+\frac{\theta_d}{q}}{\theta_N\theta_{N-1}} = \frac{\theta_d+\frac{1}{q}+\theta_{d-1}+\frac{1}{q}}{\theta_{N-1}} - \frac{\theta_d^2+\frac{\theta_d}{q}+\frac{\theta_N}{q}}{\theta_N\theta_{N-1}} <$$

$$< \frac{\theta_d+\frac{1}{q}+\theta_{d-1}+\frac{1}{q}}{\theta_{N-1}} - \frac{\theta_d^2+2\theta_d+1}{\theta_N\theta_{N-1}} = \frac{\theta_d+\frac{1}{q}}{\theta_{N-1}} + \frac{\theta_{d-1}+\frac{1}{q}}{\theta_{N-1}} - \frac{\theta_d+1}{\theta_N}\cdot\frac{\theta_d+1}{\theta_{N-1}} <$$

$$< q^{d-N+1}+q^{d-N}-q^{2d-2N+1}.$$

□