Blocking sets, minimal codes and trifferent codes

Bishnoi, Anurag; D'haeseleer, Jozefien; Gijswijt, Dion; Potukuchi, Aditya

DOI
10.1112/jlms.12938

Publication date
2024

Document Version
Final published version

Published in
Journal of the London Mathematical Society

Received: 1 February 2023 | Revised: 6 March 2024 | Accepted: 25 April 2024

DOI: 10.1112/jlms.12938

RESEARCH ARTICLE

Journal of the London Mathematical Society

Blocking sets, minimal codes and trifferent codes

Anurag Bishnoi[1] | **Jozefien D'haeseleer**[2] | **Dion Gijswijt**[1] | **Aditya Potukuchi**[3]

[1]Delft Institute of Applied Mathematics, Technische Universiteit Delft, CD Delft, The Netherlands

[2]Department of Mathematics: Analysis, Logic and Discrete Mathematics, Ghent University, Gent, Belgium

[3]Department of Electrical Engineering and Computer Science, York University, Toronto, Ontario, Canada

Correspondence
Anurag Bishnoi, Delft Institute of Applied Mathematics, Technische Universiteit Delft, 2628 CD Delft, The Netherlands.
Email: A.Bishnoi@tudelft.nl

Funding information
FWO

Abstract

We prove new upper bounds on the smallest size of affine blocking sets, that is, sets of points in a finite affine space that intersect every affine subspace of a fixed codimension. We show an equivalence between affine blocking sets with respect to codimension-2 subspaces that are generated by taking a union of lines through the origin, and strong blocking sets in the corresponding projective space, which in turn are equivalent to minimal codes. Using this equivalence, we improve the current best upper bounds on the smallest size of a strong blocking set in finite projective spaces over fields of size at least 3. Furthermore, using coding theoretic techniques, we improve the current best lower bounds on a strong blocking set. Our main motivation for these new bounds is their application to trifferent codes, which are sets of ternary codes of length n with the property that for any three distinct codewords there is a coordinate where they all have distinct values. Over the finite field $\mathbb{F}_3$, we prove that minimal codes are equivalent to linear trifferent codes. Using this equivalence, we show that any linear trifferent code of length n has size at most $3^{n/4.55}$, improving the recent upper

bound of Pohoata and Zakharov. Moreover, we show the existence of linear trifferent codes of length n and size at least $\frac{1}{3}(9/5)^{n/4}$, thus (asymptotically) matching the best lower bound on trifferent codes. We also give explicit constructions of affine blocking sets with respect to codimension-2 subspaces that are a constant factor bigger than the best known lower bound. By restricting to $\mathbb{F}_3$, we obtain linear trifferent codes of size at least $3^{23n/312}$, improving the current best explicit construction that has size $3^{n/112}$.

MSC 2020
05D40, 51E21, 51E22, 94B05 (primary)

1 | INTRODUCTION

A classic problem in finite geometry is to study sets of points that block every subspace of a specific dimension. This problem was first introduced in 1956 by Richardson [47], who called such sets in finite projective spaces blocking coalitions. We follow the now standard terminology of blocking sets [15] and study the extremal problem of determining their minimum possible size. In combinatorial terminology, finding the smallest size of a blocking set is equivalent to determining the vertex cover number of the hypergraph that has points as its vertices and subspaces of the given dimension as its edges (see [30] for a survey on covers of hypergraphs). In this paper, our main focus is on blocking sets in finite affine spaces and strong blocking sets in finite projective spaces.

For $0 \leqslant s \leqslant k$, an s-blocking set in $\mathbb{F}_q^k$ is a set of points that contains at least one point from every *affine* subspace of dimension $k-s$. Let $b_q(k,s)$ denote the smallest possible size of an s-blocking set in $\mathbb{F}_q^k$. Jamison [37], and independently Brouwer and Schrijver [17], proved that $b_q(k,1) \geqslant (q-1)k+1$, using algebraic methods. This is a foundational result for polynomial methods in combinatorics, and it is often shown as a corollary of the well-known combinatorial nullstellensatz [6, 11], or the Alon–Füredi theorem [8, 13]. Note that the lower bound of Jamison/Brouwer–Schrijver is easily seen to be tight by taking all points on the k axes of $\mathbb{F}_q^k$. Using a geometric argument (see, for example, [11, section 3]), the lower bound on $b_q(k,1)$ implies the following,

$$b_q(k,s) \geqslant (q^s-1)(k-s+1)+1. \tag{1}$$

Unlike the $s=1$ case, there is no $s>1$ for which the bound in (1) is known to be tight (for infinitely many values of q,k). In fact, it is a major open problem to determine tight lower bounds on $b_q(k,s)$, for any $s>1$. Some special cases of this problem have been studied extensively under different names. A subset $B \subseteq \mathbb{F}_q^k$ is s-blocking if and only if the set $\mathbb{F}_q^k \setminus B$ does not contain a $(k-s)$-dimensional affine subspace. Hence, it follows from the density Hales–Jewett theorem [31] that for fixed q, d, and $k \to \infty$, $b_q(k,k-d) = q^k - o(q^k)$. In the special case $d=1$ and $q=3$, 1-blocking sets are the complements of affine caps, and thus determining $b_3(k,k-1)$ is equivalent

to the famous *cap set problem*. The upper bound on affine caps proved in the work of Ellenberg and Gijswijt [25], which also uses the polynomial method, implies $b_3(k, k-1) > 3^k - 2.756^k$. Therefore, the lower bound of $b_3(k, k-1) \geqslant 3^k - 3^{k-1} - 1$ from (1) is far from the truth. More generally, for $q = 2, 3$, we have $b_q(k, k-d) \geqslant q^k - o(c^k)$ for a constant $c < q$ depending on q and d. For $q = 2$, this is implicit in [16], and for $q = 3$, this follows from the multidimensional cap set theorem [29] (see [32] for a short proof for $q = 2, 3$). The exact asymptotics $b_2(k, k-2) = 2^k - \Theta(2^{k/2})$ follows from [50].

As far as upper bounds on $b_q(k, s)$ are concerned, the general upper bound on vertex cover numbers in terms of fractional vertex cover numbers [42] implies

$$b_q(k, s) \leqslant q^s \left(1 + \ln \begin{bmatrix} k \\ s \end{bmatrix}_q \right), \tag{2}$$

which can be upper bounded by $q^s(s(k-s)\ln q + 3)$ using the inequality $\begin{bmatrix} k \\ s \end{bmatrix}_q \leqslant e^2 q^{s(k-s)}$ (see Lemma 2.3 for more precise estimates).

In this paper, we first prove the following bound, which, for fixed q and s, improves on (2) for k large enough.

Theorem 1.1. *Let s, k be integers such that $2 \leqslant s \leqslant k$ and let q be a prime power. If $q = 2$, then*

$$b_q(k, s) \leqslant \frac{s(k-s) + s + 2}{\log_q \frac{q^s}{q^s - 1}} + 1.$$

If $q \geqslant 3$, then

$$b_q(k, s) \leqslant (q^s - 1) \cdot \frac{s(k-s) + s + 2}{\log_q \frac{q^4}{q^3 - q + 1}} + 1.$$

The bound for $q \geqslant 3$ that we prove is in fact valid for $q = 2$ as well, but it is worse than the other bound, which is why we have separated the two cases.

We then focus on a particular notion of projective blocking sets and show that it is deeply connected to affine blocking sets. A *strong t-blocking set* is a set of points in a projective space that intersects every codimension-t subspace in a set that spans the subspace. For $t = 1$, they are simply known as *strong blocking sets* [24, 36]. Recently, these objects have been shown to be equivalent to minimal codes from coding theory [4]. Minimal codewords in a linear code were first studied in 1980s for decoding purposes and then for their connection to cryptography (see [19] and the references therein). This ultimately led to the study of minimal codes: linear codes where *every* codeword is minimal. Over the binary field, minimal codes are also equivalent to linear intersecting codes [20, 22], which are codes with the property that the supports of any two codewords have nonempty intersection.

The newfound equivalence between minimal codes and strong blocking sets has immensely increased the interest in proving bounds on the smallest size of a strong blocking sets and finding explicit constructions [2, 3, 7, 12, 36]. We prove the following new equivalence between strong blocking sets and certain affine 2-blocking sets, and use it to improve the best lower and upper bounds (for $q \geqslant 3$) on the smallest size of a strong blocking set. Let $\mathrm{PG}(k-1, q)$ denote the $(k-1)$-dimensional projective space obtained from the vector space $\mathbb{F}_q^k$. The points of $\mathrm{PG}(k-1, q)$

correspond to lines passing through the origin in $\mathbb{F}_q^k$ (see Section 2 for further details). Therefore, for every set $\mathcal{L}$ of points in $\mathrm{PG}(k-1,q)$, we can construct the set $B = \cup_{\ell\in\mathcal{L}}\ell$ of points in $\mathbb{F}_q^k$. This allows us to translate the properties of $\mathcal{L}$ in the projective space to properties of the set B in the affine space.

Lemma 1.2. *Let $\mathcal{L}$ be a set of points in $\mathrm{PG}(k-1,q)$. Then, $\mathcal{L}$ is a strong $(s-1)$-blocking set if and only if the set $B = \cup_{\ell\in\mathcal{L}}\ell \subseteq \mathbb{F}_q^k$ is an affine s-blocking set.*

Let $b_q^*(k,t)$ denote the minimum size of a strong t-blocking set in $\mathrm{PG}(k-1,q)$. From this equivalence, and the upper bound on $b_q(k,2)$ given by Theorem 1.1, we derive the following upper bound on $b_q^*(k,1)$, which improves the previous best upper bound (see [36, Theorem 1.5]) of

$$b_q^*(k,1) \leqslant (q+1)\frac{2(k-1)}{1+\frac{1}{(q+1)^2\ln q}}$$

for all $q \geqslant 3$ and k sufficiently large.

Theorem 1.3. *The minimum size $b_q^*(k,1)$ of a strong blocking set $\mathrm{PG}(k-1,q)$ satisfies*

$$b_q^*(k,1) \leqslant (q+1)\frac{2k}{\log_q\left(\frac{q^4}{q^3-q+1}\right)}.$$

Using a mix of coding theoretic and geometric arguments, we then prove the following new lower bound on the size of a strong blocking set.

Theorem 1.4. *For any prime power q, there is a constant $c_q > 1$ such that every strong blocking set in $\mathrm{PG}(k-1,q)$ has size at least $(c_q - o(1))(q+1)(k-1)$, where $o(1)$ only depends on k.*

The constant c_q can be taken to be the unique solution $x \geqslant 1$ to the equation

$$M_q\left(\frac{q-1}{x(q+1)}\right) = \frac{1}{x(q+1)},$$

where M_q is the function appearing in the McEliece, Rodemich, Ramsey and Welch (MRRW) bound for linear codes (see Theorem 2.10 below). We do not have a closed formula for c_q, but for any q, it can be computed efficiently up to an arbitrary order of precision using a computer. Some estimates on c_q have been obtained in [48]. For every $q \geqslant 3$, our result improves the previous best lower bound of $(q+1)(k-1)$ [4]. For $q = 2$, our result matches the current best lower bound, which can be deduced from [38].

1.1 | Linear trifferent codes

Our study of affine 2-blocking sets and strong blocking sets is mainly motivated by a new connection to the trifference problem, which we establish in this paper. A *perfect q-hash* code of length

n is a subset C of $\{0, 1, \dots, q-1\}^n$ such that for any q distinct elements in C, there is a coordinate where they have pairwise distinct values. Understanding the largest possible size of a perfect q-hash code is a natural extremal problem that has gained much attention since the 1980s because of its connections to various topics in cryptography, information theory, and computer science [34, 40, 53, 54]. We will focus on the $q = 3$ case where these codes are also known as *trifferent codes*, and the problem of determining their largest possible size is called the *trifference problem*. Let $T(n)$ denote the largest size of a trifferent code of length n. The exact value of $T(n)$ is only known for n up to 10, where the last six values were obtained very recently via computer searches [28, 41]. Asymptotically, the upper bound

$$T(n) \leqslant 2(3/2)^n \tag{3}$$

obtained by Körner [39] in 1973 is still the best known upper bound, despite considerable effort (see, for example, [23] where it is shown that a direct application of the slice rank method will not improve the bound.) Similarly, the current best lower bound

$$T(n) \geqslant (9/5)^{n/4} \tag{4}$$

was proved by Körner and Marton [40] in 1988, who used a "probabilistic lifting" of the optimal trifferent code of length 4. A natural restriction of the trifference problem is to study *linear* trifferent codes, that is, trifferent codes C in $\mathbb{F}_3^n$ which are also vector subspaces. This restriction is motivated by the fact that the best known explicit constructions of trifferent codes are linear [53]. Moreover, the probabilistic construction of Körner and Marton [40] uses an optimal linear trifferent code in $\mathbb{F}_3^4$. Let $T_L(n)$ denote the largest size of a linear trifferent code of length n. Pohoata and Zakharov [46] have recently proven the following upper bound on $T_L(n)$, which shows a big separation from the known upper bounds on $T(n)$:

$$T_L(n) \leqslant 3^{(1/4-\epsilon)n}. \tag{5}$$

The ϵ in their result is a small positive number, not determined explicitly. We prove an equivalence between linear trifferent codes and affine 2-blocking sets in $\mathbb{F}_3^k$ that are a union of lines through the origin. By Lemma 1.2, this also implies an equivalence between strong blocking sets over $\mathbb{F}_3$ and linear trifferent codes. In fact, we show that a linear code C is trifferent if and only if it is minimal. By using our new lower bounds on strong blocking sets, we deduce the following improvement to (5) and prove a lower bound on $T_L(n)$ by using Theorem 1.3.

Theorem 1.5. *For n large enough, the largest size of linear trifferent code of length n has the following bounds:*

$$\tfrac{1}{3}(9/5)^{n/4} \leqslant T_L(n) \leqslant 3^{n/4.55}.$$

In [53], it was shown that $T_L(n) \geqslant 3^{n/112}$, via an explicit construction, whereas our bound is roughly $3^{n/7.48}$. Note that our lower bound on $T_L(n)$ is only a factor of 3 away from the best lower bound $T(n) \geqslant (9/5)^{n/4}$ given in (4). Moreover, the lower bound on $T(n)$ was obtained by constructing nonlinear trifferent codes [40], whereas we have constructed

linear trifferent codes.[†] Even a tiny further improvement will break the current best lower bounds for the trifference problem, which have not been improved since 1988. Therefore, our results give a new motivation for studying linear trifferent codes and strong blocking sets.

Our lower bounds on trifferent codes so far, which follow from our upper bounds on affine 2-blocking sets, are based on probabilistic constructions. It is of great interest to also obtain explicit constructions (see, for example, [53] and the references therein). In this direction, we first provide an explicit construction of affine 2-blocking sets whose sizes are just a constant factor away from the best lower bound (given in (1)).

Theorem 1.6. *There is an absolute constant c, such that for every prime power q, and k large enough, we can explicitly construct $c(q+1)k$ lines through the origin in $\mathbb{F}_q^k$ whose union blocks every codimension-2 affine subspace, thus implying*

$$b_q(k,2) \leqslant c(q^2-1)k+1.$$

Our construction is based on a recent breakthrough on explicit constructions of strong blocking sets [7]. By restricting to $q=3$, and using a different construction of strong blocking sets [12], we obtain a new explicit construction of linear trifferent codes, which improves the current best explicit construction of length-n linear trifferent codes from dimension $n/112$ (obtained in [53]) to dimension $n/48$. By using a linear trifferent code of dimension 6 in $\mathbb{F}_3^{24}$ and standard concatenation with algebraic geometric codes, we prove the following.

Theorem 1.7. *There exists an infinite sequence of lengths n for which there is an explicit construction of linear trifferent codes of dimension $\lceil 23n/312 \rceil$.*

1.2 | Outline of the paper

In Section 2, we describe some basic theory of finite geometry and error-correcting codes. We also recall previous results on strong blocking sets and prove Lemma 1.2. In Section 3, we prove Theorem 1.1. We use this bound for the case $s=2$, along with Lemma 1.2, to prove Theorem 1.3. In Section 4, we prove Theorem 1.4 using the MRRW bound from coding theory and lower bounds on affine blocking sets. In Section 5, we prove Theorem 1.6 using the new explicit construction of strong blocking sets. Finally, in Section 6, we focus on linear trifferent codes and prove Theorems 1.5 and 1.7. The diagram in Figure 1 summarizes all the equivalences between blocking sets, minimal codes, and trifferent codes, which form the backbone of our work.

2 | PRELIMINARIES

Throughout this paper, we will use q to denote a prime power. A projective space of dimension $k-1$ over the finite field $\mathbb{F}_q$ is defined as

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

[†] It has been pointed out to us by the referee that the idea of Körner and Marton can also be used to get a construction of linear trifferent codes that have size at least $(9/5)^{n/4}$.

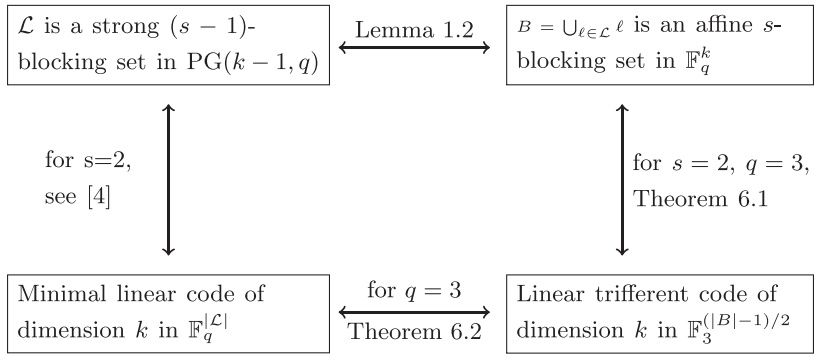

FIGURE 1 Equivalences between blocking sets and codes.

where $u \sim v$ if $u = \lambda v$ for some nonzero $\lambda \in \mathbb{F}_q$. The equivalence class that a nonzero vector v belongs to is denoted by $[v]$. The 1-dimensional, 2-dimensional, ..., $(k-1)$-dimensional vector subspaces of $\mathbb{F}_q^k$ correspond to the points, lines, ..., hyperplanes of $\mathrm{PG}(k-1,q)$. In fact, we will often identify the points of $\mathrm{PG}(k-1,q)$ with the 1-dimensional vector subspaces of $\mathbb{F}_q^k$, that is, lines of the affine space $\mathbb{F}_q^k$ that pass through the origin. Note that while the dimension of a projective subspace is one less than the dimension of its corresponding vector subspace, the codimensions remain the same. For a subset S of points in $\mathrm{PG}(k-1,q)$, the subspace formed by taking the linear span of S is denoted by $\langle S\rangle$. We refer to [18] for further details on projective spaces.

Definition 2.1 (q-binomial coefficient). For integers $0 \leqslant s \leqslant k$, the q-binomial coefficient is defined as

$$\begin{bmatrix} k \\ s \end{bmatrix}_q = \frac{(q^k-1)\cdots(q^{k-s+1}-1)}{(q^s-1)\cdots(q-1)},$$

where we define the empty product to be 1. For other values of s and k, we define $\begin{bmatrix} k \\ s \end{bmatrix}_q$ to be zero.

The number $\begin{bmatrix} k \\ s \end{bmatrix}_q$ is also known as the Gaussian coefficient. We will often use the fact that $\begin{bmatrix} k \\ s \end{bmatrix}_q = \begin{bmatrix} k \\ k-s \end{bmatrix}_q$. A straightforward double counting argument shows the following.

Lemma 2.2.

(a) *The number of* $(s-1)$*-dimensional subspaces of* $\mathrm{PG}(k-1,q)$ *is equal to* $\begin{bmatrix} k \\ s \end{bmatrix}_q$.

(b) *The number of* s*-dimensional affine subspaces of* $\mathbb{F}_q^k$ *is equal to* $q^{k-s}\begin{bmatrix} k \\ s \end{bmatrix}_q$.

We will use the following estimates on Gaussian coefficients.

Lemma 2.3. *Let* q *be a prime power and let* $1 \leqslant s \leqslant k$ *be integers.*

(a) *We have:*

$$1 \leqslant q^{-s(k-s)}\begin{bmatrix} k \\ s \end{bmatrix}_q \leqslant \frac{q}{q-1}e^{\frac{q}{(q^2-1)(q-1)}}.$$

(b) *If $s \geqslant 3$ and $k \geqslant s+3$, we have:*

$$\frac{q^3}{(q^2-1)(q-1)} \leqslant q^{-s(k-s)} \begin{bmatrix} k \\ s \end{bmatrix}_q.$$

Note that the upper bound in (a) is decreasing in q and is less than 2 for $q \geqslant 3$.

Proof. We first prove part (a). Since $\frac{q^n-1}{q^m-1} \geqslant \frac{q^n}{q^m}$ for any positive integers $n \geqslant m$, we have

$$\begin{bmatrix} k \\ s \end{bmatrix}_q = \prod_{i=0}^{s-1} \frac{q^{k-i}-1}{q^{s-i}-1} \geqslant \prod_{i=0}^{s-1} \frac{q^{k-i}}{q^{s-i}} = q^{s(k-s)}.$$

For the other inequality, we use

$$\begin{bmatrix} k \\ s \end{bmatrix}_q = \prod_{i=0}^{s-1} \frac{q^{k-i}-1}{q^{s-i}-1} \leqslant \prod_{i=0}^{s-1} \frac{q^{k-i}}{q^{s-i}-1} = q^{s(k-s)} \cdot \prod_{i=1}^{s} \frac{q^i}{q^i-1}.$$

Since

$$\prod_{i=1}^{s} \frac{q^i}{q^i-1} \leqslant \prod_{i=1}^{\infty} \frac{q^i}{q^i-1} = \frac{q}{q-1} \prod_{i=2}^{\infty} \left(1 + \frac{1}{q^i-1}\right) \leqslant \frac{q}{q-1} e^{\sum_{i=2}^{\infty} \frac{1}{q^i-1}} \leqslant \frac{q}{q-1} e^{\frac{q}{(q^2-1)(q-1)}},$$

where we used that $\sum_{i=2}^{\infty} \frac{1}{q^i-1} \leqslant \sum_{i=2}^{\infty} \frac{1}{q^i-q^{i-2}} = \frac{1}{q^2-1}\frac{q}{q-1}$, the inequality follows for all prime powers q.

For part (b), it can be easily verified that

$$\frac{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)}{q^3-1} \geqslant \frac{q^k q^{k-1} q^{k-2}}{q^3}$$

since $k \geqslant 6$. It follows that

$$\begin{aligned} \begin{bmatrix} k \\ s \end{bmatrix}_q &= \frac{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)}{(q^3-1)(q^2-1)(q-1)} \cdot \frac{q^{k-3}-1}{q^s-1} \cdots \frac{q^{k-s+1}-1}{q^4-1} \\ &\geqslant \frac{q^3}{(q^2-1)(q-1)} q^{3k-9} \cdot q^{(k-s-3)(s-3)} \\ &= \frac{q^3}{(q^2-1)(q-1)} q^{(k-s)s}, \end{aligned}$$

where in the inequality, we used $k-3 \geqslant s$. □

Lemma 2.4. *Let H be an affine hyperplane in $\mathbb{F}_q^k$ that does not pass through the origin. The number of i-dimensional affine subspaces disjoint from H and passing through the origin is equal to $\begin{bmatrix} k-1 \\ i \end{bmatrix}_q$.*

Proof. Any such subspace must be contained in the unique hyperplane parallel to H that passes through the origin, and by Lemma 2.2 the number of i-dimensional vector subspaces of a $(k-1)$-dimensional vector space is equal to $\begin{bmatrix} k-1 \\ i \end{bmatrix}_q$. □

Definition 2.5. Let H be a $(k-s)$-dimensional affine subspace of $\mathbb{F}_q^k$, not passing through origin. We denote by $n_q(k,s)$ the number of s-dimensional affine subspaces through the origin that are disjoint from H.

Note that $n_q(k,s)$ is independent of the particular choice of H since the general linear group acts transitively on $(k-s)$-dimensional not passing through the origin. A formula is given by the following lemma.

Lemma 2.6. *We have*

$$n_q(k,s) = \sum_{i=1}^{s} q^{(s-i)(k-i-s+1)} \begin{bmatrix} s-1 \\ i-1 \end{bmatrix}_q \begin{bmatrix} k-s \\ i \end{bmatrix}_q.$$

Proof. Let H be a $(k-s)$-dimensional affine subspace of $\mathbb{F}_q^k$ not passing through origin and let H' be the $(k-s+1)$-dimensional subspace spanned by H and the origin. For $1 \leqslant i \leqslant s$, let $\mathcal{S}_i$ denote the set of s-dimensional subspaces through the origin, disjoint from H, that intersect H' in an i-dimensional subspace. As $\mathcal{S}_1 \cup \cdots \cup \mathcal{S}_s$ is a partition of the set of subspaces that we need to count, we have $n_q(k,s) = \sum_{i=1}^{s} |\mathcal{S}_i|$. Therefore, it suffices to show $|\mathcal{S}_i| = q^{(s-i)(k-i-s+1)} \begin{bmatrix} s-1 \\ i-1 \end{bmatrix}_q \begin{bmatrix} k-s \\ i \end{bmatrix}_q$. The number of ways of picking an i-dimensional subspace in H' that is disjoint from H is equal to $\begin{bmatrix} k-s \\ i \end{bmatrix}_q$ by Lemma 2.4. Once we have picked such a subspace T, the number of ways of picking an s-dimensional subspace S such that $S \cap H' = T$ amounts to picking $s-i$ remaining basis vectors outside H', which gives us exactly

$$\frac{(q^k - q^{k-s+1}) \cdots (q^k - q^{k-i})}{(q^s - q^i) \cdots (q^s - q^{s-1})} = q^{(s-i)(k-i-s+1)} \begin{bmatrix} s-1 \\ i-1 \end{bmatrix}_q$$

choices for S. □

2.1 | Error-correcting codes

We now recall some definitions and results from coding theory (see [35] for a standard reference).

Definition 2.7. The support of a vector $v \in \mathbb{F}_q^n$ is the set

$$\operatorname{supp}(v) := \{i \ : \ v_i \neq 0\} \subseteq [n].$$

The Hamming weight of v is

$$\operatorname{wt}(v) := |\operatorname{supp}(v)|.$$

The Hamming weight induces a metric on $\mathbb{F}_q^n$, given by $d(u,v) := \mathrm{wt}(u-v)$, which is known as the *Hamming distance*.

Definition 2.8. An $[n,k,d]_q$ code C is a k-dimensional subspace of $\mathbb{F}_q^n$, with *minimum distance*

$$d := \min\{\mathrm{wt}(v) \ : \ v \in C \setminus \{\vec{0}\}\}.$$

The elements of C are called *codewords*. A *generator matrix* for C is a matrix $G \in \mathbb{F}_q^{k\times n}$ such that

$$C = \{uG \ : \ u \in \mathbb{F}_q^k\}.$$

The rate of C is equal to k/n and the relative Hamming distance of C is equal to d/n.

Definition 2.9. Let $\{n_i\}_{i\geqslant 1}$ be an increasing sequence of lengths and suppose that there exist sequences $\{k_i\}_{i\geqslant 1}$ and $\{d_i\}_{i\geqslant 1}$ such that for all $i \geqslant 1$, there exists an $[n_i,k_i,d_i]_q$ code C_i. Then, the sequence $\mathcal{C} = \{C_i\}_{i\geqslant 1}$ is called a family of codes. The rate of $\mathcal{C}$ is defined as

$$R(\mathcal{C}) = \lim_{i\to\infty} \frac{k_i}{n_i},$$

and the relative distance of $\mathcal{C}$ is defined as

$$\delta(\mathcal{C}) = \lim_{i\to\infty} \frac{d_i}{n_i},$$

assuming that these limits exist.

A family $\mathcal{C}$ for which $R(\mathcal{C}) > 0$ and $\delta(\mathcal{C}) > 0$, is known as an *asymptotically good code*, and various explicit constructions of such codes are known [35, 52]. However, the problem of understanding the optimal trade-off between the rate and relative distance of a family of codes is in general not well understood. As a result, the following open question lies at the heart of the subject:

> What is the *largest* rate that can be achieved for a family of codes of a given relative distance δ?

For our purposes, we will focus on upper bounds on the rate. To continue, let us define the following two functions. The q-ary entropy is defined by:

$$\mathrm{H}_q(x) := x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x).$$

Define

$$M_q(\delta) := \mathrm{H}_q\left(\frac{1}{q}\left(q-1-(q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)}\right)\right).$$

A relevant property of M_q is that it provides an asymptotic upper bound on the rate of any code with a given relative distance.

Theorem 2.10 (MRRW bound for q-ary codes [1, 44]). *For any fixed alphabet size q, and relative distance $\delta > 0$, any family of q-ary codes with relative distance δ and rate R satisfies*

$$R \leqslant M_q(\delta).$$

One may verify that M_q is a continuous and strictly decreasing function in the domain $[0, 1 - 1/q]$, satisfying $M_q(0) = 1$ and $M_q(1 - 1/q) = 0$, which can be used to show that the constant c_q appearing in Theorem 1.4 is well defined. Note that c_q is also equal to the maximum x for which $M_q((q-1)/(x(q+1))) \leqslant 1/(x(q+1))$ and $x \geqslant 1$ (see Appendix A for further details).

2.2 | Strong blocking sets

Definition 2.11. Let C be an $[n, k, d]_q$ code. A nonzero codeword $v \in C$ is said to be *minimal* if $\mathrm{supp}(v)$ is minimal with respect to inclusion in the set

$$\{\mathrm{supp}(c) \ : \ u \in C \setminus \{\vec{0}\}\}.$$

The code C is a *minimal (linear) code* if all its nonzero codewords are minimal.

So a linear code is minimal if for all $u, v \in C$, we have: $\mathrm{supp}(u) \subsetneq \mathrm{supp}(v) \Rightarrow u = 0$.

Definition 2.12. A set S of points in a projective space is called a strong blocking set if for every hyperplane H, we have $\langle S \cap H \rangle = H$.

These special kinds of (projective) blocking sets have been studied under the names of generator sets [26] and cutting blocking sets [4], but we adopt the terminology of strong blocking sets used in the earliest work [24].

Definition 2.13. An $[n, k, d]_q$ code C is nondegenerate if there is no coordinate where every codeword has 0 entry.

The following is a standard equivalence between nondegenerate codes and certain sets of points in the projective space (see, for example, [52, Theorem 1.1.6]).

Lemma 2.14. *Let C be a nondegenerate $[n, k, d]_q$ code and let $G = (g_1 \mid \ldots \mid g_n) \in \mathbb{F}_q^{k \times n}$ be any of its generator matrices. Let $\mathcal{P} = \{[g_1], \ldots, [g_n]\}$ be the (multi)set of points in $\mathrm{PG}(k-1, q)$ given by G. Then,*

$$d = n - \max_H \{|\{i \ : \ [g_i] \in H\}|\},$$

where the maximum is taken over all hyperplanes H. Conversely for $d > 0$, any set of n points in $\mathrm{PG}(k-1, q)$ whose maximum intersection with a hyperplane has size $n - d$ gives rise to a

nondegenerate $[n, k, d]_q$ *code by taking a generator matrix whose columns are the coordinates of these n points.*

In particular, Lemma 2.14 implies that if a set of n points in $\mathrm{PG}(k-1, q)$ meets every hyperplane in at most m points, then there exists an $[n, k, n-m]_q$ code.

Under this correspondence, minimality of an $[n, k, d]_q$ code has been shown to be equivalent to the corresponding point set giving rise to a strong blocking set in $\mathrm{PG}(k-1, q)$.

Theorem 2.15 (see [4, 51]). *Let C be a nondegenerate $[n, k, d]_q$ code and let $G = (g_1 \mid \ldots \mid g_n) \in \mathbb{F}_q^{k\times n}$ be any of its generator matrices. The following are equivalent:*

(i) *C is a minimal code.*
(ii) *The set $\{[g_1], \ldots, [g_n]\}$ is a strong blocking set in* $\mathrm{PG}(k-1, q)$.

Remark 2.16. Note that the Hamming distance d plays no role in the definition of minimal codes. However, it can be shown that if an $[n, k, d]_q$ code is minimal, then $d \geqslant (q-1)(k-1)+1$ (see [4, Theorem 2.8]). This implies that any minimal $[n, k, d]_q$ code where k is a linear function of n is asymptotically good, which is another motivation for studying these codes.

The main problem is to find small strong blocking sets in $\mathrm{PG}(k-1, q)$, which is then equivalent to finding short minimal codes of dimension k. The following is the best lower bound on the size of a strong blocking set, for all $q \geqslant 3$, and it was proved using the polynomial method.

Theorem 2.17 (see [4, Theorem 2.14]). *Let $S \subseteq \mathrm{PG}(k-1, q)$ be a strong blocking set. Then*

$$|S| \geqslant (q+1)(k-1).$$

Remark 2.18. This is in general not tight. For $q = 2$, a better bound follows from [38] and Lemma 1.2 and for $k = 3$, a better lower bound follows from [10] as than a strong blocking set equivalent to a 2-fold blocking set.

The following is the best upper bound on the smallest size of a strong blocking set.

Theorem 2.19 (see [36]). *The smallest size of a strong blocking set in* $\mathrm{PG}(k-1, q)$ *is at most*

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

Remark 2.20. For $q = 2$, this bound already appears in [45], where it is attributed to Komlós.

We now prove the new characterization of strong blocking sets based on affine blocking sets, outlined in Lemma 1.2. First, we define a generalization of strong blocking sets, which also appears in [27, Definition 2] under the name of generator sets.

Definition 2.21. A set of points in PG$(k-1,q)$ is called a strong t-blocking set if it intersects every codimension-t subspace in a set of points that spans the subspace.

Proof of Lemma 1.2. First assume that $\mathcal{L}$ is a strong $(s-1)$-blocking set in PG $(k-1,q)$. Let $V \subseteq \mathbb{F}_q^k$ be a codimension-s vector subspace and let $u \in \mathbb{F}_q^k \setminus V$. It suffices to show $B \cap (V+u) \neq \emptyset$. Let $W = \langle V, u\rangle = \cup_{\lambda \in \mathbb{F}_q}(V+\lambda u)$ be the codimension-$(s-1)$ vector subspace spanned by $V \cup \{u\}$. Then, W meets $\mathcal{L}$ in a spanning set. In particular, there exists an element $b \in B$ such that $b \in W \setminus V$. Thus, we can write $b = v + \lambda u$ for some $v \in V$ and $\lambda \neq 0$. Then, $b' = \lambda^{-1}b$ is contained in B as B is closed under taking scalar multiples, and b' is contained in $V+u$ as $b' = \lambda^{-1}v + u$ and $\lambda^{-1}v \in V$.

Now assume that B blocks all codimension-s affine subspaces. Say $\mathcal{L}$ is not a strong $(s-1)$-blocking set. Then, there is some codimension-$(s-1)$ vector subspace V such that $\mathcal{L} \cap V$ is contained inside a codimension-s vector subspace V' of V. Then, the set B does not block any affine codimension-s subspace contained in $V \setminus V'$ that is parallel to V'. □

Remark 2.22. By combining Lemma 1.2 and (1), we get a new proof of the lower bound on strong blocking sets given in Theorem 2.17 (see [36] for another proof that uses (1)).

3 | UPPER BOUNDS ON BLOCKING SETS

In this section, we give a probabilistic construction of s-blockings sets in $\mathbb{F}_q^k$, thus obtaining an upper bound on $b_q(k,s)$. For $q=2$, we simply pick random points and show that if the number of points is large enough, then the probability that they form an s-blocking set is positive. Our novel idea for $q \geqslant 3$ is to randomly pick s-dimensional linear subspaces instead. We start with a preliminary lemma that estimates $n_q(k,s)$ as defined in Definition 2.5

Lemma 3.1. *Let q be a prime power. Let $2 \leqslant s \leqslant k$ be integers. We have the following estimate on $n_q(k,s)$.*

$$n_q(k,s) \leqslant \frac{q^3-q+1}{q^4}\begin{bmatrix}k\\ s\end{bmatrix}_q.$$

Proof. We will split the proof into three cases: $s=2$; $s \geqslant 3, k \geqslant s+3$; $s \geqslant 3, s \leqslant k \leqslant s+2$. Case $s=2$. We use Lemma 2.6 and write out the given expression for $s=2$. We obtain

$$\begin{aligned}\frac{n_q(k,2)}{\begin{bmatrix}k\\ 2\end{bmatrix}_q} &= \frac{\begin{bmatrix}1\\ 0\end{bmatrix}_q\begin{bmatrix}k-2\\ 1\end{bmatrix}_q q^{k-2} + \begin{bmatrix}1\\ 1\end{bmatrix}_q\begin{bmatrix}k-2\\ 2\end{bmatrix}_q}{\begin{bmatrix}k\\ 2\end{bmatrix}_q}\\ &\leqslant \frac{(q^{k-2}-1)(q^k-q^{k-2}+q^{k-3}-1)}{(q^k-1)(q^{k-1}-1)}\\ &\leqslant \frac{1}{q}\frac{q^k-q^{k-2}+q^{k-3}-1}{(q^k-1)}\end{aligned}$$

$$= \frac{1}{q}\left(1 - \frac{q^{k-2} - q^{k-3}}{q^k - 1}\right)$$
$$\leqslant \frac{1}{q}(1 - q^{-2} + q^{-3})$$
$$= \frac{q^3 - q + 1}{q^4}.$$

The inequality in the second line is an equality if $k - 2 \geqslant 2$.

Case $s \geqslant 3$ and $k \geqslant s + 3$. We will use the q-Vandermonde identity (see [49], solution of exercise 1.100):

$$\begin{bmatrix} m+n \\ \ell \end{bmatrix}_q = \sum_j \begin{bmatrix} n \\ j \end{bmatrix}_q \begin{bmatrix} m \\ \ell - j \end{bmatrix}_q q^{(m-\ell+j)j}.$$

Substituting $\ell = s$, $m = k - s$, $n = s - 1$, and $j = s - i$, we obtain

$$\begin{bmatrix} k-1 \\ s \end{bmatrix}_q = \sum_{i=1}^{s} \begin{bmatrix} s-1 \\ s-i \end{bmatrix}_q \begin{bmatrix} k-s \\ i \end{bmatrix}_q q^{(k-s-i)(s-i)}, \tag{6}$$

which is the form we will use.

Using again Lemma 2.6, we obtain

$$n_q(k,s) = \sum_{i=1}^{s} \begin{bmatrix} s-1 \\ i-1 \end{bmatrix}_q \begin{bmatrix} k-s \\ i \end{bmatrix}_q q^{(s-i)(k-i-s+1)}$$
$$= \sum_{i=1}^{s} \begin{bmatrix} s-1 \\ s-i \end{bmatrix}_q \begin{bmatrix} k-s \\ i \end{bmatrix}_q q^{(k-s-i)(s-i)} q^{s-i}$$
$$\leqslant (q^{s-1} - q^{s-2}) \begin{bmatrix} k-s \\ 1 \end{bmatrix}_q q^{(k-s-1)(s-1)} + q^{s-2}\left(\sum_{i=1}^{s} \begin{bmatrix} s-1 \\ s-i \end{bmatrix}_q \begin{bmatrix} k-s \\ i \end{bmatrix}_q q^{(k-s-i)(s-i)}\right).$$

The first summand can be upper bounded by

$$(q^{s-1} - q^{s-2}) \begin{bmatrix} k-s \\ 1 \end{bmatrix}_q q^{(k-s-1)(s-1)} \leqslant \frac{q^{(k-s)s}}{q} \leqslant \frac{(q^2-1)(q-1)}{q^4} \begin{bmatrix} k \\ s \end{bmatrix}_q,$$

where we used Lemma 2.3(b) in the second inequality.

The second summand can be upper bounded using the q-Vandermonde identity (6):

$$q^{s-2}\left(\sum_{i=1}^{s} \begin{bmatrix} s-1 \\ s-i \end{bmatrix}_q \begin{bmatrix} k-s \\ i \end{bmatrix}_q q^{(k-s-i)(s-i)}\right) = q^{s-2} \begin{bmatrix} k-1 \\ s \end{bmatrix}_q \leqslant \frac{1}{q^2} \begin{bmatrix} k \\ s \end{bmatrix}_q.$$

The result now follows from combining the two bounds and the fact that $\frac{(q^2-1)(q-1)}{q^4} + \frac{1}{q^2} = \frac{q^3-q+1}{q^4}$.

Case $s \geqslant 3$ and $s \leqslant k \leqslant s + 2$. If $k = s$, we have $n_q(k,s) = 0 \leqslant \frac{q^3-q+1}{q^4} \begin{bmatrix} s \\ s \end{bmatrix}_q$ as required.

If $k = s + 1$, then by Lemma 2.6, we have $n_q(k, s) = q^{s-1}$ and

$$\frac{q^3 - q + 1}{q^4} \begin{bmatrix} k \\ s \end{bmatrix}_q = \frac{q^{s+4} - q^{s+2} + q^{s+1} - q^3 + q - 1}{(q-1)q^4}.$$

We leave it to the reader to verify that indeed $q^{s-1}(q-1)q^4 \leqslant q^{s+4} - q^{s+2} + q^{s+1} - q^3 + q - 1$.

Finally, suppose $k = s + 2$. We have

$$n_q(k, s) = q^{2(s-1)} \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q + q^{s-2} \begin{bmatrix} s-1 \\ 1 \end{bmatrix}_q = \frac{q^{2s} - q^{2s-2} + q^{2s-3} - q^{s-2}}{q-1} \leqslant \frac{q^3 - q + 1}{q-1} q^{2s-3}.$$

On the other hand, using that $(q^{s+2} - 1)(q^{s+1} - 1)q^2 \geqslant q^{s+2}q^{s+1}(q^2 - 1)$, we have

$$\begin{bmatrix} k \\ s \end{bmatrix}_q = \frac{(q^{s+2} - 1)(q^{s+1} - 1)}{(q^2 - 1)(q - 1)} \geqslant \frac{q^{2s+1}}{q-1}.$$

Combining the two inequalities, we obtain $\begin{bmatrix} k \\ s \end{bmatrix}_q \frac{q^3-q+1}{q^4} \geqslant n_q(k, s)$. □

Proof of Theorem 1.1. First let $q = 2$. Let $P_1, \ldots, P_m$ be points in $\mathbb{F}_2^k$ chosen uniformly at random independently from each other. Let H be a codimension-s affine subspace. The probability that H does not contain any $P_1, \ldots, P_m$ is equal to $(1 - 2^{-s})^m$. Since there are in total $2^s \begin{bmatrix} k \\ k-s \end{bmatrix}_2 = 2^s \begin{bmatrix} k \\ s \end{bmatrix}_2$ choices for H, the probability that $B = \{P_1, \ldots, P_m\}$ is not an s-blocking set is at most

$$\left(\frac{2^s - 1}{2^s}\right)^m \cdot 2^s \begin{bmatrix} k \\ s \end{bmatrix}_2.$$

By Lemma 2.3, this probability is upper bounded by

$$\left(\frac{2^s - 1}{2^s}\right)^m 2^{s(k-s)+s+1} e^{2/3} < 2^{-m \log_2 \left(\frac{2^s}{2^s-1}\right) + s(k-s)+s+2}.$$

It follows that the probability is less than 1 for $m \geqslant \frac{s(k-s)+s+2}{\log_2 \frac{2^s}{2^s-1}}$, proving that there exists a collection of $\lceil \frac{s(k-s)+s+2}{\log_2 \frac{2^s}{2^s-1}} \rceil$ points blocking all codimension-s affine subspaces in $\mathbb{F}_2^k$.

We now consider the case $q \geqslant 3$. Let

$$m \geqslant -1 + \frac{s(k-s) + s + 2}{\log_q \left(\frac{q^4}{q^3-q+1}\right)}$$

be an integer and let $\pi_1, \ldots, \pi_m$ be s-dimensional spaces through the origin chosen uniformly at random, and independently from each other.

For any codim-s affine subspace H that does not pass through the origin, the probability that $\pi_1, \ldots, \pi_m$ are disjoint from H is at most $\left(\frac{q^3-q+1}{q^4}\right)^m$ by Lemma 3.1. The number of such H equals $(q^s - 1)\begin{bmatrix} k \\ s \end{bmatrix}_q$. Hence, the expected number of H that are disjoint from $\pi_1, \ldots, \pi_m$ is at most

$$\left(\frac{q^3 - q + 1}{q^4}\right)^m \cdot (q^s - 1) \begin{bmatrix} k \\ s \end{bmatrix}_q \leqslant \frac{q^4}{q^3 - q + 1} \cdot q^{-s(k-s)-s-2}(q^s - 1) \begin{bmatrix} k \\ s \end{bmatrix}_q$$

$$\begin{aligned} &< \frac{2q^4}{q^3-q+1} \cdot q^{-2} \\ &\leqslant \frac{2q^2}{q^3-q+1} \\ &\leqslant 1. \end{aligned}$$

Here, we used $\begin{bmatrix} k \\ s \end{bmatrix}_q \leqslant 2q^{s(k-s)}$, see Lemma 2.3(a).

So there is an instance where $B = \pi_1 \cup \cdots \cup \pi_m$ is a s-blocking set. By taking m as small as possible, we have $m \leqslant (s(k-s)+s+2) / \log_q \left(\frac{q^4}{q^3-q+1}\right)$, so we obtain

$$b_q(k,s) \leqslant (q^s-1)\frac{s(k-s)+s+2}{\log_q \left(\frac{q^4}{q^3-q+1}\right)} + 1$$

as required. □

Remark 3.2. For a fixed s, picking random points instead of picking random s-dimensional subspaces through the origin gives the upper bound of $\sim (q^s \ln q)s(k-s)$, which is worse for every $q \geqslant 3$, since $\ln q > 1$ for $q > e$. It can also be shown that picking i-dimensional subspaces, for any $i < s$, gives us worse bounds for $q \geqslant 3$.

Proof of Theorem 1.3. Let $s = 2$ and $q \geqslant 3$. In the proof of Theorem 1.1 above, we have a random collection of planes through the origin whose union blocks every codimension-2 affine subspace in $\mathbb{F}_q^k$. Each plane consists of $q+1$ lines through the origin, which implies that we have a set of at most $(q+1)2k/\log_q \left(\frac{q^4}{q^3-q+1}\right)$ lines through the origin in $\mathbb{F}_q^k$ whose union blocks every codimension-2 affine subspace. By Lemma 1.2, this collection of lines corresponds to a strong blocking set in $\mathrm{PG}(k-1,q)$ of the same size. □

Remark 3.3. Our upper bound improves the previous best upper bound on strong blocking sets (see Theorem 2.19) for all $q \geqslant 3$. Independent of our work, Alfarano, Borello, and Neri have obtained the same upper bound in [3] using different techniques. We have also been informed by the authors of [36] that a more careful analysis of their argument implies our upper bound.

Remark 3.4. Our upper bound on affine s-blocking sets also implies that for $2 \leqslant s \leqslant k$, the smallest size of a strong $(s-1)$-blocking set in $\mathrm{PG}(k-1,q)$, for $q \geqslant 3$, is at most

$$\frac{q^s-1}{q-1} \cdot \frac{s(k-s)+s+2}{\log_q \left(\frac{q^4}{q^3-q+1}\right)}.$$

4 | LOWER BOUNDS ON STRONG BLOCKING SETS

In this section, we prove Theorem 1.4. Let q be a prime power.

Lemma 4.1. *Let k be a positive integer. Then, there is a $[b_q^*(k,1), k, (q-1)(k-1)+1]_q$ code.*

Proof. Let $\{[g_1], \dots, [g_n]\} \subseteq \mathrm{PG}(k-1,q)$ be a strong blocking set of size $n := b_q^*(k,1)$ and let C be the nondegenerate code with generator matrix $G = (g_1 \mid \dots \mid g_n)$. By Theorem 2.15, C is a minimal code, which has minimum distance $d \geqslant (q-1)(k-1)+1$ by Remark 2.16. □

Proof of Theorem 1.4. Recall that c_q is the unique solution $x \geqslant 1$ to $M_q\left(\frac{q-1}{x(q+1)}\right) = \frac{1}{x(q+1)}$. In Appendix A, we show that c_q is well defined and that $c_q > 1$. Let c be a constant such that $1 < c < c_q$. We will show $b_q^*(k,1) \geqslant c(q+1)(k-1)$ for k large enough.

Set $R = \frac{1}{c(q+1)}$ and $\delta = \frac{q-1}{c(q+1)}$. Note that $\delta < 1 - \frac{1}{q}$. Since $c < c_q$ and M_q is strictly decreasing on $[0, 1-1/q]$, we have $M_q(\delta) < R$. By the MRRW bound for q-ary codes, Theorem 2.10, there is an integer k_0 such that for all $k \geqslant k_0$, there is no linear code $C \subseteq \mathbb{F}_q^n$ with rate at least R and relative minimum distance at least δ.

Now let $k \geqslant k_0$. By Lemma 4.1, there is a code C of block length $n = b_q^*(k,1)$, dimension k, and minimum distance $d \geqslant (q-1)(k-1)+1$. It follows that $b_q^*(k,1) \geqslant c(q+1)(k-1)$ since otherwise the code C has rate $\frac{k}{n} > \frac{1}{c(q+1)} = R$ and relative distance

$$\frac{d}{n} > \frac{(q-1)(k-1)+1}{c(q+1)(k-1)} > \delta.$$

This concludes the proof. □

Remark 4.2. From Lemma 1.2 and (1), it follows that every strong $(s-1)$-blocking set in $\mathrm{PG}(k-1,q)$ has size at least $\frac{q^s-1}{q-1}(k-s+1)$. Using an inductive argument, we can also improve this lower bound by a constant factor, for every fixed q, s, and large k.

5 | EXPLICIT CONSTRUCTIONS

In Section 3, we constructed s-blocking sets by picking random s-dimensional subspaces through the origin in $\mathbb{F}_q^k$. However, for explicit constructions, we will pick 1-dimensional subspaces as then we can use the connection to strong $(s-1)$-blocking sets in PG $(k-1,q)$ outlined in Lemma 1.2. If the strong $(s-1)$-blocking set has size m, then the corresponding affine s-blocking set has size $(q-1)m+1$. For example, if $q > s(k-s)$, there exists an explicit construction of strong $(s-1)$-blocking sets of size at most $(s(k-s)+1)(q^s-1)/(q-1)$ in $\mathrm{PG}(k-1,q)$ [27, 33], which we can use to give an explicit construction of affine s-blocking sets of size at most $(q^s-1)s(k-s)+q^s$. While this is a good explicit construction, it requires the field to be large with respect to k and s. We will focus on fixed q, s, and large k.

The main focus of explicit constructions has been on the special case of strong 1-blocking sets, as these objects are equivalent to minimal codes [4]. An easy construction, known as the "tetrahedron," is as follows. Take the union of all lines joining pairs of k points in general position to get a strong blocking set of size $\binom{k}{2}(q-1)+k$ in $\mathrm{PG}(k-1,q)$, and thus an affine 2-blocking set of size $\binom{k}{2}(q-1)^2 + k(q-1)+1$ in $\mathbb{F}_q^k$. Note that the dependency on the dimension k is quadratic in this construction. For $q=2$, minimal codes are equivalent to intersecting codes, and thus we already have explicit constructions of strong blocking sets in $\mathbb{F}_2^k$ of size linear in k [22]. Recently, an explicit construction of a strong blocking set of size linear in the dimension, for any fixed $q \geqslant 3$, was obtained by Bartoli and Borello [12, Corollary 3.3]. The same construction also appears in an earlier work of Cohen, Mesnager, and Randriam [21], and the main idea is to concatenate algebraic

geometric codes with the simplex code. They proved that for every prime power q, there exists an infinite sequence of k's such that there is an explicit construction of a strong blocking set in the projective space $\mathrm{PG}(k-1,q)$ of size $\sim q^4k/4$. The problem of giving an explicit construction, which also has a linear dependence on q, has recently been solved in [7].

Theorem 5.1 (Alon, Bishnoi, Das, Neri 2023). *There is an absolute constant c such that for every prime power q and k large enough, there is an explicit construction of strong blocking sets in* $\mathrm{PG}(k-1,q)$ *of size at most $c(q+1)k$.*

Proof of Theorem 1.6. Let S be an explicitly constructed strong blocking set of size at most $c(q+1)k$ in $\mathrm{PG}(k-1,q)$. By Lemma 1.2, the union of lines in $\mathbb{F}_q^k$ corresponding to the points of S gives us an explicit construction of an affine-2 blocking set in $\mathbb{F}_q^k$ of size $(q-1)c(q+1)k+1 = c(q^2-1)k+1$. □

For the sake of completeness, we give a sketch of the construction in [7].

Lemma 5.2. *Let $\mathcal{M}=\{P_1,\dots,P_n\}$ be a set of points in* $\mathrm{PG}(k-1,q)$ *and let $G=(\mathcal{M},E)$ be a graph on these points. If for every $S\subseteq\mathcal{M}$, there exists a connected component C in $G-S$ such that*

$$\langle S\cup C\rangle = \mathrm{PG}(k-1,q),$$

then the set

$$\bigcup_{P_iP_j\in E}\langle P_i,P_j\rangle$$

is a strong blocking set.

For a graph G, its vertex integrity [9] is defined as

$$\iota(G)=\min_{S\subseteq V(G)}(|S|+\kappa(G-S)),$$

where $\kappa(G-S)$ denotes the size of the largest connected component of the graph obtained by deleting the set S of vertices from G. Graphs with high vertex integrity along with points in $\mathrm{PG}(k-1,q)$ that have low intersection with every hyperplane give rise to the construction that we want.

Corollary 5.3. *Let $\mathcal{P}=\{P_1,\dots,P_n\}$ be a set of points in* $\mathrm{PG}(k-1,q)$ *such that every hyperplane meets $\mathcal{P}$ in at most $n-d$ points and let G be a graph on $\mathcal{P}$ with $\iota(G)\geqslant n-d+1$. Then the set*

$$\bigcup_{P_iP_j\in E}\langle P_i,P_j\rangle$$

is a strong blocking set.

A set of n points in $\mathrm{PG}(k-1,q)$ that meets every hyperplane in at most $n-d$ points is equivalent to a (nondegenerate) $[n,k,d]_q$ code (see Lemma 2.14). Therefore, if we pick our set $\mathcal{P}$ corresponding to an asymptotically good linear code and our graph G to be a bounded degree graph with $\iota(G)\geqslant n-d+1$, then we can get a construction where for any fixed q the size of the strong blocking set is linear in qk.

Corollary 5.4. *Say there exists a family of codes C with lengths $\{n_i\}_{i\geqslant 1}$, rate R, and relative distance δ, and a family of graphs G_i on n_i vertices with maximum degree Δ and $\iota(G_i) > (1-\delta)n_i$. Then, there exists strong blocking sets of size $\Delta n_i/2$ in $\mathrm{PG}(Rn_i - 1, q)$, for al $i \geqslant 1$.*

It is shown in [7] that constant degree expander graphs G on n vertices have the property $\iota(G) = \Omega(n)$. The explicit constructions of these graphs [43] and asymptotically good linear codes [52] thus imply Theorem 5.1, and we refer to [7] for the best values of the constant c obtained from this construction.

6 | LINEAR TRIFFERENT CODES

Recall that a linear subspace C of $\mathbb{F}_3^n$ is called a *linear trifferent code* if for all distinct $x, y, z \in C$ there exists a coordinate i such that $\{x_i, y_i, z_i\} = \mathbb{F}_3$. The maximum size of a linear trifferent code is denoted by $T_L(n)$.

We say that an (affine) 2-blocking set $S \subseteq \mathbb{F}_3^k$ is *symmetric* if it is of the form $S = \{\vec{0}\} \cup B \cup -B$ for some set $B \subseteq \mathbb{F}_3^k$. So by Lemma 1.2, a set $S \subseteq \mathbb{F}_3^k$ is a symmetric 2-blocking set if and only if it is of the form $S = \cup_{\ell\in\mathcal{L}}\ell$ for a strong blocking set $\mathcal{L} \subseteq \mathrm{PG}(k-1, 3)$.

In [46], it was shown that a linear trifferent code of dimension k in $\mathbb{F}_3^n$ gives rise to a symmetric 2-blocking set in $\mathbb{F}_3^k$. We prove that this relation goes both ways.

Theorem 6.1. *Let $G \in \mathbb{F}_3^{k\times n}$ be a matrix of rank k. Let B be the set of columns of G and let C be the row-space of G. Then, C is a linear trifferent code in $\mathbb{F}_3^n$ if and only if $\{\vec{0}\} \cup B \cup -B$ is a 2-blocking set in $\mathbb{F}_3^k$.*

Proof. We first note that every $x \in C$ is of the form $x = u^\top G$ for a unique $u \in \mathbb{F}_3^k$ (as G has rank k) and the i-th coordinate of x is equal to $u^\top b$, where b is the i-th column of G.

For the forward implication, suppose $\{\vec{0}\} \cup B \cup -B$ is a 2-blocking set. Since C is a linear subspace, we only need to show the trifferent property for triples of distinct vectors $\vec{0}, c, c' \in C$. Writing $c = u^\top G$ and $c' = v^\top G$, it suffices to show that there is a column b of G such that $\{u^\top b, v^\top v\} = \{-1, 1\}$. Since u and v are distinct and nonzero, the set $S = \{x \in \mathbb{F}_3^m : u^\top x = 1, v^\top x = -1\}$ contains an affine subspace of codimension 2. Since $\{\vec{0}\} \cup B \cup -B$ is a 2-blocking set, it must intersect S. Hence, since S does not contain the zero vector, it contains a vector $x \in B \cup -B$. If $x \in B$, we can take $b = x$ and otherwise we can take $b = -x$.

For the backward implication, suppose that C is a trifferent code. Let $V \subseteq \mathbb{F}_3^k$ be an affine subspace of codimension 2 with $0 \notin V$. It suffices to show that there is a $b \in B$ with $b \in V$ or $-b \in V$. We can write $V = \{x \in \mathbb{F}_3^k : u^\top x = 1, v^\top x = -1\}$ for certain linearly independent $u, v \in \mathbb{F}_3^k$. Applying the trifferent property to the three distinct vectors $\vec{0}$, $u^\top G$, $v^\top G$, there is a $b \in B$ such that $\{u^\top b, v^\top b\} = \{-1, 1\}$. Hence, $b \in V$ or $-b \in V$ as required. □

From Lemma 1.2, Theorem 2.15, and Theorem 6.1, we can deduce that a linear code $C \subseteq \mathbb{F}_3^n$ is minimal if and only if it is trifferent. We give a direct short proof of this equivalence.

Theorem 6.2. *A linear code $C \subseteq \mathbb{F}_3^n$ is trifferent if and only if it is minimal.*

Proof. First suppose that C is not minimal. Then, there exist distinct nonzero codewords $u, v \in C$ with $\mathrm{supp}(u) \subsetneq \mathrm{supp}(v)$. Let $w = -u$, which must also lie in C as C is linear. Then there is no index i such that $\{u_i, v_i, w_i\} = \mathbb{F}_3$, since $v_i = 0$ implies $u_i = w_i = 0$ and $u_i = 0 \iff w_i = 0$. We conclude that C is not a trifferent code.

For the other direction, suppose that C is not a trifferent code. Let $u, v, w \in C$ be distinct elements such that $\{u_i, v_i, w_i\} \neq \mathbb{F}_3$ for every index i. We may assume $w = \vec{0}$ (otherwise replace u, v, w by $u - w, v - w, w - w$, respectively). Note that this implies $u, v \neq \vec{0}$. Since there is no index i for which $\{u_i, v_i\} = \{1, 2\}$, we have $\mathrm{supp}(u + v) = \mathrm{supp}(u) \cup \mathrm{supp}(v)$. Moreover, since u and v are distinct, $\mathrm{supp}(u) \neq \mathrm{supp}(v)$, which implies $\mathrm{supp}(u) \subsetneq \mathrm{supp}(u + v)$ or $\mathrm{supp}(v) \subsetneq \mathrm{supp}(u + v)$. We conclude that C is not a minimal code. □

The minimum size of a subset $B \subseteq \mathbb{F}_q^k$ such that $\cup_{\zeta \in \mathbb{F}_q} \zeta B$ is a 2-blocking set in $\mathbb{F}_q^k$ is equal to $b_q^*(k, 1)$ by Lemma 1.2. Moreover, we have $b_q(k, 2) \leqslant (q - 1)b_q^*(k, 1) + 1$. Note that $b_3^*(k, 1)$ is the smallest size of a symmetric 2-blocking set in $\mathbb{F}_3^k$ as defined before.

Corollary 6.3. *For all positive integers k, n, we have*

$$T_L(n) \geqslant 3^k \iff b_3^*(k, 1) \leqslant n.$$

Proof. For the forward implication, suppose $C \subseteq \mathbb{F}_3^n$ is a linear trifferent code with $|C| \geqslant 3^k$. Let $G \in \mathbb{F}_3^{k \times n}$ be a matrix whose rows are k linearly independent vectors from C. Let B be the set of columns of G. Then, $|B| = n$ and $\{\vec{0}\} \cup B \cup -B$ is a 2-blocking set in $\mathbb{F}_3^k$. So $b_3^*(k, 1) \leqslant n$.

For the backward implication, let $\{\vec{0}\} \cup B \cup -B$ be a 2-blocking set in $\mathbb{F}_3^k$ with $|B| = b_3^*(k, 1) \leqslant n$. Let $G \in \mathbb{F}_3^{k \times n}$ be the matrix with the elements of B as columns (each element of B occurs at least once as a column). Note that since $\{\vec{0}\} \cup B \cup -B$ is a 2-blocking set, it is not contained in a linear hyperplane of $\mathbb{F}_3^k$. So the matrix G has rank k. It follows that the row space of G is a k-dimensional linear trifferent code, so $T_L(n) \geqslant 3^k$. □

6.1 | Lower bound

By Theorem 1.1, we have $b_3(k, 2) \leqslant 1 + 16k/\log_3(81/25)$. Moreover, the obtained random 2-blocking set is a union of lines by construction. Therefore, we also have $b_3^*(k, 1) \leqslant 8k/\log_3(81/25)$. Let $k = \lfloor n \frac{\log_3(81/25)}{8} \rfloor$. Then, $b_3^*(k, 1) \leqslant n$. From Corollary 6.3, it follows that

$$T_L(n) \geqslant 3^k \geqslant \tfrac{1}{3} 3^{n \frac{\log_3(81/25)}{8}} = \tfrac{1}{3}(9/5)^{n/4},$$

thus proving the lower bound in Theorem 1.5.

6.2 | Upper bound

Let $C \subseteq \mathbb{F}_3^n$ be a linear trifferent code of size $k = T_L(n)$. Then by Theorem 6.1, C gives rise to a set $B \subseteq \mathbb{F}_3^k$ of size n such that $\{\vec{0}\} \cup B \cup -B$ is an affine 2-blocking set. The equivalence given in Lemma 1.2 shows that we thus have a strong blocking set of size $m \leqslant n$ in $\mathrm{PG}(k - 1, 3)$. A computer calculation shows $c_3 > 1.1375$, so by Theorem 1.4, we have $n \geqslant m > 4.55(k - 1)$ for sufficiently

large k. Therefore, $T_L(n) < n/4.55 + 1$ for sufficiently large n, thus proving the upper bound in Theorem 1.5.

6.3 | Explicit construction

The explicit construction outlined in Section 5 gives us an affine 2-blocking set in $\mathbb{F}_3^k$ of size $8ck + 1$. This gives us an explicit construction of linear trifferent codes of length n and dimension at least $\frac{n}{4c}$ because the construction is from a strong blocking set, and hence a union of lines through the origin. The best constant c that we get from [7] is not good enough to improve the construction from [53], which has size dimension $n/112$. However, the construction in [12] does manage to improve the state of the art for $q = 3$. In particular, Corollary 3.3 in [12] (with $q_0 = 3$) implies that there is an explicit construction of strong blocking sets of size at most $48k_i$ in $\mathrm{PG}(k-1, q)$, for an infinite sequence of $\{k_i\}_{i\geqslant 1}$ (see [12, Theorem 3.2] for the exact value of k_i). Therefore, we get an explicit construction of linear trifferent codes of length $n_i \leqslant 48k_i$ and dimension k_i. We now improve this explicit construction by computing $T_L(n)$ for some small values of n. For fixed dimension k, the minimum size of a symmetric 2-blocking set in $\mathbb{F}_3^k$ can be found using integer linear programming:

$$
2b_3^*(k,1)+1 = \begin{array}{lll}
\min \sum_{v\in\mathbb{F}_3^k} x_v & & \\
\text{s.t.} \sum_{v\in W} & x_v \geqslant 1, & \forall W \subseteq \mathbb{F}_3^k \text{ co-dim 2 affine subspace} \\
\sum_{v\in H} & x_v \geqslant 2k-1, & \forall H \subseteq \mathbb{F}_3^k \text{ affine hyperplane} \\
& x_{\vec{0}} = 1 & \\
& x_v - x_{-v} = 0 & \forall v \in \mathbb{F}_3^k \setminus \{\vec{0}\} \\
& x_v \in \{0,1\}, & \forall v \in \mathbb{F}_3^k.
\end{array}
$$

The inequalities $\sum_{v\in H} x_v \geqslant 2k-1$ are redundant and follow from the bound $b_q(k,1) \geqslant (q-1)(k-1)+1$. However, adding these inequalities seems to significantly speed up computations.[†] We obtained the following explicit values for small k:

k	2	3	4	5	6
$b_3^*(k,1)$	4	9	14	19	22–24

By Theorem 6.1, this implies

$$
T_L(n) = \begin{cases}
3^1 & \text{for } n \leqslant 3, \\
3^2 & \text{for } 4 \leqslant n \leqslant 8, \\
3^3 & \text{for } 9 \leqslant n \leqslant 13, \\
3^4 & \text{for } 14 \leqslant n \leqslant 18, \\
3^5 & \text{for } 19 \leqslant n \leqslant 21.
\end{cases}
$$

[†] Using Gurobi 10.0, the values for $k \leqslant 5$ were found within a few minutes on a personal computer. We were not able to compute the exact value of $b_3^*(6,1)$.

In particular, we have found a linear trifferent code of dimension 6 and length 24, that we now use to find our general explicit construction.

Proof of Theorem 1.7. Let C_{in} be the $[24, 6]_3$ trifferent code defined by the following generator matrix.

$$\begin{bmatrix} 101111101000011011111111 \\ 012200000101120112210201 \\ 121212202202012220112100 \\ 110110100011120021110011 \\ 220002101012122202102210 \\ 010002111020111202200000 \end{bmatrix}$$

Let C_{out} be an explicit infinite family of $[N, RN, \delta N]_{3^6}$ codes with $\delta = 2/3$ and $R = 1/3 - 1/(\sqrt{3^6} - 1)$. Such a family can be constructed using algebraic-geometric codes [52]. Then, by the argument in [5], we know that C_{out} has the trifference property. Therefore, the concatenation $C_{\text{out}} \circ_\pi C_{\text{in}}$ is an $\mathbb{F}_3$-linear trifferent code of length $n = 24N$ and dimension $k = 6RN$, and $k/n = R/4 = 23/312$. □

7 | CONCLUSION

In this paper, we established new connections between affine blocking sets, strong blocking sets, and trifferent codes. We obtained new bounds on affine blocking sets, which improve the state of the art for bounds on the latter two objects as well. Moreover, using the recent explicit constructions of strong blocking sets, we gave new explicit constructions of trifferent codes, beating the current bound. Despite this progress, many interesting problems remain open.

Recall that $b_q(k, s)$ denotes the smallest size of an affine s-blocking set in $\mathbb{F}_q^k$. While we can prove upper bounds on $b_q(k, s)$ that, for any fixed s, are only a constant factor away from the lower bound given in (1), the problem of determining the asymptotics of $b_q(k, s)$ when s varies with k is wide open.

Question 7.1. What is the asymptotic growth of $b_q(k, s)$, for fixed q, $s = \Theta(k)$, and $k \to \infty$?

While we could improve the lower bounds on strong $(s-1)$-blocking sets, we are unable to improve the lower bounds on affine s-blocking sets given in (1), for fixed s and q, k large. In particular, we ask the following.

Question 7.2. For every fixed prime power q, is there a constant $C_q > 1$ such that $b_q(k, 2) \geqslant C_q q^2 k$, for large enough k?

Finally, we proved a lower bound on linear trifferent codes that is asymptotically equal to the best lower bound on trifferent codes. Our lower bound is based on the new upper bound on strong blocking sets, obtained by picking a random set of planes through the origin in $\mathbb{F}_q^k$. Any improvement in our argument would be very interesting, as it might lead to a breakthrough for the trifference problem.

Question 7.3. Is $\liminf_{n\to\infty} \frac{\log_3(T_L(n))}{n} > \frac{\log_3(9/5)}{4}$?

The data on $T_L(n)$ for small n, that we computed in Section 5, suggest that $\lim_{n\to\infty} \log_3(T_L(n))/n = 1/5$, but we are not too confident to make that conjecture.

While it is natural to extend the notion of linear perfect 3-hash codes to linear perfect q-hash codes, with $q > 3$, the following argument shows that these objects are trivial. Let $\mathbb{F}_q$ be a finite field with $q > 3$. We show that there is no linear perfect q-hash code $C \subseteq \mathbb{F}_q^n$ of dimension $\geqslant 2$. Suppose $C \subseteq \mathbb{F}_q^n$ is a subspace of dimension $\geqslant 2$, and let u, v be two linearly independent vectors. Write $\mathbb{F}_q \setminus \{0\} = \{\xi^i : 0 \leqslant i \leqslant q-2\}$ and consider the set of vectors $\{u, \zeta u\} \cup \{v, \zeta v, \zeta^2 v, \dots, \zeta^{q-3} v\}$. Say there is a coordinate i where they are all distinct. Since $q > 3$, u_i and v_i must both be nonzero. But we then have q distinct nonzero coordinates, which is impossible. So C cannot be a perfect q-hash code.

Therefore, it is more sensible to study linear codes $C \subseteq \mathbb{F}_q^n$, with the property that for any t distinct codewords in C, there is a coordinate where they are all pairwise distinct, for some parameter $t < q$. Such codes have been studied in the literature under the name of linear perfect hash families, and in fact it can be shown that these codes cannot exist for $t \geqslant c\sqrt{q}$ for some constant c (see [14, Section 5]). In [53], an explicit construction is given that has dimension at least a linear function of n, when $t = O(q^{1/4})$. It would be interesting to improve these results on perfect hash families in view of our work.

APPENDIX A

Lemma A.1. *For every prime power q, $M_q((q-1)/(q+1)) < 1/(q+1)$.*

Proof. For $q = 2$, one can easily verify that $M_2(1/3) < 1/3$, so we assume $q \geqslant 3$ for the rest of the argument. Let $\delta := \frac{q-1}{q+1}$. We have, after a little algebraic manipulation,

$$\begin{aligned} x_\delta &:= 1 - \frac{1}{q} - \left(1 - \frac{2}{q}\right)\delta - \frac{2}{q}\sqrt{(q-1)\delta(1-\delta)} \\ &= \frac{q-1}{q(q+1)}\left(3 - 2\sqrt{2}\right). \end{aligned}$$

Let $w := 3 - 2\sqrt{2}$, so that $x_\delta = w\frac{q-1}{q(q+1)}$, and so one may verify that

$$-\frac{(q-1)}{q} w \log_q w < 0.19 \tag{A1}$$

for $q \geqslant 3$. We also have the following inequality for every $q \geqslant 3$,

$$\frac{q-1}{q}\log_q(q(q+1)) = \frac{2(q-1)}{q} + \frac{(q-1)}{q}\log_q(1+1/q) < \frac{2(q-1)}{q} + \frac{q-1}{q^2} < 2. \tag{A2}$$

Here, we have used the fact

$$\log_q(1+1/q) = \frac{\ln(1+1/q)}{\ln q} < \frac{1}{q},$$

for $q \geqslant 3$. Finally, note that

$$x_\delta = \frac{w(q-1)}{q(q+1)} < \frac{w}{q+1} \tag{A3}$$

This gives us

$$\begin{aligned} M_q\left(\frac{q-1}{q+1}\right) &= x_\delta \log_q(q-1) - x_\delta \log_q x_\delta - (1-x_\delta)\log_q(1-x_\delta) \\ &\leqslant x_\delta \log_q(q-1) - x_\delta \log_q x_\delta - \log_q(1-x_\delta) \\ &\leqslant x_\delta \log_q\left(\frac{q-1}{x_\delta}\right) + 2x_\delta \\ &= -\frac{w(q-1)}{q(q+1)} \log_q w + \frac{w(q-1)}{q(q+1)} \log_q(q(q+1)) + 2x_\delta \\ &\leqslant \frac{0.19 + 4w}{q+1} \\ &< \frac{1}{q+1}. \end{aligned}$$

For the second inequality, we used the fact $-\log_q(1-x) < 2x$ for $x < 0.5$, and for the second last inequality, we used (A1),(A2), and (A3). □

Corollary A.2. *There is a unique solution c_q to $M_q((q-1)/(x(q+1)) = 1/(x(q+1))$, and $x \geqslant 1$. Moreover, $c_q > 1$.*

Proof. The function $f(y) := M_q((q-1)y/(q+1))$ is a continuous strictly decreasing function for $0 \leqslant y \leqslant 1$, with $f(0) = 1$, and the function $g(y) := y/(q+1)$ is a continuous strictly increasing function, with $g(0) = 0$. We have just shown that $g(1) > f(1)$, and thus there must exist a unique $0 < y_q < 1$ for which $f(y_q) = g(y_q)$. Therefore, $c_q = 1/y_q > 1$. □

Remark A.3. The proof also shows that c_q is the maximum $x \geqslant 1$ for which $M_q((q-1)/(x(q+1)) \leqslant 1/(x(q+1))$. Using similar arguments, one may show $c_q > 1 + 1/(2000q)$, for all prime powers q.

ACKNOWLEDGMENTS

The research of Jozefien D'haeseleer is supported by the FWO (Research Foundation Flanders). We thank Alessandro Neri and the anonymous reviewer for their helpful comments.

JOURNAL INFORMATION

The *Journal of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. M. Aaltonen, *Linear programming bounds for tree codes (corresp.)*, IEEE Trans. Inform. Theory **25** (1979), no. 1, 85–90.
2. G. N. Alfarano, M. Borello, and A. Neri, *A geometric characterization of minimal codes and their asymptotic performance*, Adv. Math. Commun. **16** (2022), no. 1, 115–133.
3. G. N. Alfarano, M. Borello, and A. Neri, *Outer strong blocking sets*, Electron. J. Combin. **31** (2024), no. 2, P2.18.
4. G. N. Alfarano, M. Borello, A. Neri, and A. Ravagnani, *Three combinatorial perspectives on minimal codes*, SIAM J. Discrete Math. **36** (2022), no. 1, 461–489.
5. N. Alon, *Explicit construction of exponential sized families of k-independent sets*, Discrete Math. **58** (1986), no. 2, 191–193.
6. N. Alon, *Combinatorial nullstellensatz*, Combin. Probab. Comput. **8** (1999), no. 1-2, 7–29.
7. N. Alon, A. Bishnoi, S. Das, and A. Neri, *Strong blocking sets and minimal codes from expander graphs*, arXiv:arXiv:2305.15297, 2023.
8. N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes*, European J. Combin. **14** (1993), no. 2, 79–83.
9. K. S. Bagga, L. W. Beineke, W. D. Goddard, M. J. Lipman, and R. E. Pippert, *A survey of integrity*, Discrete Appl. Math. **37** (1992), 13–28.
10. S. Ball, *Multiple blocking sets and arcs in finite planes*, J. Lond. Math. Soc. **54** (1996), no. 3, 581–593.
11. S. Ball, *The polynomial method in Galois geometries*, J. De Beule and L. Storme (eds.), Current research topics in Galois geometry, chapter 5, Nova Science Publishers, Inc., New York, 2011, pp. 105–130.
12. D. Bartoli and M. Borello, *Small strong blocking sets by concatenation*, SIAM J. Discrete Math. **37** (2023), 65–82.
13. A. Bishnoi, P. L. Clark, A. Potukuchi, and J. R Schmitt, *On zeros of a polynomial in a finite grid*, Combin. Probab. Comput. **27** (2018), no. 3, 310–333.
14. S. R. Blackburn and P. R. Wild, *Optimal linear perfect hash families*, J. Combin. Theory Ser. A **83** (1998), no. 2, 233–250.
15. A. Blokhuis, P. Sziklai, and T. Szönyi, *Blocking sets in projective spaces*, J. De Beule and L. Storme (eds.), Current research topics in Galois geometry, chapter 3, Nova Science Publishers, Inc., New York, 2011, pp. 61–184.
16. J. E. Bonin and H. Qin, *Size functions of subgeometry-closed classes of representable combinatorial geometries*, Discrete Math. **224** (2000), no. 1-3, 37–60.
17. A. E. Brouwer and A. Schrijver, *The blocking number of an affine space*, J. Combin. Theory Ser. A **24** (1978), 251–253.
18. R. Casse, *Projective geometry: an introduction*. Oxford University Press, Oxford, 2011.
19. H. Chabanne, G. Cohen, and A. Patey, *Towards secure two-party computation from the wire-tap channel*. In: H. S. Lee, D. G. Han (eds.), Information Security and Cryptology – ICISC 2013. ICISC 2013. Lecture Notes in Computer Science(), vol 8565. Springer, Cham, 2014, https://doi.org/10.1007/978-3-319-12160-4_3
20. G. Cohen and A. Lempel, *Linear intersecting codes*, Discrete Math. **56** (1985), no. 1, 35–43.
21. G. Cohen, S. Mesnager, and H. Randriam, *Yet another variation on minimal linear codes*, Adv. Math. Commun. **10** (2016), no. 1, 53–61.
22. G. D. Cohen and G. Zémor, *Intersecting codes and independent families*, IEEE Trans. Inform. Theory **40** (1994), no. 6, 1872–1881.
23. S. Costa and M. Dalai, *A gap in the slice rank of k-tensors*, J. Combin. Theory Ser. A **177** (2021), 105335.
24. A. A. Davydov, M. Giulietti, S. Marcugini, and F. Pambianco, *Linear nonbinary covering codes and saturating sets in projective spaces*, Adv. Math. Commun. **5** (2011), no. 1, 119.
25. J. S. Ellenberg and D. Gijswijt, *On large subsets of with no three-term arithmetic progression*, Ann. of Math. **185** (2017), 339–343, https://annals.math.princeton.edu/2017/185-1/p08
26. S. L. Fancsali and P. Sziklai, *Lines in Higgledy-Piggledy arrangement*, Electron. J. Combin. **21** (2014), P2.56, https://www.combinatorics.org/ojs/index.php/eljc/article/view/v21i2p56
27. S. L. Fancsali and P. Sziklai, *Higgledy-Piggledy subspaces and uniform subspace designs*, Des. Codes Cryptogr. **79** (2016), no. 3, 625–645.
28. S. Della Fiore, A. Gnutti, and S. Polak, *The maximum cardinality of trifferent codes with lengths 5 and 6*, Ex. Counterex. **2** (2022), https://www.sciencedirect.com/science/article/pii/S2666657X22000039
29. J. Fox and H. T. Pham, *Popular progression differences in vector spaces*, Int. Math. Res. Not. **2021** (2021), no. 7, 5261–5289.

30. Z. Füredi, *Matchings and covers in hypergraphs*, Graphs Combin. **4** (1988), no. 1, 115–206.
31. H. Furstenberg and Y. Katznelson, *A density version of the Hales-Jewett theorem*, J. Anal. Math. **57** (1991), no. 1, 64–119.
32. D. Gijswijt, *Excluding affine configurations over a finite field*, Discrete Analysis (2023), https://discreteanalysisjournal.com/article/91186-excluding-affine-configurations-over-a-finite-field
33. V. Guruswami and S. Kopparty, *Explicit subspace designs*, Combinatorica **36** (2016), no. 2, 161–185.
34. V. Guruswami and A. Riazanov, *Beating Fredman-Komlós for perfect k-hashing*, J. Combin. Theory Ser. A **188** (2022), 105580.
35. V. Guruswami, A. Rudra, and M. Sudan, *Essential coding theory*, 2022, http://www.cse.buffalo.edu/atri/courses/coding-theory/book
36. T. Héger and Z. L. Nagy, *Short minimal codes and covering codes via strong blocking sets in projective spaces*, IEEE Trans. Inform. Theory **68** (2021), no. 2, 881–890.
37. R. E. Jamison, *Covering finite fields with cosets of subspaces*, J. Combin. Theory Ser. A **22** (1977), no. 3, 253–266.
38. G. Katona and J. Srivastava, *Minimal 2-coverings of a finite affine space based on* GF(2), J. Statist. Plann. Inference **8** (1983), no. 3, 375–388.
39. J. Körner, *Coding of an information source having ambiguous alphabet and the entropy of graphs*. 6th Prague conference on information theory, 1973, pp. 411–425.
40. J. Körner and K. Marton, *New bounds for perfect hashing via information theory*, Eur. J. Combin. **9** (1988), no. 6, 523–530.
41. S. Kurz, *Trifferent codes with small lengths*, Ex. Counterex **5** (2024), 100139.
42. L. Lovász, *On the ratio of optimal integral and fractional covers*, Discrete Math. **13** (1975), no. 4, 383–390.
43. A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277.
44. R. McEliece, E. Rodemich, H. Rumsey, and L. Welch, *New upper bounds on the rate of a code via the Delsarte-Macwilliams inequalities*, IEEE Trans. Inform. Theory **23** (1977), no. 2, 157–166.
45. D. Miklós, *Linear binary codes with intersection properties*, Discrete Appl. Math. **9** (1984), no. 2, 187–196.
46. C. Pohoata and D. Zakharov, *On the trifference problem for linear codes*, IEEE Trans. Inform. Theory **68** (2022), no. 11, 7096–7099.
47. M. Richardson, *On finite projective games*, Proc. Amer. Math. Soc. **7** (1956), no. 3, 458–465.
48. M. Scotti, *On the lower bound for the length of minimal codes*, Discrete Math. **347** (2024), 113676.
49. R. P. Stanley, *Enumerative combinatorics*, 2nd ed., Cambridge studies in advanced mathematics, vol. 1, Cambridge University Press, New York, 2011, p. 135.
50. M. Tait and R. Won, *Improved bounds on sizes of generalized caps in* AG(n, q), SIAM J. Discrete Math. **35** (2021), no. 1, 521–531.
51. C. Tang, Y. Qiu, Q. Liao, and Z. Zhou, *Full characterization of minimal linear codes as cutting blocking sets*, IEEE Trans. Inform. Theory **67** (2021), no. 6, 3690–3700.
52. M. Tsfasman and S. G. Vladut, *Algebraic-geometric codes*, vol. 58, Springer Science & Business Media, Dordrecht, 2013, https://link.springer.com/book/10.1007/978-94-011-3810-9
53. H. Wang and C. Xing, *Explicit constructions of perfect hash families from algebraic curves over finite fields*, J. Combin. Theory Ser. A **93** (2001), no. 1, 112–124.
54. C. Xing and C. Yuan, *Beating the probabilistic lower bound on perfect hashing*. Proceedings of the 2021 ACM-SIAM symposium on discrete algorithms (SODA), SIAM, 2021, pp. 33–41, https://epubs.siam.org/doi/abs/10.1137/1.9781611976465.3