Citation (APA)
Bishnoi, A., & Tomon, I. (2026). Explicit Constructions of Optimal Blocking Sets and Minimal Codes. *Combinatorica*, *46*(2), Article 13. https://doi.org/10.1007/s00493-026-00202-5

Combinatorica (2026) 46:13
https://doi.org/10.1007/s00493-026-00202-5

ORIGINAL PAPER

Explicit Constructions of Optimal Blocking Sets and Minimal Codes

Anurag Bishnoi[1] · **István Tomon**[2]

Received: 25 November 2024 / Revised: 26 March 2025 / Accepted: 16 January 2026

Abstract
A strong s-blocking set in a projective space is a set of points that intersects each codimension-s subspace in a spanning set of the subspace. We present an explicit construction of such sets in a $(k-1)$-dimensional projective space over $\mathbb{F}_q$ of size $O_s(q^s k)$, which is optimal up to the constant factor depending on s. This also yields an optimal explicit construction of affine blocking sets in $\mathbb{F}_q^k$ with respect to codimension-$(s+1)$ affine subspaces, and of s-minimal codes. Our approach is motivated by a recent construction of Alon, Bishnoi, Das, and Neri of strong 1-blocking sets, which uses expander graphs with a carefully chosen set of vectors as their vertex set. The main novelty of our work lies in constructing specific hypergraphs on top of these expander graphs, where tree-like configurations correspond to strong s-blocking sets. We also discuss some connections to size-Ramsey numbers of hypergraphs, which might be of independent interest.

1 Introduction

A blocking set in a finite projective or affine space is a set of points that intersects every subspace of a given dimension non-trivially. In graph terminology, these are vertex covers of the hypergraphs whose vertex sets are points of the finite space and edges are the subspaces of the fixed dimension. These objects have been studied extensively in finite geometry [13, 15], and many connections have been found with related areas like coding theory. A natural strengthening of this object, that incorporates more geometrical structure, is a *strong s-blocking set*: a set B of points in the projective space $\mathrm{PG}(k-1, q)$, that meets every subspace S of codimension-s in a set of points

---

Research supported in part by the Swedish Research Council grant VR 2023-03375.

✉ Anurag Bishnoi
A.Bishnoi@tudelft.nl

István Tomon
istvantomon@gmail.com

[1] Delft University of Technology, Delft, Netherlands

[2] Umeå University, Umeå, Sweden

that spans S. We can also think of B as a collection of pairwise linearly independent vectors in $\mathbb{F}_q^k$ such that the span $\langle B \cap S\rangle$ is equal to S for every vector subspace S of (vector) dimension $k-s$. For $s = 1$, these objects are simply known as strong blocking sets [17, 22], and they have also been studied under the names of cutting blocking sets [1, 14] and generating sets [19, 20]. Finding the smallest size of a strong blocking set is a major open problem in finite geometry, whose importance has increased significantly in the last few years due to its connection to finding short minimal codes [1, 32]. More recently, it has been shown in [12] that strong blocking sets of size n over $\mathbb{F}_3^k$ are equivalent to linear trifferent codes of length n and dimension k, thus tying them to another important open problem in information theory, *the trifference problem*.

In [12, Lemma 1.2], it was shown that a strong s-blocking set of size n in the projective space $\mathrm{PG}(k-1, q)$ gives rise to an affine blocking set of size $(q-1)n+1$ in $\mathbb{F}_q^k$ with respect to the $(k-s-1)$-dimensional affine subspaces. An application of the polynomial method [15], combined with a geometric argument [9, Section 3], then implies that a strong s-blocking set in $\mathrm{PG}(k-1, q)$ must be of size at least $(q^{s+1}-1)(k-s)/(q-1)$. For $s = 1$, this lower bound was improved in [12, Theorem 1.4] to $c_q(q+1)(k-1)$ for a constant $c_q > 1$ that does not have a closed formula, but it can be computed by solving an equation involving the q-ary entropy function and the linear-programming bound from coding theory. The best upper bounds are obtained by taking a random collection of s-dimensional (projective) subspaces [12, Remark 3.4] and they are of the order $(q^{s+1}-1)((s+1)(k-s-1))/(q-1)$, which is roughly $s+1$ times the lower bound. Therefore, it is still an open problem to determine the smallest size of a strong s-blocking set for every $s \geq 1$.

As the random construction suggests, a useful way of constructing strong s-blocking sets is by using a collection of s-dimensional projective subspaces in $\mathrm{PG}(k-1, \mathbb{F})$, for an arbitrary field $\mathbb{F}$, whose union meets every codimension-s subspace in a spanning set; this is also known as a 'higgledy-piggledy' arrangement of subspaces [20] and it has connections with subspace designs [21]. Over characteristic 0 fields, or finite fields of sufficiently large size with respect to the dimension, we know an explicit construction of such higgledy-piggledy subspaces [20], and thus strong s-blocking sets, which is a constant factor away (for a fixed s and k) from the lower bound. The main challenge is then to give constructions in $\mathrm{PG}(k-1, q)$ where both q and s are fixed, and $k \to \infty$. This is also the setting that is more interesting from a coding-theoretic point of view where we need a fixed alphabet size.

In [5], an explicit construction of size $O(qk)$ was obtained for strong 1-blocking sets in $\mathrm{PG}(k-1, q)$ using constant-degree expander graphs. This solved the main open problem on constructing short minimal codes because of their known equivalence with strong blocking sets [1, 32]. Here, a linear code $C \leq \mathbb{F}_q^n$ is called *minimal* if there are no two linearly independent codewords x, y in C for which the support of x is a subset of the support of y. A natural generalization of this, called *s-minimal code*, is a linear code C that contains no two distinct s-dimensional subspaces U, V for which the support of U is contained in the support of V. Here, the support of a vector subspace is the set of coordinate positions where at least one vector in the subspace has a non-zero entry.

1.1 Our results

We give the first explicit constructions of strong s-blocking sets, whose size is optimal as a function of both q and k for $s > 1$. In particular, we explicitly construct strong s-blocking sets of size $O_s(q^s k)$ in $PG(k-1, q)$. This is indeed optimal up to the dependence of the constant factor on s by the aforementioned lower bound $(q^{s+1} - 1)(k-s)/(q-1)$.

Our construction is a far reaching generalization of the approach of [5], which constructs a strong 1-blocking set. In [5], the authors consider an expander graph G, whose vertices are $O(k)$ vectors in 'general position'. Then the desired strong 1-blocking set is the collection of 1-dimensional subspaces, that is, points of $\mathrm{PG}(k-1, q)$, that are contained in the union of the 2-dimensional subspaces spanned by the edges of G. We extend this approach to hypergraphs. We define an $(s+1)$-uniform hypergraph H, whose vertex set is a set of $O_s(k)$ vectors in $\mathbb{F}_q^k$ in 'general position'. Then our strong s-blocking set B is the collection of 1-dimensional subspaces that are contained in the union of the $(s+1)$-dimensional subspaces spanned by the edges of H. We build H on top of an expander graph G of degree $O_s(1)$, by including all $(s+1)$-tuples of vertices of distance at most $s+1$ from a given vertex in G. This ensures that H has $O_s(k)$ edges, and thus B has $O_s(q^s k)$ elements. We discuss expander graphs and the notion of 'general position' in Section 2. Given a codimension-s subspace L, the intersection of B and L naturally gives rise to a certain subhypergraph in H. We argue that the existence of large tree-like configurations in this hypergraph ensures that $L \cap B$ spans L. These tree-like configurations and their relationship to spanning sets is discussed in Section 3.

First, we present a construction for $s = 2$ to illustrate the core of our ideas, which can be found in Section 4.1. Then, in Section 4.2, we explore connections of strong blocking sets to a popular topic of extremal combinatorics, known as size-Ramsey numbers. We use recent results of Letzter, Pokrovskiy and Yepremyan [26] about the size-Ramsey numbers of tight paths to construct strong s-blocking sets of size $O_s(q^s k)$ for large prime powers q with respect to s. Here, unfortunately, the constant hidden by the $O_s(.)$ notation is astronomical as a function of s. We improve this in Section 4.3, where we present a self-contained construction of strong s-blocking sets of size at most $2^{O(s^2 \log s)} q^s k$ for every prime power q sufficiently large with respect to s. We treat small prime powers q separately in Section 4.4, where we provide explicit constructions of size at most $q^{O(s^2)} k$ (which is of the promised form $O_s(q^s k)$ assuming q is bounded by a function of s).

Finally, by a known duality between strong s-blocking sets and s-minimal codes (see Example 3.2 in [35]), these also provide the first explicit constructions of asymptotically optimal s-minimal codes. For completeness, we also discuss this relationship between strong s-blocking sets and s-minimal codes in Section 2.2.

2 Background

2.1 Expander graphs

In this section, we define and collect some useful properties of expander graphs.

Definition 1 (Expander graph) An *(n, d, λ)-graph* is a d-regular connected graph on n vertices such that every eigenvalue of the adjacency matrix other than d is at most λ in absolute value.

Expander graphs are of high importance in computer science [7, 23], coding theory [5, 30], and combinatorics [26], as witnessed by countless applications. A family of constant degree expanders usually refers to some infinite family of (n_i, d, λ)-expanders, where $n_i \to \infty$, and $\lambda < \varepsilon d$ for some $\varepsilon \in (0, 1)$. The Alon-Boppana theorem tells us that an (n, d, λ)-graph can only exist if $\lambda \geq 2\sqrt{d-1} - o_n(1)$. Graphs achieving this theoretical barrier are called *Ramanujan graphs* and the celebrated result of Lubotzky, Phillips and Sarnak [27] gives explicit constructions of such graphs for an infinite family of parameters.

Lemma 1 *Let $q > p$ be primes congruent to 1 modulo 4. Then there is an explicit construction of an $(n, p+1, 2\sqrt{p})$-graph for some $n = \Theta(q^3)$.*

Unfortunately, there are no known explicit constructions of Ramanujan graphs for every pair of parameters (n, d). However, the previous lemma implies that for every d and n sufficiently large with respect to d, there is a d_0-regular Ramanujan graph on n_0 vertices, where $d_0 = \Theta(d)$ and $n_0 = (1 + o(1))n$, by well known results on the distribution of primes. Alon [4] presents further explicit and strongly explicit constructions of almost Ramanujan graphs for every n. For our purposes, given the parameter s, we need an infinite family of explicit (n, d, λ)-graphs, where $d = O_s(1)$ and $\lambda \leq \varepsilon d$ for some fixed $\varepsilon = \varepsilon(s) > 0$. The existence of such a family is guaranteed by Lemma 1.

One of the key technical results about expander graphs is the *Expander mixing lemma*. Given a subset U of the vertices of a graph G, $G[U]$ denotes the subgraph of G induced on U. Also, if U and V are disjoint sets of vertices, then $G[U, V]$ is the induced bipartite subgraph of G with parts U and V.

Lemma 2 (Expander mixing lemma *[7]) Let G be an (n, d, λ)-graph. Then for every $U \subset V(G)$,*

$$\left|2e(G[U]) - \frac{d}{n}|U|^2\right| \leq \lambda|U|.$$

Also, for every pair of disjoint $U, V \subset V(G)$,

$$\left|e(G[U, V]) - \frac{d}{n}|U||V|\right| \leq \lambda\sqrt{|U||V|}.$$

One of the simple consequences of the Expander mixing lemma is the following statement.

Lemma 3 *Let G be an (n, d, λ)-graph, and let H be a subgraph of G with at least λn edges. Then H has a connected component of size at least $e(H)/d$.*

Proof Let $U_1, \ldots, U_s$ be the vertex sets of connected components of H, and let $b = \max_{i \in [s]} |U_i|$. By the first part of the Expander mixing lemma, we have

$$e(G[U_i]) \leq \frac{d}{2n}|U_i|^2 + \frac{\lambda}{2}|U_i| \leq \left(\frac{db}{2n} + \frac{\lambda}{2}\right)|U_i|$$

for $i = 1, \ldots, s$. Therefore,

$$e(H) \leq \sum_{i=1}^{s} e(G[U_i]) \leq \sum_{i=1}^{s} \left(\frac{db}{2n} + \frac{\lambda}{2}\right)|U_i| = \frac{db + \lambda n}{2}.$$

Comparing the left and right hand side, we get

$$b \geq \frac{2e(H) - \lambda n}{d} \geq \frac{e(H)}{d}.$$

□

Another useful corollary is the following.

Lemma 4 *Let G be an (n, d, λ)-graph, and let $U \subset V(G)$. Then $G[U]$ has a connected component of size at least $|U| - \frac{2\lambda n}{d}$.*

Proof Let $U_1, \ldots, U_s$ be the vertex sets of connected components of $G[U]$, and let $b = \max_{i \in [s]} |U_i|$. Then by the Expander mixing lemma,

$$e(G[U_i]) \leq \frac{d}{2n}|U_i|^2 + \frac{\lambda}{2}|U_i| \leq \left(\frac{db}{2n} + \frac{\lambda}{2}\right)|U_i|.$$

On the other hand, $e(G[U]) \geq \frac{d}{2n}|U|^2 - \frac{\lambda}{2}|U|$. Hence,

$$\frac{d}{2n}|U|^2 - \frac{\lambda}{2}|U| \leq \sum_{i=1}^{s} \left(\frac{db}{2n} + \frac{\lambda}{2}\right)|U_i| = \left(\frac{db}{2n} + \frac{\lambda}{2}\right)|U|.$$

From this, we get

$$b \geq |U| - \frac{2\lambda n}{d}.$$

□

Finally, we need the following technical result.

Lemma 5 *Let G be an (n, d, λ)-graph, and let $U_0, \ldots, U_t \subset V(G)$ be disjoint sets such that $|U_0| > t\lambda n/d$, and $|U_i| \geq \lambda n/d$ for $i = 1, \ldots, t$. Then there is a vertex $x \in U_0$ that sends an edge to every U_i, $i = 1, \ldots, t$.*

Proof The second part of the Expander mixing lemma implies that there is an edge between any two sets of size more than $b = \lambda n/d$. Hence, if $W_i \subset U_0$ is the set of vertices that send an edge to U_i, then $|W_i| \geq |U_0| - b$. But then $|\bigcap_{i=1}^t W_i| \geq |U_0| - bt > 0$. Any vertex $x \in \bigcap_{i=1}^t W_i$ suffices. □

2.2 Coding theory

In this section we define the basic notions from coding theory that we will need later, and prove the relation between s-minimal codes and strong s-blocking sets.

An $[n, k, d]_q$ code is a k-dimensional vector subspace of $\mathbb{F}_q^n$ such that every non-zero vector in this subspace has Hamming weight at least d, that is, it has at least d non-zero coordinates, and there is a vector with Hamming weight equal to d. The parameter n is the length of the code, k its dimension, and d is the minimum distance of the code. There are two matrices associated with a k-dimensional code $C < \mathbb{F}_q^n$. A *generator matrix* of C is a $k \times n$ matrix, whose rows are the vectors of a basis of C. A *check matrix* of C is an $(n - k) \times n$ matrix, whose null-space is C.

The *dual code* of C, denoted by $C^\perp$, is the code generated by the rows of the check matrix, or equivalently, the subspace orthogonal to C. It is easy to observe that a check matrix of C is a generator matrix of $C^\perp$, and vice versa.

We now define minimal codes and for self-containment prove their equivalence with strong blocking sets, which was observed by Alfarano, Borello, Neri, and Ravagnani [3] for $s = 1$ but the proof of the general case is very similar. The support of a vector subspace X of $\mathbb{F}_q^n$, denoted by $\text{supp}(X)$, is the set of coordinate positions i such that there is a vector $x \in X$ with $x_i \neq 0$.

Definition 2 (Minimal codes) An $[n, k, d]_q$ code C is called s-minimal if for any two distinct s-dimensional subspaces X, Y of C, $\text{supp}(X) \not\subset \text{supp}(Y)$ and $\text{supp}(Y) \not\subset \text{supp}(X)$.

In other words, the supports of s-dimensional subspaces in an s-minimal code must form an antichain in the boolean poset $2^{[n]}$.

Theorem 6 *Let G be a $k \times n$ matrix over $\mathbb{F}_q$ such that all of its columns are non-zero and pairwise linearly independent. Then the row-space of G is an s-minimal code if and only if the columns of G form a strong s-blocking set.*

Proof Let $C < \mathbb{F}_q^n$ be the row-space of G. An s-dimensional subspace X of C can be uniquely identified with the row space of MG, where M is a full rank $s \times k$ matrix. Moreover, the null-space of M gives us a codimension s-subspace in $\mathbb{F}_q^k$ which contains the i-th column of G if and only if the i-th coordinate is equal to 0 in all codewords of X. Let ϕ be the bijection from the codimension-s subspaces of $\mathbb{F}_q^k$ to the s-dimensional subspaces of C that maps the null space of M to the row space of MG.

The columns do not form a strong s-blocking set in $\mathbb{F}_q^k$ if and only if there is a codimension-s subspace H such that the set of columns of G that lie in H are all contained in a subspace T of one dimension less. Thus we can find a distinct codimension-s subspace $H' < \mathbb{F}_q^k$ such that $H \cap H' = T$ and all columns of G that are contained in H are also contained in H'. This happens if and only if $[n] \setminus \text{supp}(\phi(H)) \subset [n] \setminus \text{supp}(\phi(H'))$, which is equivalent to C not being s-minimal. □

2.3 Points in general position

Our constructions require a supply of $n = O_s(k)$ vectors $W \subset \mathbb{F}_q^k$ with the following two properties: for some fixed $\varepsilon = \varepsilon(s) > 0$, every set of εn elements of W span the whole space, and every $s + 1$ elements of W are linearly independent. Explicit constructions of such sets can be found in coding theory, as follows.

We need the following well known properties of generator and check matrices of a linear code. If C is an $[n, k, d]_q$-code, and H is a check-matrix of C, then any $d - 1$ columns of H are linearly independent. Moreover, if G is a generator matrix of C, then any $n - d + 1$ columns of G span the whole space. Therefore, the required set can be constructed by using the columns of the generator matrix of an $[n, k, d]_q$ code C where $n = O_s(k)$, $d \geq (1 - \varepsilon)n + 1$ and the minimum distance of the dual code $C^\perp$ satisfies $d^\perp \geq s + 2$.

Definition 3 (Rate and relative distance) Let $\{n_i\}_{i\geq 1}$ be an increasing sequence of positive integers and suppose that there exist sequences $\{k_i\}_{i\geq 1}$ and $\{d_i\}_{i\geq 1}$ such that for all $i \geq 1$ there is an $[n_i, k_i, d_i]_q$ code $\mathcal{C}_i$. Then $\{\mathcal{C}_i\}_{i\geq 1}$ is called an $(R, \delta)_q$-family of codes, where the rate R of this family is defined as

$$R := \liminf_{i\to\infty} \frac{k_i}{n_i},$$

and the relative distance δ is defined as

$$\delta := \liminf_{i\to\infty} \frac{d_i}{n_i}.$$

The main problem in coding theory is to study the trade-off between the rate and the relative distance of codes. A family of codes for which $R > 0$ and $\delta > 0$, is known as an *asymptotically good code*. The Gilbert-Varshamov bound, which follows from a probablistic argument, shows the existence of such codes for every $\delta \in [0, 1 - 1/q)$ and $R = 1 - H_q(\delta)$, where

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

is the q-ary entropy function. The first *explicit construction* of asymptotically good codes was given by Justesen [25], who showed that for every $0 < R < 1/2$, there is an explicit family of codes with rate R and relative distance $\delta \geq (1 - 2R)H_q^{-1}\left(\frac{1}{2}\right)$. Improving the values of the rate R and the relative distance δ has been an active area of research in coding theory since the 1970s. One of the most significant developments was the use of modular curves to show that, for every square $q \geq 49$, there are explicit constructions of linear codes over $\mathbb{F}_q$ that beat the Gilbert-Varshamov bound (see [16, 33] for some recent surveys on these constructions). Another useful tool for constructing explicit codes is expander graphs [30].

We first note that these well-known explicit constructions of asymptotically good codes [6, 25, 33, 34] and the discussion above implies the following construction where we do not have any restriction on the dual distance. This will suffice for small prime powers.

Lemma 7 *There exists* $\delta > 0$ *and* $C > 0$ *such that the following holds for every prime power* q*, and sufficiently large* k*. There exists an explicit construction of a set* $W \subset \mathbb{F}_q^k$ *of size at most* Ck *such that any* $(1-\delta)|W|$ *elements of* W *span* $\mathbb{F}_q^k$*.*

For larger prime powers, we need the following stronger result.

Lemma 8 *For every integer* s *and* $\varepsilon_0 > 0$*, there exists* C *such that the following holds. Let* q *be a prime power and* k *be an integer, both sufficiently large with respect to* s *and* ε_0*. Then there exists an explicit construction of a set* $W \subset \mathbb{F}_q^k$ *of size at most* Ck *such that any* $s+1$ *elements of* W *are linearly independent, and any* $\varepsilon_0|W|$ *elements of* W *span* $\mathbb{F}_q^k$*.*

Proof For every $R \in (0,1)$, asymptotic Goppa codes provide an $(R,\delta)_q$-family of codes for some δ satisfying $R+\delta \geq 1-1/A(q)$, where $A(q)$ is Ihara's constant (see Section 2.9 in [24]). It is known that for q square we have $A(q) = \sqrt{q}-1$ and for arbitrary q we have $A(q) = \Omega(\log q)$ (see [11] for further discussion). From Theorem 2.69 and 2.71 in [24] it can be derived that the relative distance of the dual code satisfies $\delta^{\perp} = \delta + 2R - 1 \geq R - 1/A(q)$. Therefore the columns of the generator matrix of an $[n,k,d]_q$ code from this $(R,\delta)_q$-family give rise to non-zero vectors $v_1,\ldots,v_n$ in $\mathbb{F}_q^k$, such that any r of them are linearly independent and any $n-d+1$ of them span the whole space, with

$$\lim_{n\to\infty} \frac{k}{n} = R,$$

$$\lim_{n\to\infty} \frac{n-d}{n} \leq R + 1/A(q),$$

$$\lim_{n\to\infty} \frac{r}{n} \geq R - 1/A(q).$$

For our construction we pick q sufficiently large such that $1/A(q) < \varepsilon_0/4$, and set $R = 2/A(q)$. Then $R + 1/A(q) < 3\varepsilon_0/4$ and $R - 1/A(q) \geq 1/A(q)$, so if k is sufficiently large, there is a set of vectors $W \subset \mathbb{F}_q^k$ with the desired properties. □

Remark 9 An alternative construction can be obtained via asymptotically-good self-dual codes [31, Theorem 1.6], which also works for large enough q. For $q = 2$ there is another construction of self-dual codes given in [8], motivated by quantum error correction, that we can use.

3 The Hypergraph of Linear Combinations

Given a set $U \subset \mathbb{F}_q^k$, we denote by $\operatorname{span}(U)$ or $\langle U\rangle$ the linear subspace spanned by U, and $\dim(U)$ denotes the dimension of $\operatorname{span}(U)$. Say that a linear combination $a_1v_1 + \cdots + a_rv_r$ of the set of vectors $\{v_1,\ldots,v_r\}$ is *proper* if none of the coefficients a_i is equal to 0.

Given a set of vectors $W \subset \mathbb{F}_q^k$ and a target set $R \subset \mathbb{F}_q^k$, we associate the pair (W,R) with a hypergraph as follows.

Definition 4 (Proper linear combination hypergraph) For $W, R \subset \mathbb{F}_q^k$, let $H_{W\to R}$ be the hypergraph whose vertex set is W, and a subset $X \subset W$ forms an edge if there is a proper linear combination of the elements of X contained in R. We refer to this hypergraph as the *proper linear combination hypergraph* of (W, R).

Definition 5 (Proper span) Given a hypergraph H on vertex set $W \subset \mathbb{F}_q^k$, the *proper span* of H, denoted by $\mathrm{pspan}(H)$, is the set of all $v \in \mathbb{F}_q^k$ such that v can be written as a proper linear combination of the elements of an edge of H.

With these definitions in hand, our aim in this section is to prove that for certain tree-like hypergraphs H, if H is a subhypergraph of $H_{W\to R}$, then $\mathrm{pspan}(H) \cap R$ spans a subspace of large dimension in R. To this end, we first define our notion of tree-like hypergraphs.

Definition 6 (s-tree-like hypergraph) Given a positive integer s, a hypergraph is *s-bounded* if the size of every edge is at most s. A hypergraph H is *s-tree-like* if it is s-bounded and there is an ordering $v_1, \dots, v_n$ of the vertices of H such that the vertex v_i in the subhypergraph of H induced on $\{v_i, \dots, v_n\}$ has degree 1 for $i = 1, \dots, n - s + 1$.

The main lemma of this section is the following.

Lemma 10 *Let $W, R \subset \mathbb{F}_q^k$. If $H_{W\to R}$ contains an s-tree-like subhypergraph H on vertex set U, then*

$$\dim(\mathrm{pspan}(H) \cap R) \geq \dim(U) - s + 1.$$

Proof Let $v_1, \dots, v_n$ be an ordering of U satisfying that the vertex v_ℓ in the subhypergraph of H induced on $\{v_\ell, \dots, v_n\}$ has degree 1 for $\ell = 1, \dots, n - s + 1$. Let e_ℓ denote the unique edge containing v_ℓ contained in $\{v_\ell, \dots, v_n\}$. Define the $(n - s + 1) \times n$ sized matrix M over $\mathbb{F}_q$ as follows. As e_ℓ is an edge of $H_{W\to R}$, there exist coefficients $a_1, \dots, a_n \in \mathbb{F}_q^n$ such that $\sum_{i=1}^n a_i v_i \in R$, and $a_i \neq 0$ if and only if $v_i \in e_\ell \subset \{v_\ell, \dots, v_n\}$. Set $M(\ell, i) = a_i$.

Then M is an upper triangular matrix such that $M(\ell, \ell) \neq 0$ for $\ell = 1, \dots, n-s+1$, thus $\mathrm{rank}(M) = n - s + 1$. Let N be the $n \times k$ matrix, whose rows are the vectors $v_1, \dots, v_n$. Then $\mathrm{rank}(N) = \dim(U)$ and the rows of the matrix $M \cdot N$ are elements of $\mathrm{pspan}(H) \cap R$. Thus,

$$\dim(\mathrm{pspan}(H) \cap R) \geq \mathrm{rank}(M \cdot N) \geq \mathrm{rank}(M) + \mathrm{rank}(N) - n = \dim(U) - s + 1.$$

Here, the second inequality is due to Sylvester's rank inequality. □

4 Constructions of Strong Blocking Sets

4.1 Codimension 2

As a warm-up, in this section, we present an explicit construction of a strong 2-blocking set of size $O(q^2k)$ for every sufficiently large prime power q and sufficiently large k.

Given a set $B \subset \mathbb{F}_q^k$, let $\tilde{B} \subset PG(k-1, q)$ denote $B/\sim$, where $x \sim y$ if $x = cy$ for some $c \neq 0$.

Construction. Let $\alpha := 1/8$ and $d = 258$, then $d-1$ is a prime congruent to 1 modulo 4. Let $\lambda := 2\sqrt{d-1} \approx 32.06$, and note that $\alpha > \lambda/d$ is satisfied.

- Assume that q is a prime power sufficiently large to satisfy the requirements of Lemma 8 with $s = 2$ and $\varepsilon_0 = \alpha/2$. That is, there is an explicit construction $W_0 \subset \mathbb{F}_q^k$ of $n_0 = O(k)$ vectors such that any subset of W_0 of size at least $\alpha n_0/2$ spans $\mathbb{F}_q^k$, and any three vectors in W_0 are linearly independent.
- Let $n_0 \geq n = (1 + o(1))n_0$ for which there is an explicit construction G of an (n, d, λ)-graph. This exists by Lemma 1. Associate the vertices of G with an arbitrary n element subset W of W_0. Note that any αn elements of W span $\mathbb{F}_q^k$, and any 3 elements of W are linearly independent.
- A *cherry* in G is a 3 element set $\{x, y, z\}$ such that $xy, xz \in E(G)$. Let H be the 3-uniform hypergraph, whose edges are the cherries of G.
- Let $B = \bigcup_{f \in E(H)} \text{span}(f)$.

Theorem 11 *$\tilde{B}$ is a strong 2-blocking set of size $O(q^2k)$ in $PG(k-1, q)$.*

Proof As G is d-regular, it contains at most nd^2 cherries, so $|B| \leq q^3nd^2 = O(q^3n)$. Therefore, $|\tilde{B}| = O(q^2k)$.

Next, we prove that for every $(k-2)$-dimensional subspace $L < \mathbb{F}_q^k$, the set $L \cap B$ spans L. Define the hypergraph F on vertex set W as follows: for every cherry $\{x_1, x_2, x_3\}$, there exists at least one non-zero point $a_1x_1 + a_2x_2 + a_3x_3$ in L for some $a_1, a_2, a_3 \in \mathbb{F}_q$. Here, we are using that any three elements of W are linearly independent. Add to the hypergraph F the set $\{x_i : a_i \neq 0\}$ as an edge. Then F is 3-bounded, and each cherry contributes a 1, 2, or 3 element edge to F. Furthermore, $\text{pspan}(F) \subset B$ and F is a subhypergraph of the proper linear combination hypergraph $H_{W \to L}$.

Let $A \subset W$ be the set of one-element edges of F. Then $|A| < \alpha n$, otherwise $\dim(A) = k$, which is impossible as $A \subset L$. Let G' be the subgraph of G composed of those edges, that are also edges of F. Then G' has no component of size more than αn. Indeed, otherwise, if T is a tree of size αn in G', then T is a 2-tree-like subhypergraph of F satisfying $\dim(V(T)) = k$. Hence, by Lemma 10,

$$\dim(\text{pspan}(F) \cap L) \geq \dim(V(T)) - 1 > \dim(L),$$

contradiction. As G' has no component of size at least αn, Lemma 3 implies that $e(G') \leq \alpha dn$.

Finally, let G^* be the subgraph of G composed of those edges that are disjoint from A, and are not contained in G'. Then

$$e(G^*) \geq e(G) - |A|d - e(G') \geq \frac{dn}{2} - \alpha dn - \alpha dn \geq \frac{dn}{4}.$$

Using Lemma 3 again, we conclude that G^* contains a connected component of size at least $n/4$. Let T be a spanning tree of G^* and let $y_1, \ldots, y_m$ be an enumeration

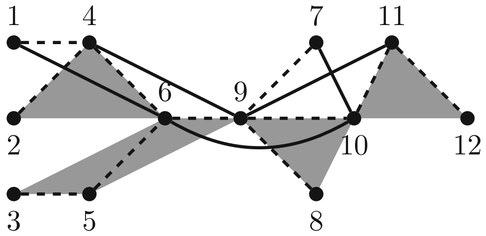


Fig. 1 An illustration of a 3-tree-like subhypergraph K we might find. The dashed edges are the edges of the tree T, while the black and gray edges (which have size 2 and 3, respectively) are the edges of K. The edges of K in order are $\{1, 6\}$, $\{2, 4, 6\}$, $\{3, 5, 6\}$, $\{4, 9\}$, $\{5, 6, 9\}$, $\{6, 10\}$, $\{7, 10\}$, $\{8, 9, 10\}$, $\{9, 11\}$, $\{10, 11, 12\}$.

of the vertices of T such that y_i is a leaf of the subtree $T[y_i, \dots, y_m]$. We define a 3-tree-like subhypergraph K of F as follows. For every $i \in \{1, \dots, n-2\}$, there exists $i < j < j'$ such that $y_i y_j$ and $y_j y_{j'}$ are edges of T. But then $\{y_i, y_j, y_{j'}\}$ is a cherry of G, and none of the sets $\{y_i\}$, $\{y_j\}$, $\{y_{j'}\}$, $\{y_i, y_j\}$, $\{y_j y_{j'}\}$ is an edge of F, so at least one of $\{y_i, y_{j'}\}$ or $\{y_i, y_j, y_{j'}\}$ is an edge of F. Add this edge to K. Then, K is 3-tree-like on vertex set $\{y_1, \dots, y_m\} \subset W$, where $m \geq n/4 > \alpha n$, so

$$\dim(\text{pspan}(K) \cap L) \geq \dim(K) - 2 = k - 2,$$

by Lemma 10. In conclusion, $\text{pspan}(K) \cap L \subset B \cap L$, thus $B \cap L$ spans L. See Figure 1 for an illustration of K. □

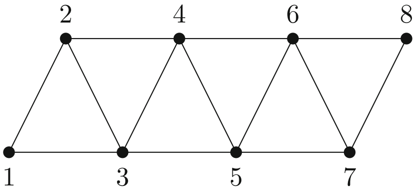
4.2 Explicit constructions via size-Ramsey numbers

In this section, we present an explicit construction of a strong s-blocking set of size $O_s(q^s k)$ in $PG(k-1, q)$, assuming q is sufficiently large with respect to s. Here, the constant hidden by the $O_s(.)$ notation is astronomical as a function of s, which will be greatly improved in Section 4.3 by a different construction. However, the construction presented in this section highlights some interesting connections to extremal combinatorics, in particular to the theory of *size-Ramsey numbers*, so we believe it is beneficial to present it.

Given r-uniform hypergraphs G, H_1, H_2, we write $(H_1, H_2) \to G$ if for any coloring of the edges of G with red or blue, G contains either a red copy of H_1 or a blue copy of H_2. The *size-Ramsey number* of (H_1, H_2) is the smallest number of edges in an r-uniform hypergraph G for which $(H_1, H_2) \to G$, and it is denoted by $\hat{r}(H_1, H_2)$. In case $H_1 = H_2 = H$, we may write simply $H \to G$ instead of $(H, H) \to G$, and $\hat{r}(H)$ instead of $\hat{r}(H, H)$.

This notion was first introduced by Erdős, Faudree, Rousseau and Schelp in 1978 [18] as a natural extension of the usual hypergraph Ramsey numbers. We highlight that the traditional Ramsey number $r(H_1, H_2)$ of (H_1, H_2) is the minimal number of vertices in a graph G for which $(H_1, H_2) \to G$ (in which case we can always assume that G is a complete graph). One of the earliest results concerning size-Ramsey numbers is due to Beck [10], who showed that if P_n is the path of length n, then

Fig. 2 An illustration of a 3-uniform tight path of length 6.



$\hat{r}(P_n) = O(n)$. In the past four decades, this area went through tremendous growth, and the following theorem of Letzter, Pokrovskiy, and Yepremyan [26] generalizes a long list of results in the topic. The r-uniform *tight path* of length ℓ, denoted by $P_{r,\ell}$, is a sequence of $\ell+r-1$ vertices $v_1, \dots, v_{\ell+r-1}$ such that $\{v_i, \dots, v_{i+r-1}\}$ is an edge for $i = 1, \dots, \ell$. See Figure 2 for an illustration. The *t-power* of such a tight path, denoted by $P^t_{r,\ell}$, is the r-uniform hypergraph whose edges are all the r-sets contained in some interval of length $r + t - 1$ among $v_1, \dots, v_{\ell+r-1}$.

In [26], it is proved that for every r, t, there exists $C = C(r, t) > 0$ such that

$$\hat{r}(P^t_{r,n}) \le Cn.$$

For our applications, we need bounds on the size-Ramsey number of $(P_{r,n}, K_{r,t})$, where $K_{r,t}$ denotes the r-uniform clique of size t. However, noting that $P^t_{r,n}$ contains both $P_{r,n}$ and $K_{r,t}$, we get the following immediate corollary of the previous theorem. For every r, t, there exists $C = C(r, t) > 0$ such that

$$\hat{r}(P_{r,n}, K_{r,t}) \le Cn.$$

Moreover, one can explicitly define a hypergraph H with at most Cn edges such that every two coloring of the edges of H contains a monochromatic copy of $P^t_{r,n}$. Given a graph G, let G^u be the u-power of G, that is, any two vertices of distance at most u are joined by an edge. Also, $G[K_D]$ denotes the D-blow-up of G, which is the graph in which every vertex is replaced by a clique of size D, and if there is an edge between two vertices in G, then all edges are drawn between the corresponding cliques of $G[K_D]$. We also use $K_r(G)$ to denote the r-uniform hypergraph, whose edges are the r-cliques of G. Let G be an ε-expander, which is defined to be a graph that satisfies that between any pair of vertex sets of size at least $\varepsilon \cdot v(G)$, there is an edge. By the Expander Mixing lemma, (n, d, λ)-expanders satisfy this property with $\varepsilon = \lambda/d$. The following is a (very) special subcase of Theorem 6.1 in [26], where we only use that $P^t_{r,\ell}$ contains both a tight path of length ℓ, and a clique of size t.

Theorem 12 *Let r, t be integers, then if ε^{-1} and Δ are sufficiently large with respect to r, t, and α, u, D are sufficiently large with respect to ε, Δ, the following holds. Let n be an integer, let G be an ε-expander on at least αn vertices of maximum degree Δ, and let $H = K_r(G^u[K_D])$. Then*

$$(P_{r,n}, K_{r,t}) \to H.$$

We point out that if G has maximum degree d, then $v(H) = Dv(G)$ and $e(H) \leq (2d)^{ur}v(H)$. Unfortunately, the dependence of the parameters $\varepsilon, \Delta, \alpha, u, D$ on r and t is quite poor. While in [26] there are no explicit dependencies calculated, these parameters grow at least as fast as the usual Ramsey number of an r-uniform clique of size t. This number is at least $2^{2^{\cdots 2^{\Omega(t)}}}$, where the tower is of height $r - 2$.

To construct our strong s-blocking set in $\mathbb{F}_q^k$, we consider the $(s+1)$-uniform hypergraph H given by the previous theorem (with parameters t, n chosen appropriately with respect to s and k) and associate its vertices with certain vectors in $\mathbb{F}_q^k$. Then our strong s-blocking set B is the set of all linear combinations of the edges of H. Given a hyperplane L of codimension s, L defines a two coloring on the edges, where an edge is colored red if there is a proper linear combination of the vertices of the edge contained in L, otherwise it is colored blue. In our next lemma, we show that if any $s + 1$ vertices of H are linearly independent, then this coloring cannot contain a large blue clique.

Lemma 13 *For every positive integer s, there exists $R = R(s)$ such that the following holds for every prime power q larger than s. Let $U \subset \mathbb{F}_q^k$ be a set of R vectors such that every $s + 1$ elements of U are linearly independent. If L is an s-codimensional subspace of $\mathbb{F}_q^k$, then $H_{U\to L}$ contains an edge of size exactly $s + 1$.*

Proof We show that $R = (s + 2)!$ suffices. Assume that $H_{U\to L}$ contains no edge of size $s + 1$. For every $1 \leq \ell \leq s$, let F_ℓ be the ℓ-uniform hypergraph formed by the ℓ-element edges of $H_{U\to L}$. □

Claim 14 F_ℓ contains no set of edges whose union has size $s + 1$.

Proof Assume to the contrary that $e_1, \ldots, e_m \in E(F_\ell)$ such that $|e_1 \cup \cdots \cup e_m| = s+1$. Then for every $i = 1, \ldots, m$ and $x \in e_i$ there exists $a_{i,x} \in \mathbb{F}_q \setminus \{0\}$ such that

$$y_i = \sum_{x\in e_i} a_{i,x}x \in L.$$

But then for arbitrary $b_1, \ldots, b_m \in \mathbb{F}_q$, we also have

$$\sum_{i=1}^{m} b_i y_i = \sum_{x\in e_1\cup\cdots\cup e_m} \left(\sum_{i:x\in e_i} b_i a_{i,x} \right) \cdot x \in L.$$

Using our assumption $q > s$, we can choose $b_1, \ldots, b_m$ such that none of the coefficients $\sum_{i:x\in e_i} b_i a_{i,x}$ is 0. Indeed, choosing $b_1, \ldots, b_m$ randomly from the uniform distribution on $\mathbb{F}_q$, the probability that $\sum_{i:x\in e_i} b_i a_{i,x} = 0$ is $1/q$, so with probability at least $1 - s/q$, none of the coefficients are 0. This is a contradiction, as then L contains a proper linear combination of the elements of $e_1 \cup \cdots \cup e_m$, so $e_1 \cup \cdots \cup e_m$ is an $s + 1$ element edge of $H_{U\to R}$. □

In particular, the previous claim implies that F_ℓ contains no $(s+2-\ell)$-star, that is, $s+2-\ell$ edges, all of which intersect in a set of size $\ell-1$. As the number of $(\ell-1)$-sets is $\binom{R}{\ell-1}$, this gives

$$e(F_\ell) \leq (s+1-\ell)\binom{R}{\ell-1} \leq s\binom{R}{\ell-1}.$$

Let H_ℓ be the $(s+1)$-uniform hypergraph of those edges e which contain some edge of F_ℓ. Then

$$e(H_\ell) \leq \binom{R-\ell}{s+1-\ell} e(F_\ell) \leq s\binom{R}{\ell-1}\binom{R-\ell}{s+1-\ell} \leq R^s.$$

Therefore, the total number of edges in the union of $H_1, \dots, H_s$ is at most sR^s. Hence, if $R=(s+2)!$, then $sR^s < \binom{R}{s+1}$, which means that some $(s+1)$-element set $f \subset U$ is not an edge of any of the $H_1, \dots, H_s$. In other words, no linear combination of elements of f is contained in L. But as the element of f span a subspace of dimension $s+1$, this is impossible, contradiction.

After these preparations, let us present our construction in detail.

Construction. Let $t=R$ be given by Lemma 13, let $r=s+1$, and let $\varepsilon, \alpha > 0$ and integers u, D be given by Theorem 12. Let $d=p+1$, where p is the smallest prime congruent to 1 mod 4 larger than $16/\varepsilon^2$, and let $\lambda = 2\sqrt{d-1}$. Note that $\lambda/d < \varepsilon$.

- Let q be a prime power and k be an integer, both sufficiently large such that Lemma 8 holds with $\varepsilon_0 = 1/(2D\alpha)$. That is, there is a set $W_0 \in \mathbb{F}_q^k$ of $m_0 = O_{s,\varepsilon_0}(k)$ vectors such that any $m_0/(2D\alpha)$ elements of W_0 span $\mathbb{F}_q^k$, and any $s+1$ are linearly independent.
- Let $n_0 = m_0/D$, and let G be an explicit construction of an (n,d,λ)-graph for some $n_0 > n = (1+o(1))n_0$. This exists by Lemma 1. Note that G is an ε-expander.
- Let $H = K_r(G^u[K_D])$, then $m := v(H) = Dn > m_0/2$. Associate an m element subset W of W_0 arbitrarily with the vertices of H. Write $\ell = m/(\alpha D)$, and note that any ℓ elements of W span $\mathbb{F}_q^k$, and any $s+1$ are linearly independent. Moreover, $(P_{r,\ell}, K_{r,t}) \to H$.
- Let $B = \bigcup_{f\in E(H)} \operatorname{span}(f)$.

Theorem 15 *$\tilde{B}$ is a strong s-blocking set of size $O_s(q^s k)$ in $PG(k-1,q)$.*

Proof The parameters $t, r, \varepsilon, \alpha, u, D, d$ only depend on s, which implies that $m = O_s(k)$. Hence, $|B| \leq |E(H)|q^{s+1} \leq (2d)^{ur}m = O_s(q^{s+1}k)$ and $\tilde{B} = O_s(q^s k)$.

We show that for every s-codimensional subspace $L < \mathbb{F}_q^k$, $B \cap L$ spans L. Color each edge $f \in E(H)$ with red or blue as follows. If there is a proper linear combination of the elements of f that is contained in L, then color f red, otherwise color f blue. Note that the red edges are also edges of $H_{W\to L}$. By Lemma 13, this coloring contains no blue clique of size t. Hence, H must contain a red tight path P of size ℓ. Then

$\dim(V(P)) = k$, as any ℓ elements of $V(H)$ span $\mathbb{F}_q^k$. But a tight path is also an r-tree-like hypergraph, hence Lemma 10 implies that

$$\dim(\mathrm{pspan}(H) \cap L) \geq \dim(V(P)) - r + 1 = k - s.$$

Hence, as $\mathrm{pspan}(H) \subset B$, we conclude that $B \cap L$ spans L. □

4.3 Optimal constructions for large primes

In this section, we present our best construction of a strong s-blocking set, assuming q is sufficiently large with respect to s.

Construction. Let $r = s + 1$, and let $d = p + 1$, where p is the smallest prime congruent to 1 mod 4 such that $p > 64r^2$, and let $\lambda = 2\sqrt{d-1}$.

- Let q be a prime power and k be an integer, both sufficiently large such that Lemma 8 holds with $\varepsilon_0 = 1/(8rd^r)$. That is, there is a set $W_0 \subset \mathbb{F}_q^k$ of $n_0 = O_{s,\varepsilon}(k)$ vectors such that any r elements of W_0 are linearly independent, and any $n_0/(8rd^r)$ elements of W_0 span $\mathbb{F}_q^k$.
- Let $n_0 > n = (1 + o(1))n_0$ be such that there exists an (n, d, λ)-graph G. This exists by Lemma 1. Let W be an n element subset of W_0, and assign the elements of W to the vertices of G. Note that any $n/(4rd^r)$ elements of W span $\mathbb{F}_q^k$.
- Let $H = K_r(G^r)$, that is, the edges of H are those r-tuples, whose every vertex is within distance at most r from some vertex $x \in V(G)$. Note that $e(H) \leq nd^{r^2}$.
- Let $B = \bigcup_{f \in E(H)} \mathrm{span}(f)$.

Theorem 16 *$\tilde{B}$ is a strong s-blocking of size $2^{O(s^2 \log s)}kq^s$ in $PG(k-1, q)$.*

Proof The size of B is at most $e(H)q^{s+1} \leq nd^{r^2}q^{s+1} = 2^{O(s^2 \log s)}kq^{s+1}$. Hence, $|\tilde{B}| = 2^{O(s^2 \log s)}kq^s$.

We show that if $L \subset \mathbb{F}_q^k$ has codimension s, then $L \cap B$ spans L. For an integer t and vertex $x \in V(G)$, let $B_t(x)$ denote the set of vertices of G of distance at most t from x. Given an integer $\ell \in [r]$ and a vertex $x \in V(G)$, say that

(i) x is *ℓ-full* if for every ℓ-tuple of vertices $f \subset B_{\ell-1}(x)$, the span of f intersects L non-trivially.

Observe that every vertex x is $(s+1)$-full, as L has codimension s. Also, a vertex is 1-full if and only if $x \in L$. If a vertex x is 1-full, color it with color 1, otherwise, color x with an integer $\ell \in \{2, \ldots, s+1\}$ such that x is ℓ-full, but not $(\ell-1)$-full. Then every vertex is colored with some color. Therefore, there exists a color $\ell \in [r]$ such that the set of vertices $U_0 \subset V(G)$ of color ℓ has size at least n/r. If $\ell = 1$, it means that every element of U_0 is contained in L. But every n/r vertices of $V(G)$ span $\mathbb{F}_q^k$, a contradiction. Hence, we may assume that $\ell \geq 2$. As $|U_0| \geq n/r \geq 4\lambda n/d$, we can apply Lemma 4 to find $U \subset U_0$ of size at least $n/r - \frac{2\lambda n}{d} \geq n/(2r)$ such that $G[U]$ is connected. Let $|U| = m$, let T be a spanning tree of $G[U]$, and let $x_1, \ldots, x_m$ be an enumeration of the elements of U such that x_i is a leaf in the subtree $T[x_i, \ldots, x_m]$.

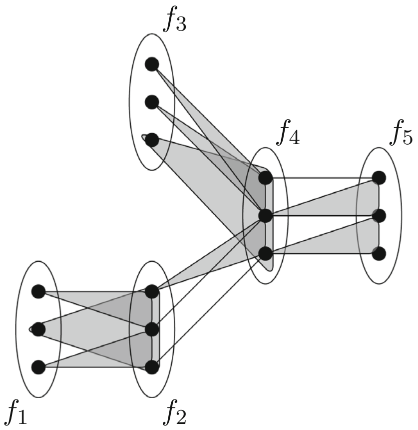


Fig. 3 An illustration for the proof of Theorem 16. An example of an $\ell = 4$-tree-like hypergraph we might build on the union of the edges $f_1, \dots, f_5$.

As x_i is not $(\ell - 1)$-full, there exists an $(\ell - 1)$-tuple $f_i \subset B_{\ell-2}(x_i)$ such that the span of f_i intersects L trivially. Let $F = \bigcup_{i=1}^{m} f_i$. Note that the sets $f_1, \dots, f_m$ are not necessarily disjoint. However, f_i is contained in $B_{\ell-2}(x_i)$, hence f_i and f_j are disjoint if the distance of x_i and x_j is more than $2(\ell - 2)$. The number of vertices of distance at most $2\ell - 4$ is at most $d^{2\ell-4}$, so U contains at least $|U|/d^{2\ell-4} \geq |U|/d^{2s}$ vertices, any pair of which are at distance more than $2\ell - 4$. This implies $|F| \geq |U|/d^{2s} \geq n/(4rd^{2s})$, so the elements of F span $\mathbb{F}_q^k$.

We show that $H_{W \to L}[F]$ contains an ℓ-tree-like spanning subhypergraph. For $i = 1, \dots, m$, let $F_i = f_m \cup f_{m-1} \cup \dots \cup f_{m-i+1}$. Let H_1 be the empty hypergraph on vertex set $F_1 = f_m$, then H_1 is ℓ-tree-like. Having already constructed an ℓ-tree-like hypergraph H_i on vertex set F_i for some $i \in [m-1]$, we construct H_{i+1} as follows. As x_{m-i} is a leaf in $T[x_{m-i}, \dots, x_m]$, it has a unique neighbour x_z in this tree with $z \in \{m - i + 1, \dots, m\}$. For every $y \in f_{m-i} \setminus F_i$, consider the ℓ-tuple $g = \{y\} \cup f_z$. Here, $y \in f_{m-i} \subset B_{\ell-2}(x_{m-i})$, but x_{m-i} is a neighbour of x_z, so $y \in B_{\ell-1}(x_z)$ as well. Also, $f_z \subset B_{\ell-2}(x_z)$, so $g \subset B_{\ell-1}(x_z)$. Thus, by (i), there is a non-zero linear combination of elements of g contained in L. Let $g'_y \subset g$ be such that a proper linear combination of elements of g'_y is in L, then g'_y is an edge of $H_{W \to L}[F]$. Also, me must have $y \in g'_y$, otherwise $g'_y \subset f_z$, contradicting that the span f_z intersects L trivially. Define H_{i+1} to be the hypergraph on $F_{i+1} = F_i \cup f_{m-i}$ we get by adding the edges g'_y to H_i for every $y \in f_{m-i} \setminus F_i$. Then H_{i+1} is an ℓ-tree-like subhypergraph spanning $H_{W \to L}[F_{i+1}]$. In conclusion, H_m is an ℓ-tree-like subhypergraph of $H_{W \to L}$ on vertex set $F_m = F$. But then by Lemma 10,

$$\dim(\mathrm{pspan}(H_m) \cap L) \geq \dim(F) - \ell + 1 = k - \ell + 1.$$

This is impossible if $\ell \leq s$, as the dimension of L is $k - s$. Therefore, we must have $\ell = s + 1$, in which case the previous inequality tells us that $B \cap L$ spans L. See Figure 3 for an illustration of the ℓ-tree-like hypergraph H_m. □

4.4 Optimal constructions for small primes

Finally, we present our construction for small prime powers q. In this setting, our goal is to show that there is an explicit strong s-blocking set of size $O_{s,q}(k)$, as we imagine q being bounded by some function of s.

Construction. Let $r = s+1$, let $\varepsilon = \delta/2$, where δ is given by Lemma 7. Let $d = p+1$, where p is the smallest prime congruent to 1 modulo 4 larger than $16q^{4s}/\varepsilon^2$. Let $\lambda = 2\sqrt{d-1}$, then $\lambda/d < \varepsilon/(2q^{2s})$.

- Assume that k is sufficiently large satisfying the requirements of Lemma 7, and sufficiently large with respect to q. Let $W_0 \subset \mathbb{F}_q^k$ be a set of $n_0 = O(k)$ vectors such that any $(1-\delta)n_0$ elements of W_0 spans $\mathbb{F}_q^k$.
- Let $n_0 > n = (1+o(1))n_0$ for which there is an explicit (n, d, λ)-graph G. This exists by Lemma 1 (here, we are using the assumption that k is sufficiently large with respect to q, so n is sufficiently large with respect to d). Let W be an arbitrary n element subset of W_0, and associate the elements of W to the vertices of G. Note that any $(1-\varepsilon)n$ elements of W span $\mathbb{F}_q^k$.
- Let H be the r-uniform hypergraph on vertex set W, where $f \in W^{(r)}$ is an edge if there is some $x \in W$ such that every element of f is within distance at most one from x in G.
- Let $B = \bigcup_{f\in H} \mathrm{span}(f)$.

Theorem 17 *$\tilde{B}$ is a strong s-blocking set of size $q^{O(s^2)}k$ in $P(k-1, q)$.*

Proof The size of B is at most $q^{s+1}e(H) \le q^{s+1}(2d)^r n \le q^{O(s^2)}k$, so $|\tilde{B}| = q^{O(s^2)}k$ as well.

We show that if $L < \mathbb{F}_q^k$ has codimension s, then $B \cap L$ spans L. Let $w_1, \ldots, w_s$ be a basis of the orthogonal complement of L. For every $z \in \mathbb{F}_q^s$, let $U_z \subset V(G)$ be the set of vertices $x \in V(G)$ such that $\langle x, w_i\rangle = z(i)$. Then U_z is the intersection of W with a coset of L. In particular, the sets U_z for $z \in \mathbb{F}_q^s$ partition $V(G)$ into q^s parts, and $U_0 = L \cap W$. Observe that for every z, if $x, y \in U_z$, then $x - y \in L$. Hence, if $z \ne 0$, then $\{x, y\}$ is an edge of the proper linear combination hypergraph $H_{W\to L}$. In particular, every edge of $G[U_z]$ is an edge of $H_{W\to L}$. In general, we observe that if $x_1 \in U_{z_1}, \ldots, x_u \in U_{z_u}$, then a linear combination $a_1x_1 + \cdots + a_ux_u$ is contained in L if and only if $a_1z_1 + \cdots + a_uz_u = 0$.

Let $b = \lambda n/d$, and let $S \subset \mathbb{F}_q^s$ be the set of vectors z such that $|U_z| > (q^s+2)b$. Furthermore, let $V_z \subset U_z$ be the vertex set of the largest component of $G[U_z]$, then $|V_z| \ge |U_z| - 2b > q^s b$ by Lemma 4. Let $V' = \bigcup_{z\in S} V_z$, then

$$\begin{aligned}|V'| &= \sum_{z\in S}|V_z| \ge n - \sum_{z\notin S}|U_z| - \sum_{z\in S} 2b \ge n - q^s(q^s+2)b - 2bq^s\\ &> n(1 - 2q^{2s}\lambda/d) \ge n(1-\varepsilon).\end{aligned}$$

Therefore, V' spans $\mathbb{F}_q^k$. Next, our goal is to construct an r-tree-like subhypergraph of $H_{W\to L}$, whose every edge is contained in some edge of H.

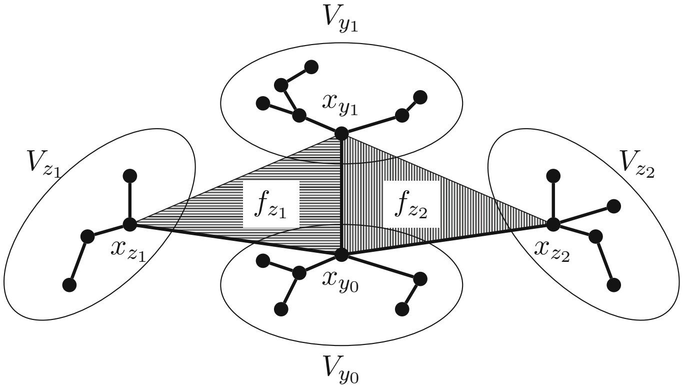


Fig. 4 An illustration for the proof of Theorem 17.

If S only contains the zero vector, then $V' = V_0$, and $V' \subset L$, which contradicts that L does not span the whole space. Hence, we may assume that S contains at least one non-zero vector. Let $Y \subset S$ be a basis of the subspace of $\mathbb{F}_q^s$ spanned by S. So $1 \leq |Y| \leq s$, and select an arbitrary $y_0 \in Y$. Apply Lemma 5 to the sets $(V_z)_{z \in S}$ with V_{y_0} playing the role of V_0. We have $|V_z| \geq |S|\lambda n/d$ for every $z \in S$, so the condition of Lemma 5 is satisfied. Hence, there exists a vertex $x_{y_0} \in V_{y_0}$ such that for every $z \in S \setminus \{y_0\}$, there exists some $x_z \in V_z$ such that $\{x_{y_0}, x_z\}$ is an edge of G. Now for every $z \in S \setminus Y$, the $|Y| + 1$ vectors z, $\{y\}_{y \in Y}$ are linearly dependent. More precisely, there is a linear combination summing to zero, where the coefficient of z is not zero. Hence, $H_{W \to L}$ contains an edge f_z such that $x_z \in f_z \subset \{x_z\} \cup \{x_y : y \in Y\}$. Observe that f_z is also a subset of some edge of H. The union of these edges f_z for $z \in S \setminus Y$ is an $(|Y| + 1)$-tree-like subhypergraph of $H_{W \to L}$, whose union is the set of vertices $\{x_z : z \in S\}$. In order to cover the rest of the vertices of V', we observe that $G[V_z]$ has a spanning tree T_z. But then there is an enumeration $v_1, \dots, v_{|V_z|}$ of the vertices of T_z such that v_i is a leaf in $T_z[v_i, \dots, v_{|V_z|}]$, and $v_{|V_z|} = x_z$. Now the edges f_z for $z \in S \setminus Y$ together with the edges of the trees T_z for $z \in S$ form an $(|Y| + 1)$-tree-like subhypergraph H_0 of $H_{W \to L}$ on vertex set V'. This is witnessed by any ordering of V' in which the vertices $\{x_y : y \in Y\}$ come last, preceded by any ordering of $\{x_z : z \in S \setminus Y\}$, and before that any ordering of the rest of the vertices which respects the orderings of the trees T_z. See Figure 4 for an illustration.

The proper span of H_0 is contained in B, and by Lemma 10,

$$\dim(\text{pspan}(H_0) \cap L) \geq \dim(V') - (|Y| + 1) + 1 \geq k - s.$$

Therefore, we must have $|Y| = s$, and $B \cap L$ spans L, finishing the proof. □

Acknowledgements We would like to thank the organizers of DiGReSS workshop at Umeå, 2024, where this research was initiated. Also, we would like to thank Peter Beelen, Alessandro Neri, and Tovohery H. Randrianarisoa for valuable discussions, and the anonymous referee for many useful comments and suggestions.

References

1. Alfarano, G.N., Borello, M., Neri, A.: A geometric characterization of minimal codes and their asymptotic performance. Adv. Math. Commun. **16**(1), 115–133 (2022)
2. Alfarano,G. N., Borello,M., Neri,A.: Outer strong blocking sets. Preprint arXiv:2301.09590 (2023)
3. Alfarano, G.N., Borello, M., Neri, A., Ravagnani, A.: Three combinatorial perspectives on minimal codes. SIAM J. Discrete Math. **36**(1), 461–489 (2022)
4. Alon, N.: Explicit expanders of every degree and size. Combinatorica **41**, 447–463 (2021)
5. Alon, N., Bishnoi, A., Das, S., Neri, A.: Strong blocking sets and minimal codes from expander graphs. Trans. Amer. Math. Soc. **377**, 5389–5410 (2024)
6. Alon, N., Bruck, J., Naor, J., Naor, M., Roth, R.M.: Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. IEEE Trans. Inf. Theory **38**(2), 509–516 (1992)
7. Alon, N., Chung, F.R.K.: Explicit construction of linear sized tolerant networks. Discret. Math. **72**(1–3), 15–19 (1988)
8. Ashikhmin, A., Litsyn, S., Tsfasman, M.A.: Asymptotically good quantum codes. Phys. Rev. A **63**, 032311 (2001)
9. Ball,S.: The polynomial method in Galois geometries. In Current Research Topics in Galois Geometry, J. De Beule and L. Storme (eds.), Nova Sci. Publ. (2011): 105–130, Chapter 5
10. Beck, J.: On size Ramsey number of paths, trees, and circuits. I. J. Graph Theory **7**, 115–129 (1983)
11. Beelen,P.: A survey on recursive towers and Ihara's constant. Preprint arXiv:2203.03310 (2022)
12. Bishnoi,A., D'haeseleer, J., Gijswijt,D., Potukuchi,A.: Blocking sets, minimal codes and trifferent codes. J. Lond. Math. Soc. 109 (6) (2024): e12938
13. Blokhuis,A., Sziklai,P., Szonyi,T.: Blocking sets in projective spaces. In Current Research Topics in Galois Geometry, Nova Sci. Publ., New York, NY, USA (2011): 61–84
14. Bonini, M., Borello, M.: Minimal linear codes arising from blocking sets. J. Algebr. Comb. **53**, 327–341 (2021)
15. Brouwer, A.E., Schrijver, A.: The blocking number of an affine space. J. Comb. Theory Ser. A **24**(2), 251–253 (1978)
16. Couvreur, A., Randriambololona, H.: Algebraic geometry codes and some applications, pp. 307–362. Chapman and Hall/CRC, In Concise Encyclopedia of Coding Theory (2021)
17. Davydov, A.A., Giulietti, M., Marcugini, S., Pambianco, F.: Linear nonbinary covering codes and saturating sets in projective spaces. Adv. Math. Commun. **5**(1), 119–147 (2011)
18. Erdős, P., Faudree, R.J., Rousseau, C.C., Schelp, R.H.: The size Ramsey number. Period. Math. Hungar. **9**, 145–161 (1978)
19. Fancsali,S., Sziklai,P.: Lines in higgledy-piggledy arrangement. Electron. J. Comb. 21 (2014)
20. Fancsali, S.L., Sziklai, P.: Higgledy-piggledy subspaces and uniform subspace designs. Des. Codes Cryptogr. **79**, 625–645 (2016)
21. Guruswami, V., Kopparty, S.: Explicit subspace designs. Combinatorica **36**(2), 161–185 (2016)
22. Héger, T., Nagy, Z.L.: Short minimal codes and covering codes via strong blocking sets in projective spaces. IEEE Trans. Inf. Theory **68**(2), 881–890 (2021)
23. Hoory, S., Linial, N., Wigderson, A.: Expander graphs and their applications. Bull. Am. Math. Soc. **43**(4), 439–561 (2006)
24. Høholdt,T., Van Lint,J. H., Pellikaan,R.: Algebraic geometry codes. Handbook of Coding Theory 1 (Part 1) (1998): 871–961. Elsevier Amsterdam
25. Justesen, J.: Class of constructive asymptotically good algebraic codes. IEEE Trans. Inf. Theory **18**(5), 652–656 (1972)

26. Letzter,S., Pokrovskiy,A., Yepremyan,L.: Size-Ramsey numbers of powers of hypergraph trees and long subdivisions. Preprint arXiv:2103.01942 (2021)
27. Lubotzky, A., Phillips, R., Sarnak, P.: Ramanujan graphs. Combinatorica **8**(3), 261–277 (1988)
28. MacWilliams, F.J., Sloane, N.J.A., Thompson, J.G.: Good self-dual codes exist. Discrete Math. **3**(1–3), 153–162 (1972)
29. Quebbemann, H.G.: On even codes. Discrete Math. **98**, 29–34 (1991)
30. Sipser, M., Spielman, D.A.: Expander codes. IEEE Trans. Inf. Theory **42**(6), 1710–1722 (1996)
31. Stichtenoth, H.: Transitive and Self-dual Codes Attaining the Tsfasman-Vladut-Zink Bound. IEEE Trans. Inf. Theory **52**, 2218–2224 (2006)
32. Tang, C., Qiu, Y., Liao, Q., Zhou, Z.: Full characterization of minimal linear codes as cutting blocking sets. IEEE Trans. Inf. Theory **67**(6), 3690–3700 (2021)
33. Tsfasman,M., Vladut,S. G.: Algebraic-geometric codes. Springer Science & Business Media, Vol. 58 (2013)
34. Tsfasman, M., Vladut, S.G., Zink, T.: Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. Math. Nachr. **109**(1), 21–28 (1982)
35. Xu,Y., Kan,H., Han,G.: r-minimal codes with respect to rank metric. IEEE Transactions on Information Theory (2025)