Evasive Sets, Covering by Subspaces, and Point-Hyperplane Incidences

Benny Sudakov[1] · István Tomon[2]

Abstract

Given positive integers $k \leq d$ and a finite field $\mathbb{F}$, a set $S \subset \mathbb{F}^d$ is (k, c)-*subspace evasive* if every k-dimensional affine subspace contains at most c elements of S. By a simple averaging argument, the maximum size of a (k, c)-subspace evasive set is at most $c|\mathbb{F}|^{d-k}$. When k and d are fixed, and c is sufficiently large, the matching lower bound $\Omega(|\mathbb{F}|^{d-k})$ is proved by Dvir and Lovett. We provide an alternative proof of this result using the random algebraic method. We also prove sharp upper bounds on the size of (k, c)-evasive sets in case d is large, extending results of Ben-Aroya and Shinkar. The existence of optimal evasive sets has several interesting consequences in combinatorial geometry. We show that the minimum number of k-dimensional linear hyperplanes needed to cover the grid $[n]^d \subset \mathbb{R}^d$ is $\Omega_d\left(n^{\frac{d(d-k)}{d-1}}\right)$, which matches the upper bound proved by Balko et al., and settles a problem proposed by Brass et al. Furthermore, we improve the best known lower bound on the maximum number of incidences between points and hyperplanes in $\mathbb{R}^d$ assuming their incidence graph avoids the complete bipartite graph $K_{c,c}$ for some large constant $c = c(d)$.

Keywords Codes · Evasive sets · Covering problems

Mathematics Subject Classification 51A20 · 94B05 · 94B27

Benny Sudakov
benjamin.sudakov@math.ethz.ch

István Tomon
istvan.tomon@umu.se

[1] ETH Zurich, Zurich, Switzerland

[2] Umeå University, Umeå, Sweden

⚛️ Springer

1 Introduction

Given a finite field $\mathbb{F}$, a set of points $S \subset \mathbb{F}^d$ is (k, c)-*subspace evasive* if no k-dimensional affine subspace contains more than c elements of S. This notion was first investigated in an influential work of Pudlák and Rödl [18], who observed that explicit constructions of evasive sets in $\mathbb{F}_2^n$ can be transformed to give explicit constructions of bipartite Ramsey graphs. In particular, they showed that a $(d/2, c)$-evasive set $S \subset \mathbb{F}_2^d$ can be used to construct a bipartite graph with vertex classes of size $|S|$ containing no complete or empty bipartite graph with parts of size more than c. Evasive sets also have application in coding theory in the context of list-decoding, and in combinatorial geometry, where they can be used to get incidence bounds.

1.1 Evasive Sets and Coding Theory

Error-correcting codes are used for controlling errors in data transmission over noisy or unreliable communication channels and they were extensively studied in the last 70 years in information theory, computer science and telecommunication. An $[m, r, t]$-*code over the field* $\mathbb{F}$ is a linear subspace $L < \mathbb{F}^m$ of dimension r such that the Hamming distance between any two distinct elements of L is at least t, or equivalently, L contains no nonzero vector with less than t nonzero coordinates. In practice, an $[m, r, t]$-code can be used to send r ($\mathbb{F}$-ary) bits of data using m bits, and is capable of correcting $(t-1)/2$ faulty bits. In other words, the Hamming balls of radius $\lfloor (t-1)/2 \rfloor$ centered at the code words of L are disjoint, which gives the celebrated Hamming bound $m \le O_t \left(|\mathbb{F}|^{\frac{(m-r)}{\lfloor (t-1)/2 \rfloor} - 1} \right)$ (see, e.g., [22]).

A matrix $M \in \mathbb{F}^{(m-r) \times m}$, whose kernel is L, is a *parity-check matrix* of L. It is easy to show that L is an $[m, r, t]$-code if and only if any $t-1$ columns of M are linearly dependent. Therefore, the problem of constructing $[m, r, t]$-codes is equivalent to the construction of a set S of m vectors in $\mathbb{F}^{m-r}$, forming the columns of M, such that no $(t-2)$-dimensional subspace contains $t-1$ elements of S. Writing $d = m - r$ and $k = t - 2$, the Hamming bound shows that if $S \subset \mathbb{F}^d$ such that no k-dimensional linear subspace contains $k + 1$ elements of S, then

$$|S| \le O_k \left(|\mathbb{F}|^{\frac{d}{\lfloor (k+1)/2 \rfloor} - 1} \right). \tag{1}$$

A list-decoding problem deals with the case when we receive message with more than $(t-1)/2$ faulty bits. In this case we might not be able to uniquely determine the original message, but we can sometimes output a small list of possibilities. An error correcting code $L \subset \mathbb{F}^m$ is (ρ, c) *list-decodable* if the Hamming ball of radius ρm around every element of L contains at most c elements of L. In 2011, Guruswami [14] discovered an important connection between evasive sets and *list-decodable codes*. He showed in [14] that if $|\mathbb{F}| = d^{O(1/\varepsilon^2)}$ and there exists $S \subset \mathbb{F}^d$ such that S is $(1/\varepsilon, c)$-subspace evasive of size $|S| \ge |\mathbb{F}|^{d(1-\epsilon)}$, then it is possible to construct a code $L \subset \mathbb{F}^m$ of size $|\mathbb{F}|^{\delta m}$ which is $(1 - \delta - 2\varepsilon, c)$ list-decodable.

Furthermore, Guruswami [14] observed that a random set S of size $|\mathbb{F}|^{d-k-\delta}$ is $(k, O(kd/\delta))$-subspace evasive with high probability, and so such a set can be used to construct list-decodable codes of near optimal capacity. In this setting, one thinks of k being fixed, while d and (possibly $|\mathbb{F}|$) are large. Taking $\delta = \varepsilon d$ in the above result implies that a random set of $|\mathbb{F}|^{d(1-\varepsilon)}$ points is (k, c)-subspace evasive with $c = O(k/\varepsilon)$. Notably, c does not depend on $|\mathbb{F}|$ or d. This simple probabilistic argument vastly outperforms every known explicit construction, so the main focus here is to find deterministic (k, c)-subspace evasive sets S of size $|\mathbb{F}|^{d(1-\varepsilon)}$ with c small as possible, see e.g. [4, 10]. On the other hand, Ben-Aroya and Shinkar [4] proved that when $\varepsilon^{-1} \leq k^{O(1)}$, the bound $c = O(k/\varepsilon)$ cannot be improved, therefore the probabilistic construction is optimal. We extend this result, showing that it remains true for every $\varepsilon^{-1} = 2^{O(k)}$ as well.

Theorem 1.1 *Let $\mathbb{F}$ be a field, k be a positive integer, and $0 < \varepsilon < 1/20$, then if d is sufficiently large with respect to k, the following holds. Let $S \subset \mathbb{F}^d$ such that $|S| \geq |\mathbb{F}|^{d(1-\varepsilon)}$. Then S is not $\left(k, \frac{k-\log_2(1/\varepsilon)}{8\varepsilon}\right)$-subspace evasive.*

Theorem 1.1 shows that if $\varepsilon^{-1} = 2^{k-1}$, then a set of size more than $|\mathbb{F}|^{d(1-\epsilon)}$ is not $(k, \Omega(2^k))$-evasive, while the result becomes meaningless if $\varepsilon^{-1} \geq 2^k$. Observe that the latter is a natural barrier, as in case $\mathbb{F} = \mathbb{F}_2$, a k-dimensional affine subspace cannot contain more than 2^k points. Therefore, if one wants to extend Theorem 1.1 beyond $\varepsilon^{-1} \geq 2^k$, the field $\mathbb{F}$ also has to play some role. This setting, already for $k = 1$, seems extremely difficult. Bounding the size of a set in $\mathbb{F}_3^d$ containing no three points on a line is equivalent with the famous *Cap set problem*, for which the upper bound 2.756^d was recently proved by Ellenberg and Gijswijt [11], following the breakthrough of Croot, Lev, and Pach [9]. However, similar results are already not known for four points on a line.

It appears, that the upper bound on evasiveness behaves very differently in the regime when c is close to k. In this case, we show that the Hamming bound mentioned above can be used to estimate the size of $(k, k + C)$-subspace evasive sets, where $C < k/2$. Interestingly, the method of proof for this range of parameters is fundamentally different from that in Theorem 1.1. While the proof of this theorem is mostly combinatorial, relying on a generalization of the Erdős Box theorem [12], the proof of the following result (such as the proof of the Hamming bound) is based on coding theory.

Theorem 1.2 *Let $S \subset \mathbb{F}^d$ be $(k, k + C)$-subspace evasive, where $C \leq \frac{k}{2} - 1$. Then*

$$|S| \leq 4k|\mathbb{F}|^{\frac{d}{\lfloor k/2(C+1)\rfloor}}.$$

Using the standard probabilistic argument, one can easily show that the bound in this theorem is optimal up to a factor of 2 in the exponent.

1.2 Evasive Sets Over Large Fields

Motivated by applications in combinatorial geometry, another interesting setting is to consider large (k, c)-subspace evasive sets in $\mathbb{F}^d$, where we think of k and d as

fixed, while $|\mathbb{F}|$ is arbitrarily large. Clearly, a simple averaging argument shows that a (k, c)-subspace evasive set in $\mathbb{F}^d$ can have size at most $c|\mathbb{F}|^{d-k}$. As mentioned above, the probabilistic argument shows that a random set of $|\mathbb{F}|^{d-k-\delta}$ points is (k, c)-subspace evasive for $\delta = \Theta(kd/c)$. Note that, however, a random set of $\Omega_d(|\mathbb{F}|^{d-k})$ points does intersect many k-dimensional affine subspaces in $\Omega_d(\log |\mathbb{F}|)$ elements with high probability. Dvir and Lovett [10] (see Theorem 2.4 together with Claim 3.5) showed that this can be improved, by giving an explicit algebraic construction of a (k, c)-subspace evasive set of size $\Omega(|\mathbb{F}|^{d-k})$, where c depends only on d and k.

Theorem 1.3 [10] *For every pair of positive integers k, d satisfying $k \leq d$, there exists a positive integer $c = c(d, k)$ such that the following holds. For every finite field $\mathbb{F}$, there exists a (k, c)-subspace evasive set of size $|\mathbb{F}|^{d-k}/3$ in $\mathbb{F}^d$.*

To provide a different perspective and for the convenience of the reader, we give a short, alternative proof of this theorem. Note the striking difference between the bound of Theorem 1.3 and the lower bounds in case c being small. This leads to the natural question about the dependence of $c(d, k)$ on the parameters d and k. The proof of Dvir and Lovett [10] gives $c(d, k) = d^k$ (if $|\mathbb{F}|$ is sufficiently large), which is likely to be far from optimal, while our proof gives even worse bounds. On the other hand, applying Theorem 1.1 with $\varepsilon = \max\{\frac{k}{d}, \frac{1}{2^{k-1}}\}$, we get the lower bound $c(d, k) = \Omega(\min\{d, 2^k\})$. This might raise the question whether $c(d, k)$ can be bounded by a function of k alone. However, this is not true already for $k = 1$. Indeed, if d is sufficiently large with respect to k and $\mathbb{F}$, then the density Hales-Jewett theorem [13] implies that any subset $S \subset \mathbb{F}^d$ of size at least $\frac{1}{|\mathbb{F}|^k}|\mathbb{F}|^d$ contains a *combinatorial line*, which in turn is also a complete 1-dimensional affine subspace.

1.3 Covering by Subspaces

Theorem 1.3 has a number of interesting applications in combinatorial geometry. The following problem first appeared in a paper of Brass and Knauer [5] in connection to point-hyperplane incidences, which we discuss in more detail in the next subsection. Given positive integers n, k, d, c with $k \leq d$, determine the maximum number of lattice points in the grid $[n]^d = \{1, \ldots, n\}^d$ with no k-dimensional linear or affine subspace containing more than c of them (over $\mathbb{R}$). Let $\ell(d, k, n, c)$ denote this maximum in the linear case, and $a(d, k, n, c)$ in the affine case. Here, we are interested in the behavior of $\ell(d, k, n, c)$ and $a(d, k, n, c)$ as a function of n, while we think of k, d, c as fixed. Clearly, we have $a(d, k, n, c) \leq cn^{d-k}$ as we can cover $[n]^d$ by n^{d-k} affine hyperplanes of dimension k. On the other hand, a probabilistic argument of Brass and Knauer [5] shows that for every $\varepsilon > 0$ there exists $c = c(d, k, \varepsilon)$ such that $a(d, k, n, c) \geq n^{d-k-\varepsilon}$. The tight result $a(d, k, n, k+1) = \Omega_d(n^{d-k})$ was only known in the two special cases when $k = 1$ or $k = d - 1$. A straightforward application of Theorem 1.3 lets us close the gap between the lower and upper bound for every $k < d$ and sufficiently large c.

Theorem 1.4 *For every pair of positive integers k, d satisfying $k \leq d$, there exists a positive integer $c = c(d, k)$ such that the following holds. For every positive integer n there exists a set $S \subset [n]^d$ of size at least $(n/2)^{d-k}$ such that no k-dimensional affine hyperplane contains more than c elements of S.*

Indeed, let p be any prime between $n/2$ and n, which exists by Bertrand's postulate. Let $c = c(d, k)$ be the constant guaranteed by Theorem 1.3, and let $S_0 \subset \mathbb{F}_p^d$ be a set of $p^{d-k} \geq (n/2)^{d-k}$ vectors such that no k-dimensional affine subspace contains more than c elements of S_0. Setting S to be the set of lattice points in $[p]^d$ that are congruent to the elements of S_0 modulo p gives the desired set.

Determining $\ell(d, k, n, c)$ seems to be more difficult. Brass and Knauer [5] conjectured that $\ell(d, k, n, k) = \Theta_d(n^{d(d-k)/(d-1)})$. However, this was refuted by Lefmann [17] for most values of k and d, as he showed that $\ell(d, k, n, k) = O_d(n^{d/\lfloor k/2 \rfloor})$ (akin the Hamming bound, mentioned in the previous subsection). Similarly to the affine case, bounding $\ell(d, k, n, c)$ is closely related to the problem of bounding $g(d, k, n)$, which is the minimum number of k-dimensional linear hyperplanes in a covering of $[n]^d$. Indeed, we trivially have $\ell(d, k, n, c) \leq cg(d, k, n)$. The problem of estimating $g(d, k, n)$ was proposed by Brass et al. [6] (Problem 6 in Chapter 10.2). Bárány et al. [3] resolved the $k = d - 1$ case of both problems by showing that $\Omega_d(n^{d/(d-1)}) = \ell(d, d-1, n, d-1) \leq (d-1)g(d, d-1, n) = O_d(n^{d/(d-1)})$. In general, Balko et al. [2] showed that $g(d, k, n) = O_d(n^{d(d-k)/(d-1)})$ and $g(d, k, n) > n^{d(d-k)/(d-1)-o(1)}$, where the lower bound comes from proving $\ell(d, k, n, c) \geq n^{d(d-k)/(d-1)-\varepsilon}$ for some $\varepsilon = \varepsilon_{d,k}(c)$ tending to 0 as c tends to infinity. If $k = 1$, it was shown by Konyagin and Sudakov [15] that the $o(1)$ and ε terms can be removed, closing the gap in this case. Here, we close the gap for all values of k and d.

Theorem 1.5 *For every pair of positive integers k, d satisfying $k \leq d$, there exist a positive integer $c = c(d, k)$ and real number $C = C(d, k) > 0$ such that the following holds. For every positive integer n there exists a set $S \subset [n]^d$ of size at least $Cn^{d(d-k)/(d-1)}$ such that no k-dimensional linear hyperplane contains more than c elements of S.*

Corollary 1.6 *Let k, d be positive integers satisfying $k < d$, then there exists $C > 0$ such that the following holds for every positive integer n. The number of k-dimensional hyperplanes in any covering of $[n]^d$ is at least $Cn^{d(d-k)/(d-1)}$.*

We will give a very short alternative proof of Corollary 1.6 as well, which does not rely on Theorem 1.5. Finally, let us remark that $c = c(d, k)$ denotes the same function in Theorems 1.3, 1.4 and 1.5.

1.4 Point-Hyperplane Incidences

One of the fundamental results in combinatorial geometry is the Szemerédi-Trotter theorem [21], which states that the number of incidences between n points and m lines is $O((mn)^{2/3} + m + n)$, and this bound is the best possible. Extending this result to higher dimensions is a notorious open problem. Given a set of points P and set of hyperplanes $\mathcal{H}$ in $\mathbb{R}^d$, let $I(P, \mathcal{H})$ denote the number of incidences between P and $\mathcal{H}$, that is, the number of pairs $(p, H) \in P \times \mathcal{H}$ such that $p \in H$. Note that in $\mathbb{R}^3$, by taking n points on a single line and m planes containing this line, we have a collection of n points and m planes with mn incidences. Therefore, in order to avoid this triviality, we forbid a complete bipartite graph $K_{c,c}$ in the incidence graph of the configuration.

I.e., if P is a set of n points and $\mathcal{H}$ is a set of m hyperplanes in $\mathbb{R}^d$, we are interested in the maximum of $I(P, \mathcal{H})$ as a function of m and n assuming there are no c hyperplanes containing the same c points. Let $f(d, n, m, c)$ denote this maximum.

It follows from works of Chazelle [8], Brass and Knauer [5] and Apfelbaum and Sharir [1] that

$$f(d, n, m, c) = O_{d,c}((mn)^{1-1/(d+1)} + m + n).$$

However, this bound is only known to be sharp in case $d = 2$. Brass and Knauer [5] observed that large sets of lattice points satisfying the conditions of Theorems 1.4 and 1.5 can be used to provide lower bounds for $f(d, n, m, c)$. For every pair of integers m and n, and real number $\varepsilon > 0$, they showed that there exists c such that

$$f(d, n, m, c) \geq \begin{cases} (mn)^{1-2/(d+3)-\varepsilon} & \text{if } d \text{ is odd and } d > 3, \\ (mn)^{1-2(d+1)/(d+2)^2-\varepsilon} & \text{if } d \text{ is even,} \\ \Omega((mn)^{7/10}) & \text{if } d = 3. \end{cases}$$

By improving the known lower bounds on $\ell(d, k, n, c)$, Balko et al. [2] improved the lower bounds on $f(d, n, m, c)$ as well for $d \geq 4$. By using Theorems 1.4 and 1.5, we further improve their result, and as these theorems are optimal (up to the value of c), we reach the full potential of the approach outlined by Brass and Knauer [5].

Theorem 1.7 *For every positive integer d there exists c such that the following holds. Let m, n be positive integers, then there exists a set of n points P and a set of m hyperplanes $\mathcal{H}$ in $\mathbb{R}^d$ such that the incidence graph of P and $\mathcal{H}$ is $K_{c,c}$-free, and*

$$I(P, \mathcal{H}) \geq \begin{cases} \Omega_d((mn)^{1-(2d+3)/(d+2)(d+3)}) & \text{if } d \text{ is odd,} \\ \Omega_d((mn)^{1-(2d^2+d-2)/(d+2)(d^2+2d-2)}) & \text{if } d \text{ is even.} \end{cases}$$

In certain asymmetric settings, i.e when n is much larger than m, better bounds are known, see [19].

The rest of this paper is organized as follows. In Sect. 2, we prove Theorems 1.1 and 1.4. Then, in Sect. 3, we prove Theorem 1.3. In Sect. 4, we prove Theorem 1.5, and give an alternative proof of Corollary 1.6. Finally, in Sect. 5, we give a proof sketch of Theorem 1.7.

2 Lower Bounds for Evasiveness

In this section, we prove Theorems 1.1 and 1.4. In order to prove Theorem 1.1, we consider a variant of the Erdős Box theorem [12]. This theorem is a generalization of the Kővári-Sós-Turán theorem [16], providing upper bounds on the maximum number of edges of an r-partite r-uniform hypergraph with parts of size n containing no copy of the complete r-partite r-uniform hypergraph $K_{s_1,\dots,s_r}$. As we require a version of the Box theorem in which the parts of the host hypergraph have different sizes (which is not a standard setting), we present a short proof of the result that we need. With slight abuse of notation, given an r-uniform r-partite hypergraph H with vertex

classes $V_1, \ldots, V_r$, we view edges of H as both r-element subsets of the vertex set, and elements of the Cartesian product $V_1 \times \cdots \times V_r$. We also denote by $X^{(s)}$ all s-element subsets of the set X.

Lemma 2.1 *Let r and $s_1, \ldots, s_r \geq 2$ be positive integers. Let H be an r-partite r-uniform hypergraph with vertex classes $V_1, \ldots, V_r$ such that $|V_i| \geq s_i^2 |V_r|^{\frac{1}{s_i \cdots s_{r-1}}}$ for $i \in [r-1]$. If H has at least*

$$2 s_r^{\frac{1}{s_1 \cdots s_{r-1}}} |V_1| \ldots |V_{r-1}| |V_r|^{1 - \frac{1}{s_1 \cdots s_{r-1}}}$$

edges, then there exists $S_1 \subset V_1, \ldots, S_r \subset V_r$ such that $|S_i| = s_i$ for $i \in [r]$, and $S_1 \times \cdots \times S_r \subset E(H)$.

Proof We prove this by induction on r. In case $r = 1$, H has at least $2s_1$ edges, so the statement is true. Let us assume that $r \geq 2$. Let $U = V_2 \times \cdots \times V_r$ and let

$$t \geq 2 s_r^{\frac{1}{s_1 \cdots s_{r-1}}} |V_1| \ldots |V_{r-1}| |V_r|^{1 - \frac{1}{s_1 \cdots s_{r-1}}}$$

be the number of edges of H. For each $f \in U$, let $d(f)$ denote the number of edges of H containing f. Also, for every set of vertices $W \subset V_1$, let

$$N(W) = \{ f \in U : \forall v \in W, \{v\} \cup f \in E(H) \}.$$

Then we have the following equality:

$$\sum_{W \in V_1^{(s_1)}} |N(W)| = \sum_{f \in U} \binom{d(f)}{s_1}.$$

By the convexity of the function $\binom{x}{s_1}$, and recalling that $\sum_{f \in U} d(f) = t$, we can write the following inequality:

$$\sum_{f \in U} \binom{d(f)}{s_1} \geq |U| \binom{t/|U|}{s_1} \geq \frac{t^{s_1}}{2 s_1! |U|^{s_1 - 1}}.$$

The last inequality holds by the condition $t/|U| \geq 2|V_1||V_r|^{-\frac{1}{s_1 \cdots s_{r-1}}} > 2 s_1^2$. Therefore, by the pigeonhole principle, there exists $S_1 \in V_1^{(s_1)}$ such that

$$|N(S_1)| \geq \frac{t^{s_1}}{2 s_1! |U|^{s_1 - 1} \binom{|V_1|}{s_1}} \geq \frac{t^{s_1}}{2|V_1|^{s_1} |U|^{s_1 - 1}} \geq 2 s_r^{\frac{1}{s_2 \cdots s_{r-1}}} |V_2| \ldots |V_{r-1}| |V_r|^{1 - \frac{1}{s_2 \cdots s_{r-1}}}$$

Let H' be the $(r-1)$-partite $(r-1)$-uniform hypergraph with vertex classes $V_2, \ldots, V_r$ and set of edges $E(H') = N(S_1)$. Then we can apply our induction hypothesis to conclude that there exist $S_2 \subset V_2, \ldots, S_r \subset V_r$ such that $|S_i| = s_i$ for $i = 2, \ldots, r$,

and $S_2 \times \cdots \times S_r \subset E(H')$. But then $S_1 \times \cdots \times S_r \subset V_1 \times \cdots \times V_r$, so $S_1, \ldots, S_r$ satisfy the required properties. □

Now we are ready to prove Theorem 1.1.

Proof of Theorem 1.1 Let us introduce some parameters. Let $r = \lfloor \log_2(1/\varepsilon) \rfloor - 1$, then we may assume that $r \leq k$, otherwise the statement of the theorem is vacuous. For $i \in [r-1]$, let $t_i = \lceil \frac{d2^{i+1-r}}{3} \rceil$, and set $T = t_1 + \cdots + t_{r-1}$. Observe that $T < \frac{2d}{3}$, assuming d is sufficiently large with respect to r. Furthermore, for $i = 1, \ldots, r-1$, let $V_i = \mathbb{F}^{t_i}$, and let $V_r = \mathbb{F}^{d-T}$. We will view $\mathbb{F}^d$ as the Cartesian product $V_1 \times \cdots \times V_r$. Define the r-partite r-uniform hypergraph H on the vertex classes $V_1, \ldots, V_r$ such that $v \in V_1 \times \cdots \times V_r$ is an edge if $v \in S$.

We would like to apply Lemma 2.1 with $s_1 = \cdots = s_{r-1} = 2$ and $s_r = k - r + 2$ to the hypergraph H to find suitable sets $S_1, \ldots, S_r$. However, in order to do this, we need to verify that H satisfies the conditions of the lemma. First of all, for $i \in [r-1]$, we have

$$|V_i| = |\mathbb{F}|^{t_i} \geq |\mathbb{F}|^{\frac{d2^{i+1-r}}{3}} \geq 4|\mathbb{F}|^{(d-T)2^{i-r}} = s_i^2 |V_r|^{\frac{1}{s_i \cdots s_{r-1}}},$$

where the second inequality holds assuming d is sufficiently large with respect to r. Furthermore, note that $\frac{1}{8\varepsilon} < s_1 \ldots s_{r-1} = 2^{r-1} \leq \frac{1}{4\varepsilon}$, and

$$\frac{d-T}{s_1 \ldots s_{r-1}} \geq 4\varepsilon(d-T) > \frac{4\varepsilon d}{3}.$$

Therefore, we can write

$$2s_r^{\frac{1}{s_1 \cdots s_{r-1}}} |V_1| \ldots |V_{r-1}||V_r|^{1-\frac{1}{s_1 \cdots s_{r-1}}} < 2k^{8\varepsilon}|\mathbb{F}|^{d(1-4\varepsilon/3)} \leq |S|.$$

Here, the last inequality holds by assuming d is sufficiently large with respect to k. Thus, the conditions of Lemma 2.1 are satisfied, so we can find $S_1 \subset V_1, \ldots, S_r \subset V_r$ such that $|S_i| = s_i$ for $i \in [r]$, and $W = S_1 \times \cdots \times S_r \subset S$. Let $S_i = \{u_i, v_i\}$ for $i \in [r-1]$, and let $S_r = \{w_0 \ldots w_{k-r+1}\}$. Given $w \in V_i$ for some $i \in [r]$, let $w' \in \mathbb{F}^d$ denote the vector which agrees with w on V_i, and vanishes on all other coordinates. Then W is contained in the affine subspace

$$\left(w'_0 + \sum_{i=1}^{r-1} u'_1 \right) + \text{span}\langle \{v'_i - u'_i : i \in [r-1]\} \cup \{w'_i - w'_0 : i \in [k-r+1]\}\rangle,$$

which clearly has dimension at most k. Finally, as $|W| = 2^{r-1}(k-r+1) > \frac{k-\log_2(1/\varepsilon)}{8\varepsilon}$, this shows that S is not $(k, \frac{k-\log_2(1/\varepsilon)}{8\varepsilon})$-subspace evasive. □

Finally, let us present the proof of Theorem 1.2.

Proof of Theorem 1.2 For the convenience of the reader, we first recall the proof of the Hamming bound, that is (1). Let $S \subset \mathbb{F}^d$ be a set of vectors such that no k-dimensional linear subspace contains $k + 1$ elements. Without loss of generality, assume that S spans $\mathbb{F}^d$. Let $M \in \mathbb{F}^{d \times |S|}$ be a matrix, whose columns are the elements of S. Then $L = \ker(M) < \mathbb{F}^{|S|}$ does not contain a vector with at most $k + 1$ non-zero coordinates, which implies that L is an $[|S|, |S| - d, k + 2]$-code. Hence, the Hamming balls of radius $r = \lfloor \frac{k+1}{2} \rfloor$ around the elements of L are disjoint. The size of such a ball is at least $(|\mathbb{F}| - 1)^r \binom{|S|}{r} \geq 2^{-r} |\mathbb{F}|^r \binom{|S|}{r}$, which gives that $|L| \cdot 2^{-r} |\mathbb{F}|^r \binom{|S|}{r} \leq |\mathbb{F}|^{|S|}$. From this, we get $\binom{|S|}{r} \leq 2^r |\mathbb{F}|^{d-r}$, which further implies $|S| \leq 2k|\mathbb{F}|^{d/r-1}$.

Now let us turn to the proof of Theorem 1.2. Write $k = k_1 + \cdots + k_{C+1}$, where $k_i \in \{\lfloor \frac{k}{C+1} \rfloor, \lceil \frac{k}{C+1} \rceil\}$ for $i \in [C + 1]$. Note that $\lfloor \frac{k_i+1}{2} \rfloor > \lfloor \frac{k}{2(C+1)} \rfloor$. Hence, by the above discussion, if $|S| \geq 2k|\mathbb{F}|^{\frac{d}{\lfloor k/2(C+1) \rfloor}} + k + C + 1$, we can find disjoint subsets $W_1, \ldots, W_{C+1} \subset S$ such that $|W_i| = k_i + 1$ and W_i spans a linear subspace of dimension at most k_i for $i \in [C + 1]$. Indeed, select $W_1, \ldots, W_{C+1}$ one-by-one, at each step deleting the selected set from S. But then $W = W_1 \cup \cdots \cup W_{C+1}$ spans a linear subspace of dimension at most k, and $|W| = k + C + 1$, showing that S is not $(k, k + C)$-evasive. □

3 Optimal Constructions of Evasive Sets

In this section, we give an alternative proof of Theorem 1.3. Our proof is based on the random algebraic method pioneered by Bukh, and uses the ideas from his paper [7]. With slight abuse of notation, let us exchange k with $d - k$ for our (and the reader's) future convenience, so we prove the following analogue of Theorem 1.3.

Theorem 3.1 *For every pair of positive integers k, d satisfying $k \leq d$, there exists a positive integer $c = c(d, d - k)$ such that the following holds. For every finite field $\mathbb{F}$, there exists a $(d - k, c)$-subspace evasive (multi-)set of size $|\mathbb{F}|^k$ in $\mathbb{F}^d$.*

Let $D = (d+1)k+1$, $p = |\mathbb{F}|$ (so p is a prime power), and let $\mathcal{Q}_D < \mathbb{F}[x_1, \ldots, x_k]$ denote the space of polynomials of (total) degree at most D on k variables. Write

$$\Lambda_D = \{\alpha \in \mathbb{N}^k : \alpha(1) + \cdots + \alpha(k) \leq D\},$$

which is the set of possible exponents of the monomials of the polynomials in $\mathcal{Q}_D$. Let $q_1, \ldots, q_d$ be random elements of $\mathcal{Q}_D$ chosen independently from the uniform distribution, and set $\mathbf{q} = (q_1, \ldots, q_d)$. Our goal is to show that the set

$$S = \{\mathbf{q}(\mathbf{x}) : \mathbf{x} \in \mathbb{F}_p^k\}$$

has the property that the no $(d - k)$-dimensional affine subspace of $\mathbb{F}^d$ contains more than c elements of H with high probability, if c is sufficiently large with respect to k and d.

We prepare the proof of this with a number of claims. First, let us state three simple observations that we will use repeatedly.

(i) If $M \in \mathbb{F}^{k \times d}$ has rank k, and $\mathbf{v} \in \mathbb{F}^d$ is chosen randomly from the uniform distribution, then $M\mathbf{v}$ is uniformly distributed in $\mathbb{F}^k$.

(ii) If $X_1, \ldots, X_d$ are uniformly distributed random variables in $\mathbb{F}$, then $X_1, \ldots, X_d$ are independent if and only if $(X_1, \ldots, X_d)$ is uniformly distributed in $\mathbb{F}^d$.

(iii) If $X_1, \ldots, X_d$ are independent, uniformly distributed random variables on $\mathbb{F}$, and $Y_1, \ldots, Y_d$ are random variables on $\mathbb{F}$ such that X_i and Y_j are independent for any $i, j \in [d]$, then $X_1 + Y_1, \ldots, X_d + Y_d$ are independent and uniformly distributed.

Claim 3.2 *Let $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{F}^d$ be linearly independent vectors. Then the polynomials $\langle \mathbf{q}, \mathbf{v}_1 \rangle, \ldots, \langle \mathbf{q}, \mathbf{v}_k \rangle$ are independent and uniformly distributed in $\mathcal{Q}_D$.*

Proof Let $M \in \mathbb{F}^{d \times k}$ be the matrix, whose rows are $\mathbf{v}_1, \ldots, \mathbf{v}_k$. For $\alpha \in \Lambda_D$ and $i \in [d]$, let $c_{i,\alpha}$ be the coefficient of the monomial $\mathbf{x}^\alpha = x_1^{\alpha(1)} \ldots x_k^{\alpha(k)}$ in q_i, and let $\mathbf{c}_\alpha = (c_{1,\alpha}, \ldots, c_{d,\alpha})$. Observe that the $d \cdot |\Lambda_D|$ random variables $(c_{i,\alpha})_{i \in [d], \alpha \in \Lambda_D}$ are independent and uniformly distributed in $\mathbb{F}$.

The coefficient of $\mathbf{x}^\alpha$ in $\langle \mathbf{q}, \mathbf{v}_i \rangle$ is $(M\mathbf{c}_\alpha)(i)$. As $M\mathbf{c}_\alpha$ is uniformly distributed in $\mathbb{F}^k$ and $(\mathbf{c}_\alpha)_{\alpha \in \Lambda_D}$ are independent, this proves the claim. $\qquad \square$

Claim 3.3 *Let $\mathbf{z} \in \mathbb{F}^k$ and $i \in [d]$. Then $q_i(\mathbf{z})$ is uniformly distributed in $\mathbb{F}$.*

Proof This follows as the constant term of q_i is uniformly distributed in $\mathbb{F}$. $\qquad \square$

Claim 3.4 *Let $s \leq \min\{D, |\mathbb{F}|^{1/2}\}$, and let $\mathbf{z}_1, \ldots, \mathbf{z}_s \in \mathbb{F}^k$ be pairwise distinct vectors. Then the $d \cdot s$ random variables $(q_i(\mathbf{z}_j))_{i \in [d], j \in [s]}$ are independent.*

Proof First, suppose that the first coordinates of the vectors $\mathbf{z}_1, \ldots, \mathbf{z}_s$ are pairwise distinct. For $\alpha \in \{0, 1, \ldots, s-1\}$ and $i \in [d]$, let $c_{i,\alpha}$ be the coefficient of x_1^α in q_i. Also, let $\mathbf{c}_i = (c_{i,0}, \ldots, c_{i,s-1})$ and $\mathbf{y}_i = (1, \mathbf{z}_i(1), \mathbf{z}_i(1)^2, \ldots, \mathbf{z}_i(1)^{s-1})$. Then $\mathbf{y}_1, \ldots, \mathbf{y}_s$ are linearly independent, using that $\mathbf{z}_1(1), \ldots, \mathbf{z}_s(1)$ are pairwise distinct, and so the Vandermonde determinant is nonzero. Let $M \in \mathbb{F}_p^{s \times s}$ be the matrix whose rows are $\mathbf{y}_1, \ldots, \mathbf{y}_s$. Then M has rank s, so $M\mathbf{c}_i$ is uniformly distributed in $\mathbb{F}_p^s$. As $\mathbf{c}_1, \ldots, \mathbf{c}_d$ are independent, we get that the $d \cdot s$ numbers $((M\mathbf{c}_i)(j))_{i \in [d], j \in [s]}$ are independent. But $q_i(\mathbf{z}_j) = X_{i,j} + Y_{i,j}$, where $X_{i,j} = (M\mathbf{c}_i)(j)$, and $X_{i,j}$ and $Y_{i',j'}$ are independent (since these variables depend on disjoint sets of random coefficients), hence $(q_i(\mathbf{z}_j))_{i \in [d], j \in [s]}$ are independent as well (see (iii)).

Now consider the general case. We show that there exists an invertible matrix $M \in \mathbb{F}^{k \times k}$ such that $M\mathbf{z}_1, \ldots, M\mathbf{z}_s$ have pairwise distinct first coordinates. As M is a change of basis, the polynomial q_i' defined as $q_i'(\mathbf{x}) = q_i(M^{-1}\mathbf{x})$ is also uniformly distributed in $\mathcal{Q}_{p,D}$, so then we are done by the previous argument. Choose M randomly from the uniform distribution on all invertible matrices. Then for $1 \leq i < j \leq s$, we have $\mathbb{P}(M\mathbf{z}_i(1) = M\mathbf{z}_j(1)) = (|\mathbb{F}|^{k-1} - 1)/(|\mathbb{F}|^k - 1) < 1/|\mathbb{F}|$ as $M(\mathbf{z}_i - \mathbf{z}_j)$ is uniformly distributed on $\mathbb{F}^k \setminus \{0\}$. Hence, by Markov's inequality, the probability that there exists $1 \leq i < j \leq s$ such that $M\mathbf{z}_i(1) = M\mathbf{z}_j(1)$ is at most $\binom{s}{2}/|\mathbb{F}| < 1$, implying the existence of the desired matrix M. $\qquad \square$

Let V be a $(d-k)$-dimensional affine subspace of $\mathbb{F}^d$ and let $\mathbf{z} \in \mathbb{F}^k$. Let $I(\mathbf{z}, V)$ be the indicator random variable of the event $\{q(\mathbf{z}) \in V\}$. Then there exist k linearly

independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_k \in \mathbb{F}^d$ and $\mathbf{b} \in \mathbb{F}^k$ such that $I(\mathbf{z}, V) = 1$ if and only if $\langle q(\mathbf{z}), \mathbf{v}_i \rangle = \mathbf{b}(i)$ for every $i \in [k]$. Furthermore, set

$$N(V) = \sum_{\mathbf{z} \in \mathbb{F}^k} I(\mathbf{z}, V).$$

Let $\mathbf{e}_1, \ldots, \mathbf{e}_d \in \mathbb{F}^d$ be the unit basis, that is, $\mathbf{e}_i(j) = 1$ if $i = j$, and $\mathbf{e}_i(j) = 0$ otherwise. Let E be the $(d - k)$-dimensional linear subspace with normal vectors $e_1, \ldots, e_k$. By Claim 3.2 and 3.3, $N(V)$ has the same distribution as $N(E)$, so for simplicity, write $N = N(E)$ and $I(\mathbf{z}) = I(\mathbf{z}, E)$. Also, observe that $I(\mathbf{z})$ is the indicator random variable of the event $q_1(\mathbf{z}) = \cdots = q_k(\mathbf{z}) = 0$. Therefore, by Claim 3.3 and 3.4, we have that $\mathbb{P}(I(\mathbf{z}) = 1) = 1/|\mathbb{F}|^k$, and if $s \leq \min\{D, |\mathbb{F}|^{1/2}\}$ and $\mathbf{z}_1, \ldots, \mathbf{z}_s \in \mathbb{F}^k$ are distinct, then $I(\mathbf{z}_1), \ldots, I(\mathbf{z}_s)$ are independent.

Claim 3.5 *Let $s \leq \min\{D, |\mathbb{F}|^{1/2}\}$. Then $\mathbb{E}(N^s) \leq s^{s+1}$*

Proof We can write

$$\mathbb{E}(N^s) = \sum_{\mathbf{z}_1, \ldots, \mathbf{z}_s \in \mathbb{F}_p^k} \mathbb{E}(I(\mathbf{z}_1) \ldots I(\mathbf{z}_s)).$$

Here, the s-wise independence of the variables $I(\mathbf{z})$ guarantees that $\mathbb{E}(I(\mathbf{z}_1) \ldots I(\mathbf{z}_s)) = |\mathbb{F}|^{-kr}$, where r is the number of different elements among $\mathbf{z}_1, \ldots, \mathbf{z}_s$. The number of choices of $(\mathbf{z}_1, \ldots, \mathbf{z}_s)$ containing r distinct entries is at most $r^s p^{kr}$ (as there are at most $|\mathbb{F}|^{kr}$ choices for the r vectors, and each r-tuple of vectors yields at most r^s such s-tuples). Hence, we arrive to the bound

$$\mathbb{E}(N^s) \leq \sum_{r=1}^{s} r^s |\mathbb{F}|^{kr} \cdot |\mathbb{F}|^{-kr} < s^{s+1}.$$

$\square$

A crucial ingredient in the proof is the following fact from algebraic geometry, which says that a variety in $\mathbb{F}_p^k$ contains either at most a constant number of points (depending only on the degree of the variety), or at least $\Omega(p)$ points. In our case, this means that N is either bounded by a constant, or at least $\Omega(p)$. But as the higher moments of N are bounded by a constant, it is very unlikely that $N = \Omega(p)$.

Lemma 3.6 *[7] For every k and D there exists a constant c such that the following holds. Suppose that $q_1, \ldots, q_k \in \mathbb{F}[x_1, \ldots, x_k]$ are polynomials of degree at most D. Then the size of the variety*

$$W = \{\mathbf{x} \in \mathbb{F}^k : q_1(\mathbf{x}) = \cdots = q_k(\mathbf{x}) = 0\}$$

is either at most c, or at least $|\mathbb{F}| - c|\mathbb{F}|^{1/2}$.

Now everything is prepared to prove our main theorem.

Proof of Theorem 3.1 Clearly, it is enough to prove the theorem in case $|\mathbb{F}|$ is sufficiently large with respect to d and k. Let c be the constant given by Lemma 3.6 (with respect to k and D), and suppose that $|\mathbb{F}| > \max\{(2c)^2, (2D)^{D+1}\}$.

We show that the multiset $S = \{\mathbf{q}(\mathbf{z}) : \mathbf{z} \in \mathbb{F}^k\}$ satisfies the assertion of the theorem with positive probability. Let V be a $(d-k)$-dimensional affine subspace of $\mathbb{F}^d$. Then $|V \cap S| = N(V)$, so by Claim 3.5 applied with $s = D$, we have $\mathbb{E}(|V \cap S|^D) \le D^{D+1}$. Applying Markov's inequality, for every $\lambda > 0$, we have

$$\mathbb{P}(|V \cap S| \ge \lambda) \le \mathbb{P}(|V \cap S|^D \ge \lambda^D) \le \frac{D^{D+1}}{\lambda^D}.$$

But note that by Lemma 3.6, we have either $|V \cap S| \le c$, or $|V \cap S| \ge |\mathbb{F}| - c|\mathbb{F}|^{1/2} > |\mathbb{F}|/2$. Hence, we can further write

$$\mathbb{P}(|V \cap S| > c) = \mathbb{P}\left(|V \cap S| \ge \frac{|\mathbb{F}|}{2}\right) \le \frac{(2D)^{D+1}}{|\mathbb{F}|^D}.$$

The number of different $(d-k)$-dimensional affine subspaces in $\mathbb{F}^d$ is at most $(|\mathbb{F}|^d)^k \cdot |\mathbb{F}|^k = |\mathbb{F}|^{(d+1)k}$, as there are at most $(|\mathbb{F}|^d)^k$ choices for the k normal vectors, and at most $|\mathbb{F}|^k$ translations. Therefore, the expected number of hyperplanes V violating $|V \cap S| \le c$ is at most

$$\frac{|\mathbb{F}|^{(d+1)k} \cdot (2D)^{D+1}}{|\mathbb{F}|^D} \le \frac{(2D)^{D+1}}{|\mathbb{F}|} < 1,$$

recalling that $D = (d+1)k + 1$. This finishes the proof. □

4 Covering by Hyperplanes

In this section, we prove Theorem 1.5, and provide and alternative proof of Corollary 1.6.

Given a prime p and vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_p^d$, write $\mathbf{x} \sim \mathbf{y}$ if there exists $\lambda \in \mathbb{F}_p \setminus \{0\}$ such that $\mathbf{x} = \lambda\mathbf{y}$. A crucial observation is that the $\sim$ equivalence class of each vector contains an element, whose every coordinate is contained in the interval $[-p^{(d-1)/d}, p^{(d-1)/d}]$. This follows from Dirichlet's theorem on simultaneous approximations (see e.g. [20], Chapter 2, Theorem 1A), but we also provide a simple proof for completeness.

Lemma 4.1 *Let d, n be positive integers, let $p \le n^{d/(d-1)}$ be a prime, and let $\mathbf{x} \in \mathbb{F}_p^d \setminus \{0\}$. Then there exists $\mathbf{y} \in \mathbb{F}_p^d$ such that $\mathbf{x} \sim \mathbf{y}$ and $\mathbf{y}(i) \in [-n, n]$ for $i \in [d]$.*

Proof For every $\mathbf{z} \in \mathbb{F}_p^d$ and positive integer t, define the "ball of radius t centered at $\mathbf{z}$" as

$$B_t(\mathbf{z}) = \{\mathbf{v} \in \mathbb{F}_p^d : \forall i \in [d], \mathbf{v}(i) - \mathbf{z}(i) \in [-t, t]\}.$$

Then for $t \leq (p-1)/2$, we have $|B_t(\mathbf{z})| = (2t+1)^d$. Let $t = p^{(d-1)/d}/2$, then t satisfies $p \cdot (2t+1)^d > p^d$. Hence, by the pigeonhole principle, there exists $\lambda_1 \neq \lambda_2 \in \mathbb{F}_p$ such that $B_t(\lambda_1 \mathbf{x}) \cap B_t(\lambda_2 \mathbf{x}) \neq \emptyset$. But then setting $\mathbf{y} = (\lambda_1 - \lambda_2)\mathbf{x} \neq 0$, we have $\mathbf{x} \sim \mathbf{y}$ and $\mathbf{y}(i) \in [-2t, 2t] \subset [-n, n]$. $\qquad\square$

Proof of Theorem 1.5 Let p be a prime such that $n^{d/(d-1)}/2 < p < n^{d/(d-1)}$, which exists by Bertrand's postulate. Let $c = c(d, k)$ be the constant provided by Theorem 1.3, and let $S_0 \subset \mathbb{F}_p^d$ be a multiset of p^{d-k} vectors such that no k-dimensional (linear) subspace contains more than c elements of S_0. By Lemma 4.1, for every $\mathbf{x} \in S_0$ there exists $\mathbf{x}^* \in [-n, n]^d$ such that $\mathbf{x}^* \equiv \lambda\mathbf{x} \pmod{p}$ for some $\lambda \neq 0$. In particular, no k-dimensional linear hyperplane contains more than c elements of $S^* = \{\mathbf{x}^* : \mathbf{x} \in S_0\}$. By the pigeonhole principle, there exists $S' \subset S^*$ of size at least $p^{d-k}/3^d$ such that every element of S' have the same sign-pattern. Let S be the set of vectors we get after changing the 0 entries of the elements of S' to 1, and multiplying the negative coordinates by -1. Then S is contained in $[n]^d$, it has at least $p^{d-k}/3^d \geq n^{d(d-k)/(d-1)}/6^d$ elements, and it is easy to check that no k-dimensional linear hyperplane contains more than c elements of S. $\qquad\square$

Proof of Corollary 1.6 For slight convenience, we consider the grid $[-n, n]^d$ instead of $[n]^d$. This does not change the problem up to the value of C for the following reason. If $[n]^d$ can be covered by N linear hyperplanes of dimension k, then $[-n, n]^d$ can be covered by $3^d N$ linear hyperplanes of dimension k, as we can partition $[-n, n]^d$ into 3^d parts with respect to the signs of the vectors, and each part requires at most N hyperplanes.

Let p be a prime such that $n^{d/(d-1)}/2 < p < n^{d/(d-1)}$, which exists by Bertrand's postulate. For every $\mathbf{x} \in \mathbb{F}_p^d$, let $\mathbf{x}^* \in [-n, n]^d$ be an arbitrary vector such that $\mathbf{x} \sim \mathbf{x}^*$, and let

$$S = \{\mathbf{x}^* : \mathbf{x} \in \mathbb{F}_p^d \setminus \{0\}\} \subset [-n, n]^d.$$

Then $|S| = (p^d - 1)/(p - 1) \geq p^{d-1}$.

Suppose that $S' \subset S$ spans a linear hyperplane of dimension at most k over $\mathbb{R}$. Then S' spans a subspace of $\mathbb{F}_p^d$ of dimension at most k. As S' contains at most one element of each equivalence class of $\sim$, we get that $|S'| \leq (p^k - 1)/(p - 1) \leq 2p^{k-1}$. Hence, any covering of S with linear hyperplanes contains at least $|S|/2p^{k-1} \geq p^{d-k}/2 \geq n^{d(d-k)/(d-1)}/2^{k+1}$ elements. $\qquad\square$

5 Incidences

As the proof of Theorem 1.7 is essentially identical to the proofs of [5] and [2], let us only give a very brief outline of it.

Proof sketch of Theorem 1.7 Let $k = \lfloor d/2 \rfloor - 1$, $n_0 \approx n^{1/(d-k)}$ and $m_0 \approx (m/n_0)^{(d-1)/(dk+2d-1)}$. Let $P \subset [n_0]^d$ be a maximal set of lattice points such that no k-dimensional affine subspace contains more than $c_1 = c(d, k)$ points of P, then

$|P| \approx n_0^{d-k} \approx n$ by Theorem 1.4. Also, let $N \subset [m_0]^d$ be a maximal set of lattice points such that no $(d-k-1)$-dimensional linear subspace contains more than $c_2 = c(d, d-k-1)$ points of N, then $|N| \approx m_0^{d(k+1)/(d-1)}$ by Theorem 1.5. Let $\mathcal{H}$ be the set of all hyperplanes whose normal vector is in N and contains at least one point of P. Then $|\mathcal{H}| \lesssim m_0 n_0 |N| \approx m$ as the scalar product $\langle \mathbf{x}, \mathbf{y} \rangle$ for any $\mathbf{x} \in P$ and $\mathbf{y} \in N$ is contained in $[dm_0 n_0]$. Furthermore, the incidence graph of $(P, \mathcal{H})$ is K_{c_1+1, c_2+1}-free, as the intersection of any $c_2 + 1$ elements of $\mathcal{H}$ is an at most a k-dimensional affine hyperplane. Finally, $I(P, \mathcal{H}) = |P||N|$, as for each $\mathbf{y} \in N$, the hyperplanes in $\mathcal{H}$ with normal vector $\mathbf{y}$ form a partition of P. Plugging in our bounds on $|P|$ and $|N|$ gives the desired result. See [2] for the precise calculations, that give almost the same bounds. $\qquad \square$

References

1. Apfelbaum, R., Sharir, M.: Large complete bipartite subgraphs in incidence graphs of points and hyperplanes. SIAM J. Discrete Math. **21**(3), 707–725 (2007)
2. Balko, M., Cibulka, J., Valtr, P.: Covering lattice points by subspaces and counting point-hyperplane incidences. Discrete Comput. Geom. **61**, 325–354 (2019)
3. Bárány, I., Harcos, G., Pach, J., Tardos, G.: Covering lattice points by subspaces. Period Math. Hung. **43**(1–2), 93–103 (2001)
4. Ben-Aroya, A., Shinkar, I.: A note on subspace evasive sets. Chicago J. Theor. Comput. Sci. **9**, 1–11 (2014)
5. Brass, P., Knauer, C.: On counting point-hyperplane incidences. Comput. Geom. **25**(1–2), 13–20 (2003)
6. Brass, P., Moser, W., Pach, J.: Research Problems in Discrete Geometry. Springer, New York (2005)
7. Bukh, B.: Random algebraic construction of extremal graphs. Bull. Lond. Math. Soc. **47**(6), 939–945 (2015)
8. Chazelle, B.: Cutting hyperplanes for divide-and-conquer. Discrete Comput. Geom. **9**(2), 145–158 (1993)
9. Croot, E., Lev, V., Pach, P.P.: Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. Ann. Math. **185**(1), 331–337 (2017)
10. Dvir, Z., Lovett, S.: Subspace evasive sets, in Proceedings of the forty-fourth annual ACM symposium on Theory of computing 351–358 (2012)
11. Ellenberg, J., Gijswijt, D.: On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. Ann. Math. Second Series **185**(1), 339–343 (2017)
12. Erdős, P.: On extremal problems of graphs and generalized hypergraphs. Israel J. Math. **2**, 183–190 (1964)

13. Furstenberg, H., Katznelson, Y.: A density version of the Hales-Jewett theorem. J. Anal. Math. **57**(1), 64–119 (1991)
14. Guruswami, V.: Linear-algebraic list decoding of folded reed-solomon codes. In Proceedings of the 26th IEEE Conference on Computational Complexity (2011)
15. Konyagin, S., Sudakov, B.: An extremal problem for integer sparse recovery. Linear Algebra Appl. **586**, 1–6 (2020)
16. Kővári, T., Sós, V., Turán, P.: On a problem of K. Zarankiewicz, Colloq. Math. **3**, 50–57 (1954)
17. Lefmann, H.: Extensions of the No-Three-In-Line problem, preprint (2012). www.tu-chemnitz.de/informatik/ThIS/downloads/publications/lefmann_no_three_submitted.pdf
18. Pudlák, P., Rödl, V.: Pseudorandom sets and explicit construction of Ramsey graphs. Quaderni Mat. **13**, 327–346 (2004)
19. Sheffer, A.: Lower bounds for incidences with hypersurfaces, Discrete Analysis Paper No. 16 (2016)
20. Schmidt, W.M.: Diophantine Approximation, Lecture Notes in Mathematics, vol. 785. Springer, Berlin (1980)
21. Szemerédi, E., Trotter, W.T.: Extremal problems in discrete geometry. Combinatorica **3**(3–4), 381–392 (1983)
22. van Lint, J.H.: Introduction to coding theory, 3rd edition, Graduate Texts in Mathematics 86. Springer, Berlin (1999)