Large \((k; r, s; n, q)\)-sets in Projective Spaces

Ferdinand Ihringer, Jacques Verstraëte

11 Nov 2022

Abstract

A \((k; r, s; n, q)\)-set (short: \((r, s)\)-set) of \(\text{PG}(n, q)\) is a set of points \(X\) with \(|X| = k\) such that no \(s\)-space contains more than \(r\) points of \(X\). We investigate the asymptotic size of \((r, s)\)-sets for \(n\) fixed and \(q \to \infty\). In particular, we show the existence of \((3, 2)\)-sets of size \((1 + o(1))q^{3/2}\) for \(n = 6\), \((4, 2)\)-sets of size \((1 + o(1))q^{2/3}\), and \((9, 2)\)-sets of size \((1 + o(1))q^2\) for \(n = 4\). We also generalize a bound by Rao from 1947 and show that an \((r, s)\)-set has size at most \(O(q^{2 - 1})\) if there exist integers \(d, e \geq 2\) such that \(s = d(e - 1)\) and \(r = de - 1\).

1 Introduction

Let \(\text{PG}(n, q)\) denote the finite projective space whose points and lines are the 1- and 2-dimensional subspaces of \(\mathbb{F}_q^n\), respectively. A cap is a set \(X\) of points in \(\text{PG}(n, q)\) such that no line intersects \(X\) in more than 2 points. More generally, a set \(X\) in \(\text{PG}(n, q)\) is commonly called \((k; r, s; n, q)\)-set if each \(s\)-space contains at most \(r\) points of \(X\) and \(|X| = k\). The present work is concerned with \((k; r, s; n, q)\)-sets for fixed \(n\) and asymptotic behavior for \(q \to \infty\). In the following we abbreviate \((k; r, s; n, q)\) as \((r, s)\)-set (as for us \(n\) is fixed, \(k\) not exact, and we consider asymptotics in \(q\)). A \((2, 1)\)-set is known as a cap, a \((r, r - 1)\)-set is known as a generalized cap, a \((n, n - 1)\)-set is known as an arc and corresponds to an MDS code. Hirschfeld surveys upper and lower bounds of \((r, s)\)-sets of maximal size in \([14]\). In other literature \((r, s)\)-sets are known as \((s, r)\)-subspace evasive sets, see also \([13, 15]\).

An \((s, 1)\)-set in \(\text{PG}(n, q)\) has size at most \(O(q^{n-1})\). This bound is known to be tight for \(n = 2, 3\). Segre showed in 1959 \([17]\) (c.f. \([7]\)) that the largest cap has at least size \(\Omega(q^{2n-1})\). The first open case for caps is \(\text{PG}(4, q)\) for which the largest known constructions have size \((3 + o(1))q^2\), see \([8]\). Dvir and Lovett showed in \([5]\) (Theorem 2.4 together with Claim 3.5) that for \(q\) sufficiently large, there exists an \((n, s)\)-set of size \(\frac{1}{2}q^{n-s}\). Also see \([18]\) for a construction using random polynomials (based on the method developed by Bukh in \([3]\)). In Section \([2]\), we give an explicit \((n, 1)\)-set of size \((q - 1)^{n-1}\) in \(\text{PG}(n, q)\).

In Section \([3]\) we establish simple upper and lower bounds on the size of the largest \((r, s)\)-sets for \(r \leq 2s - 1\). Sudakov and Tomon show in \([15]\) Theorem 1.2 that an \((r, s)\)-set with \(r \leq \frac{d}{2} s - 1\) has at most size \(4s \cdot q^{\frac{m(r)}{m(r)}}\) where \(D(r, s) = \lfloor \frac{s}{2(r-s+1)} \rfloor\). The following lower bound was observed for \(s = r - 1\) by Rao \([16]\) p. 136 and Bose \([2]\) Eq. 5.64. Their result has been rediscovered by Tait and Won in 2021.
Lemma 2.2. The curve

Proof.

Put

for $(1, x, y, z)$.

Theorem 2.1. Let $X$ be an $(r, s)$-set in $\text{PG}(n, q)$ such that there exist integers $d, e \geq 2$ with $s = d(e - 1)$ and $r = de - 1$. Then $|X| \leq C_d e q^{r+1} + e$ where $C_d e = \sqrt{e! (d - 1)^{1 + 2d - 1} + 1 - 2q^{-1}}$, for $q > 2e$. Particularly, $|X| \leq C_2 e q^{n + 1} + e = C_2 e q^{2n+1} + e$ for $s = r - 1$ even, and $|X| \leq C_2 e q^{2(n-1)} + e$ for $r = 2s - 1$.

In Section 4 we investigate the special case of planes. In particular, we provide a construction for a $(3, 2)$-set of size $\Theta(q^{3/2})$ in $\text{PG}(6, q)$ which combines algebraic and probabilistic methods. This improves on the trivial lower bound of $\Omega(q^{4/3})$. We also show for $n = 4$ that $(9, 2)$-sets of size $(1 + o(1))q^2$ exist for $q$ sufficiently large, improving the result by Dvir and Lovett for that case. We conclude in Section 5 with product type constructions for $(r, s)$-sets using field reduction.

2 Lines

Throughout the whole text, we identify a vector of the form $(1, x_1, \ldots, x_n)$ with the (affine) point $((1, x_1, \ldots, x_n))$ of $\text{PG}(n, q)$. We assume that $n \geq 2$. Our main result on lines is as follows:

Theorem 2.1. There exists a $(n, 1)$-set of size $(q - 1)^{n-1}$ in $\text{PG}(n, q)$.

We shall prove this in two lemmas. Let $x \in \mathbb{F}_q^{n-1}$. Define

$$F_0(x) = \prod_{i=1}^{n-1} x_i, \quad F_i(x) = x_i F_0(x) \text{ for } i \in \{1, \ldots, n-1\}.$$ 

Put $F(x) = (1, F_0(x), \ldots, F_{n-1}(x))$. We denote $\mathbb{F}_q \setminus \{0\}$ by $\mathbb{F}_q^*$ and write $\mathbb{F}_q^{n-1}$ for $(\mathbb{F}_q^*)^{n-1}$. Put $X = \{F(x) : x \in \mathbb{F}_q^{n-1}\}$.

Lemma 2.2. The curve $X$ has $(q-1)^{n-1}$ points.

Proof. Let $u \in X$. Then there exists an $x \in \mathbb{F}_q^{n-1}$ such that $u = F(x)$. As $x_1 \cdots x_{n-1} \neq 0$, we have $x = (u_2/u_1, \ldots, u_n/u_1)$.

Lemma 2.3. No line intersects $X$ in more than $n$ points.

Proof. Suppose that three distinct points $u, v, w \in X$ with $u = F(x), v = F(y)$, and $w = F(z)$ for $x, y, z \in \mathbb{F}_q^{n-1}$ are collinear. Then the following matrix has rank 2 (if the rank is 1, then $x = y = z$; if the rank is 3, then $\langle u, v, w \rangle$ is a plane):
By subtracting $z_i$-times the second row from the $(i+1)$-th row for $i \in \{1, \ldots, n-1\}$ and subtracting $F_0(z)$-times the first row from the second, we obtain

$$M := \begin{pmatrix} 1 & 1 & 1 \\ F_0(x) - F_0(z) & F_0(y) - F_0(z) & 0 \\ (x_1 - z_1)F_0(x) & (y_1 - z_1)F_0(y) & 0 \\ (x_2 - z_2)F_0(x) & (y_2 - z_2)F_0(y) & 0 \\ \vdots & \vdots & \vdots \\ (x_{n-1} - z_{n-1})F_0(x) & (y_{n-1} - z_{n-1})F_0(y) & 0 \end{pmatrix}. $$

Consider

$$M' := \begin{pmatrix} F_0(x) - F_0(z) & F_0(y) - F_0(z) \\ (x_1 - z_1)F_0(x) & (y_1 - z_1)F_0(y) \\ (x_2 - z_2)F_0(x) & (y_2 - z_2)F_0(y) \\ \vdots & \vdots \\ (x_{n-1} - z_{n-1})F_0(x) & (y_{n-1} - z_{n-1})F_0(y) \end{pmatrix}. $$

The matrix $M$ has rank 2 if and only if $M'$ has rank 1. This is precisely the case when all $(2 \times 2)$-submatrices $\tilde{M}$ of $M'$ have rank at most 1, that is $\det(\tilde{M}) = 0$. Hence, we obtain that

$$(F_0(x) - F_0(z))F_0(y)(y_i - z_i) = (F_0(y) - F_0(z))F_0(x)(x_i - z_i) \quad (1)$$

for $i \in \{1, \ldots, n-1\}$, and

$$(x_1 - z_1)(y_i - z_i) = (y_1 - z_1)(x_i - z_i) \quad (2)$$

for $i \in \{2, \ldots, n-1\}$. Here we use that $F_0(x), F_0(y) \neq 0$.

We want to show that no line contains more than $n$ points.

If $F_0(x) = F_0(y) = F_0(z)$, then the equations in (2) plus $F_0(x) = F_0(y) = F_0(z)$ determine the entries of $z$ as the solution to polynomials of degree $n-1$. Hence, there are at most $n-3$ nontrivial solutions for $z$.

Otherwise, Equation (1) for $i = 1$ together with the equations in (2) determines the entries of $z$ as the solution to polynomials of degree $n$. Hence, we have at most $n-2$ nontrivial solutions.

Note that the points of $X$ lie on the affine curve

$$X_1^n - X_2 \cdots X_n = 0,$$

and (if we switch the first two coordinates) the projective curve

$$X_0^n - X_1 X_2 \cdots X_n = 0.$$

It seems to be highly natural do study these curves over finite fields. Note that the canonical affine part of the last curve, that is

$$\{(1, \frac{1}{x_1 \cdots x_{n-1}}, x_1, x_2, \ldots, x_{n-1}) : x \in F_q^{*n-1}\},$$

satisfies Lemma 2.2 and Lemma 2.3 as well.
Hence, if we take \( p \in X \) entry in the table, indexed by \( r \) and \( r - s \).

\[ \begin{array}{|c|ccccc|}
\hline
r - s & 1 & 2 & 3 & 4 & 5 & 6 \\
\hline
s = 1 & n-1 & & & & & \\
s = 2 & \frac{n-1}{2} & n-2 & & & & \\
s = 3 & \frac{n-2}{3} & \frac{n-1}{2} & n-3 & & & \\
s = 4 & \frac{n-2}{3} & \frac{n-3}{2} & \frac{n-2}{2} & n-4 & & \\
s = 5 & \frac{n-3}{4} & \frac{n-3}{2} & \frac{n-3}{2} & \frac{n-2}{2} & \frac{n-1}{2} & n-5 \\
s = 6 & & & & & & n-6 \\
\hline
\end{array} \]

Table 1: The upper bounds \( O(q^m) \) on the size of a \((r,s)\)-set from Theorem 1.1.

Lemma 3.3 and Lemma 3.2 for small \( s \) and sufficiently large \( n \). Here \( m \) is the entry in the table, indexed by \( r \) and \( r - s \).

3 Simple Bounds on \((r,s)\)-Sets

We write \( \binom{n+1}{k+1} \) for the number of \( k \)-spaces in \( \text{PG}(n,q) \). For our estimates, we will use that \( \binom{n+1}{k+1} = (1 + o(1))q^{k+1}(n-k) \) (as \( q \to \infty \)). The following result was observed for \( s = r - 1 \) by Gilbert [11, I.4] and Varshamov [20] and is well-known in coding theory as the Gilbert-Varshamov bound.

Lemma 3.1. Let \( s + 1 \geq r \geq 3 \). There exists a \((r,s)\)-set in \( \text{PG}(n,q) \) of size \( (\frac{r+1}{r!} + o(1))q^{n-s-s(n-s)/r} \) (as \( q \to \infty \)).

Proof. Delete points from \( \text{PG}(n,q) \) with probability \( p \). Let \( X \) denote the resulting set of points. For a random \( s \)-space \( S \), we have

\[ \mathbb{P}(|X \cap S| \geq r + 1) \leq \binom{r+1}{r+1} p^{r+1}. \]

Hence, if we take \( p = (1 + o(1))q^{-s(n-s)/r - s} \) and let \( S \) denote the set of \( s \)-spaces which meet \( X \) in at least \( r + 1 \) points, then

\[ \mathbb{E}(|S|) \leq \binom{n+1}{s+1} \binom{r+1}{r+1} p^{r+1} = \frac{1}{(r+1)!} (1 + o(1))q^{n-s-s(n-s)/r}. \]

Furthermore, we have

\[ \mathbb{E}(|X|) = p \binom{n+1}{1} = (1 + o(1))q^{n-s-s(n-s)/r}. \]

Hence, we can delete the at most \((r + 1) \cdot \frac{1}{(r+1)!} (1 + o(1))q^{n-s-s(n-s)/r}\) points of \( X \) in any \( s \)-space that intersects \( X \) in at least \( r + 1 \) points and we obtain an \((r,s)\)-set of size

\[ \frac{r!-1}{r!} (1 + o(1))q^{n-s-s(n-s)/r}. \]

The following statement was already observed by Gulati [12] for \( s = r - 1 \).

Lemma 3.2. Let \( m \geq 1 \). Let \( B \) be the maximal size of an \((r,s)\)-set in \( \text{PG}(n,q) \). Then \(|X| - m \leq B\) for an \((r + m, s + m)\)-set \( X \) in \( \text{PG}(n + m, q) \).

Proof. Let \( S \) be the subspace spanned by \( m \) points of \( X \). The projection of \( X \setminus S \) onto a complement of \( S \) is an \((r,s)\)-set in \( \text{PG}(n,q) \).
Recall for the following that an \((r,s)\)-set with \(r \leq s\) contains at most \(r\) points. If an \((r,s)\)-set \(X\) meets an \(m\)-space \(S\) in \(d\) points of \(X\) for some \(d \leq r\), then in the quotient of \(S\) we find an \((r-d,s-m-1)\)-set \(X'\) of size \(|X|-d\). If \(s-m-1 \geq r-d\), then \(|X'| \leq r-d\), so \(|X| \leq r\). We call an \((r,s)\)-set \(X\) proper if no \(m\)-space contains \(m+1+r-s\) (or more) points. Any \((r,s)\)-set \(X\) with \(|X| > r\) is proper.

**Proof of Theorem 1.1.** Any \(e = s/d+1\) points of \(X\) span a subspace of dimension at most \(e-1\). Let \(Y_1, \ldots, Y_d \subseteq X\) sets of size \(e\). Let \(\hat{Y}_i\) denote the set of points of \(\PG(n,q)\) in \(\langle Y_i \rangle \setminus X\), but not in the span of any \((e-1)\)-subset of \(Y_i\).

Put \(y = |\bigcup_{i=1}^d \hat{Y}_i|\). We claim that \(\bigcap_{i=1}^d \hat{Y}_i\) spans a subspace of dimension at most \((y - d + 1) - 1 = y - d\) that contains at least \(y\) points of \(X\). But \(y - d + 1 + r - s = y\), so \(X\) is not proper, thus \(|X| \leq r\) and we are done.

Hence, a point \(P\) not in \(X\) lies in at most \(d-1\) sets \(\hat{Y}_i\). Double count \(e\)-tuples \(Y \subseteq X\) and points \(P\) not in \(X\) with \(P \in \langle Y \rangle\). We obtain that

\[
\left(\binom{|X|}{e}\right) \left(\binom{e}{1} - \binom{e}{e-1} \right) \leq (d-1) \left(\binom{n+1}{1} - |X|\right).
\]

Using \(1 \leq \binom{m}{1}/q^{m-1} \leq 1 + 2q^{-1} \leq 2\), we obtain

\[
\frac{(|X|-e)^e}{e!} q^{e-1} (1 - 2eq^{-1}) \leq (1 + 2q^{-1})(d-1)q^n.
\]

Rearranging for \(|X|\) yields the assertion. The special cases are for \(d = 2\) and \(e = 2\).

**Lemma 3.3.** Let \(X\) be a \((r,s)\)-set in \(\PG(n,q)\) with \(s \geq 1\). Then \(|X| \leq r \left(\binom{n-s+1}{1}+1\right)\).

**Proof.** Fix a \((r-1)\)-space \(S\) which intersects \(X\) in at least \(s\) points. Then each \(s\)-space \(T\) in \(\PG(n,q)\) through \(S\) contains at most \(r\) elements of \(X\). There are \(\binom{n-s+1}{1}\) such \(T\).

4 Planes

4.1 Plane Sets in \(\PG(6,q)\)

We construct a \((3,2)\)-set of size \((1+o(1))q^{3/2}\) in \(\PG(6,q)\). The (trivial) lower bound from Lemma 3.3 is \(\Omega(q^{4/3})\), while the (trivial) upper bound from Theorem 1.1 is \(O(q^{5/2})\). Put

\[X = \{(1, x, x^2, x^3, y, y^2, y^3) : x, y \in F_q\}.\]

Clearly, \(|X| = q^2\).

**Lemma 4.1.** Let \(s_1, s_2, s_3, s_4 \in X\) be four pairwise distinct points in a plane of \(\PG(6,q)\) with \(s_1 = (1, x_1, x_1^2, x_1^3, y_1, y_1^2, y_1^3)\). Then it holds that \(|\{x_1, x_2, x_3, x_4\}| = |\{y_1, y_2, y_3, y_4\}| = 2\).
Theorem 1.1 gives

\[
\begin{pmatrix}
1 & 1 & 1 & 1 \\
x_1 & x_2 & x_3 & x_4 \\
x_1' & x_2' & x_3' & x_4' \\
y_1 & y_2 & y_3 & y_4 \\
y_1' & y_2' & y_3' & y_4'
\end{pmatrix}
\]

has at most rank 3. The top-left $4 \times 4$ submatrix of $M$ is a Vandermonde matrix of rank at most 3. Hence, if the $x_1, x_2, x_3$ are pairwise distinct, then $x_4 \in \{x_1, x_2, x_3\}$. If $x_4 = x_i$ for some $i \in \{1, 2, 3\}$, then also $y_4 = y_i$. But then $s_4 = s_i$ which is a contradiction. Hence, $|\{x_1, x_2, x_3, x_4\}| \leq 2$, and similarly, $|\{y_1, y_2, y_3, y_4\}| \leq 2$. If any of the inequalities above is not obtained, then again two $s_i$ are identical, so this does not happen.

Let $G$ be a bipartite $C_4$-free graph with $(1 + o(1))q^{3/2}$ edges and $q$ vertices in each half of the bipartition. Such graphs exists, for instance see [11] §3.1. Identify the points and lines of $G$ with two distinct copies of $\mathbb{F}_q$. Put

\[X' = \{(1, x, x^2, x^3, y, y^2, y^3) : x, y \in \mathbb{F}_q, xy \text{ is an edge of } G\}.\]

**Theorem 4.2.** We have $|X'| = (1 + o(1))q^{3/2}$ and $X'$ is a $(3, 2)$-set.

**Proof.** The graph $G$ has $(1 + o(1))q^{3/2}$ edges, so $|X'| = (1 + o(1))q^{3/2}$. Lemma 4.1 says that four point $s_1, s_2, s_3, s_4$ in $X$ which lie in a plane are precisely those with WLOG $x_1 = x_2, x_3 = x_4, y_4 = y_1$, and $y_2 = y_3$ (in the notation of Lemma 4.1). This does not happen in $X'$ as $(x_1, y_1), (x_1, y_2), (x_3, y_2), (x_3, y_1)$ would correspond to a quadrangle in $G$.

Now assume that $q = q_0^2$ for some prime power $q_0$. In this case there exists a natural choice for $G$. Let $G'$ be the incidence graph of $\text{PG}(2, q_0)$. It is well-known that the graph $G$ is $C_4$-free. Remove all points on a fixed line $L$ from $G$, and remove all lines on a fixed point on $L$ from $G$. Then $G'$ has $q$ lines and $q$ points. (If one wishes for a completely explicit construction, then identifying $\mathbb{F}_q$ with $\mathbb{F}_{q_0}^2$ is a natural choice.) Let $X''$ be the point set $X'$ with $G'$ for $G$.

**Corollary 4.3.** For $q$ a square, we have $|X''| = q^{3/2}$ and $X''$ is a $(3, 2)$-set.

### 4.2 Random $(4, 2)$-sets from Quadrics

Theorem 1.1 gives $(\sqrt{2} + o(1))q^{n-1}$ as an upper bound for $(3, 2)$-sets in $\text{PG}(n, q)$, that is a set of points with at most 3 in each plane. Here we show that one can obtain examples of that size if we allow up to 4 points on a plane, so $(4, 2)$-sets. Note that for $(4, 2)$-sets we only have Lemma 4.1, which states an upper bound of $O(q^{n-2})$.

**Theorem 4.4.** Let $m \geq 2$ and put $n = 2m - 1$. There exists a $(4, 2)$-set in $\text{PG}(n, q)$ of size $(1 + o(1))q^{n-1}$. 

6
Proof. Let $Q_1, \ldots, Q_m$ be random irreducible quadrics. Put $X = \bigcap_{i=1}^m Q_i$. As $Q_i$ has $(1 + o(1))q^{n-1}$ points, we find $\mathbb{E}(|X|) = (1 + o(1))q^{n-m} = (1 + o(1))q^{m-1}$. Recall that a conic is determined by 5 points, two conics intersect in at most 4 points, and that there are $(1 + o(1))q^5$ conics in $\text{PG}(2, q)$.

Let $C_1$ and $C_2$ be random conics. Then

$$\mathbb{P}(|C_1 \cap C_2| > 4) = \mathbb{P}(|C_1 \cap C_2| = q + 1) = (1 + o(1))q^{-5}. $$

Let $\mathcal{C}$ be the set of planes which intersect $X$ in a conic plane. There are $(1 + o(1))q^{3(n-2)}$ conic planes in $Q_1$. Hence,

$$\mathbb{E}(|\mathcal{C}|) = (1 + o(1))q^{3(n-2)} \cdot (1 + o(1))q^{-5(m-1)} = (1 + o(1))q^{-m+4}. $$

Hence, the expected number of points of $X$ in a conic plane is at most $(1 + o(1))q^{-m+3}$ as each of them has at most $q + 1$ points in $X$.

Let $L_1$ and $L_2$ be random singular lines in two of the quadrics. Then $\mathbb{P}(L_1 = L_2) = (1 + o(1))q^{-3}$. Let $\mathcal{L}$ be the set of lines which are completely contained in $X$. There are $\binom{n+1}{2} = (1 + o(1))q^{2(n-1)}$ lines in $\text{PG}(n-1, q)$, so

$$\mathbb{E}(|\mathcal{L}|) = (1 + o(1))q^{2(n-1)} \cdot (1 + o(1))q^{-3m} = q^{-m-4}. $$

Hence, we can delete all points of $X$ in conic planes and complete lines to obtain some $X'$ with $\mathbb{E}(|X'|) = (1 + o(1))\mathbb{E}(|X|) = (1 + o(1))q^{-m+1}$.  

4.3 Random $(9, 2)$-sets from Cubic Curves

Lemma 4.5 gives $O(q^2)$ as an upper bound for a $(9, 2)$-set in $\text{PG}(4, q)$. Dvir and Lovett show that there exists a $(16, 2)$-set. Here we show that cubic polynomials give rise to a $(9, 2)$-set of size $(1 + o(1))q^2$.

**Lemma 4.5.** In $\text{PG}(2, q)$ the number of irreducible cubic curves is $(1 + o(1))q^9$, the number of reducible cubic curves containing a conic is $O(q^7)$, and the number of reducible cubic curves containing no conic is $O(q^6)$.

**Proof.** Nine points determine a cubic curve. As 9 points in general position determine a cubic, the number is at least

$$(1 + o(1))\frac{q^{2 \cdot 9}}{q^9} = (1 + o(1))q^9. $$

Next we estimate the number of reducible cubic curves. These consist of three lines, or a line and a conic. Recall that there are $O(q^2)$ lines and $O(q^5)$ quadratic curves in $\text{PG}(2, q)$.

**Lemma 4.6.** Let $C_1, C_2$ two random irreducible cubic curves in $\text{PG}(2, q)$. Then

$$\mathbb{P}(|C_1 \cap C_2| > 9) \leq (1 + o(1))q^{-9}. $$

**Proof.** By Bézout’s Theorem, $|C_1 \cap C_2| \leq 9$ or $C_1 = C_2$. Lemma 4.5 shows the assertion.

**Theorem 4.7.** There exists a $(9, 2)$-set in $\text{PG}(4, q)$ of size $(1 + o(1))q^2$. 

7
Proof. Let $C_1, C_2$ be random cubic surfaces. Put $X = C_1 \cap C_2$. As $|C_1| = (1 + o(1))q^9 = |C_2|$. Let $Y_{i,j}$ be the set of planes which intersects $C_1 \cap C_2$ in more than 9 points and have an $i$-space (respectively, $j$-space) as the largest subspace contained in $C_1$ (respectively, $C_2$). By Lemma 4.5
\[ \mathbb{E}(|Y_{i,j}|) = \left[ \frac{n}{q} \right] q^{-9} < (1 + o(1))q^{-1} \text{ for } j \in \{0, 1, 2\}. \]
By Lemma 4.5 \[ \mathbb{E}(|Y_{i,j}|) = \left[ \frac{n}{q} \right] q^{-2} < 1 + o(1) \text{ for } j \in \{0, 1\}. \]
Hence, by Lemma 4.6, we can delete the at most $(1 + o(1))q$ points of $X$ in $\bigcup Y_{i,j}$ and obtain a $(9, 2)$-set of size $(1 + o(1))q^2$. \qed

5 Product Constructions via Field Reduction

We present a generic product construction for $(r, s)$-sets.

**Lemma 5.1.** Let $X$ be a proper $(r, r-1)$-set in $\text{PG}(N-1, q)$ and let $Y$ be an $(r, s)$-set in $\text{PG}(M-1, q^N)$. Then there exists an $(r, s)$-set in $\text{PG}(NM-1, q)$ of size $|X| \cdot |Y|$.

**Proof.** By field reduction, the elements of $Y$ correspond to $(N-1)$-spaces in $\text{PG}(NM-1, q)$. Arbitrarily pick a copy of $X$ in each such $(N-1)$-space. We obtain a set $Z$ of size $|X| \cdot |Y|$.

It remains to show that $Z$ is an $(r, s)$-set. For this, consider a $s$-space $S$. Let $T_1, \ldots, T_m$ be the set of $(N-1)$-spaces in $Y$ which $S$ meets. As $Y$ is an $(r, s)$-set, $\sum_{i=1}^{m} \dim(S \cap T_i) + 1 \leq r$. As $X$ is a proper $(r, r-1)$-set, $|S \cap T_i \cap Z| \leq \dim(S \cap T_i) + 1$. As $S \cap Z = \bigcup_{i=1}^{m} S \cap T_i \cap Z$, $Z$ is a $(r, s)$-set. \qed

This way we obtain

(i) caps of size $(1 + o(1))q^{\frac{n}{2}}$ in $\text{PG}(n, q)$ for $n = 4^m - 1$ by multiplying $m$ ovoids of $\text{PG}(3, q)$ (This is best known, see [7]);

(ii) $(3, 2)$-sets of size $(1 + o(1))q^{\frac{n}{2}}$ in $\text{PG}(n, q)$ for $n = 4^m - 1$ by multiplying $m$ rational normal curves of $\text{PG}(4, q)$ (Lemma 5.1 $Cq^{\frac{n}{2}}$);

(iii) $(3, 2)$-sets of size $(1 + o(1))q^{\frac{n}{2}}$ in $\text{PG}(n, q)$ for $n = 7 \cdot 4^m - 1$ by multiplying the Construction in Theorem 4.2 with $m-1$ rational normal curves of $\text{PG}(4, q)$;

(iv) $(r, r-1)$-sets of size $(1 + o(1))q^{\frac{n}{r-1}}$ in $\text{PG}(n, q)$ for $n = (c+1)^m - 1$ by multiplying $m$ rational normal curves of $\text{PG}(c, q)$ (Lemma 5.1 $Cq^{\frac{n}{r-1}}$).

6 Concluding Remarks

Let us conclude with some open problems and conjectures. For $q$ fixed and $n \to \infty$, Ellenberg and Gijswijt famously showed that a cap has at most size $O(2.756^n)$ [9], while a cap due to Edel has size $\Omega(2.2174^n)$ [6]. Note that the results by Ellenberg and Gijswijt have been generalized to $(r, r-1)$-sets in [1].

For our setting of $q \to \infty$ and $n$ fixed, we believe the following to be true.

**Conjecture 6.1.** There exists a constant $\varepsilon > 0$ such that the size of a cap in $\text{PG}(n, q)$ is bounded by $O(q^{n-1-\varepsilon})$. 
**Problem 6.2.** Find a set of $\Omega(q^3)$ points in $\text{PG}(4,q)$ with at most $O(q^5)$ triples of collinear points.

Using [4, Theorem 3], such an $(r,1)$-set implies the existence of a cap of size $C'q^2\sqrt{\log q}$ in $\text{PG}(4,q)$. This approach was suggested by Dhruv Mubayi.

The rational normal curve gives an example of size $q+1$ for a set of points with no 4 coplanar (a $(3,2)$-set), while in $\text{PG}(4,q)$ the best known upper bound is $(\sqrt{2} + o(1))q^{2\frac{3}{2}}$. In light of this, the following is the first important open problem in the investigation of $(r,s)$-sets.

**Problem 6.3.** Find a $(3,2)$-set in $\text{PG}(4,q)$ of size $\Omega(q^{1+\varepsilon})$.

**Acknowledgment** We thank David Conlon, Dhruv Mubayi, Leo Storme, Benny Sudakov, and István Tomon for comments on an earlier version of this document. The first author is supported by a postdoctoral fellowship of the Research Foundation – Flanders (FWO).

**References**

[1] M. Bennett, **Bounds on sizes of generalized caps in $\text{AG}(n,q)$ via the Croot-Lev-Pach polynomial method**, J. Combin. Theory Ser. A 168 (2019) 255–271.

[2] R. C. Bose, **Mathematical Theory of the Symmetrical Factorial Design**, Sankhya 8(2) (1947) 107–166.

[3] B. Bukh, **Random algebraic construction of extremal graphs**, Bull. London Math. Soc. 47 (2015) 939–945.

[4] R. A. Duke, H. Lefmann, V. Rödl, **On Uncrowded Hypergraphs**, Random Structures and Algorithms 6(2–3) (1995) 209–212.

[5] Z. Dvir, S. Lovett, **Subspace Evasive Sets**, STOC ’12: Proceedings of the forty-fourth annual ACM symposium on Theory of computing (2012) 351–358.

[6] Y. Edel, **Extensions of generalized product caps**, Des. Codes Cryptogr. 31(1) (2004) 5–14.

[7] Y. Edel, J. Bierbrauer, **Recursive constructions for large caps**, Bull. Belg. Math. Soc. 6 (1999) 249–258.

[8] Y. Edel, J. Bierbrauer, **Caps of order $3q^2$ in affine 4-space in characteristic 2**, Finite Fields Appl. 10 (2004) 168–182.

[9] J. S. Ellenberg, D. Gijswijt, **On large subsets of $\mathbb{F}_q^n$ with no three-term progression**, Ann. of Math. 185 (2017) 339–343.

[10] Z. Füredi, M. Simonovits, **The History of Degenerate (Bipartite) Extremal Graph Problems**, pp. 169–264 in: Erdős Centennial, Springer Berlin Heidelberg, 2013.
[11] E. N. Gilbert, *A comparison of signalling alphabets*, Bell System Tech. J. 31 (1952) 504–522.

[12] B. R. Gulati, *On maximal (k, t)-sets*, Ann. Inst. Statist. Math. 23 (1971) 279–292, 527–529.

[13] V. Guruswami, *Linear-algebraic list decoding of folded Reed-Solomon codes*, in: Proceedings of the 26th IEEE Conference on Computational Complexity, 2011.

[14] J. W. P. Hirschfeld, *Maximum sets in finite projective spaces*, Surveys in Combinatorics Invited Papers for the Ninth British Combinatorial Conference 1983, 55–76, 1983.

[15] P. Pudlák, V. Rödl, *Pseudorandom sets and explicit construction of Ramsey graphs*, Quaderni di Matematica 13 (2004) 327–346.

[16] C. R. Rao, *Factorial experiments derivable from combinatorial arrangements of arrays*, J. Roy. Statist. Soc. 9 (1947) 128–139.

[17] B. Segre, *Le geometrie di Galois*, Ann. Mat. Pura Appl. 48(4) (1959) 1–96.

[18] B. Sudakov, I. Tolom, *Evasive sets, covering by subspaces, and point-hyperplane incidences*, arXiv:2207.13077 [math.CO] (2022).

[19] M. Tait and R. Won, *Improved Bounds on Sizes of Generalized Caps in AG(n, q)*, SIAM J. Discrete Math. 35(1) (2021) 521–531.

[20] R. R. Varshamov, *Estimate of the number of signals in error correcting codes*, Dokl. Akad. Nauk SSSR 117 (1957) 739–741.