Bounds on sizes of caps in $AG(n, q)$ via the Croot-Lev-Pach polynomial method

Michael Bennett

June 15, 2018

Abstract

In 2016, Ellenberg and Gijswijt employed a method of Croot, Lev, and Pach to show that a maximal cap in $AG(n, 3)$ (sometimes referred to as a cap set) has size $O(2^{0.756n})$. In this paper, we show that the result can be extended to caps in $AG(n, q)$ for arbitrary $q$; that is, subsets of $AG(n, q)$ containing no three points on a line are exponentially small. Moreover, we will generalize the notion of caps and find upper bounds on the sizes of subsets of $AG(n, q)$ containing no $m$ points on any $(m-2)$-flat.

1 Introduction and main theorem

Let $q$ be a power of a prime. A cap is a set of points in the projective geometry $PG(n, q)$, no three of which lie on a common line. A cap $A$ is maximal if for any other cap $B$, $|B| \leq |A|$, and we denote the size of a maximal cap in $PG(n, q)$ by $m_2(n, q)$. Caps may be similarly defined in the affine space $AG(n, q)$. The problem of finding maximal caps has been studied extensively in both types of spaces (see for instance, [9] or [11]). One of the primary motivations behind the study of caps is their application to coding theory. See, for instance, section 17.2 of [2] for a detailed explanation of the connection between caps and linear codes.

One question that arises in the investigation of maximal caps is how they grow with $n$. In particular, we would like to find bounds on

$$
\mu(q) = \limsup_{n \to \infty} \frac{\log_q (m_2(n, q))}{n}.
$$

While we will be working exclusively in affine space in this paper, note that if $A$ is a maximal cap in $AG(n, q)$, then a maximal cap in $PG(n, q)$ has at most $|A|(1 + o(1))$ points. Therefore, any bounds on $\mu(q)$ apply to both affine and projective space. Trivially, we have $\mu(q) \leq 1$, and a lower bound of $2/3$ can be achieved quite easily: it is well known that a maximal cap $P \subset AG(3, q)$ has $q^2$ points (see, for instance, [5]). Then $P^k \subset AG(3k, q)$ is a cap of $q^{2k}$ points.

Recently, the problem of finding better estimates for $\mu(3)$ has been of great interest. It was long suspected that $\mu(3) < 1$, but it took some time to find an appropriate method of attack. In 1985, Meshulam ([8]) proved that $m_2(n, 3) < \frac{2}{n} \cdot 3^n$ using Fourier techniques. In 2011, Bateman and
Katz ([1]) combined these Fourier techniques with spectral methods to show that there is an $\epsilon > 0$ independent of $n$ so that $m_2(n, 3) = O\left(\frac{3^n}{n^{1+\epsilon}}\right)$. It was not until 2016 that Ellenberg and Gijswijt ([3]) used a polynomial method developed by Croot, Lev, and Pach ([3]) to show that $\mu(3) < 0.923$, rendering the problem essentially solved. Note, however, that this result is not known to be sharp. Currently, the best known bounds are (approximately) $0.724 < \mu(3) < 0.923$, with the lower bound due to Edel ([4]).

In 2001, Hirschfeld and Storme collected the best known bounds on maximal caps in $PG(n, q)$. While they are nontrivial, one can see in [7] that the best upper bounds for $m_2(n, 3)$ are $O(q^{n-1})$ (tables 4.4(i) and (ii)), while the lower bounds are $O(q^{2n/3})$ (tables 4.6(i), (ii),(iii)). In terms of $\mu(q)$, this still leaves us with the trivial bounds mentioned above: $2/3 \leq \mu(q) \leq 1$. The goal of this paper is to extend this result to caps in $AG(n, q)$ and obtain $\mu(q) < 1 - \epsilon$, where $\epsilon$ is roughly $\log_q\left(\frac{3}{2}\right)$. When $q$ is large, the gap between $2/3$ and $1 - \epsilon$ is still quite significant; it seems that there is more work to be done before we have a good understanding of maximal caps in higher dimensions. It is also important to mention that the bound on $m_2(n, q)$ that we will derive here is only competitive with the trivial $m_2(n, q) < O(q^{n-1})$ when $n$ is much larger than $\log(q)$.

In our main result, we will be looking at a generalization of caps. Rather than just restricting the number of points on lines, we can restrict the number of points on $k$-dimensional affine subspaces of $AG(n, q)$.

Definition 1.1. For any integer $m \geq 3$, a set $A \subset AG(n, q)$ is $m$-general if no $m$ points of $A$ lie on a single $(m-2)$-flat. Equivalently, $A$ is $m$-general if any $m$-point subset of $A$ is in general position.

Note that a cap is the same as a $3$-general set. In the language of [7], an $m$-general set $A$ is essentially the same as an $(|A|, m - 1)$-set, though by our definition, any $m$-general set is also $k$-general for $3 \leq k \leq m$. If the maximum size of an $m$-general set is $M_{m-1}(n, q)$ (the notation used in [7]), let

$$\mu_m(q) = \limsup_{n \to \infty} \frac{\log_q(M_{m-1}(n, q))}{n}.$$  

Trivially, we have $\frac{1}{m-1} \leq \mu_m(q) \leq 1$. The lower bound is due to the following observation: Suppose $A$ is an $m$-general set in $AG(n, q)$. Then there are precisely $\binom{|A|}{m-1}$ distinct $(m-2)$-flats each containing $m-1$ points of $A$. The sum of these flats covers at most $q^{n-2}\binom{|A|}{m-1}$ points of $AG(n, q)$. So as long as $q^{n-2}\binom{|A|}{m-1} < q^n$, there are other points that can be added to $A$ to create a larger $m$-general set. Solving for $|A|$ gives the result.

Theorem 1.2. Let $n$ be a positive integer, $q$ a power of a prime $p$, and $m$ an integer such that $3 \leq m \leq n+2$. Suppose also that $q$ is odd, or $m$ and $q$ are both even. Then

$$M_{m-1}(n, q) < 2m + m \cdot \min_{t \in (0,1)} \left(t^{\frac{m-1}{m-2}} \cdot \frac{1-t^q}{1-t}\right)^n \leq 2m + m \cdot \left(\frac{me^{1-\alpha}}{m^2 - \alpha m + \alpha q + C}\right)^n,$$

where $C$ depends only on $m$ and $0 < \alpha < 1$.

In particular, this tells us that

$$\mu_m(q) \leq 1 - \log_q\left(\frac{m^2 - \alpha m + \alpha q + C}{me^{1-\alpha}}\right) + O((q \log q)^{-1}). \quad (1.1)$$
Remark 1.3. The restriction \( m \leq n + 2 \) makes sense, as in the space \( AG(n, q) \), it is not possible to have \( n + 2 \) points in general position. On the other hand, the omission of the case where \( q \) is even and \( m \) is odd is not founded on any geometric principles; it is merely an artifact of the methodology we will see here. It is very possible that a similar result holds for this case using a slightly different approach.

2 Rank of a function

Our result relies heavily on the methods of Croot, Lev, and Pach as outlined by Tao in \([10]\). Tao introduces the “rank” of a function, which has a close connection with matrix rank:

**Definition 2.1.** The function \( F : A^k \to X \) is said to have rank \( r \) \((\text{rank}(F) = r)\) if \( r \) is the smallest integer that allows us to write

\[
F(x_1, x_2, \ldots, x_k) = \sum_{n=1}^{r} f_n(x_{m_n})g_n(x_1, \ldots, x_{m_n-1}, x_{m_n+1}, \ldots, x_k),
\]

for some \( m_n \in \{1, 2, \ldots, k\} \) and functions

\[
f_n : A \to X \quad g_n : A^{k-1} \to X.
\]

For instance, if \( F : \mathbb{R}^2 \to \mathbb{R} \), where

\[
F(x, y) = x^2y + xy^2 + 2x + y^2 + y + 2,
\]

then \( F \) has rank 2, since \( F(x, y) \) can be written as \((x^2 + 1)y + (x + 1)(y^2 + 2)\) but cannot be written in the form \( f(x)g(y) \). We will occasionally abuse notation and write, for instance, “\( \text{rank}(x^2y + xy^2 + 2x + y^2 + y + 2) = 2 \)” when we mean “\( \text{rank}(F) = 2 \).”

It is important to note here that the rank of a function depends on the number of variables \( F \) takes. If \( F \) is a function of \( k \) variables, but only \( k - 1 \) of them appear in the definition of \( F \), then the rank of \( F \) is 1 (or 0 if \( F \) is identically 0). For instance,

\[
F(x, y, z) = x^2y + xy^2 + 2x + y^2 + y + 2
\]

is a rank 1 function, since \( F(x, y, z) = f(z)g(x, y) \), where \( f(z) = 1 \) and \( g(x, y) = F(x, y, 0) \). When clarity is needed, we will say that the \( \text{k-rank} \) of \( F \) is \( r \) \((\text{rank}_k(F) = r)\) to stress that its rank, as a function of \( k \) variables, is \( r \).

Before looking at some properties of rank, we introduce a useful bit of notation:

**Definition 2.2.** Let \( A = \{a_1, \ldots, a_{|A|}\} \) be a finite set and \( f \) a function on \( A \). We define \( \nu_{\text{row}}(f), \nu_{\text{col}}(f) \) to be the \( |A| \)-dimensional row vector and column vector with \( f(a_i) \) in the \( i^{\text{th}} \) position.
Proposition 2.3. Let $A = \{a_1, \ldots, a_{|A|}\}$ be a finite set, $X$ a field, and $\mathcal{F}_k$ the vector space over $X$ of $k$-variable functions $f : A^k \to X$. Let $F, G \in \mathcal{F}_k$. Then the following properties hold:

**R.1** $\text{rank}_k(F + G) \leq \text{rank}_k(F) + \text{rank}_k(G)$.

**R.2** If $B \subset A$, then $\text{rank}_k(F|_B) \leq \text{rank}_k(F)$.

**R.3** $\text{rank}_k(F) \leq |A|$.

**R.4** If $H \in \mathcal{F}_2$ and $M$ is the $|A| \times |A|$ matrix with $m_{ij} = H(a_i, a_j)$, then $\text{rank}_2(H) \geq \text{rank}(M)$.

For properties **R.5** **R.6** **R.7** $f_n \in \mathcal{F}_1$, $g_n \in \mathcal{F}_k$, and the function $h \in \mathcal{F}_{k+1}$ is defined by

$$h(x, y_1, y_2, \ldots, y_k) = \sum_{n=1}^r f_n(x)g_n(y_1, \ldots, y_k).$$

**R.5** If $\{\tilde{f}_n : 1 \leq n \leq r \} \subset \mathcal{F}_1$ so that $\{f_n : 1 \leq n \leq r \} \subset \text{span}\{\tilde{f}_n : 1 \leq n \leq r \} \subset \mathcal{F}_k$ so that

$$h(x, y_1, \ldots, y_k) = \sum_{n=1}^r \tilde{f}_n(x)\tilde{g}_n(y_1, \ldots, y_k).$$

**R.6** Let $M$ be the $|A| \times r$ matrix whose columns are $v_{\text{col}}(f_n)$. Then $\text{rank}_{k+1}(h) \leq \text{rank}(M)$.

**R.7** If $\text{rank}_{k+1}(h) = r$, then the $f_n$ are linearly independent in $\mathcal{F}_1$.

*Proof.* Properties **R.1** and **R.2** are trivial.

**R.3** Let $\delta_a$ be the function on $A$ which is 1 at $a$ and 0 otherwise. Then

$$F(x_1, x_2, \ldots, x_k) = \sum_{a \in A} \delta_a(x_1)F(a, x_2, x_3, \ldots, x_k).$$

**R.4** Suppose $F$ has rank $r$. Then $F(x, y) = \sum_{n=1}^r f_n(x)g_n(y)$ for functions $f_n, g_n : A \to X$.

For each $n$, let $M_n$ be the $|A| \times |A|$ matrix $v_{\text{col}}(f_n)v_{\text{row}}(g_n)$. Since each $M_n$ has rank at most 1, $M = \sum_{n=1}^r M_n$ is a matrix of rank at most $r$.

**R.5** For each fixed choice of $(y_1, \ldots, y_k) \in A^k$, elementary linear algebra tells us there are elements $s_n(y_1, \ldots, y_k) \in X$ for $1 \leq n \leq r$ so that

$$\sum_{n=1}^r g_n(y_1, \ldots, y_k)v_{\text{col}}(f_n) = \sum_{n=1}^r s_n(y_1, \ldots, y_k)v_{\text{col}}(\tilde{f}_n).$$

Thus we may simply define the functions $\tilde{g}_n$ by $\tilde{g}_n(y_1, \ldots, y_k) = s_n(y_1, \ldots, y_k)$.

Properties **R.6** and **R.7** follow immediately from **R.5**.

\[ \Box \]
3 Setup for the Proof of Theorem 1.2

Fix integers \( n \) and \( m \) with \( 3 \leq m \leq n + 2 \). For any set \( S \subset AG(n, q) \), define \( G^S_m : S^m \to \mathbb{F}_q \) by

\[
G^S_m(x_1, \ldots, x_m) = \sum_{t_1, \ldots, t_{m-1} \in \mathbb{F}_q} \prod_{j=1}^n \left[ 1 - \left( \sum_{i=1}^{m-1} t_i (x_i - x_{mj}) \right)^{q-1} \right].
\]

(3.1)

where \( x_{ij} \) is the \( j \)th coordinate of point \( x_i \).

Notice that the bracketed expression is equal to 1 if

\[
\begin{bmatrix}
  t_1 \\
  t_2 \\
  \vdots \\
  t_{m-1}
\end{bmatrix} \cdot
\begin{bmatrix}
  x_{1j} - x_{mj} \\
  x_{2j} - x_{mj} \\
  \vdots \\
  x_{(m-1)j} - x_{mj}
\end{bmatrix} = 0,
\]

and equal to 0 otherwise. Thus \( G^S_m(x_1, \ldots, x_m) \) is equal to the number of elements, modulo \( p \), in

\[
\text{null} \left\{ x_i - x_m : 1 \leq i \leq m - 1 \right\}.
\]

Since the size of a vector space over \( \mathbb{F}_q \) must be a power of \( q \), we see that \( G^S_m(x_1, \ldots, x_m) \) evaluates to 1 if the vectors of \( \{ x_i - x_m : 1 \leq i \leq m - 1 \} \) are linearly independent, and 0 otherwise.

Now suppose that the set \( A \) is \( k \)-general. If \( x_1, \ldots, x_k \) are points of \( A \), then \( \{ x_i - x_k : 1 \leq i \leq k - 1 \} \) is a set of \( k - 1 \) linearly independent vectors if and only if \( x_1, \ldots, x_k \) are all distinct. Therefore, if we define a function \( T^S_m : S^m \to \mathbb{F}_q \) for any set \( S \subset AG(n, q) \) by

\[
T^S_m(x_1, \ldots, x_m) = \begin{cases} 
1 & \text{all } x_j \text{ are distinct} \\
0 & \text{otherwise}
\end{cases},
\]

(3.2)

then \( T^S_m = G^S_m \) when \( S \) is \( m \)-general.

From here, the general idea is to follow the procedure of [10]. We will divide our argument into three lemmas:

**Lemma 3.1.** Let \( S \subset AG(n, q) \) and \( m \geq 2 \). If \( q \) is odd or \( q \) and \( m \) are both even, then

\[
\text{rank}(T^S_m) \geq |S| - 2m + 3.
\]

**Lemma 3.2.** For any set \( S \subset AG(n, q) \) and \( m \geq 3 \),

\[
\text{rank}(G^S_m) \leq m \cdot \min_{t \in (0, 1)} \left( t^{-\frac{q-1}{m}} \cdot \frac{1 - t^q}{1 - t} \right)^n.
\]
Lemma 3.3. Fix an integer \( m \geq 3 \) and let
\[
h_q(x) = x - \frac{x^q}{m} \cdot \frac{1 - x^q}{1 - x}.
\]
Then on \((0,1)\), \(h_q\) attains its minimum value of
\[
\frac{m e^{1-\frac{m}{n}}}{m^2 - (m-1)\alpha} q + \Theta(1)
\]
at \(x_0 = x_0(q) = \frac{q + \alpha - 1}{q + m - 1} + O(q^{-2})\), where \(\alpha\) is the unique value in \((0,1)\) satisfying
\[
\alpha = \frac{m^2 - (m-1)\alpha}{\epsilon^{m-\alpha}}.
\]

When \(A \subset AG(n,q)\) is \(m\)-general (and \(q\) is even or \(m\) is odd) combining lemmas 3.1 and 3.2 gives us
\[
|A| - 2m + 3 \leq \text{rank}(T_m^A) = \text{rank}(G_m^A) \leq m \cdot \min_{t \in (0,1)} \left(t - \frac{\alpha + 1}{m} \cdot \frac{1 - t^q}{1 - t}\right)^n,
\]
and therefore
\[
m_2(n,q) \leq 2m + m \cdot \min_{t \in (0,1)} \left(t - \frac{\alpha + 1}{m} \cdot \frac{1 - t^q}{1 - t}\right)^n.
\]
In lemma 3.3 we verify that \(\min_{t \in (0,1)} \left(t - \frac{\alpha + 1}{m} \cdot \frac{1 - t^q}{1 - t}\right)\) is well-defined and bounded above by
\[
\frac{m e^{1-\frac{m}{n}}}{m^2 - \alpha m + \alpha} q + C,
\]
completing the proof of theorem 1.2.

Remark 3.4. In lemma 3.1 we see that the rank of \(T_m^S\) is typically around \(|S|\), but this is surprisingly does not hold when \(p = 2\) and \(m\) is odd, hence the omission of that case. Indeed, in characteristic 2 it is easy to verify that
\[
T_{2k+1}^S(x_1, x_2, \ldots, x_{2k+1}) = \sum_{i=1}^{2k+1} T_{2k}^S(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{2k+1})
\]
and thus \(\text{rank}(T_{2k+1}^S) \leq 2k + 1\).
4 Proof of lemma 3.1

We proceed by induction on $m$ and begin with the case $m = 2$. Enumerate $B = \{b_1, \ldots, b_{|B|}\}$ and let $M$ be the matrix with $m_{ij} = T_2^B(b_i, b_j)$. By the definition of $T_2^B$, $M$ is the matrix which has zeros along the diagonal and ones everywhere else. Thus $M$ has rank at least $|B| - 1$, and by claim 4 rank($T_2^B$) $\geq |B| - 1$. (Note: The matrix $M$ has rank $|B|$ unless $|B| \equiv 1 \mod p$, when the rank is $|B| - 1$.)

We will first consider the case where $q$ is odd. Fix an integer $k \geq 2$ and assume that for any $S \subseteq AG(n, q)$, rank$_j(T_j^S) \geq |S| - 2j + 3$ when $2 \leq j \leq k$. Fix $B \subseteq AG(n, q)$ and let $r$ be the $(k + 1)$-rank of $T_{k+1}^B$. Then there are functions $f_{i, \alpha} : B \to \mathbb{F}_q$, $g_{i, \alpha} : B^k \to \mathbb{F}_q$ so that

$$T_{k+1}^B(x_1, \ldots, x_{k+1}) = \sum_{i=1}^{k+1} \sum_{\alpha \in I_i} f_{i, \alpha}(x_i)g_{i, \alpha}(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{k+1})$$

(4.1)

where the indexing sets $I_i$ are disjoint and $\sum_{i=1}^{k+1} |I_i| = r$. Let $\mathbb{1}_B : B \to \mathbb{F}_q$ be the function which is identically 1 on $B$.

**Case 1:** $p \not| k$, or $p | k$ and $\mathbb{1}_B \notin \bigcap_{i=1}^{k+1} \text{span} \left( \{ f_{i, \alpha} : \alpha \in I_i \} \right)$

If $p \not| k$, let

$$H = \text{span} \left( \{ \mathbb{1}_B \} \cup \{ f_{k+1, \alpha} : \alpha \in I_{k+1} \} \right).$$

Otherwise, since $T_{k+1}^B$ is symmetric in all variables, we may assume without loss of generality that $\mathbb{1}_B \notin \text{span} \left( \{ f_{i, \alpha} : \alpha \in I_{k+1} \} \right)$ and let

$$H = \text{span} \left( \{ f_{k+1, \alpha} : \alpha \in I_{k+1} \} \right).$$

In either case, let $H^\perp$ be the orthogonal complement of $H$ with respect to the usual inner product.

Because the dimension of $H$ is at most $|I_{k+1}| + 1$, the dimension $d$ of $H^\perp$ is at least $|B| - |I_{k+1}| - 1$. Find a set $B' \subseteq B$ and an appropriate basis $\mathcal{U} = \{ h_1, h_2, \ldots, h_d \}$ for $H^\perp$ so that $|B'| = d$ and

$$\begin{bmatrix} v_{\text{col}}(h_1|_{B'}) & v_{\text{col}}(h_2|_{B'}) & \cdots & v_{\text{col}}(h_d|_{B'}) \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \cdots & 0 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{bmatrix}$$

(see definition 2.2). If $p \not| k$, we simply let $\tilde{h} = h_d$. Otherwise, since $\mathbb{1}_B \notin H$, there must be a function $\tilde{h} \in \mathcal{U}$ so that $\tilde{h}$ is not orthogonal to $\mathbb{1}_B$, i.e. $\sum_{b \in B} \tilde{h}(b) \neq 0$. 





Multiplying both sides of (4.2) by \( \tilde{h}(x_{k+1}) \) and summing over \( x_{k+1} \in B \), the right side becomes
\[
\sum_{i=1}^{k} \sum_{\alpha \in I_i} \left( f_{i,\alpha}(x_i) \sum_{x_{k+1} \in B} \tilde{h}(x_{k+1}) g_{i,\alpha}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k+1}) \right),
\]
which has rank at most \( r - |I_{k+1}| \).

On the left side we get
\[
\sum_{x_{k+1} \in B} \tilde{h}(x_{k+1}) T_{k+1}^B(x_1, \ldots, x_{k+1})
\]
\[
= T_k^B(x_1, \ldots, x_k) \sum_{x \in B \setminus \{x_1, \ldots, x_k\}} \tilde{h}(x)
\]
\[
= T_k^B(x_1, \ldots, x_k) \left( \sum_{x \in B} \tilde{h}(x) - \sum_{i=1}^{k} \tilde{h}(x_i) \right).
\]

Let \( B'' = \{ b \in B : \tilde{h}(b) = 1 \} \) and notice that \( |B''| \geq d - 1 \). Restrict the domain of both (4.2) and (4.3) to \( (B'')^k \). By (R.2) the rank of (4.2) is still no more than \( r - |I_{k+1}| \). Note that the second sum in (4.3) simplifies to \( k \) since \( \tilde{h} |_{B''} \equiv 1 \). If \( p \nmid k \), then the first sum is 0 since \( 1_B \in H \). If \( p \mid k \), then the first sum is some nonzero constant by our construction of \( \tilde{h} \). In either case, we are left with \( cT_k^{B''}(x_1, \ldots, x_k) \) for some \( c \neq 0 \), and \( \text{rank}(cT_k^{B''}) \geq |B''| - 2k + 3 \) by the inductive hypothesis. Comparing the ranks of (4.2) and (4.3) we see
\[
r - |I_{k+1}| \geq |B''| - 2k + 3 \geq |B| - |I_{k+1}| - 2k + 1
\]
and thus
\[
\text{rank}(T_{k+1}^B) = r \geq |B| - 2(k + 1) + 3.
\]

**Case 2:** \( p \mid k \) and \( 1_B \in \bigcap_{i=1}^{k+1} \text{span} \left( \{ f_{i,\alpha} : \alpha \in I_i \} \right) \).

Notice that \( k + 1 \geq 3 \), \( T_{k+1}^B \) is symmetric, and \( r \leq |B| \) by (R.3). Therefore, we may assume without loss of generality that \( |I_k| + |I_{k+1}| < |B| \). For \( i = k, k + 1 \), let
\[
H_i = \text{span} \left( \{ f_{i,\alpha} : \alpha \in I_i \} \right)
\]
and let \( H_i^\perp \) be the orthogonal complement.

Because the dimension of \( H_i \) is \( |I_i| \) (by R.7), the dimension \( d_i \) of \( H_i^\perp \) is \( |B| - |I_i| \). Find a set \( B_i \subset B \) and an appropriate basis \( U_i = \{ h_{i,1}, h_{i,2}, \ldots, h_{i,d_i} \} \) for \( H_i^\perp \) so that \( |B_i| = d_i \) and
\[
\begin{bmatrix}
\text{v} \text{col} (h_{i,1} | B_i) & \text{v} \text{col} (h_{i,2} | B_i) & \cdots & \text{v} \text{col} (h_{i,d_i} | B_i)
\end{bmatrix} =
\begin{bmatrix}
0 & 1 & 1 & \cdots & 1 & 1 \\
1 & 0 & 1 & \cdots & 1 & 1 \\
1 & 1 & 0 & \cdots & 1 & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1 & 1 & 1 & \cdots & 0 & 1 \\
1 & 1 & 1 & \cdots & 1 & 1
\end{bmatrix}
\]
Abbreviating \{x_1, x_2, \ldots, x_{k-1}\} as \mathcal{X} and expanding,

\[
T^B_{k-1}(x_1, \ldots, x_{k-1}) \left[ \sum_{x \in \mathcal{X}} \bar{h}_k(x) \left( \sum_{y \in \mathcal{X}} \bar{h}_{k+1}(y) - \sum_{x, y \in \mathcal{B} \setminus \mathcal{X}} \bar{h}_k(x) \bar{h}_{k+1}(y) \right) \right] - \sum_{x \in \mathcal{B}} \bar{h}_k(x) \bar{h}_{k+1}(x) + \sum_{i=1}^{k-1} \bar{h}_k(x_i) \bar{h}_{k+1}(x_i) \]  

we have

\[
T^B_{k-1}(x_1, \ldots, x_{k-1}) \left[ \sum_{x \in \mathcal{X}} \bar{h}_k(x) \left( \sum_{y \in \mathcal{X}} \bar{h}_{k+1}(y) - \sum_{x, y \in \mathcal{B} \setminus \mathcal{X}} \bar{h}_k(x) \bar{h}_{k+1}(y) \right) \right] - \sum_{x \in \mathcal{B}} \bar{h}_k(x) \bar{h}_{k+1}(x) + \sum_{i=1}^{k-1} \bar{h}_k(x_i) \bar{h}_{k+1}(x_i) \]  

for some \( c \neq 0 \).

Let \( B' = \{ x \in B : \bar{h}_{k+1}(x) = \bar{h}_k(x) = 1 \} \). By our constructions of \( \bar{h}_{k+1} \) and \( \bar{h}_k \),

\[
|B'| \geq |B_k| - 1 + |B_{k+1}| - 1 - |B| = |B| - |I_k| - |I_{k+1}| - 2. \]

Restrict the domains of both expressions \(4.4\) and \(4.5\) to \((B')^k\). Since \( p \mid k \), expression \(4.5\) simplifies to

\[
T^B_{k-1}(x_1, \ldots, x_{k-1})((k-1)^2 - c + (k-1)) = -cT^B_{k-1}(x_1, \ldots, x_{k-1}),
\]

a function whose \((k-1)\)-rank is at least \(|B'|-2k+5\) by our inductive hypothesis. Comparing the ranks of \(4.4\) and \(4.5\), we see

\[
r - |I_{k+1}| - |I_k| \geq |B'|-2k+5 \geq |B| - |I_k| - |I_{k+1}| - 2k + 3
\]
and thus 
\[ \text{rank}(T_{B}^{k+1}) = r \geq |B| - 2(k+1) + 5 \geq |B| - 2(k+1) + 3. \]

This completes the induction for odd \( q \).

To prove the result for even \( q \), we only need to make slight adjustments to case 2. Let \( k \geq 3 \) be odd and assume that \( \text{rank}(T_{k-1}^{S}) \geq |S| - 2(k-1) + 3 \).

Notice that when \( |B| \leq 5 \), the desired result \( \text{rank}(T_{B}^{k+1}) \geq |B| - 2(k+1) + 3 \) is trivial, and therefore we may assume \( |B| > 5 \). In particular, this allows us to assume without loss of generality that \( |I_k| + |I_{k+1}| < |B| - 2 \).

Let \( H_i = \text{span} (\{I_B\} \cup \{f_{i,\alpha} : \alpha \in I_i\}) \). This time, we only know that the dimension \( d_i \) of \( H_i^\perp \) is at least \( |B| - |I_i| - 1 \), but we still have

\[ d_k + d_{k+1} \geq 2|B| - |I_k| - |I_{k+1}| - 2 > |B|. \]

We construct \( B_i, U_i, \tilde{h}_i, \) and \( B' \) as before. Again, we multiply both sides of 4.1 by \( \tilde{h}_k(x_k)\tilde{h}_{k+1}(x_{k+1}) \), sum over all \( x_k, x_{k+1} \in B \), and restrict to \( B' \) to get

\[ cT_{k-1}^{B'}(x_1, \ldots, x_{k-1}) = \sum_{i=1}^{k-1} \sum_{\alpha \in I_i} f_{i,\alpha}(x_i) \sum_{x_k, x_{k+1} \in B} \tilde{h}_k(x_k)\tilde{h}_{k+1}(x_{k+1})g_{i,\alpha}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{k+1}) \]

for some \( c \neq 0 \). However, in this case,

\[ |B'| \geq |B_k| - 1 + |B_{k+1}| - 1 - |B| \geq |B| - |I_k| - |I_{k+1}| - 4. \]

Nevertheless, comparing the ranks of both sides of the equation still yields

\[ \text{rank}(T_{k+1}^{B}) = r \geq |B| - 2(k+1) + 3, \]

completing the induction.

5 Proof of lemma 3.2

Looking back at equation 3.1, we see \( G_m^S \) is a polynomial in \( mn \mathbb{F}_q \)-valued variables \( x_{ij} \). Let \( P \) be the set of monomials appearing in the expansion of \( G_m^S \). Each monomial \( \rho \in P \) can be written as

\[ \rho(x_1, \ldots, x_m) = c \prod_{i=1}^{m} \prod_{j=1}^{n} x_{ij}^{e_{ij}}, \]

where the coefficient \( c \in \mathbb{F}_q \) and the \( e_{ij} \in \mathbb{Z} \) depend on \( \rho \).

By 3.1 each \( e_{ij} \) is no greater than \( q - 1 \) and

\[ \sum_{i=1}^{m} \sum_{j=1}^{n} e_{ij} \leq (q - 1)n. \]
Thus, there must be some index $i$ for which $\sum_{j=1}^{n} e_{ij} \leq \frac{(q-1)n}{m}$. For each $\rho \in P$, choose such an index and call it $\kappa = \kappa(\rho)$. We then separate out the $\kappa$-factors of $\rho$:

$$\rho(x_1, \ldots, x_m) = e \prod_{j=1}^{n} x_{\kappa_j}^{e_{kj}} \prod_{i \neq \kappa, j=1}^{n} x_{ij}^{e_{ij}}.$$

Letting $f_{\rho}(x_{\kappa}) = \prod_{j=1}^{n} x_{\kappa_j}^{e_{kj}}$ and $g_{\rho}(x_1, \ldots, x_{\kappa-1}, x_{\kappa+1}, \ldots, x_m) = e \prod_{i \neq \kappa, j=1}^{n} x_{ij}^{e_{ij}}$, we have

$$G_{m}^{S}(x_1, \ldots, x_m) = \sum_{i=1}^{m} \sum_{\rho \in P}^{\kappa(\rho) = i} f_{\rho}(x_i) g_{\rho}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m).$$

Next, group together the polynomials with matching \textit{“$\kappa$-factors,”} i.e. for $e = (e_1, e_2, \ldots, e_n) \in \mathbb{Z}^n$,

$$M_i(e) = \left\{ \rho \in P : \kappa(\rho) = i, f_{\rho}(x_i) = \prod_{j=1}^{n} x_{ij}^{e_{ij}} \right\}.$$

We then reorganize the sum:

$$G_{m}^{S}(x_1, \ldots, x_m) = \sum_{i=1}^{m} \sum_{e \in \mathbb{Z}^n} \left[ \left( \prod_{j=1}^{n} x_{\kappa_j}^{e_{kj}} \right) \sum_{\rho \in M_i} g_{\rho}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m) \right].$$

Notice that the expression in square brackets is a function of rank 1. Therefore, by the rank of $G_{m}^{S}$ is bounded above by

$$m \cdot \max_{1 \leq i \leq m} \# \{ e \in \mathbb{Z}^n : M_i(e) \neq \emptyset \}.$$

As we observed earlier, $M_i(e)$ is empty unless $e_j \leq q - 1$ for all $j$ and $\sum_{j=1}^{n} e_j \leq \frac{(q-1)n}{m}$. Thus the rank of $G_{m}^{S}$ is bounded above by the number of $n$-tuples in $\mathbb{Z}^n$ in which each coordinate is no greater than $q - 1$ and the sum of the coordinates is no greater than $\frac{(q-1)n}{m}$.

For $\alpha, \beta, \gamma \in \mathbb{N}$, let $\Lambda(\alpha, \beta, \gamma)$ be the number of $\alpha$-tuples of elements in $\{0, 1, 2, \ldots, \beta\}$ with sum no greater than $\gamma$. It is easy to verify that the number of $\alpha$-tuples with sum \textit{equal} to $i$ is

$$[x^i] \left( \frac{1 - x^{\beta+1}}{1 - x} \right)^{\alpha}$$

and therefore

$$\Lambda(\alpha, \beta, \gamma) = \sum_{i=0}^{\gamma} [x^i] \left( \frac{1 - x^{\beta+1}}{1 - x} \right)^{\alpha}.$$

We can derive a slight variation on the familiar saddle point bound: suppose that $f(x) = \sum_{i=0}^{\infty} c_i x^i$ on $(0, 1)$ and each $c_i$ is a non-negative real. Then for any non-negative integer $N$ and any $t \in (0, 1)$, we have

$$\sum_{i=0}^{N} [x^i] f(x) = \sum_{i=0}^{N} c_i \leq \sum_{i=0}^{\infty} c_i t^{i-N} = t^{-N} f(t).$$
Therefore

\[ \Lambda (\alpha, \beta, \gamma) \leq t^{-\gamma} \left( \frac{1 - t^{\beta+1}}{1 - t} \right)^{\alpha} \]

for all \( t \in (0, 1) \). Applying this to the problem at hand,

\[
\rank(G^S_m) \leq m \cdot \Lambda \left( n, q - 1, \left\lfloor \frac{(q-1)n}{m} \right\rfloor \right) = m \cdot \min_{t \in (0,1)} \left( t^{-\left\lfloor \frac{(q-1)n}{m} \right\rfloor} \left( \frac{1 - t^q}{1 - t} \right)^{\alpha} \right). 
\]

6 Proof of lemma 3.3

To verify that the minimum at \( x_0 \) is well-defined, let \( s = \frac{q-1}{m} \) and write

\[
h_q(x) = \left(\sum_{i=0}^{\lfloor s \rfloor - 1} x^i \right) + \left( x^{\lfloor s \rfloor} + x^{\lfloor s \rfloor + 1} \right) + \left( q^{-1} \sum_{i=\lfloor s \rfloor + 2} x^i \right).
\]

As a sum of functions that are convex on \((0, 1)\), \( h_q \) is also convex. Consequently, anywhere its derivative vanishes on \((0, 1)\) must be the unique minimum on that interval. Taking the derivative, we find

\[
h'_q(x) = \frac{x - \frac{q-1}{m}}{m(1-x)} \cdot r_q(x)
\]

where

\[
r_q(x) = (q + m - 1)x - (q - 1) - x^q((q - 1)(m - 1)(1 - x) + m).
\] (6.1)

Given that

\[
h'_q(1) = \frac{q(q - 1)(m - 2)}{2m} > 0,
\]

there must indeed be a unique minimum occurring at some value \( x_0 \), and moreover, \( x_0 = \frac{q + \beta - 1}{q + m - 1} \) for some \( \beta \in (0, m) \).

To get a better estimate for \( \beta \), notice that

\[
0 = r_q \left( \frac{q + \beta - 1}{q + m - 1} \right) = \beta - \left( 1 + \frac{m - \beta}{q + \beta - 1} \right)^{-q} \left[ m^2 + \beta - m \beta - \frac{m(m - 1)(m - \beta)}{q + m - 1} \right]
\]

\[= \beta - \frac{m^2 - (m - 1)\beta}{e^{m-\beta}}(1 - O(q^{-1})).\]

Let \( f(x) = x - \frac{m^2 - (m - 1)x}{e^{m-x}} \). We leave it to the reader to check that
• \( f(x) \) has exactly one zero in \((0, 1)\)
• \( .25 < f'(x) < 1 \) on \((0, 1)\).

If \( \alpha \) is that unique zero, then \( f(\beta) = O(q^{-1}) \) and \( f(\alpha) = 0 \), giving us

\[
\frac{f(\alpha) - f(\beta)}{\alpha - \beta} = O(q^{-1}).
\]

Using the mean value theorem along with \( .25 < f'(x) < 1 \), we conclude that \( \alpha = \beta + O(q^{-1}) \).

To finish, we will estimate

\[
h_q \left( \frac{q + \alpha - 1}{q + m - 1} + O(q^{-2}) \right).
\]

We can simplify this computation by rearranging the equation \( r_q(x_0) = 0 \) to get

\[
1 - x_0^q = \frac{qm}{m + (q - 1)(m - 1)(1 - x_0)},
\]

and thus

\[
h_q \left( \frac{q + \alpha - 1}{q + m - 1} + O(q^{-2}) \right) = \left( \frac{q + \alpha - 1}{q + m - 1} + O(q^{-2}) \right)^{-\frac{qm}{m + (q - 1)(m - 1)\left(1 - \frac{q + \alpha - 1}{q + m - 1} - O(q^{-2})\right)}} \frac{qm(q + m - 1)(1 + O(q^{-2}))}{m(q + m - 1) + (q - 1)(m - 1)(m - \alpha)}
\]

\[
= e^{1 - \frac{q}{m}} (1 + O(q^{-1})) \cdot \frac{qm(q + m - 1)(1 + O(q^{-2}))}{m^2q - \alpha(m - 1)(q - 1)} + O(1).
\]

7 Estimates on the size of \( m \)-general sets for certain \( q \) and \( m \)

Inequality [1.1] allows us to estimate \( \mu_m(q) \) for large values of \( q \). Table [1.3] gives the asymptotic values for some small values of \( m \). These asymptotic estimates are useful when \( q \) is a fixed large number, but we can compute the exact values of \( \min_{t \in (0, 1)} \left( t^{-\frac{q - 1}{m}} \cdot \frac{1 - t^q}{1 - t} \right) \) when \( q \) is small. For instance, if \( q = m = 3 \), we can solve \( r_3(x_0) = 0 \) (see equation [0.1]) with the quadratic formula to get \( x_0 = \sqrt[3]{3} - 1 \). Theorem [1.2] then recovers the same result as [6], namely

\[
m_2(n, 3) < 6 + 3 \cdot (h_3(x_0))^n = O(2.756^n),
\]

or \( \mu(3) < 0.923 \).
Another particularly interesting case is \( q = 2, \ m = 4 \), since 2-flats in \( AG(n, 2) \) have exactly 4 points. We find that the largest set \( A \subset AG(n, 2) \) in which no 2-flat is "fully covered" by points of \( A \) has \( M_3(n, 2) < 8 + 4(1.755)^n \) points, hence \( \mu_4(2) < 0.813 \).

Table 1 shows the upper bounds for \( \mu_m(q) \) given by a direct calculation of

\[
\log_q \left( \min_{t \in (0,1)} \left( t^{-\frac{a-1}{m}} \cdot \frac{1-t^q}{1-t} \right) \right).
\]

Note that some boxes are unfilled because we did not obtain estimates in the cases where \( q \) is even and \( m \) is odd.

| \( m \) | \( \mu_m(q) \ < \ldots \) | \( 2 \) | \( 3 \) | \( 4 \) | \( 5 \) | \( 7 \) | \( 8 \) | \( 9 \) | \( 11 \) |
|-----|-----------------|-----|-----|-----|-----|-----|-----|-----|-----|
| 3   | 1 - \log_q(1.188) | 0.923 | 0.930 | 0.935 | 0.938 | 0.941 |
| 4   | 1 - \log_q(1.504) | 0.813 | 0.821 | 0.829 | 0.836 | 0.846 | 0.851 | 0.854 | 0.861 |
| 5   | 1 - \log_q(1.853) | 0.735 | 0.756 | 0.771 | 0.782 | 0.791 |
| 6   | 1 - \log_q(2.212) | 0.651 | 0.665 | 0.679 | 0.690 | 0.708 | 0.716 | 0.722 | 0.734 |
| 7   | 1 - \log_q(2.577) | 0.609 | 0.636 | 0.657 | 0.673 | 0.685 |
| 8   | 1 - \log_q(2.944) | 0.544 | 0.562 | 0.577 | 0.591 | 0.613 | 0.622 | 0.631 | 0.644 |

(a) Bounds for small \( m \) and large \( q \)

(b) Bounds for specific small \( m \) and \( q \)
References

[1] M. Bateman, N. Katz, New bounds on cap sets, J. Amer. Math. Soc. 25 (2012), no. 2, 585-613.

[2] J. Bierbrauer, Introduction to Coding Theory, Second Edition, Chapman & Hall/CRC Press, 2010.

[3] E. Croot, V. Lev, P. Pach, Progression-free sets in $\mathbb{Z}_n^4$ are exponentially small, Ann. of Math. 185 (2017), no. 1, 331-337.

[4] Y. Edel, Extensions of generalized product caps., Des. Codes Cryptogr. 31 (2004), no. 1, 514.

[5] Y. Edel, S. Ferret, I, Landjev, L. Storme The classification of the largest caps in $AG(5, 3)$, J. Comb. Theory Ser. A 99 (2002), no. 1, 95-110.

[6] J. Ellenberg, D. Gijswijt, On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression, Ann. of Math. 185 (2017), no. 1, 339-343.

[7] J. Hirschfeld, L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, Finite Geometries, Proceedings 3 (2001), 201-246.

[8] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, J. Comb. Theory Ser. A 71 (1995), no. 1, 168-172.

[9] A. Potechin, Maximal caps in $AG(6, 3)$, Des. Codes Cryptogr. 46 (2008), 243-259.

[10] T. Tao, “A symmetric formulation of the Croot-Lev-Pach-Ellenberg-Gijswijt capset bound” What’s new, 18 May 2016, https://terrytao.wordpress.com/2016/05/18/a-symmetric-formulation-of-the-croot-lev-pach-ellenberg-gijswijt-capset-bound/, accessed 17 Aug. 2017.

[11] J. Thas, On $k$-caps in $PG(n, q)$ with $q$ even and $n \geq 4$, Discrete Math. 341 (2018), 1072–1077.