THE MAXIMUM SIZE OF A PARTIAL SPREAD IN A FINITE PROJECTIVE SPACE

ESMERALDA NĂSTASE

MATHEMATICS DEPARTMENT
XAVIER UNIVERSITY
CINCINNATI, OHIO 45207, USA

PAPA SISSOKHO

MATHEMATICS DEPARTMENT
ILLINOIS STATE UNIVERSITY
NORMAL, ILLINOIS 61790, USA

Abstract. Let n and t be positive integers with $t < n$, and let q be a prime power. A *partial* $(t-1)$*-spread* of $\mathrm{PG}(n-1,q)$ is a set of $(t-1)$-dimensional subspaces of $\mathrm{PG}(n-1,q)$ that are pairwise disjoint. Let $r = n \bmod t$. We prove that if $t > (q^r-1)/(q-1)$, then the maximum size, i.e., cardinality, of a partial $(t-1)$-spread of $\mathrm{PG}(n-1,q)$ is $(q^n - q^{t+r})/(q^t-1)+1$. This essentially settles a main open problem in this area. Prior to this result, this maximum size was only known for $r \in \{0,1\}$ and for $r = q = 2$.

Keywords: Galois geometry; partial spreads; subspace partitions; subspace codes.

Mathematics Subject Classification: 51E23; 05B25; 94B25.

1. Introduction

Let n and t be positive integers with $t < n$, and let q be a prime power. Let $\mathrm{PG}(n-1,q)$ denote the $(n-1)$-dimensional projective space over the finite field $\mathbb{F}_q$. A *partial* $(t-1)$*-spread* S of $\mathrm{PG}(n-1,q)$ is a collection of $(t-1)$-dimensional subspaces of $\mathrm{PG}(n-1,q)$ that are pairwise disjoint. If S contains all the points of $\mathrm{PG}(n-1,q)$, then it is called a $(t-1)$*-spread*. It follows from the work of André [1] that a $(t-1)$-spread of $\mathrm{PG}(n-1,q)$ exists if and only if $t-1$ divides $n-1$.

Given positive integers n and t with $t < n$, the problem of finding the maximum size, i.e., cardinality, of a partial $(t-1)$-spread of $\mathrm{PG}(n-1,q)$

---

nastasee@xavier.edu, psissok@ilstu.edu.

is rather a natural one. It is directly related to the general problem of classifying the *maximal* partial $(t-1)$-spread. A maximal partial $(t-1)$-spread is a set of $(t-1)$-dimensional subspaces which cannot be extended to a larger set. This problem has been extensively studied [6, 13, 15, 20]. Besides their traditional relevance to Galois geometry, partial $(t-1)$-spreads are used to build byte-correcting codes (e.g., see [7, 19]), 1-perfect mixed error-correcting codes (e.g., see [18, 19]), orthogonal arrays and (s, k, λ)-nets (e.g., see [4]). More recently, partial $(t-1)$-spreads have also attracted renewed attention since they can be viewed as *subspace codes*. In Section 4, we shall say more about the connection between our results and subspace codes.

Let $\mu_q(n,t)$ denote the maximum size of any partial $(t-1)$-spread of $\mathrm{PG}(n-1,q)$. The problem of determining $\mu_q(n,t)$ is a long standing open problem. A general upper bound for $\mu_q(n,t)$ is given by the following theorem of Drake and Freeman [4].

Theorem 1. *Let* $r = n \bmod t$. *Then* $\mu_q(n,t) \leq \dfrac{q^n - q^r}{q^t - 1} - \lfloor \omega \rfloor - 1$, *where* $2\omega = \sqrt{4q^t(q^t - q^r) + 1} - (2q^t - 2q^r + 1)$.

The following result is due to André [1] for $r = 0$. For $r = 1$, it is due to Hong and Patel [19] when $q = 2$, and Beutelspacher [3] when $q > 2$.

Theorem 2. *Let* $r = n \bmod t$. *Then* $\mu_q(n,t) \geq \dfrac{q^n - q^{t+r}}{q^t - 1} + 1$, *where equality holds if* $r \in \{0, 1\}$.

In light of Theorem 2, it was later conjectured (e.g., see [5, 19]) that the value of $\mu_q(n,t)$ is given by the lower bound in Theorem 2. However, this conjecture was disproved by the second author of this paper and his co-authors [11] who proved the following result.

Theorem 3. *If* $n \geq 8$ *and* $n \bmod 3 = 2$, *then* $\mu_2(n,3) = \dfrac{2^n - 2^5}{7} + 2$.

Very recently, Kurz [22] posted a preprint in which he proves the following theorem which upholds the lower bound for $\mu_q(n,t)$ when $q = 2$, $r = 2$, and $t > 3$.

Theorem 4. *If* $n > t > 3$ *and* $n \bmod t = 2$, *then*

$$\mu_2(n,t) = \frac{2^n - 2^{t+2}}{2^t - 1} + 1.$$

In this paper, we prove that the conjectured value of $\mu_q(n,t)$ holds for almost all values of the parameters n, q, and t. The following theorem, our main result, generalizes Theorem 2 (set $r = 1$) and Theorem 4 (set $r = 2$ and $q = 2$). In particular, this is the first comprehensive result with the exact value of $\mu_q(n,t)$ for almost all values of the parameters n, q, and t.

Theorem 5. *Let* $r = n \bmod t$. *If* $t > \dfrac{q^r-1}{q-1}$, *then*

$$\mu_q(n,t) = \frac{q^n - q^{t+r}}{q^t-1} + 1.$$

We can use the language of graph theory to reformulate Theorem 5 as follows. Let $\mathcal{H}_q(n,t)$ be the hypergraph whose vertices are the points of $\mathrm{PG}(n-1,q)$ and whose edges are its $(t-1)$-subspaces. Then $\mathcal{H}_q(n,t)$ is a $(q^t-1)/(q-1)$-uniform hypergraph. Now Theorem 5 implies that if $r = n \bmod t$ and $t > (q^r-1)/(q-1)$, then the maximum size of a matching in $\mathcal{H}_q(n,t)$ is $(q^n - q^{t+r})/(q^t-1) + 1$.

The general strategy of the proof of Theorem 5 is due to Beutelspacher who used it to prove Theorem 2. This strategy relies on *subspace partitions* which we shall discuss in Section 2. Beutelspacher's approach was further extended by Kurz to prove Theorem 4. In this paper, we developed an averaging argument to further extend this method and prove our main result (see Theorem 5) in Section 3.

2. SUBSPACE PARTITIONS

Let $V = V(n,q)$ denote the vector space of dimension n over $\mathbb{F}_q$. For any subspace U of V, let U^* denote the set of nonzero vectors in U. A *d-subspace* of $V(n,q)$ is a d-dimensional subspace of $V(n,q)$; this is equivalent to a *$d-1$-subspace* in $\mathrm{PG}(n-1,q)$.

A *subspace partition* $\mathcal{P}$ of V, also known as a *vector space partition*, is a collection of nontrivial subspaces of V such that each vector of V^* is in exactly one subspace of $\mathcal{P}$ (e.g., see Heden [15] for a survey on subspace partitions). The *size* of a subspace partition $\mathcal{P}$ is the number of subspaces in $\mathcal{P}$.

Suppose that there are s distinct dimensions, $d_s > \cdots > d_1$, that occur in a subspace partition $\mathcal{P}$, and let n_i denote the number of i-subspaces in $\mathcal{P}$. Then the expression $[d_s^{n_{d_s}}, \ldots, d_1^{n_{d_1}}]$ is called the *type* of $\mathcal{P}$.

Remark 6. *A partial* $(t-1)$*-spread of* $\mathrm{PG}(n-1,q)$ *of size* n_t *is a partial* t*-spread of* $V(n,q)$ *of size* n_t. *This is equivalent to a subspace partition of* $V(n,q)$ *of type* $[t^{n_t}, 1^{n_1}]$. *We will use this subspace partition formulation in the proof of Lemma 9.*

To state the next lemmas, we need the following definitions. For any integer $i \geq 1$, let

$$\Theta_i = \frac{q^i - 1}{q - 1}.$$

Then, for $i \geq 1$, Θ_i is the number of 1-subspaces in an i-subspace of $V(n,q)$. Let $\mathcal{P}$ be a subspace partition of $V = V(n,q)$ of type $[d_s^{n_{d_s}}, \ldots, d_1^{n_{d_1}}]$. For any hyperplane H of V, let $b_{H,d}$ be the number of d-subspaces in $\mathcal{P}$ that are contained in H and set $b_H = [b_{H,d_s}, \ldots, b_{H,d_1}]$. Define the set $\mathcal{B}$ of *hyperplane types* as follows:

$$\mathcal{B} = \{b_H : \ H \text{ is a hyperplane of } V\}.$$

For any $b \in \mathcal{B}$, let s_b denote the number of hyperplanes of V of type b.

We will also use Lemma 7 and Lemma 8 by Heden and Lehmann [16].

Lemma 7. *Let $\mathcal{P}$ be a subspace partition of $V(n,q)$ of type $[d_s^{n_{d_s}}, \ldots, d_1^{n_{d_1}}]$. If H is a hyperplane of $V(n,q)$ and $b_{H,d}$ is as defined above, then*

$$|\mathcal{P}| = 1 + \sum_{i=1}^{s} b_{H,d_i} q^{d_i}.$$

Lemma 8. *Let $\mathcal{P}$ be a subspace partition of $V(n,q)$, and let $\mathcal{B}$ and s_b be as defined above. Then*

$$\sum_{b \in \mathcal{B}} s_b = \Theta_n,$$

and for any d-subspace of $\mathcal{P}$, the following holds:

$$\sum_{b \in \mathcal{B}} b_d s_b = n_d \Theta_{n-d}.$$

3. Proof of Theorem 5

Let $n = kt + r$ and $1 \leq r \leq t - 1$. Throughout this section we assume this definition of n. We use the following notation:

$$\ell = \frac{q^{n-t} - q^r}{q^t - 1}. \tag{1}$$

Then the lower bound for $\mu_q(n,t)$ in Theorem 2 can be written as:

$$\mu_q(n,t) \geq \ell q^t + 1.$$

We now prove our main lemma.

Lemma 9. *Let n and t be positive integers with $t < n$, let q be a prime power, and let $r = n \bmod t$. If $r \geq 1$ and $t > \Theta_r$, then $\mu_q(n,t) \leq \ell q^t + 1$.*

Proof. Recall that $\Theta_i = (q^i - 1)/(q - 1)$ for any integer $i \geq 1$. For convenience, we also set

$$\delta_i = \frac{q^i - 2q^{i-1} + 1}{q - 1}.$$

Since $q \geq 2$, we have the following easy facts, which we will use throughout the proof.

$$0 < \delta_i < q^{i-1};\ \delta_i \bmod q^{i-1} = \delta_i;\ 1 + \delta_{i+1} = q\delta_i;\ \text{and}\ \frac{\delta_{i+1}}{q} < \delta_i. \tag{2}$$

The proof is by contradiction. So assume that $\mu_q(n,t) > \ell q^t + 1$. Then $\mathrm{PG}(n-1,q)$ has a $(t-1)$-partial spread of size $\ell q^t + 2$. Thus, it follows from Remark 6 that there exists a subspace partition $\mathcal{P}_0$ of $V(n,q)$ of type $[t^{n_t}, 1^{n_1}]$, where

$$n_t = \ell q^t + 2 \text{ and } n_1 = \left(\frac{q^r - 1}{q - 1} - 1\right) q^t + \frac{q^{t+1} - 2q^t + 1}{q - 1} = (\Theta_r - 1)q^t + \delta_{t+1}. \tag{3}$$

We will prove by induction that for each integer j with $0 \leq j \leq \Theta_r - 1$, there exists a subspace partition $\mathcal{P}_j$ of $H_j \cong V(n-j,q)$ of type

$$[t^{m_{j,t}}, (t-1)^{m_{j,t-1}}, \ldots, (t-j)^{m_{j,t-j}}, 1^{m_{j,1}}], \tag{4}$$

where $m_{j,t}, \ldots, m_{j,t-j}$, $m_{j,1}$, and c_j are nonnegative integers such that

$$\sum_{i=t-j}^{t} m_{j,i} = n_t = \ell q^t + 2, \tag{5}$$

and

$$m_{j,1} = c_j q^{t-j} + \delta_{t+1-j}, \text{ and } 0 \leq c_j \leq \Theta_r - 1 - j. \tag{6}$$

The base case, $j = 0$, holds since $\mathcal{P}_0$ is a subspace partition of $H_0 = V(n,q)$ with type $[t^{n_t}, 1^{n_1}]$, and with the properties given in (3), which thus satisfies the conditions specified in (4), (5), and (6).

For the inductive step, suppose that for some j, with $0 \leq j < \Theta_r - 1$, we have constructed a subspace partition $\mathcal{P}_j$ of $H_j \cong V(n-j,q)$ of the type given in (4), and with the properties given in (5) and (6). We then use Lemma 8 to determine the average, $b_{avg,1}$, of the values $b_{H,1}$

over all hyperplanes H of H_j.

$$b_{avg,1} = \frac{\sum_{b\in\mathcal{B}} b_1\ s_b}{\sum_{b\in\mathcal{B}} s_b} = \frac{m_{j,1}\Theta_{n-1-j}}{\Theta_{n-j}} = \left(c_j q^{t-j} + \delta_{t+1-j}\right)\left(\frac{q^{n-1-j}-1}{q^{n-j}-1}\right)$$

$$< \frac{c_j q^{t-j} + \delta_{t+1-j}}{q} \tag{7}$$

$$< c_j q^{t-j-1} + \delta_{t-j}.$$

It follows from (7) that there exists a hyperplane H_{j+1} of H_j with

$$b_{H_{j+1},1} \le b_{avg,1} < c_j q^{t-j-1} + \delta_{t-j}. \tag{8}$$

Next, we apply Lemma 7 and (2) to the partition $\mathcal{P}_j$ and the hyperplane H_{j+1} of H_j to obtain:

$$1 + b_{H_{j+1},1}\ q + \sum_{i=t-j}^{t} b_{H_{j+1},i}\ q^i = |\mathcal{P}_j| = n_t + m_{j,1}$$

$$= \ell q^t + 2 + c_j q^{t-j} + \delta_{t+1-j}$$

$$= 1 + \ell q^t + c_j q^{t-j} + q\delta_{t-j}, \tag{9}$$

where $0 \le c_j \le \Theta_r - 1 - j$. Simplifying (9) yields

$$b_{H_{j+1},1} + \sum_{i=t-j}^{t} b_{H_{j+1},i}\ q^{i-1} = \ell q^{t-1} + c_j q^{t-j-1} + \delta_{t-j}. \tag{10}$$

Then, it follows from (2) and (10) that

$$b_{H_{j+1},1} \bmod q^{t-j-1} = \delta_{t-j}. \tag{11}$$

By (8) and (11), there exists a nonnegative integer c_{j+1} such that

$$m_{j+1,1} = b_{H_{j+1},1} = c_{j+1} q^{t-j-1} + \delta_{t-j}, \text{ and } 0 \le c_{j+1} \le \Theta_r - 2 - j. \tag{12}$$

Let $\mathcal{P}_{j+1}$ be the subspace partition of H_{j+1} defined by:

$$\mathcal{P}_{j+1} = \{W \cap H_{j+1} :\ W \in \mathcal{P}_j\}.$$

Since $t - j > 2$ (because $j + 1 < \Theta_r < t$) and $\dim(W \cap H_{j+1}) \in \{\dim W, \dim W - 1\}$ for each $W \in \mathcal{P}_j$, it follows that $\mathcal{P}_{j+1}$ is a subspace partition of H_{j+1} of type

$$[t^{m_{j+1,t}}, (t-1)^{m_{j+1,t-1}}, \ldots, (t-j-1)^{m_{j+1,t-j-1}}, 1^{m_{j+1,1}}], \tag{13}$$

where $m_{j+1,t}, m_{j+1,t-1}, \ldots, m_{j+1,t-j-1}$ satisfy

$$\sum_{i=t-j-1}^{t} m_{j+1,i} = \sum_{i=t-j}^{t} m_{j,i} = n_t. \tag{14}$$

The inductive step follows since $\mathcal{P}_{j+1}$ is a subspace partition of $H_{j+1} \cong V(n-j-1, q)$ of the type given in (13), which satisfies the conditions in (14) and (12).

Thus far, we have shown that the desired subspace partition $\mathcal{P}_j$ of H_j exists for any integer j such that $0 \le j \le \Theta_r - 1$.

For the final part of the proof, we set $j = \Theta_r - 1$ and show that the existence of the subspace partition $\mathcal{P}_{\Theta_r-1}$ of H_{Θ_r-1} leads to a contradiction. If $j = \Theta_r - 1$, then it follows from (6) that $c_{\Theta_r-1} = 0$ and $m_{\Theta_r-1,1} = \delta_{t+2-\Theta_r}$. We use Lemma 8 one last time to determine the average, $b_{avg,1}$, of the values $b_{H,1}$ over all hyperplanes H of H_{Θ_r-1}. We obtain,

$$\begin{aligned} b_{avg,1} = \frac{\sum_{b\in\mathcal{B}} b_1\ s_b}{\sum_{b\in\mathcal{B}} s_b} = \frac{m_{\Theta_r-1,1}\Theta_{n-\Theta_r}}{\Theta_{n-\Theta_r+1}} &= \delta_{t+2-\Theta_r}\frac{q^{n-\Theta_r}-1}{q^{n-\Theta_r+1}-1} \\ &< \frac{\delta_{t+2-\Theta_r}}{q} \\ &< \delta_{t+1-\Theta_r}. \end{aligned} \tag{15}$$

It follows from (15) that there exists a hyperplane H^* of H_{Θ_r-1} with

$$b_{H^*,1} \le b_{avg,1} < \delta_{t+1-\Theta_r}. \tag{16}$$

We then use Lemma 7 and (2) on the partition $\mathcal{P}_{\Theta_r-1}$ and the hyperplane H^* of H_{Θ_r-1} to obtain:

$$\begin{aligned} 1 + b_{H^*,1}\ q + \sum_{i=t-\Theta_r+1}^{t} b_{H^*,i}\ q^i = |\mathcal{P}_{\Theta_r-1}| &= n_t + m_{\Theta_r-1,1} \\ &= \ell q^t + 2 + \delta_{t+2-\Theta_r} \\ &= 1 + \ell q^t + q\delta_{t+1-\Theta_r}, \end{aligned} \tag{17}$$

Simplifying (17) yields

$$b_{H^*,1} + \sum_{i=t-\Theta_r+1}^{t} b_{H^*,i}\ q^{i-1} = \ell q^{t-1} + \delta_{t+1-\Theta_r}. \tag{18}$$

Then, (2) and (18) imply that

$$b_{H^*,1} \bmod q^{t-\Theta_r} = \delta_{t+1-\Theta_r}. \tag{19}$$

Since $t - \Theta_r \ge 1$, it follows from (18) and (19) that $b_{H^*,1} \ge \delta_{t+1-\Theta_r}$, which contradicts (16). Thus, $\mu_q(n,t) \le \ell q^t + 1$ and the proof is complete. □

Proof of Theorem 5. For $r = 0$, Theorem 5 is just the result of André [1], and for $r = 1$, it follows from Theorem 2. For $r \geq 2$, Theorem 5 holds since the lower bound for $\mu_q(n, t)$ given in Theorem 2 and the upper bound given in Lemma 9 are equal. $\square$

4. Concluding Remarks

Applying the same averaging method used in the proof of Lemma 9 substantially improves the upper bound given by Drake and Freeman (see Theorem 1) in some of the remaining cases, i.e., when $t \in [r+1, \Theta_r]$. However, we omit those types of results here and will address them elsewhere. For instance, we can prove the following lemma.

Lemma 10. *Let n and t be positive integers with $t < n$, and let $r = n \bmod t$. If $r \geq 2$ and $t = \Theta_r$, then $\mu_q(n, t) \leq \ell q^t + q$.*

Remark 11. *If n, t, and r satisfy the hypothesis of Lemma 10, then (after some simplifications) Theorem 1 yields $\mu_q(n, t) \leq \ell q^t + \left\lceil \frac{q^r}{2} \right\rceil$.*

As mentioned in the introduction (Section 1), our result (Theorem 5) settles almost all the remaining cases of one of the main unsolved problems related to partial $(t-1)$-spreads over $\mathrm{PG}(n-1, q)$. As a corollary, Theorem 5 also settles several open problems in the area of subspace coding that were raised by Etzion [8], Etzion–Storme [9], and Heinlein et al. [17].

A *subspace code* over $\mathrm{PG}(n-1, q)$ is a collection of subspaces of $\mathrm{PG}(n-1, q)$ (e.g., see [9, Section 4] for a recent survey). In their seminal paper, Köetter and Kschischang [21] showed that subspace codes were well-suited for error-correction in the new model for information transfer called *network coding* [2]. Partial $(t-1)$-spreads form an important class of subspace codes, called *Grassmannian codes* (e.g., see [21, 10, 12]). Our result implies that the largest known partial $(t-1)$-spread codes are optimal for almost all values of n, t, and q.

References

[1] J. André, Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe, *Math Zeit.* **60** (1954), 156–186.

[2] R. Ahlswede, N. Cai, S.-Yen, R. Li, R. Yeung, Network information flow, *IEEE Trans. Inf. Theory* **46** (2000), 1204–1216.

[3] A. Beutelspacher, Partial spreads in finite projective spaces and partial designs, *Math. Zeit.* **145** (1975), 211–229.

[4] D. Drake and J. Freeman, Partial t-spreads and group constructible (s, r, μ)-nets, *J. Geom.* **13** (1979), 211–216.

[5] J. Eisfeld and L. Storme, (Partial) t-spreads and minimal t-covers in finite spaces, *Lecture notes from the Socrates Intensive Course in Finite Geometry and its Applications, Ghent, April 2000, Published electronically at http://www.maths.qmul.ac.uk/∼leonard/partialspreads/eisfeldstorme.ps.*

[6] J. Eisfeld , L. Storme , and P. Sziklai, On the spectrum of the sizes of maximal partial line spreads in $PG(2n, q)$, $n \geq 3$, *Designs Codes Crypt.* **36** (2005), 101–110.

[7] T. Etzion, Perfect byte-correcting codes, *IEEE Trans. Inf. Theory* **44** (1998), 3140–3146.

[8] T. Etzion, Problems on q-analogs in coding theory, *http://arxiv.org/abs/1305.6126.*

[9] T. Etzion and L. Storme, Galois geometries and coding theory, *Designs Codes Crypt.* **78** (2016), 311–350.

[10] T. Etzion A. Vardy, Error-correcting codes in projective space, *IEEE Trans. Inf. Theory* **57** (1998), 1165–1173.

[11] S. El-Zanati, H. Jordon, G. Seelinger, P. Sissokho, and L. Spence, The maximum size of a partial 3-spread in a finite vector space over GF(2), *Designs Codes Crypt.* **54** (2010), 101–107.

[12] E. Gorla and A. Ravagnani, Partial spreads in random network coding, *Fin. Fields Appl.* **26** (2014), 104–115.

[13] A. Gács and T. Szönyi, On maximal partial spreads in $PG(n, q)$, *Designs Codes Crypt.* **29** (2003), 123–129.

[14] O. Heden, A survey on perfect codes, *Adv. Math. Commun.* **2** (2008), 223–247.

[15] O. Heden, A survey of the different types of vector space partitions, *Disc. Math. Algo. Appl.* **4** (2012), 1–14.

[16] O. Heden and J. Lehmann, Some necessary conditions for vector space partitions, *Discrete Math.* **312** (2012), 351–361.

[17] D. Heinlein, M. Kiermaier, S. Kurz, and A. Wassermann, Tables of subspace codes, *http://arxiv.org/abs/1601.02864.*

[18] M. Herzog and J. Schönheim, Group partition, factorization and the vector covering problem, *Canad. Math. Bull.* **15(2)** (1972), 207–214.

[19] S. Hong and A. Patel, A general class of maximal codes for computer applications, *IEEE Trans. Comput.* **C-21** (1972), 1322–1331.

[20] D. Jungnickel and L. Storme, A note on maximal partial spreads with deficiency $q + 1$, q even, *J. Combin. Theory Ser. A* **102** (2003), 443–446.

[21] R. Köetter and F. Kschischang, A general class of maximal codes for computer applications, *IEEE Trans. Inf. Theory* **54** (2008), 3575–3591.

[22] S. Kurz, Improved upper bounds for partial spreads, *http://arxiv.org/abs/1512.04297.*