THE MAXIMUM SIZE OF A PARTIAL 3-SPREAD IN A FINITE VECTOR SPACE OVER $GF(2)$

S. EL-ZANATI, H. JORDON, G. SEELINGER, P. SISSOKHO, AND L. SPENCE

4520 MATHEMATICS DEPARTMENT
ILLINOIS STATE UNIVERSITY
NORMAL, ILLINOIS 61790–4520, U.S.A.

ABSTRACT. Let $n \geq 3$ be an integer, let $V_n(2)$ denote the vector space of dimension n over $GF(2)$, and let c be the least residue of n modulo 3. We prove that the maximum number of 3-dimensional subspaces in $V_n(2)$ with pairwise intersection $\{0\}$ is $\frac{2^n-2^c}{7} - c$ for $n \geq 8$ and $c = 2$. (The cases $c = 0$ and $c = 1$ have already been settled.) We then use our results to construct new optimal orthogonal arrays and (s, k, λ)-nets.

1. Introduction

Let n be a positive integer and let q be a prime power. Let $V_n(q)$ denote the vector space of dimension n over $GF(q)$ and let $t \leq n$ be a positive integer. We write $W \cong V_n(q)$ if W is a vector space that is isomorphic to $V_n(q)$. A *partial t-spread* of $V_n(q)$ is a collection $S = \{W_1, \ldots, W_k\}$ of t-dimensional subspaces of $V_n(q)$ such that $W_i \cap W_j = \{0\}$ for $1 \leq i < j \leq k$. We call k the *size* of the partial t-spread S. Moreover, we call S *maximal* if $\left(V_n(q) \setminus \bigcup_{i=1}^{k} W_i\right) \cup \{0\}$ does not contain a t-dimensional subspace, and we call S *maximum* if it has the largest possible size. Finally, if $\bigcup_{i=1}^{k} W_i = V_n(q)$, then S is simply called a *t-spread*.

It is easy to see that a t-spread of $V_n(q)$ exists if and only if t divides n. On the other hand, partial t-spreads of $V_n(q)$ exist whenever $t \leq n$. Given a partial t-spread S, one open question is to find conditions under which S is maximal, and another is to find conditions under which S is maximum. Partial t-spreads have applications to the construction of byte-error-detecting and single-error-correcting codes (see [6, 17]) and to orthogonal arrays and (s, k, λ)-nets (see [8]). The problem of

Key words and phrases. Spreads; partial spreads; orthogonal arrays; (s, k, λ)-nets.

finding maximal partial t-spreads is also well-studied in finite geometry (see [1, 9, 10, 12, 13, 15, 16, 18] and the references therein).

Let $\mu_q(n,t)$ denote the size of a maximum partial t-spread in $V_n(q)$ and let c be the least residue of n modulo t. Obviously, the maximal partial t-spread problem is dependent on the problem of determining $\mu_q(n,t)$. If $c=0$, then we simply obtain a t-spread and it is well-known that $\mu_q(n,t)=(q^n-1)/(q^t-1)$ in this case (see [2]). In general, very little is known about the exact value of $\mu_q(n,t)$ when $c \neq 0$. However, a few special cases have been settled. If $c=1$, then Hong and Patel [17] proved that $\mu_q(n,t)=(q^n-q)/(q^t-1)-(q-1)$ when $q=2$, and Beutelspacher [2] extended this result to any prime power q.

In this paper, we prove that $\mu_2(n,3)=(2^n-2^c)/7-c$ for $n \geq 8$ and $c=2$. Combining this with the above result of Hong and Patel yields the full formula for $\mu_2(n,3)$ (see Theorem 5). Our results disprove a conjecture by Eisfeld and Storme [9] stating that $\mu_q(n,t) \leq (q^n - q^c)/(q^t-1)-(q^c-1)$, and a conjecture by Hong and Patel [17] stating that $\mu_2(n,t)=(2^n-2^c)/(2^t-1)-(2^c-1)$.

The rest of this paper is organized as follows. In Section 2, we provide the main results of this paper and in Section 3, we apply these results to construct new optimal orthogonal arrays and (s,k,λ)-nets.

2. Main results

2.1. Existence of a partial 3-spread of size 34 in $V_8(2)$.

The heart of our proof for Theorem 5 is the construction of a partial 3-spread of size 34 in $V_8(2)$. This construction uses a computer search. To explain the idea behind this computer search, we start with the concept of vector space partition (see [3, 4, 5, 14] and the references therein).

A *vector space partition* (or simply *partition*) of $V=V_n(q)$ is a collection $\mathcal{P}$ of subspaces of V such that each nonzero vector of V appears in exactly one of the subspaces in $\mathcal{P}$. We say that $\mathcal{P}$ is a partition of V of *type* $d_1^{a_1}\ldots d_k^{a_k}$ if it contains a_i subspaces of dimension d_i for all $1 \leq i \leq k$, and

$$\sum_{i=1}^{k} a_i(q^{d_i}-1)=q^n-1.$$

It is clear from the above definition that a partial t-spread of $V_n(q)$ of size k is equivalent to a partition of $V_n(q)$ of type $t^k 1^x$, where $x=(q^n-1)/(q-1)-k(q^t-1)/(q-1)$.

Bu [5] described the following simple method for constructing vector space partitions. Let $V=V_{n+1}(q)$ have a partition into the subspaces

$W_1, \ldots, W_k$. Let V' be an n-dimensional subspace of V and set $W_i' = W_i \cap V'$ for $1 \leq i \leq k$. Then the subspaces $W_1', \ldots, W_k'$ form a partition $\mathcal{P}'$ of $V' \cong V_n(q)$. A partition of V' with the same type as $\mathcal{P}'$ is called a *seed partition of* $\mathcal{P}$ (or simply a seed partition if $\mathcal{P}$ is clear from the context). So, instead of trying to find $\mathcal{P}$ directly, we start with a seed partition $\mathcal{Q}$ and use a computer search to extend it to a partition of the same type as $\mathcal{P}$. However, this process is not necessarily successful for every seed partition $\mathcal{Q}$ (see Remark 1). To apply this idea to our problem, assume that there exists a partition $\mathcal{P}$ of $V = V_8(2)$ of type $3^{34}1^{17}$ (i.e., a partial 3-spread of size 34). Then using basic counting arguments, it can be shown that the partition $\mathcal{P}$ induces in $V' \cong V_7(2)$ a potential partition $\mathcal{Q}$ of type $3^6 2^{28} 1^1$, $3^5 2^{29} 1^5$, $3^4 2^{30} 1^9$, $3^3 2^{31} 1^{13}$, or $3^2 2^{32} 1^{17}$. Partitions of $V_7(2)$ of types $3^5 2^{29} 1^5$, $3^4 2^{30} 1^9$, $3^3 2^{31} 1^{13}$, and $3^2 2^{32} 1^{17}$ exist (see [11]); there is no partition of $V_7(2)$ of type $3^6 2^{28} 1^1$ (see Theorem 4 in [14]).

We now explain the setup for our computer search using a seed partition of type $3^5 2^{29} 1^5$. In the following, we denote the vector $[\alpha_7, \ldots, \alpha_0]$ of $V_8(2)$ by the integer $\sum_{i=0}^{7} \alpha_i 2^i$ and say that it has *even* (*odd*) *weight* if there is an even (odd) number of nonzero coordinates. Thus, $V_8(2)$ can be partitioned into two sets $\mathcal{E}$ and $\mathcal{O}$, consisting of the even and odd weight vectors respectively. Observe that $\mathcal{E} \cong V_7(2)$.

Step 1: Start with a partition of $\mathcal{E}$ into 5 subspaces of dimension 3 (denoted by $A_1, \ldots, A_5$), 29 subspaces of dimension 2 ($B_1, \ldots, B_{29}$), and 5 subspaces of dimension 1 ($C_1, \ldots, C_5$).

Step 2: Let G be the graph with vertex set

$$V(G) = \Big\{ S \cup B_i : S \subseteq \mathcal{O},\ S \cup B_i \cong V_3(2), \text{ and } 1 \leq i \leq 29 \Big\},$$

and edge set

$$E(G) = \big\{ \{X, Y\} : X, Y \in V(G) \text{ and } X \cap Y = \{0\} \big\}.$$

Step 3: Search for a complete subgraph H of size 29 in G. If we denote the elements of $V(H)$ by A_i, $6 \leq i \leq 34$, then $\{A_1, \ldots, A_{34}\}$ is a partial 3-spread of size 34 in $V_8(2)$.

Since $V_8(2)$ can be partitioned into $\mathcal{E}$ and $\mathcal{O}$ and since each B_i is a 2-dimensional subspace of $\mathcal{E}$, it follows that B_i determines a unique partition of the set $\mathcal{O}$ into 32 subsets of size 4. Thus, there are $29 \cdot 32 = 928$ vertices in G. The size of the search space resulting from the above method is

$$\binom{|V(G)|}{29} = \binom{928}{29},$$

which is large. However, it is considerably smaller than the size of the search space resulting from a direct approach, which is

$$\binom{\text{Number of 3-dimensional subspaces in } V_8(2)}{34} = \binom{97155}{34}.$$

Thus the use of a seed partition gives us a more efficient means of searching for a partition of $V_8(2)$ of type $3^{34}1^{17}$.

Remark 1. *In general, we cannot expect each seed partition $\mathcal{Q}$ to be extendable to a partition $\mathcal{P}$ of the desired type. We still need to understand the key properties of a "good" seed partition.*

Here is an example[1] of a partial 3-spread of size 34 in $V_8(2)$, i.e., a partition $\mathcal{P}$ of $V_8(2)$ of type $3^{34}1^{17}$. This example also provides a partition of $V_8(2)$ of type $3^{34}2^{1}1^{14}$ by combining the three 1-dimensional subspaces $\{122\}$, $\{133\}$, and $\{255\}$.

Example 2.

$$\begin{aligned}
A_1 &= \{5, 75, 78, 169, 172, 226, 231\}\\
A_2 &= \{6, 43, 45, 195, 197, 232, 238\}\\
A_3 &= \{3, 29, 30, 108, 111, 113, 114\}\\
A_4 &= \{20, 72, 92, 130, 150, 202, 222\}\\
A_5 &= \{33, 68, 101, 144, 177, 212, 245\}\\
A_6 &= \{2, 61, 63, 65, 67, 124, 126\}\\
A_7 &= \{4, 19, 23, 66, 70, 81, 85\}\\
A_8 &= \{1, 86, 87, 140, 141, 218, 219\}\\
A_9 &= \{9, 16, 25, 35, 42, 51, 58\}\\
A_{10} &= \{7, 99, 100, 147, 148, 240, 247\}\\
A_{11} &= \{38, 76, 106, 155, 189, 215, 241\}\\
A_{12} &= \{24, 40, 48, 69, 93, 109, 117\}\\
A_{13} &= \{12, 103, 107, 132, 136, 227, 239\}\\
A_{14} &= \{56, 88, 96, 152, 160, 192, 248\}\\
A_{15} &= \{39, 94, 121, 153, 190, 199, 224\}\\
A_{16} &= \{11, 34, 41, 196, 207, 230, 237\}\\
A_{17} &= \{15, 97, 110, 167, 168, 198, 201\}\\
A_{18} &= \{32, 84, 116, 159, 191, 203, 235\}\\
A_{19} &= \{55, 71, 112, 154, 173, 221, 234\}\\
A_{20} &= \{50, 80, 98, 145, 163, 193, 243\}\\
A_{21} &= \{13, 54, 59, 131, 142, 181, 184\}\\
A_{22} &= \{53, 74, 127, 134, 179, 204, 249\}\\
A_{23} &= \{8, 18, 26, 166, 174, 180, 188\}\\
A_{24} &= \{31, 64, 95, 164, 187, 228, 251\}
\end{aligned}$$

[1]We omit the zero vector when listing the vectors of a subspace.

$A_{25} = \{60, 90, 102, 138, 182, 208, 236\}$
$A_{26} = \{27, 73, 82, 135, 156, 206, 213\}$
$A_{27} = \{37, 77, 104, 146, 183, 223, 250\}$
$A_{28} = \{17, 105, 120, 171, 186, 194, 211\}$
$A_{29} = \{52, 79, 123, 158, 170, 209, 229\}$
$A_{30} = \{47, 89, 118, 128, 175, 217, 246\}$
$A_{31} = \{10, 22, 28, 129, 139, 151, 157\}$
$A_{32} = \{46, 83, 125, 143, 161, 220, 242\}$
$A_{33} = \{21, 36, 49, 205, 216, 233, 252\}$
$A_{34} = \{44, 91, 119, 137, 165, 210, 254\}$

2.2. **Maximum Partial 3-spreads in $V_n(2)$.**

We will use the following theorem. The lower bound is attributed to Beutelspacher [2] and Hong–Patel [17], and the upper bound is due to Drake–Freeman [8].

Theorem 3 ([2, 8, 17])**.** *Let $n \geq 3$ and $t \leq n$ be positive integers, and let q be a prime power. Let c be the least residue of n modulo t, and let θ be defined by*

$$2\theta = \sqrt{1 + 4q^t(q^t - q^c)} - (2q^t - 2q^c + 1).$$

Then

$$\frac{q^n - q^c}{q^t - 1} - (q^c - 1) \leq \mu_q(n, t) \leq \frac{q^n - q^c}{q^t - 1} - \lfloor \theta \rfloor - 1.$$

We will also use the following result of Bu [5].

Lemma 4 ([5])**.** *Let n and d be integers such that $1 \leq d \leq n/2$, and let q be a prime power. Then $V_n(q)$ can be partitioned into 1 subspace of dimension $n - d$ and q^{n-d} subspaces of dimension d.*

We now prove our main theorem.

Theorem 5. *Let $n \geq 3$ be an integer and c be the least residue of n modulo 3. Then the maximum number of 3-dimensional subspaces in $V_n(2)$ with pairwise intersection $\{0\}$ is*

$$\mu_2(n, 3) = \begin{cases} 1 & \text{if} \quad 3 \leq n < 6, \\ \frac{2^n - 2^c}{7} - c & \text{if} \quad n \geq 6. \end{cases}$$

Proof. If $n < 6$, then the theorem is trivial. If $n \geq 6$, then we have the following cases.
Case 1: $c = 0$. Then 3 divides n and a 3-spread of size $(2^n - 1)/7$ exists (see Bu [5]).

Case 2: $c = 1$. Then the theorem follows from the work of Hong and Patel [17]. However, we include the proof for completeness. By Theorem 3, we have $\mu_2(n,3) < \frac{2^n-2}{7}$. So it suffices to show that $V_n(2)$ can be partitioned into $\frac{2^n-2}{7} - 1$ subspaces of dimension 3 and 8 subspaces of dimension 1. Such a partition can be obtained by recursively applying Lemma 4 on $V_{n-3i}(2)$ for $1 \le i \le (n-7)/3$ and then extracting an additional 3-dimensional subspace from $V_4(2)$.

Case 3: $c = 2$. By Theorem 3, $\mu_2(n,3) < \frac{2^n-2^2}{7} - 1$. So it suffices to show that $V_n(2)$ can be partitioned into $\frac{2^n-2^2}{7} - 2$ subspaces of dimension 3 and 17 subspaces of dimension 1. Let $n = 3m+2$ for some positive integer m. The proof now proceeds by induction on m. Since $n \ge 6$, it follows that $m \ge 2$. If $m = 2$, then Example 2 yields a partition of $V_8(2)$ with 34 subspaces of dimension 3 and 17 subspaces of dimension 1. Now assume that for all $2 \le k < m$, $V_{3k+2}(2)$ can be partitioned into $\frac{2^{3k+2}-2^2}{7} - 2$ subspaces of dimension 3 and 17 subspaces of dimension 1. By Lemma 4, $V_{3m+2}(2)$ can be partitioned into a subspace L of dimension $3m-1$ and 2^{3m-1} subspaces of dimension 3. By the induction hypothesis, the subspace $L \cong V_{3(m-1)+2}(2)$ can be partitioned into $\frac{2^{3m-1}-2^2}{7} - 2$ subspaces of dimension 3 and 17 subspaces of dimension 1. Thus $V_n(2) = V_{3m+2}(2)$ can be partitioned into

$$\frac{2^{3m-1}-2^2}{7} - 2 + 2^{3m-1} = \frac{2^{3m+2}-2^2}{7} - 2 = \frac{2^n-2^2}{7} - 2$$

subspaces of dimension 3 and 17 subspaces of dimension 1.

This concludes the proof of the theorem. □

3. An Application to Orthogonal Arrays and (s, k, λ)-nets

In this section, we give an application of partial 3-spreads of $V_n(2)$ to orthogonal arrays, and (s,k,λ)-nets (see [8]). We start with some general definitions from [7] (Section 6 in Chapter III).

An *orthogonal array* of size N with k constraints, s levels, strength r, and index λ is a $k \times N$ array with entries from a set of $s \ge 2$ symbols, having the property that in every $r \times N$ sub-matrix, every $r \times 1$ column vector appears $\lambda = N/s^r$ times. It is denoted by $OA_\lambda(N,k,s,r)$ or $OA_\lambda(k,s,r)$, and if $r = 2$, we simply write $OA_\lambda(k,s)$. An (s,k,λ)-*net* is a set X with λs^2 points together with a set D of ks subsets (blocks) of X, each of size λs, such that: (1) The set of all blocks is partitioned into k parallel classes, each containing s disjoint blocks, and (2) every two non-parallel blocks intersect in λ points. We note that an $OA_\lambda(k,s)$ is equivalent to an (s,k,λ)-net (see Theorem 6.6 in [7]).

The following method of Drake and Freeman [8] shows how to construct an (s, k, λ)-net (and thus an $OA_\lambda(k, s)$) via partial t-spreads. Suppose that $n \geq 2t$ and consider a partition of $V_n(q)$ of type $t^k 1^x$, where $x = (q^n - 1)/(q - 1) - k(q^t - 1)/(q - 1)$ and $W_1, \ldots, W_k$ are the t-dimensional subspaces. For each $1 \leq i \leq k$, let

$$W_i^* = \{u \in V_n(q) : \langle u, v \rangle = 0 \text{ for every } v \in W_i\},$$

where $\langle , \rangle$ is the standard dot product. Then W_i^* is an $(n-t)$-dimensional subspace of $V_n(q)$. By setting $X = V_n(q)$ and

$$D = \{B : B \text{ is a coset of } W_i^*,\ 1 \leq i \leq k\},$$

it is easy to check that the resulting incidence structure is a (q^t, k, q^{n-2t})-net or equivalently an $OA_\lambda(k, q^t)$ with $\lambda = q^{n-2t}$.

In light of the above discussion, the following result is a direct corollary of Theorem 5. An analogous version of this corollary holds for $(8, k, 2^{n-6})$-nets.

Corollary 6. *Let $n \geq 6$ be an integer and c be the least residue of n modulo 3. Then there exists an orthogonal array $OA_\lambda(k, 8)$ with $\lambda = 2^{n-6}$ and*

$$k = \mu_2(n, 3) = \begin{cases} 1 & \text{if} \quad 3 \leq n < 6, \\ \frac{2^n - 2^c}{7} - c & \text{if} \quad n \geq 6. \end{cases}$$

Moreover, these orthogonal arrays are optimal, i.e., they have the largest possible number of constraints k for a fixed λ.

Proof. The existence follows from Theorem 5, and the optimality follows from the Bose-Bush bound on k (see [7]). □

Finally, it is interesting to note that the upper bound in Theorem 3 on which our main result (Theorem 5) relies was established by Drake and Freeman [8] using this very same Bose-Bush bound.

References

[1] J. De Beule and K. Metsch, The maximum size of a partial spread in $H(5, q^2)$ is $q^3 + 1$, *J. of Combin. Theory, Series A* **114** (2007), 761–768

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

[3] A. Beutelspacher, Partitions of finite vector spaces: an application of the Frobenius number in geometry, *Arch. Math.* **31** (1978), 202–208.

[4] A. Blinco, S. El-Zanati, G. Seelinger, P. Sissokho, L. Spence, and C. Vanden Eynden, On Vector space partitions and uniformly resolvable designs, *Designs, Codes and Crypt.* **15** (2008), 69-77.

[5] T. Bu, Partitions of a vector space, *Discrete Math.* **31** (1980), 79–83.

[6] W. Clark and L. Dunning, Partial partitions of vector spaces arising from the construction of byte error control codes, *Ars Combin.* **33** (1992), 161–177.

[7] C. Colbourn and M. Greig, Orthogonal arrays of index more than one, in: The CRC handbook of combinatorial designs. Edited by C. Colbourn and J. Dinitz. *CRC Press Series on Discrete Mathematics and its Applications,* CRC Press, Boca Raton, FL (2007), 219–228.

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

[9] J. Eisfeld and L. Storme, (Partial) t-spreads and minimal t-covers in finite spaces, *http://citeseer.ist.psu.edu/427583.html*, 29 pp.

[10] 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, and Crypt.*, **36** (2005), 101–110.

[11] S. El-Zanati, G. Seelinger, P. Sissokho, L. Spence, and C. Vanden Eynden, On partitions of finite vector spaces of small dimension over $GF(2)$, *Discrete Mathematics*, (2008), available online.

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

[13] P. Govaerts and L. Storme, On a particular class of minihypers and its applications. I. The result for general q, *Designs, Codes, and Crypt.*, **28** (2003), 51–63.

[14] O. Heden, Partitions of finite abelian groups, *Europ. J. Combin.* **7** (1986), 11–25.

[15] O. Heden, A Maximal Partial Spread of Size 45 in $PG(3, 7)$, *Designs, Codes, and Crypt.*, **22** (2001), 331–334.

[16] O. Heden, Maximal partial spreads and the modular n-queen problem III, *Discrete Math.*, **243** (2002), 135–150.

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

[18] 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.