

HEDEN'S BOUND ON THE TAIL OF A VECTOR SPACE PARTITION

SASCHA KURZ*

ABSTRACT. A vector space partition of \mathbb{F}_q^v is a collection of subspaces such that every non-zero vector is contained in a unique element. We improve a lower bound of Heden on the number of elements of the smallest occurring dimension.

1. INTRODUCTION

In this note we translate Heden [5] into geometry and find that the same theory now only takes a small fraction of the space. Having decoded the approach using mixed perfect 1-codes, we go along the lines of [7] and improve Heden's result a little. In [7] analytic solutions of linear programming methods for projective linear codes or sets of points have been applied in order to compute upper bounds for partial spreads. Interestingly enough, the very same happened in [3], where the authors translated and improved a lower bound of Heden on the size of maximal partial line spreads.

Let $q > 1$ be a prime power and v a positive integer. A *vector space partition* \mathcal{P} of \mathbb{F}_q^v is a collection of subspaces with the property that every non-zero vector is contained in a unique member of \mathcal{P} . If \mathcal{P} contains m_d subspaces of dimension d , then \mathcal{P} is of type $k^{m_k} \dots 1^{m_1}$. We may leave out some of the cases with $m_d = 0$. If d_1 is the smallest dimension with $m_{d_1} \neq 0$, we call m_{d_1} the length of the tail. Subspaces of dimension d are also called *d-spaces*. 1-spaces are called *points* and each k -space contains $\begin{bmatrix} k \\ 1 \end{bmatrix}_q := \frac{q^k - 1}{q - 1}$ points. Heden's main result is:

Theorem 1. (Theorem 1 in [5]) *Let \mathcal{P} be a vector space partition of type $d_1^{u_1} \dots d_2^{u_2} d_1^{u_1}$ of \mathbb{F}_q^v , where $u_1, u_2 > 0$.*

- (i) *If $q^{d_2 - d_1}$ does not divide u_1 and if $d_2 < 2d_1$, then $u_1 \geq q^{d_1} + 1$;*
- (ii) *if $q^{d_2 - d_1}$ does not divide u_1 and if $d_2 \geq 2d_1$, then either d_1 divides d_2 and $u_1 = \begin{bmatrix} d_2 \\ 1 \end{bmatrix}_q / \begin{bmatrix} d_1 \\ 1 \end{bmatrix}_q$ or $u_1 > 2q^{d_2 - d_1}$;*
- (iii) *if $q^{d_2 - d_1}$ divides u_1 and $d_2 < 2d_1$, then $u_1 \geq q^{d_2} - q^{d_1} + q^{d_2 - d_1}$;*
- (iv) *if $q^{d_2 - d_1}$ divides u_1 and $d_2 \geq 2d_1$, then $u_1 \geq q^{d_2}$.*

The other theorems of [5] are as follows: Theorems 2 and 3 classify the possible sets of d_1 -spaces for $u_1 = q^{d_1} + 1$ and $u_1 = \begin{bmatrix} d_2 \\ 1 \end{bmatrix}_q / \begin{bmatrix} d_1 \\ 1 \end{bmatrix}_q$, respectively. Theorem 4 is the direct application of Theorem 3 and Theorem 1(i).

2. SETS OF DISJOINT k -SPACES AND THEIR INCIDENCES WITH HYPERPLANES

For a positive integer k let \mathcal{N} be a set of pairwise disjoint k -spaces in \mathbb{F}_q^v , where v is minimal. By a_i we denote the number of hyperplanes H of \mathbb{F}_q^v with $\#(\mathcal{N} \cap H) := \#\{U \in \mathcal{N} : U \leq H\} = i$ and set $n := \#\mathcal{N}$. Double-counting the incidences of the tuples (H) , (B_1, H) , and (B_1, B_2, H) , where H is a hyperplane and $B_1 \neq B_2$ are elements of \mathcal{N} contained in H gives:

$$\sum_{i=0}^{n-1} a_i = \begin{bmatrix} v \\ 1 \end{bmatrix}_q, \quad \sum_{i=0}^{n-1} i a_i = n \cdot \begin{bmatrix} v - k \\ 1 \end{bmatrix}_q, \quad \text{and} \quad \sum_{i=0}^{n-1} i(i-1) a_i = n(n-1) \cdot \begin{bmatrix} v - 2k \\ 1 \end{bmatrix}_q. \quad (1)$$

For three different elements B_1, B_2, B_3 of \mathcal{N} their span $\langle B_1, B_2, B_3 \rangle$ has a dimension i between $2k$ and $3k$. Denoting the number of corresponding triples by b_i , double-counting gives:

$$\sum_{i=0}^{n-1} i(i-1)(i-2) a_i = \sum_{i=2k}^{3k} b_i \begin{bmatrix} v - i \\ 1 \end{bmatrix}_q \quad \text{and} \quad \sum_{i=2k}^{3k} b_i = n(n-1)(n-2). \quad (2)$$

Given parameters q, k, n , and v the so-called (*integer*) *linear programming method*, developed for association schemes by Delsarte [4], asks for a solution of the equation system given by (1) and (2) with $a_i, b_i \in \mathbb{R}_{\geq 0}$ ($a_i, b_i \in \mathbb{N}$). If no solution exists, then no corresponding set \mathcal{N} can exist. For $k = 1$ one can take the elements of \mathcal{N} as the columns of a generator matrix of a projective linear code over \mathbb{F}_q . In this case, the equations from (1) and (2) correspond to the first four MacWilliams identities, see e.g. [6].

Lemma 2. *If $a_i = 0$ for all $i \neq r > 0$ and $k < v$ in the above setting, then there exists an integer $s \geq 2$ with $v = sk$ and \mathcal{N} consists of $\frac{q^v - 1}{q^k - 1}$ disjoint k -spaces partitioning \mathbb{F}_q^v . Additionally we have $r = \frac{q^{v-k} - 1}{q^k - 1}$.*

* Grant KU 2430/3-1 – *Integer Linear Programming Models for Subspace Codes and Finite Geometry* – German Research Foundation.

PROOF. Solving (1) for r , a_r , and n gives $n = \frac{q^{2v-k} - q^v - q^{v-k} + 1}{q^v - q^{v-k} - q^k + 1}$. Writing $v = sk + t$ with $s, t \in \mathbb{N}$ and $0 \leq t < k$ we obtain $n = \sum_{i=1}^s q^{v-ik} + \frac{q^{v-k+t} - q^{v-k} - q^t + 1}{q^v - q^{v-k} - q^k + 1}$. Since $n \in \mathbb{N}$ and $0 \leq q^{v-k+t} - q^{v-k} - q^t + 1 < q^v - q^{v-k} - q^k + 1$ we have $q^{v-k+t} - q^{v-k} - q^t + 1 = 0$ so that $t = 0$ and $n = \frac{q^v - 1}{q^k - 1}$. Counting points gives that \mathcal{N} partitions \mathbb{F}_q^v . \square

We remark that $r = 0$ forces $n \in \{0, 1\}$ so that \mathcal{N} is empty or consists of a single k -space in \mathbb{F}_q^k and $v = k$ implies the latter case. So, this degenerated cases correspond to $s \in \{0, 1\}$ in Lemma 2. As pointed out after [5, Theorem 2], such results can be proved in different ways. While the case that only one a_i is non-zero is rather special, we can show that many a_i are equal to zero in our setting.

Lemma 3. *Let \mathcal{P} be a vector space partition of type $d_1^{u_1} \dots d_2^{u_2} d_1^{u_1}$ of \mathbb{F}_q^v , where $u_1, u_2 > 0$, and \mathcal{N} be the set of d_1 -spaces. Then, we have $\#\mathcal{N} \equiv \#(\mathcal{N} \cap H) \pmod{q^{d_2-d_1}}$ for every hyperplane H of \mathbb{F}_q^v .*

PROOF. For each $U \in \mathcal{P}$ we have $\dim(U \cap H) \in \{\dim(U), \dim(U) - 1\}$. So counting points in \mathbb{F}_q^v and H gives the existence of integers a, a' with $m \cdot \begin{bmatrix} d_2 \\ 1 \end{bmatrix}_q + aq^{d_2} + u_1 \begin{bmatrix} d_1 \\ 1 \end{bmatrix}_q = \begin{bmatrix} v \\ 1 \end{bmatrix}_q$ and $m \cdot \begin{bmatrix} d_2-1 \\ 1 \end{bmatrix}_q + a'q^{d_2-1} + u_1'q^{d_1-1} + u_1 \begin{bmatrix} d_1-1 \\ 1 \end{bmatrix}_q = \begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q$, where $m := \sum_{i=2}^l u_i$ and $u_1' := \#(\mathcal{N} \cap H)$. By subtraction we obtain $mq^{d_2-1} + aq^{d_2} - a'q^{d_2-1} + u_1q^{d_1-1} - u_1'q^{d_1-1} = q^{v-1}$, so that $u_1q^{d_1-1} \equiv u_1'q^{d_1-1} \pmod{q^{d_2-1}}$. \square

Definition 4. Let \mathcal{N} be a set of k -spaces in \mathbb{F}_q^v . If there exists a positive integer r such that a_i is non-zero only if $\#\mathcal{N} - i$ is divisible by q^r and the k -spaces are pairwise disjoint, then we call \mathcal{N} q^r -divisible.

Using the notation of Lemma 3, \mathcal{N} is $q^{d_2-d_1}$ -divisible. For $d_1 = 1$, taking the elements of \mathcal{N} as columns of a generator matrix, we obtain a projective linear code, whose Hamming weights are divisible by q^{d_2-1} .

Lemma 5. *For a q^r -divisible set \mathcal{N} of k -spaces in \mathbb{F}_q^v , there exists a hyperplane H with $\#(\mathcal{N} \cap H) \leq n/q^k$.*

PROOF. Let i be the smallest index with $a_i \neq 0$. Then, the first two equations of (1) are equivalent to $\sum_{j \geq 0} a_{i+q^r j} = \begin{bmatrix} v \\ 1 \end{bmatrix}_q$ and $\sum_{j \geq 0} (i + q^r j) \cdot a_{i+q^r j} = n \begin{bmatrix} v-k \\ 1 \end{bmatrix}_q$. Subtracting i times the first equation from the second equation gives $\sum_{j > 0} q^r j a_{i+q^r j} = n \cdot \frac{q^{v-k} - 1}{q-1} - i \cdot \frac{q^v - 1}{q-1}$. Since the left-hand side is non-negative, we have $i \leq \frac{q^{v-k} - 1}{q-1} \cdot n \leq \frac{n}{q^k}$. \square

Stated less technical, the proof of Lemma 5 is given by the fact that the hyperplane with the minimum number of k -spaces contains at most as many k -spaces as the average number of k -spaces per hyperplane.

Lemma 6. *Let $m \in \mathbb{Z}$ and \mathcal{N} be a q^r -divisible set of k -spaces in \mathbb{F}_q^v . Then, $\tau(n, q^r, q^k, m) \cdot q^{v-2k-2r} - m(m-1) \geq 0$, where $\tau(n, \Delta, u, m) := \Delta^2 u^2 m(m-1) - n(2m-1)u(u-1)\Delta + n(u-1)(n(u-1)+1)$.*

PROOF. With $y = q^{v-2k}$, $u = q^k$, and $\Delta = q^r$, we can rewrite the equations of (1) to $u^2 y - 1 = (q-1) \sum_{i \in \mathbb{Z}} a_i$, $n \cdot (uy - 1) = (q-1) \sum_{i \in \mathbb{Z}} i a_i$, and $n(n-1) \cdot (y-1) = \sum_{i \in \mathbb{Z}} i(i-1) a_i$. $(n-m\Delta)(n-(m-1)\Delta)$ times the first minus $2n - (2m-1)\Delta - 1$ times the second plus the third equation gives $y \cdot \tau(n, \Delta, u, m) - \Delta^2 m(m-1) = (q-1) \sum_{i \in \mathbb{Z}} (n-m\Delta-i)(n-(m-1)\Delta-i) a_i = (q-1) \sum_{h \in \mathbb{Z}} \Delta^2 (m-h)(m-h+1) a_{n-h\Delta} \geq 0$. \square

Lemma 7. *If \mathcal{N} is a q -divisible set of k -spaces in \mathbb{F}_q^v of cardinality $q^k + 1$, then \mathcal{N} partitions \mathbb{F}_q^{2k} .*

PROOF. Setting $c_i := (q-1)a_{1+iq}$ and $l := q^{k-1} - 1$ we can rewrite the equations of (1) to $\sum_{i=0}^l c_i = q^v - 1$, $\sum_{i=0}^l (1+iq)c_i = (q^k + 1)(q^{v-k} - 1)$, and $\sum_{i=0}^l iq(1+iq)c_i = (q^k + 1)q^k (q^{v-2k} - 1)$. Since $ql + 1$ times the second minus $ql + 1$ times the first minus the third equation gives $0 \leq \sum_{i=0}^l iq^2(l-i)c_i = -q^{k+1}(q^{v-2k} - 1)$, we have $v = 2k$. Every point of \mathbb{F}_q^v is covered by an element from \mathcal{N} due to $\begin{bmatrix} 2k \\ 1 \end{bmatrix}_q / \begin{bmatrix} k \\ 1 \end{bmatrix}_q = q^k + 1$. \square

3. PROOF OF HEDEN'S RESULTS AND FURTHER IMPROVEMENTS

Let \mathcal{P} be a vector space partition of type $d_1^{u_1} \dots d_2^{u_2} d_1^{u_1}$ of \mathbb{F}_q^v , where $u_1, u_2 > 0$, and \mathcal{N} the set of d_1 -spaces.

Assume that $q^{d_2-d_1}$ does not divide u_1 . We have $\#(\mathcal{N} \cap H) \geq 1$ for every hyperplane H due to Lemma 3, so that Lemma 5 gives $u_1 \geq q^{d_1}$. Thus, we have $u_1 \geq q^{d_1} + 1$ and can apply Lemma 7. If $u_1 < 2q^{d_2-d_1}$ we can apply Lemma 2 so that either d_2 divides d_1 and $u_1 = (q^{d_2} - 1)/(q^{d_1} - 1)$ or $u_1 > 2q^{d_2-d_1}$.

Assume that $q^{d_2-d_1}$ divides u_1 . Setting $\Delta = q^{d_2-d_1}$, $u = q^{d_1}$, $n = l\Delta$, and $m = l^\dagger$ for some integer l , we conclude $\tau(n, \Delta, u, m) = l\Delta(\Delta l - \Delta u + u - 1) \geq 0$ from Lemma 6, so that $l \geq \lceil u - \frac{u}{\Delta} + \frac{1}{\Delta} \rceil$. The right-hand side is equal to $u = q^{d_1}$ if $d_2 \geq 2d_1$ and to $u - u/\Delta + 1 = q^{d_1} - q^{2d_1-d_2} + 1$ otherwise, which is equivalent to $n \geq q^{d_2}$ and $n \geq q^{d_2} - q^{d_1} + q^{d_2-d_1}$. We remark that equality is achievable in the latter case via the 2-weight codes constructed in [2] (with parameters $n' = d_1$ and $m = d_2 - d_1$). We do not know whether the corresponding $q^{d_2-d_1}$ -divisible set of d_1 -spaces can be realized as a vector space partition of \mathbb{F}_q^v .[‡] For the first case a construction is given by lifted maximum rank distance codes, cf. [5, Example 1].

[†]The choice for m can be obtained by minimizing $\tau(n, \Delta, u, m)$, i.e., solving $\frac{\partial \tau(n, \Delta, u, m)}{\partial m} = 0$ and rounding.

[‡]A suitable test case might be to decide whether a vector space partition of type $4^4 3^{135} 2^6$ exists in \mathbb{F}_2^{10} .

The above comprises [5, Theorems 1-4]. Just Theorem 1(i), for the case where d_1 does not divide d_2 , leaves some space for improving the lower bound on u_1 . To that end we analyze Lemma 6 in more detail.

Proposition 8. *Let \mathcal{N} be a q^r -divisible set of k -spaces in \mathbb{F}_q^v , $u = q^k$ and $\Delta = q^r$. Then, $n \notin \left[1, \frac{q^{k+r}-1}{q^r-1}\right)$ and $n \notin \left[\left\lceil \frac{1}{u-1} \cdot (\Delta um - \frac{\Delta u+1}{2} - \frac{1}{2}\sqrt{\omega}) \right\rceil, \left\lceil \frac{1}{u-1} \cdot (\Delta um - \frac{\Delta u+1}{2} + \frac{1}{2}\sqrt{\omega}) \right\rceil\right]$, where $\omega = (\Delta u - 2m)^2 + (2\Delta u + 1 - 4m^2)$, for all $m \in \mathbb{N}$ with $2 \leq m \leq \lfloor \frac{\Delta u}{4} + \frac{1}{2} + \frac{1}{4\Delta u} \rfloor$.*

PROOF. We set $\bar{\Delta} = \Delta u$ and $\bar{n} = n(u-1)$ so that $\tau(n, \Delta, u, m) = \bar{\Delta}^2 m(m-1) - \bar{n}\bar{\Delta}(2m-1) + \bar{n}(\bar{n}+1)$. We have $\tau(n, \Delta, u, m) \leq 0$ iff $\left| \bar{n} - \bar{\Delta}m + \frac{\bar{\Delta}+1}{2} \right| \leq \frac{1}{2}\sqrt{\bar{\Delta}^2 - 4m\bar{\Delta} + 2\bar{\Delta} + 1}$ and $m \leq \frac{\bar{\Delta}}{4} + \frac{1}{2} + \frac{1}{4\bar{\Delta}}$. Rewriting and applying Lemma 6 with $1 \leq m \leq \lfloor \frac{\Delta u}{4} + \frac{1}{2} + \frac{1}{4\Delta u} \rfloor$ gives the result since $m(m-1) > 0$ for $m \geq 2$. \square

Proposition 9. *Let \mathcal{N} be a q^r -divisible set of k -spaces in \mathbb{F}_q^v , where $r = ak + b$ with $a, b \in \mathbb{N}$, $0 < b < k$ and $a \geq 1$. Then, $n \geq \frac{q^{(a+2)k}-1}{q^k-1} = q^r \cdot q^{k-b} + \frac{q^r \cdot q^{k-b}-1}{q^k-1} = \Delta q^{k-b} + q^k\Theta + 1$, where $\Delta := q^r$ and $\Theta := \frac{q^{ak}-1}{q^k-1}$.*

PROOF. From Lemma 2 we conclude $n \geq 2q^r$ and set $u = q^k$. For $2 \leq m \leq q^{k-b}$ we have $2\Delta u + 1 - 4m^2 > 0$, so that Proposition 8 gives $n \notin \left[\left\lceil \frac{\Delta u(m-1)-1/2+m}{u-1} \right\rceil, \left\lceil \frac{\Delta um-1/2-m}{u-1} \right\rceil\right]$. Since $\Delta(m-1) \leq \left\lceil \frac{\Delta u(m-1)-1/2+m}{u-1} \right\rceil = \Delta(m-1) + \left\lceil \frac{\Delta(m-1)-1/2+m}{u-1} \right\rceil \leq \Delta m$ and $\left\lceil \frac{\Delta um-1/2-m}{u-1} \right\rceil = \Delta m + mq^b\Theta + \left\lceil \frac{mq^b-1/2-m}{q^k-1} \right\rceil = \Delta m + mq^b\Theta$, we conclude $n \notin [\Delta m, \Delta m + mq^b\Theta]$ for $2 \leq m \leq q^{k-b}$.

It remains to show $n \notin [\Delta m, \Delta m + mq^b\Theta + 1, \Delta(m+1) - 1] =: I_m$ for all $2 \leq m \leq q^{k-b} - 1$. If $n \in I_m$, then we can write $n = \Delta m + mq^b\Theta + x$ with $x \geq 1$ and $mq^b\Theta + x < \Delta$, so that $q^k \cdot (mq^b\Theta + x) = \Delta m + mq^b\Theta + (xq^k - mq^b) < \Delta m + mq^b\Theta + x = n$, which contradicts Lemma 5. \square

In other words, in the case of Theorem 1(i), where $d_2 = ad_1 + b$ with $0 < b < d_1$ and $a, b \in \mathbb{N}$, we have $u_1 \geq q^{d_2-d_1} \cdot q^{d_1-b} + \frac{q^{(a+1)d_1}-1}{q^{d_1}-1} = \frac{q^{(a+2)d_1}-1}{q^{d_1}-1}$, which can be attained by an d_1 -spread in $\mathbb{F}_q^{(a+2)d_1}$. Without the knowledge of b , we can state $u_1 \geq q \cdot q^{d_2-d_1} + \left\lceil \frac{q^{d_2+1}-1}{q^{d_1}-1} \right\rceil$, which also improves Theorem 1(i) and is tight whenever $d_2 + 1$ is divisible by d_1 . Summarizing our findings we obtain:

Theorem 10. *For a non-empty q^r -divisible set \mathcal{N} of k -spaces in \mathbb{F}_q^v the following bounds on $n = \#\mathcal{N}$ are tight.*

- (i) *We have $n \geq q^k + 1$ and if $r \geq k$ then either k divides r and $n \geq \frac{q^{k+r}-1}{q^k-1}$ or $n \geq \frac{q^{(a+2)k}-1}{q^k-1}$, where $r = ak + b$ with $0 < b < k$ and $a, b \in \mathbb{N}$.*
- (ii) *Let q^r divide n . If $r < k$ then $n \geq q^{k+r} - q^k + q^r$ and $n \geq q^{k+r}$ otherwise.*

While the smallest cardinality of a non-empty q^r -divisible set of k -spaces over \mathbb{F}_q has been determined, the spectrum of possible cardinalities remains widely unknown. For $k = 1$ [6, Theorem 12] states that either $n > rq^{r+1}$ or there exists integers a, b with $n = a \binom{r+1}{1}_q + bq^{r+1}$ and bounds for the maximum excluded cardinality have been determined in [1]. However, Lemma 5 and Lemma 6, applied via Proposition 8, give restrictions going far beyond Theorem 10. For $q = 2$, $r = 3$, $k = 2$, and $n \leq 81$ we exemplarily state that only $n \in \{21, 32, 33, 42, 43, 44, 52, \dots, 55, 62, \dots, 66, 72, \dots, 78\}$ might be attainable. The mentioned constructions cover the cases $n \in \{21, 32, 42, 53, 63, 64, 74\} \subseteq \{21a + 32b : a, b \in \mathbb{N}\}$. Replacing the lines by their contained 3 points, we obtain 2^4 -divisible sets of 1-spaces in \mathbb{F}_q^v of cardinality $3n$, for which two further exclusion criteria have been presented in [6], excluding the cases $n \in \{33, 44\}$. [6, Lemma 23] is based on a cubic polynomial obtained from (1) and (2), similar to the quadratic polynomial from Lemma 6 obtained from (1). Here, the presence of k additional b_i -variables may make the analysis more difficult for $k > 1$. For a q^r -divisible set \mathcal{N} of 1-spaces we have that $\mathcal{N} \cap H$ is q^{r-1} -divisible for every hyperplane H , which allows a recursive application of the linear programming method. For $k > 1$ we need to consider k -spaces and $k-1$ -spaces in H , see [6, Section 6.3], which makes the bookkeeping more complicated.

REFERENCES

- [1] D. Heinlein, T. Honold, M. Kiermaier, S. Kurz, and A. Wassermann, *Projective divisible binary codes.*, The Tenth International Workshop on Coding and Cryptography 2017, 10 pages.
- [2] J. Bierbrauer and Y. Edel, *A family of 2-weight codes related to BCH-codes*, Journal of Combinatorial Designs **5** (1997), no. 5, 391.
- [3] A. Blokhuis, A.E. Brouwer, and H.A. Wilbrink, *Heden's bound on maximal partial spreads*, Discrete Mathematics **74** (1989), no. 3, 335–339.
- [4] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips research reports (1973), no. 10, 103.
- [5] O. Heden, *On the length of the tail of a vector space partition*, Discrete Mathematics **309** (2009), no. 21, 6169–6180.
- [6] T. Honold, M. Kiermaier, and S. Kurz, *Partial spreads and vector space partitions*, Network Coding and Subspace Designs (M. Greferath, M.O. Pavčević, N. Silberstein, and A. Vazquez-Castro, eds.), Springer, to appear.
- [7] S. Kurz, *Packing vector spaces into vector spaces*, The Australasian Journal of Combinatorics **68** (2017), no. 1, 122–130.