

Open access • Book Chapter • DOI:10.1007/978-3-319-70293-3_7

Partial spreads and vector space partitions — Source link []

Thomas Honold, Michael Kiermaier, Sascha Kurz

Institutions: Zhejiang University, University of Bayreuth

Published on: 30 Jan 2018 - arXiv: Combinatorics (Springer, Cham)

Topics: Vector space and Finite geometry

Related papers:

- · Packing vector spaces into vector spaces
- · Coding for Errors and Erasures in Random Network Coding
- A Rank-Metric Approach to Error Control in Random Network Coding
- The maximum size of a partial spread in a finite projective space
- · Improved upper bounds for partial spreads



PARTIAL SPREADS AND VECTOR SPACE PARTITIONS

THOMAS HONOLD, MICHAEL KIERMAIER, AND SASCHA KURZ

ABSTRACT. Constant dimension codes with the maximum possible minimum distance have been studied under the name of partial spreads in finite geometry for several decades. It is no surprise that the sharpest bounds on the maximal code sizes are typically known for this subclass. The seminal works of André, Segre, Beutelspacher, and Drake & Freeman date back to 1954, 1964, 1975, and 1979, respectively. Until recently, there was almost no progress besides some computer based constructions and classifications. It turns out that vector space partitions provide the appropriate theoretical framework, Here, we provide an historic account and an interpretation of the classical results from a modern point of view. To this end, we introduce all required methods from the theory of vector space partitions and finite geometry in a tutorial style. We guide the reader to the current frontiers of research in that field.

1. INTRODUCTION

Let \mathbb{F}_q be the finite field with q elements, where q > 1 is a prime power. By \mathbb{F}_q^v we denote the standard vector space of dimension $v \ge 1$ over \mathbb{F}_q . The set of all subspaces of \mathbb{F}_q^n , ordered by the incidence relation \subseteq , is called (v-1)-dimensional projective geometry over \mathbb{F}_q and denoted by $\mathrm{PG}(v-1,\mathbb{F}_q)$. It forms a finite modular geometric lattice with meet $X \wedge Y = X \cap Y$ and join $X \vee Y = X + Y$. The points of $\mathrm{PG}(v-1,\mathbb{F}_q)$ are the 1-dimensional subspaces of \mathbb{F}_q^v . Instead of $\mathrm{PG}(v-1,\mathbb{F}_q)$ we will mainly use the notation \mathbb{F}_q^v in the following, pointing to fact that the dimensions differ by one in both notations. The set of all k-dimensional subspaces of an \mathbb{F}_q vector space V will be denoted by $\begin{bmatrix} V\\ k \end{bmatrix}_q$. For $v = \dim(V)$, its cardinality is given by the Gaussian binomial coefficient

$$\begin{bmatrix} v \\ k \end{bmatrix}_q := \begin{cases} \frac{(q^v - 1)(q^{v-1} - 1)\cdots(q^{v-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1)\cdots(q - 1)} & \text{if } 0 \le k \le v; \\ 0 & \text{otherwise,} \end{cases}$$

which does not depend on the precise choice of the \mathbb{F}_q -vector space V. The latter fact is true for all of the remaining definitions of this chapter, so that we will stick to the specialized notation \mathbb{F}_q^v . Two widely used metrics are are given by the *subspace distance* $d_S(X,Y) := \dim(X+Y) - \dim(X\cap Y) = 2 \cdot \dim(X+Y) - \dim(X) - \dim(Y)$, which is indeed the graph theoretic distance in the geometric lattice, and the *injection distance* $d_I(X,Y) := \max \{\dim(X), \dim(Y)\} - \dim(X\cap Y), \text{ where } X$ and Y are subspaces of \mathbb{F}_q^v . A set \mathcal{C} of subspaces of \mathbb{F}_q^v is called a *subspace code*. The *minimum (subspace) distance* of \mathcal{C} is given by $d = \min\{d_S(X,Y) \mid X,Y \in \mathcal{C}, X \neq Y\}$. If all elements of a subspace code \mathcal{C} have the same dimension, say k, we speak of a *constant dimension code*. For a constant dimension code \mathcal{C} we have $d_S(X,Y) = 2d_I(X,Y)$ for all $X,Y \in \mathcal{C}$, so that we will restrict ourselves to the subspace distance *d* in \mathbb{F}_q^v , where all codewords have dimension *k*. For two codewords X and Y of dimension k a subspace distance of at least *d* corresponds to $\dim(X \cap Y) \leq \frac{2k-d}{2}$. Thus, the maximum possible minimum distance of a constant dimension code with codewords of dimension k is 2k. This extremal case was also studied under the name of *partial k-spreads* in finite geometry for several decades, i.e., partial k-spreads are collections of k-dimensional subspaces of \mathbb{F}_q^v with trivial, i.e., zero-dimensional intersection. If the all-zero vector $\mathbf{0}$ is removed from the codewords, then the resulting objects can by packed into $\mathbb{F}_{q}^{v} \setminus \mathbf{0}$. In terms of the projective geometry partial spreads are packings of the set of points. It is no surprise that the sharpest bounds on the maximal code sizes $A_a^S(v,d;k)$ of constant dimension codes are typically known for this special subclass of partial spreads. In the case of a perfect packing, i.e., a partition, we speak of a k-spread. Partitions of $\mathbb{F}_q^n \setminus \mathbf{0}$, or the set of points of $\mathrm{PG}(v-1,\mathbb{F}_q)$, with elements of possibly different dimensions have been introduced under the name vector space partitions. 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 $m_d = 0$. So, partial k-spreads are just a special case of vector space partitions, where the elements all have a dimension of either k or 1. The elements of dimension 1 arise as the set of uncovered elements of points, that is why they are called *holes* in this context. It turns out that vector space partitions provide an appropriate framework to study bounds on the sizes of partial spreads.

There is a huge amount of related work that we will not cover. Partial spreads have also been studied for designs and in polar spaces, see e.g. [2, 16]. For the special case v = 2k there is a connection to translation planes [38]. From a geometric point of view, several researchers are interested in (inclusion) maximal partial spreads, while we consider only those of maximal cardinality. The classification, see e.g. [41], of all partial spreads up to isomorphism is also not treated. There is a stream of literature that characterizes the existing types of vector space partitions in \mathbb{F}_2^v for small dimensions v. Here, we give only partial details for results that are independent of the dimension v of the ambient space and refer to [23] otherwise.

The remaining part of this chapter is structured as follows. In Section 2 we review some, mostly classical, bounds and constructions for partial spreads. Introducing the concept of q^r -divisible sets and codes is introduce in Section 3, we are able to obtain improved upper bounds for partial spreads in Theorem 9 and Theorem 10. Constructions for q^r -divisible sets are presented in Section 4. Some more nonexistence results for q^r -divisible sets are presented in Section 5 before we end with a collection of open research problem in Section 6.

2. Bounds and constructions for partial spreads

Counting the points in \mathbb{F}_q^v and \mathbb{F}_q^k gives the obvious upper bound $A_q(v, 2k; k) \leq {\binom{v}{1}}_q / {\binom{k}{1}}_q = (q^v - 1) / (q^k - 1)$. The case of equality corresponds to the situation of spreads. Essentially, based on the idea of the *André-Bruck-Bose construction* [1, 10, 38], i.e., the connection to translation planes, there is the following complete characterization by Segre from 1964.

Theorem 1. ([46], [13, p. 29]) \mathbb{F}_q^v contains a k-spread if and only if k divides v, where we assume $1 \leq k \leq v$ and $k, v \in \mathbb{N}$.

Since $\frac{q^v-1}{q^k-1}$ is an integer if and only if k divides v only the constructive part needs to be shown. In this case a k-spread can be constructed from the so-called subfield construction or field reduction, see e.g. [39] for an extensive review. To this end write v = kt for a suitable integer t. The $\begin{bmatrix} t \\ 1 \end{bmatrix}_{q^k} = \frac{q^v-1}{q^k-1}$ points, i.e., the 1dimensional q^k -subspaces, of $\mathbb{F}_{q^k}^t$ clearly form a partition. Each such point consists of $q^k - 1$ non-zero vectors. Considering \mathbb{F}_{q^k} as a k-dimensional q-vector space maps the points of $\mathbb{F}_{q^k}^t$ to k-dimensional subspaces of \mathbb{F}_q^v with trivial intersection. As an example we consider the parameters q = 3, v = 4, and k = 2. Using canonical representatives in $\mathbb{F}_9 \simeq \mathbb{F}_3[x]/(x^2+1)$ the $\begin{bmatrix} 2\\1 \end{bmatrix}_9 = 10$ points in \mathbb{F}_9^2 are generated by

which form a 2-dimensional subspace in \mathbb{F}_3^4 .

If k does not divide v, then we can improve the stated upper bound by rounding down to $A_q(v, 2k; k) \leq \left\lfloor \frac{q^v - 1}{q^k - 1} \right\rfloor$, since $A_q(v, 2k; k)$ obviously is an integer. How-ever, this bound can be improved further. Before we go into the details we present another construction – the so-called *Echelon-Ferrers construction* for general subspace codes, see [18]. To this end, we remark that each k-dimensional subspace of \mathbb{F}_q^v can be written as the row-space of a full rank matrix $A \in \mathbb{F}_q^{k \times v}$. Since the application of the Gaussian elimination algorithm onto a matrix A does not change its row-space, the resulting matrix in reduced row echelon form (rre) can be used as a canonical representative for each subspace. To be precise, we denote the bijection from the subspaces to the representing matrices by τ . In our example the two vectors $\begin{pmatrix} 1\\ x+1 \end{pmatrix} \cdot 1$, $\begin{pmatrix} 1\\ x+1 \end{pmatrix} \cdot x \in \mathbb{F}_9^2$ form a \mathbb{F}_3 -basis. Mapped to \mathbb{F}_3^4 and written in rows, we obtain the (generator) matrix $A = \begin{pmatrix} 1 & 0 & 1 & 1\\ 0 & 1 & 2 & 1 \end{pmatrix}$, which is already in rre. Given a full rank matrix $A \in \mathbb{F}_q^{k \times v}$, we denote by $p(A) \in \mathbb{F}_2^v$ the binary vector whose 1-entries coincide with the pivot columns of A. For each $\pi \in \mathbb{F}_2^v$ let $\mathrm{EF}_q(\pi)$ denote the set of all $k \times v$ matrices over \mathbb{F}_q that are in reduced row echelon form with pivot columns described by π , where k is the (Hamming) weight of π . In our example we have $\pi = p(A) = (1, 1, 0, 0)$ and, more generally, $\text{EF}_q(\pi) = \begin{pmatrix} 1 & 0 & \star & \star \\ 0 & 1 & \star & \star \end{pmatrix}$, where the \star s represent arbitrary elements of \mathbb{F}_q , i.e., $|\text{EF}_q(v)| = q^4$. In general we have $\left| \text{EF}_q \Big((\pi_1, \dots, \pi_n) \Big) \right| = q^{\sum_{i=1}^n (1-\pi_i) \cdot \sum_{j=1}^i \pi_j}$ and the structure of the corresponding ma-

trices can be read off from the corresponding (Echelon)-Ferrers $diagram^1$

where the pivot columns and zeros are omitted and the stars are replaced by black disks.

For matrices $A, B \in \mathbb{F}_q^{m \times v}$ the rank distance is defined via $d_R(A, B) := \operatorname{rk}(A-B)$. The subspace distance of two subspaces with the same pivots can be computed by the rank distance of the corresponding generator matrices, see e.g. [47, Corollary 3].

Lemma 1. Let $\pi \in \mathbb{F}_2^v$ and $X, Y \in EF_q(\pi)$, then $d_S(X, Y) = 2 \cdot d_R(\tau(X), \tau(Y))$.

Let $d_H(\pi, \pi') := |\{1 \le i \le n : \pi_i \ne \pi'_i\}|$ denote the Hamming distance for two binary vectors $\pi, \pi' \in \mathbb{F}_2^v$. The subspace distance of two subspaces with different

¹A Ferrers diagram represents partitions as patterns of dots, with the *i*th row having the same number of dots as the *i*th term s_i in the partition $v = s_1 + \cdots + s_l$, where $s_1 \geq \cdots \geq s_l$ and $s_i \in \mathbb{N}_{>0}$.

pivots can be upper bounded via the Hamming distance of the corresponding pivot vectors, see [18, Lemma 2].

Lemma 2. Let $\pi, \pi' \in \mathbb{F}_2^v$, $X \in EF_q(\pi)$, and $Y \in EF_q(\pi')$, then $d_S(X,Y) \ge d_H(\pi, \pi')$.

Having Lemma 1 and Lemma 2 at hand, the Echelon-Ferrers construction from [18] works as follows: Choose a binary code S of length v and minimum Hamming distance 2δ as a so-called *skeleton code*. For each $s \in S$ construct a code $C_s \subseteq \text{EF}_q(s)$ having a minimum rank distance of at least δ . Setting $\mathcal{C} = \bigcup_{s \in S} \mathcal{C}_s$ yields a subspace code whose minimum distance is at least 2δ . The weights of the pivot vectors in S correspond to the dimensions of the codewords in \mathcal{C} .

For a vector $\pi \in \mathbb{F}_2^v$ and an integer $1 \leq \delta \leq v$ let $q^{\dim(\pi,\delta)}$ be the largest cardinality of a linear rank-metric code over $\mathrm{EF}_q(\pi)$ with rank distance at least δ .

Theorem 2. ([18, Theorem 1]) For a given $i, 0 \le i \le \delta - 1$, if ν_i is the number of dots in the Echelon-Ferrers diagram corresponding to π , which are not contained in the first i rows and not contained in the rightmost $\delta - 1 - i$ columns, then $\min_i \{\nu_i\}$ is an upper bound of $\dim(\pi, \delta)$.

The conjecture that the upper bound of Theorem 2 can be obtained for all parameters is still open. A special subcase is given by rectangular Ferrers diagrams.

Theorem 3. ([19]) Let $m, v \ge d$ be positive integers and $\mathcal{C} \subseteq \mathbb{F}_q^{m \times v}$ be a rankmetric code with minimum rank distance d. Then, $|\mathcal{C}| \le q^{\max(v,m) \cdot (\min(v,m) - d + 1)}$. Codes attaining this upper bound are called maximum rank distance (MRD) codes. They exist for all (suitable) choices of parameters.

If m < d or v < d, then only $|\mathcal{C}| = 1$ is possible, which may be summarized to the single upper bound $|\mathcal{C}| \leq \left\lceil q^{\max(v,m) \cdot (\min(v,m) - d + 1)} \right\rceil$. Using an $m \times m$ identity matrix as a prefix one obtains the so-called *lifted MRD codes*.

Theorem 4. ([48]) For $k, d, v \in \mathbb{N}_{>0}$ with $k \leq v, d \leq 2\min(k, v-k), d$ even, the size of a lifted MRD code with subspace distance d is given by $M(q, k, v, d) := q^{\max(k,v-k)\cdot(\min(k,v-k)-d/2+1)}$. If $d > 2\min(k, v-k)$, then we have M(q, k, v, d) = 1.

So, taking binary vectors π^i , where the ones are located in positions (i-1)k+1 to ik, for all $1 \le i \le \lfloor v/k \rfloor$, clearly gives a binary constant weight code of length v, weight k, and minimum Hamming distance 2k.

$$\begin{array}{c}
1 \dots 10 \dots 00 \dots 00 \dots \\
0 \dots 01 \dots 10 \dots 00 \dots \\
0 \dots 00 \dots 01 \dots 10 \dots \\
\dots \\
\dots \\
\end{array}$$

Lemma 3. For positive integers k, v with v > 2k and $v \not\equiv 0 \pmod{k}$, there exists a partial k-spread in \mathbb{F}_q^n having cardinality

$$1 + \sum_{i=1}^{\lfloor v/k \rfloor - 1} q^{v-ik} = 1 + q^{k+(v \mod k)} \cdot \frac{q^{v-k-(v \mod k)} - 1}{q^k - 1} = \frac{q^v - q^{k+(v \mod k)} + q^k - 1}{q^k - 1}.$$

Given the $(v \mod k)$ -term, a specific parameterization is useful: Write v = kt+r, where $1 \le r \le k-1$, and $A_q(kt+r, 2k; k) = q^r \cdot \frac{q^{kt}-1}{q^k-1} - s$. Lemma 3 gives $s \le q^r - 1$ and there was the wrong conjecture that this bound is sharp. $s \ge q-1$ and $s > \frac{q^r-1}{2} - \frac{q^{2r-k}}{5}$ is known, see e.g. [16] and the details presented later on.

Note that $v \equiv r \pmod{k}$, so that the residue class r seems to play a major role. Besides the case of r = 0, see Theorem 1, the next case r = 1 is solved in full generality in 1975 by Beutelspacher: **Theorem 5.** ([4]; see also [27] for the special case q = 2) For integers $1 \le k \le v$ with $v \equiv 1 \pmod{k}$ we have $A_q(v, 2k; k) = q^1 \cdot \frac{q^{v-1}-1}{q^k-1} - q + 1 = \frac{q^v - q^{k+1} + q^k - 1}{q^k - 1}$.

 $\begin{array}{l} \textit{Proof. Let } \mathcal{C} \text{ be a partial } k\text{-spread in } \mathbb{F}_q^{kt+1} \text{ of cardinality } q \cdot \frac{q^{kt}-1}{q^k-1} - s, \text{ where } s \leq q-1. \end{array} \\ \text{Since each codeword is contained in } \begin{bmatrix} k(t-1)+1\\1 \end{bmatrix}_q \text{ hyperplanes and the number of hyperplanes is given by } \begin{bmatrix} kt+1\\1 \end{bmatrix}_q, \text{ the average number of codewords per hyperplane is } \frac{|\mathcal{C}| \cdot \begin{bmatrix} k(t-1)+1\\1 \end{bmatrix}_q}{\begin{bmatrix} k^{t+1}\\1 \end{bmatrix}_q} > q \cdot \frac{q^{k(t-1)}-1}{q^k-1}. \text{ Thus, there exists a hyperplane containing } at least } \alpha := q \cdot \frac{q^{k(t-1)}-1}{q^k-1} + 1 \text{ codewords. Since } \alpha \cdot \begin{bmatrix} k\\1 \end{bmatrix}_q + (|\mathcal{C}| - \alpha) \cdot \begin{bmatrix} k-1\\1 \end{bmatrix}_q \leq \begin{bmatrix} kt\\1 \end{bmatrix}_q, \text{ we have } |\mathcal{C}| \leq q \cdot \frac{q^{kt}-1}{q^k-1} - (q-1). \end{array}$

In his original proof Beutelspacher considered the set of holes N and the average number of holes per hyperplane, which is less than the total number of holes divided by q. The crucial insight was the relation $|N| \equiv |H \cap N| \pmod{q^{k-1}}$ for each hyperplane H, i.e., the number of holes per hyperplane satisfies a certain modulo constraint. We will see this concept in full generality in Section 3. In terms of integer linear programming, the upper bound is obtained by an integer rounding cut. The construction in [4, Theorem 4.2] recursively uses arbitrary k'-spreads, so that it is more general than the one of Lemma 3.

Corollary 1. $A_2(2m,4;2) = \frac{2^{2m}-1}{3}$ and $A_2(2m+1,4;2) = \frac{2^{2m+1}-5}{3}$ for all $m \in \mathbb{N}_{\geq 2}$.

For a long time the best upper bound on $A_q(v, 2k; k)$, i.e., the best known lower bound on s was the one obtained by Drake and Freeman in 1979:

Theorem 6. (Corollary 8 in [15]) If v = kt + r with 0 < r < k, then

$$A_q(v,2k;k) \le \sum_{i=0}^{t-1} q^{ik+r} - \lfloor \theta \rfloor - 1 = q^r \cdot \frac{q^{kt} - 1}{q^k - 1} - \lfloor \theta \rfloor - 1,$$

where $2\theta = \sqrt{1 + 4q^k(q^k - q^r)} - (2q^k - 2q^r + 1).$

The authors concluded from the existence of a partial spread the existence of a (group constructible) (s, r, μ) -net and applied [8, Theorem 1B] – a necessary existence criterion formulated for orthogonal arrays of strength 2 by Bose and Bush in 1952. The underlying proof technique can be further traced back to [45] and is strongly related to the classical second-order Bonferroni Inequality [7, 20], see e.g. [29, Section 2.5] for another application for bounds on subspace codes.

Given Theorem 1 and Theorem 5 the first open binary case is $A_2(8, 6; 3)$. The construction from Lemma 3 gives a partial spread of cardinality 33, while Theorem 6 implies an upper bound of 34. In 2010 the authors of [17] found a sporadic partial 3-spread of cardinality 34 by a computer search. This completely answers the situation for partial 3-spreads in \mathbb{F}_2^n as shown by the following easy lemma.

Lemma 4. If $A_q(kt'+r, 2k; k) \ge q^r \cdot \frac{q^{kt'}-1}{q^k-1} - s$ for some integer s, then $A_q(kt+r, 2k; k) \ge q^r \cdot \frac{q^{kt}-1}{q^k-1} - s$ for all $t \ge t'$.

Proof. Let \mathcal{C} be a partial k-spread of cardinality $q^r \cdot \frac{q^{kt'}-1}{q^k-1} - s$ in $\mathbb{F}_q^{kt'+r}$. Embed \mathcal{C} into GF_q^{kt+r} such that the non-zero entries of the pivot vectors of the corresponding codewords are contained in the last kt' + r coordinates. So, we can apply the construction of Lemma 3 using only the first k(t-t') coordinates and append the embed code \mathcal{C} , see Lemma 2.

So, each constructive improvement of a lower bound for a partial k-spread gives rise to an infinite series of lower bound improvements. Unfortunately, so far, the sporadic construction in [17] is the only known example being strictly superior to the general construction of Lemma 3.

Corollary 2. For each integer $m \ge 2$ we have $A_2(3m, 6; 3) = \frac{2^{3m}-1}{7}$, $A_2(3m + 1, 6; 3) = \frac{2^{3m+1}-9}{7}$, and $A_2(3m+2, 6; 3) = \frac{2^{3m+2}-18}{7}$.

Very recently, the case $n \equiv 2 \pmod{k}$ was completely settled for $q = 2, k \ge 4$:

Theorem 7. ([36, Theorem 5]) $A_2(kt+2, 2k; k) = \frac{2^{kt+2}-3\cdot 2^k-1}{2^k-1}$ for $t \ge 2$ and $k \ge 4$.

As $A_q(k+2, 2k; k) = 1$ for $k \ge 2$, the assumption $v \ge 2k+2$ is no restriction. The case k = 3 is covered in Corollary 2. For k = 1, 2 the remainder of v is strictly smaller than 2. In other words, the binary case $v \equiv 2 \pmod{k}$ is completely resolved. The used proof technique is very similar to the one presented in the proof of Theorem 5.

Corollary 3. We have $A_2(4m, 8; 4) = \frac{2^{4m}-1}{15}$, $A_2(4m+1, 8; 4) = \frac{2^{4m+1}-17}{15}$, $A_2(4m+2, 8; 4) = \frac{2^{4m+2}-49}{15}$, and $\frac{2^{4m+3}-113}{15} \le A_2(4m+3, 8; 4) \le \frac{2^{4m+3}-53}{15}$ for all $m \ge 2$.

So, the first unknown binary case is $129 \le A_2(11,8;4) \le 133$. For r = 2 and q = 3 the upper bound of Theorem 6 could be decreased by one, see [36, Lemma 4]:

Lemma 5. For integers $t \ge 2$ and $k \ge 4$, we have $A_3(kt+2, 2k; k) \le \frac{3^{kt+2}-3^2}{3^k-1} - \frac{3^2+1}{2}$.

Again, the applied proof technique is very similar to the proof of Theorem 5. The construction of Lemma 3 is asymptotically optimal, see [44, Theorem 5]:

Theorem 8. If 0 < r < k and $k > {r \choose 1}_q$, then $A_q(kt + r, 2k; k) = \frac{q^{kt+r} - q^{k+r} + q^k - 1}{q^k - 1}$.

Choosing q = 2 and r = 2 this covers Theorem 7. Using the theory of q^r -divisible codes, presented in the next section, we can give a short and self-contained proof. We would like to remark that the very same authors have refined their analysis, additionally using Theorem 13 from the theory of vector space partitions, to obtain improved upper bounds for some of the cases $k \leq {r \brack 1}_q$ in their preprint [43]. Since we will present and prove stronger bounds, we do not go into details here.

3. q^r -divisible sets and codes

The currently most effective approach for upper bounds for partial spreads follows the original idea of Beutelspacher of considering the set of holes as an standalone object. As it appears in the proof of Beutelspacher, the number of holes in a hyperplane satisfy a certain modulo constraint. In this section we will define sets of points such that the number of points is the same for each hyperplane modulo some number. Then, we will study the properties of those discrete objects and will observe later on that the set of holes of a partial spread is exactly of that type. Without the notion of q^r -divisible sets and the reference to the *linear pro*gramming method, almost all results of this section are contained in [35]. A more extensive introduction into the topic, including constructions and relations to other combinatorial objects, is currently in preparation [24].

Definition 1. $C \subseteq PG(v-1, \mathbb{F}_q)$ is called weakly Δ -divisible for an integer $\Delta > 1$ if there exists $u \in \mathbb{N}$ with $|C \cap H| \equiv u \pmod{\Delta}$ for each hyperplane H. If $C = \emptyset$ or v = 1 we call it trivial. If $u \equiv |C| \pmod{\Delta}$ we call C (strongly) Δ -divisible. Taking the elements of $\mathcal{C} \subseteq \operatorname{PG}(v-1, \mathbb{F}_q)$, i.e., one representing vector, as columns of a generator matrix, we obtain a *linear* [n, k]-code over \mathbb{F}_q , where $n = |\mathcal{C}|$ and $\dim(\langle \mathcal{C} \rangle) = k \leq v$. Since \mathcal{C} is a set, the corresponding linear code is projective, i.e., the minimum distance of its dual code is at least 3. The term Δ -divisible translates to the fact that all weights of the corresponding linear code are divisible by Δ , which is a very nice property. In order to stress the geometric point of view we will choose the language of (projective) sets of points instead of projective linear codes. We remark that Δ -divisible codes were introduced by Ward in 1981, see [49].

If Δ divides q^{v-1} , then each weakly Δ -divisible set is (strongly) Δ -divisible. We first state the so-called *standard equations*. (These are a special case of the Mac Williams identities (4), invoking the minimum distance of the the dual code.)

Lemma 6. Let $\emptyset \neq C \subseteq PG(v-1, \mathbb{F}_q)$ with |C| = n and a_i be the number of hyperplanes containing exactly *i* points for $0 \leq i \leq n$. Then, we have

$$\sum_{i=0}^{n} a_i = \begin{bmatrix} v \\ 1 \end{bmatrix}_q,\tag{1}$$

$$\sum_{i=1}^{n} ia_i = n \cdot \begin{bmatrix} v-1\\1 \end{bmatrix}_q, and \tag{2}$$

$$\sum_{i=2}^{n} {i \choose 2} a_i = {n \choose 2} \cdot {v-2 \choose 1}_q.$$
(3)

Proof. Double-count 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 points contained in H. (If n = 1, then Equation (3) reads 0 = 0.)

Lemma 7. If $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ is weakly Δ -divisible, where Δ divides q^{v-1} , then $|\mathcal{C} \cap H| \equiv |\mathcal{C}| \pmod{\Delta}$ for each hyperplane H.

Proof. Choose $0 \le u \le q - 1$ such that $|\mathcal{C} \cap H| \equiv u \pmod{\Delta}$ for each hyperplane H. Equation (1) and Equation (2) from Lemma 6 can be rewritten to

$$(q-1)\cdot\left(\sum_{i\geq 0}a_{u+i\Delta}\right) = q^v - 1 \text{ and } (q-1)\cdot\left(\sum_{i\geq 0}(u+i\Delta)\cdot a_{u+i\Delta}\right) = n\cdot\left(q^{v-1} - 1\right).$$

The second equation minus u times the first equation, then divided by Δ gives $(q-1) \cdot (\sum_{i\geq 0} ia_{u+i\Delta}) = (n-uq)\frac{q^{\nu-1}}{\Delta} - \frac{n-u}{\Delta}$, so that $(n-u)/\Delta$ is an integer. \Box

Lemma 8. If $C \subseteq PG(v-1, \mathbb{F}_q)$ is q^r -divisible, where r < v, then each (v-j)-dimensional subspace is q^{r-j} -divisible for all $0 \le j \le r$.

Proof. It suffices to consider j = 1, where $m \ge 1$. Choose u such that $|\mathcal{C}| \equiv |\mathcal{C} \cap H| \equiv u \pmod{q^r}$ for each hyperplane H. Let S be a subspace of co-dimension 2 with $|\mathcal{C} \cap S| \equiv \overline{u} \pmod{q^{r-1}}$. Counting the total number of elements of \mathcal{C} via the q + 1 hyperplanes containing S gives $(q + 1)u - q\overline{u} \equiv u \pmod{q^r}$, i.e., $u \equiv \overline{u} \pmod{q^{r-1}}$.

The term hyperplane translates to the *residual code* of the corresponding linear code. We have weakened modulo conditions on the number of elements of subspaces or weakened divisibility conditions for the weights of the iterative residual codes.

Lemma 9. Let \mathcal{P} be a vector space partition of type $t^{m_t} \dots s^{m_s} 1^{m_1}$ of \mathbb{F}_q^v , where $n > t \ge s \ge 3$ Then, the 1-dimensional elements of \mathcal{P} form a q^{s-1} -divisible set.

Proof. Let $l, x \in \mathbb{N}_0$ with $\sum_{i=s}^t m_i = lq^s + x$ and H be a hyperplane with corresponding vector space partition \mathcal{P}' of type $t^{m'_t} \dots (s-1)^{m'_{s-1}} 1^{m'_1}$ of \mathbb{F}_q^{v-1} . Counting the number of non-zero vectors in \mathbb{F}_q^v and H yields $(lq^s + x) \cdot {s \brack 1}_q + aq^s + m_1 = {v \brack 1}_q$ and $(lq^s + x) \cdot {s-1 \brack 1}_q + a'q^{s-1} + m'_1 = {v-1 \brack 1}_q$ for some $a, a' \in \mathbb{N}_0$. q-1 times the first equation yields $-x + (q-1)m_1 \equiv -1 \pmod{q^{s-1}}$, so that $m_1 \equiv m'_1 \pmod{q^{s-1}}$. \Box

For s = 2 the two-dimensional elements of \mathcal{P} in Lemma 9 might correspond to 1-dimensional elements in \mathcal{P}' . If we distinguish those elements from the original 1-dimensional elements form \mathcal{P} lying in H, we see that the 1-dimensional elements of \mathcal{P} also form a q^1 -divisible set.

Lemma 10. Let \mathcal{P} be a vector space partition of type $t^{m_t} \dots 2^{m_2} 1^{m_1}$ of \mathbb{F}_q^v for some integers $v > t \geq 2$. Then, the 1-dimensional elements of \mathcal{P} form a q^1 -divisible set.

Proof. We denote the 1-dimensional elements of \mathcal{P} as *holes* and choose $l, x \in \mathbb{N}_0$ with $\sum_{i=2}^{t} m_i = lq^2 + x$. Let H by a hyperplane with corresponding vector space partition \mathcal{P}' of type $t^{m'_t} \dots 1^{m'_1}$ of \mathbb{F}_q^{n-1} . By \tilde{m}'_1 we denote the number of 2-dimensional elements of \mathcal{P} with 1-dimensional intersection with H and by \hat{m}'_1 we denote the number of holes contained in H, i.e., $m'_1 = \tilde{m}'_1 + \hat{m}'_1$. Counting the number of non-zero vectors in \mathbb{F}_q^n and H yields $(lq^2 + x) \cdot (q+1) + aq^2 + m_1 = {n \brack 1}_q$ and $(lq^2 + x - \tilde{m}'_1) \cdot (q+1) + a'q^2 + \tilde{m}'_1 + \hat{m}'_1 = {n-1 \brack 1}_q$ for some $a, a' \in \mathbb{N}_0$. q-1 times the first equation yields $(q-1)m_1 \equiv x-1 \pmod{q}$, so that $m_1 \equiv \hat{m}'_1 \pmod{q}$. □

Since a partial k-spread is a vector space partition of type $k^{m_k} 1^{m_1}$, the corresponding set of holes is a q^{k-1} -divisible set.

Lemma 11. No non-trivial Δ -divisible $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ with $n = |\mathcal{C}| = 1$ exists.

Proof. In Definition 1 we have to choose u = 1 due to $\Delta \ge 2$, so that all hyperplanes have to contain the unique point, which is not possible.

We remark that the standard equations from Lemma 6 have a natural generalization in the language of linear codes, see e.g. [31]. To this end let $\mathcal{C} \subset \mathrm{PG}(v-1, \mathbb{F}_q)$ and \mathcal{L} denote the corresponding linear projective code over \mathbb{F}_q . Let n denote the cardinality of \mathcal{C} , i.e., the length of \mathcal{L} , and k denote the dimension of $\langle \mathcal{C} \rangle$ and \mathcal{L} . By a_i we denote the number of hyperplanes having an intersection of cardinality i with \mathcal{C} , by A_i the number of codewords of \mathcal{L} of weight i and by A_i^{\perp} the number of codewords of weight i of the dual code \mathcal{L}^{\perp} , which has dimension n - k. The connection between the a_i and A_i is given by $A_i = (q-1)a_{n-i}$ for all $0 < i \leq n$, $A_0 = 1$, and $a_n = 0$. The weight distribution $(A_0^{\perp}, \ldots, A_n^{\perp})$ of the dual code \mathcal{L}^{\perp} can be computed from the weight distribution (A_0, \ldots, A_n) of the (primal) code \mathcal{L} . One way² to write down the underlying relation are the so-called Mac Williams identities:

$$\sum_{j=0}^{n-\nu} \binom{n-j}{\nu} A_j = q^{k-\nu} \cdot \sum_{j=0}^{\nu} \binom{n-j}{n-\nu} A_j^{\perp} \quad \text{for } 0 \le \nu \le n,$$
(4)

where, additionally, $A_0^{\perp} = 1$. The fact that the A_i^{\perp} are uniquely determined by the A_i can e.g. be seen by providing explicit equations for each A_i^{\perp} in dependence of the A_i . Those formulas involve the so-called *Krawtchouk polynomials* [34].

²Another way uses the *weight enumerator* $W_{\mathcal{L}}(x,y) = \sum_{i=0}^{n} A_i(\mathcal{L})y^i x^{n-i}$. With this, the weight enumerator of the dual code is given by $W_{\mathcal{L}^{\perp}}(x,y) = \frac{1}{|\mathcal{C}|} \cdot W_{\mathcal{C}}(x + (q-1)y, x - y)$.

We remark that we have $A_1^{\perp} = A_2^{\perp} = 0$, since the minimum distance of the dual code is at least 3, in our situation. With this, the first three equations of (4) are equivalent to the equations from Lemma 6.

Of course the A_i and the A_i^{\perp} in (4) have to be non-negative integers. Omitting the integrality condition yields the so-called *linear programming method*, see e.g. [31, Section 2.6], where the A_i and A_i^{\perp} are variables satisfying the mentioned constraints.³ Given some further constraints on the weights of the code and/or the dual code, one may check whether the corresponding polyhedron contains non-negative rational solutions. In general, this is a very powerful approach and was e.g. be used to compute bounds for codes with a given minimum distance, see [12, 40]. Here, we consider a subset of the Mac William identities and use analytical arguments.⁴

By considering the average number of points per hyperplane, we can guarantee the existence of a hyperplane containing a relatively small number of points.

Lemma 12. If $C \subseteq PG(v-1, \mathbb{F}_q)$ is q^r -divisible with $|\mathcal{C}| = a \cdot q^{r+1} + b$ for $a \in \mathbb{Z}$, $b \in \mathbb{N}_0$, then there exists a hyperplane H such that $|\mathcal{C} \cap H| \leq (a-1) \cdot q^r + b$.

Proof. Set $n = |\mathcal{C}|$ and choose a hyperplane H such that $n' := |\mathcal{C} \cap H|$ is minimal. Then, we have

$$n' \leq \underbrace{\frac{1}{\binom{v}{1}_{q}} \cdot \sum_{\text{hyperplane } H'} |\mathcal{C} \cap H'|}_{\text{average}} = n \cdot \binom{v-1}{1}_{q} / \binom{v}{1}_{q} < \frac{n}{q} \quad \text{and} \quad n' \equiv b \pmod{q^{r}}.$$

If $n' > (a-1)q^r + b$, then $n'q \ge aq^{r+1} + bq \ge aq^{r+1} + b = n$, which is a contradiction.

Corollary 4. If $C \subseteq PG(v-1, \mathbb{F}_q)$ is q^r -divisible with $|\mathcal{C}| = a \cdot q^{r+1} + b$ for integers a, b with $b \geq 0$, then there exists an (v-j)-dimensional subspace U such that $|\mathcal{C} \cap U| \leq (a-j) \cdot q^{r+1-j} + b$ and $|\mathcal{C} \cap U| \equiv b \pmod{q^{r+1-j}}$ for all $0 \leq j \leq r$.

Note that we have some freedom to choose the parameters a and b in Lemma 12. If \mathcal{C} is 2¹-divisible with cardinality 7, we may write $|\mathcal{C}| = 0 \cdot 2^2 + 7$ or $|\mathcal{C}| = 1 \cdot 2^2 + 3$ leading to the bounds $-1 \cdot 2^1 + 7 = 5$ and $0 \cdot 2^1 + 3 = 3$, respectively. For a concrete example it its easy to check algorithmically which variant gives the best bound. Here, we present a parametric approach. Given the parameters from Lemma 12 let y be a non-negative integer such that $y \equiv (q-1)b \pmod{q^{r+1}}$. With this, we have $\frac{b+y}{q} \equiv b \equiv n' \pmod{q^r}$ and via the argument of the proof of Lemma 12 we conclude $n' \leq (a-1) \cdot q^r + \frac{b+y}{q}$. Here, negative values for b are permitted as long as $y \geq 0$. Taking the smallest possibility for y clearly gives the sharpest bound.

In the context of partial spreads or, more generally, vector space partitions another parameterization using the number of non-hole elements of the vector space partition turns out to be very useful in analytical arguments. To this end we define the following abbreviation.

Definition 2. A vector space partition \mathcal{P} of \mathbb{F}_q^v has hole-type (t, s, m_1) , if it is of type $t^{m_t} \dots s^{m_s} 1^{m_1}$, for some integers $v > t \ge s \ge 2$, $m_i \in \mathbb{N}_0$ for $i \in \{1, s, \dots, t\}$, and \mathcal{P} is non-trivial.

³Typically, the A_i^{\perp} are removed from the formulation using the explicit formulas based on the Krawtchouk polynomials, which may of course also be done automatically in the preprocessing step of a customary linear programming solver.

⁴The use of special polynomial, like we will do, is well known in the context of the linear programming method, see e.g. [6, Section 18.1].

Lemma 13. Let \mathcal{P} be a vector space partition of \mathbb{F}_q^v of hole-type (t, s, m_1) , $l, x \in \mathbb{N}_0$ with $\sum_{i=s}^t m_i = lq^s + x$, and $b, c \in \mathbb{Z}$ with $m_1 = bq^s + c$. If $x \ge 1$, then there exists a hyperplane \widehat{H} with $\widehat{m}_1 = \widehat{b}q^{s-1} + \widehat{c}$ holes, where $\widehat{c} := \frac{c+x-1}{q} \in \mathbb{Z}$ and $b > \widehat{b} \in \mathbb{Z}$.

Proof. It remains to check that x - 1 plays the role of y in our above consideration.

Corollary 5. Using the notation from Lemma 13, let \mathcal{P} be a non-trivial vector space partition with $x \geq 1$. For each $0 \leq j \leq s-1$ there exists a (v-j)-dimensional subspace U containing \widehat{m}_1 holes with $\widehat{m}_1 \equiv \widehat{c} \pmod{q^{s-j}}$ and $\widehat{m}_1 \leq (b-j) \cdot q^{s-j} + \widehat{c}$, where $\widehat{c} = \frac{c + [\frac{j}{1}]_q \cdot (x-1)}{a^j}$.

Proof. It remains to note that the value of x does not change during the recursion.

So far, we can guarantee that some subspace contains not too many holes since the average number of holes per subspace would be too large otherwise. The modulo-constraints captured in the definition of a q^r -divisible set enable iterative rounding sharpening the bounds. Next, we specialize to the situation of partial spreads before we come up with some non-existence results for vector space partitions with few holes.

Lemma 14. Let \mathcal{P} be a non-trivial vector space partition of type $k^{m_k} 1^{m_1}$ of \mathbb{F}_q^v with $m_k = lq^k + x$, where $l = \frac{q^{v-k}-q^r}{q^{k}-1}$, $x \ge 1$, $k = \begin{bmatrix} r \\ 1 \end{bmatrix}_q + 1 - z + u > r$, and $u, z, r, x \in \mathbb{N}_0$. For $1 \le y \le k$ there exists a (v-k+y)-dimensional subspace U with $L \le (z+y-1)q^y + w$ holes, where $w = -(x-1)\begin{bmatrix} y \\ 1 \end{bmatrix}_q$ and $L \equiv w \pmod{q^y}$.

Proof. Apply Corollary 5 with s = k, j = k - y, and $m_1 = \begin{bmatrix} v \\ 1 \end{bmatrix}_q - m_k \cdot \begin{bmatrix} k \\ 1 \end{bmatrix}_q = \begin{bmatrix} r \\ 1 \end{bmatrix}_q q^k - \begin{bmatrix} k \\ 1 \end{bmatrix}_q (x-1).$

The parameter l is chosen in such a way that $m_k = lq^k + x$ matches the cardinality of the partial k-spread given by the construction in Lemma 3 for x = 1. Thus, the assumption $x \ge 1$ is no real restriction. Actually, the chosen parameterization using x in Lemma 13 and Corollary 5 makes it very transparent why the construction of Lemma 3 is asymptotically optimal – as stated in Theorem 8. If the dimension k of the elements of the partial spread is large enough, a sufficient number of rounding steps can be performed while the rounding process is stopped at x = 1 for the other direction. For small k we will not reach the lower bound of the construction of Lemma 3, so that there is some possible space for better constructions.

Lemma 15. Let $\Delta = q^{s-1}$, $m \in \mathbb{Z}$, and \mathcal{P} be a vector space partition of \mathbb{F}_q^v of hole-type (t, s, c). Then, $\tau_q(c, \Delta, m) \cdot \frac{q^{v-2}}{\Delta^2} - m(m-1) \geq 0$, where $\tau_q(c, \Delta, m) = m(m-1)\Delta^2 q^2 - c(2m-1)(q-1)\Delta q + c(q-1)(c(q-1)+1)$.

Proof. Consider the three equations from Lemma 6. $(c-m\Delta)(c-(m-1)\Delta)$ times the first minus $(2c-(2m-1)\Delta-1)$ times the second plus twice the third equation, and then divided by $\Delta^2/(q-1)$, gives $(q-1) \cdot \sum_{h=0}^{\lfloor c/\Delta \rfloor} (m-h)(m-h-1)a_{c-h\Delta} =$ $\tau_q(c, \Delta, m) \cdot \frac{q^{n-2}}{\Delta^2} - m(m-1)$ due to the q^{s-1} -divisibility. Finally, we observe $a_i \ge 0$ and $(m-h)(m-h-1) \ge 0$ for all $m, h \in \mathbb{Z}$.

[8, Theorem 1.B] is quite similar to Lemma 15 and its implications. The multipliers used in the proof of Lemma 15 can be directly read off from:

Lemma 16. For pairwise different numbers a, b, c the inverse matrix of

$$\begin{pmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 - a & b^2 - b & c^2 - c \end{pmatrix}$$

is given by

$$\begin{pmatrix} bc(c-b) & -(c+b-1)(c-b) & (c-b) \\ -ac(c-a) & (c+a-1)(c-a) & -(c-a) \\ ab(b-a) & -(b+a-1)(b-a) & (b-a) \end{pmatrix} \cdot ((c-a)(c-b)(b-a))^{-1}$$

Proof. Just utilize the adjoint matrix. (We remark that the determinant of the original matrix can easily be evaluated by a generalization of the Vandermonde determinant, see e.g. [33, Proposition 1].)

Although, Lemma 15 looks a bit like magic, it can be *constructed* in some explainable way. Consider the linear programming method with just the first three Mac Williams identities. For parameters excluded by Lemma 15 this small linear program is infeasible and the infeasibility can be seen at a certain basis solution, i.e., a choice of linear inequalities that are satisfied with equality. Solving for these equations, i.e., a change of basis, corresponds to a non-negative linear combination of the inequality system.⁵ In the parameteric case we have to choose the basis solution also depending on the parameters. Actually, we have implemented a degree of freedom in Lemma 15 using the parameter m. Here, the basis consists of two neighboring non-zero a_i -entries, parameterized by m, and an arbitrary a_i , which plays no role when the resulting equation is solved for all remaining a_i -terms. This way we end up with an equation of the form $\sum_{h=0}^{\lfloor c/\Delta \rfloor} (m-h)(m-h-1)a_{c-h\Delta} = \star$, where the a_i and their coefficients are non-negative. The use of the underlying quadratic polynomial is well known and frequently applied in the literature, see the remarks after Theorem 6.

Lemma 17. For integers $v > k \ge s \ge 2$ and $1 \le i \le s - 1$, there exists no vector space partition \mathcal{P} of \mathbb{F}_q^v of hole-type (k, s, c), where $c = i \cdot q^s - {s \brack 1}_q + s - 1.^6$

Proof. Assume the contrary and apply Lemma 15 with m = i(q-1). Setting i = s - 1 - y we compute $\tau_q(c, \Delta, m) = -q\Delta(y(q-1)+2) + (s-1)^2q^2 - q(s-1)(2s-5) + (s-2)(s-3)$. Using $y \ge 0$ we obtain $\tau_2(c, \Delta, m) \le s^2 + s - 2^{s+1} < 0$. For s = 2, we have $\tau_q(c, \Delta, m) = -q^2 + q < 0$ and for q, s > 2 we have $\tau_q(c, \Delta, m) \le -2q^s + (s-1)^2q^2 < 0$. Thus, Lemma 15 yields a contradiction.

Now we are ready to present the first improved (compared to Theorem 6) upper bound for partial spreads, which also covers Theorem 8 setting z = 0.

Theorem 9. For integers $r \ge 1$, $t \ge 2$, and $z, u \ge 0$ with $k = \begin{bmatrix} r \\ 1 \end{bmatrix}_q + 1 - z + u > r$ we have $A_q(v, 2k; k) \le lq^k + 1 + z(q-1)$, where $l = \frac{q^{v-k}-q^r}{q^k-1}$ and v = kt + r.

Proof. Apply Lemma 14 with x = 2 + z(q-1) and y = z + 1. If z = 0, then L < 0. For $z \ge 1$, apply Lemma 17. Thus, $A_q(n, 2k; k) \le lq^k + x - 1$.

⁵If we relax \geq 0-inequalities by adding some auxiliary variable on the left hand side and the minimization of this variable, we can remove the infeasibility, so that we apply the duality theorem of linear programming. Then, the mentioned multipliers for the inequalities are given as the solution values of the dual problem.

⁶For more general non-existence results of vector space partitions see e.g. [22, Theorem 1] and the related literature. Actually, we do not need the assumption of an underlying vector space partition of the mentioned type. The result is generally true for q^{s-1} -divisible codes, since the parameter x is just a nice technical short-cut to ease the notation.

The case z = 0 covers Theorem 8. We remark that the non-negativity of the number of holes in a certain, well-chosen, subspace is sufficient to prove that fact. The case z = 1 was announced in [44, Lemma 10] and proven in [43]. Since the known constructions for partial k-spreads give $A_q(kt+r, 2k; k) \ge lq^k + 1$, see e.g. [4] or Lemma 3, Theorem 9 is tight for $k \ge {r \brack 1}_q + 1$.

So far Lemma 15 was just applied in the case of Lemma 17 excluding the existence of some very special vector space partitions. Next, we look at a subspace and consider the number of holes, i.e., we apply Lemma 14 giving us the freedom to choose the dimension of the subspace. There Lemma 15, stating that a certain quadratic polynomial is non-negative, can be applied. By minimizing this function in terms of the free parameter m, we can obtain the following result.

Theorem 10. For integers $r \ge 1$, $t \ge 2$, $y \ge \max\{r, 2\}$, $z \ge 0$ with $u = q^y$, $y \le k$, $k = {r \choose 1}_q + 1 - z > r$, v = kt + r, and $l = \frac{q^{v-k} - q^r}{q^k - 1}$, we have $A_q(v, 2k; k) \le lq^k + \left[u - \frac{1}{2} - \frac{1}{2}\sqrt{1 + 4u(u - (z + y - 1)(q - 1) - 1)}\right]$.

Proof. From Lemma 14 we conclude $L \leq (z + y - 1)q^y - (x - 1) \begin{bmatrix} y \\ 1 \end{bmatrix}_q$ and $L \equiv -(x - 1) \begin{bmatrix} y \\ 1 \end{bmatrix}_q \pmod{q^y}$ for the number of holes of a certain (v - k + y)-dimensional subspace U. Using the notation of Lemma 14, $\mathcal{P} \cap U := \{P \cap U \mid P \in \mathcal{P}\}$ is of hole-type (k, y, L) if $y \geq 2$. Next, we will show that $\tau_q(c, \Delta, m) \leq 0$, where $\Delta = q^{y-1}$ and $c = iq^y - (x - 1) \begin{bmatrix} y \\ 1 \end{bmatrix}_q$ with $1 \leq i \leq z + y - 1$, for suitable integers x and m. Applying Lemma 15 then gives the desired contradiction, so that $A_q(n, 2k; k) \leq lq^k + x - 1$.

We choose⁷ m = i(q-1) - (x-1) + 1, so that $\tau_q(c, \Delta, m) = x^2 - (2u+1)x + u(i(q-1)+2)$. Solving $\tau_q(c, \Delta, m) = 0$ for x gives $x_0 = u + \frac{1}{2} \pm \frac{1}{2}\theta(i)$, where $\theta(i) = \sqrt{1 - 4iu(q-1) + 4u(u-1)}$. We have $\tau_q(c, \Delta, m) \leq 0$ for $|2x - 2u - 1| \leq \theta(i)$. We need to find an integer $x \geq 1$ such that this inequality is satisfied for all $1 \leq i \leq z + y - 1$. The strongest restriction is attained for i = z + y - 1. Since $z + y - 1 \leq {r \choose 1}_q$ and $u = q^y \geq q^r$, we have $\theta(i) \geq \theta(z + y - 1) \geq 1$, so that $\tau_q(c, \Delta, m) \leq 0$ for $x = \left[u + \frac{1}{2} - \frac{1}{2}\theta(z + y - 1)\right]$. With respect to Lemma 15 we remark that -m(m-1) < 0 for all $m \in \mathbb{Z} \setminus \{0, 1\}$. So, it remains to verify $\tau_q(c, \Delta, m) < 0$ for $m \in \{0, 1\}$. If i < z + y - 1 this is true due to $\theta(i) > \theta(z + y - 1)$, so that we assume i = z + y - 1. Due to Theorem 9 it suffices to consider $x \leq 1 + z(q-1)$. Thus, $m \geq (y-1)(q-1) + 1 \geq 2$.

Setting y = k, we obtain Theorem 6. Compared to [8, 15], the new ingredients essentially are q^r -divisible sets and Lemma 13, which allows to choose y < k. A weaker version of Theorem 10 was obtained independently and very recently in [43, Theorem 6,7]. Here, instead of Lemma 15 known results about vector space partitions, i.e., Theorem 13, are used.

4. Constructions for q^r -divisible sets

First we observe that we can embed every Δ -divisible set $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ into ambient spaces with dimension larger than v without destroying the Δ -divisibility. **Lemma 18.** Each (r+1)-divisible subspace $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ is q^r -divisible. *Proof.* We have $|\mathcal{C} \cap H| = {r \brack 1}_q \equiv {r+1 \brack 1}_q = |\mathcal{C}| \pmod{q^r}$ for each hyperplane H. \Box

For $\mathcal{C} \subseteq \mathrm{PG}(v-1, \mathbb{F}_q)$ we denote by $\chi^v_{\mathcal{C}}$ its characteristic function, i.e., $\chi^v_{\mathcal{C}} \colon \mathrm{PG}(v-1, \mathbb{F}_q) \to \{0, 1\}$ with $\chi^v_{\mathcal{C}}(P) = 1$ iff $P \in \mathcal{C}$.

12

⁷Solving $\frac{\partial \tau_q(c,\Delta,m)}{\partial m} = 0$, i.e., minimizing $\tau_q(c,\Delta,m)$, yields $m = i(q-1) - (x-1) + \frac{1}{2} + \frac{x-1}{q^y}$. For $y \ge r$ we can assume $x - 1 < q^y$ due to Lemma 3, so that up-rounding yields the optimum integer choice. For y < r the interval $\left[u + \frac{1}{2} - \frac{1}{2}\theta(i), u + \frac{1}{2} + \frac{1}{2}\theta(i)\right]$ may contain no integer.

Lemma 19. Let $C_i \subseteq \operatorname{PG}(v-1, \mathbb{F}_q)$ be Δ_i -divisible, $a_i \in \mathbb{Z}$ for $1 \leq i \leq m$ and $\mathcal{C} \subseteq \operatorname{PG}(v-1, \mathbb{F}_q)$. If $\chi^v_{\mathcal{C}} = \sum_{i=1}^m a_i \chi^v_{\mathcal{C}_i}$, then \mathcal{C}_i is $\operatorname{gcd}(a_1 \Delta_1, \ldots, a_m \Delta_m)$ -divisible. *Proof.* We have $|\mathcal{C}| = \sum_{i=1}^m a_i \cdot |\mathcal{C}_i|$ and $|\mathcal{C} \cap H| = \sum_{i=1}^m a_i \cdot |\mathcal{C}_i \cap H|$ for each hyperplane H. Since $|\mathcal{C}_i \cap H| \equiv |\mathcal{C}_i| \pmod{\Delta_i}$ the result follows.

Corollary 6. Each complement of an r + 1-dimensional in an r + 2-dimensional subspace of $PG(v - 1, \mathbb{F}_q)$ is q^r -divisible and has cardinality q^{r+1} .

Lemma 20. Let $C_1 \in PG(v_1 - 1, \mathbb{F}_q)$ and $C_2 \in PG(v_2 - 1, \mathbb{F}_q)$ be Δ -divisible, then there exists an Δ -divisible set $C \in PG(v_1 + v_2 - 1, \mathbb{F}_q)$ with $|C| = |C_1| + |C_2|$.

Proof. Embed C_1, C_2 in $PG(v_1 + v_2 - 1, \mathbb{F}_q)$ such that the sets are disjoint and take the union as C.

In analogy to the Frobenius Coin Problem, c.f. [5, 9, 21], we define F(q, r) as the smallest integer such that a q^r -divisible sets over \mathbb{F}_q of cardinality n exists for all integers $n \geq F(q, r)$. Using Lemma 18, Corollary 6, and Lemma 20 we conclude $F(q, r) \leq {r+1 \choose 1}_q \cdot q^{r+1} - {r+1 \choose 1}_q - q^{r+1}$ since $gcd\left({r+1 \choose 1}_q, q^{r+1}\right) = 1$.

Several of the known (families of) two-weight codes, see [11] and the online-table at http://moodle.tec.hkr.se/~chen/research/2-weight-codes for an overview, correspond to q^r -divisible sets. Codes with optimum minimum distance occasion-ally have the q^r -divisibility property, see *Best Known Linear Codes* in Magma.

5. More non-existence results for q^{r} -divisible sets

Lemma 15 can of course be applied in the general case of q^r -divisible sets.

Lemma 21. For
$$m \in \mathbb{N}_{>0}$$
, we have $\tau_q(u, \Delta, m) \leq 0$ iff $(q-1)u - (m-q/2)\Delta + \frac{1}{2} \in \begin{bmatrix} 1 & \sqrt{2+2} & \sqrt{2+2} & \sqrt{2} & \sqrt{2$

$$\left[-\frac{1}{2}\cdot\sqrt{q^2\Delta^2 - 4qm\Delta + 2q\Delta + 1}, \frac{1}{2}\cdot\sqrt{q^2\Delta^2 - 4qm\Delta + 2q\Delta + 1}\right].$$
 (5)

The last interval is non-empty, i.e., the radicand is non-negative, iff $1 \leq m \leq \lfloor (q\Delta+2)/4 \rfloor$. We have $\tau_q(u, \Delta, 1) = 0$ iff $u = (\Delta-1)/(q-1)$.

Proof. Solving $\tau_q(u, \Delta, m) = 0$ for u yields the boundaries for u stated in Inequality (5). Inside this interval we have $\tau_q(u, \Delta, m) \leq 0$. Now, $q^2 \Delta^2 - 4qm\Delta + 2q\Delta + 1 \geq 0$ is equivalent to $m \leq \frac{q\Delta}{4} + \frac{1}{2} + \frac{1}{4q\Delta}$. Rounding down the right hand side, while observing $\frac{1}{4q\Delta} < \frac{1}{4}$ yields $\lfloor (q\Delta + 2)/4 \rfloor$.

Definition 3. For $C \subseteq PG(v-1, \mathbb{F}_q)$ let $\mathcal{T}(C) := \{0 \le i \le c \mid a_i > 0\}$, where a_i denotes the number of hyperplanes with $|C \cap H| = i$.

Lemma 22. For integers $u \in \mathbb{Z}$, $m \ge 0$, and $\Delta \ge 1$ let $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ be Δ divisible of cardinality $n = u + m\Delta \ge 0$. Then, we have $(q-1) \cdot \sum_{h \in \mathbb{Z}, h \le m} ha_{u+h\Delta} = (u + m\Delta - uq) \cdot \frac{q^{v-1}}{\Delta} - m$, where we set $a_{u+h\Delta} = 0$ if $u + h\Delta < 0$.

Proof. Rewriting the equations from Lemma 6 yields $(q-1) \cdot \sum_{h \in \mathbb{Z}, h \leq m} a_{u+h\Delta} = q \cdot q^{v-1} - 1$ and $(q-1) \cdot \sum_{h \in \mathbb{Z}, h \leq m} (u+h\Delta)a_{u+h\Delta} = (u+m\Delta)(q^{v-1}-1)$. *u* times the first equation minus the second equation gives Δ times the stated equation. \Box

Corollary 7. For integers $u, m \ge 0$ and $\Delta \ge 1$ let $\mathcal{C} \subseteq PG(v-1, \mathbb{F}_q)$ satisfy $n = |\mathcal{C}| = u + m\Delta$ and $\mathcal{T}(\mathcal{C}) \subseteq \{u, u + \Delta, \dots, u + m\Delta\}$. Then, $u < \frac{m\Delta}{q-1}$ or u = m = 0.

While the quadratic inequality of Lemma 15 is based of the first three Mac Williams identities, the linear inequality of Lemma 22 is based on the first two Mac Williams identities. Lemma 21 excludes quite some values. We start by analyzing the right side of the corresponding interval.

Lemma 23. For $1 \le m \le \left\lfloor \sqrt{(q-1)q\Delta} - q + \frac{3}{2} \right\rfloor$, we have $(q-1)(n-m\Delta) - (m-q/2)\Delta + \frac{1}{2} \le \frac{1}{2} \cdot \sqrt{q^2\Delta^2 - 4qm\Delta + 2q\Delta + 1}$, where $n = m \cdot {r+1 \choose 1}_q - 1$ and $\Delta = q^r$.

Proof. Plugging in yields $q\Delta + 3 - 2m - 2q \leq \sqrt{q^2\Delta^2 - (4m - 2)q\Delta + 1}$, so that squaring and simplifying gives $m \leq \sqrt{(q - 1)q\Delta} - q + \frac{3}{2}$.

Theorem 11. Let $C \subseteq PG(v-1, \mathbb{F}_q)$ be q^1 -divisible with $2 \leq n = |\mathcal{C}| \leq q^2$, then either $n = q^2$ or q+1 divides n.

Proof. First we show $n \notin [(m-1)(q+1)+2, m(q+1)-1]$ for $1 \le m \le q-1$. To this end, we apply Lemma 21 to deduce $\tau_q(u, q, m) \le 0$ for $m+1-q \le u \le m-1$, so that the statement follows from Lemma 15. For $u \ge m+1-q$ we have

$$(q-1)u - (m-q/2)\Delta + \frac{1}{2} \ge -\frac{1}{2} \cdot \left(q^2 - 4q + 1 + 2m\right) \ge -\frac{1}{2} \cdot \left(q^2 - 2m - 3\right)$$
$$\ge -\frac{1}{2} \cdot \sqrt{q^4 - 4mq^2 + 2q^2 + 1} = -\frac{1}{2} \cdot \sqrt{q^2 \Delta^2 - 4qm\Delta + 2q\Delta + 1}$$

and for $u \leq m-1$ we have $(q-1)u - (m-q/2)\Delta + \frac{1}{2} \leq \frac{1}{2} \cdot (q^2 - 2m - 2q + 3) \leq \frac{1}{2} \cdot \sqrt{q^2 \Delta^2 - 4qm\Delta + 2q\Delta + 1}$. With respect to the estimation \star , we remark that $-4q^3 + 8q^2 - 12q + 8 + 4m(m+2q-3) \stackrel{m \leq q-1}{\leq} -4(q-1)(q^2 - 4q + 6) \stackrel{q \geq 2}{\leq} 0$. Applying Corollary 7 with u = m+1 and $\Delta = q$ yields $n \neq m(q+1) + 1$ for all $1 \leq m \leq q-2$.

Theorem 12. For the cardinality n of a q^r -divisible set C we have

$$n \notin \left[(a(q-1)+b) {r+1 \brack 1}_q + a + 1, (a(q-1)+b+1) {r+1 \brack 1}_q - 1 \right],$$

where $a, b \in \mathbb{N}_0$ with $b \leq q-2$ and $a \leq r-1$.

Proof. We prove by induction on r, set $\Delta = q^r$, and write $n = (m-1) {r+1 \choose 1}_q + x$, where $a+1 \leq x \leq {r+1 \choose 1}_q - 1$ and m-1 = a(q-1) + b for integers $0 \leq b \leq q-2$, $0 \leq a \leq r-1$. The induction start r = 1 is given by Theorem 11.

 $0 \leq a \leq r-1.$ The induction start r = 1 is given by Theorem 11. Now, assume $r \geq 2$ and conclude that for $0 \leq b' \leq q-2, 0 \leq a' \leq r-2$ we have $n' \notin \left[(a'(q-1)+b') \begin{bmatrix} r \\ 1 \end{bmatrix}_q + a' + 1, (a'(q-1)+b'+1) \begin{bmatrix} r \\ 1 \end{bmatrix}_q - 1 \right]$ for the cardinality n' of a q^{r-1} -divisible set. If $a \leq r-2$ and $x \leq \begin{bmatrix} r \\ 1 \end{bmatrix}_q - 1$, then b' = b, a' = a yields $\mathcal{T}(\mathcal{C}) \subseteq \{u, u + \Delta, \dots, u + (m-2)\Delta\}$ for $u = \Delta + (m-1) \begin{bmatrix} r \\ 1 \end{bmatrix}_q + x$. We compute $(q-1)u = q^{r+1}-q^r+(m-1)q^r-(m-1)+(q-1)x \stackrel{x\geq a+1}{\geq} (m-2)q^r+q^{r+1} > (m-2)\Delta$, so that we can apply Corollary 7. If a = r-1 and $a+1 \leq x \leq \begin{bmatrix} r \\ 1 \end{bmatrix}_q - 1$, then b' = b, a' = a = 1, so that we can apply Corollary 7. Thus, we can assume $\begin{bmatrix} r \\ 1 \end{bmatrix}_q \leq x \leq \begin{bmatrix} r+1 \\ 1 \end{bmatrix}_q - 1$ in the remaining part. Additionally we have $m \leq r(q-1)$.

We aim to apply Lemma 21. Due to Lemma 23 for the upper bound of the interval it suffices to show $r(q-1) \leq \left\lfloor \sqrt{(q-1)q\Delta} - q + \frac{3}{2} \right\rfloor$. For q = 2 the inequality is equivalent to $r \leq \left\lfloor \sqrt{2^{r+1}} - \frac{1}{2} \right\rfloor$, which is valid for $r \geq 2$. Since the right hand side is larger then $(q-1)(\sqrt{\Delta}-1)$, it suffices to show $q^{r/2} - 1 \geq r$, which is valid for $q \geq 3$ and $r \geq 2$. For the left hand side of the interval if suffices to show

$$(q-1)(n-m\Delta) - (m-q/2)\Delta + \frac{1}{2} \ge -\frac{1}{2} \cdot \sqrt{(\Delta q)^2 - (4m-2)\Delta q + 1},$$

which can be simplified to $\Delta q + 2m - 3 - 2(q-1)x \leq \sqrt{(\Delta q)^2 - (4m-2)\Delta q + 1}$ using $n = (m-1) {r+1 \brack 1}_q + x$. Since $(q-1)x \ge q^r - 1$ and $m \le r(q-1)$ it suffices to show

$$-\Delta^2 + 2rq\Delta - 2r\Delta - \Delta - r + r^2q - r^2 \le 0.$$
(6)

For q = 2 this inequality is equivalent to $-2^{2r} + r2^{r+1} + r^2 - 2 - 2^r \leq 0$, which is valid for $r \ge 2$. For r = 2 Inequality (6) is equivalent to $-q^4 + 4q^3 - 4q^2 - q^2 + 4q - 6$, which is valid for $q \in \{2,3\}$ and $q \ge 4$. For $q \ge 3$ and $r \ge 3$ we have $\Delta \ge 3rq$, so that Inequality (6) is satisfied.

In other words Theorem 12 says that the cardinality n of a q^r -divisible set can be written as $a \begin{bmatrix} r+1\\1 \end{bmatrix}_q + bq^{r+1}$ for some $a, b \in \mathbb{N}_0$ if $n \leq rq^{r+1}$. For small parameters it is possible to give exact answers, which q^r -divisible sets exist [24].

Lemma 24. Let $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ be non-trivial and 2^1 -divisible of cardinality n, then $n \geq 3$ and all cases can be realized, i.e., F(2,1) = 3.

Lemma 25. Let $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ be non-trivial and 2^2 -divisible of cardinality n, then $n \in \{7, 8\}$ or $n \ge 14$ and all mentioned cases can be realized, i.e., F(2, 2) = 14.

Lemma 26. Let $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ be non-trivial and 2^3 -divisible of cardinality n, then $n \in \{15, 16, 30, 31, 32, 45, 46, 47, 48, 49, 50, 51\}$ or $n \geq 59$ and all cases, except possibly n = 59, can be realized, i.e., $F(2,3) \in \{59, 60\}$.

For the underlying constructions we refer the reader to [24]. The non-existence results follow from lemmas 12, 15, and 22 except for the case q = 2, r = 3, n = 52.

Lemma 27. No 8-divisible $\mathcal{C} \subseteq \mathbb{F}_2^v$ of cardinality 52 exists.

Proof. From Lemma 25 we conclude that there is no hyperplane with 4 or 12 holes, i.e., $A_{40} = A_{48} = 0$. Using the abbreviation $y = 2^{\nu-3}$ the first four Mac Williams identities, see (4) are given by

$$A_{0} + A_{8} + A_{16} + A_{24} + A_{32} = 8y \cdot (A_{0}^{\perp})$$

$$52A_{0} + 44A_{8} + 36A_{16} + 28A_{24} + 20A_{32} = 4y \cdot (52A_{0}^{\perp})$$

$$\binom{52}{2}A_{0} + \binom{44}{2}A_{8} + \binom{36}{2}A_{16} + \binom{28}{2}A_{24} + \binom{20}{2}A_{32} = 2y\left(\binom{52}{2}A_{0}^{\perp}\right)$$

$$\binom{52}{3}A_{0} + \binom{44}{3}A_{8} + \binom{36}{3}A_{16} + \binom{28}{3}A_{24} + \binom{20}{3}A_{32} = y\left(\binom{52}{3}A_{0}^{\perp} + A_{3}^{\perp}\right)$$
Due to the standard distribution of the triangle of triangle of the triangle of tria

Plugging in $A_0 = A_0^{\perp} = 1$ and substituting $x = yA_3^{\perp}$ yields $A_8 = -4 + \frac{1}{512}x + \frac{7}{64}y, A_{16} = 6 - \frac{3}{512}x - \frac{17}{64}y, A_{24} = -4 + \frac{3}{512}x + \frac{397}{64}y,$ and $A_{32} = 1 - \frac{1}{512}x + \frac{125}{64}y$. Since $A_{16}, x \ge 0$, we have $y \le \frac{384}{17} < 32$, so that $v \le 7$. Since $3A_8 + A_{16} \ge 0$, we have $-6 + \frac{y}{16} \ge 0$, i.e., $y \ge 96$, so that $v \ge 10$ - a contradiction.

We remark, that we can obtain the result of Lemma 27 from the linear programming method, if we apply it for every possibility for the dimension v of the ambient space separately. Via the substitution $x = yA_3^{\perp}$, i.e., we solve a less restricted problem, we can jointly treat all cases and still have to deal with a linear program.

The non-existence of a 2^3 -divisible set of cardinality n = 52 implies the, compared to Theorem 6 tightened, upper bounds $A_2(11,8;4) \leq 132, A_2(15,8;4) \leq 132$ 2180, and $A_2(19,8;4) \leq 34948$. Here, and in general the exclusion of a specific q^r -divisible set give rise to an infinite sequence of improved upper bounds for partial spreads if it gives an improvement for at least one value of v. We remark, that Lemma 27 can be obtained from a general result, i.e., Corollary 8 with t = 3. Combining the first four Mac Williams identities we obtain an expression involving a certain cubic polynomial [24]:

Lemma 28. For $t \in \mathbb{Z}$ be an integer and $\mathcal{C} \subseteq \mathrm{PG}(v-1,\mathbb{F}_q)$ be Δ -divisible of cardinality n > 0. Then, we have $\sum_{i\geq 1} \Delta^2(i-t)(i-t-1)\cdot(g_1\cdot i+g_0)\cdot A_{i\Delta} + qhx = n(q-1)(n-t\Delta)(n-(t+1)\overline{\Delta})g_2$, where $g_1 = \Delta qh$, $g_0 = -n(q-1)g_2$, $g_2 = h - (2\Delta qt + \Delta q - 2nq + 2n + q - 2)$ and $h = \Delta^2 q^2 t^2 + \Delta^2 q^2 t - 2\Delta nq^2 t - \Delta nq^2 + 2\Delta nqt + n^2 q^2 + \Delta nq - 2n^2 q + n^2 + nq - n$.

Corollary 8. Using the notation of Lemma 28, if $n/\Delta \notin [t, t+1]$, $h \ge 0$, and $g_2 < 0$, then there exists no Δ -divisible set $C \subseteq PG(v-1, \mathbb{F}_q)$ of cardinality n.

For the best known bounds for $A_q(v, 2k; k)$, implied by the linear programming method, we refer to the online-table at http://subspacecodes.uni-bayreuth.de [25].

6. Open research problems

In this closing section we have collected some open research problems within the scope of this article. All of them presumably are accessible using the theoretical framework of q^r -divisible sets. Even more challenging, however, is the question whether similar methods can be developed for arbitrary constant-dimension codes instead of partial spreads (or vector space partitions). To be more concrete: The value $A_2(6,4;3) = 77$ is still only verified using extensive computer calculations [28]. The theoretical upper bound of 81 might be improved if one can show that not every line of \mathbb{F}_2^6 can be covered exactly nine times by the planes, c.f. [42].

6.1. Better constructions for partial spreads. So far, the only known case were the construction of Lemma 3 is batted, is based on the sporadic example of a partial 3-spread of cardinality 34 in \mathbb{F}_2^8 from [17] that can be used for $A_2(8+3k,6;3) \geq \frac{2^{8+3k-3}-2^2}{2^3-1} \cdot 2^3 + 2$, where $k \in \mathbb{N}$. A first step towards the understanding of these parameters is the classification of all 2^2 -divisible sets of cardinality 17:

$\begin{array}{c} 10000110010101110\\ 01000010111011100\\ 00100100000011000\\ 0001011100111000\\ 000010011001$	$\begin{array}{c} 10000011110100110\\ 01000001111111000\\ 0010010000110000\\ 00010010000101000\\ 0000100100100010$	10000000111011110 0100000010110000 001000000
	0000010101011111	00000001111011101

having dimensions 6, 7, and 8 respectively. While the classification, so far, is based on computer calculations⁸ one can easily see that there are exactly three solutions of the Mac Williams identities.

Lemma 29. Let C be 2^2 -divisible of cardinality 17, then $k = \dim(\langle C \rangle) \in \{6, 7, 8\}$ and the solutions of the Mac Williams identities are unique for each k: $(k, a_5, a_9, a_{13}, A_3^{\perp}) = (6, 12, 49, 2, 6), (7, 25, 95, 7, 2), (8, 51, 187, 17, 0).$

Proof. The unique solution of the standard equations is given by $a_5 = \frac{13}{16} \cdot 2^{k-2} - 1$, $a_9 = \frac{23}{8} \cdot 2^{k-2} + 3$, and $a_{13} = \frac{5}{16} \cdot 2^{k-2} - 3$ so that $k \ge 6$ since otherwise $a_{13} < 0$. Plugging in into the fourth Mac Williams identity yields $64 - 2^{k-2} = 2^{k-3} \cdot A_3^{\perp}$, so that $k \le 8$ since otherwise $A_3^{\perp} < 0$.

The partial 3-spread of cardinality 34 corresponds to the 7-dimensional hole configuration. A geometric description, using coordinates, of the hole configuration is given in [37, p. 84]. We have computationally checked that indeed all three hole configurations can be attained by a 3-spread of cardinality 34 in \mathbb{F}_2^8 . All three

⁸See http://www.rlmiller.org/de_codes and [14] for the classification of, possibly non-projective, doubly-even codes over \mathbb{F}_2^n .

configurations have non-trivial automorphism groups so that there may be some chance to also find partial 3-spreads with symmetries to eventually discover an underlying more general construction. So far we can only describe the geometric structure of the three possible hole configurations and embed them into infinite series:

Construction 1. For an integer $r \geq 1$ let E_1, E_2 be two disjoint r+2-dimensional subspaces and $L_1 \leq E_1, L_2 \leq E_2$ be subspaces of dimension r+1. Then, for $S := \langle L_1, L_2 \rangle$ we have $\dim(S) = 2r+2$. With this, set $\mathcal{C} = E_1 \setminus L_1 \cup E_2 \setminus L_2 \cup S \setminus (L_1 \cup L_2)$, i.e., $n = |\mathcal{C}| = {2r+2 \choose 1}_q - 2 \cdot {r+1 \choose 1}_q + 2 \cdot q^{r+1}$ and $k = \dim(\langle \mathcal{C} \rangle) = 2r+4$. For general field sizes q, the set \mathcal{C} is q^r -divisible and if 2|q, then \mathcal{C} is $2 \cdot q^r$ -divisible, i.e., 2^{r+1} -divisible if q = 2, where $n = 2^{2r+2} + 1$.

Proof. We have $\chi_{\mathcal{C}}^v = \chi_{E_1}^v + \chi_{E_2}^v + \chi_S^v - 2\chi_{L_1}^v - 2\chi_{L_2}^v$ and apply Lemma 18 and 19.

Construction 2. Let P be a point, $L \ge P$ be a line, $E \ge L$ be a plane, and E_i be planes for $1 \le i \le q$ such that $\dim(E_i \cap L) = 1$, $\dim(E \cap E_i) = 1$, and the E_i are pairwise disjoint. With $S_i = \langle E_i, L \rangle$ let $\mathcal{C} = P \cup (E \setminus L) \cup_{i=1}^q (S_i \setminus (E_i \cup L))$, so that $|\mathcal{C}| = 1 + q^2 + q \cdot (q^3 - q) = q^4 + 1$, $\dim(\langle \mathcal{C} \rangle) = 3 + 2q$, and \mathcal{C} is q^2 -divisible.

Proof. We have $\chi^v_{\mathcal{C}} = \chi^v_E + \sum_{i=1}^q \chi^v_{S_i \setminus E_i} - q \cdot \chi^v_L$ and apply Lemma 18 and 19. \Box

Construction 3. Let C'_1 be q-divisible with cardinality m, set $F' = \langle C'_1 \rangle$, and let P be a point outside of F'. With this, set $C_1 = \{\langle Q, P \rangle \setminus P : Q \in C'_1\}$, i.e., $|C_1| = mq$ and $\dim(\langle C_1 \rangle) = \dim(\langle C'_1 \rangle) + 1$. Let S be a solid trough P such that $S \cap \langle C_1 \rangle = P$ and let E be a plane in S that is disjoint to P. With this, set $C_2 = S \setminus \{E \cup P\}$, i.e., $|C_2| = q^3 - 1$ and $\dim(C_2) = 4$. For $C = C_1 \cup C_2$ we have $|C| = mq + q^3 - 1$ and $\dim(\langle C_1 \rangle) = \dim(\langle C'_1 \rangle) + 4$.

Lemma 30. If $m \equiv q^2 - q - 1 \equiv -q - 1 \pmod{q^2}$, then Construction 3 gives a q^2 -divisible set.

Proof. Let H be an arbitrary hyperplane. If $P \leq H$, then $|H \cap C_1| \equiv q^2 - q \pmod{q^2}$ since $m \equiv q - 1 \pmod{q}$, C'_1 is q-divisible, and each line in C_1 is intersected by Hin dimension 1 or 2. If $P \notin H$, then $|H \cap C_1| = m \equiv q^2 - q - 1 \pmod{q^2}$. If $P \leq H$, then $|H \cap C_2| \in \{q^3 - 1, q^2 - 1\}$, i.e., $|H \cap C_2| \equiv -1 \pmod{q^2}$. If $P \notin H$, then $|H \cap C_2| = q^2$, i.e., $|H \cap C_2| \equiv 0 \pmod{q^2}$.

Corollary 9. For each prime power q, there exists a q^2 -divisible set of cardinality $3q^3 - q^2 - q - 1$ and dimension $\max\{8, q+5\} \le k \le \max\{8, 2q+3\}.$

Proof. For q = 2 choose C'_1 as a projective basis of cardinality 5. For q = 3 choose C'_1 as the union of an ovoid and q - 2 lines.

So, all possible hole types of a partial 3-spread of cardinality 34 in \mathbb{F}_2^7 , i.e., 2^2 divisible sets of cardinality 17, belong to infinite families of q^r -divisible sets. Can further 2^2 -divisible sets of small cardinality be extended to an infinite family?

For the corresponding parameters over the ternary field we currently only know th bounds $244 \leq A_3(8,6;3) \leq 248$. Here, $A_3(8,6;3) = 248$ is only possible if the underlying hole configuration is a 3²-divisible set of cardinality 56, which is unique up to isomorphism and has dimension k = 6. It corresponds to an optimal twoweight code with weight distribution $0^{1}36^{616}45^{112}$. The set was first described by

q	r	n
2	3	59
2	4	129, 130, 131, 163, 164, 165, 185, 215, 216, 232, 233, 244, 245, 246, 247, 274, 275,
		277, 278, 306, 309
3	2	70, 77, 99, 100, 101, 102, 113, 114, 115, 128
4	2	$129, 150, 151, 172, 173, 193, 194, 195, 215, \ldots, 217, 236, \ldots, 239, 251, 258, 259,$
		$261, 272, 279, 280, 282, 283, 293, 301, 305, 313, 314, 322, 326, 333, 334, 335, \ldots$
5	1	40
7	1	75, 83, 91, 92, 95, 101, 102, 103, 109, 110, 111, 117, 118, 119, 125, 126, 127, 133,
		134, 135, 142, 143, 151, 159, 167

TABLE 1. Undecided cases for the existence of q^r -divisible sets.

Raymond Hill [26]. A generator matrix of the entire hole configuration is given by 10000022110100110202111100101201021211111220012002012211

0100001110121010112112001021122211121000021202220022201 0010002222022102001120010112002020200211122121222001112 0001001011222202210200221001010002222100222112122221200 00001020121022112112001021102211121000021202220212201001 00000112202002201012122002011020121222221200210020211222

Its free automorphism group has order 80640 while the corresponding image G' in the PGL has order 40320. Embedding the 6-dimensional hole configuration C in the first six coordinates of \mathbb{F}_3^8 the stabilizer of the hole configuration increases further. Here we have order 1028529653760 in PGL and order 2057059307520 in GL. Given the large automorphism group of the so-called Hill cap, is it possible to construct a partial 3-spread in \mathbb{F}_3^8 with cardinality larger than 244?

For q = 2, the next open case is $129 \le A_2(11, 8; 4) \le 132$. Here, $A_2(11, 8; 4) = 132$ corresponds to a 2³-divisible set of cardinality 67. Indeed, there are such sets for all dimensions $9 \le k \le 11$. Can one such 2³-divisible set be completed to a partial 4-spread?

Already the mentioned smallest open cases cause serious computational challenges. A promising approach is the prescription of automorphisms in order to reduce the computational complexity, see e.g. [32] for the application of this, socalled Kramer–Mesner, method to constant dimension codes. Of course, the automorphisms have to respect the hole configuration, whose automorphism group is known or can be easily computed in many cases.

6.2. Existence and classification results for q^r -divisible sets. Already for small parameters we currently can not decide the existence question for q^r -divisible sets, see Table 1.

In some cases the isomorphism types of q^r -divisible sets can be determined:

Lemma 31. Let $C \subseteq PG(v - 1, \mathbb{F}_q)$ be q^r -divisible of cardinality $\begin{bmatrix} r+1\\1 \end{bmatrix}_q$, where $r \geq 1$. Then, C is given by an (r + 1)-dimensional subspace.

An implication of this observation is that every partial k-spread of cardinality ${kt \brack 1}_q / {k \brack 1}_q - 1$ in \mathbb{F}_q^{kt} can be extended to a k-spread, provided $q \neq 2$ or $k \neq 2$.

Lemma 32. Let $C \subseteq PG(v-1, \mathbb{F}_q)$ be q^r -divisible of cardinality $2 \cdot {\binom{r+1}{1}}_q$, where $r \geq 1$ and $(q, r) \neq (2, 1)$. Then, dim(C) = 2r + 2 and the Mac Williams equations have a unique solution. For r = 1 and $q \neq 2$, the unique isomorphism type is the union of two (r+1)-flats.

Can more extendability results be obtained from the theory of q^r -divisible sets?

Lemma 33. Let $C \subseteq PG(v-1, \mathbb{F}_q)$ be q^r -divisible of cardinality q^{r+1} , where $r \geq 1$. Then, there exists a hyperplane H having empty intersection with C. A realization is given as the complement of an (r+1)-dimensional subspace in an (r+2)-dimensional subspace. For q = 2 this is unique up to isomorphism.

What about q > 2? Are there more isomorphism types? The partial plane spreads of cardinality 16 in \mathbb{F}_2^7 have been classified in [30]. Can similar results be obtained for partial *t*-spreads in \mathbb{F}_q^{kt+1} ?

6.3. Vector space partitions. The most general result on the non-existence of vector space partitions (without conditions on the dimension v of the ambient space) seems to be:

Theorem 13. (Theorem 1 in [22]) Let \mathcal{P} be a vector space partition of type $t^{m_t} \dots d_2^{m_{d_2}} d_1^{m_{d_1}}$ of \mathbb{F}_q^v , where $m_{d_2}, m_{d_1} > 0$ and $n_1 = m_{d_1}, n_2 = m_{d_2}$.

- (i) if $q^{d_2-d_1}$ does not divide n_1 and if $d_2 < 2d_1$, then $n_1 \ge q^{d_1} + 1$; (ii) if $q^{d_2-d_1}$ does not divide n_1 and if $d_2 \ge 2d_1$, then $n_1 > 2q^{d_2-d_1}$ or d_1 divides d_2 and $n_1 = (q^{d_2} - 1) / (q^{d_1} - 1);$
- (iii) if $q^{d_2-d_1}$ divides n_1 and $d_2 < 2d_1$, then $n_1 \ge q^{d_2} q^{d_1} + q^{d_2-d_1}$; (iv) if $q^{d_2-d_1}$ divides n_1 and $d_2 \ge 2d_1$, then $n_1 \ge q^{d_2}$.

For the special case $d_1 = 1$, Theorem 11 and Theorem 12, presented in the previous section, provide tighter results. For $d_1 > 1$ we might replace the d_1 dimensional subspaces by their points so that we can directly apply results for q^r -divisible sets. For vector space partitions of type ... $4^{\star}2^{\tilde{n}}$ in \mathbb{F}_2^v we obtain 2^3 divisible sets of cardinality $n = 3\tilde{n}$, so that we conclude $\tilde{n} \in \{5, 10, 15, 16\}$ or $\tilde{n} \ge 20$, see Lemma 26. Theorem 13 gives $\tilde{n} = 5$ or $\tilde{n} \ge 9$ and $4|\tilde{n}$ implies $\tilde{n} \ge 16$. However, not all results of Theorem 13 can be obtained that easy. For vector space partitions of type ... $4^*3^{\tilde{n}}$ in \mathbb{F}_2^v we obtain 2^3 -divisible sets of cardinality $n = 7\tilde{n}$, so that we conclude $\tilde{n} = 7$ or $\tilde{n} \ge 9$. Theorem 13 gives $\tilde{n} \ge 9$ and $2|\tilde{n}$ implies $\tilde{n} \geq 10$. In order to exclude $\tilde{n} = 7$ one has to look at the possible hyperplanes in our new setting. So far, we have invoked the fact that $|H \cap \mathcal{C}| \equiv |\mathcal{C}| \pmod{q^r}$. Those $|H \cap \mathcal{C}|$ have to come as a partition of type $s^a(s-1)^b$, where $a+b=\tilde{n}$. Here the possible values for b are restricted by the cases for q^{r-1} -divisible sets admitting a partition type $(s-1)^b$. This eventually further reduces the possible hyperplane types so that the linear programming method can be applied. In our situation we have $\mathcal{T}(\mathcal{C}) \subseteq \{25, 49\}$, which is excluded by Lemma 22. For the general case we propose:

Definition 4. A set $C \subseteq PG(v-1, \mathbb{F}_q)$ admits partition type $s^{m_s} \dots 1^{m_1}$ if C can be partitioned into m_i disjoint subspaces of dimension i for $1 \leq i \leq s$.

With this, we may restate that there is no 2^3 -divisible set admitting partition type 3^7 . However, we are very far from the generality and compactness of Theorem 13. Nevertheless, the sketched approach seems to be a very promising research direction from our point of view (and a natural extension of the study of q^r -divisible sets).

ACKNOWLEDGEMENT

The authors would like to acknowledge the financial support provided by COST European Cooperation in Science and Technology. The first author was also supported by the National Natural Science Foundation of China under Grant 61571006. The second and the third author are members of the Action IC1104 Random Network Coding and Designs over GF(q). The third author was supported in part by the grant KU 2430/3-1 – Integer Linear Programming Models for Subspace Codes and Finite Geometry from the German Research Foundation.

References

- J. André, Über nicht-desarguessche Ebenen mit transitiver Translationsgruppe, Mathematische Zeitschrift 60 (1954), no. 1, 156–186.
- [2] J. De Beule, A. Klein, and K. Metsch, Substructures of finite classical polar spaces, in Beule and Storme [3].
- [3] J. De Beule and L. Storme (eds.), Current research topics in Galois geometry, Nova Science Publishers, 2011.
- [4] A. Beutelspacher, Partial spreads in finite projective spaces and partial designs, Mathematische Zeitschrift 145 (1975), no. 3, 211–229.
- [5] _____, Partitions of finite vector spaces: an application of the Frobenius number in geometry, Archiv der Mathematik 31 (1978), no. 1, 202–208.
- [6] J. Bierbrauer, Introduction to coding theory, 2005.
- [7] C.E. Bonferroni, Teoria statistica delle classi e calcolo delle probabilità, Libreria internazionale Seeber, 1936.
- [8] R.C. Bose and K.A. Bush, Orthogonal arrays of strength two and three, The Annals of Mathematical Statistics (1952), 508–524.
- [9] A. Brauer, On a problem of partitions, American Journal of Mathematics **64** (1942), no. 1, 299–312.
- [10] R.H. Bruck and R.C. Bose, The construction of translation planes from projective spaces, Journal of Algebra 1 (1964), no. 1, 85–102.
- [11] R. Calderbank and W.M. Kantor, The geometry of two-weight codes, Bulletin of the London Mathematical Society 18 (1986), no. 2, 97–122.
- [12] P. Delsarte, Bounds for unrestricted codes, by linear programming, Philips Res. Rep 27 (1972), 272–289.
- [13] P. Dembowski, Finite Geometries: Reprint of the 1968 edition, Springer Science & Business Media, 2012.
- [14] C.F. Doran, M.G. Faux, S.J. Gates, T. Hübsch, K.M. Iga, G.D. Landweber, and R.L. Miller, *Codes and supersymmetry in one dimension*, Advances in Theoretical and Mathematical Physics 15 (2011), no. 6, 1909–1970.
- [15] D.A. Drake and J.W. Freeman, Partial t-spreads and group constructible (s, r, μ) -nets, Journal of Geometry **13** (1979), no. 2, 210–216.
- [16] J. Eisfeld and L. Storme, t-spreads and minimal t-covers in finite projective spaces, Lecture notes, Universiteit Gent, 29 pages (2000).
- [17] 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 and Cryptography 54 (2010), no. 2, 101–107.
- [18] T. Etzion and N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, IEEE Transactions on Information Theory 55 (2009), no. 7, 2909–2919.
- [19] E.M. Gabidulin, Theory of codes with maximum rank distance, Problemy Peredachi Informatsii 21 (1985), no. 1, 3–16.
- [20] J. Galambos, Bonferroni inequalities, The Annals of Probability (1977), 577-581.
- [21] O. Heden, The Frobenius number and partitions of a finite vector space, Archiv der Mathematik 42 (1984), no. 2, 185–192.
- [22] _____, On the length of the tail of a vector space partition, Discrete Mathematics 309 (2009), no. 21, 6169–6180.
- [23] _____, A survey of the different types of vector space partitions, Discrete Mathematics, Algorithms and Applications 4 (2012), no. 1, 14p., nr. 1250001.
- [24] D. Heinlein, T. Honold, M. Kiermaier, S. Kurz, and A. Wassermann, On projective q^r-divisible codes, In preparation, October 2016.
- [25] D. Heinlein, M. Kiermaier, S. Kurz, and A. Wassermann, *Tables of subspace codes*, University of Bayreuth, 2015, available at http://subspacecodes.uni-bayreuth.de.
- [26] R. Hill, Caps and codes, Discrete Mathematics 22 (1978), no. 2, 111-137.
- [27] S.J. Hong and A.M. Patel, A general class of maximal codes for computer applications, IEEE Transactions on Computers 100 (1972), no. 12, 1322–1331.
- [28] T. Honold, M. Kiermaier, and S. Kurz, Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4, Contemp. Math. 632 (2015), 157–176.
- [29] _____, Constructions and bounds for mixed-dimension subspace codes, Advances in Mathematics of Communication 10 (2016), no. 3, 649–682.

- [30] T. Honold, M. Kiermaier, and Sascha Kurz, Classification of large partial plane spreads in PG(6,2) and related combinatorial objects, arXiv preprint 1606.07655 (2016).
- [31] W.C. Huffman and V. Pless, Fundamentals of error-correcting codes, Cambridge university press, 2010.
- [32] A. Kohnert and S. Kurz, Construction of large constant dimension codes with a prescribed minimum distance, Mathematical methods in computer science, Springer, 2008, pp. 31–42.
- [33] C. Krattenthaler, Advanced determinant calculus, The Andrews Festschrift, Springer, 2001, pp. 349–426.
- [34] M. Krawtchouk, Sur une généralisation des polynomes dhermite, Comptes Rendus 189 (1929), no. 620-622, 5–3.
- [35] S. Kurz, Upper bounds for partial spreads, arXiv preprint 1606.08581 (2016).
- [36] _____, Improved upper bounds for partial spreads, Designs, Codes and Cryptography (to appear).
- [37] L. Lambert, Random network coding and designs over \mathbb{F}_q , Ph.D. thesis, Ghent University; Master Thesis, 2013.
- [38] M. Lavrauw and O. Polverino, *Finite semifields*, in Beule and Storme [3], pp. 129–157.
- [39] M. Lavrauw and G. Van de Voorde, Field reduction and linear sets in finite geometry, Contemp. Math 632 (2015), 271–293.
- [40] S.P. Lloyd, Binary block coding, Bell System Technical Journal 36 (1957), no. 2, 517-535.
- [41] Z.T. Mateva and S.T. Topalova, *Line spreads of* PG(5, 2), J. Combin. Des. **17** (2009), no. 1, 90–102. MR 2475427 (2010e:51008)
- [42] A. Nakić and L. Storme, On the extendability of particular classes of constant dimension codes, Designs, Codes and Cryptography 79 (2016), no. 3, 407–422.
- [43] E. Năstase and P. Sissokho, The maximum size of a partial spread ii: Upper bounds, arXiv preprint 1606.09208 (2016).
- [44] _____, The maximum size of a partial spread in a finite projective space, arXiv preprint 1605.04824 (2016).
- [45] R.L. Plackett and J.P. Burman, The design of optimum multifactorial experiments, Biometrika 33 (1946), no. 4, 305–325.
- [46] B. Segre, Teoria di galois, fibrazioni proiettive e geometrie non desarguesiane, Annali di Matematica Pura ed Applicata 64 (1964), no. 1, 1–76.
- [47] N. Silberstein and T. Etzion, Large constant dimension codes and lexicodes, Adv. Math. Commun. 5 (2011), no. 2, 177–189.
- [48] D. Silva, F.R. Kschischang, and R. Koetter, A rank-metric approach to error control in random network coding, IEEE Transactions on Information Theory 54 (2008), no. 9, 3951– 3967.
- [49] H.N. Ward, Divisible codes, Archiv der Mathematik 36 (1981), no. 1, 485-494.

THOMAS HONOLD, ZHEJIANG UNIVERSITY, 310027 HANGZHOU, CHINA *E-mail address*: honold@zju.edu.cn

MICHAEL KIERMAIER, UNIVERSITY OF BAYREUTH, 95440 BAYREUTH, GERMANY *E-mail address:* michael.kiermaier@uni-bayreuth.de

SASCHA KURZ, UNIVERSITY OF BAYREUTH, 95440 BAYREUTH, GERMANY *E-mail address*: sascha.kurz@uni-bayreuth.de