AN IMPROVEMENT OF THE JOHNSON BOUND FOR SUBSPACE CODES

ABSTRACT. Subspace codes, i.e., subset of a finite-field Grassmannian, are applied in random linear network coding. Here we give improved upper bounds based on the Johnson bound and a connection to divisible codes, which is presented in a purely geometrical way. This complements a recent approach for upper bounds on the maximum size of partial spreads based on projective q^r-divisible codes.

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 v-dimensional vector space $\mathbb{F}_q$, where $v\geq 1$. The set of all subspaces of $\mathbb{F}_q^v$, ordered by the incidence relation $\subseteq$, is called *$(v-1)$-dimensional projective geometry over* $\mathbb{F}_q$ and denoted by $\mathrm{PG}(v-1,\mathbb{F}_q)=\mathrm{PG}(\mathbb{F}_q^v)$. It forms a finite modular geometric lattice with meet $X\wedge Y=X\cap Y$, join $X\vee Y=X+Y$, and rank function $X\mapsto \dim(X)$. We will use the term *k-subspace* to denote a k-dimensional vector subspace of $\mathbb{F}_q^v$. The set of all k-subspaces of $V=\mathbb{F}_q^v$ will be denoted by $\begin{bmatrix}V\\k\end{bmatrix}_q$ and has a cardinality given by the Gaussian binomial coefficient

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

The geometry $\mathrm{PG}(v-1,\mathbb{F}_q)$ serves as input and output alphabet of the so-called *linear operator channel (LOC)* – a model for information transmission in coded packet networks subject to noise [16]. The relevant metrics on the LOC 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 can also be seen as the graph-theoretic distance in the Hasse diagram of $\mathrm{PG}(v-1,\mathbb{F}_q)$, and the *injection distance* $d_I(X,Y):=\max\{\dim(X),\dim(Y)\}-\dim(X\cap Y)$. A set $\mathscr{C}$ of subspaces of $\mathbb{F}_q^v$ is called a *subspace code*. The *minimum (subspace) distance* of $\mathscr{C}$ is given by $d=\min\{d_S(X,Y)\mid X,Y\in\mathscr{C},X\neq Y\}$. If all elements of $\mathscr{C}$ have the same dimension, we call $\mathscr{C}$ a *constant-dimension code*. For a constant-dimension code $\mathscr{C}$ we have $d_S(X,Y)=2d_I(X,Y)$ for all $X,Y\in\mathscr{C}$, so that we can restrict attention to the subspace distance, which has to be even. By $\mathrm{A}_q(v,d;k)$ we denote the maximum possible cardinality of a constant-dimension-k code in $\mathbb{F}_q^v$ with minimum subspace distance at least d. Like in the classical case of codes in the Hamming metric, the determination of the exact value or bounds for $\mathrm{A}_q(v,d;k)$ is an important problem. In this paper we will present some improved upper bounds. For a broader background we refer to [8, 9] and for the latest numerical bounds to the online tables at `http://subspacecodes.uni-bayreuth.de` [11].

For a subspace $U\leq\mathbb{F}_q^v$, the orthogonal subspace with respect to some fixed non-degenerate bilinear form will be denoted $U^\perp$. It has dimension $\dim(U^\perp)=v-\dim(U)$. For $U,W\leq\mathbb{F}_q^v$, we get that $\mathrm{d_S}(U,W)=\mathrm{d_S}(U^\perp,W^\perp)$. So, $\mathrm{A}_q(v,d;k)=\mathrm{A}_q(v,d;v-k)$ and we can assume $0\leq k\leq v-k$ in the following. If $d>2k$, then $\mathrm{A}_q(v,d;k)=1$. Otherwise we have $\mathrm{A}_q(v,2;k)=\begin{bmatrix}v\\k\end{bmatrix}_q$. Things get more interesting for $v,d\geq 4$ and $k\geq 2$.

Let $\mathscr{C}$ be a constant-dimension-k code in $\mathbb{F}_q^v$ with minimum distance d. For every point P, i.e., 1-subspace, of $\mathbb{F}_q^v$ we can consider the quotient geometry $\mathrm{PG}(\mathbb{F}_q^v/P)$ to deduce that at most $\mathrm{A}_q(v-1,d;k-1)$ elements of $\mathscr{C}$ contain P. Since $\mathbb{F}_q^v$ contains $\begin{bmatrix}v\\1\end{bmatrix}_q$ points and

every k-subspace contains $\begin{bmatrix}k\\1\end{bmatrix}_q$ points, we obtain

$$\mathrm{A}_q(v,d;k) \leq \left\lfloor \frac{\begin{bmatrix}v\\1\end{bmatrix}_q \cdot \mathrm{A}_q(v-1,d;k-1)}{\begin{bmatrix}k\\1\end{bmatrix}_q} \right\rfloor = \left\lfloor \frac{(q^v-1)\cdot \mathrm{A}_q(v-1,d;k-1)}{q^k-1} \right\rfloor, \qquad (1)$$

which was named Johnson type bound II in [26]. Recursively applied, we obtain

$$\mathrm{A}_q(v,d;k) \leq \left\lfloor \frac{q^v-1}{q^k-1} \cdot \left\lfloor \frac{q^{v-1}-1}{q^{k-1}-1} \cdot \left\lfloor \cdots \left\lfloor \frac{q^{v'+1}-1}{q^{d/2+1}-1} \cdot \mathrm{A}_q(v',d;d/2) \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor, \qquad (2)$$

where $v' = v-k+d/2$. In the case $d = 2k$ we speak of a *partial k-spread* and a *k-spread* if the code additionally has cardinality $\begin{bmatrix}v\\1\end{bmatrix}_q / \begin{bmatrix}k\\1\end{bmatrix}_q$. From the work of Segre in 1964 [22, §VI] we know that k-spreads exist if and only if k divides v. Upper bounds for partial k-spreads are due to Beutelspacher [2] and Drake & Freeman [7] and date back to 1975 and 1979, respectively. Starting from [17] several recent improvements have been obtained. Currently the tightest upper bounds, besides k-spreads, are given by and list of 21 sporadic 1-parametric series and the following two theorem stated in [18]:

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

Theorem 2. *For integers $r \geq 1$, $t \geq 2$, $y \geq \max\{r,2\}$, $z \geq 0$ with $\lambda = q^y$, $y \leq k$, $k = \begin{bmatrix}r\\1\end{bmatrix}_q + 1 - z > r$, $v = kt+r$, and $l = \frac{q^{v-k}-q^r}{q^k-1}$, we have $\mathrm{A}_q(v,2k;k) \leq$*

$$lq^k + \left\lceil \lambda - \frac{1}{2} - \frac{1}{2}\sqrt{1 + 4\lambda\left(\lambda - (z+y-1)(q-1)-1\right)} \right\rceil.$$

The special case $z = 0$ in Theorem 1 covers the breakthrough $\mathrm{A}_q(kt+r,2k;k) = 1 + \sum_{s=1}^{t-1} q^{sk+r}$ for $0 < r < k$ and $k > \begin{bmatrix}r\\1\end{bmatrix}_q$ by Năstase and Sissokho [21] from 2016, which itself covers the result of Beutelspacher. The special case $y = k$ in Theorem 2 covers the result by Drake & Freeman. A contemporary survey of the best known upper bounds for partial spreads can be found in [15].

Using the tightest known upper bounds for the sizes of partial k-spreads, there are only two explicitly known cases for $d < 2k$ where Inequality (2) can be improved: $\mathrm{A}_2(6,4;3) = 77 < 81$ [14] and $257 \leq \mathrm{A}_2(8,6;4) \leq 272 < 289$ [13]. For the details how the proposed upper bounds for constant-dimension codes relate to Inequality (2) we refer the interested reader to [1, 12]. The two mentioned improvements of Inequality (2) are based on extensive integer linear programming computations. In contrast to that, the improvements in this article are based on a self-contained theoretical argument and do not need any external computations.

The remaining part of this paper is organized as follows. In Section 2 we consider multisets $\mathscr{P}$ of points in $\mathbb{F}_q^v$ with $\#\mathscr{P} \equiv \#(\mathscr{P} \cap H)$ for every hyperplane H of $\mathbb{F}_q^v$. The set of possible cardinalities is completely characterized in Theorem 4 and used to conclude upper bounds for $\mathrm{A}_q(v,d;k)$ in Theorem 3. While it is possible to formulate the entire approach in geometrical terms, the underlying structure can possibly be best understood in terms of q^r-divisible linear codes and the linear programming method, which is the topic of Section 3. We draw a short conclusion in Section 4.

2. Main result

Taking $\mathbb{F}_q^v$ as the ambient space, we call every 1-subspace a *point* and every $(v-1)$-subspace a *hyperplane*. Given a multiset of subspaces of $\mathbb{F}_q^v$, we obtain a corresponding multiset $\mathscr{P}$ of points by replacing each subspace by its set of points. For each point P we denote the multiplicity of P in $\mathscr{P}$ by $w(P)$. We write $\#\mathscr{P} = \sum_{P \in \mathbb{F}_q^v} w(P)$ and $\#(\mathscr{P} \cap H) = \sum_{P \in H} w(P)$ for each hyperplane H.

Lemma 1. *For a non-empty multiset of subspaces of $\mathbb{F}_q^v$ with m_i subspaces of dimension i let $\mathscr{P}$ be the corresponding multiset of points. If $m_i = 0$ for all $0 \le i < k$, where $k \ge 2$, then*

$$\#\mathscr{P} \equiv \#(\mathscr{P} \cap H) \pmod{q^{k-1}}.$$

Proof. We have $\#\mathscr{P} = \sum_{i=0}^{v} m_i \begin{bmatrix} v \\ i \end{bmatrix}_q$. For an i-subspace U of $\mathbb{F}_q^v$ the dimension formula gives $\dim(U \cap H) \in \{i-1, i\}$. So for the (multi-)set $\mathscr{P}'$ of points corresponding to U, we get that $\#(\mathscr{P}' \cap H)$ is either $\begin{bmatrix} v \\ i \end{bmatrix}_q$ or $\begin{bmatrix} v \\ i-1 \end{bmatrix}_q$. This implies $\#(\mathscr{P}' \cap H) \equiv \begin{bmatrix} v \\ i \end{bmatrix}_q \pmod{q^{i-1}}$. Summing up yields the proposed result. □

Definition 1. *Let $\mathscr{P}$ be a multiset of points in $\mathbb{F}_q^v$ and $1 \le r < v$ be an integer. If $\#\mathscr{P} \equiv \#(\mathscr{P} \cap H) \pmod{q^r}$ for every hyperplane H, then $\mathscr{P}$ is called q^r-*divisible.

If we speak of a q^r-divisible multiset, we mean a multiset of points in $\mathbb{F}_q^v$ for a suitable dimension $v \in \mathbb{N}_{>0}$.

Corollary 1. *Let $\mathscr{C}$ be a constant-dimension-k code in $\mathbb{F}_q^v$, where $k \ge 2$. Then, the corresponding multiset of points is q^{k-1}-divisible.*

Note that Corollary 1 does not depended on the minimum distance of the code. It will be invoked indirectly by the following complement-type construction.

Lemma 2. *If a multiset of points $\mathscr{P}$ in $\mathbb{F}_q^v$ is q^r-divisible with $r < v$ and satisfies $w_{\mathscr{P}}(P) \le t$ for all points P in $\mathbb{F}_q^v$, then the multiset $\overline{\mathscr{P}}$ with $w_{\overline{\mathscr{P}}}(P) = t - w_{\mathscr{P}}(P)$ is also q^r-divisible.*

Proof. We have $\#\overline{\mathscr{P}} = \begin{bmatrix} v \\ 1 \end{bmatrix}_q t - \#\mathscr{P}$ and $\#(\overline{\mathscr{P}} \cap H) = \begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q t - \#(\mathscr{P} \cap H)$ for every hyperplane H. Thus, the result follows from $\begin{bmatrix} v \\ 1 \end{bmatrix}_q \equiv \begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q \pmod{q^r}$, which holds for $r < v$. □

Theorem 3. *Let $m = \begin{bmatrix} v \\ 1 \end{bmatrix}_q \cdot \mathrm{A}_q(v-1, d; k-1) - \begin{bmatrix} k \\ 1 \end{bmatrix}_q \cdot \left\lfloor \frac{\begin{bmatrix} v \\ 1 \end{bmatrix}_q \cdot \mathrm{A}_q(v-1,d;k-1)}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} \right\rfloor + \begin{bmatrix} k \\ 1 \end{bmatrix}_q \cdot \delta$ for some $\delta \in \mathbb{N}_0$. If no q^{k-1}-divisible multiset of points in $\mathbb{F}_q^v$ of cardinality m exists, then*

$$\mathrm{A}_q(v, d; k) \le \left\lfloor \frac{\begin{bmatrix} v \\ 1 \end{bmatrix}_q \cdot \mathrm{A}_q(v-1, d; k-1)}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} \right\rfloor - \delta - 1.$$

Proof. Let $\mathscr{C}$ be a code with cardinality $\left\lfloor \frac{\begin{bmatrix} v \\ 1 \end{bmatrix}_q \cdot \mathrm{A}_q(v-1,d;k-1)}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} \right\rfloor - \delta$ and matching parameters. Let $\mathscr{P}$ be the corresponding multiset of points and $t = \mathrm{A}_q(v-1, d; k-1)$. Then we can apply Corollary 1 and Lemma 2 to deduce that $\overline{\mathscr{P}}$ is q^{k-1}-divisible with cardinality m, which is a contradiction. □

In view of Theorem 3 it is worthwhile to study the possible cardinalities of q^r-divisible multisets of points.

Lemma 3. *Let $\mathscr{P}$ be a non-empty q^r-divisible multiset of points, then there exists a hyperplane H with $\#(\mathscr{P} \cap H) < \#\mathscr{P}/q$.*

Proof. Assume that $\mathscr{P}$ *lives* in $\mathbb{F}_q^v$ for a certain dimension v. Summing over all hyperplanes gives $\sum_{\bar{H} \le \mathbb{F}_q^v} \#(\mathscr{P} \cap \bar{H}) = \#\mathscr{P} \cdot \begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q$, so that we obtain $\#\mathscr{P} \cdot \begin{bmatrix} v-1 \\ 1 \end{bmatrix}_q / \begin{bmatrix} v \\ 1 \end{bmatrix}_q < \#\mathscr{P}/q$ on average. Choosing a hyperplane H that minimizes $\#(\mathscr{P} \cap H)$ completes the proof. □

Lemma 4. *If $\mathscr{P}_1$ and $\mathscr{P}_2$ are q^r-divisible multisets, then there exists a q^r-divisible multiset of cardinality $\#\mathscr{P}_1 + \#\mathscr{P}_2$.*

Proof. Let $\mathscr{P}_1 \in \mathbb{F}_q^{v_1}$ and $\mathscr{P}_2 \in \mathbb{F}_q^{v_2}$. Embed both multisets in $\mathbb{F}_q^{\max\{v_1, v_2\}}$ and consider their union/sum, which gives a q^r-divisible multiset. □

For each $r \in \mathbb{N}_{>0}$ the q^r-fold duplicate of a point is a q^r-divisible multiset of cardinality q^r and each $(r+1)$-subspace corresponds to a q^r-divisible (multi)-set of cardinality $\begin{bmatrix} r+1 \\ 1 \end{bmatrix}_q = \frac{q^{r+1}-1}{q-1}$. By the previous lemma there exist q^r-divisible multisets of cardinality $a_1 q^r + a_2 \begin{bmatrix} r+1 \\ 1 \end{bmatrix}_q$ for each $a_1, a_2 \in \mathbb{N}_0$. Since q^r and $\begin{bmatrix} r+1 \\ 1 \end{bmatrix}_q$ are coprime, for each pair of parameters q and r there only exists a finite set of cardinalities that cannot be attained by q^r-divisible multisets. For $r \in \mathbb{N}_{>0}$ and $0 \le i \le r$, we set

$$s_{i,r}^q = q^{r-i} \cdot \frac{q^{i+1}-1}{q-1} = \sum_{j=0}^{i} q^{r-j} = q^r + q^{r-1} + \cdots + q^{r-i}. \tag{3}$$

Lemma 5. *There exists a q^1-divisible multiset of points of cardinality n if and only if there are non-negative integers a_0, a_1 with $n = a_0 q + a_1(q+1) = a_0 s_{0,1}^q + a_1 s_{1,1}^q$.*

Proof. If $a_0, a_1 \in \mathbb{N}_0$ with $n = a_0 q + a_1(q+1)$ exist, then the existence of a suitable multiset is clear from Lemma 4 and the constructions above. Assume the contrary, so that $n < q^2$ and we can uniquely write $n = b_1 q + b_0$ with $b_1, b_0 \in \mathbb{N}_0$, $0 \le b_1 < q$, and $0 \le b_0 < q$. Additionally, we observe $b_1 > b_0$ since we may set $a_1 = b_0$ and $a_0 = b_0 - b_1$. For a q^1-divisible multiset of points of cardinality n we can apply Lemma 3 in order to deduce the existence of a hyperplane H with $\#(\mathscr{P} \cap H) < \#\mathscr{P}/q = n/q$, so that $\#(\mathscr{P} \cap H) \le b_1$. Since $\#(\mathscr{P} \cap H) \equiv b_0 \pmod q$ and $b_1 < b_0$ this is impossible. □

Theorem 4. *There exists a q^r-divisible multiset of points of cardinality n if and only if there are non-negative integers $a_0, \ldots, a_r$ with $n = \sum_{i=0}^r a_i s_{i,r}^q$.*

Proof. We prove by induction on r, where the case $r = 1$ is provided by Lemma 5. Given $r > 1$ we can apply the induction hypothesis to deduce the existence of q^{r-1}-divisible multisets of cardinality $s_{i,r-1}^q = s_{i,r}^q/q$ for each $0 \le i \le r-1$. Taking q copies of these, we obtain q^r-divisible multisets of cardinality $s_{i,r}^q$ for $0 \le i \le r-1$. A q^r-divisible multiset of cardinality $s_{r,r}^q$ is given by an $(r+1)$-subspace. So, it remains to show that if n cannot be written as $n = \sum_{i=0}^r a_i s_{i,r}^q$ with non-negative integers a_i, then no q^r-divisible multiset of cardinality n exists. To this end assume that $\mathscr{P}$ is a q^r-divisible multiset of cardinality $n > 0$. From Lemma 3 we conclude the existence of a hyperplane H with $b := \#(\mathscr{P} \cap H) < \#\mathscr{P}/q$. Since $\mathscr{P} \cap H$ is q^{r-1}-divisible we can use the induction hypothesis to deduce the existence of non-negative integers $e_0, \ldots, e_{r-1}$ with $b = \sum_{i=0}^{r-1} e_i s_{i,r-1}^q$. Due to $q s_{i,r-1}^q = q s_{0,r-1}^q + s_{i-1,r-1}^q$ for $1 \le i \le r-1$ we can assume $e_i \le q-1$ for all $1 \le i \le r-1$. Write $e_0 = xq + y$, where $x, y \in \mathbb{N}_0$ and $y \le q-1$. Since $\#(\mathscr{P} \cap H) \equiv \#\mathscr{P} \pmod{q^r}$ we can write $n = b - xq^r + cq^r$ for some uniquely determined $c \in \mathbb{N}_0$. Setting $t = y + \sum_{i=1}^{r-1} e_i$ and using $s_{i,r-1}^q + q^r = s_{i+1,r}^q$ for $0 \le i \le r-1$, $s_{0,r}^q = q^r$ we conclude that

$$n = b - xq^r + cq^r = (c-t) s_{0,r}^q + y s_{1,r}^q + \sum_{i=2}^{r} s_{i,r}^q.$$

Thus, $c \le t-1$ since we assume that n cannot be written as $n = \sum_{i=0}^r a_i s_{i,r}^q$. However,

$$\begin{aligned} n &= b - xq^r + cq^r \le b - xq^r + tq^r - q^r = bq + y s_{0,r-1}^q + \sum_{i=1}^{r-1} e_i s_{i,r-1}^q - q^r \\ &\le bq + (q-1) \sum_{i=0}^{r-1} s_{i,r-1}^q - q^r = bq - 1 < bq, \end{aligned}$$

which contradicts Lemma 3. □

As an example we apply Theorem 3 in order to deduce an upper bound for $\mathrm{A}_2(9,6;4)$. Since $\mathrm{A}_2(8,6;3) = 34$, we have $m = 4 + 15\delta$. Using Theorem 4 we can easily check that there is no 2^3-divisible multiset of cardinality $4 + 1 \cdot 15 = 19$. As we can write $34 = 1 \cdot 8 + 1 \cdot 12 + 1 \cdot 14 + 0 \cdot 15$, there exists a 2^3-divisible multiset of cardinality $4 + 2 \cdot 15 = 34$. So,

choosing $\delta = 1$, we obtain the improved upper bound $\mathrm{A}_2(9,6;4) \leq \left\lfloor \frac{511\cdot 34}{15} \right\rfloor - 2 = 1156 < 1158$. Combining this with the Johnson bound from Inequality (1) we obtain $\mathrm{A}_2(10,6;5) \leq \left\lfloor \frac{1023\cdot 1156}{31} \right\rfloor = 38148 < 38214$.

In our application of bounds for $\mathrm{A}_q(v,d;k)$ we have the additional requirement, that the q^{k-1}-divisible multiset of points of cardinality m in Theorem 3 has to embedded in $\mathbb{F}_q^v$, i.e., there is a restriction on the dimension of the ambient space. However, the constructive part of the proof of Theorem 4 shows that if a q^r-divisible multiset of cardinality n exists, then there also exists at least one q^r-divisible multiset of cardinality n in $\mathbb{F}_q^{r+1}$. Since $r+1 = k \leq v$, the information on the dimension gives no proper restriction.

Algorithmically the criterion of Theorem 4 can be quickly checked recursively using base q representations.

Lemma 6. *Let $r \in \mathbb{N}_{>0}$ and $n = \sum_{i=0}^{m} e_i q^i > 0$ with $e_i \in \mathbb{N}_0$ and $e_i < q$ for all $0 \leq i \leq m$. If j is the smallest index with $e_j \neq 0$ and $j < r$, then there exist non-negative integers $a_0, \ldots, a_r$ with $n = \sum_{i=0}^{r} a_i s_{i,r}^q$ if and only if $n - e_j \cdot s_{r-j,r}^q$ can be written in such a way. Moreover, $n - e_j \cdot s_{r-j,r}^q$ is divisible by q^{j+1}.*

Proof. If there exist non-negative integers $c_0, \ldots, c_r$ with $n - e_j \cdot s_{r-j,r}^q = \sum_{i=0}^{r} c_i s_{i,r}^q$, then we can choose $a_i = c_i$ for $i \neq r-j$ and $a_{r-j} = c_{r-j} + e_j$. For the other direction let there be non-negative integers $a_0, \ldots, a_r$ with $n = \sum_{i=0}^{r} a_i s_{i,r}^q$. Due to $q s_{i,r}^q = q s_{0,r}^q + s_{i-1,r}^q$ for $1 \leq i \leq r$ we can assume $0 \leq a_i \leq q-1$ for all $1 \leq i \leq r$.

Now, we recursively show that $a_{r-i} = 0$ for all $0 \leq i < j$. Since n is divisible by q^j it is divisible by q^{i+1}. As $s_{h,r}^q$ is divisible by q^{i+1} for all $0 \leq h < r-i$ and $a_{r-h} = 0$ for all $0 \leq h < i$, also $a_{r-i} s_{r-i,r}^q$ is divisible by q^{i+1} so that q divides a_{r-i}. Thus, we have $a_{r-i} = 0$.

Since $a_{r-i} = 0$ for all $0 \leq i < j$ and suffices to show $a_{r-j} = e_j$, which follows from

$$e_j q^j \equiv n = \sum_{i=0}^{r-j} a_i s_{i,r}^q \equiv a_{r-j} s_{r-j,r}^q \equiv a_{r-j} q^j \pmod{q^{j+1}}$$

and $0 \leq e_j, a_{r-j} \leq q-1$. Additionally, $n - e_j \cdot s_{r-j,r}^q$ is divisible by q^{j+1}. □

Algorithm 1
Data: field size q, cardinality n
Result: Either representation $n = \sum_{i=0}^{r} e_{r-i} s_{i,r}^q$ with $a_i \in \mathbb{N}_0$ or
$n = -mq^j + \sum_{i=0}^{j-1} e_i s_{r-i,r}^q$, $e_i \in \mathbb{N}_0$, $e_i < q$, $m \in \mathbb{N}_{>0}$.

```
for i ← 0 to r do
|  e_i ← 0
end
m ← n
for j ← 0 to r − 1 do
|  if m < 0 then
|  |  m ← (−1) · m
|  |  return
|  end
|  e_j ← m − q · ⌊m/q⌋
|  m ← (m − e_j · s^q_{r−j,r−j})/q
end
e_r ← m
```

Since $s_{r-j,r}^q = q^j \cdot s_{r-j,r-j}^q$, Algorithm 1 either computes a representation $n = \sum_{i=0}^{r} a_i s_{i,r}^q$, with $a_i = e_{r-i}$ or it computes a representation $n = -mq^j + \sum_{i=0}^{j-1} e_i s_{r-i,r}^q$ with $m \in \mathbb{N}_{>0}$. Since $-mq^r$ can obviously not be written as $m = \sum_{i=0}^{r} a_i' s_{i,r}^q$ with non-negative integers a_i',

the latter representation is a certificate for the fact that there are no non-negative integers a_i with $n = \sum_{i=0}^{r} a_i s_{i,r}^q$ using Lemma 6.

As an example we apply Theorem 3 in order to deduce an upper bound for $\mathrm{A}_3(11,6;4)$. Since $\mathrm{A}_3(10,6;3) = 2269$, we have $m = 17 + 40\delta$. For $\delta = 3$ we obtain $m = 137 =: n$ and Lemma 6 refers back to $137 - 2 \cdot 40 = 57$, $57 - 1 \cdot 39 = 18$, and $18 - 2 \cdot 36 = -54$, i.e., Algorithm 1 computes the representation $137 = -2 \cdot s_{0,3}^3 + 2 \cdot s_{1,3}^3 + 1 \cdot s_{2,3}^3 + 2 \cdot s_{3,3}^3$. Thus, no 3^3-divisible multiset of cardinality 137 exists and $\mathrm{A}_3(11,6;4) \leq \left\lfloor \frac{(3^{11}-1)\cdot 2269}{3^4-1} \right\rfloor - 4 = 5024299 < 5024303$. For $n = 17 + 4 \cdot 40 = 177$ we can read of the representation $177 = 1 \cdot 27 + 2 \cdot 36 + 2 \cdot 39 + 0 \cdot 40$.

In analogy to the *Frobenius Coin Problem*, cf. [4], we define $\mathrm{F}(q,r)$ as the smallest positive integer such that a q^r-divisible multisets with cardinality n exists for all integers $n > \mathrm{F}(q,r)$.

Proposition 1. *For every prime power q and $r \in \mathbb{N}_{>0}$ we have* $\mathrm{F}(q,r) = r \cdot q^{r+1} - \frac{q^{r+1}-1}{q-1}$.

Proof. Since $r \cdot q^{r+1} - \frac{q^{r+1}-1}{q-1} = -q^r + \sum_{i=1}^{r} (q-1) s_{i,r}$ Lemma 6 ends with $-q^r$ after r steps, i.e., Algorithm 1 provides this certificate of non-existence of the desired sum-representation, so that $\mathrm{F}(q,r) \geq r \cdot q^{r+1} - \frac{q^{r+1}-1}{q-1}$. For the other direction let $n = m + \sum_{i=0}^{j-1} e_i s_{r-i,r}^q$ be the certificate for non-existence from Algorithm 1 for some $0 \leq j < r$. Then $m < 0$ and $q^j | m$, so that $m \leq -q^j$. Using $e_i \leq q-1$ for $0 \leq i < j$ we conclude

$$\begin{aligned} n &\leq -r^j + \sum_{i=0}^{j-1} e_i s_{r-i,r} \leq -q^j + (q-1) \sum_{i=0}^{j-1} s_{r-i,r} \\ &\leq -q^r + (q-1) \sum_{i=0}^{r-1} s_{r-i,r} = -q^r + (q-1) \sum_{i=1}^{r} s_{i,r} = r \cdot q^{r+1} - \frac{q^{r+1}-1}{q-1}, \end{aligned}$$

which completes the proof. □

Actually, we can analyze our previous example for general q using Algorithm 1:

Proposition 2. *For all prime powers $q \geq 2$ we have* $\mathrm{A}_q(11,6;4) \leq q^{14} + q^{11} + q^{10} + 2q^7 + q^6 + q^3 + q^2 - 2q + 1 = (q^2 - q + 1)(q^{12} + q^{11} + q^8 + q^7 + q^5 + 2q^4 + q^3 - q^2 - q + 1)$.

Proof. Since $10 \equiv 1 \pmod 3$ we have $\mathrm{A}_2(10,6;3) = q^7 + q^4 + 1$ and

$$\frac{(q^{11}-1)(q^7+q^4+1)}{q^4-1} = q^{14} + q^{11} + q^{10} + 2q^7 + q^6 + q^3 + q^2 - 1 + \frac{q^2+2q+2}{q^3+q^2+q+1},$$

so that $m = q^2 + 2q + 2 + (q^3 + q^2 + q + 1)\delta$ in Theorem 3. Since

$$\begin{aligned} & (q^2+2q+2) + (2q-3) \cdot (q^3+q^2+q+1) \\ = \; & -2 \cdot q^3 + (q-1) \cdot (q^3+q^2) + 1 \cdot (q^3+q^2+q) + (q-1) \cdot (q^3+q^2+q+1) \end{aligned}$$

Lemma 6 and Theorem 4 tell us that we can choose $\delta = 2q-3$ in Theorem 3, which gives the proposed upper bound. □

We remark that our choice of δ is maximal since

$$\begin{aligned} m &= (q^2+2q+2) + (2q-2) \cdot (q^3+q^2+q+1) \\ &= (q-2) \cdot q^3 + (q-1) \cdot (q^3+q^2) + 2 \cdot (q^3+q^2+q) + 0 \cdot (q^3+q^2+q+1), \end{aligned}$$

i.e., a q^3-divisible multiset of cardinality m exists. In fact we have $m > \mathrm{F}(q,r)$ in our parametric example. In general we always have $\delta \leq (q-1)r - 1$.

3. DIVISIBLE CODES AND THE LINEAR PROGRAMMING METHOD

It is well-known (see, e.g., [23, 6, Prop. 1]) that the relation $C \to \mathscr{C}$, associating with a full-length linear $[n,v]$ code C over $\mathbb{F}_q$ the n-multiset $\mathscr{C}$ of points in $\mathrm{PG}(v-1,\mathbb{F}_q)$ defined by the columns of any generator matrix, induces a one-to-one correspondence between classes of (semi-)linearly equivalent spanning multisets and classes of (semi-)monomially equivalent full-length linear codes. The importance of the correspondence lies in the fact that it relates coding-theoretic properties of C to geometric or combinatorial properties of $\mathscr{C}$ via

$$\mathrm{w}(\mathbf{aG}) = n - \#\{1 \le j \le n; \mathbf{a}\cdot\mathbf{g}_j = 0\} = n - \#(\mathscr{C} \cap \mathbf{a}^\perp), \tag{4}$$

where w denotes the Hamming weight, $\mathbf{G} = (\mathbf{g}_1|\ldots|\mathbf{g}_n) \in \mathbb{F}_q^{v\times n}$ a generating matrix of C, $\mathbf{a}\cdot\mathbf{b} = a_1b_1 + \cdots + a_vb_v$, and $\mathbf{a}^\perp$ is the hyperplane in $\mathrm{PG}(v-1,\mathbb{F}_q)$ with equation $a_1x_1 + \cdots + a_vx_v = 0$.

A linear code C is said to be Δ-*divisible* ($\Delta \in \mathbb{Z}_{>1}$) if all nonzero codeword weights are multiples of Δ. They have been introduced by Ward in 1981, see [24] and [25] for a survey. So, given a q^r-divisible multiset $\mathscr{P}$ in $\mathbb{F}_q^v$ of cardinality n there is a corresponding q^r-divisible linear $[n,k]$ code C, where $k \le v$.

The famous *MacWilliams Identities*, [19]

$$\sum_{j=0}^{n-i}\binom{n-j}{i}A_j = q^{k-i}\cdot\sum_{j=0}^{i}\binom{n-j}{n-i}A_j^\perp \quad \text{for } 0 \le i \le n, \tag{5}$$

relate the weight distributions (A_i), $(A_i^\perp)$ of the (primal) code C and the dual code $C^\perp = \{\mathbf{y} \in \mathbb{F}_q^n; x_1y_1 + \cdots + x_ny_n = 0 \text{ for all } \mathbf{x} \in C\}$. Since the A_i and $A_i^\perp$ count codewords of weight i, they have to be non-negative integers. In our context we have $A_0 = A_0^\perp = 1$, $A_1^\perp = 0$, and $A_i = 0$ for all i that are not divisible by q^r. Treating the remaining A_i and $A_i^\perp$ as non-negative real variable one can check feasibility via linear programming, which is known as the *linear programming method* for the existence of codes, see e.g. [5, 3].

As demonstrated in e.g. [15], the average argument of Lemma 3 is equivalent to the linear programming method applied to the first two MacWilliams Identities, i.e., $i = 0, 1$. So, the proof of Theorem 4 shows that invoking the other Equations gives no further restrictions for the possible lengths of divisible codes. This is different in the case of partial k-spreads, i.e., the determination of $\mathrm{A}_q(v,2k;k)$. Here the multisets of points in Corollary 1 are indeed sets that correspond to projective linear codes, which are characterized by the additional condition $\mathrm{d}(C^\perp) \ge 3$, i.e., $A_2^\perp = 0$. The upper bound of Năstase and Sissokho can be concluded from the first two MacWilliams Identities, i.e., the average argument of Lemma 3. Theorem 2 is based on the first three MacWilliams Identities while also the forth MacWilliams Identity is needed for the mentioned 21 sporadic 1-parametric series listed in [18]. The characterization of the possible lengths of q^r-divisible projective linear codes is more difficult than in the non-projective case of Theorem 4. For the corresponding Frobenius number the sharpest upper bound in the binary case $q = 2$ is $\overline{\mathrm{F}}(2,r) \le 2^{2r} - 2^{r-1} - 1$ and it is unclear whether a 2^3-divisible projective linear code of length 59 exists [10].

4. CONCLUSION

We have presented a connection between q^r-divisible linear codes and upper bounds for constant-dimension codes, which improves the best known upper bounds in many cases. The framework of q^r-divisible linear codes covers constant-dimension codes and partial spreads, while the latter substructures call for projective linear codes as a special subclass of q^r-divisible linear codes. Here, we have characterized all possible lengths of q^r-divisible codes. This problem is open in the case of projective q^r-divisible linear codes. It is very likely that more sophisticated methods from coding theory, beyond the pure application of the linear programming method, are needed in order to decide the non-existence question

in a few more cases.[1] If the possible q^r-divisible codes are classified for the parameters of a desired constant-dimension code, one may continue the analysis and look at the union of the k-dimensional codewords and their restrictions. Using the language of minihypers, the authors of [20] have obtained some extendability results for constant-dimension codes. It seems worthwhile to compare and possibly combine both methods.

ACKNOWLEDGEMENT

The second 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

[1] C. Bachoc, A. Passuello, and F. Vallentin. Bounds for projective codes from semidefinite programming. *Advances in Mathematics of Communications*, 7(2):127–145, 2013.
[2] A. Beutelspacher. Partial spreads in finite projective spaces and partial designs. *Mathematische Zeitschrift*, 145(3):211–229, 1975.
[3] J. Bierbrauer. *Introduction to coding theory*. 2005.
[4] A. Brauer. On a problem of partitions. *American Journal of Mathematics*, 64(1):299–312, 1942.
[5] P. Delsarte. Bounds for unrestricted codes, by linear programming. *Philips Res. Rep*, 27:272–289, 1972.
[6] S. Dodunekov and J. Simonis. Codes and projective multisets. *The Electronic Journal of Combinatorics*, 5(R37):1–23, 1998.
[7] D. Drake and J. Freeman. Partial t-spreads and group constructible (s,r,μ)-nets. *Journal of Geometry*, 13(2):210–216, 1979.
[8] T. Etzion and L. Storme. Galois geometries and coding theory. *Designs, Codes and Cryptography*, 78(1):311–350, 2016.
[9] M. Greferath, M. Pavčević, N. Silberstein, and A. Vazquez-Castro, editors. *Network Coding and Subspace Designs*. Springer, 2017.
[10] D. Heinlein, T. Honold, M. Kiermaier, S. Kurz, and A. Wassermann. Projective divisible binary codes. In *The Tenth International Workshop on Coding and Cryptography*, pages 1–10, 2017. arXiv preprint 1703.08291.
[11] D. Heinlein, M. Kiermaier, S. Kurz, and A. Wassermann. *Tables of subspace codes*. University of Bayreuth, 2015. available at http://subspacecodes.uni-bayreuth.de.
[12] D. Heinlein and S. Kurz. Asymptotic bounds for the sizes of constant dimension codes and an improved lower bound. In *5th International Castle Meeting on Coding Theory and Applications*, pages 1–30, 2017. arXiv preprint 1705.03835.
[13] D. Heinlein and S. Kurz. A new upper bound for subspace codes. In *The Tenth International Workshop on Coding and Cryptography*, pages 1–9, 2017. arXiv preprint 1703.08712.
[14] T. Honold, M. Kiermaier, and S. Kurz. Optimal binary subspace codes of length 6, constant dimension 3 and minimum distance 4. *Contemp. Math.*, 632:157–176, 2015.
[15] T. Honold, M. Kiermaier, and S. Kurz. Partial spreads and vector space partitions. In Greferath et al. [9], chapter 7. arXiv preprint 1611.06328.
[16] R. Koetter and F. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, Aug. 2008.
[17] S. Kurz. Improved upper bounds for partial spreads. *Designs, Codes and Cryptography*, published online on Oct 25, 2016, doi:10.1007/s10623-016-0290-8.
[18] S. Kurz. Packing vector spaces into vector spaces. *The Australasian Journal of Combinatorics*, 68(1):122–130, 2017.
[19] F. J. MacWilliams. A theorem on the distribution of weights in a systematic code. *The Bell System Technical Journal*, 42(1):79–94, 1963.
[20] A. Nakić and L. Storme. On the extendability of particular classes of constant dimension codes. *Designs, Codes and Cryptography*, 79(3):407–422, 2016.
[21] E. Năstase and P. Sissokho. The maximum size of a partial spread in a finite projective space. *arXiv preprint 1605.04824*, 2016.
[22] B. Segre. Teoria di galois, fibrazioni proiettive e geometrie non desarguesiane. *Annali di Matematica Pura ed Applicata*, 64(1):1–76, 1964.

[1] In this context we would like to mention that the second author recently presented the upper bound $A_2(13,10;5) \leq 259$ on a conference. The proof involves an application of the split-weight enumerator and the determination of the unique weight enumerator of a projective 2^3-divisible binary code of length 51, cf. [15].

[23] M. A. Tsfasman and S. G. Vlăduţ. Geometric approach to higher weights. *IEEE Transactions on Information Theory*, 41:1564–1588, 1995.
[24] H. Ward. Divisible codes. *Archiv der Mathematik*, 36(1):485–494, 1981.
[25] H. Ward. Divisible codes – a survey. *Serdica Mathematical Journal*, 27(4):263p–278p, 2001.
[26] S.-T. Xia and F.-W. Fu. Johnson type bounds on constant dimension codes. *Designs, Codes and Cryptography*, 50(2):163–172, 2009.

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