A NOTE ON THE LINKAGE CONSTRUCTION FOR CONSTANT DIMENSION CODES

SASCHA KURZ

ABSTRACT. Constant dimension codes are used for error control in random linear network coding, so that constructions for these codes with large cardinality have achieved wide attention in the last decade. Here, we improve the so-called linkage construction and obtain several parametric series of improvements for the code sizes.
Keywords: constant dimension codes, linkage construction, network coding
MSC: Primary 51E20; Secondary 05B25, 94B65.

1. INTRODUCTION

Let $V \cong \mathbb{F}_q^v$ be a v-dimensional vector space over the finite field $\mathbb{F}_q$ with q elements. By $\begin{bmatrix} V \\ k \end{bmatrix}$ we denote the set of all k-dimensional subspaces in V, where $0 \le k \le v$. The size of the so-called *Grassmannian* $\begin{bmatrix} V \\ k \end{bmatrix}$ is given by $\begin{bmatrix} v \\ k \end{bmatrix}_q := \prod_{i=1}^{k} \frac{q^{v-k+i}-1}{q^i-1}$. More generally, the set $P(V)$ of all subspaces of V forms a metric space with respect to the subspace distance defined by $\mathrm{d_s}(U,W) = \dim(U+W) - \dim(U \cap W) = \dim(U) + \dim(W) - 2\dim(U \cap W)$. Coding theory on $P(V)$ is motivated by Kötter and Kschischang [15] via error correcting random network coding. For $\mathcal{C} \subseteq \begin{bmatrix} V \\ k \end{bmatrix}$ we speak of a *constant dimension code* (`cdc`), where the minimum subspace distance $\mathrm{d_s}$ is always an even integer. By a $(v, N, d; k)_q$ code we denote a `cdc` in V with minimum (subspace) distance d and cardinality N. The corresponding maximum size is denoted by $A_q(v, d; k)$. In geometrical terms, a $(v, N, d; k)_q$ code $\mathcal{C}$ is a set of N k-dimensional subspaces of V, k-spaces for short, such that any $(k - d/2 + 1)$-space is contained in at most one element of $\mathcal{C}$. In other words, each two different codewords intersect in a subspace of dimension at most $k - d/2$. For two k-spaces U and W that have an intersection of dimension zero, we will say that they intersect trivially or are disjoint (since they do not share a common point). We will call 1-, 2-, 3-, and 4-spaces, points, lines, planes, and solids, respectively. For the known lower and upper bounds on $A_q(v, d; k)$ we refer to the online tables `http://subspacecodes.uni-bayreuth.de` associated with the survey [9]. Here we improve the so-called *linkage construction* [7] and obtain several parametric series of improvements.

2. PRELIMINARIES

In the following we will mainly consider the case $V = \mathbb{F}_q^v$ in order to simplify notation. We associate with a subspace $U \in \begin{bmatrix} V \\ k \end{bmatrix}$ a unique $k \times v$ matrix X_U in row reduced echelon form (`rref`) having the property that $\langle X_U \rangle = U$ and denote the corresponding bijection

$$\begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix} \to \{X_U \in \mathbb{F}_q^{k \times v} \,|\, \mathrm{rk}(X_U) = k, X_U \text{ is in } \texttt{rref}\}$$

by τ. An example is given by $X_U = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right) \in \mathbb{F}_2^{2\times 3}$, where $U = \tau^{-1}(X_U) \in \begin{bmatrix} \mathbb{F}_2^3 \\ 2 \end{bmatrix}$ is a line that contains the three points $(1,0,0)$, $(1,1,1)$, and $(0,1,1)$. With this, we can express the subspace distance between two k-dimensional subspaces $U, W \in \left[\begin{smallmatrix} V \\ k \end{smallmatrix}\right]$ via the rank of a matrix:

$$\mathrm{d_s}(U,W) = 2\dim(U+W) - \dim(U) - \dim(W) = 2\left(\mathrm{rk}\begin{pmatrix} \tau(U) \\ \tau(W) \end{pmatrix} - k\right). \tag{1}$$

By $p\colon \{M \in \mathbb{F}_q^{k\times v} \mid \mathrm{rk}(M) = k, \text{M is in } \texttt{rref}\} \to \{x \in \mathbb{F}_2^v \mid \sum_{i=1}^v x_i = k\}$ we denote the pivot positions of the matrix in `rref`. For our example X_U we we have $p(X_U) = (1,1,0)$. Slightly abusing notation we also write $p(U)$ for subspaces $U \in \left[\begin{smallmatrix} V \\ k \end{smallmatrix}\right]$ instead of $p(\tau(U))$. The Hamming distance $\mathrm{d_h}(u,w) = \#\{i \mid u_i \neq w_i\}$, for two vectors $u, w \in \mathbb{F}_2^v$, can be used to lower bound the subspace distance between two codewords.

Lemma 2.1. [3, Lemma 2] *For two subspaces $U, W \in P(V)$ we have*

$$\mathrm{d_s}(U,W) \geq \mathrm{d_h}(p(U), p(W)).$$

For two matrices $A, B \in \mathbb{F}_q^{m\times n}$ we define the rank distance $\mathrm{d_r}(A,B) := \mathrm{rk}(A-B)$. A subset $\mathcal{M} \subseteq \mathbb{F}_q^{m\times n}$ is called a rank metric code.

Theorem 2.2. *(see* [5]*) Let $m, n \geq d'$ be positive integers, q a prime power, and $\mathcal{M} \subseteq \mathbb{F}_q^{m\times n}$ be a rank metric code with minimum rank distance d'. Then, $\#\mathcal{M} \leq q^{\max\{n,m\}\cdot(\min\{n,m\}-d'+1)}$.*

Codes attaining this upper bound are called maximum rank distance (`MRD`) codes. They exist for all choices of parameters. If $m < d'$ or $n < d'$, then only $\#\mathcal{M} = 1$ is possible, which can be achieved by a zero matrix and may be summarized to the single upper bound $\#\mathcal{M} \leq \left\lceil q^{\max\{n,m\}\cdot(\min\{n,m\}-d'+1)} \right\rceil$. Using an $m \times m$ identity matrix $I_{m\times m}$ as a prefix one obtains the so-called lifted `MRD` codes, i.e., the `cdc` $\left\{\tau^{-1}(I_{m\times m}|A) \mid A \in \mathcal{M}\right\} \subseteq \begin{bmatrix} \mathbb{F}_q^{m+n} \\ m \end{bmatrix}$, where $(B|A)$ denotes the concatenation of the matrices B and A.

Theorem 2.3. [18, Proposition 4] *For positive integers k, d, v with $k \leq v$, $d \leq 2\min\{k, v-k\}$, and d even, the size of a lifted `MRD` code $\mathcal{C} \subseteq \left[\begin{smallmatrix} V \\ k \end{smallmatrix}\right]$ with minimum subspace distance d is given by*

$$\#\mathcal{C} = M(q,k,v,d) := q^{\max\{k,v-k\}\cdot(\min\{k,v-k\}-d/2+1)}.$$

If $d > 2\min\{k, v-k\}$, then we have $M(q,k,v,d) := 1$.

3. The linkage construction revisited

In this section we briefly review the so-called linkage construction with its different variants before we present our improvement in Theorem 3.2. The basic idea is the same as for lifted `MRD` codes. Instead of a $k \times k$ identity matrix $I_{k\times k}$ we can also lift any matrix of full row rank k by appending a matrix from a rank metric code. Let v, m, d, and k be integers with $2 \leq k \leq v$, $2 \leq d \leq 2k$, and $k \leq m \leq v-k$. Starting from an $(m, N, d; k)_q$ code $\mathcal{C}$ and an `MRD` code $\mathcal{M}$ of $k \times (v-m)$-matrices over $\mathbb{F}_q$ with rank distance $d/2$, we can construct a `cdc`

$$\mathcal{C}' = \left\{\tau^{-1}\left(\tau(U)|A\right) \mid U \in \mathcal{C}, A \in \mathcal{M}\right\} \subseteq \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}.$$

This generalized lifting idea was called *Construction D* in [17, Theorem 37], cf. [6, Theorem 5.1]. For different $U, U' \in \mathcal{C}$ and different $A, A' \in \mathcal{M}$ we have

$$\mathrm{d_s}\Big(\tau^{-1}\big(\tau(U)|A\big), \tau^{-1}\big(\tau(U)|A'\big)\Big) \geq 2\Big(\operatorname{rk}\big(\tau(U)\big) - k + \operatorname{rk}\big(A - A'\big)\Big) = 2\operatorname{rk}\big(A - A'\big) \geq d,$$

$$\mathrm{d_s}\Big(\tau^{-1}\big(\tau(U)|A\big), \tau^{-1}\big(\tau(U')|A\big)\Big) \geq 2\left(\operatorname{rk}\begin{pmatrix}\tau(U)\\ \tau(U')\end{pmatrix} - k\right) = \mathrm{d_s}(U, U') \geq d,$$

and

$$\mathrm{d_s}\Big(\tau^{-1}\big(\tau(U)|A\big), \tau^{-1}\big(\tau(U')|A'\big)\Big) \geq 2\left(\operatorname{rk}\begin{pmatrix}\tau(U)\\ \tau(U')\end{pmatrix} - k\right) = \mathrm{d_s}(U, U') \geq d$$

due to Equation (1). Since $\mathcal{C}'$ consists of k-spaces and has minimum subspace distance at least d, we obtain

$$A_q(v,d;k) \geq A_q(m,d;k) \cdot \left\lceil q^{(v-m)(k-d/2+1)} \right\rceil \tag{2}$$

for $k \leq m \leq v-k$. In terms of pivot vectors we have that the k ones in $p(U)$ all are contained in the first m entries for all $U \in \mathcal{C}'$. Geometrically, there exists a $(v-m)$-space $W \leq \mathbb{F}_q^v$ that is disjoint to all codewords. Since $W \cong \mathbb{F}_q^{v-m}$ there exists an $(v-m, N'', d; k)_q$ code $\mathcal{C}''$ of cardinality $N'' = A_q(v-m, d; k)$ that can be embedded into W. For all $U' \in \mathcal{C}'$ and all $U'' \in \mathcal{C}''$ we have $\mathrm{d_s}(U', U'') = 2k \geq d$, so that

$$A_q(v,d;k) \geq A_q(m,d;k) \cdot \left\lceil q^{(v-m)(k-d/2+1)} \right\rceil + A_q(v-m,d;k) \tag{3}$$

for $k \leq m \leq v-k$. This is called *linkage construction* in [7, Theorem 2.3], cf. [17, Corollary 39]. However, the assumption $\dim(U' \cap U'') = 0$ can be weakened if $d < 2k$. Let W' be an arbitrary $\left(v-m+k-\frac{d}{2}\right)$-space containing W and $\mathcal{C}''$ be a $(v-m+k-d/2, N'', d; k)_q$ $\mathtt{cdc}$ embedded in W'. For all $U' \in \mathcal{C}'$ and all $U'' \in \mathcal{C}''$ we have $\mathrm{d_s}(U', U'') = 2k - 2\dim(U' \cap U'') \geq 2k - 2\dim(U' \cap W') \geq d$, so that

$$A_q(v,d;k) \geq A_q(m,d;k) \cdot \left\lceil q^{(v-m)\cdot(k-d/2+1)} \right\rceil + A_q(v-m+k-d/2,d;k) \tag{4}$$

for $k \leq m \leq v-k$. This is called *improved linkage construction*, see [11, Theorem 18, Corollary 4]. Interestingly enough, in more than half of the cases covered in [9], the best known lower bound for $A_q(v,d;k)$ is obtained via this inequality. The dimension of the utilized subspace W' is tight in general. However, we may also consider geometrically more complicated objects than subspaces.

Definition 3.1. Let $B_q(v, v-m, d; k)$ denote the maximum number of k-spaces in $\mathbb{F}_q^v$ with minimum subspace distance d such that there exists a $(v-m)$-space W which intersects every chosen k-space in dimension at least $d/2$, where $0 \leq m \leq v$.

Theorem 3.2.

$$A_q(v,d;k) \geq A_q(m,d;k) \cdot \left\lceil q^{(v-m)(k-d/2+1)} \right\rceil + B_q(v, v-m, d; k)$$

for $k \leq m \leq v-k$.

Proof. Let $k \leq m \leq v-k$ be an arbitrary integer, $\mathcal{C}$ be an $(m, N, d; k)_q$ code, where $N = A_q(m,d;k)$, and $\mathcal{M}$ an $\mathtt{MRD}$ of $k \times (v-m)$-matrices over $\mathbb{F}_q$ with rank distance $d/2$. With this we set $\mathcal{C}' := \left\{\tau^{-1}(\tau(U)|A) \mid U \in \mathcal{C}, A \in \mathcal{M}\right\} \subseteq \begin{bmatrix}\mathbb{F}_q^v\\ k\end{bmatrix}$, i.e., we apply the lifting construction to $\mathcal{C}$. As argued before, there exists a $(v-m)$-space W that is disjoint from all elements from

$\mathcal{C}'$. Now let $\mathcal{C}'' \subseteq \begin{bmatrix} \mathbb{F}_q^v \\ k \end{bmatrix}$ be a $\texttt{cdc}$ with minimum subspace distance d such that every codeword intersects W in dimension at least $d/2$, which has the maximum possible cardinality.

For each $U' \in \mathcal{C}'$ and each $U'' \in \mathcal{C}''$ we have $\dim(U' \cap U'') \le k - d/2$ since $\dim(U') = \dim(U'') = k$, $\dim(U' \cap W) = 0$, and $\dim(U'' \cap W) \ge d/2$. Thus, $\mathrm{d_s}(U', U'') \ge d$ and $A_q(v,d;k) \ge \#\mathcal{C}' + \#\mathcal{C}'' = A_q(m,d;k) \cdot \lceil q^{(v-m)(k-d/2+1)} \rceil + B_q(v, v-m, d; k)$. $\square$

The determination of $B_q(v, v-m, d; k)$ or $B_q(v_1, v_2, d; k)$ is a hard problem in general. So, we provide several parametric examples how Theorem 3.2 can be applied to obtain improved lower bounds for $A_q(v,d;k)$ in the next section.

An application of the linkage construction is a lower bound for $A_q(v,4;2)$. If $v \ge 4$ we can use Inequality (3) with $m = 2$ to conclude $A_q(v,4;2) \ge q^{v-2} + A_q(v-2,4;2)$. Since $A_q(3,4;2) = A_q(2,4;2) = 1$ this gives $A_q(v,4;2) \ge q^{v-2} + q^{v-4} + \dots + q^2 + q^0 = \left[\begin{smallmatrix} v \\ 1 \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right]_q$ for even $v \ge 2$ and $A_q(v,4;2) \ge q^{v-2} + q^{v-4} + \dots + q^3 + q^0 = \left[\begin{smallmatrix} v \\ 1 \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right]_q - \frac{q^2}{q+1}$ for odd $v \ge 3$, by induction on v. These lower bounds are indeed tight, see e.g. [1, Theorem 4.2]. If v is even and the maximum cardinality $A_q(v,4;2) = \left[\begin{smallmatrix} v \\ 1 \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} 2 \\ 1 \end{smallmatrix}\right]_q$ is attained the corresponding code is called a line spread. In general we call a set of pairwise disjoint lines a partial line spread. If v is odd and we do not fill the final plane with a single codeword, then we get a partial line spread of cardinality $A_q(v,4;2) - 1$ that is disjoint from a fixed plane π.

4. Results: Lower bounds for $A_q(v,d;k)$

Proposition 4.1. *If $v_1 \ge v_2 + 2 \ge k + 1$ and $k \ge 3$, then*

$$B_q(v_1, v_2, 2k-2; k) \ge A_q(v_2, 2k-4; k-1).$$

Proof. Let $\mathcal{F}$ be an arbitrary set of $(k-1)$-spaces in $W \cong \mathbb{F}_q^{v_2}$ that are pairwise intersecting in at most a point. For each point P in W we denote the set of elements of $\mathcal{F}$ that contain P by $\mathcal{F}_P$, i.e., $\mathcal{F}_P = \{U \in \mathcal{F} \mid P \le U\}$. Considering the elements of $\mathcal{F}_P$ modulo P gives a partial $(k-2)$-spread in $W/P \simeq \mathbb{F}_q^{v_2-1}$, so that $\#\mathcal{F}_P \le \left[\begin{smallmatrix} v_2-1 \\ 1 \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} k-2 \\ 1 \end{smallmatrix}\right]_q$.

We choose $\mathcal{F}$ such that $\#\mathcal{F} = A_q(v_2, 2k-4; k-1)$ and let $V \cong \mathbb{F}_q^{v_1}$ such that $W \le V$. For each $(k-1)$-space $U \in \mathcal{F}$ we construct a k-space $f(U) \in V$ with $\dim(f(U) \cap W) = k-1$. In the beginning we set $f(U) = \varnothing$ for all $U \in \mathcal{F}$ and say that $f(U)$ is not determined. For the construction, we loop over all $\left[\begin{smallmatrix} v_2 \\ 1 \end{smallmatrix}\right]_q$ points P of W and initialize $\mathcal{P}_P$ with the set of $\left[\begin{smallmatrix} v_1 \\ 1 \end{smallmatrix}\right]_q - \left[\begin{smallmatrix} v_2 \\ 1 \end{smallmatrix}\right]_q$ points of V that are not contained in W. For each $U \in \mathcal{F}_P$, where $f(U)$ is already determined, i.e., $f(U) \ne \varnothing$, we remove the q^{k-1} points of $f(U) \backslash W$ from $\mathcal{P}_P$. For each other $U \in \mathcal{F}_P$ we iteratively choose a point $Q \in \mathcal{P}_P$, set $f(U) = \langle U, P \rangle$, and remove the q^{k-1} points of $f(U) \backslash W$ from $\mathcal{P}_P$. Since

$$\begin{aligned} \#\{P \le V \mid \dim(P) = 1, P \not\le W\} &\ge q^{v_1-1} \\ &\overset{v_1 \ge v_2+2}{\ge} q^{v_2+1} > q^{k-1} \cdot \left[\begin{smallmatrix} v_2-k+2 \\ 1 \end{smallmatrix}\right]_q \\ &\overset{k \ge 3}{\ge} q^{k-1} \cdot \left[\begin{smallmatrix} v_2-1 \\ 1 \end{smallmatrix}\right]_q / \left[\begin{smallmatrix} k-2 \\ 1 \end{smallmatrix}\right]_q \end{aligned}$$

the sets $\mathcal{P}_P$ never get empty during the construction.

Now consider $\mathrm{d_s}(f(U), f(U'))$ for different $U, U' \in \mathcal{F}$. If U and U' are disjoint in W then $f(U)$ and $f(U')$ can share at most a point. If there exists a point P in W that is contained in U

and U', then by the construction for $\mathcal{F}_P$ the codewords $f(U)$ and $f(U')$ share no point outside W, i.e., $\Big(f(U)\cap f(U')\Big)\backslash W=\emptyset$, so that $\mathrm{d_s}(f(U),f(U'))\ge 2k-2$. □

Applying Theorem 3.2 directly gives:

Theorem 4.2.

$$A_q(v,2k-2;k)\ge A_q(m,2k-2;k)\cdot q^{2(v-m)}+A_q(v-m,2k-4;k-1)$$

for $m\ge k\ge 3$.

Let us consider two examples. For $q\ge 3$ the best known lower bound for $A_q(10,4;3)$ is obtained by the linkage construction, i.e., Inequality (3), with $m=7$. More precisely, we have $A_q(7,4;3)\ge q^8+q^5+q^4+q^2-q$ for every prime power q [13, Theorem 4]. (For $q=2,3$ better constructions are known [10, 13].) Lifting gives an extra factor of q^6 and linkage as well as improved linkage, i.e., Inequality (3) and Inequality (4), give only one additional codeword, so that

$$A_q(10,4;3)\ge\left(q^8+q^5+q^4+q^2-q\right)\cdot q^6\,+\,1=q^{14}+q^{11}+q^{10}+q^8-q^7+1.$$

Applying Theorem 4.2 with $m=7$ gives $A_q(10,4;3)\ge q^{14}+q^{11}+q^{10}+q^8-q^7+q^2+q+1$, since $A_q(3,2;2)=A_q(3,2;1)=q^2+q+1$. We remark that the lower bound $B_q(v,3,4;3)\ge q^2+q+1$, obtained from Proposition 4.1, is indeed attained with equality for all $v\ge 3$.

For $q\ge 3$ the best known lower bound for $A_q(11,6;4)$ is obtained by the so-called Echelon-Ferrers construction, see e.g. [3], which is the other construction that gives the best known lower bounds in more than half of the cases (counting ties) [9].[1] In a nutshell, for suitable pivot vectors $p_1,\dots,p_r\in\mathbb{F}_2^v$ subcodes $\mathcal{C}_i$ whose codewords all have pivot vector p_i are constructed using lifted versions of suitably restricted rank-metric codes. For the combination of these subcodes Lemma 2.1 is used. In our case the pivot vectors are given by 11110000000, 00101110000, 00011001100, 10000101010, 01000011001, 00100000111, and we have $A_q(11,6;4)\ge q^{14}+q^8+q^4+q^3+q^2+q+1$. If we apply Theorem 3.2 with $m=4$, we obtain

$$A_q(11,6;4)\ge 1\cdot q^{14}+B_q(11,7,6;4)\ge q^{14}+q^8+q^5+q^4+q^2-q.$$

We can also obtain other constructions from the literature as special cases, see the subsequent discussion.

Corollary 4.3.

(a) $A_q(v,2k-2;k)\ge q^{2(v-k)}+A_q(v-k,2k-4;k-1)$ *for* $k\ge 3$.
(b) $A_q(3k-3,2k-2;k)\ge q^{4k-6}+q^{k-1}+1$ *for* $k\ge 3$.

PROOF. For part (a) we apply Theorem 4.2 with $m=k$. Specializing to $v=3k-3$ and using $A_q(2k-3,2k-4;k-1)=A_q(2k-3,2k-4;k-2)=q^{k-1}+1$, see [1, Theorem 4.2], then gives part (b). □

With the extra condition $q^2+q+1\ge 2\lfloor v/2\rfloor-3$ part (a) is equivalent to [4, Theorem 16, Construction 1]. For e.g. $v=8$ and $k=3$ the corresponding lower bound $A_q(8,4;3)\ge q^{10}+\left[{5\atop 2}\right]_q=q^{10}+q^6+q^5+2q^4+2q^3+2q^2+q+1$ is indeed the best known lower bound for $q\ge 3$. Part (b) matches the coset construction [12, Theorem 11], which is valid for $k\ge 4$.

[1] More precisely, http://subspacecodes.uni-bayreuth.de/cdctoplist/ compares the success of different constructions for `cdcs`.

Moreover, this explicit lower bound matches the best known lower bound for $k = 4, 5, 6, 7$ and $q \ge 2$, where it is also achieved by the Echelon-Ferrers construction.

For $k = 3$ the following proposition strictly improves the previously best known lower bounds for $q \ge 4$ and $t \ge 1$.

Proposition 4.4. *For $t \ge 0$ we have*

$$\begin{aligned} A_q(7+3t, 4; 3) &\ge \left(q^8 + q^5 + q^4 + q^2 - q\right) \cdot q^{6t} + \left[{3t \atop 2} \right]_q, \\ A_q(8+3t, 4; 3) &\ge \left(q^{10} + q^6 + q^5 + 2q^4 + 2q^3 + 2q^2 + q + 1\right) \cdot q^{6t} + \left[{3t \atop 2} \right]_q, \text{ and} \\ A_q(9+3t, 4; 3) &\ge \left(q^{12} + 2q^8 + 2q^7 + q^6 + 2q^5 + 2q^4 - 2q^2 - 2q + 1\right) \cdot q^{6t} + \left[{3t \atop 2} \right]_q. \end{aligned}$$

PROOF. For $t = 0$ we have $A_q(7, 4; 3) \ge q^8 + q^5 + q^4 + q^2 - q$ [13], $A_q(8, 4; 3) \ge q^{10} + q^6 + q^5 + 2q^4 + 2q^3 + 2q^2 + q + 1$, and $A_q(9, 4; 3) \ge q^{12} + 2q^8 + 2q^7 + q^6 + 2q^5 + 2q^4 - 2q^2 - 2q + 1$ [16, Corollary 4]. For $t \ge 1$ let $a \in \{7, 8, 9\}$, $v = a + 3t$, and $m = v - 3t$, i.e., $m = a$. Applying Theorem 4.2 with $k = 3$ gives the stated formulas. □

The last two parametric inequalities also strictly improve the best known lower bounds for $q = 3$ and $t \ge 1$. Also for $k > 3$ strict improvements can be concluded from Theorem 4.2.

Proposition 4.5. *We have*

$$\begin{aligned} A_q(10, 6; 4) &\ge q^{12} + q^6 + 2q^2 + 2q + 1, \\ A_q(13, 6; 4) &\ge q^{18} + q^{12} + 2q^8 + 2q^7 + q^6 + q^5 + q^4 + 1, \text{ and} \\ A_q(14, 6; 4) &\ge q^{20} + q^{14} + q^{11} + q^{10} + q^8 - q^7 + q^2 + q + 1. \end{aligned}$$

PROOF. Since $A_q(6, 4; 3) \ge q^6 + 2q^2 + 2q + 1$, see e.g. [14, Theorem 2], we conclude $A_q(10 + 4t, 6; 4) \ge q^{12} + q^6 + 2q^2 + 2q + 1$ from Corollary 4.3.(a) setting $k = 4$. Using Proposition 4.4 we conclude the second and the third lower bound from Corollary 4.3.(a) with $k = 4$. □

The previous exemplary constructions all use Theorem 4.2 based on Proposition 4.1 (or corollaries thereof), which gives a lower bound on $B_q(v_1, v_2, d; k)$ for $d = 2k - 2$. For $d < 2k - 2$ lower bounds for $B_q(v_1, v_2, d; k)$ can also yield strict improvements for $A_q(v, d; k)$ (and $q \ge 3$).

Proposition 4.6. *We have*

$$A_q(12, 4; 4) \ge q^{24} + q^{20} + q^{19} + 3q^{18} + 2q^{17} + 3q^{16} + q^{15} + q^{14} + q^{12} + q^{10} + 2q^8 + 2q^6 + 2q^4 + q^2 + 1$$

and

$$A_q(13, 4; 4) \ge q^{27} + q^{23} + q^{22} + 3q^{21} + 2q^{20} + 3q^{19} + q^{18} + q^{17} + q^{15} + q^{12} + q^{10} + q^9 + q^8 + q^7 + q^6 + q^5 + q^3.$$

PROOF. It has been proved several times that

$$A_q(8, 4; 4) \ge q^{12} + q^8 + q^7 + 3q^6 + 2q^5 + 3q^4 + q^3 + q^2 + 1,$$

see e.g. [4, Theorem 18, Remark 6]. Using Theorem 3.2 with $m = 8$ gives

$$A_q(12, 4; 4) \ge A_q(8, 4; 4) \cdot q^{12} + B_q(12, 4, 4; 4)$$

and

$$A_q(13, 4; 4) \ge A_q(8, 4; 4) \cdot q^{15} + B_q(13, 5, 4; 4).$$

Let W be an arbitrary but fix solid, i.e., a 4-space, in $V = \mathbb{F}_q^{12}$. For each line L in W there exist $q^8 + q^6 + q^4 + q^2$ solids in V that intersect W in L and have pairwise subspace distance

$d = 4$, as we will show subsequently. To this end, consider a line spread $\mathcal{P}$ of $V/L \cong \mathbb{F}_q^{10}$. For each representative L_i of the $A_q(10, 4; 2) = q^8 + q^6 + q^4 + q^2 + 1$ elements of $\mathcal{P}$ in V we can construct the solid $\langle L_i, L\rangle$. By construction, these solids have pairwise subspace distance 4 and contain L. W.l.o.g. we can assume $\langle L_1, L\rangle = W$. Now we apply this construction for every line L of a line spread $\mathcal{P}_W$ of W of cardinality $A_q(4, 4; 2) = q^2 + 1$. Additionally adding W itself as a codeword gives $B_q(12, 4, 4; 4) \ge (q^2 + 1)(q^8 + q^6 + q^4 + q^2 + 1)$. Finally, we check that for different $L, L' \in \mathcal{P}_W$ and different L_j, L_i as defined above, we have $\dim(\langle L, L_i\rangle \cap \langle L, L_j\rangle) = 2$, $\dim(\langle L, L_i\rangle \cap \langle L', L_i\rangle) = 2$, $\dim(\langle L, L_i\rangle \cap \langle L', L_j\rangle) \le 2$, and $\dim(\langle L, L_i\rangle \cap W) \le 2$, so that the minimum subspace distance is 4.

For $B_q(13, 5, 4; 4)$ we set $V = \mathbb{F}_q^{13}$ and choose a 5-space W in V, which admits a partial line spread of cardinality $A_q(5, 4; 2) = q^3 + 1$. Again, we extend each such line L to several solids in V intersecting W only in L and having pairwise subspace distance 4. To that end, we consider a partial line spread of $V/L \cong \mathbb{F}_q^{11}$ that is disjoint from a plane π. (L and a representative of π are disjoint and generate W.) The maximum size of this partial line spread is $A_q(11, 4; 2) - 1 = q^9 + q^7 + q^5 + q^3$, so that $B_q(13, 5, 4; 4) \ge (q^3 + 1)(q^9 + q^7 + q^5 + q^3)$ using a similar distance analysis as above. (Again, we may add an additional solid contained in W as a codeword.) $\square$

We remark that the previously best known lower bound for $A_q(12, 4; 4)$ and $A_q(13, 4; 4)$ for all $q \ge 2$ is given by the improved linkage construction for $m = 8$, i.e.,

$$\begin{aligned} A_q(12,4;4) &\ge A_q(8,4;4)\cdot q^{12} + A_q(6,4;4) = A_q(8,4;4)\cdot q^{12} + A_q(6,4;2) \\ &\ge q^{24} + q^{20} + q^{19} + 3q^{18} + 2q^{17} + 3q^{16} + q^{15} + q^{14} + q^{12} + q^4 + q^2 + 1 \end{aligned}$$

and

$$A_q(13,4;4) \ge A_q(8,4;4)\cdot q^{15} + A_q(7,4;4) = A_q(8,4;4)\cdot q^{12} + A_q(7,4;2),$$

where $A_q(7, 4; 2) = q^5 + q^3 + 1$. Very recently, the lower bound for $A_q(12, 4; 4)$ was further improved in [2, Theorem 5.4].

Another case where Theorem 3.2 yields a strict improvement is $A_q(16, 6; 5)$. Here the previously best known lower bound is obtained via the (improved) linkage construction with $m = 11$, i.e.,

$$\begin{aligned} A_q(16,6;5) &\ge A_q(11,6;5)\cdot q^{15} + A_q(7,6;5) \\ &= A_q(11,6;5)\cdot q^{15} + A_q(5,6;5) = A_q(11,6;5)\cdot q^{15} + 1. \end{aligned}$$

So, we get a strict improvement if $B(16, 5, 6; 5) > 1$, which is certainly true. E.g., in a 5-space W of $V = \mathbb{F}_q^{16}$ we can choose $\left[{5 \atop 3}\right]_q = \left[{5 \atop 2}\right]_q = q^6+q^5+2q^4+2q^3+2q^2+q+1$ different planes that pairwise intersect in a point, i.e., that have subspace distance 2. In $V/W \cong \mathbb{F}_q^{11}$ we can choose a partial line spread of cardinality at least $\left[{5 \atop 2}\right]_q < q^9 < A_q(11, 4; 2)$, so that we can extend each of the planes by a disjoint line from the partial line spread to obtain $\left[{5 \atop 2}\right]_q$ 5-spaces with pairwise subspace distance $2 + 4 = 6$, i.e., $B(16, 5, 6; 5) \ge \left[{5 \atop 2}\right]_q = q^6 + q^5 + 2q^4 + 2q^3 + 2q^2 + q + 1$ and

$$A_q(16,6;5) \ge A_q(11,6;5)\cdot q^{15} + \left[{5 \atop 2}\right]_q . \tag{5}$$

5. CONCLUSION

We have generalized the linkage construction, which is one of the two most successful construction strategies for `cdcs` with large size, in our main theorem 3.2. This comes at the cost of introducing the new quantity $B_q(v_1, v_2, d; k)$. In Section 4 we have demonstrated that via this approach several parametric series of improvements for $A_q(v, d; k)$ can be obtained. For $d = 2k - 2$ we gave a general lower bound for $B_q(v_1, v_2, d; k)$ in terms of $A_q(v, d; k)$, see Proposition 4.1 and for $d < 2k - 2$ we have obtained a few lower bounds for $B_q(v_1, v_2, d; k)$ for specific instances $(v_1, v_2, d; k)$. In [19] lifted `MRD` codes have been augmented by adding an additional `cdc` $\mathcal{C}$, which is constructed via rank metric codes with bounds on the rank of the matrices. It turns out that $\mathcal{C}$ corresponds to a `cdc` that matches the requirements of Definition 3.1, i.e., the results of [19] can be reformulated as lower bounds for $B_q(v_1, v_2, d; k)$. This is remarked explicitly in [8], see also [16, Lemma 4.1].

The study of lower and upper bounds for $B_q(v_1, v_2, d; k)$ might be a promising research direction on its own. We remark that the linkage construction can also be generalized to mixed dimension codes, i.e., sets of codewords from $P(V)$ with arbitrary dimensions. However, other known constructions are superior to that approach.

ACKNOWLEDGMENT

The author would like to thank the anonymous referees of for their careful reading, very helpful remarks, suggestions, and patience, which significantly improved the presentation of this paper. One referee even improved the initial statement of Proposition 4.4 and Proposition 4.6.

REFERENCES

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

[2] A. Cossidente, S. Kurz, G. Marino, and F. Pavese. Combining subspace codes. *arXiv preprint 1911.03387*, 2019.

[3] T. Etzion and N. Silberstein. Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams. *IEEE Transactions on Information Theory*, 55(7):2909–2919, 2009.

[4] T. Etzion and N. Silberstein. Codes and designs related to lifted MRD codes. *IEEE Transactions on Information Theory*, 59(2):1004–1017, 2013.

[5] E. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.

[6] H. Gluesing-Luerssen, K. Morrison, and C. Troha. Cyclic orbit codes and stabilizer subfields. *Advances in Mathematics of Communications*, 9(2):177–197, 2015.

[7] H. Gluesing-Luerssen and C. Troha. Construction of subspace codes through linkage. *Advances in Mathematics of Communications*, 10(3):525–540, 2016.

[8] D. Heinlein. Generalized linkage construction for constant–dimension codes. *arXiv preprint 1910.11195v2*, 2019.

[9] D. Heinlein, M. Kiermaier, S. Kurz, and A. Wassermann. Tables of subspace codes. *arXiv preprint 1601.02864*, 2016.

[10] D. Heinlein, M. Kiermaier, S. Kurz, and A. Wassermann. A subspace code of size 333 in the setting of a binary q-analog of the Fano plane. *Advances in Mathematics of Communications*, 13(3):457–475, August 2019.

[11] D. Heinlein and S. Kurz. Asymptotic bounds for the sizes of constant dimension codes and an improved lower bound. In *International Castle Meeting on Coding Theory and Applications*, pages 163–191. Springer, 2017.

[12] D. Heinlein and S. Kurz. Coset construction for subspace codes. *IEEE Transactions on Information Theory*, 63(12):7651–7660, 2017.

[13] T. Honold and M. Kiermaier. On putative q-analogues of the Fano plane and related combinatorial structures. In *Dynamical systems, number theory and applications*, pages 141–175. World Sci. Publ., Hackensack, NJ, 2016.

[14] T. Honold, M. Kiermaier, and S. Kurz. Optimal binary subspace codes of length 6, constant dimension 3 and minimum subspace distance 4. In *Topics in finite fields*, volume 632 of *Contemporary Mathematics*, pages 157–176. Amer. Math. Soc., Providence, RI, 2015.

[15] R. Kötter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

[16] S. Kurz. Subspaces intersecting in at most a point. *Designs Codes and Cryptography*, to appear, arXiv preprint 1907.02728, 2019.

[17] N. Silberstein and A.-L. Trautmann. Subspace codes based on graph matchings, Ferrers diagrams, and pending blocks. *IEEE Transactions on Information Theory*, 61(7):3937–3953, 2015.

[18] D. Silva, F. Kschischang, and R. Kötter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, 2008.

[19] L. Xu and H. Chen. New constant–dimension subspace codes from maximum rank distance codes. *IEEE Transactions on Information Theory*, 64(9):6315–6319, 2018.

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