View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by EPub Bayreuth

COSET CONSTRUCTION FOR SUBSPACE CODES

DANIEL HEINLEIN AND SASCHA KURZ

Abstract. One of the main problems of the young research area of network coding is to compute good lower and upper bounds of the achievable so-called subspace codes in $\mathcal{P}_q(n)$ for a given minimal distance. Here we generalize a construction of Etzion and Silberstein to a wide range of parameters. This construction, named *coset construction*, improves several of the previously best known subspace codes and attains the MRD bound for an infinite family of parameters.

1. Introduction

Let $\mathbb{F}_q$ be the finite field of order q and V be a vector space of dimension n over $\mathbb{F}_q$. Since V is isomorphic to $\mathbb{F}_q^n$, we will assume $V = \mathbb{F}_q^n$ in the following. By $\mathcal{G}_q(n,k)$ we denote the set of all k-dimensional subspaces of $\mathbb{F}_q^n$, where $0 \le k \le n$. The *projective space* of order n over $\mathbb{F}_q$ is given by $\mathcal{P}_q(n) = \cup_{0 \le k \le n} \mathcal{G}_q(n,k)$. It is well known that

$$d_S(U,W) := \dim U + \dim W - 2\dim(U \cap W)$$

is a metric on $\mathcal{P}_q(n)$ [1]. Thus, one can define codes on $\mathcal{P}_q(n)$ and $\mathcal{G}_q(n,k)$, which are called *subspace codes* and *constant dimension codes*, respectively.[1] We say that $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is an $(n,M,d)_q$ code (in projective space) if $|\mathcal{C}| = M$ and $d(U,V) \ge d$ for all $U,V \in \mathcal{C}$. If $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ for some k, we speak of an $(n,M,d;k)_q$ code. The *minimum distance* of a code $\mathcal{C} \subseteq \mathcal{P}_q(n)$ is denoted by $D_S(\mathcal{C}) := \min_{U \ne V \in \mathcal{C}} d_S(U,V)$. One major problem is the determination of the maximum size $A_q(n,d)$ of an (n,M,d) code in $\mathcal{P}_q(n)$ and the maximum size $A_q(n,d;k)$ of an $(n,M,d;k)$ code in $\mathcal{G}_q(n,k)$. Bounds for $A_q(n,d)$ and $A_q(n,d;k)$ were heavily studied since a while, see e.g. the survey [11] or the new on-line database at `subspacecodes.uni-bayreuth.de` [13]. The aim of this paper is to describe a general construction for $(n,M,d;k)_q$ and $(n,M,d)_q$ codes that is capable to improve some of the so far best known lower bounds on $A_q(n,d;k)$. The construction, which we will call coset construction, is motivated by the construction of [10, Theorem 18].

1991 *Mathematics Subject Classification.* Primary 05B25, 51E20; Secondary 51E22, 51E23.

Key words and phrases. Constant dimension codes, subspace codes, subspace distance, Echelon-Ferrers construction.

The work of the authors was supported by the ICT COST Action IC1104 and grants KU 2430/3-1, WA 1666/9-1 – "Integer Linear Programming Models for Subspace Codes and Finite Geometry" – from the German Research Foundation.

[1] The distance function d_S is known as *subspace distance* and one of the two distance functions that can be motivated by an information-theoretic analysis of the so-called Koetter-Kschischang-Silva model [22]. The second distance function is the so-called *injection distance* $d_I(U,V) := \max\{\dim U, \dim V\} - \dim(U \cap V)$. For two subspaces of the same dimension we have $d_S(U,V) = 2d_I(U,V)$, i.e., the two metrics are equivalent on $\mathcal{G}_q(n,k)$, and $d_I(U,V) \le d_S(U,V) \le 2d_I(U,V)$ in general.

With respect to lower bounds on $A_q(n, d; k)$, an asymptotically optimal[2] construction is given by lifted maximum-rank-distance codes [22, 12]. The concept of maximum-rank-distance codes was generalized from rectangular matrices to matrices with a (structured) set of prescribed zeros in [9] and used to combine several maximum-rank-distance codes to a constant dimension code – the so-called multilevel or Echelon-Ferrers construction. Most of the best known lower bounds on $A_q(n, d; k)$ arise from this construction. However, it is rather general and involves several search spaces or optimization problems in order to be evaluated optimally. For special subclasses explicit variants of the construction and indeed explicit formulas for the sizes of the corresponding codes have been obtained, see [23]. We remark that additional refinements of the Echelon-Ferrers construction have been proposed recently, see [10, 21].

The remaining part of the paper is organized as follows. In Section 2 we collect some facts about representations of subspaces, MRD codes, parallelisms, and the Echelon-Ferrers construction. The main idea of the coset construction is described in Section 3. Since this construction has several degrees of freedom, we present some first insights on the choice of "good" parameters in Section 4. After listing some examples improving several lower bounds on $A_q(n, d; k)$ in Section 5 we draw a conclusion in Section 6.

2. Preliminaries

In this section we summarize some notation and well known insights that will be used in the later parts of the paper.

2.1. **Gaussian elimination and representations of subspaces.**

Let $A \in \mathbb{F}_q^{k\times n}$ be a matrix of (full) rank k. The row-space of A forms k-dimensional subspace of $\mathbb{F}_q^n$. The matrix A is called *generator matrix* of a given element of $\mathcal{G}_q(n, k)$. Since the application of the Gaussian elimination algorithm onto a generator matrix A does not change the row-space, we can restrict ourselves onto generator matrices which are in *reduced row echelon form* (rre), i.e., the matrix has the shape resulting from a Gaussian elimination. The representation is unique and does not depend on the elimination algorithm. This well-known connection is indeed a bijection, which we denote by $\tau : \mathcal{G}_q(n, k) \to \left\{A' \in \mathbb{F}_q^{k\times n} : \operatorname{rk}(A') = k,\ A' \text{ in rre}\right\}$. This observation is capable to easily explain many properties of $\mathcal{G}_q(n, k)$ so that we commonly identify the elements of $\mathcal{G}_q(n, k)$ with their corresponding generator matrices in reduced row echelon form.

Given a matrix $A \in \mathbb{F}_q^{k\times n}$ of full rank we denote by $p(A) \in \mathbb{F}_2^n$ the binary vector whose 1-entries coincide with the pivot columns of A. For each $v \in \mathbb{F}_2^n$ let $\mathrm{EF}_q(v)$ denote the set of all $k \times n$ matrices over $\mathbb{F}_q$ that are in reduced row echelon form with pivot columns described by v, where k is the weight of v.

Example 1. *For $v = (1, 0, 1, 1, 0)$ we have*

$$\mathrm{EF}_q(v) = \begin{pmatrix} 1 & \star & 0 & 0 & \star \\ 0 & 0 & 1 & 0 & \star \\ 0 & 0 & 0 & 1 & \star \end{pmatrix},$$

where the $\star$s represent arbitrary elements of $\mathbb{F}_q$, i.e., $|\mathrm{EF}_q(v)| = q^4$.

[2] To be more precise, the rate of transmission $\frac{\log_q |\mathcal{C}|}{n\cdot\max_{U\in\mathcal{C}} \dim(U)}$ is asymptotically optimal [15]. A rough estimation between $|\mathcal{C}|$ and the Singleton bound yields an approximation factor of at most 4.

In general we have

$$\left|\mathrm{EF}_q\Big((v_1,\dots,v_n)\Big)\right| = q^{\sum\limits_{i=1}^{n}(1-v_i)\cdot\sum\limits_{j=1}^{i} v_j}$$

and the structure of the corresponding matrices can be read off from the corresponding *(Echelon)-Ferrers diagram*[3]

$$\begin{array}{cc} \bullet & \bullet \\ & \bullet \\ & \bullet \end{array},$$

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

By summing over all binary vectors of weight k in $\mathbb{F}_2^n$ one can compute

$$|\mathcal{G}_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q := \prod_{i=1}^{k} \frac{q^{n-k+i}-1}{q^i-1},$$

where $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is called *Gaussian binomial coefficient.*

Later on we will use the inverse operation of deleting the pivot columns of a matrix in rre form:

Definition 2. *Let $B \in \mathbb{F}_q^{k\times n}$ be a full-rank matrix in rre form and $F \in \mathbb{F}_q^{k'\times(n-k)}$ be arbitrary, where $k, k', n \in \mathbb{N}$ and $k \le n$. Let further f^i denote the ith column of F. Then, $G = \varphi_B(F)$ denotes the $k' \times n$ matrix over $\mathbb{F}_q$ whose columns are given by $g^i = \mathbf{0} \in \mathbb{F}_q^{k'}$ if $v_i = 1$ and $g^i = f_{i-s_i}$ otherwise, where $(v_1,\dots,v_n) = p(B)$ and $s_i = \sum_{j=1}^{i} v_j$, for all $1 \le i \le n$.*

Example 3. *For*

$$B = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } F = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

we have $p(B) = (0,1,0,1,0,1)$ and

$$\varphi_B(F) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

2.2. **MRD codes and the Echelon-Ferrers construction.** For matrices $A, B \in \mathbb{F}_q^{m\times n}$ the *rank distance* is defined via $d_R(A,B) := \mathrm{rk}(A-B)$. It is indeed a metric, as observed in [12]. The maximum possible cardinality of a rank-metric code with given minimum rank distance is exactly determined in all cases.

Theorem 4. *(see* [12]*) Let $m, n \ge d$ be positive integers, q a prime power, and $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ be a rank-metric code with minimum rank distance d. Then, $|\mathcal{C}| \le q^{\max(n,m)\cdot(\min(n,m)-d+1)}$. Codes attaining this upper bound are called maximum-rank distance (MRD) codes. They exist for all (suitable) choices of parameters.*

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

[3] A Ferrers diagram represents partitions as patterns of dots, with the nth row having the same number of dots as the nth term s_n in the partition $n = s_1 + \dots + s_l$, where $s_1 \ge \dots \ge s_l$ and $s_i \in \mathbb{N}_{>0}$ [3]. Usually a Ferrers diagram is depicted in such a way that it is the vertically mirrored version of the above constructed (Echelon)-Ferrers diagram.

Theorem 5. *(see* [22]*) For positive integers k, d, n with $k \le n$, $d \le 2\min(k, n-k)$, and $d \equiv 0 \pmod 2$, the size of a lifted MRD code in $G_q(n,k)$ with subspace distance d is given by*

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

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

The subspace distance of two subspaces with the same pivots can be computed by the rank distance of the corresponding generator matrices.

Lemma 1. *(*[20, Corollary 3]*) Let $v \in \mathbb{F}_2^n$ and $U, W \in \operatorname{EF}_q(v)$, then $d_S(U,W) = 2 \cdot d_R\Big(\tau(U), \tau(W)\Big)$.*

So, in order to construct a $(n, M, 2\delta; k)$ code, it suffices to select a subset of $\operatorname{EF}_q(v)$ with minimum rank distance δ. Let $d_H(v,v') := |\{1 \le i \le n : v_i \ne v'_i\}|$ denote the *Hamming distance* for two binary vectors $v, v' \in \mathbb{F}_2^n$.

Lemma 2. *(*[9, Lemma 2]*) Let $v, v' \in \mathbb{F}_2^n$, $U \in \operatorname{EF}_q(v)$, and $W \in \operatorname{EF}_q(v')$, then $d_S(U,W) \ge d_H(v,v')$.*

Having Lemma 1 and Lemma 2 at hand, the Echelon-Ferrers construction from [9] works as follows: For two integers k and δ choose a binary constant weight code $\mathcal{S}$ of length n, weight k, and minimum Hamming distance 2δ as a so-called *skeleton code*. For each $s \in \mathcal{S}$ construct a code $\mathcal{C}_s \subseteq \operatorname{EF}_q(s)$ having a minimum rank distance of at least δ. Setting $\mathcal{C} = \cup_{s\in\mathcal{S}}\mathcal{C}_s$ yields a $(n, M, 2\delta; k)$ code.[4]

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

Theorem 6. *(*[9, 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 v, 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 $\dim(v,\delta)$.*

The conjecture that the upper bound of Theorem 6 can be obtained for all parameters is still unrefuted. Several of the currently best known lower bounds for constant dimension codes are obtained via the Echelon-Ferrers construction. We remark that for the special binary vector $v = (1, \ldots, 1, 0, \ldots, 0)$ of length n and weight k, the rank-metric codes of maximum cardinality in $\operatorname{EF}_q(v)$ are given by lifted MRD codes, see Theorem 5. So, the Echelon-Ferrers construction uses building blocks that can be seen as generalizations of MRD codes. For the other direction, it is possible to improve the best currently known upper bounds on $A_q(n, d; k)$ for constant dimension codes that contain the lifted MRD code.

Theorem 7. *(see* [10, Theorem 10 and 11]*) Let $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, where $n \ge 2k$, with minimum subspace distance d that contains the lifted MRD code.*

- *If $d = 2(k-1)$ and $k \ge 3$, then $|\mathcal{C}| \le q^{2(n-k)} + A_q(n-k, 2(k-2); k-1)$;*
- *if $d = k$, where k is even, then $|\mathcal{C}| \le q^{(n-k)(k/2+1)} + \begin{bmatrix} n-k \\ k/2 \end{bmatrix}_q \frac{q^n - q^{n-k}}{q^k - q^{k/2}} + A_q(n-k, k; k)$.*

[4] We remark that Lemma 2 does not need two binary vectors v, v' of the same weight, i.e., the very same approach can be used to construct subspace codes. The only necessary modification is to choose a general binary code $\mathcal{S}$ of length n and minimum Hamming distance d as skeleton code. The codes $\mathcal{C}_s$ need to have a rank distance of at least $d/2$. For the parameters $q = 2$, $n = 8$, and $d = 3$ this constructions yields a $(8, 4907, 3)$ code.

2.3. **Parallelisms and packings of $\mathcal{G}_q(n,k)$.** Let X be a set. A *packing* $P = \{P_1, \dots, P_l\}$ of X is a set of subsets $P_i \subseteq X$ such that $P_i \cap P_j = \emptyset$ for all $1 \le i < j \le l$, i.e., the subsets P_i are pairwise disjoint. A *spread* is a subset of $\mathcal{G}_q(n,k)$ that partitions the corresponding set of points, i.e., the elements have a pairwise trivial intersection. Counting the points yields that the size of a spread is $\frac{\left[{n \atop 1}\right]_q}{\left[{k \atop 1}\right]_q} = \frac{q^n-1}{q^k-1}$. A spread is a special constant dimension code with subspace distance $d = 2 \cdot k$. Spreads exist if and only if k divides n, see [2]. With this, a *parallelism* in $\mathcal{G}_q(n,k)$ is a packing of spreads such that it partitions $\mathcal{G}_q(n,k)$.

Parallelisms in $\mathcal{G}_q(n,k)$ are known to exist for:

(1) $q = 2, k = 2$ and n even;
(2) $k = 2$, all q and $n = 2^m$ for $m \ge 2$;
(3) $n = 4$, $k = 2$, and $q \equiv 2 \pmod 3$;
(4) $q = 2, k = 3, n = 6$,

see e.g. [11].

3. The coset construction

The main idea of the coset construction is to use a collection of codewords having a generator matrix of the form

$$\begin{pmatrix} A & \varphi_B(F) \\ 0 & B \end{pmatrix},$$

where the matrices A, B, and F come from certain sets that are combined in such a way that the resulting subspace code has a large minimum subspace distance. In this subspace, the vectors have the shape $(\lambda \cdot A, \lambda \cdot F + \mu \cdot B)$. So $\lambda \cdot F$ is the offset for the coset of the suffixes, i.e., the vector $\lambda \cdot A$ is prefix for every vector in the coset $\lambda \cdot F + B$.

Lemma 3. *(Coset construction) Let q be a prime power and $n, k, n', k' \in \mathbb{N}$ satisfy $1 \le k \le n/2$, $1 \le k' \le n'$, and $1 \le k - k' \le n - n'$. Let further $\mathcal{A} = \dot\cup_{1 \le i \le l} \mathcal{A}_i$, $\mathcal{B} = \dot\cup_{1 \le i \le l} \mathcal{B}_i$, where $\emptyset \ne \mathcal{A}_i \subseteq \mathcal{G}_q(n',k')$ and $\emptyset \ne \mathcal{B}_i \subseteq \mathcal{G}_q(n-n',k-k')$ for all $1 \le i \le l$, and $\overline{F} \subseteq \mathbb{F}_q^{k' \times (n-n'-k+k')}$. With this, we have that $\mathcal{C}\left((\mathcal{A}_i)_i, (\mathcal{B}_i)_i, \overline{F}\right) :=$*

$$\left\{\tau^{-1}\left(\begin{smallmatrix} A & \varphi_B(F) \\ 0 & B \end{smallmatrix}\right) \,:\, \tau^{-1}(A) \in \mathcal{A}_i, \tau^{-1}(B) \in \mathcal{B}_i, 1 \le i \le l, F \in \overline{F}\right\}$$

is a subset of $\mathcal{G}_q(n,k)$, i.e., a constant dimension code where the codewords have dimension k.

Proof. For an arbitrary but fixed index $1 \le i \le l$ let A, B be matrices with $\tau^{-1}(A) \in \mathcal{A}_i$ and $\tau^{-1}(B) \in \mathcal{B}_i$. We can easily check that $A \in \mathbb{F}_q^{k' \times n'}$ is a full-rank matrix in rre form. Similarly, $B \in \mathbb{F}_q^{(k-k') \times (n-n')}$ is a full-rank matrix in rre form. For each matrix $F \in \overline{F}$ we have $F \in \mathbb{F}_q^{k' \times (n-n'-k+k)}$, so that $\varphi_B(F) \in \mathbb{F}_q^{k' \times (n-n')}$. The dimensions fit so that

$$M := \begin{pmatrix} A & \varphi_B(F) \\ 0 & B \end{pmatrix} \in \mathbb{F}_q^{k \times n}.$$

Moreover $\varphi_B(F)$ has zero columns at the positions of the pivot columns of B. Since A has k' and B has $k - k'$ pivot columns, M has exactly k pivot columns and full rank. Thus, $\tau^{-1}(M) \in \mathcal{G}_q(n,k)$. □

The number l of disjoint subsets for $\mathcal{A}$ and $\mathcal{B}$ is called the *length* of the specific coset construction. We remark that we have excluded the ranges for the parameters k', n' where the construction would be degenerated in the sense that either A or B have to be empty matrices. Nevertheless, the degenerated case $k' = k$ has a nice interpretation. Here B is an empty matrix and A is a $k \times n'$ matrix. If additionally $n' = k$ then A is an identity matrix and we are in the case of lifted MRD codes.

Lemma 4. *Let q, n, k, n', k' be parameters satisfying the conditions from Lemma 3, $A, A' \in \mathbb{F}_q^{k' \times n'}$ and $B, B' \in \mathbb{F}_q^{(k-k')\times(n-n')}$ be full-rank matrices in rre form. Let further d be a positive integer and $F, F' \in \mathbb{F}_q^{k' \times (n-n'-k+k')}$. If*

$$d_S(\tau^{-1}(A), \tau^{-1}(A')) + d_S(\tau^{-1}(B), \tau^{-1}(B')) \geq d \tag{1}$$

or $d_R(F, F') \geq d/2$ then

$$d_S\left(\tau^{-1}\begin{pmatrix} A & \varphi_B(F) \\ 0 & B \end{pmatrix}, \tau^{-1}\begin{pmatrix} A' & \varphi_{B'}(F') \\ 0 & B' \end{pmatrix}\right) \geq d.$$

Proof. For $U, V \in \mathcal{G}_q(n, k)$ we have

$$d_S(U, V) = 2(\dim(U + V) - k) = 2\left(\operatorname{rk}\begin{pmatrix} U \\ V \end{pmatrix} - k\right).$$

Assuming $A = A'$ and $B = B'$ we conclude

$$\begin{aligned}
& d_S\left(\tau^{-1}\left(\begin{pmatrix} A & \varphi_B(F) \\ 0 & B \end{pmatrix}\right), \tau^{-1}\left(\begin{pmatrix} A & \varphi_B(F') \\ 0 & B \end{pmatrix}\right)\right) \\
= \;& 2\left(\operatorname{rk}\begin{pmatrix} A & \varphi_B(F) \\ 0 & B \\ A & \varphi_B(F') \\ 0 & B \end{pmatrix} - k\right) \\
= \;& 2\left(\operatorname{rk}\begin{pmatrix} A & 0 \\ 0 & \varphi_B(F') - \varphi_B(F) \\ 0 & B \end{pmatrix} - k\right) \\
= \;& 2\left(\operatorname{rk}(A) + \operatorname{rk}\begin{pmatrix} \varphi_B(F') - \varphi_B(F) \\ B \end{pmatrix} - k\right)
\end{aligned}$$

Since the pivot columns of B in $\varphi_B(F') - \varphi_B(F)$ consists solely of zeros, we have

$$\begin{aligned}
& 2\left(\operatorname{rk}(A) + \operatorname{rk}\begin{pmatrix} \varphi_B(F') - \varphi_B(F) \\ B \end{pmatrix} - k\right) \\
= \;& 2(\operatorname{rk}(A) + \operatorname{rk}(\varphi_B(F') - \varphi_B(F)) + \operatorname{rk}(B) - k) \\
= \;& 2(k' + \operatorname{rk}(F' - F) + k - k' - k) \\
= \;& 2\operatorname{rk}(F' - F) = 2d_R(F, F').
\end{aligned}$$

For $A \neq A'$ or $B \neq B'$ we similarly conclude

$$\begin{aligned}
& d_S\left(\tau^{-1}\left(\begin{pmatrix} A & \varphi_B(F) \\ 0 & B \end{pmatrix}\right), \tau^{-1}\left(\begin{pmatrix} A' & \varphi_{B'}(F') \\ 0 & B' \end{pmatrix}\right)\right) \\
= \;& 2\left(\operatorname{rk}\begin{pmatrix} A & \varphi_B(F) \\ 0 & B \\ A' & \varphi_{B'}(F') \\ 0 & B' \end{pmatrix} - k\right) \qquad (2) \\
\geq \;& 2\left(\operatorname{rk}\begin{pmatrix} A \\ A' \end{pmatrix} + \operatorname{rk}\begin{pmatrix} B \\ B' \end{pmatrix} - k\right),
\end{aligned}$$

using the fact that $\operatorname{rk}\begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} \geq \operatorname{rk}(X) + \operatorname{rk}(Z)$ with equality if Y is zero and swapping rows or columns, respectively, does not change the rank. We continue with

$$\begin{aligned} & 2\left(\operatorname{rk}\begin{pmatrix}A\\A'\end{pmatrix}+\operatorname{rk}\begin{pmatrix}B\\B'\end{pmatrix}-k\right), \\ = \quad & 2\left(\frac{d_S(A,A')}{2}+k'+\frac{d_S(B,B')}{2}+k-k'-k\right) \\ = \quad & d_S(A,A')+d_S(B,B'). \end{aligned}$$

□

We remark that condition (1) of Lemma 4 is trivially satisfied for the special case of distance $d = 4$.

Next we demonstrate that the coset construction from Lemma 3 can in general not be obtained by an application of the Echelon-Ferrers construction. It is easy to construct a family of examples with subspace distance d but whose pivot vectors have Hamming distance 2, so that they cannot be used in the Echelon-Ferrers construction. To this end, let q be an arbitrary prime power, d an even integer ≥ 2, and $n, k, n', k' \in \mathbb{N}$ such that $\frac{d}{4} \leq k', n'-k', k-k', n-n'-k+k'$. For the sake of this example we use:

$$\begin{aligned} A_1 &:= \begin{pmatrix} I_{k'-1} & 0 & M & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \\ A_2 &:= \begin{pmatrix} I_{k'-1} & 0 & M+N & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ B_1 &:= \begin{pmatrix} I_{k-k'} & M' \end{pmatrix} \\ B_2 &:= \begin{pmatrix} I_{k-k'} & M'+N' \end{pmatrix} \end{aligned}$$

with arbitrary matrices $M, N \in \mathbb{F}_q^{(k'-1)\times(n'-k'-1)}$ of full rank[5], $M', N' \in \mathbb{F}_q^{(k-k')\times(n-n'-k+k')}$, where $I_\star$ denotes the identity matrix. Then, for arbitrary $F_1, F_2 \in \mathbb{F}_q^{k'\times(n-n'-k+k')}$:

$$d_H\left(p\left(\begin{pmatrix}A_1 & F_1\\0 & B_1\end{pmatrix}\right), p\left(\begin{pmatrix}A_2 & F_2\\0 & B_2\end{pmatrix}\right)\right) = 2$$

but

$$\begin{aligned} & d_S\left(\begin{pmatrix}A_1 & F_1\\0 & B_1\end{pmatrix}, \begin{pmatrix}A_2 & F_2\\0 & B_2\end{pmatrix}\right) \\ & \geq 2\left(\operatorname{rk}\begin{pmatrix}A_1\\A_2\end{pmatrix}+\operatorname{rk}\begin{pmatrix}B_1\\B_2\end{pmatrix}-k\right) \\ & = 2((k'+1+\operatorname{rk}(N))+(k-k'+\operatorname{rk}(N'))-k) \\ & = 2(1+\min\{k', n'-k'\}+ \\ & \quad \min\{k-k', n-n'-k+k'\}) \geq d. \end{aligned}$$

3.1. **A multilevel coset construction.** In this subsection we want to use the coset construction in combinations with other construction. At first we show that it is compatible with the Echelon-Ferrers construction.

Lemma 5. *Let $U \in \mathcal{G}_q(n', k')$, $V \in \mathcal{G}_q(n-n', k-k')$, $F \in \mathbb{F}_q^{k'\times(n-n')}$, and $X \in \mathcal{G}_q(n, \tilde{k})$. Let s be the sum of the first n' entries in the pivot vector $p(X)$ of X, i.e., $s := \sum_{i=1}^{n'} p(X)_i$. If $d \leq |s-k'| + \left|\tilde{k}-s-k+k'\right|$ then $d_S(X, W) \geq d$, where*

$$W = \tau^{-1}\left(\begin{pmatrix}\tau(U) & \varphi_{\tau(V)}(F)\\ 0 & \tau(V)\end{pmatrix}\right).$$

[5] I.e. $\operatorname{rk}(N) = \min\{k'-1, n'-k'-1\}$, and $\operatorname{rk}(N') = \min\{k-k', n-n'-k+k'\}$.

Proof. Let $x := p(X)$ and $w := p(W)$ the pivot vectors of X and W, respectively. From the construction we know $\sum_{i=1}^{n'} x_i = s$, $\sum_{i=1}^{n'} w_i = k'$, $\sum_{i=n'+1}^{n} x_i = \tilde{k} - s$, and $\sum_{i=n'+1}^{n} w_i = k - k'$, so that

$$d_H(x, w) \geq |s - k'| + \left|(\tilde{k} - s) - (k - k')\right| \geq d.$$

Applying Lemma 2 yields the stated lower bound on the subspace distance. □

For the special case $\tilde{k} = k$, i.e., the constant dimension case, we have $|s - k'| + \left|\tilde{k} - s - k + k'\right| = 2 \cdot |s - k'|$. There is also an easy-to-check sufficient criterion whether the union of two codes constructed by the coset construction have a subspace distance of at least d.

Lemma 6. *Let $\mathcal{C}_i$ be codes having subspace distance at least d and that are obtained from the coset construction with suitable parameters n, k_i, n_i', and k_i' for $i = 1, 2$, where we assume $k_1 \leq k_2$. Let $f(m) = |m - k_1'| + |m - \gamma|$ and*

$$K = \left\{\underline{\beta}, \overline{\beta}, \gamma\right\} \cap \left[\,\underline{\beta}, \overline{\beta}\,\right],$$

where $\underline{\beta} = \max\{k_2' - k_2 + k_1, 0\}$, $\overline{\beta} = \min\{k_1, k_2'\}$, and $\gamma = k_1' + k_2 - k_1$. If $d \leq \min_{m \in K} f(m)$, then $D_S(\mathcal{C}_1 \cup \mathcal{C}_2) \geq d$.

Proof. At first we observe that we have $d_H(u, v) \geq |a - b|$ for $u, v \in \mathbb{F}_2^n$ with $\|u\|_1 = a$ and $\|v\|_1 = b$.

We set $x := p(W_1)$ and $y := p(W_2)$, where W_i are matrices corresponding to an arbitrary but fixed codeword from $\mathcal{C}_i$ each, see the formulation of Lemma 5. Let x^1 consist of the first k_1 entries of x, y^1 consist of the first k_1 entries of y, x^2 consist of the last $n - k_1$ entries of x, and y^2 consist of the last $n - k_1$ entries of y. with $m := \|y^1\|_1$, where

$$\underline{\beta} = \max\{k_2' - k_2 + k_1, 0\} \leq m \leq \min\{k_1, k_2'\} = \overline{\beta},$$

we have $d_H\left(x^1, y^1\right) \geq |m - k_1'|$ and $d_H\left(x^2, y^2\right) \geq |m - \gamma|$. Thus $f(m) \leq d_H(x, y)$ is minimized for one of the values $m \in K$. Applying Lemma 2 yields the stated lower bound on the subspace distance. □

We remark that Lemma 6 is best possible in the sense that the estimations on the Hamming distance of two binary vectors with known weights and weights of two suffixes, of possibly different lengths, is tight. Performing similar analyses on generalized structures like

$$\begin{pmatrix} A & \varphi_B(F) & \varphi_C(G) \\ 0 & B & \varphi_C(H) \\ 0 & 0 & C \end{pmatrix}$$

may have the potential to yield stronger bounds.

4. Optimal choices for the parameters of the coset construction

The coset construction from the previous section is far from being explicit, i.e., there are several degrees of freedom. The cardinality of a subspace code obtained from the coset construction with length l is given by

$$\left|\mathcal{C}\left((\mathcal{A}_i)_i, (\mathcal{B}_i)_i, \overline{F}\right)\right| = \left|\overline{F}\right| \cdot \overbrace{\sum_{i=1}^{l} |\mathcal{A}_i| \cdot |\mathcal{B}_i|}^{\Lambda :=}. \qquad (3)$$

Given q, n, and the desired even subspace distance d, the aim is to maximize (3) under the restrictions of Lemma 4. Obviously, this term is maximal if both $\left|\overline{F}\right|$

and the sum are maximal. Thus, we may choose an MRD code, with appropriate parameters, for $\overline{F}$, so that

$$|\overline{F}| = \left\lceil q^{\max\{k',n-n'-k+k'\}\cdot(\min\{k',n-n'-k+k'\}-d/2+1)}\right\rceil$$

in the optimum, see Theorem 4.

The sets $\mathcal{A}_i$ and $\mathcal{B}_i$ need to have additional structure.

Lemma 7. *For a code obtained from the construction of Lemma 3 with* $d := D_S\Big(\mathcal{C}\big((\mathcal{A}_i)_i, (\mathcal{B}_i)_i, \overline{F}\big)\Big)$*, length* l*, and parameters* q, n, k, n', k' *we have* $D_S(\mathcal{A}_i) \ge d$ *and* $D_S(\mathcal{B}_i) \ge d$ *for all* $1 \le i \le l$.

Proof. If $U \neq U' \in \mathcal{A}_i$, then there exists $V \in \mathcal{B}_i$ such that Condition (1) yields $d \le d_S(U,U') + d_S(V,V) = d_S(U,U')$. A similar conclusion can be drawn for the elements in $\mathcal{B}_i$. □

From this we can conclude an upper bound on Λ.

Corollary 1. *Using the notation from Lemma 3 and Equation (3) we have*

$$\Lambda \le \min\left\{ \begin{bmatrix} n' \\ k' \end{bmatrix}_q \cdot A_q(n-n', d; k-k'), \begin{bmatrix} n-n' \\ k-k' \end{bmatrix}_q \cdot A_q(n', d; k') \right\}.$$

Proof. Due to Lemma 7 we have $|\mathcal{A}_i| \le A_q(n', d; k')$, so that

$$\sum_{i=1}^{l} |\mathcal{A}_i| \cdot |\mathcal{B}_i| \le A_q(n', d; k') \cdot \sum_{i=1}^{l} |\mathcal{B}_i| \le A_q(n', d; k') \cdot \begin{bmatrix} n-n' \\ k-k' \end{bmatrix}_q.$$

Interchanging the roles of the $\mathcal{A}_i$ and $\mathcal{B}_i$ yields the other stated upper bound. □

Corollary 2. *The upper bound of Corollary 1 can be attained if* $d \le 4$ *and both* $\mathcal{G}_q(n', k')$ *and* $\mathcal{G}_q(n-n', k-k')$ *admit parallelisms.*

The dependency between the cardinalities of the $\mathcal{A}_i$ and $\mathcal{B}_i$ in optimal solutions of (3) is already decoupled to some extend, but we can even do more.

Lemma 8. *For a code obtained from the construction of Lemma 3 with* $d := D_S\Big(\mathcal{C}\big((\mathcal{A}_i)_i, (\mathcal{B}_i)_i, \overline{F}\big)\Big)$*, length* l*, and parameters* q, n, k, n', k'*, there exists an integer* d'[6] *such that* $D_S(\mathcal{A}) \ge d'$ *and* $D_S(\mathcal{B}) \ge d - d'$*, where* $\mathcal{A} = \cup_i \mathcal{A}_i$ *and* $\mathcal{B} = \cup \mathcal{B}_i$.

Proof. Let $U, U' \in \mathcal{A}$ with $d_S(U,U') = D_S(\mathcal{A}) =: d'$ and $V, V' \in \mathcal{B}$ with $d_S(V,V') = D_S(\mathcal{B}) =: d''$. Choosing $F = F' = \mathbf{0}$[7] we can conclude $d'' \ge d - d'$ from Inequality (1). □

Lemma 9. *For a code obtained from the construction of Lemma 3 with* $d := D_S\Big(\mathcal{C}\big((\mathcal{A}_i)_i, (\mathcal{B}_i)_i, \overline{F}\big)\Big)$*, length* l*, and parameters* q, n, k, n', k'*, then for each permutation* $\beta : \{1, \ldots, l\} \to \{1, \ldots, l\}$ *we have* $D_S\Big(\mathcal{C}\big((\mathcal{A}_i)_i, \big(\mathcal{B}_{\beta(i)}\big)_i, \overline{F}\big)\Big) = d$.

Proof. Apply Lemma 4. □

The question which permutation β of Lemma 9 maximizes the crucial parameter Λ can be answered easily.

[6] In later applications we will commonly assume $2 \le d' \le d-2$, since the other values lead to trivial cases where either $|\mathcal{A}| = 1$ or $|\mathcal{B}| = 1$.

[7] W.l.o.g. we can also assume that $\overline{F}$ contains the zero matrix, since the rank distance is invariant with respect to translations.

Lemma 10. *Let $a_1 \ge \cdots \ge a_l$ and $b_1 \ge \cdots \ge b_l$ positive integers. For each permutation $\beta : \{1,\dots,l\} \to \{1,\dots,l\}$, we have*

$$\sum_{i=1}^{l} a_i \cdot b_i \ge \sum_{i=1}^{l} a_i \cdot b_{\beta(i)}.$$

Proof. For integers $a > a'$ and $b < b'$ we have

$$(ab + a'b') - (ab' + a'b) = (a - a') \cdot (b - b') < 0.$$

□

Having these ingredients at hand we can generalize and improve the upper bound from Corollary 1 resting on the analytical solution of another optimization problem.

Lemma 11. *Let α, β, $\overline{\alpha}$, $\overline{\beta}$, and l be positive integers with $\alpha, \beta \ge l$. An optimal solution of the non-linear integer programming problem*

$$\begin{array}{rlrl} & \max \sum_{i=1}^{l} a_i \cdot b_i & & \\ & \sum_{i=1}^{l} a_i \le \alpha & & \sum_{i=1}^{l} b_i \le \beta \\ 1 \le a_i \le \overline{\alpha} & \forall 1 \le i \le l & 1 \le b_i \le \overline{\beta} & \forall 1 \le i \le l \\ a_i, b_i \in \mathbb{Z} & \forall 1 \le i \le l & & \end{array}$$

is given by

1. *$a_i^\star = \overline{\alpha}$, $b_i^\star = \overline{\beta}$ for all $1 \le i \le l$ if $\overline{\alpha} \cdot l \le \alpha$ and $\overline{\beta} \cdot l \le \beta$;*
2. *$a_i^\star = \overline{\alpha}$, $b_i^\star = 1 + \min\{\overline{\beta} - 1, \max\{0, \beta - l - (i-1) \cdot \big(\overline{\beta} - 1\big)\}$ for all $1 \le i \le l$ if $\overline{\alpha} \cdot l \le \alpha$ and $\overline{\beta} \cdot l > \beta$;*
3. *$a_i^\star = 1 + \min\{\overline{\alpha} - 1, \max\{0, \alpha - l - (i-1) \cdot (\overline{\alpha} - 1)\}$, $b_i^\star = \overline{\beta}$ for all $1 \le i \le l$ if $\overline{\alpha} \cdot l > \alpha$ and $\overline{\beta} \cdot l \le \beta$;*
4. *$a_i^\star = 1 + \min\{\overline{\alpha} - 1, \max\{0, \alpha - l - (i-1) \cdot (\overline{\alpha} - 1)\}$, $b_i^\star = 1 + \min\{\overline{\beta} - 1, \max\{0, \beta - l - (i-1) \cdot \big(\overline{\beta} - 1\big)\}$ for all $1 \le i \le l$ if $\overline{\alpha} \cdot l > \alpha$ and $\overline{\beta} \cdot l > \beta$.*

Proof. W.l.o.g. we can additionally assume $a_1 \ge \cdots \ge a_l$ and $b_1 \ge \cdots \ge b_l$ without decreasing the maximal target value of the optimization problem. Let us allow $a_i, b_i \in \mathbb{R}$ for a moment, i.e., we consider the standard relaxation, and denote a corresponding optimal solution by $\tilde{a}_i$, $\tilde{b}_i$.

For real numbers $a' \ge a''$ and $b' \ge b''$ we have

$$(a'b' + a''b'') - 2 \cdot \frac{a' + a''}{2} \cdot \frac{b' + b''}{2} = \frac{(a' - a'') \cdot (b' - b'')}{2} \ge 0,$$

so that we can assume $\tilde{a}_i = \tilde{a}_j =: \tilde{a}$ and $\tilde{b}_i = \tilde{b}_j =: \tilde{b}$, for all $1 \le i, j \le l$, w.l.o.g.

Either we have $l\tilde{a} = \alpha$ or $\tilde{a} = \overline{\alpha}$, since otherwise we could slightly increase $\tilde{a}$ and improve the target value. The same reasoning applies to $\tilde{b}$.

If $\tilde{a} = \overline{\alpha}$ and $\tilde{b} = \overline{\beta}$, then we are in case (1). Next we consider the case where $\tilde{a} = \overline{\alpha}$ and $\tilde{b} < \overline{\beta}$ so that $\tilde{b} = \beta / l$. Since $\sum_{i=1}^{l} b_i \overline{\alpha} = \overline{\alpha} \cdot \sum_{i=1}^{l} b_i$ it suffices to determine integers $1 \le b_i^\star \le \overline{\beta}$ with $\sum_{i=1}^{l} b_i^\star = \beta$. This is done in the formula of case (2). The underlying idea is the following: Start with $b_i^\star = 1$ for all $1 \le i \le l$; observe $\beta \ge l$. Then fill up the $b_i^\star$ with increasing indices up to $\overline{\beta}$ as long as the sum does not violate β. Case (3) describes the symmetric situation. It remains to assume $\overline{\alpha} \cdot l > \alpha$ and $\overline{\beta} \cdot l > \beta$. Let $\hat{a}_i$, $\hat{b}_i$ be an optimal solution of our initial optimization problem where we assume $\hat{a}_1 \ge \cdots \ge \hat{a}_l$ and $\hat{b}_1 \ge \cdots \ge \hat{b}_l$. Let further f be the smallest index such that $\hat{a}_f < \overline{\alpha}$ and r be the largest index such that

$\hat{a}_r > 1$. If either f, r does not exist or $f = r$, then the solution $\hat{a}_i$ has the shape described in case (4). But, for $f < r$ we could improve the target value by

$$(\hat{a}_f + 1) \cdot \hat{b}_f + (\hat{a}_r - 1) \cdot \hat{b}_r - \hat{a}_f \cdot \hat{b}_f - \hat{a}_r \cdot \hat{b}_r = \hat{b}_f - \hat{b}_r \geq 0,$$

so that we may assume that this case does not occur. The same reasoning applies for the $\hat{b}_i$. □

Lemma 12. *Using the notation from Lemma 3 and Equation (3) we have*

$$\Lambda \leq \max_{d' \in 2\mathbb{Z}\,:\, 0<d'<d} \quad \max_{1 \leq l \leq \min\{A_q(n',d';k'), A_q(n-n',d-d';k-k')\}} \sum_{i=1}^{l} a_i \cdot b_i,$$

where the a_i, b_i are given by Lemma 11 for

$$\begin{aligned} \alpha &= A_q(n', d'; k'), \\ \beta &= A_q(n-n', d-d'; k-k'), \\ \overline{\alpha} &= A_q(n', d; k'), \\ \overline{\beta} &= A_q(n-n', d; k-k'). \end{aligned}$$

Proof. From Lemma 8 we conclude $|\mathcal{A}| \leq A_q(n', d'; k')$ and $|\mathcal{B}| \leq A_q(n - n', d - d'; k - k')$. The possible values for the length l are part of the stated optimization formulation. For each index $1 \leq i \leq l$ we have $|\mathcal{A}_i| \leq A_q(n', d; k')$ and $|\mathcal{B}_i| \leq A_q(n - n', d; k - k')$ due to Lemma 7. It remains to check that we can apply Lemma 11. □

Fixing the parameter d' from Lemma 8 one can state a lower bound on the maximal value of Λ.

Lemma 13. *Let $d' \in 2\mathbb{Z}$ with $2 \leq d' \leq d - 2$, then we have*

$$\Lambda \geq M(q, k', n', d) \cdot M(q, k - k', n - n', d) \cdot l$$

with

$$l = \min\left\{ \frac{M(q, k', n', d')}{M(q, k', n', d)}, \frac{M(q, k - k', n - n', d - d')}{M(q, k - k', n - n', d)} \right\}.$$

for, with respect to Lemma 3, feasible parameters q, n, k, n', k', d.

Proof. Similar to the proof of [10, Lemma 5], we consider $\mathcal{A}$ as an MRD code with parameters $k' \times n'$ with distance d' and $\mathcal{B}$ as an MRD with parameters $(k - k') \times (n - n')$ with distance $d - d'$. Let $\mathcal{S}_{\mathcal{A}}$ be an MRD code with parameters $k' \times n'$ with distance $d > d'$ and $\mathcal{S}_{\mathcal{B}}$ be an MRD code with parameters $(k - k') \times (n - n')$ with distance $d > d - d'$. We choose the $\mathcal{A}_i$ as the cosets of $\mathcal{S}_{\mathcal{A}}$ in $\mathcal{A}$ and $\mathcal{B}_i$ as the cosets of $\mathcal{S}_{\mathcal{B}}$ in $\mathcal{B}$. For $\mathcal{S}_{\mathcal{A}}$ there are exactly $\frac{M(q,k',n',d')}{M(q,k',n',d)}$ cosets and for $\mathcal{S}_{\mathcal{B}}$ there are exactly $\frac{M(q,k-k',n-n',d-d')}{M(q,k-k',n-n',d)}$ cosets. Since $d_R(A + C, B + C) = d_R(A, B)$ for all suitable matrices $A, B, C \in \mathbb{F}_q^{s \times t}$, we have $D_S(\mathcal{A}_i), D_S(\mathcal{B}_i) \geq d$ for all $1 \leq i \leq l$. □

Combining a lifted MRD code with a code constructed from Lemma 13 yields an $(9, 1032, 6; 4)_2$ code, which improves the previously best known codes, see Subsection 5.2.

We can formulate the following greedy-type algorithm to construct sequences $\mathcal{A}_i$ and $\mathcal{B}_i$ that yield a "reasonable" lower bound on Λ.

Algorithm 8.

```
$\mathcal{R}_{\mathcal{A}} = \mathcal{G}_q(n', k')$
$i = 0$
```

```
while $\mathcal{R}_{\mathcal{A}} \neq \emptyset$:
    $i = i + 1$
    select constant dimension code $\mathcal{A}_i$ of maximum
    cardinality in $\mathcal{R}_{\mathcal{A}}$ with $D_S(\mathcal{A}_i) \ge d$
    $\mathcal{R}_{\mathcal{A}} = \mathcal{R}_{\mathcal{A}} \setminus \{V \mid D_S(\mathcal{A}_i \cup \{V\}) \le d' - 1\}$
$l_{\mathcal{A}} = i$
$\mathcal{R}_{\mathcal{B}} = \mathcal{G}_q(n - n', k - k')$
$i = 0$
while $\mathcal{R}_{\mathcal{B}} \neq \emptyset$:
    $i = i + 1$
    select constant dimension code $\mathcal{B}_i$ of maximum
    cardinality in $\mathcal{R}_{\mathcal{B}}$ with $D_S(\mathcal{B}_i) \ge d$
    $\mathcal{R}_{\mathcal{B}} = \mathcal{R}_{\mathcal{B}} \setminus \{V \mid D_S(\mathcal{B}_i \cup \{V\}) \le d - d' - 1\}$
$l_{\mathcal{B}} = i$
$l = \min\{l_{\mathcal{A}}, l_{\mathcal{B}}\}$
```

Unfortunately, this algorithm is not capable of determining the optimal Λ in general. If we use

$$\begin{aligned} E \quad := \quad & \{\text{all constant dimension codes in } \mathcal{G}_q(\tilde{n}, \tilde{k}) \\ & \text{with subspace distance } d\} \end{aligned}$$

as ground set and $I := \{\text{disjoint subsets of } E\}$ as independent sets, then this forms no *matroid* and hence greedy will not yield an optimal solution in general, see e.g. [7]. To be more precise, the independent set exchange property fails: Use for example $U \neq V \in \mathcal{G}_q(\tilde{n}, \tilde{k})$ with $d_S(U, V) \ge d$, $A := \{\{U\}, \{V\}\} \in I$ and $B := \{\{U, V\}\} \in I$. Although A is larger than B we cannot add an element of A to B without losing the independence.

4.1. **Decomposing constant dimension codes.** Due to Lemma 8 we can construct the necessary parts of the coset construction of Lemma 3 starting from constant dimension codes $\mathcal{A}$ and $\mathcal{B}$ with $D_S(\mathcal{A}) \ge d'$ and $D_S(\mathcal{B}) \ge d - d'$. The aim is to partition the codewords of $\mathcal{A}$ into subcodes $\mathcal{A}_i$ for $1 \le i \le l_{\mathcal{A}}$ in such a way that $D_S(\mathcal{A}_i) \ge d$. Simultaneously, we aim to partition the codewords of $\mathcal{B}$ into subcodes $\mathcal{B}_i$ for $1 \le i \le l_{\mathcal{B}}$ in such a way that $D_S(\mathcal{B}_i) \ge d$. Setting the length l of the coset construction to $l := \min\{l_{\mathcal{A}}, l_{\mathcal{B}}\}$, we observe that trying to maximize the cardinalities $|\mathcal{A}_i|$ or $|\mathcal{B}_i|$ for $i > l$ has no benefit, so that we may simply complete a given packing by singletons. Or, in other words, we directly start from packings within $\mathcal{A}$ and $\mathcal{B}$.

However, the design of suitable $\mathcal{A}_i$ is not that obvious since the Λ-part of the target function (3) comprises a non-linear integer optimization problem. Ignoring almost all of the geometric restrictions from $\mathcal{P}_q(n)$, we are able to exactly solve the mentioned optimization problem in Lemma 11. In general this gives us an upper bound only. To obtain tighter bounds one has to go a bit more into the details. In Lemma 12 we have only used the implication $|\mathcal{A}_i| \le A_q(n', d; k')$ from $D_S(\mathcal{A}_i) \ge d$, which is valid for all $\cup_{i=1}^{l} \mathcal{A}_i \subseteq \mathcal{A} \subseteq \mathcal{G}_q(n', k')$. For a given $\mathcal{A}$ we may be able to determine tighter bounds on the cardinalities of the $\mathcal{A}_i$s. Since the only change in the setting is the exclusion of the possible codewords in $\mathcal{G}_q(n', k') \backslash \mathcal{A}$ this subproblem can be formulated as an independent set problem and be solved using several algorithmic approaches, see e.g. [16]. We will present an explicit example of this technique in Subsection 5.3.

Having candidates for the $\mathcal{A}_i$ at hand it remains to select a subset of the candidates that are pairwise disjoint. This subproblem can also be formulated as a (restricted) independent set problem of a, possibly large, graph $G = (V, E)$. To this end, let κ be a suitable upper bound on the cardinalities of the $|\mathcal{A}_i|$ and S_i be the set of subsets of $\mathcal{A}$ of cardinality i having a subspace distance of at least d. Setting $S = \cup_{1 \le i \le \kappa} S_i$ one can consider the optimization problem

$$\begin{aligned} \max \sum_{s \in S} |s| \cdot x_s & & (4) \\ \sum_{s \in S} x_s = l & & \\ x_a + x_b \le 1 & \qquad \forall a \neq b \in S : a \cap b \neq \emptyset & \\ x_s \in \{0,1\} & \qquad \forall s \in S & \end{aligned}$$

for a given number l of parts of the desired packing. Notwithstanding that the target function of ILP formulation (4) completely ignores the correlation with the sizes of the items of the second packing on Λ, it can be used to determine the exact value of Λ in special cases, see Subsection 5.3. Setting $V = S$ and taking edges $e = \{s_1, s_2\} \in E$ iff $s_1 \cap s_2 \neq \emptyset$, this corresponds to a vertex-weighted independent set problem with an additional restriction on the number of chosen vertices. The algorithmic approaches described on [16] can be adopted easily for this extra requirements.

Since the two subproblems from this subsection on their own even might be too hard, we may apply heuristic approaches only. The very successful approach of prescribing automorphisms can also be applied here. Here the prescribed subgroup of automorphisms has to be a subgroup of the automorphism group of $\mathcal{A}$ which typically is much smaller than $\mathrm{GL}(n, q)$. However, “good” codes often have non-trivial automorphism groups.

5. Examples

In this section we describe the details of the coset construction for some specific parameters where we were able to improve the best known constructions.

5.1. $n = 8$, $d = 4$, $k = 4$, and $q = 2$ revisited.

We apply the coset construction with $n' = 4$, $k' = 2$, $d' = 2$ and use a parallelism in $\mathcal{G}_2(4,2)$ for the $\mathcal{A}_i$ and $\mathcal{B}_i$. Here we have $l = 7$ and $|\mathcal{A}_i| = |\mathcal{B}_i| = 5$ for all $1 \le i \le 7$. Thus, $\Lambda = 7 \cdot 5 \cdot 5 = 175$. Since $|\overline{F}| = 4$, the corresponding code obtained from the coset construction has cardinality 700. Adding the lifted MRD codes for the pivot vectors $(1,1,1,1,0,0,0,0)$ and $(0,0,0,0,1,1,1,1)$ gives $A_2(8,4;4) \ge 4096 + 700 + 1 = 4797$. This is Theorem 18 in [10]. Here, the MRD bound from Theorem 7 is attained. Recently, a $(8, 4801, 4; 4)_2$ code has been found by a heuristic computer search [6].

As already observed in [10], the crucial ingredient for the feasibility of the above construction is the existence of a parallelism in $\mathcal{G}_q(4,2)$. Performing the above cardinality computations for arbitrary q we obtain $A_q(8,4;4) \ge q^{12} + \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q (q^2+1)q^2 + 1$, which also attains the MRD bound from Theorem 7.

The authors of [10] have remarked that they believe that their construction from their Theorem 18 can be generalized to further parameters assuming the existence of a corresponding parallelism. This is indeed the case.

Theorem 9. *If $\mathcal{P}_1$ is a parallelism in $\mathcal{G}_q(n', k')$ and $\mathcal{P}_2$ a parallelism in $\mathcal{G}_q(n - n', k - k')$, then we can choose $\mathcal{A} = \mathcal{P}_1$, $\mathcal{B} = \mathcal{P}_2$, and $d = 4$ in the coset construction. The corresponding code $\mathcal{C}$ attains the upper bound of Corollary 1. If additionally $k - k' \ge 2$ and $n' - k' \ge 2$, then $\mathcal{C}$ is compatible with the lifted MRD code having pivot vector $(\underbrace{1, \dots, 1}_{k}, 0, \dots, 0)$.*

5.2. $n = 9$, $d = 6$, $k = 4$, **and general field sizes** q**.** Combining the MRD code $\mathcal{C}_1$ with pivot vector $v = (1,1,1,1,0,0,0,0,0)$ and cardinality 1024 with the code $\mathcal{C}_2$ obtained from the explicit construction of Lemma 13 of cardinality 8 improves the previously best known lower bound. Since the MRD bound from Theorem 7 is missed by one, we were motivated to look for a coset construction yielding a larger addendum than 8.

Theorem 10. $A_q(9,6;4) \ge q^{10} + q^3 + 1$.

Proof. We choose $n' = 4$, $k' = 1$, and $d' = 2$ in the coset construction. For the choice of $\mathcal{A}$ and $\mathcal{B}$ we observe $A_q(4,2;1) = q^3 + q^2 + q + 1$ and $A_q(5,4;3) = A_q(5,4;2) = q^3 + 1$, see e.g. [5]. Choose $\mathcal{A}$ and $\mathcal{B}$ as arbitrary codes attaining the mentioned upper bounds. Choosing a trivial packing of $\mathcal{B}$ into singletons yields a code $\mathcal{C}$ of cardinality q^3+1. Adding the lifted MRD code of size q^{10} gives the stated upper bound. □

We remark that the codes from Theorem 10 meets the MRD bound from Theorem 7. The underlying construction can be generalized even more.

Theorem 11. *For each $k \ge 4$ and arbitrary q we have*

$$A_q(3k-3, 2k-2; k) \ge q^{4k-6} + \frac{q^{2k-3} - q}{q^{k-2} - 1} - q + 1.$$

Proof. We choose $n' = k$, $k' = 1$, and $d' = 2$ in the coset construction. For the choice of $\mathcal{A}$ and $\mathcal{B}$ we observe $A_q(k,2;1) = \begin{bmatrix} k \\ 1 \end{bmatrix}_q$ and

$$\begin{aligned} A_q(2k-3, 2k-4; k-1) &= A_q(2k-3, 2k-4; k-2) \\ &\overset{[5]}{=} \frac{q^{2k-3} - q}{q^{k-2} - 1} - q + 1 < \begin{bmatrix} k \\ 1 \end{bmatrix}_q . \end{aligned}$$

Chose $\mathcal{A}$ and $\mathcal{B}$ as arbitrary codes attaining the mentioned upper bounds. Choosing a trivial packing of $\mathcal{B}$ into singletons yields a code $\mathcal{C}$ of cardinality $\frac{q^{2k-3}-q}{q^{k-2}-1} - q + 1$. Adding a $(k \times (3k-3))$ lifted MRD code gives the stated upper bound. □

We remark that the codes from Theorem 11 meet the MRD bound from Theorem 7.

5.3. $n = 10$, $d = 6$, $k = 4$, **and** $q = 2$**.** For the coset construction we choose $n' = 4$ and $k' = 1$. Since $\mathcal{A} \subseteq \mathcal{G}_2(4,1)$ we can only have $D_S(\mathcal{A}_i) = 2$, so that we must choose $d' = 2$. Then, we can choose $\mathcal{A} = \mathcal{G}_2(4,1)$ and $\begin{bmatrix} 4 \\ 1 \end{bmatrix}_2 = 15$ singletons $\mathcal{A}_i$, which is obviously best possible. For $\mathcal{B} \subseteq \mathcal{G}_2(6,3)$ we have the condition $D_S(\mathcal{B}) \ge 4$. Reasonable candidates for $\mathcal{B}$ might be the five isomorphism types of $(6,77,4;3)_2$ codes attaining the maximum cardinality $A_2(6,4;3) = 77$, see [14]. Using the first subproblem from Subsection 4.1 we computationally obtain the upper bound $|\mathcal{B}_i| \le 5 =: \kappa$ for four out of the five isomorphism types. This information is enough to conclude the upper bound $\Lambda(\mathcal{B}) \le 15 \cdot 5 = 75$. For the remaining isomorphism type, i.e., the self-dual code having 168 automorphisms which was labeled as "type A", we have $|\mathcal{B}_i| \le 7 =: \kappa$. So, we solve the optimization problem (4) for $l = 15$. The sizes of the requested sets S_I are stated in Table 1. The optimal target value is 76 and there exists a solution where the sizes of the elements in the packing are given by 4, 4, 4, 5, 5, 5, 5, 5, 5, 5, 5, 5, 5, 7, 7. Since in our situation we have $|\mathcal{A}_i| = 1$ for all i, the target function of (4) coincides with the expression for Λ. Also the predefinition of $l = 15$ results in the maximum possible value, since we have $l \le 15$ from the $\mathcal{A}$-part and the existence of a packing of $\mathcal{B}$ into l' sets implies the existence of packings into $l \ge l'$ sets. In general it is far from being obvious that we obtain the best possible codes from the coset construction by choosing codes for

$\mathcal{B}$ that have the maximal possible cardinality $A_q(n-n', d; k-k')$. However, in our situation each choice for $\mathcal{B}$ different from the five considered isomorphism types of $(6, 77, 4; 3)_2$ codes has a cardinality of at most 76, so that $\sum_i |\mathcal{A}_i| \cdot |\mathcal{B}_i| \le 76$.

Theorem 12. *For $n = 10$, $k = 4$, $n' = 6$, $k' = 3$, $q = 2$, and $d = 6$, the maximum achievable Λ of the coset construction is given by* 76.

$i =$	1	2	3	4	5	6	7
$\|S_i\| =$	77	840	2240	1792	560	112	16

Table 1. Sizes of S_i for $1 \le i \le 7 = \kappa$.

For general field sizes q we may choose $\mathcal{A} = \mathcal{G}_q(4,1)$ and $\begin{bmatrix}4\\1\end{bmatrix}_q = q^3 + q^2 + q + 1$ singletons $\mathcal{A}_i$. For $\mathcal{B}$ one may choose a $(6, q^6 + 2q^2 + 2q + 1, 4; 3)_q$ code, see [14]. Can one analytically describe packings of $(6, q^6 + 2q^2 + 2q + 1, 4; 3)_q$ codes into $q^3 + q^2 + q + 1$ parts of large cardinality?

Theorem 13. $A_2(10, 6; 4) \ge 4173$.

Proof. Let $\mathcal{C}_2$ be the code from the coset construction as outlined above. There is exactly one pivot vector $v = (1, 1, 1, 1, 0, 0, 0, 0, 0, 0)$ satisfying the condition from Lemma 5. The corresponding code $\mathcal{C}_1$ is the MRD code of size $\lceil 2^{6(4-3+1)} \rceil = 4096$, so that $|\mathcal{C}_1 \cup \mathcal{C}_2| = 4172$. By a computer search we found a single codeword that can be added to $\mathcal{C}_1 \cup \mathcal{C}_2$. □

We remark that the code from Theorem 13 meets the MRD bound from Theorem 7. The Echelon-Ferrers construction yields a code $\mathcal{C}$ with $4132 \le |\mathcal{C}| \le 4167$[8] and no better bound was known previously.

6. Conclusion

The arguably most successful general applicable construction for both constant dimension and subspace codes of large minimum subspace distance is the Echelon-Ferrers construction from [9]. Here, we have introduced a generalization of the construction of [10, Theorem 18], which we call *coset construction*. It turned out that the new construction is provably superior to the Echelon-Ferrers construction for some special parameters, see Subsection 5.3. We were able to apply the coset construction to an infinite family of constant dimension codes that improve the previously best known lower bounds and attain the MRD bound from Theorem 7, see Theorem 11. So far all improvements include the usage of a lifted MRD code of maximal shape, so that these approaches are all limited by the MRD bound from Theorem 7. For the relatively small addendums constructed by the coset construction, we may utilize subcodes that have a larger cardinality than the corresponding value of the MRD bound, see Subsection 5.3. The constructions of subspace codes based on the coset construction typically should yield many non-isomorphic codes, since there are already many non-isomorphic MRD codes, see e.g. [4, 18]. In Section 4 we have obtained some first insights on the optimal choice of parameters for the coset construction and related optimization problems. However, we are rather faraway from a clear assessment of the capabilities of the coset construction. This can be seen for example at the following facts. Nevertheless, the coset construction is principally applicable for general subspace codes, we so far have not found

[8] Assuming that the upper bound of Theorem 6 is tight, the maximal cardinality of an $(10, M, 6; 4)_2$ code obtained from the general Echelon-Ferrers construction would be 4167. Using just the known constructions for good codes in $\mathrm{EF}_q(v)$, we could explicitly construct a code of cardinality 4132.

a single example improving one of the currently known lower bounds. Also the stated examples of applications of the coset construction in Section 5 are merely a collection of sporadic coincidences. A more systematic analysis of “good” choices of parameters is needed. To this end we propose some strongly related open research questions:

- generalize the MRD bound of Theorem 7 to a larger class of parameters;
- construct more examples of codes attaining the MRD bound of Theorem 7;
- enlarge the list of known parallelisms;
- apply the coset construction to improve a lower bound on $A_q(n,d)$;
- study upper bounds on $(n,M,d;k)_q$ codes that contain $(n,M',d';k)_q$ subcodes where $d'>d$[9];
- classify all codes attaining cardinality $A_q(n,d;k)$ up to isomorphisms extendability results, see e.g. [19][10];
- study packings of $(6,q^6+2q^2+2q+1,4;3)_q$ codes into q^3+q^2+q+1 parts of large cardinality;
- study packings of the known best constructions for partial spreads into $\begin{bmatrix}m\\1\end{bmatrix}_q$ parts of large cardinality for different values of m[11].

References

[1] R. Ahlswede, H.K. Aydinian, and L.H. Khachatrian, *On perfect codes and related concepts*, Designs, Codes and Cryptography **22** (2001), no. 3, 221–237.

[2] J. André, *Über nicht-desarguessche Ebenen mit transitiver Translationsgruppe*, Mathematische Zeitschrift **60** (1954), no. 1, 156–186.

[3] G.E. Andrews, *The theory of partitions*, no. 2, Cambridge university press, 1998.

[4] T.P. Berger, *Isometries for rank distance and permutation group of gabidulin codes*, IEEE Transactions on Information Theory **49** (2003), no. 11, 3016–3019.

[5] A. Beutelspacher, *Partial spreads in finite projective spaces and partial designs*, Mathematische Zeitschrift **145** (1975), no. 3, 211–229.

[6] M. Braun, P. Östergård, and A. Wassermann, *New lower bounds for constant dimension subspace codes*, submitted (2015), 9.

[7] J. Edmonds, *Matroids and the greedy algorithm*, Mathematical programming **1** (1971), no. 1, 127–136.

[8] 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.

[9] 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.

[10] ______, *Codes and designs related to lifted mrd codes*, IEEE Transactions on Information Theory **59** (2013), no. 2, 1004–1017.

[11] T. Etzion and L. Storme, *Galois geometries and coding theory*, Designs, Codes and Cryptography (2015), 1–40.

[12] E.M. Gabidulin, *Theory of codes with maximum rank distance*, Problemy Peredachi Informatsii **21** (1985), no. 1, 3–16.

[9] Such results would give upper bounds on the achievable parameters κ, see Subsection 4.1, and might be a first hint which constant dimension codes may be appropriate for $\mathcal{A}$ and $\mathcal{B}$, see also the example of Subsection 5.3.

[10] The “optimality” of example from Subsection 5.3 heavily relies on the classification of $(6,77,4;3)_2$ codes and it possibly was only a matter of coincidence that we do not needed to look at codes of smaller cardinalities.

[11] The construction of Theorem 11 can easily by generalized to parameters $n=n'+2k-3$, where $k\ge 3$ and $n'\ge 3$. For $k'=1$, $d'=2$, we can choose $\mathcal{A}=\mathcal{G}_q(n',1)$ and $\mathcal{B}$ as a (maximal) partial $(k-2)$-spread $\mathcal{P}$ in $\mathbb{F}_q^{n-n'}$. Then, a packing of $\mathcal{P}$ into $\begin{bmatrix}n'\\1\end{bmatrix}_q$ parts is needed. For the parameters of Theorem 11 this packing trivially exists. We remark that the maximum size of partial $\tilde{k}$-spreads in $\mathbb{F}_q^{\tilde{n}}$ is known for $\tilde{n}\equiv 0,1 \pmod{\tilde{k}}$ for arbitrary q, see e.g. [5], and for $\tilde{n}\equiv 2 \pmod{\tilde{k}}$ and $q=2$, see [8, 17].

[13] D. Heinlein, M. Kiermaier, S.Kurz, and A. Wassermann, *Tables of subspace codes*, University of Bayreuth, 2015, available at `http://subspacecodes.uni-bayreuth.de`.

[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** (2015), 157–176.

[15] R. Koetter and F.R. Kschischang, *Coding for errors and erasures in random network coding*, IEEE Transactions on Information Theory **54** (2008), no. 8, 3579–3591.

[16] 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.

[17] S. Kurz, *Improved upper bounds for partial spreads*, arXiv preprint: 1512.04297, 8 pages (2015), 8.

[18] K. Morrison, *Equivalence for rank-metric and matrix codes and automorphism groups of gabidulin codes*, IEEE Transactions on Information Theory **60** (2014), no. 11, 7035–7046.

[19] A. Nakić and L. Storme, *On the extendability of particular classes of constant dimension codes*, Designs, Codes and Cryptography (2015), 1–16.

[20] N. Silberstein and T. Etzion, *Large constant dimension codes and lexicodes*, Adv. Math. Commun. **5** (2011), no. 2, 177–189.

[21] N. Silberstein and A.-L. Trautmann, *Subspace codes based on graph matchings, ferrers diagrams and pending blocks*, arXiv preprint: 1404.6723 (2014).

[22] 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.

[23] V. Skachek, *Recursive code construction for random networks*, IEEE Transactions on Information Theory **56** (2010), no. 3, 1378–1382.

E-mail address: `daniel.heinlein@uni-bayreuth.de`

E-mail address: `sascha.kurz@uni-bayreuth.de`