New Lower Bounds for Constant Dimension Codes

Natalia Silberstein
Dep. of Electrical & Computer Eng.
University of Texas at Austin
Austin, TX, USA
Email: natalys@austin.utexas.edu

Anna-Lena Trautmann
Inst. of Mathematics
University of Zurich
Zurich, Switzerland
Email: anna-lena.trautmann@math.uzh.ch

***Abstract*—This paper provides new constructive lower bounds for constant dimension codes, using Ferrers diagram rank metric codes and pending blocks. Constructions for two families of parameters of constant dimension codes are presented. The examples of codes obtained by these constructions are the largest known constant dimension codes for the given parameters.**

I. Introduction

Let $\mathbb{F}_q$ be the finite field of size q. Given two integers k, n, such that $0 \leq k \leq n$, the set of all k-dimensional subspaces of $\mathbb{F}_q^n$ forms the Grassmannian over $\mathbb{F}_q$, denoted by $\mathcal{G}_q(k,n)$. It is well known that the cardinality of the Grassmannian is given by the *q-ary Gaussian coefficient*

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \overset{\text{def}}{=} |\mathcal{G}_q(k,n)| = \prod_{i=0}^{k-1} \frac{q^{n-i}-1}{q^{k-i}-1}.$$

The Grassmannian space is a metric space, where the *subspace distance* between any two subspaces X and Y in $\mathcal{G}_q(k,n)$, is given by

$$d_S(X,Y) \overset{\text{def}}{=} \dim X + \dim Y - 2\dim\bigl(X \cap Y\bigr). \quad (1)$$

We say that $\mathbb{C} \subseteq \mathcal{G}_q(k,n)$ is an $(n,M,d,k)_q$ *code in the Grassmannian*, or *constant-dimension code*, if $M = |\mathbb{C}|$ and $d_S(X,Y) \geq d$ for all distinct elements $X,Y \in \mathbb{C}$. Note, that the minimum distance d of $\mathbb{C}$ is always even. $A_q(n,d,k)$ will denote the maximum size of an $(n,M,d,k)_q$ code.

Constant dimension codes have drawn a significant attention in the last five years due to the work by Koetter and Kschischang [8], where they presented an application of such codes for error-correction in random network coding. Constructions and bounds for constant dimension codes were given in [1], [2], [3], [4], [6], [7], [9], [11], [13], [17].

In this paper we focus on constructions of large constant dimension codes. In particular, we generalize the ideas used for constructing codes in the Grassmannian from [2], [3], [17] and obtain new lower bounds on $A_q(n,d,k)$. In Section II we introduce the necessary definitions and present two known constructions which will be the starting point to our new constructions. In Section III we introduce the notation of pending blocks. In Sections IV and V we present our new constructions. It appears that the codes obtained by these constructions are the largest known constant dimension codes for the given parameters.

II. Preliminaries

In this section we briefly provide the definitions and previous results used in our constructions. More details can be found in [2], [3], [17].

Let X be a k-dimensional subspace of $\mathbb{F}_q^n$. We represent X by the matrix RE(X) in reduced row echelon form, such that the rows of RE(X) form the basis of X. The *identifying vector* of X, denoted by $v(X)$, is the binary vector of length n and weight k, where the k *ones* of $v(X)$ are exactly in the positions where RE(X) has the leading coefficients (the pivots).

The *Ferrers tableaux form* of a subspace X, denoted by $\mathcal{F}(X)$, is obtained from RE(X) first by removing from each row of RE(X) the *zeroes* to the left of the leading coefficient; and after that removing the columns which contain the leading coefficients. All the remaining entries are shifted to the right. The *Ferrers diagram* of X, denoted by $\mathcal{F}_X$, is obtained from $\mathcal{F}(X)$ by replacing the entries of $\mathcal{F}(X)$ with dots.

Given $\mathcal{F}(X)$, the unique corresponding subspace $X \in \mathcal{G}_q(k,n)$ can easily be found. Also given $v(X)$, the unique corresponding $\mathcal{F}_X$ can be found. When we fill the dots of a Ferrers diagram by elements of $\mathbb{F}_q$, we obtain a $\mathcal{F}(X)$ for some $X \in \mathcal{G}_q(k,n)$.

In the following we will consider Ferrers diagrams rank-metric codes which are closely related to constant dimension codes. For two $m \times \ell$ matrices A and B over $\mathbb{F}_q$ the *rank distance*, $d_R(A,B)$, is defined by $d_R(A,B) \overset{\text{def}}{=} \text{rank}(A-B)$.

Let $\mathcal{F}$ be a Ferrers diagram with m dots in the rightmost column and ℓ dots in the top row. A code $\mathcal{C}_\mathcal{F}$ is an $[\mathcal{F},\rho,\delta]$ *Ferrers diagram rank-metric (FDRM) code* if all codewords of $\mathcal{C}_\mathcal{F}$ are $m \times \ell$ matrices in which all entries not in $\mathcal{F}$ are *zeroes*, they form a linear subspace of dimension ρ of $\mathbb{F}_q^{m \times \ell}$, and for any two distinct codewords A and B, $d_R(A,B) \geq \delta$. If $\mathcal{F}$ is a rectangular $m \times \ell$ diagram with $m \cdot \ell$ dots then the FDRM code is a classical rank-metric code [5], [12]. The following theorem provides an upper bound on the cardinality of $\mathcal{C}_\mathcal{F}$.

Theorem 1. *[2] Let $\mathcal{F}$ be a Ferrers diagram and $\mathcal{C}_\mathcal{F}$ the corresponding FDRM code. Then $|\mathcal{C}_\mathcal{F}| \leq q^{\min_i\{w_i\}}$, where w_i is the number of dots in $\mathcal{F}$ which are not contained in the first i rows and the rightmost $\delta - 1 - i$ columns ($0 \leq i \leq \delta - 1$).*

A code which attains the bound of Theorem 1 is called a *Ferrers diagram maximum rank distance (FDMRD) code*.

Remark 2. *Maximum rank distance (MRD) codes are a class of $[\mathcal{F},\ell(m-\delta+1),\delta]$ FDRM codes, $\ell \geq m$, with a full $m \times \ell$*

The second author was partially supported by SNF grant no. 138080 and Forschungskredit of the University of Zurich, grant no. 57104103.

diagram $\mathcal{F}$, which attain the bound of Theorem 1 [5], [12].

It was proved in [2] that for general diagrams the bound of Theorem 1 is attained for $\delta = 1, 2$. Some special cases, when this bound is attained for $\delta > 2$, can also be found in [2].

For a codeword $A \in \mathcal{C}_{\mathcal{F}} \subseteq \mathbb{F}_q^{k \times (n-k)}$ let $A_{\mathcal{F}}$ denote the part of A related to the entries of $\mathcal{F}$ in A. Given an FDMRD code $\mathcal{C}_{\mathcal{F}}$, a lifted FDMRD code $\mathbb{C}_{\mathcal{F}}$ is defined as follows:

$$\mathbb{C}_{\mathcal{F}} = \{X \in \mathcal{G}_q(k,n) : \mathcal{F}(X) = A_{\mathcal{F}},\ A \in \mathcal{C}_{\mathcal{F}}\}.$$

This definition is the generalization of the definition of a lifted MRD code [15]. Note, that all the codewords of a lifted MRD code have the same identifying vector of the type $(\underbrace{11...1}_{k}\underbrace{000...00}_{n-k})$. The following lemma [2] is the generalization of the result given in [15].

Lemma 3. *If $\mathcal{C}_{\mathcal{F}} \subset \mathbb{F}_q^{k \times (n-k)}$ is an $[\mathcal{F}, \rho, \delta]$ Ferrers diagram rank-metric code, then its lifted code $\mathbb{C}_{\mathcal{F}}$ is an $(n, q^{\rho}, 2\delta, k)_q$ constant dimension code.*

A. The multilevel construction and pending dots construction

It was proved in [2] that for $X, Y \in \mathcal{G}_q(k,n)$ we have $d_S(X,Y) \geq d_H(v(X), v(Y))$, where d_H denotes the Hamming distance; and if $v(X) = v(Y)$ then $d_S(X,Y) = 2d_R(\text{RE}(X), \text{RE}(Y))$. The multilevel construction [2] of constant dimension code is based on these properties of d_S.

Multilevel construction. First, a binary constant weight code of length n, weight k, and Hamming distance 2δ is chosen to be the set of the identifying vectors for $\mathbb{C}$. Then, for each identifying vector a corresponding lifted FDRM code with minimum rank distance δ is constructed. The union of these lifted FDRM codes is an $(n, M, 2\delta, k)_q$ code.

In the construction provided in [3], for $k = 3$ and $\delta = 2$, in the stage of choosing the identifying vectors for a code $\mathbb{C}$, a set of vectors with minimum (Hamming) distance $2\delta - 2 = 2$ is allowed, by using a method based on pending dots in a Ferrers diagram [17].

The *pending dots* of a Ferrers diagram $\mathcal{F}$ are the leftmost dots in the first row of $\mathcal{F}$ whose removal has no impact on the size of the corresponding Ferrers diagram rank-metric code. The following lemma follows from [17].

Lemma 4. *Let X and Y be two subspaces in $\mathcal{G}_q(k,n)$ with $d_H(v(X), v(Y)) = 2\delta - 2$, such that the leftmost* one *of $v(X)$ is in the same position as the leftmost* one *of $v(Y)$. Let P_X and P_Y be the sets of pending dots of X and Y, respectively. If $P_X \cap P_Y \neq \varnothing$ and the entries in $P_X \cap P_Y$ (of their Ferrers tableaux forms) are assigned with different values in at least one position, then $d_S(X,Y) \geq 2\delta$.*

Example 5. *Let X and Y be subspaces in $\mathcal{G}_q(3,6)$ which are given by the following generator matrices:*

$$\begin{pmatrix} 1 & \textcircled{0} & 0 & v_1 & v_2 & 0 \\ 0 & 0 & 1 & v_3 & v_4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \textcircled{1} & u_1 & 0 & u_2 & 0 \\ 0 & 0 & 0 & 1 & u_3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

where $v_i, u_i \in \mathbb{F}_q$, and the pending dots are emphasized by circles. Their identifying vectors are $v(X) = 101001$ and $v(Y) = 100101$. Clearly, $d_H(v(X), v(Y)) = 2$, while $d_S(X,Y) \geq 4$.

The following lemma which follows from a one-factorization and near-one-factorization of a complete graph [10] will be used in our constructions.

Lemma 6. *Let D be the set of all binary vectors of length m and weight 2.*

- *If m is even, D can be partitioned into $m-1$ classes, each of $\frac{m}{2}$ vectors with pairwise disjoint positions of* ones*;*
- *If m is odd, D can be partitioned into m classes, each of $\frac{m-1}{2}$ vectors with pairwise disjoint positions of* ones.

The following construction for $k = 3$ and $d = 2\delta = 4$ based on pending dots from [3] will be used as a base step of our recursive construction proposed in the sequel.

Construction 0. Let $n \geq 8$ and $q^2 + q + 1 \geq \ell$, where $\ell = n - 4$ for odd n and $\ell = n - 3$ for even n. In addition to the lifted MRD code (which has the identifying vector $v_0 = (11100\ldots0)$), the final code $\mathbb{C}$ will contain the codewords with identifying vectors of the form $(x||y)$, where the prefix $x \in \mathbb{F}_2^3$ is of weight 1 and the suffix $y \in \mathbb{F}_2^{n-3}$ is of weight 2. By Lemma 6, we partition the set of suffixes into ℓ classes $P_1, P_2, \ldots, P_\ell$ and define the following three sets:

$$\mathcal{A}_1 = \{(001||y) : y \in P_1\},$$

$$\mathcal{A}_2 = \{(010||y) : y \in P_i, 2 \leq i \leq \min\{q+1, \ell\}\},$$

$$\mathcal{A}_3 = \begin{cases} \{(100||y) : y \in P_i,\ q+2 \leq i \leq \ell\} & \text{if } \ell > q+1 \\ \varnothing & \text{if } \ell \leq q+1 \end{cases}.$$

Elements with the same prefix and distinct suffices from the same class P_i have Hamming distance 4. When we use the same prefix for two different classes P_i, P_j, we assign different values in the pending dots of the Ferrers tableaux forms. Then the corresponding lifted FDMRD codes of subspace distance 4 are constructed, and their union with the lifted MRD code forms the final code $\mathbb{C}$ of size $q^{2(n-3)} + \begin{bmatrix} n-3 \\ 2 \end{bmatrix}_q$.

In the following sections we will generalize this construction and obtain codes for any $k \geq 4$ with minimum subspace distance $d = 4$ and with $d = 2(k-1)$.

III. Pending Blocks

To present the new constructions for constant dimension codes, we first need to extend the definition of pending dots of [17] to a two-dimensional setting.

Definition 7. *Let $\mathcal{F}$ be a Ferrers diagram with m dots in the rightmost column and ℓ dots in the top row. We say that the $\ell_1 < \ell$ leftmost columns of $\mathcal{F}$ form a* pending block *(of size ℓ_1) if the upper bound on the size of FDMRD code $\mathcal{C}_{\mathcal{F}}$ from Theorem 1 is equal to the upper bound on the size of $\mathcal{C}_{\mathcal{F}}$ without the ℓ_1 leftmost columns.*

Example 8. *Consider the following Ferrers diagrams:*

$$\mathcal{F}_1 = \begin{array}{ccccc} \bullet & \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet & \bullet \\ & & \bullet & \bullet & \bullet \end{array}, \quad \mathcal{F}_2 = \begin{array}{ccc} \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \end{array}.$$

For $\delta = 3$ by Theorem 1 both codes $\mathcal{C}_{\mathcal{F}_1}$ and $\mathcal{C}_{\mathcal{F}_2}$ have $|\mathcal{C}_{\mathcal{F}_i}| \leq q^3$, $i = 1, 2$. The diagram $\mathcal{F}_1$ has the pending block $\begin{array}{cc} \bullet & \bullet \\ & \bullet \end{array}$ and the diagram $\mathcal{F}_2$ has no pending block.

Definition 9. *Let $\mathcal{F}$ be a Ferrers diagram with m dots in the rightmost column and ℓ dots in the top row, and let $\ell_1 < \ell$, and $m_1 < m$. If the (m_1+1)st row of $\mathcal{F}$ has less dots than the m_1th row of $\mathcal{F}$ and at most $m - \ell_1$ dots, then the ℓ_1 leftmost columns of $\mathcal{F}$ are called a* quasi-pending block *(of size $m_1 \times \ell_1$).*

Note, that a pending block is also a quasi-pending block.

Theorem 10. *Let $X, Y \in \mathcal{G}_q(k,n)$, such that* $\mathrm{RE(X)}$ *and* $\mathrm{RE(Y)}$ *have a quasi-pending block of size $m_1 \times \ell_1$ in the same position and $d_H(v(X), v(Y)) = d$. Denote the submatrices of $\mathcal{F}(X)$ and $\mathcal{F}(Y)$ corresponding to the quasi-pending blocks by B_X and B_Y, respectively. Then $d_S(X,Y) \geq d + 2\mathrm{rank}(B_X - B_Y)$.*

Proof: After row reduction one can easily see that $\mathrm{rank}\begin{bmatrix} \mathrm{RE(X)} \\ \mathrm{RE(Y)} \end{bmatrix} \geq k + \frac{d}{2} + \mathrm{rank}(B_X - B_Y)$, which implies the statement. The detailed proof can be found in [14]. ■

This theorem implies that for the construction of an $(n, M, 2\delta, k)$-code, by filling the (quasi-)pending blocks with a suitable Ferrers diagram rank metric code, one can choose a set of identifying vectors with lower minimum Hamming distance than 2δ.

IV. Constructions for $(n, M, 4, k)_q$ Codes

In this section we present a construction based on quasi-pending blocks for $(n, M, 4, k)_q$ codes with $k \geq 4$ and $n \geq 2k+2$. This construction will then give rise to new lower bounds on the size of constant dimension codes with the minimum distance 4. First we need the following results. (The proofs can be found in [14].)

Lemma 11. *Let $n \geq 2k+2$. Let v be an identifying vector of length n and weight k, such that there are $k-2$ many ones in the first k positions of v. Then the Ferrers diagram arising from v has more or equally many dots in the first row than in the last column, and the upper bound for the dimension of a Ferrers diagram code with minimum distance 2 is the number of dots that are not in the first row.*

Lemma 12. *The number of all matrices filling the Ferrers diagrams arising from all elements of $\mathbb{F}_q^k$ of weight $k-2$ as identifying vectors is $\nu := \sum_{j=0}^{k-2} \sum_{i=j}^{k-2} q^{i+j} - 1$.*

We can now describe the construction ($k \geq 4, n \geq 2k+2$):

Construction Ia. First, by Lemma 6, we partition the weight-2 vectors of $\mathbb{F}_2^{n-k}$ into classes $P_1, \dots, P_\ell$ of size $\frac{\bar{\ell}}{2}$ (where $\ell = \bar{\ell} - 1 = n-k-1$ if $n-k$ even and $\ell = \bar{\ell}+1 = n-k$ if $n-k$ odd) with pairwise disjoint positions of the ones.

1) We define the following sets of identifying vectors (of weight k):
$$\begin{aligned} \mathcal{A}_0 &= \{(1\dots1||0\dots0)\}, \\ \mathcal{A}_1 &= \{(0011\dots1||y) : y \in P_1\}, \\ \mathcal{A}_2 &= \{(0101\dots1||y) : y \in P_2, \dots, P_{q+1}\}, \\ &\vdots \\ \mathcal{A}_{\binom{k}{2}} &= \{(1\dots1100||y) : y \in P_\mu, \dots, P_\nu\}. \end{aligned}$$
such that the prefixes in $\mathcal{A}_1, \dots, \mathcal{A}_{\binom{k}{2}}$ are all vectors of $\mathbb{F}_2^k$ of weight $k-2$. The number of P_i's used in each set depends on the size of the quasi-pending block arising in the k leftmost columns of the respective matrices. Thus, ν is the value from Lemma 12 and $\mu := \nu - q^{2(k-2)}$.

2) For each vector v_j in a given $\mathcal{A}_i$ for $i \in \{2, \dots, \binom{k}{2}\}$ assign a different matrix filling for the quasi-pending block in the k leftmost columns of the respective matrices. Fill the remaining part of the Ferrers diagram with a suitable FDMRD code of minimum rank distance 2 and lift the code to obtain $\mathbb{C}_{i,j}$. Define $\mathbb{C}_i = \bigcup_{j=1}^{|\mathcal{A}_i|} \mathbb{C}_{i,j}$.

3) Take the largest known code $\bar{\mathbb{C}} \subseteq \mathcal{G}_q(k, n-k)$ with minimum distance 4 and append k zero columns in front of every matrix representation of the codewords.

4) The following union of codes forms the final code $\mathbb{C}$:
$$\mathbb{C} = \bigcup_{i=0}^{\binom{k}{2}} \mathbb{C}_i \cup \bar{\mathbb{C}}$$
where $\mathbb{C}_0$ is the lifted MRD code corresponding to $\mathcal{A}_0$.

Remark 13. *If $\ell < \nu$, then we use only the sets $\mathcal{A}_0, \dots, \mathcal{A}_i$ ($i \leq \binom{k}{2}$) such that all of $P_1, \dots, P_\ell$ are used once.*

Theorem 14. *If $\ell \leq \nu$, a code $\mathbb{C} \subseteq \mathcal{G}_q(k,n)$ constructed according to Construction I has minimum subspace distance 4 and cardinality*
$$|\mathbb{C}| = q^{(k-1)(n-k)} + q^{(n-k-2)(k-3)} \begin{bmatrix} n-k \\ 2 \end{bmatrix}_q + A_q(n-k, 4, k).$$

Proof: It holds that $|\mathbb{C}_0| = q^{(k-1)(n-k)}$ and $|\bar{\mathbb{C}}| = A_q(n-k, 4, k)$. Because of the assumption on k and q it follows from Lemma 12 that all the $y_i \in \mathbb{F}_2^{n-k}$ are used for the identifying vectors, hence a cardinality of $|\mathcal{G}_q(2, n-k)|$ for the lower two rows. Moreover, we can fill the second to $(k-2)$-nd row of the Ferrers diagrams with anything in the construction of the FDMRD code, hence at least $q^{(n-k-2)(k-3)}$ possibilities.

The minimum distance follows from Theorem 10 and Lemma 11. See the detailed proof in [14]. ■

Corollary 15. *Let $k \geq 4, n \geq 2k+2$ and $\sum_{j=0}^{k-2} \sum_{i=j}^{k-2} q^{i+j} - 1 \geq n-k$ if $n-k$ is odd (otherwise $\geq n-k-1$). Then*
$$A_q(n,4,k) \geq q^{(k-1)(n-k)} + q^{(n-k-2)(k-3)} \begin{bmatrix} n-k \\ 2 \end{bmatrix}_q + A_q(n-k,4,k).$$

This bound is always tighter than the ones given by the Reed-Solomon like construction [8] and the multicomponent extension of this [6], [16].

Note, that in Construction Ia we did not use the dots in the quasi-pending blocks for the construction of FDMRD codes. Thus, the bound of Corollary 15 is not tight. To make it tighter, one can use less pending blocks and larger FDMRD codes, as illustrated in the following construction. We denote by P_y the class of suffixes which contains the suffix vector y (in the partition of Lemma 6).

Construction Ib. First, in addition to $\mathcal{A}_0$ of Construction Ia, we define the following sets of identifying vectors:

$$\bar{\mathcal{A}}_1 = \{(11...1100||y) : y \in P_{1100...00}\},$$

$$\bar{\mathcal{A}}_2 = \{(11...1010||y) : y \in P_{1010...00}\},$$

$$\bar{\mathcal{A}}_3 = \{(11...0110||y) : y \in P_{1001...00}\},$$

$$\bar{\mathcal{A}}_4 = \{(11...1001||y) : y \in P_{0110...00}\}.$$

All the other identifying vectors are distributed as in Construction Ia. The steps $2) - 4)$ of Construction Ia remain the same. Then the lower bound on the cardinality becomes

Corollary 16. *If $\sum_{j=0}^{k-2} \sum_{i=j}^{k-2} q^{i+j} - \sum_{i=4}^{5} q^{2k-i} - 2q^{2k-6} \geq n-k$, then*

$$A_q(n,4,k) \geq q^{(k-1)(n-k)} + q^{(n-k-2)(k-3)} \begin{bmatrix} n-k \\ 2 \end{bmatrix}_q$$

$$+(q^{2(k-3)}-1)q^{(k-1)(n-k-2)} + (q^{2(k-3)-1}-1)q^{(k-1)(n-k-2)-1}$$

$$+2(q^{2(k-4)}-1)q^{(k-1)(n-k-2)-2} + A_q(n-k,4,k).$$

Note, that one can use this idea on more $\mathcal{A}_i$'s, as long as there are enough pending blocks such that all P_i's are used.

Moreover, instead of using all the classes P_i we can use the classes which contribute more codewords more than once with the disjoint prefixes. We illustrate this idea for a code having $k = 4$ and $n = 10$. It appears, that the code obtained by this construction is the largest known code.

Example 17. *Let $q = 2, k = 4$, $n = 10$. We partition the binary vectors of length 6 and weight 2 into the following 5 classes: $P_1 = \{110000, 001010, 000101\}, P_2 = \{101000, 010001, 000110\}, P_3 = \{011000, 100100, 000011\}$, $P_4 = \{010100, 100010, 001001\}, P_5 = \{100001, 010010, 001100\}$. We define $\mathcal{A}_0$ as previously and*

$$\mathcal{A}_1 = \{(1100||y) : y \in P_1\}, \mathcal{A}_2 = \{(0011||y) : y \in P_1\},$$

$$\mathcal{A}_3 = \{(0110||y) : y \in P_4\}, \mathcal{A}_4 = \{(1001||y) : y \in P_4\},$$

$$\mathcal{A}_5 = \{(1010||y) : y \in P_2 \cup P_3\}, \mathcal{A}_6 = \{(0101||y) : y \in P_2 \cup P_3\},$$

where we use the pending dot in $\mathcal{A}_5$ and $\mathcal{A}_6$. Note, that we do not use P_5. Also, the FDMRD codes are now constructed for the whole Ferrers diagrams (without the pending dot), and not only for the last 6 columns. We can add $A_2(6,4,4) = A_2(6,4,2) = (2^6-1)/(2^2-1) = 21$ codewords corresponding to step 4) in Construction Ia. The size of the final code is $2^{18} + 37477$. The largest previously known code was obtained by the multilevel construction and has size $2^{18} + 34768$ [2].

In the following we discuss a construction of a new constant dimension code with minimum distance 4 from a given one.

Theorem 18. *Let $\mathbb{C}$ be an $(n, M, 4, k)_q$ constant dimension code. Let Δ be an integer such that $\Delta \geq k$. Then, there exists an $(n' = n + \Delta, M', 4, k)_q$ code $\mathbb{C}'$ with $M' = Mq^{\Delta(k-1)}$.*

Proof: To the generator matrix of each codeword of $\mathbb{C}$ we append a $[k \times \Delta, \Delta(k-1), 2]$-MRD code in the additional columns. ■

Example 19. *We take the $(8, 2^{12} + 701, 4, 4)_2$ code $\mathbb{C}$ constructed in [3] and apply on it Theorem 18 with $\Delta = 4$. Then the code $|\mathbb{C}'| = 2^{24} + 701 \cdot 2^{12} = 2^{24} + 2871296$. The largest previously known code of size $2^{24} + 2290845$ was obtained in [2].*

V. Construction for $(n, M, 2(k-1), k)_q$ Codes

In this section we provide a recursive construction for $(n, M, 2(k-1), k)_q$ codes, which uses the pending dots based construction described in Section II as an initial step. Codes obtained by this construction contain the lifted MRD code. An upper bound on the cardinality of such codes is given in [3]. The codes obtained by Construction 0 attain this bound for $k = 3$. Our recursive construction provides a new lower bound on the cardinality of such codes for general k.

First, we need the following lemma which is a simple generalization of Lemma 11.

Lemma 20. *Let $n-k-2 \geq n_1 \geq k-2$ and v be an identifying vector of length n and weight k, such that there are $k-2$ many ones in the first n_1 positions of v. Then the Ferrers diagram arising from v has more or equally many dots in any of the first $k-2$ rows than in the last column, and the upper bound for the dimension of a Ferrers diagram code with minimum distance $k-1$ is the number of dots that are not in the first $k-2$ rows.*

Remark 21. *If an $m \times \ell$-Ferrers diagram has δ rows with ℓ dots each, then the construction of [2] provides respective FDMRD codes of minimum distance $\delta + 1$ attaining the bound of Theorem 1.*

Lemma 22. *For an $m \times \ell$-Ferrers diagram where the jth row has at least x more dots than the $(j+1)$th row for $1 \leq j \leq m-1$ and the lowest row has x many dots, one can construct a FDMRD code with minimum rank distance m and cardinality q^x.*

The proofs for Lemmas 20 and 22 can be found in [14].

Construction II. Let $s = \sum_{i=3}^{k} i$, $n \geq s + 2 + k$ and $q^2 + q + 1 \geq \ell$, where $\ell = n - s$ for odd $n - s$ (or $\ell = n - s - 1$ for even $n - s$).

Identifying vectors: In addition to the identifying vector $v_{00}^k = (11\ldots1100\ldots0)$ of the lifted MRD code $\mathbb{C}_*^k$ (of size $q^{2(n-k)}$ and distance $2(k-1)$), the other identifying vectors of the codewords are defined as follows. First, by Lemma 6, we partition the weight-2 vectors of $\mathbb{F}_2^{n-s}$ into classes $P_1, \ldots, P_\ell$ of size $\frac{\bar{\ell}}{2}$ (where $\ell = \bar{\ell} - 1 = n - s - 1$ if $n - s$ even and $\ell = \bar{\ell} + 1 = n - s$ if $n - s$ odd) with pairwise disjoint positions of the ones. We define the sets of identifying vectors by a recursion. Let v_0 and $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3 \subseteq \mathbb{F}_q^{n-s+3}$, as defined in Construction 0. Then $v_{00}^3 = v_0$,

$$\mathcal{A}_0^3 = \emptyset,\ \mathcal{A}_i^3 = \mathcal{A}_i,\ 1 \leq i \leq 3.$$

For $k \geq 4$ we define:

$$\mathcal{A}_0^k = \{v_{01}^k, \ldots, v_{0k-3}^k\},$$

where $v_{0j}^k = (000\, w_j^k\, || v_{0j-1}^{k-1})$ $(1 \leq j \leq k-3)$, such that the w_j^k are all different weight-1 vectors of $\mathbb{F}_2^{k-3}$. Furthermore we define:

$$\mathcal{A}_1^k = \{(0010\dots00||z) : z \in \mathcal{A}_1^{k-1}\},$$
$$\mathcal{A}_2^k = \{(0100\dots00||z) : z \in \mathcal{A}_2^{k-1}\},$$
$$\mathcal{A}_3^k = \{(1000\dots00||z) : z \in \mathcal{A}_3^{k-1}\},$$

such that the prefixes of the vectors in $\bigcup_{i=0}^{3} \mathcal{A}_i^k$ are vectors of $\mathbb{F}_2^k$ of weight 1. Note, that the suffix $y \in \mathbb{F}_q^{n-s}$ (from Construction 0) in all the vectors from $\mathcal{A}_1^k$ belongs to P_1, the suffix y in all the vectors from $\mathcal{A}_2^k$ belongs to $\bigcup_{i=2}^{\min\{q+1,\ell\}} P_i$, and the suffix y in all the vectors from $\mathcal{A}_3^k$ belongs to $\bigcup_{i=q+2}^{\ell} P_i$ (the set $\mathcal{A}_3^k$ is empty if $\ell \leq q+1$).

Pending blocks:

- All Ferrers diagrams that correspond to the vectors in $\mathcal{A}_1^k$ have a common pending block with $k-3$ rows and $\sum_{i=3}^{k-j} i$ dots in the jth row, for $1 \leq j \leq k-3$. We fill each of these pending blocks with a different element of a suitable FDMRD code with minimum rank distance $k-3$ and size q^3, according to Lemma 22. Note, that the initial conditions always imply that $q^3 \geq \ell$.
- All Ferrers diagrams that correspond to the vectors in $\mathcal{A}_2^k$ have a common pending block with $k-2$ rows and $\sum_{i=3}^{k-j} i + 1$ dots in the jth row, $1 \leq j \leq k-2$. Every vector which has a suffix y from the same P_i will have the same value $a_i \in \mathbb{F}_q$ in the first entry in each row of the common pending block, s.t. the vectors with suffixes from the different classes will have different values in these entries. (This corresponds to a FDMRD code of distance $k-2$ and size q.) Given the filling of the first entries of every row, all the other entries of the pending blocks are filled by a FDMRD code with minimum distance $k-3$, according to Lemma 22.
- All Ferrers diagrams that correspond to the vectors in $\mathcal{A}_3^k$ have a common pending block with $k-2$ rows and $\sum_{i=3}^{k-j} i+2$ dots in the jth row, $1 \leq j \leq k-2$. The filling of these pending blocks is analogous to the previous case, but for the suffixes from the different P_i-classes we fix the first two entries in each row of a pending block. Hence, there are q^2 different possibilities.

Ferrers tableaux forms: On the dots corresponding to the last $n-s-2$ columns of the Ferrers diagrams for each vector v_j in a given $\mathcal{A}_i^k$, $0 \leq i \leq 3$, we construct a FDMRD code with minimum distance $k-1$ (according to Remark 21) and lift it to obtain $\mathbb{C}_{i,j}^k$. We define $\mathbb{C}_i^k = \bigcup_{j=1}^{|\mathcal{A}_i^k|} \mathbb{C}_{i,j}^k$.

Code: The final code is defined as

$$\mathbb{C}^k = \bigcup_{i=0}^{3} \mathbb{C}_i^k \cup \mathbb{C}_*^k.$$

Theorem 23. *The code $\mathbb{C}^k$ obtained by Construction II has minimum distance $2(k-1)$ and cardinality $|\mathbb{C}^k| = q^{2(n-k)} + q^{2(n-(k+(k-1)))} + \ldots + q^{2(n-(\sum_{i=3}^{k} i))} + \begin{bmatrix} n-(\sum_{i=3}^{k} i) \\ 2 \end{bmatrix}_q$.*

Proof: The cardinality of $\mathbb{C}^k$ follows from the following observation: $|\mathbb{C}^k| = |\mathbb{C}^{k-1}| + q^{2(n-k)}$ for any $k \geq 4$. The minimum distance follows from Theorem 10, Lemma 3 and Lemma 20. (For details see [14]).

■

Corollary 24. *Let $n \geq s+2+k$ and $q^2+q+1 \geq \ell$, where $s = \sum_{i=3}^{k} i$ and $\ell = n-s$ for odd $n-s$ (or $\ell = n-s-1$ for even $n-s$). Then*

$$A_q(n, 2(k-1), k) \geq \sum_{j=3}^{k} q^{2(n-\sum_{i=j}^{k} i)} + \begin{bmatrix} n-(\sum_{i=3}^{k} i) \\ 2 \end{bmatrix}_q .$$

Example 25. *Let $k=4$, $d=6$, $n=13$, and $q=2$. The code $\mathbb{C}^4$ obtained by Construction II has the cardinality $2^{18}+2^{12}+\begin{bmatrix} 6 \\ 2 \end{bmatrix}_q = 2^{18}+4747$ (the largest previously known code is of cardinality $2^{18}+4357$ [2]).*

Example 26. *Let $k=5$, $d=8$, $n=19$, and $q=2$. The code $\mathbb{C}^5$ obtained by Construction II has the cardinality $2^{28}+2^{20}+2^{14}+\begin{bmatrix} 7 \\ 2 \end{bmatrix}_q = 2^{28}+1067627$ (the largest previously known code is of cardinality $2^{28}+1052778$ [2]). (For more details see [14].)*

References

[1] M. Bossert and E. M. Gabidulin, "One family of algebraic codes for network coding," in *Proc. IEEE ISIT*, pp. 2863 - 2866, June 2009.

[2] T. Etzion and N. Silberstein, "Error-correcting codes in projective space via rank-metric codes and Ferrers diagrams," *IEEE Trans. Inform. Theory*, vol. 55, no.7, pp. 2909–2919, July 2009.

[3] T. Etzion and N. Silberstein, "Codes and designs related to lifted MRD codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 2, pp. 1004–1017, February 2013.

[4] T. Etzion and A. Vardy, "Error-correcting codes in projective space," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1165–1173, February 2011.

[5] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Problems of Information Transmission*, vol. 21, pp. 1-12, July 1985.

[6] E. M. Gabidulin and N. I. Pilipchuk, "Multicomponent network coding," in *Proc. Workshop on Coding and Cryptography*, pp. 443-452, 2011.

[7] M. Gadouleau and Z. Yan, "Constant-rank codes and their connection to constant-dimension codes," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3207-3216, July 2010.

[8] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3579-3591, August 2008.

[9] A. Kohnert and S. Kurz, "Construction of large constant-dimension codes with a prescribed minimum distance," *Lecture Notes in Computer Science*, vol. 5393, pp. 31–42, December 2008.

[10] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge University Press, 2001 (second edition).

[11] F. Manganiello, E. Gorla, and J. Rosenthal, "Spread codes and spread decoding in network coding," in *Proc. IEEE ISIT*, pp. 881–885, July 2008.

[12] R. M. Roth, "Maximum-rank array codes and their application to crisscross error correction," *IEEE Trans. Inform. Theory*, vol. 37, no.3, pp. 328-336, March 1991.

[13] V. Skachek, "Recursive code construction for random networks," *IEEE Trans. Inform. Theory*, vol. 56, no. 3, pp. 1378–1382, March 2010.

[14] N. Silberstein and A.-L. Trautmann, "New lower bounds for constant dimension codes," arXiv:1301.5961.

[15] D. Silva, F. R. Kschischang, and R. Koetter, "A Rank-metric approach to error control in random network coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, pp. 3951-3967, September 2008.

[16] A.-L. Trautmann, "A lower bound for constant dimension codes from multi-component lifted MRD codes," arXiv:1301.1918.

[17] A.-L. Trautmann and J. Rosenthal, "New improvements on the echelon-Ferrers construction," in *Proc. Int. Symp. on Math. Theory of Networks and Systems*, pp. 405–408, July 2010.