Constructions for constant dimension codes

Tao (弢) Feng (冯)

Department of Mathematics
Beijing Jiaotong University

Joint work with Shuangqing Liu and Yanxun Chang

July 1, 2019

Outline

1. Background and Definitions
2. Constructions for CDCs
   - Lifted maximum rank distance codes
   - Lifted Ferrers diagram rank-metric codes
   - Parallel constructions
   - Summary - Working points
3. Constructions for FDRM codes
   - Preliminaries
   - Via different representations of elements of a finite field
   - Based on Subcodes of MRD Codes
   - New FDRM codes from old

Network coding

Network coding, introduced in the paper [a], refers to coding at the intermediate nodes when information is multicasted in a network. Often information is modeled as vectors of fixed length over a finite field $\mathbb{F}_q$, called *packets*. To improve the performance of the communication, intermediate nodes should forward random linear $\mathbb{F}_q$-combinations of the packets they receive. Hence, the vector space spanned by the packets injected at the source is globally preserved in the network when no error occurs.

[a] R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, Network information flow, *IEEE Trans. Inf. Theory*, 46 (2000), 1204–1216.

A nice reference: C. Fragouli and E. Soljanin, Network coding fundamentals, *Foundations and Trends in Networking*, 2 (2007), 1–133.

Subspace codes and constant-dimension codes

Let $\mathbb{F}_q^n$ be the set of all vectors of length n over $\mathbb{F}_q$. $\mathbb{F}_q^n$ is a vector space with dimension n over $\mathbb{F}_q$.

- This observation led Kötter and Kschischang [a] to model network codes as subsets of projective space $\mathcal{P}_q(n)$, the set of all subspaces of $\mathbb{F}_q^n$, or of Grassmann space $\mathcal{G}_q(n,k)$, the set of all subspaces of $\mathbb{F}_q^n$ having dimension k.
- Subsets of $\mathcal{P}_q(n)$ are called *subspace codes* or *projective codes*, while subsets of the Grassmann space are referred to as *constant-dimension codes* or *Grassmann codes*.

[a] R. Kötter and F.R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inf. Theory*, 54 (2008), 3579–3591.

The subspace distance

Definition

The subspace distance

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &:= \dim\,(\mathcal{U}+\mathcal{V}) - \dim\,(\mathcal{U}\cap\mathcal{V}) \\ &= \dim\,\mathcal{U} + \dim\,\mathcal{V} - 2\dim(\mathcal{U}\cap\mathcal{V}) \end{aligned}$$

for all $\mathcal{U},\mathcal{V}\in\mathcal{P}_q(n)$ is used as a distance measure for subspace codes.

- This talk only focuses on constant dimension codes (CDC).
- An $(n,d,k)_q$-CDC with M codewords is written as $(n,M,d,k)_q$-CDC.

The subspace distance

Definition

The subspace distance

$$d_S(\mathcal{U},\mathcal{V}) := \dim\ (\mathcal{U}+\mathcal{V}) - \dim\ (\mathcal{U}\cap\mathcal{V})$$
$$= \dim \mathcal{U} + \dim\ \mathcal{V} - 2\dim(\mathcal{U}\cap\mathcal{V})$$

for all $\mathcal{U},\mathcal{V}\in\mathcal{P}_q(n)$ is used as a distance measure for subspace codes.

- This talk only focuses on constant dimension codes (CDC).
- An $(n,d,k)_q$-CDC with M codewords is written as $(n,M,d,k)_q$-CDC.
- Given n,d,k and q, denote by $A_q(n,d,k)$ the maximum number of codewords among all $(n,d,k)_q$-CDCs.
- An $(n,d,k)_q$-CDC with $A_q(n,d,k)$ codewords is said to be optimal.

Some upper bounds

- Singleton bound (Theorem 9 in [a]):

$$A_q(n, 2\delta, k) \leq \begin{bmatrix} n-\delta+1 \\ k-\delta+1 \end{bmatrix}_q .$$

- Johnson-Type bound (Theorem 3 in [b])

$$A_q(n, 2\delta, k) \leq \frac{q^n-1}{q^k-1} A_q(n-1, 2\delta, k-1).$$

[a] R. Kötter and F.R. Kschischang, Coding for errors and erasures in random network coding, *IEEE Trans. Inf. Theory*, 54 (2008), 3579–3591.

[b] S.-T. Xia and F.-W. Fu, Johnson type bounds on constant dimension codes, *Des. Codes Cryptogr.*, 50 (2009), 163–172.

- http://subspacecodes.uni-bayreuth.de. (Maintained by Daniel Heinlein, Michael Kiermaier, Sascha Kurz, Alfred Wassermann)

Remarks on parameters n, d and k

- By taking orthogonal complements of subspaces for each codeword of an $(n, d, k)_q$-CDC, one can get an $(n, d, n-k)_q$-CDC.

Proposition

$A_q(n, d, k) = A_q(n, d, n-k)$.

Proof.

$$\begin{aligned} d_S(\overline{\mathcal{U}}, \overline{\mathcal{V}}) &= \dim \overline{\mathcal{U}} + \dim \overline{\mathcal{V}} - 2\dim(\overline{\mathcal{U}} \cap \overline{\mathcal{V}}) \\ &= n - \dim \mathcal{U} + n - \dim \mathcal{V} - 2(n - \dim(\mathcal{U} + \mathcal{V})) \\ &= 2\dim(\mathcal{U} + \mathcal{V}) - \dim \mathcal{U} - \dim \mathcal{V} \\ &= \dim\ (\mathcal{U} + \mathcal{V}) - \dim\ (\mathcal{U} \cap \mathcal{V}) = d_S(\mathcal{U}, \mathcal{V}). \end{aligned}$$

□

- Therefore, assume that $n \geq 2k$.

Remarks on parameters n, d and k

- For $\mathcal{U} \neq \mathcal{V} \in \mathcal{G}_q(n,k)$,

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= \dim \mathcal{U} + \dim \mathcal{V} - 2\dim(\mathcal{U} \cap \mathcal{V}) \\ &= 2k - 2\dim(\mathcal{U} \cap \mathcal{V}). \end{aligned}$$

- Therefore, assume that $n \geq 2k \geq d$.

Matrix representation of subspaces

- For $\mathcal{U} \neq \mathcal{V} \in \mathcal{G}_q(n,k)$,

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= 2k - 2\dim(\mathcal{U} \cap \mathcal{V}) \\ &= 2 \cdot rank \begin{pmatrix} \mathbf{U} \\ \mathbf{V} \end{pmatrix} - 2k, \end{aligned}$$

  where $\mathbf{U} \in Mat_{k\times n}(\mathbb{F}_q)$ is a matrix such that $\mathcal{U}$ =rowspace($\mathbf{U}$).
- The matrix **U** is usually not unique.

Outline

Rank metric codes

Let $\mathbb{F}_q^{m\times n}$ denote the set of all $m \times n$ matrices over $\mathbb{F}_q$. It is an $\mathbb{F}_q$-vector space.

- The rank distance on $\mathbb{F}_q^{m\times n}$ is defined by

$$d_R(\mathbf{A}, \mathbf{B}) = rank(\mathbf{A} - \mathbf{B})$$

for $\mathbf{A}, \mathbf{B} \in \mathbb{F}_q^{m\times n}$.

- An $[m \times n, k, \delta]_q$ rank metric code $\mathcal{D}$ is a k-dimensional $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{m\times n}$ with *minimum rank distance*

$$\delta = \min_{\mathbf{A},\mathbf{B}\in\mathcal{C},\mathbf{A}\neq\mathbf{B}} \{d_R(\mathbf{A}, \mathbf{B})\}.$$

Maximum rank distance codes

Singleton-like upper bound for MRD codes

Any rank-metric codes $[m \times n, k, \delta]_q$ code satisfies that

$$k \leq \max\{m, n\}(\min\{m, n\} - \delta + 1).$$

When the equality holds, $\mathcal{D}$ is called a *linear maximum rank distance code*, denoted by an MRD$[m \times n, \delta]_q$ code. Linear MRD codes exists for all feasible parameters[a] [b] [c].

[a] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory A*, 25 (1978), 226–241.

[b] È.M. Gabidulin, Theory of codes with maximum rank distance, *Problems Inf. Transmiss.*, 21 (1985), 3–16.

[c] R.M. Roth, Maximum-rank array codes and their application to crisscross error correction, *IEEE Trans. Inf. Theory*, 37 (1991), 328–336.

Lifted MRD codes

Theorem

Let $n \geq 2k$. The lifted MRD code

$$\mathcal{C} = \{(\boldsymbol{I}_k \mid \boldsymbol{A}) : \boldsymbol{A} \in \mathcal{D}\}$$

is an $(n, q^{(n-k)(k-\delta+1)}, 2\delta, k)_q$-CDC, where $\mathcal{D}$ is an MRD$[k \times (n-k), \delta]_q$ code [a].

[a] D. Silva, F.R. Kschischang, and R. Kötter, A rank-metric approach to error control in random network coding, *IEEE Trans. Inf. Theory*, 54 (2008), 3951–3967.

- Recall that $d_S(\mathcal{U}, \mathcal{V}) = 2 \cdot rank\binom{\mathbf{U}}{\mathbf{V}} - 2k$.

Lifted MRD codes

Proof.

It suffices to check the subspace distance of $\mathcal{C}$. For any $\mathcal{U}, \mathcal{V} \in \mathcal{C}$ and $\mathcal{U} \neq \mathcal{V}$, where $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A})$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{B})$, we have

$$d_S(\mathcal{U}, \mathcal{V}) = 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A} \\ \boldsymbol{I}_k & \boldsymbol{B} \end{pmatrix} - 2k = 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A} \\ \boldsymbol{O} & \boldsymbol{B} - \boldsymbol{A} \end{pmatrix} - 2k$$
$$= 2 \cdot rank(\boldsymbol{B} - \boldsymbol{A}) \geq 2\delta.$$

□

Lifted MRD codes

Proof.

It suffices to check the subspace distance of $\mathcal{C}$. For any $\mathcal{U}, \mathcal{V} \in \mathcal{C}$ and $\mathcal{U} \neq \mathcal{V}$, where $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A})$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{B})$, we have

$$\begin{aligned} d_S(\mathcal{U}, \mathcal{V}) &= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A} \\ \boldsymbol{I}_k & \boldsymbol{B} \end{pmatrix} - 2k = 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A} \\ \boldsymbol{O} & \boldsymbol{B} - \boldsymbol{A} \end{pmatrix} - 2k \\ &= 2 \cdot rank(\boldsymbol{B} - \boldsymbol{A}) \geq 2\delta. \end{aligned}$$

□

- Silva, Kschischang and Kötter pointed out that lifted MRD codes can result in asymptotically optimal CDCs, and can be decoded efficiently in the context of random linear network coding.

Outline

Ferrers diagram rank-metric codes

- To obtain optimal CDCs, Etzion and Silberstein [1] presented an effective construction, named the multilevel construction, which generalizes the lifted MRD codes construction by introducing a new family of rank-metric codes: Ferrers diagram rank-metric codes.
- A Ferrers diagram $\mathcal{F}$ is a pattern of dots such that all dots are shifted to the right of the diagram and the number of dots in a row is less than or equal to the number of dots in the row above.
- For example, let $\mathcal{F} = [2, 3, 4, 5]$ be a 5×4 Ferrers diagram:

$$\mathcal{F} = \begin{array}{cccc} \bullet & \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet \\ & & \bullet & \bullet \\ & & & \bullet \end{array}, \quad \mathcal{F}^t = \begin{array}{ccccc} \bullet & \bullet & \bullet & \bullet & \bullet \\ & \bullet & \bullet & \bullet & \bullet \\ & & \bullet & \bullet & \bullet \\ & & & \bullet & \bullet \end{array}.$$

[1] T. Etzion and N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, *IEEE Trans. Inf. Theory*, 55 (2009), 2909–2919.

Ferrers diagram rank-metric codes

- Let $\mathcal{F}$ be a Ferrers diagram of size $m \times n$. A Ferrers diagram code $\mathcal{C}$ in $\mathcal{F}$ is an $[m \times n, k, \delta]_q$ rank metric code such that all entries not in $\mathcal{F}$ are 0. Denote it by an $[\mathcal{F}, k, \delta]_q$ code.

Ferrers diagram rank-metric codes

- Let $\mathcal{F}$ be a Ferrers diagram of size $m \times n$. A Ferrers diagram code $\mathcal{C}$ in $\mathcal{F}$ is an $[m \times n, k, \delta]_q$ rank metric code such that all entries not in $\mathcal{F}$ are 0. Denote it by an $[\mathcal{F}, k, \delta]_q$ code.
- An $[\mathcal{F}, k, \delta]_q$ code exists if and only if an $[\mathcal{F}^t, k, \delta]_q$ code exists.
- W.l.o.g, assume that $m \geq n \geq \delta$.

Matrix representation of a codeword in subspace codes

Example

An $\mathcal{U} \in \mathcal{G}_2(7,3)$ is listed below:

$$\begin{array}{lll} (0,0,0,0,0,0,0), & (1,0,1,1,0,0,0), & (1,0,0,1,1,0,1), \\ (1,0,1,0,0,1,1), & (0,0,1,0,1,0,1), & (0,0,0,1,0,1,1), \\ (0,0,1,1,1,1,0), & (1,0,0,0,1,1,0). & \end{array}$$

The basis of $\mathcal{U}$ can be represented by a 3×7 matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

However there exists a unique matrix representation of elements of the Grassmannian, namely the reduced row echelon forms.

The identifying vector

Definition

The identifying vector $v(\mathbf{U})$ of a matrix $\mathbf{U}$ in reduced row echelon form is the binary vector of length n and weight k such that the $1's$ of $v(\mathbf{U})$ are in the positions where $\mathbf{U}$ has its leading ones.

Example

The basis of $\mathcal{U}$ can be represented by a 3×7 matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Its identifying vector is (1011000).

Two basic lemmas

Lemma 1 [Etzion and Silberstein, 2009]

Let $\mathcal{U}$ and $\mathcal{V} \in \mathcal{G}_q(n,k)$ and **U** and **V** their reduced row echelon matrices representation, respectively. Let $v(\mathbf{U}) = v(\mathbf{V})$. Then

$$d_S(\mathcal{U},\mathcal{V}) = 2d_R(\mathbf{D_U},\mathbf{D_V}),$$

where $\mathbf{D_U}$ and $\mathbf{D_V}$ denote the submatrices of **U** and **V**, respectively, without the columns of their leading ones.

- To prove it, simply use the fact that $d_S(\mathcal{U},\mathcal{V}) = 2 \cdot rank\binom{\mathbf{U}}{\mathbf{V}} - 2k$.

Two basic lemmas

Lemma 2 [Etzion and Silberstein, 2009]

Let $\mathcal{U}$ and $\mathcal{V} \in \mathcal{G}_q(n,k)$, and **U** and **V** be their reduced row echelon matrices representation, respectively. Then

$$d_S(\mathcal{U},\mathcal{V}) \geq d_H(v(\mathbf{U}), v(\mathbf{V})).$$

Example

Task: Construct a constant-dimension code in $\mathbb{F}_2^6$ with subspace distance 4 and each codeword having dimension 3.

Step 1: Let $n = 6$, $k = 3$, and

$$\mathcal{C} = \{(111000, 100110, 010101, 001011)\}$$

be a constant weight code of length 6, weight 3, and minimum Hamming distance 4.

Step 2:

$$(111000) : \begin{pmatrix} 1 & 0 & 0 & \bullet & \bullet & \bullet \\ 0 & 1 & 0 & \bullet & \bullet & \bullet \\ 0 & 0 & 1 & \bullet & \bullet & \bullet \end{pmatrix} \longrightarrow \begin{pmatrix} \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \end{pmatrix}$$

$$(100110) : \begin{pmatrix} 1 & \bullet & \bullet & 0 & 0 & \bullet \\ 0 & 0 & 0 & 1 & 0 & \bullet \\ 0 & 0 & 0 & 0 & 1 & \bullet \end{pmatrix} \longrightarrow \begin{pmatrix} \bullet & \bullet & \bullet \\ 0 & 0 & \bullet \\ 0 & 0 & \bullet \end{pmatrix}$$

Example

Step 2 (Cont.):

$$(010101):\begin{pmatrix} 0 & 1 & \bullet & 0 & \bullet & 0 \\ 0 & 0 & 0 & 1 & \bullet & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} \bullet & \bullet \\ 0 & \bullet \end{pmatrix}$$

$$(001011):\begin{pmatrix} 0 & 0 & 1 & \bullet & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} \bullet \end{pmatrix}$$

Multilevel construction [Etzion and Silberstein, 2009]

1. Take a binary Hamming code of length n, weight k and minimum Hamming distance 2δ.
2. Find the corresponding matrices (i.e., Ferrers diagrams) such that these codewords are their identifying vectors.
3. Fill each of the Ferrers diagrams with a compatible Ferrers diagram code with minimum rank distance δ.

One can check (with the two Lemmas) that the row spaces of the resulting matrices form a constant dimension code in $\mathcal{G}_q(n, k)$ with minimum subspace distance 2δ.

[2] A.-L. Trautmann and J. Rosenthal, New improvements on the Echelon-Ferrers construction, in Proc. 19th Int. Symp. Math. Theory Netw. Syst., Jul. 2010, 405–408.

Multilevel construction [Etzion and Silberstein, 2009]

1. Take a binary Hamming code of length n, weight k and minimum Hamming distance 2δ.
2. Find the corresponding matrices (i.e., Ferrers diagrams) such that these codewords are their identifying vectors.
3. Fill each of the Ferrers diagrams with a compatible Ferrers diagram code with minimum rank distance δ.

One can check (with the two Lemmas) that the row spaces of the resulting matrices form a constant dimension code in $\mathcal{G}_q(n,k)$ with minimum subspace distance 2δ.

- Remark: the skeleton codes; lexicodes; pending dots[2]

[2] A.-L. Trautmann and J. Rosenthal, New improvements on the Echelon-Ferrers construction, in Proc. 19th Int. Symp. Math. Theory Netw. Syst., Jul. 2010, 405–408.

Remark [Liu, Chang, F., 2019+]

(n, k, d)	known lower bound	improved lower bound
(10,5,6)	$q^{15} + q^6 + 2q^2 + q + 1$	$q^{15} + q^6 + 2q^2 + q + 2$
(11,5,6)	$q^{18} + q^9 + q^6$ $+q^5 + 3q^4 + 3q^3 + 3q^2 + q$	$q^{18} + q^9 + q^6$ $+3q^5 + 3q^4 + q^3 + 3q^2 + q + 1$
(14,4,6)	$q^{20} + q^{14} + q^{10} + q^9$ $+q^8 + 2(q^6 + q^5 + q^4) + q^3 + q^2$	$q^{20} + q^{14} + q^{10} + q^9$ $+2q^8 + O(q^8)$

Outline

Xu and Chen's Construction

Theorem [Xu and Chen, 2018]

For any positive integers k and δ such that $k \geq 2\delta$,

$$A_q(2k, 2\delta, k) \geq q^{k(k-\delta+1)} + \sum_{i=\delta}^{k-\delta} A_i,$$

where A_i denotes the number of codewords with rank i in an MRD$[k \times k, \delta]_q$ code [a].

[a] L. Xu and H. Chen, New constant-Dimension subspace codes from maximum rank distance codes, *IEEE Trans. Inf. Theory*, 64 (2018), 6315–6319.

- Their proof depends on some knowledge of linearized polynomials.

Rank distribution

Theorem

Let $\mathcal{D}$ be an MRD$[m \times n, \delta]_q$ code, and $A_i = |M \in \mathcal{D} : rank(M) = i|$ for $0 \leq i \leq n$. Its rank distribution is given by $A_0 = 1$, $A_i = 0$ for $1 \leq i \leq \delta - 1$, and

$$A_{\delta+i} = \begin{bmatrix} n \\ \delta + i \end{bmatrix}_q \sum_{j=0}^{i} (-1)^{j-i} \begin{bmatrix} \delta + i \\ i - j \end{bmatrix}_q q^{\binom{i-j}{2}} (q^{m(j+1)} - 1)$$

for $0 \leq i \leq n - \delta$ [a] [b].

[a] P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, *J. Combin. Theory A*, 25 (1978), 226–241.

[b] È.M. Gabidulin, Theory of codes with maximum rank distance, *Problems Inf. Transmiss.*, 21 (1985), 3–16.

Rank metric codes with given ranks

- Let $K \subseteq \{0, 1, \ldots, n\}$ and δ be a positive integer.

Definition

$\mathcal{D} \subseteq \mathbb{F}_q^{m \times n}$ is an $(m \times n, \delta, K)_q$ rank metric code with given ranks (GRMC) if it satisfies

(1) $rank(\boldsymbol{D}) \in K$ for any $\boldsymbol{D} \in \mathcal{D}$;

(2) $d_R(\boldsymbol{D}_1, \boldsymbol{D}_2) := rank(\boldsymbol{D}_1 - \boldsymbol{D}_2) \geq \delta$ for any $\boldsymbol{D}_1 \neq \boldsymbol{D}_2 \in \mathcal{D}$.

- When $K = \{0, 1, \ldots, n\}$, a GRMC is just a usual rank-metric code (not necessarily linear).

Rank metric codes with given ranks

- Let $K \subseteq \{0, 1, \ldots, n\}$ and δ be a positive integer.

Definition

$\mathcal{D} \subseteq \mathbb{F}_q^{m\times n}$ is an $(m \times n, \delta, K)_q$ rank metric code with given ranks (GRMC) if it satisfies

(1) $rank(\boldsymbol{D}) \in K$ for any $\boldsymbol{D} \in \mathcal{D}$;

(2) $d_R(\boldsymbol{D}_1, \boldsymbol{D}_2) := rank(\boldsymbol{D}_1 - \boldsymbol{D}_2) \geq \delta$ for any $\boldsymbol{D}_1 \neq \boldsymbol{D}_2 \in \mathcal{D}$.

- When $K = \{0, 1, \ldots, n\}$, a GRMC is just a usual rank-metric code (not necessarily linear).
- If $|\mathcal{D}| = M$, then it is often written as an $(m \times n, M, \delta, K)_q$-GRMC.

Parallel construction

Theorem [Liu, Chang, F., 2019+]

Let $n \geq 2k \geq 2\delta$. If there exists a $(k \times (n-k), M, \delta, [0, k-\delta])_q$-GRMC, then there exists an $(n, q^{(n-k)(k-\delta+1)} + M, 2\delta, k)_q$-CDC.

Parallel construction

Theorem [Liu, Chang, F., 2019+]

Let $n \geq 2k \geq 2\delta$. If there exists a $(k \times (n-k), M, \delta, [0, k-\delta])_q$-GRMC, then there exists an $(n, q^{(n-k)(k-\delta+1)} + M, 2\delta, k)_q$-CDC.

Proof.

- $\mathcal{D}_1$: MRD$[k \times (n-k), \delta]_q$ code.
- $\mathcal{D}_2$: $(k \times (n-k), M, \delta, [0, k-\delta])_q$-GRMC.
- $\mathcal{C}_1 = \{(\boldsymbol{I}_k \mid \boldsymbol{A}) : \boldsymbol{A} \in \mathcal{D}_1\}$.
- $\mathcal{C}_2 = \{(\boldsymbol{B} \mid \boldsymbol{I}_k) : \boldsymbol{B} \in \mathcal{D}_2\}$.
- Then $\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$ forms an $(n, q^{(n-k)(k-\delta+1)} + M, 2\delta, k)_q$-CDC.

$\square$

Parallel construction

Proof.

For any $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A}) \in \mathcal{C}_1$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{B} \mid \boldsymbol{I}_k) \in \mathcal{C}_2$, where $\boldsymbol{A} = (\underbrace{\boldsymbol{A}_1}_{n-2k} \mid \underbrace{\boldsymbol{A}_2}_{k})$ and $\boldsymbol{B} = (\underbrace{\boldsymbol{B}_1}_{k} \mid \underbrace{\boldsymbol{B}_2}_{n-2k})$, we have

$$d_S(\mathcal{U}, \mathcal{V}) = 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{B}_1 & \boldsymbol{B}_2 & \boldsymbol{I}_k \end{pmatrix} - 2k$$

Parallel construction

Proof.

For any $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A}) \in \mathcal{C}_1$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{B} \mid \boldsymbol{I}_k) \in \mathcal{C}_2$, where $\boldsymbol{A} = (\underbrace{\boldsymbol{A}_1}_{n-2k} \mid \underbrace{\boldsymbol{A}_2}_{k})$ and $\boldsymbol{B} = (\underbrace{\boldsymbol{B}_1}_{k} \mid \underbrace{\boldsymbol{B}_2}_{n-2k})$, we have

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{B}_1 & \boldsymbol{B}_2 & \boldsymbol{I}_k \end{pmatrix} - 2k \\ &= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{O} & \boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 & \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2 \end{pmatrix} - 2k \end{aligned}$$

Parallel construction

Proof.

For any $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A}) \in \mathcal{C}_1$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{B} \mid \boldsymbol{I}_k) \in \mathcal{C}_2$, where $\boldsymbol{A} = (\underbrace{\boldsymbol{A}_1}_{n-2k} \mid \underbrace{\boldsymbol{A}_2}_{k})$ and $\boldsymbol{B} = (\underbrace{\boldsymbol{B}_1}_{k} \mid \underbrace{\boldsymbol{B}_2}_{n-2k})$, we have

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{B}_1 & \boldsymbol{B}_2 & \boldsymbol{I}_k \end{pmatrix} - 2k \\ &= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{O} & \boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 & \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2 \end{pmatrix} - 2k \\ &= 2 \cdot rank(\boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 \mid \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \end{aligned}$$

Parallel construction

Proof.

For any $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A}) \in \mathcal{C}_1$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{B} \mid \boldsymbol{I}_k) \in \mathcal{C}_2$, where $\boldsymbol{A} = (\underbrace{\boldsymbol{A}_1}_{n-2k} \mid \underbrace{\boldsymbol{A}_2}_{k})$ and $\boldsymbol{B} = (\underbrace{\boldsymbol{B}_1}_{k} \mid \underbrace{\boldsymbol{B}_2}_{n-2k})$, we have

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{B}_1 & \boldsymbol{B}_2 & \boldsymbol{I}_k \end{pmatrix} - 2k \\ &= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{O} & \boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 & \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2 \end{pmatrix} - 2k \\ &= 2 \cdot rank(\boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 \mid \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\ &\geq 2 \cdot rank(\boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \end{aligned}$$

Parallel construction

Proof.

For any $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A}) \in \mathcal{C}_1$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{B} \mid \boldsymbol{I}_k) \in \mathcal{C}_2$, where $\boldsymbol{A} = (\underbrace{\boldsymbol{A}_1}_{n-2k} \mid \underbrace{\boldsymbol{A}_2}_{k})$ and $\boldsymbol{B} = (\underbrace{\boldsymbol{B}_1}_{k} \mid \underbrace{\boldsymbol{B}_2}_{n-2k})$, we have

$$
\begin{aligned}
d_S(\mathcal{U}, \mathcal{V}) &= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{B}_1 & \boldsymbol{B}_2 & \boldsymbol{I}_k \end{pmatrix} - 2k \\
&= 2 \cdot rank \begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{O} & \boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 & \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2 \end{pmatrix} - 2k \\
&= 2 \cdot rank(\boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 \mid \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\
&\geq 2 \cdot rank(\boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\
&\geq 2k - 2 \cdot rank(\boldsymbol{B}_1\boldsymbol{A}_2)
\end{aligned}
$$

Parallel construction

Proof.

For any $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A}) \in \mathcal{C}_1$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{B} \mid \boldsymbol{I}_k) \in \mathcal{C}_2$, where $\boldsymbol{A} = (\underbrace{\boldsymbol{A}_1}_{n-2k} \mid \underbrace{\boldsymbol{A}_2}_{k})$ and $\boldsymbol{B} = (\underbrace{\boldsymbol{B}_1}_{k} \mid \underbrace{\boldsymbol{B}_2}_{n-2k})$, we have

$$\begin{aligned}
d_S(\mathcal{U},\mathcal{V}) &= 2\cdot rank\begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{B}_1 & \boldsymbol{B}_2 & \boldsymbol{I}_k \end{pmatrix} - 2k \\
&= 2\cdot rank\begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{O} & \boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 & \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2 \end{pmatrix} - 2k \\
&= 2\cdot rank(\boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 \mid \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\
&\geq 2\cdot rank(\boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\
&\geq 2k - 2\cdot rank(\boldsymbol{B}_1\boldsymbol{A}_2) \\
&\geq 2k - 2\cdot rank(\boldsymbol{B}_1)
\end{aligned}$$

Parallel construction

Proof.

For any $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A}) \in \mathcal{C}_1$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{B} \mid \boldsymbol{I}_k) \in \mathcal{C}_2$, where $\boldsymbol{A} = (\underbrace{\boldsymbol{A}_1}_{n-2k} \mid \underbrace{\boldsymbol{A}_2}_{k})$ and $\boldsymbol{B} = (\underbrace{\boldsymbol{B}_1}_{k} \mid \underbrace{\boldsymbol{B}_2}_{n-2k})$, we have

$$\begin{aligned}
d_S(\mathcal{U},\mathcal{V}) &= 2\cdot rank\begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{B}_1 & \boldsymbol{B}_2 & \boldsymbol{I}_k \end{pmatrix} - 2k \\
&= 2\cdot rank\begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{O} & \boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 & \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2 \end{pmatrix} - 2k \\
&= 2\cdot rank(\boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 \mid \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\
&\geq 2\cdot rank(\boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\
&\geq 2k - 2\cdot rank(\boldsymbol{B}_1\boldsymbol{A}_2) \\
&\geq 2k - 2\cdot rank(\boldsymbol{B}_1) \\
&\geq 2k - 2\cdot rank(\boldsymbol{B})
\end{aligned}$$

Parallel construction

Proof.

For any $\mathcal{U} = \text{rowspace}(\boldsymbol{I}_k \mid \boldsymbol{A}) \in \mathcal{C}_1$ and $\mathcal{V} = \text{rowspace}(\boldsymbol{B} \mid \boldsymbol{I}_k) \in \mathcal{C}_2$, where $\boldsymbol{A} = (\underbrace{\boldsymbol{A}_1}_{n-2k} \mid \underbrace{\boldsymbol{A}_2}_{k})$ and $\boldsymbol{B} = (\underbrace{\boldsymbol{B}_1}_{k} \mid \underbrace{\boldsymbol{B}_2}_{n-2k})$, we have

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= 2\cdot rank\begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{B}_1 & \boldsymbol{B}_2 & \boldsymbol{I}_k \end{pmatrix} - 2k \\ &= 2\cdot rank\begin{pmatrix} \boldsymbol{I}_k & \boldsymbol{A}_1 & \boldsymbol{A}_2 \\ \boldsymbol{O} & \boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 & \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2 \end{pmatrix} - 2k \\ &= 2\cdot rank(\boldsymbol{B}_2 - \boldsymbol{B}_1\boldsymbol{A}_1 \mid \boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\ &\geq 2\cdot rank(\boldsymbol{I}_k - \boldsymbol{B}_1\boldsymbol{A}_2) \\ &\geq 2k - 2\cdot rank(\boldsymbol{B}_1\boldsymbol{A}_2) \\ &\geq 2k - 2\cdot rank(\boldsymbol{B}_1) \\ &\geq 2k - 2\cdot rank(\boldsymbol{B}) \geq 2\delta. \end{aligned}$$

□

Lower bound for GRMCs

Given m, n, K and δ, denote by $A_q^R(m \times n, \delta, K)$ the maximum number of codewords among all $(m \times n, \delta, K)_q$-GRMCs.

Theorem [Liu, Chang, F., 2019+]

Let $m \geq n$ and $1 \leq \delta \leq n$. Let t_1 be a nonnegative integer and t_2 be a positive integer such that $t_1 \leq t_2 \leq n$. Then

$$A_q^R(m \times n, \delta, [t_1, t_2]) \geq \begin{cases} \sum_{i=t_1}^{t_2} A_i(\delta), & t_2 \geq \delta; \\ \max_{\max\{1,t_1\} \leq a < \delta} \{\lceil \frac{\sum_{i=\max\{1,t_1\}}^{t_2} A_i(a)}{q^{m(\delta-a)} - 1} \rceil\}, & t_2 < \delta, \end{cases}$$

where $A_i(x)$ denotes the number of codewords with rank i in an MRD$[m \times n, x]_q$ code.

Lower bound for GRMCs

Given m, n, K and δ, denote by $A_q^R(m \times n, \delta, K)$ the maximum number of codewords among all $(m \times n, \delta, K)_q$-GRMCs.

Theorem [Liu, Chang, F., 2019+]

Let $m \geq n$ and $1 \leq \delta \leq n$. Let t_1 be a nonnegative integer and t_2 be a positive integer such that $t_1 \leq t_2 \leq n$. Then

$$A_q^R(m \times n, \delta, [t_1, t_2]) \geq \begin{cases} \displaystyle\sum_{i=t_1}^{t_2} A_i(\delta), & t_2 \geq \delta; \\ \displaystyle\max_{\max\{1,t_1\} \leq a < \delta} \{\lceil \frac{\sum_{i=\max\{1,t_1\}}^{t_2} A_i(a)}{q^{m(\delta-a)} - 1} \rceil\}, & t_2 < \delta, \end{cases}$$

where $A_i(x)$ denotes the number of codewords with rank i in an MRD$[m \times n, x]_q$ code.

Lower bound for CDCs

Theorem [Liu, Chang, F., 2019+]

Let $n \geq 2k > 2\delta > 0$. Then

$$A_q(n, 2\delta, k) \geq q^{(n-k)(k-\delta+1)} + \begin{cases} \sum_{i=\delta}^{k-\delta} A_i(\delta) + 1, & k \geq 2\delta; \\ \max_{1 \leq a < \delta} \{\lceil \frac{\sum_{i=1}^{k-\delta} A_i(a)}{q^{m(\delta-a)} - 1} \rceil\}, & k < 2\delta, \end{cases}$$

where $A_i(x)$ denotes the number of codewords with rank i in an MRD$[m \times n, x]_q$ code.

Remarks

When $K = \{t\}$ for $0 \leq t \leq n$, an $(m \times n, M, \delta, K)_q$-GRMC is often called a constant-rank code [a].

[a] M. Gadouleau and Z. Yan, Constant-rank codes and their connection to constant-dimension codes, *IEEE Trans. Inform. Theory*, 56 (2010), 3207–3216.

Remarks

Using multilevel constructions and parallel constructions simultaneously, we can produce some CDCs with large size.
Here we just show one example.

Theorem [Liu, Chang, F., 2019+]

For $\delta \geq 2$,

$$q^{2\delta(\delta+1)} + (q^{2\delta} - 1)\begin{bmatrix} 2\delta \\ \delta \end{bmatrix}_q + q^{(\lfloor \frac{\delta}{2} \rfloor + 1)\delta} + q^{\delta} + 1 \leq A_q(4\delta,\ 2\delta,\ 2\delta) \leq q^{2\delta(\delta+1)} + (q^{2\delta} + q^{\delta})\begin{bmatrix} 2\delta \\ \delta \end{bmatrix}_q + 1.$$

- For $\delta \geq 3$,

$$\frac{\textit{the lower bound}}{\textit{the upper bound}} > 0.999260.$$

Outline

Summary - Working points

1. Show more lower bounds and upper bounds on $(m \times n, \delta, K)_q$ rank metric code with given ranks (GRMC).
2. How to use multilevel constructions and parallel constructions at the same time efficiently?
3. How to choose identifying vectors?
4. Establish constructions for Ferrers diagram rank-metric (FDRM) codes.

Outline

Upper bound on the size of FDRM codes

Theorem [Etzion and Silberstein, 2009]

Let δ be a positive integer and $\mathcal{F}$ be a Ferrers diagram. An $[\mathcal{F}, k, \delta]_q$ code satisfies

$$k \leq \min_{0 \leq i \leq \delta - 1} v_i,$$

where v_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.

- An FDRM code which attains the upper bound is called *optimal*.

Example

For $0 \le i \le \delta - 1$, v_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.

Example

Let $\delta = 2$ and

$$\mathcal{F} = \begin{matrix} \bullet & \bullet \\ \bullet & \bullet \end{matrix}.$$

One can take $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ as a basis of $[\mathcal{F}, 2, 2]_2$ code, which is optimal.

Recall: MRD codes

Singleton-like upper bound for MRD codes

Any rank-metric codes $[m \times n, k, \delta]_q$ code satisfies that

$$k \leq \max\{m, n\}(\min\{m, n\} - \delta + 1).$$

When the equality holds, $\mathcal{C}$ is called a *linear maximum rank distance code*, denoted by an MRD$[m \times n, \delta]_q$ code. Linear MRD codes exists for all feasible parameters.

Conjecture

Conjecture

For every $m \times n$-Ferrers diagram $\mathcal{F}$, every finite field $\mathbb{F}_q$, and every $\delta \leq min\{m, n\}$, there exists an optimal $[\mathcal{F}, k, \delta]_q$ code.

Remark

- The upper bound still holds for FDRM codes defined on any field.
- For algebraically closed field the bound sometimes cannot be attained [3].
- This talk only focuses on finite fields.

[3] E. Gorla and A. Ravagnani, Subspace codes from Ferrers diagrams, *J. Algebra and its Appl.*, 16 (2017), 1750131.

The cases of $\delta = 1, 2, 3$

Theorem

- For any $\mathcal{F}$, there exists an optimal $[\mathcal{F}, k, 1]_q$ codes, which is trivial.
- For any $\mathcal{F}$, there exists an optimal $[\mathcal{F}, k, 2]_q$ codes[a];
- For any square $\mathcal{F}$, there exists an optimal $[\mathcal{F}, k, 3]_q$ codes[b].

[a] T. Etzion and N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, *IEEE Trans. Inf. Theory*, 55 (2009), 2909–2919.

[b] T. Etzion, E. Gorla, A. Ravagnani and A. Wachter-Zeh, Optimal Ferrers diagram rank-metric codes, *IEEE Trans. Inf. Theory*, 62 (2016), 1616–1630.

Upper triangular shape with $\delta = n - 1$

Theorem

- Let $n \geq 3$. Assume $\mathcal{F} = [1, 2, \ldots, n]$ is an $n \times n$ Ferrers diagram. There exists an optimal $[\mathcal{F}, 3, n-1]_q$ code for any prime power q[a].

[a] J. Antrobus and H. Gluesing-Luerssen, Maximal Ferrers diagram codes: constructions and genericity considerations, arXiv:1804.00624v1.

References

1. T. Etzion, N. Silberstein, Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams, *IEEE Trans. Inf. Theory*, 55 (2009), 2909–2919.
2. T. Etzion, E. Gorla, A. Ravagnani, A. Wachter-Zeh, Optimal Ferrers diagram rank-metric codes, *IEEE Trans. Inf. Theory*, 62 (2016), 1616–1630.
3. T. Zhang, G. Ge, Constructions of optimal Ferrers diagram rank metric codes, *Des. Codes Cryptogr.*, 87 (2019), 107–121.
4. S. Liu, Y. Chang, T. Feng, Constructions for optimal Ferrers diagram rank-metric codes, *IEEE Trans. Inf. Theory*, 65 (2019), 4115–4130.
5. J. Antrobus, H. Gluesing-Luerssen, Maximal Ferrers diagram codes: constructions and genericity considerations, arXiv:1804.00624v1.
6. S. Liu, Y. Chang, T. Feng, Several classes of optimal Ferrers diagram rank-metric codes, arXiv:1809.00996v1.

Outline

Vector representation

- Let $\boldsymbol{\beta} = (\beta_0, \beta_1, \ldots, \beta_{m-1})$ be an ordered basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.
- There is a natural bijective map Ψ_m from $\mathbb{F}_{q^m}^n$ to $\mathbb{F}_q^{m\times n}$ as follows:

$$\Psi_m : \mathbb{F}_{q^m}^n \longrightarrow \mathbb{F}_q^{m\times n}$$
$$\mathbf{a} = (a_0, a_1, \ldots, a_{n-1}) \longmapsto \mathbf{A},$$

where $\mathbf{A} = \Psi_m(\mathbf{a}) \in \mathbb{F}_q^{m\times n}$ is defined such that for any $0 \le j \le n-1$

$$a_j = \sum_{i=0}^{m-1} A_{i,j}\beta_i.$$

- For $a \in \mathbb{F}_{q^m}$, write $\Psi_m((a))$ as $\Psi_m(a)$.
- Ψ_m satisfies linearity, i.e., $\Psi_m(x\boldsymbol{a}_1 + y\boldsymbol{a}_2) = x\Psi_m(\boldsymbol{a}_1) + y\Psi_m(\boldsymbol{a}_2)$ for any $x, y \in \mathbb{F}_q$ and $\boldsymbol{a}_1, \boldsymbol{a}_2 \in \mathbb{F}_{q^m}^n$.

Theorem [Zhang, Ge, DCC, 2019]

If there exists an $[\mathcal{F}, k, \delta]_{q^m}$ code, where $\mathcal{F} = [\gamma_0, \gamma_1, \ldots, \gamma_{n-1}]$, then there exists an $[\mathcal{F}', mk, \delta]_q$ code, where $\mathcal{F}' = [m\gamma_0, m\gamma_1, \ldots, m\gamma_{n-1}]$.

Matrix representation

Let $g(x) = x^m + g_{m-1}x^{m-1} + \cdots + g_1 x + g_0 \in \mathbb{F}_q[x]$ be a primitive polynomial over $\mathbb{F}_q$, whose companion matrix is

$$\boldsymbol{G} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -g_0 \\ 1 & 0 & 0 & \cdots & 0 & -g_1 \\ 0 & 1 & 0 & \cdots & 0 & -g_2 \\ 0 & 0 & 1 & \cdots & 0 & -g_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -g_{m-1} \end{pmatrix}.$$

By the Cayley-Hamilton theorem in linear algebra, $\boldsymbol{G}$ is a root of $g(x)$. The set $\mathcal{A} = \{\boldsymbol{G}^i : 0 \le i \le q^m - 2\} \cup \{\boldsymbol{0}\}$ equipped with the matrix addition and the matrix multiplication is isomorphic to $\mathbb{F}_{q^m}$.

Matrix representation

Theorem [Liu, Chang, F., arXiv:1809.00996]

If there exists an $[\mathcal{F}, k, \delta]_{q^m}$ code, where $\mathcal{F} = [\gamma_0, \gamma_1, \dots, \gamma_{n-1}]$, then there exists an $[\mathcal{F}', mk, m\delta]_q$ code, where

$$\mathcal{F}' = [\underbrace{m\gamma_0, \dots, m\gamma_0}_{m}, \underbrace{m\gamma_1, \dots, m\gamma_1}_{m}, \dots, \underbrace{m\gamma_{n-1}, \dots, m\gamma_{n-1}}_{r}].$$

Example

If there exists an optimal $[\mathcal{F}, \gamma_0, n]_{q^m}$ code $\mathcal{F} = [\gamma_0, \gamma_1, \dots, \gamma_{n-1}]$, then there exists an optimal $[\mathcal{F}', m\gamma_0, mn]_q$ code, where

$$\mathcal{F}' = [\underbrace{m\gamma_0, \dots, m\gamma_0}_{m}, \underbrace{m\gamma_1, \dots, m\gamma_1}_{m}, \dots, \underbrace{m\gamma_{n-1}, \dots, m\gamma_{n-1}}_{m}].$$

Outline

Basic idea

Basic lemma

Let $m \geq n$ and $0 \leq \lambda_0 \leq \lambda_1 \leq \cdots \leq \lambda_{\kappa-1} \leq m$.

- Let $\mathbf{G}$ be a generator matrix of a systematic MRD$[m \times n, \delta]_q$ code, i.e., $\mathbf{G}$ is of the form $(\mathbf{I}_\kappa | \mathbf{A})$, where $\kappa = n - \delta + 1$.
- Let $\mathbf{U} = \{(u_0, \ldots, u_{\kappa-1}) \in \mathbb{F}_{q^m}^{\kappa} :$ $\Psi_m(u_i) = (u_{i,0}, \ldots, u_{i,\lambda_i - 1}, 0, \ldots, 0)^T, u_{i,j} \in \mathbb{F}_q, i \in [\kappa], j \in [\lambda_i]\}$.

Then $\mathcal{C} = \{\Psi_m(\mathbf{c}) : \mathbf{c} = \mathbf{uG}, \mathbf{u} \in \mathbf{U}\}$ is an optimal $[\mathcal{F}, \sum_{i=0}^{k-1} \lambda_i, \delta]_q$ code, where $\mathcal{F} = [\gamma_0, \gamma_1, \ldots, \gamma_{n-1}]$ satisfies $\gamma_i = \lambda_i$ for each $i \in [k]$ and $\gamma_i = m$ for $k \leq i \leq n-1$.

Example

Theorem A [Etzion and Silberstein, 2009]

Let $m \geq n$. If $\mathcal{F}$ is an $m \times n$ Ferrers diagram and

$$\gamma_{n-\delta+1} \geq m,$$

i.e., each of the rightmost $\delta - 1$ columns of $\mathcal{F}$ has at least m dots, then there exists an optimal $[\mathcal{F}, k, \delta]_q$ code for any prime power q, where $k = \sum_{i=0}^{n-\delta} \gamma_i$.

- As a corollary, for any $\mathcal{F}$, there exists an optimal $[\mathcal{F}, k, 2]_q$ codes.

Improved example

Theorem B [Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016]

If $\mathcal{F}$ is an $m \times n$ Ferrers diagram and

$$\gamma_{n-\delta+1} \geq n,$$

i.e., each of the rightmost $\delta - 1$ columns of $\mathcal{F}$ has at least n dots, then there exists an optimal $[\mathcal{F}, k, \delta]_q$ code for any prime power q, where $k = \sum_{i=0}^{n-\delta} \gamma_i$.

- To prove it, truncate $\mathcal{F}$ to a $\max\{\gamma_{n-\delta}, n\} \times n$ Ferrers diagram. Then use Theorem A.

Remarks

- Basic Lemma can only be used to construct optimal FDRM codes satisfying $v_0 = \sum_{i=0}^{n-\delta} \gamma_i \leq \min_{i\in[\delta]} v_i$, where v_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.
- Basic Lemma only gives details of the leftmost k columns of the Ferrers diagram used for codewords in $\mathcal{C}$. However, if we could know more about the initial systematic MRD code, then it would be possible to give a complete characterization of $\mathcal{C}$.

A class of systematic MRD codes

Lemma [Antrobus and Gluesing-Luerssen, arXiv:1804.00624]

Let $m \geq n \geq \delta \geq 2$ and $k = n - \delta + 1$. Let q be any prime power. Let $a_1, a_2, \ldots, a_k \in \mathbb{F}_{q^m}$ satisfying that $1, a_1, a_2, \ldots, a_k$ are $\mathbb{F}_q$-linearly independent.

- Then there exists a matrix $\boldsymbol{A} \in \mathbb{F}_{q^m}^{k \times (n-k)}$ such that its first column is given by $(a_1, a_2, \ldots, a_k)^T$ and $\mathbf{G} = (\boldsymbol{I}_k | \boldsymbol{A})$ is a generator matrix of a systematic MRD$[m \times n, \delta]_q$ code.

A class of optimal FDRM codes

Theorem [Liu, Chang, F., arXiv:1809.00996]

Let $m \geq n \geq \delta \geq 2$ and $k = n - \delta + 1$. If an $m \times n$ Ferrers diagram $\mathcal{F}$ satisfies

(1) $\gamma_k \geq n$ or $\gamma_k - k \geq \gamma_i - i$ for each $i = 0, 1, \ldots, k-1$,

(2) $\gamma_{k+1} \geq n$,

then there exists an optimal $[\mathcal{F}, \sum_{i=0}^{k-1} \gamma_i, \delta]_q$ code for any prime power q.

This theorem requires each of the rightmost $\delta - 2$ columns of $\mathcal{F}$ has at least n dots and relaxes the condition on the $(\delta - 1)$-th column from the right end.

A class of square optimal FDRM codes with $\delta = 4$

Corollary [Liu, Chang, F., arXiv:1809.00996]

Let

$$\mathcal{F} = [2, 2, \gamma_2, \ldots, \gamma_{n-4}, n-1, n, n]$$

be an $n \times n$ Ferrers diagram, where $\gamma_i \leq i + 2$ for $2 \leq i \leq n-4$. Then there exists an optimal $[\mathcal{F}, \sum_{i=2}^{n-4} \gamma_i + 4, 4]_q$ code for any integer $n \geq 6$ and any prime power q.

Another class of systematic MRD codes

Lemma [Liu, Chang, F., arXiv:1804.01211]

Let η, r, d, κ and μ be positive integers such that $\kappa = \eta - r - d + 1$, $r < \kappa$ and $\eta \leq \mu + r$. Then there exists a matrix $\mathbf{G} \in \mathbb{F}_{q^\mu}^{\kappa \times \eta}$ of the following form

$$\begin{pmatrix}
1 & & & & & & \alpha_{0,\kappa} & \cdots & \alpha_{0,\eta-r-1} & 0 & 0 & \cdots & 0 \\
& 1 & & & & & \alpha_{1,\kappa} & \cdots & \alpha_{1,\eta-r-1} & \alpha_{1,\eta-r} & 0 & \cdots & 0 \\
& & \ddots & & & & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
& & & 1 & & & \alpha_{r-1,\kappa} & \cdots & \alpha_{r-1,\eta-r-1} & \alpha_{r-1,\eta-r} & \alpha_{r-1,\eta-r+1} & \cdots & 0 \\
& & & & 1 & & \alpha_{r,\kappa} & \cdots & \alpha_{r,\eta-r-1} & \alpha_{r,\eta-r} & \alpha_{r,\eta-r+1} & \cdots & \alpha_{r,\eta-1} \\
& & & & & \ddots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
& & & & & 1 & \alpha_{\kappa-1,\kappa} & \cdots & \alpha_{\kappa-1,\eta-r-1} & \alpha_{\kappa-1,\eta-r} & \alpha_{\kappa-1,\eta-r+1} & \cdots & \alpha_{\kappa-1,\eta-1}
\end{pmatrix}$$

satisfying that for each $0 \leq i \leq r$, the sub-matrix obtained by removing the first i rows, the leftmost i columns and the rightmost $r - i$ columns of $\mathbf{G}$ can produce an MRD$[\mu \times (\eta - r), d + i]_q$ code.

Restricted Gabidulin codes

For any positive integer i and any $a \in \mathbb{F}_{q^m}$, set $a^{[i]} \triangleq a^{q^i}$.

Gabidulin code

Let $m \geq n$ and q be any prime power. A Gabidulin code $\mathcal{G}[m \times n, \delta]_q$ is an MRD$[m \times n, \delta]_q$ code whose generator matrix **G** in vector representation is

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ g_0^{[1]} & g_1^{[1]} & \cdots & g_{n-1}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_0^{[n-\delta]} & g_1^{[n-\delta]} & \cdots & g_{n-1}^{[n-\delta]} \end{pmatrix},$$

where $g_0, g_1, \ldots, g_{n-1} \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$.

A class of optimal FDRM codes

Theorem [Liu, Chang, F., arXiv:1809.00996]

Let l be a positive integer. Let $1 = t_0 < t_1 < t_2 < \cdots < t_l$ be integers such that $t_1 \mid t_2 \mid \cdots \mid t_l$. Let $t_2 = t_1 s_2$. Let r be a nonnegative integer and δ, n, k be positive integers satisfying $r + 1 \leq \delta \leq n - r$, $t_{l-1} < n - r \leq t_l$, $k = n - \delta + 1$ and $k \leq t_1$. Let $\mathcal{F} = [\gamma_0, \gamma_1, \ldots, \gamma_{n-1}]$ be an $m \times n$ Ferrers diagram $(m = \gamma_{n-1})$ satisfying

(1) $\gamma_{k-1} \leq wt_1$,

(2) $\gamma_k \geq wt_1$ for $k < t_1$ and $\delta \geq 2$,

(3) $\gamma_{t_\theta} \geq t_{\theta+1}$ for $1 \leq \theta \leq l - 1$,

(4) $\gamma_{n-r+h} \geq t_l + \sum_{j=0}^{h} \gamma_j$ for $0 \leq h \leq r - 1$,

where $w = 1$ if $l = 1$, and $w \in \{1, 2, \ldots, s_2\}$ if $l \geq 2$. Then there exists an optimal $[\mathcal{F}, \sum_{i=0}^{k-1} \gamma_i, \delta]_q$ code for any prime power q.

Corollaries

Corollaries

(1) Take $l = 1$, $r = 0$ and $t_1 = n \leq m$. Then Theorem 3 in [Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016] is obtained.

(2) Take $l = 1$, $r = 1$ and $t_1 = n - r$. Then Theorem 8 in [Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016] is obtained.

(3) Take $w = 1$ and $r = 0$. Then Theorem 3.2 in [Zhang, Ge, DCC, 2019], which requires each of the first k columns of $\mathcal{F}$ contains at most t_1 dots. Here the theorem relaxes this restriction condition and requires each of the first k columns of $\mathcal{F}$ contains at most t_2 dots.

(4) Take $w = 1$ and $r = 1$. Theorem 3.6 in [Zhang, Ge, DCC, 2019] is obtained.

Outline

New Ferrers diagram rank-metric codes from old

Construction A [Liu, Chang, F., IEEE IT, 2019]

Let $\mathcal{F}_i$ for $i = 1, 2$ be an $m_i \times n_i$ Ferrers diagram, and $\mathcal{C}_i$ be an $[\mathcal{F}_i, k_1, \delta_i]_q$ code. Let $\mathcal{D}$ be an $m_3 \times n_3$ Ferrers diagram and $\mathcal{C}_3$ be a $[\mathcal{D}, k_2, \delta]_q$ code, where $m_3 \geq m_1$ and $n_3 \geq n_2$. Let $m = m_2 + m_3$ and $n = n_1 + n_3$. Let

$$\mathcal{F} = \begin{pmatrix} \mathcal{F}_1 & \hat{\mathcal{D}} \\ & \mathcal{F}_2 \end{pmatrix}$$

be an $m \times n$ Ferrers diagram $\mathcal{F}$, where $\hat{\mathcal{D}}$ is obtained by adding the fewest number of new dots to the lower-left corner of $\mathcal{D}$ such that $\mathcal{F}$ is a Ferrers diagram. Then there exists an $[\mathcal{F}, k_1 + k_2, \min\{\delta_1 + \delta_2, \delta\}]_q$ code.

To obtain optimal FDRM codes, it is often required that $\mathcal{C}_3$ is an optimal $[\mathcal{D}, k_2, \delta]_q$ code. If the optimality of $\mathcal{C}_3$ is unknown, then what shall we do?

New Ferrers diagram rank-metric codes from old

Construction A [Liu, Chang, F., IEEE IT, 2019]

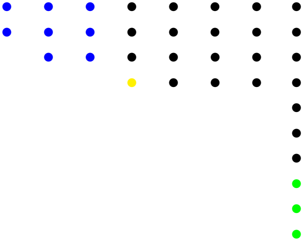
Let $\mathcal{F}_i$ for $i = 1, 2$ be an $m_i \times n_i$ Ferrers diagram, and $\mathcal{C}_i$ be an $[\mathcal{F}_i, k_1, \delta_i]_q$ code. Let $\mathcal{D}$ be an $m_3 \times n_3$ Ferrers diagram and $\mathcal{C}_3$ be a $[\mathcal{D}, k_2, \delta]_q$ code, where $m_3 \geq m_1$ and $n_3 \geq n_2$. Let $m = m_2 + m_3$ and $n = n_1 + n_3$. Let

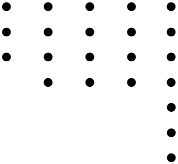
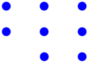
$$\mathcal{F} = \begin{pmatrix} \mathcal{F}_1 & \hat{\mathcal{D}} \\ & \mathcal{F}_2 \end{pmatrix}$$

be an $m \times n$ Ferrers diagram $\mathcal{F}$, where $\hat{\mathcal{D}}$ is obtained by adding the fewest number of new dots to the lower-left corner of $\mathcal{D}$ such that $\mathcal{F}$ is a Ferrers diagram. Then there exists an $[\mathcal{F}, k_1 + k_2, \min\{\delta_1 + \delta_2, \delta\}]_q$ code.

A natural idea is to remove a sub-diagram from $\mathcal{D}$ to obtain a new Ferrers diagram $\mathcal{D}'$ such that the FDRM code in $\mathcal{D}'$ is optimal, and then mix the removed sub-diagram to $\mathcal{F}_1$ or $\mathcal{F}_2$.

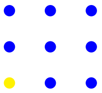
Example: optimal $[\mathcal{F}, 10, 4]_q$ code

$\mathcal{F} =$  .

$\mathcal{F}_4 =$  , $\mathcal{F}_2 =$, $\mathcal{F}_1 =$  , $\mathcal{F}_3 =$  .

Example: optimal $[\mathcal{F}, 10, 4]_q$ code

Take a proper combination $\mathcal{F}_{12}$ of $\mathcal{F}_1$ and $\mathcal{F}_2$ as follows



$$\triangleq \mathcal{F}_{12}.$$

Now construct a new Ferrers diagram

$$\mathcal{F}^* = \begin{pmatrix} \mathcal{F}_{12} & \mathcal{F}_4 \\ & \mathcal{F}_3 \end{pmatrix}.$$

By Construction A, we have an $[\mathcal{F}^*, 10, 4]_q$ code $\mathcal{C}^*$ for any prime power q, where an optimal $[\mathcal{F}_{12}, 3, 3]_q$ code $\mathcal{C}_{12}$ exists, an optimal $[\mathcal{F}_4, 7, 4]_q$ code $\mathcal{C}_4$ exists and an optimal $[\mathcal{F}_3, 3, 1]_q$ code $\mathcal{C}_3$ is trivial.

Note that the above procedure from $\mathcal{F}$ to $\mathcal{F}^*$ yields a natural bijection from $\mathcal{F}$ to F^*.

Proper combination of Ferrers diagrams

Let $\mathcal{F}_1$ be an $m_1 \times n_1$ Ferrers diagram, $\mathcal{F}_2$ be an $m_2 \times n_2$ Ferrers diagram and $\mathcal{F}$ be an $m \times n$ Ferrers diagram. Let ϕ_l for $l \in \{1, 2\}$ be an injection from $\mathcal{F}_l$ to $\mathcal{F}$ (in the sense of set-theoretical language). $\mathcal{F}$ is said to be a *proper combination* of $\mathcal{F}_1$ and $\mathcal{F}_2$ on a pair of mappings ϕ_1 and ϕ_2, if

- $\phi_1(\mathcal{F}_1) \cap \phi_2(\mathcal{F}_2) = \varnothing$;
- $|\mathcal{F}_1| + |\mathcal{F}_2| = |\mathcal{F}|$;
- for any $l \in \{1, 2\}$ and any two different elements $(i_{l,1}, j_{l,1})$, $(i_{l,2}, j_{l,2})$ of $\mathcal{F}_l$, set $\phi_l(i_{l,1}, j_{l,1}) = (i'_{l,1}, j'_{l,1})$ and $\phi_l(i_{l,2}, j_{l,2}) = (i'_{l,2}, j'_{l,2})$; $i'_{l,1} = i'_{l,2}$ or $j'_{l,1} = j'_{l,2}$ whenever $i_{l,1} = i_{l,2}$ or $j_{l,1} = j_{l,2}$.

Condition (3) means that if two dots in $\mathcal{F}_l$ for $l \in \{1, 2\}$ are in the same row or same column, then their corresponding two dots in $\mathcal{F}$ are also in the same row or same column.

Construction B

Let

$$\mathcal{F} = \begin{array}{r|ccc|ccc|ccc|l}
 & \multicolumn{3}{c|}{\overbrace{\qquad\qquad}^{n_1}} & \multicolumn{6}{c|}{\overbrace{\qquad\qquad\qquad\qquad\qquad\qquad}^{n_4}} & \\
m_1 \{ & \bullet & \cdots & \bullet & \bullet & \cdots & \bullet & \bullet & \cdots & \bullet & \\
 & \vdots & \mathcal{F}_1 & \vdots & \vdots & & & & \mathcal{F}_4 & \vdots & \\
 & \circ & \cdots & \bullet & \bullet & \cdots & \bullet & \bullet & & \bullet & \} m_4 \\
 & & & & \circ & \cdots & \circ & \bullet & & \bullet & \\
 & & & & \vdots & \mathcal{F}_2 & \vdots & \vdots & & \vdots & \\
 & & & & \circ & \cdots & \circ & \bullet & \cdots & \bullet & \\
 & & & & & & & \circ & \cdots & \bullet & \\
 & & & & & & & \vdots & \mathcal{F}_3 & \vdots & \} m_3 \\
 & & & & & & & \circ & \cdots & \bullet &
\end{array}$$

be an $m \times n$ Ferrers diagram, where $\mathcal{F}_i$ is an $m_i \times n_i$ Ferrers sub-diagram, $1 \leq i \leq 4$, satisfying that $m = m_3 + m_4$, $n = n_1 + n_4$, $m_4 \geq m_1 + m_2$ and $n_4 \geq n_2 + n_3$. Note that the dots " $\bullet$ " in $\mathcal{F}$ have to exist, whereas the dots " $\circ$ " can exist or not.

Construction B

Construction B [Liu, Chang, F., IEEE IT, 2019]

Suppose that

- $\mathcal{F}_{12}$ is a proper combination of $\mathcal{F}_1$ and $\mathcal{F}_2$, and $\mathcal{C}_{12}$ is an $[\mathcal{F}_{12}, k_1, \delta_1]_q$ code;
- there exist an $[\mathcal{F}_3, k_3, \delta_3]_q$ code $\mathcal{C}_3$ and an $[\mathcal{F}_4, k_4, \delta_4]_q$ code $\mathcal{C}_4$.

Then there exists an $[\mathcal{F}, k, \delta]_q$ code $\mathcal{C}$, where $k = \min\{k_1, k_3\} + k_4$ and $\delta = \min\{\delta_1 + \delta_3, \delta_4\}$.

Thank you for your attention!

Questions? Comments?