Self-dual rank metric codes

Lucky Galvez, Jon-Lark Kim

Department of Mathematics

Sogang University

Seoul, South Korea

The 5th Sino-Korea Conference on Coding Theory and Related Topics
Shanghai University, China
July 5, 2018

Table of Contents

Introduction

Rank metric codes

- In 1951, the *rank metric* was introduced by Hua as an "arithmetic distance" for matrices over a finite field $\mathbb{F}_q$.
- The rank distance d_R between two square matrices M and N over the finite field $\mathbb{F}_q$ is the rank of their difference, i.e., $d_R(M, N) = \text{rank}(M - N)$.
- In 1978, Delsarte defined the rank distance on the set of bilinear forms (which can also be seen as the set of rectangular matrices). He proposed the construction of optimal matrix codes attaining a Singleton-type bound using the rank metric.
- Codes consisting of matrices over finite fields (matrix codes) with the rank metric have been used in many applications: network coding, space-time coding, array codes, etc.
- In 1985, Gabidulin introduced the notion of rank metric codes in vector representation over an extension field of $\mathbb{F}_q$.

Introduction

Self-dual codes

- Self-dual matrix codes are said to exhibit good trade-off between the dimension and minimum distance.
- In the Hamming metric, a way to construct new self-dual codes from a self-dual code of smaller size, called the *building-up construction*:
  - binary case by Kim, J.-L.
  - $\mathbb{F}_q$ where q is a power of 2 or $q \equiv 1 \mod 4$ by Kim, J.L. and Lee, Y. (2004)
  - $\mathbb{F}_q$ where $q \equiv 3 \mod 4$ by by Kim, J.L. and Lee, Y. (2015)
  - certain rings
- The building-up construction proved to be an efficient way to contruct self-dual codes, as there are many new self-dual codes, often with the best minimum distance, were obtained this way.
- In 2015, Morrison characterized matrix codes and classified self-dual matrix codes of small size over small finite fields.

Background

Matrix codes

$\mathcal{M}_{m\times n}(\mathbb{F}_q)$: the vector space of $m \times n$ matrices over $\mathbb{F}_q$

Definition

An $m \times n$ linear matrix code C over $\mathbb{F}_q$ is a subspace of $\mathcal{M}_{m\times n}(\mathbb{F}_q)$. If C is of dimension k, then C is called an $[m \times n, k]$ linear matrix code over $\mathbb{F}_q$. An $m \times n$ matrix $X \in C$ is called a codeword of C.

For any $X, Y \in \mathcal{M}_{m\times n}(\mathbb{F}_q)$, the function $\langle X, Y\rangle = trace(XY^T) = \sum_{i=1}^{m}[XY^T]_{ii}$, is an inner product.

Definition

The *dual* of an $[m \times n, k]$ matrix code C over $\mathbb{F}_q$ is given by

$$C^\perp = \{X \in \mathcal{M}_{m\times n}(\mathbb{F}_q) |\, \langle X, Y\rangle = 0 \text{ for all } Y \in C\}.$$

The matrix code C is *self-orthogonal* if $C \subset C^\perp$ and *self-dual* if $C = C^\perp$.

Rank metric

Definition

Let C be an $m \times n$ matrix code over $\mathbb{F}_q$ and $X \in C$.

1. The (rank) weight of X, denoted $wt_R(X)$, is the rank of the matrix X.
2. The (rank) distance between two codewords $X_1, X_2 \in C$ is the rank of their difference $X_1 - X_2$, i.e.,

$$d_R(X_1, X_2) = wt_R(X_1 - X_2).$$

3. The minimum (rank) distance of C, denoted $d = d_R(C)$, is the minimum distance between two distinct codewords in C, which is also the minimum weight of nonzero codewords in C, i.e.,

$$d = d_R(C) = \min_{X_1, X_2 \in C,\ X_1 \neq X_2} d_R(X_1, X_2) = \min_{\mathbf{0} \neq X \in C} wt_R(X).$$

Matrix codes and block codes

- Define the map $\rho : \mathcal{M}_{m\times n}(\mathbb{F}_q) \to \mathbb{F}_q^{mn}$ by

$$\rho(A)\rho([a_{ij}]) = (a_{11}, a_{21}, \ldots, a_{m1}, a_{12}, \ldots, a_{m2}, \ldots, a_{mn})$$

$$A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \leftrightarrow \rho(A) = (1, 2, 3, 4, 5, 6, 7, 8, 9)$$

Matrix codes and block codes

- Define the map $\rho : \mathcal{M}_{m\times n}(\mathbb{F}_q) \to \mathbb{F}_q^{mn}$ by

$$\rho(A)\rho([a_{ij}]) = (a_{11}, a_{21}, \ldots, a_{m1}, a_{12}, \ldots, a_{m2}, \ldots, a_{mn})$$

$$A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \leftrightarrow \rho(A) = (1, 2, 3, 4, 5, 6, 7, 8, 9)$$

- For an $[m \times n, k]$ matrix code C over $\mathbb{F}_q$, there corresponds an $[mn, k]$ linear block code $\mathscr{C} = \rho(C) = \{\rho(A) : A \in C\}$ over $\mathbb{F}_q$.

Matrix codes and block codes

- Define the map $\rho : \mathcal{M}_{m\times n}(\mathbb{F}_q) \to \mathbb{F}_q^{mn}$ by

$$\rho(A)\rho([a_{ij}]) = (a_{11}, a_{21}, \ldots, a_{m1}, a_{12}, \ldots, a_{m2}, \ldots, a_{mn})$$

$$A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \leftrightarrow \rho(A) = (1, 2, 3, 4, 5, 6, 7, 8, 9)$$

- For an $[m \times n, k]$ matrix code C over $\mathbb{F}_q$, there corresponds an $[mn, k]$ linear block code $\mathscr{C} = \rho(C) = \{\rho(A) : A \in C\}$ over $\mathbb{F}_q$.
- $\langle X, Y\rangle = trace(XY^T) = \rho(X) \cdot \rho(Y)$

Matrix codes and block codes

- Define the map $\rho : \mathcal{M}_{m\times n}(\mathbb{F}_q) \to \mathbb{F}_q^{mn}$ by

$$\rho(A)\rho([a_{ij}]) = (a_{11}, a_{21}, \ldots, a_{m1}, a_{12}, \ldots, a_{m2}, \ldots, a_{mn})$$

$$A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \leftrightarrow \rho(A) = (1, 2, 3, 4, 5, 6, 7, 8, 9)$$

- For an $[m \times n, k]$ matrix code C over $\mathbb{F}_q$, there corresponds an $[mn, k]$ linear block code $\mathscr{C} = \rho(C) = \{\rho(A) : A \in C\}$ over $\mathbb{F}_q$.
- $\langle X, Y \rangle = trace(XY^T) = \rho(X) \cdot \rho(Y)$
- $\rho(C^\perp) = \rho(C)^\perp$

Matrix codes and block codes

- Define the map $\rho : \mathcal{M}_{m\times n}(\mathbb{F}_q) \to \mathbb{F}_q^{mn}$ by

$$\rho(A)\rho([a_{ij}]) = (a_{11}, a_{21}, \ldots, a_{m1}, a_{12}, \ldots, a_{m2}, \ldots, a_{mn})$$

$$A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \leftrightarrow \rho(A) = (1,2,3,4,5,6,7,8,9)$$

- For an $[m \times n, k]$ matrix code C over $\mathbb{F}_q$, there corresponds an $[mn, k]$ linear block code $\mathscr{C} = \rho(C) = \{\rho(A) : A \in C\}$ over $\mathbb{F}_q$.
- $\langle X, Y\rangle = trace(XY^T) = \rho(X) \cdot \rho(Y)$
- $\rho(C^\perp) = \rho(C)^\perp$
- C is self-dual $\Leftrightarrow \mathscr{C} = \rho(C)$ is self-dual

Matrix codes and block codes

- Define the map $\rho : \mathcal{M}_{m\times n}(\mathbb{F}_q) \to \mathbb{F}_q^{mn}$ by

$$\rho(A)\rho([a_{ij}]) = (a_{11}, a_{21}, \ldots, a_{m1}, a_{12}, \ldots, a_{m2}, \ldots, a_{mn})$$

$$A = \begin{bmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{bmatrix} \leftrightarrow \rho(A) = (1, 2, 3, 4, 5, 6, 7, 8, 9)$$

- For an $[m \times n, k]$ matrix code C over $\mathbb{F}_q$, there corresponds an $[mn, k]$ linear block code $\mathscr{C} = \rho(C) = \{\rho(A) : A \in C\}$ over $\mathbb{F}_q$.
- $\langle X, Y\rangle = trace(XY^T) = \rho(X) \cdot \rho(Y)$
- $\rho(C^\perp) = \rho(C)^\perp$
- C is self-dual $\Leftrightarrow \mathscr{C} = \rho(C)$ is self-dual
- A generator matrix for $\mathscr{C} = \rho(C)$ is also called the generator matrix for C

Building-up constructions

Self-dual rank codes over $\mathbb{F}_{2^r}$

Theorem

Let C be a self-dual $2 \times (n-1)$ matrix code over $\mathbb{F}_{2^r}$ with generator matrix $G = [g_i]$. Then the code whose generator matrix is either:

(i) $G' = [1\,1] \oplus G$ *or*

(ii) $$G' = \left[\begin{array}{cc|c} 1 & 0 & x \\ \hline y_1 & y_1 & g_1 \\ \vdots & \vdots & \vdots \\ y_{n-1} & y_{n-1} & g_{n-1} \end{array}\right],$$ *where* $x \in \mathbb{F}_{2^r}^{2(n-1)}$ *such that* $x \cdot x = 1$

and $y_i = x \cdot g_i$ *for* $1 \leq i \leq n-1$

is a self-dual $2 \times n$ matrix code over $\mathbb{F}_{2^r}$.

Proposition

Any self-dual $2 \times n$ matrix code C' over $\mathbb{F}_{2^r}$ is obtained from some self-dual $2 \times (n-1)$ matrix code C over $\mathbb{F}_{2^r}$ by the construction method in the above theorem.

Self-dual rank codes over $\mathbb{F}_{2^r}$

Example. Let C be the binary self-dual 2×3 matrix code with generator matrix $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$, i.e., the matrix code with basis

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \right\}.$$

Applying the theorem with $x = (1\,1\,1\,0\,0\,0)$, we get the 2×4 matrix code C_1 with generator matrix $G_1 = \left[\begin{array}{cc|cccccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right]$ self-dual, with the following basis

$$\left\{ \left[\begin{array}{c|ccc} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right], \left[\begin{array}{c|ccc} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right], \left[\begin{array}{c|ccc} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{array}\right], \left[\begin{array}{c|ccc} 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right] \right\}.$$

Self-dual rank codes over $\mathbb{F}_q$, $q \equiv 1 \mod 4$

Theorem

Suppose $q \equiv 1 \mod 4$ and $c \in \mathbb{F}_q^*$ such that $c^2 = -1$. Let $G = [g_i]$ be a generator matrix of a self-dual $2 \times (n-1)$ matrix code over $\mathbb{F}_q$. Then the code generated by either of the following:

(i) $\mathcal{G} = \begin{bmatrix} 1 & c \end{bmatrix} \oplus G$

(ii) $\mathcal{G} = \left[\begin{array}{cc|c} 1 & 0 & x \\ \hline -y_1 & -cy_1 & g_1 \\ \vdots & \vdots & \vdots \\ -y_n & -cy_n & g_{n-1} \end{array}\right]$ *where $x \in \mathbb{F}_q^n$ such that $x \cdot x = -1$ and* $y_i = x \cdot g_i$,

is a self-dual $2 \times n$ matrix code over $\mathbb{F}_q$.

Self-dual rank codes over $\mathbb{F}_q$, $q \equiv 1 \mod 4$

Theorem

Suppose $q \equiv 1 \mod 4$ *and* $c \in \mathbb{F}_q^*$ *such that* $c^2 = -1$. *Let* $G = [g_i]$ *be a generator matrix of a self-dual* $2 \times (n-1)$ *matrix code over* $\mathbb{F}_q$. *Then the code generated by either of the following:*

(*i*) $\mathcal{G} = \begin{bmatrix} 1 & c \end{bmatrix} \oplus G$

(*ii*) $\mathcal{G} = \left[\begin{array}{cc|c} 1 & 0 & x \\ \hline -y_1 & -cy_1 & g_1 \\ \vdots & \vdots & \vdots \\ -y_n & -cy_n & g_{n-1} \end{array}\right]$ *where* $x \in \mathbb{F}_q^n$ *such that* $x \cdot x = -1$ *and* $y_i = x \cdot g_i$,

is a self-dual $2 \times n$ *matrix code over* $\mathbb{F}_q$.

Proposition

Every $2 \times n$ self-dual matrix code over $\mathbb{F}_q$ can be obtained from a $2 \times (n-1)$ self-dual matrix code by the above construction.

Self-dual rank codes over $\mathbb{F}_q,\ q \equiv 1 \mod 4$

Corollary

For $m > 2$ even, any self-dual $m \times n$ matrix code over $\mathbb{F}_{2^r}$ can be obtained from an $m \times (n-1)$ self-dual matrix code by the previous construction.

Corollary

Assume $m > 2$ is even and $q \equiv 1 \mod 4$. Let C be a self-dual $m \times (n-1)$ code over $\mathbb{F}_q$ with generator matrix G. Then the code obtained by applying the previous construction to G $\frac{m}{2}$ times is a self-dual $m \times n$ matrix code.

Self-dual rank codes over $\mathbb{F}_q,\ q \equiv 3 \mod 4$

Theorem

Suppose $q \equiv 3 \mod 4$ and n is even. Let $G = [g_i]$ be a generator matrix for a $2 \times (n-2)$ self-dual matrix code. Then the code generated by

$$\mathcal{G} = \left[\begin{array}{cccc|c} 1 & 0 & a & c & x_1 \\ 0 & 1 & b & d & x_2 \\ \hline -s_1 & -t_1 & as_1 + bt_1 & cs_1 + dt_1 & g_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -s_{n-2} & -t_{n-2} & as_{n-2} + bt_{n-2} & cs_{n-2} + dt_{n-2} & g_{n-2} \end{array}\right],$$

where $a, b, c, d \in \mathbb{F}_q$ such that $a^2 + c^2 = b^2 + d^2 = -1$, $ab + cd = 0$, $2s_i = x_1 \cdot g_i$ and $2t_i = x_2 \cdot g_i$, and $x_i \cdot x_j = 0$ for $i, j = 1, 2$.

is a self-dual $2 \times n$ matrix code over $\mathbb{F}_q$.

Classification of self-dual matrix codes

Equivalence of matrix codes

Definition

Two $[m \times n, k]$ matrix codes over $\mathbb{F}_q$ are said to be linearly matrix-equivalent if there exists a linear matrix-equivalence map f between them, that is, an invertible map f that preserves the rank weight of all matrices in $\mathcal{M}_{m \times n}(\mathbb{F}_q)$. Otherwise, they are called linearly matrix-inequivalent.

Additional condition: for $m \times n$ linear codes C, f must satisfy $f(C^{\perp}) = (f(C))^{\perp}$ to guarantee that self-dual codes are mapped to self-dual codes.

Equivalence of matrix codes

Equivalence map on the generator matrix of self-dual matrix codes:

Proposition (Morrison,2014)

$$Equiv_{Mat}^{SD}(\mathcal{M}_{m\times n}(\mathbb{F}_q)) = \begin{cases} \{T^i(R\otimes L^T) : i=0,1; L,R\in GO_m(\mathbb{F}_q)\}, & \text{if } m=n \\ \{R\otimes L^T : R\in GO_n(F), L\in GO_m(\mathbb{F}_q)\}, & \text{if } m\neq n \end{cases}$$

where $GO_n(\mathbb{F}_q) = \{A \in GL_n(F) : AA^T = \lambda I_n \text{ for some } \lambda \in \mathbb{F}_q^*\}$ and T is the matrix corresponding to transposition, i.e, the $m^2 \times m^2$ matrix $T = [E_{ji}]_{ij}$ whose $(i,j)^{th}$ block is the $m\times m$ matrix E_{ji}, the matrix with 1 on the $(j,i)^{th}$ entry and 0 elsewhere.

The following mass formula applies to matrix codes:

$$b\prod_{i=1}^{\frac{mn}{2}-1}(q^i+1) = \sum_{\text{linearly matrix-inequivalent } C_i} \frac{|Equiv_{Mat}^{SD}(\mathbb{F}_q^{m\times n})|}{|Aut_{Mat}^{SD}(C_i)|}$$

where $b=1$ if $2|q$ and $b=2$ if $2\nmid q$.

Classifying self-dual matrix codes

Example. We classify binary self-dual 2×2 matrix codes.

The only self-dual 2×1 matrix code is generated by $[1\,1]$,

- we have the 2×2 matrix code C_1 with generator matrix

$$G_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

- Using the vector $(0\,1)$ we get the 2×2 matrix code C_2 with generator matrix

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}.$$

All the nonzero codewords in C_1 has rank weight 1 but there are rank weight 2 codewords in C_2.

So C_1 and C_2 are linearly matrix-inequivalent.

Mass formula confirms that these are complete representatives.

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_2$

Size	Code	Construction	x	G	$\lvert Aut^{SD}_{Mat}(C)\rvert$	Wt Dist
2×2	C_1	(i)		[1 1]	4	(1, 3, 0)
	C_2	(ii)	(01)	[1 1]	8	(1, 1, 2)
2×3	D_1	(i)		C_1	12	(1, 7, 0)
	D_2	(i)		C_2	4	(1, 3, 4)
	D_3	(ii)	(0010)	C_1	4	(1, 5, 2)
	D_4	(ii)	(0010)	C_2	2	(1, 3, 4)
	D_5	(ii)	(0111)	C_2	6	(1, 1, 6)
2×4	E_1	(i)		D_1	96	(1, 15, 0)
	E_2	(i)		D_2	16	(1, 7, 8)
	E_3	(i)		D_3	16	(1, 9, 6)
	E_4	(i)		D_4	4	(1, 5, 10)
	E_5	(i)		D_5	12	(1, 3, 12)
	E_6	(ii)	(011010)	D_1	96	(1, 7, 8)
	E_7	(ii)	(101010)	D_1	96	(1, 9, 6)
	E_8	(ii)	(011010)	D_2	16	(1, 3, 12)
	E_9	(ii)	(101111)	D_2	16	(1, 5, 10)
	E_{10}	(ii)	(010011)	D_2	32	(1, 5, 10)
	E_{11}	(ii)	(011001)	D_2	32	(1, 3, 12)
	E_{12}	(ii)	(001000)	D_3	32	(1, 9, 6)
	E_{13}	(ii)	(111000)	D_3	32	(1, 3, 12)
	E_{14}	(ii)	(000100)	D_4	4	(1, 3, 12)
	E_{15}	(ii)	(011010)	D_4	12	(1, 1, 14)
	E_{16}	(ii)	(001000)	D_4	16	(1, 7, 8)
	E_{17}	(ii)	(010011)	D_4	16	(1, 1, 14)
	E_{18}	(ii)	(011001)	D_4	8	(1, 3, 12)
	E_{19}	(ii)	(000100)	D_5	16	(1, 1, 14)
	E_{20}	(ii)	(110100)	D_5	48	(1, 3, 12)

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_2$

Size	Code	Construction	x	G	$\lvert Aut^{SD}_{Mat}(C)\rvert$	Wt Dist
2×5	F_1	(i)		E_1	1440	(1, 31, 0)
	F_2	(i)		E_2	12	(1, 15, 16)
	F_3	(i)		E_3	36	(1, 17, 14)
	F_4	(i)		E_4	96	(1, 9, 22)
	F_5	(i)		E_5	96	(1, 7, 24)
	F_6	(i)		E_8	4	(1, 7, 24)
	F_7	(i)		E_9	8	(1, 9, 22)
	F_8	(i)		E_{12}	16	(1, 13, 18)
	F_9	(i)		E_{13}	16	(1, 7, 24)
	F_{10}	(i)		E_{14}	12	(1, 5, 26)
	F_{11}	(i)		E_{15}	48	(1, 3, 28)
	F_{12}	(i)		E_{16}	16	(1, 9, 22)
	F_{13}	(i)		E_{17}	32	(1, 3, 28)
	F_{14}	(i)		E_{18}	32	(1, 5, 26)
	F_{15}	(i)		E_{19}	96	(1, 3, 28)
	F_{16}	(i)		E_{20}	96	(1, 5, 26)
	F_{17}	(ii)	(11100101)	E_{14}	6	(1, 1, 30)
	F_{18}	(ii)	(10100001)	E_{14}	4	(1, 3, 28)
	F_{19}	(ii)	(11111000)	E_{14}	10	(1, 3, 28)
	F_{20}	(ii)	(01001111)	E_{14}	12	(1, 1, 30)
	F_{21}	(ii)	(11110010)	E_{14}	12	(1, 7, 24)
	F_{22}	(ii)	(00001011)	E_{15}	36	(1, 1, 30)

*The classifications for 2×4 and 2×5 self-dual matrix codes over $\mathbb{F}_2$ are open from Morrison's classification.

*We have also found 442 linearly-inequivalent 4×3 matrix codes over $\mathbb{F}_2$.

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_3$

Size	Code	(a, b, c, d)	x_1 x_2	G_0	$\lvert Aut^{SD}_{Mat}(C)\rvert$	Wt Dist
2×2	C_1			$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$	16	(1, 0, 8)
2×4	D_1	(1, 1, 1, 2)	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	C_1	24	(1, 0, 80)
	D_2	(1, 1, 1, 2)	$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	C_1	192	(1, 0, 80)
	D_3	(1, 1, 1, 2)	$\begin{bmatrix} 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	C_1	288	(1, 8, 72)
	D_4	(1, 1, 1, 2)	$\begin{bmatrix} 1 & 2 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	C_1	72	(1, 0, 80)
	D_5	(1, 1, 1, 2)	$\begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	C_1	8	(1, 32, 48)
	D_6	(1, 1, 1, 2)	$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix}$	C_1	72	(1, 0, 80)
	D_7	(1, 1, 1, 2)	$\begin{bmatrix} 0 & 2 & 1 & 1 \\ 2 & 1 & 1 & 0 \end{bmatrix}$	C_1	384	(1, 4, 76)
	D_8	(1, 1, 1, 2)	$\begin{bmatrix} 2 & 2 & 0 & 1 \\ 1 & 2 & 1 & 0 \end{bmatrix}$	C_1	48	(1, 16, 64)
	D_9	(1, 1, 2, 1)	$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	C_1	288	(1, 0, 80)
	D_{10}	(1, 1, 2, 1)	$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$	C_1	576	(1, 4, 76)
	D_{11}	(1, 1, 2, 1)	$\begin{bmatrix} 2 & 2 & 2 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	C_1	192	(1, 8, 72)
	D_{12}	(1, 1, 2, 1)	$\begin{bmatrix} 0 & 1 & 2 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	C_1	64	(1, 20, 60)
	D_{13}	(1, 2, 2, 2)	$\begin{bmatrix} 2 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	C_1	32	(1, 8, 72)

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ where $\omega^2 + \omega + 1 = 0$

Size	Code	Construction	x	G	$\lvert Aut^{SD}_{Mat}(C)\rvert$	Wt Dist
2×2	C_1	(i)		[1 1]	96	(1, 15, 0)
	C_2	(ii)	$(\omega^2\omega)$	[1 1]	48	(1, 3, 12)
	C_3	(ii)	(01)	[1 1]	48	(1, 3, 12)
2×3	D_1	(i)		C_1	720	(1, 63, 0)
	D_2	(i)		C_2	48	(1, 15, 48)
	D_3	(ii)	$(0\omega^2\omega^2 1)$	C_1	144	(1, 27, 36)
	D_4	(ii)	$(0\omega^2\omega^2 1)$	C_2	18	(1, 9, 54)
	D_5	(ii)	$(\omega^2 1\omega 1)$	C_2	30	(1, 3, 60)
2×4	E_1	(i)		D_1	46080	(1, 255, 0)
	E_2	(i)		D_2	768	(1, 63, 192)
	E_3	(i)		D_3	2304	(1, 75, 180)
	E_4	(i)		D_4	72	(1, 21, 234)
	E_5	(i)		D_5	120	(1, 15, 240)
	E_6	(ii)	$(\omega^2\omega\omega\omega^2 10)$	D_1	46080	(1, 63, 192)
	E_7	(ii)	$(\omega^2\omega\omega^2\omega\omega\omega^2)$	D_1	46080	(1, 63, 192)
	E_8	(ii)	$(1010\omega^2\omega)$	D_1	46080	(1, 63, 192)
	E_9	(ii)	$(\omega^2\omega 10\omega^2\omega)$	D_1	46080	(1, 75, 180)
	E_{10}	(ii)	$(\omega^2\omega\omega\omega^2 10)$	D_2	2304	(1, 27, 228)
	E_{11}	(ii)	$(10\omega^2\omega\omega\omega^2)$	D_2	768	(1, 15, 240)
	E_{12}	(ii)	$(01\omega^2 0\omega 1)$	D_2	768	(1, 15, 240)
	E_{13}	(ii)	$(\omega\omega^2 1\omega^2 1\omega^2)$	D_2	3072	(1, 15, 240)
	E_{14}	(ii)	$(\omega^2\omega\omega 01\omega^2)$	D_2	3072	(1, 15, 240)
	E_{15}	(ii)	$(10\omega\omega\omega\omega)$	D_2	2304	(1, 27, 228)
	E_{16}	(ii)	$(01\omega 0\omega 0)$	D_2	768	(1, 15, 240)
	E_{17}	(ii)	$(\omega^2\omega\omega^2\omega\omega\omega^2)$	D_2	2304	(1, 27, 228)

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ where $\omega^2 + \omega + 1 = 0$

Size	Code	Construction	x	G	$\lvert Aut^{SD}_{Mat}(C)\rvert$	Wt Dist
(cont)	E_{18}	(ii)	$(101\omega^2\omega^2 1)$	D_2	3072	$(1, 15, 240)$
	E_{19}	(ii)	$(\omega\omega^2 1\omega\omega 1)$	D_2	3072	$(1, 27, 228)$
	E_{20}	(ii)	$(\omega 0\omega^2 000)$	D_3	9216	$(1, 75, 180)$
	E_{21}	(ii)	$(\omega 0\omega^2 0\omega^2\omega^2)$	D_3	3072	$(1, 15, 240)$
	E_{22}	(ii)	$(1\omega 0\omega\omega\omega)$	D_4	384	$(1, 3, 252)$
	E_{23}	(ii)	$(000\omega^2 0\omega)$	D_4	120	$(1, 3, 252)$
	E_{24}	(ii)	$(\omega^2\omega\omega\omega^2 10)$	D_4	72	$(1, 9, 246)$
	E_{25}	(ii)	$(11\omega^2\omega\omega^2\omega^2)$	D_4	72	$(1, 9, 246)$
	E_{26}	(ii)	$(\omega\omega\omega\omega\omega\omega^2)$	D_4	381	$(1, 3, 252)$
	E_{27}	(ii)	$(01\omega^2 0\omega 1)$	D_4	120	$(1, 3, 252)$
	E_{28}	(ii)	$(\omega^2 0\omega^2\omega 1\omega)$	D_4	72	$(1, 9, 246)$
	E_{29}	(ii)	$(\omega^2 10\omega 01)$	D_4	120	$(1, 3, 252)$
	E_{30}	(ii)	$(\omega 10\omega^2\omega\omega^2)$	D_4	192	$(1, 15, 240)$
	E_{31}	(ii)	$1\omega 01\omega^2 0)$	D_4	384	$(1, 3, 252)$
	E_{32}	(ii)	$(\omega^2 10\omega^2\omega\omega)$	D_4	1152	$(1, 39, 216)$
	E_{33}	(ii)	$(000\omega^2 0\omega)$	D_5	384	$(1, 3, 252)$
	E_{34}	(ii)	$(11\omega^2\omega\omega^2\omega^2)$	D_5	384	$(1, 3, 252)$
	E_{35}	(ii)	$(00\omega 1\omega^2 1)$	D_5	1920	$(1, 15, 240)$
	E_{36}	(ii)	$(\omega^2 001\omega^2 0)$	D_5	384	$(1, 3, 252)$

*The classifications for 2×3 and 2×4 self-dual matrix codes over $\mathbb{F}_4$ are open from Morrison's classification.

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_5$

Size	Code	Construction	c	x	G	$Aut^{SD}_{Mat}(C)$	Wt Dist
2×2	C_1	(i)	2		[1 2]	4	$(1,24,0)$
	C_2	(i)	2		[1 3]	8	$(1,8,16)$
2×3	D_1	(i)	2		C_1	2	$(1,124,0)$
	D_2	(i)	2		C_2	30	$(1,28,96)$
	D_3	(ii)	2	(2000)	C_1	12	$(1,44,80)$
	D_4	(ii)	3	(2000)	C_1	120	$(1,12,112)$
	D_5	(ii)	2	(0200)	C_1	20	$(1,28,96)$
	D_6	(ii)	3	(2210)	C_1	80	$(1,4,120)$
	D_7	(ii)	3	(3210)	C_1	48	$(1,4,120)$
2×4	E_1	(i)	2		D_1	2	$(1,624,0)$
	E_2		2		D_2	240	$(1,128,496)$
	E_3		2		D_3	72	$(1,144,480)$
	E_4		2		D_4	3600	$(1,32,592)$
	E_5		2		D_6	1600	$(1,24,600)$
	E_6		2		D_7	1152	$(1,24,600)$
	E_7		3		D_2	450	$(1,48,576)$
	E_8		3		D_3	144	$(1,64,560)$
	E_9		3		D_4	7200	$(1,16,608)$
	E_{10}		3		D_5	200	$(1,48,576)$
	E_{11}		3		D_6	4800	$(1,8,616)$
	E_{12}		3		D_7	5760	$(1,8,616)$
	E_{13}	(ii)	2	(200000)	D_7	1440	$(1,24,600)$
	E_{14}		3	(221000)	D_6	2400	$(1,0,624)$
	E_{15}		3	(221000)	D_7	2880	$(1,8,616)$
	E_{16}		3	(002000)	D_6	1800	$(1,16,608)$
	E_{17}		3	(212000)	D_6	2400	$(1,0,624)$
	E_{18}		3	(122000)	D_7	1920	$(1,0,624)$
	E_{19}		3	(303100)	D_7	96	$(1,24,600)$
	E_{20}		3	(000200)	D_7	800	$(1,0,624)$
	E_{21}		3	(103200)	D_6	80	$(1,0,624)$
	E_{22}		2	(000030)	D_3	12	$(1,144,480)$
	E_{23}		3	(000030)	D_3	144	$(1,64,560)$
	E_{24}		3	(000030)	D_4	120	$(1,48,576)$

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$ where $\alpha^3 + \alpha + 1 = 0$

Size	Code	Construction	x	G	$\lvert Aut^{SD}_{Mat}(C)\rvert$	Wt Dist
2×2	C_1	(i)		[1 1]	448	$(1, 63, 0)$
	C_2	(ii)	$(\alpha^3 \alpha)$	[1 1]	448	$(1, 7, 56)$
	C_3	(ii)	$(\alpha \alpha^3)$	[1 1]	448	$(1, 7, 56)$
	C_4	(ii)	(01)	[1 1]	896	$(1, 7, 56)$
	C_5	(ii)	$(\alpha^4 \alpha^5)$	[1 1]	448	$(1, 7, 56)$
2×3	D_1	(i)		C_1	28224	$(1, 511, 0)$
	D_2	(i)		C_2	448	$(1, 63, 448)$
	D_3	(ii)	$(0\alpha^2 \alpha \alpha^5)$	C_1	3136	$(1, 119, 392)$
	D_4	(ii)	$(\alpha 0 \alpha^6 \alpha^4)$	C_2	98	$(1, 21, 490)$
	D_5	(ii)	$(\alpha^3 \alpha^3 \alpha^4 \alpha^5)$	C_2	126	$(1, 7, 504)$

*These classifications for self dual matrix codes over $\mathbb{F}_8$ are open from Morrison's classification.

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_9 = \mathbb{F}_3[\alpha]$ where $\alpha^2 + 2\alpha + 2 = 0$

Size	Code	Construction	c	x	G	$\lvert Aut_{Mat}^{SD}(C)\rvert$	Wt Dist
2×2	C_1	(i)	α^2		$[1\ \alpha^2]$	4	(1, 80, 0)
	C_2	(i)	α^2		$[1\ \alpha^6]$	16	(1, 16, 64)
2×3	D_1	(i)	α^2		C_1	2	(1, 728, 0)
	D_2	(i)	α^2		C_2	90	(1, 88, 640)
	D_3	(ii)	α^6	$(\alpha^2 111)$	C_1	576	(1, 8720)
	D_4	(ii)	α^2	$(\alpha^2 111)$	C_2	160	(1, 8, 720)
	D_5	(ii)	α^2	$(\alpha^6 111)$	C_1	72	(1, 88, 640)
	D_6	(ii)	α^6	$(\alpha^6 111)$	C_1	720	(1, 24, 704)
	D_7	(ii)	α^2	$(\alpha^2 0 \alpha^2 1)$	C_2	20	(1, 152, 576)

Enumeration of Linearly Matrix-Inequivalent Self-dual Matrix Codes over $\mathbb{F}_{13}$

Size	Code	Construction	c	x	G	$\lvert Aut_{Mat}^{SD}(C)\rvert$	Wt Dist
2×2	C_1	(i)	5		[1 5]	4	(1, 168, 0)
	C_2	(i)	5		[1 8]	24	(1, 24, 144)
2×3	D_1	(i)	5		C_1	2	(1, 2196, 0)
	D_2	(i)	5		C_2	182	(1, 180, 2016)
	D_3	(ii)	5	(5000)	C_1	28	(1, 324, 1872)
	D_4	(ii)	8	(5000)	C_1	2184	(1, 36, 2160)
	D_5	(ii)	5	(4300)	C_1	156	(1, 180, 2016)
	D_6	(ii)	8	(6110)	C_1	1872	(1, 12, 2184)
	D_7	(ii)	8	(1610)	C_1	336	(1, 12, 2184)

*These classifications for self dual matrix codes over $\mathbb{F}_{13}$ are open from Morrison's classification.

Concluding Remarks

Concluding Remarks

- Using the building-up constructions we are able to confirm and extend the results of Morrison in 2015.
- However, we have stopped the classification of self-dual matrix codes of larger sizes due to the lack of computing resource.
- It will be interesting to classify or construct more self-dual matrix codes with larger sizes, i.e., matrix codes with four or more rows.
- The building-up constructions can also be used to construct optimal self-dual codes of larger sizes over larger finite fields, in which not much are known today.

References

- E.M. Gabidulin. Theory of codes with maximum rank distance. *Problemy Peredachi Informatsii*, 21(1):3–16, 1985.
- W.C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields and Their Applications*, 11(3):451–490, 2005.
- J.-L. Kim and Y. Lee. Euclidean and hermitian self-dual mds codes over large finite fields. *Journal of Combinatorial Theory, Series A*, 105(1):79–95, 2004.
- J.-L. Kim and Y. Lee. An efficient construction of self-dual codes. *Bull. Korean Math. Soc*, 52(3):915–923, 2015.
- H. Lee and Y. Lee. Construction of self-dual codes over finite rings $\mathbb{Z}_{p^m}$. *Journal of Combinatorial Theory, Series A*, 115(3):407–422, 2008.
- K. Morrison. Equivalence for rank-metric and matrix codes and automorphism groups of gabidulin codes. *IEEE Transactions on Information Theory*, 60(11):7035–7046, 2014.
- K. Morrison. An enumeration of the equivalence classes of self-dual matrix codes. *Advances in Mathematics of Communications*, 9(4):415 – 436, May 2015.

THANK YOU!!!