On Some Special Matrices and Their Application to Code Construction

D. Mokhtari, K. Guenda, T.A. Gulliver, N. Aydin, and P. Liu
CIRM: Alcocrypt

:

Feb. 2023

Previous work

- K. C. Gupta and I. G. Ray, On constructions of MDS matrices from companion matrices for lightweight cryptography, Lecture Notes in Computer Science, vol. 8128, 2013.
- K. C. Gupta, S. K. Pandey, I. G. Ray, and S. Samanta, Cryptographically significant MDS matrices over finite fields : A brief survey and some generalized results, Advances in Mathematics of Communications, 2019.
- I. Irwansyah, I. Mushtadi-Alamsyah, and F. Yuliawan, A construction of MDS involutory matrices using MDS self-dual codes : A preliminary result, Journal of Physics : Conference Series, 2021.

Previous work

- K. C. Gupta and I. G. Ray, On constructions of MDS matrices from companion matrices for lightweight cryptography, Lecture Notes in Computer Science, vol. 8128, 2013.
- K. C. Gupta, S. K. Pandey, I. G. Ray, and S. Samanta, Cryptographically significant MDS matrices over finite fields : A brief survey and some generalized results, Advances in Mathematics of Communications, 2019.
- I. Irwansyah, I. Mushtadi-Alamsyah, and F. Yuliawan, A construction of MDS involutory matrices using MDS self-dual codes : A preliminary result, Journal of Physics : Conference Series, 2021.

Previous work

- K. C. Gupta and I. G. Ray, On constructions of MDS matrices from companion matrices for lightweight cryptography, Lecture Notes in Computer Science, vol. 8128, 2013.
- K. C. Gupta, S. K. Pandey, I. G. Ray, and S. Samanta, Cryptographically significant MDS matrices over finite fields : A brief survey and some generalized results, Advances in Mathematics of Communications, 2019.
- I. Irwansyah, I. Mushtadi-Alamsyah, and F. Yuliawan, A construction of MDS involutory matrices using MDS self-dual codes : A preliminary result, Journal of Physics : Conference Series, 2021.

Some Definitions

- A linear code of length over $\mathbb{F}_q$ of length n is a subspace of $\mathbb{F}_q^n$
- $C^\perp = \{x \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \text{ for all } y \in C\}$ (dual code)
- $C \cap C^\perp = \{0\}$ (Linear Complementary Dual (LCD) code)
- $C = C^\perp$ (self-dual code)
- $C = \sigma(C^\perp)$ (isodual code), σ a permutation.

Some Definitions

- A linear code of length over $\mathbb{F}_q$ of length n is a subspace of $\mathbb{F}_q^n$
- $C^\perp = \{x \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \text{ for all } y \in C\}$ (dual code)
- $C \cap C^\perp = \{0\}$ (Linear Complementary Dual (LCD) code)
- $C = C^\perp$ (self-dual code)
- $C = \sigma(C^\perp)$ (isodual code), σ a permutation.

Some Definitions

- A linear code of length over $\mathbb{F}_q$ of length n is a subspace of $\mathbb{F}_q^n$
- $C^\perp = \{x \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \text{ for all } y \in C\}$ (dual code)
- $C \cap C^\perp = \{0\}$ (Linear Complementary Dual (LCD) code)
- $C = C^\perp$ (self-dual code)
- $C = \sigma(C^\perp)$ (isodual code), σ a permutation.

Some Definitions

- A linear code of length over $\mathbb{F}_q$ of length n is a subspace of $\mathbb{F}_q^n$
- $C^\perp = \{x \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \text{ for all } y \in C\}$ (dual code)
- $C \cap C^\perp = \{0\}$ (Linear Complementary Dual (LCD) code)
- $C = C^\perp$ (self-dual code)
- $C = \sigma(C^\perp)$ (isodual code), σ a permutation.

Some Definitions

- A linear code of length over $\mathbb{F}_q$ of length n is a subspace of $\mathbb{F}_q^n$
- $C^\perp = \{x \in \mathbb{F}_q^n : \langle x, y \rangle = 0 \text{ for all } y \in C\}$ (dual code)
- $C \cap C^\perp = \{0\}$ (Linear Complementary Dual (LCD) code)
- $C = C^\perp$ (self-dual code)
- $C = \sigma(C^\perp)$ (isodual code), σ a permutation.

Some Definitions

- $MM^t = M^tM = \lambda I_n$ for λ in $\mathbb{F}_q$ (λ-orthogonal matrix)
- $MM = \lambda I$ (λ-involution matrix)
- M is MDS if every submatrix of M is nonsingular

Some Definitions

- $MM^t = M^tM = \lambda I_n$ for λ in $\mathbb{F}_q$ (λ-orthogonal matrix)
- $MM = \lambda I$ (λ-involution matrix)
- M is MDS if every submatrix of M is nonsingular

Some Definitions

- $MM^t = M^tM = \lambda I_n$ for λ in $\mathbb{F}_q$ (λ-orthogonal matrix)
- $MM = \lambda I$ (λ-involution matrix)
- M is MDS if every submatrix of M is nonsingular

Contributions

- We give methods to obtain λ-orthogonal MDS matrices from existing matrices.
- We characterize λ-orthogonal Cauchy matrices and construct new λ-orthogonal MDS matrices from them.
- We construct LCD, isodual, and self-dual MDS codes from these matrices.

Contributions

- We give methods to obtain λ-orthogonal MDS matrices from existing matrices.
- We characterize λ-orthogonal Cauchy matrices and construct new λ-orthogonal MDS matrices from them.
- We construct LCD, isodual, and self-dual MDS codes from these matrices.

Contributions

- We give methods to obtain λ-orthogonal MDS matrices from existing matrices.
- We characterize λ-orthogonal Cauchy matrices and construct new λ-orthogonal MDS matrices from them.
- We construct LCD, isodual, and self-dual MDS codes from these matrices.

MDS Matrices and Monomial Matrices

(Irwansyah and Mushtadi-Alamyah J. Phys.)
If A is an MDS matrix and $M_{\sigma_1}, \ldots, M_{\sigma_t}$, $M'_{\sigma_1}, \ldots, M'_{\sigma_s}$ are monomial matrices in $\mathcal{M}_{n,n}(\mathbb{F}_{p^m})$, then the matrix

$$M_{\sigma_1} \ldots M_{\sigma_t} A M_{\sigma'_1} \ldots M_{\sigma'_s}$$

is also an MDS matrix.

New λ-orthogonal Matrices (Permutation Matrices)

Let A be a λ-orthogonal matrix, then the following statements hold :

- If P_σ is a permutation matrix, then the matrices $P_\sigma A$, AP_σ and $P_\sigma A P_\sigma$ are also λ-orthogonal.
- If A is a symmetric matrix, then A is a λ-involution matrix. Further, for any permutation matrix P_σ, the matrix $P_\sigma A P_\sigma^t$ is also a λ-involution matrix.
- If there exists a permutation matrix such that $A^t P_\sigma^t = P_\sigma A$, then $P_\sigma A$ is a λ-involution matrix.

New λ-orthogonal Matrices (Permutation Matrices)

Let A be a λ-orthogonal matrix, then the following statements hold :

- If P_σ is a permutation matrix, then the matrices $P_\sigma A$, AP_σ and $P_\sigma A P_\sigma$ are also λ-orthogonal.
- If A is a symmetric matrix, then A is a λ-involution matrix. Further, for any permutation matrix P_σ, the matrix $P_\sigma A P_\sigma^t$ is also a λ-involution matrix.
- If there exists a permutation matrix such that $A^t P_\sigma^t = P_\sigma A$, then $P_\sigma A$ is a λ-involution matrix.

New λ-orthogonal Matrices (Permutation Matrices)

Let A be a λ-orthogonal matrix, then the following statements hold :

- If P_σ is a permutation matrix, then the matrices $P_\sigma A$, AP_σ and $P_\sigma A P_\sigma$ are also λ-orthogonal.
- If A is a symmetric matrix, then A is a λ-involution matrix. Further, for any permutation matrix P_σ, the matrix $P_\sigma A P_\sigma^t$ is also a λ-involution matrix.
- If there exists a permutation matrix such that $A^t P_\sigma^t = P_\sigma A$, then $P_\sigma A$ is a λ-involution matrix.

Question :
From λ-orthogonal matrices can we have other λ-orthogonal matrices using monomial matrices $M = DP_\sigma$? if yes, under which conditions ?

New λ-orthogonal Matrices (Monomial Matrices)

Let M be a monomial matrix and A be a λ-orthogonal matrix.

- Then MA is a λ-orthogonal matrix if and only if $M = DP_\sigma$, where P_σ is a permutation matrix and $D = \text{diag}(\alpha_1, \ldots, \alpha_n)$ such that $\alpha_i^2 = 1$.
- AM is a λ-orthogonal matrix if and only if $M = P_\sigma D$, where P_σ is a permutation matrix and $D = \text{diag}(\alpha_1, \ldots, \alpha_n)$ such that $\alpha_i^2 = 1$.

New λ-orthogonal Matrices (Monomial Matrices)

Let M be a monomial matrix and A be a λ-orthogonal matrix.

- Then MA is a λ-orthogonal matrix if and only if $M = DP_\sigma$, where P_σ is a permutation matrix and $D = \text{diag}(\alpha_1, \ldots, \alpha_n)$ such that $\alpha_i^2 = 1$.
- AM is a λ-orthogonal matrix if and only if $M = P_\sigma D$, where P_σ is a permutation matrix and $D = \text{diag}(\alpha_1, \ldots, \alpha_n)$ such that $\alpha_i^2 = 1$.

Theorem

Let A be an λ-orthogonal MDS matrix, and $M_{\sigma_1} = D_1 P_{\sigma_1}$ and $M_{\sigma_2} = D_2 P_{\sigma_2}$ be two monomial matrices where $D_1 = \text{diag}(\alpha_1, \ldots, \alpha_n)$ and $D_2 = \text{diag}(\beta_1, \ldots, \beta_n)$ are diagonal matrices and the P_{σ_i} are permutation matrices. Then $M_{\sigma_1} A M_{\sigma_2}$ is a λ-orthogonal MDS matrix if and only if the matrices D_1 and D_2 are such that ${\alpha_j}^2 = 1$ and ${\beta_j}^2 = 1$.

Theorem

Let A be a λ-orthogonal MDS matrix and
$M_{\sigma_1} = D_1 P_{\sigma_1}, \ldots, M_{\sigma_s} = D_s P_{\sigma_s}$ be monomial matrices where
$D_i = \text{diag}({\alpha_1}^i, \ldots, {\alpha_n}^i)$ are diagonal matrices and the P_{σ_i} are permutation matrices.
Then $M_{\sigma_1} \ldots M_{\sigma_t} A M_{\sigma_{t+1}} \ldots M_{\sigma_s}$ is a λ-orthogonal MDS matrix if and only if for all $1 \leq i \leq s$, D_i is such that $({\alpha^i}_j)^2 = 1$ for all $1 \leq j \leq n$.

MDS Cauchy Matrices

Given two sequences $x_0, x_1, \ldots, x_{n-1}$ and $y_0, y_1, \ldots, y_{n-1}$ where the elements of each sequence are distinct, the Cauchy matrix is

$$M = \left(\frac{1}{x_i + y_j} \right)$$

$$\det(M) = \frac{\prod_{0 \le i < j \le n-1} (x_j - x_i)(y_j - y_i)}{\prod_{0 \le i < j \le n-1} (x_i + y_j)}$$

Since the x_is and y_js are distinct, then provided $x_i + y_j \neq 0$, any square submatrix of a Cauchy matrix is nonsingular over any finite field. Hence the Cauchy matrices are MDS.

Proposition

Let $M = \left(\frac{1}{x_i+y_j}\right)$ be a Cauchy matrix. Then M is λ-orthogonal if and only if for each $1 \leq j \leq n$

$$\sum_{i=1}^{n} \frac{1}{(x_j + y_i)^2} = \lambda$$

and for all k, j, $1 \leq k \leq n$, $1 \leq j \leq n$, $k \neq j$, $\sum_{i=1}^{n} \frac{1}{(x_k+y_i)(x_j+y_i)} = 0$.

Proposition

Let $M = \left(\frac{1}{x_i + y_j}\right)$ be a Cauchy matrix over $\mathbb{F}_q$ and let $D_1 = \text{diag}(\alpha_1, \ldots, \alpha_n)$ and $D_2 = \text{diag}(\beta_1, \ldots, \beta_n)$ be two diagonal matrices.
If for all $1 \leq k \leq n$

$$\frac{\alpha_1\beta_1}{(x_k + y_1)^2} + \frac{\alpha_2\beta_2}{(x_k + y_2)^2} + \cdots + (\frac{\alpha_n\beta_n}{(x_k + y_n)^2} = \lambda$$

and

$$\sum_{i=1}^{n} \frac{\alpha_i\beta_i}{(x_k + y_i)(x_j + y_i)} = 0$$

then the matrix MD_1D_2 is MDS λ-orthogonal.

Question

- If $(I|A)$ is (MDS, LCD-isodual, LCD, isodual...) what is the code $(I|M_{\sigma_1}AM_{\sigma_2})$
- The code $(I|M_{\sigma_1}AM_{\sigma_2})$ is a monomial code (MDS, LCD-isodual, LCD, isodual...)

Question

- If $(I|A)$ is (MDS, LCD-isodual, LCD, isodual...) what is the code $(I|M_{\sigma_1}AM_{\sigma_2})$
- The code $(I|M_{\sigma_1}AM_{\sigma_2})$ is a monomial code (MDS, LCD-isodual, LCD, isodual...)

Code Constructions

We construct

- Isodual codes (some are MDS)
- LCD codes (some are MDS)
- Self-dual MDS codes

LCD and MDS codes

Proposition (Massey)

A linear code C with generator matrix G and parity check matrix H is LCD if and only if one of the following conditions hold :

(i) GG^t is invertible

(ii) HH^t is invertible

MDS Codes

An $[n, k, d]$ code with generator matrix $G = [I|A]$, where A is a $k \times (n-k)$ matrix is MDS if and only if every square submatrix formed from any i rows and i columns, $i = 1, 2, \ldots, \min\{k, n-k\}$ of A is nonsingular.

Preliminary Results

Let A be a zero-orthogonal matrix, and let M and N be λ-orthogonal and λ'-orthogonal matrices, respectively. Then the matrix

$$G = \begin{bmatrix} M & -MA^t \\ A & N \end{bmatrix}$$

is a $\lambda\lambda'$-orthogonal matrix.

Example Over $\mathbb{F}_3$

Orthogonal matrix

$$M = \begin{bmatrix} 0 & 0 & 2 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Zero-orthogonal matrix

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 1 & 1 & 1 \end{bmatrix}$$

With $N = I$, we have the orthogonal matrix

$$C = \begin{bmatrix} 0 & 0 & 2 & 1 & 2 & 1 \\ 0 & 1 & 0 & 2 & 1 & 2 \\ 1 & 0 & 0 & 2 & 1 & 2 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 2 & 2 & 2 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

New Isodual Codes

Let A be a square matrix over $\mathbb{F}_q$. Then if A is such that $A^t = \pm Q_1 A Q_2$, where Q_1 and Q_2 are monomial matrices satisfying $Q_1 Q_2 = I$, then the code generated by the matrix $(I|A)$ is an isodual code.

Isodual Codes from Cauchy Matrices

Let $M = \left(\frac{1}{x_i + y_j}\right)$ be a Cauchy matrix with $x_i + y_j = x_j + y_i$ for $1 \leq i \leq n$, $1 \leq j \leq n$. Then the code with generator matrix $(I|M)$ is an isodual MDS code.

Example over $\mathbb{F}_8$

- Let α be a primitive element of $\mathbb{F}_8$.
- Let A be the Cauchy matrix given by

$$A = \begin{bmatrix} \frac{1}{\alpha} & \frac{1}{1+\alpha+\alpha^2} & \frac{1}{\alpha^2} \\ \frac{1}{1+\alpha+\alpha^2} & \frac{1}{\alpha} & 1 \\ \frac{1}{\alpha^2} & 1 & \frac{1}{\alpha} \end{bmatrix}$$

- Then the matrix A is symmetric MDS.
- The code with generator matrix $(I|A)$ is a $[6, 3, 4]$ MDS isodual code.

LCD Codes

- If A is a zero-orthogonal matrix, then the code generated by the matrix $(I|A)$ is an LCD code.
- If A is a λ-orthogonal matrix over a field of characteristic p, then if $1 + \lambda \neq 0 \bmod p$, the matrix $G = (I|A)$ generates an LCD code.
- Let G generate an LCD code, and for $1 \leq i \leq s$, let M_i be matrices which satisfy $M_i M_i^t = \lambda_i I$ for some $\lambda \in \mathbb{F}_q^*$.
  Then the matrix

$$\begin{bmatrix} GM_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & GM_s \end{bmatrix}$$

  generates an LCD code.

- If A is a zero-orthogonal matrix, and M and N are λ-orthogonal λ'-orthogonal matrices, respectively, then the matrices

$$G_1 = \begin{bmatrix} M & -MA^t \end{bmatrix}$$

and

$$G_2 = \begin{bmatrix} M & -MA^t \\ A & N \end{bmatrix}$$

generate LCD codes.

LCD MDS Codes from Cauchy Matrices

If $M = \left(\frac{1}{x_i+y_j}\right)_{i,j}$ (Cauchy matrix over $\mathbb{F}_q$), then the following result holds :

- If for $1 \leq j \leq n$, $\sum_{i=1}^{n} \frac{1}{(x_j+y_i)^2} = \lambda$ and $1 + \lambda \neq 0 \bmod p$, and for all k, j, $1 \leq k \leq n$, $1 \leq j \leq n$, $k \neq j$, $\sum_{i=1}^{n} \frac{1}{(x_k+y_i)(x_j+y_i)} = 0$, then the code with generator matrix $(I|M)$ is an LCD MDS code.

Characterization of Self-dual MDS Codes

A code C over $\mathbb{F}_{2^m}$ is an $[n, n/2, n/2+1]$ Euclidean self-dual MDS code if and only if it has a systematic generator matrix of the form $G = (I|M)$ where M is an orthogonal MDS matrix.

Mameri-Aissanni Algorithm AAECC 2019

Input : vector space $E = \mathbb{F}_{2^r}$ and symmetric bilinear form $\langle , \rangle$.

1. For $i = 1$ do
   (a) Randomly choose a vector $X^{(1)} \in E$
   (b) If $\langle 1, X^{(1)} \rangle \neq 0$, then set $U_1 = X^{(1)}$ and $R_1 = \frac{U_1}{\langle 1, U^{(1)} \rangle}$
   (c) If $R_1 \neq 1$, then set $E_1 = R_1$, else return to 1(a)

2. For $i = 2$ to $k - 1$ do
   (a) Randomly choose $X^{(i)} \in E$
   (b) Compute $U_i = X^{(i)} \oplus \sum \langle X^{(i)}, E_j \rangle E_j$
   (c) If $\langle 1, U_i \rangle \neq 0$, then set $R_i = \frac{U_i}{\langle 1, U_i \rangle}$
   (d) If $E_1 \oplus \ldots E_{i-1} \oplus R_i \neq 1$, then $E_i = R_i$, else return to 2(a)

3. For $i = k$ do
   (a) Randomly choose $X^{(k)} \in E$
   (b) Compute $U_k = X^{(k)} \oplus \sum_{j=1} \langle X^{(i)}, E_j \rangle E_j$
   (c) If $\langle 1, U_m \rangle \neq 0$, then set $E_m = \frac{U_m}{\langle 1 U^{(m)} \rangle}$, else return to 3(a)

Output $m \times m$ orthogonal matrix $M = (E_1, \ldots, E_m)$

The matrix M obtained using the Algorithm satisfies the condition that any $r \leq m$ columns are linearly independent.

New MDS Codes

Let M be an $m \times m$ matrix obtained using the Algorithm.

- For any $r \leq m$, let M_r be the matrix formed by the first r columns of M.
- The code with generator matrix $G = (I_r | {M_r}^t)$ is an $[m + r, r, m + 1]$ MDS code.

- Let M be the matrix obtained using the Algorithm.
  Then the code with generator matrix (I_m, M) is self-dual MDS.

Bibliography

- C. Carlet, S. Mesnager, C. Tang, and Y. Qi, New characterization and parametrization of LCD codes, *IEEE Transactions on Information Theory*, 2019.
- K. C. Gupta, S. K. Pandey, I. G. Ray, and S. Samanta, Cryptographically significant MDS matrices over finite fields : A brief survey and some generalized results, Advances in Mathematics of Communications, 2019.
- I. Irwansyah, I. Mushtadi-Alamsyah, and F. Yuliawan A construction of MDS involutory matrices using MDS self-dual codes : A preliminary result, Journal of Physics : Conference Series, 2021.
- A. Mameri and A. Aissani, 'Orthogonal matrix and its application in Bloom's threshold scheme, Applicable Algebra in Engineering, Communication and Computing, 2019.
- M. Shi, L. Xu, and P. Solé, Construction of isodual codes from polycirculant matrices, Design Codes Cryp., 2020.

Thank you for your attention