Orthogonal θ-Circulant MDS Matrices over Finite Fields

PPMI FMIPA ITB 2026 Doctoral Research Grant

Intan Muchtadi-Alamsyah[1], Fajar Yuliawan[1], Romsto R. Pajarillo[2,3]

[1] Algebra Research Group, FMIPA, Institut Teknologi Bandung, Indonesia
[2] Doctoral Program in Mathematics, Institut Teknologi Bandung, Indonesia
[3] Institute of Mathematical Sciences, University of the Philippines Los Baños, Philippines

Abstract

We investigate the existence and construction of orthogonal θ-circulant MDS matrices over finite fields. Keeping the field and automorphism fixed, compression produces smaller matrices while preserving orthogonality, involutivity, and the MDS property. We study the inverse problem, lifting, and provide existence results and explicit constructions. Compression also yields nonexistence results, recovering known restrictions for ordinary circulant matrices.

Keywords: orthogonal MDS matrices, θ-circulant matrices, q-polynomial ring, compression, lifting

Introduction

Let q be a prime power. A circulant matrix with entries $h_0, h_1, \dots, h_{m-1} \in \mathbb{F}_q$ is given by

$$\operatorname{circ}(h_0, h_1, \dots, h_{m-1}) = \begin{pmatrix} h_0 & h_1 & \dots & h_{m-1} \\ h_{m-1} & h_0 & \dots & h_{m-2} \\ \vdots & \vdots & \ddots & \vdots \\ h_1 & h_2 & \dots & h_0 \end{pmatrix}.$$

A circulant matrix is determined by its first row, reducing storage. Orthogonality and involutivity give $C^{-1} = C^T$ and $C^{-1} = C$, respectively. An MDS matrix has every square submatrix nonsingular and provides maximal linear branch number for diffusion in block ciphers. These properties motivate the search for structured matrices combining efficient representation, simple inversion, and strong diffusion.

In characteristic $p = 2$, Gupta and Ray proved the nonexistence of orthogonal circulant MDS matrices of size 2^n, $n \geq 2$, and of involutory circulant MDS matrices of size $n \geq 3$. For characteristic $p \geq 2$, Cauchois and Loidreau showed nonexistence of involutory circulant MDS matrices of size $2n$, $n \geq 2$. Adhiguna et al also proved no orthogonal circulant MDS matrices of size of sp for $p > 2$, $s \geq 2$; and of size $4n$, $n \geq 1$, for $p = 2$.

To explore further possibilities for existence, Cauchois and Loidreau generalized the concept of circulant matrix to θ-circulant matrix. Cauchois and Loidreau used q-polynomials to capture the cyclic structure of these matrices. Let θ be an automorphism of the field $\mathbb{F}_{q^m}$. Consider the ring of q-polynomials

$$\mathbb{F}_{q^m}[X;\theta] = \left\{ f\langle X\rangle = \sum_i a_i X^i : a_i \in \mathbb{F}_{q^m} \right\}$$

with the ordinary addition of polynomials and with multiplication $*$ defined by $X * a = \theta(a)X$ and, hence, $X^k a = a^{[k]} X^k$, where $a^{[k]} = \theta^k(a)$.

A θ-circulant matrix associated with a q-polynomial

$$h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{m-1} h_i X^i \in \mathbb{F}_{q^m}[X;\theta]$$

is defined by

$$C_{h,\theta} = \theta\text{-circ}(h_0, \dots, h_{m-1}) = \begin{pmatrix} h_0 & h_1 & \dots & h_{m-1} \\ h_{m-1}^{[1]} & h_0^{[1]} & \dots & h_{m-2}^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[m-1]} & h_2^{[m-1]} & \dots & h_0^{[m-1]} \end{pmatrix}.$$

Cauchois and Loidreau gave q-polynomial criteria for involutory θ-circulant MDS matrices; Adhiguna et al. established corresponding criteria for orthogonal matrices.

Objective of the Study

We investigate when smaller and larger orthogonal θ-circulant MDS matrices can be constructed over the same field and with the same automorphism.

Research Method

Fix the field and automorphism. For an admissible divisor $s < m$ satisfying $\operatorname{ord}(\theta) \mid s$, *compression* reduces a size-m matrix to size s by summing coefficients whose indices are congruent modulo s. The resulting matrix is the *seed*, and the original matrix is a *lift* of that seed. *Lifting* is the inverse problem: constructing a larger matrix whose compression equals a prescribed seed.

Discussion & Result

I. Algebraic Framework. Work in $\mathbb{F}_{q^r}[X;\theta]$, where $X * a = \theta(a)X$. The compatibility condition

"$\operatorname{ord}(\theta)$ divides m,"

that is, $\theta^m = \mathrm{id}$ makes $X^m - 1$ central, so the quotient by $\langle X^m - 1\rangle$ a well-defined ring.

II. Compression. We now state our main result.

Theorem 1. Suppose $\operatorname{ord}(\theta) \mid s$ and $m = \ell s$. Set $Y = X^s$. The compression of

$$h\langle X\rangle = (X^m - 1) + \sum_{i=0}^{s-1} \left(\sum_{u=0}^{\ell-1} h_{i+us} Y^u \right) X^i \in \mathbb{F}_{q^r}[X;\theta]$$

is

$$\bar{h}\langle X\rangle = (X^s - 1) + \sum_{i=0}^{s-1} \left(\sum_{u=0}^{\ell-1} h_{i+us} \right) X^i \in \mathbb{F}_{q^r}[X;\theta].$$

Equivalently, reduce modulo $X^s - 1$ by adding coefficients whose indices agree modulo s. Compression preserves orthogonality, involutivity, and MDS property, each independently.

Example. Let $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha)$ where $\alpha^4 + \alpha + 1 = 0$. Take $\theta(z) = z^4$ so $\operatorname{ord}(\theta) = 2$. The orthogonal MDS matrix below compresses from size $m = 4$ to an orthogonal MDS matrix of size $s = 2$.

$$C_{h,\theta} = \theta\text{-circ}(\alpha^2, \alpha^8, \alpha, \alpha)$$
$$\downarrow$$
Combine entries with subscripts congruent modulo $s = 2$.
$$\downarrow$$
$$C_{\bar{h},\theta} = \theta\text{-circ}(\alpha^2 + \alpha, \alpha^8 + \alpha)$$

Picture 1. Compression of size 4 to size 2

III. Lifting. Every size-m orthogonal seed admits a size-mt orthogonal lift for every positive integer t in odd characteristic, and every positive odd integer t in characteristic 2.

We now investigate size-2 orthogonal θ-circulant MDS matrices in characteristic 2. Define

$$\operatorname{Fix}(\theta) = \{a \in \mathbb{F}_{q^r} : \theta(a) = a\}.$$

Theorem 2. Let $\theta^2 = \mathrm{id}$ in characteristic 2.
1. A size-2 orthogonal θ-circulant MDS matrix exists if and only if $|\operatorname{Fix}(\theta)| > 2$. Each is of the form θ-circ$(a, a+1)$ where $a \in \backslash\operatorname{Fix}(\theta) - \{0,1\}$.
2. Let θ-circ$(a, a+1)$ be orthogonal MDS. Then

$$\theta\text{-}\operatorname{circ}(a+u, a+1+v, u, v)$$

is an orthogonal lift if and only if

$$a[\theta(v) + v] + (a+1)[\theta(u) + u] + a(a+1) = 0.$$

This orthogonal lift exists if and only if $\theta \neq \mathrm{id}$. If $\theta \neq \mathrm{id}$ and $w = u = v$ with $w + \theta(w) = a(a+1)$, the lift is MDS.

Theorem 3. Let $\operatorname{ord}(\theta) = 2$ in characteristic 2. No orthogonal θ-circulant MDS matrix of size $8n$ exists, $n \geq 1$.

Further lifting and obstructions are summarized below. All seeds are orthogonal MDS.

Characteristic Two	Odd Characteristic
$\theta = \mathrm{id}$	
Size-2 seeds exist if and only if $\lvert\mathbb{F}_{q^r}\rvert > 2$. *Lifting size 2 to size 4* Nonexistence at size $4n$ for $n \geq 1$.	No size-2 seeds exist. Nonexistence at size $2n$ for $n \geq 1$.
$\operatorname{ord}(\theta) = 2$	
Size-2 seeds exist if and only if $\lvert\operatorname{Fix}(\theta)\rvert > 2$. Nonexistence at size $2n$ for $n \geq 1$, when $\operatorname{Fix}(\theta) = \mathbb{F}_2$. *Lifting size 2 to size 4* Every seed admits size-4 orthogonal MDS lift *Lifting size 4 to size 8* Nonexistence at size $8n$ for $n \geq 1$. *Lifting size 4 to size 12* One orthogonal MDS is verified computationally.	Size-2 seeds exist if and only if $\lvert\operatorname{Fix}(\theta)\rvert > 3$. Nonexistence at size $2n$ for $n \geq 1$, when $\operatorname{Fix}(\theta) = \mathbb{F}_3$. *Lifting size 2 to size 4* Every seed admits size-4 orthogonal lift but none is MDS. Nonexistence at size $4n$ for $n \geq 1$.
$\operatorname{ord}(\theta) = 3$	
Size-3 seeds exist and constructions were presented. *Lifting size 3 to size 6* Every size-3 orthogonal MDS seed admits a size-6 MDS lift if $\lvert\operatorname{Fix}(\theta)\rvert \geq 2^8$.	In general, for odd characteristic, if $\theta^k = \mathrm{id}$ for odd k, then we have: Nonexistence at size $2nk$ for $n \geq 1$. *Lifting size 3 to size 6* Nonexistence at size $6n$ for $n \geq 1$.

Picture 2. Summary of MDS lifting and size obstructions

In characteristic 2, every size-2 orthogonal MDS seed for a nontrivial involution admits a size-4 MDS lift. For automorphisms of order 3, every size-3 orthogonal MDS seed admits a size-6 MDS lift when the fixed field has at least 256 elements. In contrast, orthogonal lifts need not be MDS, as the odd-characteristic cases demonstrate.

For $\theta = \mathrm{id}$, compression recovers Adhiguna et al.'s nonexistence results for orthogonal circulant MDS matrices: sizes $4n$ in characteristic two and sizes $2n$ in odd characteristic, $n \geq 1$.

Conclusion

Compression constructs smaller orthogonal θ-circulant MDS matrices at admissible divisors while keeping the field and automorphism fixed. Conversely, lifting yields explicit larger MDS matrices under suitable conditions. The nonexistence results show that such constructions cannot always be extended to larger sizes and recover known restrictions for ordinary circulant matrices.

References

V. Cauchois, P. Loidreau, On circulant involutory MDS matrices, Des. Codes Cryptogr., 87, (2019), 249–260. doi: 10.1007/s10623-018-0520-3.

K. C. Gupta, I. G. Ray, Cryptographically significant MDS matrices based on circulant and circulant-like matrices for lightweight applications, Cryptography and Communications, 7, (2015), 257–287.

I. Adhiguna, I. S. Noor Arifin, F. Yuliawan, and I. Muchtadi-Alamsyah, On Orthogonal Circulant MDS Matrices, *International Journal of Mathematics and Computer Science* **17**(4) (2022), 1619–1637.