Hadamard matrices from the Multiplication Table of the Finite Fields

*Min-Ho Shin, **Jong-Seon No, *Hong-Yeop Song

*Yonsei University of Seoul Korea

**Seoul National University of Seoul Korea

Contents

- **Introduction**
  - **Hadamard matrices**
  - **binary m-sequences**
  - **Relation**
- **Constructions**
  - **Theorem1. Construction with canonical basis**
  - **Theorem2. Construction with any basis**
- **Remarks**

Introduction

‣ Hadamard matrix

- **Definition** : A *Hadamard matrix* of order n is an n by n matrix with entries +1 or -1 such that

$$HH^T = nI$$

- **Example 1.** Hadamard matrix of order 8

+	+	+	+	+	+	+	+
+	−	+	−	+	−	+	−
+	+	−	−	+	+	−	−
+	−	−	+	+	−	−	+
+	+	+	+	−	−	−	−
+	−	+	−	−	+	−	+
+	+	−	−	−	−	+	+
+	−	−	+	−	+	+	−

Note1 Any two rows of H are orthogonal.
(this property does not change if we permute rows or columns or if we multiply some rows or columns by -1)

Note2 Two such Hadamard matrices are called *equivalent.*

"+" denotes +1, "−" denotes -1

Relation between Hadamard matrices and ECC

- All the rows of a Hadamard matrix of order n form an **orthogonal code** of length n and size n.

- All the rows of a Hadamard matrix of order n and their complements form a **biorthogonal code** of length n and size $2n$

- All the rows of a normalized Hadamard matrix of order n without their first component form a **simplex code** of length $n-1$ and size n

m-sequences

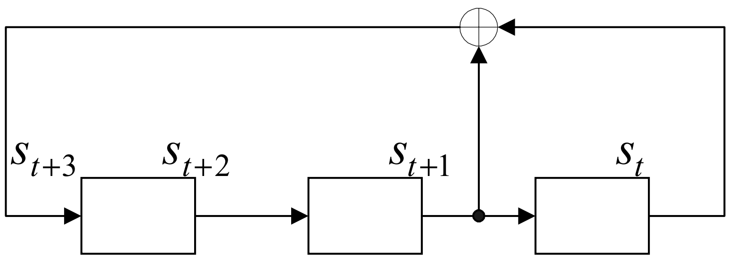
- **Definition** : Maximal length LFSR(Linear Feedback Shift Register) sequences
- A linear recurring sequence (degree m) over F_q with recurrence relation

$$s_t = \sum_{i=0}^{m-1} a_i s_{t-i} \qquad a_i \in F_q$$

can be generated by an m-stage LFSR with a characteristic polynomial

$$f(x) = x^m - a_1 x^{m-1} - a_2 x^{m-2} - \cdots - a_m$$

- **Example 2.** Generation of a binary m-sequence with 3-stage LFSR



- linear recurrence (degree 3)

$$s_t = s_{t-2} + s_{t-3}$$

- characteristic polynomial

$$f(x) = x^3 + x + 1$$

- s_t has a period $2^3 - 1 = 7$

m-sequences(cont'd)

- Facts
  - An LFSR produces an m-sequence over GF(2) if and only if its characteristic polynomial is primitive.
  - m-sequences are analytically represented by the *trace function*

$$s_t = \mathrm{tr}_1^n(\theta\alpha^t) \qquad \theta \in \mathrm{GF}(2^n) - \{0\}$$

$$\alpha : \text{primitive in } \mathrm{GF}(2^n)$$

where trace function $\mathrm{tr}(\cdot)$ *maps* $\mathrm{GF}(2^n)$ *into* GF(2)

- Properties(selected)
  - Ideal autocorrelation property(period N)

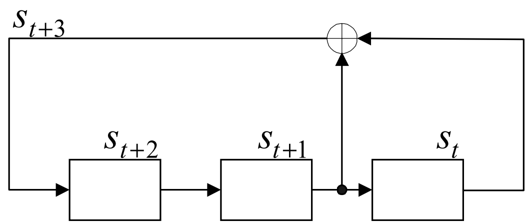
$$\phi_b(\tau) = \sum_{t=0}^{N-1} (-1)^{s_t + s_{t+\tau}} = \begin{cases} N & \tau \equiv 0 \mod N \\ -1 & \tau \not\equiv 0 \mod N \end{cases}$$

  - Cycle and add property : the sum of m-sequence $\{s_t\}$ and its τ -shift $\{s_{t+\tau}\}$ is another shift $\{s_{t+\tau'(\tau)}\}$ of the same m-sequence

$$\mathrm{s_t} + \mathrm{s}_{\mathrm{t}+\tau} = \mathrm{s}_{\mathrm{t}+\tau'(\tau)} \Leftrightarrow \mathrm{tr}_1^n(\theta\alpha^t) + \mathrm{tr}_1^n(\theta\alpha^{t+\tau}) = \mathrm{tr}_1^n(\theta\alpha^{t+\tau'(\tau)})$$

Relation between Hadamard matrices and binary *m*-sequences

- **Example 3.** *m*-sequence (period $2^3 - 1$) vs Hadamard matrix(order 2^3)



$\{s_{t+2}\}$	$\{s_{t+1}\}$	$\{s_t\}$
0	0	1
1	0	0
0	1	0
1	0	1
1	1	0
1	1	1
0	1	1

$$s_t = \mathrm{tr}_1^3(\alpha^t)$$

Cyclic Hadamard matrix
(order 8)

0	0	0	0	0	0	0	0
0	1	0	0	1	0	1	1
0	0	0	1	0	1	1	1
0	0	1	0	1	1	1	0
0	1	0	1	1	1	0	0
0	0	1	1	1	0	0	1
0	1	1	1	0	0	1	0
0	1	1	0	0	1	0	1

$$(\text{"0"} \Leftrightarrow +1,\ \text{"1"} \Leftrightarrow -1)$$

Relation (in general)

- $\{s_t\}$ binary *m*-sequence of period $N = 2^n - 1$

$$s_0 \; s_1 \; s_2 \cdots s_{N-2} \; s_{N-1}$$

- With trace representation

$$s_t = \mathrm{tr}_1^n(\theta\alpha^t)$$

$$\theta \in \mathrm{GF}(2^n) - \{0\}$$

$$\alpha : \text{primitive in } \mathrm{GF}(2^n)$$

- $(N+1)$ by $(N+1)$ matrix

$$H = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{bmatrix}$$

- matrix C : N by N **circulant** matrix generated by cyclic shift of $\{s_t\}$

- With trace representation

$$C = (c_{ij}) \quad 0 \le i, j \le N-1$$

$$c_{ij} = \mathrm{tr}_1^n(\theta\alpha^{i+j})$$

- By autocorrelation property of the *m*-sequence, dot product of any two rows of N by N matrix C is -1(after changing "0"to +1, "1" to -1)
- Hence $(N+1)$ by $(N+1)$ matrix H defined as above is a Hadamard matrix of order 2^n

Constructions

▸ Construction in GF(2^n)

- **Example 4.** From multiplication table of GF(2^3) with canonical basis.
  α : primitive in GF(2^3) satisfying $\alpha^3+\alpha+1=0$

Field generation

Power	Polynomial	Vector		
0	0	0	0	0
1	1	1	0	0
α	α	0	1	0
α^2	α^2	0	0	1
α^3	$1+\alpha$	1	1	0
α^4	$\alpha+\alpha^2$	0	1	1
α^5	$1+\alpha+\alpha^2$	1	1	1
α^6	$1+\alpha^2$	1	0	1

Multiplication table

·	0	1	α	α^2	α^3	α^4	α^5	α^6
0	0	0	0	0	0	0	0	0
1	0	1	α	α^2	α^3	α^4	α^5	α^6
α	0	α	α^2	α^3	α^4	α^5	α^6	1
α^2	0	α^2	α^3	α^4	α^5	α^6	1	α
α^3	0	α^3	α^4	α^5	α^6	1	α	α^2
α^4	0	α^4	α^5	α^6	1	α	α^2	α^3
α^5	0	α^5	α^6	1	α	α^2	α^3	α^4
α^6	0	α^6	1	α	α^2	α^3	α^4	α^5

2^3-1

2^3-1

Note 1 each successive sequence (vector represented) from α^ith coefficient is cyclically equivalent *m*-sequence .

Note 2 (2^3-1) by (2^3-1) matrix is circulant.

- **Example 4.** (cont'd)

  Hadamard matrices from the vector represented multiplication table of canonical basis

0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0	0 0 0
0 0 0	1 0 0	0 1 0	0 0 1	1 1 0	0 1 1	1 1 1	1 0 1
0 0 0	0 1 0	0 0 1	1 1 0	0 1 1	1 1 1	1 0 1	1 0 0
0 0 0	0 0 1	1 1 0	0 1 1	1 1 1	1 0 1	1 0 0	0 1 0
0 0 0	1 1 0	0 1 1	1 1 1	1 0 1	1 0 0	0 1 0	0 0 1
0 0 0	0 1 1	1 1 1	1 0 1	1 0 0	0 1 0	0 0 1	1 1 0
0 0 0	1 1 1	1 0 1	1 0 0	0 1 0	0 0 1	1 1 0	0 1 1
0 0 0	1 0 1	1 0 0	0 1 0	0 0 1	1 1 0	0 1 1	1 1 1

0	0	0	0	0	0	0	0
0	1	0	0	1	0	1	1
0	0	0	1	0	1	1	1
0	0	1	0	1	1	1	0
0	1	0	1	1	1	0	0
0	0	1	1	1	0	0	1
0	1	1	1	0	0	1	0
0	1	1	0	0	1	0	1

$$s_t = \mathrm{tr}_1^3(\alpha^t)$$

0	0	0	0	0	0	0	0
0	0	1	0	1	1	1	0
0	1	0	1	1	1	0	0
0	0	1	1	1	0	0	1
0	1	1	1	0	0	1	0
0	1	1	0	0	1	0	1
0	1	0	0	1	0	1	1
0	0	0	1	0	1	1	1

$$s_{t+2} = \mathrm{tr}_1^3(\alpha^{t+2})$$

0	0	0	0	0	0	0	0
0	0	0	1	0	1	1	1
0	0	1	0	1	1	1	0
0	1	0	1	1	1	0	0
0	0	1	1	1	0	0	1
0	1	1	1	0	0	1	0
0	1	1	0	0	1	0	1
0	1	0	0	1	0	1	1

$$s_{t+1} = \mathrm{tr}_1^3(\alpha^{t+1})$$

Theorem 1.

Let $\mathrm{GF}(2^n)$ be the finite field with 2^n elements, and $\alpha \in \mathrm{GF}(2^n)$ be a primitive element.

Consider the multiplication table of $\mathrm{GF}(2^n)$ with borders

$$0,\ 1,\ \alpha,\ \alpha^2,\ \cdots\ ,\ \alpha^{2^n-3},\ \alpha^{2^n-2}\ .$$

Let the entries of this table be vector-represented over GF(2) using the canonical basis

$$1,\ \alpha,\ \alpha^2,\ \cdots\ ,\ \alpha^{n-1}\ .$$

For $i = 0, 1, \cdots, n-1$, let H_i be the $2^n \times 2^n$ matrix obtained by taking the *i*-th component of all the entries of the multiplication table.

Then, these *n* matrices H_i are Hadamard matrices, and they are equivalent only by column permutation

- **Example 6.** From multiplication table of $\mathrm{GF}(2^3)$ with arbitrary basis.
  α: primitive in $\mathrm{GF}(2^3)$ satisfying $\alpha^3+\alpha+1=0$
  (change coordinates from canonical basis to the β basis)

  $\forall x \in \mathrm{GF}(2^3)$ by canonical basis expansion and β basis expansion

  $$x = x_0 + x_1\alpha + x_2\alpha^2 \qquad\qquad x = x_0'\beta_0 + x_1'\beta_1 + x_2'\beta_2$$

  Define binary row vectors $\underline{\mathbf{x}}$ and $\underline{\mathbf{x}}'$ by

  $$\underline{\mathbf{x}} = (x_0, x_1, x_2) \qquad\qquad \underline{\mathbf{x}}' = (x_0', x_1', x_2')$$

  Let β basis arbitrary

  $$\beta_0 = \alpha^5 = 1+\alpha+\alpha^2$$
  $$\beta_1 = \alpha^4 = \alpha+\alpha^2$$
  $$\beta_2 = \alpha^3 = 1+\alpha$$

  From above relation define 3 by 3 matrices A and B

  $$B = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \qquad A = B^{-1} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

  Then we can change the coordinates as follows

  $$\underline{\mathbf{x}}' = \underline{\mathbf{x}}\,A \qquad\qquad \underline{\mathbf{x}} = \underline{\mathbf{x}}'\,B$$

- **Example 6.** (cont'd)

Canonical basis		β basis	
	$\underline{\mathbf{x}}$	$\underline{\mathbf{x}}'$	
Power	$1 \quad \alpha \quad \alpha^2$	$\alpha^5 \quad \alpha^4 \quad \alpha^3$	Check
0	0 0 0	0 0 0	0
1	1 0 0	1 1 0	$\alpha^5+\alpha^4 = 1$
α	0 1 0	1 1 1	$\alpha^5+\alpha^4+\alpha^3 = \alpha$
α^2	0 0 1	1 0 1	$\alpha^5+\alpha^3 = \alpha^2$
α^3	1 1 0	0 0 1	$\alpha^3 = \alpha^3$
α^4	0 1 1	0 1 0	$\alpha^4 = \alpha^4$
α^5	1 1 1	1 0 0	$\alpha^5 = \alpha^5$
α^6	1 0 1	0 1 1	$\alpha^4+\alpha^3 = \alpha^6$

$$\underline{\mathbf{x}}' = \underline{\mathbf{x}}\begin{bmatrix}1 & 1 & 0\\ 1 & 1 & 1\\ 1 & 0 & 1\end{bmatrix}$$

$$\begin{aligned} H_0 &\Leftrightarrow \mathrm{tr}_1^3(\alpha^t)\\ H_1 &\Leftrightarrow \mathrm{tr}_1^3(\alpha^{t+2})\\ H_2 &\Leftrightarrow \mathrm{tr}_1^3(\alpha^{t+1}) \end{aligned}$$

$$\begin{aligned} \mathrm{tr}_1^3(\alpha^t)+\mathrm{tr}_1^3(\alpha^{t+2})+\mathrm{tr}_1^3(\alpha^{t+1}) &= \mathrm{tr}_1^3(\alpha^{t+5}) \Leftrightarrow H_0'\\ \mathrm{tr}_1^3(\alpha^t)+\mathrm{tr}_1^3(\alpha^{t+2}) &= \mathrm{tr}_1^3(\alpha^{t+6}) \Leftrightarrow H_1'\\ \mathrm{tr}_1^3(\alpha^{t+2})+\mathrm{tr}_1^3(\alpha^{t+1}) &= \mathrm{tr}_1^3(\alpha^{t+4}) \Leftrightarrow H_2' \end{aligned}$$

- **Example 6.** (cont'd)

Canonical basis

β basis

$$\mathrm{tr}_1^3(\alpha^t) \Leftrightarrow H_0 = \begin{bmatrix} 0&0&0&0&0&0&0&0\\ 0&1&0&0&1&0&1&1\\ 0&0&0&1&0&1&1&1\\ 0&0&1&0&1&1&1&0\\ 0&1&0&1&1&1&0&1\\ 0&0&1&1&1&0&1&1\\ 0&1&1&1&0&1&1&0\\ 0&1&1&0&1&1&0&1 \end{bmatrix}$$

$$H_0' = UH_0 \quad \Longleftrightarrow \quad H_0 = U^T H_0'$$

$$H_0' = \begin{bmatrix} 0&0&0&0&0&0&0&0\\ 0&1&1&1&0&1&1&0\\ 0&1&1&0&1&1&0&1\\ 0&1&0&1&1&0&1&1\\ 0&0&1&1&0&1&1&1\\ 0&1&1&0&1&1&1&0\\ 0&1&0&1&1&1&0&1\\ 0&0&1&1&1&0&1&1 \end{bmatrix} \Leftrightarrow \mathrm{tr}_1^3(\alpha^{t+5})$$

$$U = \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&1\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0 \end{bmatrix}$$

Note the transformation matrix U is a permutation matrix. i.e $UU^T = I$

Hence two such matrices are equivalent by row(or column) permutation

Theorem 2.

Representation of elements in $\mathrm{GF}(2^n)$ in Theorem 1 can be done by using any basis.

Relation of Hadamard matrices and *m*-sequences (canonical basis)

$$H_i \Leftrightarrow \mathrm{tr}_1^n(\theta_i \alpha^t)$$

The β basis can be represented by

$$\beta_j = \sum_{i=0}^{n-1} b_{ij}\alpha^i, \qquad b_{ij} \in \{0,\ 1\}, \qquad 0 \le j \le n-1$$

Define the *n* by *n* matrix $B = (b_{ij})$ and $A = B^{-1} = (a_{ij})$

Then H_i' are related to the *m*-sequences as follows(β basis)

$$H_i' \Leftrightarrow \sum_{k=0}^{n-1} a_{ki}\mathrm{tr}_1^n(\theta_k \alpha^t) = \mathrm{tr}_1^n\left(\left(\sum_{k=0}^{n-1} a_{ki}\theta_k\right)\alpha^t\right) = \mathrm{tr}_1^n(\theta_i' \alpha^t)$$

Note $\quad \theta_i' = \sum_{k=0}^{n-1} a_{ki}\theta_k \in \mathrm{GF}(2^n) - \{0\}$

Remarks

- Non-basis representation may not work

Example 7. A matrix obtained from the non-basis vector represented multiplication table of $GF(2^4)$

0	0 0 0 0	0 0 0 0
1	1 0 0 0	1 0 0 0
α	0 1 0 0	0 1 0 0
α^2	0 0 1 0	0 0 1 0
α^3	**0 0 0 1**	**1 1 0 1**
α^4	1 0 0 1	1 0 0 1
α^5	**1 1 0 1**	**0 1 0 1**
α^6	1 1 1 1	1 1 1 1
α^7	1 1 1 0	1 1 1 0
α^8	0 1 1 1	0 1 1 1
α^9	1 0 1 0	1 0 1 0
α^{10}	**0 1 0 1**	**0 0 0 1**
α^{11}	1 0 1 1	1 0 1 1
α^{12}	1 1 0 0	1 1 0 0
α^{13}	0 1 1 0	0 1 1 0
α^{14}	0 0 1 1	0 0 1 1

$$H_0 = \begin{array}{cl} \begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&1&1&0&1&1&0&1&0&1&1&0&0\\
0&0&0&1&1&0&1&1&0&1&0&1&1&0&0&1\\
0&0&1&1&0&1&1&0&1&0&1&1&0&0&1&0\\
0&1&1&0&1&1&0&1&0&1&1&0&0&1&0&0\\
0&1&0&1&1&0&1&0&1&1&0&0&1&0&0&1\\
0&0&1&1&0&1&0&1&1&0&0&1&0&0&1&1\\
0&1&1&0&1&0&1&1&0&0&1&0&0&1&1&0\\
0&1&0&1&0&1&1&0&0&1&0&0&1&1&0&1\\
0&0&1&0&1&1&0&0&1&0&0&1&1&0&1&1\\
0&1&0&1&1&0&0&1&0&0&1&1&0&1&1&0\\
0&0&1&1&0&0&1&0&0&1&1&0&1&1&0&1\\
0&1&1&0&0&1&0&0&1&1&0&1&1&0&1&0\\
0&1&0&0&1&0&0&1&1&0&1&1&0&1&0&1\\
\mathbf{0}&\mathbf{0}&0&1&\mathbf{0}&0&\mathbf{1}&1&0&\mathbf{1}&1&0&1&0&\mathbf{1}&1\\
\mathbf{0}&\mathbf{0}&1&0&\mathbf{0}&1&\mathbf{1}&0&1&\mathbf{1}&0&1&0&1&\mathbf{1}&0
\end{bmatrix} & \begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \Leftarrow 15\text{th row} \\ \Leftarrow 16\text{th row} \end{array} \end{array}$$

Note 15th row and 16th row are not orthogonal