IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024TAP0009

Publicized:2024/09/02

This advance publication article will be replaced by the finalized version after proofreading.

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER Special Section on Information Theory and Its Applications

New Varieties of Hadamard-type Matrices over Finite Fields and Their Properties*

Iori KODAMA†, *Nonmember and* **Tetsuya KOJIMA**††a), *Senior Member*

SUMMARY Hadamard matrix is defined as a square matrix where any components are -1 or $+1$, and where any pairs of rows are mutually orthogonal. On the other hand, Hadamard-type matrix on finite fields has been proposed. This matrix is a similar one as a binary Hadamard matrix, but has multi-valued components on finite fields. To be more specific, we consider $n \times n$ matrices that have their elements on the given finite fields $GF(p)$, and satisfy $HH^T \equiv nI \mod p$, where I is an identity matrix. Any additions and multiplications should be executed under modulo p. In this paper, the authors introduce some new Hadamard-type matrices found in computer searches as well as their properties. Specifically, we define special types of Hadamard-type matrices called cyclic Hadamard-type matrices on finite fields, and propose the methods to generate them. In addition, it is shown that the order of an arbitrary Hadamard-type matrix of odd order is limited to quadratic residues of the given prime p. Some methods to extend the order of Hadamard-type matrices are also discussed.
key words: *Hadamard-type matrix, finite field, cyclic matrix, quadratic residue*

1. Introduction

Hadamard matrix is defined as a square matrix H with $\{-1, +1\}$ entries where any pairs of two rows are mutually orthogonal [1]. In other words, H satisfies $HH^T = nI$, where ^{T} implies the transposition of the matrix, I stands for an identity matrix, and n is the order of the matrix. Hadamard matrices can be applied into many fields such as coding theory, radio communications, statistical estimation, compressed sensing, and so on[2], [3]. In addition, they can be used to generate error correcting codes such as Walsh-Hadamard codes or Reed-Muller codes, and also to generate spread spectrum sequences like n-shift orthogonal sequences and complete complementary codes (CCC)[4].

The authors have extended the concept of the original binary Hadamard matrices into finite fields $GF(p)$, where p is an odd prime[5]–[7]. To be more specific, such matrices can be defined as the square matrices on $GF(p)$, where any pairs of rows are mutually orthogonal. Any additions and multiplications are executed under modulo p. We call such a matrix Hadamard-type matrix on $GF(p)$, which can be written as H-type matrix in short.

In [5], the authors have classified H-type matrices into three different types, and proposed the methods to generate them. However, the norm of each row in the generated matrices is not constant in many cases, which implies that $HH^T \not\equiv nI \mod p$. The only type satisfying $HH^T \equiv nI \mod p$ is the one that is essentially identical to original binary Hadamard matrix on $\{-1, +1\}$.

On the other hand, the authors have also proposed a way to generate H-type matrices H on $GF(p)$ for any odd prime p, where the norm of every row is identical[6], [7]. In other words, these matrices have almost same properties as the original Hadamard matrices on $\{-1, +1\}$. The proposed generation method employs the cyclic groups on $GF(p)$, and is based on the inner products of the conjugate vectors specially defined by the authors using the multiplicative inverses on $GF(p)$. However, it has been pointed out that such inner products do not satisfy the inner product axioms[6], [7].

In this study, we are only concerned with the H-type matrices on $GF(p)$ that are not based on such inner products and that satisfy $HH^T \equiv nI \mod p$. In this paper, we introduce some H-type matrices discovered by the brute-force searches. These newly discovered matrices are different from those generated in the previous studies[5], [7]. Especially, we proposed the methods to generate special types of these matrices called cyclic H-type matrices. In addition, it is proved that the orders of any H-type matrices of odd order on finite fields are limited to the quadratic residues of p. The paper also includes the discussion on the way to extend the order of H-type matrices.

2. Preliminaries

2.1 Notations

In this paper, the following notations are used otherwise stated.

- p : odd prime number
- ^{T} : transposition of matrices
- I : identity matrix
- O : null matrix
- $\left(\dfrac{n}{p}\right)$: Legendre symbol
- $\sqrt{n}$: square root of an element n on $GF(p)$
- $A \otimes B$: Kronecker product of the matrices A and B

†The author is with the Advanced Course of Mechanical and Computer Systems Engineering, National Institute of Technology, Tokyo College, Hachioji-shi, 193-0997, Japan.
††The author is with the Department of Computer Systems, National Institute of Technology, Tokyo College, Hachioji-shi, 193-0997, Japan.
*The contents of this paper have been partly presented at the IEICE Technical Conferences on Information Theory in Japanese from 2022 to 2024[8]–[10].
a) E-mail: kojt@tokyo-ct.ac.jp, kojt@ieee.org

- $\mathbb{Z}_m$: residue class ring modulo m

2.2 Hadamard-type Matrices on Finite Fields

As mentioned above, we are only concerned with the Hadamard-type matrices satisfying $HH^T \equiv nI \mod p$ on finite fields. They should be generated without employing the special inner products defined in [6], [7]. These matrices are called as Hadamard-type matrices in narrow sense in [8], and defined as follows.

Definition 1 (Hadamard-type Matrix): For any odd prime p, Hadamard-type matrix on $GF(p)$ of order n is defined as a square matrix of order n on $GF(p)$, that is, an $n \times n$ matrix on $\{0, 1, \ldots, p-1\}$, where any pairs of rows are mutually orthogonal as well as the norm of each row is identical to n. In other words, a Hadamard-type matrix H on $GF(p)$ of order n should satisfy

$$HH^T \equiv nI \mod p. \tag{1}$$

In this paper, such a matrix is also called H-type matrix in short.

It is assumed that any additions and multiplications on $GF(p)$ are executed under modulo p.

Remark 1: If the order n of the matrix is a quadratic residue of p, the identity matrix multiplied by $\sqrt{n}$, that is,

$$H = \sqrt{n} \cdot I \tag{2}$$

can be considered as a special case of H-type matrix. As described in Sect.2.1, $\sqrt{n}$ stands for a square root of n on $GF(p)$, where n must be a quadratic residue of the given prime p. If n is a quadratic non-residue, $\sqrt{n}$ does not have any values on $GF(p)$.

Example 1:

$$H \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 \\ 1 & 4 \end{bmatrix} \tag{3}$$

is an H-type matrix on $GF(5)$ of order 2 since $HH^T \equiv 2I \mod 5$. This is trivial because $4 \equiv -1 \mod 5$, which implies that the matrix H is essentially same as a binary Hadamard matrix:

$$H' \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{4}$$

In our previous studies, any ways to generate an H-type matrix other than this type and the trivial cases such as Eq.(2) have not been proposed unless a specially defined inner product on finite fields[5]–[7] is employed.

For a given prime p, H-type matrices can be defined in a prime finite field $GF(p)$ as well as in its extension $GF(p^m)$[6], [7]. In the following, we consider only $GF(p)$ for simplicity.

3. New Examples of H-type Matrices on Finite Fields

The authors have discovered some new varieties of H-type matrices on finite fields by brute-force searches. Here are some examples.

Example 2:

$$H \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 8 & 10 \\ 1 & 1 & 7 & 4 & 9 \\ 1 & 8 & 4 & 6 & 3 \\ 1 & 10 & 9 & 3 & 10 \end{bmatrix} \tag{5}$$

is an H-type matrix of order 5 on $GF(11)$ since $HH^T \equiv 5I \mod 11$.

Example 3:

$$H \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 9 & 9 & 9 \\ 1 & 9 & 5 & 9 & 9 \\ 1 & 9 & 9 & 5 & 9 \\ 1 & 9 & 9 & 9 & 5 \end{bmatrix} \tag{6}$$

is also an H-type matrix of order 5 on $GF(11)$ since $HH^T \equiv 5I \mod 11$.

As stated above, the only type of H-type matrices known in the previous studies[5]–[7] is the one that is essentially identical to original binary Hadamard matrix on $\{-1, +1\}$, such as that shown in Example 1. On the other hand, the matrices shown in Examples 2 and 3 have not been known in the previous studies. Obviously, the methods to generate them have been also unknown so far.

Note that the elements in the first row and the first column of the matrices (5) and (6) are all '1'. Such matrices are called as standard-form H-type matrices. We have searched only standard-from H-type matrices in the brute-force searches. There is no loss of generality in this limitation. It is possible to generate various H-type matrices by multiplying any diagonal matrices to standard-form H-type matrices.

Also note that the 4×4 sub-matrix obtained by removing the first row and the first column from the matrix H shown in Eq.(6) is a cyclic matrix. In the following section, we propose the methods to generate such matrices.

4. Cyclic H-type Matrices

4.1 Standard-Form Cyclic H-type Matrices

The matrix given in Example 3 is a special case of H-type matrices on finite fields. The definition of such type of matrices can be given as follows.

Definition 2: (Standard-form Cyclic H-type Matrix) An H-type matrix of the form:

$$H \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & a & b & \cdots & b \\ 1 & b & a & \cdots & b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & b & b & \cdots & a \end{bmatrix} \quad (7)$$

is defined as a standard-form cyclic H-type matrix on finite fields.

Note that the orthogonality of an H-type matrix (7) holds even if any two rows or columns are swapped. It implies that any square matrices on $GF(p)$ satisfying the following conditions have the same properties as a standard-form cyclic H-type matrix:

- all the elements in the first row and the first column are 1,
- in the sub-matrix obtained by removing the first row and the first column, any rows or columns have only one 'a', and
- the other elements are all 'b',

where a and b are arbitrary elements on the given finite field. In the following, we are only concerned with the matrices of the form (7) without loss of generality.

The method to generate the standard-form cyclic H-type matrices can be given by the following theorem.

Theorem 1: A standard-form cyclic H-type matrix of order n on $GF(p)$ exists if and only if there are two different elements a and b on $GF(p)$ satisfying the following two conditions:

$$1 - 2b - (n-1)b^2 \equiv 0 \mod p, \quad (8)$$

$$a \equiv -1 - (n-2)b \mod p. \quad (9)$$

Proof. Under the assumption that any rows or columns can be swapped, the necessary and sufficient conditions that an H-type matrix H can be written in the form of Eq.(7) are given as follows:

$$1 + a + (n-2)b \equiv 0 \mod p, \quad (10)$$
$$1 + 2ab + (n-3)b^2 \equiv 0 \mod p, \quad (11)$$
$$1 + a^2 + (n-2)b^2 \equiv n \mod p, \quad (12)$$

where Eqs.(10) and (11) implies the orthogonality between the first row and any other rows and the orthogonality between any two different rows except for the first row, respectively. On the other hand, Eq.(12) means that the norm of each row except for the first row is n.

First, we show that Eqs.(8) and (9) hold for any standard-form cyclic H-type matrices that satisfy Eqs.(10), (11) and (12). It can be obviously shown that Eq.(9) holds by solving Eq.(10) for a. On the other hand, by substituting Eq.(9) into Eq.(11), we can obtain

$$1 + 2(-1 - (n-2)b)b + (n-3)b^2 \equiv 0 \mod p, \quad (13)$$

which is identical to Eq.(8).

Next, we show Eqs.(10), (11) and (12) hold if we assume two conditions (8) and (9). Firstly, Eq.(10) obviously holds from Eq.(9). By substituting Eq.(9) into the $l.h.s.$ of Eq.(11), we get

$$\begin{aligned} &1 + 2ab + (n-3)b^2 \\ &\quad \equiv 1 + 2(-1 - (n-2)b)b + (n-3)b^2 \\ &\quad \equiv 1 - 2b - (n-1)b^2 \equiv 0 \mod p \end{aligned} \quad (14)$$

from Eq.(8). To show that Eq.(12) holds, we put the $l.h.s.$ of Eq.(12) as

$$Z \stackrel{\text{def}}{=} 1 + a^2 + (n-2)b^2. \quad (15)$$

Then, by substituting Eq.(9) into $Z - n$, it can be shown that

$$\begin{aligned} Z - n &\equiv -n + 1 + a^2 + (n-2)b^2 \\ &\equiv -n + 1 + \{-1 - (n-2)b\}^2 + (n-2)b^2 \\ &\equiv -n + 2 + 2(n-2)b + (n-2)^2b^2 \\ &\qquad + (n-2)b^2 \mod p. \end{aligned} \quad (16)$$

If $n \neq 2$, by dividing the both sides of Eq.(16) by $(n-2)$, we have

$$\begin{aligned} \frac{Z-n}{n-2} &= -1 + 2b + (n-2)b^2 + b^2 \\ &= -1 + 2b + (n-1)b^2 \equiv 0 \mod p \end{aligned} \quad (17)$$

according to Eq.(8). Therefore, we have $Z \equiv n \mod p$, which is identical to Eq.(12). If $n = 2$, we obtain $a \equiv -1 \mod p$ from Eq.(9). By substituting it into the $l.h.s.$ of Eq.(12), we have

$$1 + (-1)^2 = 1 + 1 = 2 = n. \quad (18)$$

Now we proved the theorem. □

Given a prime number p and the order n of the matrix, two elements a and b can be evaluated by solving the set of equations (8) and (9).

Example 4: Given $p = 11$ and $n = 5$, the set of two equations can be expressed as

$$\begin{cases} 1 - 2b - 4b^2 \equiv 0 \mod 11, \\ a \equiv -1 - 3b \mod 11. \end{cases} \quad (19)$$

The solutions of these equations can be obtained as $(a, b) \equiv (0, 7)$ and $(5, 9) \mod 11$. If we take $(a, b) = (5, 9)$, we can get the H-type matrix H given in Eq.(6).

Any standard-form cyclic H-type matrices satisfy the following theorem.

Theorem 2: For any standard-form cyclic H-type matrices,

$$(a - b)^2 \equiv n \mod p. \quad (20)$$

Proof. For any standard-form cyclic H-type matrices, Eqs.(11) and (12) hold. By taking the differences of both sides of these equations, we have

$$a^2 - 2ab + b^2 \equiv n \mod p, \tag{21}$$

which is identical to Eq.(20). □

Theorem 2 implies that the order of a standard-form cyclic H-type matrix should be a quadratic residue of the given p.

4.2 (Non-standard-form) Cyclic H-type Matrices

Similarly to Definition 2, it is possible to define non-standard-form cyclic H-type matrices.

Definition 3: (Cyclic H-type Matrix) An H-type matrix of the form:

$$H \stackrel{\text{def}}{=} \begin{bmatrix} a & b & \cdots & b \\ b & a & \cdots & b \\ \vdots & \vdots & \ddots & \vdots \\ b & b & \cdots & a \end{bmatrix} \tag{22}$$

is defined as a cyclic H-type matrix on finite fields.

Note that the orthogonality of rows and columns holds even if any two rows or columns are swapped in the matrix (22) in a similar way as standard-form cyclic H-type matrices. It implies that any square matrices on $GF(p)$ satisfying the following conditions have the same properties as a cyclic H-type matrix:

- any rows or columns have only one 'a', and
- the other elements are all 'b'.

The generation method of the cyclic H-type matrices can be given by the following theorem.

Theorem 3: A cyclic H-type matrix of order n on $GF(p)$ exists if and only if there are two different elements a and b on $GF(p)$ satisfying the following two conditions:

$$a \equiv -\frac{(n-2)}{2} \cdot b \mod p, \tag{23}$$

$$b^2 \equiv \frac{4}{n} \mod p, \tag{24}$$

where the order n satisfies $n \not\equiv 0 \mod p$.

Proof. In a similar way as the proof of Theorem 1, under the assumption that any rows or columns can be swapped, the necessary and sufficient conditions that an H-type matrix H can be written in the form of Eq.(22) are given as follows:

$$2ab + (n-2)b^2 \equiv 0 \mod p, \tag{25}$$

$$a^2 + (n-1)b^2 \equiv n \mod p, \tag{26}$$

where Eq.(25) implies the orthogonality between any two different rows, while Eq.(26) means that the norm of each row is congruent to n modulo p.

First, we show that Eqs.(23) and (24) hold for any standard-form cyclic H-type matrices that satisfy Eqs.(25) and (26). Note that it is impossible to obtain any pairs of solutions where $a \equiv 0$ or $b \equiv 0 \mod p$ are satisfied under the two conditions (23) and (24). So we assume $b \not\equiv 0 \mod p$ in the following. From Eq.(25), we can obtain

$$ab \equiv -\frac{(n-2)}{2} b^2 \mod p, \tag{27}$$

which implies that Eq.(23) holds since $b \not\equiv 0 \mod p$. On the other hand, by substituting Eq.(23) into Eq.(26), we can obtain

$$\left(-\frac{n-2}{2} \cdot b\right)^2 + (n-1)b^2 \equiv n \mod p, \tag{28}$$

which leads to

$$\left\{(n-2)^2 + 4(n-1)\right\} b^2 \equiv 4n \mod p. \tag{29}$$

Therefore we can get

$$n^2 b^2 \equiv 4n \mod p, \tag{30}$$

which is identical to Eq.(24) since $n \not\equiv 0 \mod p$.

Next, we show Eqs.(25) and (26) hold if we assume two conditions (23) and (24). By substituting Eq.(23) into the $l.h.s.$ of Eq.(25), we get

$$2\left(-\frac{n-2}{2} \cdot b\right) b + (n-2)b^2$$
$$= -(n-2)b^2 + (n-2)b^2 \equiv 0 \mod p, \tag{31}$$

which is identical to Eq.(25). Similarly, by substituting Eq.(23) into the $l.h.s.$ of Eq.(26), we obtain

$$\left(-\frac{(n-2)}{2} \cdot b\right)^2 + (n-1)b^2$$
$$= \frac{\left\{(n-2)^2 + 4(n-1)\right\} b^2}{4}$$
$$= \frac{n^2 b^2}{4}, \tag{32}$$

which leads to Eq.(26) by applying Eq.(24).

Now we proved the theorem. □

Given a prime number p and the order n of the matrix, two elements a and b can be evaluated by solving the set of Eqs.(23) and (24).

Example 5: Given $p = 11$ and $n = 5$, the solutions of Eqs.(23) and (24) can be obtained as $(a, b) \equiv (2, 6)$ and $(9, 5) \mod 11$. Therefore, the matrices

$$H \stackrel{\text{def}}{=} \begin{bmatrix} 2 & 6 & 6 & 6 & 6 \\ 6 & 2 & 6 & 6 & 6 \\ 6 & 6 & 2 & 6 & 6 \\ 6 & 6 & 6 & 2 & 6 \\ 6 & 6 & 6 & 6 & 2 \end{bmatrix} \tag{33}$$

and

$$H' \stackrel{\text{def}}{=} \begin{bmatrix} 9 & 5 & 5 & 5 & 5 \\ 5 & 9 & 5 & 5 & 5 \\ 5 & 5 & 9 & 5 & 5 \\ 5 & 5 & 5 & 9 & 5 \\ 5 & 5 & 5 & 5 & 9 \end{bmatrix} \tag{34}$$

can be generated. It is easily confirmed that $HH^T \equiv 5I \mod 11$ and $H'H'^T \equiv 5I \mod 11$ are satisfied.

Note that Theorem 2 also holds for cyclic H-type matrices. It implies that the order of cyclic H-type matrices should be also a quadratic residue of the given p.

5. Orders of H-type Matrices

5.1 Orders of H-type Matrices of Odd Order

As shown in Theorem 2, the orders of cyclic H-type matrices on $GF(p)$ are limited to quadratic residues of the given prime p. In this section, we show that the orders of any H-type matrices of odd order are limited to quadratic residues of p.

First, we introduce the following lemma on the determinant of an H-type matrix.

Lemma 1: For any odd prime p and any positive integer n satisfying $n \geq 2$, any H-type matrices of order n on $GF(p)$ satisfy

$$(\det H)^2 \equiv n^n \mod p. \tag{35}$$

Proof. From the definition, any H-type matrices of order n satisfies Eq.(1). Consider the determinants of the both sides of Eq.(1). For the $l.h.s.$ of Eq.(1), it can be shown that

$$\det HH^T = \det H \cdot \det H^T = (\det H)^2. \tag{36}$$

On the other hand, for the $r.h.s.$ of Eq.(1), we obtain

$$\det(nI) = n^n. \tag{37}$$

From these equations, the lemma can be proved. □

Here we have the following theorem on the order of an H-type matrix of odd order.

Theorem 4: Consider an odd prime p and a positive odd integer n satisfying $n \geq 2$ and $n \not\equiv 0 \mod p$. Then, there exists an H-type matrix of order n on $GF(p)$ if and only if n is a quadratic residue of p.

Proof. First, we show that if n is a quadratic residue of p, then an H-type matrix exists. This is trivial according to Theorem 2 if we consider a cyclic H-type matrix of order n.

Next, we prove that if an H-type matrix of order n exists, n is a quadratic residue of p, that is, $\left(\frac{n}{p}\right) = 1$. We consider the proof by contraposition. So we show that any H-type matrices of order n do not exist if $\left(\frac{n}{p}\right) \neq 1$. From the assumption, $\left(\frac{n}{p}\right) \neq 0$. Therefore, we can only consider the case of $\left(\frac{n}{p}\right) = -1$. Since n is an odd integer, we have

$$\left(\frac{n^n}{p}\right) = \left(\frac{n}{p}\right)^n = \left(\frac{n}{p}\right) = -1, \tag{38}$$

which implies that n^n is a quadratic non-residue of p. On the other hand, from Lemma 1, n^n is congruent to $(\det H)^2$ modulo p. This is contradiction since $\left(\frac{n^n}{p}\right) = -1$. Therefore, we cannot consider such $\det H$ satisfying Lemma 1, which implies that there are no H-type matrices H satisfying Lemma 1.

Now we proved the theorem. □

5.2 Extension of the Orders of H-type Matrices

It is possible to extend the orders of H-type matrices by some simple calculations. In this section, we introduce some of them.

5.2.1 Extension by Kronecker Products

As discussed in [5]–[7], it is possible to extend the order of an H-type matrix by Kronecker products of H-type matrices. Here is an example.

Example 6: Consider two H-type matrices of order 2 and 3 on $GF(13)$ such that

$$H' \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 \\ 1 & 12 \end{bmatrix}, \qquad H'' \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 4 & 8 \\ 1 & 8 & 4 \end{bmatrix}.$$

From these matrices, we can generate an H-type matrix of order 6 on $GF(13)$ as

$$\begin{aligned} H &= H' \otimes H'' \\ &\equiv \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 4 & 8 & 1 & 4 & 8 \\ 1 & 8 & 4 & 1 & 8 & 4 \\ 1 & 1 & 1 & 12 & 12 & 12 \\ 1 & 4 & 8 & 12 & 9 & 5 \\ 1 & 8 & 4 & 12 & 5 & 9 \end{bmatrix} \mod 13, \end{aligned} \tag{39}$$

which satisfies $HH^T \equiv 6I \mod 13$.

5.2.2 Block Diagonalization by Two H-type Matrices

It is possible to extend the order of H-type matrices on $GF(p)$ as follows:

$$H_n = \begin{bmatrix} \sqrt{\frac{n}{k}} H_k & O \\ O & \sqrt{\frac{n}{m}} H_m \end{bmatrix}, \tag{40}$$

where H_n is an H-type matrix of order n and $n = m + k$. In this case, $\left(\frac{k}{p}\right) = \left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) = 1$ have to be satisfied. Note that the fraction such as $\frac{n}{k}$ has an integer value on $GF(p)$. If its value is a quadratic residue of p, $\sqrt{\frac{n}{k}}$ also has an integer value on $GF(p)$.

Example 7: Consider three quadratic residues $k = 2, m = 5$ and $n = 7$ on $GF(31)$ satisfying $n = k + m$. Based on a standard-form cyclic H-type matrices of order 2 and 5 on $GF(31)$:

$$H_2 \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 \\ 1 & 30 \end{bmatrix} \tag{41}$$

and

$$H_5 \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 9 & 9 & 9 \\ 1 & 9 & 3 & 9 & 9 \\ 1 & 9 & 9 & 3 & 9 \\ 1 & 9 & 9 & 9 & 3 \end{bmatrix}, \tag{42}$$

we can generate an H-type matrix of order 7 on $GF(31)$ as

$$H_7 = \begin{bmatrix} \sqrt{\frac{7}{2}}H_2 & O \\ O & \sqrt{\frac{7}{5}}H_5 \end{bmatrix} \equiv \begin{bmatrix} 9H_2 & O \\ O & 12H_5 \end{bmatrix}$$
$$= \begin{bmatrix} 9 & 9 & 0 & 0 & 0 & 0 & 0 \\ 9 & 22 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 12 & 12 & 12 & 12 & 12 \\ 0 & 0 & 12 & 5 & 15 & 15 & 15 \\ 0 & 0 & 12 & 15 & 5 & 15 & 15 \\ 0 & 0 & 12 & 15 & 15 & 5 & 15 \\ 0 & 0 & 12 & 15 & 15 & 15 & 5 \end{bmatrix} \mod 31, \tag{43}$$

which satisfies $H_7 H_7^T \equiv 7I \mod 31$.

As mentioned in Remark 1, an identity matrix can be regarded as a special case of an H-type matrix. Therefore, by employing $H_k \stackrel{\text{def}}{=} \sqrt{k} I_k$ in Eq.(40), it is also possible to extend the order of an H-type matrix by employing an identity matrix such as

$$H_n = \begin{bmatrix} \sqrt{n} I_{n-m} & O \\ O & \sqrt{\frac{n}{m}} H_m \end{bmatrix}, \tag{44}$$

where H_n is an H-type matrix of order n and I_{n-m} is the identity matrix of order $k = (n-m)$. In this case, $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) = 1$ have to be satisfied.

Example 8: Consider two quadratic residues $m = 3$ and $n = 5$ on $GF(11)$. Based on a standard-form cyclic H-type matrix of order $m = 3$ on $GF(11)$:

$$H_3 \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 8 \\ 1 & 8 & 2 \end{bmatrix}, \tag{45}$$

we can generate an H-type matrix of order 5 on $GF(11)$ as

$$H_5 = \begin{bmatrix} \sqrt{5} I_{5-3} & O \\ 0 & \sqrt{\frac{5}{3}} H_3 \end{bmatrix} \equiv \begin{bmatrix} 4I_2 & O \\ O & 3H_3 \end{bmatrix}$$
$$\equiv \begin{bmatrix} 4 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 3 & 3 & 3 \\ 0 & 0 & 3 & 6 & 2 \\ 0 & 0 & 3 & 2 & 6 \end{bmatrix} \mod 11, \tag{46}$$

which satisfies $H_5 H_5^T = 5I \mod 11$.

Remark 2: In the previous studies[5]–[7], H-type matrices are defined as a square matrix with 'non-zero' entries, where any two rows are mutually orthogonal. This is partly because the generation methods of H-type matrices proposed in these studies are based on cyclic groups on $GF(p)$.

However, H-type matrices with zero elements can be obtained such as H_7 in Example 7 and H_5 in Example 8. Another example can be obtained according to Example 4. In Example 4, the solutions $(a, b) = (0, 7)$ and $(5, 9)$ are obtained. If we take $(a, b) = (0, 7)$ instead of $(5, 9)$, we have another H-type matrix on $GF(11)$:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 7 & 7 & 7 \\ 1 & 7 & 0 & 7 & 7 \\ 1 & 7 & 7 & 0 & 7 \\ 1 & 7 & 7 & 7 & 0 \end{bmatrix}, \tag{47}$$

which includes zero elements.

Zero elements can be employed in standard-form cyclic H-type matrices since there is no need to consider any cyclic groups in order to generate these matrices. On the other hand, there are no non-standard-form cyclic H-type matrices with zero entries because it is impossible to obtain any pairs of solutions where $a \equiv 0$ or $b \equiv 0 \mod p$ are satisfied under the two conditions (23) and (24) as mentioned in the proof of Theorem 3.

Remark 3: There are only three different elements including '1' in any standard-form cyclic H-type matrices. Also, there are only two different elements in any non-standard-form cyclic H-type matrices.

As shown in the above examples, it is possible to increase the number of different elements if the order of the matrix is extended by any of the above methods. Specifically, the matrices H, H_7 and H_5 in Examples 6, 7 and 8 have six, six and five elements including 0 and 1, respectively.

Note that given a prime p, even the order of the extended H-type matrices in Examples 7 and 8 are quadratic residues of p. It implies that order of the H-type matrices extended from any H-type matrices of odd orders on $GF(p)$ by each of the above methods is a product of arbitrary quadratic residues of p.

6. Some Miscellaneous Remarks

6.1 H-type Matrices of Even Order

As described in Theorem 4, the order of an H-type matrix of odd order is limited to a quadratic residue of the given prime

p. Here we discuss H-type matrices of even order.

Even in this case, it is possible to extend the order of H-type matrices by applying Kronecker products according to the way described in Sect. 5.2.1. We have the following properties on H-type matrices of even order.

Corollary 1: Suppose that for any odd prime p, an even integer n satisfies $n \not\equiv 0 \mod p$ and $n = 2^m q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$, where $q_1, q_2, \ldots, q_k$ are different odd primes and $k, m, \alpha_1, \alpha_2, \ldots, \alpha_k$ are positive integers. Then an H-type matrix of order n on $GF(p)$ exists if $\left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right) = \cdots = \left(\frac{q_k}{p}\right) = 1$.

Proof. As described in Theorem 4, an H-type matrix of odd order exists for each of the different odd quadratic residues $q_1, q_2, \ldots, q_k$ under the given prime p. The order of an extended H-type matrix by Kronecker products of such matrices of odd order is a product of the corresponding quadratic residues of p. In addition, it is possible to extend the order of any H-type matrices by 2^m times by applying Kronecker product m times. □

Note that the inverse of Corollary 1 does not hold in general. In other words, an H-type matrix on $GF(p)$ possibly has the order including a quadratic non-residue of p in its prime factors. Here is an example.

Example 9: For a quadratic non-residue 6 of $p = 7$, there is an H-type matrix of order 6 on $GF(7)$:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 2 & 4 & 5 \\ 1 & 1 & 4 & 2 & 5 & 1 \\ 1 & 2 & 2 & 6 & 4 & 6 \\ 1 & 4 & 5 & 4 & 4 & 3 \\ 1 & 5 & 1 & 6 & 3 & 5 \end{bmatrix}, \tag{48}$$

which satisfies $HH^T \equiv 6I \mod 7$. Note that the order 6 includes another quadratic non-residue 3 of $p = 7$ in its prime factor.

6.2 H-type Matrices on Residue Class Ring

In the previous studies[5]–[7], we are only concerned with H-type matrices on 'finite fields.' In this section, we discuss whether H-type matrices can be obtained not only on finite fields, but also on residue class rings based on non-primes.

Consider the following example for standard-form cyclic H-type matrices.

Example 10: Consider $m = 6$ as a non-prime. Assume that $m = 6$ and $n = 4$. In other words, we consider whether we can generate any cyclic H-type matrices of order 4 on $\mathbb{Z}_6$. In this case, from Eqs.(8) and (9), the set of two equations can be expressed as

$$1 - 2b - 3b^2 \equiv 0 \mod 6 \tag{49}$$

and

$$a \equiv -1 - 2b \mod 6. \tag{50}$$

From Eq.(49), we have

$$3b^2 + 4b + 1 = (3b+1)(b+1) \equiv 0 \mod 6. \tag{51}$$

However, the element '3' does not have any multiplicative inverse on $\mathbb{Z}_6$. It means that we have only one integer solution for b on $\mathbb{Z}_6$ in this case, that is, $b \equiv 5 \mod 6$. When $b \equiv 5 \mod 6$, the solution for a can be obtained as $a \equiv 1 \mod 6$ from Eq.(50). As a result, a standard-form cyclic H-type matrix can be obtained as:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 5 & 5 \\ 1 & 5 & 1 & 5 \\ 1 & 5 & 5 & 1 \end{bmatrix}, \tag{52}$$

which satisfies $HH^T \equiv 4I \mod 6$. In this case, we have only one solution on $\mathbb{Z}_6$.

Next, let us consider examples for non-standard-form cyclic H-type matrices.

Example 11: Consider the same case as the previous example, that is, the case where $m = 6$ and $n = 4$. For Eqs.(23) and (24), we have a couple of solutions $(a, b) \equiv (5, 1), (1, 5) \mod 6$ on $\mathbb{Z}_6$. As a result, we have two different cyclic H-type matrices on residue class ring $\mathbb{Z}_6$, that is,

$$H = \begin{bmatrix} 1 & 5 & 5 & 5 \\ 5 & 1 & 5 & 5 \\ 5 & 5 & 1 & 5 \\ 5 & 5 & 5 & 1 \end{bmatrix} \tag{53}$$

and

$$H' = \begin{bmatrix} 5 & 1 & 1 & 1 \\ 1 & 5 & 1 & 1 \\ 1 & 1 & 5 & 1 \\ 1 & 1 & 1 & 5 \end{bmatrix}, \tag{54}$$

which satisfies $HH^T \equiv 4I \mod 6$ as well as $H'H'^T \equiv 4I \mod 6$. Note that, in this case, the relation $H' \equiv 5 \cdot H \mod 6$ is satisfied.

In general, Eq.(24) has a solution $b \equiv \pm 1 \mod m$ on $\mathbb{Z}_m$ at least if $n = 4$. In this case, a can also be obtained on $\mathbb{Z}_m$ from Eq.(23). Therefore, cyclic H-type matrices of order 4 on $\mathbb{Z}_m$ can be obtained.

Here is another example for $n \neq 4$.

Example 12: Consider the case where $m = 8$ and $n = 6$, that is, cyclic H-type matrices of order 6 on $\mathbb{Z}_8$. In this case, from Eqs.(23) and (24), the set of two equations can be expressed as

$$\begin{cases} a \equiv -2b \mod 8, \\ b^2 \equiv \dfrac{2}{3} \mod 8. \end{cases} \tag{55}$$

Note that there are not any integer solutions for b on $\mathbb{Z}_8$.

Therefore, we can conclude that there are no cyclic H-type matrices of order 6 on $\mathbb{Z}_8$.

From these examples, it is shown that cyclic H-type matrices cannot be always generated on residue class rings.

6.3 Generation of Involutory Matrices

Involutory matrix A is defined as a square matrix that is identical to its own inverse A^{-1}. Therefore, an involutory matrix A satisfies $A^2 = I$. For example, an identity matrix I or any permutation matrices are involutory matrices.

It is easy to show that an involutory matrix can be generated by a standard-form or a non-standard-form cyclic H-type matrix.

Corollary 2: Given an H-type matrix H given in the form of Eqs.(7) or (22), the matrix $M \overset{\text{def}}{=} \dfrac{1}{(a-b)} H$ is an involutory matrix.

Proof. Note that a cyclic H-type matrix is symmetric. According to Theorem 2, it is trivial that $HH^T = H^2 \equiv nI \equiv (a-b)^2 I \mod p$. □

Example 13:

$$H \overset{\text{def}}{=} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 8 & 4 \\ 1 & 4 & 8 \end{bmatrix} \tag{56}$$

is a standard-form cyclic H-type matrix of order 3 on $GF(13)$. Note that $(a, b) = (8, 4)$. Then,

$$\begin{aligned} M &= \frac{1}{a-b} \cdot H = \frac{1}{4} \cdot H \\ &\equiv 10 \cdot H \equiv \begin{bmatrix} 10 & 10 & 10 \\ 10 & 2 & 1 \\ 10 & 1 & 2 \end{bmatrix} \mod 13 \end{aligned} \tag{57}$$

is an involutory matrix, which satisfies $M^2 \equiv I \mod 13$.

In general, any block-diagonal matrices obtained from involutory matrices are also involutory matrices. Here is an example.

Example 14: Based on the involutory matrix M obtained as Eq.(57) in Example 13, a block-diagonal matrix:

$$M' = \begin{bmatrix} 10 & 10 & 10 & & & \\ 10 & 2 & 1 & & O & \\ 10 & 1 & 2 & & & \\ & & & 10 & 10 & 10 \\ & O & & 10 & 2 & 1 \\ & & & 10 & 1 & 2 \end{bmatrix} \tag{58}$$

can be constructed, which satisfies $M'^2 = I \mod 13$.

Even if the matrix H is not a cyclic H-type matrix, it is possible to generate an involutory matrix.

Corollary 3: Given a symmetric H-type matrix H of odd order, the matrix $M \overset{\text{def}}{=} \dfrac{1}{\sqrt{n}} H$ is an involutory matrix.

Proof. If an H-type matrix H of order n on $GF(p)$ is symmetric, $HH^T = H^2 \equiv nI \mod p$. It is always possible to generate $M \overset{\text{def}}{=} \dfrac{1}{\sqrt{n}} H$, which obviously satisfies $M^2 \equiv I \mod p$ since the order n of H is a quadratic residue of p according to Theorem 4. □

Example 15: The matrix H given as Eq.(5) in Example 2 is not cyclic, but a symmetric H-type matrix of order 5 on $GF(11)$. Note that the order 5 of H is a quadratic residue of $p = 11$. Then the matrix

$$\begin{aligned} M &= \frac{1}{\sqrt{n}} \cdot H \\ &= \frac{1}{\sqrt{5}} \cdot H \\ &\equiv \frac{1}{4} \cdot H \\ &\equiv 3 \cdot H \equiv \begin{bmatrix} 3 & 3 & 3 & 3 & 3 \\ 3 & 6 & 3 & 2 & 8 \\ 3 & 3 & 10 & 1 & 5 \\ 3 & 2 & 1 & 7 & 9 \\ 3 & 8 & 5 & 9 & 8 \end{bmatrix} \mod 11 \end{aligned} \tag{59}$$

is an involutory matrix, which satisfies $M^2 \equiv I \mod 11$.

6.4 The Number of H-type Matrices on Finite Fields

On H-type matrices on finite fields, one question may naturally arise: How many H-type matrices exist for the given prime p and the order n? Table 1 shows the number of H-type matrices for some combinations of the parameters p and n, which has been counted by computer searches. Duplicates due to swapping of rows and columns are not counted in Table 1.

Table 1 The Number of H-type matrices for some given p and n.

Prime p	Order n	Number of H-type matrices
3	4	12
11	3	86
13	3	138

This table implies that there exist quite less number of H-type matrices compared to all possible square matrices of the given order on finite fields. However, it can be seen that there are many more options for H-type matrices on finite fields in comparison with the case of the conventional binary Hadamard matrices. Note that for standard-form or non-standard-form cyclic H-type matrices, there are only two options at most for the given prime p and the order n. In addition, it is still unknown how to generate many of these H-type matrices except for the cyclic H-type matrices, the identity matrices and the obvious cases shown in Example 1, which is essentially identical to binary Hadamard matrices. It is one of the very important open problems to find the way to generate such H-type matrices on finite fields.

7. Summary

In this paper, we introduce some new varieties of H-type matrices on finite fields and its properties. Specifically, the new results shown in this paper are as follows.

- Some new kinds of H-type matrices can be found by brute-force searches.
- We define cyclic H-type matrices, give ways to generate them, and show that their orders are limited to quadratic residues of the given prime.
- It is shown that the order of an arbitrary H-type matrix of odd order is limited to a quadratic residue of the given prime.
- Some methods to extend the orders of H-type matrices are given.
- It is shown that we can generate an H-type matrix of even order by extending H-type matrices of odd order. However, the orders of H-type matrices of even order are not always quadratic residues of the given prime.
- It is shown that an H-type matrix based on a non-prime on residue class ring cannot be always generated.
- It is shown that an involutory matrix can be generated by using a cyclic H-type matrix or a symmetric H-type matrix of odd order.
- We count all possible H-type matrices for some combinations of the given prime p and the order n through computer searches.

In our brute-force searches, we have found many examples of H-type matrices other than cyclic H-type matrices or symmetric H-type matrices. It is interesting to give the methods to generate such "irregular" H-type matrices in our future study. The necessary and sufficient conditions for the existence of H-type matrices of even order is still unknown. This is another interesting topic to tackle in the future.

Acknowledgments

The authors sincerely thank to Prof. Yasuyuki Nogami of Okayama University, Japan and Prof. Satoshi Uehara of the University of Kitakyushu, Japan for their fruitful discussions.

References

[1] J. Hadamard, "Résolution d'une question relative aux determinants," Bulletin des Sciences Math'ematiques, vol.17, no.2, pp.240–246, Sept. 1893.
[2] A. Hedayat and W.D. Wallis, "Hadamard matrices and their applications," Annals of Statistics, vol.6, no.6, pp.1184–1238, Nov. 1978.
[3] K.J. Horadam, Hadamard Matrices and Their Applications, Princeton University Press, Princeton, NJ, USA, Dec. 2006.
[4] N. Suehiro and M. Hatori, "N-shift cross-orthogonal sequences," IEEE Trans. Inf. Theory, vol.34, no.1, pp.143–146, Jan. 1988.
[5] T. Kojima, "Hadamard-type matrices on finite fields and their applications," IEICE Technical Report, vol.117, no.394, pp.43–48, Jan. 2018.
[6] T. Kojima, "Hadamard-type Matrices on Finite Fields and Complete Complementary Codes," IEICE Trans. Fundamentals, vol.E102-A, no.12, pp.1651–1658, Dec. 2019.
[7] T. Kojima, "Hadamard-type Matrices on Finite Fields and Some Open Problems," IEICE Technical Report, vol.119, no.198, pp.29–34, Sept. 2019.
[8] I. Kodama and T. Kojima, "Cyclic Hadamard-type Matrices on Finite Fields and Their Properties (in Japanese)," IEICE Technical Report, vol.122, no.355, pp.211–216, Jan. 2023.
[9] T. Kojima and I. Kodama, "Some Remarks on Hadamard-type Matrices over Residue Class Rings or Finite Fields," IEICE Technical Report, vol.123, no.14, pp.67–72, May 2023.
[10] I. Kodama and T. Kojima, "On Hadamard-type Matrices of Odd Order over Finite Fields (in Japanese)," IEICE Technical Report, vol.123, no.338, pp.57–61, Jan. 2024.

Iori Kodama graduated from the Department of Computer Science, National Institute of Technology, Tokyo College, Japan. Since 2023, he has been a student in the Advanced Course of Mechanical and Computer Systems Engineering, National Institute of Technology, Tokyo College, Japan. He has studied computer sciences and discrete mathematics especially on algebraic systems.

Tetsuya Kojima received the B.E., M.E., and D.E. degrees in information engineering from Hokkaido University, Sapporo, Japan, in 1992, 1994 and 1997, respectively. From 1997 to 2001, he was with the Graduate School of Information Systems, the University of Electro-Communications, Tokyo, Japan as a research associate. In 2001, he joined the Department of Computer Science, National Institute of Technology, Tokyo College, Tokyo, Japan, as research associate, and is currently a professor. From April, 2010 to March, 2011, he was a visiting researcher at the University of Melbourne, Australia. Prof. Kojima has served as an organizing committee member of many international and domestic conferences including a general co-chair of the Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA '17) held in Sapporo, Japan and the general chair of the 45th Symposium on Information Theory and Its Applications (SITA 2022) held in Noboribetsu, Hokkaido, Japan. He has also served as a chair in academic societies, which includes IEICE Tokyo Section, IEICE Technical Committee on Information Theory as well as IEICE Sub-society of Information Theory and Its Applications. His research interests include the sequence design and its applications to communication systems and information hiding as well as other applications of information theory. He is a member of IEEE.