

# New Constructions of Quaternary Hadamard Matrices <sup>1</sup>

\*Ji-Woong Jang<sup>O</sup>, \*Sang-Hyo Kim, \*Jong-Seon No, and +Habong Chung  
 \*Seoul National University, +Hongik University  
 {stasera,kimsh}@ccl.snu.ac.kr, jsno@snu.ac.kr, habchung@hongik.ac.kr

## Abstract

In this paper, we propose two new construction methods for quaternary Hadamard matrices. By the first method, which is applicable for any positive integer  $n$ , we are able to construct a quaternary Hadamard matrix of order  $2^n$  from a binary sequence with ideal autocorrelation. The second method also gives us a quaternary Hadamard matrix of order  $2^n$  from a binary extended sequence of period  $2^n - 1$ , where  $n$  is a composite number.

## I. Introduction

A generalized Hadamard matrix  $\mathcal{H}$  of order  $N$  is an  $N \times N$  matrix satisfying  $\mathcal{H}\mathcal{H}^\dagger = NI_N$ , where  $\dagger$  denotes the conjugate transpose and  $I_N$  is the identity matrix of order  $N$  [3]. In other words, any two distinct rows of  $\mathcal{H}$  are orthogonal. For this reason, Hadamard matrices have been studied for the applications in many areas such as wireless communication systems, coding theory, and signal design[1]. Hadamard matrices have strong ties to sequences. Matsufuji and Suehiro proposed the complex Hadamard matrices related to bent sequences[7]. Popovic, Suehiro, and Fan[10] proposed orthogonal sets of quaternary sequences by using quadriphase sequence family  $\mathcal{A}$  by Boztas, Hammons, and Kumar[2].

In this paper, we propose two new construction methods for quaternary Hadamard matrices. By the first method, which is applicable for any positive integer  $n$ , we are able to construct a quaternary Hadamard matrix of order  $2^n$  from a binary sequence with ideal autocorrelation. The second method also gives us a quaternary Hadamard matrix of order  $2^n$  from a binary extended sequence of period  $2^n - 1$ , where  $n$  is a composite number.

Let  $F_{2^n}$  be the finite field with  $2^n$  elements. Let  $F_{2^n}^* = F_{2^n} \setminus \{0\}$  and  $s(x)$  be a mapping from  $F_{2^n}$  to  $F_2$  or  $Z_4$ . If we restrict the mapping  $s(x)$  to  $F_{2^n}^*$  and replace  $x$  by  $\alpha^t$ , where  $\alpha$  is a primitive element in  $F_{2^n}$ , then we can obtain a sequence  $s(\alpha^t)$ ,  $0 \leq t \leq 2^n - 2$ , of period  $2^n - 1$ . Hence, for convenience, we will use the expression ‘a binary or quaternary sequence  $s(\alpha^t)$  of period  $2^n - 1$ ’ interchangeably with ‘a mapping  $s(x)$  from  $F_{2^n}$  to  $F_2$  or  $Z_4$ ’.

It is not difficult to see that a variable  $v$  over  $Z_4$  can be expressed using two binary variables  $v_1$  and  $v_2$

as  $v = v_1 + 2v_2$  where addition is modulo 4. Let us define two maps  $\phi$  and  $\psi$  as  $\phi(v) = v_1$ ,  $\psi(v) = v_2$ .

It can be shown that  $\phi(v - w)$  and  $\psi(v - w)$  of the difference  $v - w$  are expressed as

$$\begin{aligned}\phi(v - w) &= v_1 + w_1 \\ \psi(v - w) &= v_1w_1 + w_1 + w_2 + v_2.\end{aligned}\quad (1)$$

## II. Preliminaries

**Lemma 1** For a positive integer  $n$ , let  $g(t)$  be a binary sequence of period  $2^n - 1$  with ideal autocorrelation. Then for any  $z$ ,  $1 \leq z \leq 2^n - 2$ , the following sequence  $q_z(t)$  is balanced over  $Z_4$ .

$$q_z(t) = g(t) + 2g(t + z).$$

□

Using the above lemma, we get the quaternary Hadamard matrices as in the following theorem.

**Theorem 1** Let  $n$  be an integer and  $g(t)$ ,  $0 \leq t \leq 2^n - 2$ , be a sequence of period  $2^n - 1$  with ideal autocorrelation. Then the following matrix  $\mathcal{H}_Q$  is the  $2^n \times 2^n$  quaternary Hadamard matrix.

$$\mathcal{H}_Q = (h_{ij}), \quad 0 \leq i, j \leq 2^n - 1$$

where  $h_{ij}$  is given as

$$h_{ij} = \begin{cases} 1, & \text{for } i = 0 \text{ or } j = 0 \\ w_4^{2g(j-1)}, & \text{for } i = 1 \text{ and } 1 \leq j \leq 2^n - 1 \\ w_4^{g_{i-1}(j-1)}, & \text{otherwise.} \end{cases}$$

□

<sup>1</sup>This work was supported in part by BK21 and ITRC program.

Using extended sequences with ideal autocorrelation by No, Yang, Chung, and Song[9], we can construct the quaternary Hadamard matrix as in the following theorem.

**Theorem 2** Let  $n$  and  $m$  be integers such that  $m|n$ , and  $r$  is an integer such that  $1 \leq r \leq 2^m - 2$  and  $\gcd(r, 2^m - 1) = 1$ . Let  $T = \frac{2^n - 1}{2^m - 1}$  and  $f(y)$  be the sequence from  $F_{2^m}$  to  $F_2$  which has balance and difference-balance property. Let  $s_i(\alpha^t)$  be the sequence in the set  $\mathcal{S}$  defined as follows :

$$\mathcal{S} = \{s_i(\alpha^t) \mid 0 \leq i \leq 2^m - 2, 0 \leq t \leq 2^n - 2\}$$

where  $s_i(\alpha^t)$  is defined as

$$\begin{aligned} s_0(\alpha^t) &= 2f([\text{tr}_m^n(\alpha^t)]^r) \\ s_i(\alpha^t) &= f([\text{tr}_m^n(\alpha^t)]^r + 2f([\text{tr}_m^n(\beta^i \alpha^t)]^r), \\ &1 \leq i \leq 2^n - 2 \end{aligned}$$

where  $\beta = \alpha^T$  is a primitive element in  $F_{2^m}$ .

Then we can construct the  $2^n \times 2^n$  quaternary Hadamard matrix  $\mathcal{H}_L$  as follows:

$$\mathcal{H}_L = (h_{ij})$$

where  $h_{ij}$  is given as

$$h_{ij} = \begin{cases} 1, & \text{if } i = 0 \text{ or } j = 0 \\ w_4^{s_{\lfloor (i-1)/T \rfloor}(j-1+it)}, & \text{otherwise} \end{cases}$$

where  $\lfloor x \rfloor$  denotes the greatest integer not exceeding  $x$  and  $i_T = (i - 1) \bmod T$ . □

**Lemma 2** Let  $m$ ,  $e$ , and  $n$  be positive integers such that  $n = em$ . Let  $q = 2^m$  and  $A = \{1, \alpha, \dots, \alpha^{T-1}\}$ , where  $\alpha$  is a primitive element in  $F_{2^n}$  and  $T = \frac{q^e - 1}{q - 1}$ . Let  $v(x)$  be a function from  $F_{q^e}$  onto  $F_q$  with balance and difference-balance property. Further assume that  $v(x)$  satisfies  $v(yx) = yv(x)$  for any  $y \in F_q$  and  $x \in F_{q^e}$ . For a given  $\delta \in F_{q^e} \setminus F_q$ , let  $M_\delta(a, b)$  be the number of  $x_2 \in A$  satisfying

$$\begin{aligned} v(\delta x_2) &= a \\ v(x_2) &= b, \quad a, b \in F_q. \end{aligned} \quad (2)$$

Then, we have

$$\begin{aligned} M_\delta(0, 0) &= \frac{q^{e-2} - 1}{q - 1} = \frac{2^{n-2m} - 1}{2^m - 1} \\ \sum_{c \in F_q^*} M_\delta(c, 0) &= \sum_{c \in F_q^*} M_\delta(0, c) = q^{e-2} = 2^{n-2m} \\ \sum_{d \in F_q^*} M_\delta(cd, d) &= q^{e-2} = 2^{n-2m}, \quad \text{for any } c \in F_q^*. \end{aligned}$$

□

**Lemma 3** Let  $s(x)$  be a function from any domain  $B$  to  $Z_4$ , where  $s(0) = 0$ . Define two Boolean constituent functions of  $s(x)$  and their modulo-2 sum as

$$\begin{aligned} \phi_s(x) &= \phi(s(x)), \\ \psi_s(x) &= \psi(s(x)), \\ \mu_s(x) &= \phi_s(x) + \psi_s(x). \end{aligned} \quad (3)$$

Let  $N_f(c)$  denote the number of occurrences of  $f(x) = c$  as  $x$  varies over  $B$ . Then, we have

$$\sum_{x \in B} \omega_4^{s(x)} = (N_{\psi_s}(0) - N_{\mu_s}(1)) + j(N_{\mu_s}(1) - N_{\psi_s}(1)).$$

□

Now we are ready to prove Theorem 2.

**Proof of Theorem 2 :** Let  $v_i$  be the  $i$ th row of  $\mathcal{H}_L$ ,  $0 \leq i \leq 2^n - 1$ . We have to show that  $v_i v_k^\dagger = 0$  for all  $i \neq k$ . The case when  $i = 0$ , it is manifest that  $v_0 v_k^\dagger = 0$  for all  $k \neq 0$ .

Now, for any nonzero  $i$  and  $k$ ,  $i \neq k$ ,  $v_i v_k^\dagger$  can be expressed as

$$v_i v_k^\dagger = 1 + \sum_{x \in F_{2^m}^*} w_4^{s_{i'}(\delta x) - s_{k'}(x)}$$

where  $\delta = \alpha^{iT - kT}$ ,  $i' = \lfloor (i - 1)/T \rfloor$ , and  $k' = \lfloor (k - 1)/T \rfloor$ . For  $\delta = \alpha^{iT - kT}$ , showing that  $v_i v_k^\dagger = 0$  is equivalent to showing that the crosscorrelation  $R_{i', k'}(\delta)$  between  $s_{i'}(x)$  and  $s_{k'}(x)$  is  $-1$ .

For  $a, b \in F_{2^m} \setminus F_2$ , let  $d(x, \eta) = \{f(\eta x) + 2f(a\eta x)\} - \{f(x) + 2f(bx)\}$ . Define  $S_{\psi_d}$  and  $S_{\mu_d}$  as

$$S_{\psi_d} = \sum_{x \in F_{2^m}^*} \sum_{\eta \in F_{2^m}^*} (-1)^{\psi(d(x, \eta))}$$

$$S_{\mu_d} = \sum_{x \in F_{2^m}^*} \sum_{\eta \in F_{2^m}^*} (-1)^{\mu(d(x, \eta))}.$$

Then from (1) and (3),  $S_{\psi_d}$  and  $S_{\mu_d}$  can be expressed as

$$S_{\psi_d} = \sum_{x \in F_{2^m}^*} \sum_{\eta \in F_{2^m}^*} (-1)^{f(\eta x)f(x)+f(x)+f(bx)+f(a\eta x)} \quad (4)$$

$$S_{\mu_d} = \sum_{x \in F_{2^m}^*} \sum_{\eta \in F_{2^m}^*} (-1)^{f(\eta x)f(x)+f(\eta x)+f(bx)+f(a\eta x)}. \quad (5)$$

Now, let  $I_1(x)$  and  $I_2(x)$  be the inner summation in (4),

$$\sum_{\eta \in F_{2^m}^*} (-1)^{f(\eta x)f(x)+f(x)+f(bx)+f(a\eta x)}$$

for the cases when  $f(x) = 0$  and  $f(x) = 1$ , respectively, i.e.,

$$I_1(x) = \sum_{\eta \in F_{2^m}^*} (-1)^{f(bx)+f(a\eta x)}$$

$$I_2(x) = \sum_{\eta \in F_{2^m}^*} (-1)^{f(\eta x)+1+f(bx)+f(a\eta x)}.$$

Since  $f(x)$  is balanced and difference balanced,  $S_{\psi_d}$  can be expressed as

$$\begin{aligned} S_{\psi_d} &= \sum_{x \in \{x|f(x)=0, x \in F_{2^m}^*\}} I_1(x) \\ &+ \sum_{x \in \{x|f(x)=1, x \in F_{2^m}^*\}} I_2(x) \\ &= \sum_{x \in \{x|f(x)=1, x \in F_{2^m}^*\}} (-1)^{f(bx)} \\ &- \sum_{x \in \{x|f(x)=0, x \in F_{2^m}^*\}} (-1)^{f(bx)}. \end{aligned}$$

Finally, from the difference-balance property of  $f(x)$ , we have

$$S_{\psi_d} = 1.$$

By the similar way, we get  $S_{\mu_d} = 1$ .

Now consider two sequences in  $\mathcal{S}$  given by

$$\begin{aligned} s_{i'}(x) &= f([\text{tr}_m^n(x)]^r) + 2f(a^r[\text{tr}_m^n(x)]^r) \\ s_{k'}(x) &= f([\text{tr}_m^n(x)]^r) + 2f(b^r[\text{tr}_m^n(x)]^r) \end{aligned}$$

where  $a = \beta^{i'}$  and  $b = \beta^{k'}$  for nonzero  $i'$  and  $k'$ . Then  $R_{i',k'}(\delta)$  is given by

$$\begin{aligned} R_{i',k'}(\delta) &= \sum_{x \in F_{2^n}^*} \omega_4^{s_{i'}(\delta x) - s_{k'}(x)} \\ &= \sum_{x_2 \in A} \sum_{x_1 \in F_{2^m}^*} \omega_4^{f(x_1^r[\text{tr}_m^n(\delta x_2)]^r)} \\ &\quad \cdot \omega_4^{2f(x_1^r a^r[\text{tr}_m^n(\delta x_2)]^r)} \\ &\quad \cdot \omega_4^{-f(x_1^r[\text{tr}_m^n(x_2)]^r)} \\ &\quad \cdot \omega_4^{2f(x_1^r b^r[\text{tr}_m^n(x_2)]^r)}. \end{aligned}$$

**Case 1)**  $i' \neq k'$  for nonzero  $i'$  and  $k'$  :

For  $\delta \notin F_{2^m}$ , with the replacement of  $\text{tr}_m^n(\delta x_2)$  by  $cd$  and  $\text{tr}_m^n(x_2)$  by  $d$  and also from Lemma 2,  $R_{i',k'}(\delta)$  is rewritten as

$$\begin{aligned} R_{i',k'}(\delta) &= 2^{n-2m} \sum_{c \in F_{2^m}^*} \sum_{x_1 \in F_{2^m}^*} \omega_4^{\{f([x_1 c]^r) + 2f([x_1 a c]^r)\}} \\ &\quad \cdot \omega_4^{-\{f(x_1^r) + 2f([x_1 b]^r)\}} \\ &+ \frac{2^{n-2m} - 1}{2^m - 1} \sum_{x_1 \in F_{2^m}^*} \omega_4^0 \\ &+ 2^{n-2m} \sum_{x_1 \in F_{2^m}^*} \omega_4^{\{f([x_1 c]^r) + 2f([x_1 a c]^r)\}} \\ &+ 2^{n-2m} \sum_{x_1 \in F_{2^m}^*} \omega_4^{-\{f([x_1 c]^r) + 2f([x_1 b c]^r)\}}. \end{aligned}$$

From Lemma 3 and the facts that  $S_{\psi_d} = 1$  and  $S_{\mu_d} = 1$ ,  $R_{i',k'}(\delta)$  can be computed as

$$R_{i',k'}(\delta) = 2^{n-2m} + 2^{n-2m} - 1 + 2 \times 2^{n-2m}(-1) = -1.$$

For  $\delta = 1$ , from the difference-balance property of  $f(x)$  we have

$$\begin{aligned} R_{i',k'}(1) &= \sum_{x \in F_{2^n}^*} \omega_4^{(f([\text{tr}_m^n(x)]^r) + 2f(a^r[\text{tr}_m^n(x)]^r))} \\ &\quad \cdot \omega_4^{-(f([\text{tr}_m^n(x)]^r) + 2f(b^r[\text{tr}_m^n(x)]^r))} \\ &= -1. \end{aligned}$$

**Case 2)**  $i' = k'$  for nonzero  $i'$  and  $k'$  :

Obviously,  $R_{i',i'}(1) = 2^n - 1$ . When  $\delta \notin F_{2^m}$ , similar to case 1 we have,

$$R_{i',i'}(\delta) = -1.$$

**Case 3)**  $i' = 0$  or  $k' = 0$  :

In this case, it is easy to show that  $R_{i',0}(\delta) = R_{0,i'}(\delta) = -1$  for  $\delta \notin F_{2^m}$  and  $R_{0,0}(\delta) = -1$  for  $\delta \neq 1$ .  $\square$

## References

- [1] S.S. Again, *Hadamard matrices and their Applications*, Lecture Notes in Mathematics, vol. 1168, New York: Springer-Verlag, 1980.
- [2] S. Boztas, R. Hammons, and P. V. Kumar, "4-phase sequences with near optimum correlation properties," *IEEE Trans. on Inform. theory*, vol. 38, pp. 1101–1113, May, 1992.
- [3] R. Craigen, "Hadamard matrices and designs," Chapter IV. 24, *CRC Handbook of Combinatorial Designs*, Edited by C. J. Colbourn and J. H. Dinitz, CRC Press, New York, pp. 370-377, 1996
- [4] J. -H. Kim and H. -Y. Song, "Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation," *J. Commun. Networks*, vol. 1, no. 1, pp. 14-18, Mar. 1999.
- [5] S.H. Kim, J.W. Jang, J.S. No, and H. Chung "New construction of quaternary low correlation zone sequences", *preprint*.
- [6] S.-H. Kim, H. Chung, and J.-S. No, "New cyclic relative difference sets constructed from  $d$ -homogeneous functions with difference-balanced property," submitted to *IEEE Trans. Inform. Theory*, Aug. 2003.
- [7] S. Matsufuji and N. Suehiro, "Complex Hadamard matrices related to bent sequences," *IEEE Trans. on Inform. Theory*, vol. 42, no. 2, p. 637, Mar. 1996.
- [8] J.-S. No, "New cyclic difference sets with Singer parameters constructed from  $d$ -homogeneous functions," accepted for publication in *Designs, Codes and Cryptography*, Feb. 2003.

- [9] J.-S. No, K. Yang, H. Chung, and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property," in *Proc. IEEE Int. Symp. Inform. Theory and Its Appl. (ISITA '96)*, Victoria, British Columbia, Canada, Sept. 1996, pp. 837–840.
- [10] B. M. Popovic, N. Suehiro, and P. Z. Fan, "Orthogonal sets of quadriphase sequences with good correlation properties," *IEEE Trans. on Inform. Theory*, vol. 48, no. 4, pp. 956–959, Apr. 2002.