New Constructions of Quaternary Hadamard Matrices

Ji-Woong Jang[1], Sang-Hyo Kim[1], Jong-Seon No[1], and Habong Chung[2]

[1] School of Electrical Engineering and Computer Science,
Seoul National University, Seoul 151-742, Korea
{stasera, shkim}@ccl.snu.ac.kr, jsno@snu.ac.kr
[2] School of Electronics and Electrical Engineering,
Hong-Ik University, Seoul 121-791, Korea
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.

1 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 [3,8,13]. 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[1,4,14,15,16]. Hadamard matrices have strong ties to sequences. Matsufuji and Suehiro proposed the complex Hadamard matrices related to bent sequences[9]. Popovic, Suehiro, and Fan[12] 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. Before we proceed to the next section, let us clarify some terms and notations used throughout this paper.

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 α^t, where α is a primitive element in F_{2^n}, then we can obtain a sequence $s(\alpha^t)$, $0 \le t \le 2^n - 2$, of period $2^n - 1$. Hence, for convenience, we

T. Helleseth et al. (Eds.): SETA 2004, LNCS 3486, pp. 361–372, 2005.

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'.

For $\delta \in F_{2^n}^*$, the crosscorrelation function between two quaternary sequences $s_i(x)$ and $s_j(x)$ is defined as

$$R_{i,j}(\delta) = \sum_{x \in F_{2^n}^*} \omega_4^{s_i(x\delta) - s_j(x)},$$

where w_4 is a complex fourth root of unity.

Let $f(x)$ be a mapping from F_{2^n} onto F_{2^m}, where $m|n$. The function $f(x)$ is said to be *balanced* if each nonzero element of F_{2^m} appears 2^{n-m} times and zero element $2^{n-m} - 1$ times in the list $\{f(x) | \, x \in F_{2^n}^*\}$. A function $f(x)$ is said to be *difference-balanced* if $f(\delta x) - f(x)$ is balanced for any $\delta \in F_{2^n} \backslash \{0, 1\}$. It is easy to see that the binary sequence with difference-balance property has the ideal autocorrelation property necessarily and sufficiently.

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 ϕ and ψ as

$$\phi(v) = v_1, \quad \psi(v) = v_2.$$

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

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

2 New Constructions of Quaternary Hadamard Matrices

In this section, we propose two constructions for quaternary Hadamard matrices from binary sequences with ideal autocorrelation.

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, $1 \le z \le 2^n - 2$, the following sequence $q_z(t)$ given by

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

is balanced over Z_4.

Proof . Let $N_z(a, b), \ a, b \in \{0, 1\}$ be the number of t such that $g(t) = a$ and $g(t + z) = b$. Since $g(t)$ has the ideal autocorrelation property, it is balanced and difference-balanced. Thus we have

$$\begin{aligned} N_z(0,0) + N_z(0,1) &= 2^{n-1} - 1 \\ N_z(0,0) + N_z(1,0) &= 2^{n-1} - 1 \\ N_z(0,0) + N_z(1,1) &= 2^{n-1} - 1. \end{aligned}$$

Finally, from the facts that

$$\sum_a \sum_b N_z(a,b) = 2^n - 1,$$

we can conclude that $q_z(t)$ is balanced. □

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

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

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

where h_{ij} is given as

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

Proof . Let u_i be the ith row of $\mathcal{H}_Q$. It is clear that $u_i u_i^\dagger = 2^n,\ 0 \le i \le 2^n - 1$. In proving the orthogonality between u_i and u_k, we should consider the following three cases.

Case 1) $i = 0$ and $1 \le k \le 2^n - 1$:

From Lemma 1 and balance property of $g(t)$ and $q_k(t)$, it is clear that u_0 is orthogonal to u_k, for any k, $1 \le k \le 2^n - 1$.

Case 2) $i = 1$, $2 \le k \le 2^n - 1$:

In this case, $u_1 u_k^\dagger$ is given as

$$\begin{aligned} u_1 u_k^\dagger &= 1 + \sum_{t=0}^{2^n-2} w_4^{2g(t)-g(t)-2g(t+k-1)} \\ &= 1 + \sum_{t=0}^{2^n-2} w_4^{g(t)-2g(t+k-1)}. \end{aligned}$$

From Lemma 1, it is straightforward that $g(t) - 2g(t+k-1)$ is also balanced and thus $u_1 u_k^\dagger = 0$, i.e., u_1 is orthogonal to u_k.

Case 3) $2 \le i < k \le 2^n - 1$:
In this case, $u_i u_k^\dagger$ is given as

$$\begin{aligned} u_i u_k^\dagger &= 1 + \sum_{t=0}^{2^n-2} w_4^{\{g(t)+2g(t+i-1)\}-\{g(t)+2g(t+k-1)\}} \\ &= 1 + \sum_{t=0}^{2^n-2} w_4^{2(g(t+i-1)+g(t+k-1))} \\ &= 1 + \sum_{t=0}^{2^n-2} (-1)^{g(t+i-1)+g(t+k-1)}. \end{aligned}$$

From the difference-balance property of $g(t)$, $u_i u_k^\dagger = 0$. □

Here is an example of an 8×8 quaternary Hadamard matrix constructed from the above theorem.

Example 1. Let α be a primitive element in F_{2^3}. Using the m-sequence $\mathrm{tr}_1^3(\alpha^t)$ of period 7, we can construct the quaternary sequences of period 7 as

$$\begin{aligned} s_0(t) &= 2\mathrm{tr}_1^3(\alpha^t) \\ s_i(t) &= \mathrm{tr}_1^3(\alpha^t) + 2\mathrm{tr}_1^3(\alpha^{t+i}),\ 1 \le i \le 6, \end{aligned}$$

which gives us $\mathcal{H}_Q$

$$\mathcal{H}_Q = \begin{bmatrix} \omega_4^0 & \omega_4^0 & \omega_4^0 & \omega_4^0 & \omega_4^0 & \omega_4^0 & \omega_4^0 & \omega_4^0 \\ \omega_4^0 & \omega_4^2 & \omega_4^0 & \omega_4^0 & \omega_4^2 & \omega_4^0 & \omega_4^2 & \omega_4^2 \\ \omega_4^0 & \omega_4^1 & \omega_4^0 & \omega_4^2 & \omega_4^1 & \omega_4^2 & \omega_4^3 & \omega_4^3 \\ \omega_4^0 & \omega_4^1 & \omega_4^2 & \omega_4^0 & \omega_4^3 & \omega_4^2 & \omega_4^3 & \omega_4^1 \\ \omega_4^0 & \omega_4^3 & \omega_4^0 & \omega_4^2 & \omega_4^3 & \omega_4^2 & \omega_4^1 & \omega_4^1 \\ \omega_4^0 & \omega_4^1 & \omega_4^2 & \omega_4^2 & \omega_4^3 & \omega_4^0 & \omega_4^1 & \omega_4^3 \\ \omega_4^0 & \omega_4^3 & \omega_4^2 & \omega_4^2 & \omega_4^1 & \omega_4^0 & \omega_4^3 & \omega_4^1 \\ \omega_4^0 & \omega_4^3 & \omega_4^2 & \omega_4^0 & \omega_4^1 & \omega_4^2 & \omega_4^1 & \omega_4^3 \end{bmatrix}.$$

□

No, Yang, Chung, and Song constructed *extended sequences* with ideal autocorrelation from sequences of shorter period with ideal autocorrelation[11].

Theorem 2 (No, Yang, Chung, and Song[11]). Let n and m be positive integers such that $m|n$. Let $f(y)$ be the function from F_{2^m} to F_2 with difference-balance property such that $f(0) = 0$. Let r be an integer such that $\gcd(r, 2^m - 1) = 1$ and $1 \le r \le 2^m - 2$. Then the sequence of period $2^n - 1$ defined by

$$f([\mathrm{tr}_m^n(x)]^r)$$

has the ideal autocorrelation property. □

Using the extended sequences, we can construct the quaternary Hadamard matrix as in the following theorem.

Theorem 3. Let n and m be integers such that $m|n$, and r be an integer such that $1 \le r \le 2^m - 2$ 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 the balance and difference-balance properties. Let $s_i(\alpha^t)$ be defined as

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

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

Then the following matrix $\mathcal{H}_L$ is a $2^n \times 2^n$ quaternary Hadamard matrix.

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

where h_{ij} is given as

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

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

Proof of the above theorem requires following lemmas.

Lemma 2. Let m, e, and n be positive integers such that $n = em$. Let $q = 2^m$ and $A = \{1, \alpha, \cdots, \alpha^{T-1}\}$, where α 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 the balance and difference-balance properties. 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

$$v(\delta x_2) = a \quad \text{and} \quad v(x_2) = b, \quad a, b \in F_q.$$

Then, we have

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

Proof. Let $N_\delta(a, b)$ be the number of $x \in F_{q^e}^*$ satisfying $v(\delta x) = a$ and $v(x) = b$. Let $x = x_1x_2$, where $x_1 \in F_q$ and $x_2 \in A$. Because $v(x)$ is difference-balanced, $v(\delta x) - v(cx) = v(\delta x) - cv(x)$ is balanced for any $c \in F_q^*$ and 0 occurs $q^{e-1} - 1$ times as x varies over $F_{q^e}^*$. Thus we have

$$\sum_{a \in F_q} N_\delta(ca, a) = q^{e-1} - 1. \tag{2}$$

Since $v(x)$ is balanced, we have

$$\sum_{a\in F_q} N_\delta(a,0) = \sum_{b\in F_q} N_\delta(0,b) = q^{e-1} - 1. \tag{3}$$

Also, note that

$$\sum_{a\in F_q}\sum_{b\in F_q} N_\delta(a,b) = q^e - 1. \tag{4}$$

Now, we have

$$\begin{aligned}\sum_{a\in F_q}\sum_{b\in F_q} N_\delta(a,b) &= \sum_{a\in F_q} N_\delta(a,0) + \sum_{b\in F_q} N_\delta(0,b)\\ &\quad -N_\delta(0,0) + \sum_{c\in F_q^*}\sum_{a\in F_q^*} N_\delta(a,ca)\\ &= \sum_{a\in F_q} N_\delta(a,0) + \sum_{b\in F_q} N_\delta(0,b) - N_\delta(0,0)\\ &\quad + \sum_{c\in F_q^*}\left\{\sum_{a\in F_q} N_\delta(a,ca) - N_\delta(0,0)\right\}. \end{aligned}\tag{5}$$

Plugging (2), (3), and (4) into (5), we have

$$N_\delta(0,0) = q^{e-2} - 1. \tag{6}$$

From (2) and (6), we also have

$$\sum_{a\in F_q^*} N_\delta(ca,a) = \sum_{a\in F_q} N_\delta(ca,a) - N_\delta(0,0) = q^{e-2}(q-1).$$

Let $\beta = \alpha^T$. For a given x_2 such that $v(\delta x_2) = cv(x_2)$, the ordered pair $(v(\delta x), v(x)) = (x_1 v(\delta x_2), x_1 v(x_2))$ takes each value in the list

$$(c,1), (c\beta,\beta), \cdots, (c\beta^{q-2}, \beta^{q-2})$$

exactly once as x_1 varies over F_q^*. Therefore we have

$$\sum_{a\in F_q^*} N_\delta(ca,a) = (q-1)\sum_{a\in F_q^*} M_\delta(ca,a),$$

which, in turn, tells us that

$$\sum_{a\in F_q^*} M_\delta(ca,a) = q^{e-2}.$$

Similarly, we have

$$M_\delta(0,0) = \frac{N_\delta(0,0)}{q-1} = \frac{q^{e-2}-1}{q-1}$$
$$\sum_{c\in F_q^*} M_\delta(c,0) = \frac{\sum_{c\in F_q^*} N_\delta(c,0)}{q-1} = q^{e-2}$$
$$\sum_{c\in F_q^*} M_\delta(0,c) = \frac{\sum_{c\in F_q^*} N_\delta(0,c)}{q-1} = q^{e-2}.$$

□

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 $s(x)$ as

$$\phi_s(x) = \phi(s(x)), \quad \psi_s(x) = \psi(s(x))$$

and their modulo-2 sum as

$$\mu_s(x) = \phi_s(x) + \psi_s(x). \tag{7}$$

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

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

Proof . It is clear that

$$\sum_{x\in B} \omega_4^{s(x)} = (N_s(0) - N_s(2)) + j(N_s(1) - N_s(3))$$

and

$$N_{\psi_s}(1) = N_s(2) + N_s(3) \tag{8}$$
$$N_{\psi_s}(0) = 2^n - N_{\psi_s}(1) = N_s(0) + N_s(1) \tag{9}$$
$$N_{\mu_s}(1) = N_s(1) + N_s(2). \tag{10}$$

From (8), (9), and (10), we have

$$N_s(0) - N_s(2) = N_{\psi_s}(0) - N_{\mu_s}(1)$$
$$N_s(1) - N_s(3) = N_{\mu_s}(1) - N_{\psi_s}(1).$$

Thus we prove the lemma. □

Corollary 1. Let $s(x)$ be a function from F_{2^n} to Z_4. Then,

$$\sum_{x \in F_{2^n}} \omega_4^{s(x)} = 0$$

if and only if the functions $\psi_s(x)$ and $\mu_s(x)$ are balanced.

□

Now we are ready to prove Theorem 3.

Proof of Theorem 3. Let v_i be the ith row of $\mathcal{H}_L$, $0 \le i \le 2^n - 1$. We have to show that $v_i v_k^\dagger = 0$ for all $i \ne k$. The case when $i = 0$ is simple. Since v_0 is an all one sequence, we need to show that the row sum is zero for each row $v_k, k \ne 0$. From the structure of $\mathcal{H}_L$, it is manifest that the rows v_{1+lT} through $v_{T+lT}, 0 \le l \le 2^m - 2$, are the cyclic shifts of $s_l(x)$. Also note that $s_0(x)$ is balanced since it is in fact the binary extended sequence, and $s_l(x), l \ne 0$, is also balanced from Lemma 1. Thus we have $v_0 v_k^\dagger = 0$ for all $k \ne 0$.

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

$$\begin{aligned} v_i v_k^\dagger &= 1 + \sum_{t=0}^{2^n-2} w_4^{s_{\lfloor (i-1)/T \rfloor}(t+i_T) - s_{\lfloor (k-1)/T \rfloor}(t+k_T)} \\ &= 1 + \sum_{x \in F_{2^n}^*} w_4^{s_{i'}(\delta x) - s_{k'}(x)}, \end{aligned}$$

where $\delta = \alpha^{i_T - k_T}$, $i' = \lfloor (i-1)/T \rfloor$, and $k' = \lfloor (k-1)/T \rfloor$. For $\delta = \alpha^{i_T - k_T}$, 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 $a, b \in F_{2^m} \setminus F_2$, define two quaternary sequences $u_a(x)$ and $u_b(x)$ of period $2^m - 1$ as

$$\begin{aligned} u_a(x) &= f(x) + 2f(ax) \\ u_b(x) &= f(x) + 2f(bx) \end{aligned}$$

and let $d(x, \eta) = u_a(\eta x) - u_b(x)$. Define S_{ψ_d} and S_{μ_d} as

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

Then from (1) and (7), S_{ψ_d} and S_{μ_d} can be expressed as

$$S_{\psi_d} = \sum_{x \in F_{2^m}^*} \sum_{\eta \in F_{2^m}^*} (-1)^{f(\eta x)f(x) + f(x) + f(bx) + f(a\eta x)} \tag{11}$$

$$S_{\mu_d} = \sum_{x \in F_{2^m}^*} \sum_{\eta \in F_{2^m}^*} (-1)^{f(\eta x)f(x) + f(\eta x) + f(bx) + f(a\eta x)}. \tag{12}$$

Now, let $I_1(x)$ and $I_2(x)$ be the inner summation in (11),

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

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

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

and

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

Then S_{ψ_d} can be expressed as

$$S_{\psi_d} = \sum_{x \in \{x | f(x)=0, x \in F_{2^m}^*\}} I_1(x) + \sum_{x \in \{x | f(x)=1, x \in F_{2^m}^*\}} I_2(x). \tag{13}$$

The first term in (13) is computed as

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

since $f(x)$ is balanced.

The second term in (13) is computed as

$$\begin{aligned} \sum_{x \in \{x | f(x)=1, x \in F_{2^m}^*\}} I_2(x) &= \sum_{x \in \{x | f(x)=1, x \in F_{2^m}^*\}} (-1)^{f(bx)+1} \sum_{\eta \in F_{2^m}^*} (-1)^{f(\eta x)+f(a\eta x)} \\ &= \sum_{x \in \{x | f(x)=1, x \in F_{2^m}^*\}} (-1)^{f(bx)} \end{aligned}$$

since $f(x)$ is difference-balanced.

Thus, we have

$$S_{\psi_d} = \sum_{x \in \{x | f(x)=1, x \in F_{2^m}^*\}} (-1)^{f(bx)} - \sum_{x \in \{x | f(x)=0, x \in F_{2^m}^*\}} (-1)^{f(bx)}.$$

Finally, from the difference-balance property, we have

$$(f(x), f(bx)) = \begin{cases} (0,0), & 2^{m-2} - 1 \text{ times} \\ (1,0), & 2^{m-2} \text{ times} \\ (0,1), & 2^{m-2} \text{ times} \\ (1,1), & 2^{m-2} \text{ times}, \end{cases}$$

as x varies over $F_{2^m}^*$. Therefore, we have

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

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

Now consider two sequences

$$s_{i'}(x) = f([\mathrm{tr}_m^n(x)]^r) + 2f(a^r[\mathrm{tr}_m^n(x)]^r)$$
$$s_{k'}(x) = f([\mathrm{tr}_m^n(x)]^r) + 2f(b^r[\mathrm{tr}_m^n(x)]^r),$$

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

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

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

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

$$\begin{aligned} R_{i',k'}(\delta) =& \sum_{d\in F_{2^m}^*} M_\delta(cd,d) \sum_{c\in F_{2^m}^*}\sum_{x_1\in F_{2^m}^*} \omega_4^{\{f([x_1cd]^r)+2f([x_1acd]^r)\}-\{f([x_1d]^r)+2f([x_1bd]^r)\}} \\ &+ M_\delta(0,0)\sum_{x_1\in F_{2^m}^*}\omega_4^0 \\ &+ \sum_{c\in F_{2^m}^*} M_\delta(c,0)\sum_{x_1\in F_{2^m}^*}\omega_4^{\{f([x_1c]^r)+2f([x_1ac]^r)\}} \\ &+ \sum_{c\in F_{2^m}^*} M_\delta(0,c)\sum_{x_1\in F_{2^m}^*}\omega_4^{-\{f([x_1c]^r)+2f([x_1bc]^r)\}} \\ =& 2^{n-2m}\sum_{c\in F_{2^m}^*}\sum_{x_1\in F_{2^m}^*}\omega_4^{\{f([x_1c]^r)+2f([x_1ac]^r)\}-\{f(x_1^r)+2f([x_1b]^r)\}} \\ &+ \frac{2^{n-2m}-1}{2^m-1}\sum_{x_1\in F_{2^m}^*}\omega_4^0 \\ &+ 2^{n-2m}\sum_{x_1\in F_{2^m}^*}\omega_4^{\{f([x_1c]^r)+2f([x_1ac]^r)\}} \\ &+ 2^{n-2m}\sum_{x_1\in F_{2^m}^*}\omega_4^{-\{f([x_1c]^r)+2f([x_1bc]^r)\}}. \end{aligned}$$

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 $\delta = 1$, we have

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

from the difference-balance property of $f(x)$.

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

Obviously, $R_{i',i'}(1) = 2^n - 1$. When $\delta \notin F_{2^m}$, the correlation function is given as

$$\begin{aligned} R_{i',i'}(\delta) &= 2^{n-2m} \sum_{c \in F_{2^m}^*} \sum_{x_1 \in F_{2^m}^*} \omega_4^{\{f([x_1c]^r)+2f([x_1ac]^r)\}-\{f(x_1^r)+2f([x_1a]^r)\}} \\ &\quad + \frac{2^{n-2m}-1}{2^m-1} \sum_{x_1 \in F_{2^m}^*} \omega_4^0 \\ &\quad + 2^{n-2m} \sum_{x_1 \in F_{2^m}^*} \omega_4^{\{f([x_1c]^r)+2f([x_1ac]^r)\}} \\ &\quad + 2^{n-2m} \sum_{x_1 \in F_{2^m}^*} \omega_4^{\{f(x_1^rc^r)+2f([x_1ac]^r)\}} \\ &= 2^{n-2m} + 2^{n-2m} - 1 + 2 \times 2^{n-2m}(-1) = -1. \end{aligned}$$

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 $\delta \neq 1$. □

Here is an example of 64×64 quaternary Hadamard matrix constructed from the Theorem 3.

Example 2. Let α be a primitive element in F_{2^6}. Let $T = \frac{2^6-1}{2^3-1} = 9$ and $r = 5$. Using the GMW-sequence $\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^t)]^r)$ of period 63, we can construct quaternary sequences of period 63 as

$$\begin{aligned} s_0(t) &= 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^t)]^5) \\ s_i(t) &= \mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^t)]^r) + 2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{t+9i})]^5), \ 1 \le i \le 8. \end{aligned}$$

These sequences make a quaternary Hadamard matrix as

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

where h_{ij} is given as

$$h_{ij} = \begin{cases} w^0 & \text{if } i = 0 \text{ or } j = 0 \\ w^{2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{j-1+i_9})]^5)} & \text{if } 1 \le i \le T \text{ and } j \neq 0 \\ w^{\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{j-1+i_9})]^r)+2\mathrm{tr}_1^3([\mathrm{tr}_3^6(\alpha^{j-1+i_9+9\lfloor (i-1)/9 \rfloor})]^5)} & \text{otherwise,} \end{cases}$$

where $i_9 = (i-1) \bmod 9$.

□

References

1. Again, S.S. : Hadamard matrices and their Applications. Lecture Notes in Mathematics, Vol. 1168, Springer-Verlag, New York (1980)
2. Boztas, S., Hammons, R., and Kumar, P.V.: 4-phase sequences with near optimum correlation properties. IEEE Trans. on Inform. theory, Vol. 38, (1992) 1101-1113
3. Craigen, R.: 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 (1996) 370-377
4. Kim, J.-H. and Song, H.-Y.: Existence of cyclic Hadamard difference sets and its relation to binary sequences wiht ideal autocorrelation. J. Commun. Networks, Vol. 1, No. 1, (1999) 14-18
5. Kim, S.H., Jang, J.W., No, J.S., and Chung, H.: New construction of quaternary low correlation zone sequences. submitted to IEEE Trans. Inform. Theory, (2004)
6. Kim, S.-H., Chung, H., No, J.-S., and Helleseth, T.: New cyclic relative difference sets constructed from d-homogeneous functions with difference-balanced property. to appear in IEEE Trans. Inform. Theory
7. Klapper, A.: d-form sequence: Families of sequences with low correlation values and large linear spans. IEEE Trans. Inform. Theory, Vol. 41, No. 2, (1995) 423-431
8. van Lint, J.H. and Wilson, R. M.: A course in combinatorics, Cambridge Univ. Press, New York (1992)
9. Matsufuji, S. and Suehiro, N.: Complex Hadamard matrices related to bent sequences. IEEE Trans. on Inform. Theory, Vol. 42, No. 2, (1996) 637
10. No, J.-S.: New cyclic difference sets with Singer parameters constructed from d-homogeneous functions. Designs. Codes and Cryptography, Vol. 33, Issue 3, (2004) 199–213
11. No, J.-S., Yang, K., Chung, H., and Song, H.-Y.: On the construction of binary sequences with ideal autocorrelation property. Proc. IEEE Int. Symp. Inform. Theory and Its Appl. (ISITA'96), Victoria, British Columbia, Canada (1996) 837-840
12. Popovic, B.M., Suehiro, N., and Fan, P. Z.: Orthogonal sets of quadriphase sequences with good correlation properties. IEEE Trans. on Inform. Theory, Vol. 48, No. 4, (2002) 956-959
13. Seberry, J. and Yamada, M.: Hadamard matrices, sequences, and block design. Contemporary Design Theory: Collection of Surveys,(1992) 431-569
14. Simon, M. K. *et al.*: Spread Spectrum Communications, Vol. 1, Rockville, MD: Computer Science Press, 1985; revised ed., McGraw-Hill, (1994)
15. Song, H.-Y. and Golomb, S.W.: On the existence of cyclic Hadamard difference sets. IEEE Trans. Inform. Theory, Vol. IT-40, (1994) 1266-1268
16. TIA/EIA/IS-95: Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System. Telecommunications Industry Association as a North American 1.5 MHz Cellular CDMA Air-Interface Standard, (1993)