New Constructions of Balanced Quasi-Cyclic Generalized Hadamard Matrices[1]

*Ji-Woong Jang$^{\text{O}}$, *Jong-Seon No, and **Habong Chung
*School of Electrical Engineering and Computer Science and INMC, Seoul National University
∗∗School of Electronics and Electrical Engineering, Hong-Ik University
Email: jsno@snu.ac.kr

Abstract

In this paper, we define quasi-cyclic (QC) generalized Hadamard matrices and balanced QC generalized Hadamard matrices. Then we propose a new construction method for QC generalized Hadamard matrices. The proposed matrices are constructed from the balanced optimal low correlation zone (LCZ) sequence set which has correlation value -1 within low correlation zone.

1. Introduction

A generalized Hadamard matrix $\mathcal{H}(q,u)$ of order u is a $u \times u$ matrix over the set of complex q-th roots of unity satisfying $\mathcal{H}(q,u)\mathcal{H}^{\dagger}(q,u) = uI_u$, where † denotes the conjugate transpose and I_u is the identity matrix of order u [1], [2]. For brevity, we use the notation $\mathcal{H}$ interchangeably $\mathcal{H}(q,u)$ if specifying q and u is unnecessary. In other words, the definition implies that any two distinct rows of $\mathcal{H}$ are orthogonal. For this reason, generalized Hadamard matrices have been studied for the applications in many areas such as wireless communication systems, coding theory, and signal design [1].

In this paper, we define quasi-cyclic (QC) generalized Hadamard matrices and balanced QC generalized Hadamard matrices. Then we propose a new construction method for QC generalized Hadamard matrices. The proposed matrices are constructed from the balanced optimal low correlation zone (LCZ) sequence set which has correlation value -1 within low correlation zone.

2. Preliminaries

Given a q-ary sequence $s(t)$ of period N, the autocorrelation $R_a(\tau)$ of the sequence at shift τ is defined by

$$R_a(\tau) = \sum_{t=0}^{N-1} \omega^{s(t)-s(t+\tau)}$$

where ω is a primitive complex q-th root of unity. A q-ary sequence $s(t)$ of period N is said to have ideal autocorrelation property if

$$R_a(\tau) = \begin{cases} N, & \text{if } \tau = 0 \\ -1, & \text{otherwise.} \end{cases}$$

For an integer q, let N be a positive integer such that $N \equiv -1 \bmod q$ and $s(t)$ a q-ary sequence of period N. Then the sequence $s(t)$ is said to be *balanced* if the number of occurrences of 0 in a period of the sequence is at most one less than the number of occurrences of any other symbols in nonzero element of Z_q or some subgroup of Z_q.

The sequence $\omega^{s(t)}$ can be considered as the complex counterpart of $s(t)$. Throughout the rest of this paper, when we mention a sequence with some correlation property, we interchangeably imply $s(t)$ or $\omega^{s(t)}$ if no confusion is caused by the context.

Let $s(t)$ be a q-ary sequence of period N. Let $\mathcal{H}_C$ be an $(N+1)\times(N+1)$ generalized Hadamard matrix defined by

$$\mathcal{H}_C(q, N+1) = (h_{ij})$$

where h_{ij} is given as

$$h_{ij} = \begin{cases} 1, & \text{if } i = 0 \text{ or } j = 0 \\ \omega^{s_i(j-1)}, & \text{otherwise.} \end{cases}$$

Then the matrix $\mathcal{H}_C$ is called a *cyclic generalized Hadamard matrix* if $s_i(t) = s(t+i-1)$ where addition is computed modulo N.

Let $\mathcal{H}^s$ be the $N \times N$ submatrix of an $(N+1)\times(N+1)$ generalized Hadamard matrix $\mathcal{H}$ obtained by deleting the first row and the first column of $\mathcal{H}$. The definition of cyclic generalized Hadamard matrix implies that $\mathcal{H}^s$ is a circulant matrix and each row of $\mathcal{H}^s$ can be considered as some cyclic shift of a sequence of period N with ideal autocorrelation property.

Thus an $(N+1)\times(N+1)$ cyclic generalized Hadamard matrix completely characterizes a sequence

[1] This research was supported by the MIC, Korea, under the ITRC support program and by the MOE, the MOCIE, and the MOLAB, Korea, through the fostering project of the Lab. of Excellency.

with ideal autocorrelation of period N, and vice versa. And in this sense, we may call this sequence as the sequence associated with the cyclic generalized Hadamard matrix, and vice versa.

Now, let us broaden this idea of association, i.e., a generalized Hadamard matrix associated with a set of sequences instead of a single sequence. In this context, we can define a quasi-cyclic (QC) generalized Hadamard matrix as follows.

Definition 1 [QC generalized Hadamard matrix] Let $\mathbf{S}$ be a set of M cyclically inequivalent q-ary sequences of period N. Let $\mathcal{H}_{QC}$ be an $(N+1)\times(N+1)$ generalized Hadamard matrix defined by

$$\mathcal{H}_{QC}(q, N+1) = (c_{ij})$$

where c_{ij} is given as

$$c_{ij} = \begin{cases} 1, & \text{if } i=0 \text{ or } j=0 \\ \omega^{s_i(j-1)}, & \text{otherwise.} \end{cases}$$

If each of $s_i(t)$, $1 \le t \le N$, can be expressed as a cyclic shift (including zero shift) of some member in $\mathbf{S}$, then we call $\mathcal{H}_{QC}$ a *quasi-cyclic generalized Hadamard matrix* associated with $\mathbf{S}$.

□

If each member in the set $\mathbf{S}$ is picked as some row in $\mathcal{H}^s_{QC}$ the same number of times, we call $\mathcal{H}_{QC}$ a *balanced quasi-cyclic generalized Hadamard matrix.*

3. A Construction Method of Balanced Quasi-Cyclic Hadamard Matrices Associated with an Optimal LCZ Sequence Set

In this section, we propose a new construction method of balanced QC generalized Hadamard matrices associated with an optimal LCZ sequence set that has the correlation value -1 within low correlation zone.

Let $\mathcal{S}$ be a set of M sequences of period N. If the magnitude of correlation function between any two sequences in $\mathcal{S}$ takes the values less than or equal to ϵ within the range $-L < \tau < L$, of the offset τ, then $\mathcal{S}$ is called an LCZ sequence set with parameters (N, M, L, ϵ) [7].

Tang, Fan, and Matsufuji [9] derived the lower bound on the size of an LCZ sequence set using the Welch bound [10].

Theorem 2 [Tang, Fan, and Matsufuji [9]] Let $\mathcal{S}$ be an LCZ sequence set with parameters (N, M, L, ϵ). Then,

$$M \le \Big\lfloor \frac{N^2 - \epsilon^2}{L(N-\epsilon^2)} \Big\rfloor \tag{1}$$

where $\lfloor x \rfloor$ denotes the greatest integer not exceeding x.

□

An LCZ sequence set achieving the equality in the above bound is called an *optimal LCZ sequence set.* And if all the sequences in the LCZ sequence set are balanced, we call it a *balanced LCZ sequence set.* Associated with the balanced optimal LCZ sequence set that has correlation value -1 within the low correlation zone, we can construct the balanced QC generalized Hadamard matrix as in the following theorem.

Theorem 3 Let L, M and N be integers such that $N = ML$. Let $\mathcal{S} = \{s_i(t)\}$ be the balanced optimal LCZ sequence set with parameters $(N, M, L, 1)$. Suppose that the correlation value between any two sequences in $\mathcal{S}$ within the low correlation zone be -1. Then we can construct an $(N+1)\times(N+1)$ balanced QC generalized Hadamard matrix

$$\mathcal{H}_{LC}(q, N+1) = (h_{jk})$$

where h_{jk} is given as

$$h_{jk} = \begin{cases} 1, & \text{if } j=0 \text{ or } k=0 \\ w^{s_{\lfloor (j-1)/L \rfloor}(k-1+j_L)}, & \text{otherwise} \end{cases}$$

and $j_L = (j-1) \bmod L$.

Proof: What we are going to show is that each row in $\mathcal{H}_{LC}$ is orthogonal to every other row in $\mathcal{H}_{LC}$, all sequences in $\mathcal{S}$ appear exactly the same number of times as some rows of $\mathcal{H}^s_{LC}$ in the form of their cyclic shifts (including zero shift), and they are balanced.

Since rows in $\mathcal{H}^s_{LC}$ are cyclic shifts of the sequences in $\mathcal{S}$, it is clear that all rows in $\mathcal{H}^s_{LC}$ are balanced. From the definition of h_{jk}, it is manifest that all sequences in $\mathcal{S}$ have the same number of occurrences as rows in $\mathcal{H}^s_{LC}$.

Let v_i be the ith row of $\mathcal{H}_{LC}$, $0 \le i \le N$. We have to show that $v_i v_k^\dagger = 0$ for all $i \ne k$. Since v_0 is an all one sequence and each v_i, $1 \le i \le N$, comes from some balanced sequence, it is clear that $v_0 v_i^\dagger = 0$ for all $1 \le i \le N$. From the structure of $\mathcal{H}_{LC}$, it is manifest that the rows v_{1+lL} through $v_{L+lL}, 0 \le l \le M-1$, are the cyclic shifts of $\omega^{s_l(t)}$. And for all $1 \le i < k \le N$, we can rewrite $v_i v_k^\dagger$ as follows

$$v_i v_k^\dagger = 1 + \sum_{t=0}^{N-1} w^{s_{\lfloor (i-1)/L \rfloor}(t+\tau_i) - s_{\lfloor (k-1)/L \rfloor}(t+\tau_k)}$$

where $\tau_i = i - 1 - \lfloor (i-1)/L \rfloor L$ and $\tau_k = k - 1 - \lfloor (k-1)/L \rfloor L$.

From the property of LCZ sequence set with correlation value -1 within the low correlation zone, it is clear that

$$\sum_{t=0}^{N-1} w^{s_{\lfloor (i-1)/L \rfloor}(t+\tau_i) - s_{\lfloor (k-1)/L \rfloor}(t+\tau_k)} = -1.$$

□

Using the optimal LCZ sequence set in [3] and Theorem 3, we have the following corollary.

Corollary 4 Let m and n be integers such that $m|n$. Let p be a prime and α a primitive element in F_{p^n}. Let $v(\cdot)$ be a 1-form function from F_{p^m} to F_p and $f(x)$ a 1-form function from F_{p^n} to F_{p^m}. Let $\mathcal{S}_p$ be an optimal p^2-ary LCZ sequence set with parameters $(p^n-1, p^m-1, (p^n-1)/(p^m-1), 1)$ defined by

$$\mathcal{S}_p = \{s_i(t) \mid 0 \leq i \leq p^m-2\}$$

where $s_i(t)$ is given as

$$s_i(t) = \begin{cases} pf([v(\alpha^{\frac{p^n-1}{p^m-1}i}x)]^r), & \\ & \text{if } \alpha^{\frac{p^n-1}{p^m-1}i} \in F_p \\ f([v(x)]^r) + pf([v(\alpha^{\frac{p^n-1}{p^m-1}i}x)]^r), & \\ & \text{otherwise.} \end{cases}$$

Then we can construct a $p^n \times p^n$ balanced QC generalized Hadamard matrix

$$\mathcal{H}_{LC}(p^2, p^n) = (h_{jk})$$

where h_{jk} is given as

$$h_{jk} = \begin{cases} 1, & \text{if } j=0 \text{ or } k=0 \\ w^{s_{\lfloor (j-1)/L \rfloor}(k-1+j_L)}, & \text{otherwise} \end{cases}$$

and $L = (p^n-1)/(p^m-1)$ and $j_L = (j-1) \bmod L$. □

In fact, all the entries $s \in \{0,1,2,3\}$ in $\mathcal{H}_{LC}$ should be $(\sqrt{-1})^s \in \{\pm 1, \pm j\}$. Nevertheless, we stick to the above form (even if it is not right) simply because of the visual purpose. Note that rows v_1 through v_5 come from $s_0(t)$, v_6 through v_{10} from $s_1(t)$, and v_{11} through v_{15} from $s_2(t)$.

Here is another corollary for Theorem 3.

Corollary 5 Let m and n be integers such that $m|n$. Let p be a prime and $f(t)$ a p-ary sequence of period p^m-1 with ideal autocorrelation. Let $\{f_i(t) \mid 0 \leq i \leq p^m-2\}$ be a set of cyclic shifts of $f(t)$, such that $f_i(t) = f(t+i)$, $t = 0, 1, 2, \cdots, p^m-2$. From the result of [4], we can construct so-called a column sequence set $\mathcal{S}$ for binary LCZ sequence set of period p^n-1 as

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

where $s_i(t)$ is given as

$$s_i(t) = \begin{cases} f_i(p^m-2-1-t), & 0 \leq t \leq \frac{p^m-1}{2} \\ f_i(t+(p^m-1)/2), & \frac{p^m-1}{2}+1 \leq t \leq p^m-2. \end{cases} \tag{2}$$

Let α be a primitive element in F_{p^n}. Let $c_i(\beta^t) = s_i(t)$, where β is a primitive element in F_{p^m}. Using the column sequence set $\mathcal{S}$, we can construct the optimal p-ary LCZ set $\mathcal{L}_p$ with parameters $(p^n-1, p^m-1, (p^n-1)/(p^m-1), 1)$ as

$$\mathcal{L}_p = \{l_i(t) \mid 0 \leq i \leq p^m-2 \text{ and } 0 \leq t \leq p^n-2\}$$

where $l_i(t)$ is given as

$$l_i(t) = c_i(\mathrm{tr}_m^n(\alpha^t)).$$

Using the LCZ sequence set $\mathcal{L}_p$, we can construct a balanced QC generalized Hadamard matrix

$$\mathcal{H}_{LP}(p, p^n) = (h_{jk})$$

where h_{jk} is given as

$$h_{jk} = \begin{cases} 1, & \text{if } j=0 \text{ or } k=0 \\ w^{l_{\lfloor (j-1)/L \rfloor}(k-1+j_L)}, & \text{otherwise} \end{cases}$$

and $L = (p^n-1)/(p^m-1)$ and $j_L = (j-1) \bmod L$. □

References

[1] S. S. Agaian, *Hadamard matrices and their Applications,* Lecture Notes in Mathematics, vol. 1168, New York: Springer-Verlag, 1980.

[2] A. T. Butson, "Generalized Hadamard matrices," *Proc. Am. Math. Soc.*, vol. 13, pp. 894–898, 1962.

[3] J.-W. Jang, J.-S. No, and H. Chung, "A new construction of optimal p^2-ary low correlation zone sequences using unified sequences," *submitted to IEICE Fundamentals*, Dec. 2005.

[4] J.-W. Jang, J.-S. No, H. Chung, and X. Tang, "New sets of optimal p-ary low correlation zone sequences," *submitted to IEEE Trans. Inform. Theory*, Mar. 2005.

[5] S.-H. Kim, J.-W. Jang, J.-S. No, and H. Chung, "New constructions of quaternary low correlation zone sequences," *IEEE Trans. Inform. Theory*, vol. 51, no. 4, pp. 1469–1477, April 2005.

[6] A. Klapper, "*d*-form sequence: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 423–431, Mar. 1995.

[7] B. Long, P. Zhang, and J. Hu, "A generalized QS-CDMA system and the design of new spreading codes," *IEEE Trans. Veh. Technol.*, vol. 47, pp. 1268–1275, Nov. 1998.

[8] J. S. No, "*p*-ary unified sequences: *p*-ary extended *d*-form sequences with ideal autocorrelation property," *IEEE Trans. Inform. Theory*, vol. 48, no. 9, pp. 2540–2546, Sept. 2002.

[9] X. H. Tang, P. Z. Fan, and S. Matsufuji, "Lower bounds on correlation of spreading sequence set with low or zero correlatoin zone," *Electon. Lett.*, vol. 36, no. 6, pp. 551–552, Mar. 2000.

[10] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. 20, no. 3, pp. 397–399, May 1974.