AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **60(3)** (2014), Pages 255–262

A class of quaternary noncyclic Hadamard matrices*

Udaya Parampalli

Department of Computing and Information Systems
University of Melbourne
VIC 3010
Australia
udaya@unimelb.edu.au

Serdar Boztaş

School of Mathematical and Geospatial Sciences
RMIT University
VIC 3001
Australia
serdar.boztas@rmit.edu.au

Dedicated to Professor Kathy Horadam on her sixtieth birthday

Abstract

A normalized Hadamard matrix is said to be completely noncyclic if no two row vectors are shift equivalent in its punctured matrix (i.e., with the first column removed). In this paper we present an infinite recursive construction for completely noncyclic quaternary Hadamard matrices. These Hadamard matrices are useful in constructing low correlation zone sequences.

1 Introduction

If H is a Hadamard matrix of order N, then we have $HH^\star = N \cdot I_N$, where I_N is the identity matrix of order N and $H^\star$ is complex conjugate of the transpose of H. In this paper we deal with a quaternary Hadamard matrix, which is a square matrix over $\{1, -1, i, -i\}, i = \sqrt{-1}$, whose rows are mutually complex orthogonal. It is well

* The work of the authors was supported by an Australia-China linkage project of DIISR, Australia.

known that any Hadamard matrix can be normalized such that its first row and first column are all ones vectors. In this paper, all the Hadamard matrices involved are normalized.

Definition 1 *Let $a = (a_0 \cdots a_{N-1})$ and $b = (b_0 \cdots b_{N-1})$ be two vectors, or two sequences, of length N. Then a and b are said to be shift-equivalent if there exists an integer $0 < \tau < N$ such that $b = L^\tau(a)$, where L is the left cyclic shift operator, i.e., $L^\tau(a) = (a_\tau \cdots a_{N-1} a_0 \cdots a_{\tau-1})$.*

Definition 2 *Given an $N \times N$ matrix M, let $\hat{M}$ be defined as the $N \times (N-1)$ matrix obtained from M by removing its first column.*

A normalized Hadamard matrix H is said to be completely noncyclic if all the row vectors of $\hat{H}$ are shift distinct. In this paper we present an infinite recursive construction for completely noncyclic quaternary Hadamard matrices.

Hadamard matrices have been studied extensively and a huge collection of results on their properties exists [1, 3, 5, 8]. However, most of the studies concentrate on solving real Hadamard conjecture which states that an $N \times N$ binary Hadamard matrix exists for all positive integers N which are multiples of 4 [3]. The completely noncyclic property we consider in this paper has only recently been investigated and arises in connection with the generation of low correlation zone (LCZ) sequences [2, 11, 12, 13]. A 4-tuple (N, M, L_{cz}, ϵ) is a family of M low correlation zone sequences of period N having low correlation value ϵ within the zone L_{cz} [13].

LCZ sequences are used as signature sequences in quasi-synchronous code-division multiple access (QS-CDMA) communication systems [6, 13]. In a QS-CDMA system, the relative time delay between the signature sequences of different users is random but restricted to a certain time range $\{\pm 1, \pm 2, \cdots \pm T\}$, where T is much smaller than the period of the sequences. The LCZ sequences have the property that they possess very small correlation for time delays within T, for example in this paper it is fixed to be -1. Due to this property, such sequences can be employed to decrease both multiple access interference and multipath interference in a QS-CDMA system [6]. In the literature, numerous constructions of LCZ sequence sets have been reported [2, 4, 6, 7, 10, 11] which can all be explained by the interleaved technique in [10, 11] or the subfield construction in [2].

Recently, an interesting connection between Hadamard matrices and the LCZ sequences was pointed out in [11, 12]. Using an interleaved method, a family of binary LCZ sequences of length $2^n - 1$ and low correlation zone length $L_{cz} = \frac{2^n-1}{2^m-1}$ where $m|n$ and $m \geq 2$ was constructed in [7, 11, 12]. The method used is quite general and works over quaternary modulation. In order to construct the quaternary LCZ sequences of length $2^n - 1$ and low correlation zone length $L_{cz} = \frac{2^n-1}{2^m-1}$ where $m|n$ and $m \geq 2$, the interleaved method requires a set U of sequences of length $2^m - 1$ over $\{1, -1, i, -i\}$ satisfying:

P1. Balance property, i.e., in any sequence three elements of $\{1, -1, i, -i\}$ occur with equal frequency 2^{m-2}, with the remaining element occuring with frequency $2^{m-2} - 1$;

P2. Inner product property, i.e., the inner product between any two distinct sequences in U is -1, i.e., $\sum_{i=0}^{N-1} a_i \bar{b}_i = -1$ for any two sequences $a = (a_0 \cdots a_{N-1})$ and $b = (b_0 \cdots b_{N-1})$ in U, where $\bar{b}_i$ represents the complex conjugate of b_i;

P3. Shift distinct property, i.e., no two sequences in U are equivalent with respect to the cyclic shift operator.

It was pointed out in [7, 11, 12] that such a set can be obtained from the shift distinct row vectors of a $2^m \times (2^m - 1)$ punctured normalized Hadamard matrix, leaving the first all ones row vector. A more general construction in [2] uses subfield decomposition and a completely noncyclic binary Hadamard matrix to derive low correlation zone sequences.

In this paper, we present a class of completely noncyclic quaternary Hadamard matrices of size 2^m, $m \geq 3$. These matrices, when used in the LCZ constructions in [2, 7, 11, 12] result in optimal LCZ sequence sets.

The paper is organized as follows. In Section 2, we give necessary conditions for shift equivalence of the recursively defined rows. Section 3 discusses the noncyclic property of a class of Hadamard matrices first introduced by Elliot and Rao [3].

2 Necessary conditions for shift equivalence

In this section we will consider a general recursive construction of 2^m quaternary vectors of period 2^m. We will derive necessary conditions for cyclic shift equivalence of quaternary vectors in the recursive construction. These conditions will be used to prove completely non-cylic property of a family of quaternary Hadamard matrices.

Let $-a$ be the negation of a, where a could be a quaternary symbol or a sequence or a matrix. Denote by $\mathbf{1}_{2^m-1}$ the all one vectors of length $2^m - 1$ and by $\oslash_{2^m-1} = (-1, 1, \cdots, -1, 1, -1)$ the vector of alternate 1's and -1's of length $2^m - 1$ with starting entry -1.

Let φ_m and ψ_m be any quaternary matrices of size 2^m by $2^m - 1$, $m \geq 1$. Note that the matrices have 2^m row sequences of length $N = 2^m - 1$. Now consider the matrix φ_{m+1} of length $2^{m+1} - 1$ defined by

$$\varphi_{m+1} = \begin{pmatrix} \varphi_m & \mathbf{1}_{2^m}^T & \varphi_m \\ \psi_m & -\mathbf{1}_{2^m}^T & -\psi_m \end{pmatrix}. \tag{1}$$

In the following theorem, a set of necessary conditions on two shift equivalent row sequences in φ_{m+1} is given. Theorem 1 is an adaptation of [13, Theorem 1] to the quaternary case, but with slightly different terminology. In particular the "codes" are hidden, and the results are described in the terminology of matrices.

Theorem 1 *Suppose that a quaternary matrix φ_{m+1}, $m \geq 1$, is constructed by* (1). *Further assume that φ_m and ψ_m contain no repeated rows. Then, any two row vectors $c, d \in \varphi_{m+1}$ are shift equivalent only if they satisfy any of the following conditions:*

I. $c = (a\ 1\ a)$ *and* $d = (b\ 1\ b)$, *where* $a, b \in \varphi_m$, $b = L^\tau(a)$ *for some* τ *such that* $0 < \tau < 2^m - 1$ *and* $a_0 = a_1 = \cdots = a_{\tau-1} = 1$,

II. $c = (a\ 1\ a)$ *and* $d = (-a\ -1\ a)$, *where* $a \in \varphi_m$, $-a \in \psi_m$ *with* $a = \oslash_{2^m-1}$;

III. $c = (a\ -1\ -a)$ *and* $d = (a\ 1\ a)$, *where* $a \in \varphi_m$ *and* $a \in \psi_m$ *with* $a = \oslash_{2^m-1}$ *and* $\tau = 2^m - 1$;

IV. $c = (a\ -1\ -a)$ *and* $d = (b\ -1\ -b)$, *where* $a, b \in \psi_m$ *with the conditions,* $b_i = a_{i+\tau}$, $0 \le i < 2^m - 1 - \tau$, $a_0 = a_1 = \cdots = a_{\tau-1} = 1$, $b_{2^m-1-\tau} = b_{2^m-1-\tau+1} = \cdots = b_{2^m-2} = -1$; *and* $0 < \tau < 2^m - 1$;

V. $c = (a\ -1\ -a)$ *and* $d = (b\ -1\ -b)$, *where* $a, b \in \psi_m$ *with* $a = \mathbf{1}_{2^m-1}$, $b = -\mathbf{1}_{2^m-1}$ *and* $\tau = 2^m - 1$.

Proof: The proof goes along the same lines as in [13, Theorem 1].Suppose that two row vectors $c, d \in \varphi_{m+1}$ are shift equivalent, say $d = L^\tau(c)$ for a shift $\tau > 0$. Since $d = L^\tau(c)$ is equivalent to $c = L^{2^{m+1}-1-\tau}(d)$, without loss of generality it is sufficient that we consider only those shifts in the range $0 < \tau < 2^m$.

From (1), any row vectors c and d of φ_{m+1} have to satisfy one of the following four conditions:

1. $c = (a\ 1\ a)$ and $d = (b\ 1\ b)$ where $a \neq b \in \varphi_m$ by our assumptions;
2. $c = (a\ 1\ a)$ and $d = (b\ -1\ -b)$ where $a \in \varphi_m$ and $b \in \psi_m$;
3. $c = (a\ -1\ -a)$ and $d = (b\ 1\ b)$ where $a \in \psi_m$ and $b \in \varphi_m$;
4. $c = (a\ -1\ -a)$ and $d = (b\ -1\ -b)$ where $a \neq b \in \psi_m$ by our assumptions.

We will systematically list the conditions obtained by the elementwise equivalence of the equation $d = L^\tau(c)$ for each of the above cases. For example, consider the case 1 above. First, we consider what happens when $\tau = 2^m - 1$. Then, d and $L^\tau(c)$ are illustrated below:

$$\begin{array}{rcl} d & = & (b_0\ \ b_1\ \ \cdots\ \ b_{N-1}\ \ \ 1\ \ \ b_0\ \ b_1\ \ \cdots\ \ b_{N-1}), \\ L^\tau(c) & = & (1\ \ a_0\ \ \cdots\ \ a_{N-2}\ \ a_{N-1}\ \ a_0\ \ a_1\ \ \cdots\ \ a_{N-1}). \end{array}$$

The relation $d = L^{2^m-1}(c)$ implies that $a = b$ which is impossible as a and b are assumed to be different. Secondly, we consider the case 1 above with $0 < \tau < 2^m - 1$. The row vectors d and $L^\tau(c)$ are represented in the two lines given below:

$$\begin{array}{cccccccccccccc} (b_0 & \cdots & b_{N-\tau-1} & b_{N-\tau} & b_{N-\tau+1} & \cdots & b_{N-1} & 1 & b_0 & \cdots & b_{N-\tau-1} & b_{N-\tau} & \cdots & b_{N-1}) \\ (a_\tau & \cdots & a_{N-1} & 1 & a_0 & \cdots & a_{\tau-2} & a_{\tau-1} & a_\tau & \cdots & a_{N-1} & a_0 & \cdots & a_{\tau-1}) \end{array}$$

Equating d with $L^\tau(c)$ elementwise leads to the conditions $I.$ of the theorem. We repeat the above method to derive conditions II, III, IV V of the theorem by considering elementwise equivalence of $d = L^\tau(c)$ for all other cases.

3 Completely Noncyclic property of Elliot-Rao Hadamard matrices

We first provide a definition of Sylvester Hadamard matrices.

Definition 3 *Let m be a positive integer. A Sylvester matrix of order 2^m, $m \geq 1$ is defined recursively as $S_m = S_1 \otimes S_{m-1}$, where $S_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, and $\otimes$ represents the Kronecker product of matrices.*

From Definition 3, it is easy to see that the row vectors of the S_m are shift distinct. However, when the first column is removed from the matrix, it is not clear how many row vectors are still shift distinct. In [13], it is shown that $\hat{S}_m$ has exactly $2^m - m$ cyclically distinct vectors.

Below we introduce Elliot-Rao Hadamard matrices as given in the research monograph [3, p 78.]. Let

$$C_1 = \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}, C_2 = \begin{bmatrix} S_1 & S_1 \\ C_1 & -C_1 \end{bmatrix}.$$

Then for $m \geq 3$, an Elliot-Rao Hadamard matrix is represented by the recursion:

$$C_m = \begin{bmatrix} C_{m-1} & C_{m-1} \\ C_1 \otimes S_{m-2} & -C_1 \otimes S_{m-2} \end{bmatrix}, m \geq 3, \tag{2}$$

where S_m is a Sylvester Hadamard matrix of order 2^m.

The example of Elliot-Rao matrix for $m = 2$ is given as follows.

$$C_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \\ 1 & i & -1 & -i \end{bmatrix},$$

We are interested in showing that all vectors of $\hat{C}_m$ are cyclically distinct.

It can be easily observed that the row vectors of $\hat{C}_2$ are shift distinct and hence C_2 is completely noncyclic. In the following theorem, we prove that $C_m, m \geq 2$ is completely noncyclic.

Theorem 2 *The Elliot-Rao Hadamard matrix C_m, $m \geq 2$ is completely noncyclic.*

Proof: We will consider $\hat{C}_m$. Then $\hat{C}_{m+1}$ can be represented as:

$$\hat{C}_{m+1} = \varphi_{m+1} = \begin{pmatrix} \varphi_m & \mathbf{1}_{2^m}^T & \varphi_m \\ \psi_m & -\mathbf{1}_{2^m}^T & -\psi_m \end{pmatrix}, \tag{3}$$

with starting matrix $\varphi_2 = \hat{C}_2$ and ψ_m is realized by another recursion given by $\psi_m = \hat{D}_m$, where

$$D_m = C_1 \otimes S_{m-1}. \tag{4}$$

So for $m = 2$, D_2 is given as follows:

$$D_2 = \begin{bmatrix} 1 & 1 & -i & -i \\ 1 & -1 & -i & i \\ 1 & 1 & i & i \\ 1 & -1 & i & -i \end{bmatrix}.$$

From above it is clear that the recursion (3) is in the form required for Theorem 1. We prove that the row vectors are cyclically distinct by using mathematical induction. Since the starting matrix φ_2 has cyclically distinct row vectors, Case I of Theorem 1 is not applicable. Also $\oslash_{2^m-1}$ belongs to φ_m, but because of (4), $\oslash_{2^m-1} \notin \psi_m$. With the same logic as before, $-\mathbf{1}_{2^m-1} \notin \psi_m$. Hence the situations in Case II, Case III and Case V of Theorem 1 can never happen. Similarly Case IV of Theorem 1 can never happen as the second half of row sequences in ψ_m contain only elements from $\{i, -i\}$. Hence no two rows in $\hat{C}_{m+1}$ are cyclic shifts of each other. □

3.1 Low Correlation zone sequences

As explained in Section 1, the row vectors of $\hat{C}_m$ satisfies the requirements of the set U with property P1 to P3. We have the following result.

Proposition 1 (Tang-Fan-Matsufuji bound [9]) *Given a (N, M, L_{cz}, ϵ) LCZ sequence set S with parameters: sequence length $N := 2^n - 1$, low correlation zone length $L_{cz} = \frac{2^n-1}{2^m-1}$, and the low correlation value $\epsilon := -1$, its size M satisfies*

$$M \leq \left\lfloor \frac{2^n(2^m-1)}{2^n-1} \right\rfloor = 2^m - 1.$$

We have the following result on number of balanced sequences obtained from Elliot-Rao Hadamard matrices.

Lemma 1 *There are exactly $2^m - 2$ balanced rows in $\hat{C}_m$, for $m \geq 2$.*

Proof: The result follows from mathematical induction. From inspection it is clear that the first two rows of $\hat{C}_2$ are not balanced. The first one is all 1 sequence and the second one is a sequence of alternating 1s and -1s. These two sequences exist in each $\hat{C}_m$ due to the recursion (2). All other row sequences are balanced with each symbol from $\{1, -1, i, -i\}$ occurring equally often. □

By omitting the first column of C_m, $m \geq 3$, we can obtain a maximum number of $2^m - 2$ sequences meeting the properties P1,P2 and P3 of Section 1.0.

Thus, the nonzero row sequences of $\hat{C}_m, m \geq 3$, can be used to construct $2^m - 2$ LCZ sequences of length $2^n - 1$, $m|n$, which is almost optimal with respect to the Tang-Fan-Matsufuji bound in Proposition 1.

An example of Elliot-Rao matrices for $m = 3$ is given below to illustrate that it has $2^3 - 2$ sequences (making up its 6×7 lower right submatrix) meeting the properties P1,P2 and P3 of Section 1.

$$C_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & 1 & -i & -i & -1 & -1 & i & i \\ 1 & -1 & -i & i & -1 & 1 & i & -i \\ 1 & 1 & i & i & -1 & -1 & -i & -i \\ 1 & -1 & i & -i & -1 & 1 & -i & i \end{bmatrix}.$$

Remark 1: In contrast to the quaternary Hadamard matrices considered in this paper, it is not possible to obtain completely noncyclic Binary Hadamard matrices in sizes 4 and 8 due to the existence of an upper bound on the number of cyclically distinct sequences in small lengths [13].

Acknowledgments

We express our sincere gratitude to the second reviewer whose comments significantly changed the paper for the better.

References

[1] R. Craigen and H. Kharaghani, Hadamard Matrices and Hadamard Designs, In *Handbook of Combinatorial Designs: Second Edition* (Eds. C.J. Colbourn and J.H. Dinitz), Chapman and Hall, CRC, 2007.

[2] G. Gong, S.W. Golomb and H-Y. Song, A note on low correlation zone signal sets, *IEEE Trans. Inform. Theory* 53 (2007), 2575–2581.

[3] K.J. Horadam, *Hadamard Matrices*, Princeton University Press, 2007.

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

[5] P.H.J. Lampio, F. Szöllősi and P.R.J. Ostergard, The quaternary complex Hadamard matrices of orders 10, 12, and 14, *Discrete Math.* 313 (2013), 189–206.

[6] B. Long, P. Zhang and J. Hu, A generalized QS-CDMA system and design of new spreading codes, *IEEE Trans. Veh. Technol.* 47 (1998), 1268–1275.

[7] U. Parampalli and X.H. Tang, Low Correlation Zone Sequences from Interleaved Construction, *IEICE Trans. Fundamentals* E93-A:11 (2010), 2220–2226.

[8] J. Seberry and M. Yamada, Hadamard matrices, sequences, and block designs, In *Contemporary Design Theory: A Collection of Essays*, (Eds. J.H. Dinitz and D.R. Stinson), New York: Wiley, 1992.

[9] X.H. Tang, P.Z. Fan and S. Matsufuji, Lower bounds on the maximum correlation of sequence set with low or zero correlation zone, *Electron. Lett.* 36 (2000), 551–552.

[10] X.H. Tang and P.Z. Fan, Generalized d-Form sequence and LCZ sequences based on the interleaving technique, *Proc. 7th Int. Symp. Communication Theory and Applications* (*ISCTA'03*), (2003), Ambleside, UK, 276–281.

[11] X.H. Tang and P. Udaya, New construction of low correlation zone sequences from Hadamard matrices, *Proc. IEEE Int. Symp. Information Theory 2005* (*ISIT'05*), (2005), Adelaide, Australia, 482–486.

[12] X.H. Tang and P. Udaya, New recursive construction of low correlation zone sequences, *Proc. Second Int'l. Workshop on Sequence Design and Its Applics. to Communications* (*IWSDA'05*), (2005), Shimonoseki, Yamaguchi, Japan, 86–89.

[13] X.H. Tang and U. Parampalli, On the Noncyclic Property of Sylvester Hadamard matrices, *IEEE Trans. Inform. Theory* 56 (2010), 4653–4658.

(Received 20 Dec 2011; revised (reports sent Nov 2012): 7 Apr 2014, 30 Aug 2014)