New Constructions of Complete Non-cyclic Hadamard Matrices, Related Function Families and LCZ Sequences

Krystal Guo* and Guang Gong

*Department of Combinatorics and Optimizations
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada
{kguo, ggong}@uwaterloo.ca

Abstract. A Hadamard matrix is said to be completely non-cyclic (CNC) if there are no two rows (or two columns) that are shift equivalent in its reduced form. In this paper, we present three new constructions of CNC Hadamard matrices. We give a primary construction using a flipping operation on the submatrices of the reduced form of a Hadamard matrix. We show that, up to some restrictions, the Kronecker product preserves the CNC property of Hadamard matrices and use this fact to give two secondary constructions of Hadamard matrices. The applications to construct low correlation zone sequences are provided.

Keywords: Hadamard matrices, completely non-cyclic type, shift-distinctness, low correlation zone sequences

1 Introduction and the Basic Definitions

Low correlation zone sequences (LCZ) signal sets have important applications in quasi-synchronous code division multiple access (CDMA) applications, proposed in 1992 [3]. There has been considerable work towards constructions of these sequences. The first construction of LCZ set, given in [11] in 1998, produces a LCZ signal set whose size is not maximized. Following this approach, many different constructions have been proposed, including approaches in [12] [9] [13] [8] [10] [16] [1]. In 2007, Gong, Golomb, and Song [5] describe a general approach to the construction of LCZ sequences using sequences with subfield decompositions. Constructions of this type of LCZ signal sets with maximum size are in one-to-one correspondence with constructions of completely non-cyclic Hadamard matrices.

In this paper, we will show three new constructions of such Hadamard matrices. The first and third new constructions generalize two known

constructions in [8] and with improved results. The second construction is the Kronecker product of matrices, which we show to preserve the completely non-cyclic property, under some conditions.

We now introduce basic concepts and definitions which will be used throughout the paper.

A. Basic Concepts about Sequences. Let p be a prime number, $\mathbb{F}_p$ denote a finite field with p elements, and $\mathbf{a} = \{a_i\}$ be a sequence over $\mathbb{F}_p$, of period N. The shift operator is defined by $L(\mathbf{a}) := (a_1, a_2, \cdots)$. So, $L^r(\mathbf{a}) = (a_r, a_{r+1}, \cdots)$. For two sequences, $\mathbf{a}$ and $\mathbf{b}$, if $\mathbf{b} = L^r(\mathbf{a})$, then $\mathbf{a}$ and $\mathbf{b}$ are called *shift equivalent*, denoted $\mathbf{a} \sim \mathbf{b}$. Otherwise, we say that $\mathbf{a}$ and $\mathbf{b}$ are *shift distinct* and write $\mathbf{a} \nsim \mathbf{b}$. If the elements of $\mathbf{a}$ satisfies the linear recursive relation: $a_{r+k} = \sum_{i=0}^{r-1} c_i a_{i+k}, k \in \mathbb{Z}$, where $c_i \in \mathbb{F}_p$ and $t(x) = x^r - \sum_{i=0}^{r-1} c_i x^i$ is the polynomial with the smallest degree which recursively generates $\mathbf{a}$, then the degree of $t(x)$ is called the *linear span* of $\mathbf{a}$, denoted $l(\mathbf{a})$.

When $N \,|\, p^n - 1$, we can associate the sequence $\mathbf{a}$ with a function $f(x)$ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ such that $a_i = f(\alpha^i), i \in \mathbb{Z}$, where α is an element in $\mathbb{F}_{p^n}$ with order N. Then $\mathbf{a}$ is called an *evaluation* of $f(x)$. In this paper, we assume that $f(0) = 0$. We say that $\mathbf{a}$ is *balanced* if $|N_a - N_b| \leq 1$ for any $a, b \in \mathbb{F}_p$ where $N_x = |\{a_i = x \,|\, 0 \leq i < N\}|$. Let $\omega = e^{2\pi i/p}$ be a primitive pth root of unity. The *periodic crosscorrelation* of $\mathbf{a}$ and $\mathbf{b}$ is defined by $C_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} \omega^{b_{i+\tau} - a_i},\ 0 \leq \tau \leq N-1$ where the indices are computed modulo $N-1$. If $\mathbf{b} = \mathbf{a}$, we write $C_{\mathbf{a},\mathbf{b}}(\tau)$ as $C_{\mathbf{a}}(\tau)$ and call it the *autocorrelation* of $\mathbf{a}$. If $\mathbf{a}$ is balanced and $C_{\mathbf{a}}(\tau) = \begin{cases} N,\ \tau \equiv 0 \pmod{N} \\ -1, \tau \not\equiv 0 \pmod{N}, \end{cases}$ then we say that $\mathbf{a}$ has an *(ideal) 2-level autocorrelation function.*

B. Hadamard Matrices and CNC Hadamard Matrices. A *Hadamard matrix* of order n is a $n \times n$ matrix H with entries in $\{1, -1\}$, such that $HH^T = H^T H = nI_n$, where I_n is the n by n identity matrix. By applying elementary "Hadamard-preserving" operations, the matrix H can always be transformed into a special form in which all entries in the first row and the first column are equal to 1, see [2][4]. Without loss of generality, all the Hadamard matrices in this paper will be assumed to be in this form. The *reduced form* of H, denoted H^- is the matrix obtained from H by deleting the first row and the first column. A Hadamard matrix is said to be *completely non-cyclic (CNC) with respect to row (or column) shifts* if any two rows (respectively columns) in the reduced form of H are shift distinct.

One can see that, up to cyclic shifts, there is a unique sequence of length 3 consisting of two -1's and one 1. This implies that there is no CNC Hadamard matrix of order 4. By a similar enumeration, there are five shift-distinct sequences of length 7 consisting of four -1's and three 1's, which implies that there is no CNC Hadamard matrix of order 8. The smallest value of q for which there exists a CNC Hadamard matrix of order 2^q is 4.

A *generalized Hadamard matrix* is a matrix $H = (h_{ij})_{v\times v}$ where $h_{ij} = \omega^{s_{ij}}, s_{ij} \in \mathbb{F}_p$ of order v such that $HH^* = vI_v$, where H^* is the conjugate transpose of H and ω is a primitive pth root of unity. Reduced form and the CNC property are analogously defined for generalized Hadamard matrices.

C. Equivalent Problem. A *low correlation zone signal set with parameters* (N, r, δ, d) is a set $\mathcal{K}$ consisting of r shift-distinct sequences over $\mathbb{F}_p$ with period N which satisfies that $|C_{\mathbf{a},\mathbf{b}}(\tau)| \leq \delta$ for all τ such that $|\tau| < d$, when $\mathbf{a}, \mathbf{b} \in \mathcal{K}$, and $\tau \neq 0$, when $\mathbf{a} = \mathbf{b}$. It has been shown in the literature [13][8][5], that a construction of an LCZ signal set with the parameters $(q^m - 1, q - 1, -1, d)$ where $d = (q^m - 1)/(q - 1)$ $(q = p^n)$ is equivalent to a construction of a family of functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, denoted as S, satisfying the following three conditions:

(a) Each function in S is balanced,
(b) The sum of any two functions in S is also balanced, and
(c) Any two sequences obtained from the functions in S by evaluation are shift distinct.

The number of functions in S, denoted $|S|$, cannot exceed $q - 1$. Gong, Golomb and Song [5] point out that a construction of S with maximal size is equivalent to a construction of a CNC Hadamard matrix of order q. In the literature, there are only three known constructions for the CNC Hadamard matrices of order q, of which the first two appear in [8] and one of them also appears in [13] as a somehow equivalent case, and the third in [5].

See [4] for further background on the theory of sequences and known constructions of 2-level autocorrelation sequences (see Chapters 8-9).

The rest of the paper is organized as follows. In Section 2, we present a new primary construction for CNC Hadamard matrices of order $q = p^n$ based on 2-level autocrrelation sequences over F_p and the flipping operator. In Section 3, we assert, under some restrictions, that Kronecker products of CNC Hadamard matrices are again CNC Hadamard matrices.

In Section 4, we give a construction using the Kronecker product and 2-level autocorrelation sequences. Section 5 provides the related functions and LCZ signal sets, and Section 6 includes concluding remarks.

[6] is a full version of this paper.

2 A Primary Construction of CNC Hadamard Matrices Using Flipping Operator

In this section, we present a new primary construction for CNC generalized Hadamard matrices of order $q = p^n$, where p is a prime. We assume that $N = p^n - 1$. For a given 2-level autocorrelation sequence $\mathbf{a} = (a_0, \cdots, a_{N-1})$ over $\mathbb{F}_p$, we may construct a circular matrix $C(\mathbf{a}) = (a_{ij})$ where $a_{ij} = a_{i+j}$. Let $b_i = \omega^{a_i}$, where ω is a primitive pth root of unity. Then we have the circular matrix $C(\mathbf{b})$, also written symbolically as $C(\mathbf{b}) = \omega^{C(\mathbf{a})}$. Let $H(\mathbf{a}) = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1^T} & \omega^{C(\mathbf{a})} \end{pmatrix}$. Then $H(\mathbf{a})$ is a Hadamard matrix if $p = 2$ and a generalized Hadamard matrix otherwise. We will give a construction of CNC Hadamard matrices by applying the flipping operation on the submatrices of $C(\mathbf{a})$.

Let $\mathbf{x} = (x_0, x_1, \cdots, x_{k-1})$ and R_k be the back diagonal identity matrix of order k, i.e., the entries of the back diagonal is equal to 1, and the other entries are zeros. Then $\mathbf{x}R_k = (x_{k-1}, \cdots, x_1, x_0)$, R_k is referred to as a *flipping operator*. Note that the flipping operation does not change the Hadamard property.

Construction 1. Let $\mathbf{e} = (e_0, e_1, \cdots, e_{2h-1})$ be a positive integer sequence satisfying that $\sum_{i=0}^{2h-1} e_i = N, e_i > 0$. We denote the first e_0 columns in $C(\mathbf{a})$ as an $N \times e_0$ submatrix A_0, the second e_1 columns in $C(\mathbf{a})$ as an $N \times e_1$ submatrix A_1, and so on. Then $C(\mathbf{a}) = (A_0, A_1, \cdots, A_{2h-1})$. Let

$$E(\mathbf{a}) = \left(A_0, A_1R_{e_1}, A_2, A_3R_{e_3}, \cdots, A_{2h-2}, A_{2h-1}R_{e_{2h-1}}\right).$$

Note that $E(\mathbf{a})$ is resulted from $C(\mathbf{a})$ by flipping h blocks of the columns. Let $H^- = \omega^{E(\mathbf{a})}$. Then

$$H = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1^T} & \omega^{E(\mathbf{a})} \end{pmatrix} \tag{1}$$

is again a Hadamard matrix.

Theorem 1. *Assume that* $l(\mathbf{a}) < \frac{N}{2(4h)}$ *where* h *is a positive integer and* $l(\mathbf{a}) < e_i < N - l(\mathbf{a})$. *Then any two row vectors in* $\omega^{E(\mathbf{a})}$ *(equivalently in* $E(\mathbf{a})$*) are shift distinct. Thus* H*, defined in (1), is a CNC Hadamard matrix.*

In order to prove Theorem 1, we need some basic properties of the linear spans of sequences and their corresponding reciprocal sequences, which are summarized below.

Property 1. Assume that $\mathbf{a} = \{a_i\}$ is a sequence over $\mathbb{F}_p$ with period N. Let $\mathbf{b} = \{b_i\}$ be the reciprocal sequence of $\mathbf{a}$, i.e., $b_0 = a_0$ and $b_i = a_{N-i}, 0 < i < N$.

(a) $l(\mathbf{a}) = l(\mathbf{b})$.
(b) $l(\mathbf{x} + L^\tau(\mathbf{x})) \le l(\mathbf{x})$ where $\mathbf{x} \in \{\mathbf{a}, \mathbf{b}\}$.
(c) $l(\mathbf{a} + L^\tau(\mathbf{b})) \le l(\mathbf{a}) + l(\mathbf{b}) \le 2\max\{l(\mathbf{a}), l(\mathbf{b})\}$.
(d) Maximum length of the runs of zeros in $\mathbf{a}$ is upper bounded by $l(\mathbf{a})-1$, i.e., there are at most $l(\mathbf{a}) - 1$ consecutive zeros in $\mathbf{a}$.
(e) $\mathbf{b} = L^{N-1}(\mathbf{a}R_N)$. Thus $l(\mathbf{a}R_N) = l(\mathbf{a})$.

Proof of Theorem 1. We only need to prove the row distinctness of $H^- = \omega^{E(\mathbf{a})}$, which is equivalent to the row shift-distinctness of $E(\mathbf{a})$. If there are two row vectors in $E(\mathbf{a})$, say $\mathbf{u}, \mathbf{v}$ which are shift equivalent, i.e., there is $r \ge 0$ such that $\mathbf{u} = L^r\mathbf{v}$, then $\mathbf{u} - L^r\mathbf{v} = \mathbf{0}$. According to the construction, we can consider their respective index sets of $\mathbf{u}$ and $\mathbf{v}$, each having $2h$ separating lines (including the last end point) at $\sum_{j=0}^{i} e_j, i = 0, \cdots, 2h-1$ and at $\sum_{j=0}^{i}(e_j + r), i = 0, \cdots, 2h-1$ (recall that the index is reduced by modulo N). Note that the multi-set $Q = \{e_i, e_i + r \mid 0 \le i < 2h\}$ has at most $4h$ different elements. Therefore, $\mathbf{u} - L^r\mathbf{v}$ can be divided into at most $4h$ blocks, each of which consists of consecutive elements of one of the three types of the sequences in Table 1 where $R = R_N$, the flipping operator defined at the beginning of this section. Their respective linear

Table 1. Types of the full sequences containing the segments of $\mathbf{u} - L^r\mathbf{v}$

		Type	Linear Span
$\mathbf{a} \pm L^i(\mathbf{a})$	$0 \le i < N$	1	$l(\mathbf{a})$
$\mathbf{a}R \pm L^j(\mathbf{a}R)$	$0 \le j < N$	2	$l(\mathbf{a})$
$\mathbf{a} \pm L^k(\mathbf{a}R)$	$0 \le k < N$	3	$\le 2l(\mathbf{a})$

spans are determined by Property 1 where we exclude the cases that the sequences are zero sequences in the first two cases in Table 1. Therefore, according to Property 1, the sequences of Types 1 and 2 have at most $l(\mathbf{a}) - 1$ consecutive zeros and the sequences of Type 3 have at most $2l(\mathbf{a}) - 1$ consecutive zeros.

Case 1: $|Q| = 4h$ and each block has the equal length, which is equal to $\frac{N}{4h}$. This is possible only when $\frac{N}{4h}$ is an integer. In this case, a block in $\mathbf{u}-L^r\mathbf{v}$ gives $\frac{N}{4h}$ consecutive zeros. Since $l(\mathbf{a}) < \frac{N}{8h}$, we have $2l(\mathbf{a})-1 < \frac{N}{4h}$, which is a contradiction.

Case 2: Each block does not have the equal length. According to the pigeon hole principle, there is at least one block with length $> \frac{N}{4h}$. Hence, this block gives more than $\frac{N}{4h}$ consecutive zeros, which is a contradiction, since there are at most $2l(\mathbf{a}) - 1$ consecutive zeros where $2l(\mathbf{a}) - 1 < \frac{N}{4h}$. □

If $h = 1$, then we can have a more refined result shown below by carefully examining patterns appeared in $\mathbf{u}-L^r\mathbf{v}$ in the proof of Theorem 1.

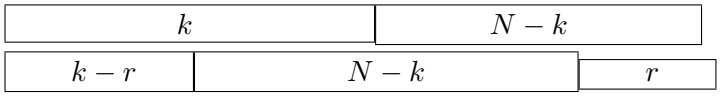
Theorem 2. *With the same notation as in Theorem 1, we assume that* $l(\mathbf{a}) < \frac{N}{4}$, $h = 1$, $\mathbf{e} = (e_0, e_1)$, *and* $3l(\mathbf{a}) < e_0 < N - 3l(\mathbf{a})$. *Then* H *is a CNC Hadamard matrix.*

Proof. We proceed as in the proof of Theorem 1 until we divide into the two cases.

We now write $e_0 = k$, so that $e_1 = N - k$. Without loss of generality, we can assume that $\mathbf{u}$ is the sequence from the first row of $E(\mathbf{a})$, and $\mathbf{v}$ is the tth row of $E(\mathbf{a})$. Since the case $k < N/2$ or $N - k < N/2$ can be processed similarly, we may assume that $t < k < N/2$.

Configuration 1: $r = k$. There are three sections which are overlapped with lengths k, $(N-k)-k$, and k added up to N. Since $k > 3l(\mathbf{a})$, then the block with length k has k consecutive zeros in $\mathbf{u} - L^r(\mathbf{v})$. On the other hand, any block in $\mathbf{u} - L^r(\mathbf{v})$ is a block in a sequence with the linear span at most $2l(\mathbf{a})$. Thus, it has at most $2l(\mathbf{a})$ consecutive zeros, which is a contradiction, since $2l(\mathbf{a}) < 3l(\mathbf{a}) < k$.

Configuration 2: $0 < r < k$ or $k < r < N - 1$. The proof of the latter case can be proceeded in the same way as the former case, so we omit it. For $0 < r < k$, we also could have $r < N - k$ or $r \geq N - k$. We will only show the case $r < N - k$ and the proof for $r \geq N - k$ is similar. Then we have four blocks with the following lengths configuration:



In details, we have the following pattern.

$$\begin{array}{rcl} \mathbf{u} & = & a_0 \ \cdots \ a_{k-1-r} \| a_{k-r} \cdots a_{k-1} \| a_{N-1} \ \cdots \ a_{k+r} \| a_{k+r-1} \cdots \ a_k \\ L^r(\mathbf{v}) & = & a_{t+r} \cdots \ a_{t+k-1} \| a_{t-1} \ \cdots \ a_{t-r} \| a_{t-1-r} \cdots \ a_{t+k} \| \ a_t \ \ \cdots \ a_{t+r-1} \end{array}$$

Thus the four blocks of $\mathbf{u} - L^r(\mathbf{v})$ has the following length patterns according to Table 1 in the proof of Theorem 1.

Segment	Type	Length
1	1	$k-r$
3	2	$N-k-r$
$2,4$	3	r

(Note. For a different range of r, the only difference is that those blocks correspond to their respective types of sequences in a different order.)

The average length is $N/4$. The case that $N-k-r = r = k = N/4$ is possible only when $\frac{N}{4}$ is an integer. In this case, the first block gives $N/4$ consecutive zeros of Type 1 sequences with linear span $l(\mathbf{a})$. According to Property 1-(d), it has at most $l(\mathbf{a})-1$ consecutive zeros. From the assumption that $l(\mathbf{a}) < N/4$, we have $l(\mathbf{a}) - 1 < N/4$, which is a contradiction. Thus, we only need to consider the case that not all the blocks have the same length. According to Property 2 below we have $\mathbf{u} \nsim \mathbf{v}$.

Thus H is a CNC Hadamard matrix.

Property 2. With the same notation in the proof of Theorem 2, let that $\mathbf{u}$ be the sequence from the first row of $E(\mathbf{a})$, and $\mathbf{v}$, the tth row of $E(\mathbf{a})$, $k < N/2$. If the lengths of the corresponding blocks in $\mathbf{u} = L^r(\mathbf{v})$ are $k-r$, r, $N-k-r$, and r respectively, which are not equal, then $\mathbf{u} \nsim \mathbf{v}$.

The proof of Property 2 is omitted here due to the lack of space. The reader is referring to the full version of this work [6].

Remark 1. The construction given in [8] (Theorem 17) can be considered as a special case of Theorem 1 when $h = 1$. However, the result given by Theorem 2 is an improvement of that result; Theorem 17 of [8] requires that $l(\mathbf{a}) < N/6$ and, here, Theorem 2 only needs that $l(\mathbf{a}) < N/4$. This bound also answered the question, addressed in [8] (Theorem 17), about whether there exists a general class when $l(\mathbf{a}) \geq N/6$.

3 CNC Property of Kronecker Products

In this section, we discuss the Kronecker product of two CNC Hadamard matrices. We then provide a construction using the Kronecker product and 2-level autocorrelation sequences in the next section. For these two sections, we will proceed the binary case for simplicity. For general p, the results are similar to the binary case, so we omit here.

For matrices $A = (a_{ij})$ and B, the *Kronecker product* of A and B, denoted $A \otimes B$, is:

$$A \otimes B = \begin{pmatrix} a_{00}B & a_{01}B & \cdots & a_{0,n-1}B \\ a_{10}B & a_{11}B & \cdots & a_{1,n-1}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1,0}B & a_{n-1,1}B & \cdots & a_{n-1,n-1}B \end{pmatrix}.$$

In this section, we denote by $\tilde{\mathbf{j}}_n$ the row vector of n alternating ± 1s; that is

$$\tilde{\mathbf{j}}_n := \left(1 \; -1 \; 1 \cdots (-1)^{n-1}\right).$$

We may omit the subscript when the dimension of the vector is implicit. Note that a CNC Hadamard matrix does not guarantee that any two rows of the matrix are shift distinct.

Theorem 3. (Construction 2) *If A and B are Hadamard matrices such that the following are true:*

i) for any two rows of A, $\mathbf{a} = (1, \mathbf{a}^-)$ and $\mathbf{a}' = (1, \mathbf{a}'^-)$, $\mathbf{a} \nsim \pm\mathbf{a}'$ and $\mathbf{a}^- \nsim \pm\mathbf{a}'^-$,
ii) for any two rows of B, $\mathbf{b} = (1, \mathbf{b}^-)$ and $\mathbf{b}' = (1, \mathbf{b}'^-)$, $\mathbf{b} \nsim \pm\mathbf{b}'$ and $\mathbf{b}^- \nsim \pm\mathbf{b}'^-$,
iii) the orders of A and B are both greater than 3, and
iv) $\tilde{\mathbf{j}}$ is not a row in the reduced form of A or B,

then $A \otimes B$ is CNC Hadamard matrix and its rows are also shift distinct.

From the conditions i)-ii), we know that both A and B are CNC. Theorem 3 can be seen as a direct consequence of the following lemma. Since this lemma is technical and straightforward, we will omit the proof here. The proof of Theorem 3 is given in the full version of this work [6].

For a vector

$$\mathbf{x} = \left(x_0, x_1, \cdots, x_{d-1}\right)$$

of order d, let $\mathbf{x}^-$ denote $\mathbf{x}$ with the first entry removed;

$$\mathbf{x}^- = \left(x_1, x_2, \cdots, x_{d-1}\right).$$

Lemma 1. *If* $\mathbf{a}, \mathbf{a}', \mathbf{b}$ *and* $\mathbf{b}'$ *be row vectors such that the following are true:*

i) $\mathbf{a} \nsim \pm\mathbf{a}'$ *and* $\mathbf{a}^- \nsim \pm\mathbf{a}'^-$*, and*
ii) either $\mathbf{b} \nsim \pm\mathbf{b}'$ *and* $\mathbf{b}^- \nsim \pm\mathbf{b}'^-$*, or* $\mathbf{b} = \mathbf{b}'$*.*

Then $\mathbf{a} \otimes \mathbf{b} \nsim \mathbf{a}' \otimes \mathbf{b}'$ *and* $(\mathbf{a} \otimes \mathbf{b})^- \nsim (\mathbf{a}' \otimes \mathbf{b}')^-$

4 A Secondary Construction from the Kronecker Product and 2-level Autocorrelation Sequences

In this section, we show a construction for CNC Hadamard matrices using the Kronecker product and 2-level autocorrelation sequences.

Let $\mathbf{u}$ and $\mathbf{v}$ be two 2-level autocorrelation sequences over $\mathbb{F}_2$ of period $N = 2^n - 1$ (they may be equal). Recall that R_N the back diagonal identity matrix of order N. Thus $\mathbf{v}R_N = (v_{N-1}, \cdots, v_1, v_0)$ is also a 2-level autocorrelation sequence, which is a shift of the reciprocal of $\mathbf{v}$ (see Property 1). For $p = 2$, recall the following notation

$$H(\mathbf{x}) = \begin{pmatrix} 1 & \mathbf{1} \\ \mathbf{1^T} & (-1)^{C(\mathbf{x})} \end{pmatrix}$$

where $C(\mathbf{x})$ is the circular matrix defined in Section 2.

Construction 3. Let I_k be the identity matrix of order k. Let

$$B = \begin{pmatrix} H(\mathbf{a}) & H(\mathbf{b}P) \\ H(\mathbf{a}) & -H(\mathbf{b}P) \end{pmatrix} \text{ where } \begin{cases} P = R_N & \text{for } \mathbf{a} \sim \mathbf{b} \\ P \in \{I_N, R_N\} & \text{for } \mathbf{a} \nsim \mathbf{b}. \end{cases}$$

Let A be a ± 1 matrix of order m. We define

$$H = A \otimes B.$$

Thus, B can be considered as the case that $A = (1)$ for $m = 1$.

Theorem 4. *Assume that either both* $\mathbf{a}$ *and* $\mathbf{b}$ *are shift-distinct quadratic sequences with* $P = I_N$ *or at least one of them is not a quadratic sequence with* $l(\mathbf{a}) + l(\mathbf{b}) < 2^{n-1} - 1$*. Then* B *is a CNC Hadamard matrices with order* 2^{n+1}*, and for two rows* $\mathbf{b}$ *and* $\mathbf{b}'$ *in* B*,* $\mathbf{b} \nsim \pm\mathbf{b}'$ *and* $\mathbf{b}^- \nsim \pm\mathbf{b}'^-$*.*

In order to prove Theorem 4, we need some properties of the quadratic residue sequences summarized in the following property.

Property 3. (a) If $\mathbf{a}$ is a binary 2-level autocorrelation sequence, then $l(\mathbf{a}) \leq 2^{n-1} - 1$. The upper bound is achieved by a quadratic residue sequence.

(b) There are only two shift-distinct quadratic residue sequences with period $N = 2^n - 1$ where N is a prime and $N \equiv 3 \pmod{N}$, say $\mathbf{a}$ and $\mathbf{b}$. Note that $\mathbf{a}$ and $\mathbf{b}$ are reciprocal. Thus, $\mathbf{b}$ can obtained from $\mathbf{a}$ by two methods, i.e., $b_0 = a_0 = 1$, and $b_i = a_i + 1$ or $b_i = a_{N-i}, i = 1, \cdots, N-1$. The crosscorrelation of $\mathbf{a}$ and $\mathbf{b}$ is bounded by 3. Thus $\mathbf{a} + L^k(\mathbf{b})$ has maximum $2^{n-1} - 3$ zeros in one period.

Proof of Theorem 4. We first need to prove the CNC property of B. However, a proof can be given in a similar way as the proof for Theorems 1- 2 where the length of zero runs in the investigated sequences are bounded by Property 3, we omit it here (the reader can find the proof in the full version of this work). Thus, B is a CNC Hadamard matrix and for any two rows $\mathbf{b}^-$ and $\mathbf{b}'^-$ in B^-, $\mathbf{b}^- \nsim \pm\mathbf{b}'^-$. Note that if there are two rows in B which are shift equivalent, then the overlapping patterns in those two rows have the length patterns by adding 1 or subtracting 1 in the case of the reduced form of B for which the zeros and their corresponding elements are excluded. Thus, a similar argument to prove the CNC property of B can be applied to this case. Thus, for two rows $\mathbf{b}$ and $\mathbf{b}'$ in B, $\mathbf{b} \nsim - \pm \mathbf{b}'$.

□

Remark 2. In [8], it is proved that B is a CNC Hadamard by using $\mathbf{b}R_N$ where $\mathbf{a}$ and $\mathbf{b}$ could be the same, and the bound for the linear span is shown to be $l(\mathbf{a}) + l(\mathbf{b}) + \max\{l(\mathbf{a}), l(\mathbf{b})\} \leq N \Longrightarrow l(\mathbf{a}) \leq N/3$ when $l(\mathbf{a}) = l(\mathbf{b})$. The result obtained in Theorem 4 is an improvement, since if $\mathbf{a} \nsim \mathbf{b}$, we could use both $\mathbf{b}$ and $\mathbf{b}R_N$, and the bound on the linear span is larger, i.e., $l(\mathbf{a}) \leq N/2$ when $l(\mathbf{a}) = l(\mathbf{b})$. Theorem 4 also shows that if both $\mathbf{a}$ and $\mathbf{b}$ are shift-distinct quadratic residue sequences with $P = I_N$, then the result is true without imposing any conditions on the linear span of the sequences.

Theorem 5. *With the notation in Construction 3, let A be a CNC Hadamard matrix of order $m > 1$ such that $\mathbf{u} \nsim \pm\mathbf{v}$ where $\mathbf{u}$ and $\mathbf{v}$ are any two rows from A. Then $H = A \otimes B$, as constructed in Construction 3, is a CNC Hadamard matrix with order $m2^{n+1}$.*

Proof. Let $\mathbf{e}$ and $\mathbf{d}$ be two different rows in B. From Theorem 4, $\mathbf{e} \nsim \pm\mathbf{d}$. From the construction of B in Construction 3, $\tilde{\mathbf{j}}$ is not a row in B. Thus for $m > 3$ both A and B satisfy the conditions in Theorem 3. Therefore, H is a CNC Hadamard matrix. Note that if $m = 3$, there are no Hadamard matrices [2].

For $m = 2$, we have $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. In this case, $H = A \otimes B = \begin{pmatrix} B & B \\ B & -B \end{pmatrix}$. For any two rows from H^-, if they are taken from the upper half of H^-, then they are shift distinct, since any two rows in B are shift distinct (similar arguments as that in the proof of Theorem 3). If one row from the upper half of H and the other from the lower half or both from then lower half then the argument can be proceeded similarly as the proofs Theorems 1-2, we omit it here due to the lack of space.

Thus H is a CNC Hadamard matrix.

5 Related Functions and LCZ Signal Sets

Let $q = p^n$ and $H = (\omega^{a_{ij}})$ be a CNC Hadamard matrix of order q constructed using one of the constructions in Sections 2 and 3, where ω is a pth primitive root of unity α. Let α be a primitive element in $\mathbb{F}_q$. We construct a family of functions from $\mathbb{F}_q$ to $\mathbb{F}_p$ as follows. For each $i = 0, \cdots, q-1$, let $f_i(\alpha^j) = a_{ij}, 0 \le j < q$ and $f_i(0) = 0$ (recall H is in the normal form). Then $S = \{f_i(x) \,|\, 1 \le i < q\}$ is a set consisting of $q-1$ functions which satisfy the three conditions listed in Section 1-C. In addition, S has maximum size.

Let $d = (q^m-1)/(q-1)$. According to the work in [5], we can construct LCZ signal sets with parameters $(q^m-1, q-1, 1, d)$ with maximum size as follows. A function $h(x)$, from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, is said to be *difference balanced* if for any $0 \neq \lambda \in \mathbb{F}_{q^m}$ and $a \in \mathbb{F}_q$, $h(x) - h(\lambda x) = a$ has q^{m-1} solutions in $\mathbb{F}_{q^m}$. We say that $h(x)$ is $\mathbb{F}_q$-*linear* if $h(ax) = ah(x)$. Let β a primitive element in $\mathbb{F}_{q^m}$, and $h(x)$ be a function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ with the difference balance property and $\mathbb{F}_q$-linear property. Let $g_i(x) = f_i(x) \circ h(x)$, for $1 \le i < q$ and where $\circ$ is the composition operator. Then the evaluation of $g_i(x)$ at β, denoted as $\mathbf{a}_i$, is a 2-level autocorrelation sequence over $\mathbb{F}_p$ with period q^m-1. The construction for 2-level autocorrelation sequences is referred to as *a subfield decomposition construction* in [4]. Hence $\mathcal{K} = \{\mathbf{a}_i \,|\, 1 \le i < q\}$ is an LCZ set with parameters $(q^m-1, q-1, 1, d)$. (Note. Here we replace the 2-tuple balance property for $h(x)$ in [5] by

the difference balance and F_q-linear.) All LCZ signal sets corresponding to CNC Hadamard matrices constructed from Construction 1 for $h > 1$, Construction 2, Construction 3 for $m > 1$ and the case employing quadratic sequences for $m = 1$, are new. In the cases from Construction 1 for $h = 1$ and Construction 3 for $m = 1$ give LCZ signal sets with the improved results.

6 Concluding Remarks

In this work, we present three new constructions for CNC Hadamard matrices. The first construction is obtained by alternating the column blocks and the flipped column blocks in the circular matrix generated by a 2-level autocorrelation sequence over $\mathbb{F}_p$. Then we have showed that the Kronecker product of two CNC Hadamard matrices A and B is still a CNC Hadamard matrix provided that the row shift-distinctness also holds in those two CNC Hadamard matrices and the alternating vector is not a row vector of either A or B. The third construction is given by a combination of the Kronecker product and the circular matrices generated by 2-level autocorrelation sequences. The first and third construction contain two known constructions in [8] as special cases, but with improved bounds for the restrictions on the linear spans of 2-level autocorrelation sequences and new cases. Note that the third known construction for CNC Hadamard matrices in the literature is presented in [5], which is not any special case of the three constructions obtained in this work.

It is worth to point out that for the binary case, there are other constructions for Hadamard matrices which also give CNC Hadamard matrices. For example, the Hadamard matrices from the Turyn construction [14] [15] [7] are CNC Hadamard matrices. This can be easily seen from the construction from many examples, but work is needed to write out the proof. We currently work on that. In general, the orders of those Hadamard matrices are not powers of 2. Note that the motivation for the investigation of the CNC property is for the constructions of a set consisting of 2^n functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ which satisfies that each function in the set is balanced, the sum of any two function is balanced, and any two functions, considered as sequences with period $2^n - 1$, are shift distinct. If the order of a CNC Hadamard matrix is not 2^n, then its corresponding function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is not balanced. Thus, those types of CNC Hadamard matrices cannot be used in the construction of low correlation zone sequences with parameters $(q^m - 1, q - 1, 1, \frac{q^m-1}{q-1})$ where $q = 2^n$. However, the problem itself is interesting theoretically.

Acknowledgement

The work was conducted when the first author was supported by the NSERC Undergraduate Research Scholarship in Spring 2008. The work is supported by NSERC Discovery Grant.

References

1. J.H. Chung and K.C. Yang. Design of m-ary low correlation zone sequence sets by interleaving. In S.W. Golomb, M.G. Parker, A. Pott, and A. Winterhof, editors, *Sequences and Their Applications - SETA 2008, 5th International Conference, Lexington, KY, USA, September 14-18, 2008, Proceedings*, volume 5203 of *Lecture Notes in Computer Science*, pages 313–321. Springer, 2008.
2. R. Craigen. Hadamard matrices and designs. In C. J. Colbourn and J. H. Dinitz, editors, *CRC Handbook of Combinatorial Designs*, pages 370–377. CRC Press, 1996.
3. R. De Gaudenzi, C. Elia, and R. Viola. Bandlimited quasi-synchronous cdma: A novel satellite access technique for mobile and personal communication systems. *IEEE Journal on Selected Areas in Communications*, 10(2):328–343, 1992.
4. S.W. Golomb and G. Gong. *Signal design for good correlation – for wireless communication, cryptography, and radar*. Cambridge University Press, Cambridge, 2005.
5. G. Gong, S.W. Golomb, and H.Y. Song. A note on low-correlation zone signal sets. *IEEE Trans. Inform. Theory*, 53(7):2575–2581, 2007.
6. K. Guo and G. Gong. New constructions of complete non-cyclic hadamard matrices, related function families and lcz sequences. *Technical Report, University of Waterloo, CACR 2010-14*, 2010.
7. W.H. Holzmann, H. Kharaghani, and B. Tayfeh-Rezaie. Williamson matrices up to order 59. *Des. Codes Cryptography*, 46(3):343–352, 2008.
8. Jang. J.W., J.S. No, H.B. Chung, and X.H. Tang. New sets of optimal p-ary low-correlation zone sequences. *IEEE Transactions on Information Theory*, 53(2):815–821, 2007.
9. S.H. Kim, J.W. Jang, J.S. No, and H.B. Chung. New constructions of quaternary low correlation zone sequences. *IEEE Transactions on Information Theory*, 51(4):1469–1477, 2005.
10. Y.S. Kim, J.W. Jang, J.S. No, and H.B. Chung. New design of low-correlation zone sequence sets. *IEEE Transactions on Information Theory*, 52(10):4607–4616, 2006.
11. B. Long, P. Zhang, and J. Hu. A generalized qs-cdma system and the design of new spreading codes. *IEEE Trans. Veh. Technol*, 47(6):1268–1275, 1998.
12. X.H. Tang and P.Z. Fan. A class of pseudonoise sequences over gf(p) with low correlation zone. *IEEE Transactions on Information Theory*, 47(4):1644–1649, 2001.
13. X.H. Tang and P. Udaya. New recursive construction of low correlation zone sequences. *Proceedings of Second Int. Workshop Sequence Design and Its Applications to Communication, Shimonoseki, Japan, Oct. 10-14*, 2005.
14. R.J. Turyn. An infinite class of williamson matrices. *J. Comb. Theory, Ser. A*, 12(3):319–321, 1972.

15. R.J. Turyn. Hadamard matrices, baumert-hall units, four-symbol sequences, pulse compression, and surface wave encodings. *J. Comb. Theory, Ser. A*, 16(3):313–333, 1974.
16. Z.C. Zhou, X.H. Tang, and G. Gong. A new class of sequences with zero or low correlation zone based on interleaving technique. *IEEE Trans. Inform. Theory*, 54(9):4267–4273, 2008.