Binary Sequence Pairs with Ideal Correlation and Cyclic Difference Pairs

Seok-Yong Jin

The Graduate School

Yonsei University

Department of Electrical and Electronic Engineering

Binary Sequence Pairs with Ideal Correlation and Cyclic Difference Pairs

by

Seok-Yong Jin

A Dissertation Submitted to the

Graduate School of Yonsei University

in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

Supervised by

Professor Hong-Yeop Song, Ph.D.

Department of Electrical and Electronic Engineering
The Graduate School

YONSEI University

June 2009

This certifies that the dissertation of
Seok-Yong Jin is approved.

Thesis Supervisor: Hong-Yeop Song

Kwang Soon Kim

Jang-Won Lee

Habong Chung

Dong-Joon Shin

The Graduate School
Yonsei University
June 2009

Contents

List of Figures

List of Tables

ABSTRACT

Binary Sequence Pairs with Ideal Correlation and Cyclic Difference Pairs

Seok-Yong Jin
Department of Electrical and Electronic Eng.
The Graduate School
Yonsei University

In this dissertation, we investigate the existence and properties of binary sequence pairs having a two-level correlation function, mostly focusing on the case where all the out-of-phase correlation values between two sequences are zero, which is called the ideal two-level correlation function. The cyclic difference pairs is introduced in association with binary sequences pairs having a two-level correlation function.

The multipliers of cyclic difference pairs are developed in a parallelled way from the theory of multipliers of cyclic difference sets. We define multipliers of cyclic difference pairs and present an existence theorem for multipliers, which can be applied for checking the nonexistence of certain cyclic difference pairs in question.

For ideal cyclic difference pairs, some necessary conditions are given. We construct a class of binary sequence pairs of period $v = 4u$ for every positive integer u, having ideal two-level correlation where their in-phase correlation coefficient is four. We verify

that the corresponding cyclic difference pairs have -1 as a multiplier.

We determine the nonexistence of some ideal cyclic difference pairs of small sizes by multiplier arguments. Together with an exhaustive computer search, we completely determine the existence of ideal cyclic difference pairs of periods up to 30. We verify that the ideal binary sequence pairs generated by the construction given in this dissertation are unique for period equal to or less than 30, under correlation preserving transformations.

We conjecture that if there exists a binary sequence pair with ideal two-level correlation then its in-phase correlation coefficient must be four. This implies so called the circulant Hadamard matrix conjecture.

Key words : Ideal two-level correlation, Cyclic difference pair, Cyclic Hadamard difference pair, Cyclic difference set, Cyclic Hadamard difference set, Multiplier, Hadamard matrix

Chapter 1

Introduction

Wide range of communication systems usually require signals with good correlation properties. We consider binary sequence pairs with an ideal periodic correlation function, which could be viewed as a kind of generalization from binary sequences having good correlation characteristic. They have in close connection with such structures as binary matrices including Hadamard matrices and cyclic difference sets.

This introductory chapter consists as follows. In Section 1.1 we review general correlation property required for signals in communication systems. Some formal definitions are presented. As a motivation, in Section 1.2 we introduce the topic described above in terms of binary circulant matrices, cyclic difference sets, and polynomials with binary coefficients. Some existence problem known as circulant Hadamard matrix conjecture might be a reason why we take into account pairs of sequences instead of single sequences with desired correlation property. In Section 1.3 we briefly summarize previous works. The remaining sections are for overview and notations.

1.1 Correlation property required for signals in communication systems

Communication systems in many cases require sets of signals which have the following properties [63]:

1. each signal in the set is easy to distinguish from the time shifted version of itself.

2. each signal in the set is easy to distinguish from (the possibly time-shifted version of) every other signal in the set.

The followings are generally known [22, 23, 25, 27, 49, 63]. The signals with the first property is said to have a good auto-correlation property and they are important for such applications as ranging, radar, and spread-spectrum communication systems [69]. The set of signals with the second property is said to have a good cross-correlation property and it is important for simultaneous ranging to several targets, multiple-terminal system identification, and code-division multiple-access (CDMA) communication system.

According to applications, some systems prefer signals with good periodic correlation properties and some other systems require signals with good non-periodic correlation characteristic. Both are related in some manner, and generally signals with good aperiodic correlation property gives signals with good periodic correlation property [1]. When we restrict to periodic signals, it can be shown that [63] the mean-squared difference between continuous time signal $x(t)$ and $y(t)$ leads to the following definition of the periodic correlation function $\theta_{x,y}(\cdot)$ between the sequences $\mathbf{x} = (x_i)$ and $\mathbf{y} = (y_i)$

[1] Jedwab [40] reports that Richard Turyn started his work [75] in the purpose of constructing binary signals with best non-periodic correlation properties known as Barker sequences, and obtained a seminal result on the nonexistence of binary signals with the perfect periodic correlation property.

of period v

$$\theta_{x,y}(\tau) = \sum_{i=0}^{v-1} x_i y_{i+\tau},$$

where the subscript takes modulo v. When the symbol set is the binary symbol $\{0, 1\}$, the periodic correlation function between $(0, 1)$-sequences $\mathbf{a} = (a_i)$ and $\mathbf{b} = (b_i)$ of period v is defined as

$$\theta_{a,b}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i + a_{i+\tau}}. \tag{1.1}$$

If two sequences $\mathbf{a}$ and $\mathbf{b}$ are identical, their correlation function is denoted by $\theta_a(\tau)$ and called an auto-correlation function.

Then the design of signal sets with the property described at the beginning can be reduced to the problem of finding the sets of periodic sequences with the following properties:

1. for each sequence (x_i) of period v in the set, $|\theta_{x,x}(\tau)|$ is as small as possible for $1 \leq \tau \leq v - 1$

2. for each pair of sequences (x_i) and (y_i), $|\theta_{x,y}(\tau)|$ is as small as possible for all τ.

Generally, the set of sequences with low cross-correlation values are generated from the sequences with well-described auto-correlation property by some tradeoff between auto-correlation values and cross-correlation values. For example, Gold [21] and Kasami [45, 46] made sets of sequences with low cross-correlation values from the maximal length sequences, frequently abbreviated as m-sequences or PN-sequences which can be generated conveniently from linear feedback shift regsters [23, 27, 72]. There has been large amount of research for the construction of signal sets with favourable cross-correlation

properties from sequences with good auto-correlation function, such as m-sequences and Sidel'nikov sequences [68]. See a survey article by Helleseth and Kumar [39], Helleseth [38], and the chapter by Golomb and Gong [27, Chapter 10]. For Gold sequences, see [8], and for Kasami set of sequence, see [47].

In (1.1), $\theta_{a,b}(\tau)$ for all nonzero $\tau = 1, \ldots, v-1$ are called the out-of-phase or off-peak correlation coefficients, while $\theta_{ab}(0)$ is called the in-phase correlation. Hence the in-phase auto-correlation value equals always the period, peak value which is maximum possible. The most important property possessed by PN-sequences which leads to the construction of signal sets with good cross-correlation values might be the fact that they have a *flat* out-of-phase auto-correlation coefficients. Since $\theta_a(0) = v$ always, such sequences are said to have a two-level correlation function.

Definition 1.1 A binary $(0,1)$-sequence $\mathbf{a} = (a_i)$ of period v is said to have a *two-level auto-correlation function* if its correlation function $\theta_a(\tau)$ is such that

$$\theta_a(\tau) = \begin{cases} v & \tau \equiv 0 \pmod{v}, \\ \gamma(\neq v) & \text{otherwise.} \end{cases}$$

When the absolute value of γ is relatively small compared with the in-phase value v, the sequence itself finds many useful applications in communications, navigation, and synchronization. Of course such sequence could be used for the construction of sets of sequences with good cross-correlation property, as mentioned. Hence, a binary sequence having the two-level correlation with $\gamma = 0$ is said to have *ideal* two-level correlation function and such sequence is just called the *perfect* or *ideal* sequence. Unfortunately there is a strong evidence (Theorem 2.3) that there are no perfect sequences except for a trivial case of period four. Instead, there is a rich class of examples with $\gamma = -1$

including m-sequences, so balanced binary sequences with $\gamma = -1$ are also called to have an ideal two-level auto-correlation. These points are explained in Chapter 2.

The concept of the perfect ideal auto-correlation could be generalized to a *pair* of binary sequences, which is a topic of this dissertation.

Definition 1.2 A *pair* $(\mathbf{a}, \mathbf{b})$ of binary sequences $\mathbf{a} = (a_i)$ and $\mathbf{b} = (b_i)$ of the same length v is said to have a *two-level correlation function* if

$$\theta_{a,b}(\tau) = \begin{cases} \Gamma_1 & \tau \equiv 0 \pmod{v} \\ \Gamma_2 (\neq \Gamma_1) & \text{otherwise.} \end{cases}$$

If $\Gamma_2 = 0$, $(\mathbf{a}, \mathbf{b})$ is said to be a binary sequence pair with *perfect* or *ideal* two-level correlation [17, 77]. ■

With some abuse of language, we just call such sequence pair with $\Gamma_2 = 0$ as an *ideal* sequence pair.

1.2 Motivation by means of related problems

1.2.1 Binary circulant matrices

Let $\mathbf{a} = (a_i)_{i=0}^{v-1}$ be a binary $(0, 1)$-sequence with a two-level correlation function where the out-of-phase correlation value is γ. If we constitute the circulant matrix M_a of zeros and ones associated with $\mathbf{a}$, i.e., whose first row is $\mathbf{a}$, then it is easy to know that

$$M_a M_a^T = pI + qJ$$

for some integers p and q, where I is the identity matrix and J is the matrix of all ones of order v. For an ideal case with $\gamma = 0$, if we consider a binary $(+1, -1)$-sequence $\alpha = (\alpha_i)$ defined by $\alpha_i = (-1)^{a_i}$, then we know that

$$M_\alpha M_\alpha^T = vI. \tag{1.2}$$

A binary square matrix satisfying (1.2) is called a Hadamard matrix. Specifically, a v by v $(+1, -1)$ matrix H such that $HH^T = vI$ is called a Hadamard matrix of order v. Hadamard matrices satisfy Hadamard's determinant inequality with equality [66] and hence have maximum determinant. They have many applications: for constructing simplex codes [73] and for Hadamard transforms [54], only mention a few. Hadamard matrices exist for infinitely many orders and there have been known various constructions [9, 66]. However, research over last fifty years has failed to determine the existence of Hadamard matrices which are *circulant*: it has been believed that there is no circulant Hadamard matrix of order greater than 4 and there is a strong evidence that this is true, but the existence determination is still open and known as circulant Hadamard matrix conjecture. See Section 2.2 of Chapter 2.

In summary, if we have a single binary sequence of period v having a two-level correlation function then we have a circulant Hadamard matrix of order v and vice versa, as shown in (1.2). Since neither a circulant solution to the matrix equation (1.2) nor a proof for the nonexistence has been found if $v > 4$, it would be a natural question to ask whether there exists a pair of circulant matrices satisfying (1.4) instead of (1.3) and to

ask what properties they have if they turns out to exist.

$$MM^T = vI \tag{1.3}$$

$$MN^T = vI \tag{1.4}$$

1.2.2 Cyclic difference sets and pairs

Now let us define a set $A := \{0 \leq i \leq v-1 : a_i = 1\}$ for a given $(0,1)$-binary sequence $\mathbf{a}$ of period v having a two-level auto-correlation function. If we view A as a subset of $\mathbb{Z}_v$, the integers modulo v, then A must have some combinatorial regularity, forced by the fact that $\mathbf{a}$ has a two-level auto-correlation function. A subset with such regularity is called a cyclic difference set. Historically, it is believed [43] that difference sets were first introduced by Singer [70] in 1938 from a study of finite projective geometry, but their systematic study started with the fundamental 1947 paper [34] by M. Hall, Jr. who introduced the important concept of multipliers. Finally, Bruck [6] initiated the investigation of difference sets in general groups. The extensive presentation of cyclic difference sets could be found in Baumert [2], and difference sets in general (abelian) groups in Chapter VI of Beth, Jungnickel and Lenz [5]. There are also a series of surveys given by Jungnickel [42], by Jungnickel and Pott [43], by Arasu and Pott [1], and by Jungnickel, Pott, and Smith [44]. For a quick start, the short chapter of Ryser's monograph [62] could be recommended.

Likewise, for a given binary sequence pair $(\mathbf{a}, \mathbf{b})$ with a two-level correlation function, we may define a set pair (A, B) in the same way. Again, the fact that $\mathbf{a}$ and $\mathbf{b}$ have a two-level correlation function enforces some combinatorial regularity on the pair

(A, B). In this dissertation we call such pairs as "cyclic difference pairs" and investigate binary sequence pairs with a two-level correlation function in terms of "cyclic difference pairs."

1.2.3 Polynomials with binary coefficients

The correlation profile of given sequences could be conveniently expressed in terms of polynomials. Let $p(z) = \sum_{i=0}^{v-1} a_i z^i$ and $q(z) = \sum_{i=0}^{v-1} b_i z^i$ be the Hall polynomials associated with the sequences $\mathbf{p} = (p_i)$ and $\mathbf{q} = (q_i)$ of period v, where z is indeterminate. Then it is easily checked that

$$p(z)q(z^{-1}) \equiv \theta_{pq}(0) + \sum_{\tau=1}^{v-1} \theta_{pq}(\tau) z^{v-\tau} \pmod{z^v - 1}, \tag{1.5}$$

where $q(z^{-1}) = q_0 + z^v \left(q_1 z^{-1} + \ldots q_{v-1} z^{-(v-1)}\right)$ is called the reciprocal of $q(z)$. Hence, if we have an ideal binary sequence pair $(\mathbf{a}, \mathbf{b})$ with the out-of-phase correlation value $\Gamma_2 = 0$ and the in-phase correlation Γ_1, then we have a solution to

$$p(z)q(z) \equiv r \pmod{z^v - 1}$$

with $p(z) = a(z)$, $q(z)$ being the reciprocal of $b(z)$, and $r = \Gamma_1$.

1.3 Previous works

In [17] some elementary properties of perfect binary sequence pairs of length being a power of 2 are given, including their Walsh-Hadamard transforms. In [77] the intuitive

"uniqueness" of binary sequence pairs with a two-level correlation is shown: if $(\mathbf{a}, \mathbf{b})$ and $(\mathbf{a}, \mathbf{c})$ are binary sequence pairs having the same two-level correlation function with $\Gamma_1 > \Gamma_2$ then $\mathbf{b}$ and $\mathbf{c}$ are identical. A class of binary sequence pairs having two-level correlation with $v = 2n^2 - 1$, $\Gamma_1 = 2n^2 - 8n + 11$ and $\Gamma_2 = 2n^2 - 8n + 7$ is constructed in [77], which is not perfect at all. Observe the difference between Γ_1 and Γ_2 in this construction is 4.

Li, Gao and Zhao [52] have shown an example of binary sequence pair with ideal two-level correlation of period 8, and they generate a set of pairs of zero correlation zone [16, 32] (ZCZ) sequences using Gong's interleaved structure [29, 30]. When their set of ZCZ sequence pairs is applied to synchronous CDMA systems [15], it shows [52] slightly better performance at high signal to noise ratio compared to the system with Gold sequences. However, the example of ideal binary sequence pair appeared in [52] has no explanation on how it is constructed.

For radar applications, on the other hand, Golomb [24] investigated two sequences with perfect correlation. Here, the pair of sequences is not necessarily over the binary alphabet.

1.4 Overview

In Chapter 2 we consider binary sequences having a two-level auto-correlation function with small out-of-phase correlation coefficients. They are closely related to cyclic difference sets and cyclic Hadamard matrices. We explain such relation and some basic

properties of cyclic difference sets including the concept of multipliers. Such relation and properties will be generalized in a parallel way to the case of pairs of binary sequences in Chapter 3. We also briefly summarize known results concerning the construction and existence of cyclic difference sets and cyclic Hadamard matrices, thereby binary sequences with ideal two-level auto-correlation function.

In Chapter 3 we consider a *pair* of binary sequences having a two-level correlation function. Such pairs of sequences are closely related to "cyclic difference pairs" as mentioned. This relation could be an analogy of the relation between binary sequences with a two-level auto-correlation function and cyclic difference sets, and it enables one to use the terms "binary sequence pairs with two-level correlation" and "cyclic difference pairs" interchangeably. We will focus mostly on the case where the out-of-phase correlation coefficient is zero, that is, *ideal* sequence pairs.

1.5 Notations

We define some notations to be used in the remaining of this thesis. Let $\mathbf{s} = (s_0, s_1, \ldots, s_{v-1})$, $s_i \in \{0, 1\}$, be a binary sequence with period v. Its support set $supp(\mathbf{s})$ is defined by $S = \{i : s_i = 1\} \subset [v] := \{0, 1, \cdots, v-1\}$. Then $\mathbf{s}$ is called the characteristic sequence of S. We define the following, where the subscripts of the sequence are taken modulo v, and $|S|$ and/or $\#S$ denotes the number of elements of a finite set S.

- Weight: $wt(\mathbf{s}) = \#\{i : s_i = 1, 0 \le i \le v-1\} = |S|$.

- Cyclic shift: $\rho^{(j)}(\mathbf{s}) = (s_j, s_{j+1}, \cdots, s_{j+v-1})$. The support set of $\rho^{(j)}(\mathbf{s})$ is denoted by $j + S := \{j + s \pmod v : s \in S\}$.

- d-Decimation: $\mathbf{s}^{(d)} = \left(s_{d\cdot 0}, s_{d\cdot 1}, \ldots, s_{d\cdot(v-1)}\right)$. The support set of $\mathbf{s}^{(d)}$ is denoted by $dS := \{ds \pmod v : s \in S\}$.

- Negation: $\mathbf{s}' = \left(s'_0, \ldots, s'_{v-1}\right)$, where $s'_i = s_i + 1 \pmod 2$. The support set of $\mathbf{s}'$ is denoted by $S^C := [v] \backslash S$.

- Even-position negation: $\mathbf{s}_E = (u_0, \ldots, u_{v-1})$, $u_i = s'_i$ if i is odd, and $u_i = s_i$ if i is even, for all $i = 0, 1, \ldots, v-1$. The support set of $\mathbf{s}_E$ is denoted by S_E.

- Polynomial representation: The sequence $\mathbf{s}$ is sometimes represented by associated Hall polynomial $s(z) = s_0 + s_1 z^1 + \ldots + s_{v-1} z^{v-1} \pmod{z^v - 1}$.

- Associated circulant matrix: $M_s = (m_{ij})$, where $m_{ij} = s_{i-j \pmod v}$, $i, j = 0, \ldots, v-1$.

$$M_s = \begin{bmatrix} s_0 & s_{v-1} & s_{v-2} & \cdots & s_1 \\ s_1 & s_0 & s_{v-1} & \cdots & s_2 \\ s_2 & s_1 & s_0 & \cdots & s_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{v-1} & s_{v-2} & s_{v-3} & \cdots & s_0 \end{bmatrix}.$$

  Then the sequence $\mathbf{s}$ is called the defining array of M_s.

Chapter 2

Cyclic Difference Sets, Binary Sequences and Their Correlation Properties

2.1 Binary sequences with two-level auto-correlation and cyclic difference sets

Let $\mathbf{a} = (a_i)_{i=0,\ldots,v-1}$ be a binary sequence having a two-level correlation function

$$\theta_a(\tau) = \begin{cases} v & \tau \equiv 0 \pmod{v}, \\ \gamma(\neq v) & \text{otherwise.} \end{cases} \tag{2.1}$$

Let $A := supp(\mathbf{a})$ and $k := wt(\mathbf{a})$. The auto-correlation function of a binary sequence just counts the number of agreements of the sequence with its translate by a shift of τ minus the number of disagreements, $\theta_a(\tau)$ is determined by the difference function

$$d_A(\tau) = |A \cap (\tau + A)|,$$

where $\tau + A = \{\tau + i \pmod{v} : i \in A\}$. In particular, $d_A(0) = k$ and $\theta_a(0) = v$. For $\tau \not\equiv 0 \pmod{v}$, by counting how many times 1's of $\mathbf{a}$ coincide with those in $\rho^{(\tau)}(\mathbf{a})$, we have

$$\theta_a(\tau) = v - 4\left(k - d_A(\tau)\right). \tag{2.2}$$

Since $\mathbf{a}$ has a two-level correlation function, $d_A(\tau)$ is some fixed constant regardless of τ. Put this as λ, that is,

$$d_A(\tau) = \lambda, \forall \tau \not\equiv 0 \pmod{v}. \tag{2.3}$$

From (2.1) and (2.2) we have

$$\gamma = v - 4(k - \lambda). \tag{2.4}$$

The support set A of a binary sequence with two-level auto-correlation, viewed as a k-subset of $\mathbb{Z}_v$, always satisfies the condition (2.3), and is called a cyclic difference set. The following is a formal definition of a cyclic difference set, drawn from [62].

Definition 2.3 (Cyclic Difference Set) Let $D = \{d_1, d_2, \ldots, d_k\}$ be a k-set of integers modulo v such that every $a \not\equiv 0 \pmod{v}$ can be expressed in exactly λ ways in the form

$$d_i - d_j \equiv a \pmod{v},$$

where d_i and d_j are in D. We suppose further that

$$0 < \lambda < k < v - 1. \tag{2.5}$$

The inequality (2.5) serves only to exclude certain degenerate configurations. A set D fulfilling these requirements is called a *cyclic difference set* (CDS) with parameters v, k, and λ. ■

A cyclic difference set with parameters v, k, and λ can be defined not only in a cyclic group (integers mod v) but in any group of order v. The equivalent definition [43] is as

follows. Let G be an additively written group of order v, and D a k-subset of G. Then D is called a (v, k, λ)-difference set if its list of differences, that is

$$\Delta D = \{d - d' : d, d' \in D, d \neq d'\}$$

contains each non-zero element of G precisely λ times. If G is cyclic (abelian, non-abelian, repspectively), D is likewise called cyclic (abelian, non-abelian, respectively). Any group G contains *trivial* difference sets, namely ϕ, $\{g\}$, $G\backslash\{g\}$ and G, each of them does not satisfy the inequality (2.5), where g is an arbitrary element of G. A further important parameter is the *order* $n := k - \lambda$ of D. Sometimes we write the parameters in the form $(v, k, \lambda; n)$ in order to emphasize the importance of the order n.

Although there are extensive developments in the theory of difference sets in a general group, we are interested only in cyclic difference sets exclusively in this thesis due to the well known correspondence between binary sequences with a two-level auto-correlation function and cyclic difference sets. For example, we have Theorem 2.1.

Theorem 2.1 (Jungnickel and Pott [43]) Let $\mathbf{a}$ be a periodic binary sequence with period v and with weight k, such that $\mathbf{a}$ has a two-level auto-correlation function with all the out-of-phase correlation coefficients equal to γ. Then

$$D := \{g \in \mathbb{Z}_v : a_g = 1\},$$

where we identify $\mathbb{Z}_v$ with the integers 0, 1, ..., $v - 1$, is a cyclic (v, k, λ)-difference set, where

$$\gamma = v - 4(k - \lambda) = v - 4n.$$

Moreover, any cyclic difference set arises in this way. ■

Example 2.1 Let $D = \{0, 5, 7, 10, 11, 13, 14\}$ be a 7-subset of $\mathbb{Z}_{15}$. Then D is a $(15, 7, 3)$-CDS. Each nonzero element of $\mathbb{Z}_{15}$ is written as differences modulo 15 in three ways:

$$1 = 0 - 14 = 11 - 10 = 14 - 13, \qquad 2 = 0 - 13 = 7 - 5 = 13 - 11,$$

$$3 = 10 - 7 = 13 - 10 = 14 - 11, \qquad 4 = 0 - 11 = 11 - 7 = 14 - 10,$$

$$5 = 0 - 10 = 5 - 0 = 10 - 5, \qquad 6 = 5 - 14 = 11 - 5 = 13 - 7,$$

$$7 = 5 - 13 = 7 - 0 = 14 - 7, \qquad 8 = 0 - 7 = 7 - 14 = 13 - 5,$$

$$9 = 5 - 11 = 7 - 13 = 14 - 5, \qquad 10 = 0 - 5 = 5 - 10 = 10 - 0,$$

$$11 = 7 - 11 = 10 - 14 = 11 - 0, \qquad 12 = 7 - 10 = 10 - 13 = 11 - 14,$$

$$13 = 5 - 7 = 11 - 13 = 13 - 0, \qquad 14 = 10 - 11 = 13 - 14 = 14 - 0.$$

The characteristic binary sequence $\mathbf{a} = (a_i) = (100001010011011)$ of period 15 and weight 7, given by $a_i = 1$ if $i \in D$ and $a_i = 0$ if $i \notin D$, is shown in Figure 2.1. Observe that $\mathbf{a}$ is balanced and is a maximal length sequence of period $2^4 - 1$, in fact. ■

By counting the number of differences of ΔD in two ways we have an immediate necessary condition for the existence of a cyclic difference set, and equivalently of a binary sequence with two-level auto-correlation.

$$\lambda(v - 1) = k(k - 1) \tag{2.6}$$

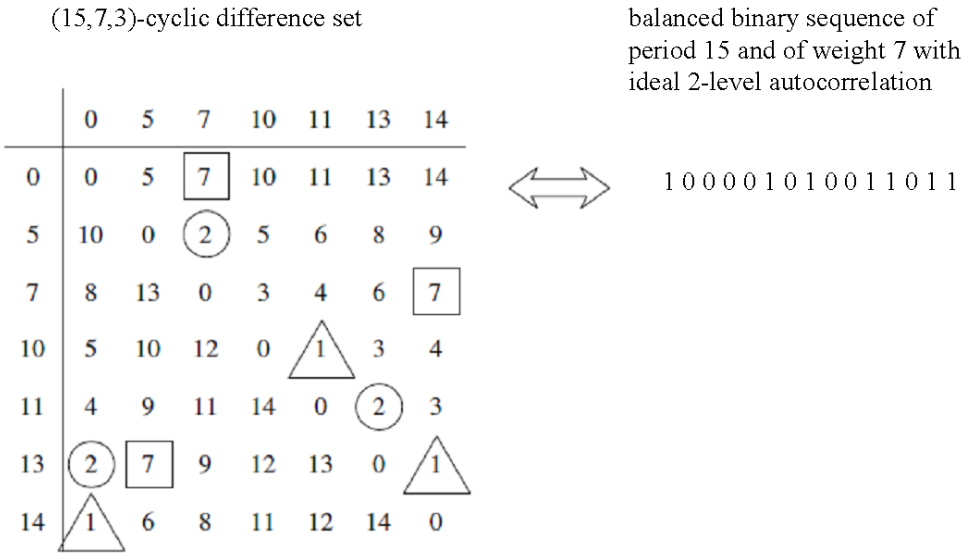

Figure 2.1: $(15, 7, 3)$-cyclic difference set and the corresponding characteristic binary sequence

2.2 Ideal binary sequences and cyclic Hadamard difference sets

We mention the two most interesting cases, namely perfect sequences with $\gamma = 0$ and $\gamma = -1$, which are in connection with cyclic Hadamard matrices.

2.2.1 The case with $\gamma = 0$ and circulant Hadamard matrices

From (2.4) and (2.6) we have $v = 4n$ and $4n\lambda = (\lambda + n)^2 - n$. As a consequence n is a square and we write the parameters in the form

$$(v, k, \lambda; n) = (4u^2, 2u^2 - u, u^2 - u; u^2) \tag{2.7}$$

In fact we take the case with $2k \leq v$ out of two possibilities, it is due to the fact that the complement set $D^C := G \backslash D$ in a group G is again a $(v, v-k, v-2k+\lambda; n)$-difference set in G with the same order n, if D is a (v, k, λ)-difference set.

Difference sets with their parameters given as (2.7) are called Hadamard difference sets. In this thesis, a Hadamard difference set in a cyclic group is called a *circulant Hadamard difference set*. Let $\mathbf{a} = (a_i)_{i=0,\ldots,v-1}$ be the characteristic binary sequence of a circulant Hadamard difference set. Then it is obvious that the real vector $\underline{\alpha} = (\alpha_i)$ and all its cyclic shifts constitute row vectors of a circulant Hadamard matrix, where $\alpha_i = (-1)^{a_i}$. Conversely the support set of any row vector of circulant Hadamard matrix is a circulant Hadamard difference set, where the elements of row vector are properly converted to 0 and 1.

The only known circulant Hadamard difference set is the trivial $(4, 1, 0)$-difference

set. Its characteristic binary sequence (0001) gives a circulant Hadamard matrix

$$H_4 = \begin{bmatrix} - & + & + & + \\ + & - & + & + \\ + & + & - & + \\ + & + & + & - \end{bmatrix}.$$

Indeed, it is widely believed that this is the only example.

Conjecture 2.1 (Circulant Hadamard Matrix Conjecture) There is no nontrivial circulant Hadamard difference set. Equivalently, there is no perfect binary sequence with all out-of-phase correlation coefficients being zero and period greater than 4. ■

This simply stated conjecture has been standing more than fifty years since early 1960's [62], and there is even an article [53] that considers wrong "proofs" of this conjecture. There have been two significant results toward this conjecture. Turyn in his 1965 paper [75] showed by "size arguments" that if a $(4u^2, 2u^2 - u, u^2 - u)$-circulant Hadamard difference set exists then u *must be odd* and the circulant Hadamard matrix conjecture is true for $u < 55$ [75, 76]. Some decades later, Schmidt [64] overcome the the limit of self-conjugacy and obtain the exponent bound (Theorem 2.2) and correspondingly the best known result (Theorem 2.3) up to now:

Theorem 2.2 (Schmidt [64]) If there is a Hadamard difference set in a cyclic group of order $v = 4u^2$ then $F(v,u)^2/\varphi\left(F(v,u)\right) \geq v$, where $\varphi(\cdot)$ is the euler totient function and $F(m,n)$ is defined as below. ■

Definition 2.4 (Schmidt [64]) Let m, n be positive integers, and let $m = \prod_{i=1}^{t} {p_i}^{c_i}$ be

the prime power decomposition of m. For each prime divisor q of n let

$$m_q := \begin{cases} \prod_{p_i \neq q} p_i & \text{if } m \text{ is odd or } q = 2 \\ 4 \prod_{p_i \neq 2,q} p_i & \text{otherwise} \end{cases}.$$

Let $\mathcal{D}(n)$ be the set of prime divisors of n. We define $F(m,n) = \prod_{i=1}^{t} p_i^{b_i}$ to be the minimum multiple of $\prod_{i=1}^{t} p_i$ such that for every pair (i,q), $i \in \{i, \ldots, t\}$, $q \in \mathcal{D}(n)$, at least one of the following conditions is satisfied.

(a) $q = p_i$ and $(p_i, b_i) \neq (2,1)$,

(b) $b_i = c_i$,

(c) $q \neq p_i$ and $q^{ord_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_1+1}}$. ■

Theorem 2.3 (Schmidt [64]) There is no circulant Hadamard matrix of order v in the range $4 < v \leq 10^{11}$ with the possible exceptions of $v = 4u^2$ with $u \in \{165, 11715, 82005\}$.

■

2.2.2 The case with $\gamma = -1$ and cyclic Hadamard matrices

From (2.4) and (2.6) we have $v = 4n-1$ and $\lambda(4n-1) = (\lambda+n)^2 - n$, and hence the parameters take the form

$$(v, k, \lambda; n) = (4n-1, 2n-1, n-1; n) \tag{2.8}$$

Difference sets with their parameters given as (2.8) are called Payley-Hadamard difference sets. In particular, cyclic difference sets of this type are called cyclic Hadamard difference sets (CHDSs), and the corresponding characteristic binary sequences, which are *balanced* and hence useful for various applications, are just called Hadamard sequences in the literature [27, 72]. The naming is from the fact that one may construct

a cyclic Hadamard matrix of order $v+1=4n$ using an Hadamard sequence of period $v=4n-1$ as follows: Let $\underline{\alpha}$ be a Hadamard sequence of period v whose entries are converted to $+1$ and -1. We compose a $v \times v$ circulant matrix M whose rows are exactly $\underline{\alpha}$ and its cyclic shifts, and then add the border, a vector of $+1$'s, to the top row and leftmost column of M to obtain a square matrix of order $v+1$. Then we have a cyclic Hadamard matrix of order $v+1=4n$.

Unlike circulant Hadamard difference sets with parameters (2.7), Payley-Hadamard cyclic differense sets and consequently Hadamard sequences exist in abundance. See Chapter 8 and 9 of [27] for details. They are known to exist for period v by the following constructions.

- $v=p$ is a prime congruent to $3 \pmod 4$: Quadratic residue (Legendre symbol) construction [23, 27] and Hall's sextic residue construction [35] whenever p is a prime of the form $p=4x^2+27$,
- $v=p(p+2)$ is a product of twin primes: Jacobi symbol construction [74],
- $v=2^m-1$: In this case various constructions are now available.

Up to now, it is known that no other periods allow Hadamard sequences. It is verified [4, 28, 41, 50, 71] up to $v<10000$, except for the following 7 cases: 3439, 4355, 8591, 8835, 9135, 9215, 9423.

The existence and classification problem for Hadamard sequences of period $v=2^m-1$ and correspondingly Payley-Hadamard cyclic difference sets with parameters of the form

$$v=2^m-1, k=2^{m-1}-1, \text{ and } \lambda=2^{m-2}-1 \tag{2.9}$$

is an another topic of much interest. The classical constructions include:

- Singer difference sets [70] and maximal length sequences [23, 27];
- Gordon, Mills and Welch difference sets [33] and GMW sequences [65], cascaded GMW sequences [51], generalized GMW sequences [10, 30], whenever m is a composite number;
- Quadratic residue sequences whenever $v = 2^m - 1$ itself is a Mersenne prime, Hall's sextic residue sequences whenever $2^m - 1$ is a prime of the form $4x^2 + 27$, and Jacobi symbol construction whenever $2^m - 1$ is a product of twin primes;

In addition to the constructions listed above, various Hadamard sequences have been newly founded since the mid of 1990's. They include:

- Multiple trace term sequences including 3-term and 5-term sequences [13, 61] and their Welch-Gong sequences [27];
- Maschietti's hyperoval construction [56] from Segre hyperoval [67] and Glynn Type I and Type II hyperovals [19];
- Kasami power function construction [12–14, 60];

Moreover, it is known that there exists a method such as iterative decimation Hadamard transform [27, 31], which convert a given cyclic Hadamard sequences to another (possibly unknown) Hadamard sequences. There is some optimism that all the constructions which yield cyclic Hadamard sequences are now known [26], but this has not been proved. Cyclic difference sets with parameters (2.9) have been completely classified

up to $m \leq 10$: for $m = 7$ by Baumert [2, 3], for $m = 8$ by Cheng [7], for $m = 9$ by Kim and Song [48], and lastly for $m = 10$ by Gaal and Golomb in 2000 [18]. In 2006 Golomb and Gong state [27] that exhaustive computer searches to find all cyclic Hadamard sequences of period $2^m - 1$ are not feasible for any $m \geq 11$[1].

2.3 Multipliers of cyclic difference sets

Since the concept of multipliers has been first introduced into the study of difference sets by Marshall Hall, Jr. in 1947 [34], it has provided a powerful technique for the derivation of both existence and nonexistence theorems. Let $D = \{d_1, d_2, \ldots, d_k\}$ be a (v, k, λ)-cyclic difference set. Obviously $s+D := \{s+d_1, s+d_2, \ldots, s+d_k\}$, which is called a *translate* or *shift* of D, is again a cyclic difference set with the same parameters, where the addition is taken modulo v. It is easily checked that $tD := \{td_1, td_2, \ldots, td_k\}$ is also a cyclic difference set with the same parameters, if t is coprime with v. For two cyclic difference sets D and $D' = \{d'_1, d'_2, \ldots, d'_k\}$ with the same parameters v, k, and λ, if tD and $s + D'$ are the same k-subsets of $\mathbb{Z}_v$, then it is natural to define D and D' as the same/equivalent difference set.

Definition 2.5 (Multiplier of CDS) Let D be a (v, k, λ)-cyclic difference set. If there exist an integer t relatively prime to v satisfying

$$tD = s + D,$$

[1] In 2006 Golomb reported that exhaustive computer searches for $m = 11$ and $m = 12$ had been on-going [26].

for some arbitrary integer s, then t is called a *multiplier* of D, where $s + D = \{s + d \pmod{v} : d \in D\}$ and $tD = \{td \pmod{v} : d \in D\}$ and we take the equality in the sense that tD and $s + D$ are the same k-subsets of $\mathbb{Z}_v$. If $tD = D$ we say that D is *fixed* by the multiplier t. ■

We always have the trivial multiplier $t = 1$. It is easily checked that the set of multipliers of a cyclic difference set form a multiplicative group, which is called the *multiplier group* of the difference set. Here are some results concerning the fix structure of the multiplier group. The following two lemmas were originally stated for abelian difference sets in their original form in McFarland and Mann [57], but we state them with a restriction to cyclic difference sets. It is known that the second lemma is due to Marshall Hall, Jr. We shall extend the second lemma to the case of cyclic difference pairs in chapter 3.

Lemma 2.1 (McFarland and Mann [57]) Let D be a (v, k, λ)-cyclic difference set, and let t be a multiplier of D. Then there is at least one translate $s + D$ which is fixed by t. ■

Lemma 2.2 (Hall) Let D be a (v, k, λ)-cyclic difference set, where k is relatively prime to v. Then there is an integer s such that $s + D$ is fixed by every multiplier. ■

One has the following much stronger result due to McFarland and Rice [58].

Theorem 2.4 (McFarland and Rice [58]) Every cyclic difference set has a translate fixed by all its multipliers. ■

As a corollary to this, we have Theorem 2.5, just quoted from [5, Theorem VI.2.9].

Theorem 2.5 Let D be a (v, k, λ)-cyclic difference set, and let t be a multiplier of D. Assume without loss of generality that D is fixed by t. Then D is a union of cyclotomic cosets with respect to t modulo v. Hence, k is a sum of some coset sizes. ■

In order to apply the preceding results, one need results which guarantee the existence of some multipliers for difference sets whose existence are not yet known. The first seminal result (Theorem 2.6) which rely only on the parameters of the difference sets in question was originally proved for cyclic difference sets with $\lambda = 1$ by Hall [34] and later extended to the case of general λ in the form stated in Theorem 2.6 by Hall and Ryser [37]. For completeness we just state one more important result (Theorem 2.7) of the same type, which was initially obtained for general (abelian) difference sets by Menon [59].

Theorem 2.6 (First multiplier theorem by Hall and Ryser) Let D be a (v, k, λ)-cyclic difference set, and let p be a prime dividing $n = k - \lambda$ but not v. If $p > \lambda$, then p is a multiplier of D. ■

Theorem 2.7 (Second multiplier theorem by Menon) Let D be a (v, k, λ)-cyclic difference set, and let $d > \lambda$ be a divisor of $n = k - \lambda$ with $\gcd(d, v) = 1$. Moreover, let t be an integer such that for each prime p dividing d there exists an integer j with $t \equiv p^j \pmod{v}$. Then t is a multiplier of D. ■

Corollary 2.1 ([43]) Let D be a (v, k, λ)-cyclic difference set and assume that $n = k - \lambda$ is a power of a prime p not dividing v. Then p is a multiplier for D. ■

For circulant Hadamard difference sets, these multiplier theorems are meaningless, since it is transparent that the parameters of a non-trivial $(4u^2, 2u^2 - u, u^2 - u)$-CDS, even if it exists, do not give a prime divisor of $n = u^2$ which is coprime with $v = 4u^2$. However for Hadamard-Paley cyclic difference sets, above multiplier thorems are extremely useful. We observe that if n is a prime then every $(v, k, \lambda) = (4n - 1, 2n - 1, n - 1)$ Hadamard-Paley CDS has always its order n as a multiplier by Theorem 2.6. In particular, $n = 2^m - 2$ is a multiplier of $(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$-CDS by Theorem 2.6. Moreover, 2 is a multiplier by Corollary 2.1. The exhaustive search of Hadamard sequences of period $2^m - 1$, summarized in previous section, would not be feasible without this fact.

In summary, all known example of cyclic (moreover abelian) difference sets admit every prime divisor p of n as a multiplier, regardless whether or not $p > \lambda$ [43], but the question as to whether it is always true is open and leads to the major conjecture on multipliers of difference sets.

Conjecture 2.2 (Multiplier conjecture [43]) Every prime divisor of the order n of a $(v, k, \lambda; n)$-abelian difference set is a multiplier. In other words, Theorem 2.6 holds without the assumption $p > \lambda$. ■

We conclude this chapter with an example illustrating the role of multipliers for the existence/nonexistence of certain cyclic difference sets in question.

Example 2.2 (a) If a $(15, 7, 3)$-CDS D exists, then 2 has to be a multiplier of D and it

is a union of cyclotomic cosets below, by Theorem 2.5.

$$C_0 = \{0\}, C_1 = \{5, 10\}, C_2 = \{1, 2, 4, 8\}, C_3 = \{3, 6, 12, 9\}, C_4 = \{7, 14, 13, 11\}$$

Since the size of D is 7, it must be a union of the form $C_0 \cup C_1 \cup C_i$ for some $i \in \{2, 3, 4\}$. $D = C_0 \cup C_1 \cup C_4$ is indeed a $(15, 7, 3)$-CDS fixed by 2, which was given in Example 2.1. The characteristic binary sequence $\mathbf{a} = (100001010011011)$ of D has the property $a_i = a_{2i}$ for all i, and we say that $\mathbf{a}$ is in characteristic phase.

(b) Similarly, if a $(31, 10, 3)$-CDS D exists then 7 has to be a multiplier. Since 31 is prime, there are only two cosets modulo 31 with respect to 7, namely $C_0 = \{0\}$ and $C_1 = \mathbb{Z}_{31} \backslash \{0\}$. Since C_1 has more than 10 elements, no $(31, 10, 3)$-CDS can exist.

Chapter 3

Cyclic Difference Pairs and Binary Sequence Pairs with Ideal Correlation Properties

We consider a pair of two (not necessarily distinct) binary sequences of arbitrary (but fixed) period with a two-level correlation function. In Section 3.1, we explain the relation between such sequences pairs and cyclic difference pairs which are defined in this chapter. Due to the one-to-one correspondence between them, one could use the terms "binary sequence pairs with two-level correlation" and "cyclic difference pairs" interchangeably. It is shown that the concept of multipliers of cyclic difference sets can also be generalized to cyclic difference pairs. We define a multiplier of cyclic difference pairs, and then we generalize results of cyclic difference sets to cyclic difference pairs in a parallel way: an existence theorem of multipliers and results concerning the fix structure of the multiplier group of a given cyclic difference pair are established.

From Section 3.2 on, we will focus mostly on ideal case where the out-of-phase correlation coefficient is zero. Some necessary conditions for the existence of ideal cyclic

difference pairs are obtained. In Section 3.3, we construct a class of ideal cyclic difference pairs with special parameters, which corresponds to a class of binary sequence pairs whose in-phase correlation coefficient is 4 and all the out-of-phase correlation values are zero. We observe some properties of those pairs. In Section 3.4, we apply the multiplier theorem given in Section 3.1 to prove the nonexistence of certain ideal cyclic difference pairs in question. By an exhaustive computer search for short periods, we verify that up to periods less than or equal to 30 there is no other perfect binary sequence pair than the one generated by the construction in Section 3.3.

3.1 Structure and properties of binary sequence pairs and associated cyclic difference pairs

Let $\mathbf{a} = (a_i)$ and $\mathbf{b} = (b_i)$ be binary $\{0, 1\}$ sequences of length v having a two-level periodic correlation function

$$\theta_{a,b}(\tau) = \begin{cases} \Gamma(\neq \gamma) & \tau \equiv 0 \pmod{v}, \\ \gamma & \text{else.} \end{cases} \tag{3.1}$$

Let $A := supp(\mathbf{a})$, $B := supp(\mathbf{b})$, and $k_a := wt(\mathbf{a})$, $k_b := wt(\mathbf{b})$, and $k := |A \cap B|$. It is well known that the correlation between $\mathbf{a}$ and $\mathbf{b}$ are determined by the difference function

$$d_{A,B}(\tau) = |A \cap (\tau + B)|,$$

where $\tau + B = \{\tau + i \pmod{v} : i \in B\}$. By counting how many times 1's in the

sequence $\mathbf{a}$ coincide with those in $\mathbf{b}$ shifted by τ, we have

$$\theta_{a,b}(\tau) = v - 2\,(k_a + k_b) + 4d_{A,B}(\tau). \tag{3.2}$$

By definition, $d_{A,B}(0) = |A \cap B|$ equals to k. Since $\theta_{a,b}(\tau)$ is a some fixed constant for all nonzero τ, so is $d_{A,B}(\tau)$. Put this as λ, that is,

$$d_{A,B}(\tau) = \lambda, \forall \tau = 1, \ldots, v-1. \tag{3.3}$$

From (3.1) and (3.2), we have

$$v - 2\,(k_a + k_b) + 4k = \Gamma, \tag{3.4}$$

and

$$v - 2\,(k_a + k_b) + 4\lambda = \gamma. \tag{3.5}$$

Comparing (3.4) and (3.5), we have

$$\Gamma - \gamma = 4(k - \lambda).$$

If we count all differences $x - y$, $x \in A$ and $y \in B$, we have from (3.3)

$$k_a k_b = \lambda(v-1) + k, \tag{3.6}$$

which is an immediate necessary condition for the existence of a binary sequence pair having a two level correlation.

Generally, the support sets of a pair of binary sequences having a two-level correlation function always satisfies a kind of condition like (3.3), and this leads to the following definition of a cyclic difference pair.

Definition 3.1 (Cyclic difference pair) Let X and Y be (not-necessarily distinct) k_x-subset and k_y-subset of $\mathbb{Z}_v$, respectively. Let $|X \cap Y| = k$. Then the pair (X, Y) is called an $(v, k_x, k_y, k, \lambda)$-*cyclic difference pair* (CDP) if, for every nonzero $w \in \mathbb{Z}_v$, w can be expressed in exactly λ ways in the form $w = x - y \pmod{v}$, where $x \in X$ and $y \in Y$. In particular, when $v - 2(k_x + k_y) + 4\lambda = 0$ and $k \neq \lambda$, it is called an *ideal* cyclic difference pair. ■

We summarize the association with binary sequence pairs having a two-level correlation function and cyclic difference pairs as Theorem 3.1.

Theorem 3.1 (One-to-one Correspondence) Let $(\mathbf{a}, \mathbf{b})$ be a binary sequence pair with period v, $A = supp(\mathbf{a})$, $B = supp(\mathbf{b})$, $wt(\mathbf{a}) = k_a$, $wt(\mathbf{b}) = k_b$, and $k = |A \cap B|$. Then, $(\mathbf{a}, \mathbf{b})$ has a two-level correlation function if and only if the associated support set pair (A, B) is a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair, where the in-phase correlation coefficient Γ and out-of-phase correlation coefficients γ of $(\mathbf{a}, \mathbf{b})$ satisfy the relation (3.4) and (3.5), respectively.

We say that $(\mathbf{a}, \mathbf{b})$ is the *characteristic binary sequence pair* of a given $(v, k_a, k_b, k, \lambda)$-cyclic difference pair (A, B). We say in particular the pair $(\mathbf{a}, \mathbf{b})$ or (A, B) is ideal if $\gamma = 0$.

A cyclic difference pair can be described in terms of associated polynomials as well as circulant matrices.

Proposition 3.1 Let A be a k_a-subset and B a k_b-subset of $\mathbb{Z}_v$ such that $|A \cap B| = k$. Let $\mathbf{a}$ and $\mathbf{b}$ be the characteristic binary sequence of A and B, respectively. Denote the

associated Hall polynomial of $\mathbf{a}$ and $\mathbf{b}$ by $a(z)$ and $b(z)$, respectively. Then, (A, B) is a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair if and only if

$$a(z)b(z^{-1}) \equiv (k-\lambda) + \lambda(1 + z + \cdots + z^{v-1}) \pmod{z^v - 1}. \tag{3.7}$$

Proof: We calculate the product as

$$a(z)b(z^{-1}) \equiv \sum_{\tau=0}^{v-1} d_{A,B}(\tau) z^{v-\tau} \pmod{z^v - 1}.$$

The substitution of $d_{A,B}(\tau = 0) = k$ and $d_{A,B}(\tau \neq 0) = \lambda$ completes the proof.

Proposition 3.2 Assume the same notation in Proposition 3.1. Let M_a and M_b be the associated circulant matrix of $\mathbf{a}$ and $\mathbf{b}$, respectively. Then, (A, B) is a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair if and only if

$$M_a {M_b}^T = (k-\lambda)I + \lambda J,$$

where I is the identity matrix of order v and J is the $v \times v$ matrix of all 1's, and ${M_b}^T$ denotes the transpose of M_b.

Proof: Observe that the (i, j) element m_{ij} of $M_a {M_b}^T$ for $0 \leq i, j \leq v-1$ is the ordinary dot product of the i-th row of M_a and the j-th row of M_b. Therefore, $m_{ij} = d_{A,B}(j-i)$, where $j - i$ is taken mod v.

Corollary 3.1 Assume that a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair (A, B) exists. Let $(\mathbf{a}, \mathbf{b})$ be the corresponding characteristic binary sequence pair, and let M_a and M_b be the associated circulant matrices of $\mathbf{a}$ and $\mathbf{b}$, respectively. Then,

$$\det(M_a {M_b}^T) = \det(M_a) \cdot \det(M_b) = k_a k_b (k-\lambda)^{v-1}, \tag{3.8}$$

where $\det(M_a)$ and $det(M_b)$ respectively denotes the determinant of M_a and M_b.

Proof: We take the matrix $(k-\lambda)I + \lambda J$ and apply some elementary column and row operations to make it lower triangular form [62, p. 99]. Then it follows that $\det\big((k-\lambda)I + \lambda J\big) = (k+(v-1)\lambda)(k-\lambda)^{v-1}$.

Now we introduce some transformations which convert a given CDP to another. They are closely related to general correlation-preserving transformations [20]. For an ideal binary sequence pair of period being a power of two, Proposition 3.3 was partially presented in [17]. However, it is obvious that these transforms can be applied to any CDPs: not only ideal but arbitrary CDPs, and CDPs with no restrictions on period at all. We state Proposition 3.3 in terms of cyclic difference pairs rather than using sequence notations, and we specify the parameters of the transformed cyclic difference pairs.

Proposition 3.3 Let (A, B) be a $(v, k_a, k_b, k, \lambda)$-CDP.

1. $(\tau + A, \tau + B)$ is a $(v, k_a, k_b, k, \lambda)$-CDP for all $\tau = 0, 1, \cdots, v-1$.

2. (dA, dB) is a $(v, k_a, k_b, k, \lambda)$-CDP, where d is an integer relatively prime to v.

3. (B, A) is a $(v, k_b, k_a, k, \lambda)$-CDP.

4. (A, B^C) is a (v, k_a, $v-k_b$, k_a-k, $k_a-\lambda$)-CDP, and (A^C, B) is a (v, $v-k_a$, k_b, k_b-k, $k_b-\lambda$)-CDP, where $A^C = \mathbb{Z}_v \backslash A$ and $B^C = \mathbb{Z}_v \backslash B$.

5. (A^C, B^C) is a $(v, v-k_a, v-k_b, k', \lambda')$-CDP, where $k' = k + v - (k_a + k_b)$ and $\lambda' = \lambda + v - (k_a + k_b)$.

The proof is straightforward. In fact, we have one more transformation which can be applied to only ideal CDPs. We present it later in Section 3.2.

3.1.1 Multipliers of cyclic difference pairs

In Chapter 2 we see that the concept of multipliers plays an important role in the development of difference set theory. We can define a multiplier of cyclic difference pairs in a similar way.

Definition 3.2 Let (A, B) be a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair. If there exist an integer t relatively prime to v such that $(tA, tB) = (s + A, s + B)$ for some integer s, we say that t is a multiplier of the cyclic difference pair (A, B). If $s = 0$ we say that (A, B) is fixed by the multiplier t. It is easily checked that the set of multipliers of a cyclic difference pair form a multiplicative group.

Theorem 3.2 (Multiplier theorem for CDP) Let (A, B) be a cyclic difference pair with parameters v, k_a, k_b, k, and λ. Let p be a prime divisor of $k - \lambda$ and suppose that $p \nmid v$ and $p > \lambda$. Then p is a multiplier of (A, B).

Proof: We want to show that for some integer s,

$$\big(a(z^p), b(z^p)\big) = \big(z^s a(z), z^s b(z)\big),$$

that is, $a(z^p) \equiv z^s a(z) \pmod{z^v - 1}$ and $b(z^p) \equiv z^s h_b(z) \pmod{z^v - 1}$.

Since (A, B) is a CDP we have, by proposition 3.1,

$$a(z)b(z^{-1}) \equiv (k - \lambda) + \lambda T(z) \pmod{z^v - 1},$$

where $T(z) = 1 + z + \cdots + z^{v-1}$. By hypothesis $p \mid k - \lambda$ and $p \nmid v$. If $p \mid k_a$ then $p \mid k_a k_b = \lambda v + (k - \lambda)$ and hence $p \mid \lambda$, whereas $p > \lambda$. Thus $p \nmid k_a$, and $p \nmid k_b$ by the

same way.

$$k_a^{p-1} = k_b^{p-1} = 1 \pmod{p}.$$

We now multiply this equation by $a(z)^{p-1}$, and apply the fact that $f(z)T(z) = f(1)T(z) \pmod{z^v - 1}$ for an arbitrary polynomial $f(z)$ with integral coefficients. Then the resulting expression is in the form

$$a(z^p)b(z^{-1}) = \lambda T(z) + pR(z) \pmod{z^v - 1},$$

where $R(z)$ is a polynomial with integral coefficients. In fact, $p > \lambda$ implies that $R(z)$ has nonnegative integral coefficients. Next we multiply this equation by $a(z)$ and we have

$$(k - \lambda)a(z^p) = pR(z)a(z) \pmod{z^v - 1}.$$

Since all coefficients of $R(z)$ are nonnegative integers $R(z)$ cannot have more than one non-vanishing term. Hence, we have

$$a(z^p) = a(z)z^{s_a}, \tag{3.9}$$

for some integer s_a.

Since (B, A) is also a CDP with the same parameters k and λ by Proposition 3.3, we have in this time

$$b(z)a(z^{-1}) \equiv (k - \lambda) + \lambda T(z) \pmod{z^v - 1},$$

and it follows that for some integer s_b

$$b(z^p) \equiv b(z)z^{s_b} \pmod{z^v - 1}. \tag{3.10}$$

Again by Proposition 3.3 (pA, pB) is also a CDP with the same parameters of (A, B). Since the polynomial pair associated to (pA, pB) is $\big(a(z^p), b(z^p)\big)$, we use Proposition 3.1 and above two relations (3.9) and (3.10) to write down

$$\begin{aligned}(k-\lambda)+\lambda T(z) &\equiv a(z^p)b(z^{-p}) \pmod{z^v-1}\\ &\equiv z^{s_a-s_b}a(z)b(z^{-1}) \pmod{z^v-1}.\end{aligned}$$

Thus $s_a - s_b \equiv 0 \pmod{v}$. Putting $s_a = s_b = s$ concludes the proof. ■

In order to apply Theorem 3.2 for checking the existence/nonexistence of certain CDPs in question, we extend some of the results concerning the fix structure of CDSs given in Chapter 2. In the following, Lemma 3.1 is from Hall's lemma (Lemma 2.2), and Theorem 3.3, a CDP-version of Theorem 2.5, is useful for checking the non-existence of certain CDPs.

Lemma 3.1 Let (A, B) be a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair where either k_a or k_b is relatively prime to v. Then there is an integer $0 \le s < v$ such that the translate $(s + A, s + B)$ is fixed by every multiplier.

Proof: Assume without loss of generality k_a is prime to v. Write $A = \{a_1, \ldots, a_{k_a}\}$, where $a_i \in \mathbb{Z}_v$, $i = 1, \ldots, k_a$. Since k_a is prime to v there is exactly one $s \in \mathbb{Z}_v$ satisfying

$$a_1 + \ldots + a_{k_a} + sk_a \equiv 0 \pmod{v}.$$

For any multiplier t of (A, B), we have $\big(t(s+A), t(s+B)\big) = \big(s'+A, s'+B\big)$ for a suitable integer $0 \leq s' < v$, and especially $t(s+A) = s'+A$. Then we have

$$\begin{aligned} 0 &= t(a_1 + \ldots + a_{k_a} + sk_a) \\ &= t\big((s+a_1) + \ldots_+ (s+a_{k_a})\big) \\ &= (s'+a_1) + \ldots + (s'+a_{k_a}) \\ &= a_1 + \ldots + a_{k_a} + s'k_a, \end{aligned}$$

where all the equalities hold mod v. Therefore $s'k_a \equiv sk_a \pmod{v}$, hence $s' = s$. ■

Theorem 3.3 Let (A, B) be an $(v, k_a, k_b, k, \lambda)$-cyclic difference pair such that either k_a or k_b is relatively prime to v. Let t be a multiplier of (A, B) and assume without loss of generality that (A, B) is fixed by t. Then both A and B are unions of cyclotomic cosets with respect to t modulo v. Hence, k_a is a sum of some of the coset sizes, and so is k_b. ■

3.2 Necessary condition for the existence of ideal cyclic difference pairs

For the existence of an ideal $(v, k_a, k_b, k, \lambda)$-CDP or an ideal binary sequence pair with $\gamma = 0$, we have

$$v - 2(k_a + k_b) + 4\lambda = 0, \tag{3.11}$$

and hence

$$\Gamma = 4(k - \lambda). \tag{3.12}$$

The relation (3.11) shows obviously that v *must be even* for the existence of ideal pairs. Moreover, (3.11) and (3.6) limit the values of k_a and k_b as a solution to the quadratic equation

$$x^2 - (v/2 + 2\lambda)x + \lambda v + (k - \lambda) = 0. \tag{3.13}$$

We will further investigate the consequences of (3.13) in Theorem 3.4. Using (3.11) and (3.6) again we know

$$(v - 2k_a)(v - 2k_b) = 4(k - \lambda). \tag{3.14}$$

Due to Proposition 3.3 we assume without loss of generality $v/2 \geq k_a \geq k_b \geq k$. Since $\Gamma \neq 0$ by definition, we can assume by (3.12) and (3.14)

$$v/2 > k_a \geq k_b \geq k > \lambda$$

when we refer to a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair in the remaining. If $\lambda = 0$, since $k = k_a k_b \geq k_a$ by (3.6) and $k \leq k_a$ by definition, then we have $k_a = k_b = k = 1$ and hence, $v = \Gamma = 4$ by (3.11) and (3.12). It is interesting to see that if there is an ideal cyclic difference pair (A, B) with $\lambda = 0$ then $A = B$ and it degenerates to a circulant Hadamard difference set. One trivial example $\mathbf{a} = \mathbf{b} = (0001)$ is at the same time the only *known* characteristic sequence of $(4u^2, 2u^2 - u, u^2 - u)$-cyclic Hadamard difference set as we mentioned in Chapter 2.

In the case of the cyclic Hadamard difference set assuming it exists, one may count the number of 1's at the even and odd positions of the characteristic binary sequence. For an ideal cyclic difference pair we have a similar relation. Let (A, B) be an ideal CDP. Let e_a and e_b be the number of even integers which belong to A and B respectively.

Then by evaluating (3.7) at $z = -1$, we have

$$(k_a - 2e_a)(k_b - 2e_b) = k - \lambda. \tag{3.15}$$

In addition to the transformations of Proposition 3.3 we have one more transformation which can be applied to only ideal CDPs.

Proposition 3.4 Let (A, B) be an ideal $(v, k_a, k_b, k, \lambda)$-CDP and $(\mathbf{a}, \mathbf{b})$ the corresponding characteristic binary sequence pair. Let $(\mathbf{a}_E, \mathbf{b}_E)$ be the even-position negated pair of $(\mathbf{a}, \mathbf{b})$. We denote by A_E and B_E the support set of $\mathbf{a}_E$ and $\mathbf{b}_E$ respectively. Then (A_E, B_E) is an ideal $(v, k''_a, k''_b, k'', \lambda'')$-CDP with the parameters $k''_a = k_a + (v/2 - 2e_a)$, $k''_b = k_b + (v/2 - 2e_b)$, $k'' = k + (v/2 - (e_a + e_b))$ and $\lambda'' = \lambda + (v/2 - (e_a + e_b))$.

Proof: For arbitrary two binary sequences $\mathbf{p}$ and $\mathbf{q}$ of the same length, $\theta_{\mathbf{p_E},\mathbf{q_E}}(\tau) = (-1)^\tau \theta_{\mathbf{p},\mathbf{q}}(\tau)$. Since $\theta_{\mathbf{a_E},\mathbf{b_E}}(\tau) = 0$ for all $\tau \not\equiv 0 \pmod{v}$, we have

$$\theta_{\mathbf{a_E},\mathbf{b_E}}(\tau) = \theta_{\mathbf{a},\mathbf{b}}(\tau), \tag{3.16}$$

for all $\tau = 0, 1, \ldots, v-1$. The fact that $(\mathbf{a_E}, \mathbf{b_E})$ is an ideal binary sequence pair means (A_E, B_E) is also an ideal CDP by Theorem 3.1. The weights k''_a and k''_b are easily obtained by counting the number of 1's and 0's in even and odd positions of $\mathbf{a}$ and $\mathbf{b}$, respectively. Then by (3.16) for $\tau = 0$ we have $v - 2(k''_a + k''_b) + 4k'' = v - 2(k_a + k_b) + 4k$, and hence we determine k'' as in the statement. λ'' is determined similarly. ■

We remark that the parameter $n := k - \lambda$ plays an important role in the characterization of $(v, k_a, k_b, k, \lambda)$-CDP likewise (v, k, λ)-CDS, as shown in (3.7), (3.8), (3.14), and (3.15). Sometimes we use $(v, k_a, k_b, k, \lambda; n)$ notation if it is clearer.

Theorem 3.4 (Parameterization) For a given $n = k - \lambda > 0$, if there exists an ideal $(v, k_a, k_b, k, \lambda; n)$-cyclic difference pair, then v must be even, and it has parameters as follows.

(a) When $v = 0 \pmod 4$, $k_a + k_b$ is even, and necessarily $n \not\equiv 2 \pmod 4$. For some positive integer u we have

$$(v, k_a, k_b, k, \lambda) = (4u, 2u - l + m, 2u - l - m, u - l + n, u - l),$$

where $l > m \geq 0$ are the integers such that $n = l^2 - m^2$, and $u \geq n + m$.

(b) When $v \equiv 2 \pmod 4$, $n = k - \lambda$ is necessarily even and $k_a + k_b$ is odd. For some positive integer u, we have

$$(v, k_a, k_b, k, \lambda) = (4u + 2,\ 2u + 1 - l + m,\ 2u - l - m,\ u - l + n,\ u - l),$$

where $l > m \geq 0$ are the integers satisfying $4n = (2l + 1)^2 - (2m + 1)^2$, that is $n = (l + m + 1)(l - m)$, and $u \geq n + m$.

Proof: The fact that v must be even comes from (3.11). We recall that k_a and k_b are the integer roots of the quadratic equation (3.13). If $v \equiv 0 \pmod 4$, put $v = 4u$ for some $u \geq 1$. Since the discriminant of (3.13) is an integer square, we have $n = (u - \lambda)^2 - m^2$ for some integer $m \geq 0$. Since n is a difference between two squares, $n \not\equiv 2 \pmod 4$. If $(u - \lambda) = \sqrt{n + m^2}$, put $u - \lambda = l$ and we have λ and k as in the theorem. Then, the remaining parameters k_a and k_b are given as in the statement by solving (3.13) under the assumption of $k_a \geq k_b$. It is easy to check the case with $(u - \lambda) = -\sqrt{n + m^2}$ results in the complement of the CDP assumed in the theorem. Since $k_b \geq k$, we have $u \geq n + m$. The case of $v \equiv 2 \pmod 4$ can be done similarly. ■

Example 3.1 We list the parameters of some ideal $(v, k_a, k_b, k, \lambda)$-CDPs for small $n = k - \lambda$, assuming they exist. If $v \equiv 0 \pmod 4$, we have

- $n = 1, (l, m) = (1, 0)$: $(4u,\ 2u-1,\ 2u-1,\ u,\ u-1)$, $u \geq 1$,
- $n = 3, (l, m) = (2, 1)$: $(4u,\ 2u-1,\ 2u-3,\ u+1,\ u-2)$, $u \geq 4$,
- $n = 4, (l, m) = (2, 0)$: $(4u,\ 2u-2,\ 2u-2,\ u+2,\ u-2)$, $u \geq 4$,
- $n = 5, (l, m) = (3, 2)$: $(4u,\ 2u-1,\ 2u-5,\ u+2,\ u-3)$, $u \geq 7$,
- $n = 7, (l, m) = (4, 3)$: $(4u,\ 2u-1,\ 2u-7,\ u+3,\ u-4)$, $u \geq 10$.

With $v \equiv 2 \pmod 4$ we have

- $n = 2, (l, m) = (1, 0)$: $(4u+2,\ 2u,\ 2u-1,\ u+1,\ u-1)$, $u \geq 2$,
- $n = 4, (l, m) = (2, 1)$: $(4u+2,\ 2u,\ 2u-3,\ u+2,\ u-2)$, $u \geq 5$,
- $n = 6$: We have two possibilities

  1) $(l, m) = (5, 0)$: $(4u+2,\ 2u-1,\ 2u-2,\ u+4,\ u-2)$, $u \geq 6$,

  2) $(l, m) = (7, 2)$: $(4u+2,\ 2u,\ 2u-5,\ u+3,\ u-3)$, $u \geq 8$. ■

3.3 Ideal cyclic difference pairs with $k - \lambda = 1$

We consider ideal cyclic difference pairs with $k - \lambda = 1$, the smallest possible value for $k - \lambda$. In this case, the in-phase correlation coefficient Γ of the associated binary

sequence pair is constant regardless of the period, that is

$$\Gamma = 4(k - \lambda) = 4.$$

Among the list in Example 3.1, the case where $k - \lambda = 1$ is quite interesting. Observe that the parameter set $(v, k_a, k_b, k, \lambda; n) = (4u, 2u - 1, 2u - 1, u, u - 1; 1)$ is similar to those of $(v, k, \lambda; n) = (4u - 1, 2u - 1, u - 1; u)$-CDS of Hadamard-Paley type. In this sense, we call an ideal $(v, k_a, k_b, k, \lambda)$-CDP with $k - \lambda = 1$ as a cyclic Hadamard difference pair (CHDP). A special case of Theorem 3.4 for $k - \lambda = 1$ could be summarized as:

Corollary 3.2 If an ideal $(v, k_a, k_b, k, \lambda)$-CDP with $k - \lambda = 1$ and $v/2 \geq k_a \geq k_b \geq k > \lambda$ exists, then the followings hold:

1. The in-phase and out-of-phase correlation coefficient of the characteristic binary sequence pair is given as $\Gamma = 4$ and $\gamma = 0$, respectively.

2. $(v, k_a, k_b, k, \lambda) = (4u, 2u - 1, 2u - 1, u, u - 1)$ for some positive integer $u \geq 1$ and either $e_a = e_b = u - 1$ or $e_a = e_b = u$.

Proof: The only thing to show is the values e_a and e_b. They come from (3.15). ■

We now explain how to construct an ideal CDP of length $v = 4u$ and $n = k - \lambda = 1$. As we mentioned in Chapter 1, there are some examples of ideal binary sequence pairs of period being small powers of 2. The following construction is a full generalization.

Theorem 3.5 Let $v = 4u$ and $k_a = k_b = 2u - 1$ for an arbitrary integer $u \geq 2$. We define k_a-subset A and k_b-subset B of $\mathbb{Z}_v$ as

$$A = \{0, 1, \ldots, 2u - 2\}$$

and

$$B = 2u + A_E,$$

where A_E is the support set of the even-position negation of the characteristic binary sequence of A. Then (A, B) is a cyclic Hadamard difference pair with parameters $v = 4u$, $k_a = k_b = 2u - 1$, $k = u$, $\lambda = u - 1$ (and hence $n = k - \lambda = 1$). When $v = 4$ with $u = 1$, the pair degenerates to a single set $A = B = \{0\} \subset \mathbb{Z}_4$, which is a trivial $(4, 1, 0)$-cyclic Hadamard difference set, corresponding to the 4×4 circulant Hadamard matrix.

Proof: Obviously $|A| = |B| = 2u - 1$. It is enough to show that

$$a(z)b(z^{-1}) \equiv 1 + (u-1)(1 + z^1 + \cdots + z^{4u-1}) \pmod{z^{4u} - 1}. \tag{3.17}$$

Equivalently we need to show that (3.17) holds for every complex v-th root of unity. The case of $a(1)b(1)$ and $a(-1)b(-1)$ are easily checked. Now for any complex v-th root of unity ω with $\omega^2 \neq 1$, we have

$$a(\omega) \equiv 1 + \omega^1 + \cdots + \omega^{2u-2} = \frac{1 - \omega^{2u-1}}{1 - \omega},$$

and

$$\begin{aligned} b(\omega) &= (1 + \omega^{2u+1})\big(\omega^{0\cdot 2} + \omega^{1\cdot 2} + \cdots + \omega^{(u-2)\cdot 2}\big) + \omega^{(u-1)\cdot 2} \\ &= (1 + \omega^{2u+1}) \cdot \frac{1 - \omega^{2(u-1)}}{1 - \omega^2} + \omega^{2(u-1)} = \frac{(1 - \omega^{-1})(1 + \omega^{2u+1})}{1 - \omega^2}. \end{aligned}$$

Therefore

$$a(\omega)b(\omega^{-1}) = \frac{1 - \omega^{2u-1}}{1 - \omega} \cdot \frac{(1 - \omega)(1 + \omega^{2u-1})}{1 - \omega^{-2}} = 1,$$

which is equal to the right hand side of (3.17) evaluated at $z = \omega$ over the complex field.

Example 3.2 For $v = 20$, consider two subsets $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and $B = \{0, 2, 4, 6, 8, 11, 13, 15, 17\}$ of $\mathbb{Z}_{20}$. Then the pair (A, B) is a $(20, 9, 9, 5, 4; 1)$-CHDP. The corresponding characteristic binary sequence pair $(\mathbf{a}, \mathbf{b})$ given by

$$\begin{aligned} \mathbf{a}: &\quad 1111111110\ 0000000000 \\ \mathbf{b}: &\quad 1010101010\ 0101010100 \end{aligned}$$

has ideal two-level correlation such that $\theta_{a,b}(0) = 4$ and $\theta_{a,b}(\tau) = 0$ for all $\tau \not\equiv 0 \pmod{20}$. ■

It is not hard to show the followings are true in general for cyclic Hadamard difference pairs generated by Theorem 3.5.

Remark 3.1 Let (A, B) be the ideal CDP of length $v = 4u$, $u \geq 1$, given by the construction in Theorem 3.5. Then

(a) $A_E = 2u + B$ and $B_E = 2u + A$, and therefore $(A_E, B_E) = \big(2u + B, 2u + A\big)$.

(b) $\big((-1)A, (-1)B\big) = \big((2u + 2) + A, (2u + 2) + B\big)$.

(c) The translate $\big((1 - u) + A, (1 - u) + B\big)$ is fixed by the multiplier -1. ■

The construction in Theorem 3.5 is the result of the following observation:

Proposition 3.5 Let (A, B) be a CHDP with parameters $v = 4u$ and $k_a = k_b = 2u - 1$, generated by Theorem 3.5. Let (M_a, M_b) be the associated pair of circulant matrices. Then

$$\det(M_a) = \det(M_b) = 2u - 1.$$

Proof: The characteristic roots of a v by v circulant matrix over the complex field are determined by evaluating the Hall polynomial of its defining array at complex v-th roots

of unity [11, 55]. Since $a(1) = k_a = 2u - 1$ and $a(z) = (1 - z^{k_a})/(1 - z)$ for $z \neq 1$, we have

$$\begin{aligned}\det(M_a) &= \prod_{i=0}^{v-1} a(\epsilon^i) = (2u-1)\prod_{i=1}^{v-1} a(\epsilon^i) \\ &= (2u-1)\frac{(1-\epsilon^{k_a\cdot 1})\cdots(1-\epsilon^{k_a\cdot(v-1)})}{(1-\epsilon^1)\cdots(1-\epsilon^{v-1})} = (2u-1),\end{aligned}$$

where ϵ is a complex primitive v-th root of unity, and the last equality is due to the fact that $k_a = 2u - 1$ is relatively prime to $v = 4u$.

In order to calculate $\det(M_b)$, first we let

$$a(z) = a_0(z) + a_1(z)$$

where $a_0(z) = \sum_{i=0}^{v/2-1} a_{2i} z^{2i}$ is the even component of $a(z)$ and $a_1(z) = \sum_{i=0}^{v/2-1} a_{2i+1} z^{2i+1}$ is the odd part of $a(z)$. Since $\mathbf{b} = \rho^{2u}(\mathbf{a}_E)$, we may write $b(z)$ as

$$b(z) \equiv z^{2u}\big(E(z) - a_0(z) + a_1(z)\big) \pmod{z^v - 1},$$

where $E(z) = 1 + z^{2\cdot 1} + \ldots + z^{2(\frac{v}{2}-1)}$. Since $(1+\omega)E(\omega) = 1 + \omega + \ldots + \omega^{v-1}$, $E(\omega) = 0$ for any complex v-th root of unity ω with $\omega^2 \neq 1$, and hence

$$b(-\omega) = (-\omega)^{2u}\big(-a_0(-\omega) + a_1(-\omega)\big) = \omega^{2u} a(-\omega).$$

We directly check that $b(1) = a(1)$ and $b(-1) = a(-1)$ without difficulty. Therefore we have

$$\begin{aligned}\det(M_b) &= \prod_{i=0}^{v-1} b(\epsilon^i) = b(1)b(-1)\prod_{i=1}^{v/2-1} b(\epsilon^i)b(-\epsilon^i) \\ &= a(1)a(-1)\prod_{i=1}^{v/2-1} \epsilon^{2ui} h_a(-\epsilon^i)\epsilon^{2ui} h_a(\epsilon^i) = \prod_{i=0}^{v-1} h_a(\epsilon^i) = \det(M_a),\end{aligned}$$

which concludes the proof. ■

3.4 Existence determination of ideal cyclic difference pairs of small sizes

There are roughly two kinds of hypothetical CDPs whose existence is to be checked. In one case for which the parameters admit at least one multiplier, one can follow the scenario explained in Example 2.2. For the other case, there is no better way known so far than an exhaustive computer search.

In order to determine the existence of ideal CDPs of small sizes, first we collect all possible parameters of ideal CDPs whose existence is yet to be checked. Table 3.1 is the list for $v \equiv 0 \pmod 4$ and Table 3.2 for $v \equiv 2 \pmod 4$, both for $v \leq 40$. Unlike $(4u^2, 2u^2-u, u^2-u)$-CDSs which do not admit multipliers by known multiplier theorems, some ideal hypothetical CDPs allow multipliers by Theorem 3.2. For such lucky cases, their existence is determined in Example 3.3. For the remaining cases, we investigate their existence by an exhaustive computer search. To do this we classify binary sequences of a given period and of a given weight into cyclic equivalence classes. Proposition 3.3 and Proposition 3.4 give some help to reduce the number of objects to be checked. The result of a computer search for lengths up to 30 is summarized in Proposition 3.6.

Example 3.3 (Nonexistence of some ideal CDPs) We claim that

(a) $(16, 7, 5, 5, 2; 3)$-CDP does not exist;

Table 3.1: Parameters of suspected ideal $(v, k_a, k_b, k, \lambda)$-CDP, $4 < v \leq 40$, $v \equiv 0 \pmod 4$

v	k_a	k_b	k	λ	$k-\lambda$	Existence
8	3	3	2	1	1	Hadamard
12	5	5	3	2	1	Hadamard
16	7	7	4	3	1	Hadamard
	7	5	5	2	3	x
	6	6	6	2	4	x
20	9	9	5	4	1	Hadamard
	9	7	6	3	3	x
	8	8	7	3	4	x
24	11	11	6	5	1	Hadamard
	11	9	7	4	3	x
	10	10	8	4	4	x
28	13	13	7	6	1	Hadamard
	13	11	8	5	3	x
	12	12	9	5	4	x
	13	9	9	4	5	x
32	15	15	8	7	1	Hadamard
	15	13	9	6	3	?
	14	14	10	6	4	?
	15	11	10	5	5	?
36	17	17	9	8	1	Hadamard
	17	15	10	7	3	?
	16	16	11	7	4	?
	17	13	11	6	5	?
40	19	19	10	9	1	Hadamard
	19	17	11	8	3	?
	18	18	12	8	4	?
	19	15	12	7	5	?
	19	13	13	6	7	x

Table 3.2: Parameters of suspected ideal $(v, k_a, k_b, k, \lambda)$-CDP, $4 < v \leq 40$, $v \equiv 2 \pmod 4$

v	k_a	k_b	k	λ	$k-\lambda$	Existence
6	-	-	-	-	-	x
10	4	3	3	1	2	x
14	6	5	4	2	2	x
18	8	7	5	3	2	x
22	10	9	6	4	2	x
	10	7	7	3	4	x
26	12	11	7	5	2	x
	12	9	8	4	4	x
	11	10	10	4	6	x
30	14	13	8	6	2	x
	14	11	9	5	4	x
	13	12	11	5	6	x
34	16	15	9	7	2	?
	16	13	10	6	4	?
	15	14	12	6	6	?
	16	11	11	5	6	?
38	18	17	10	8	2	?
	18	15	11	7	4	?
	17	16	13	7	6	?
	18	13	12	6	6	?

(b) $(28, 13, 9, 9, 4; 5)$-CDP does not exist;

(c) $(40, 19, 13, 13, 6, 7)$-CDP does not exist;

Proof: To show these, suppose each of those CDPs exist.

(a) By Theorem 3.2, 3 is a multiplier of a $(16, 7, 5, 5, 2; 3)$-CDP (A, B). Using Theorem 3.3, we know that A must be a union of some cosets below and so is B, where $|A| = 7$ and $|B|$=5.

$$C_{1,1} = \{0\}, \quad C_{1,2} = \{8\},$$

$$C_{2,1} = \{2, 6\}, \quad C_{2,2} = \{4, 12\}, \quad C_{2,3} = \{10, 14\},$$

$$C_{4,1} = \{1, 3, 9, 11\}, \quad C_{4,2} = \{5, 15, 13, 7\}.$$

Since $k = |A \cap B| = |B|$, A includes B so we first determine B. Since $|B|$ is odd, it has to include one and only one coset out of two cosets of size 1. We can assume without loss of generality $C_{1,1}$ is included. Then we have two possibilities:

i) $A = B \cup C_{2,j}$ and $B = C_{1,1} \cup C_{4,i}$ for $i = 1, 2$ and $j = 1, 2, 3$;

ii) $A = C_{1,1} \cup C_{2,1} \cup C_{2,2} \cup C_{2,3}$ and $B = A \backslash C_{2,j}$ for $j = 1, 2, 3$;

It is easily verified that no combination of such pair of unions satisfies the desired difference property. Thus there does not exist a $(16, 7, 5, 5, 2; 3)$-CDP.

(b) 5 is a multiplier of $(28, 13, 9, 9, 4; 5)$-CDP, if it exists. Similarly no $(28, 13, 9, 9, 4; 5)$-CDP exists. We just list up cyclotomic cosets modulo 28 with respect to 5:

$$C_{1,0} = \{0\}, \quad C_{1,1} = \{8\},$$

$$C_{2,1} = \{2, 6\}, \quad C_{2,3} = \{4, 12\}, \quad C_{2,4} = \{10, 14\},$$

$$C_{4,1} = \{1, 3, 9, 11\}, \quad C_{4,2} = \{5, 15, 13, 7\}.$$

(c) 7 is a multiplier of $(40, 19, 13, 13, 6, 7)$-CDP, if it exists.

$$C_{1,1} = \{0\}, \quad C_{1,2} = \{20\},$$

$$C_{2,1} = \{5, 35\}, \quad C_{2,2} = \{10, 30\}, \quad C_{2,3} = \{15, 25\},$$

$$C_{4,1} = \{1, 7, 9, 23\}, \quad C_{4,2} = \{2, 14, 18, 6\}, \quad C_{4,3} = \{3, 21, 27, 29\},$$

$$C_{4,4} = \{4, 28, 36, 12\}, \quad C_{4,5} = \{8, 16, 32, 24\}, \quad C_{4,6} = \{11, 37, 19, 13\},$$

$$C_{4,7} = \{17, 39, 33, 31\}, \quad C_{4,8} = \{22, 34, 38, 26\}.$$

It can be checked that there does not exist a $(40, 19, 13, 13, 6, 7)$-CDP. ■

Proposition 3.6 1. For any $v \equiv 2 \pmod 4$ and $v \leq 30$, there does not exist an ideal CDP of period v.

2. For every $v \equiv 0 \pmod 4$ and $v \leq 30$, there exists an ideal $(v, k_a, k_b, k, \lambda)$-CDP of period v, and all of them are Hadamard CDPs, that is, $k - \lambda = 1$.

3. Moreover, every cyclic Hadamard difference pair of period ≤ 30 found by the exhaustive computer search is equivalent to that by the construction given in Theorem 3.5 up to the transformations of Proposition 3.3 and/or Proposition 3.4.

Chapter 4

Summary and Remarks

4.1 Summary

In this dissertation, we investigate a pair of binary sequences having a two-level correlation function in terms of the associated cyclic difference pairs, and the multipliers of cyclic difference pairs are developed in a parallelled way from the theory of multipliers of cyclic difference sets. For ideal cases, we determine the existence of some ideal cyclic difference pairs of small sizes, and we construct a class of binary sequence pairs of period $v = 4u$ having ideal two-level correlation with the in-phase correlation coefficient being four. More specifically, Theorem 3.5 together with Remark 3.1 gives, for every $u \geq 1$,

1. A pair of binary sequences $\mathbf{a} = (a_i)$ and $\mathbf{b} = (b_i)$ of period $v = 4u$ and of weight $wt(\mathbf{a}) = wt(\mathbf{b}) = 2u - 1$ such that

$$\theta_{ab}(0) = 4 \quad \text{and} \quad \theta_{ab}(\tau) = 0, \text{ for } \tau = 1, 2, \ldots, v-1, \tag{4.1}$$

$$\mathbf{a}_E = \rho^{(v/2)}(\mathbf{b}), \tag{4.2}$$

$$a_{v-i} = a_i \quad \text{and} \quad b_{v-i} = b_i, \forall i = 0, 1, \ldots. \tag{4.3}$$

2. An ideal cyclic difference pair (A, B), that is, $(v, k_a, k_b, k, \lambda; n)$-CDP with $v = 2(k_a + k_b) - 4\lambda$, such that

   (a) (A, B) is a $(4u,\ 2u-1,\ 2u-1,\ u,\ u-1;\ 1)$-CDP,

   (b) $A_E = (v/2) + B$,

   (c) (A, B) has -1 as its multiplier.

Thereby, whenever $\Gamma = 4$ and the degree is congruent to $3 \pmod 4$, we have a *self-reciprocal* solution to Problem A in the below, that is, a solution with the properties

$$\alpha(z) = \widetilde{\alpha(z)}, \beta(z) = \widetilde{\beta(z)}, \text{ and } -\alpha(-z) \equiv z^{(d+1)/2}\beta(z) \pmod{z^v - 1}.$$

We also have a *symmetric* solution to Problem B, whenever $w = 4$ and $v \equiv 0 \pmod 4$, with the property that the defining array of $NR^{v/2}$ is the even-position negation of the defining array of M, where R is a cyclic shift operator

$$R = \begin{bmatrix} & & & 1 \\ 1 & & & \\ & \ddots & & \\ & & 1 & \end{bmatrix}.$$

Problem A Find polynomials $\alpha(z)$ and $\beta(z)$ with coefficients from $\{+1, -1\}$ and of degree d such that

$$\alpha(z)\widetilde{\beta(z)} \equiv \Gamma \pmod{z^{d+1} - 1},$$

where $\widetilde{\beta(z)}$ is a reciprocal of $\beta(z)$.

Problem B Find v by v circulant matrices M and N whose entries are from $\{+1, -1\}$ such that

$$MN^T = wI.$$

4.2 Remarks and future directions

The sequence pair from Theorem 3.5 has the property that their in-phase correlation value is constant regardless of the period, and it is only four. This fact could be possibly one reason why the communication systems which adopt such sequence pair do not outperform conventional systems [52]. However, in other sense it gives some insight concerning the existence of cyclic Hadamard difference sets, and thereby the circulant Hadamard matrix conjecture.

As a base line for our discussion on that point, we leave the following conjectures and open problems concerning the existence of ideal CDPs, based on the the search results (Proposition 3.6) and the observations summarized in the previous section of this chapter.

Conjecture 4.1 If there is an $(v, k_a, k_b, k, \lambda)$-ideal cyclic difference pair, then v is a multiple of 4. ■

Conjecture 4.2 If there is an ideal $(v, k_a, k_b, k, \lambda)$-cyclic difference pair with $v/2 \geq k_a \geq k_b \geq k > \lambda$, then $k - \lambda = 1$. ■

Conjecture 4.3 If there is an ideal cyclic difference pair, then it is equivalent to the cyclic Hadamard difference pair generated by the construction given in Theorem 3.5, up to the transformations of Proposition 3.3 and 3.4. ■

Note that Conjecture 4.3 implies Conjecture 4.2 obviously, and Conjecture 4.2 implies Conjecture 4.1, by Theorem 3.4. Conjecture 4.2 also implies the circulant Hadamard matrix conjecture (Conjecture 2.1), since an ideal $(v, k_a, k_b, k, \lambda)$-CDP (A, B) with $A = B$ degenerates to the (v, k, λ)-circulant Hadamard difference set.

Problem 1 Find an ideal cyclic difference pair with $v \equiv 2 \pmod 4$ and $k - \lambda = 2$ (smallest possible). ■

Problem 2 Find an ideal cyclic difference pair with $v \equiv 0 \pmod 4$ and $k - \lambda > 1$. ■

Problem 3 Find an ideal CDP with $n = 1$ and $v \equiv 0 \pmod 4$ which is not equivalent to the pair given by Theorem 3.5. ■

Toward Conjecture 4.1 in the relation with Propblem 1, we currently believe that $k - \lambda$ is at least a sum of two integral squares if there is an ideal CDP with $v \equiv 2 \pmod 4$, which is supported by the result on integral matrices.

Theorem 4.1 (Hall [36]) There exists an integral square marix A of order n such that $A^T A = mI$, m a positive integer if and only if:
1) for n odd m is a square;
2) for $n \equiv 2 \pmod 4$ m is a sum of two integral squares;
3) for $n \equiv 0 \pmod 4$ m is any positive integer. ■

Though it is quite impetuous, concerning Conjecture 4.2 and Problem 2, it seems that the properties (4.2) and (4.3) is in fact *necessary* for an ideal binary sequence pair to exist. In other words, if an ideal cyclic difference pair (A, B) exists, then it has

-1 as a multiplier and A and B are related in a way of either $A_E = (v/2) + B$ or $A_E = (v/2) + B^C$. If we restrict to cyclic difference pairs (A, B) with $A = B$, i.e., cyclic difference sets, it is well known that minus one is never a multiplier of a non-trivial cyclic difference sets [2, Theorem 3.3]. Then we leave the unifying conjecture concerning the existence of ideal cyclic difference pairs as the following.

Conjecture 4.4 (Unifying conjecture on ideal CDP) If there exists an ideal cyclic difference pair (A, B) on the integers modulo v, then

(a) -1 $(= v - 1)$ is a multiplier, and

(b) Either $A_E = (v/2) + B$ or $A_E = (v/2) + B^C$, where A_E is the support set of the even-position negation of the characteristic binary sequence of A, and B^C is the complement of B. ■

Bibliography

[1] K. T. Arasu and A. Pott, "Theory of difference sets," in *Wiley Encyclopedia of Electrical and Electronics Engineering 21*, J. G. Webster, Ed. New York, USA: John Wiley & Sons, 1999, pp. 682–694.

[2] L. D. Baumert, *Cyclic Difference Sets*, ser. Lecture Nots in Mathematics 182. New York, USA: Springer-Verlag, 1971.

[3] L. D. Baumert and H. Fredricksen, "The cyclotomic numbers of order eighteen with applications to difference sets," *Mathematics of Computation*, vol. 21, no. 98, pp. 204–219, April 1967.

[4] L. D. Baumert and D. M. Gordon, "On cyclic difference sets," in *High Primes and Misdemeanours*, ser. Fields Institute Communications, Volume 41, A. van der Poorten and A. Stein, Eds. American Mathematical Society, 2004, pp. 61–68.

[5] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory, Second Edition, Vol.* 1, ser. Encyclopedia of Mathematics and Its Applications 69. New York, USA: Cambridge University Press, 1999.

[6] R. H. Bruck, "Difference sets in a finite group," *Transactions of the American Mathematical Society*, vol. 78, no. 2, March 1955.

[7] U. Cheng, "Exhaustive construction of $(255, 127, 63)$-cyclic difference sets," *Journal of Combinatorial Theory, Series A*, vol. 35, no. 2, pp. 115–125, 1983.

[8] H. Chung, "Gold sequences," in *Wiley Encyclopedia of Telecommunications, Volume 2*, J. G. Proakis, Ed. John Wiley & Sons, 2003, pp. 900–905.

[9] R. Craigen and H. Kharaghani, "Hadamard matrices and Hadamard designs," in *Handbook of Combinatorial Designs, Second Edition*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL, USA: Chapman & Hall / CRC, 2007, pp. 273–280.

[10] Z. D. Dai, G. Gong, and D. F. Ye, "Decompositions of cascaded GMW functions," *Science in China (Series A)*, vol. 44, pp. 709–717, 2001.

[11] P. J. Davis, *Circulant Matrices, Second Edition*. New York, USA: Chelsea Publishing, 1994.

[12] J. F. Dillon, "Multiplicative difference sets via additive characters," *Designs, Codes and Cryptography*, vol. 17, pp. 225–235, 1999.

[13] J. F. Dillon and H. Dobbertin, "New difference sets with Singer parameters," *Finite Fields and Their Applications*, vol. 10, pp. 342–389, 2004.

[14] H. Dobbertin, "Another proof of Kasami's theorem," *Designs, Codes, and Cryptography*, vol. 17, pp. 177–180, 1999.

[15] P. Fan and L. Hao, "Generalized orthogonal sequences and their applications in synchronous CDMA systems," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E83-A, no. 11, pp. 2054–2069, November 2000.

[16] P. Fan, N. Suehiro, N. Kuroyanagi, and X. M. Deng, "Class of binary sequences with zero correlation zone," *Electronic Letters*, vol. 35, no. 10, pp. 777–779, May 13th 1999.

[17] M. Fei, J. Ting, Z. Chenglin, and Z. Zheng, "Research on perfect dyadic binary sequence pair," *Journal of Electronics (China)*, vol. 23, no. 3, pp. 361–364, May 2006.

[18] P. Gaal and S. W. Golomb, "Exhaustive determination of $(1023, 511, 255)$-cyclic difference sets," *Mathematics of Computation*, vol. 70, no. 23, pp. 357–366, March 2000.

[19] D. G. Glynn, "Two new sequences of ovals in desarguesian planes of even order," in *Combinatorial Mathematics X*, ser. Lecture Notes in Mathematics 1036, L. R. A. Casse, Ed. Springer, 1982, pp. 217–229.

[20] M. J. E. Golay, "Complementary series," *IRE Transactions on Information Theory*, vol. 7, no. 2, pp. 82–87, April 1961.

[21] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Transactions on Information Theory*, vol. 14, pp. 154–156, January 1968.

[22] S. W. Golomb, “Construction of signals with favourable correlation properties,” in *Surveys in Combinatorics, 1991*, ser. London Mathematical Society Lecture Note Series, 166, A. D. Keedwell, Ed. New York, USA: Cambridge University Press.

[23] ——, *Shift Register Sequences, Revised Ed.* Walnut Creek, USA: Aegean Park Press, 1982, originally published by Holden-Day San Francisco, CA, 1967.

[24] ——, “Two-valued sequences with perfect periodic autocorrelation,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 28, no. 2, pp. 383–386, April 1992.

[25] ——, “Construction of signals with favourable correlation properties,” in *Difference Sets, Sequence and Their Correlation Properties*, ser. NATO Science Series C: Mathematical and Physical Sciences, Vol. 542, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds. Dordrecht, The Netherlands: Kluwer Academic Publishers, 1999, pp. 159–194.

[26] ——, “Shift register sequences—a restropective account,” in *Sequences and Their Applications - SETA 2006*, ser. Lecture Notes in Computer Science 4086, G. Gong, T. Helleseth, H.-Y. Song, and K. Yang, Eds. Berlin, Germany: Springer, 2006, pp. 1–4.

[27] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: for wireless communication, cryptography, and Radar*. New York, USA: Cambridge University Press, 2005.

[28] S. W. Golomb and H.-Y. Song, “A conjecture on the existence of cyclic hadamard

difference sets," *Journal of Statistical Planning and Inference*, vol. 62, pp. 39–41, 1997.

[29] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Transactions on Information Theory*, vol. 41, no. 2, pp. 400–411, March 1995.

[30] ——, "New designs for signal sets with low cross correlation, balance property, and large linear span: $GF(p)$ case," *IEEE Transactions on Information Theory*, vol. 48, no. 11, pp. 2847–2867, November 2002.

[31] G. Gong and S. W. Golomb, "The decimation-Hadamard transform of two-level autocorrelation sequences," *IEEE Transactions on Information Theory*, vol. 48, no. 4, pp. 853–865, April 2002.

[32] G. Gong, S. W. Golomb, and H.-Y. Song, "A note on low correlation zone signal sets," *IEEE Transactions on Information Theory*, vol. 53, no. 7, pp. 2575–2581, July 2007.

[33] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canadian Journal of Mathematics*, vol. 14, pp. 614–625, 1962.

[34] M. Hall, Jr., "Cyclic projective planes," *Duke Mathematical Journal*, vol. 14, no. 4, pp. 1079–1090, 1947.

[35] ——, "A survey of difference sets," *Proceedings of the American Mathematical Society*, vol. 7, no. 6, pp. 975–986, December 1956.

[36] ——, "Integral matrices A for which $AA^T = mI$," in *Number Theory and Algebra: Collected papers dedicated to Henry B. Mann, Arnold E. Ross and Olga Taussky-Todd*, H. Zassenhaus, Ed. New York, USA: Academic Press, 1977, pp. 119–134.

[37] M. Hall, Jr. and H. J. Ryser, "Cyclic incidence matrices," *Canadian Journal of Mathematics*, vol. 3, pp. 495–502, 1951.

[38] T. Helleseth, "Sequence correlation," in *Handbook of Combinatorial Designs, Second Edition*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL, USA: Chapman & Hall / CRC, 2007, pp. 273–280.

[39] T. Helleseth and P. V. Kumar, "Sequences with low correlation," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Elsevier Science, 1998, pp. 1765–1853.

[40] J. Jedwab, "A survey of the Merit Factor problem for binary sequences," in *Sequences and Their Applications—SETA 2004*, ser. Lecture Notes in Mathematics, LNCS 3486, T. Helleseth, D. Sarwate, H.-Y. Song, and K. Yang, Eds. Berlin, Heldelberg: Springer, 2005, pp. 30–55.

[41] S.-Y. Jin, "On the binary sequences of period 2047 with ideal autocorrelation," Master's thesis, Yonsei University, The Graduate School, Seoul, Korea, August 2003.

[42] D. Jungnickel, "Difference sets," in *Contemporary Design Theory: a Collection of Surveys*, ser. Wiley-Interscience Series in Discrete Mathematics and Optimization,

J. H. Dinitz and D. R. Stinson, Eds. New York, USA: John Wiley & Sons, 1992, pp. 242–324.

[43] D. Jungnickel and A. Pott, "Difference sets: an introduction," in *Difference Sets, Sequence and Their Correlation Properties*, ser. NATO Science Series C: Mathematical and Physical Sciences, Vol. 542, A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds. Dordrecht, The Netherlands: Kluwer Academic Publishers, 1999, pp. 259–295.

[44] D. Jungnickel, A. Pott, and K. W. Smith, "Difference sets," in *Handbook of Combinatorial Designs, Second Edition*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, USA: Chapman & Hall / CRC, 2007, pp. 419–436.

[45] T. Kasami, "Weight distributions of Bose-Chaudhuri-Hocquenghem codes," in *Combinatorial Mathematics and Its Applications*, R. C. Bose and T. A. Dowling, Eds. Chapel Hill, NC: University of North Carolina, 1969, pp. 335–357, reprinted in Elwyn R. Berlekamp, Ed., Key Papers in the Development of Coding Theory, IEEE press, New York, 1974.

[46] ——, "The weight enumerators for several classes of subcodes of the 2nd-order Reed-Muller codes," *Information and Control*, vol. 18, pp. 369–394, 1971.

[47] T. Kasami and R. Kohno, "Kasami sequences," in *Wiley Encyclopedia of Telecommunications, Volume 2*, J. G. Proakis, Ed. John Wiley & Sons, 2003, pp. 1219–1222.

[48] J.-H. Kim, "On the binary sequences of period 511 with ideal autocorrelation," Master's thesis, Yonsei University, The Graduate School, December 1997.

[49] ——, "On the hamard sequences," Ph.D. dissertation, Yonsei University, The Graduate School, Seouo, Korea, December 2001.

[50] J.-H. Kim and H.-Y. Song, "Existence of cyclic hadamard difference sets and its relation to binary sequence with ideal autocorrelation," *Journal of Communications and Networks*, vol. 1, no. 1, pp. 14–18, March 1999.

[51] A. Klapper, A. H. Chan, and M. Goresky, "Cascaded GMW sequences," *IEEE Transactions on Information Theory*, vol. 39, no. 1, pp. 177–183, January 1993.

[52] Q. Li, J. Gao, and Z. Zhao, "The application of the ZCZ sequence pairs set in QS-CDMA system," in *2007 International Workshop on Signal Design and Its Applications in Communications, (IWSDA 2007)*. IEEE, 2007, pp. 288–291.

[53] C. Lin and W. D. Wallis, "On the circulant Hadamard matrix conjecture," in *Coding Theory, Design Theory, Group Theory: Proceedings of The Marshall Hall Conference*, D. Jungnickel and S. A. Vanstone, Eds. New York, USA: John Wiley & Sons, 1993, pp. 213 – 217.

[54] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, ser. North-Holland Mathematical Library Volume 16. Amsterdam, The Netherlands: North-Holland, 1977, 1998 Tenth impression.

[55] M. Marcus and H. Minc, *A Survey of Matrix Theory and Matrix Inequalities*. New

York, USA: Dover Publications, 1992, originally published by Prindle, Weber & Schmidt, Boston, 1964.

[56] A. Maschietti, "Difference sets and hyperovals," *Designs, Codes and Cryptography*, vol. 14, pp. 89–98, 1998.

[57] R. L. McFarland and H. B. Mann, "On multipliers of difference sets," *Canadian Journal of Mathematics*, vol. 17, pp. 541–542, 1965.

[58] R. L. McFarland and B. F. Rice, "Translates and multipliers of abelian difference sets," *Proceedings of the American Mathematical Society*, vol. 68, no. 3, pp. 375–379, March 1978.

[59] P. K. Menon, "Difference sets in abelian groups," *Proceedings of the American Mathematical Society*, vol. 11, no. 3, pp. 368–376, June 1960.

[60] J.-S. No, H. Chung, and M.-S. Yun, "Binary pseudorandom sequences of period with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$," *IEEE Transactions on Information Theory*, vol. 44, no. 3, pp. 1278–1282, May 1998.

[61] J.-S. No, S. W. Golomb, G. Gong, H.-K. Lee, and P. Gaal, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 814–817, March 1998.

[62] H. J. Ryser, *Combinatorial Mathematics*, ser. The Carus Mathematical Monographs Number Fourteen. Washington DC, USA: The Mathematical Association of America, 1963.

[63] D. V. Sarwarte and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proceedings of the IEEE*, vol. 68, no. 4, pp. 593–619, 1980.

[64] B. Schmidt, *Characters and Cyclotomic Fields*, ser. Lecture Notes in Mathematics 1797. Berlin: Springer, 2002.

[65] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Transactions on Information Theory*, vol. 30, no. 3, pp. 548–553, May 1984.

[66] J. Seberry and M. Yamada, "Hadamard matrices, sequences, and block designs," in *Contemporary Design Theory: a Collection of Surveys*, ser. Wiley-Interscience Series in Discrete Mathematics and Optimization, J. H. Dinitz and D. R. Stinson, Eds. New York, USA: John Wiley & Sons, 1992, pp. 431–560.

[67] B. Segre, "Ovals in a finite projective plane," *Canadian Journal of Mathematics*, vol. 7, pp. 414–416, 1955.

[68] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and neqrly equidistance codes," *Probl. Pered. Inform.*, vol. 5, no. 1, pp. 16–22, 1969.

[69] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. New York, USA: McGraw-Hill.

[70] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Transactions of the Amererican Mathematical Society*, vol. 43, no. 3, pp. 377–385, May 1938.

[71] H.-Y. Song and S. W. Golomb, "On the existence of cyclic Hadamard difference

sets," *IEEE Transactions on Information Theory*, vol. 40, no. 4, pp. 1266–1268, July 1994.

[72] H.-Y. Song, "Feedback shift register sequences," in *Wiley Encyclopedia of Telecommunications, Volume 2*, J. G. Proakis, Ed. John Wiley & Sons, 2003, pp. 789–802.

[73] H.-Y. Song and S. W. Golomb, "Some new constructions for simplex codes," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 504–507, March 1994.

[74] R. G. Stanton and D. A. Sprott, "A family of difference sets," *Canadian Journal of Mathematics*, vol. 10, pp. 73–77, 1958.

[75] R. J. Turyn, "Character sums and difference sets," *Pacific Journal of Mathematics*, vol. 15, no. 1, pp. 319–346, 1965.

[76] ——, "Sequences with small correlation," in *Error Correcting Codes*, H. B. Mann, Ed. New York, USA: John Wiley & Sons, 1968, pp. 195–228, publication No. 21 of the Mathematics Research Center, United States Army, The University of Wisconsin.

[77] C. Xu, K. Liu, G. Li, and W. Yu, "Binary sequence pairs with two-level autocorrelation functions," in *International Conference on Wireless Communications, Networking and Mobile Computing, WiCom 2007*, Sep. 21-25 2007, pp. 1361–1364.

국 문 요 약

최적 상관 특성을 갖는 이진 신호쌍에 관한 연구

모든 시간 지연에 대해 비동기 자기상관 계수가 일정한 이진 신호는 각종 통신시스템에 사용되는 신호 집합을 생성하는 데 널리 이용되며, 순환 하다마드 행렬 및 순환 균일차이 집합과 밀접한 연관이 있다. 이 중에서 특히 자기상관 특성이 최적인, 즉 모든 시간 지연에 대한 비동기 자기상관 계수가 0인 이진 신호는 순회 하다마드 행렬과 일대일 대응 관계가 있으며 특정 성질을 갖는 순환 균일차이 집합의 존재 조건을 밝히는데 매우 중요한 역할을 한다. 그러나 최적 자기상관 특성을 갖는 이진 신호는 주기가 4보다 큰 경우에는 발견되지 않았으며, 아예 존재하지 않을 것으로 추측되고 있으나 아직 증명되지는 않았다.

본 논문에서는, 이를 이진 신호쌍으로 확장하여 그 특성을 규명한다. 즉, 모든 시간 지연에 대해 비동기 상호상관 계수가 일정한 신호쌍을 고려한다. 우선, 비동기 자기상관 계수 값이 일정한 이진 신호는 순환 균일차이 집합과 일대일 대응관계에 있음에 착안하여, 비동기 상호상관 계수가 일정한 이진 신호쌍으로부터 순환 균일차이 집합쌍을 도입하였다. 순환 균일차이 집합의 존재 조건과 특성을 규명하는 데 유용하게 사용되는 승수 개념을 순환 균일차이 집합쌍으로 확장하고, 이를 이용하여 순환 균일차이 집합쌍의 존재조건 및 그 특성을 파악하기 위한 토대를 마련하였다.

두 이진 신호 간의 비동기 상호상관 계수가 0으로 일정한 경우를 가리켜 특별

히 최적 상호상관 특성을 갖는 이진 신호쌍이라고 칭하는데, 이진 신호쌍이 최적 상관 특성을 보이기 위한 몇 가지 필요 조건이 본 논문에서 제시되었다. 나아가 주기가 4의 배수인 모든 경우, 비동기 상호상관 계수가 0으로 일정하고 동기 상호상관 계수가 4인 최적 이진 신호쌍이 존재함을 보이고, 또한 그 생성 방법을 제안하였다. 제안된 방법으로 생성된 최적 순환 균일차이 집합쌍은 -1이 승수가 됨을 확인하였다.

주기가 4의 배수가 아닌 경우에 최적 상호상관 특성을 갖는 이진 신호쌍이 존재하는지 아는지, 나아가 주기가 4의 배수인 경우에는 제안된 방법과는 다른 방법으로 생성되어 별개의 특성을 보이는 최적 이진 신호쌍이 존재하는지 아닌지를 알아보기 위하여 주기가 30이하인 범위에서 컴퓨터 전영역 조사를 실시하였다. 그 결과, 조사 범위 안에서는 주기가 4의 배수가 아닐 때는 최적 순환 균일차이 집합쌍이 존재하지 않으며, 주기가 4의 배수인 경우 발견된 모든 신호쌍은 본 논문에서 제안된 방법으로 생성되는 신호쌍과 본질적으로 동일한 특성을 가지고 있음을 확인하였다. 이에 근거하여 위와 같은 현상이 일반적으로 사실일 것으로 추측한다. 이 예상은 순회 하다마드 행렬의 존재에 관한 예상을 내포하는 일반화된 예상이다.

핵심되는 말: 최적 상관 특성, 순환 균일차이 집합, 하다마드타입 순환 균일차이 집합, 순환 균일차이 집합쌍, 하다마드타입 순환 균일차이 집합쌍, 승수, 하다마드행렬