PAPER *Special Section on Signal Design and its Application in Communications*

Binary Sequence Pairs with Two-Level Correlation and Cyclic Difference Pairs*

Seok-Yong JIN[†a)], ***Student Member and*** **Hong-Yeop SONG**[†b)], ***Nonmember***

SUMMARY We investigate binary sequence pairs with two-level correlation in terms of their corresponding cyclic difference pairs (CDPs). We define multipliers of a cyclic difference pair and present an existence theorem for multipliers, which could be applied to check the existence/nonexistence of certain hypothetical cyclic difference pairs. Then, we focus on the ideal case where all the out-of-phase correlation coefficients are zero. It is known that such an ideal binary sequence pair exists for length $v = 4u$ for every $u \geq 1$. Using the techniques developed here on the theory of multipliers of a CDP and some exhaustive search, we are able to determine that, for lengths $v \leq 30$, (1) there does not exist "any other" *ideal* binary sequence pair and (2) every example in this range is equivalent to the one of length $v = 4u$ above. We conjecture that if there is a binary sequence pair with an ideal two-level correlation then its in-phase correlation must be 4. This implies so called the circulant Hadamard matrix conjecture.

key words: *ideal two-level correlation, cyclic difference pair, cycic Hadamard difference pair, multiplier, circulant Hadamard matrix conjecture*

1. Introduction

Let $\mathbf{a} = (a_0, \cdots, a_{v-1})$ and $\mathbf{b} = (b_0, \cdots, b_{v-1})$ be binary sequences of the same length v, where $a_i, b_j \in \{0, 1\}$. Their periodic correlation function is defined as

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

where the subscript $i + \tau$ takes mod v.

When two sequences $\mathbf{a}$ and $\mathbf{b}$ are identical, this correlation is in fact an autocorrelation and denoted by $\theta_a(\tau)$. When all its out-of-phase values are the same, the sequence is said to have two-level autocorrelation:

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

It is well known [1]–[3] that balanced binary sequences having a two-level autocorrelation have many applications in communication, navigation and synchronization. Such sequences are especially useful if γ is as small as possible compared with the in-phase value v. When $\gamma = 0$, the sequence is called perfect or ideal. It is unfortunate that perfect binary sequences are "known" to exists if and only if the length $v = 4$. Ryser [4] conjectured that no nontrivial such sequence exists. Even with much progress [5]–[9], it is still widely open. It is now known that if a perfect binary sequence of length v exists then $v > 10^{11}$ with possible exceptions of $v = 4u^2$ with $u \in \{165, 11715, 82005\}$ [6].

Next level of "good" autocorrelation is the case where γ is as small as possible though not being zero. Specifically, this corresponds to the characteristic sequence of a (v, k, λ) cyclic difference set, where it is well known that $\gamma = v - 4(k - \lambda)$ [4], [10], [11]. Of these, the best is the case where $\gamma = -1$, called "cyclic Hadamard difference sets." It is also well known that multipliers have an essential role for the nonexistence of certain hypothetical difference sets.

The concept of two-level autocorrelation function of a single binary sequence could be generalized to a pair of binary sequences. A binary sequence pair $(\mathbf{a}, \mathbf{b})$ of the same length v has a two-level correlation if

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

We call the sequence pair $(\mathbf{a}, \mathbf{b})$ perfect or ideal if Γ_2 equals to zero.

In 2007, it is constructed [12] by Xu, et al. a class of binary sequence pairs of length v having a two-level correlation where $v = 2n^2 - 1$, $\Gamma_1 = 2n^2 - 8n + 11$ and $\Gamma_2 = 2n^2 - 8n + 7$, for every positive integer n. Note that $|\Gamma_1 - \Gamma_2| = 4$. The authors of this paper presented [13] in 2008 a class of binary sequence pairs of length v with an ideal two-level correlation where $v = 4u$, $\Gamma_1 = 4$ and $\Gamma_2 = 0$ for every positive integer u. It is interesting to observe that the difference between Γ_1 and Γ_2 in both cases is only 4. In fact, it turned out [14] that both constructions are part of a result [15, Thm. 4], which was published in Chinese domestic journal in Chinese. Moreover, it is easy to check that recently proposed constructions [16] are essentially the same as those given by Jia and Xu [15, Thm. 4].

Now, we focus on the existence of binary sequence pairs of length v with ideal two-level correlation, in which $\Gamma_2 = 0$. This is directly related with the existence of $v \times v$ circulant Hadamard matrices. The truth of the fact that $\Gamma_1 - \Gamma_2 = 4$ must hold always implies the famous "circulant Hadamard matrix conjecture." A binary sequence pair with an ideal two-level correlation finds many applications. For example, they can be used to generate a set of binary se-

Manuscript received January 13, 2010.

[†]The authors are with the School of Electrical and Electronics Engineering, Yonsei University, Seoul, 120-749, Korea.

[*]This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2009-0083888). Part of this has been presented at the IEEE International Symposium on Information Theory, Toronto, Ontario, Canada, July 2008. This is a full and enhanced version of those presented at ISIT 2008.

a) E-mail: sy.jin@yonsei.ac.kr
b) E-mail: hysong@yonsei.ac.kr

DOI: 10.1587/transfun.E93.A.2266

quence pairs with zero correlation zone property [17]. Some engineering applications could be found in the introductory section of [16].

In this paper we consider pairs of binary sequences of length v with a two-level correlation, and relate these with "cyclic difference pairs" (CDPs, in short). This is done in an analogy of the relation between binary sequences with a two-level autocorrelation and cyclic difference sets. Then, we solve some of existence/nonexistence of binary sequence pairs with ideal two-level correlation by investigating certain properties of (related) cyclic difference pairs. This is also done in an analogy of the nonexistence of certain cyclic difference sets.

In Sect. 2, we first define cyclic difference pairs in association with binary sequence pairs with two-level correlation, and characterize them using Hall polynomials and/or its associated circulant matrices, which are well-known techniques for the study of cyclic difference sets. We also have to carefully check all possible transformations of CDPs into another in order to characterize the equivalence of CDPs. Section 3 investigates the definition of "multipliers" of a CDP, and show non-trivially some results, which will be useful in determining the existence of certain CDPs in Sect. 4. Section 4 summarizes the current status on the existence of ideal CDPs corresponding to binary sequence pairs with ideal two-level correlation. Section 5 concludes the paper with lots of open problems.

2. Cyclic Difference Pairs and Binary Sequence Pairs with Two-Level Correlation

We will introduce and define cyclic difference pairs and give one-to-one correspondence between binary sequence pairs with a two-level correlation and cyclic difference pairs. Some properties of CDPs are discussed in terms of Hall polynomial pairs as well as certain associated circulant matrix pairs. We will begin by introducing some notations to be used in the remaining of this paper

Let $\mathbf{s} = (s_0, s_1, \cdots, s_{v-1})$ be a periodic $\{0, 1\}$-binary sequence of 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. The subscripts of the sequence are taken mod v.

- Weight: $wt(\mathbf{s}) = |\{i|s_i = 1, 0 \le i \le v-1\}| = |S|$.
- Cyclic shift: $\rho^j(\mathbf{s}) = \left(s_j, s_{j+1}, \cdots, s_{j+v-1}\right)$. Its support set is $j + S := \{j + s \pmod v | s \in S\}$.
- d-Decimation: $\mathbf{s}^{(d)} = (s_{d\cdot 0}, s_{d\cdot 1}, \cdots, s_{d\cdot(v-1)})$. Its support set is $dS := \{ds \pmod v | s \in S\}$.
- Negation: $\mathbf{s}' = \left(s'_0, \cdots, s'_{v-1}\right)$, where $s'_i = s_i + 1 \pmod 2$. Its support set is $S^C := [v] \backslash S$.
- Even-position negation: $\mathbf{s}_E = (u_0, \cdots, u_{v-1})$, $u_i = s'_i$ if i is even, and $u_i = s_i$ if i is odd. The support set of $\mathbf{s}_E$ is denoted by S_E.
- Hall polynomial: $s(z) = s_0 + s_1 z^1 + \cdots + s_{v-1} z^{v-1} \pmod{z^v - 1}$.
- Associated circulant matrix: $M_s = (m_{ij})$, where $m_{ij} = s_{i+j \ (\mathrm{mod}\ v)}$, $i, j = 0, \cdots, v-1$. The sequence $\mathbf{s}$ is called the defining array of M_s.

Let $(\mathbf{a}, \mathbf{b})$ be a pair of binary sequences of a period v having a two-level correlation

$$\theta_{a,b}(\tau) = \begin{cases} \Gamma(\neq \gamma) & \tau \equiv 0 \pmod v, \\ \gamma & \text{else}. \end{cases} \tag{1}$$

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

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

By definition, $d_{A,B}(0) = |A \cap B|$ equals to k. Since $d_{A,B}(\tau)$ is some fixed constant for nonzero τ, put this as λ, $d_{A,B}(\tau) = \lambda$, $\tau = 1, \cdots, v-1$. From (1) and (2), we have

$$v - 2(k_a + k_b) + 4k = \Gamma, \tag{3}$$

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

Comparing (3) and (4), we have

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

A binary sequence with a two-level autocorrelation induces a cyclic difference set and the converse is also true [11]. For a binary sequence pair with a two-level correlation, we may similarly define [13] the corresponding cyclic difference pair. Here, $\mathbb{Z}_v$ consists of the integers mod v, and k_x-subset of $\mathbb{Z}_v$ is a subset of size k_x of $\mathbb{Z}_v$.

Definition 1 *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 $x - y = w \pmod v$, 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.*

By counting the number of elements of $A \times B$ in two ways we have an immediate necessary condition for the existence of a cyclic difference pair (A, B) over $\mathbb{Z}_v$.

$$k_a k_b = \lambda v + (k - \lambda). \tag{5}$$

We summarize the one-to-one correspondence between the binary sequence pairs with two-level correlation and the cyclic difference pairs as follows [13]:

Theorem 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, the pair $(\mathbf{a}, \mathbf{b})$ has two-level correlation function whose in-phase* *correlation coefficient equals to* Γ *and all out-of-phase correlation coefficients equal to* γ *if and only if the pair* (A, B) *is a* $(v, k_a, k_b, k, \lambda)$*-cyclic difference pair, where* λ *and* γ *satisfy the relation (4) and* Γ *is given by the relation (3).*

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

A cyclic difference set is conveniently characterized [4] by its Hall polynomial as well as an associated circulant matrix. A cyclic difference pair can also be described in terms of Hall polynomials pair as well as associated circulant matrices:

Theorem 2 *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* $b(z)$*. Let* M_a *and* M_b *be the associated circulant matrix of* $\mathbf{a}$ *and* $\mathbf{b}$*, respectively. Then these are equivalent:*

1. (A, B) *is a* $(v, k_a, k_b, k, \lambda)$*-cyclic difference pair.*
2. $a(z)$ *and* $b(z)$ *satisfy*

$$a(z)b(z^{-1}) \equiv (k-\lambda)+\lambda(1+z+\cdots+z^{v-1}) \bmod z^v - 1. \tag{6}$$

3. ${M_a M_b}^T = (k - \lambda)I + \lambda J$*, where* I *is the identity matrix of order* v *and* J *is* $v \times v$ *matrix of all* 1*'s.*

The equivalence between the first and the second statement is due to

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

and the equivalence between the second and the third statement is obvious from its definition.

By the way, if we take the matrix $(k - \lambda)I + \lambda J$ and apply some elementary column and row operations to make it lower triangular form [4, p. 99], then we have $\det((k - \lambda)I + \lambda J) = (k + (v - 1)\lambda)(k - \lambda)^{v-1}$. It follows that if (A, B) is a $(v, k_a, k_b, k, \lambda)$-CDP then we have

$$\det({M_a M_b}^T) = k_a k_b (k - \lambda)^{v-1}. \tag{7}$$

There are some transformations which convert a given CDP into another. They are closely related to general correlation-preserving transformations which already appeared in [8], and they are partially presented in [15]. Let (A, B) be a $(v, k_a, k_b, k, \lambda)$-CDP. Then we have the following:

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 $d \in [v]$ 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 $A^C = [v]\backslash A$ and $B^C = [v]\backslash B$.
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 $\lambda' = \lambda + v - (k_a + k_b)$.
6. Assume further that (A, B) is an *ideal* $(v, k_a, k_b, k, \lambda)$-CDP. 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 $k''_a = k_a + (v/2 - 2e_a)$, $k''_b = k_b + (v/2 - 2e_b)$, $k'' = k + (v/2 - (e_a + e_b))$ and $\lambda'' = \lambda + (v/2 - (e_a + e_b))$ where e_a and e_b are nonnegative integers satisfying

$$(k_a - 2e_a)(k_b - 2e_b) = k - \lambda,$$

which follows if we evaluate (6) at $z = -1$.

3. Multipliers of Cyclic Difference Pairs

Multipliers of cyclic difference sets play an important role in the development of difference set theory. Let D be a cyclic difference set with parameters v, k, and λ. If there exists an integer t relatively prime to v satisfying

$$tD = s + D$$

for some integer s where $s + D = \{s + d \pmod{v} | d \in D\}$ and $tD = \{td \pmod{v} | d \in D\}$, then t is called a multiplier of the cyclic difference set D. Similarly we can define a multiplier of a cyclic difference pair.

Definition 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 all the multipliers of a cyclic difference pair form a group.*

Theorem 3 *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 the cyclic difference pair* (A, B)*.*

Proof: Let $(a(z), b(z))$ be the hall polynomial pair of the characteristic sequence pair $(\mathbf{a}, \mathbf{b})$ of (A, B).

We want to show that for some integer s,

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

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

Since (A, B) is a CDP we have

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

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 $p \mid k_a k_b$ and by (5) $p \mid \lambda$, whereas $p > \lambda$. Thus $p \nmid k_a$, and $p \nmid k_b$ by the same way. If we follow the same procedure in the proof of Theorem 2.1 of Chapter 9 of [4] we have

$$a(z^p) \equiv a(z)z^{s_a} \pmod{z^v - 1}, \tag{8}$$

for some integer s_a. Since (B, A) is also a CDP with the same parameters k and λ, 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

$$b(z^p) \equiv b(z)z^{s_b} \pmod{z^v - 1}. \tag{9}$$

Since (pA, pB) is also a CDP having the same parameters with those of (A, B) and the polynomial pair associated with (pA, pB) is $(a(z^p), b(z^p))$, we use (8) and (9) 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. ■

There have been developed various results [11], [18] concerning the existence and application of multipliers of (cyclic) difference sets, which could be extended to cyclic difference pairs. First we give a basic result on multipliers, which is a natural extension of [18, Lemma 2.5 Ch. VI].

Theorem 4 *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 $(t(s + A), t(s + B)) = (r + A, r + B)$ for a suitable integer $0 \le r < v$, and especially $t(s + A) = r + A$. Then we have

$$\begin{aligned}0 &= t(a_1 + \ldots + a_{k_a} + sk_a)\\ &= t((s + a_1) + \ldots + (s + a_{k_a}))\\ &= (r + a_1) + \ldots + (r + a_{k_a})\\ &= a_1 + \ldots + a_{k_a} + rk_a,\end{aligned}$$

where all the equalities hold mod v. Therefore $rk_a \equiv sk_a \pmod{v}$, and thus $r = s$. ■

The following is obvious and useful for checking the nonexistence of certain CDPs.

Theorem 5 *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.*

4. Ideal Cyclic Difference Pairs

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

$$v - 2(k_a + k_b) + 4\lambda = 0, \tag{10}$$

and hence

$$\Gamma = 4(k - \lambda). \tag{11}$$

If $\lambda = 0$, it is easy to know that $k_a = k_b = k = 1$ and $v = \Gamma = 4$ by (5), (10) and (11). It is interesting to see that if there is an ideal cyclic difference pair (A, B) with $\lambda = 0$ then $A = B$ and hence it degenerates to a cyclic difference set. One example is $\mathbf{a} = \mathbf{b} = (1000)$, the characteristic sequence of only *known* $(4u^2, 2u^2-u, u^2-u)$-cyclic difference set [11].

By virtue of the transformations of Sect. 2 we assume without loss of generality $v/2 \ge k_a \ge k_b \ge k$ and in that case $k - \lambda \ge 0$ by (12)

$$(v - 2k_a)(v - 2k_b) = 4(k - \lambda), \tag{12}$$

which comes easily from (5) and (10). Since $\Gamma \ne 0$ by definition, we always assume

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

when we refer to an ideal $(v, k_a, k_b, k, \lambda)$-cyclic difference pair in the remaining of the paper.

We remark that the parameter $k - \lambda$ plays an important role in the characterization of $(v, k_a, k_b, k, \lambda)$-CDP, as shown in (7) and (12). Sometimes we use $(v, k_a, k_b, k, \lambda; n)$ notation with $n := k - \lambda$ if it is clear.

4.1 Parameters of Ideal Cyclic Difference Pairs

The relation (10) shows obviously that v must be even for the existence of ideal pairs. Moreover (5) and (10) limit the values of k_a and k_b as a solution to the quadratic equation

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

Now, the proof of the following becomes obvious:

Proposition 1 (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.*

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

$$\left\{\begin{array}{lcl} v &=& 4u\\ k_a &=& 2u - l + m\\ k_b &=& 2u - l - m\\ k &=& u - l + n\\ \lambda &=& u - l\end{array}\right.$$

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

- *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*

$$\left\{\begin{array}{lcl} v & = & 4u+2 \\ k_a & = & 2u-l-1+m \\ k_b & = & 2u-l-m \\ k & = & u-l+n \\ \lambda & = & u-l \end{array}\right.$$

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

Example 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*

- $n = 1, (l, m) = (1, 0)$: $(4u, 2u-1, 2u-1, u, u-1)$*,* $u \geq 1$*,*
- $n = 3, (l, m) = (2, 1)$: $(4u, 2u-1, 2u-3, u+1, u-2)$*,* $u \geq 4$*,*
- $n = 4, (l, m) = (2, 0)$: $(4u, 2u-2, 2u-2, u+2, u-2)$*,* $u \geq 4$*,*

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

4.2 Ideal Cyclic Difference Pairs with $k - \lambda = 1$

In this paper we call an ideal cyclic difference pair with $k - \lambda = 1$ as a cyclic Hadamard difference pair (CHDP). A cyclic Hadamard difference pair is known to exist for every period $4u$, $u \geq 1$.

Construction A: [13], [15], [16] *Let* $v = 4u$ *and* $k_a = k_b = 2u-1$ *for an arbitrary positive integer u. We define* k_a*-subset A and* k_b*-subset B of* $\mathbb{Z}_v$ *as*

$$A = \{0, 1, \cdots, 2u-2\} \quad \text{and} \quad B = 2u + A_E.$$

Then (A, B) *is an ideal* $(4u, 2u-1, 2u-1, u, u-1)$*-cyclic difference pair.*

It is not hard to show the following for the cyclic Hadamard difference pairs given by **Construction A**:

Corollary 1 *Let* (A, B) *be the ideal CDP of length* $v = 4u$*,* $u \geq 1$*, given by* **Construction A***. Then*

1. $A_E = 2u + B$ *and* $B_E = 2u + A$*, and therefore* $(A_E, B_E) = (2u + B, 2u + A)$*.*
2. $((4u-1)A, (4u-1)B) = ((2u+2) + A, (2u+2) + B)$*.*
3. *The translate* $((u-1) + A, (u-1) + B)$ *is fixed by the multiplier* $4u - 1$*.*

In general, 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 of Theorem 6. For the other case, there is no better way known so far than an exhaustive computer search.

In order to determine the overall existence of ideal CDPs of small sizes, first we collect all possible parameters of ideal CDPs whose existence is yet to be checked. Unlike $(4u^2, 2u^2-u, u^2-u)$-cyclic difference sets which do not admit multipliers by known multiplier theorems, some hypothetical ideal CDPs allow multipliers by Theorem 3. For such lucky cases, their existence is determined in Theorem 6. 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. The result of a computer search for lengths up to 30 is summarized in Theorem 7.

Theorem 6 *The CDPs with the following parameters do not exist:* $(v, k_a, k_b, k, \lambda; n) = (16, 7, 5, 5, 2; 3)$*, or* $(28, 13, 9, 9, 4; 5)$*, or* $(40, 19, 13, 13, 6; 7)$*.*

Proof: To show the nonexistence of $(16, 7, 5, 5, 2; 3)$-CDP, suppose such a CDP (A, B) exist. Then 3 is a multiplier of (A, B) by Theorem 3. Both A and B must be unions of some cosets below by Theorem 5, where $|A| = 7$ and $|B|$=5.

$$C_0 = \{0\}, \quad C_1 = \{8\},$$
$$C_2 = \{2, 6\}, \quad C_3 = \{4, 12\}, \quad C_4 = \{10, 14\},$$
$$C_5 = \{1, 3, 9, 11\}, \quad C_6 = \{5, 15, 13, 7\}.$$

Since $k = |A \cap B| = |B|$ in this case, A includes B and hence it is easily verified that no such pair of unions satisfies the desired difference property. Thus there does not exist a $(16, 7, 5, 5, 2; 3)$-CDP. The remaining two cases can be done similarly. ■

Theorem 7
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 ideal CDP of period* ≤ 30 *found by an exhaustive computer search is equivalent to that by* **Construction A** *up to the transformations in Sect. 2.*

5. Concluding Remarks

The only *known* ideal CDP is given by **Construction A**. We may leave the following three conjectures concerning the existence of ideal CDPs. The assumption of the all three conjectures is the existence of an ideal $(v, k_a, k_b, k, \lambda)$-CDP with $v/2 \geq k_a \geq k_b \geq k > \lambda$.

- Conjecture 1: If such an ideal CDP exists, then $v \equiv 0 \pmod 4$.
- Conjecture 2: If such an ideal CDP exists, then $k - \lambda = 1$.
- Conjecture 3: Such an ideal CDP with $k - \lambda = 1$ is equivalent to the cyclic Hadamard difference pair given by **Construction A**.

Note that Conjecture 3 implies Conjecture 2, and Conjecture 2 implies Conjecture 1. Since a $(v, k_a, k_b, k, \lambda)$-CDP (A, B) with $A = B$ degenerates to the (v, k, λ)-cyclic difference set with $k_a = k_b = k$, Conjecture 2 implies the circulant Hadamard matrix conjecture.

It is remarkable that any cyclic difference set which has -1 as a multiplier has to be a trivial one [10]. As we see in Corollary 1, -1 is a multiplier of known ideal cyclic difference pairs (by **Construction A**.)

Some immediate open problems are as follows:

1. Find an ideal CDP with $n = 2$ (smallest possible) and $v \equiv 2 \pmod 4$.
2. Find an ideal CDP with $n > 1$ and $v \equiv 0 \pmod 4$.
3. Find an ideal CDP with $n = 1$ and $v \equiv 0 \pmod 4$ which is not equivalent to ones given by **Construction A**.

Acknowledgement

The authors of this paper would like to appreciate Professor G. Gong at University of Waterloo for introducing the reference [15].

References

[1] S.W. Golomb, Shift Register Sequences, Revised Edition., Aegean Park Press, Walnut Creek, USA, 1982. Originally published by Holden-Day San Francisco, CA, 1967.

[2] H.-Y. Song, “Feedback shift register sequences,” in Wiley Encyclopedia of Telecommunications, ed. J.G. Proakis, pp.789–802, John Wiley & Sons, 2003.

[3] S.W. Golomb and G. Gong, Signal Design for Good Correlation: for Wireless Communication, Cryptography, and Radar, Cambridge University Press, New York, USA, 2005.

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

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

[6] B. Schmidt, Characters and Cyclotomic Fields, Lecture Notes in Mathematics 1797, Springer, Berlin, 2002.

[7] J. Jedwab, “A survey of the merit factor problem for binary sequences,” in Sequences and Their Applications — SETA 2004, ed. T. Helleseth, D. Sarwate, H.-Y. Song, and K. Yang, Lecture Notes in Computer Science 3486, pp.30–55, Springer, Berlin, Heldelberg, 2005.

[8] M.J.E. Golay, “Complementary series,” IRE Trans. Inf. Theory, vol.7, no.2, pp.82–87, April 1961.

[9] S. Eliahou and M. Kervaire, “Barker sequences and difference sets,” L’Enseignement Mathematique, vol.38, pp.345–382, 1992.

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

[11] D. Jungnickel and A. Pott, “Difference sets: an introduction,” in Difference Sets, Sequence and Their Correlation Properties, ed. A. Pott, P.V. Kumar, T. Helleseth, and D. Jungnickel, pp.259–295, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1999.

[12] C. Xu, K. Liu, G. Li, and W. Yu, “Binary sequence pairs with two-level autocorrelation functions,” International Conference on Wireless Communications, Networking and Mobile Computing, WiCom 2007, pp.1361–1364, Sept. 2007.

[13] S.-Y. Jin and H.-Y. Song, “Note on a pair of binary sequences with ideal two-level crosscorrelation,” Proc. 2008 International Symposium on Information Theory (ISIT 2008), pp.2603–2607, Toronto, Canada, July 2008.

[14] G. Gong, Personal communications, June 29, 2009.

[15] Y.G. Jia and C.Q. Xu, “Research on differences set pairs and periodic complementary binary sequence pairs,” Chinese Journal on Communications, vol.28, no.8, pp.123–127, Aug. 2008.

[16] K. Liu, C. Xu, and K.T. Arasu, “Construction of binary sequence pairs with two-level periodic autocorrelation function,” 2009 International Workshop on Signal Design and Its Applications in Communications, (IWSDA 2009), pp.20–23, IEEE, 2009.

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

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

Seok-Yong Jin received his B.S. and M.S. degrees in Electronic Engineering from Yonsei University in 2001 and 2003, respectively. He is currently a Ph.D. candidate in the Department of Electrical and Electronic Engineering, Yonsei University. His area of research interest includes design and analysis of pseudorandom sequences, error correcting codes, and cyclic difference sets.

Hong-Yeop Song received his B.S. degree in Electronic Engineering from Yonsei University in 1984, MSEE and Ph.D. degrees from the University of Southern California, Los Angeles, CA, in 1986 and 1991, respectively, specializing in the area of communication theory and coding. He spent 2 years as a senior engineer at Qualcomm Inc., San Diego, CA, from 1994 to 1995, contributed to a team developing North American CDMA Standards for PCS and cellular air-interface systems. Finally, in the fall of 1995, he joined the Dept. of Electrical and Electronic Engineering at Yonsei University, Seoul, Korea, and is currently working as a professor. He visited Dr. G. Gong at University of Waterloo, Canada, in the year 2002. He is interested in Communication and Coding Theory, including error-correcting codes, PN sequences, and crypto algorithms. He is a senior member of IEEE, member of MAA (Mathematical Associ-ation of America), and domestic societies: IEEK, KICS, KIISC and KMS(Korean Mathematical Society).