Two-valued periodic complementary sequences

Li, Xudong; Liu, Zilong; Guan, Yong Liang; Fan, Pingzhi

2017

Li, X., Liu, Z., Guan, Y. L., & Fan, P. (2017). Two-valued periodic complementary sequences. IEEE Signal Processing Letters, 24(9), 1270-1274. doi:10.1109/LSP.2017.2722423

<https://hdl.handle.net/10356/105341>

<https://doi.org/10.1109/LSP.2017.2722423>

© 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<https://doi.org/10.1109/LSP.2017.2722423>

Downloaded on 26 Apr 2023 10:29:47 SGT

Two-Valued Periodic Complementary Sequences

Xudong Li, Zilong Liu, Yong Liang Guan, and Pingzhi Fan

Abstract—We present a novel transform for periodic complementary sets (PCSs) over two-valued alphabets from a large set of difference families. This is achieved by generalizing Golomb's idea in 1992, which was for transformed perfect sequences with zero autocorrelations only. Based on the properties of difference family, a sufficient condition for such two-valued PCSs is derived. Systematic constructions of two-valued periodic complementary pairs are presented. It is shown that many lengths for which binary PCSs do not exist become admissible for our proposed two-valued PCSs.

Index Terms—Difference family (DF), difference set, periodic autocorrelation function (ACF), periodic complementary pairs (PCPs), periodic complementary sets (PCSs).

I. INTRODUCTION

IN WIRELESS communications and radar sensing, perfect sequences (which have zero periodic autocorrelation sidelobes) are desirable for optimal performances of a variety of applications, such as spread spectrum communications, channel estimation, synchronization, and object detection or ranging [1]. For low-complexity digital implementation, perfect sequences with small alphabet sizes are demanded, nevertheless, they are limited to some short lengths. For example, the existing known binary and quaternary perfect sequences only have lengths (periods) of 4 and 2, 4, 8, 16, respectively [2]. The existing known perfect sequences over the alphabet set $\{\pm 1, \pm 2\}$ have lengths of 3, 4, 6, 7, 8, 10, 12, 28 only [3]. Polyphase perfect sequences [also known as perfect roots-of-unity sequences (PRUSs)] widely exist. However, as conjectured by Mow, the minimum alphabet size of PRUSs of length $N = sm^2$ (s, m positive integers) is $2sm$ for even s and odd m and is sm otherwise [4].

Manuscript received March 21, 2017; revised June 1, 2017; accepted June 26, 2017. Date of publication June 30, 2017; date of current version July 14, 2017. The work of Xudong Li was supported in part by the Key Natural Science Fund of Sichuan Education Department under Grant 13ZA0031, in part by the Key Scientific Research Fund of Xihua University under Grant R1222628, in part by the NSFC project under Grant U1433130/61401369, and in part by the Distinguished Young Fund of the School of Mathematics and Computer Engineering of Xihua University. The work of Zilong Liu, Yong Liang Guan, and Pingzhi Fan was supported by NSFC-NRF project under Grant 61661146003/NRF2016NRF-NSFC001-089. The work of Pingzhi Fan was also supported in part by the 111 Project under Grant 111-2-14. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Alessio Zappone. (Corresponding author: Zilong Liu.)

X. Li is with the Laboratory of Security Insurance of Cyberspace, School of Science, Xihua University, Chengdu 610039, China (e-mail: lixudong73@163.com).

Z. Liu and Y. L. Guan are with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798 (e-mail: zilongliu@ntu.edu.sg; eylguan@ntu.edu.sg).

P. Fan is with the Key Laboratory of Information Coding & Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu 610031, China (e-mail: pzf@swjtu.edu.cn).

Digital Object Identifier 10.1109/LSP.2017.2722423

A solution for this dilemma is to consider the autocorrelation function sums (ACFSs) of sequence pairs or sets, a way of sequence cooperation. Specifically, there exist large-length sequence pairs with zero out-of-phase periodic ACFSs (i.e., impulse-like autocorrelation sidelobes) and which have sequence entries drawn from a small alphabet such as the binary alphabet $\{-1, 1\}$. Such a sequence pair is called a periodic complementary pair (PCP). A generalization of PCP is called periodic complementary set (PCS) having zero ACFSs of two or more constituent sequences [5], [6]. We note that a counterpart of PCP is aperiodic complementary pair (ACP), also known as Golay complementary pair [7]. In this letter, we focus on the construction of two-valued PCP and PCS only.

The equivalence between binary PCSs and certain difference families (DFs) was pointed out by Bömer and Antweiler in [6]. Arasu and Xiang found an additional necessary condition of binary PCPs and showed that length-36 PCP does not exist [8]. Earlier, Yang proved that no length-18 binary PCP exists [9]. Doković and Kotsireas have found binary PCPs of 34, 50, 74, 122, 164, 202, 226 [10]–[12]. For binary PCPs, known admissible lengths up to 100 are

2, 4, 8, 10, 16, 20, 26, 32, 34, 40, 50, 52, 58, 64, 68, 72, 74, 80, 82

Up to date, the smallest length with undecided existence of binary PCP is 90 [12].

In this letter, we present a novel transform which is capable of producing PCS over a two-valued alphabet of $\{1, -c\}$ (c a positive number) or $\{1, \exp(\sqrt{-1}\theta)\}$ (θ a phase angle over the unitary circle) from certain DFs, each of which corresponding to a binary non-PCS. Our proposed transform generalizes and extends Golomb's transform in 1992 [13] for perfect sequences with zero autocorrelation sidelobes from cyclic difference sets.

II. PRELIMINARIES

The following notations will be used throughout this letter.

- 1) $Z_n \triangleq \{0, 1, \dots, n-1\}$ denotes the ring of integers modulo n ;
- 2) $\langle \mathbf{a}, \mathbf{b} \rangle$ denotes the inner product between two length- n sequences $\mathbf{a}$ and $\mathbf{b}$, i.e., $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{k=0}^{n-1} a_k b_k^*$;
- 3) For a length- n sequence $\mathbf{a} = [a_0, a_1, \dots, a_{n-1}]$, define $L\mathbf{a}$ as a shift operator that shifts sequence $\mathbf{a}$ cyclically to the left by one position and $L^\tau \mathbf{a}$ by τ positions.

A. Definition of PCS

Consider a set of m sequences $\mathcal{A} = \{\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^m\}$, where $\mathbf{a}^r = (a_0^r, a_1^r, \dots, a_{n-1}^r)$ is the r th ($1 \leq r \leq m$) sequence with length n . The periodic cross-correlation function between $\mathbf{a}^r$

and $\mathbf{a}^s$ at time-shift τ is defined as

$$R_{\mathbf{a}^r, \mathbf{a}^s}(\tau) \triangleq \sum_{u=0}^{n-1} a_u^r (a_{u+\tau}^s)^*, \quad 0 \leq \tau \leq n-1 \quad (1)$$

where the subscript is computed modulo n and x^* is the complex conjugate of x . When $\mathbf{a}^r = \mathbf{a}^s$, $R_{\mathbf{a}^r, \mathbf{a}^s}(\tau)$ reduces to periodic autocorrelation function (ACF), denoted by $R_{\mathbf{a}^r}(\tau)$.

Sequence set $\mathcal{A}$ is said to be a PCS if

$$\sum_{r=1}^m R_{\mathbf{a}^r}(\tau) = \begin{cases} mn, & \tau = 0, \\ 0, & 1 \leq \tau \leq n-1. \end{cases} \quad (2)$$

Each constituent sequence in a PCS is also called a periodic complementary sequence. When $m = 2$, a PCS reduces to a PCP.

B. Definition of DF

The difference function of $D \subseteq Z_n$ is defined as

$$\lambda_D(\tau) \triangleq |(\tau + D) \cap D|. \quad (3)$$

where $\tau \in \{1, \dots, n-1\}$. In another words, $\lambda_D(\tau)$ denotes the number of pairs (x, y) in D each of which has identical distance of τ , i.e., the cardinality of the multiset $\{(x, y) \in D \times D : x - y = \tau, x \neq y\}$.

Definition 1 (Difference Family (DF)) For $1 \leq r \leq m$, let X_r be a subset of Z_n which contains k_r elements. $\mathcal{X} = \{X_1, X_2, \dots, X_m\}$ is called an $(n; k_1, k_2, \dots, k_m; \lambda)$ difference family (DF) if the summation of the difference functions of $X_1, X_2, \dots, X_m$ equals the constant λ for every nonzero distance τ in Z_n , i.e., the following equation holds for any nonzero $\tau \in Z_n$,

$$\sum_{r=1}^m \lambda_{X_r}(\tau) = \lambda. \quad (4)$$

When $k_1 = k_2 = \dots = k_m = k$, such a DF is denoted by m -($n; k; \lambda$)-DF.

The definition of DF also implies the following identity:

$$\lambda(n-1) = \sum_{r=1}^m k_r(k_r - 1). \quad (5)$$

For presentation convenience, $X_1, X_2, \dots, X_m$ are referred to as the base blocks of DF $\mathcal{X}$. It is noted that when $m = 1$, a DF reduces to a difference set.

III. PCSs OVER TWO-VALUED ALPHABETS

First, consider X , a subset of Z_n , which has size of k . Construct a length- n sequence $\mathbf{a} = \{a_0, a_1, \dots, a_{n-1}\}$ using the following mapping

$$a_u = \begin{cases} \alpha, & u \in X, \\ \beta, & u \notin X \end{cases} \quad (6)$$

where $0 \leq u \leq n-1$. X is called the *support* of sequence $\mathbf{a}$ with alphabet set $\{\alpha, \beta\}$. From (6), it is clear that the number of α in the sequence $\mathbf{a}$ is k . Since the length of $\mathbf{a}$ is n , the number of

β in $\mathbf{a}$ is $n - k$. By (1), the periodic ACF of $\mathbf{a}$ can be rewritten as

$$R_{\mathbf{a}}(\tau) = \sum_{u=0}^{n-1} a_u (a_{u+\tau})^* = \langle \mathbf{a}, L^\tau \mathbf{a} \rangle \quad (7)$$

where $L^\tau \mathbf{a}$ is defined in the beginning of Section II. It is easy to see that

$$R_{\mathbf{a}}(0) = k|\alpha|^2 + (n-k)|\beta|^2. \quad (8)$$

When $1 \leq \tau \leq n-1$, denote by f_0, f_1, f_2, f_3 the occurring times of the following pairs,

$$(\alpha, \alpha^*), (\alpha, \beta^*), (\beta, \alpha^*), (\beta, \beta^*) \quad (9)$$

respectively. Clearly,

$$R_{\mathbf{a}}(\tau) = (\alpha\alpha^*) \cdot f_0 + (\alpha\beta^*) \cdot f_1 + (\beta\alpha^*) \cdot f_2 + (\beta\beta^*) \cdot f_3 \quad (10)$$

where $1 \leq \tau \leq n-1$.

It is noted that given sequence $\mathbf{a}$ with *support* X , sequence $L^\tau \mathbf{a}$ (a shifted version of $\mathbf{a}$) has *support* of

$$Y_\tau \triangleq (n - \tau) + X \bmod n. \quad (11)$$

If $u \in X \cap Y_\tau$, the mapping in (6) shows that $\mathbf{a}$ and $L^\tau \mathbf{a}$ is paired at the u th entry with identical α , i.e., the u th entry of both $\mathbf{a}$ and $L^\tau \mathbf{a}$ is α . By the definition of difference function in (3), we obtain that α in $\mathbf{a}$ is paired with α^* in $(L^\tau \mathbf{a})^*$ for $\lambda_X(n - \tau)$ times. That is, the pair (α, α^*) occurs for $\lambda_X(n - \tau)$ times. Since the total number of α in $\mathbf{a}$ is k , α in $\mathbf{a}$ is paired with β^* in $(L^\tau \mathbf{a})^*$ for $k - \lambda_X(n - \tau)$ times.

On the other hand, β in $\mathbf{a}$ is paired with β^* in $(L^\tau \mathbf{a})^*$ for

$$n - k - [k - \lambda_X(n - \tau)] = n - 2k + \lambda_X(n - \tau)$$

times as the total number of β^* in $(L^\tau \mathbf{a})^*$ is $n - k$. Similarly, β in $\mathbf{a}$ is paired with α^* in $(L^\tau \mathbf{a})^*$ for

$$(n - k) - [n - 2k + \lambda_X(n - \tau)] = k - \lambda_X(n - \tau)$$

times.

In summary, we have the following lemma.

Lemma 1: To calculate $R_{\mathbf{a}}(\tau)$ ($1 \leq \tau \leq n-1$), the periodic ACF of sequence $\mathbf{a}$, which is obtained from the mapping in (6), the occurring frequencies of the pair $(a_u, a_{u+\tau}^*)$ can be classified in the following four cases:

- (α, α^*) occurs $f_0 = \lambda_X(n - \tau)$ times;
- (α, β^*) occurs $f_1 = k - \lambda_X(n - \tau)$ times;
- (β, α^*) occurs $f_2 = k - \lambda_X(n - \tau)$ times;
- (β, β^*) occurs $f_3 = n - 2k + \lambda_X(n - \tau)$ times.

Substituting f_0, f_1, f_2, f_3 into (10), we have

$$R_{\mathbf{a}}(\tau) = \lambda_X(n - \tau)|\alpha|^2 + [n - 2k + \lambda_X(n - \tau)]|\beta|^2 + [k - \lambda_X(n - \tau)](\alpha\beta^* + \beta\alpha^*). \quad (12)$$

where $\lambda_X(\tau)$ is a difference function of X , and $\tau \in \{1, \dots, n-1\}$.

Now, we are in a position to present the first theorem of this letter.

Theorem 1: Let us consider an $(n; k_1, k_2, \dots, k_m; \lambda)$ -DF $\mathcal{X} = \{X_1, X_2, \dots, X_m\}$. Construct a length- n sequence set $\mathcal{A} = \{\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^m\}$ using the following mapping [similar to (6)] based on $\mathcal{X}$:

$$a_u^r = \begin{cases} \alpha, & u \in X_r, \\ \beta, & u \notin X_r \end{cases} \quad (13)$$

where $1 \leq r \leq m$ and $0 \leq u \leq n-1$. Based on $(n; k_1, k_2, \dots, k_m; \lambda)$ -DF $\mathcal{X} = \{X_1, X_2, \dots, X_m\}$, $\mathcal{A} = \{\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^m\}$ will be a PCS over the alphabet $\{\alpha, \beta\}$ if the following equation is satisfied:

$$\begin{aligned} & \lambda|\alpha|^2 + \left(mn - 2 \sum_{r=1}^m k_r + \lambda\right) |\beta|^2 \\ & + \left(\sum_{r=1}^m k_r - \lambda\right) (\alpha\beta^* + \beta\alpha^*) = 0. \end{aligned} \quad (14)$$

Proof: Recalling the definition of $\mathbf{a}^r$ in (13), and taking into account (8) and (12), we have

$$\begin{aligned} R_{\mathbf{a}^r}(\tau) &= \begin{cases} k_r |\alpha|^2 + (n - k_r) |\beta|^2, & \text{for } \tau = 0; \\ \lambda_{X_r}(n - \tau) |\alpha|^2 + (n - 2k_r + \lambda_{X_r}(n - \tau)) |\beta|^2 \\ + (k_r - \lambda_{X_r}(n - \tau)) (\alpha\beta^* + \beta\alpha^*), & \\ \text{for } 1 \leq \tau \leq n-1. \end{cases} \end{aligned}$$

By the definition of DF, we assert that $\lambda = \sum_{r=1}^m \lambda_{X_r}(n - \tau)$ holds for any $1 \leq \tau \leq n-1$. Therefore,

$$\begin{aligned} & \sum_{r=1}^m R_{\mathbf{a}^r}(\tau) \\ &= \begin{cases} \sum_{r=1}^m k_r |\alpha|^2 + (mn - \sum_{r=1}^m k_r) |\beta|^2, & \tau = 0, \\ \lambda |\alpha|^2 + (mn - 2 \sum_{r=1}^m k_r + \lambda) |\beta|^2 \\ + (\sum_{r=1}^m k_r - \lambda) (\alpha\beta^* + \beta\alpha^*), & 1 \leq \tau \leq n-1. \end{cases} \end{aligned} \quad (15)$$

Clearly, if

$$\begin{aligned} & \lambda |\alpha|^2 + \left(mn - 2 \sum_{r=1}^m k_r + \lambda\right) |\beta|^2 \\ & + \left(\sum_{r=1}^m k_r - \lambda\right) (\alpha\beta^* + \beta\alpha^*) = 0 \end{aligned} \quad (16)$$

we have

$$\sum_{r=1}^m R_{\mathbf{a}^r}(\tau) = \begin{cases} \sum_{r=1}^m k_r |\alpha|^2 + (mn - \sum_{r=1}^m k_r) |\beta|^2, & \tau = 0, \\ 0, & 1 \leq \tau \leq n-1. \end{cases} \quad (17)$$

Thus, we complete the proof. $\blacksquare$

Remark 1: When $m = 1$, Theorem 1 reduces to the sufficient condition of Golomb in [13, eq. (8)] for two-valued perfect sequences from cyclic difference sets. When $m \geq 2$, $\alpha = 1, \beta =$

-1 , Theorem 1 reduces to the sufficient condition for binary PCSs in [6].

In what follows, we consider the two cases of alphabet settings:

Case 1: $\alpha = 1$ and $\beta = -c$, where c is a positive number. Substituting $\alpha = 1$ and $\beta = -c$ into the mapping defined in (13) and recalling (15), we obtain

$$\sum_{r=1}^m R_{\mathbf{a}^r}(\tau) = \begin{cases} \sum_{r=1}^m k_r + (mn - \sum_{r=1}^m k_r) c^2, & \tau = 0, \\ \lambda + (mn - 2 \sum_{r=1}^m k_r + \lambda) c^2 \\ - 2(\sum_{r=1}^m k_r - \lambda) c, & 1 \leq \tau \leq n-1. \end{cases} \quad (18)$$

By setting $\sum_{r=1}^m R_{\mathbf{a}^r}(\tau) = 0$ for nonzero τ in (18), we have

$$\left(mn - 2 \sum_{r=1}^m k_r + \lambda\right) c^2 - 2 \left(\sum_{r=1}^m k_r - \lambda\right) c + \lambda = 0. \quad (19)$$

Solving the quadratic equation (19) in c , we obtain the following corollary.

Corollary 1: Based on $(n; k_1, k_2, \dots, k_m; \lambda)$ -DF $\mathcal{X} = \{X_1, X_2, \dots, X_m\}$ and the mapping defined in (13), $\{\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^m\}$ will be a PCS over the alphabet $\{1, -c\}$ if

$$c = \frac{\sum_{r=1}^m k_r - \lambda \mp \sqrt{(\sum_{r=1}^m k_r)^2 - mn\lambda}}{mn - 2 \sum_{r=1}^m k_r + \lambda} > 0, \quad (20)$$

$mn - 2 \sum_{r=1}^m k_r + \lambda \neq 0$, and $(\sum_{r=1}^m k_r)^2 - mn\lambda \geq 0$.

Remark 2: Setting $mn = 4(\sum_{r=1}^m k_r - \lambda)$ in Corollary 1, we assert that $\{\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^m\}$ will be a binary PCS ($c = 1$) or a PCS over the alphabet $\{1, -\frac{\lambda}{2 \sum_{r=1}^m k_r - 3\lambda}\}$.

Proof: When $mn = 4(\sum_{r=1}^m k_r - \lambda)$, we have

$$\begin{aligned} \left(\sum_{r=1}^m k_r\right)^2 - mn\lambda &= \left(\sum_{r=1}^m k_r\right)^2 - 4 \left(\sum_{r=1}^m k_r - \lambda\right) \lambda \\ &= \left(\sum_{r=1}^m k_r - 2\lambda\right)^2 \end{aligned}$$

From (20), we obtain that $c = 1$ or $c = \frac{\lambda}{2 \sum_{r=1}^m k_r - 3\lambda}$. Thus, we complete the proof. $\blacksquare$

Case 2: $\alpha = 1$ and $\beta = \exp(i\theta)$, where $i = \sqrt{-1}$ and θ is a phase angle. Substituting $\alpha = 1$ and $\beta = \exp(i\theta)$ (θ a phase angle) into the mapping defined in (13) and recalling (15), we obtain

$$\sum_{r=1}^m R_{\mathbf{a}^r}(\tau) = \begin{cases} mn, & \tau = 0, \\ mn - 2(\sum_{r=1}^m k_r - \lambda) \\ + 2(\sum_{r=1}^m k_r - \lambda) \cos \theta, & 1 \leq \tau \leq n-1. \end{cases} \quad (21)$$

By setting $\sum_{r=1}^m R_{\mathbf{a}^r}(\tau) = 0$ for nonzero τ in (21), we obtain the following corollary.

Corollary 2: Based on $(n; k_1, k_2, \dots, k_m; \lambda)$ -DF $\mathcal{X} = \{X_1, X_2, \dots, X_m\}$ and the mapping defined in (13),

$\{\mathbf{a}^1, \mathbf{a}^2, \dots, \mathbf{a}^m\}$ is a PCS over the alphabet $\{1, \exp(i\theta)\}$ if

$$\theta = \cos^{-1} \left(1 - \frac{mn}{2(\sum_{r=1}^m k_r - \lambda)} \right), \quad (22)$$

and $mn \leq 4(\sum_{r=1}^m k_r - \lambda)$.

A. Constructions of Two-Valued PCPs

Setting $m = 2$ in *Corollaries 1* and *2*, we obtain two-valued PCPs over alphabets $\{1, -c\}$ and $\{1, \exp(i\theta)\}$.

Example 1: Let $\{X_1, X_2\}$ be a $(12; 5, 2; 2)$ -DF, where $X_1 = \{0, 1, 2, 5, 8\}$ and $X_2 = \{0, 2\}$. Applying (20), we obtain $c = 1/2$ or $1/3$. The PCP $\{\mathbf{a}^1, \mathbf{a}^2\}$ for $c = 1/2$ and its ACFs are given below

$$\mathbf{a}^1 = (1, 1, 1, -c, -c, 1, -c, -c, 1, -c, -c, -c)$$

$$\mathbf{a}^2 = (1, -c, 1, -c, -c, -c, -c, -c, -c, -c, -c, -c)$$

$$(R_{\mathbf{a}^1}(\tau) + R_{\mathbf{a}^2}(\tau))_{\tau=0}^{11} = (45/4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

Note that in the above example, no valid θ exists [by (22)] because the constraint $n \leq 2(k_1 + k_2 - \lambda)$ cannot be met. In the next example, we present an example with valid θ .

Example 2: Let (X_1, X_2) be a $(5; 2, 2; 1)$ -DF, where $X_1 = (0, 1)$ and $X_2 = (0, 2)$. Applying (20) and (22), respectively, we have $c = 1 \pm \sqrt{6}/3$ and $\theta = \cos^{-1}(-\frac{2}{3}) \approx 131^\circ 48' 37.13''$. Thus, $\beta = \exp(i\theta) \approx -0.6667 + 0.7454i$, where $i = \sqrt{-1}$. The corresponding PCP $(\mathbf{a}^1, \mathbf{a}^2)$ as well as their ACFs are shown below:

$$\mathbf{a}^1 = (1, 1, \beta, \beta, \beta)$$

$$\mathbf{a}^2 = (1, \beta, 1, \beta, \beta)$$

$$(R_{\mathbf{a}^1}(\tau) + R_{\mathbf{a}^2}(\tau))_{\tau=0}^4 = (10, 0, 0, 0, 0).$$

We now present below a systematic construction of PCPs based on $2-(v; (n-1)/2; (n-3)/2)$ -DF obtained in [14].

First, we introduce some basic knowledge on cyclotomy which is useful for DF construction. For further reading on cyclotomy, the reader is referred to [15] and [16]. Let q be a power of an odd prime, and let ξ be a generator of multiplicative group F_q^* (which contains all the nonzero elements of finite field F_q). Assume $q-1 = dh$, where d and h are integers greater than 1. Denote by $C_0^{(d)}$ the subgroup of F_q^* generated by ξ^d , and let $C_u^{(d)} = \xi^u C_0^{(d)}$ for $1 \leq u \leq d-1$. These $C_u^{(d)}$ are called cyclotomic classes of order d with respect to F_q^* .

Lemma 2 ([14], Theorem 4.1) Consider $q \equiv 3 \pmod{4}$, a power of prime p . Generate $C_0^{(2)}$ and $C_1^{(2)}$ which are cyclotomic classes of order 2 defined by ξ . Let $n = \frac{(q-1)}{2}$ and define two subsets of the residue class ring Z_n as follow:

$$X_1 = \{(\log_\xi x)/2 : x \in (C_0^{(2)} - 1) \cap C_0^{(2)}\}$$

$$X_2 = \{(\log_\xi x - 1)/2 : x \in (C_0^{(2)} - 1) \cap C_1^{(2)}\}.$$

Then, (X_1, X_2) forms a $(n; (n-1)/2, (n-1)/2; (n-3)/2)$ -DF in Z_n .

Corollary 3: Based on X_1, X_2 obtained in *Lemma 2* and recalling (20) which is for the two-valued alphabet over real numbers, we obtain a family of PCP over the alphabet $\{1, -c\}$, where $c = 1 \pm \frac{2}{\sqrt{n+1}}$. Similarly, we obtain another family of PCP over the alphabet $\{1, \exp(j\theta)\}$, where $\theta = \cos^{-1}(-\frac{n-1}{n+1})$. Then the following equations hold:

$$\lim_{n \rightarrow +\infty} c = \lim_{n \rightarrow +\infty} \left(1 \pm \frac{2}{\sqrt{n+1}} \right) = 1 \quad (23)$$

and

$$\lim_{n \rightarrow +\infty} \theta = \lim_{n \rightarrow +\infty} \cos^{-1} \left(-\frac{n-1}{n+1} \right) = \pi. \quad (24)$$

Remark 3: The PCPs obtained in systematic construction of PCPs have the property that β tends to -1 when n becomes asymptotically large, meaning that such PCPs tend to be binary if the sequence length is sufficiently large.

Example 3: Consider $q = 23$ and $\xi = 5$, a generator of F_{23}^* . By *Lemma 2*, we obtain $2-(11; 5; 4)$ -DF as follows: $X_1 = \{0, 1, 3, 8, 10\}$, $X_2 = \{0, 3, 4, 8, 9\}$. Applying *Corollary 3*, we have $c = 1 \pm \sqrt{3}/3$ and $\theta = \cos^{-1}(-5/6) \approx 146^\circ 26' 33.68''$. The corresponding PCP $\{\mathbf{a}^1, \mathbf{a}^2\}$ is shown as follows:

$$\mathbf{a}^1 = (1, 1, \beta, 1, \beta, \beta, \beta, 1, \beta, 1)$$

$$\mathbf{a}^2 = (1, \beta, \beta, 1, 1, \beta, \beta, \beta, 1, 1, \beta).$$

If $\beta = \exp(i\theta) = \exp(i \cos^{-1}(-\frac{5}{6})) \approx -0.8333 + 0.5528i$, we have

$$(R_{\mathbf{a}^1}(\tau) + R_{\mathbf{a}^2}(\tau))_{\tau=0}^{10} = (22, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0).$$

Finally, we note that $2-(n; (n-1)/2; (n-3)/2)$ -DFs can also be obtained through some binary sequence pairs each having out-of-phase ACFs of -2 . They include, the generalized GMW sequence pair, the twin-prime sequence pair, and the Legendre sequence pair reported in [17] and *optimal* BP-ACPs of odd-lengths reported in [18].

IV. CONCLUSION

Two-valued PCSs, which include the conventional binary PCS over $\{1, -1\}$ as special cases, have been proposed. It is shown that two-valued PCSs exist for many more lengths, in contrast to the limited admissible lengths of binary PCSs. Based on [11, Tables 3– 6], admissible sequence lengths up to 50 for two-valued PCPs are summarized as follows:

$$\begin{aligned} &\{2\} \cup \{4, 5\} \cup \{7, 8, \dots, 13\} \\ &\cup \{15, 16, \dots, 43\} \cup \{45, 46, \dots, 50\}. \end{aligned}$$

Clearly, the above admissible set is larger than and subsumes the set $\{2, 4, 8, 10, 16, 20, 26, 32, 34, 40, 50\}$ for binary PCPs.

Furthermore, we have also derived a sufficient condition of two-valued PCSs based on DFs. In particular, the constructions of two-valued PCSs over the alphabets $\{1, -c\}$ and $\{1, \exp(\sqrt{-1}\theta)\}$ have been investigated. In the end, a systematic construction of two-valued PCPs has been proposed based on Ding's $2-(n; (n-1)/2; (n-3)/2)$ -DFs that are constructed from cyclotomy.

REFERENCES

- [1] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. New York, NY, USA: Wiley, 1996.
- [2] H. D. Lüke, H. D. Schotten, and H. H. -Mahram, "Binary and quadriphase sequences with optimal autocorrelation properties: A survey," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3271–3282, Dec. 2003.
- [3] X. Li, P. Fan, W. H. Mow, and M. Darnell, "Multilevel perfect sequences over integers," *Electr. Lett.*, vol. 47, pp. 496–497, Apr. 2011.
- [4] W. H. Mow, "A new unified construction of perfect root-of-unity sequences," in *Proc. Spread-Spectrum Techn. Appl.*, Mainz, Germany, Sep. 1996, pp. 955–959.
- [5] R. L. Frank, "Polyphase complementary codes," *IEEE Trans. Inf. Theory*, vol. IT-26, no. 6, pp. 641–647, Nov. 1980.
- [6] L. Bömer and M. Antweiler, "Periodic complimentary binary sequences," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1487–1494, Nov. 1990.
- [7] M. J. E. Golay, "Complementary series," *IRE Trans. Inf. Theory*, vol. IT-7, pp. 82–87, Apr. 1961.
- [8] K. T. Arasu and Q. Xiang, "On the existence of periodic complementary binary sequences," *Des. Codes Cryptogr.*, vol. 2, pp. 257–262, 1992.
- [9] H. Yang, "Maximal binary matrices and sum of two squares," *Math. Comput.*, vol. 30, pp. 148–153, 1976.
- [10] D. Z. Doković and I. S. Kotsireas, "Note on the periodic complementary sets of binary sequences," *Des. Codes Cryptogr.*, vol. 13, pp. 251–256, 1998.
- [11] D. Z. Doković and I. S. Kotsireas, "Cyclic $(v; r, s; \lambda)$ difference families with two base blocks and $v \leq 50$," *Ann. Combinatorics*, vol. 15, pp. 233–254, 2011.
- [12] D. Z. Doković and I. S. Kotsireas, "Some new periodic Golay pairs," *Numer. Algorithms*, vol. 69, pp. 523–530, 2015.
- [13] S. W. Golomb, "Two-valued sequences with perfect periodic autocorrelation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 28, no. 2, pp. 383–386, Apr. 1992.
- [14] C. Ding, "Two constructions of $(v, (v-1)/2, (v-3)/2)$ difference families," *J. Combinatorial Des.*, vol. 16, pp. 164–171, 2008.
- [15] T. Storer, *Cyclotomy and Difference Sets*. Chicago, IL, USA: Markham, 1967.
- [16] R. Lidl and H. Niederreiter, *Finite Fields (ser. Encyclopedia of Mathematics and its Applications)*, vol. 20, 2nd ed. New York, NY, USA: Cambridge Univ. Press, 1997.
- [17] X. Tang and G. Gong, "New constructions of binary sequences with optimal autocorrelation value/magnitude," *IEEE Trans. Inf. Theory*, vol. 56, no. 3, pp. 1278–1286, Mar. 2010.
- [18] A. R. Adhikary, Z. Liu, Y. L. Guan, S. Majhi, and S. Z. Budishin, "Optimal binary periodic almost-complementary pairs," *IEEE Signal Process. Lett.*, vol. 23, no. 12, pp. 1816–1820, Sep. 2016.