Optimal Partitioned Cyclic Difference Packings for Frequency Hopping and Code Synchronization

Yeow Meng Chee, *Senior Member, IEEE*, Alan C. H. Ling, and Jianxing Yin

***Abstract*—Optimal partitioned cyclic difference packings (PCDPs) are shown to give rise to optimal frequency-hopping sequences and optimal comma-free codes. New constructions for PCDPs, based on almost difference sets and cyclic difference matrices, are given. These produce new infinite families of optimal PCDPs (and hence optimal frequency-hopping sequences and optimal comma-free codes). The existence problem for optimal PCDPs in $\mathbb{Z}_{3m}$, with m base blocks of size three, is also solved for all $m \not\equiv 8, 16 \pmod{24}$.**

***Index Terms*—Almost difference sets, code synchronization, comma-free codes, cyclic difference matrices, frequency-hopping sequence (FHS), partitioned difference packings.**

I. Introduction

FREQUENCY-hopping spread spectrum (FHSS) [1] is an important communication technique to combat eavesdropping, Rayleigh fading, reduce interleaving depth and associated delay, and enable efficient frequency reuse, giving rise to robust security and reliability. As such, FHSS is widely used in military radios, CDMA and GSM networks, radars and sonars, and Bluetooth communications.

In FHSS, an ordered list of frequencies, called a frequency-hopping (FH) sequence, is allocated to each transmitter-receiver pair. Interference can occur when two distinct transmitters use the same frequency simultaneously. In evaluating the goodness of FH sequence design, the Hamming correlation function is used as an important measure. Fuji-Hara *et al.* [2] introduced a new class of combinatorial designs and showed that they are equivalent to FH sequences optimal with respect to Hamming correlation. We call these combinatorial designs partitioned cyclic difference packings (PCDPs) in this paper.

PCDPs arise in another context. In considering the construction of comma-free codes for synchronization over erroneous channels, Levenshtein [3] introduced difference system of sets (DSS) and showed how DSS can be used to construct comma-free codes. We establish connections between PCDP and DSS (and hence comma-free codes), especially PCDPs that give rise to DSS and comma-free codes optimal with respect to redundancy.

As general results, we give new constructions of PCDPs via almost difference sets and cyclic difference matrices. This gives new infinite families of optimal PCDPs. The existence problem for optimal PCDPs in $\mathbb{Z}_{3m}$, with m base blocks of size three, is also solved for all $m \not\equiv 8, 16 \pmod{24}$.

Manuscript received May 26, 2009; revised August 19, 2010. Date of current version October 20, 2010. The work of Y. M. Chee was supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03 and by the Nanyang Technological University under Research Grant M58110040. The work of J. Yin was supported by the National Science Foundation of China (NSFC) under Project 10671140.

Y. M. Chee is with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637371 (e-mail: ymchee@ntu.edu.sg).

A. C. H. Ling is with the Department of Computer Science, University of Vermont, Burlington, VT 05405 USA (e-mail: aling@emba.uvm.edu).

J. Yin is with the Department of Mathematics, Suzhou University, 215006 Suzhou, Jiangsu, China (e-mail: jxyin@suda.edu.cn).

Communicated by B. S. Rajan, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2010.2070530

II. Mathematical Preliminaries

For a positive integer n, the set $\{1, 2, \ldots, n\}$ is denoted $[n]$, and $\mathbb{Z}_n$ denotes the ring $\mathbb{Z}/n\mathbb{Z}$. The set $\mathbb{Z}_n \setminus \{0\}$ is denoted $\mathbb{Z}_n^\star$. The set of (nonzero) quadratic residues in $\mathbb{Z}_n$ is denoted $\mathbb{Z}_n^\square$ and the set of quadratic nonresidues of $\mathbb{Z}_n$ is denoted $\mathbb{Z}_n^\boxtimes$. For succinctness, we write a_b for an element $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$.

Given a collection

$$\mathcal{D} = \{D_1, D_2, \ldots, D_m\}$$

of subsets (called *base blocks*) of $\mathbb{Z}_n$, define the *difference function* $\Phi_{\mathcal{D}} : \mathbb{Z}_n^\star \to \mathbb{Z}$ such that

$$\Phi_{\mathcal{D}}(g) = \sum_{i=1}^{m} |(D_i + g) \cap D_i|.$$

For positive integers n, λ, and multiset of positive integers K, a cyclic difference packing (CDP), or more precisely an (n, K, λ)-CDP, is a collection $\mathcal{D}$ of subsets of $\mathbb{Z}_n$ such that:

i) $K = [|D| : D \in \mathcal{D}]$;
ii) $\lambda = \max_{g \in \mathbb{Z}_n^\star} \Phi_{\mathcal{D}}(g)$.

If, in addition, $\mathcal{D}$ partitions $\mathbb{Z}_n$, then $\mathcal{D}$ is a PCDP, or more precisely an (n, K, λ)-PCDP. For succinctness, we normally write the multiset K in exponential notation: $[k_1^{a_1} k_2^{a_2} \cdots k_s^{a_s}]$ denotes the multiset containing a_i occurrences of $k_i, i \in [s]$. The notion of PCDP is first introduced by Fuji-Hara *et al.* [2] in their investigation of frequency-hopping sequences, where it is referred to as "a partition type difference packing".

It is not hard to verify that the following are equivalent definitions of a PCDP:

i) $\mathcal{D}$ is an (n, K, λ)-PCDP if and only if $\mathcal{D}$ partitions $\mathbb{Z}_n$, and for any fixed $g \in \mathbb{Z}_n^\star$, the equation $x - y = g$ has at most λ solutions $(x, y) \in \cup_{D \in \mathcal{D}} D \times D$.
ii) For a set $D \subseteq \mathbb{Z}_n$, let

$$\Delta D = \{a - b : a, b \in D, a \neq b\}.$$

Then $\mathcal{D}$ is an (n, K, λ)-PCDP if and only if $\mathcal{D}$ partitions $\mathbb{Z}_n$, and the multiset

$$\Delta \mathcal{D} = \bigcup_{i=1}^{m} \Delta D_i$$

contains each element of $\mathbb{Z}_n$ at most λ times.

In the particular case where an (n, K, λ)-PCDP $\mathcal{D}$ satisfies $\Phi_{\mathcal{D}}(g) = \lambda$ for all $g \in \mathbb{Z}_n^\star$, it is known as a partitioned cyclic difference family (PCDF), or more precisely an (n, K, λ)-PCDF.

Given two positive integers n and $m < n$, it is obvious that any partition $\mathcal{D}$ of $\mathbb{Z}_n$ is an (n, K, λ)-PCDP for some λ. Furthermore, we have

$$\lambda \geq \left\lceil \frac{\sum_{i=1}^{m} |D_i|(|D_i| - 1)}{n-1} \right\rceil = \left\lceil \frac{\sum_{i=1}^{m} |D_i|^2 - n}{n-1} \right\rceil \quad (1)$$

since the multiset $\Delta\mathcal{D}$ contains $\sum_{i=1}^{m} |D_i|(|D_i| - 1)$ elements. The problem here we are concerned with is the construction of an (n, K, λ)-PCDP of m base blocks with its *index* λ as small as possible. Given n and $m < n$, the minimum λ for which there exists an (n, K, λ)-PCDP of m base blocks is denoted $\rho(n, m)$. An (n, K, λ)-PCDP of m base blocks is *optimal* if $\lambda = \rho(n, m)$.

From (1), it is clear that

$$\rho(n, m) \geq \left\lceil \frac{\sum_{i=1}^{m} |D_i|^2 - n}{n-1} \right\rceil. \quad (2)$$

The right side of (2) cannot be determined uniquely by the parameters n and m. To see when it attains the minimum for fixed n and $m < n$, we write $n = m\mu + \epsilon$ with $0 \leq \epsilon \leq m - 1$. It is well known that under the constraint $\sum_{i=1}^{m} |x_i| = n$, the sum $\sum_{i=1}^{m} x_i^2$ is minimized if and only if $|x_i - x_j| \leq 1$ for any $i, j \in [m]$. Hence, for an (n, K, λ)-PCDP $\mathcal{D} = \{D_1, \ldots, D_m\}$, the sum $\sum_{i=1}^{m} |D_i|^2$ attains the minimum if and only if $\mathcal{D}$ contains exactly ϵ base blocks of size $\mu + 1$ and $m - \epsilon$ base blocks of size μ. Consequently, we have

$$\begin{aligned}
\left\lceil \frac{\sum_{i=1}^{m} |D_i|^2 - n}{n-1} \right\rceil &= \left\lceil \frac{\epsilon(\mu+1)^2 + (m-\epsilon)\mu^2 - m\mu - \epsilon}{n-1} \right\rceil \\
&= \left\lceil \frac{2\epsilon\mu + m\mu^2 - m\mu}{n-1} \right\rceil \\
&= \left\lceil \frac{2\epsilon\mu + (n-\epsilon)(\mu-1)}{n-1} \right\rceil \\
&= \left\lceil \frac{(n-1)(\mu-1) + (\epsilon\mu + \epsilon + \mu - 1)}{n-1} \right\rceil \\
&= \left\lceil (\mu - 1) + \frac{\epsilon\mu + \epsilon + \mu - 1}{n-1} \right\rceil \\
&= \mu. \quad (3)
\end{aligned}$$

The last equality in (3) follows from the fact that $0 < \epsilon\mu + \epsilon + \mu - 1 \leq n - 1$, since $n = m\mu + \epsilon > m$ and $0 \leq \epsilon \leq m - 1$.

It now follows from (2) and (3) that for any positive integers m and $n = m\mu + \epsilon > m$ with $0 \leq \epsilon \leq m - 1$

$$\rho(n, m) \geq \mu. \quad (4)$$

We remark that for given positive integers n and $m < n$, there may exist many optimal (n, K, λ)-PCDPs attaining the bound in (4). We also note that the lower bound on the function $\rho(n, m)$ in (4) is not always attainable.

The construction of optimal PCDPs have been studied by a number of authors. For more detailed information on PCDPs and known results, the reader is referred to [2] and [4] and references therein. In this paper, we make further investigation into optimal PCDPs. The paper is organized as follows. In Section III, we present the relationship among PCDPs, frequency-hopping sequences, and comma-free codes. Sections IV–VI are devoted to constructions of PCDPs, by which a number of new infinite classes of optimal PCDPs are produced. The existence of (optimal) $(3m, [3^m], 3)$-PCDPs is also determined for all $m \not\equiv 8, 16 \pmod{24}$. As a consequence, new infinite families of optimal frequency-hopping sequences and comma-free codes are obtained.

III. Applicationsof PCDP

PCDPs are closely related to frequency-hopping sequences and comma-free codes. We develop their relationship in this section.

A. PCDPs and Frequency-Hopping Sequences

Let $F = \{f_1, f_2, \ldots, f_m\}$ be a set of available frequencies, called a *frequency library*. As usual, F^n denotes the set of all sequences of length n over F. An element of F^n is called a *frequency-hopping sequence* (FH sequence). Given two FH sequences $X = (x_0, x_1, \ldots, x_{n-1})$ and $Y = (y_0, y_1, \ldots, y_{n-1})$, define their *Hamming correlation* $H_{X,Y}(t)$ to be

$$H_{X,Y}(t) = \sum\nolimits_{i \in \mathbb{Z}_n} h[x_i, y_{i+t}], \quad t \in \mathbb{Z}_n$$

where

$$h[x, y] = \begin{cases} 1, & \text{if } x = y \\ 0, & \text{otherwise} \end{cases}$$

and all operations among position indices are performed in $\mathbb{Z}_n$. Further, define

$$H(X) = \max_{t \in \mathbb{Z}_n^\star} H_{X,X}(t).$$

An FH sequence $X \in F^n$ is called *optimal* if $H(X) \leq H(X')$ for all $X' \in F^n$. Here we assume that all transmitters use the same FH sequence, starting from different time slots. An FH sequence $X \in F^n$ with $H(X) = \lambda$ is called an (n, m, λ)-FH sequence.

FHSS and direct-sequence spread spectrum are two main spread coding technologies. In modern radar and communication systems, FHSS techniques have become very popular. FH sequences are used to specify which frequency will be used for transmission at any given time. Fuji-Hara *et al.* [2] investigated frequency-hopping multiple access (FHMA) systems with a single optimal FH sequence using a combinatorial approach. They established the correspondence between frequency-hopping sequences and PCDPs. To be more precise, they labeled a frequency library F of size m by $\mathbb{Z}_m$ and demonstrated that the set of position indices of an (n, m, λ)-FH sequence X gives an (n, K, λ)-PCDP where $\lambda = H(X)$, and vise versa. We state this correspondence in the following theorem using our notations.

Theorem 3.1 (Fuji-Hara et al. [2]): There exists an optimal (n, m, λ)-FH sequence X over the set of frequencies $F = \mathbb{Z}_m$ if and only if there exists an optimal (n, K, λ)-PCDP of m base blocks.

Theorem 3.1 reveals that in order to construct optimal FH sequences, one needs only to construct optimal PCDPs. This serves as the motivation behind our consideration of PCDPs.

B. PCDPs and Comma-Free Codes

Consider the process of transmitting data over a channel, where the data being sent is a stream of symbols from an alphabet Q of size q. The data stream consists of consecutive messages, each being a sequence of n consecutive symbols

$$\cdots \underbrace{x_1 \cdots x_n} \underbrace{y_1 \cdots y_n} \cdots .$$

The synchronization problem that arises at the receiving end is the task of correctly partitioning the data stream into messages of length n, as opposed to incorrectly conceiving a sequence of n symbols that is the concatenation of the end of one message with the beginning of another message as a single message:

$$\cdots \underbrace{x_{i+1} \cdots x_n} \underbrace{y_1 \cdots y_i} \cdots .$$

One way to resolve the synchronization problem uses comma-free codes. A code is a set $\mathcal{C} \subseteq Q^n$, with its elements called *codewords*. $\mathcal{C}$ is termed a *comma-free code* if the *concatenation*

$$T_i(x, y) = x_{i+1} \cdots x_n y_1 \cdots y_i$$

of any two not necessarily distinct codewords $x = (x_1 \cdots x_n)$ and $y = (y_1 \cdots y_n)$ is never a codeword. More generally, associated with a code $\mathcal{C} \subseteq Q^n$, one can define its *comma-free index* $I(\mathcal{C})$ as

$$I(\mathcal{C}) = \min_{x,y,z \in \mathcal{C} \text{ and } i \in [n-1]} d_H(T_i(x, y), z)$$

where $d_H(\cdot, \cdot)$ denotes the Hamming distance function. If $I(\mathcal{C}) > 0$, then $\mathcal{C}$ is a comma-free code, and hence we can distinguish a codeword from a concatenation of two codewords even in the case when up to $\lfloor (I(\mathcal{C}) - 1)/2 \rfloor$ errors have occurred [5], [6].

Codes with prescribed comma-free index can be constructed by using difference systems of sets (DSS), a combinatorial structure introduced by Levenshtein [3] (see also [6], [7]). An (n, K, η)-DSS is a collection $\mathcal{F} = \{D_1, D_2, \ldots, D_m\}$ of m disjoint subsets of $\mathbb{Z}_n$ such that the multiset

$$\{a - b \pmod n : a \in D_i, b \in D_j, i, j \in [m] \text{ and } i \neq j\}$$

contains each element of $\mathbb{Z}_n^\star$ at least η times, where $K = [|D| : D \in \mathcal{F}]$. Application of DSS to code synchronization requires that the *redundancy*

$$r_m(n, \eta) = \sum_{i=1}^{m} |D_i|$$

be as small as possible. Levenshtein [3] proved that

$$r_m(n, \eta) \geq \sqrt{\frac{\eta m(n-1)}{m-1}}. \tag{5}$$

For more detailed information on comma-free codes, the reader is referred to [6], [7] and the references therein. Here, we are interested in the link between PCDP and DSS, which is stated in the following theorem.

Theorem 3.2: Let m and $n = m\mu + \epsilon > m$ be positive integers and $0 \leq \epsilon \leq m - 1$. If an $(m\mu + \epsilon, [(\mu + 1)^\epsilon \mu^{m-\epsilon}], \mu)$-PCDP exists, then so does an $(n, [(\mu + 1)^\epsilon \mu^{m-\epsilon}], \eta)$-DSS of minimum redundancy n, where $\eta = n - \mu = (m-1)\mu + \epsilon$.

Proof: Let $\mathcal{D} = \{D_1, D_2, \ldots, D_m\}$ be an $(n, [(\mu + 1)^\epsilon \mu^{m-\epsilon}], \mu)$-PCDP. By definition of a PCDP, we have

$$\mu = \max_{g \in \mathbb{Z}_n^\star} \Phi_{\mathcal{D}}(g).$$

Let us define $\Gamma_{\mathcal{D}} : \mathbb{Z}_n^\star \to \mathbb{Z}$ such that

$$\Gamma_{\mathcal{D}}(g) = \sum_{i,j \in [m], i \neq j} |(D_i + g) \cap D_j|.$$

It follows that

$$\Phi_{\mathcal{D}}(g) + \Gamma_{\mathcal{D}}(g) = |(\mathbb{Z}_n + g) \cap \mathbb{Z}_n| = n,$$

for any $g \in \mathbb{Z}_n^\star$. Furthermore

$$\begin{aligned} \min_{g \in \mathbb{Z}_n^\star} \Gamma_{\mathcal{D}}(g) &= \min_{g \in \mathbb{Z}_n^\star} (n - \Phi_{\mathcal{D}}(g)) \\ &= n - \max_{g \in \mathbb{Z}_n^\star} \Phi_{\mathcal{D}}(g) \\ &= n - \mu. \end{aligned}$$

Hence, $\mathcal{D}$ is an $(n, [(\mu+1)^\epsilon \mu^{m-\epsilon}], \eta)$-DSS for $\eta = n - \mu$ and with redundancy $r_m(n, \eta) = n$. We now prove this redundancy to be minimum. Since $\eta = n - \mu$ and $n = m\mu + \epsilon$, the right side of the inequality (5) equals

$$\begin{aligned} \sqrt{\frac{\eta m(n-1)}{m-1}} &= \sqrt{\frac{m(n-\mu)(n-1)}{m-1}} \\ &= \sqrt{\frac{m(n-1)n - m\mu(n-1)}{m-1}} \\ &= \sqrt{\frac{m(n-1)n - (n-\epsilon)(n-1)}{m-1}} \\ &= \sqrt{\frac{(m-1)(n-1)n + \epsilon(n-1)}{m-1}}. \end{aligned}$$

This implies

$$n - 1 < \sqrt{\frac{\eta m(n-1)}{m-1}} < n$$

since $0 \leq \epsilon \leq (n-1)(m-1)$. □

Theorem 3.2 shows that the DSS derived from a PCDP of minimum index has minimum redundancy, and hence produces optimal comma-free codes with respect to the bound (5). This serves to provide another motivation behind the study of PCDPs.

IV. Constructions From Almost Difference Sets

An almost difference set in an additive group G of order n, or an $(n, k, \lambda; t)$-ADS in short, is a k-subset D of G such that the multiset $\{a - b : a, b \in D \text{ and } a \neq b\}$ contains t nonzero elements of G, each exactly λ times, and each of the remaining $n-1-t$ nonzero elements exactly $\lambda+1$ times. This is equivalent to saying that

$$\Phi_{\{D\}}(g) = |(D + g) \cap D|.$$

takes on the value λ exactly t times and the value $\lambda + 1$ exactly $n - 1 - t$ times, when g ranges over all the nonzero elements

of G. An obvious necessary condition for the existence of a $(n,k,\lambda;t)$-ADS is

$$(\lambda+1)(n-1)\equiv t \pmod{k(k-1)}.$$

In the extreme case where $t=n-1$, an $(n,k,\lambda;t)$-ADS is an (n,k,λ) *difference set* in the usual sense (see [8]). It should be apparent to the reader that an $(n,k,\lambda;t)$-ADS in $\mathbb{Z}_n$ is an $(n,\{k\},\lambda+1)$-CDP.

In this section, we construct new optimal PCDPs from almost difference sets. We begin with the following result.

Proposition 4.1: Let $n=2\mu$ be a positive integer and let D be a μ-subset of $\mathbb{Z}_n$. Let $\widehat{D}=\mathbb{Z}_n\setminus D$. If one of D and $\widehat{D}$ is an $(n,\mu,\lambda;t)$-ADS in $\mathbb{Z}_n$, then so is the other.

Proof: We need only prove that

$$\Phi_{\{D\}}(g)=\Phi_{\{\widehat{D}\}}(g)$$

for any $g\in\mathbb{Z}_{2\mu}^{\star}$. In fact, since $\{D,\widehat{D}\}$ is a partition of $\mathbb{Z}_{2\mu}$, and $|D|=|\widehat{D}|=\mu$, we have

$$|D\cap(D+g)|+|D\cap(\widehat{D}+g)|=\mu=|D\cap(\widehat{D}+g)|+|\widehat{D}\cap(\widehat{D}+g)|.$$

Hence,

$$\Phi_{\{D\}}(g)=\mu-|D\cap(\widehat{D}+g)|=\Phi_{\{\widehat{D}\}}(g).$$

This equality does not depend on the choice of $g\in\mathbb{Z}_{2\mu}^{\star}$. □

As an immediate consequence of Proposition 4.1, we have the following corollary.

Corollary 4.1: Let $n=2\mu$, $n\equiv 2 \pmod 4$. Then $\rho(n,2)$ cannot attain the lower bound μ in (4), that is, $\rho(n,2)\geq\mu+1=(n+2)/2$.

Proof: By assumption, $n=m\mu+\epsilon$ with $m=2$, $\mu=n/2$ and $\epsilon=0$. Since $n\equiv 2 \pmod 4$, μ is odd. On the other hand, for any $(2\mu,[\mu^2],\lambda)$-PCDP $\mathcal{D}=\{D_1,D_2\}$, we have

$$\Phi_{\mathcal{D}}(g)=\Phi_{\{D_1\}}(g)+\Phi_{\{D_2\}}(g)=2\Phi_{\{D_1\}}(g)$$

by Proposition 4.1. So, λ must be even. Hence, an $(n,[(n/2)^2],\mu)$-PCDP cannot exist, which implies $\rho(n,2)\geq\mu+1=(n+2)/2$. □

Now we turn to constructions.

Proposition 4.2: Let $n\equiv 0 \pmod 4$. If there exists an $(n,n/2,(n-4)/4;n/4)$-ADS in $\mathbb{Z}_n$, then there exists an optimal $(n,[(n/2)^2],n/2)$-PCDP.

Proof: Let D be the given $(n,n/2,\lambda;t)$-ADS in $\mathbb{Z}_n$, where $\lambda=(n-4)/4$ and $t=n/4$. Let $\widehat{D}=\mathbb{Z}_n\setminus D$. Then $\mathcal{D}=\{D,\widehat{D}\}$ is a partition of $\mathbb{Z}_n$ and as in the proof of Proposition 4.1, we have

$$\begin{aligned}\Phi_{\mathcal{D}}(g)&=|D\cap(D+g)|+|\widehat{D}\cap(\widehat{D}+g)|\\&=\Phi_{\{D\}}(g)+\Phi_{\{\widehat{D}\}}(g)\\&=2\Phi_{\{D\}}(g).\end{aligned}$$

Hence, for any $g\in\mathbb{Z}_n^{\star}$, $\Phi_{\mathcal{D}}(g)$ takes on the value $(n-4)/2$ exactly $t=n/4$ times and takes on the value $n/2$ exactly $n-1-t=(3n-4)/4$ times. Therefore, $\mathcal{D}$ is an $(n,[(n/2)^2],n/2)$-PCDP. Its optimality follows immediately from (4). □

Proposition 4.3: Let $n\equiv 2 \pmod 4$. If there exists an $(n,n/2,(n-2)/4;(3n-2)/4)$-ADS in $\mathbb{Z}_n$, then there exists an optimal $(n,[(n/2)^2],(n+2)/2)$-PCDP.

Proof: Employing the same technique as in the proof of Proposition 4.2, we form an $(n,[(n/2)^2],(n+2)/2)$-PCDP. The fact that its index attains the minimum follows from Corollary 4.1. □

Almost difference sets in Abelian groups have been well studied in terms of sequences with optimal autocorrelation [9], [10] and are known to exist for certain parameters n,k,λ and t. Before stating the known results on almost difference sets in $\mathbb{Z}_n$, some terminologies from finite fields are needed. Let q be a prime power. The finite field of q elements is denoted $\mathbb{F}_q$. Let ω be a primitive element of $\mathbb{F}_q$. For e dividing $q-1$, define $D_i^{(e,q)}=\omega^i\langle\omega^e\rangle$, where $\langle\omega^e\rangle$ is the unique multiplicative subgroup of $\mathbb{F}_q$ spanned by ω^e. For $0\leq h\neq r\leq e-1$, define

$$(h,r)_e=|(D_h^{(e,q)}+1)\cap D_r^{(e,q)}|.$$

These constants $(h,r)_e$ are known as cyclotomic numbers of order e. The number $(h,r)_e$ is the number of solutions to the equation $x+1=y$, where $x\in D_h^{(e,q)}$ and $y\in D_r^{(e,q)}$. The following results are known.

Proposition 4.4 (Lempel et al. [9]): Let q be an odd prime power and let $D=\log_\omega(D_1^{(2,q)}-1)$. Then:

i) D is a $(q-1,(q-1)/2,(q-3)/4,(3q-5)/4)$-ADS in $\mathbb{Z}_{q-1}$, provided $q\equiv 3 \pmod 4$;
ii) D is a $(q-1,(q-1)/2,(q-5)/4,(q-1)/4)$-ADS in $\mathbb{Z}_{q-1}$ provided $q\equiv 1 \pmod 4$.

Proposition 4.5 (Ding et al. [11]): Let $p\equiv 5 \pmod 8$ be an odd prime. It is known that $p=s^2+4t^2$ for some s and t with $s\equiv\pm 1 \pmod 4$. Set $n=2p$. Let $i,j,l\in\{0,1,2,3\}$ be three pairwise distinct integers, and

$$D_{(i,j,l)}=\Big[\{0\}\oplus(D_i^{(4,p)}\cup D_j^{(4,p)})\Big]\bigcup\Big[\{1\}\oplus(D_l^{(4,p)}\cup D_j^{(4,p)})\Big]\bigcup\{(0,0)\}.$$

Then $D_{(i,j,l)}$ is an $(n,n/2,(n-2)/4,(3n-2)/4)$-ADS in $\mathbb{Z}_2\oplus\mathbb{Z}_p$, being isomorphic to $\mathbb{Z}_{2p}$ when:

i) $t=1$ and $(i,j,l)\in\{(0,1,3),(0,2,3),(1,2,0),(1,3,0)\}$; or
ii) $s=1$ and $(i,j,l)\in\{(0,1,2),(0,3,2),(1,0,3),(1,2,3)\}$.

Combining the results of Propositions 4.2–4.5 gives us new optimal PCDPs as follows.

Theorem 4.1: There exist:

i) an optimal $(q-1,[(q-1/2)^2],(q-1)/2)$-PCDP for any prime power $q\equiv 1 \pmod 4$;

ii) an optimal $(n, [(n/2)^2], (n+2)/2)$-PCDP if $n = 2p$ or $n = q-1$ where $q \equiv 3 \pmod 4$ is a prime power and $p \equiv 5 \pmod 8$ is a prime.

V. Constructions From Cyclic Difference Matrices

Consider a $k \times n$ matrix $\mathsf{M} = (m_{ij})$, $i \in [k]$, $j \in [n]$, whose entries are taken from an additive group G of order n. If for any two distinct row indices $r, s \in [k]$, the differences $m_{rj} - m_{sj}$, $j \in [n]$, comprise all the elements of G, then the matrix M is said to be an $(n, k, 1)$ *difference matrix* (DM), or an $(n, k, 1)$-DM over G.

Our constructions require a difference matrix over the cyclic group of order n, that is $G = \mathbb{Z}_n$. In this case, the difference matrix is called *cyclic* and is denoted by $(n, k, 1)$-CDM. A cyclic DM is *normalized* if all entries in its first row and first column are zero. The property of a cyclic DM is preserved even if we add an element of $\mathbb{Z}_n$ to all entries in any row or column of the matrix. Hence, without loss of generality, one can always assume that a cyclic DM is normalized. If we delete the first row from a normalized $(n, k, 1)$-CDM, then we obtain a *derived* $(n, k-1, 1)$-CDM, each of whose rows forms a permutation on $\mathbb{Z}_n$. We adopt the terminology used in [2] and call the derived $(n, k-1, 1)$-CDM *homogeneous*. In a homogeneous cyclic DM, every row forms a permutation on the elements of $\mathbb{Z}_n$ and the entries in the first column are all zero. From the point of view of existence, a $(n, k, 1)$-CDM is obviously equivalent to a homogeneous $(n, k-1, 1)$-CDM, and we use the terms $(n, k, 1)$-CDM and homogeneous $(n, k-1, 1)$-CDM interchangeably.

Difference matrices have attracted considerable attention in design theory, since they can often be used as building blocks for other combinatorial objects. The multiplication table of $\mathbb{F}_q$ constitutes a normalized $(q, q, 1)$-DM. When q is a prime, it is a normalized $(q, q, 1)$-CDM. Hence, a homogeneous $(q, q-1, 1)$-CDM exists for any prime q. Deleting $q - 1 - k$ rows from this cyclic DM produces a homogeneous $(q, k, 1)$-CDM. We record this fact below.

Proposition 5.1: Let p be a prime and k an integer satisfying $2 \le k \le p-1$. Then there exists a homogeneous $(p, k, 1)$-CDM.

The following product construction for cyclic DMs is known (see, for example, [12] and [13]).

Proposition 5.2: If a homogeneous $(n_1, k, 1)$-CDM and a homogeneous $(n_2, k, 1)$-CDM both exist, then so does a homogeneous $(n_1 n_2, k, 1)$-CDM.

Propositions 5.1 and 5.2 now give the following existence result.

Proposition 5.3: Let $n \ge 3$ be an integer whose prime factors are at least the prime p. Then for any integer k satisfying $2 \le k \le p-1$, a homogeneous $(n, k, 1)$-CDM exists.

We also need the following result.

Proposition 5.4 (Ge [12]): Let $n \ge 5$ be an odd integer with $\gcd(n, 27) \ne 9$. Then there exists a homogeneous $(n, 3, 1)$-CDM.

Now we develop our constructions to obtain optimal PCDPs from cyclic DMs.

Theorem 5.1: Let m and μ be two positive integers. If a homogeneous $(m, \mu, 1)$-CDM exists, then so does an optimal $(m\mu, [\mu^m], \mu)$-PCDP.

Proof: Let $\mathsf{M} = (m_{ij})$, $i \in [\mu]$, $j \in [m]$, be a homogeneous $(m, \mu, 1)$-CDM over $\mathbb{Z}_m$. From M we construct another $\mu \times m$ matrix R whose entries are taken from $\mathbb{Z}_{m\mu}$ by replacing every entry m_{ij} of M with $i - 1 + m_{ij}\mu$, $i \in [\mu]$, $j \in [m]$. Write D_j for the μ-subset of $\mathbb{Z}_{m\mu}$ consisting of the elements on the j-th column of R, $j \in [m]$. Write

$$\mathcal{D} = \{D_1, D_2, \ldots, D_m\}.$$

Then the properties of a homogeneous $(m, \mu, 1)$-CDM guarantee the following conclusions:

- $\mathcal{D}$ partitions $\mathbb{Z}_{m\mu}$.
- Let $H = \mu\mathbb{Z}_m = \{j\mu : 0 \le j \le m-1\}$ be the unique additive subgroup of order m in $\mathbb{Z}_{m\mu}$. Then, for any nonzero element $g \in \mathbb{Z}_{m\mu}$, we have

$$\Phi_{\mathcal{D}}(g) = \begin{cases} 0, & \text{if } g \in H \\ \mu, & \text{otherwise.} \end{cases}$$

Therefore, $\mathcal{D}$ is an $(m\mu, [\mu^m], \mu)$-PCDP, and it is optimal, since its index meets the bound in (4). □

Applying Theorem 5.1 and Proposition 5.3, we obtain the following new infinite family of optimal PCDPs.

Theorem 5.2: Let $m \ge 3$ be an integer whose prime factors are not less than prime p. Then for any integer μ satisfying $2 \le \mu \le p-1$, an optimal $(m\mu, [\mu^m], \mu)$-PCDP exists.

Example 5.1: In Theorem 5.1, take $m = 7$, $\mu = 3$, and consider the homogeneous $(m, \mu, 1)$-CDM

$$\mathsf{M} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 0 & 3 & 6 & 2 & 5 & 1 & 4 \end{bmatrix}.$$

Replace each entry m_{ij} of M with $i - 1 + 3m_{ij}$, $i \in [3]$, $j \in [7]$, to obtain the 3×7 matrix over $\mathbb{Z}_{21}$

$$\mathsf{R} = \begin{bmatrix} 0 & 3 & 6 & 9 & 12 & 15 & 18 \\ 1 & 7 & 13 & 19 & 4 & 10 & 16 \\ 2 & 11 & 20 & 8 & 17 & 5 & 14 \end{bmatrix}.$$

Finally, take the columns of R as base blocks over $\mathbb{Z}_{21}$

$$\begin{aligned} &D_1 = \{0, 1, 2\} \quad D_2 = \{3, 7, 11\} \quad D_3 = \{6, 13, 20\} \\ &D_4 = \{8, 9, 19\} \quad D_5 = \{4, 12, 17\} \quad D_6 = \{5, 10, 15\} \\ &D_7 = \{14, 16, 18\}. \end{aligned}$$

It is readily checked that $\mathcal{D} = \{D_1, D_2, \ldots, D_7\}$ is an optimal $(21, [3^7], 3)$-PCDP, as desired.

The following result is a variant of Theorem 5.1.

Proposition 5.5: Let p be an odd prime. Then an optimal $(p^2, [\mu^{m-1}(\mu+1)^1], \mu)$-PCDP exists, where $m = p+1$ and $\mu = p-1$.

Proof: By Proposition 5.1, there exists $\mathsf{M} = (m_{ij})$, $i \in [p-1]$, $j \in [p]$, which is a homogeneous $(p, p-1, 1)$-CDM over $\mathbb{Z}_p$. As in the proof of Theorem 5.1, we construct a $(p-1) \times p$ matrix R whose entries are taken from $\mathbb{Z}_{p^2}$ by replacing every entry m_{ij} of M with $i + m_{ij}p$, $i \in [p-1]$, $j \in [p]$. Then we write D_j for the $(p-1)$-subset of $\mathbb{Z}_{p^2}$ consisting of the elements on the j-th column of R for $j \in [p]$. Then

$$\mathcal{D} = \{D_1, D_2, \ldots, D_p\}$$

is a cyclic difference packing. Observe that the rows of R are indexed by the elements of $\mathbb{Z}_p^\star$. Hence, $\mathcal{D}$ is a partition of $\mathbb{Z}_{p^2} \setminus p\mathbb{Z}_p$. On the other hand, we have

$$\Phi_{\mathcal{D}}(g) = \begin{cases} 0, & \text{if } g \in p\mathbb{Z}_p \\ p-2, & \text{otherwise.} \end{cases}$$

For the desired PCDP, let $\widehat{D_1} = D_1 \cup \{0\}$ and $D_{p+1} = \{jp : j \in [p-1]\}$. It turns out that

$$\mathcal{F} = (\mathcal{D} \setminus \{D_1\}) \bigcup \{\widehat{D_1}, D_{p+1}\}$$

is a $(p^2, [\mu^{m-1}(\mu+1)^1], \mu)$-PCDP. Its optimality is straightforward to verify. □

Example 5.2: In Proposition 5.5, take $p = 5$ (and hence $m = 6$ and $\mu = 4$), and consider the homogeneous (5, 4, 1)-CDM

$$\mathsf{M} = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 2 & 4 & 1 & 3 \\ 0 & 3 & 1 & 4 & 2 \\ 0 & 4 & 3 & 2 & 1 \end{bmatrix}.$$

Its corresponding 4×5 matrix R over $\mathbb{Z}_{25}$ is given by

$$\mathsf{R} = \begin{bmatrix} 1 & 6 & 11 & 16 & 21 \\ 2 & 12 & 22 & 7 & 17 \\ 3 & 18 & 8 & 23 & 13 \\ 4 & 24 & 19 & 14 & 9 \end{bmatrix}.$$

Then an optimal $(25, [4^5 5^1], 4)$-PCDP is formed by the following base blocks over $\mathbb{Z}_{25}$:

$$\begin{aligned} \widehat{D_0} &= \{0, 1, 2, 3, 4\} \quad & D_1 &= \{6, 12, 18, 24\} \\ D_2 &= \{8, 11, 19, 22\} \quad & D_3 &= \{7, 14, 16, 23\} \\ D_4 &= \{9, 13, 17, 21\} \quad & D_5 &= \{5, 10, 15, 20\}. \end{aligned}$$

Based on Proposition 5.5, we can establish the following new infinite series of optimal PCDPs.

Theorem 5.3: Let p be an odd prime and $n \geq 2$. Then an optimal $(p^n, [\mu^{m-1}(\mu+1)^1], \mu)$-PCDP exists, where $m = \frac{p^n-1}{p-1}$ and $\mu = p-1$.

Proof: The proof is by induction on n. If $n = 2$, the conclusion holds by Proposition 5.5. Now suppose that the assertion is true when $n = k \geq 3$. Consider the case $n = k+1$. From Proposition 5.2, we know that a homogeneous $(p^k, p-1, 1)$-CDM exists. Employing the same technique as in the proof of Proposition 5.5, from this CDM we can form a collection

$$\mathcal{D} = \{D_1, D_2, \ldots, D_{p^k}\}$$

of $(p-1)$-subsets of $\mathbb{Z}_{p^{k+1}}$ in such a way that

- $\mathcal{D}$ partitions $\mathbb{Z}_{p^{k+1}} \setminus p\mathbb{Z}_{p^k}$;
- for any $g \in \mathbb{Z}_{p^{k+1}}^\star$

$$\Phi_{\mathcal{D}}(g) = \begin{cases} 0, & \text{if } g \in p\mathbb{Z}_{p^k} \\ p-2, & \text{otherwise.} \end{cases}$$

Since $p\mathbb{Z}_{p^k}$ is isomorphic to $\mathbb{Z}_{p^k}$, by our induction hypothesis we can construct an optimal PCDP $\mathcal{F}$ of index $p-1$ in $p\mathbb{Z}_{p^k}$, which has exactly $\frac{p^k-1}{p-1} - 1$ base blocks of size $p-1$ and one base block of size p. It can be checked that $\mathcal{D} \cup \mathcal{F}$ is an optimal $(p^{k+1}, [(p-1)^{\frac{p^{k+1}-1}{p-1}-1} p^1], p-1)$-PCDP. □

VI. The Existence of $(3m, [3^m], 3)$-PCDPs

In this section, the existence of $(3m, [3^m], 3)$-PCDP is settled for all $m \not\equiv 8, 16 \pmod{24}$. PCDPs with such parameters are optimal. Our proof technique requires a generalization of cyclic difference matrices.

Let G be a cyclic group of order n containing a subgroup H of order w. A $k \times (n-w)$ matrix $\mathsf{M} = (m_{ij})$, $i \in [k]$, $j \in [n-w]$, with entries from $\mathbb{Z}_n$ is said to be a *holey* DM if for any two distinct row indices r and s of M, $r, s \in [k]$, the differences $m_{rj} - m_{sj}$, $j \in [n-w]$, comprise all the element of $G \setminus H$. For convenience, we refer to such a matrix M as an $(n, k, 1; w)$-HDM over $(G; H)$, or simply an $(n, k, 1; w)$-HDM when G and H are clear from the context. H is the *hole* of the holey DM.

The property of a holey DM is preserved even if we add any element of $\mathbb{Z}_n$ to any column of the matrix. Hence, without loss of generality, one can always assume that the all entries in the first row of an holey DM are zero. If we delete the first row from such a holey DM, then we obtain an $(n, k-1, 1; w)$-HDM, where the entries of a row consist of all the elements of $G \setminus H$, and we term the derived $(n, k-1, 1; w)$-HDM *homogeneous*. Because of this equivalence, we use the terms $(n, k, 1; w)$-HDM and homogeneous $(n, k-1, 1; w)$-HDM interchangeably.

We introduce one more object which is crucial to the construction for PCDPs in this section. Let G be a cyclic group of order n. A *partial* DM of order n (denoted $\mathrm{PDM}(n)$) is a $3 \times (n-3)$ matrix $\mathsf{M} = (m_{ij})$ with entries from G such that the entries in each row of M are distinct, and for any two distinct row indices $r, s \in [3]$, the differences $m_{rj} - m_{sj}$, $j \in [q-3]$, contains each element of G at most once. In addition, if the three sets of missing elements $D_i = G \setminus \cup_{j=1}^{q-3} \{m_{ij}\}$, $i \in [3]$, and the multiset of differences $\cup_{i=1}^{3} \{x - y : x, y \in D_i \text{ and } x \neq y\}$ contain each element of G at most three times, we called the partial DM *extendible*.

Example 6.1: An extendible PDM(8) over $\mathbb{Z}_8$

$$\begin{bmatrix} 2 & 3 & 6 & 7 & 4 \\ 1 & 6 & 3 & 5 & 4 \\ 7 & 1 & 5 & 2 & 0 \end{bmatrix}.$$

The three sets of missing elements are {0, 1, 5}, {0, 2, 7}, and {4, 3, 6}.

The following proposition gives the connection between extendible partial DMs and $(3m, [3^m], 3)$-PCDPs.

Proposition 6.1: Suppose there exists an extendible $\mathrm{PDM}(m)$. Then there exists a $(3m, [3^m], 3)$-PCDP.

Proof: For each column $[a, b, c]^T$ of the $\mathrm{PDM}(m)$, we construct a base block $\{3c, 3b + 1, 3a + 2\}$ of the PCDP. If $D_i = \{a, b, c\}$ is the set of missing element in row $i, i \in [3]$, we construct a base block $\{3a+3-i, 3b+3-i, 3c+3-i\}$ of the PCDP. This gives a total of m base blocks. It is easy to check that the conditions of an extendible partial DM ensure that the base blocks form a PCDP. □

The usefulness of holey DMs stems from the fact that they can be used to produce large extendible partial DMs by "filling in" the hole of a holey DM with a smaller extendible partial DM.

Proposition 6.2 (Filling in Hole): Suppose there exist a homogeneous $(m, 3, 1; w)$-HDM and an extendible $\mathrm{PDM}(w)$. Then there exists an extendible $\mathrm{PDM}(m)$.

Proof: Multiple each entry of the extendible $\mathrm{PDM}(w)$ by m/w and add the columns of the resulting matrix to the homogeneous $(m, 3, 1; w)$-HDM to obtain an extendible $\mathrm{PDM}(m)$. □

In view of Proposition 6.1, we employ a combination of construction techniques for extendible $\mathrm{PDM}(m)$ and $(3m, [3^m], 3)$-PCDP. The technique is recursive and so we begin with some required small ingredients in the next subsection.

A. Small Ingredients

Lemma 6.1: There exists a $(3m, [3^m], 3)$-PCDP for $m \in \{3, 9\}$

Proof: When $m = 3$, take as base blocks {0, 1, 5}, {3, 4, 8}, and {6, 7, 2}.

When $m = 9$, take as base blocks {0, 1, 2}, {3, 4, 6}, {5, 7, 10}, {8, 11, 16}, {9, 17, 22}, {12, 18, 24}, {13, 20, 26}, {14, 21, 25}, and {15, 19, 23}. □

Lemma 6.2: There exists an extendible $\mathrm{PDM}(m)$ for $m \in \{12, 16, 18, 24, 32, 54\}$.

Proof: An extendible PDM(12) is listed below:

$$\begin{bmatrix} 2 & 4 & 5 & 7 & 8 & 9 & 10 & 11 & 6 \\ 1 & 11 & 8 & 4 & 10 & 5 & 3 & 9 & 6 \\ 5 & 1 & 4 & 11 & 9 & 2 & 8 & 7 & 6 \end{bmatrix}.$$

The three sets of elements missing from each row are {0, 1, 3}, {0, 2, 7}, and {0, 3, 10}.

For $m \in \{16, 18, 24, 32, 54\}$, we start with the $(m, 4, 1; 2)$-HDM constructed in [14]. First, remove the row of all zeros from each holey DM. Then remove two columns as prescribed below:

- for $m = 16$: remove columns $[1, 2, 3]^T$ and $[-1, -2, -3]^T$;
- for $m = 18$: remove columns $[1, 2, 3]^T$ and $[-1, -2, -3]^T$;
- for $m = 24$: remove columns $[1, 2, 3]^T$ and $[-1, -2, -3]^T$;
- for $m = 32$: remove columns $[1, 2, 3]^T$ and $[-1, -2, -3]^T$;
- for $m = 54$: remove columns $[1, 10, 2]^T$ and $[2, 12, 5]^T$.

Finally, add the column $[m/2, m/2, m/2]^T$. The resulting matrices have $m-3$ columns and the sets of missing elements each row are:

- for $m = 16$: {0, 1, 15}, {0, 2, 14}, and {0, 3, 13}.
- for $m = 18$: {0, 1, 17}, {0, 2, 16}, and {0, 3, 15}.
- for $m = 24$: {0, 1, 23}, {0, 2, 22}, and {0, 3, 21}.
- for $m = 32$: {0, 1, 31}, {0, 2, 30}, and {0, 3, 29}.
- for $m = 54$: {0, 1, 2}, {0, 10, 12}, and {0, 2, 5}.

□

Lemma 6.3: There exists an extendible $\mathrm{PDM}(m)$ for all $m \in M$, where $M = \{36, 48, 64, 72, 96, 108, 128, 144, 162, 192, 256, 288, 384\}$.

Proof: For $m \in M \setminus \{36, 108, 288\}$, an $(m, 4, 1; w)$-HMD exists with $w \in \{8, 12, 16, 24\}$ [14]. Fill in the hole with an extendible $\mathrm{PDM}(w)$ (which exists by Example 6.1 or Lemma 6.2) to obtain an extendible $\mathrm{PDM}(m)$.

For $m = 36$, take the $(m, 4, 1; 2)$-HDM constructed in [13], remove the two columns $[1, 27, 2]^T$, $[28, 2, 1]^T$, and add the column $[18, 18, 18]^T$ to obtain a PDM(36).

For $m \in \{108, 288\}$, an $(m, 4, 1; w)$-HMD exists with $w \in \{12, 24\}$ [13]. Fill in the hole with an extendible $\mathrm{PDM}(w)$ (which exists by Lemma 6.2) to obtain an extendible $\mathrm{PDM}(m)$. □

B. Recursive Constructions

1) Recursive Constructions for Difference Matrices:

Proposition 6.3 (Inflation, Yin [13]): Suppose there exist an $(n, k, 1; w)$-HDM and an $(m, k, 1)$-CDM. Then there exists a $(mn, k, 1; mw)$-HDM.

In Proposition 6.3, the $(n, k, 1; w)$-HDM is said to be *inflated* by the $(m, k, 1))$-CDM to produce the $(mn, k, 1; mw)$-HDM.

Theorem 6.1 (Chang and Miao [14]): If there exists an $(m, 4, 1; 2)$-HDM, then there exists a $(64m, 4, 1; 4m)$-HDM and a $(72m, 4, 1; 12m)$-HDM.

2) Recursive Constructions for PCDP:

Proposition 6.4: Suppose there exist a $(3u, [3^u], 3)$-PCDP and a homogeneous $(v, 3, 1)$-CDM. Then there exists a $(3uv, 3^{uv}, 3)$-PCDP.

Proof: For each base block $\{a, b, c\}$ in the $(3u, [3^u], 3)$-PCDP, we construct v base blocks $\{a + 3ud_0, b + 3ud_1, c + 3ud_2\}$, where $[d_0, d_1, d_2]^T$ is a column of the homogeneous $(v, 3, 1)$-CDM. It is easy to check that the resulting collection of base blocks is a PCDP. □

Proposition 6.5: Suppose there exists a $(6m, 4, 1; 6)$-HDM. Then there exists an $(18m, [3^{6m}], 3)$-PCDP.

Proof: Suppose there exists a $(6m, 4, 1; 6)$-HDM, and hence a homogeneous $(6m, 3, 1; 6)$-HDM. For each column $[a, b, c]^T$ of the matrix, we construct a base block $\{3a, 3b + 1, 3c + 2\}$. Then add the six base blocks {0, 1, 2}, $\{m, m + 2, 3m\}$, $\{m + 1, 3m + 1, 4m + 1\}$, $\{2m, 3m + 2, 5m + 1\}$, $\{2m + 1, 4m + 2, 5m + 2\}$, $\{2m + 2, 4m, 5m\}$. This results in an $(18m, [3^{6m}], 3)$-PCDP. □

C. General Existence of Difference Matrices

Proposition 6.6: If $m > 3$ is prime and $m \equiv 3 \pmod 4$, then there exists an extendible $\mathrm{PDM}(2m)$.

Proof: We employ the construction of Dinitz and Stinson [15] for a $(2m, 4, 1; 2)$-HDM over $\mathbb{Z}_m \times \mathbb{Z}_2$. Choose any $c \in \mathbb{Z}_m^\star$ such that $c^2 - 1 \in \mathbb{Z}_m^{\boxtimes}$ (this is where $m > 3$ is required). Now let B_1 be as defined in (6), as shown at the bottom of the page. The $2(m-1)$ columns in B_1 form a homogeneous $(2m, 3, 1; 2)$-HDM over $\mathbb{Z}_m \times \mathbb{Z}_2$. Remove the columns $[1_0, c_0, (c+1)_0]^T$, $[4_0, 4c_0, 4(c+1)_0]^T$, and add the column $[0_1, 0_1, 0_1]^T$. It is easy to check that this results in an extendible $\mathrm{PDM}(2m)$. The sets of elements missing from the first row to the last row are $\{0_0, 1_0, 4_0\}$, $\{0_0, c_0, 4c_0\}$, and $\{0_0, (c+1)_0, 4(c+1)_0\}$, respectively. Finally, we note that $\gcd(m, 2) = 1$, and hence $\mathbb{Z}_m \times \mathbb{Z}_2 \simeq \mathbb{Z}_{2m}$, which is cyclic. □

Proposition 6.7: If $m \equiv 1 \pmod 4$ is a prime power, then there exists an extendible $\mathrm{PDM}(2m)$.

Proof: We employ the construction of Dinitz and Stinson [15] for a $(2m, 4, 1; 2)$-HDM over $\mathbb{Z}_m \times \mathbb{Z}_2$. Let ω be a primitive root in $\mathbb{Z}_m$ and let $c \in \mathbb{Z}_m^{\boxtimes}$. Let $t = (m-1)/4$, and define $Q = \{\omega^0, \omega^2, \ldots, \omega^{2t-2}\}$. Note that

$$Q \cup (-Q) \cup cQ \cup (-cQ) = \mathbb{Z}_m \setminus \{0\}.$$

Now let B_2 as defined in (7), as shown at the bottom of the page. Remove from B_2 the columns $\pm[1_1, c_1, (1+c)_0]^T$ and add the column $[0_1, 0_1, 0_1]^T$. The sets of elements missing from the first row to the last row are $\{0_0, 1_1, -1_1\}$, $\{0_0, c_1, -c_1\}$, and $\{0_0, (c+1)_0, -(c+1)_0\}$, respectively. Finally, we note that $\gcd(m, 2) = 1$, and hence $\mathbb{Z}_m \times \mathbb{Z}_2 \simeq \mathbb{Z}_{2m}$, which is cyclic. □

Theorem 6.2 (Yin [13]): Let $m \geq 4$ be a product of the form $2^\alpha 3^\beta p_1^{\alpha_1} \ldots p_t^{\alpha_t}$, where $p_j \geq 5$, $j \in [t]$. Then there exists a $(2m, 4, 1; w)$-HDM if one of the following conditions is satisfied:

i) $w = 2$ and $(\alpha, \beta) \neq (1, 0)$ or (0, 1);
ii) $w = 4$ and $(\alpha, \beta) = (1, 0)$;
iii) $w = 6$ and $(\alpha, \beta) = (0, 1)$.

D. Piecing Together

The easier case when m is odd is first addressed.

1) The Case $m \equiv 1 \pmod 2$:

Proposition 6.8: If m is odd, then there exists a $(3m, [3^m], 3)$-PCDP.

Proof: If $(m, 27) = 1$, then the result follows from Theorem 5.1. If $(m, 27) \in \{3, 9\}$, then apply Proposition 6.4 with $u = \gcd(m, 27)$ and $v = m/\gcd(m, 27)$. The existence of the ingredients is provided by Proposition 5.1 and Lemma 6.1. If $(m, 27) = 27$, then the result follows from Theorem 5.1 since there exists a homogeneous $(m, 3, 1)$-CDM [13]. □

2) The Case $m \equiv 0 \pmod 2$:

Proposition 6.9: If $m \equiv 2, 10 \pmod{12}$ and $m > 2$, then there exists a $(3m, [3^m], 3)$-PCDP.

Proof: Write $m = 2p_1^{\alpha_1} \ldots p_t^{\alpha_t}$, where $p_j \geq 5$, $j \in [t]$. Inflate a $(m/p_1, 4, 1; 2)$-HDM (which exists by Theorem 6.2) by a $(p_1, 4, 1)$-CDM (which exists by Proposition 5.1) to get an $(m, 4, 1, 2p_1)$-HDM. Fill in the hole with an extendible $\mathrm{PDM}(2p_1)$ from Proposition 6.6 or Proposition 6.7 to obtain an extendible $\mathrm{PDM}(m)$. The result now follows from Proposition 6.1. □

Proposition 6.10: Let $m \equiv 4, 20 \pmod{24}$. Then there exists a $(3m, [3^m], 3)$-PCDP.

Proof: By Theorem 6.2, there exists an $(m, 4, 1; 4)$-HDM, and therefore a homogeneous $(m, 3, 1; 4)$-HDM. For each column $[a, b, c]^T$ of the matrix, we construct a base block $\{a_0, b_1, c_2\}$ on $\mathbb{Z}_m \times \mathbb{Z}_3$. Since $\gcd(m, 3) = 1$, $\mathbb{Z}_m \times \mathbb{Z}_3 \simeq \mathbb{Z}_{3m}$. Add four blocks $(m/4)\{0, 1, 5\}$, $(m/4)\{2, 6, 9\}$, $(m/4)\{3, 4, 10\}$, and $(m/4)\{7, 8, 11\}$. It is easy to check that it gives the desired result. □

Proposition 6.11: Let $m \equiv 0 \pmod 6$. Then there exists a $(3m, [3^m], 3)$-PCDP.

Proof: Write $m = 2^a 3^b m'$, where $a, b \geq 1$ and $\gcd(m', 6) = 1$. We consider three cases:

$b = 1$: When $m' = 1$ and $a = 1$, apply Proposition 6.5 to a (6, 4, 1; 6)-HDM (which exists trivially) to obtain an $(18, [3^6], 3)$-PCDP.

When $m' = 1$ and $2 \leq a \leq 7$, the result is obtained by applying Proposition 6.1 to the extendible $\mathrm{PDM}(m)$s obtained from Lemma 6.2 and Lemma 6.3.

When $m' = 1$ and $a \geq 8$, take a $(2^{a-6} \cdot 3, 4, 1; 2)$-HDM, apply Theorem 6.1 to obtain a $(2^a \cdot 3, 4, 1; 2^{a-4} \cdot 3)$-HDM. Fill in the hole with an extendible $\mathrm{PDM}(2^{a-4} \cdot 3)$ (which exists by the induction hypothesis) to obtain an extendible $\mathrm{PDM}(2^a \cdot 3)$. Now apply Proposition 6.1.

When $m' > 1$ and $a = 1$, there exists a $(m, 4, 1; 6)$-HDM by Theorem 6.2. Now apply Proposition 6.5.

When $m' > 1$ and $a \geq 2$, let p be a prime factor of m' (note that $p \geq 5$). Theorem 6.2 implies the existence of an $(m/p, 4, 1; 2)$-HDM. Inflate this $(m/p, 4, 1; 2)$-HDM by a

$$B_1 = \left\{ \begin{bmatrix} y_0 \\ cy_1 \\ (c+1)y_1 \end{bmatrix}, \begin{bmatrix} y_1 \\ -cy_1 \\ -(c-1)y_0 \end{bmatrix}, \begin{bmatrix} -y_0 \\ -cy_0 \\ -(c+1)y_0 \end{bmatrix}, \begin{bmatrix} -y_1 \\ cy_0 \\ (c-1)y_1 \end{bmatrix} : y \in \mathbb{Z}_m^{\boxtimes} \right\} \tag{6}$$

$$B_2 = \left\{ \pm \begin{bmatrix} y_1 \\ cy_1 \\ (1+c)y_0 \end{bmatrix}, \pm \begin{bmatrix} cy_0 \\ y_1 \\ (1+c)y_1 \end{bmatrix}, \pm \begin{bmatrix} c^2 y_0 \\ cy_0 \\ c(1+c)y_0 \end{bmatrix}, \pm \begin{bmatrix} cy_1 \\ c^2 y_0 \\ c(c+1)y_1 \end{bmatrix} : y \in \mathbb{Z}_m^{\square} \right\} \tag{7}$$

$(p, 4, 1)$-CDM (which exists by Proposition 5.1) to obtain an $(m, 4, 1; 2p)$-HDM. Fill in the hole with an extendible $\mathrm{PDM}(2p)$ from Proposition 6.6 or Proposition 6.7 to obtain an extendible $\mathrm{PDM}(m)$. Now apply Proposition 6.1.

$b = 2$: When $m' = 1$ and $a \in [5]$, an extendible $\mathrm{PDM}(m)$ exists by Lemma 6.2 and Lemma 6.3.

When $m' = 1$ and $a = 6$, apply Theorem 6.1 with an (8, 4, 1; 2)-HDM (which exists by Theorem 6.2) to obtain a (576 , 4, 1; 96)-HDM. Fill in the hole with an extendible PDM(96) from Lemma 6.3 to obtain an extendible PDM(576) and apply Proposition 6.1.

When $m' = 1$ and $a \geq 7$, apply Theorem 6.1 to a $(m/64, 4, 1; 2)$-HDM (which exists by Theorem 6.2) to obtain a $(m, 4, 1; m/16)$-HDM. Fill in the hole with an extendible $\mathrm{PDM}(m/16)$ (which exists by the induction hypothesis) to obtain an extendible $\mathrm{PDM}(m)$. Now apply Proposition 6.1.

When $m' > 1$, let p be a prime factor of m' (note that $p \geq 5$). Theorem 6.2 implies the existence of a $(m/p, 4, 1; 2)$-HDM. Inflate this holey DM by a $(p, 4, 1)$-CDM (which exists by Proposition 5.1) to obtain a $(m, 4, 1; 2p)$-HDM. Fill in the hole with an extendible $\mathrm{PDM}(2p)$ (which exists by Proposition 6.6 or Proposition 6.7) to obtain an extendible $\mathrm{PDM}(m)$. Now apply Proposition 6.1.

$b \geq 3$: Theorem 6.2 implies the existence of an $(m/27, 4, 1; w)$-HDM, for some $w \in \{2, 4, 6\}$. Inflate this $(m/27, 4, 1; w)$-HDM by a (27, 4, 1)-CDM (which exists by Proposition 5.4) to obtain an $(m, 4, 1; 27w)$-HDM. Fill in the hole with an extendible $\mathrm{PDM}(27w)$ (which exists by Example 6.1 or Lemma 6.3) to obtain an extendible $\mathrm{PDM}(m)$. The result now follows from Proposition 6.1. □

3) Summary:

Theorem 6.3: There exists a $(3m, [3^m], 3)$-PCDP for all $m \not\equiv 8, 16 \pmod{24}$, except when $m = 2$.

Proof: Propositions 6.8, 6.9, 6.10, and 6.11 give a $(3m, [3^m], 3)$-PCDP for all $m \not\equiv 8, 16 \pmod{24}$, $m > 2$. It is easy to check that a $(6, [3^2], 3)$-PCDP cannot exist. □

VII. Concluding Remarks

In this paper, a number of new infinite families of optimal PCDPs are presented. The PCDPs obtained can be used directly to produce frequency-hopping sequences optimal with respect to Hamming correlation and comma-free codes optimal with respect to redundancy. They are also of independent interest in combinatorial design theory.

References

[1] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread spectrum communications – A tutorial," *IEEE Trans. Commun.*, vol. COM-30, no. 5, pp. 855–884, May 1982.

[2] R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequency hopping sequences: A combinatorial approach," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2408–2420, Oct. 2004.

[3] V. I. Levenshtein, "One method of constructing quasi codes providing synchronization in the presence of errors," *Problems Inform. Transmiss.*, vol. 7, no. 3, pp. 215–222, 1971.

[4] G. Ge, R. Fuji-Hara, and Y. Miao, "Further combinatorial constructions for optimal frequency-hopping sequences," *J. Comb. Theory Ser. A*, vol. 113, pp. 1699–1718, 2006.

[5] S. W. Golomb, B. Gordon, and L. R. Welch, "Comma-free codes," *Canad. J. Math.*, vol. 10, no. 2, pp. 202–209, 1958.

[6] V. D. Tonchev, "Partitions of difference sets and code syncrhonization," *Finite Fields Appl.*, vol. 11, pp. 601–621, 2005.

[7] V. I. Levenshtein, "Combinatorial problems motivated by comma-free codes," *J. Combin. Des.*, vol. 12, pp. 184–196, 2004.

[8] D. Jungnickel, A. Pott, and K. W. Smith, "Difference sets," in *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds. Boca Raton, FL: Chapman & Hall, 2007, pp. 419–435.

[9] A. Lempel, M. Cohn, and W. L. Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. IT-23, no. 1, pp. 38–42, Jan. 1977.

[10] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2834–2843, Nov. 2001.

[11] C. Ding, T. Helleseth, and H. Martinsen, "New families of binary sequences with optimal three-level autocorrelation," *IEEE Trans. Inform. Theory*, vol. 47, no. 1, pp. 428–433, Jan. 2001.

[12] G. Ge, "On $(g, 4; 1)$-difference matrices," *Discrete Math.*, vol. 301, pp. 164–174, 2005.

[13] J. Yin, "Cyclic difference packing and covering arrays," *Des. Codes Cryptogr.*, vol. 37, no. 2, pp. 281–292, 2005.

[14] Y. Chang and Y. Miao, "Constructions for optimal optical orthogonal codes," *Discrete Math.*, vol. 261, pp. 127–139, 2003.

[15] J. H. Dinitz and D. R. Stinson, "MOLS with holes," *Discrete Math.*, vol. 44, pp. 145–154, 1983.

Yeow Meng Chee (SM'08) received the B.Math. degree in computer science and combinatorics and optimization and the M.Math. and Ph.D. degrees in computer science, all from the University of Waterloo, Waterloo, ON, Canada, in 1988, 1989, and 1996, respectively.

Currently, he is an Associate Professor at the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Prior to this, he was Program Director of Interactive Digital Media R&D in the Media Development Authority of Singapore, a Postdoctoral Fellow at the University of Waterloo and IBM's Zürich Research Laboratory, General Manager of the Singapore Computer Emergency Response Team, and Deputy Director of Strategic Programs at the Infocomm Development Authority, Singapore. His research interest lies in the interplay between combinatorics and computer science/engineering, particularly combinatorial design theory, coding theory, extremal set systems, and electronic design automation.

Alan C. H. Ling was born in Hong Kong in 1973. He received the B.Math., M.Math., and Ph.D. degrees in combinatorics and optimization from the University of Waterloo, Waterloo, ON, Canada, in 1994, 1995, and 1996, respectively.

He worked at the Bank of Montreal, Montreal, QC, Canada, and Michigan Technological University, Houghton, prior to his present position as Associate Professor of Computer Science at the University of Vermont, Burlington. His research interests concern combinatorial designs, codes, and applications in computer science.

Jianxing Yin received the B.Sc. degree from Suzhou University, China, in 1977.

Since 1977, he has been a Teacher in the Department of Mathematics, Suzhou University, and is also currently a Full Professor there. His research interests include applications of combinatorial designs in coding theory and cryptography.