ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Journal of Combinatorial Theory, Series A 113 (2006) 1699–1718

Journal of Combinatorial Theory Series A

www.elsevier.com/locate/jcta

Further combinatorial constructions for optimal frequency-hopping sequences ☆

Gennian Ge [a], Ryoh Fuji-Hara [b], Ying Miao [b]

[a] *Department of Mathematics, Zhejiang University, Hangzhou, Zhejiang 310027, PR China*
[b] *Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba 305-8573, Japan*

Received 20 September 2005

Available online 15 June 2006

Abstract

Frequency-hopping multiple-access (FHMA) spread-spectrum communication systems employing multiple frequency shift keying as data modulation technique were investigated by Fuji-Hara, Miao and Mishima [R. Fuji-Hara, Y. Miao, M. Mishima, Optimal frequency hopping sequences: A combinatorial approach, IEEE Trans. Inform. Theory 50 (2004) 2408–2420] from a combinatorial approach, where a correspondence between frequency-hopping (FH) sequences and partition-type cyclic difference packings was established, and several combinatorial constructions were provided for FHMA systems with a single optimal FH sequence. In this paper, by means of this correspondence, we describe more combinatorial constructions for such optimal FH sequences. As a consequence, more new infinite series of optimal FH sequences are obtained.

Keywords: Combinatorial design; Frequency-hopping sequence; Optimal; Partition-type cyclic difference packing; Projective geometry

☆ Research supported by National Natural Science Foundation of China under Grant No. 10471127, Zhejiang Provincial Natural Science Foundation of China under Grant No. R604001, the Scientific Research Foundation for the Returned Overseas Chinese Scholars, State Education Ministry, and JSPS Grant-in-Aid for Scientific Research (C) under Contract No. 18540109.

E-mail addresses: gnge@zju.edu.cn (G. Ge), fujihara@sk.tsukuba.ac.jp (R. Fuji-Hara), miao@sk.tsukuba.ac.jp (Y. Miao).

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2006.03.019

1. Introduction

In modern radar and communication systems, frequency-hopping (FH) spread-spectrum techniques have become very popular (see [9], for example). The hopping sequences are used to specify which frequency will be used for transmission at any given time. Each FH sequence $X = (x_0, x_1, \ldots, x_{v-1})$, where $x_i \in F = \{f_0, f_1, \ldots, f_{m-1}\}$, of length v has an alphabet F of large size which is equal to the number of available frequencies. In multiple-access spread-spectrum communication systems and multi-user radar systems, mutual interference occurs when two or more transmitters transmit on the same frequency at the same time. Normally it is desirable to keep the mutual interferences, or the Hamming cross-correlation function (CCF) and the out-of-phase Hamming auto-correlation function (ACF), as low as possible. In addition, it is also required that the frequency-hopping signals have the in-phase Hamming auto-correlation function (ACF) as impulsive as possible so as to minimize any ambiguity about the source identity and the information in communication systems, or to maximize the resolution in radar systems. For any two periodic integer sequences $\{a_i^{(r)}\}$ and $\{a_i^{(s)}\}$ of period v, their Hamming function value is given by the number of coincidences, or hits, for relative time delay τ, i.e.

$$\lambda_{r,s}(\tau) = \sum_{0 \leqslant i \leqslant v-1} a_i^{(r)} \circ a_{i+\tau}^{(s)},$$

where

$$a_i^{(r)} \circ a_{i+\tau}^{(s)} = \begin{cases} 0, & \text{if } a_i^{(r)} \neq a_{i+\tau}^{(s)}, \\ 1, & \text{if } a_i^{(r)} = a_{i+\tau}^{(s)}, \end{cases}$$

and all operations among position indices are performed modulo v. If $r \neq s$, $\lambda_{r,s}(\tau)$ is the Hamming CCF value. If $r = s$, $\lambda_{r,r}(\tau)$ is the out-of-phase Hamming ACF value for $\tau \not\equiv 0 \pmod{v}$ and the in-phase Hamming ACF value for $\tau \equiv 0 \pmod{v}$.

Fuji-Hara, Miao and Mishima [11] investigated frequency-hopping multiple-access (FHMA) systems with a single optimal FH sequence from a combinatorial approach. They [11] established a correspondence between frequency-hopping sequences and partition-type cyclic difference packings, which reveals that in order to construct optimal FH sequences, one needs only to construct their corresponding partition-type cyclic difference packings. Various combinatorial constructions can be found in [11] for such FHMA systems with a single optimal FH sequence.

The purpose of this paper is to provide further combinatorial constructions for optimal FH sequences, given the length v and the frequency alphabet, in addition to those found in [11]. We adopt the definitions in [11,14]. Let $\mathcal{X}(v; F)$ be the set of all sequences of length v over a given frequency alphabet F. For $\{a_i^{(r)}\} \in \mathcal{X}(v; F)$, define $H(\{a_i^{(r)}\}) = \max_{0<\tau<v}\{\lambda_{r,r}(\tau)\}$. As in [11], here we assume again that all transmitters use the same FH sequence, starting from different time slots. That is, we only consider the auto-correlation properties of FH sequences. If $H(\{a_i^{(r_0)}\}) \leqslant H(\{a_i^{(r)}\})$ for all $\{a_i^{(r)}\} \in \mathcal{X}(v; F)$, then $\{a_i^{(r_0)}\}$ is said to be optimal. The following is the well-known Lempel–Greenberger bound.

Lemma 1.1. [14] *For every FH sequence $\{a_i^{(r)}\}$ of length v over a frequency alphabet F of size m,*

$$H\left(\{a_i^{(r)}\}\right) \geqslant \frac{(v-\epsilon)(v+\epsilon-m)}{m(v-1)},$$

where ϵ is the least non-negative residue of v modulo m.

The following corollary makes the bound easier to use.

Corollary 1.2. [11] *For every FH sequence* $\{a_i^{(r)}\}$ *of length* v *over a frequency alphabet* F *of size* m,

$$H\left(\{a_i^{(r)}\}\right) \geqslant \begin{cases} k, & \text{if } v \neq m, \\ 0, & \text{if } v = m, \end{cases}$$

where $v = km + \epsilon$, $0 \leqslant \epsilon \leqslant m - 1$.

In this paper, we try to provide more systematic constructions for optimal FH sequences from a combinatorial approach. In Section 2, we recall the correspondence between FH sequences and partition-type cyclic difference packings. In Section 3, we provide two constructions from projective geometries. In Section 4, we describe a construction from a special kind of difference sets, where such difference sets can again be obtained from projective geometries. Section 5 is devoted to the constructions from cyclic pairwise balanced designs. Constructions from near resolvable cyclic balanced incomplete block designs and $\mathbf{Z}$-cyclically resolvable 1-rotational balanced incomplete block designs are investigated in Section 6. A recursive construction described in [11] is slightly generalized in Section 7. Finally, a brief summary is given in Section 8.

2. Known combinatorial characterization

Fuji-Hara, Miao and Mishima [11] characterized FH sequences in terms of partition-type cyclic difference packings.

Let $\mathcal{P} = \{B_0, B_1, \ldots, B_{m-1}\}$ be a collection of m subsets (called blocks) of $\mathbf{Z}_v$. $\mathcal{P}$ is said to form a cyclic difference packing over $\mathbf{Z}_v$ and is denoted by m-DP(v, K, λ), where $K = \{|B_i|\colon 0 \leqslant i \leqslant m-1\}$, if for each $d \in \mathbf{Z}_v \setminus \{0\}$, the ordered pairs $(b, b') \in B_i \times B_i$ such that $d \equiv b - b' \pmod v$ appear at most λ times in $B_0, B_1, \ldots, B_{m-1}$, and furthermore for at least one $d_0 \in \mathbf{Z}_v \setminus \{0\}$, the ordered pairs $(b, b') \in B_i \times B_i$ with $d_0 \equiv b - b' \pmod v$ appear exactly λ times in $B_0, B_1, \ldots, B_{m-1}$. If each $d \in \mathbf{Z}_v \setminus \{0\}$ appears exactly λ times as the differences arising from $B_0, B_1, \ldots, B_{m-1}$, then $\mathcal{P}$ is called a cyclic difference family and is denoted by m-DF(v, K, λ), or simply DF(v, K, λ). When $K = \{k\}$, it is simply referred to as an m-DP(v, k, λ) (or a DF(v, k, λ) for the corresponding case). An m-DP(v, K, λ) $\mathcal{P} = \{B_0, B_1, \ldots, B_{m-1}\}$ is called a partition-type cyclic difference packing if every element of $\mathbf{Z}_v$ is contained in exactly one block in $\mathcal{P}$. The notions of (partition-type) difference packings and difference families over any additive Abelian group can also be defined in a similar way.

We can view FH sequences from a set-theoretic perspective. Assume that the frequency alphabet $F = \{0, 1, \ldots, m-1\}$. An FHS$(v, m, \lambda)$, which denotes an FH sequence $\{a_i^{(r)}\}$ with length v, frequency alphabet size $|F| = m$ and $H(\{a_i^{(r)}\}) = \lambda$, can be interpreted as a family of m subsets $B_0, B_1, \ldots, B_{m-1}$ of $\mathbf{Z}_v$ such that each subset B_j corresponds to frequency $j \in F$ and the elements in each subset B_j specify the position-indices in the FH sequence $\{a_i^{(r)}\}$ at which frequency j appears.

The following theorem clarifies the connection between FH sequences and partition-type cyclic difference packings.

Theorem 2.1. [11] *There exists an* FHS(v, m, λ) *over a frequency alphabet* $F = \{0, 1, \ldots, m-1\}$ *if and only if there exists a partition-type cyclic* m-DP(v, K, λ), $\mathcal{P} = \{B_0, B_1, \ldots, B_{m-1}\}$,

over $\mathbf{Z}_v$, *where* $K = \{|B_i|\colon\ 0 \leqslant i \leqslant m-1\}$. *Furthermore, this FH sequence is optimal if* $\lambda = \lfloor v/m \rfloor$ *for* $v > m$ *and if* $\lambda = 0$ *for* $v = m$.

When $v = km + m - 1$ for $k \geqslant 1$, we have the following fine characterization.

Theorem 2.2. [11] *Let* $v = km + m - 1$ *with* $k \geqslant 1$. *Then there exists an optimal* $\mathrm{FHS}(v, m, k)$ *if and only if there exists a partition-type cyclic* m-$\mathrm{DF}(v, \{k, k+1\}, k)$ *in which* $m - 1$ *blocks are of size* $k + 1$ *and the remaining one is of size* k.

According to Theorems 2.1 and 2.2, in order to construct optimal FH sequences, we only need construct their corresponding partition-type cyclic difference packings. Fuji-Hara, Miao and Mishima [11] constructed many infinite series of optimal FH sequences in this way. In the remainder of this paper, we provide more evidences to show that this approach is very effective.

3. Constructions from projective geometries

In [11], Fuji-Hara, Miao and Mishima described a geometric construction for optimal FH sequences from a parallel class of t-flats in an affine space $\mathrm{AG}(n, q)$. In this section, we describe two more geometric constructions for optimal FH sequences from some special t-flats in a projective space $\mathrm{PG}(n, q)$.

Let q be a prime power and $n \geqslant 3$ be an integer. In an n-dimensional projective space $\mathrm{PG}(n, q)$, there are $v = \frac{q^{n+1}-1}{q-1}$ points which can be represented by the elements of $\mathbf{Z}_v$, and there are $\frac{(q^{n+1}-1)(q^n-1)\cdots(q^{n-k+1}-1)}{(q^{k+1}-1)(q^k-1)\cdots(q-1)}$ k-flats, i.e., k-dimensional subspaces, each having $\frac{q^{k+1}-1}{q-1}$ points. Denote the set of planes, i.e., 2-flats, of $\mathrm{PG}(n, q)$ containing a common line l_0, i.e., a 1-flat, by $W = \{H_1, H_2, \ldots, H_m\}$. It is clear that the number of planes in W is $m = \frac{q^{n-1}-1}{q-1}$, and $\{l_0, H_1 \setminus l_0, \ldots, H_m \setminus l_0\}$ forms a partition of $\mathrm{PG}(n, q)$.

For the ease of description, we use some notations. For given subsets D, A, B in $\mathbf{Z}_v$, let ΔD be the multi-set $\{x - y\colon\ x, y \in D,\ x \neq y\}$, and $\Delta(A, B)$ be the multi-set $\{x - y\colon\ x \in A,\ y \in B\}$. The notation $\Delta A = \lambda B$, where λ is a positive integer, means that each element of B occurs exactly λ times in ΔA, and the notation $A + B$ means their concatenation.

Theorem 3.1. *Let* q *be a prime power and* $n \geqslant 3$ *be an integer. Then* $\{l_0, H_1 \setminus l_0, H_2 \setminus l_0, \ldots, H_m \setminus l_0\}$ *is a partition-type cyclic* $(m+1)$-$\mathrm{DP}(v, \{q^2, q+1\}, q^2-1)$ *over* $\mathbf{Z}_v$, *where* $m = \frac{q^{n-1}-1}{q-1}$ *and* $v = \frac{q^{n+1}-1}{q-1}$.

Proof. Let L_a be the set of lines in $\mathrm{PG}(n, q)$ incident with a point a. We first consider the multi-set of differences $\sum_{l \in L_a} \Delta l$ of all lines in L_a, and show that $\sum_{l \in L_a} \Delta l = (q+1)(\mathbf{Z}_v \setminus \{0\})$. All lines in $\mathrm{PG}(n, q)$ are generated from a set of base lines by the Singer automorphism $\alpha : x \mapsto x + 1$, where $x \in \mathbf{Z}_v$. When n is even, there is no short orbit of lines. If we take one line from each orbit of lines, then the set of these lines forms a cyclic difference family $\mathrm{DF}(v, q+1, 1)$ over $\mathbf{Z}_v$. L_a contains exactly $q + 1$ lines in each orbit, which implies that $\sum_{l \in L_a} \Delta l = (q+1)(\mathbf{Z}_v \setminus \{0\})$. When n is odd, there is a short orbit of lines with $L = \{0, s, 2s, \ldots, qs\}$, $s = \frac{q^{n+1}-1}{q^2-1}$, being its representative base line. L_a contains exactly one line h in this short orbit, and $q + 1$ lines in each of other orbits. Clearly $\Delta h = (q+1)(L \setminus \{0\})$, and $\sum_{l \in L_a} \Delta l = (q+1)(\mathbf{Z}_v \setminus \{0\})$.

Next we consider $D_a = \sum_{l \in L_a} \Delta(l \setminus \{a\})$. Every point of $\mathrm{PG}(n,q)$ except a appears exactly once in L_a. For any $d \in \mathbf{Z}_v \setminus \{0\}$, there exist points x, y such that $d = x - a = a - y$. When at least one of n and q is even, then x, y are two different points. When both of n and q are odd, then $x = y$ if and only if $d = v/2$. This difference $d = v/2$ comes exactly from the pair of points $\{a, a + v/2\}$ in the base line h of the short orbit. In any case, $D_a = (q+1)(\mathbf{Z}_v \setminus \{0\}) - 2(\mathbf{Z}_v \setminus \{0\}) = (q-1)(\mathbf{Z}_v \setminus \{0\})$.

By assumption, l_0 is a line contained in the planes $H_1, H_2, \ldots, H_m$. Consider the set of lines $M = \bigcup_{a \in l_0} (L_a \setminus l_0)$ incident with exactly one point of l_0. Then $\sum_{l \in M} \Delta(l \setminus l \cap l_0) = \sum_{a \in l_0} D_a - \sum_{a \in l_0} \Delta(l_0 \setminus \{a\}) = (q+1)(q-1)(\mathbf{Z}_v \setminus \{0\}) - ((q+1)\Delta l_0 - 2\Delta l_0) = (q^2-1) \times (\mathbf{Z}_v \setminus \{0\}) - (q-1)\Delta l_0$. For any two points x, y in $H_i \setminus l_0$, $i = 1, 2, \ldots, m$, since there is exactly one line in M containing x and y, the total differences of the partition $\{l_0, H_1 \setminus l_0, H_2 \setminus l_0, \ldots, H_m \setminus l_0\}$ can be computed in the following way:

$$\sum_{1 \leqslant i \leqslant m} \Delta(H_i \setminus l_0) + \Delta l_0 = \sum_{l \in M} \Delta(l \setminus l \cap l_0) + \Delta l_0 = \left(q^2 - 1\right)\left(\mathbf{Z}_v \setminus \{0\}\right) - (q-2)\Delta l_0.$$

This shows that $\{l_0, H_1 \setminus l_0, H_2 \setminus l_0, \ldots, H_m \setminus l_0\}$ forms a partition-type cyclic $(m+1)$-$\mathrm{DP}(v, \{q^2, q+1\}, q^2-1)$ over $\mathbf{Z}_v$. $\square$

In most cases, the partition-type cyclic difference packings obtained in Theorem 3.1 correspond to optimal FH sequences.

Theorem 3.2. *If $n = 3$ and $q \leqslant 3$ or $n \geqslant 4$, then there exists an optimal* $\mathrm{FHS}((q^{n+1}-1)/(q-1), (q^{n-1}-1)/(q-1)+1, q^2-1)$.

Proof. According to Theorem 2.1, the partition-type cyclic difference packing obtained in Theorem 3.1 corresponds to an $\mathrm{FHS}(v, m+1, q^2-1)$, where $v = \frac{q^{n+1}-1}{q-1}$ and $m = \frac{q^{n-1}-1}{q-1}$. The optimality comes from the fact that

$$\begin{aligned}\left\lfloor \frac{v}{m+1} \right\rfloor &= \left\lfloor \frac{(q^{n+1}-1)/(q-1)}{(q^{n-1}-1)/(q-1)+1} \right\rfloor = \left\lfloor \frac{q^{n+1}-1}{q^{n-1}+q-2} \right\rfloor \\ &= \begin{cases} q^2-q+2, & \text{when } n=3 \text{ and } q \geqslant 3, \\ 3, & \text{when } n=3 \text{ and } q=2, \\ q^2-1, & \text{when } n \geqslant 4. \end{cases} \qquad \square\end{aligned}$$

In the remainder of this section, we describe our second geometric construction for optimal FH sequences. Consider t-flats in $\mathrm{PG}(n,q)$ such that $(t+1) \mid (n+1)$. In this case, there is a t-flat S such that $S = \{0, s, 2s, \ldots, (k-1)s\}$, where $s = \frac{q^{n+1}-1}{q^{t+1}-1}$ and $k = \frac{q^{t+1}-1}{q-1}$. Clearly the multi-set of differences ΔS is $\Delta S = k(S \setminus \{0\})$.

Let $W = \{F_1, F_2, \ldots, F_u\}$, $u = \frac{q^{n-t}-1}{q-1}$, be the set of all $(t+1)$-flats containing S. There is an automorphism σ of $\mathrm{PG}(n,q)$ such that $\sigma : x \mapsto x + s$, which fixes the t-flat S. This implies that the $(t+1)$-flats $F_1, \sigma F_1, \ldots, \sigma^{k-1} F_1$ all contain S. If $n = 2t+1$, then $k = u$ and there are no more $(t+1)$-flats can contain S, that is, W can be generated from F_1, i.e., $W = \{F_1, \sigma F_1, \ldots, \sigma^{k-1} F_1\}$. In this case, clearly $\Delta F_i = \Delta F_j$ for any $F_i, F_j \in W$.

In what follows, we always assume that $n = 2t+1$.

Again, let L_a be the set of lines in $\mathrm{PG}(n,q)$ incident with a point a. Then as in the proof of Theorem 3.1, we know that $\sum_{l \in L_a} \Delta l = (q+1)(\mathbf{Z}_v \setminus \{0\})$. Let $L(S)$ be the set of lines contained

in S. Then for any difference $d \in S \setminus \{0\}$, $d \in \Delta l$ if and only if $l \in L(S)$, which means that if $a \in S$, then $\sum_{l \in L_a \setminus L(S)} \Delta l = (q+1)(\mathbf{Z}_v \setminus S)$. Since $\Delta(\{a\}, \mathbf{Z}_v \setminus S) = \Delta(\mathbf{Z}_v \setminus S, \{a\}) = \mathbf{Z}_v \setminus S$, we know that $D'_a = \sum_{l \in L_a \setminus L(S)} \Delta(l \setminus \{a\}) = \sum_{l \in L_a \setminus L(S)} \Delta l - \Delta(\{a\}, \mathbf{Z}_v \setminus S) - \Delta(\mathbf{Z}_v \setminus S, \{a\}) = (q-1)(\mathbf{Z}_v \setminus S)$.

Lemma 3.3. $\sum_{a \in S} D'_a = k(q-1)(\mathbf{Z}_v \setminus S)$.

Let $A_i = F_i \setminus S$ be the affine part of the $(t+1)$-flat F_i for $i = 1, 2, \ldots, k$. Then we have the following lemmas.

Lemma 3.4. *For any $i = 1, 2, \ldots, k$, $\Delta A_i = (q-1)(\mathbf{Z}_v \setminus S)$.*

Proof. Since W can be generated from F_1 by σ, $\sigma S = S$, and $A_i = F_i \setminus S$, we know that $\Delta A_i = \Delta(F_i \setminus S) = \Delta F_i - \Delta(F_i, S) - \Delta(S, F_i) = \Delta F_j - \Delta(F_j, S) - \Delta(S, F_j) = \Delta A_j$ for any $i, j = 1, 2, \ldots, k$. Let $M(S) = \bigcup_{a \in S} L_a$. Then $M(S) \setminus L(S)$ is the set of lines of $\mathrm{PG}(n, q)$ each of which intersects S at exactly one point. Any line of A_i is contained in $M(S) \setminus L(S)$ and any line of $M(S) \setminus L(S)$ is contained in exactly one A_i. Therefore, for any $i = 1, 2, \ldots, k$, $\Delta A_i = \frac{1}{u} \sum_{l \in M(S) \setminus L(S)} \Delta(l \setminus l \cap S) = \frac{1}{k} \sum_{a \in S} D'_a = (q-1)(\mathbf{Z}_v \setminus S)$. $\square$

Lemma 3.5. *For any $i = 1, 2, \ldots, k$, $\Delta(S, A_i) = \Delta(A_i, S) = \mathbf{Z}_v \setminus S$.*

Proof. For any $i = 1, 2, \ldots, k$, we have

$$\begin{aligned}
\Delta(A_i, S) &= \Delta\big(A_i, \{0, s, \ldots, (k-1)s\}\big) = \sum_{0 \leqslant j \leqslant k-1} \Delta\big(A_i, \{js\}\big) \\
&= \sum_{0 \leqslant j \leqslant k-1} \{x - js \colon x \in A_i\} = \sum_{0 \leqslant j \leqslant k-1} \sigma^{-j} A_i = \sum_{0 \leqslant j \leqslant k-1} A_j \\
&= \mathbf{Z}_v \setminus S.
\end{aligned}$$

In a similar way, we can prove that $\Delta(S, A_i) = \mathbf{Z}_v \setminus S$. $\square$

Lemma 3.6. *For any $i = 1, 2, \ldots, k$, $\Delta F_i = (q+1)(\mathbf{Z}_v \setminus S) + k(S \setminus \{0\})$.*

Proof. $\Delta F_i = \Delta(A_i \cup S) = \Delta A_i + \Delta(S, A_i) + \Delta(A_i, S) + \Delta S = (q-1)(\mathbf{Z}_v \setminus S) + 2(\mathbf{Z}_v \setminus S) + k(S \setminus \{0\}) = (q+1)(\mathbf{Z}_v \setminus S) + k(S \setminus \{0\})$. $\square$

Theorem 3.7. *Let $v = (q^{2t+2} - 1)/(q-1)$ and $k = (q^{t+1} - 1)/(q-1)$, where q is a prime power and t is a positive integer. Then*

(1) *$\{F_1, A_2, \ldots, A_k\}$ forms a partition-type cyclic k-$\mathrm{DP}(v, \{(q^{t+2}-1)/(q-1), q^{t+1}\}, q^{t+1}+1)$ over $\mathbf{Z}_v$; and*
(2) *$\{S, A_1, \ldots, A_k\}$ forms a partition-type cyclic $(k+1)$-$\mathrm{DP}(v, \{(q^{t+1}-1)/(q-1), q^{t+1}\}, q^{t+1}-1)$ over $\mathbf{Z}_v$.*

Proof. Since S is the t-flat fixed by σ, and $F_1, F_2, \ldots, F_k$ are exactly the $(t+1)$-flats containing S, we know that both $\{F_1, A_2, \ldots, A_k\}$ and $\{S, A_1, \ldots, A_k\}$ form a partition of $\mathrm{PG}(n, q)$. Meanwhile it follows from Lemmas 3.4 and 3.6 that $\Delta F_1 \cup \sum_{2 \leqslant j \leqslant k} \Delta A_j = (q+1)(\mathbf{Z}_v \setminus S) +$

$k(S\setminus\{0\})+(k-1)(q-1)(\mathbf{Z}_v\setminus S)=(q^{t+1}+1)(\mathbf{Z}_v\setminus S)+k(S\setminus\{0\})$. Also, $\Delta S\cup\sum_{1\leqslant j\leqslant k}\Delta A_j = k(S\setminus\{0\})+k(q-1)(\mathbf{Z}_v\setminus S)=(q^{t+1}-1)(\mathbf{Z}_v\setminus S)+k(S\setminus\{0\})$. The assertions then follow. □

Theorem 3.8. *Let $v=(q^{2t+2}-1)/(q-1)$ where q is a prime power and t is a positive integer. Then there exist*

(1) *an optimal* $\mathrm{FHS}((q^{2t+2}-1)/(q-1),(q^{t+1}-1)/(q-1),q^{t+1}+1)$; *and*
(2) *an optimal* $\mathrm{FHS}((q^{2t+2}-1)/(q-1),(q^{t+1}-1)/(q-1)+1,q^{t+1}-1)$ *for* $q=2$ *and* 3.

Proof. According to Theorem 2.1, the partition-type cyclic difference packings obtained in Theorem 3.7 correspond to an $\mathrm{FHS}(v,k,q^{t+1}+1)$ and an $\mathrm{FHS}(v,k+1,q^{t+1}-1)$, respectively, where $v=\frac{q^{2t+2}-1}{q-1}$ and $k=\frac{q^{t+1}-1}{q-1}$. The optimality of the first FH sequence comes from the fact that $\lfloor\frac{v}{k}\rfloor=\lfloor\frac{(q^{n+1}-1)/(q-1)}{(q^{t+1}-1)/(q-1)}\rfloor=\lfloor\frac{q^{n+1}-1}{q^{t+1}-1}\rfloor=\lfloor\frac{q^{2t+2}-1}{q^{t+1}-1}\rfloor=q^{t+1}+1$. In a similar way, we can show the optimality of the second FH sequence. □

4. A construction from difference sets

In this section, we describe a construction for optimal FH sequences from a special kind of difference sets. A k-subset D of $\mathbf{Z}_v$ is a cyclic (v,k,λ) difference set, denoted by $\mathrm{DS}(v,k,\lambda)$, if every non-zero element of $\mathbf{Z}_v$ has exactly λ representations as a difference $d-d'$ with elements d and d' from D. In other words, a cyclic $\mathrm{DS}(v,k,\lambda)$ is a cyclic $\mathrm{DF}(v,k,\lambda)$ with only one block.

We look at the following example of cyclic difference sets.

Example 4.1. The 7-subset $\{0,1,2,4,5,8,10\}$ in $\mathbf{Z}_{15}$ forms a cyclic $\mathrm{DS}(15,7,3)$. This difference set contains the subgroup $5\mathbf{Z}_3=\{0,5,10\}$ of $\mathbf{Z}_{15}$, and its other four elements are distinct representatives of cosets of this subgroup $5\mathbf{Z}_3$. Also, the three elements in $5\mathbf{Z}_3$ are distinct representatives of the subgroup $3\mathbf{Z}_5$ and its two cosets. Then $\{D\setminus 5\mathbf{Z}_3,(D\setminus 5\mathbf{Z}_3)+5,(D\setminus 5\mathbf{Z}_3)+10\}=\{\{1,2,4,8\},\{6,7,9,13\},\{11,12,14,3\}\}$ forms a partition of $\mathbf{Z}_{15}\setminus 5\mathbf{Z}_3$. Let $B_0=D\cap 3\mathbf{Z}_5=\{0,1,2,4,5,8,10\}\cap\{0,3,6,9,12\}=\{0\}$, $B_1=(D+5)\cap 3\mathbf{Z}_5=\{5,6,7,9,10,13,0\}\cap\{0,3,6,9,12\}=\{0,6,9\}$, $B_2=(D+10)\cap 3\mathbf{Z}_5=\{10,11,12,14,0,3,5\}\cap\{0,3,6,9,12\}=\{0,3,12\}$. We can easily verify that $\{B_1\setminus\{0\},B_2\setminus\{0\}\}$ forms a cyclic $\mathrm{DF}(5,2,1)$ defined over $3\mathbf{Z}_5$ which partitions $3\mathbf{Z}_5\setminus\{0\}$.

More generally, we consider a cyclic $\mathrm{DS}(n((n-1)^2+1),n+(n-1)^2,n)$, D, which contains the subgroup $((n-1)^2+1)\mathbf{Z}_n=\{0,(n-1)^2+1,\ldots,(n-1)((n-1)^2+1)\}$, that is, $((n-1)^2+1)\mathbf{Z}_n\subseteq D$, for any odd integer n. In such a difference set, all the differences in $((n-1)^2+1)\mathbf{Z}_n\setminus\{0\}$ come from $((n-1)^2+1)\mathbf{Z}_n$, which implies that the other $(n-1)^2$ elements in D should be distinct representatives of cosets of $((n-1)^2+1)\mathbf{Z}_n$, that is, D consists of n elements in $((n-1)^2+1)\mathbf{Z}_n$ and one element in each of the remaining $(n-1)^2$ cosets of $((n-1)^2+1)\mathbf{Z}_n$. This implies that $\{(D\setminus((n-1)^2+1)\mathbf{Z}_n)+i((n-1)^2+1): i=0,1,\ldots,n-1\}$ forms a partition of $\mathbf{Z}_{n((n-1)^2+1)}\setminus((n-1)^2+1)\mathbf{Z}_n$. Let

$$B_i=\big(D+i\big((n-1)^2+1\big)\big)\cap n\mathbf{Z}_{(n-1)^2+1},\quad i=0,1,\ldots,n-1.$$

Since n is odd, $\gcd(n,(n-1)^2+1)=1$, the n elements of $((n-1)^2+1)\mathbf{Z}_n$ form a system of distinct representatives of the subgroup $n\mathbf{Z}_{(n-1)^2+1}$ and its $n-1$ cosets, and furthermore,

$B_i \cap ((n-1)^2+1)\mathbf{Z}_n = \{0\}$ for $i = 0, 1, \ldots, n-1$. We can also know that $B_i \cap B_j = \{0\}$ for all $0 \leqslant i < j \leqslant n-1$. Let $x \in B_i \cap B_j$, $0 \leqslant i < j \leqslant n-1$, that is, $x = d_i + i((n-1)^2+1) = d_j + j((n-1)^2+1)$ for some $d_i, d_j \in D$ with $d_i \neq d_j$. Then $d_i \equiv d_j \pmod{(n-1)^2+1}$, which implies that both d_i and d_j should be in $((n-1)^2+1)\mathbf{Z}_n$ and therefore x also should be in $((n-1)^2+1)\mathbf{Z}_n$. But we know that $B_i \cap ((n-1)^2+1)\mathbf{Z}_n = \{0\}$ for $i = 0, \ldots, n-1$, so we should have $x = 0$, which means that $B_i \cap B_j = \{0\}$ for all $0 \leqslant i < j \leqslant n-1$. Deleting the element 0 from each B_i, $i = 0, 1, \ldots, n-1$, we obtain n new blocks B'_i which partition $n\mathbf{Z}_{(n-1)^2+1} \setminus \{0\}$. All the differences in $n\mathbf{Z}_{(n-1)^2+1} \setminus \{0\}$ come from $D \cap (n\mathbf{Z}_{(n-1)^2+1} + i)$ for $i = 0, \ldots, n-1$. This implies that the differences from $B'_0, \ldots, B'_{n-1}$ cover each non-zero element of $n\mathbf{Z}_{(n-1)^2+1}$ exactly $n-2$ times, remembering that $\{B'_0, \ldots, B'_{n-1}\}$ forms a partition of $n\mathbf{Z}_{(n-1)^2+1} \setminus \{0\}$. That is, $\{B'_0, \ldots, B'_{n-1}\}$ forms a cyclic $\mathrm{DF}((n-1)^2+1, \{|B_i|-1\colon i = 0, \ldots, n-1\}, n-2)$ defined over $n\mathbf{Z}_{(n-1)^2+1}$ which partitions $n\mathbf{Z}_{(n-1)^2+1} \setminus \{0\}$.

Theorem 4.2. *Let n be an odd integer, and D be a cyclic* $\mathrm{DS}(n((n-1)^2+1), n+(n-1)^2, n)$ *defined over $\mathbf{Z}_{n((n-1)^2+1)}$ such that $D \supseteq ((n-1)^2+1)\mathbf{Z}_n$. Then $\{B_0 \setminus \{0\}, B_1 \setminus \{0\}, \ldots, B_{n-1} \setminus \{0\}\}$ forms a cyclic* $\mathrm{DF}((n-1)^2+1, \{|B_i|-1\colon i = 0, \ldots, n-1\}, n-2)$ *defined over $n\mathbf{Z}_{(n-1)^2+1}$ which partitions $n\mathbf{Z}_{(n-1)^2+1} \setminus \{0\}$.*

If there exists a block B_{i_0} such that $B_{i_0} = \{0\}$, then $B'_{i_0} = \emptyset$. By taking $\{0\}$ as a new block of size 1, we obtain a partition-type cyclic n-$\mathrm{DP}((n-1)^2+1, \{1\} \cup \{|B_i|-1\colon i \in \{0, \ldots, n-1\} \setminus \{i_0\}\}, n-2)$, $\{\{0\}, B'_i\colon i \in \{0, \ldots, n-1\} \setminus \{i_0\}\}$, which corresponds to an optimal $\mathrm{FHS}((n-1)^2+1, n, n-2)$ by Theorem 2.1. Furthermore, if there exists at least one other block, say B_{i_1}, such that $x + y \not\equiv 0 \pmod{n((n-1)^2+1)}$ for all $x, y \in B'_{i_1}$, then by adding the element 0 to B'_{i_1}, we obtain a partition-type cyclic $(n-1)$-$\mathrm{DP}((n-1)^2+1, \{|B_{i_1}|\} \cup \{|B_i|-1\colon i \in \{0, \ldots, n-1\} \setminus \{i_0, i_1\}\}, n-1)$, which corresponds to an optimal $\mathrm{FHS}((n-1)^2+1, n-1, n-1)$ by Theorem 2.1.

Theorem 4.3. *Let n be an odd integer, and D be a cyclic* $\mathrm{DS}(n((n-1)^2+1), n+(n-1)^2, n)$ *defined over $\mathbf{Z}_{n((n-1)^2+1)}$ such that $D \supseteq ((n-1)^2+1)\mathbf{Z}_n$ and $B_{i_0} = \{0\}$ for some $i_0 \in \{0, 1, \ldots, n-1\}$. Then there exists an optimal* $\mathrm{FHS}((n-1)^2+1, n, n-2)$. *Furthermore, if there exists at least one other block, say B_{i_1}, such that $x + y \not\equiv 0 \pmod{n((n-1)^2+1)}$ for all $x, y \in B_{i_1} \setminus \{0\}$, then there exists an optimal* $\mathrm{FHS}((n-1)^2+1, n-1, n-1)$.

The difference set in Example 4.1 satisfies the condition that $B_0 = \{0\}$. Therefore we obtain an optimal $\mathrm{FHS}(5, 3, 1)$. However, there is no $i \in \{1, 2\}$ such that for all $x, y \in B_i \setminus \{0\}$, $x + y \not\equiv 0 \pmod{15}$, so we cannot obtain an optimal $\mathrm{FHS}(5, 2, 2)$ in the way described above.

Now we turn to the construction of an infinite series of such special cyclic difference sets. In [16] Tran van Trung constructed an infinite series of $(2^{2n}+1, 2^n, 2^n-1)$ near resolvable designs from classical inversive planes of even order. A close look at his construction shows that his idea can also be used to construct cyclic difference sets satisfying the conditions in Theorem 4.3. We describe the construction below.

An inversive plane of order q is a 3-$(q^2+1, q+1, 1)$ design, which can be constructed, say, from an ovoid in the projective space $\mathrm{PG}(3, q)$. An ovoid of $\mathrm{PG}(3, q)$ is a point set $\mathcal{O}$ such that no three points are collinear and that for any point $x \in \mathcal{O}$ the tangent lines of $\mathcal{O}$ at x contain the point set of a plane, the tangent plane at x. There are $q+1$ tangent lines of $\mathcal{O}$ at x. The other q^2 lines through x meet $\mathcal{O}$ in one other point. This implies that $|\mathcal{O}| = q^2+1$. Every non-tangent

plane B through $x \in \mathcal{O}$ contains $q+1$ lines through x, exactly one of them is a tangent line and the other q lines meet $\mathcal{O}$ in one other point. This means $|B \cap \mathcal{O}| = q+1$. Since any three points of $\mathcal{O}$ are not on a line, they determine a unique non-tangent plane. Therefore, $\mathcal{O}$ and the q^3+q intersection sets of non-tangent planes with $\mathcal{O}$ provide a 3-$(q^2+1, q+1, 1)$ design, an inversive plane. A pencil in a 3-$(q^2+1, q+1, 1)$ design is a set of q blocks through x such that any two of them have only the point x in common. The point x is called the carrier of the pencil.

We consider inversive planes and ovoids in $\mathrm{PG}(3, 2^m)$, which are called classical. Let $\mathrm{PG}_2(3, 2^m)$ denote the point-hyperplane $(2^{3m}+2^{2m}+2^m+1, 2^{2m}+2^m+1, 2^m+1)$ design. By Singer's theorem $\mathrm{PG}_2(3, 2^m)$ admits a cyclic automorphism α of order $2^{3m}+2^{2m}+2^m+1$ and can be represented by a cyclic difference set. Let $\beta = \alpha^{2^m+1}$ and $\gamma = \alpha^{2^{2m}+1}$ denote automorphisms of $\mathrm{PG}_2(3, 2^m)$ of order $2^{2m}+1$ and 2^m+1, respectively. Tran van Trung [16] showed that

(1) each point orbit of β is a classical ovoid $\mathcal{O}$;
(2) each point orbit $L_i, i = 0, 1, \ldots, 2^{2m}$, of γ is a tangent line of $\mathcal{O}$; and
(3) among the 2^m+1 planes containing L_i exactly one is a tangent plane of $\mathcal{O}$ and the intersection sets of the other 2^m planes with $\mathcal{O}$ form a pencil in the inversive plane associated with $\mathcal{O}$.

Tran van Trung [16] also showed that each plane contains exactly one point orbit of γ and has exactly one point in common with any of the 2^{2m} remaining point orbits of γ.

Let $\mathcal{O}_0$ be the point orbit $\{0, 2^m+1, \ldots, 2^{2m}(2^m+1)\} = (2^m+1)\mathbf{Z}_{2^{2m}+1}$ of β which is a classical ovoid, and L_0 be the point orbit $\{0, 2^{2m}+1, \ldots, 2^m(2^{2m}+1)\} = (2^{2m}+1)\mathbf{Z}_{2^m+1}$ of γ which is a tangent line of $\mathcal{O}_0$. We choose a tangent plane P_0 of $\mathcal{O}_0$ which contains the point orbit L_0 of γ, and let D denote P_0's representing cyclic $\mathrm{DS}(2^{3m}+2^{2m}+2^m+1, 2^{2m}+2^m+1, 2^m+1)$. Then $D \supseteq L_0 = (2^{2m}+1)\mathbf{Z}_{2^m+1}$. Since for each $i = 1, \ldots, 2^m$, the plane $D + i(2^{2m}+1)$ is a non-tangent plane containing $L_0 = (2^{2m}+1)\mathbf{Z}_{2^m+1}$, we know that $\{(D + i(2^{2m}+1)) \cap (2^m+1)\mathbf{Z}_{2^{2m}+1}\colon\ i = 1, \ldots, 2^m\}$ forms a pencil in the classical inverse plane associated with $\mathcal{O}_0 = (2^m+1)\mathbf{Z}_{2^{2m}+1}$. Therefore, $D \cap (2^m+1)\mathbf{Z}_{2^{2m}+1} = \{0\}$, $|(D + i(2^{2m}+1)) \cap (2^m+1)\mathbf{Z}_{2^{2m}+1}| = 2^m+1$ for $i = 1, \ldots, 2^m$, and $((D + i(2^{2m}+1)) \cap (2^m+1)\mathbf{Z}_{2^{2m}+1}) \cap ((D + j(2^{2m}+1)) \cap (2^m+1)\mathbf{Z}_{2^{2m}+1}) = \{0\}$ for $0 \leqslant i < j \leqslant 2^m$.

Lemma 4.4. *Let $n = 2^m+1$ where m is a positive integer. Then there exists a cyclic $\mathrm{DS}(n((n-1)^2+1), n+(n-1)^2, n)$, D, defined over $\mathbf{Z}_{n((n-1)^2+1)}$ such that $D \supseteq ((n-1)^2+1)\mathbf{Z}_n$, $D \cap n\mathbf{Z}_{(n-1)^2+1} = \{0\}$, and $|(D + i((n-1)^2+1)) \cap n\mathbf{Z}_{(n-1)^2+1}| = n$ for $i = 1, \ldots, n-1$.*

Applying Theorem 4.3 with Lemma 4.4, we immediately obtain the following result.

Theorem 4.5. *There exists an optimal* $\mathrm{FHS}(2^{2m}+1, 2^m+1, 2^m-1)$ *for any positive integer m.*

As an example, we consider the construction of an optimal $\mathrm{FHS}(17, 5, 3)$.

Example 4.6. Let $\alpha = (0, 1, \ldots, 84)$ be the Singer cyclic automorphism for the $(85, 21, 5)$ point-hyperplane design $\mathrm{PG}_2(3, 4)$ having $D = \{0, 1, 2, 4, 7, 8, 14, 16, 17, 23, 27, 28, 32, 34, 43, 46, 51, 54, 56, 64, 68\}$ as a base block for α, which is in fact a cyclic $\mathrm{DS}(85, 21, 5)$. Then

$$\beta = \alpha^5 = (0, 5, \ldots, 80)(1, 6, \ldots, 81)(2, 7, \ldots, 82)(3, 8, \ldots, 83)(4, 9, \ldots, 84),$$

and

$$\gamma = \alpha^{17} = (0, 17, 34, 51, 68)(1, 18, 35, 52, 69)\cdots(16, 33, 50, 67, 84).$$

Let $\mathcal{O}_0 = \{0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80\}$ be the first point orbit of β. The 17 point orbits of γ form tangent lines at the 17 points of $\mathcal{O}_0$. Now D contains the point orbit $L_0 = (0, 17, 34, 51, 68)$ of γ and is the tangent plane of $\mathcal{O}_0$ at 0. The other four planes $D_i = \{x + i \times 17 \pmod{85}\colon\ x \in D\}$, $i = 1, 2, 3, 4$, also contain $(0, 17, 34, 51, 68)$ and intersect $\mathcal{O}_0$ in five points each. The four intersection sets that form a pencil with the carrier 0 in the associated 3-(17, 5, 1) design of $\mathcal{O}_0$ are

$$\{0, 25, 40, 45, 60\},\ \{0, 5, 35, 50, 80\},\ \{0, 20, 30, 55, 65\},\ \{0, 10, 15, 70, 75\}.$$

Deleting the point 0 from each of the above four intersection sets, we obtain a cyclic DF(17, 4, 3) defined over $5\mathbf{Z}_{17}$,

$$\{25, 40, 45, 60\},\ \{5, 35, 50, 80\},\ \{20, 30, 55, 65\},\ \{10, 15, 70, 75\},$$

which partition $5\mathbf{Z}_{17} \setminus \{0\}$. Taking $\{0\}$ as a new block of size 1, we obtain a partition-type cyclic 5-DP(17, {1, 4}, 3),

$$\{0\},\ \{25, 40, 45, 60\},\ \{5, 35, 50, 80\},\ \{20, 30, 55, 65\},\ \{10, 15, 70, 75\},$$

which corresponds to an optimal FHS(17, 5, 3).

Finally we should note that, as was pointed out by one of the anonymous referees, [8] is a better and earlier reference for the idea contained in this construction.

5. Constructions from cyclic PBDs

Let K be a set of positive integers and λ a positive integer. We consider a pairwise balanced design PBD(v, K, λ), $(X, \mathbf{B})$, where X is a v-set of points, $\mathbf{B}$ a collection of subsets of X with sizes from K (called blocks) such that every pair of distinct points occurs in exactly λ blocks. Let σ be a permutation on X. For any block $B = \{b_1, b_2, \ldots, b_k\} \in \mathbf{B}$, define $B^\sigma = \{b_1^\sigma, b_2^\sigma, \ldots, b_k^\sigma\}$. If $\mathbf{B}^\sigma = \{B^\sigma\colon\ B \in \mathbf{B}\} = \mathbf{B}$, then σ is an automorphism of the PBD(v, K, λ) $(X, \mathbf{B})$. The set of all such permutations forms a group under composition called the full automorphism group of the pairwise balanced design. Any of its subgroups is called an automorphism group of the pairwise balanced design. A PBD(v, K, λ) admitting a cyclic and point-regular automorphism group is a cyclic PBD(v, K, λ). For a cyclic PBD(v, K, λ) $(X, \mathbf{B})$, the point set X can be identified with $\mathbf{Z}_v$. In this case, the pairwise balanced design has an automorphism $\sigma : i \mapsto i + 1 \pmod{v}$.

For a cyclic PBD(v, K, λ) $(Z_v, \mathbf{B})$, let $B = \{b_1, b_2, \ldots, b_k\}$ be a block in $\mathbf{B}$. The block orbit containing B is the set of the following distinct blocks:

$$B^{\sigma^i} = B + i = \{b_1 + i, b_2 + i, \ldots, b_k + i\} \pmod{v}$$

for $i \in \mathbf{Z}_v$. If a block orbit has v distinct blocks, i.e., its setwise stabilizer G_B is equal to the subgroup $\{0\}$ of $\mathbf{Z}_v$, then this block orbit is full, otherwise short. Choose an arbitrarily fixed block from each block orbit and call it a base block.

We should note that a cyclic PBD(v, K, λ) may have short block orbits. However in this section, when we say a cyclic PBD$(v, \{k_1, k_2, \ldots, k_t\}, 1)$, we always mean a cyclic PBD$(v, \{k_1, k_2, \ldots, k_t\}, 1)$ without short block orbits, that is, the design is generated by successively adding 1 to each of the base blocks $B_1, B_2, \ldots, B_t$ modulo v, where the setwise stabilizer

G_{B_i} is equal to the subgroup $\{0\}$ of $\mathbf{Z}_v$ and $|B_i| = k_i$ for each $1 \leqslant i \leqslant t$. In other words, a cyclic PBD$(v, \{k_1, k_2, \ldots, k_t\}, 1)$ is equivalent to a t-DF$(v, \{k_1, k_2, \ldots, k_t\}, 1)$ defined over $\mathbf{Z}_v$, i.e., a collection of blocks $B_1, B_2, \ldots, B_t$ of $\mathbf{Z}_v$ such that the multi-set of the differences

$$\sum_{i=1}^{t} \Delta B_i = \{a - b\colon a, b \in B_i,\ 1 \leqslant i \leqslant t,\ a \neq b\}$$

cover each non-zero element in $\mathbf{Z}_v$ exactly once, and $|B_i| = k_i$ for each $1 \leqslant i \leqslant t$.

Theorem 5.1. *Suppose that there exists a cyclic* PBD$(v, \{k_1, k_2, \ldots, k_t\}, 1)$ *with* $2 \leqslant k_1 \leqslant k_2 \leqslant \cdots \leqslant k_t$. *Let* $\lambda = \max\{k_1 - 1, k_t - 2\}$. *If* $1 + \sum_{i=1}^{t} k_i(k_i - k_t + 1) \geqslant 0$, *then there exists an optimal* FHS$(v, \sum_{i=1}^{t} k_i, \lambda)$ *derived from a partition-type cyclic* $(\sum_{i=1}^{t} k_i)$-DP$(v, \{k_1, k_1 - 1, k_2 - 1, \ldots, k_t - 1\}, \lambda)$ *over* $\mathbf{Z}_v$.

Proof. Let $\mathbf{B} = \{B_1, B_2, \ldots, B_t\}$ be the t base blocks of the cyclic PBD$(v, \{k_1, k_2, \ldots, k_t\}, 1)$ such that $|B_i| = k_i$ for $1 \leqslant i \leqslant t$. Since the setwise stabilizer G_{B_i} for each B_i is equal to $\{0\}$, i.e., the block orbit generated by B_i is a full orbit having v distinct blocks, we know that there are exactly k_i blocks $B_i^1, B_i^2, \ldots, B_i^{k_i}$ in this block orbit each of which contains the element $0 \in \mathbf{Z}_v$. Then we can prove that

$$\mathcal{P} = \left\{B_1^1, B_1^2 \setminus \{0\}, \ldots, B_1^{k_1} \setminus \{0\}, B_2^1 \setminus \{0\}, \ldots, B_2^{k_2} \setminus \{0\}, \ldots, B_t^1 \setminus \{0\}, \ldots, B_t^{k_t} \setminus \{0\}\right\}$$

forms a partition-type cyclic $(\sum_{i=1}^{t} k_i)$-DP$(v, \{k_1, k_1 - 1, k_2 - 1, \ldots, k_t - 1\}, \lambda)$ over $\mathbf{Z}_v$, where $\lambda = \max\{k_1 - 1, k_t - 2\}$.

Since $(\mathbf{Z}_v, \mathbf{B})$ is a cyclic pairwise balanced design with $\lambda = 1$, it is easy to see that $\mathcal{P}$ forms a partition of the point set $\mathbf{Z}_v$, and for any non-zero element d, d and $v - d$ of $\mathbf{Z}_v$ cannot appear in B_1^1 simultaneously. In this case, as a difference arising from each block in $\mathcal{P}$, each non-zero element $d \in \mathbf{Z}_v$ occurs $k_1 - 1$ times if $d \in B_1^1$ or $v - d \in B_1^1$, otherwise $k_i - 2$ times if $d \in B_i^j$ or $v - d \in B_i^j$ with $(i, j) \neq (1, 1)$ for $i = 1, 2, \ldots, t$ and $j = 1, 2, \ldots, k_i$. Therefore, noting that $k_1 \leqslant k_2 \leqslant \cdots \leqslant k_t$, we obtain a partition-type cyclic $(\sum_{i=1}^{t} k_i)$-DP$(v, \{k_1, k_1 - 1, k_2 - 1, \ldots, k_t - 1\}, \lambda)$ over $\mathbf{Z}_v$. This corresponds to an FHS$(v, \sum_{i=1}^{t} k_i, \lambda)$ by Theorem 2.1.

To prove the optimality, we write $v = \lambda \cdot (\sum_{i=1}^{t} k_i) + r$, and need to show that $0 \leqslant r \leqslant \sum_{i=1}^{t} k_i - 1$. Noting that $(\mathbf{Z}_v, \mathbf{B})$ is a cyclic PBD$(v, \{k_1, k_2, \ldots, k_t\}, 1)$, we have $v - 1 = k_1(k_1 - 1) + k_2(k_2 - 1) + \cdots + k_t(k_t - 1)$. The proof is divided into the following two subcases.

(1) When $\lambda = k_1 - 1$, that is, $k_1 - 1 \geqslant k_t - 2$. In this case, $k_t - k_1 \leqslant 1$. Then $r = (\sum_{i=1}^{t} k_i(k_i - 1) + 1) - (k_1 - 1)(\sum_{i=1}^{t} k_i) = 1 + \sum_{i=1}^{t} k_i(k_i - k_1)$. Since $2 \leqslant k_1 \leqslant k_2 \leqslant \cdots \leqslant k_t$, we have $0 \leqslant k_i - k_1 \leqslant 1$ for $i = 1, 2, \ldots, t$, which implies that $0 \leqslant r \leqslant 1 + \sum_{i=2}^{t} k_i = 1 - k_1 + \sum_{i=1}^{t} k_i(k_i - k_1) \leqslant \sum_{i=1}^{t} k_i - 1$.

(2) When $\lambda = k_t - 2$, that is, $k_1 - 1 \leqslant k_t - 2$. Since case (1) covers $k_1 - 1 = k_t - 2$, we need only consider the case $k_1 - 1 < k_t - 2$, that is, $k_t - k_1 \geqslant 2$. In this case, $r = (\sum_{i=1}^{t} k_i(k_i - 1) + 1) - (k_t - 2)(\sum_{i=1}^{t} k_i) = 1 + \sum_{i=1}^{t} k_i(k_i - k_t + 1)$. Since $2 \leqslant k_1 \leqslant k_2 \leqslant \cdots \leqslant k_t$ and $k_t - k_1 \geqslant 2$, we can know that $r = 1 + k_1(k_1 - k_t + 1) + \sum_{i=2}^{t} k_i(k_i - k_t + 1) \leqslant 1 - k_1 + \sum_{i=2}^{t} k_i \leqslant 1 - 2k_1 + \sum_{i=1}^{t} k_i \leqslant \sum_{i=1}^{t} k_i - 3$, and by assumption, $r = 1 + \sum_{i=1}^{t} k_i(k_i - k_t + 1) \geqslant 0$. $\square$

When $K = \{k\}$, the pairwise balanced design becomes a balanced incomplete block design (or briefly BIBD), and we obtain a result originally due to Fuji-Hara, Miao and Mishima [11].

Corollary 5.2. *If there exists a cyclic BIBD* $B(v,k,1)$ *with* $v \equiv 1 \pmod{k(k-1)}$, *then there exists an optimal* $\mathrm{FHS}(v,(v-1)/(k-1),k-1)$ *derived from a partition-type cyclic* $((v-1)/(k-1))$-$\mathrm{DP}(v,\{k-1,k\},k-1)$ *over* $\mathbf{Z}_v$.

Proof. It is well known (see [4] or [6]) that in a cyclic BIBD $B(v,k,1)$ with $v \equiv 1 \pmod{k(k-1)}$, for any base block B, the setwise stabilizer G_B is equal to $\{0\}$. Then apply Theorem 5.1. □

Similar to Theorem 5.1, we have the following construction.

Theorem 5.3. *Suppose that there exists a cyclic* $\mathrm{PBD}(v,\{k_1,k_2,\ldots,k_t\},1)$ *with* $2 \leqslant k_1 \leqslant k_2 \leqslant \cdots \leqslant k_t$ *and* $k_t \geqslant 3$. *If* $3+\sum_{i=1}^{t-1} k_i(k_i-k_t+1) \geqslant 0$, *then there exists an optimal* $\mathrm{FHS}(v,1+\sum_{i=1}^{t} k_i,k_t-2)$ *derived from a partition-type cyclic* $(1+\sum_{i=1}^{t} k_i)$-$\mathrm{DP}(v,\{1,k_1-1,k_2-1,\ldots,k_t-1\},k_t-2)$ *over* $\mathbf{Z}_v$.

Proof. Similar to the proof of Theorem 5.1, we let $B_i^1, B_i^2, \ldots, B_i^{k_i}$ be the k_i blocks containing the element 0, which are in the full block orbit generated by B_i. Then we can know that

$$\mathcal{P} = \left\{\{0\}, B_1^1 \setminus \{0\}, \ldots, B_1^{k_1} \setminus \{0\}, B_2^1 \setminus \{0\}, \ldots, B_2^{k_2} \setminus \{0\}, \ldots, B_t^1 \setminus \{0\}, \ldots, B_t^{k_t} \setminus \{0\}\right\}$$

forms a partition-type cyclic $(1+\sum_{i=1}^{t} k_i)$-$\mathrm{DP}(v,\{1,k_1-1,k_2-1,\ldots,k_t-1\},k_t-2)$ over $\mathbf{Z}_v$.

We prove the optimality. Write $v=(k_t-2)\cdot(1+\sum_{i=1}^{t} k_i)+r$. Then $r=3+\sum_{i=1}^{t-1} k_i(k_i-k_t+1)$. We need only show that $0 \leqslant r \leqslant \sum_{i=1}^{t} k_i$. The first inequality comes from the assumption. The second inequality comes from the assumption that $k_t \geqslant 3$ and the fact that $k_i(k_i-k_t+1) \leqslant k_i$ for $i=1,2,\ldots,t-1$. □

Corollary 5.4. *If there exists a cyclic BIBD* $B(v,k,1)$ *with* $v \equiv 1 \pmod{k(k-1)}$, *then there exists an optimal* $\mathrm{FHS}(v,1+(v-1)/(k-1),k-2)$ *derived from a partition-type cyclic* $(1+(v-1)/(k-1))$-$\mathrm{DP}(v,\{1,k-1\},k-2)$ *over* $\mathbf{Z}_v$.

Proof. The conclusion follows immediately from Theorem 5.3. □

We illustrate the above two constructions by the following lemma.

Lemma 5.5. *There exists an optimal* $\mathrm{FHS}(v,m,\lambda)$ *for* $(v,m,\lambda) \in \{(31,11,2),(31,12,2),(53,16,3),(53,17,3)\}$.

Proof. There exist both a cyclic $\mathrm{PBD}(31,\{3,4,4\},1)$ over $\mathbf{Z}_{31}$ with base blocks

$$\{0,7,18\},\ \{0,1,3,9\},\ \{0,4,14,19\},$$

and a cyclic $\mathrm{PBD}(53,\{3,3,5,5\},1)$ over $\mathbf{Z}_{53}$ with base blocks

$$\{0,8,30\},\ \{0,12,28\},\ \{0,1,3,7,20\},\ \{0,5,14,32,43\},$$

none of them having short block orbits.

(1) The following base blocks

$$\{0,7,18\},\ \{13,20\},\ \{24,11\},\ \{1,3,9\},\ \{22,23,25\},\ \{28,29,6\},$$
$$\{30,2,8\},\ \{4,14,19\},\ \{12,16,26\},\ \{17,21,5\},\ \{27,10,15\}$$

form a partition-type cyclic 11-DP(31, {2, 3}, 2) over $\mathbf{Z}_{31}$, which corresponds to an optimal FHS(31, 11, 2) over a frequency alphabet of size 11.

(2) The following base blocks

$$\{0\},\ \{7,18\},\ \{13,20\},\ \{24,11\},\ \{1,3,9\},\ \{22,23,25\},\ \{28,29,6\},$$
$$\{30,2,8\},\ \{4,14,19\},\ \{12,16,26\},\ \{17,21,5\},\ \{27,10,15\}$$

form a partition-type cyclic 12-DP(31, {1, 2, 3}, 2) over $\mathbf{Z}_{31}$, which corresponds to an optimal FHS(31, 12, 2) over a frequency alphabet of size 12.

(3) The following base blocks

$$\{0,8,30\},\ \{23,31\},\ \{45,22\},\ \{12,28\},\ \{25,37\},\ \{41,16\},$$
$$\{1,3,7,20\},\ \{33,34,36,40\},\ \{46,47,49,13\},\ \{50,51,4,17\},\ \{52,2,6,19\},$$
$$\{5,14,32,43\},\ \{10,15,24,42\},\ \{21,26,35,11\},\ \{39,44,18,29\},\ \{48,9,27,38\}$$

form a partition-type cyclic 16-DP(53, {2, 3, 4}, 3) over $\mathbf{Z}_{53}$, which corresponds to an optimal FHS(53, 16, 3) over a frequency alphabet of size 16.

(4) The following base blocks

$$\{0\},\ \{8,30\},\ \{23,31\},\ \{45,22\},\ \{12,28\},\ \{25,37\},\ \{41,16\},$$
$$\{1,3,7,20\},\ \{33,34,36,40\},\ \{46,47,49,13\},\ \{50,51,4,17\},\ \{52,2,6,19\},$$
$$\{5,14,32,43\},\ \{10,15,24,42\},\ \{21,26,35,11\},\ \{39,44,18,29\},\ \{48,9,27,38\}$$

form a partition-type cyclic 17-DP(53, {1, 2, 4}, 3) over $\mathbf{Z}_{53}$, which corresponds to an optimal FHS(53, 17, 3) over a frequency alphabet of size 17. □

In [5], Buratti gave a general construction for difference families over finite fields which, in some cases, gives rise to cyclic PBDs satisfying the requirements in Theorems 5.1 or 5.3. Given parameters p, m and λ, where p is a prime, in order to construct an optimal FHS(p, m, λ), we first try to find t positive integers $k_1, \ldots, k_t$, $2 \leqslant k_1 \leqslant \cdots \leqslant k_t$, such that

(1) $m = \sum_{i=1}^{t} k_t$, $\lambda = \max\{k_1 - 1, k_t - 2\}$, and $1 + \sum_{i=1}^{t} k_i(k_i - k_t + 1) \geqslant 0$; or
(2) $m = 1 + \sum_{i=1}^{t} k_t$, $\lambda = k_t - 2$, $k_t \geqslant 3$, and $3 + \sum_{i=1}^{t-1} k_i(k_i - k_t + 1) \geqslant 0$,

then apply Buratti's construction [5] to construct the desired cyclic PBD$(p, \{k_1, \ldots, k_t\}, \lambda)$, and finally apply Theorems 5.1 or 5.3 to obtain the desired optimal FH sequence. We use one of his results to illustrate the construction procedure described above.

Corollary 5.6. *Let $p = 18u + 1$ be a prime and let 3^e be the highest power of 3 dividing u. Then, if 3 is not a 3^{e+1}th power in $\mathbf{Z}_p$, there exist both an optimal* FHS$(p, 7u, 2)$ *and an optimal* FHS$(p, 1 + 7u, 2)$.

Proof. Taking $k_1 = \cdots = k_u = 3$ and $k_{u+1} = \cdots = k_{2u} = 4$, we construct a cyclic PBD$(p, \{k_1, \ldots, k_{2u}\}, 1)$ by Buratti's construction [5]. Let ϵ be a primitive 3rd root of unity in GF(p). Let $A_1 = \{\epsilon - 1, (\epsilon - 1)\epsilon, (\epsilon - 1)\epsilon^2\}$ and $A_2 = \{0, 1, \epsilon, \epsilon^2\}$. Since 3 is not a 3^{e+1}th power in GF(p), there is a suitable $f \leqslant e$ such that 3 is a 3^fth power but not a 3^{f+1}th power in GF(p). Then [5, Theorem 3.6] asserts that the following set of $2u$ base blocks

$$\left\{A_h \omega^{3^{f+1}i+j}\colon\ h = 1, 2,\ 0 \leqslant i < u/3^f,\ 0 \leqslant j < 3^f\right\}$$

generates a PBD$(p, \{\overbrace{3, \ldots, 3}^{u}, \overbrace{4, \ldots, 4}^{u}\}, 1)$, which is clearly cyclic. The assertions then follow from Theorems 5.1 and 5.3. □

6. Constructions from near resolvable cyclic BIBDs and Z-cyclically resolvable 1-rotational BIBDs

In this section, we use near resolvable cyclic BIBDs and **Z**-cyclically resolvable 1-rotational BIBDs to construct optimal FH sequences.

A cyclic $B(v, k, k-1)$ $(\mathbf{Z}_v, \mathbf{A})$ is near resolvable if its collection $\mathbf{A}$ of blocks can be partitioned into near resolution classes each of which misses a single point and contains every point of the design exactly once, and every other point of the design is absent from exactly one near resolution class. In this section, we deal with a near resolvable cyclic $B(kt+1, k, k-1)$ over $\mathbf{Z}_{kt+1}$, having $t(kt+1)$ blocks partitioned into t full orbits of length $kt+1$, so that all the $t(kt+1)$ near resolution classes can be generated from an initial near resolution class.

Theorem 6.1. *Suppose that there exists a near resolvable cyclic $B(kt+1, k, k-1)$.*

(1) *If $2 \leqslant k \leqslant t+2$, then there exists an optimal* FHS$(kt+1, t+1, k-1)$ *derived from a partition-type cyclic* $(t+1)$-DP$(kt+1, \{1, k\}, k-1)$ *over* $\mathbf{Z}_{kt+1}$.
(2) *If the near resolvable cyclic $B(kt+1, k, k-1)$ contains a base block B such that for all $x, y \in B$, $x + y \not\equiv 0 \pmod{kt+1}$, then there exists an optimal* FHS$(kt+1, t, k)$ *derived from a partition-type cyclic* t-DP$(kt+1, \{k, k+1\}, k)$ *over* $\mathbf{Z}_{kt+1}$.

Proof. Let $\mathcal{P} = \{B_1, B_2, \ldots, B_t\}$ be the initial near resolution class missing the element $0 \in \mathbf{Z}_{kt+1}$. If $2 \leqslant k \leqslant t+2$, then $\{\{0\}, B_1, B_2, \ldots, B_t\}$ forms a partition-type cyclic $(t+1)$-DP$(kt+1, \{1, k\}, k-1)$ over $\mathbf{Z}_{kt+1}$, which corresponds to an optimal FHS$(kt+1, t+1, k-1)$ by Theorem 2.1. On the other hand, if there is at least one base block, say B_1, such that for all $x, y \in B_1$, $x + y \not\equiv 0 \pmod{kt+1}$, then it can be easily seen that $\{B_1 \cup \{0\}, B_2, \ldots, B_t\}$ forms a partition-type cyclic t-DP$(kt+1, \{k, k+1\}, k)$ over $\mathbf{Z}_{kt+1}$, which corresponds to an optimal FHS$(kt+1, t, k)$ by Theorem 2.1. □

There are several infinite series of near resolvable cyclic BIBDs which satisfy the conditions in Theorem 6.1.

Corollary 6.2. *Let k, t be integers such that $kt+1$ is a prime.*

(1) *If $2 \leqslant k \leqslant t+2$, then there exists an optimal* FHS$(kt+1, t+1, k-1)$.
(2) *If k is odd, then there exists an optimal* FHS$(kt+1, t, k)$.

Proof. Let θ be a primitive element of $GF(kt+1)$. Then the required near resolution classes of a near resolvable cyclic $B(kt+1, k, k-1)$ can be obtained by developing the following near resolution class modulo $kt+1$:

$$\{\theta^0, \theta^t, \ldots, \theta^{(k-1)t}\},\ \{\theta^1, \theta^{t+1}, \ldots, \theta^{(k-1)t+1}\},\ \ldots,\ \{\theta^{t-1}, \theta^{2t-1}, \ldots, \theta^{kt-1}\}.$$

Then apply Theorem 6.1. On the other hand, if k is odd, then $it \not\equiv jt + kt/2 \pmod{kt}$ for $0 \leqslant i, j \leqslant k-1$, which ensures that the sum of any two points within each of the above blocks is always non-zero in $\mathbf{Z}_{kt+1}$. Then again apply Theorem 6.1. □

In connection with a cyclic $B(v,k,\lambda)$ $(\mathbf{Z}_v, \mathbf{A})$, a BIBD $B(v,k,\lambda)$ $(X, \mathbf{B})$ is said to be 1-rotational if it admits an automorphism σ consisting of a single fixed point and one cycle of length $v-1$. In this case, the point set X can be identified with $\mathbf{Z}_{v-1} \cup \{\infty\}$ and the 1-rotational BIBD has an automorphism $\sigma : i \mapsto i+1 \pmod{v-1}$ and $\infty \mapsto \infty$. The orbit containing a block $B \in \mathbf{B}$ is the set of the following blocks:

$$B^{\sigma^i} = B + i = \{b + i\colon b \in B\} \pmod{v-1}$$

for $i \in \mathbf{Z}_{v-1}$, where $\infty + i = i + \infty = \infty$. If a block orbit has $v-1$ distinct blocks, then this block orbit is full, otherwise short. A 1-rotational $B(v,k,\lambda)$ $(\mathbf{Z}_{v-1} \cup \{\infty\}, \mathbf{B})$ is resolvable if the collection $\mathbf{B}$ of blocks can be partitioned into resolution classes $\mathcal{R}_1, \ldots, \mathcal{R}_r$, $r = \lambda(v-1)/(k-1)$, such that every point of $\mathbf{Z}_{v-1} \cup \{\infty\}$ is contained in exactly one block in each resolution class. A 1-rotational $B(v,k,\lambda)$ is $\mathbf{Z}$-cyclically resolvable if the blocks of the ith resolution class $\mathcal{R}_i$ are the $(i-1)$th translates of the blocks of the resolution class $\mathcal{R}_1$, i.e., $\mathcal{R}_i = \mathcal{R}_1^{\sigma^{i-1}} = \mathcal{R}_1 + (i-1) \pmod{v-1}$ for all i, $1 \leqslant i \leqslant r$, where $\mathcal{R}_1 + (i-1) \pmod{v-1} = \{B + (i-1) \pmod{v-1}\colon B \in \mathcal{R}_1\}$.

Theorem 6.3. *If there exists a* $\mathbf{Z}$*-cyclically resolvable* 1*-rotational* $B(kt,k,k-1)$*, then there exists an optimal* FHS$(kt-1,t,k-1)$ *derived from a partition-type cyclic* t-DP$(kt-1, \{k-1,k\}, k-1)$ *over* $\mathbf{Z}_{kt-1}$.

Proof. Let $\mathcal{R}_1 = \{B_1, B_2, \ldots, B_{t-1}, B_\infty\}$ be the first resolution class, where $\infty \in B_\infty$. Then clearly $\{B_1, B_2, \ldots, B_{t-1}, B_\infty \setminus \{\infty\}\}$ forms a partition-type cyclic t-DP$(kt-1, \{k-1,k\}, k-1)$ over $\mathbf{Z}_{kt-1}$. Applying Theorem 2.1, we obtain the desired optimal FHS$(kt-1,t,k-1)$. □

$\mathbf{Z}$-cyclic whist tournaments for $4t$ players are special $\mathbf{Z}$-cyclically resolvable 1-rotational $B(kt,k,k-1)$ with $k=4$. A whist tournament Wh$(4t)$ for $4t$ players is a schedule of games each involving two players opposing two others, such that

(1) the games are arranged into $4t-1$ rounds, each of t games;
(2) each player plays in exactly one game in each round;
(3) each player partners every other player exactly once; and
(4) each player opposes every other player exactly twice.

A Wh$(4t)$ is $\mathbf{Z}$-cyclic if the players are $\infty, 0, 1, \ldots, 4t-2$ and each round is obtained from the previous one by adding 1 modulo $4t-1$ to each non-∞ entry. By ignoring the order in each game, we immediately obtain a $\mathbf{Z}$-cyclically resolvable 1-rotational $B(4t,4,3)$ over $\mathbf{Z}_{4t-1} \cup \{\infty\}$.

Corollary 6.4. *Let* P *denote any product of primes* p *with each* $p \equiv 1 \pmod 4$. *Then there exists an optimal* FHS$(4t-1,t,3)$ *in the following cases*:

(1) $4t \leqslant 64$.
(2) $4t = 4^i, i \geqslant 1$.
(3) $4t = qP + 1, q \in \{7, 11, 19, 23, 31, 43, 47, 59\}$.
(4) $4t = 3P + 1$*, where all* $p-1$ *are divisible by the same power of* 2.
(5) $4t = qr^2P + 1$*,* q *and* r *distinct primes,* $q, r \equiv 3 \pmod 4$, $q < 60, r < 500$.

Proof. A $\mathbf{Z}$-cyclic Wh$(4t)$ is known to exists in these cases (see [2], for example). Then apply Theorem 6.3. □

Since the publication of [2], there have been a few additional advances on $\mathbf{Z}$-cyclic WH$(4t)$. We also note that some combinatorial structures related with $\mathbf{Z}$-cyclic whist tournaments such as $\mathbf{Z}$-cyclic generalized whist tournaments, $\mathbf{Z}$-cyclic pitch tournaments and cyclic frames can also be used to construct optimal FH sequences in a similar way. In the remainder of this section, we describe a few constructions for cyclic frames and $\mathbf{Z}$-cyclically resolvable 1-rotational BIBDs. The interested readers may refer to [1,3,10] for more details on $\mathbf{Z}$-cyclic whist tournaments, $\mathbf{Z}$-cyclic generalized whist tournaments and $\mathbf{Z}$-cyclic pitch tournaments.

Let K be a set of positive integers. A group divisible design (K,λ)-GDD is a triple $(X,\mathbf{G},\mathbf{B})$ where X is a finite set of points, $\mathbf{G}$ is a set of subsets of X called groups which partition X, $\mathbf{B}$ is a collection of subsets of X called blocks with sizes from K such that every pair of points from distinct groups occurs in exactly λ blocks, and no pair of points belonging to a group occurs in any block. We use the usual exponential notation for the type of GDDs. Thus a GDD of type $1^i 2^j \ldots$ is one in which there are i groups of size 1, j groups of size 2, and so on. A (k,λ)-frame of type T is a $(\{k\},\lambda)$-GDD $(X,\mathbf{G},\mathbf{B})$ of type T in which the collection $\mathbf{B}$ of blocks can be partitioned into holey resolution classes each of which partitions $X \setminus G_i$ for some $G_i \in \mathbf{G}$.

Let $(X,\mathbf{G},\mathbf{B})$ be a (K,λ)-GDD of type h^n, and σ be a permutation on X. For any subset $T = \{x_1,\ldots,x_k\} \subseteq X$, define $T^\sigma = \{x_1^\sigma,\ldots,x_k^\sigma\}$. If $\mathbf{G}^\sigma = \{G^\sigma\colon\ G \in \mathbf{G}\} = \mathbf{G}$ and $\mathbf{B}^\sigma = \{B^\sigma\colon\ B \in \mathbf{B}\} = \mathbf{B}$, then σ is an automorphism of the GDD $(X,\mathbf{G},\mathbf{B})$. Any automorphism σ partitions $\mathbf{B}$ into equivalence classes called the block orbits of $\mathbf{B}$ under σ. An arbitrary set of representatives for these block orbits of $\mathbf{B}$ is the base blocks of the GDD. If there is an automorphism consisting of a single cycle of length $|X| = nh$, then the (K,λ)-GDD is said to be cyclic and denoted by (K,λ)-CGDD. For a (K,λ)-CGDD, the point set X can be identified with $\mathbf{Z}_{nh}$. In this case, the design has an automorphism $\sigma : i \mapsto i+1 \pmod{nh}$, and each group must be the subgroup $n\mathbf{Z}_h$ of $\mathbf{Z}_{nh}$ or its cosets. In the remainder of this section, when we say a (K,λ)-CGDD, we always mean a (K,λ)-CGDD in which each of its block orbits under the automorphism σ contains exactly nh distinct blocks.

In a $(k,k-1)$-frame of type h^n, it is well known (see [12], for example) that there are h holey resolution classes associated with each group, and there are altogether nh holey resolution classes. If the underlying GDD of a $(k,k-1)$-frame of type h^n is cyclic with respect to an automorphism $\sigma : i \mapsto i+1 \pmod{nh}$ of order $nh = |X|$, such that the blocks of the jth holey resolution class $\mathcal{R}_j$ are the jth translates of the blocks of the resolution class $\mathcal{R}_0$, i.e., $\mathcal{R}_j = \mathcal{R}_0^{\sigma^j} = \mathcal{R}_0 + j \pmod{nh}$ for all $j \in \mathbf{Z}_{nh}$, then the frame is said to be cyclic with respect to σ. The class $\mathcal{R}_0$ is an initial holey resolution class of this cyclic frame. A cyclic $(k,k-1)$-frame of type 1^n is just a near resolvable cyclic $B(n,k,k-1)$.

Let $\mathcal{R}$ be a holey resolution class associated with the group $n\mathbf{Z}_h$ of a cyclic $(k,k-1)$-frame of type h^n defined over $\mathbf{Z}_{nh}$, and $\mathcal{R}'$ be a resolution class of a $\mathbf{Z}$-cyclically resolvable 1-rotational $B(h+1,k,k-1)$ defined over $n\mathbf{Z}_h \cup \{\infty\}$ where ∞ is a new point such that $\sigma : \infty \mapsto \infty$. Then $\mathcal{R} \cup \mathcal{R}'$ is a resolution class of $\mathbf{Z}_{nh} \cup \{\infty\}$, and by adding i modulo nh, $i \in \mathbf{Z}_{nh}$, to each point of the blocks in $\mathcal{R} \cup \mathcal{R}'$, we obtain nh distinct resolution classes of $\mathbf{Z}_{nh} \cup \{\infty\}$.

Theorem 6.5. *If there exist both a cyclic $(k,k-1)$-frame of type h^n and a $\mathbf{Z}$-cyclically resolvable 1-rotational $B(h+1,k,k-1)$, then there exists a $\mathbf{Z}$-cyclically resolvable 1-rotational $B(nh+1,k,k-1)$.*

Now we provide some direct and recursive constructions for cyclic frames.

Lemma 6.6. *If $u \equiv 1 \pmod 4$ is a prime or $u = 9$, then there exists a cyclic $(4,3)$-frame of type 3^u.*

Proof. Write $u = 4n+1$ and let θ be a primitive element of $GF(u)$. For u a prime, Moore [15] showed that the following is the required initial class:

$$\begin{aligned}
&\{(\theta^i,0),(\theta^{n+i},1),(\theta^{2n+i},0),(\theta^{3n+i},1)\}, \quad 0 \leqslant i \leqslant n-1,\\
&\{(\theta^i,1),(\theta^{2n+i},1),(\theta^{3n+i},2),(\theta^{n+i},2)\}, \quad 0 \leqslant i \leqslant n-1,\\
&\{(\theta^i,2),(\theta^{3n+i},0),(\theta^{n+i},0),(\theta^{2n+i},2)\}, \quad 0 \leqslant i \leqslant n-1.
\end{aligned}$$

These $3n$ base blocks form a holey resolution class on $Z_u \times Z_3$ with hole $\{0\} \times Z_3$. Since $Z_u \times Z_3 \cong Z_{3u}$, it is an initial class.

For $u = 9$, the required initial class is as follows:

$$\begin{aligned}
&\{1,2,3,5\}, \quad \{4,12,15,26\}, \quad \{6,19,21,25\},\\
&\{7,20,14,24\}, \quad \{8,13,16,23\}, \quad \{10,17,11,22\}. \qquad \square
\end{aligned}$$

Given positive integers n and h, let $I_n = \{1,2,\ldots,n\}$ and $X = I_n \times \mathbf{Z}_h$. The elements of X are denoted by (a,b). Suppose that a $(k,k-1)$-frame of type h^n has n special holey resolution classes $\mathcal{R}_0, \mathcal{R}_h, \ldots, \mathcal{R}_{(n-1)h}$, whose elements form a partition of the sets $X \setminus \{1\} \times \mathbf{Z}_h$, $X \setminus \{2\} \times \mathbf{Z}_h$, $\ldots$, $X \setminus \{n\} \times \mathbf{Z}_h$, respectively, such that for any fixed $i \in \{0,1,\ldots,n-1\}$, the holey resolution class $\mathcal{R}_{ih+j}$ can be obtained from the holey resolution class $\mathcal{R}_{ih}$ by adding j modulo h to the second component of each element, where $j \in \mathbf{Z}_h$. Such a $(k,k-1)$-frame is said to be group cyclic. The classes $\mathcal{R}_0, \mathcal{R}_h, \ldots, \mathcal{R}_{(n-1)h}$ are the initial holey resolution classes. It is easy to see that a cyclic $(k,k-1)$-frame of type h^n can also be regarded as a group cyclic $(k,k-1)$-frame of the same type h^n by using the automorphism $\sigma^h : i \mapsto i+h \pmod{nh}$.

Theorem 6.7. *Suppose that there exists a $(K,1)$-CGDD of type g^n. If there exists a group cyclic $(l,l-1)$-frame of type h^k for each $k \in K$, then there exists a cyclic $(l,l-1)$-frame of type $(hg)^n$.*

Proof. Let $\mathbf{F}$ be the collection of base blocks of the $(K,1)$-CGDD and $B = \{b_1,b_2,\ldots,b_k\}$ be a base block in $\mathbf{F}$. By assumption, we have a group cyclic $(l,l-1)$-frame of type h^k defined over $B \times \mathbf{Z}_h$ with initial holey resolution classes $\mathcal{R}_{b_1}(B), \mathcal{R}_{b_2}(B), \ldots, \mathcal{R}_{b_k}(B)$, whose elements form a partition of the sets $(B \setminus \{b_1\}) \times \mathbf{Z}_h$, $(B \setminus \{b_2\}) \times \mathbf{Z}_h$, $\ldots$, $(B \setminus \{b_k\}) \times \mathbf{Z}_h$, respectively. Now we construct a collection $\mathbf{A}_{b_i}(B)$ of new base blocks by replacing each point (b_x, y) of all the blocks of the initial class $\mathcal{R}_{b_i}(B)$ by $(b_x - b_i) + ygn \pmod{hgn}$, where $b_i, b_x \in B$, $b_x \neq b_i$, and $y \in \mathbf{Z}_h$. As B ranges over $\mathbf{F}$ and b_i ranges over B, we obtain a collection $\mathbf{A} = \bigcup_{B\in\mathbf{F}} \bigcup_{b_i \in B} \mathbf{A}_{b_i}(B)$ of new base blocks. Then it is readily checked that $\Delta\mathbf{A} = \bigcup_{B\in\mathbf{F}} \Delta(\bigcup_{b_i\in B} \mathbf{A}_{b_i}(B)) = \bigcup_{B\in\mathbf{F}} \bigcup_{b_i,b_j\in B} \{(b_i - b_j) + (y_s - y_t)gn\colon\ b_i \neq b_j,\ y_s, y_t \in \mathbf{Z}_h\} = (l-1)(\mathbf{Z}_{hgn} \setminus n\mathbf{Z}_{gh})$, and $\mathbf{A}$ is an initial holey resolution class of the desired cyclic $(l,l-1)$-frame of type $(hg)^n$ missing the group $n\mathbf{Z}_{gh}$, noting that $\mathbf{F}$ is the collection of base blocks of the $(K,1)$-CGDD, and every element z of $\mathbf{Z}_{hgn} \setminus \{0,n,2n,\ldots,(hg-1)n\}$ can be written as $z = u \cdot gn + r$ such that $0 \leqslant u \leqslant h-1$, $0 \leqslant r \leqslant gn-1$ and $r \neq 0,n,2n,\ldots,(g-1)n$. $\square$

Since a cyclic $(l,l-1)$-frame is also a group cyclic $(l,l-1)$-frame, we have the following corollary.

Corollary 6.8. *Suppose that there exists a $(K,1)$-CGDD of type g^n. If there exists a cyclic $(l,l-1)$-frame of type h^k for each $k \in K$, then there exists a cyclic $(l,l-1)$-frame of type $(hg)^n$.*

We illustrate Theorem 6.7 with the following lemma.

Lemma 6.9. *There exists a cyclic $(4,3)$-frame of type 3^{81}.*

Proof. From [13, Lemma 3.4], we have a cyclic $B(81,5,1)$, which is also a $(\{5\},1)$-CGDD of type 1^{81}. From Lemma 6.6, we have a cyclic $(4,3)$-frame of type 3^5. Applying Corollary 6.8 gives the desired cyclic $(4,3)$-frame of type 3^{81}. □

Infinite series and sporadic examples of cyclic GDDs and BIBDs can be found in [6]. By Theorems 6.3, 6.5 and 6.7, we can obtain many new optimal FH sequences.

7. A general recursive construction

In [11], Fuji-Hara, Miao and Mishima provided a recursive construction for partition-type cyclic difference packings. In this section, we describe a slight generalization of their recursive construction.

We first recall the notion of a partition-type cyclic difference packing with a hole. Let H be a subset of $\mathbf{Z}_v$ and $\mathbf{P} = \{B_1, B_2, \ldots, B_l\}$ be a partition of $\mathbf{Z}_v \setminus H$ such that $0 \in H$ and $\{|B_i|\colon 1 \leqslant i \leqslant l\} = K$. $\mathbf{P}$ is called a partition-type cyclic difference packing l-DP(v,K,λ) with a hole H if any integer $d \in \mathbf{Z}_v \setminus H$ can be represented as the difference $a-b$, $a,b \in B_i$, $a \neq b$, $1 \leqslant i \leqslant l$, in at most λ ways, and one integer $d_0 \in \mathbf{Z}_v \setminus H$ can be represented in exactly λ ways, whereas no integer in H can be represented in such a way.

A case of particular interest in this section is when H is the union of several mutually distinct additive subgroups $G_1, G_2, \ldots, G_r$ and G of $\mathbf{Z}_v$ of orders $g_1, g_2, \ldots, g_r$ and g, respectively, such that $G_i \cap G_j = G$ for any i and j satisfying $1 \leqslant i < j \leqslant r$. Such a partition-type cyclic l-DP(v,K,λ) with the hole $H = \bigcup_{i=1}^r G_i$ is said to be $(g_1, g_2, \ldots, g_r; g)$-regular. Fuji-Hara, Miao and Mishima [11] considered the case $G = \{0\}$, i.e., $g = |G| = 1$. However, in this paper, we do not impose any restriction on the size of G. If $r = 1$, we simply write g_1-regular for such a partition-type cyclic difference packing.

We also need the notion of a homogeneous difference matrix. Let $\Sigma = (\delta_{ij})$ be a $t \times \lambda n$ matrix with entries from $\mathbf{Z}_n$ such that any element of $\mathbf{Z}_n$ appears in every row exactly λ times. If each element of $\mathbf{Z}_n$ occurs exactly λ times among the differences $\sigma_{hj} - \sigma_{ij}$, $j = 1, 2, \ldots, \lambda n$, for any $h \neq i$, where $1 \leqslant h, i \leqslant t$, then Σ is called a homogeneous $(n,t;\lambda)$ difference matrix over $\mathbf{Z}_n$.

For any subset S in $\mathbf{Z}_n$, we define a subset $S \oplus v\mathbf{Z}_n$ in $\mathbf{Z}_{nv}$ by $S \oplus v\mathbf{Z}_n = \{s + vz\colon s \in S, z \in \mathbf{Z}_n\}$.

Theorem 7.1. *Suppose that there exists a partition-type cyclic l-DP(v,K,λ) with a $(g_1, g_2, \ldots, g_r; u)$-regular hole $H = \bigcup_{i=1}^r G_i$ over $\mathbf{Z}_v$ such that $G_i \cap G_j = G$ for any i and j satisfying $1 \leqslant i < j \leqslant r$. If there exists a homogeneous $(n,k;1)$ difference matrix over $\mathbf{Z}_n$, where k is the maximum integer in K, then there exists a partition-type cyclic nl-DP(nv,K,λ) with an $(ng_1, ng_2, \ldots, ng_r; nu)$-regular hole $H \oplus v\mathbf{Z}_n = \bigcup_{i=1}^r (G_i \oplus v\mathbf{Z}_n)$ over $\mathbf{Z}_{nv}$ such that $(G_i \oplus v\mathbf{Z}_n) \cap (G_j \oplus v\mathbf{Z}_n) = G \oplus v\mathbf{Z}_n$. Furthermore, if there exists a partition-type cyclic l_j-DP(ng_j,K,λ) with an nu-regular hole $\frac{g_j}{u}\mathbf{Z}_{nu}$ over $\mathbf{Z}_{ng_j}$ for $1 \leqslant j \leqslant t$, where*

$t \leqslant r-1$, then there exists a partition-type cyclic $(nl + \sum_{j=1}^{t} l_j)$-DP$(nv, K, \lambda)$ with an $(ng_{t+1}, ng_{t+2}, \ldots, ng_r; nu)$-regular hole $\bigcup_{i=t+1}^{r}(G_i \oplus v\mathbf{Z}_n)$ over $\mathbf{Z}_{nv}$ such that $(G_i \oplus v\mathbf{Z}_n) \cap (G_j \oplus v\mathbf{Z}_n) = G \oplus v\mathbf{Z}_n$ for $t+1 \leqslant i < j \leqslant r$.

Proof. Let $\Sigma = (\sigma_{ij})$ be a homogeneous $(n, k; 1)$ difference matrix over $\mathbf{Z}_n$. Let $G_1, G_2, \ldots, G_r$ and G be mutually distinct additive subgroups of $\mathbf{Z}_v$ of orders $g_1, g_2, \ldots, g_r$ and g, respectively, such that $G_i \cap G_j = G$ for any i and j satisfying $1 \leqslant i < j \leqslant r$, and $H = G \cup (G \setminus G_1) \cup \cdots \cup (G \setminus G_r)$ is the hole of the partition-type cyclic l-DP(v, K, λ). For each block $B_i = \{b_{i1}, \ldots, b_{is}\}$ of the partition-type cyclic l-DP(v, K, λ) with a $(g_1, g_2, \ldots, g_r; u)$-regular hole H, where $s \leqslant k$, construct the following n new blocks:

$$B_i^{(j)} = \{b_{i1} + \sigma_{1j}v, \ldots, b_{is} + \sigma_{sj}v\} \pmod{nv}, \quad j = 1, \ldots, n.$$

Then, in a way similar to [11], we can readily check that these newly defined blocks form the desired partition-type cyclic nl-DP(nv, K, λ) with an $(ng_1, ng_2, \ldots, ng_r; nu)$-regular hole $H \oplus v\mathbf{Z}_n$ over $\mathbf{Z}_{nv}$.

If there exists a partition-type cyclic l_j-DP(ng_j, K, λ) over $\mathbf{Z}_{ng_j}$ with an nu-regular hole $\frac{g_j}{u}\mathbf{Z}_{nu}$ for $1 \leqslant j \leqslant t$, where $t \leqslant r-1$, then by adding the new blocks $\frac{v}{g_j}B = \{\frac{v}{g_j}b_i\colon\ b_i \in B\}$ for all blocks B in the partition-type cyclic l_j-DP(ng_j, K, λ), $1 \leqslant j \leqslant t$, we immediately obtain a partition-type cyclic $(nl + \sum_{j=1}^{t} l_j)$-DP$(nv, K, \lambda)$ with an $(ng_{t+1}, \ldots, ng_r; nu)$-regular hole $\bigcup_{i=t+1}^{r}(G_i \oplus v\mathbf{Z}_n)$ over $\mathbf{Z}_{nv}$ such that $(G_i \oplus v\mathbf{Z}_n) \cap (G_j \oplus v\mathbf{Z}_n) = G \oplus v\mathbf{Z}_n$ for $t+1 \leqslant i < j \leqslant r$. $\square$

The above construction for partition-type cyclic difference packings is quite general. If we take $t = r-1$, and assume that there exists a partition-type cyclic l_r-DP(ng_r, K, λ) over $\mathbf{Z}_{ng_r}$, then in a similar way to the proof of Theorem 7.1, by adding the new blocks $\frac{v}{g_r}B = \{\frac{v}{g_r}b_i\colon b_i \in B\}$ for all blocks B in the partition-type cyclic l_r-DP(ng_r, K, λ) into the collection of blocks of the partition-type cyclic $(nl + \sum_{j=1}^{r-1} l_j)$-DP$(nv, K, \lambda)$ with an ng_r-regular hole $G_r \oplus v\mathbf{Z}_n$ over $\mathbf{Z}_{nv}$, we obtain a partition-type cyclic $(nl + \sum_{j=1}^{r} l_j)$-DP$(nv, K, \lambda)$, which may correspond to an optimal FH sequence in some case. Ingredient partition-type cyclic difference packings required in Theorem 7.1 can be found in, for example, [11] and the previous sections of this paper. Results on difference matrices can be found in [7].

8. Conclusions

In this paper, we followed the style in [11] to investigate FHMA spread-spectrum communication systems with a single optimal FH sequence. Such optimal FH sequences were constructed via partition-type cyclic difference packings from various combinatorial structures including t-flats in a projective space, difference sets satisfying certain special conditions, cyclic PBDs, near resolvable cyclic BIBDs, $\mathbf{Z}$-cyclically resolvable 1-rotational BIBDs, cyclic frames, and difference matrices. These enriched our knowledge on optimal FH sequences.

FHMA spread-spectrum communication systems with plural optimal FH sequences should also have close relation with combinatorial design theory. An investigation of FHMA systems with plural optimal FH sequences from a combinatorial viewpoint is clearly worthy of further research.

Acknowledgments

The authors thank Professor Q. Xiang at the University of Delaware and Professor L. Zhu at Suzhou University for their helpful discussions on the constructions in Sections 4 and 6, respectively, and the two anonymous referees for their helpful comments. Special thanks goes to Professor Henk C.A. van Tilborg for organizing the symposium in honor of Professor J.H. van Lint.

References

[1] R.J.R. Abel, N.J. Finizio, M. Greig, S.J. Lewis, Pitch tournament designs and other BIBDs—Existence results for the case $v = 8n$, J. Combin. Des. 9 (2001) 334–356.
[2] I. Anderson, Whist tournaments, in: C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996, pp. 504–508.
[3] I. Anderson, N.J. Finizio, Some new **Z**-cyclic whist tournament designs, Discrete Math. 293 (2005) 19–28.
[4] T. Beth, D. Jungnickel, H. Lenz, Design Theory, second ed., Cambridge Univ. Press, Cambridge, UK, 1999.
[5] M. Buratti, Pairwise balanced designs from finite fields, Discrete Math. 208/209 (1999) 103–117.
[6] C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996.
[7] C.J. Colbourn, W. De Launey, Difference matrices, in: C.J. Colbourn, J.H. Dinitz (Eds.), The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 1996, pp. 287–297.
[8] G.L. Ebert, Partitioning projective geometries into caps, Canad. J. Math. 37 (1985) 1163–1175.
[9] P. Fan, M. Darnell, Sequence Design for Communications Applications, Research Studies Press, Taunton, 1996.
[10] N.J. Finizio, B.J. Travers, **Z**-cyclic generalized whist frames and **Z**-cyclic generalized whist tournaments, Discrete Math. 279 (2004) 215–223.
[11] R. Fuji-Hara, Y. Miao, M. Mishima, Optimal frequency hopping sequences: A combinatorial approach, IEEE Trans. Inform. Theory 50 (2004) 2408–2420.
[12] S. Furino, Y. Miao, J. Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence, CRC Press, Boca Raton, FL, 1996.
[13] G. Ge, J. Yin, Constructions for optimal $(v, 4, 1)$ optical orthogonal codes, IEEE Trans. Inform. Theory 47 (2001) 2998–3004.
[14] A. Lempel, H. Greenberger, Families of sequences with optimal Hamming correlation properties, IEEE Trans. Inform. Theory IT-20 (1974) 90–94.
[15] E.H. Moore, Tactical memoranda I–III, Amer. J. Math. 18 (1896) 264–303.
[16] Tran van Trung, Constructions for near resolvable designs and BIBDs, J. Combin. Des. 7 (1999) 227–231.