New families of optimal frequency hopping sequence sets

Jingjun Bao, Lijun Ji

Abstract—Frequency hopping sequences (FHSs) are employed to mitigate the interferences caused by the hits of frequencies in frequency hopping spread spectrum systems. In this paper, we present some new algebraic and combinatorial constructions for FHS sets, including an algebraic construction via the linear mapping, two direct constructions by using cyclotomic classes and recursive constructions based on cyclic difference matrices. By these constructions, a number of series of new FHS sets are then produced. These FHS sets are optimal with respect to the Peng-Fan bounds.

Index Terms—Frequency hopping sequences (FHSs), Hamming correlation, partition-type balanced nested cyclic difference packing, Peng-Fan bounds.

I. INTRODUCTION

FREQUENCY hopping (FH) multiple-access is widely used in the modern communication systems such as ultrawideband (UWB), military communications, Bluetooth and so on, for example, [2], [3], [12], [14]-[16], [19], [21]-[24], and the references therein. Moreover, some generic extension methods have been proposed [4], [5], [22], which obtain some new optimal FHS sets.

In this paper, we present some constructions for FHS sets with optimal Hamming correlations. First of all, we present an algebraic construction for optimal FHS sets by using linear mapping. Secondly, we give two direct constructions for FHS sets by using cyclotomic classes. Finally, we present recursive constructions for FHS sets, which increase their lengths and alphabet sizes, and preserve their maximum Hamming correlations. Our constructions yield optimal FHS sets with new and flexible parameters not covered in the literature. The parameters of FHS sets with optimal Hamming correlations from the known constructions and the new ones are listed in the table.

The remainder of this paper is organized as follows. Section II introduces the known bounds on the Hamming correlations of FHSs and FHS sets. Section III gives an algebraic construction of FHS sets. Section IV presents two direct constructions and recursive constructions of FHS sets. Section V concludes this paper with some remarks.

II. PRELIMINARIES

For any positive integer \( l \geq 2 \), let \( F = \{f_0, f_1, \ldots, f_{l-1}\} \) be a set of \( l \) available frequencies, also called an alphabet. A sequence \( X = \{x(t)\}_{t=0}^{n-1} \) is called a frequency hopping sequence (FHS) of length \( n \) over \( F \) if \( x(t) \in F \) for \( 0 \leq t \leq n-1 \). For any two FHSs \( X = \{x(t)\}_{t=0}^{n-1} \) and \( Y = \{y(t)\}_{t=0}^{n-1} \) of length \( n \) over \( F \), their Hamming correlation \( H_{X,Y} \) is defined by

\[
H_{X,Y}(\tau) = \sum_{t=0}^{n-1} h[x(t), y(t+\tau)], 0 \leq \tau < n, \quad (1)
\]

where \( h[a, b] = 1 \) if \( a = b \) and 0 otherwise, and the addition is performed modulo \( n \). If \( x(t) = y(t) \) for \( 0 \leq t \leq n-1 \), i.e., \( X = Y \), we call \( H_{X,X}(\tau) \) the Hamming autocorrelation of \( X \); otherwise, we say \( H_{X,Y}(\tau) \) the Hamming cross-correlation of \( X \) and \( Y \). For any two distinct sequences \( X \) and \( Y \) over \( F \), we define

\[
H(X) = \max_{0 \leq \tau < n} \{H_{X,X}(\tau)\}
\]

and

\[
H(X,Y) = \max_{0 \leq \tau < n} \{H_{X,Y}(\tau)\}.
\]

Lempel and Greenberger established the following lower bound on \( H(X) \) [17].

Lemma 2.1: [17] For every FHS \( X \) of length \( n \) over an alphabet of size \( l \), it holds that

\[
H(X) \geq \frac{(n-\epsilon)(n+\epsilon-l)}{ln-1}, \quad (2)
\]

where \( \epsilon \) is the least nonnegative residue of \( n \) modulo \( l \).

In general, it is more convenient to use a simplified version of the Lempel-Greenberger bound given in Corollary 1.2 of [14].

Lemma 2.2: [14] For every FHS \( X \) of length \( n \) over an alphabet of size \( l \), it holds that

\[
H(X) \geq \begin{cases} k & \text{if } n \neq l, \\
0 & \text{if } n = l,
\end{cases}
\]
| Length               | Number of sequences | $H_{max}$ | Alphabet size | Constraints                                                                 | Reference |
|---------------------|---------------------|-----------|---------------|------------------------------------------------------------------------------|-----------|
| $p^t(p^m - 1)$      | $\frac{a}{p}$       | $p^b$     | $a + 1$       | $p^m - 1 = ab$, $a \geq p'(b + 1)$, $\gcd(p', p^m - 1) = 1$                | [19]      |
| $q^m - 1$           | $q^u$               | $q^m - u$ | $q^u$         | $m > u \geq 1$                                                               | [24]      |
| $\frac{q^m - 1}{d}$ | $d$                 | $\frac{q^m - u}{d}$ | $q^u$         | $d|q - 1$, $m > u \geq 1$, $\gcd(d, m) = 1$                                 | [24]      |
| $2^d - 1$           | $2^d - 1$           | $2^t - 1$ | $2^t$         | $q + 1 \equiv d \pmod{2d}$                                                   | [11]      |
| $tp^m$              | $\frac{1}{p}$       | $tp$      | $p$           | $p > t \geq 2$                                                               | [9]       |
| $t2^{m-1}$          | $\frac{1}{d}$       | $t2^{m-1}$ | $q$           | $d \geq t \geq 2$, $d|q - 1$, $\gcd(m, d) = 1$                             | [5]       |
| $v$                 | $f$                 | $e$       | $\frac{v-1}{e} + 1$ | $v$ is not a prime or $v$ is a prime with $f \geq e > 1$                   | [23]      |
| $p(p^m - 1)$        | $p^m - 1$           | $p^m - u + 1$ | $p^u$         | $m > u > 1$                                                                  | Theorem 4.1 |
| $tv$                | $\frac{1}{l}$       | $t$       | $v$           | $p_1 > t > 1$                                                                 | Theorem 4.3 |
| $3v$                | 2                   | 4         | $\frac{3v+1}{4}$ | $\text{each } p_j \equiv 1 \pmod{4}$ and $v \not\equiv 0 \pmod{25}$        | Corollary 3.8 |
| $\frac{w(q^m - 1)}{d}$ | $d$                 | $\frac{w(q^m - u)}{d}$ | $wq^u$         | $\gcd(d, m) = 1$, $q_1 > q^m - u$, $m > u \geq 1$                          | Corollary 4.13 |
| $vw$                | $f$                 | $e$       | $\frac{v-1}{e}w + \frac{w-1}{e} + 1$ | $e \geq e^t \geq 2$, $f \geq 2$, $v \geq e^2$, $q_1 \geq p_1$            | Theorem 4.16 |
| $vw(p^m - 1)$       | $\frac{a}{p}$       | $p^b$     | $\alpha w + \frac{(v-1)w}{e} + \frac{w-1}{e} + 1$ | $p^m - 1 = ab$, $a \geq p'(b + 1)$, $b \geq e \geq e^t \geq 2$, $\gcd(p', p^m - 1) = 1$, $q_1 \geq p_1 > p^m - 1$ | Theorem 4.18 |

$q$ is a prime power; $p, p'$ are primes; $v$ is an integer with prime factor decomposition $v = p_1^{m_1}p_2^{m_2} \cdots p_s^{m_s}$ with $p_1 < p_2 < \ldots < p_s$; $e$ is an integer such that $\gcd(p_1 - 1, p_2 - 1, \ldots, p_s - 1)$, and $f = \frac{p_1 - 1}{e}$; $w$ is any integer with prime factor decomposition $w = q_1^{n_1}q_2^{n_2} \cdots q_t^{n_t}$ with $q_1 < q_2 < \ldots < q_t$; $e'$ is an integer such that $e' | \gcd(q_1 - 1, q_2 - 1, \ldots, q_t - 1)$; $t, m, d, u, a$ and $b$ are positive integers.

Lemma 2.3: [18] Let $S$ be a set of $M$ sequences of length $n$ over an alphabet $F$ of size $l$. Define $I = \left\lfloor \frac{nm - l}{nM - l} \right\rfloor$. Then

$$H(S) \geq \left\lfloor \frac{(nm - l)n}{(nM - 1)l} \right\rfloor$$

and

$$H(S) \geq \left\lfloor \frac{2(nM - (1 + l)H)}{(nM - 1)M} \right\rfloor.$$  

A FHS set is called optimal if one of the bounds in Lemma 2.3 is met. We give a simplified version of the Peng-Fan bound [4] in the following corollary.

Corollary 2.4: Let $S$ be a set of $M$ sequences of length $n$ over an alphabet $F$ of size $l$ with $M > 1$. Then

$$H(S) \geq \begin{cases} k & \text{if } \epsilon M < l, \text{ and} \\ k + 1 & \text{otherwise,} \end{cases}$$
where $\epsilon$ is the least nonnegative residue of $n$ modulo $l$ and $k = \frac{n - \epsilon}{l}$. This implies that when $n > l$, if

$$H(S) = \begin{cases} k & \text{if } \epsilon M < l, \\ k + 1 & \text{otherwise,} \end{cases}$$

then the FHS set is optimal.

**Proof:** Denote $I = \left\lfloor \frac{nM}{l} \right\rfloor$, then $nM = lI + r$, where $r$ is a nonnegative integer and $r < l$. Simple computation shows that $I = \left\lfloor \frac{nM}{l} \right\rfloor = \left\lfloor \frac{k + \epsilon}{l} \right\rfloor = kM + \left\lfloor \frac{n - \epsilon}{l} \right\rfloor$. Since $-1 < \frac{1}{l} \leq 0$, we obtain

$$\begin{bmatrix} 2lm - (l + 1)M \\ m - 1 \end{bmatrix} = \begin{bmatrix} l(l + 2r - 1) \\ l(r - 1) \end{bmatrix} = \begin{bmatrix} \frac{lm}{l} + \frac{l(r - 1)}{m} \\ m(l + r - 1) \end{bmatrix} = \begin{bmatrix} 2lm - (l + 1)M \\ m - 1 \end{bmatrix} = \begin{bmatrix} k + \frac{n - \epsilon}{l} \\ m \end{bmatrix} = \begin{cases} k & \text{if } \epsilon M < l, \\ k + 1 & \text{otherwise.} \end{cases}$$

This completes the proof.

Our objective is to construct as many FHS sets attaining the bound (4) as possible.

### III. Algebraic Construction

In this section, we use a linear mapping from $(GF(p^m), +)$ to $(GF(p^u), +)$ to present an optimal $(p(p^m - 1), p^{u-1}, p^{m-u-1}; p^u)$-FHS set.

**Construction A** Let $p$ be a prime and let $u, m$ be two positive integers with $1 < u \leq m$. Let $\alpha, \beta$ be primitive elements of $GF(p^m)$ and $GF(p^u)$ respectively. Define a mapping $\sigma$ from $(GF(p^m), +)$ to $(GF(p^u), +)$ by $\sigma(a_0 + a_1 \alpha + \cdots + a_{m-1}\alpha^{m-1}) = a_0 + a_1 \beta + \cdots + a_{u-1}\beta^{u-1}$ for any $a_0, a_1, \ldots, a_{m-1} \in GF(p)$, and denote $R = \{a_0 + a_1 \alpha + \cdots + a_{m-1}\alpha^{m-1} : a_0, a_1, \ldots, a_{m-1} \in GF(p)\}$. Let $S = \{X^u : a \in R\}$ be a set of $p^u-1$ FHSs of length $p(p^m - 1)$ over $GF(p^u)$, where $X^u = \{X^u(t)\}_{t=1}^{p(p^m - 1)-1}$ is defined by $X^u(t) = \sigma(\alpha(t)\alpha^{m-1}) + (t)p + a$, and $\langle x \rangle_y$ denotes the least nonnegative residue of $x$ modulo $y$ for any positive integer $y$ and any integer $x$.

**Theorem 3.1:** The FHS set $S$ generated by Construction A is an optimal $(p(p^m - 1), p^{u-1}, p^{m-u-1}; p^u)$-FHS set.

**Proof:** By the definition of $\sigma$, it is clear that $\sigma$ is a linear mapping from $(GF(p^m), +)$ to $(GF(p^u), +)$ of rank $u$. For any $y \in GF(p^u)$, denote $N_y = \{x \in GF(p^m) : \sigma(x) = y\}$. By the linear algebra theorem the number of solutions of the equation $\sigma(x) = y$ is $p^{m-u}$. That is $|N_y| = p^{m-u}$ for any $y \in GF(p^u)$.

For $0 \leq \tau < p(p^m - 1)$ and $a, b \in R$, the Hamming correlation $H_{X^u, X^u}(\tau)$ is given by

$$H_{X^u, X^u}(\tau) = \sum_{t=0}^{p(p^m - 1)-1} h[\sigma(\alpha(t)\alpha^{m-1}) + (t)p + a, \sigma(\alpha(t+\tau)\alpha^{m-1}) + (t + \tau)p + b] = \sum_{t=0}^{p(p^m - 1)-1} h[a - b - (\tau)p, \sigma(\alpha(t)\alpha^{m-1}(\alpha^{m-1} - 1))].$$

Let $\tau_0 = (\tau)p^{m-1}$ and $\tau_1 = (\tau)p$. According to the values of $a, b$ and $\tau$, we compute $H_{X^u, X^u}(\tau)$ in four cases.

**Case 1:** $a = b$ and $\tau_1 = 0$. In this case $\tau_0 \neq 0$ and $\alpha^{m-1}(\alpha^{m-1} - 1)$ is given by

$$H_{X^u, X^u}(\tau) = \sum_{t=0}^{p(p^m - 1)-1} h[0, \sigma(\alpha(t)\alpha^{m-1})] = \sum_{x \in N_0} |\{t \equiv t_x \mod p^m - 1 : 0 \leq t < p(p^m - 1)\}| = p^{m-u} - 1.$$
Since \( k = \left\lfloor \frac{p}{q} \right\rfloor = \left\lfloor \frac{p^{m-1}}{p^n} \right\rfloor = p^{m-1-u} - 1 \), we have that
\[
\epsilon = n - kl = p(p^{m-1} - (p^{m-u+1} - 1)p^u = p^u - p, \quad \text{and} \\
\epsilon M - l = p^{u-1}(p^u - p) - p^u = (p^{u-1} - 2)p^u \geq 0.
\]
By Corollary 2.4, \( S \) is also optimal. This completes the proof. 

IV. COMBINATORIAL CONSTRUCTIONS

A. Combinatorial Characterization of FHS Sets

Following [16], we describe a connection between FHS sets and partition-type BNCDDPs in this subsection.

Throughout this paper, we always assume that \( I = \{0, 1, 2, \ldots, l-1\} \) and \( \mathbb{Z}_n \) is the residual class-ring of integers modulo \( n \).

An \((n, \lambda; l)\)-FHS, \( X = (x(0), x(1), \ldots, x(n-1)) \), over a frequency library \( F \), can be interpreted as a family of \( l \) sets \( B_0, B_1, \ldots, B_{l-1} \) such that each set \( B_i \) corresponds to frequency \( i \in F \) and the elements in each set \( B_i \) specify the position indices in the FHS \( X \) at which frequency \( i \) appears.

Associated with a non-empty subset \( B \subseteq \mathbb{Z}_n \), the difference list of \( B \) from combinatorial design theory is defined to be the multiset
\[
\Delta(B) = \{a - b : a, b \in B \land a \neq b\}.
\]
For any family \( B = \{B_0, B_1, \ldots, B_{l-1}\} \) of \( l \) non-empty subsets (called base blocks) of \( \mathbb{Z}_n \), define the difference list of \( B \) to be the union of multisets
\[
\Delta(B) = \bigcup_{i \in I} \Delta(B_i).
\]
If the difference list \( \Delta(B) \) contains each non-zero residue of \( \mathbb{Z}_n \) at most \( l \) times, then \( B \) is said to be an \((n, K, \lambda)\)-CDF (cyclic difference packing), where \( K = \{|B_i| : i \in I_i\} \). The number \( l \) of the base blocks in \( B \) is referred to as the size of the CDP. If the difference list \( \Delta(B) \) contains each non-zero residue of \( \mathbb{Z}_n \) exactly \( l \) times, \( B \) is said to be an \((n, K, \lambda)\)-CDF (cyclic difference family). When \( K = \{k\} \), we simply write \( k \) for \( \{k\} \).

An \((n, K, \lambda)\)-CDF with a collection of blocks \( B = \{B_0, B_1, \ldots, B_{l-1}\} \) is called a partition-type cyclic difference packing if every element of \( \mathbb{Z}_n \) is contained in exactly one base block of \( B \).

In 2004, Fuji-Hara et al. [14] revealed a connection between FHS and partition-type cyclic difference packings as follows.

**Theorem 4.1**: [14] There exists an \((n, \lambda; l)\)-FHS over a frequency library \( F \) if and only if there exists a partition-type \((n, K, \lambda)\)-CDF of size \( l \), \( B = \{B_0, B_1, \ldots, B_{l-1}\} \) over \( \mathbb{Z}_n \), where \( K = \{|B_i| : 0 \leq i \leq l-1\} \).

Let \( A, B \) be two non-empty subsets of \( \mathbb{Z}_n \). The list of external difference of ordered pair \((A, B)\) is the multiset
\[
\Delta_E(A, B) = \{y - x : (x, y) \in A \times B\}.
\]
Note that the list of external difference \( \Delta_E(A, B) \) may contain zero. For any residue \( d \in \mathbb{Z}_n \), the number of occurrences of \( d \) in \( \Delta_E(A, B) \) is clearly equal to \(|(A + d) \cap B|\).

Let \( B_j, 0 \leq j \leq M - 1 \), be a collection of \( l \) subsets of \( \mathbb{Z}_n \) where \( B_j = \{B_{j0}^l, B_{j1}^l, \ldots, B_{j(l-1)}^l\} \). The list of external difference of ordered pair \((B_j, B_{j'})\), \( 0 \leq j \neq j' < M \), is the union of multisets
\[
\Delta_E(B_j, B_{j'}) = \bigcup_{i \in I} \Delta_E(B_i^j, B_i^{j'}).
\]
The set \( \{B_0, \ldots, B_{M-1}\} \) of CDPs is said to be balanced nested with index \( \lambda \) and denoted by \((n, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCDF if each \( B_j \) is an \((n, K_j, \lambda)\)-CDF of size \( l \) and \( \Delta_E(B_j, B_{j'}) \) contains each residue of \( \mathbb{Z}_n \) at most \( \lambda \) times for any \( j \neq j' \). If each \( B_j \) is a partition-type CDP, then the \((n, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCDF is called partition-type. For convenient, the number \( l \) of the base blocks in \( B_j \) is also said to be the size of the BNCDF.

In 2009, Ge et al. [16] revealed a connection between FHS sets and partition-type BNCDDPs as follows.

**Theorem 4.2**: [16] There exists an \((n, M, \lambda; l)\)-FHS set over a frequency library \( F \) if and only if there exists a partition-type \((n, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCDF of size \( l \), \( \{B_j : 0 \leq j < M\} \) over \( \mathbb{Z}_n \), where \( B_j = \{B_{j0}^l, B_{j1}^l, \ldots, B_{j(l-1)}^l\} \) and \( K_j = \{|B_i^j| : 0 \leq i \leq l-1\} \) for \( 0 \leq j < M \).

B. Direct Constructions of Optimal FHS Sets

In this subsection, we give two direct constructions for FHS sets.

Let \( A \) be a subset of \( \mathbb{Z}_n \), we define \( \lambda \cdot [A] = \bigcup_{i = 0}^{\lambda - 1} A \), where \( \bigcup \) denotes the multiset union. Define \( U(\mathbb{Z}_n) \) the set of all units in \( \mathbb{Z}_n \).

**Theorem 4.3**: Let \( v \) be an odd integer and \( v_1 \) the least prime divisor of \( v \). For any integer \( t \) with \( 1 < t < p_1 \), there exists an optimal \( (tv, \left\lfloor \frac{p_1 - 1}{v_1} \right\rfloor, t; v) \)-FHS set.

**Proof**: Denote \( a = \left\lfloor \frac{p_1 - 1}{v_1} \right\rfloor \) and write \( v = p_1^{m_1}p_2^{m_2} \cdots p_s^{m_s} \) for \( s \) positive integers \( m_1, m_2, \ldots, m_s \) and \( s \) distinct primes \( p_1, p_2, \ldots, p_s \). For \( 0 \leq i \leq ta - 1 \), by the Chinese Remainder Theorem, there exists a unique element \( \theta_i \) such that
\[
\theta_i \equiv i + 1 \pmod{p_1^{m_1}} \quad \text{for} \quad 1 \leq j \leq s.
\]
Clearly, for \( 0 \leq x \neq y < ta \), \( \theta_x \) and \( \theta_y \) belong to \( U(\mathbb{Z}_n) \).

By Theorem 4.2, we need to construct a partition-type \((tv, \{K_0, \ldots, K_{n-1}\}, t)\)-BNCDF of size \( v \) over \( \mathbb{Z}_{tv} \).

For \( 0 \leq u < a \) and \( 0 \leq c < v \), set
\[
B_u^c = \{b + c\theta_{b+t} : 0 \leq b < t\}, \quad \text{and} \\
B_u = \{B_u^c : 0 \leq c < v\}.
\]

Firstly, we show that each \( B_u \) is a partition-type \((tv, t, t)\)-CDP.
Since \( \theta_{b+ut} \in U(\mathcal{Z}_v) \) for \( 0 \leq b < t \), we have that
\[
\bigcup_{0 \leq c < v} B^c_{v} = \bigcup_{0 \leq c < v} \bigcup_{0 \leq b < t} \{ b + ct \theta_{b+ut} \} = \bigcup_{0 \leq b < t} \{ b + ct : 0 \leq c < v \} = \mathbb{Z}_v.
\]

Thus, \( B_u \) is a partition of \( \mathbb{Z}_v \).

Since \( \theta_{j+ut} - \theta_{b+ut} \in U(\mathcal{Z}_v) \) for \( 0 \leq b < j < t \), we get
\[
\Delta(B_u) = \bigcup_{c=0}^{v-1} \Delta(B^c_{v} \setminus B^c_{v}) = \bigcup_{c=0}^{v-1} \{ j - b + ct(\theta_{j+ut} - \theta_{b+ut}) : 0 \leq b < j < t \} = \{ j - b + ct : 0 \leq b < j < t, 0 \leq c < v \} = t[\mathbb{Z}_v \setminus t\mathbb{Z}_v],
\]
where \( tz_{tv} = \{ 0, t, 2t, \ldots, (v-1)t \} \). Hence, \( B_u \) is a partition-type \( (tv, t) \)-CDF for \( 0 \leq u < v \).

Secondly, we show that \( \Delta_E(B_{a}, B'_{a}) \) contains each element of \( \mathbb{Z}_v \), at most \( t \) times for \( 0 \leq u \neq u' < a \).

Since \( \theta_{j+ut} - \theta_{b+ut} \in U(\mathcal{Z}_v) \) for \( 0 \leq b, j < t \), we get
\[
\Delta_E(B_{a}, B'_{a}) = \bigcup_{c=0}^{v-1} \Delta_E(B^c_{v} \setminus B^c_{v} \setminus B^c_{v}) = \bigcup_{c=0}^{v-1} \{ j - b + ct(\theta_{j+ut} - \theta_{b+ut}) : 0 \leq b, j < t \} = \{ j - b + ct : 0 \leq b, j < t, 0 \leq c < v \} = t[\mathbb{Z}_v \setminus t\mathbb{Z}_v].
\]

It follows that \( \{ B_{a} : 0 \leq u < a \} \) is a partition-type \( (tv, \{ K_0, \ldots, K_{a-1} \}, t) \)-BNCDF of size \( v \).

Finally, applying Theorem 4.2 we obtain a \( (tv, \{ \frac{3p+1}{t} \}, t) \)-FHS set. Since \( \epsilon = 0 \), by Corollary 4.4 this FHS set is also optimal. \( \blacksquare \)

**Theorem 4.4:** For any prime \( p \equiv 1 \pmod{4} \), there exists an optimal \( (3p, 2; 3p+1) \)-FHS set.

**Proof:** Let \( \alpha \) be a primitive element in \( \mathbb{Z}_p \) and let \( t = \frac{p-1}{4} \). Then
\[
\frac{\alpha^t - 1}{\alpha^t + 1} = \frac{\alpha^t + \alpha^{2t}}{\alpha^t + 1} = \alpha^{t}\tag{5}
\]
and
\[
\bigcup_{0 \leq i < t} \{ \alpha^i, -\alpha^i, \alpha^{i+t}, -\alpha^{i+t} \} = \mathbb{Z}_p \setminus \{ 0 \} \tag{6}
\]

Since \( \gcd(3, p) = 1 \), we have that \( \mathbb{Z}_{3p} \) is isomorphic to \( \mathbb{Z}_3 \times \mathbb{Z}_p \). Let
\[
A_0 = \{ 0, \alpha^i, (0, -\alpha^i), (1, \alpha^{i+t}), (1, -\alpha^{i+t}) \}, \quad A_1 = A_0 + (1, 0), \quad A_2 = A_0 + (2, 0), \quad B_0 = \{ 0, \alpha^{i+1} \}, \quad B_1 = \{ 0, -\alpha^{i+1} \}, \quad B_2 = \{ 1, \alpha^{i+t+1} \}, \quad B_3 = \{ 1, -\alpha^{i+t+1} \},
\]
where \( 0 \leq i < t \). Set
\[
B_0 = \{ A_1^j : 0 \leq i < t, 0 \leq j < 3 \} \cup \{ \mathbb{Z}_3 \times \{ 0 \} \}, \quad B_1 = \{ A_1^j : 0 \leq i < t, 0 \leq j < 3 \} \cup \{ \mathbb{Z}_3 \times \{ 0 \} \}.
\]

In view of equality (5), each \( B_i \) \( (0 \leq i < 2) \) is a partition of \( \mathbb{Z}_3 \times \mathbb{Z}_p \). Next we show that \( \{ B_0, B_1 \} \) is a \( (3p, \{ 3, 4 \}, 3, 4) \)-BNCDF.

Firstly, we show that each \( B_i \) is a \( (3p, \{ 3, 4 \}, 3) \)-CDF of size \( \frac{3p+1}{4} \).

It is straightforward that
\[
\Delta(B_0) = \bigcup_{z=0}^{2} \{ z \} \times \Delta_z, \quad \Delta_0 = 3 \bigcup_{i=0}^{t-1} \{ \pm 2\alpha^i, \pm 2\alpha^{i+t} \},
\]
\[
\Delta_1 = 3 \bigcup_{i=0}^{t-1} \{ \pm \alpha^i(\alpha^t - 1), \pm \alpha^i(\alpha^t + 1) \} \cup \{ 0 \}, \quad \Delta_2 = -\Delta_1.
\]

In view of equality (5) and equality (6), we have
\[
\Delta(B_0) = 3[\mathbb{Z}_3 \times \mathbb{Z}_p \setminus \{ (0, 0) \}] + (0, 0)
\]
Similarly, we have \( \Delta(B_1) = 3[\mathbb{Z}_3 \times \mathbb{Z}_p \setminus \{ (0, 0) \}] \). Thus, each \( B_i \) is a \( (3p, \{ 3, 4 \}, 3) \)-CDF.

Secondly, we show that \( \Delta_E(B_0, B_1) \) contains each element of \( \mathbb{Z}_3 \times \mathbb{Z}_p \) at most four times.

It is straightforward that
\[
\Delta_E(B_0, B_1) = \bigcup_{0 \leq i < t} \Delta_E(A_i^j, B_j^i) \bigcup \Delta_E(\mathbb{Z}_3 \times \{ 0 \}, \mathbb{Z}_3 \times \{ 0 \}) = \bigcup_{z=0}^{2} \{ z \} \times \Delta_z, \quad \Delta_0 = \bigcup_{0 \leq i < t} \{ \pm \alpha^i(1-\alpha), \pm \alpha^i(1+\alpha), \pm \alpha^{i+t}(1-\alpha), \pm \alpha^{i+t}(1+\alpha) \} \cup \{ 0 \}.
\]
\[
\Delta_1 = \pm \alpha^{i+t}(\alpha-1), \pm (\alpha^t-\alpha)\alpha^t, \pm (\alpha^t+\alpha)\alpha^t, \pm (1-\alpha^{t+1})\alpha^t, \pm (1+\alpha^{t+1})\alpha^t \cup \{ 0, 0, 0 \}, \quad \Delta_2 = -\Delta_1.
\]

In view of equality (6), we have that
\[
\bigcup_{0 \leq i < t} \{ \pm \alpha^i(1-\alpha), \pm \alpha^{i+t}(1-\alpha) \} = \mathbb{Z}_p \setminus \{ 0 \} \quad \text{and} \quad \bigcup_{0 \leq i < t} \{ \pm \alpha^i(1+\alpha), \pm \alpha^{i+t}(\alpha+1) \} = \mathbb{Z}_p \setminus \{ 0 \}.
\]

Since \( \frac{\alpha^{t}-\alpha}{1+\alpha^{t}} = \frac{\alpha^{t}+\alpha^{2t}}{1+\alpha^{t}} = \alpha^t \) and \( \frac{\alpha^{t}+\alpha}{1+\alpha^{t}} = \frac{\alpha^{t}-\alpha^{2t+1}}{1+\alpha^{t}} = \alpha^t \), we get
\[
\bigcup_{0 \leq i < t} \{ \pm (\alpha^t-\alpha)\alpha^t, \pm (1+\alpha^{t+1})\alpha^t \} = \mathbb{Z}_p \setminus \{ 0 \}, \quad \bigcup_{0 \leq i < t} \{ \pm (\alpha^t+\alpha)\alpha^t, \pm (1-\alpha^{t+1})\alpha^t \} = \mathbb{Z}_p \setminus \{ 0 \}.
\]

Thus, \( \Delta_E(B_0, B_1) = \bigcup_{0 \leq i < t} \{ \pm (\alpha^t-\alpha)\alpha^t, \pm (1+\alpha^{t+1})\alpha^t \} \cup \mathbb{Z}_3 \times (\mathbb{Z}_p \setminus \{ 0 \}) \cup 3[\{ (0, 0), (1, 0), (2, 0) \}] \). It follows that \( \{ B_0, B_1 \} \) is our required BNCDF. By Theorem 4.2 there exists a \( (3p, 2; 3p+1) \)-FHS set.
Finally, we show that such an FHS set is optimal. Since \( k = \lceil \frac{q}{3} \rceil = \lceil \frac{3p - 3}{3} \rceil = 3 \), we get \( \epsilon = 3p - 3 \times \frac{3p-1}{3} = \frac{3p-3}{3} \) and \( \epsilon M - l = \frac{3p-3}{3} \times \frac{3p-1}{3} = \frac{3p-7}{3} \geq 0 \). By Corollary 2.4, this FHS set is optimal. This completes the proof. ■

C. Recursive constructions of optimal FHS sets

In this subsection, recursive constructions are used to construct optimal FHS sets. These recursive constructions are based on cyclic difference matrices (CDMs).

A \((w, t, 1)\)-CDM is a \( w \times t \) matrix \( D = (d_{ij}) \) \((0 \leq i < t-1, 0 \leq j < w-1)\) with entries from \( \mathbb{Z}_w \) such that, for any two distinct rows \( R_i \) and \( R_j \), the vector difference \( R_i - R_j \) contains every residue of \( \mathbb{Z}_w \) exactly once. It is easy to see that the property of a difference matrix is preserved even if we add any element of \( \mathbb{Z}_w \) to all entries in any row or column of the difference matrix. Then, without loss of generality, we can assume that all entries in the first row are zero. Such a difference matrix is said to be normalized. The \((w, t-1, 1)\)-CDM obtained from a normalized \((w, t, 1)\)-CDM by deleting the first row is said to be homogeneous. The existence of a homogeneous \((w, t-1, 1)\)-CDM is equivalent to that of a \((w, t-1, 1)\)-CDM. Observe that cyclic difference matrices have been extensively studied. A large number of known \((w, t, 1)\)-CDMs are well documented in [8]. In particular, the multiplication table of the prime field \( \mathbb{Z}_p \) is a \((p, p, 1)\)-CDM. By using the usual product construction of CDMs, we have the following existence result.

Lemma 4.5: [8] Let \( w \) and \( t \) be integers with \( w \geq t \geq 3 \). If \( w \) is odd and the least prime factor of \( w \) is not less than \( t \), then there exists a \((w, t-1, 1)\)-CDM.

In 2009, Ge et al. [16] used cyclic difference matrices to establish a recursive construction for partition-type BNCRDPs so as to give a recursive construction of FHS sets. We generalize this construction via balanced nested cyclic relative difference packings.

An \((mg, g, K, \lambda)\)-cyclic relative difference packing (briefly CRDP) is an \((mg, K, \lambda)\)-CDP \( B \) over \( \mathbb{Z}_{mg} \) such that \( \Delta(B) \) contains each element of \( \mathbb{Z}_{mg} \setminus mg \mathbb{Z}_{mg} \) at most \( \lambda \) times and no element of \( mg \mathbb{Z}_{mg} \) occurs, where \( \mathbb{Z}_{mg} = \{0, \ldots, mg - m\} \).

Let \( B_j = \{B_j^0, B_j^1, \ldots, B_{j-u_{-1}}\} \) be an \((mg, g, K_j, \lambda)\)-CRDP over \( \mathbb{Z}_{mg} \) for \( 0 \leq j < M - 1 \). The set \( \{B_0, \ldots, B_{M-1}\} \) is referred to as an \((mg, g, \{K_0, K_1, \ldots, K_{M-1}\}, \lambda)\)-BNCRDP (balanced nested cyclic relative difference packing) over \( \mathbb{Z}_{mg} \) if \( \Delta_B(B_j, B_j') \) contains each element of \( \mathbb{Z}_{mg} \setminus mg \mathbb{Z}_{mg} \) at most \( \lambda \) times and no element of \( mg \mathbb{Z}_{mg} \) occurs for any \( j \neq j' \). For convenience, the size \( u \) of \( B_j \) is also said to be the size of the BNCRDP.

One importance of BNCRDP is that we can put an appropriate BNCDP on its subgroup to derive a new BNCDP.

Lemma 4.6: Suppose there exists an \((mg, g, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCRDP of size \( u \) such that each \((mg, g, K_j, \lambda)\)-CRDP is a partition of \( \mathbb{Z}_{mg} \setminus mg \mathbb{Z}_{mg} \) for \( 0 \leq j < M \). If there exists a partition-type \((g, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCDP of size \( r \) over \( \mathbb{Z}_g \), then there exists a partition-type \((mg, \{K_0 \cup K_0', \ldots, K_{M-1} \cup K_{M-1}', \lambda\})\)-BNCDP of size \( u + r \) over \( \mathbb{Z}_{mg} \).

Proof: Let \( \{B_0, \ldots, B_{M-1}\} \) be a given \((mg, g, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCRDP over \( \mathbb{Z}_{mg} \), where \( B_j = \{B_j^i : 0 \leq i < u\} \) for \( 0 \leq j < M \). Let \( \{A_0, \ldots, A_{M-1}\} \) be a partition-type \((g, \{K_0', \ldots, K_{M-1}'\}, \lambda)\)-BNCDP over \( \mathbb{Z}_g \), where \( A_j = \{A_j^i : 0 \leq i < r\} \) for \( 0 \leq j < M \). For \( 0 \leq j < M \), set \( P_j = \{mA_j^i : 0 \leq i < r\} \) and \( T_j = B_j \cup P_j \). Since \( A_j \) is a partition of \( \mathbb{Z}_g \), we have that \( P_j \) is a partition of \( m \mathbb{Z}_mg \), consequently, \( T_j \) is a partition of \( \mathbb{Z}_{mg} \). It remains to prove that \( \{T_j : 0 \leq j < M\} \) is an \((mg, \{K_0 \cup K_0', \ldots, K_{M-1} \cup K_{M-1}'\}, \lambda)\)-BNCDP over \( \mathbb{Z}_{mg} \).

On one hand, since \( B_j : 0 \leq j < M \) is an \((mg, g, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCRDP over \( \mathbb{Z}_{mg} \), we have that \( \Delta(B_j) \) contains each residue of \( \mathbb{Z}_{mg} \setminus mg \mathbb{Z}_{mg} \) at most \( \lambda \) times and no element of \( mg \mathbb{Z}_{mg} \) occurs. Since \( \{A_j : 0 \leq j < M\} \) is an \((mg, g, \{K_0', \ldots, K_{M-1}'\}, \lambda)\)-BNCDP over \( \mathbb{Z}_g \), we have that \( \Delta(T_j) \) contains each non-zero element of \( \mathbb{Z}_{mg} \) at most \( \lambda \) times. Thus, \( \Delta(T_j) \) contains each non-zero element of \( \mathbb{Z}_{mg} \) at most \( \lambda \) times, \( \{T_j : 0 \leq j < M\} \) is an \((mg, \{K_0 \cup K_0', \ldots, K_{M-1} \cup K_{M-1}'\}, \lambda)\)-BNCDP over \( \mathbb{Z}_{mg} \).

This completes the proof. ■

Theorem 4.7: Assume that \( \{B_0, \ldots, B_{M-1}\} \) is an \((mg, g, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCRDP of size \( u \) such that each \( B_j \) is a partition of \( \mathbb{Z}_{mg} \setminus mg \mathbb{Z}_{mg} \), where \( B_j = \{B_j^i : 0 \leq i < u\} \) for \( 0 \leq j < M \). If there exists a homogeneous \((w, t, 1)\)-CDM over \( \mathbb{Z}_w \) with \( t = \max \{ \sum_{0 \leq i < u} |B_j^i| : 0 \leq j < u\} \), then there exists an \((mgw, gw, \{K_0, \ldots, K_{M-1}\}, \lambda)\)-BNCRDP of size \( uw \), \( \{B_0, \ldots, B_{M-1}\} \), such that each \( B_j \) is a partition of \( \mathbb{Z}_{mgw} \setminus mgw \mathbb{Z}_{mgw} \) at \( 0 \leq j < M \).

Proof: Let \( \Gamma = (\gamma_i, j) \) be a given homogeneous \((w, t, 1)\)-CDM over \( \mathbb{Z}_w \). For each collection of the following \( M \) blocks

\[ B^0_i = \{a_{i,0}, \ldots, a_{i,0,k_0}\}, \]
\[ B^1_i = \{a_{i,1,k_0+1}, \ldots, a_{i,1,k_1}\}, \]
\[ \vdots \]
\[ B^{M-1}_i = \{a_{i,M-1,k_{m-2}+1}, \ldots, a_{i,M-1,k_{m-1}}\}, \]

where \( 0 \leq i < u \), we construct the following \( uw \) new blocks:

\[ B^j_{i,s} = \{a_{i,j,k_{j-1}+1} + mg\gamma_{k_{j-1}+1,s}, \ldots, a_{i,j,k_j} + mg\gamma_{k_j,s}\}, \]

where \( 0 \leq j < M, 0 \leq s < w \).

Set

\[ B^j = \{B^j_{i,s} : 0 \leq i < u, 0 \leq s < w\}, \]
\[ B^j' = \{B^j_{i,s} : 0 \leq j < M\} \].
It is left to show that $B'$ is the required BNCRDP.

Since $B_j$ is a partition of $Z_{mg} \setminus mZ_{mg}$ and each row of $\Gamma$ is a permutation of $Z_w$, we obtain that $B_j$ is a partition of $Z_{mng} \setminus mZ_{mng}$ and the size of $B_j$ is $uw$ for any $0 \leq j < M$.

Since $B_j$ is an $(m,g,K_j,\lambda)$-CRDP of size $u$, the difference list $\Delta(B_j)$ contains each element of $Z_{mng} \setminus mZ_{mng}$ at most $\lambda$ times and no element of $mZ_{mng}$ occurs. Simple computation shows that

$$\Delta(B_j') = \bigcup_{0 \leq c < u, 0 \leq s < c} \Delta(B_j(s,s))$$

$$= \bigcup_{0 \leq s < u} \{a - b + cmg : a, b \in B_j^s, 0 \leq c < w\}$$

$$= \bigcup_{\tau \in \Delta(B_j)} (mg\mathbb{Z}_{mng} + \tau),$$

consequently, the difference list $\Delta(B_j')$ contains each element of $Z_{mng} \setminus mZ_{mng}$ at most $\lambda$ times and no element of $mZ_{mng}$ occurs. So, each $B_j'$ is an $(mg, gw, K_j, \lambda)$-CRDP of size $uw$.

Since $\Delta(E(B_j, B_j'))$ contains each residue of $Z_{mg} \setminus mZ_{mg}$ at most $\lambda$ times and no element of $mZ_{mng}$ occurs for $0 \leq j \neq j' < M$, we get

$$\Delta(E(B_j, B_j')) = \bigcup_{0 \leq c < u, 0 \leq c < w} \Delta(E(B_j(s,s), B_j'(s,s)))$$

$$= \bigcup_{0 \leq s < u} \{b - a + cmg : (a, b) \in B_j^s \times B_j'^s, 0 \leq c < w\}$$

$$= \bigcup_{\tau \in \Delta(E(B_j, B_j'))} (mg\mathbb{Z}_{mng} + \tau),$$

consequently, the difference list $\Delta(E(B_j', B_j'))$ contains each residue of $Z_{mg} \setminus mZ_{mg}$ at most $\lambda$ times and no element of $mZ_{mng}$. This completes the proof.

Combining Theorem 4.7 with Theorem 4.4 establishes the following corollary.

**Corollary 4.8:** There exists an optimal $(n, 2, 4; \frac{n+1}{d})$-FHS set for all $n = 3p_1p_2 \ldots p_u$ with $n \not\equiv 0 \pmod{25}$ and each $p_j \equiv 1 \pmod{4}$ being a prime.

**Proof:** We first prove that there exists a partition-type $(n, \{3, 4\}, \{3, 4\}, 4)$-BNCRD of size $\frac{n+1}{d}$ over $\mathbb{Z}_n$ by induction on $n$. Without loss of generality, let $p_1 < p_2 \leq \ldots \leq p_u$.

For $u = 1$, the assertion holds by Theorem 4.4. Assume that the assertion holds for $u = r$ and consider $u = r + 1$. Deleting the block $\{(0, 0), (1, 0), (2, 0)\}$ from $B_r$ in the proof of Theorem 4.4 where $0 \leq t < 2$, we obtain a $(3p_1, 3, \{4\}, \{4\}, 4)$-BNCRD of size $\frac{3p_1 - 3}{d}$ such that each $B_r'$ is a partition of $Z_{3p_1} \setminus p_1Z_{3p_1}$. Since $3p_1 \equiv 3 \pmod{25}$ and each $p_j \equiv 1 \pmod{4}$ is a prime, we have $p_j \geq 13$ for $2 \leq j \leq r + 1$. By Lemma 4.3 there exists a homogeneous $(p_2 \ldots p_{r+1}, 8, 1)$-CDM. Since $8 \equiv |B_1^1| + |B_1^2|$ where $B_1^1 \subset B_1'$ and $B_1^2 \subset B_1'$ for $0 \leq i < \frac{3p_1 - 3}{d}$, applying Theorem 4.7 yields a $(3p_1 \ldots p_{r+1}, 3p_2 \ldots p_{r+1}, \{4\}, \{4\}, 4)$-BNCRD of size $\frac{3p_1 \ldots p_{r+1} - 3p_2 \ldots p_{r+1}}{d}$ over $Z_{3p_1 \ldots p_{r+1}}$ such that each CRDP is a partition of $Z_{3p_1 \ldots p_{r+1}} \cup p_1Z_{3p_1 \ldots p_{r+1}}$. By induction hypothesis there exists a partition-type $(3p_2 \ldots p_{r+1}, \{3, 4\}, \{3, 4\}, 4)$-BNCRD over $Z_{3p_2 \ldots p_{r+1}}$ of size $\frac{3p_2 \ldots p_{r+1}}{d}$ such that each CRDP is a partition of $Z_{3p_2 \ldots p_{r+1}} \cup p_2Z_{3p_2 \ldots p_{r+1}} - p_1Z_{3p_2 \ldots p_{r+1}}$. So, the conclusion holds by induction.

By Theorem 4.2 there exists an $(n, 2, 4; \frac{n+1}{d})$-FHS set. It remains to show that such an FHS set is optimal.

Since $k = \left\lceil \frac{n}{d} \right\rceil = \left\lceil \frac{n}{d} \right\rceil = 3$, we get $\epsilon = n - 3 \times \frac{n+1}{d} = \frac{n-3}{d}$ and $\epsilon M - l = 2 \times \frac{n-3}{d} - \frac{n+1}{d} = \frac{n-7}{d} > 0$. By Corollary 4.3, this FHS set is optimal.

It is worth pointing out that the construction of FHS sets in [16, Theorem 3.10] is just a special case of Theorem 4.7. The construction of FHS sets in [16, Theorem 3.10] require that one frequency of an $(n, M, \lambda; l)$-FHS set appears in a fixed position and other frequencies appear in different positions. Such a FHS set is in fact equivalent to an $(n, 1, \{K_0, \ldots, K_M-1\}, \lambda)$-BNCRDP of size $l - 1$. Applying Theorem 4.7 with a homogeneous $(w, t, 1)$-CDM yields a $(nw, w, \{K_0, \ldots, K_M-1\}, \lambda)$-BNCRDP of size $(l - 1)w$. Further, applying Lemma 4.6 with a partition-type $(w, \{K_0, \ldots, K_M-1\}, \lambda)$-BNCRDP of size $r$ yields a partition-type $(nw, \{K_0 \cup K_1, \ldots, \{K_M-1 \cup K_M\}, \lambda)$-BNCRDP of size $(l - 1)w + r$, which corresponds to an $(nw, M, \lambda; (l - 1)w + r)$-FHS set.

**Theorem 4.9:** [16] Assume that $S$ is an $(n, M, \lambda; l)$-FHS set in which one frequency appears in a fixed position, say the 0th position, and each of the other frequencies appears in different non-0th positions of the $M$ FHSs of $S$. Assume also that $T$ is a $(w, M, \lambda; r)$-FHS set. If there exists a homogeneous $(w, t, 1)$-CDM over $Z_w$, where $t$ is the maximum number of total occurrences that frequencies appear in all the $M$ FHSs of $S$, then there also exists an $(nw, M, \lambda; (l - 1)w + r)$-FHS set.

When we replace the BNCRDP in Theorem 4.7 with a partition-type BNCRD, the same procedure yields a new partition-type BNCRD, which is stated in terms of FHS set below. Since the proof is similar to that of Theorem 4.7 we omit it here.

**Theorem 4.10:** Assume that $S$ is an $(n, M, \lambda; l)$-FHS set. If there exists a homogeneous difference matrix $(w, t, 1)$-DM over $Z_w$, where $t$ is the maximum number of total occurrences that frequencies appear in all the $M$ FHSs of $S$, then there also exists an $(nw, M, \lambda; lw)$-FHS set.

Applying Theorem 4.10 and Lemma 4.3 gives the following corollary.

**Corollary 4.11:** Assume that $S$ is an $(n, M, \lambda; l)$-FHS set. Let $w$ be an odd integer and let $q_1$ be the least prime divisor of $w$. If $t < q_1$, where $t$ is the maximum number of total occurrences that frequencies appear in all the $M$ FHSs of $S$, then there exists an $(nw, M, \lambda; lw)$-FHS set.

Remark: Compared with the Construction A in [4], the construction for FHS sets from Corollary 4.11 does not require the constraint gcd$(w, n) = 1$. As noted in [4], the resultant $(nw, M, \lambda; lw)$-FHS set is optimal if the $(n, M, \lambda; l)$-FHS set is optimal.

**Lemma 4.12:** [24] Let $m, u$ be positive integers with $u < m$, $q$ a prime power and let $d$ be a positive integer such that $d|q - 1$ and gcd$(d, m) = 1$. Then there exists an optimal $(\frac{q^m - 1}{d}, d, \frac{q^m - 1}{d}; g^u)$-FHS set.

From the construction in [24], the maximum number of total occurrences that frequencies appear in all FHSs of the
Let $v > 1$ be an odd integer. An element $g \in U(Z_v)$ is called a primitive root modulo $v$ if its multiplicative order modulo $v$ is $\varphi(v)$, where $\varphi(v)$ denotes the Euler function which counts the number of positive integers less than and coprime to $v$. It is well known that for an odd prime $p$, there exists an element $g$ such that $g$ is a primitive root modulo $p^t$ for all $t \geq 1$ [1].

Let $v$ be an odd integer of the form $v = p_1^{m_1}p_2^{m_2} \cdots p_s^{m_s}$ for $s$ positive integers $m_1, m_2, \ldots, m_s$ and distinct primes $p_1, p_2, \ldots, p_s$. Let $e > 1$ be a common factor of $p_1-1, p_2-1, \ldots, p_s-1$. Define $f = \min\{\frac{v-1}{e} : 1 \leq i \leq s\}$. For each $i$ with $1 \leq i \leq s$, let $g_i$ be a primitive root modulo $p_i^{m_i}$ for all $t \geq 1$. By the Chinese Remainder Theorem, there exist unique elements $g, a \in U(Z_v)$ such that

$$g \equiv g_i^{f_i p_i^{m_i-1}} \pmod{p_i^{m_i}}$$

for $1 \leq i \leq s$, and

$$a \equiv g_i \pmod{p_i^{m_i}}$$

for $1 \leq i \leq s$,

then the multiplicative order of $g$ modulo $v$ is $e$, the list of differences arising from $G = \{1, g, g^2, \ldots, g^{f-1}\}$ is a subset of $U(Z_v)$ and $a g^e - g^e \in U(Z_v)$ for $1 \leq t < f$ and $0 \leq e, c' < e$.

For $x, y \in Z_v \setminus \{0\}$, the binary relation $\sim$ defined by $x \sim y$ if and only if there exists a $g' \in G$ such that $x g' = y$ is an equivalence relation over $Z_v \setminus \{0\}$. Then its equivalence classes are the subsets $xG, x \in Z_v \setminus \{0\}$, of $Z_v$. Denote by $R$ a system of distinct representatives for the equivalence classes modulo $G$ of $Z_v \setminus \{0\}$. For $0 \leq t < f$, let $r \in R$, set

$$B_r^t = \{ra^t g^j : 0 \leq j < e\}$$

and define

$$B_t = \bigcup_{r \in R} B_r^t = \{ra^t g^j : r \in R, 0 \leq j < e\} = Z_v \setminus \{0\}.$$

Thus, $B_t$ is a $(v, 1, e, e-1)$-CRDP for $0 \leq t < f$.

For $0 \leq t \neq t' < f$, since $a^{t-t'}g^{t-t'} - 1 \in U(Z_v)$ and $\{ra^t g^j : r \in R, 0 \leq j < e\} = Z_v \setminus \{0\}$, we get

$$\Delta(B_t, B_{t'}) = \bigcup_{r \in R} \Delta((ra^t g^j : 0 \leq j < e)) = \bigcup_{r \in R} \{ra^t(g^{j'} - g^j) : 0 \leq j' \neq j < e\} = \bigcup_{r \in R} \{ra^t g^j(g^{e-1} - 1) : 0 \leq j < e, 1 \leq e < e\} = (e-1)[Z_v \setminus \{0\}].$$

Therefore, by

$$\Delta_e(B_t, B_{t'}) = \bigcup_{r \in R} \Delta_e(B_r^t, B_r^{t'}) = \bigcup_{r \in R} \Delta_e(B_r^t, B_r^{t'}) = \bigcup_{r \in R} \{ra^t g^{j'} - ra^t g^j : 0 \leq j', j < e\} = \bigcup_{r \in R} \{ra^t g^j(a^{j'-j}g^{e-1} - 1) : 0 \leq j < e\} = \{e[Z_v \setminus \{0\}]\}.$$

It follows that $\{B_t : 0 \leq t < f\}$ is a $(v, 1, \{K_0, K_1, \ldots, K_{f-1}\}, e)$-BNCRDP with each $B_t$ being a partition of $Z_v \setminus \{0\}$, where $K_0 = K_1 = \cdots = K_{f-1} = \{e\}$.

The discussion above establishes the following lemma.

**Lemma 4.13:** Let $v$ be an odd integer of the form $p_1^{m_1}p_2^{m_2} \cdots p_s^{m_s}$ for $s$ positive integers $m_1, m_2, \ldots, m_s$ and distinct primes $p_1, p_2, \ldots, p_s$. Let $e > 1$ be a common factor of $p_1-1, p_2-1, \ldots, p_s-1$ and let $f = \min\{\frac{v-1}{e} : 1 \leq i \leq s\}$. Then there exists a $(v, 1, \{K_0, K_1, \ldots, K_{f-1}\}, e)$-BNCRDP of size $\frac{v-1}{e}$ such that each CRDP is a partition of $Z_v \setminus \{0\}$, where $K_0 = K_1 = \cdots = K_{f-1} = \{e\}$.

Adding the block $\{0\}$ to $B_t$ for each $0 \leq t < f$, the new collection is a partition-type $(v, \{K'_0, \ldots, K'_{f-1}\}, e)$-BNCRDP of size $\frac{v-1}{e} + 1$ where $K'_0 = \cdots = K'_{f-1} = \{1, e\}$, which corresponds to a $(v, f, e, \frac{v-1}{e} + 1)$-FHS set. Such an FHS set can also be obtained from Construction A in [23] by using generalized cyclotomy. In comparison, our method is quite neat and more clear to understand.

**Corollary 4.15:** [23] Under the hypotheses of Lemma 4.13, there exists a partition-type $(v, \{K'_0, \ldots, K'_{f-1}\}, e)$-BNCRDP of size $\frac{v-1}{e} + 1$ where $K'_0 = \cdots = K'_{f-1} = \{1, e\}$.

**Theorem 4.16:** Let $w$ be an odd integer of the form $q_1^{n_1}q_2^{n_2} \cdots q_t^{n_t}$ for $t$ positive integers $n_1, n_2, \ldots, n_t$ and $t$ primes $q_1, q_2, \ldots, q_t$ such that $q_1 < \cdots < q_t$, and let $e'$ be a positive integer such that $e'|q_1 - 1$ for $1 \leq i \leq t$. Let parameters $v, p_1, e$ and $f$ be the same as those in the hypotheses of Lemma 4.14.

If $2 \leq e' \leq e$, $q_1 \geq p_1 > 2e$ and $v \geq e' 3$, then there exists an optimal $(vw, \frac{v}{w} - 1, e, \frac{v}{w} - 1)$-FHS set. 

**Proof:** By Lemma 4.13 there exists a $(v, 1, \{K_0, \ldots, K_{f-1}\}, e)$-BNCRDP of size $\frac{v}{w} - 1$, \[ B_{j'} : 0 \leq j' < \frac{v}{w} - 1 \] such that each $B_{j'}$ is a partition of $Z_v \setminus \{0\}$, where $K = K_0 = \cdots = K_{f-1} = \{e\}$. Since $p_1 < q_1$, by Lemma 4.5 there exists a homogeneous $(w, p_1 - 1, 1)$-CDM over $Z_{v_w}$. Since $p_1 - 1 = \sum_{j=0}^{ \frac{v}{w} - 1 - 1} |B_j^t|$ for $0 \leq i < \frac{v}{w} - 1$, applying Theorem 4.7 yields a $(wv, w, \{K_0', \ldots, K_{f'-1}\}, e')$-BNCRDP of size $\frac{v}{w} - 1$ such that each CRDP is a partition of $Z_{v_{w'}} \setminus \{0\}$. By Corollary 4.13 there exists a partition-type $(w, \{K_0', \ldots, K_{f'-1}\}, e')$-BNCRDP of size $\frac{v}{w} - 1 + 1$, where $K'_0 = \cdots = K'_{f'-1} = \{1, e'\}$. Since $\frac{v}{w} - 1 \cdot e' > p_1 - 1 \cdot e$, applying Lemma 4.6 we obtain a partition-type $(wv, \{K_0, \ldots, K_{f-1}\}, e')$-BNCRDP of size $\frac{v}{w} - 1 + 1$, where $K'_0 = \cdots = K'_{f'-1} = \{1, e, e'\}$. Therefore, by
Theorem 4.17 there is a \((vw, \frac{p-1}{p'}, e; \frac{w}{e} + \frac{w-1}{e} + 1)\)-FHS set. It remains to prove that such an FHS set is optimal.

Since \(v \geq e^2\), simple computation shows that \(e - 1 \leq \frac{w - l}{e} < e\). Consequently,

\[
k = \left\lceil \frac{vw}{e} + \frac{w-1}{e} + 1 \right\rceil = e - 1, \quad \text{and}
\]

\[
e = n - kl = vw - (e - 1)\left(\frac{w}{e} + \frac{w-1}{e} + 1\right)
\]

\[
= \frac{w}{e} - (e - 1)\left(\frac{w}{e} + \frac{w-1}{e} + 1\right) + w - e + 1.
\]

Since \(w \geq p_1 \geq 2e, v \geq e^2\) and \(e \geq e' \geq 2, we get

\[
\epsilon M - l \geq 2e - l
\]

\[
= \frac{w}{e} - 2e\left(\frac{w}{e} + \frac{w-1}{e} + 1\right) + 2(w - 2e + 1)
\]

\[
\geq \frac{w}{e}(w - 1) + (2w - 2e + 1)
\]

\[
\geq \epsilon M - l = 2e - l > 0.
\]

By Corollary 4.4, this FHS set is optimal. This completes the proof.

Remark: Compared with the construction A in [23], the construction for FHS set from Theorem 4.16 does not require the constraint \(e \geq \text{gcd}(p_1 - 1, p_2 - 1, \ldots, p_{M-1}, q_1 - 1, \ldots, q_{M-1})\). From Theorem 4.16 we can obtain many FHS sets with new and flexible parameters.

Similar to the construction of FHS sets in Theorem 4.16, we can obtain more FHS sets by using known FHS sets, Theorem 4.17 and Theorem 4.4. Here, we give another example.

Lemma 4.17: Assume that there exists an \((n, M, \lambda; t)\)-FHS set. Then, for any integer \(t\) with \(1 \leq t \leq M\), there exists a \((\lfloor \frac{n}{M}, \frac{1}{M}, t; \lambda; t)\)-FHS set.

Theorem 4.18: Let \(p, p'\) be primes and let \(m, a, b\) be positive integers such that \(p^m - 1 = ab\) and \(p^{b+1} \leq a\). Let parameters \(v, p_1, e, f\) and \(w, q_1, e'\) be the same as those in the hypotheses of Theorem 4.16. If \(p^m - 1 < p_1 \leq q_1\) and \(e \leq b\), then there exists an optimal \((p'vw(p^m - 1), \lfloor \frac{p'}{p}\rfloor, p'b; avw + \frac{w}{e} + \frac{w-1}{e} + 1)\)-FHS set.

Proof: Let \(M = \lfloor \frac{p}{p'} \rfloor\). Since \(\text{gcd}(p', p^m - 1) = 1\), we have that \(Z_{p'}(p^m - 1)\) is isomorphic to \(Z_{p'} \times Z_{p^m - 1}\). From the construction of \((p'(p^m - 1), \lfloor \frac{p}{p'} \rfloor, p'b; a; 1)\)-FHS set in [19], there exists a base block \(\{i, c\} : 0 \leq i < p'\) for some \(c\) in the corresponding partition-type BNCDF over \(Z_{p'} \times Z_{p^m - 1}\). We translate blocks to obtain a \((p'(p^m - 1), \lfloor \frac{p}{p'} \rfloor, \{K_0, \ldots, K_{M-1}\}, p'b)\)-BNCDF of size \(a\) with each CRDP being a part of \(Z_{p'}(p^m - 1) \setminus \{p^m - 1\}\), where \(K_0 = \ldots = K_{M-1} = \{p'b, p'(b - 1)\}\).

Since \(p^m - 1 < p_1 \leq q_1\), there exists a homogeneous \((vw, p^m - 1, 1)\)-CDM over \(Z_{vw}\) by Lemma 4.5. Since the block size is at most \(p'b\), the sum of the cardinalities of \(M\) blocks is at most \(Mpb\), which is not greater than \(p^m - 1\). Applying Theorem 4.17, yields a \((p'vw(p^m - 1), p'vw, \{K_0, \ldots, K_{M-1}\}, p'b)\)-BNCDF of size \(a\) such that each CRDP is a partition of \(Z_{p'}vw(p^m - 1) \setminus \{p^m - 1\}\) over \(Z_{vw}\). Since there exists a \((vw, \frac{p-1}{p'}, e; \frac{w}{e} + \frac{w-1}{e} + 1)\)-FHS set by Theorem 4.16 applying Lemma 4.17 yields a \((p'vw, \lfloor \frac{p-1}{p'} \rfloor, p'b; \frac{w}{e} + \frac{w-1}{e} + 1)\)-FHS set. By Theorem 4.12 there is a partition-type \((p'vw, \{K_0, \ldots, K_{M-1}\}, p'b)\)-BCNDF of size \(\frac{w}{e} + \frac{w-1}{e} + 1\), where \(M' = \lfloor \frac{p-1}{p'} \rfloor\). Since \(2 \leq l \leq b\) and \(p_1 > p^m - 1\), it holds that \(M' = \lfloor \frac{p}{p'} \rfloor \geq \frac{ab}{p'}\).

Since \(2 \leq e' \leq e, p'(b+1) \leq a\), we have \(p'b < p'(b+1)\), \(p'b \leq ab\).

Hence,

\[
k = \left\lceil \frac{p'vw(p^m - 1)}{e} \right\rceil = p'b - 1, \quad \text{and}
\]

\[
e = p'vw(p^m - 1) - (p'b - 1)(avw + \frac{w}{e} + \frac{w-1}{e} + 1)
\]

\[
= avw + (1 - p'b)(\frac{w}{e} + \frac{w-1}{e} + 1).
\]

Since \(b\) is a positive integer, \(M = \lfloor \frac{p}{p'} \rfloor\) and \(p'(b+1) \leq a\), we have \(M > b+1\) and \((M-1)a > M(p'b-1) + 1\). Then,

\[
\epsilon M - l = M(aw + (1 - p'b)\left(\frac{w}{e} + \frac{w-1}{e} + 1\right))
\]

\[
-(aw + \frac{w}{e} + \frac{w-1}{e} + 1)
\]

\[
= (M-1)aw - (M-1)(aw + \frac{w}{e} + \frac{w-1}{e} + 1)
\]

\[
= (M-1)(aw - \frac{w}{e} + \frac{w-1}{e} + 1)
\]

\[
= (M-1)a(aw - \frac{w}{e} + \frac{w-1}{e} + 1)
\]

\[
> 0.
\]

By Corollary 4.4 this FHS set is optimal. This completes the proof.

Remark: Compared with the construction A in [23], the construction for FHS set from Theorem 4.16 does not require the constraint \(e \geq \text{gcd}(p_1 - 1, p_2 - 1, \ldots, p_{M-1}, q_1 - 1, \ldots, q_{M-1})\). From Theorem 4.16 we can obtain many FHS sets with new and flexible parameters.

Similar to the construction of FHS sets in Theorem 4.16, we can obtain more FHS sets by using known FHS sets, Theorem 4.17 and Theorem 4.4. Here, we give another example.

Lemma 4.17: Assume that there exists an \((n, M, \lambda; t)\)-FHS set. Then, for any integer \(t\) with \(1 \leq t \leq M\), there exists a \((\lfloor \frac{n}{M}, \frac{1}{M}, t; \lambda; t)\)-FHS set.
V. Concluding Remarks

We showed an algebraic construction, two direct constructions and recursive constructions for FHS sets. From these constructions, we obtained many infinitely families of new optimal FHS sets with respect to the Peng-Fan bound (4). Our combinatorial constructions generalized the previous methods, the recursive construction for BNCDPs in [10] became a special case of Theorem 4.7. The constraint \(g(v, n) = 1\) of Construction A in [4] was removed, the existence proof of optimal FHS sets with respect to the Peng-Fan bound (4). Our constructions, we obtained many infinitely families of new constructions and recursive constructions for FHS sets. From these special case of Theorem 4.7, the constraint \(g(v, n) = 1\) of Construction A in [4] was removed, the existence proof of optimal FHS sets via cyclotomy,

### References

[1] T. M. Apostol, Introduction to Analytic Number Theory. New York, NY, USA: Springer-Verlag, 1976.

[2] Bluetooth Special Interest Group (SIG), Washington, DC, USA. (2003, Nov.). Specification of the Bluetooth System-Core. Available: [http://www.bluetooth.org](http://www.bluetooth.org)

[3] W. Chu and C. J. Colbourn, "Optimal frequency-hopping sequences via cyclotomy," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1139-1141, Mar. 2005.

[4] J.-H. Chung, G. Gong, and K. Yang, "New classes of optimal frequency-hopping sequences by composite lengths," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3688-3697, Jun. 2014.

[5] J.-H. Chung, Y. K. Han, and K. Yang, "New classes of optimal frequency-hopping sequences by interleaving techniques," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5783-5791, Dec. 2009.

[6] J.-H. Chung and K. Yang, "k-fold cyclotomy and its application to frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2306-2317, Apr. 2011.

[7] J.-H. Chung and K. Yang, "Optimal frequency-hopping sequences with new parameters," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1685-1693, Apr. 2010.

[8] C. J. Colbourn and J. H. Dinitz, The CRC Handbook of Combinatorial Designs, CRC Press, Boca Raton, FL, 2007.

[9] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, and M. Mishima, "Sets of frequency hopping sequences: bounds and optimal constructions," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3297-3304, Jul. 2009.

[10] C. Ding, M. J. Moisio, and J. Yuan, "Algebraic constructions of optimal frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2606-2610, Jul. 2007.

[11] C. Ding, Y. Yang, and X. Tang, "Optimal sets of frequency hopping sequences from linear cyclic codes," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3605-3612, Jul. 2010. pp. 2606-2610, Jul. 2007.

[12] C. Ding and J. Yin, "Sets of optimal frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3741-3745, Aug. 2008.

[13] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. London, U.K.: Wiley, 1996.

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

[15] G. Ge, R. Fuji-Hara, and Y. Miao, "Further combinatorial constructions for optimal frequency-hopping sequences," *J. Combin. Theory Ser. A*, vol. 113, no. 8, pp. 1699-1718, Nov. 2006.

[16] G. Ge, Y. Miao, and Z. Yao, "Optimal frequency hopping sequences: Auto- and cross-correlation properties," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 867-879, Feb. 2009.

[17] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming-correlation properties," *IEEE Trans. Inf. Theory*, vol. 20, no. 1, pp. 90-94, Jan. 1974.

[18] D. Peng and P. Fan, "Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2149-2154, Sep. 2004.

[19] W. Ren, F. Fu, and Z. Zhou, "New sets of frequency-hopping sequences with optimal Hamming correlation," *Des. Codes Cryptogr.*, vol. 72, pp. 423-434, Aug. 2014.

[20] L. Yang and G. B. Giannakis, "Ultra-wideband communications: An idea whose time has come," *IEEE Signal Process. Mag.*, vol. 21, no. 6, pp. 26-54, Nov. 2004.

[21] Y. Yang, X. Tang, P. Udaya, and D. Peng, "New bound on frequency hopping sequence sets and its optimal constructions," *IEEE Trans. Inf. Theory*, vol. 57, no. 11, pp. 7605-7613, Nov. 2011.

[22] X. Zeng, H. Cai, X. Tang, and Y. Yang, "A class of optimal frequency hopping sequences with new parameters," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4899-4907, Jul. 2012.

[23] X. Zeng, H. Cai, X. Tang, and Y. Yang, "Optimal frequency hopping sequences of odd length," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 3237-3248, May 2013.

[24] Z. Zhou, X. Tang, D. Peng, and U. Parampalli, "New constructions for optimal sets of frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3831-3840, Jun. 2011.