Frequency hopping sequences with optimal partial Hamming correlation

Jingjun Bao and Lijun Ji

Abstract—Frequency hopping sequences (FHSs) with favorable partial Hamming correlation properties have important applications in many synchronization and multiple-access systems. In this paper, we investigate constructions of FHSs and FHS sets with optimal partial Hamming correlation. We first establish a correspondence between FHS sets with optimal partial Hamming correlation and multiple partition-type balanced nested cyclic difference packings with a special property. By virtue of this correspondence, some FHSs and FHS sets with optimal partial Hamming correlation are constructed from various combinatorial structures such as cyclic difference packings, and cyclic relative difference families. We also describe a direct construction and two recursive constructions for FHS sets with optimal partial Hamming correlation. As a consequence, our constructions yield new FHSs and FHS sets with optimal partial Hamming correlation.

Index Terms—Frequency hopping sequences (FHSs), partial Hamming correlation, partition-type cyclic difference packings, cyclic relative difference families, cyclotomy.

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, [5], [17], [29]. In FH multiple-access communication systems, frequency hopping sequences are employed to specify the frequency on which each sender transmits a message at any given time. An important component of FH spread-spectrum systems is a family of sequences having good correlation properties for sequence length over suitable number of available frequencies. The optimality of correlation property is usually measured according to the well-known Lempel-Greenberger bound and Peng-Fan bounds. During these decades, many algebraic or combinatorial constructions for FHSs or FHS sets meeting these bounds have been proposed, see [7]-[11], [14]-[15], [18], [20]-[21], [30]-[33], and the references therein.

Compared with the traditional periodic Hamming correlation, the partial Hamming correlation of FHSs is much less well studied. Nevertheless, FHSs with good partial Hamming correlation properties are important for certain application scenarios where an appropriate window length shorter than the total period of the sequences is chosen to minimize the synchronization time or to reduce the hardware complexity of the FH-CDMA receiver [13]. Therefore, for these situations, it is necessary to consider the partial Hamming correlation rather than the full-period Hamming correlation.

In 2004, Eun et al. [16] generalized the Lempel-Greenberger bound on the periodic Hamming autocorrelation to the case of partial Hamming autocorrelation, and obtained a class of FHSs with optimal partial autocorrelation [28]. In 2012, Zhou et al. [34] extended the Peng-Fan bounds on the periodic Hamming correlation of FHS sets to the case of partial Hamming correlation. Based on m-sequences, Zhou et al. [34] constructed both individual FHSs and FHS sets with optimal partial Hamming correlation. Very recently, Cai et al. [6] improved lower bounds on partial Hamming correlation of FHSs and FHS sets, and based on generalized cyclotomy, they constructed FHS sets with optimal partial Hamming correlation.

In this paper, we present some constructions for FHSs and FHS sets with optimal partial Hamming correlation. First of all, we give combinatorial characterizations of FHSs and FHS sets with optimal partial Hamming correlation. Secondly, by employing partition-type balanced nested cyclic difference packings, cyclic relative difference families, and cyclic relative difference packings, we obtain some FHSs and FHS sets with optimal partial Hamming correlation. Finally, we present two recursive constructions for FHS sets, which increase their lengths and alphabet sizes, and preserve their optimal partial Hamming correlations. Our constructions yield optimal FHSs and FHS sets with new and flexible parameters not covered in the literature. The parameters of FHSs and FHS sets with optimal partial Hamming correlation from the known results 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 partial Hamming correlation of FHSs and FHS sets. Section III presents combinatorial characterizations of FHSs and FHS sets with optimal partial Hamming correlation. Section IV gives some combinatorial constructions of FHSs and FHS sets with optimal partial Hamming correlation by using partition-type balanced nested cyclic difference packings, cyclic relative difference families and cyclotomic classes. Section V presents a direct construction of FHS sets with optimal partial Hamming correlation. Section VI presents two recursive constructions of FHS sets with optimal partial Hamming correlation. Section VII concludes this paper with some remarks.

II. LOWER BOUNDS ON THE PARTIAL HAMMING CORRELATION OF FHSS AND FHS SETS

In this section, we introduce some known lower bounds on the partial Hamming correlation of FHSs and FHS sets.
### Known and New FHSs with Optimal Partial Hamming Correlation

| Length   | Alphabet size | $H_{\text{max}}$ over correlation windows of length $L$ | Number of sequences | Constraints | Source |
|----------|---------------|-------------------------------------------------------|---------------------|-------------|--------|
| $q^2 - 1$ | $q$           | $\left\lceil \frac{L}{q-1} \right\rceil$           | 1                   |             | [16]   |
| $q^m - 1$ | $q^{m-1}$     | $\left\lceil \frac{L(q-1)}{q^m-1} \right\rceil$     | 1                   | $\gcd(d, m) = 1$, $d | (q-1)$ | [34]   |
| $\frac{q^{m-1}}{d}$ | $q^{m-1}$     | $\left\lceil \frac{L(q-1)}{q^m-1} \right\rceil$     | $d$                 |             | [34]   |
| $ev$     | $v$           | $\left\lceil \frac{L}{v} \right\rceil$              | $f$                 |             | [6]    |
| $2v$     | $v$           | $\left\lceil \frac{L}{v} \right\rceil$              | 1                   |             | Theorem 4.1 |
| $2v + 1$ | $\frac{2v+1}{v}$ | $\left\lceil \frac{L}{v} \right\rceil$              | 1                   | $p_i \equiv 1 \pmod{12}$ is a prime | Theorem 4.2 |
| $8v$     | $\frac{8v+1}{3}$ | $\left\lceil \frac{L}{v} \right\rceil$              | 1                   | $p_i \equiv 1 \pmod{6}$ is a prime | Theorem 4.4 |
| $32v$    | $\frac{32v+1}{3}$ | $\left\lceil \frac{L}{v} \right\rceil$              | 1                   | $p_i \equiv 1 \pmod{12}$ is a prime | Theorem 4.4 |
| $3v$     | $\frac{3v+1}{v}$ | $\left\lceil \frac{L}{v} \right\rceil$              | 1                   | $p_i \equiv 1 \pmod{4}$ is a prime | Theorem 4.4 |
| $4v$     | $\frac{4v+2}{3}$ | $\left\lceil \frac{L}{v} \right\rceil$              | 1                   | $p_i \equiv 7 \pmod{12}$ is a prime | Theorem 6.5 |
| $6v$     | $2v + 1$      | $\left\lceil \frac{L}{v} \right\rceil$              | 1                   | $p_i \equiv 5 \pmod{8}$ is a prime | Theorem 6.5 |
| $p(p^m - 1)$ | $p^m$      | $\left\lceil \frac{L}{p^m - 1} \right\rceil$       | $p^{m-1}$           | $m \geq 2$ | Theorem 5.1 |
| $evw$    | $(v-1)w + \frac{ev}{w}$ | $\left\lceil \frac{L}{ev} \right\rceil$            | $f$                 | $q_i \geq p_i > 2e$, $v > e(e-2)$ and $\gcd(w, e) = 1$ | Corollary 6.6 |
| $vq^{m-1}$ | $\frac{vq^{m-1}}{d}$ | $\left\lceil \frac{(q-1)L}{v(q^{m-1}-1)} \right\rceil$ | $d$                 | $\frac{m}{d-1}|p_i - 1$ for $1 \leq i \leq s$ | Corollary 6.1 |

$q$ is a prime power;
$v$ is an integer with prime factor decomposition $v = p_1^{n_1}p_2^{n_2} \cdots p_s^{n_s}$ with $p_1 < p_2 < \ldots < p_s$;
e, f are integers such that $e > 1$ and $e \mid \gcd(p_1 - 1, p_2 - 1, \ldots, p_s - 1)$, and $f = \frac{p_1 - 1}{e}$;
w is an integer with prime factor decomposition $w = q_1^{n_1}q_2^{n_2} \cdots q_t^{n_t}$ with $q_1 < q_2 < \ldots < q_t$;
r is an integer such that $r > 1$ and $r \mid \gcd(e, q_1 - 1, q_2 - 2, \ldots, q_t - 1)$;
p is a prime;
d, m are positive integers.

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 all $0 \leq t \leq n-1$. For any two FHSs $X = \{x(t)\}_{t=0}^{n-1}$ and $Y = \{y(t)\}_{t=0}^{n-1}$ of length $n$ over $F$, the partial Hamming correlation function of $X$ and $Y$ for a correlation window length $L$ starting at $j$ is defined by

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

where $L, j$ are integers with $1 \leq L \leq n$, $0 \leq j < n$, $h[a, b] = 1$ if $a = b$ and 0 otherwise, and the addition is performed modulo $n$. In particular, if $L = n$, the partial Hamming correlation function defined in (1) becomes the conventional periodic Hamming correlation [24].

If $x(t) = y(t)$ for all $0 \leq t \leq n-1$, i.e., $X = Y$, we call $H_{X, Y}(\tau; j|L)$ the partial Hamming autocorrelation of $X$; otherwise, we say $H_{X, Y}(\tau; j|L)$ the partial Hamming cross-correlation of $X$ and $Y$. For any two distinct sequences $X, Y$ over $F$ and given integer $1 \leq L \leq n$, we define

$$H(X; L) = \max_{0 \leq j < n} \max_{1 \leq \tau < n} \{H_{X, X}(\tau; j|L)\}$$

and

$$H(X, Y; L) = \max_{0 \leq j < n} \max_{0 \leq \tau < n} \{H_{X, Y}(\tau; j|L)\}.$$
Lemma 2.1: (6) Let $X$ be an FHS of length $n$ over an alphabet of size $l$. Then, for each window length $L$ with $1 \leq L \leq n$,

$$H(X; L) \geq \left\lceil \frac{L}{n} \left( \frac{(n-\epsilon)(n+\epsilon-l)}{l(n-1)} \right) \right\rceil,$$

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

Recall that the correlation window length may change from case to case according to the channel conditions in practical systems. Hence, it is very desirable that the involved FHSs have optimal partial Hamming correlation for any window length. The following definition is originated from the terminology of strictly optimal FHSs in [16].

Definition 2.2: Let $X$ be an FHS of length $n$ over an alphabet $F$. It is said to be strictly optimal or an FHS with optimal partial Hamming correlation if the bound in Lemma 2.1 is met for an arbitrary correlation window length $L$ with $1 \leq L \leq n$.

When $L = n$, the bound in Lemma 2.1 is exactly the Lempel-Greenberger bound [24]. It is clear that each strictly optimal FHS is also optimal with respect to the Lempel-Greenberger bound, but not vice versa [16].

Let $S$ be a set of $M$ FHSs of length $n$ over an alphabet $F$ of size $l$. For any given correlation window length $L$, the maximum nontrivial partial Hamming correlation $H(S; L)$ of the sequence set $S$ is defined by

$$H(S; L) = \max_{X \in S} \max_{X \neq Y} \max_{X,Y \in S} H(X; Y; L).$$

Throughout this paper, we use $(n, M, \lambda; l)$ to denote a set $S$ of $M$ FHSs of length $n$ over an alphabet $F$ of size $l$, where $\lambda = H(S; n)$, and we use $(n, \lambda; l)$ to denote an FHS $X$ of length $n$ over an alphabet $F$ of size $l$, where $\lambda = H(X; n)$.

When $L = n$, Peng and Fan [26] described the following bounds on $H(S; n)$, which take into consideration the number of sequences in the set $S$.

Lemma 2.3: (24) Let $S$ be a set of $M$ sequences of length $n$ over an alphabet $F$ of size $l$. Define $I = \left\lceil \frac{ML}{n} \right\rceil$. Then

$$H(S; n) \geq \left\lceil \frac{(nM - l)n}{(nM - 1)l} \right\rceil,$$

and

$$H(S; n) \geq \left\lceil \frac{2lnM - (I + 1)l}{(nM - 1)l} \right\rceil.$$
If the difference list $\Delta(B)$ contains each non-zero residue of $Z_n$ exactly $\lambda$ times, then $B$ is a cyclic difference family and denoted by $(n, K, \lambda)$-CDF.

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

In 2004, Fuji-Hara et al. [18] revealed a connection between FHSs and partition-type cyclic difference packings as follows.

**Theorem 3.1:** ([18]) 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 $Z_n$, where $K = \{|B_i| : 0 \leq i \leq l - 1\}$.

Fuji-Hara et al. [18] also gave a simplified version of the Lempel-Greenberger bound as follows.

**Lemma 3.2:** ([18]) For an arbitrary $(n, \lambda; l)$-FHS, it holds that

$$\lambda \geq \left\{\begin{array}{ll} k & \text{if } n \neq l, \\
0 & \text{if } n = l, \end{array}\right. $$

where $n = kl + \epsilon$, $0 \leq \epsilon \leq l - 1$. This implies that when $n > l$, the sequence is optimal if $\lambda = k$.

**Lemma 3.3:** ([18]) Let $n = kl + l - 1$ with $k \geq 1$. Then there exists an optimal $(n, k; l)$-FHS if and only if there exists a partition-type $(n, (k, k + 1, k), k)$-CDF in which $l - 1$ blocks are of size $k + 1$ and the remaining one is of size $k$.

For a $u$-tuple $T = (a_0, a_1, \ldots, a_{u-1})$ over $Z_n$, the multiset $\Delta_i(T) = \{a_{j+i} - a_j : 0 \leq j \leq u - 1\}$ is called $i$-apart difference list of the tuple, where $1 \leq i \leq u$, $j + i$ is reduced modulo $u$, and $a_{j+i} - a_j$ is taken as the least positive residue modulo $n$.

For a partition-type CDP of size $l$ over $Z_n$, $B = \{B_0, B_1, \ldots, B_{l-1}\}$, for $1 \leq \tau n$. Let $D(\tau) = \min_{1 \leq \tau n} \min\{g : g \in \nats \cup \Delta_i(\overline{D}(\tau))\}$, for $1 \leq i \leq \lambda = \max\{|D(\tau)| : 1 \leq \tau \leq n\}$, where $\Delta_i(\overline{D}(\tau)) = \emptyset$ if $D(\tau) = \emptyset$ or $i > |D(\tau)|$. We call $\overline{D}(\tau)$ the orbit cycle of $\tau$ in $B$ and $d^B_i$ the minimal $i$-apart distance of all orbits. Note that $D(\tau) = D(\overline{D}(\tau) + \tau \mod n)$ and $\min\{g : g \in \nats \cup \Delta_i(\overline{D}(\tau))\} = \min\{g : g \in \nats \cup \Delta_i(\overline{D}(\tau))\}$.

We illustrate the definition of $d^B_i$ in the following example.

**Example 3.4:** In this example, we construct a partition-type $(30, 11, 2)$-CDP, $B$, with $d^B_i = 15i$ for $0 < i \leq 2$.

Set

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

It is readily checked that $B$ is a $(30, 11, 2)$-CDP. By the fact $\min\{g : g \in \nats \cup \Delta_i(\overline{D}(\tau))\} = \min\{g : g \in \nats \cup \Delta_i(\overline{D}(\tau))\}$, we only need to compute $\overline{D}(\tau)$ for $1 \leq \tau \leq 15$, so as to obtain $d^B_i$. Simple computation shows that

$$\overline{D}(1) = (1, 16), \overline{D}(2) = (7, 22), \overline{D}(3) = (8, 23),$$

$$\overline{D}(4) = (3, 18), \overline{D}(5) = (0, 15), \overline{D}(6) = (3, 18),$$

$$\overline{D}(7) = (6, 21), \overline{D}(8) = (11, 26), D(9) = \emptyset,$$

$$D(10) = \emptyset, \overline{D}(11) = (8, 23), \overline{D}(12) = (2, 17),$$

$$\overline{D}(13) = (1, 16), \overline{D}(14) = (13, 28), \overline{D}(15) = (10, 25).$$

Then, $d^B_i = 15i$ for $0 < i \leq 2$. By direct check or by Theorem 3.5, the corresponding FHS is a strictly optimal $(30, 2; 11)$-FHS.

We are in a position to give a combinatorial characterization of strictly optimal FHSs.

**Theorem 3.5:** There is a strictly optimal $(n, \lceil n \rceil : l)$-FHS with respect to the bound (3) if and only if there exists a partition-type $(n, K, \lceil n \rceil)$-CDF of size $l$, $B = \{B_0, B_1, \ldots, B_{l-1}\}$ over $Z_n$, such that $d^B_i \geq \frac{ni}{l+1}$ for $1 \leq i \leq \frac{ni}{l+1}$, where $K = \{|B_i| : 0 \leq r \leq l - 1\}$.

**Proof:** Let $X$ be an FHS of length $n$ over $F = \FHS$. Let $B_r = \{t : x(t) = r, 0 \leq t \leq n - 1\}$ for each $r \in F$. Then $B_r$ is the set of position indices in the sequence $X = (x(0), \ldots, x(n-1))$ at which the frequency $r$ appears. By Theorem 3.3, the sequence $X$ is an $(n, \lceil n \rceil : l)$-FHS over $F$ if and only if $B = \{B_0, B_1, \ldots, B_{l-1}\}$ is a partition-type $(n, K, \lceil n \rceil)$-CDF of size $l$, where $K = \{|B_r| : 0 \leq r \leq l - 1\}$. It is left to show that $X$ is strictly optimal with respect to the bound (2) if and only if $d^B_i \geq \frac{ni}{l+1}$ for $1 \leq i \leq \frac{ni}{l+1}$.

Denote $\lambda = \frac{n}{l+1}$. By Lemma 2.1, $X$ is strictly optimal with respect to bound (2) if and only if $H_X(X; jL) \leq \frac{\lambda}{\lambda}$ for $1 \leq L \leq n$, i.e., for $1 \leq i \leq \lambda$, the inequality $H_X(X; jL) \leq L$ holds for $\frac{n(i-1)}{\lambda} < L \leq \lambda$. We show that the inequality $H_X(X; jL) \leq L$ holds for $\frac{n(i-1)}{\lambda} < L \leq \frac{ni}{\lambda}$ if and only if $d^B_i \geq \frac{ni}{\lambda}$.

By the definition of $H_X(X; jL)$ and $D(\tau)$, we have

$$H_X(X; jL) = |D(\tau; jL)| = D(\tau; jL) \cap \{j, j+1, j+2, \ldots, j+L-1\}$$

and the arithmetic $j + t \leq L - 1$ is reduced modulo $n$. Denote $d_i(\tau) = \min\{g : g \in \nats \cup \Delta_i(\overline{D}(\tau))\}$. Clearly, $\max\{|D(\tau; jL)|\} \leq i$ if and only if $L \leq d_i(\tau)$. Hence, $H_X(X; jL) \leq \frac{ni}{\lambda}$ if and only if $L \leq d_i(\tau)$ for $1 \leq \tau \leq n$, i.e., $L \leq d^B_i$ for $1 \leq \tau \leq n$. It follows that $H_X(X; jL) \leq i$ for $\frac{n(i-1)}{\lambda} < L \leq \frac{ni}{\lambda}$ if and only if $d^B_i \geq \frac{ni}{\lambda}$. This completes the proof.

An $(mg, k, \lambda)$-cyclic relative difference family (briefly CRDF) is an $(mg, k, \lambda)$-CDF over $Z_{mg}$, $B = \{B_i : i \in I_0\}$, such that no element of $mZ_{mg}$ occurs in $\Delta(B)$, where $mZ_{mg} = \{0, m, \ldots, (g - 1)m\}$. The number $u$ of the base blocks in $B$ is referred to as the size of the CRDF. If $\Delta(B)$ contains each element of $mZ_{mg} \setminus mZ_{mg}$ exactly $\lambda$ times and no element of $mZ_{mg}$ occurs, then $B$ is called an $(mg, k, \lambda)$-cyclic relative difference family (briefly CRDF).
One importance of a CRDP is that we can put an appropriate CDP on its subgroup to derive a new CDP. We state a simple but useful fact in the following lemma.

**Lemma 3.6:** Let $B$ be an $(mg, g, K, 1)$-CRDP of size $u$ over $\mathbb{Z}_m$ relative to $mg$, whose elements of base blocks, together with $0, m, \ldots, (s-1)m$, form a complete system of representatives for the cosets of $sm\mathbb{Z}_mg$ in $\mathbb{Z}_mg$, where $s|g$. Let $A$ be a partition-type $(g, K', \frac{s}{k})$-CDP of size $r$ over $\mathbb{Z}_g$ with $d^A_i \geq si$ for $1 \leq i \leq \frac{s}{k}$. Then there exists a partition-type $(mg, K \cup K', \frac{s}{k})$-CDP of size $\frac{gu}{s} + r$, $D$ such that $d^D_i \geq ism$ for $1 \leq i \leq \frac{u}{s}$.

**Proof:** Let $B' = \{B + jsm : B \in B, 0 \leq j < \frac{s}{k}\}$, $A' = \{mA : A \in A\}$ and $D = B' \cup A'$. Since $B$ is an $(mg, g, K, 1)$-CRDP of size $u$ over $\mathbb{Z}_m$ relative to $mg$ and all elements of base blocks, together with $0, m, 2m, \ldots, (s-1)m$, form a complete system of representatives for the cosets of $sm\mathbb{Z}_mg$ in $\mathbb{Z}_mg$, we have that $\Delta(B) \subset B' \cup A'$. Similarly, since $A$ is a partition-type $(g, K', \frac{s}{k})$-CDP of size $r$ over $\mathbb{Z}_g$, we get $\bigcup_{mA \in A} \Delta(mA) = m\Delta(A)$ and $A'$ is a partition of $\mathbb{Z}_mg$. Since $A$ and $A'$ are partition-types, $B'$ and $D$ are partition-types.

Clearly, if $\tau \in \Delta(B)$, then the orbit cycle $\hat{\Delta}(\tau)$ of $\tau$ in $D$ is the orbit cycle $\hat{\Delta}(\tau)$ of $\tau$ in $D$ is of the form $(a_0, a_0 + sm, a_0 + 2sm, \ldots, a_0 + (s-1)sm)$, and if $\tau \in \Delta(A')$, then the orbit cycle $\hat{\Delta}(\tau)$ of $\tau$ in $D$ is of the form $(b_0, b_0 + sm, b_0 + 2sm, \ldots, b_0 + (s-1)sm)$, where $(b_0, b_0 + sm, b_0 + 2sm, \ldots, b_0 + (s-1)sm)$ is the orbit cycle $\hat{\Delta}(\tau)$ of $\tau$ in $A$, otherwise $\Delta(D) = \emptyset$. Hence, $d^D_i(\tau) = ism$ for $\tau \in \Delta(B)$, $d^D_i(\tau) \geq ism$ for $\tau \in \Delta(A')$ because $d^A_i \geq si$ for $1 \leq i \leq \frac{s}{k}$, and $d^D_i(\tau) = mg$ for $\tau \notin \Delta(D)$, where $d^D_i(\tau) = \min\{g : g \in \{mg\} \cup \Delta_i(\hat{\Delta}(\tau))\}$. It follows that $d^D_i(\tau) = \min\{d^A_i(\tau) : 0 < \tau < mg\} = ism$ for $1 \leq i \leq \frac{s}{k}$. Therefore, $D$ is the required partition-type $(mg, K \cup K', \frac{s}{k})$-CDP. This completes the proof.

As a consequence of the above lemma, we have the following result.

**Theorem 3.7:** Let $k$ and $v$ be positive integers with $k+1|v-1$. Then there exists a strictly optimal $(kv, k, \frac{k+1}{k+1})$-FHS if and only if there exists a resolvable $(kv, k, k+1, 1)$-CRDP.

**Proof:** By Lemma 3.5 and Theorem 3.3, there is a strictly optimal $(kv, k, \frac{k+1}{k+1})$-FHS if and only if there is a partition-type $(kv, \{k, k+1\}, k)$-CDP over $\mathbb{Z}_{kv}$ with $d_i \geq vi$ for $1 \leq i \leq k$, in which $\frac{kv-k}{k+1}$ blocks are of size $k+1$ and the remaining one is of size $k$. We shall prove that such a partition-type $(kv, \{k, k+1\}, k)$-CDP exists if and only if there is a resolvable $(kv, k, k+1, 1)$-CDP relative to $v\mathbb{Z}_{kv} = \{0, v, \ldots, (k-1)v\}$.

Let $B$ be such a partition-type $(kv, \{k, k+1\}, k)$-CDP where $B = \{B_0, B_1, \ldots, B_{(k-2)/(k+1)}\}$. By the definition of CDP, for $1 \leq \tau \leq kv - 1$, each difference $\tau$ occurs exactly $k$ times, thus $\hat{D}(\tau) = (a_0, a_1, \ldots, a_{k-1})$ is a $k$-tuple vector of distinct elements. Clearly, $d_i(\tau) = \min\{g : g \in \{kv\} \cup \Delta_i(D(\tau))\} \leq \frac{kv}{v}$. Since $d_i(\tau) \geq vi$, we have $d_i(\tau) = vi$. This leads to $a_{i+1} = a_i + v$ for $0 \leq i \leq k-1$. Hence, for any pair $\{a, b\}$ contained in some base block of $B$, the pair $\{a+v, b+v\}$ is also contained in a base block of $B$. Since $B$ is a partition-type CDP, the set $B_j + v$ is also a base block of $B$ and one base block of $B$ is of the form $v\mathbb{Z}_{kv} + t$. Without loss of generality, let $B_{(kv-k)/(k+1)} = v\mathbb{Z}_{kv} + t$ and $B_j + v = B_j + v_{j-1}$ for $0 \leq j < (kv-k)/(k+1)$, where $v_{j-1}$ is reduced modulo $kv-k$. It is easy to see that $B_0, B_1, \ldots, B_{(k-2)/(k+1)}$ is the set of base blocks of a resolvable $(kv, k, k+1, 1)$-CDP relative to $v\mathbb{Z}_{kv}$.

Conversely, suppose that there is a resolvable $(kv, k, k+1, 1)$-CDP over $v\mathbb{Z}_{kv}$ relative to $v\mathbb{Z}_{kv}$. Then $s = \frac{k+1}{k+1}$. Since $A = \{\mathbb{Z}_k\}$ is the trivial partition-type $(k, k)$-CDP with $d^A_i = i$ for $1 \leq i \leq k$, applying Lemma 3.6 yields a partition-type $(kv, \{k, k+1\}, k)$-CDP of size $\frac{kv}{k+1}$, $D$, such that $d^D_i \geq vi$ for $1 \leq i \leq k$. This completes the proof.
Let $B_j, 0 \leq j \leq M - 1$, be a collection of $l$ subsets $B_0^j, \ldots, B_{l-1}^j$ of $\mathbb{Z}_n$, respectively. The list of external difference of ordered pair $(B_j, B_{j'})$, $0 \leq j \neq j' < M$, is the union of multisets

$$\Delta_E(B_j, B_{j'}) = \bigcup_{i \in \mathbb{I}_j} \Delta_E(B_i^j, B_i^{j'}).$$

If each $B_j$ is an $(n, K_j, \lambda)$-CDP of size $l$, and $\Delta_E(B_j, B_{j'})$ contains each residue of $\mathbb{Z}_n$ at most $\lambda$ times for $0 \leq j \neq j' < M$, then the set $\{B_0, \ldots, B_{M-1}\}$ of CDPs is said to be balanced nested with index $\lambda$ and denoted by $(n, \{K_0, \ldots, K_{M-1}\}, \lambda)$-BNCDP. If each $B_j$ is a partition-type CDP for $0 \leq j < M$, then the set $\{B_0, \ldots, B_{M-1}\}$-BNCDP 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 BNCDP.

In 2009, Ge et al. [21] revealed a connection between FHS sets and partition-type BNCDPs as follows.

**Theorem 3.9:** (21) There exists an $(n, M, \lambda;l)$-FHS set over a frequency library $F$ if and only if there exists a partition-type $(n, \{K_0, K_1, \ldots, K_{M-1}\}, \lambda)$-BNCDP of size $l$.

Let $B = \{B_X : X \in S\}$ be a family of $M$ partition-type CDPs of size $l$ over $\mathbb{Z}_n$, where $B_X = \{B_X^0, B_X^1, \ldots, B_X^{l-1}\}, X \in S$. For two distinct partition-type CDPs $B_X, B_Y$, and for $0 \leq \tau \leq n - 1$, let

$$D(X,Y)(\tau) = \{a : 0 \leq a < n, (a, a + \tau) \in B_X^i \times B_Y^j, \text{ for some } i \in I\},$$

$$D(X,Y)(\tau) = \{a_0, a_1, \ldots, a_{\tau-1}\},$$

where $0 \leq a_0 < \cdots < a_{\tau-1} < n$

and $a_{\tau-1}, a_1, \ldots, a_0 = D(X,Y)(\tau)$,

$$d(X,Y)_i^\tau = \min \left\{g : g \in \{n\} \cup \Delta_i(D(X,Y)(\tau)) \right\},$$

for $0 \leq i \leq \max\{D(X,Y)(\tau) : 0 \leq \tau < n\}$ and

$$d_i^B = \min \left\{d(X,Y)_i^\tau \mid X \in S \right\},$$

where $\Delta_i(D(X,Y)(\tau)) = \emptyset$ if $D(X,Y)(\tau) = \emptyset$ or $i > D(X,Y)(\tau)$. If $X = Y$, then $D(X,X)(\tau), D(X,X)(\tau)$ and $d(X,X)_i^\tau$ are the same as $D(\tau), D(\tau)$ and $d(\tau)$, respectively.

Note that $D(X,Y)(\tau) \equiv D(X,Y)(\tau) + \tau$ (mod n) and

$$\frac{\Delta_i(D(X,Y)(\tau))}{\Delta_i(D(X,Y)(\tau))} = \min \left\{g : g \in \{n\} \cup \Delta_i(D(X,Y)(\tau)) \right\}.$$

We illustrate the definition of $d_i^B$ of a set of CDPs in the following example.

**Example 3.9:** In this example, we construct a partition-type $(24, \{2, 3\}, \{2, 3\}, \{2, 3\})$-BNCDP, $B$, with $d_i^B$ = 8i for $1 \leq i \leq 3$.

Set

$$B_0^i = \{4, 8\}, \quad B_1^i = \{0, 20\}, \quad B_2^i = \{12, 16\},$$

$$B_3^i = \{9, 22, 23\}, \quad B_4^i = \{1, 14, 15\}, \quad B_5^i = \{6, 7, 17\},$$

$$B_6^i = \{2, 19, 21\},\quad B_7^i = \{11, 13, 18\}, \quad B_8^i = \{3, 5, 10\},$$

where $j \in \{0, 1, 2\}$ and the subscript is performed modulo 9. Let $B^i = \{B^i_j : 0 \leq \tau < 8\}$ for $j \in \{0, 1, 2\}$ and $B = \{B^0, B^1, B^2\}$.

Clearly, $\Delta(B^i) = 3 \cdot [\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 11, \pm 17]$.

$$\Delta^i(B^i, B^j) = \Delta^i(B^i, B^j) = 3 \cdot [\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 11, \pm 17].$$

Then $B$ is a partition-type $(24, \{2, 3\}, \{2, 3\}, \{2, 3\})$-BNCDP.

For each $\tau \in \Delta(B^i), 0 \leq \tau < 3$, the orbit cycle $D(B^i, B^j)(\tau)$ of $\tau$ is of the form $(a, a + 8, a + 16)$ for some $a$, for example, $D(B^i, B^j)(4) = (4, 12, 20)$.

Therefore, $\Delta_i(D(B^i, B^j)(\tau)) = \Delta_i(D(B^i, B^j)(\tau)) = 8i$ for $1 \leq i \leq 3$. So, for $0 \leq k < j < 2$ and $1 \leq i \leq 3$, we have

$$d_i^B = \min \min \{g : g \in \{24\} \cup \Delta_i(D(B^i, B^j)(\tau)) \} = 8i,$$

$$d_i^B = \min \min \{d_i^B : 0 \leq \tau < 24, 0 \leq k < j < 2 \}.$$
and only if $L \leq d_{i}^{s}(X, Y)(\tau)$ for $0 \leq \tau < n$ if $X \neq Y$ and for $1 \leq \tau < n$ if $X = Y$, i.e., $L \leq d_{i}^{s}(X, Y) = \min_{\tau \geq 1} \{d_{i}^{s}(X, Y)(\tau)\}$.

It follows that $H(X; Y; L) \leq i$ for $\frac{n(i-1)}{\lambda} < L \leq \frac{ni}{\lambda}$ if and only if $d_{i}^{s}(X, Y) \geq \frac{ni}{\lambda}$. Hence, $H(S; L) = \max_{0 \leq i \leq n} \frac{1}{\sum_{x \in S} x} \max_{\tau \geq 1} \{H(X, Y; \tau; j; L)\} \leq i$ for $\frac{n(i-1)}{\lambda} < L \leq \frac{ni}{\lambda}$ if and only if $d_{i}^{s}(X, Y) \geq \frac{ni}{\lambda}$.

For $0 \leq j \neq j' < M$, $\Delta_{E}(D_{j}, D_{j'}) = \left(\bigcup_{i=0}^{u-1} \bigcup_{i' = 0}^{q-1} \Delta_{E}(B_{(k, i), j}, B_{(k, i'), j'})\right) \cup \Delta_{E}(A_{j}, A_{j'}) = \left(\bigcup_{i' = 0}^{q-1} \Delta_{E}(B_{j} + i'sm, B_{j'} + i'sm)\right) \cup \Delta_{E}(A_{j}, A_{j'})$.

Since $(B_{j}, B_{j'}) = (0 \leq j < M)$ is an $(mg, g, \{K_{0}, \ldots, K_{M-1}\}, 1)$-BNCRD, we have that $\Delta(B_{j}, B_{j'}) \subseteq mZ_{mg} \setminus mZ_{mg}$ and $\Delta_{E}(B_{j}, B_{j'}) \subseteq mZ_{mg} \setminus mZ_{mg}$ for $0 \leq j \neq j' < M$. Since $(A_{j}, A_{j'}) = (0 \leq j \leq M - 1)$ is a $(g, \{K_{0}, \ldots, K_{M-1}\}, \frac{4}{s})$-BNCRD, we have that $\Delta(A_{j}, A_{j'})$ contains each non-zero element of $mZ_{mg}$ at most $\frac{4}{s}$ times and $\Delta_{E}(A_{j}, A_{j'})$ contains each element of $mZ_{mg}$ at most $\frac{4}{s}$ times for $j \neq j'$. It follows that $\Delta_{E}(D_{j}, D_{j'})$ contains each element of $\frac{4}{s}$ times. Similarly, $\Delta(D_{j}, D_{j'})$ contains each non-zero element of $Z_{mg}$ at most $\frac{4}{s}$ times. Hence, $D$ is a partition-type $(mg, \{K_{0} \cup K_{0'}, \ldots, K_{M-1} \cup K_{M-1}', \frac{4}{s}\})$-BNCRD of size $\frac{4m + 1}{s} + L Z_{mg}$.

From the construction, it is easy to see that if $\tau \in \Delta_{E}(B_{j}, B_{j'})$, then the orbit cycle $D_{(j, j')}(\tau)$ of $\tau$ in $(D_{j}, D_{j'})$ is of the form $(a_{0}, a_{0} + sm, a_{0} + 2sm, \ldots, a_{0} + mg - sm)$, and if $\tau \in \Delta_{E}(A_{j}, A_{j'})$, then the orbit cycle $D_{(j, j')}(\tau)$ of $\tau$ in $(D_{j}, D_{j'})$ is of the form $(mb_{0}, mb_{1}, \ldots, mb_{e-1})$ where $(b_{0}, b_{1}, \ldots, b_{e-1})$ is the orbit cycle of $\frac{q}{s}$ in $(A_{j}, A_{j'})$.

Lemma 3.11: Suppose that there exists an $(mg, g, \{K_{0}, \ldots, K_{M-1}\}, 1)$-BNCRD of size $u$, $(B_{0}, \ldots, B_{M-1})$, such that all elements of base blocks of $B_{j}$, together with $0, m, \ldots, (s-1)m$, form a complete system of representatives for the cosets of $smZ_{mg} \subseteq Z_{mg}$ for $0 \leq j < M$, where $s/g$. If there exists a partition-type $(g, \{K_{0}', \ldots, K_{M-1}'\}, \frac{4}{s})$-BNCRD of size $l$, $A$ such that $d_{i}^{A} \geq si$ for $1 \leq i < \frac{q}{s}$, then there exists a partition-type $(mg, \{K_{0} \cup K_{0}', \ldots, K_{M-1} \cup K_{M-1}', \frac{4}{s}\})$-BNCRD of size $\frac{4m + 1}{s} + L$, $D$ such that $d_{i}^{D} \geq ism$ for $1 \leq i \leq \frac{4}{s}$.

Proof: Denote $B_{j} = \{B_{k_{j}} : 0 \leq k < u\}$ for $0 \leq j < M$ and let $A = \{A_{0}, A_{1}, \ldots, A_{M-1}\}$ be a partition-type $(g, \{K_{0}', \ldots, K_{M-1}'\}, \frac{4}{s})$-BNCRD of size $l$ over $Z_{mg}$ with $d_{i}^{A} \geq si$ for $1 \leq i < \frac{q}{s}$, where $A_{j} = \{A_{j} : 0 < r < l\}$. For $0 \leq j < M$, set

$A_{j}' = \{mA_{j} : 0 < r < l\}$,

$B_{(k, i)} = B_{k} + i'sm$ for $0 \leq k < u \text{ and } 0 < i < \frac{q}{s}$, and $D_{j} = \{B_{(k, i)} : 0 \leq k < u, 0 \leq i < \frac{q}{s}\} \cup A_{j}'$,

then the size of $D_{j}$ is $\frac{4m + 1}{s} + l$.

Let $D = \{D_{j} : 0 \leq j < M\}$. It remains to prove that $D$ is a partition-type $(mg, \{K_{0} \cup K_{0}', \ldots, K_{M-1} \cup K_{M-1}', \frac{4}{s}\})$-BNCRD over $Z_{mg}$ with $d_{i}^{D} \geq ism$ for $1 \leq i \leq \frac{4}{s}$.

Since all elements of base blocks of $B_{j}$, together with $0, m, \ldots, (s-1)m$, form a complete system of representatives for the cosets of $smZ_{mg} \subseteq Z_{mg}$, we have $\{B_{(k, i)} : 0 \leq k < u, 0 \leq i < \frac{q}{s}\}$ is a partition of $Z_{mg} \setminus mZ_{mg}$. Since $A_{j}$ is a partition-type $(g, \{K_{0}', \ldots, K_{M-1}'\}, \frac{4}{s})$-BNCRD, we have that $A_{j}'$ is a partition of $mZ_{mg}$ and $D_{j}$ is a partition of $Z_{mg}$.

IV. COMBINATORIAL CONSTRUCTIONS

A. Direct constructions of strictly optimal $(n, 2; |\frac{4}{s}|)$-FHSs

Construction A1: Let $u$ be a positive integer and let $X = x(t)$ be the FHS of length $2u$ over $\mathbb{Z}_{u}$ defined by $x(t) = x(2t_{1} + t_{0}) = (-1)^{t_{0}}t_{1}$, where $t = t_{2} + t_{1}$, $0 \leq t_{0} < 2$, $0 \leq t_{1} < u$.

Theorem 4.1: For a positive integer $u$, the FHS $X$ in Construction A1 is a strictly optimal $(2u, 2; u)$-FHS, and $H(X; L) = \left(\frac{1}{s}\right)$ for $1 \leq L \leq 2u$.

Proof: For $0 \leq r < u$, denote $B_{r} = \{t : x(t) = r, 0 \leq t < 2u\}$, then we have

$B_{j} = \{2j, 1 - 2j\} \mod 2u$ for $0 \leq j < u$,

$D(1 - aj) = (2j, 2j + u) \mod 2u$ for $0 \leq j \leq \left\lfloor \frac{u - 1}{2}\right\rfloor$,

$D(1 - aj) = (2j - u, 2j) \mod 2u$ for $\left\lfloor \frac{u + 1}{2}\right\rfloor \leq j < u$.

$D(k) = \emptyset$, if $k \not\equiv \pm(1 - 4j), 0 \leq j < u$. 

$\square$
By the fact \( \min \{ g : g \in \{2u\} \cup \Delta_i(\overline{D}(\tau)) \} = \min \{ g : g \in \{2u\} \cup \Delta_i(\overline{D}(-\tau)) \} \), we have \( d_1 = u \) and \( d_2 = 2u \). Then, \( \{B_0, \cdots, B_{u-1}\} \) is a partition-type \((2u, 2, 2)-CDP\) of size \( u \) with \( d_i = \frac{nu}{2} \) for \( 0 < i \leq 2 \). Therefore, by Theorem 3.5, \( X \) is strictly optimal with respect to the bound (2).

Remark: When \( u \) is an odd integer, a strictly optimal \((2u, 2; u)\)-FHS can also be obtained from [6].

Construction A2: Let \( n \) be an odd integer and let \( X = \{x(t)\}_{t=0}^{n-1} \) be the FHS of length \( n \) over \( \mathbb{Z}_{(n-1)/2} \) defined by \( x(t) = j \) for \( t \in B_j \), \( 0 \leq j < \frac{n+1}{2} \), where \( B_j \) are defined as follows:

If \( n = 8a + 1 \), then
\[
\begin{align*}
B_0 &= \{0, 4a + 1, 8a\}; \\
B_1 &= \{4a - 1, 4a\}; \\
B_{1+r} &= \{r, 2a - 2 + 2r\} \text{ for } 1 \leq r \leq a; \\
B_{a+1+r} &= \{a + r, 2a - 1 + 2r\} \text{ for } 1 \leq r \leq a - 1; \\
B_{2a+r} &= B_{1+r} + 4a + 1 \pmod{n} \text{ for } 1 \leq r \leq 2a - 1.
\end{align*}
\]

If \( n = 8a + 3 \), then
\[
\begin{align*}
B_0 &= \{0, 4a + 1, 4a + 2\}; \\
B_1 &= \{2a, 6a + 3\}; \\
B_2 &= \{2a + 1, 6a + 1\}; \\
B_3 &= \{6a + 2, 6a + 4\}; \\
B_{3+r} &= \{r, 4a + 1 - r\} \text{ for } 1 \leq r \leq 2a - 1; \\
B_{2a+r} &= B_{3+r} + 4a + 2 \pmod{n} \text{ for } 1 \leq r \leq 2a - 2.
\end{align*}
\]

If \( n = 8a + 5 \), then
\[
\begin{align*}
B_0 &= \{0, 4a + 2, 4a + 3\}; \\
B_1 &= \{2a + 1, 6a + 5\}; \\
B_2 &= \{2a + 2, 6a + 3\}; \\
B_3 &= \{1, 6a + 4\}; \\
B_{3+r} &= \{2a + 2 + r, 6a + 3 - r\} \text{ for } 1 \leq r \leq 2a - 1; \\
B_{2a+r} &= B_{3+r} + 4a + 3 \pmod{n} \text{ for } 1 \leq r \leq 2a - 1.
\end{align*}
\]

If \( n = 8a + 7 \), then
\[
\begin{align*}
B_0 &= \{0, 4a + 3, 4a + 4\}; \\
B_r &= \{r, 2a + 2r\} \text{ for } 1 \leq r \leq a + 1; \\
B_{a+r} &= \{a + 1 + r, 2a + 1 + 2r\} \text{ for } 1 \leq r \leq a; \\
B_{2a+r} &= B_r + 4a + 4 \pmod{n} \text{ for } 1 \leq r \leq 2a + 1.
\end{align*}
\]

Theorem 4.2: For any odd integer \( n \geq 5 \), the FHS \( X \) in Construction A2 is strictly optimal \((n; \frac{n+1}{2})\)-FHS and \( H(X; L) = \left[ \frac{L}{2} \right] \) for \( 1 \leq L \leq n \).

Proof: By Theorem 3.5, we only need to show that \( \{B_j : 0 \leq j < \frac{n-1}{2}\} \) is a partition-type \((n, \{2, 3\}, 2)\)-CDP with \( d_i \geq \left[ \frac{nu}{2} \right] \) for \( 1 \leq i \leq \left[ \frac{(n-1)/2}{2} \right] \). Clearly, \( B = \{B_j : 0 \leq j < \frac{n-1}{2}\} \) is a partition of \( \mathbb{Z}_n \).

Then, it holds that \( d_1 = 4a \) and \( \lambda = \max\{|D(\tau)| : 0 < \tau < 4a\} = 2 \). Therefore, by Theorem 3.5, the sequence \( X \) is strictly optimal with respect to the bound (2).

Case 2: \( n = 8a + 3 \). By Construction A2, we have
\[
\begin{align*}
\overline{D}(1) &= (4a + 1), \quad \overline{D}(4a + 1) = (0, 2 + 4a), \quad \overline{D}(2) = (2 + 6a), \\
\overline{D}(4a) &= (1 + 2a, 3 + 6a), \quad \overline{D}(3) = (2a - 1), \quad \overline{D}(4a + 1 - 2r) = (r, r + 4a + 1), 1 \leq r \leq 2a - 2.
\end{align*}
\]

Then, it holds that \( d_1 = 4a + 1 \) and \( \lambda = \max\{|D(\tau)| : 0 < \tau < 4a + 1\} = 2 \). Therefore, by Theorem 3.5, the sequence \( X \) is strictly optimal with respect to the bound (2).

Case 3: \( n = 8a + 5 \). By Construction A2, we have
\[
\begin{align*}
\overline{D}(1) &= (4a + 2), \quad \overline{D}(4a + 2) = (0, 3 + 4a), \\
\overline{D}(2a + 2) &= (4 + 6a), \quad \overline{D}(4a + 1) = (2a + 2, 5 + 6a), \quad \overline{D}(4a + 1 - 2r) = (2a + 2 + r, r + 6a + 5), 1 \leq r \leq 2a - 1.
\end{align*}
\]

Then, it holds that \( d_1 = 4a + 3 \) and \( \lambda = \max\{|D(\tau)| : 0 < \tau < 4a + 2\} = 2 \). Therefore, by Theorem 3.5, the sequence \( X \) is strictly optimal with respect to the bound (2).

Case 4: \( n = 8t + 7 \). By Construction A2, we have
\[
\begin{align*}
\overline{D}(1) &= (4t + 3), \quad \overline{D}(4t + 3) = (0, 4 + 4t), \\
\overline{D}(2t + r) &= (r, r + 4t + 4) \text{ for } 1 \leq r \leq t + 1, \quad \overline{D}(t + r) = (t + 1 + r, r + 5t + 5), 1 \leq r \leq t.
\end{align*}
\]

Then, it holds that \( d_1 = 4a + 3 \) and \( \lambda = \max\{|D(\tau)| : 0 < \tau < 4t + 3\} = 2 \). Therefore, by Theorem 3.5, the sequence \( X \) is strictly optimal with respect to the bound (2). This completes the proof.

B. Strictly optimal FHSs from resolvable CRDFs

In this subsection, we construct resolvable CRDFs by using cyclotomic classes in order to obtain strictly optimal FHSs.

Resolvable CRDFs have been intensively studied in design theory, see [12]. We quote some results of resolvable CRDFs in the following lemma.

Lemma 4.3: (1) There exists a resolvable \((v, 2, 3, 1)\)-CRDF for all \( v \) of the form \( 2^k p_1 p_2 \cdots p_s \) where \( k \in \{1, 5\} \) and each \( p_j \equiv 1 \pmod{12} \) is a prime (\([3], [4]\)).

(2) There exists a resolvable \((v, 2, 3, 1)\)-CRDF for all \( v \) of the form \( 8p_1 p_2 \cdots p_s \) where each \( p_j \equiv 1 \pmod{6} \) is a prime (\([3]\)).

(3) There exists a resolvable \((v, 3, 4, 1)\)-CRDF for all \( v \) of the form \( 3p_1 p_2 \cdots p_s \) where each \( p_j \equiv 1 \pmod{4} \) is a prime (\([4]\)).

The application of Lemma 3.6 to the CRDFs in Lemma 4.3 yields the following strictly optimal FHSs.

Theorem 4.4: (1) There exists a strictly optimal \((v, 2, \frac{v+1}{3})\)-FHS for all \( v \) of the form \( 2^k p_1 p_2 \cdots p_s \) where \( k \in \{1, 5\} \) and each \( p_j \equiv 1 \pmod{12} \) is a prime.

(2) There exists a strictly optimal \((v, 2, \frac{v+1}{3})\)-FHS for all \( v \) of the form \( 8p_1 p_2 \cdots p_s \) where each \( p_j \equiv 1 \pmod{6} \) is a prime.
(3) There exists a strictly optimal \( (v, 3; \frac{v+1}{2}) \)-FHS for all \( v \) of the form \( 3p_1p_2\cdots p_s \) where each \( p_i \equiv 1 \pmod{4} \) is a prime.

Let \( q \) be a prime power with \( q = ef + 1 \) and \( GF(q) \) be the finite field of \( q \) elements. Given a primitive element \( \alpha \) of \( GF(q) \), define \( C_0^\alpha = \{ \alpha^i : 0 \leq i < j \leq f-1 \} \), the multiplicative group generated by \( \alpha^e \), and

\[
C_i^e = \alpha^i C_0^0
\]

for \( 1 \leq i \leq e-1 \). Then \( C_0^0, C_1^e, \ldots, C_{e-1}^e \) partition \( GF(q)^* = GF(q) \setminus \{0\} \). The \( C_i^e \) \((0 \leq i < e)\) are known as cyclotomic classes of index \( e \) (with respect to \( GF(q) \)). Given a list \( \{a_1, a_2, \ldots, a_e\} \) of elements in \( GF(q)^* \), if each cyclotomic class \( C_i^e \), \( 0 \leq i \leq e \), contains exactly one element of the list, then we say that the list forms a complete system of distinct representatives of cyclotomic classes.

In the theory of cyclotomy, the numbers of solutions of

\[
x + 1 = y, \quad x \in C_i^e, \quad y \in C_j^e
\]

are called cyclotomic numbers of order \( e \) respect to \( GF(q) \) and denoted by \( (i, j)_e \).

**Lemma 4.5:** There exists a resolvable \((4p, 4, 3, 1)\)-CRDF for any prime \( p \equiv 7 \pmod{12} \).

**Proof:** Let \( \varepsilon \) be a primitive sixth root of unity in \( \mathbb{Z}_p \). Clearly, \( e^5 \) is also a primitive sixth root of unity and \( 1 - \varepsilon + \varepsilon^2 = 0 \). Thus, \( \varepsilon^{2+1} = -\varepsilon^{2+1} = 1 - \varepsilon = -\varepsilon^2 \in C_1^e \) since \(-1 \in C_0^e \). Without loss of generality, we may assume that \( \varepsilon + 1 \in C_0^e \). Since \( \gcd(4, p) = 1 \), we have that \( \mathbb{Z}_p \) is isomorphic to \( \mathbb{Z}_4 \times \mathbb{Z}_p \). Denote by \( R \) a complete system of representatives for the cosets \( \mathbb{Z}_n^e \). Thus, we need the cyclotomic numbers \( (j-a, j)_e \).

Then

\[
\bigcup_{B \in \mathcal{B}} B \equiv \bigcup_{r \in R} \big\{ (1, r), (0, r^2), (0, r^4) \big\} \pmod{\{0, 0\}, \{0, 2\}}.
\]

In view of (5), \( s = \frac{4}{3} \times 2 = 2 \), \( 1, 2, \varepsilon \in C_1^e \), we have

\[
\bigcup_{B \in \mathcal{B}} B \equiv \bigcup_{i=0}^{1} \{ (0, 0), (1, 0) \} \\pmod{\{0, 0\}, \{0, 2\}}.
\]

Hence, all elements of base blocks of \( \mathcal{B} \), together with \( \{0, 0\} \) and \( \{1, 0\} \), form a complete system of representatives for the

\[
\{0, 0\}, \{2, 0\} \subset \mathbb{Z}_4 \times \mathbb{Z}_p.
\]

It is left to check that \( \mathcal{B} \) is a \((4p, 4, 3, 1)\)-CRDF.

Therefore, \( \mathcal{B} \) is a resolvable \((4p, 4, 3, 1)\)-CRDF.

**Lemma 4.6:** There exists a resolvable \((6p, 6, 3, 1)\)-CRDF for any prime \( p \equiv 5 \pmod{8} \).

**Proof:** For \( p = 5 \), it exists by Example 3.4. For other prime \( p \equiv 5 \pmod{8} \), \( \varepsilon \) be a primitive fourth root of unity in \( \mathbb{Z}_p \). Then \( \varepsilon \in C_2^4 \). Let \( \varepsilon \in C_4^4 \) and \( 1 + \varepsilon \in C_2^4 \), where \( a \in \{1, 3\} \) and \( j \in \{0, 1, 2, 3\} \). We first show that there exists an element \( z \) such that \( \frac{2r}{1+z} (z+1), \frac{2r}{1+z} (z+e) \in C_2^4 \). For this purpose, we need the cyclotomic numbers \( (j-a, j)_4 \).

Then

\[
\bigcup_{B \in \mathcal{B}} B \equiv \bigcup_{r \in R} \big\{ (0, r), (0, r^2), (0, r^4) \big\} \pmod{\{0, 0\}, \{0, 4\}}.
\]

where \( p = x^2 + 4y^2 \) with \( x \equiv 1 \pmod{4} \). Since \( p = x^2 + 4y^2 \), we have that \( \frac{x^2 + 4y^2}{p} \leq \sqrt{p} \) and \( \{x^2 + 4y^2 \} \leq 5(x^2 + 4y^2) = 5p \). Thus \( \frac{p+1+2r+8y}{16} > 0 \) and \( \frac{p-3-2r^2}{16} > 0 \) for \( p \geq 29 \), i.e., for any \( 0 \leq j < 4 \), the cyclotomic number \( (j-a, j)_4 > 0 \) if \( p \geq 29 \). Hence, there exists an element \( z_j \in C_2^4 \) such that \( z_j + 1 \in C_2^4 \). Thus, for each \( p \equiv 5 \pmod{8} \) with \( p \geq 29 \) there exists an element \( z \) such that \( \frac{2r}{1+z} (z+1), \frac{2r}{1+z} (z+e) \in C_2^4 \). For \( p = 13 \), take \( \varepsilon = 8 \) and \( z = 11 \). Then \( \frac{2r}{1+z} (z+1), \frac{2r}{1+z} (z+e) \in C_2^4 \).

Since \( \gcd(6, p) = 1 \), we have that \( \mathbb{Z}_6^p \) is isomorphic to \( \mathbb{Z}_6 \times \mathbb{Z}_p \). Set

\[
\mathcal{B} = \{ \{0, w\}, \{0, -w\}, \{1, w\} \} \subset \mathbb{Z}_4^0
\]

Then

\[
\bigcup_{B \in \mathcal{B}} B \equiv \bigcup_{w \in \mathbb{Z}_4^0} \big\{ (1, w), (3, w) \big\} \pmod{\{0, 0\}, \{0, 2\}}.
\]

Therefore, \( \mathcal{B} \) is a resolvable \((4p, 4, 3, 1)\)-CRDF.
Since \( \varepsilon \in C^1_2 \) and \(-1 \in C^1_2\), we have
\[
\bigcup_{B \in \mathcal{B}} \{ (0,0), (1,0), (2,0) \} \\
\equiv 2 \bigcup_{i=0}^2 \{ i \} \times Z_p \quad (\text{mod} \{ (0,0), (3,0) \}).
\]

Hence, all elements of base blocks of \( \mathcal{B} \), together with \( (0,0), (1,0) \) and \( (2,0) \), form a complete system of representatives for the cosets \( \{ (0,0), (3,0) \} \) in \( Z_6 \times Z_p \). It is left to check that \( \mathcal{B} \) is a \( (6p, 6, 3, 1) \)-CRDF.

It is straightforward that
\[
\Delta(B) = 5 \bigcup_{b=0}^5 \{ b \} \times \Delta_b,
\]
where \( \Delta_0 = \bigcup_{w \in C^3_2} \{ \pm 2w, \pm 2w \varepsilon \}, \)
\[
\Delta_1 = \bigcup_{w \in C^3_2} \{ \varepsilon w + 1, \varepsilon w(2z + 2), -w(2z + 2) \},
\]
\[
\Delta_2 = \bigcup_{w \in C^3_2} \{ \varepsilon w(1 + \varepsilon), w(2\varepsilon z), -w(2\varepsilon z) \},
\]
\[
\Delta_3 = \bigcup_{w \in C^3_2} \{ \pm 2w(2z + 1), \pm 2w(2z + 1) \},
\]
\[
\Delta_4 = -\Delta_2, \quad \text{and} \quad \Delta_5 = -\Delta_1.
\]

Since \( \varepsilon \in C^1_2, -1 \in C^1_2, \varepsilon(1+\varepsilon) = \varepsilon - 1 \) and \( \frac{(2z+2)(2z+1)}{1+\varepsilon}, -\frac{2z}{1+\varepsilon} \in C^1_2 \). We have that
\[
\Delta(B) = Z_6 \times (Z_p \setminus \{ 0 \}).
\]

Therefore, \( \mathcal{B} \) is a resolvable \((6p, 6, 3, 1)\)-CRDF.

The application to the CRDFs in this subsection yields the following strictly optimal FHSs.

**Corollary 4.7:** (1) There exists a strictly optimal \((4p, 2; \frac{4p+2}{1+\varepsilon})\)-FHS for any prime \( p \equiv 7 \) (mod 12).

(2) There exists a strictly optimal \((6p, 2; 2p+1)\)-FHS for any prime \( p \equiv 5 \) (mod 8).

**Proof:** In the following, we only prove the case (1). The other case can be handled similarly. By Lemma 4.3, there exists a resolvable \((4p, 4, 3, 1)\)-CRDF for any prime \( p \equiv 7 \) (mod 12). By Theorem 4.1 and Theorem 3.5, there is a partition-type \((4,2,2)\)-CDP of size 2 over \( Z_4 \) with \( d_i = 2i \) for \( 1 \leq i \leq 2 \). By applying Lemma 4.6 with \( s = 2 \), we obtain a partition-type \((4p, 2, 3, 2)\)-CDP over \( Z_{4p} \) with \( d_i \geq 2p \) for \( 1 \leq i \leq 2 \). Further, applying Theorem 3.5 yields a strictly optimal \((4p, 2; \frac{4p+2}{1+\varepsilon})\)-FHS.

**C. A cyclotomic construction of strictly optimal FHS sets**

In this subsection, we obtain a class of partition-type BNCDFPs with a special property by using cyclotomic classes, from which we obtain a new construction of strictly optimal FHS sets.

Let \( v \) be an odd integer with \( v > 1 \) and denote by \( U(Z_v) \) the set of all units in \( Z_v \). 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 \( p^b \) for all \( b \geq 1 \).

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 \( s \) distinct primes \( p_1, p_2, \ldots, p_s \). Let \( e \) be a common factor of \( p_1 - 1, p_2 - 1, \ldots, p_s - 1 \) and \( e > 1 \). Define \( f = \min \left( \frac{p_i - 1}{e} : 1 \leq i \leq s \right) \).

For \( 1 \leq i \leq s \), let \( g_i \) be a primitive root modulo \( p_i^{m_i} \). By the Chinese Remainder Theorem, there exist unique elements \( g_a, g_b \in U(Z_v) \) such that
\[
g \equiv g_i^{p_i^{m_i-1}} (\text{mod } p_i^{m_i}) \quad \text{for all } 1 \leq i \leq s,
\]
\[
a \equiv g_i (\text{mod } p_i^{m_i}) \quad \text{for all } 1 \leq i \leq s,
\]
then the multiplicative order of \( g \) modulo \( v \) is \( e \), the list of differences arising from \( G = \{ 1, g, \ldots, g^{e-1} \} \) is a subset of \( U(Z_v) \) and \( a'g^e - g' \in U(Z_v) \) for \( 1 \leq t < f \) and \( 0 \leq c, c' < e \).

**Lemma 4.8:** Let \( v \) be a positive 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 \( s \) distinct primes \( p_1, p_2, \ldots, p_s \). We claim that \( g \) is a resolvable \((6p, 6, 3, 1)\)-CRDF, to form a complete system of representatives for the cosets of \( vU(Z_v) \) in \( Z_v \), where \( K_0 = \cdots = K_{f-1} = \{ e \} \).

**Proof:** Let \( g \) and \( a \) be defined as above and denote \( G = \{ 1, g, \ldots, g^{e-1} \} \). Then \( G \) is a multiplicative cyclic subgroup of order \( e \) of \( Z_v \) and \( \Delta(G) \subset U(Z_v) \). 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 \( xg^r = y \) 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 \( Z_v \setminus \{ 0 \} \), then \( |R| = \frac{v-1}{e} \) and
\[
\{ ra^b \} : r \in R, 0 \leq j < e = Z_v \setminus \{ 0 \},
\]
for any integer \( b \). Since \( gcd(u, v) = 1 \), we have that \( Z_{uv} \) is isomorphic to \( Z_u \times Z_v \).

Let \( B^r_b = \{ \frac{mb}{e}, ra^b g^t \} : 0 \leq j < e \} \cap (0, R) \geq 0 \leq b < f \),
\[
B^r_b : \{ b \} \in R \subseteq (0, 0).
\]

We claim that \( \{ B^r_b : 0 \leq b < f \} \) is an \((uv, 0, \{ e \}, \{ e \}, \ldots, \{ e \}, 1)\)-BNCDF such that all elements of base blocks of \( B^r_b \), together with \( (0, 0) \), form a complete system of representatives for the cosets of \( Z_u \times \{ 0 \} \) in \( Z_u \times Z_v \).

In view of equality (6), it holds that
\[
\bigcup_{r \in R} B^r_b \cap \{ (0,0) \}
\]
\[
= \bigcup_{r \in R} \{ \frac{mb}{e}, ra^b g^t \} : 0 \leq j < e \} \cap \{ (0,0) \}
\]
\[
\equiv \{ 0 \} \times \varepsilon \times \{ 0 \} \quad (\text{mod } Z_v \setminus \{ 0 \}).
\]

It follows that all elements of base blocks of \( B^r_b \), together with \((0,0)\), form a complete system of representatives for the cosets of \( Z_u \times \{ 0 \} \) in \( Z_u \times Z_v \).

For \( 0 \leq b < f \), we show that \( \Delta(B^r_b) \) contains each non-zero element of \( Z_u \times Z_v \) at most once.
In view of equality (6), we get
\[
\Delta(B_b) = \bigcup_{r \in R} \Delta\{(\frac{j}{r}, ra^b g^j) : 0 \leq j < e\}
\]
\[
= \bigcup_{r \in R} \{(\frac{j}{r}, ra^b g^j) - (\frac{j}{r}, ra^b g^j) : 0 \leq j < e\}
\]
\[
= \bigcup_{r \in R} \{(\frac{(j-1)}{r}, ra^b (g^j - g^j)) : 0 \leq j < e\}
\]
\[
= \bigcup_{r \in R} \{(\frac{(j-1)}{r}, ra^b (g^j - 1)) : 0 \leq j < e\}
\]
\[
= \bigcup_{r \in R} \{(\frac{m}{e}, ra^b g^j (g^j - 1)) : 0 \leq j < e\}
\]
\[
= \bigcup_{r \in R} \{(\frac{m}{e}, Z_u \setminus \{0\}) \times (Z_v \setminus \{0\})\}.
\]

Hence, each \(B_b\) is an \((u, v, e, 1, 1)\)-CRDP.

For \(0 \leq b \neq b' < f\), according to equality (6) and \(a^{b - b'} g^{j - 1}\), suppose that the parameters are the same as the hypotheses of Lemma 4.8. Then there exists a \((u, v, e, 1, 1)\)-BCNCDP of size \(\frac{m}{e} + 1\) with \(d_i \geq i\) for \(1 \leq i \leq u\) where \(K_0 = \cdots = K_{f-1} = \{e\}\). Let \(A_k = \{j + k : 0 \leq j < e\}\) and \(A'_k = \{k : 0 \leq k < \frac{m}{e}\}\) for \(0 \leq b < f\), it is easy to see that \(\{A_0, \ldots, A_{f-1}\}\) is a partition-type \((u, \{K_0, \ldots, K_{f-1}\}\), \(u\))-BCNCDP of size \(\frac{m}{e}\) with \(\frac{m}{e} \geq u\) for \(1 \leq j \leq u\). Applying Lemma 3.11 with \(g = u\) and \(s = 1\) yields the following corollary.

**Corollary 4.9**: Suppose that the parameters \(v, e, f, u\) are the same as those in the hypotheses of Lemma 4.8. Then there exists a \((u, \{K_0, \ldots, K_{f-1}\}, u)\)-BCNCDP of size \(\frac{m}{e}\) with \(d_i \geq i\) for \(1 \leq i \leq u\) where \(K_0 = \cdots = K_{f-1} = \{e\}\).

Furthermore, when \(u = e\), by Theorem 3.10 the BCNCDP in Corollary 4.9 is a strictly optimal FHS set. So, we have the following corollary.

**Corollary 4.10**: Suppose that the parameters \(v, e, f, u\) are the same as those in the hypotheses of Lemma 4.8. Then there exists a strictly optimal \((e, v, f, e, v)\)-FHS set \(S\) with partial Hamming \(H(S; L) = \left\lfloor \frac{m}{e} \right\rfloor\) for \(1 \leq L \leq ev\).

**Lemma 4.8** interprets the generalized cyclotomic construction in (6) for FHS sets via cyclotomic cosets. In comparison, our method is quite neat and more clear to understand.

**V. A DIRECT CONSTRUCTION OF STRICTLY OPTIMAL FHS SETS**

In this section, we use finite fields to give a direct construction of strictly optimal FHS sets.

**Construction B** Let \(p\) be a prime and let \(m\) be an integer with \(m > 1\). Let \(K\) be a primitive element of \(GF(p^m)\) and denote \(R = \{\sum_{i=0}^{m-1} a_i \alpha_i : a_i \in GF(p), 1 \leq i < m\}\). Let \(S = \{X^a : a \in R\} \) be a set of \(p^{m-1}\) FHSs of length \(p(p^m - 1)\), where \(X^a = \{X^a(t)\}_{t=0}^{p^m-1}\) is defined by \(X^a(t) = \alpha(t)^a + \{t\} + a\) and \(\{t\} + a\) denotes the least nonnegative residue of \(z\) modulo \(u\) for any positive integer \(u\) and any integer \(z\).

**Theorem 5.1**: Let \(p\) be a prime and let \(m\) be an integer with \(m > 1\). Then the FHS set in Construction B is strictly optimal \((p(p^m - 1), p^{m-1}, p, p^m)\)-FHS set with respect to the bound (6) over the alphabet \(GF(p^m)\).

**Proof**: Firstly, we prove that \(H(S; L) = \left\lfloor \frac{L}{p^m - 1} \right\rfloor\) for \(1 \leq L \leq p(p^m - 1)\). For \(0 \leq \tau, j \leq p(p^m - 1) - 1\) and \(a, b \in R\), the partial Hamming correlation \(H_{X^a, X^b}(\tau)\) is given by

\[
H_{X^a, X^b}(\tau : j|L) = \sum_{t=j}^{j+L-1} h[X^a(t), X^b(t + \tau)]
\]

\[
= \sum_{t=j}^{j+L-1} h[\alpha(t)^{p^m-1} + \{t\} + a, \alpha(t+\tau)^{p^m-1} + \{t+\tau\} + b]
\]

\[
= \sum_{t=j}^{j+L-1} h[a - b - \{\tau\} + \{\tau\} + a, \alpha(t)^{p^m-1} (\alpha(t)^{p^m-1} - 1)]
\]

Denote \(\tau_0 = \{\tau\} + 1\) and \(\tau_1 = \{\tau\}\). According to the values of \(a, b\) and \(\tau\), we distinguish four cases.

Case 1: \(a = b\) and \(\tau_0 = 0\). In this case \(\tau_0 \neq 0\) and \(\alpha^{\tau_0 - 1} \in GF(p^m)\). Then

\[
H_{X^a, X^b}(\tau : j|L) = \sum_{t=j}^{j+L-1} h[0, \alpha(t)^{p^m-1} (\alpha^{\tau_0 - 1} - 1)]
\]

\[
= 0.
\]

Case 2: \(a = b\) and \(\tau_1 \neq 0\). If \(\tau_0 = 0\), then

\[
H_{X^a, X^b}(\tau : j|L) = \sum_{t=j}^{j+L-1} h[-\tau_1, 0] = 0.
\]

Otherwise, let \(t_0\) be an integer such that \(-\tau_1 = \alpha(t_0)^{p^m-1} (\alpha^{\tau_0 - 1} - 1)\). Then

\[
H_{X^a, X^b}(\tau : j|L) = \sum_{t=j}^{j+L-1} h[\tau_1, \alpha(t_0)^{p^m-1} (\alpha^{\tau_0 - 1} - 1)]
\]

\[
= \sum_{t=j}^{j+L-1} ||\{t : t \equiv t_0 \mod (p^m - 1)\}||
\]

\[
\leq \left\lfloor \frac{L}{p^m - 1} \right\rfloor .
\]

Case 3: \(a \neq b\) and \(\tau_0 = 0\). Since \(a - b \notin GF(p)\), we have \(a - b \neq \tau_1\). Then

\[
H_{X^a, X^b}(\tau : j|L) = \sum_{t=j}^{j+L-1} h[a - b - \tau_1, 0] = 0.
\]
Case 4: \( a \neq b \) and \( \tau_0 \neq 0 \). Clearly, \( a - b - \tau_1 \neq 0 \). Let \( t_0 \) be an integer such that \( a - b - \tau_1 = \alpha^{(t_0)p^{m-1}}(\alpha^{\tau_0} - 1) \). Then,

\[
H_{X^t} = \sum_{t=0}^{L} h[a - b - \tau_1, \alpha^{(t)p^{m-1}}(\alpha^{\tau_0} - 1)]
\]

Finally, we prove that \( H(S; L) \geq \left( \frac{L}{p^{m-1}} \right) \). Note that \( S \) contains \( p^{m-1} \) FHSs of length \( p(p^{m-1}) \) over an alphabet of size \( p^m \). Since \( I = \left\{ \frac{p(p^{m-1})}{p^m} \right\} = p^m - 1 \), by Lemma 2.4 we get

\[
H(S; L) \geq \left( \frac{L}{p^{m-1}} \right) \left( \frac{2(p^{m-1})p(p^{m-1})}{p^{m-1} - 1} \right)
\]

Therefore, \( \{ X^a : a \in R \} \) is a strictly optimal \( (p(p^{m-1})-1), p^{m-1}, p; p^m) \)-FHS set with respect to the bound (4).

We illustrate the idea of Theorem 5.1 with \( m = 2 \) and \( p = 3 \) in the following example.

**Example 5.2:** Using the primitive polynomial \( f(x) = x^2 + x + 2 \in GF(3)[x] \), we construct the GF(9) as \( GF(3)[\alpha]/f(\alpha) \) where \( \alpha^2 + \alpha + 2 = 0 \). The 9 elements of \( GF(9) \) can be represented in the form \( a_0 + a_1 \alpha, a_0, a_1 \in GF(3) \). The FHS set \( S = \{ X^0, X^a, X^{2a} \} \) generated by Construction B is given by

\[
X^0 = (1, \alpha + 1, 2\alpha, 2\alpha + 2, 0, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2)
\]

\[
X^a = (\alpha + 1, 2\alpha + 1, 0, 2\alpha, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2)
\]

\[
X^{2a} = (2\alpha + 1, 1, 1, 0, \alpha + 2, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2, 2\alpha + 2)
\]

It is readily checked that \( S = \{ X^0, X^a, X^{2a} \} \) is a strictly optimal \( (24, 3, 3; 9) \)-FHS set with respect to the bound (4). Such an FHS set is the same as that in Example 3.3.

**VI. TWO RECURSIVE CONSTRUCTIONS OF STRICTLY OPTIMAL FHS SETS**

In this section, two recursive constructions are used to construct strictly optimal individual FHSs and FHS sets. The first recursive construction is based on the cyclic difference matrix (CDM).

A \( (w, t, 1) \)-CDM is a \( t \times w \) matrix \( D = (d_{ij}) \) \( (0 \leq i < t, 0 \leq j < w) \) with entries from \( Z_w \) such that, for any two distinct rows \( R_r \) and \( R_h \), the vector difference \( R_h - R_r \) contains every residue of \( Z_w \) exactly once. It is easy to see that the property of a difference matrix is preserved even if we add any element of \( Z_w \) 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 an \( (w, t, 1) \)-CDM. Observe that difference matrices have been extensively studied. A large number of known \( (w, t, 1) \)-CDMs are well documented in [12]. In particular, the multiplication table of the prime field \( Z_p \) is a \( (p, p, 1) \)-CDM. By using the usual product construction of CDMS, we have the following existence result.

**Lemma 6.1:** (12) 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 an \( (w, t, 1) \)-CDM.

**Theorem 6.2:** Assume that \( \{ B_0, \ldots, B_{M-1} \} \) is an \( (mg, g, \{ K_0, K_1, \ldots, K_{M-1} \}, 1) \)-BNCRDP of size \( u \) such that all elements of base blocks of \( B_j \), together with \( 0, m, \ldots, (s - 1)m \), form a complete system of representatives for the cosets of \( smZ_{mg} \) in \( Z_{mg} \) for \( 0 \leq j < M \), where \( s | g \) and \( B_j = \{ B_{j_0}, B_{j_1}, \ldots, B_{j_{M-1}} \} \). Then there exists a homogeneous \( (w, t, 1) \)-CDM over \( Z_{uw} \) with \( t = \max \{ \sum_{0 \leq i < u} |B_i^j| \} \) and gcd\( (w, 2) = 1 \), then there also exists an \( (mgw, gw, \{ K_0, K_1, \ldots, K_{M-1} \}, 1) \)-BNCRDP of size \( uw \), \( B' = \{ B'_{j_0}, B'_{j_1}, \ldots, B'_{j_{M-1}} \} \) such that all elements of base blocks of \( B'_{j_i} \), together with \( 0, m, \ldots, (sw - 1)m \), form a complete system of representatives for the cosets of \( smuwZ_{mgw} \) in \( Z_{mgw} \) for \( 0 \leq j < M \).

**Proof:** Let \( \Gamma = \{ \gamma_{i,j} \} \) be a homogeneous \( (w, t, 1) \)-CDM over \( Z_{uw} \). For each collection of the following \( M \) blocks:

\[
B_i^0 = \{ a_i, 0, 1, \ldots, a_i, 0, k_i \},
\]

\[
B_i^1 = \{ a_i, 1, k_0, 1, \ldots, a_i, 1, 1 \},
\]

\[
\vdots
\]

\[
B_i^{M-1} = \{ a_i, M-1, k_{M-1}+1, \ldots, a_i, M-1, k_{M-1} \},
\]

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

\[
B'_{(i,k)} = \{ a_i, j_{i+1} + mgk_{j_i+1,1} + \ldots, a_i, j_{i+k} + mgk_{j_i+k} \},
\]

\[
0 \leq j < M, 0 \leq k < w.
\]

Set

\[
B'_{j} = \{ B'_{(i,k)} : 0 \leq i < u, 0 \leq k < w \},
\]

\[
B'' = \{ B'_{j} : 0 \leq j < M \},
\]

then the size of \( B'' \) is \( uw \) for \( 0 \leq j < M \). It is left to show that \( B'' \) the required \( (mgw, gw, \{ K_0, K_1, \ldots, K_{M-1} \}, 1) \)-BNCRDP.
 Firstly, we show that all elements of base blocks $B'_i$, together with $0, m, \ldots, (sw - 1)m$, form a complete system of representatives for the cosets of $smwZ_{mgw}$ in $Z_{mgw}$. Since $gcd(w, \frac{4}{3}) = 1$, we have that $\{c \cdot \frac{4}{3} : 0 \leq c < w\} \equiv \{0, 1, \ldots, w - 1\} \pmod{w}$. It follows that $\{ms \cdot \frac{4}{3} : 0 \leq c < w\} \equiv \{csmw : 0 \leq c < w\} \pmod{smw}$. Clearly, $\bigcup_{0 \leq i < w} B'_i(k) = \bigcup_{z \in B'_i} \{z + csmw : 0 \leq c < w\}$, since all elements of base blocks of $B'_i$ together with $0, m, 2m, \ldots, (s - 1)m$, form a complete system of representatives for the cosets of $smwZ_{mgw}$ in $Z_{mgw}$, we have that $\bigcup_{0 \leq i < w} B'_i = \{0, 1, 2, \ldots, sm - 1\} \{0, m, \ldots, sm - m\} \pmod{smw}$, and

$$
\bigcup_{0 \leq i < u, 0 \leq k < w} B'_i(k) = \bigcup_{0 \leq i < u} \bigcup_{0 \leq k < w} \{z + csmw : 0 \leq c < w\} = \bigcup_{0 \leq i < u} \bigcup_{z \in B'_i} \{z + csmw : 0 \leq c < w\} = \bigcup_{z \in I_{sw}} \{z + csmw : 0 \leq c < w\} = I_{smw} \{0, m, \ldots, smw - m\} \pmod{smw},
$$
as desired.

Secondly, we show that each $B'_i$ is an $(mgw, gw, K_j, 1)$-CRDP. Since $B_j$ is an $(mg, g, K_j, 1)$-CRDP, we have $\Delta(B_j) \subset Z_{mgw} \setminus mZ_{mgw}$. Simple computation shows that

$$
\Delta(B'_i) = \bigcup_{0 \leq i < u, 0 \leq k < w} \Delta(B'_i(k)) = \bigcup_{0 \leq i < u, 0 \leq k < w} \{a - b + csmw : a \neq b \in B'_i, 0 \leq c < w\} = \bigcup_{\tau \in \Delta(B_j)} (mgZ_{mgw} + \tau) \subset Z_{mgw} \setminus mZ_{mgw}.
$$

It follows that $B'_i$ is an $(mgw, gw, K_j, 1)$-CRDP. Finally, we show $\Delta(B'_i, B'_j) \subset Z_{mgw} \setminus mZ_{mgw}$ for $0 \leq j \neq j' \leq M$. Since $\Delta(B'_i, B'_j) \subset Z_{mgw} \setminus mZ_{mgw}$, we get

$$
\Delta(B'_i, B'_j) = \bigcup_{0 \leq i < u, 0 \leq k < w} \Delta(B'_i(k), B'_j(k)) = \bigcup_{0 \leq i < u, 0 \leq k < w} \{b - a + csmw : (a, b) \in B'_i \times B'_j, 0 \leq c < w\} = \bigcup_{\tau \in \Delta(B'_i, B'_j)} (mgZ_{mgw} + \tau) \subset Z_{mgw} \setminus mZ_{mgw}.
$$

Therefore, $B'_i$ is the required BNCRDP. This completes the proof.

The significance of Theorem 6.2 is that it gives us an effective way to construct a BNCRDP such that all elements of base blocks of each CRDP, together with $0, m, \ldots, (sw - 1)m$, form a complete system of representatives for the cosets of $smwZ_{mgw}$ in $Z_{mgw}$, which is crucial to our investigation of this paper.

By employing Theorem 6.2 we obtain the following construction for resolvable CRDFs.

**Corollary 6.3:** Assume that there exists a resolvable $(mg, g, k, 1)$-CRDP, a resolvable $(gw, g, k, 1)$-CRDP and a $(w, k + 1, 1)$-CDM. If $gcd(w, k - 1) = 1$, then there exists a resolvable $(mgw, g, k, 1)$-CRDP.

**Proof:** Since there exists a $(w, k + 1, 1)$-CDM, there exists a homogeneous $(w, k, 1)$-CDM. Since there exists a resolvable $(mg, g, k, 1)$-CRDP and $gcd(w, k - 1) = 1$, applying Theorem 6.2 with $M = 1$ and $s = \frac{4}{3}$ gives a resolvable $(mgw, gw, k, 1)$-CRDP $B$. Let $A$ be a resolvable $(gw, g, k, 1)$-CRDP. Then, $B(\bigcup(mA : A \in A))$ is a resolvable $(mgw, gw, k, 1)$-CRDP, where $mA = \{ma : a \in A\}$.

Remark: When $g = k - 1$, the recursive construction for CRDFs from Corollary 6.3 has been given [23].

Applying Corollary 6.3 with the known resolvable CRDFs in section IV-B, we get the following new resolvable CRDFs.

**Corollary 6.4:** (1) There exists a resolvable $(v, 4, 3, 1)$-CRDF for all $v$ of the form $4p_1p_2 \ldots p_u$ where each $p_j = 7$ (mod 12) is a prime.

(2) There exists a resolvable $(v, 6, 3, 1)$-CRDF for all $v$ of the form $6p_1p_2 \ldots p_u$ where each $p_j = 5$ (mod 8) is a prime.

**Proof:** We only prove the first case. The other case can be handled similarly. We prove it by induction on $t$. For $u = 1$, by Lemma 4.5 the assertion holds. Assume that the assertion holds for $u = r$ and consider $u = r + 1$. Start with a resolvable $(4p_1p_2 \ldots p_r, 4, 3, 1)$-CRDF over $Z_{4p_1p_2 \ldots p_r}$ which exists by induction hypothesis. By Lemma 6.1 and Lemma 6.5 there exists a $(p_{r+1}, 5, 1)$-CDM and a resolvable $(4p_{r+1}, 4, 3, 1)$-CRDF. Applying Corollary 6.3 yields a resolvable $(4p_{r+1}p_{r+2} \ldots p_{r+5}, 4, 3, 1)$-CRDF. So, the conclusion holds by induction.

The application to the CRDFs in Corollary 6.4 gives the following strictly optimal FHSs.

**Theorem 6.5:** (1) There exists a strictly optimal $(v, 2, \frac{v+2}{3})$-FHS for all $v$ of the form $4p_1p_2 \ldots p_u$ where each $p_j = 7$ (mod 12).

(2) There exists a strictly optimal $(v, 2, \frac{v+1}{2})$-FHS for all $v$ of the form $6p_1p_2 \ldots p_u$ where each $p_j = 5$ (mod 8).

**Proof:** We only prove the second case. The first case can be handled similarly. By Corollary 6.4 there exists a resolvable $(v, 6, 3, 1)$-CRDF. By Theorem 6.1 and Theorem 3.5 there exists a $(6, 2, 2)$-CDP, $A$ of size 3 with $d_0^A \geq \frac{4}{7} A = 3i$ for $1 \leq i \leq 2$. Applying Lemma 3.6 with $g = 6$ and $s = 3$, there exists a partition-type $(v, [2, 3, 2])$-CDP over $Z_v$ with $d_1^A \geq \frac{4}{7} A = 3i$, we obtain a strictly optimal $(v, 2, \frac{v+1}{2})$-FHS.

By virtue of Lemma 4.8 we can apply Theorem 6.2 to produce the following series of strictly optimal FHS sets meeting the lower bound [4].

**Corollary 6.6:** Let $v$ be an odd integer of the form $v = p_1^m \cdot p_2^m \cdot \cdots \cdot p_n^m$ for $s$ positive integers $m_1, m_2, \ldots, m_s$ and $s$ primes $p_1, p_2, \ldots, p_s$ with $p_1 < p_2 < \cdots < p_s$. Let $e$ be a common factor of $p_1 - 1, p_2 - 1, \ldots, p_s - 1$ such that $2 < e < p_1$ and let $f = \frac{4}{3}$. Let $w$ be an odd integer of the form $w = q_1^m q_2^m \cdots q_t^m$ for $t$ positive integers $n_1, n_2, \ldots, n_t$ and $t$ distinct primes $q_1, q_2, \ldots, q_t$ with $q_1 < \cdots < q_t$ such that $p_1 \leq q_1$ and $gcd(e, w) = 1$. Let $r$ be a common factor of $e, q_1 - 1, q_2 - 1, \ldots, q_t - 1$ with $r > 1$. If $v > e(v - 2)$, then there exists a strictly optimal $(ewv, f, e; (v - 1)w + \frac{4vw}{3})$-FHS set with respect to the bound [4].

**Proof:** Firstly, we prove that there exists a partition-type $(ewv, \{K_0', \ldots, K_{f-1}'\}, e)$-BNCRDP of size $(v - 1)w + \frac{4vw}{3}, S'$
such that $d^S_i \geq wv$ for $1 \leq i \leq e$, where $K'_0 = \cdots = K'_{f-1} = \{e, r\}$.

By Lemma 3.8, there exists an $(ev, \{K_0, \ldots, K_{f-1}\})$-BNCRDP of size $\frac{ev}{e}$ such that all elements of base blocks of each CRDP, together with 0, form a complete system of representatives for the cosets of $w\mathbb{Z}_v^e$ in $\mathbb{Z}_{ev}$ where $K_0 = \cdots = K'_{f-1} = \{e\}$. Since $p_1 \leq q_1$, by Lemma 6.1 there exists a homogeneous $(w, p_1 - 1)$-CDM over $\mathbb{Z}_w$. Since $gcd(e, w) = 1$, applying Theorem 6.2 with $g = e$, $s = 1$ yields an $(ew, ev, \{K_0, K_1, \ldots, K_{f-1}\}, 1)$-BNCRDP of size $\frac{ev}{e}$ such that all elements of base blocks of each CRDP, together with $0, \ldots, (w-1)v$, form a complete system of representatives for the cosets of $wv\mathbb{Z}_{ewv}$ in $\mathbb{Z}_{ewv}$. By Corollary 4.9 there exists a partition-type $(ew, \{K'_0, \ldots, K'_{f-1}\}, e)$-BNCRDP of size $\frac{ev}{e}$, $S$ with $d^S_i \geq w$ for $1 \leq i \leq e$, where $K'_0 = \cdots = K'_{f-1} = \{r\}$. By applying Lemma 3.10 with $g = ev$ and $s = w$ we obtain a partition-type $(ew, \{K'_0, \ldots, K'_{f-1}\}, e)$-BNCRDP of size $(v-1)w + \frac{ev}{e}$, $S'$ with $d^S_i \geq wv$ for $1 \leq i \leq e$, where $K'_0 = \cdots = K'_{f-1} = \{e, r\}$.

Finally, we show $\frac{2InM-(I+1)H}{(n-M-I)M} = e$. By definition, we have

$$I = \frac{ewv - p_1}{(v-1)w + \frac{ev}{e}} = \frac{rvv(p_1-1)}{(v+1)(r-1)} \geq \frac{p_1-1}{p_1-1} = \begin{cases} p_1-1 & \text{if } r = e, \\
p_1-2 & \text{if } r < e. \end{cases}$$

If $r = e$, we have

$$\frac{2InM-(I+1)H}{(n-M-I)M} = \frac{2(p_1-1)ewv-p_1}{(ewv-1)\{ewv-1\}} = \frac{e(p_1-1)wv}{wv(p_1-1)-1} = e - \frac{ewv}{wv(p_1-1)-1} = e.$$

Otherwise, we have

$$\frac{2InM-(I+1)H}{(n-M-I)M} = \frac{2(p_1-2)ewv + p_1 - (p_1-1) - (p_1-2)wv - w + \frac{ev}{e}}{(ewv-1)\{ewv-1\}} = e - \frac{wv + (p_1-2)e}{wv(p_1-1)-1}.$$  

Since $p_1 > 2e$, $e \geq r \geq 2$ and $v > e(e-2)$, we have $v(p_1 - 1) > ev + \frac{ev}{e} = \frac{(p_1-2)e}{r}$, which leads to

$$0 < \frac{wv + (p_1-2)e}{wv(p_1-1)-1} < 1.$$  

(7)

It follows from (7) that $\frac{2InM-(I+1)H}{(n-M-I)M} = e$. By Theorem 3.10 $S'$ is a strictly optimal $(ewv, f, e; (v-1)w + \frac{ev}{e})$-FHS set with respect to the bound (4). This completes the proof.

Now, we present the second recursive construction.

**Construction C:** 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 $s$ distinct primes $p_1, p_2, \ldots, p_s$. Let $e$ be a common factor of $p_1-1, p_2-1, \ldots, p_s-1$ with $e > 1$, and let $f = \min \{\frac{p_i-1}{e} : 1 \leq i \leq s\}$. Let $\{X_0, X_1, \ldots, XM-1\}$ be an $(e, M, \lambda, I)$-FHS set over $F$, where $X_i = \{x_i(t)\}_{t=0}^{e-1}$ and $M \leq f$. For $0 \leq i < M$, let $Y_i = \{y_i(t)\}_{t=0}^{e-1}$ be the FHS over $\mathbb{Z}_v \times F$, defined by

$$y_i(t) = ((a^i g^t \cdot y_i(t)), x_i(t)),$$

where $a$ and $g$ are defined in Section IV-C. $(z)_a$ denotes the least nonnegative residual of $z$ modulo $a$ for any positive integer $a$ and any integer $z$.

**Lemma 6.7:** Let $Y_i$ and $Y_j$ be any two FHSs in Construction C. Then for $0 \leq \tau, c < ve$ and $1 \leq L \leq ve$, it holds that $H_{Y_i, Y_j}(\tau, c|L) \leq H_{X_i, X_j}(\langle \tau \rangle, c|k|\{\frac{L}{f}\})$ for some $k$ with $0 \leq k < e$.

**Proof:** By definition,

$$h[y_i(t), y_j(t + \tau)] = h[\langle a^i g^t \cdot y_i(t) \rangle, \langle a^j g^{(t+\tau)}(t + \tau) \rangle, x_j(t + \tau)] = h[\langle a^i g^t \cdot y_i(t) \rangle, \langle a^j g^{(t+\tau)}(t) \rangle, x_j(t + \tau)] = h[\langle a^i - a^j g^\tau \rangle, \langle a^j g^{(t+\tau)} \rangle, x_j(t + \tau)].$$

According to the parameters $i, j, \tau$, we distinguish two cases. Case 1: $i = j$ and $(\tau)_e = 0$. Since $g^\tau = 1$ and $x_i(t) = x_j(t + \tau)_e$, we get

$$H_{Y_i, Y_j}(\tau, c|L) = \sum_{t=0}^{c+L-1} h[y_i(t), y_j(t + \tau)] = \sum_{t=0}^{c+L-1} h[0, (a^i g^\tau)] = \begin{cases} L & \text{if } \tau = 0, \\
0 & \text{otherwise}. \end{cases}$$

The last equality holds since $gcd(v, e) = 1$. Therefore, $H_{Y_i, Y_j}(\tau, c|L) \leq H_{X_i, X_j}(\langle \tau \rangle, c|k|\{\frac{L}{f}\})$ for $0 \leq k < e$.

Case 2: $i \neq j$ or $(\tau)_e \neq 0$. In this case, $a^i - a^j g^\tau \in U(\mathbb{Z}_v)$. Set

$$t_0 \equiv a^i g^\tau \cdot (a^i - a^j g^\tau)^{-1} \mod v.$$

Then $h[\langle (a^i - a^j g^\tau) t \rangle, \langle a^i g^\tau \rangle, x_j(t + \tau)] = 1$ if and only if $\langle t \rangle_v = \langle t_0 \rangle_v$. Since $e(p_1 - 1)$ for $0 < r \leq s$, it holds that $v \equiv 1 \mod e$. Then

$$H_{Y_i, Y_j}(\tau, c|L) = \sum_{t=0}^{c+L-1} h[y_i(t), y_j(t + \tau)] = \sum_{t=0}^{c+L-1} h[\langle a^i - a^j g^\tau \rangle, \langle a^j g^\tau \rangle, x_j(t + \tau)] = \sum_{t_0 + av \in e_c, c_1, \ldots, c_{c-1}} h[x_i(t_0 + av), x_j(t + \tau)] \leq H_{X_i, X_j}(\langle \tau \rangle, c|t_0 + [\frac{c+L-1-t_0}{e}]|\{\frac{L}{f}\}).$$
This completes the proof.

Theorem 6.8: Let \( v \) be an odd integer of the form \( v = p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s} \) for some positive integers \( m_1, m_2, \ldots, m_s \) and \( s \) distinct primes \( p_1, p_2, \ldots, p_s \). Let \( e \) be a positive integer such that \( e|p_i - 1 \) for \( 1 \leq i \leq s \). If there is a strictly optimal \((e, M; \lambda; l)\)-FHS with respect to the bound (2) over \( F \) such that \( \lambda|e \) and \( e > l \), then the sequence \( Y \) in Construction C is a strictly optimal \((ve, \lambda; v\ell)\)-FHS with respect to the bound (2).

Proof: We first prove that \( Y \) in Construction C is a \((ve, \lambda; v\ell)\)-FHS. Let \( X \) be a strictly optimal \((e, M; \lambda; l)\)-FHS, we have \( \lambda|e \leq \ell \leq (\lambda + 1)l \). Let \( e = \lambda l + 1 \), \( 0 \leq \ell < \lambda \), then \( ve = \lambda(v\ell) + v \). Since \( X \) meets the bound (2) by Lemma 2.1, we get

\[
H(X; L') = \left[ \frac{e}{e} \left( \frac{(e - e)(e + e - l)}{e(e - l)} \right) \right] = \left[ \frac{\lambda L'}{e} \right]
\]

for \( 1 \leq L' \leq e \). By Lemma 6.7, we have \( H(Y, ve) = \max_{1 \leq \ell < ve} \{ H(Y, X; \ell)(ve, \ell) \} \leq \max_{1 \leq \ell < ve} \{ H(Y, X; (\ell)(ve, \ell)) \} = \lambda \).

By Lemma 3.2, we have \( H(Y, ve) = \lambda \), i.e., \( Y \) is a \((ve, \lambda; v\ell)\)-FHS.

It remains to prove that \( Y \) is strictly optimal with respect to the bound (2). On one hand, by Lemma 2.1, we have that

\[
H(Y; L) \leq \left[ \frac{\lambda L}{ve} \right] = \left[ \frac{\lambda}{ve} \right]
\]

for \( 1 \leq L \leq ve \). On the other hand, by Lemma 6.7, equality (8) and the fact that \( \frac{\lambda}{ve} \) is an integer, we have

\[
H(Y; L) \leq H(Y; [\frac{\lambda}{ve}]) = \left[ \frac{\lambda}{ve} \right] = \left[ \frac{\lambda}{ve} \right],
\]

where the last equality holds because of the property of ceiling function given in page 71 of [22]. Therefore, \( H(Y; L) = \left[ \frac{\lambda L}{ve} \right] \). This completes the proof.

Theorem 6.9: Let \( v \) be an odd integer of the form \( p_1^{m_1} p_2^{m_2} \cdots p_s^{m_s} \) for some positive integers \( m_1, m_2, \ldots, m_s \) and \( s \) primes \( p_1, p_2, \ldots, p_s \) such that \( p_1 < p_2 < \cdots < p_s \). Let \( e > 1 \) be an integer such that \( e|p_i - 1 \) for \( 0 < i \leq s \), and \( f = \min \{ \frac{e}{p_i^k} : 1 \leq i \leq s \} \). Let \( M \) be a positive integer such that \( M \leq f \). If there is a strictly optimal \((e, M; \lambda; l)\)-FHS with respect to the bound (4) over \( F \), then we have \( A = \{ Y_0, Y_1, \ldots, Y_{M-1} \} \) generated by Construction C is a strictly optimal \((ve, M, \lambda; \ell)\)-FHS set with respect to the bound (4).

Proof: Since \( A \) meets the bound (4), \( A \) is an optimal FHS set and \( H(A; e) = \lambda \). By Lemma 6.7, we have \( H(B; ve) \leq H(A; e) = \lambda \). By Lemma 2.3, we have that \( B \) is a \((ve, M, \lambda; v\ell)\)-FHS set with respect to the bound (4).

It remains to prove that \( B \) is a strictly optimal FHS set with respect to the bound (4). By the definition of \( I \) in Lemma 2.3, we have \( I = \left[ \frac{\lambda}{ve} \right] \). Set \( eM = H + r \) where \( r \) is the least nonnegative residue module \( l \). Since \( A \) is a strictly optimal \((e, M; \lambda; l)\)-FHS set with respect to the bound (4), we get

\[
H(A; L) = \left[ \frac{L}{e} \left( \frac{2IeM - (I + 1)H}{(eM - 1)M} \right) \right] = \left[ \frac{\lambda}{ve} \right]
\]

for \( 1 \leq L \leq e \). Obviously, \( \frac{1}{\lambda} < \frac{I}{H} \leq \frac{I}{M} \). Therefore,

\[
\lambda = \left( \frac{I(1 + H - r)}{(I + 1)(H - r)} \right) = \left[ \frac{1}{M} \right]
\]

On one hand, by Lemma 6.7 and equality (9), we have

\[
H(B; L) \leq H(A; \frac{L}{v}) = \left[ \frac{\lambda}{v} \cdot \frac{L}{v} \right] = \left[ \frac{\lambda}{ve} \cdot \lambda \right],
\]

where the last equality holds by the property of ceiling function given in page 71 of [22] since \( \frac{\lambda}{ve} \) is an integer. On the other hand, by Lemma 2.4, we get

\[
H(B; L) \geq \left[ \frac{2Iv}{ve} \left( \frac{M - (I + 1)I}{(ve)^2M - 1} \right) \right] = \left[ \frac{I}{M} \right]
\]

where the last equality holds because of equality (10).

From equalities (11) and (12), we have \( H(B; L) = \left[ \frac{\lambda}{ve} \cdot \lambda \right] \). Therefore, \( B \) is a strictly optimal FHS set with respect to the bound (4). This completes the proof.

Theorem 6.10: Let \( d, m \) be positive integers with \( m \geq 2 \) and let \( q \) be a prime power such that \( d|q - 1 \). Then there is a strictly optimal \((\frac{q-1}{d}; \frac{d}{q}; \frac{q-1}{d}; \frac{d}{q^m-1})\)-FHS set \( S \), and \( H(S; L) = \left[ \frac{d(q - 1)}{q^m - 1} \right] \) for \( 1 \leq L \leq \frac{d(q - 1)}{q^m - 1} \).

By applying Theorem 6.9 with \( \lambda = \frac{q^m - 1}{d} \), \( M = d \) and \( \lambda = \frac{q^m - 1}{d} \) to Theorem 6.10, we can obtain the following corollary.

Corollary 6.11: Let \( d, m \) be positive integers with \( m \geq 1 \) and let \( q \) be a prime power such that \( d|q - 1 \). Then there is a strictly optimal \((\frac{a^{m-1}}{d}; \frac{d}{a^m}; \frac{d}{a^m}; \frac{vq^{-m}}{a^{m-1}}; \frac{vq^{-m}}{a^m})\)-FHS set with respect to the bound (4).

VII. Concluding Remarks

In this paper, a combinatorial characterization of strictly optimal FSHSs and FHS set was obtained. Some new individual FHSs and FHS sets having strictly optimal Hamming correlation with respect to the bounds were presented. It would be nice if more individual FHSs and FHS sets whose partial Hamming correlation achieves the lower bounds could be constructed. It may be possible that some lower bounds on the partial Hamming correlation of FHSs could be improved from the combinatorial characterization.
REFERENCES

[1] T. M. Apostol, Introduction to Analytic Number Theory. New York, NY, USA: Springer-Verlag, 1976.
[2] T. Beth, D. Jungnickel and H. Lenz, Design theory, Cambridge University Press, Cambridge, 1999.
[3] M. Buratti and F. Zuanni, “Explicit constructions for 1-rotational Kirkman triple systems,” Utilitas Math., Vol. 59, pp. 27-30, 2001.
[4] M. Buratti and F. Zuanni, “G-invariantly resolvable Steiner 2-designs arising from 1-rotational difference families,” Bull. Belg. Math. Soc., Vol. 5, pp. 221-235, 1998.
[5] Bluetooth Special Interest Group (SIG), Washington, DC, USA. (2003, Nov.). Specification of the Bluetooth System-Core [Online]. Available: http://www.bluetooth.org
[6] H. Cai, Z. Zhou, Y. Yang, and X. Tang, “A new construction of frequency hopping sequences with optimal partial Hamming correlation,” IEEE Trans. Inf. Theory, vol. 60, no.9, pp. 5782-5790, 2014.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] C. J. Colbourn, Difference matrices, in: The CRC Handbook of Combinatorial Designs, C. J. Colbourn and J. H. Dinitz (Editors), CRC Press, Boca Raton, FL, 2007, 411-419.
[13] 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.
[14] 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.
[15] C. Ding and J. Yin, “Sets of optimal frequency-hopping sequences,” IEEE Trans. Inf. Theory, vol. 54, no. 8, pp. 3741-3745, Aug. 2008.
[16] Y.-C. Eun, S.-Y. Jin, Y.-P. Hong, and H.-Y. Song, “Frequency hopping sequences with optimal partial auto-correlation properties,” IEEE Trans. Inf. Theory, vol. 50, no. 10, pp. 2438-2442, Oct. 2004.
[17] P. Fan, and M. Darnell, Sequence Design for Communications Applications. London, U.K.: Wiley, 1996.
[18] 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.
[19] S. Furino, Y. Miao, and J. Yin, Frames and Resolvable Designs: Uses, Constructions, and Existence. Boca Raton, FL: CRC, 1996.
[20] 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.
[21] 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.
[22] L. Graham, E. Knuth, and O. Patashnik, Concrete mathematics, Addison-Wesley Publishing Company, America, 1994.
[23] M. Jimbo and S. A. Vanstone, “Recursive constructions for resolvable and doubly resolvable 1-rotational Steiner 2-designs,” Utilitas Math., vol. 26, pp. 45-61, 1984.
[24] 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.
[25] E. H. Moore. Tactical Memoranda I-III. Amer. J. Math., vol. 18, pp. 264-303, 1896.
[26] 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.
[27] T. Storer, Cyclotomy and Difference Sets, Chicago, IL: Markham, 1967.
[28] P. Udaya and M. U. Siddiqi, “Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings,” IEEE Trans. Inf. Theory, vol. 44, no. 4, pp. 1492-1503, Jul. 1998.
[29] 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.
[30] 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.
[31] 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.
[32] 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.
[33] 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.
[34] Z. Zhou, X. Tang, X. Niu, and U. Parampalli, “New classes of frequency hopping sequences with optimal partial correlation,” IEEE Trans. Inf. Theory, vol. 58, no. 1, pp. 453-458, Jan. 2012.