MORE CYCLOTOMIC CONSTRUCTIONS OF OPTIMAL
FREQUENCY-HOPPING SEQUENCES

SHANDING XU1,2,3, XIWANG CAO2,4, JIAFU MI2 AND CHUNMING TANG3

1Department of Mathematics and physics, Nanjing Institute of Technology
Nanjing 211167, China

2Department of Mathematics, Nanjing University of Aeronautics and Astronautics
Nanjing 210016, China

3Key Laboratory of Mathematics and Interdisciplinary Sciences
Guangdong Higher Education Institutes
Guangzhou University, Guangzhou 510006, China

4State Key Laboratory of Information Security, Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, China

(Communicated by Sergio R. Lopez-Permouth)

Abstract. In this paper, some general properties of the Zeng-Cai-Tang-Yang cyclotomy are studied. As its applications, two constructions of frequency-hopping sequences (FHSs) and two constructions of FHS sets are presented, where the length of sequences can be any odd integer larger than 3. The FHSs and FHS sets generated by our construction are (near-) optimal with respect to the Lempel–Greenberger bound and Peng–Fan bound, respectively. By choosing appropriate indexes and index sets, a lot of (near-) optimal FHSs and FHS sets can be obtained by our construction. Furthermore, some of them have new parameters which are not covered in the literature.

1. Introduction

For convenience, we introduce the following notation in this paper:

- \( \langle x \rangle_y \): the least nonnegative residue of \( x \) modulo \( y \) for two positive integers \( x \) and \( y \);
- \( \lceil z \rceil \): the least integer greater than or equal to \( z \);
- \( \lfloor z \rfloor \): the largest integer less than or equal to \( z \);
- \( \mathbb{Z}_v \): the residue class ring modulo \( v \) for a positive integer \( v \);
- \( \mathbb{Z}_v^* \): the set consisting of all elements in \( \mathbb{Z}_v \) relatively prime to \( v \);
- \( (\mathbb{Z}_v)^k \): the \( k \)-dimensional space over \( \mathbb{Z}_v \);
- \( a \mid b \): the integer \( a \) divides the integer \( b \).

Let \( F = \{ f_0, f_1, ..., f_{l-1} \} \) be an alphabet of \( l \) available frequencies. A sequence \( X = \{ x_0, x_1, ..., x_{n-1} \} \) is called a frequency-hopping sequence (FHS) of length \( n \) over \( F \) if \( x_t \in F \) for \( 0 \leq t < n \). Given any two sequences \( X = \{ x_0, x_1, ..., x_{n-1} \} \) and \( Y = \{ y_0, y_1, ..., y_{n-1} \} \) of length \( n \) over \( F \), the periodic Hamming correlation \( H_{X,Y} \).
is defined by

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

where \( h[a,b] = 1 \) if \( a = b \) and 0 otherwise, and the addition operation in the subscript is performed modulo \( n \).

The maximum Hamming out-of-phase autocorrelation \( H(X) \) of \( X \) and the maximum Hamming crosscorrelation \( H(X,Y) \) for two distinct FHSs \( X \) and \( Y \) are defined, respectively, by

\[ H(X) = \max_{1 \leq \tau < n} \{ H_{X,X}(\tau) \}; \quad H(X,Y) = \max_{0 \leq \tau < n} \{ H_{X,Y}(\tau) \}. \]

Throughout this paper, let \( (n,l,\lambda) \) denote an FHS \( X \) of length \( n \) over an alphabet \( F \) of size \( l \) with \( \lambda = H(X) \). In this case, we say that the sequence \( X \) has parameters \( (n,l,\lambda) \).

To estimate the measurement of a single FHS \( X \), Lempel and Greenbeberger in 1974 established the first bound of \( H(X) \) as follows.

**Lemma 1.1.** (The Lempel-Greenberger bound)\[20\] For any FHS \( X \) of length \( n \) over an alphabet \( F \) of size \( l \), we have

\[ H(X) \geq \left\lceil \frac{(n-\langle n \rangle l)(n+\langle n \rangle l - l)}{l(n-1)} \right\rceil. \]

The Lempel-Greenberger bound can also be rewritten by the following lemma.

**Lemma 1.2.** [15] For any FHS \( X \) of length \( n \) over an alphabet \( F \) of size \( l \),

\[ H(X) \geq \begin{cases} 0, & \text{if } n = l \\ \lceil n/l \rceil, & \text{otherwise}. \end{cases} \]

An FHS \( X \) is called optimal with respect to the Lempel-Greenberger bound if the Lempel-Greenberger bound in Lemma 1.1 or Lemma 1.2 is met with equality. Furthermore, an \( (n,l,\lambda) \)-FHS \( X \) is said to be near-optimal with respect to the Lempel-Greenberger bound if \( H(X) \) is bigger than the right-hand side of (2) or (3) by one.

Let \( S \) be the set of \( M \) FHSs of length \( n \) over an alphabet \( F \) of size \( l \), the maximum Hamming correlation of \( S \) is defined by

\[ H(S) = \max \left\{ \max_{X \in S} \{ H(X) \}, \max_{X,Y \in S} \{ H(X,Y) \} \right\}. \]

Henceforth, we use \( (n,M,\lambda;l) \) to denote an FHS set \( S \) containing \( M \) FHSs of length \( n \) over an alphabet \( F \) of size \( l \) with \( \lambda = H(S) \), and we also say that the set \( S \) has parameters \( (n,M,\lambda;l) \).

In 2004, Peng and Fan developed the following bound on \( H(S) \) by taking into account the parameter \( M \).

**Lemma 1.3.** (The Peng-Fan bound)\[21\] Let \( S \) be the set of \( M \) FHSs of length \( n \) over an alphabet \( F \) of size \( l \). Then

\[ H(S) \geq \left\lceil \frac{(nM-l)n}{(nM-1)l} \right\rceil. \]

Recently, Xu et al. [23] provided a simplified form of the Peng-Fan bound as follows.
Lemma 1.4. [23] Let $S$ be the set of $M$ FHSs of length $n$ over an alphabet $F$ of size $l$. Then

$H(S) \geq \begin{cases} 
0 & \text{if } M = 1 \text{ and } n = l \\
 a + 1 & \text{if } n(M - l) > a(lnM - 1) \\
 a & \text{otherwise}
\end{cases}$

where $a = \lfloor n/l \rfloor$.

An FHS set $S$ is called optimal with respect to the Peng-Fan bound if one of the Peng-Fan bounds in Lemma 1.3 or Lemma 1.4 is met with equality. Roughly speaking, an FHS set $S$ is called near-optimal with respect to the Peng-Fan bound if $H(S)$ is bigger than the right-hand side of (4) or (5) by one.

In general, optimal FHSs with respect to the Lempel-Greenberger bound and optimal FHS sets with respect to the Peng-Fan bound do not always exist for all lengths and alphabet sizes. However, it is a difficult problem to verify whether an optimal FHS with respect to the Lempel-Greenberger bound or an optimal FHS set with respect to the Peng-Fan bound exists for a given length and a given alphabet size. Under the circumstances, it is also valuable to construct more near-optimal FHSs or FHS sets. So far both algebraic and combinatorial constructions of such sequences were provided (see, for example, [19, 15, 4, 16, 12, 13, 17, 14, 18, 5, 6, 9, 7, 28, 25, 26, 27, 22, 24, 3]). Based on cyclotomies, many optimal FHSs and FHS sets have been constructed. More specifically, the classical cyclotomy over a prime field $\mathbb{F}_p$ was employed to construct optimal FHSs and FHS sets in [4] and [6]. Chung et al. [5] made a slight modification of the construction in [4] and obtained more optimal FHSs. By introducing the discrete logarithm function, Ding and Yin [13] generalized the construction in [4] to a general finite field $\mathbb{F}_{p^r}$. They used the cyclotomy over $\mathbb{F}_{p^r}$ to construct optimal FHSs with very flexible parameters. Later, Han and Yang [18] improved Ding and Yin’s construction from the viewpoint of Sidelnikov sequences. In 2011, Chung and Yang [7] applied $k$-fold cyclotomy to construct optimal FHSs and FHS sets. Later, Zeng et al. [27] presented a construction of optimal FHS sets and two constructions of optimal FHSs based on the Zeng-Cai-Tang-Yang cyclotomy. Ren et al. [22] proposed a construction of optimal FHS sets employing the technique of cyclotomy over $\mathbb{F}_{p^r}$ and the Chinese Remainder Theorem. Recently, Xu et al. [24] presented a construction of a class of optimal FHSs by means of the cyclotomy on $\mathbb{Z}_{p^2}$.

Our purpose in this paper is to design more (near-) optimal FHSs and FHS sets for some cases which are not covered in the literature based on the Zeng-Cai-Tang-Yang cyclotomy. By means of the above cyclotomy and choosing appropriate indexes and index sets, two classes of (near-) optimal FHSs with respect to the Lempel-Greenberger bound, see Constructions A and B, and two classes of (near-) optimal FHS sets with respect to the Peng-Fan bound, see Constructions C and D, are presented, where the length of FHSs can be any odd integer larger than 3. Some parameters of (near-) optimal FHSs and FHS sets constructed in [6], [7], [27] and [8] can be obtained by our construction, see Remark 2 and Remark 3. Most importantly, our constructions can generate some FHSs and FHS sets with new parameters.

The rest of this paper is organized as follows. In Section 2, we introduce the Zeng-Cai-Tang-Yang cyclotomy and discuss its general properties. In Section 3, we give two constructions of FHSs and two constructions of FHS sets. Finally, Section 4 concludes this paper.
2. ZENG-CAI-TANG-YANG CYCLOTOMY AND ITS PROPERTIES

In this section we introduce the definition and some properties of the Zeng-Cai-Tang-Yang cyclotomy [27]. This cyclotomy will be used to construct more (near-) optimal FHSs and FHS sets later.

For a positive integer \(v\), an integer \(a\) in \(\mathbb{Z}_v^*\) is called a primitive root modulo \(v\) if the multiplicative order of \(a\) modulo \(v\) is equal to \(\phi(v)\), where \(\phi(v)\) is the Euler function. It is well known that there exists \(g_0\) such that \(g_0\) is a primitive root modulo \(p^j\) for all \(j \geq 1\) [1], where \(p\) is an odd prime. For a subset \(H\) of \(\mathbb{Z}_v\) and an element \(a\) in \(\mathbb{Z}_v\), define \(a + H\) and \(aH\) as

\[ a + H = \{a + h : h \in H\}, \quad a \cdot H = \{a \cdot h : h \in H\}. \]

A partition \(\{D_0, D_1, \cdots, D_{d-1}\}\) of \(\mathbb{Z}_v^*\) is a family of subsets of \(\mathbb{Z}_v^*\) satisfying

\[ D_i \cap D_j = \emptyset, \text{ for any } i \neq j, \text{ and } \bigcup_{i=0}^{d-1} D_i = \mathbb{Z}_v^*. \]

If \(D_0\) is a multiplicative subgroup of \(\mathbb{Z}_v^*\) and \(D_i = a_iD_0\) with \(a_i \in \mathbb{Z}_v^*\), \(1 \leq i < d\), then \(D_0, D_1, \cdots, D_{d-1}\) are called cyclotomic classes of order \(d\).

Let \(v\) be an odd positive integer. Then \(v\) can be written as

\[ v = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k} \]

for \(k\) odd primes \(p_1, p_2, \cdots, p_k\) with \(2 < p_1 < p_2 < \cdots < p_k\) and \(k\) positive integers \(m_1, m_2, \cdots, m_k\). For any \(i\) with \(1 \leq i \leq k\), let \(g_i\) be a primitive root modulo \(p_i^{m_i}\) for all \(i \geq 1\). And let \(e > 1\) be a common factor of \(p_1 - 1, p_2 - 1, \cdots\) and \(p_k - 1,\) i.e.

\[ p_i - 1 = ef_i \]

for \(k\) positive integers \(f_i\) with \(1 \leq i \leq k\). Obviously, \(f_1 < f_2 < \cdots < f_k\). By the Chinese Remainder Theorem [10], there exists a unique integer \(g_{(v)} \in \mathbb{Z}_v^*\) satisfying

\[ g_{(v)} \equiv g_i^{p_i^{m_i}-1} \pmod{p_i^{m_i}} \]

for all \(1 \leq i \leq k\).

Let \(h_j \in \mathbb{Z}_{v_{(v)}}^*\) satisfying

\[ h_j = \begin{cases} g_j & \text{mod } p_i^{m_i} \\ 1 & \text{mod } p_i^{m_i} \end{cases} \text{ for } i \neq j \text{ and } 1 \leq i \leq k. \]

It turns out in [27] that the multiplicative order of \(g_{(v)}\) modulo \(v\) is \(e\) and thus the set

\[ D_{(v)} = \{g_{(v)}^s : 0 \leq s < e\} \]

is a cyclic subgroup of order \(e\) of \(\mathbb{Z}_{v_{(v)}}^*\).

Let

\[ \Psi_{v_{(v)}} = \mathbb{Z}_{f_1p_1^{m_1}-1} \times \mathbb{Z}_{(p_2-1)p_2^{m_2}-1} \times \cdots \times \mathbb{Z}_{(p_k-1)p_k^{m_k}-1} \]

and for any \(I = (i_1, i_2, \cdots, i_k) \in \Psi_{v_{(v)}}\), define \(D_{I_{(v)}}\) as

\[ D_{I_{(v)}} = H_I^{(v)} D_{(v)} \]

where \(H_{(v)} = (h_1, h_2, \cdots, h_k)\) and \(H_{I_{(v)}} = h_1^{i_1}h_2^{i_2} \cdots h_k^{i_k} \pmod{v}\). It is proved that \(\{D_{I_{(v)}} : I \in \Psi_{v_{(v)}}\}\) is a partition of \(\mathbb{Z}_{v_{(v)}}^*\) in [27]. In accordance with the notation of [11], we call \(D_{I_{(v)}}\), \(I \in \Psi_{v_{(v)}}\), cyclotomic classes of order \(\phi(v)/e\) with respect to \(v\).

This cyclotomy is usually referred to as the Zeng-Cai-Tang-Yang cyclotomy.
For fixed $I$ and $J$ with $I, J \in \Psi_v^{(e)}$, the corresponding cyclotomic numbers of order $\phi(v)/e$ are defined by

$$\left( I, J \right)^{(v)}_{\phi(v)/e} = |(D_I^{(v)} + 1) \cap D_J^{(v)}|.$$  

(8)

In 2013, the Zeng-Cai-Tang-Yang cyclotomic method was used to construct FHSs with optimal Hamming correlation. In the next section, we will further employ it to construct more (near-) optimal FHSs. To this end, we recall some necessary properties of the cyclotomic classes and cyclotomic numbers which were first introduced in [27].

Lemma 2.1. [27] If $a \in D_I^{(v)}$ for some $I \in \Psi_v^{(e)}$, then $aD_J^{(v)} = D_{I+J}^{(v)}$ for any $J \in \Psi_v^{(e)}$.

Lemma 2.2. $-1 \in D^{(v)}$ if $e$ is even and $-1 \in D_E^{(v)}$ if $e$ is odd, where

$$E = \left( \frac{f_1 p_1^m - 1}{2}, \frac{f_2 p_2^m - 1}{2}, \cdots, \frac{f_k p_k^m - 1}{2} \right).$$

Proof. Suppose that $-1 \in D_I^{(v)}$, where $I = (i_1, i_2, \cdots, i_k) \in \Psi_v^{(e)}$, then there exists an integer $s$ with $0 \leq s < e$ such that

$$H_{i(v)}^I g_{i(v)} \equiv -1 \pmod{v}.$$  

(9)

By the Chinese Remainder Theorem, (9) is equivalent to

$$\left\{ \begin{array}{l}
i_1 \equiv \frac{ef_1 p_1^{m_1} - 1}{2} - sf_1 p_1^{m_1} - 1 \pmod{ef_1 p_1^{m_1} - 1} \\
i_j \equiv \frac{(p_j - 1)p_j^{m_j} - 1}{2} - sf_j p_j^{m_j - 1} \pmod{(p_j - 1)p_j^{m_j - 1}} \end{array} \right. \text{ for } 2 \leq j \leq k.$$

By (10) and $I \in \Psi_v^{(e)}$, if $e$ is even, then $i_1 = 0$, $s = \frac{e}{2}$ and hence $i_j = 0$ for any $2 \leq j \leq k$. If $e$ is odd, then $i_1 = \frac{ef_1 p_1^{m_1} - 1}{2}$, $s = \frac{e-1}{2}$ and hence $i_j = \frac{f_j p_j^{m_j} - 1}{2}$ for any $2 \leq j \leq k$. Therefore, we have $-1 \in D^{(v)}$ if $e$ is even and $-1 \in D_E^{(v)}$ otherwise.

Lemma 2.3. [27] For $I = (i_1, i_2, \cdots, i_k) \in \Psi_v^{(e)}$ and $J = (j_1, j_2, \cdots, j_k) \in \Psi_v^{(e)}$, the cyclotomic numbers defined in (8) have the following properties:

1. $\left( I, J \right)^{(v)}_{\phi(v)/e} = \left( -I, J - I \right)^{(v)}_{\phi(v)/e}$ if $e$ is even

2. $\left( I, J \right)^{(v)}_{\phi(v)/e} = \left( J + E, I + E \right)^{(v)}_{\phi(v)/e}$ if $e$ is odd.

Let

$$N_J = \left\{ \frac{jd}{f_d} \pmod{e} : j_d \equiv 0 \pmod{f_d}, 1 \leq d \leq k \right\}.$$  

Then

$$\sum_{I \in \Psi_v^{(e)}} \left( I, J \right)^{(v)}_{\phi(v)/e} = e - |N_J|.$$  

(11)

Lemma 2.4. Let $J = (j_1, j_2, \cdots, j_k) \in \Psi_v^{(e)}$ satisfying $0 \leq j_d < f_1$, $1 \leq d \leq k$. Then we have

$$\sum_{I \in \Psi_v^{(e)}} \left( I + J \right)^{(v)}_{\phi(v)/e} = \sum_{I \in \Psi_v^{(e)}} \left( I, J + I \right)^{(v)}_{\phi(v)/e} = \left\{ \begin{array}{ll}e, & \text{if } 1 \leq j_d < f_1, 1 \leq d \leq k \\\ne - 1, & \text{otherwise.} \end{array} \right.$$
Lemma 2.5. Let

\[ \sum_{I \in \Phi(v)} (I + J, I)_{\phi(v)/e} = \sum_{I \in \Phi(v)} (-I - J, -J)_{\phi(v)/e} = \sum_{I \in \Phi(v)} (I, -J)_{\phi(v)/e}. \]

Applying Lemma 2.3-(2), \( N_J = \{0\} \) if there exists an integer \( d \) with \( 1 \leq d \leq k \) such that \( j_d = 0 \) and \( N_J = 0 \) otherwise due to \( 1 \leq j_d < f_1 \) with \( 1 \leq d \leq k \). Hence, the assertion is proved.

Let \( v_1 > 1 \) be a factor of \( v \) and \( \pi(v_1) \) denote the number of different prime factors of \( v_1 \). Then there exist \( \pi(v_1) \) integers \( t_1, t_2, \ldots, t_{\pi(v_1)} \in \{1, 2, \ldots, k\} \) and \( \pi(v_1) \) integers \( m'_1, m'_2, \ldots, m'_{\pi(v_1)} \) such that

\[ v_1 = \prod_{t=1}^{\pi(v_1)} p_{t_1}^{m'_1} p_{t_2}^{m'_2} \cdots p_{t_{\pi(v_1)}}^{m'_{\pi(v_1)}} \]

where \( 1 \leq m'_i \leq m_i \) for any \( 1 \leq i \leq \pi(v_1) \). It follows again from the Chinese Remainder Theorem that there exists a unique integer \( g(v_1) \in \mathbb{Z}_v^* \) satisfying

\[ g(v_1) \equiv f_{t_i}^{m'_i - 1} \pmod{p_{t_i}^{m_i}} \]

for all \( 1 \leq i \leq \pi(v_1) \), where \( g_t, 1 \leq i \leq \pi(v_1) \), is the primitive root of \( p_{t_i}^{m_i} \) for \( j \geq 1 \). Hence, \( D_{v_1}^{v_1} = \{g_s^{v_1} : 0 \leq s \leq e\} \) is a cyclic group of order \( e \) of \( \mathbb{Z}_v^* \). Define \( D_{v_1}^{v_1} = H_{v_1}^l D_{v_1}^{v_1} \) for \( H_{v_1} = (h_{t_1}, h_{t_2}, \ldots, h_{t_{\pi(v_1)}}) \) and \( l_{v_1} = (t_1, t_2, \ldots, t_{\pi(v_1)}) \in \Phi_e(v_1) \), where each \( h_{t_i}(1 \leq i \leq \pi(v_1)) \) is given by (6) and \( \Psi_e(v_1) \) is similarly defined as \( \Psi_e(v) \) in (7).

Lemma 2.5. [27] For an odd positive integer \( v = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} \), we have

\[ \mathbb{Z}_v \setminus \{0\} = \bigcup_{1 < v_1, v_1 | v} \bigcup_{\Phi_e(v_1)} \bigg( \frac{v}{v_1} D_{v_1}^{v_1} \bigg). \]

The following results will be needed in the sequel.

Lemma 2.6. [2] For any element \( a \in \mathbb{Z}_v \setminus \{0\} \),

\[ \sum_{1 < v_1, v_1 | v, \Phi_e(v_1)} |(\frac{v}{v_1} D_{v_1}^{v_1} + a) \cap \frac{v}{v_1} D_{v_1}^{v_1}| = e - 1. \]

Lemma 2.7. Let \( a \in \mathbb{Z}_v^* \) with \( 1 < v_1, v_1 | v \). For \( J_{v_1} = (j_1, j_2, \ldots, j_{\pi(v_1)}) \in \Phi_e(v_1) \) satisfying \( 1 \leq j_d < f_1, 1 \leq d \leq \pi(v_1) \),

\[ \sum_{I_{v_1} \in \Phi_e(v_1)} |(D_{I_{v_1} + J_{v_1}} + a) \cap D_{I_{v_1}}^{v_1}| = e. \]

Proof. Let \( a^{-1} \in D_{K_{v_1}}^{v_1} \) with \( K_{v_1} \in \Phi_e(v_1) \). Then

\[ \sum_{I_{v_1} \in \Phi_e(v_1)} |(D_{I_{v_1} + J_{v_1}} + a) \cap D_{I_{v_1}}^{v_1}| \]

\[ = \sum_{I_{v_1} \in \Phi_e(v_1)} |(a^{-1} D_{I_{v_1} + J_{v_1}} + 1) \cap a^{-1} D_{I_{v_1}}^{v_1}| \]

\[ = \sum_{I_{v_1} \in \Phi_e(v_1)} |(D_{I_{v_1} + J_{v_1} + K_{v_1}} + 1) \cap D_{I_{v_1} + K_{v_1}}^{v_1}| \]
Otherwise, there exist two integers \( s \) and \( v \) such that \( \gcd(1^s, s-1^s, v) = 1 \).

Now we will distinguish the following two cases to discuss the solutions of (16).

Case 1. \( s_1 = s_2 \). In this case, (16) is equivalent to
\[
\frac{v}{v_1} H_{(v_1)}^{I_{v_1}} g_{(v_1)}^{s_2} (1 - H_{(v_1)}^{I_{v_1}}) \equiv \frac{v}{v_2} b \quad (\text{mod } v).
\]

Then \( \gcd(1 - H_{(v_1)}^{I_{v_1}}, v_1) = 1 \). Otherwise, there exists an integer \( r \) with \( 1 \leq r \leq \pi(v_1) \) such that \( 1 - H_{(v_1)}^{I_{v_1}} \equiv 0 \pmod{p_r} \), which is equivalent to \( j_r \equiv 0 \pmod{e f_r} \), a contradiction to \( 1 \leq j_r < f_1 \). Furthermore, by (6), we have \( \gcd(H_{(v_1)}^{I_{v_1}} g_{(v_1)}^{s_2} (1 - H_{(v_1)}^{I_{v_1}}), v_1) = 1 \). So
\[
\frac{v}{v_1} = \frac{v}{v_1} \gcd(H_{(v_1)}^{I_{v_1}} g_{(v_1)}^{s_2} (1 - H_{(v_1)}^{I_{v_1}}), v_1) = \gcd(H_{(v_1)}^{I_{v_1}} g_{(v_1)}^{s_2} (1 - H_{(v_1)}^{I_{v_1}}), v)
\]
\[
= \gcd(\frac{v}{v_1} b, v) = \frac{v}{v_2}.
\]
Therefore, \( v_1 = v_2 \), which is in contradiction with \( v_1 \neq v_2 \).

Case 2. \( s_1 \neq s_2 \). In that case, the discussion is divided into two subcases.

Case 2-1. There exist two integers \( r_1 \) and \( c_{r_1} \) such that \( p_{c_{r_1}} \mid \frac{v}{v_2} \) and \( p_{c_{r_1}} \mid \frac{v}{v_1} \), where \( 1 \leq r_1 \leq k \) and \( 1 \leq c_{r_1} \leq m_{r_1} \). Obviously, \( p_{r_1} \mid v_1 \). By (16), we have
\[
\frac{v}{v_1} H_{(v_1)}^{I_{v_1}} (g_{(v_1)}^{s_2} - H_{(v_1)}^{I_{v_1}} g_{(v_1)}^{s_2}) \equiv 0 \pmod{p_{c_{r_1}}},
\]
which implies
\begin{equation}
    g_{\pi(\nu_1)}^{r_{\nu_1}'} = H_{\pi(\nu_1)}^{f_{\nu_1}} g_{\pi(\nu_1)}^{s_{\nu_1}} \pmod{p_{\nu_1}}
\end{equation}
according to (6) and $p_{\nu_1}^{r_{\nu_1}} \nmid \frac{\nu}{\nu_1}$. By $p_{\nu_1} \mid \nu_1$, there exists an integer $l$ with $1 \leq l \leq \pi(\nu_1)$ such that $p_{\nu_1} = p_{\nu_1}^{l}$. Then (18) is equivalent to
\begin{equation}
    s_2 f_{\nu_1}^{m_2^{l} - 1} \equiv j_1 + s_1 f_{\nu_1}^{m_1^{l} - 1} \pmod{f_{\nu_1}}.
\end{equation}
Hence, $j_1 = 0$, which is in contradiction with $1 \leq j_1 < f_1$.

**Case 2-2.** There exist two integers $r_2$ and $c_{r_2}$ such that $p_{r_2}^{c_{r_2}} \mid \frac{\nu}{\nu_1}$ and $p_{r_2}^{c_{r_2}} \nmid \frac{\nu}{\nu_2}$, where $1 \leq r_2 \leq k$ and $1 \leq c_{r_2} \leq m_{r_2}$. Obviously, $p_{r_2} \mid \nu_2$. By $p_{r_2}^{c_{r_2}} \mid \frac{\nu}{\nu_2}$ and $p_{r_2}^{c_{r_2}} \nmid \frac{\nu}{\nu_1}$, a contradiction to $b \in \mathbb{Z}_{\nu_2}$. \(\square\)

**Remark 1.** Lemma 2.8 can be viewed as a generalization of Lemma 11 in [27]. In other words, if we choose $I_{\nu_1} = (a_1 - a_2)I_0 \in \Psi_{\nu_1}^{(e)}$, where $1 \leq a_1, a_2 < f_1$ with $a_1 \neq a_2$ and $I_0$ is the $\pi(\nu_1)$-dimensional all-ones vector, then Lemma 2.8 is in accord with Lemma 11 in [27]. Note that Lemma 2.8 is very important to construct more optimal FHS sets in Section 3, see the proofs of Constructions C and D for details.

Let $\nu_1$ be an odd positive integer with $1 < \nu_1, \nu_1|v$. For $I_{\nu_1} = (i_1, i_2, \cdots, i_{\pi(\nu_1)}') \in \Psi^{(e)}_{\nu_1}$ and $J = (j_1, j_2, \cdots, j_{\pi(\nu_1)}') \in (\mathbb{Z}_{f_1})^k$, define the operation \(I_{\nu_1} \oplus J\) as the following:
\begin{equation}
I_{\nu_1} \oplus J = (i_1 + j_1, i_2 + j_2, \cdots, i_{\pi(\nu_1)} + j_{\pi(\nu_1)})
\end{equation}
where the operation $i_1 + j_1$ is performed in the ring $\mathbb{Z}_{f_1^{m_1^{l} - 1}}$ and the operations $i_r + j_r$ ($2 \leq r \leq \pi(\nu_1)$) are performed in the ring $\mathbb{Z}_{(p_{r_1}^{c_{r_1}} - 1)p_{r_2}^{c_{r_2}} - 1}$, respectively.

Obviously, if $\pi(\nu_1) = k$, then $I_{\nu_1} \oplus J = I_{\nu_1} + J$.

The following result follows directly from Lemmas 2.7 and 2.8, which will be useful in this paper.

**Lemma 2.9.** For any element $a \in \mathbb{Z}_v \setminus \{0\}$ and $J = (j_1, j_2, \cdots, j_k)$ with $1 \leq j_d < f_1$, $1 \leq d \leq k$,
\begin{equation}
    \sum_{\begin{subarray}{c}i_{\nu_1} \in \Psi^{(e)}_{\nu_1} \setminus v_1, v_1|v, I_{\nu_1} \end{subarray}} \left|\left(\frac{v}{v_1} D_{I_{\nu_1} \oplus J} - a\right) \cap \frac{v}{v_1} D_{I_{\nu_1}}^{(v_1)} \right| = e.
\end{equation}

3. **More optimal FHSs and FHS sets based on the Zeng-Cai-Tang-Yang cyclotomy**

In this section, we will propose two constructions of FHSs and two constructions of FHS sets based on the Zeng-Cai-Tang-Yang cyclotomy in Section 2. Before presenting our construction, we will give some necessary notation below.

Define a set $A$ as
\begin{equation}
A = \left\{ \frac{v}{v_1} D_{I_{\nu_1}}^{(v_1)} : 1 < \nu_1, \nu_1|v, I_{\nu_1} \in \Psi^{(e)}_{\nu_1} \right\} \cup \{0\}.
\end{equation}

Obviously, $|A| = \frac{v - 1}{e} + 1$ since $|D_{I_{\nu_1}}^{(v_1)}| = e$ for each $1 < \nu_1, \nu_1|v$, and $I_{\nu_1} \in \Psi^{(e)}_{\nu_1}$. Let $\varphi(x)$ be any bijection from $A$ to $\mathbb{Z}_{\frac{v - 1}{e} + 1}$, where $A$ is defined by (22).
Define a set $U$ as
\begin{equation}
U = \{(i_1, i_2, \ldots, i_k) \in (\mathbb{Z}_{f_1})^k : 1 \leq i_d < f_1 \text{ with } 1 \leq d \leq k \text{ and } 2 \nmid i_1\}
\end{equation}
and a set $V$ as
\begin{equation}
V = \{I_i \in (\mathbb{Z}_{f_1})^k : 0 \leq i < f_1, \text{ and any component of } I_i - I_j \text{ with } i \neq j \text{ is not equal to } 0\}.
\end{equation}

It is easy to prove that $|U| = \lfloor f_1/2 \rfloor (f_1 - 1)^{k-1}$ and there exist $(f_1!)^{k-1}$ $V$s satisfying the above definitions. Furthermore, there is the following special case:
\begin{equation}
V = \{i i_0 : 0 \leq i < f_1\}
\end{equation}
where $I_0$ is the $k$-dimensional all-ones vector.

From now on, denote the first component of a vector $I$ by $\Lambda(I)$.

**Construction A**: Let the set $U$ defined as above and $I \in U$. And let $X(t) = \{x(t)_{v-1}^{(I)}\}_{t=0}^{v-1}$ be an FHS of length $v$ over $\mathbb{Z}_{v-1}^*$ defined by
\begin{equation}
x(t) = \begin{cases} 
\phi(0), & \text{if } t = 0 \\
\phi\left( \frac{v}{v_i} D_{I_{v_i}}^{(I)} \right), & \text{if } t \in \frac{v}{v_i} D_{I_{v_i}}^{(I)} \bigcup \frac{v}{v_i} D_{I_{v_i} \oplus I}^{(I)} \text{ and } 2 \mid \Lambda(I_{v_i})
\end{cases}
\end{equation}
where $1 < v_1, v_1 \mid v$, $I_{v_1} \in \Psi^{(c)}$.

**Theorem 3.1.** If $e$ is odd, $p_i \equiv 3 \pmod{4}$ for $1 \leq i \leq k$ and $I \in U$, then the FHS $X(t)$ generated by Construction A is optimal when $v$ is composite or $v = ef + 1$ is a prime with $v \equiv 3 \pmod{4}$ and $4e \leq f + 4$.

**Proof.** The Hamming out-of-phase autocorrelation $H_{X(t)}(\tau)$ of $X(t)$ at shift $\tau \neq 0$ is given by
\begin{align*}
H_{X(t)}(\tau) &= \sum_{1 < v_1, v_1 \mid v, \atop I_{v_1} \in \Psi^{(c)}_{1:2|\Lambda(I_{v_1})}} |\frac{v}{v_1} D_{I_{v_1}}^{(I)} \bigcup \frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)} + \tau| \bigcap \frac{v}{v_1} D_{I_{v_1}}^{(I)} \bigcup \frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)}| \\
&= \sum_{1 < v_1, v_1 \mid v, \atop I_{v_1} \in \Psi^{(c)}_{1:2|\Lambda(I_{v_1})}} |\frac{v}{v_1} D_{I_{v_1}}^{(I)} + \tau| \bigcap \frac{v}{v_1} D_{I_{v_1}}^{(I)} + \sum_{1 < v_1, v_1 \mid v, \atop I_{v_1} \in \Psi^{(c)}_{1:2|\Lambda(I_{v_1})}} |\frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)} + \tau| \bigcap \frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)}| \\
&+ \sum_{1 < v_1, v_1 \mid v, \atop I_{v_1} \in \Psi^{(c)}_{1:2|\Lambda(I_{v_1})}} |\frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)} + \tau| \bigcap \frac{v}{v_1} D_{I_{v_1}}^{(I)}| \\
&= \sum_{1 < v_1, v_1 \mid v, \atop I_{v_1} \in \Psi^{(c)}_{1:2|\Lambda(I_{v_1})}} |\frac{v}{v_1} D_{I_{v_1}}^{(I)} + \tau| \bigcap \frac{v}{v_1} D_{I_{v_1}}^{(I)} + \sum_{1 < v_1, v_1 \mid v, \atop I_{v_1} \in \Psi^{(c)}_{1:2|\Lambda(I_{v_1})}} |\frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)} + \tau| \bigcap \frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)}| \\
&\quad + \sum_{1 < v_1, v_1 \mid v, \atop I_{v_1} \in \Psi^{(c)}_{1:2|\Lambda(I_{v_1})}} |\frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)} + \tau| \bigcap \frac{v}{v_1} D_{I_{v_1}}^{(I)}| \\
&= e - 1 + \sum_{1 < v_1, v_1 \mid v, \atop I_{v_1} \in \Psi^{(c)}_{1:2|\Lambda(I_{v_1})}} |\frac{v}{v_1} D_{I_{v_1}}^{(I)} + \tau| \bigcap \frac{v}{v_1} D_{I_{v_1} \oplus I}^{(I)}|.
\end{align*}
where the last equality is from Lemma 2.6.

Let \( \tau = \frac{v}{v_2} b \) where \( b^{-1} \in D_{J_{v_2}}^{(v_2)} \) with \( J_{v_2} \in \Psi_{v_2}^{(e)} \). By Lemmas 2.1, 2.3 and 2.8, we have

\[
H_{X(I)}(\tau) = e - 1 + \sum_{I_{v_2} \in \Psi_{v_2}^{(e)}, 2 \nmid \Lambda(I_{v_2})} (I_{v_2} + J_{v_2} \oplus I, I_{v_2} + J_{v_2})_{\phi(v_2)}^{(v_2)} / \epsilon
\]

\[
\geq e - 1 + \sum_{I_{v_2} \in \Psi_{v_2}^{(e)}, 2 \nmid \Lambda(I_{v_2})} (I_{v_2} + J_{v_2} \oplus I, I_{v_2} + J_{v_2})_{\phi(v_2)}^{(v_2)} / \epsilon
\]

\[
+ \sum_{I_{v_2} \in \Psi_{v_2}^{(e)}, 2 \nmid \Lambda(I_{v_2})} (I_{v_2} + J_{v_2} + E_{v_2}, I_{v_2} + J_{v_2} + E_{v_2} \oplus I)_{\phi(v_2)}^{(v_2)} / \epsilon
\]

where \(-1 \in D_{E_{v_2}}^{(v_2)} \). Note that \( \frac{f_1}{2} \) is odd for \( 1 \leq i \leq k \) since \( p_i = e f_i + 1 \equiv 3 \pmod{4} \). Consequently, we have

\[
H_{X(I)}(\tau) = e - 1 + \sum_{I_{v_2} \in \Psi_{v_2}^{(e)}} (I_{v_2}, I_{v_2} \oplus I)_{\phi(v_2)}^{(v_2)} / \epsilon = 2e - 1
\]

where the last equality is from Lemma 2.4.

Thus, \( X(I) \) has parameters \((v, \frac{v}{v_2} - 1, 2e - 1)\). Note that \( v = (2e - 1)(\frac{v}{v_2} - 1) + \left( \frac{v}{v_2} - 2\right) \). On one hand, if \( v = (2e - 1) \) is a prime and \( 4e \leq f + 4 \), then \( \frac{v}{v_2} - 2 \geq 0 \). On the other hand, if \( v \) is composite, then \( v \geq p_i^2 \geq (2e + 1)^2 \). Hence, \( \frac{v}{v_2} - 2 \geq 4 \). According to Lemma 1.2, the FHS \( X(I) \) is optimal for any \( I \in U \) with \( 2 \nmid \Lambda(I) \).

Example 3.2. Let \( v = 589 = 19 \times 31, e = 3, f_1 = 6 \) and \( f_2 = 10 \). The set \( A \) defined by (22) can be given as

\[
\{(589)^{0,0}, \ldots, (589)^{1,0}, (589)^{0,29}, \ldots, (589)^{1,1}, \ldots, (19)^{0,129}, \ldots, (589)^{5,0}, \ldots, (589)^{5,1}, \ldots, (589)^{5,29}, \ldots, (31)^{0,129}, \ldots, (31)^{5, 129}, \ldots, (19)^{0,129}, \ldots, (31)^{5, 129}, \ldots, (31)^{5, 129}, \ldots\}
\]

Define \( \varphi \left( \frac{v}{v_2} D_{I_{v_1}}^{(v_1)} \right) = i - 1 \) if \( 2 \mid \Lambda(I_{v_1}) \) and \( \varphi \left( \frac{v}{v_2} D_{I_{v_1}}^{(v_1)} \right) \) is the ith set in (25). Note that \( U = \{(1,1), (1,2), (1,3), (1,4), (1,5), (3,1), (3,2), (3,3), (3,4), (3,5)\} \) defined by (23).

When \( I = (1,1) \) in Construction A, we have

\[
\{X(I)(t)\}^{589}_{t=0} = \{196, 0, 13, 0, 88, 140, 75, 15, 18, 71, 62, 123, 3, 88, 140, 1, 140, 146, 137, 75, 180, 8, 18, 16, 67, 133, 60, 25, 62, 76, 148, 25, 190, 129, 3, 120, 128, 120, 74, 184, 12, 21, 13, 63, 139, 61, 12, 80, 66, 146, 6, 73, 137, 8, 136, ...
\]
is easily calculated by adding $\Delta$ to \\
where $I$ is odd, \\
Therefore, $X^{(I)}$ is an optimal $(589,99,5)$-FHS for any $I \in U$. \hfill $\square$

The first element $\varphi\{\emptyset\}$ of $X^{(I)}$ in Construction A may be replaced by $\varphi(D^{(v)})$. Then, the alphabet size and the maximum Hamming out-of-phase autocorrelation are slightly changed.

**Construction B**: Let the set $U$ defined as above and $I \in U$. And let $Y^{(I)} = \{y^{(I)}_t\}_{t=0}^{v-1}$ be an FHS of length $v$ over $\mathbb{Z}_{\frac{3}{2}}$ defined by

$$x^{(I)}_t = \begin{cases} 
\varphi(D^{(v)}), & \text{if } t = 0 \\
\varphi\left(\frac{v_1}{v_1} D^{(v)}_{I, v_1}\right), & \text{if } t \in \frac{v_1}{v_1} D^{(v)}_{I, v_1} \cup \frac{v_1}{v_1} D^{(v)}_{E, v_1} \cup I \text{ and } 2 \mid \Lambda(I_{v_1}) \end{cases}$$

where $1 < v_1, v_1 \mid v$, $I_{v_1} \in \Psi^{(v)}_{v_1}$.

**Theorem 3.3.** If $e$ is odd, $p_i \equiv 3 \pmod{4}$ for $1 \leq i \leq k$ and $I \in U$, then the FHS $Y^{(I)}$ generated by Construction B is optimal when $v$ is composite or $v = ef + 1$ is a prime with $v \equiv 3 \pmod{4}$ and $I \neq \frac{1}{2}$, otherwise near-optimal.

**Proof.** The Hamming out-of-phase autocorrelation $H_{X^{(I)}}(\tau)$ of $Y^{(I)}$ at shift $\tau \neq 0$ is easily calculated by adding $\Delta$ to $H_{X^{(I)}}(\tau)$ in the proof of Theorem 3.1, where

$$\Delta = |\{\tau, -\tau\} \cap (D^{(v)} \cup D^{(v)}_{I})|.$$

If $v = ef + 1$ is an odd prime with $v \equiv 3 \pmod{4}$, then we have

$$\Delta = \begin{cases} 
1, & \text{if } \tau \in D^{(v)} \cup D^{(v)}_{I} \cup D^{(v)}_{E} \cup D^{(v)}_{E+I} \\
0, & \text{otherwise} \end{cases}$$
for \( I \neq \frac{I}{2} \), and
\[
\Delta = \begin{cases} 
2, & \text{if } \tau \in D^{(v)} \cup D^{(v)}_I \\
0, & \text{otherwise}
\end{cases}
\]
for \( I = \frac{I}{2} \). Therefore, Construction B gives optimal \((v, \frac{v-1}{2e}, 2e)\)-FHSs with respect to the Lempel-Greenberger bound if \( I \neq \frac{I}{2} \), while \( Y^{(I)} \) is a near-optimal \((v, \frac{v-1}{2e}, 2e+1)\)-FHS with respect to the Lempel-Greenberger bound.

If \( v \) is composite, then \( \frac{f_p}{2} \geq 2 \), which implies that \( \tau \) and \(-\tau\) cannot belong to \( D^{(v)} \cup D^{(v)}_I \) at the same time. Thus
\[
\Delta = \begin{cases} 
1, & \text{if } \tau \text{ or } -\tau \in D^{(v)} \cup D^{(v)}_I \\
0, & \text{otherwise.}
\end{cases}
\]

Therefore, any \( Y^{(I)} \) is an optimal \((v, \frac{v-1}{2e}, 2e)\)-FHS with respect to the Lempel-Greenberger bound. 

\[\square\]

**Remark 2.**

(1) In theorems 3.1 and 3.3, the Hamming out-of-phase autocorrelation of \( X^{(I)} \) and \( Y^{(I)} \) are invariant under the selection \( I \in U \), respectively.

(2) If \( v \) is an odd prime with \( v \equiv 3 \pmod{4} \) and \( I = 2a + 1 \), then Construction A and Construction B are exactly the same as the second construction and first construction in [6], respectively.

(3) If \( v = 2^{m_1} 3^{m_2} \cdots p_k \) for \( k \) different odd primes \( p_i \) with \( p_i \equiv 3 \pmod{4} \), then the FHSs generated by Construction B share the same parameters with those generated in Construction B of [7] by applying \( k \)-fold cyclotomy.

(4) If \( v = 2^{m_1} 3^{m_2} \cdots p_k^{m_k} \) for \( k \) different odd primes \( p_i \) with \( p_i \equiv 3 \pmod{4} \) and \( I = yI_0 \), where \( I_0 \) is the \( k \)-dimensional all-ones vector, then Construction B is exactly the same as Construction C in [27]. In other words, compared with Construction C in [27], Construction B in our paper derives more optimal FHSs by choosing appropriate index \( I \) from the set \( U \), which can be seen from Example 3.2.

(5) Compared with Construction C in [27], Construction A slightly changes the alphabet size and derives more optimal FHSs with respect to the Lempel-Greenberger bound which are not covered in the literature.

**Construction C:** Let the set \( V \) defined as above. And let \( S = \{S^{(I)}\}_{I \in V} \) be an FHS set of \( f_1 \) FHSs of length \( v \) over \( \mathbb{Z}_{\frac{v-1}{2e}+1} \) and \( S^{(I)} = \{s_0^{(I)}, s_1^{(I)}, \cdots, s_{v-1}^{(I)}\} \) with
\[
s_t^{(I)} = \begin{cases} 
\varphi(\{0\}), & \text{if } t = 0 \\
\varphi(\frac{v}{v_1} D_{I_0}^{(v_1)}), & \text{if } t \in \frac{v}{v_1} D_{I_0}^{(v_1)} \oplus I 
\end{cases}
\]
where \( 1 < v_1, v_1|v, I_0 \in \Psi^{(v)}_{v_1} \).

**Theorem 3.4.** Let the set \( V \) defined as above and \( f_1 > 1 \). Then the FHS set \( S \) has the following properties:

(1) The family size is \( M = f_1 \), the sequence length \( n = v \), and \( |F| = \frac{v-1}{2e} + 1 \);

(2) The Hamming out-of-phase autocorrelation of \( S^{(I)} \in S \) for any \( I \in V \) is given by

\[
H_{S^{(I)}}(\tau) = \frac{1}{e} - 1;
\]

(3) The Hamming crosscorrelation between any two distinct FHSs \( S^{(I)}, S^{(J)} \in S \) with \( I, J \in V \) is given by

\[
H_{S^{(I)}, S^{(J)}}(\tau) = \begin{cases} 
1, & \text{if } \tau = 0 \\
\frac{1}{e}, & \text{otherwise.}
\end{cases}
\]
Proof. (1) It is clear.

(2) The Hamming out-of-phase autocorrelation of $S^{(I)}$ at shift $\tau$ with $\tau \neq 0$ is

$$H_{S^{(I)}}(\tau) = \sum_{1 < v_1, v_1, \tau, \nu \in \mathbb{Z}_e} \left| \left( \frac{v}{v_1} D_{I_1}^{(v_1)} + \tau \right) \cap \left( \frac{v}{v_1} D_{I_1}^{(v_1)} \right) \right| = e - 1$$

where the last equality comes from Lemma 2.6.

(3) For any FHSs $S^{(I)}, S^{(J)} \in S$ with $I \neq J$ and $I, J \in V$, their Hamming crosscorrelation at shift $\tau \neq 0$ is given by

$$H_{S^{(I)}, S^{(J)}}(\tau) = \sum_{1 < v_1, v_1, \tau, \nu \in \mathbb{Z}_e} \left| \left( \frac{v}{v_1} D_{I_1}^{(v_1)} + \tau \right) \cap \left( \frac{v}{v_1} D_{I_1}^{(v_1)} \right) \right| = e$$

where the last equality comes from the definition of $V$ and Lemma 2.9. If $\tau = 0$, then it is obvious that $H_{S^{(I)}, S^{(J)}}(\tau) = 1$. \hfill \Box

Corollary 3.5. If $f_1 > 1$, then the FHS set $S$ generated by Construction C is optimal with respect to the Peng-Fan bound when $v$ is composite or $v = ef + 1$ is prime with $f \geq e > 1$.

Proof. If $f_1 > 1$ and $v$ is composite, by Theorem 3.4, then the set $S$ has parameters $(v, f_1, e; \frac{v-1}{e} + 1)$. Note that $a = \lfloor \frac{v}{e} \rfloor = \lfloor \frac{v-1}{e} \rfloor = e - 1$ and

$$n(nM - l) - al(nM - l) = v(vf_1 - \frac{v-1}{e} - 1) = (v - 1)(\frac{v-1}{e} + 1)(vf_1 - 1) = (f_1 - 1)v^2 - f_1 - 1 - (e - 2)(fv_1 - 1)$$

Considering the facts $p_1 < p_2 < \cdots < p_k$, $p_r = ef_r + 1$ for $1 \leq r \leq k$ and $v$ is composite, we have $v \geq p_1^2$, which results in

$$(f_1 - 1)v^2 - f_1 - 1 - e(e - 2)(fv_1 - 1) > (f_1 - 1)v^2 - ep_1 + p_1 v \geq ((f_1 - 1)p_1 - e + 1)p_1 v > 0.$$  

Therefore, by Lemma 1.4, the FHS set $S$ with parameters $(v, f_1, e; \frac{v-1}{e} + 1)$ is optimal with respect to the Peng-Fan bound when $v$ is composite.

With a slight modification of the above proof, we can get the proof when $v = ef + 1$ is prime with $f \geq e > 1$. The proof is complete. \hfill \Box

Corollary 3.6. Each FHS in the $S$ generated by Construction C is optimal with respect to the Lempel-Greenberger bound when $v$ is composite or $v = ef + 1$ is a prime with $f \geq e > 1$.

Proof. We only give the proof when $v$ is a prime with $f \geq e > 1$ since the other is completely parallel. When $v$ is a prime, each FHS generated by our construction has parameters $(v, f + 1, e - 1)$ from the proof of Theorem 3.4. According to Lemma 1.2, the fact $v = (e - 1)(f + 1) + f + 2 - e$ implies that each FHS is optimal with respect to the Lempel-Greenberger bound. \hfill \Box
Example 3.7. Let $v = 175 = 5^2 \times 7$, $e = 2$, $f_1 = 2$ and $f_2 = 3$. The set $A$ defined by (22) can be given as

$$D(\tau_0), D(\tau_1), \ldots, D(\tau_{175}), D(\tau_{176}), \ldots, D(\tau_{1775}), D(\tau_{1776}), \ldots, D(\tau_{17875})$$

$$D(\tau_{1776}), \ldots, D(\tau_{17875}), 5D(\tau_{17876}), \ldots, 5D(\tau_{178775}), 5D(\tau_{178776}), \ldots, 5D(\tau_{1787875}), 7D(\tau_{1787876})$$

$$\ldots, 7D(\tau_{17878775}), 25D(\tau_{17878776}), 25D(\tau_{17878777}), 25D(\tau_{17878778}), 35D(\tau_{17878779}), 35D(\tau_{17878780}), \{0\}.$$ 

Define $\varphi(D(\tau_i)) = i - 1$ if $\varphi(D(\tau_i))$ is the $i$th set in (26), $1 \leq i \leq 87$, and $\varphi(\{0\}) = 87$. By (24), $V = \{(0,0), (1,1)\}$ or $V = \{(0,1), (1,0)\}$. If $V = \{(0,0), (1,1)\}$, then it is in accord with Example 1 in [27]. If $V = \{(0,1), (1,0)\}$, then the FHS set $S = \{S^{(0,1)}, S^{(1,0)}\}$ generated by Construction B is the following.

When $I = (0,1)$ in Construction C, we have

$$S(I)(t) = \{87, 5, 19, 6, 39, 65, 26, 72, 59, 13, 70, 51, 46, 47, 75, 66, 16, 57, 33,$$

$$25, 60, 73, 8, 22, 3, 82, 4, 20, 78, 41, 62, 24, 30, 58, 14, 85, 53, 43, 45,$$

$$48, 71, 17, 76, 35, 28, 64, 36, 7, 23, 77, 84, 1, 18, 9, 40, 63, 81, 32, 55,$$

$$12, 67, 52, 44, 74, 50, 68, 15, 54, 34, 29, 86, 38, 10, 21, 0, 83, 2, 80, 11,$$

$$37, 61, 27, 31, 56, 79, 69, 49, 42, 42, 49, 69, 79, 56, 31, 27, 61, 37, 11,$$

$$80, 2, 83, 0, 21, 10, 38, 86, 29, 34, 54, 15, 68, 50, 74, 44, 52, 67, 12, 55,$$

$$32, 81, 63, 40, 9, 18, 1, 84, 77, 23, 7, 36, 64, 28, 35, 76, 17, 71, 48, 45,$$

$$43, 53, 85, 14, 58, 30, 24, 62, 41, 78, 20, 4, 82, 3, 22, 8, 73, 60, 25, 33,$$

$$57, 16, 80, 57, 45, 66, 51, 70, 13, 59, 72, 26, 65, 39, 6, 19, 5\}.$$ 

When $J = (1,0)$ in Construction C, we have

$$S(J)(t) = \{87, 54, 14, 1, 34, 66, 21, 81, 48, 8, 65, 46, 41, 36, 74, 61, 11, 52, 28, 20,$$

$$67, 72, 3, 17, 58, 84, 59, 15, 77, 30, 69, 19, 25, 53, 9, 86, 42, 38, 40, 43,$$

$$60, 6, 75, 24, 23, 71, 31, 2, 12, 76, 83, 56, 13, 4, 35, 70, 80, 27, 50, 7, 62,$$

$$47, 39, 73, 45, 63, 10, 49, 29, 18, 85, 33, 5, 16, 55, 82, 57, 79, 0, 32, 68,$$

$$22, 26, 51, 78, 64, 44, 37, 37, 44, 64, 78, 51, 26, 22, 68, 32, 0, 79, 57, 82,$$

$$55, 16, 5, 33, 85, 18, 29, 49, 10, 63, 45, 73, 39, 47, 62, 7, 50, 27, 80, 70,$$

$$35, 4, 13, 56, 83, 76, 12, 2, 31, 71, 23, 24, 75, 6, 60, 43, 40, 38, 42, 86, 9,$$

$$53, 25, 19, 69, 30, 77, 15, 59, 84, 58, 17, 3, 72, 67, 20, 28, 52, 11, 61, 74,$$

$$36, 41, 46, 65, 8, 48, 81, 21, 66, 34, 1, 14, 54\}.$$ 

Then we have

$$H_{S(I)}(\tau) = H_{S(J)}(\tau) = \begin{cases} 175, & \text{if } \tau = 0 \\ 1, & \text{otherwise} \end{cases}$$

and

$$H_{S(I),S(J)}(\tau) = \begin{cases} 1, & \text{if } \tau = 0 \\ 2, & \text{otherwise} \end{cases}.$$ 

Therefore, $S$ is an optimal FHS set with parameters $(175, 2, 2; 88)$ and each FHS in $S$ is an optimal FHS with parameters $(175, 88, 1)$.
The first element \( \varphi(\{0\}) \) of \( S(I) \) in Construction C may be replaced by \( \varphi(D^{(e)}) \). Then, the alphabet size and the maximum Hamming correlation value are slightly changed.

**Construction D**: Let the set \( V \) defined as above. And let \( Z = \{Z(i)\}_{I \in V} \) be an FHS set of \( f_1 \) FHSs of length \( v \) over \( \mathbb{Z}_{v-1} \) and \( Z(i) = \{z_0^{(i)}, z_1^{(i)}, \ldots, z_{v-1}^{(i)}\} \) with

\[
z_t^{(i)} = \begin{cases} \psi(D^{(v)}), & \text{if } t = 0 \\ \psi(\frac{v}{v_1}D^{(v)}_{l,v_1}), & \text{if } t \in \frac{v}{v_1}D^{(v)}_{l,v_1} \end{cases}
\]

where \( 1 < v_1, v_1 | v, I_{v_1} \in \Psi^{(e)} \).

**Theorem 3.8.** Let \( E \) be defined as Lemma 2.1 and the set \( V \) defined as above. Then the FHS set \( Z \) has the following properties:

1. The family size is \( M = f_1 \), the sequence length \( n = v \), and \( |F| = \frac{v-1}{e} \);
2. The Hamming out-of-phase autocorrelation of \( \psi(Z(I)) \in Z \) for any \( I \in V \) is given by
   
   \[
   H_{Z(I)}(\tau) = \begin{cases} e, & \text{if } \tau \in D_{I+1}^{(v)} \cup D_{I+1}^{(v)} \\ e-1, & \text{otherwise.} \end{cases}
   \]

3. When \( e \) is even,
   
   \[
   H_{Z(I)}(\tau) = \begin{cases} e+1, & \text{if } \tau \in D_{I}^{(v)} \\ e-1, & \text{otherwise.} \end{cases}
   \]

3. The Hamming crosscorrelation between any two distinct FHSs \( Z(I), Z(J) \in Z \) with \( I, J \in V \) is given by
   
   \[
   H_{Z(I), Z(J)}(\tau) = \begin{cases} 1, & \text{if } \tau = 0 \\ e+2, & \text{if } I + \frac{\tau}{2} \equiv J \pmod{f} \text{ and } \tau \in D_{I}^{(v)} \\ e+1, & \text{if } I + \frac{\tau}{2} \not\equiv J \pmod{f} \text{ and } \tau \in D_{I}^{(v)} \cup D_{J}^{(v)} \\ e, & \text{otherwise.} \end{cases}
   \]

3. When \( \psi \) is odd and \( e \) is even,
   
   \[
   H_{Z(I), Z(J)}(\tau) = \begin{cases} 1, & \text{if } \tau = 0 \\ e+1, & \text{if } \tau \in D_{I+1}^{(v)} \cup D_{J}^{(v)} \\ e, & \text{otherwise.} \end{cases}
   \]

3. When \( \psi \) is even and \( e \) is odd,
   
   \[
   H_{Z(I), Z(J)}(\tau) = \begin{cases} 1, & \text{if } \tau = 0 \\ e+1, & \text{if } \tau \in D_{I+1}^{(v)} \cup D_{J}^{(v)} \\ e, & \text{otherwise.} \end{cases}
   \]

**Proof.**

1. It is clear.
2. The Hamming out-of-phase autocorrelation of \( Z(I) \) at shift \( \tau \) with \( \tau \neq 0 \) is

\[
H_{Z(I)}(\tau) = \sum_{1 < v_1, v_1 \mid v, I_{v_1} \in \Psi^{(e)}} |(\psi(\frac{v}{v_1}D_{l,v_1}^{(v)} + \tau) \cap \frac{v}{v_1}D_{l,v_1}^{(v)}| + |\{\tau, -\tau\} \cap D_{I}^{(v)}|
\]
where the last equality comes from Lemma 2.6. Then by Lemma 2.2, the results follow.

(3) For any FHSs $Z^{(I)}, Z^{(J)} \in Z$ with $I \neq J$ and $I, J \in V$, their Hamming crosscorrelation at shift $\tau$ with $\tau \neq 0$ is given by

$$H_{Z^{(I)}, Z^{(J)}}(\tau) = \sum_{1 < v_1, v_2 \mid v, l_{v_1} \in \Psi^{(v)}} |(\frac{v}{v_1} D_{I_{v_1} \oplus I + \tau}^{(v_1)}) \cap \frac{v}{v_1} D_{I_{v_1} \oplus J}^{(v_1)}| + |\{\tau\} \cap \{0\}|$$

$$= e + |\{\tau\} \cap \{0\}| + |\{\tau\} \cap D_{I}^{(v)}| + |\{-\tau\} \cap D_{I}^{(v)}|$$

where the last equality comes from the definition of $V$ and Lemma 2.9. Combining Lemma 2.2, the statements follow.

**Corollary 3.9.** If $f_1 > 1$, then the FHS set $Z$ generated by Construction $D$ is near-optimal with respect to the Peng-Fan bound when $v$ is composite or $v = ef + 1$ is prime with $2 \nmid e$, and optimal with respect to the Peng-Fan bound when $v = ef + 1$ is prime with $2 \mid e$.

**Proof.** If $f_1 > 1$ and $v$ is composite, by Theorem 3.8, then the set $Z$ has parameters $(v, f_1, e + 1; \frac{v-1}{e})$. Note that $a = \lfloor \frac{n}{e} \rfloor = e$ and

$$n(nM - l) - al(nM - 1) = v(vf_1 - \frac{v - 1}{e}) - (v - 1)(vf_1 - 1) = v + vf_1 - \frac{v - 1}{e} - 1.$$

Considering the facts $p_1 < p_2 < \cdots < p_k$, $p_r = ef_r + 1$ for $1 \leq r \leq k$ and $v$ is composite, we have $v \geq p_1^2$, which results in

$$v + vf_1 - \frac{v - 1}{e} - 1 \leq v + vf_1 - \frac{v - 1}{e} - 1 = v + vf_1 - vf_1(p_1 + 1) - 1 = v - vf_1(p_1 - 1) < 0.$$

Therefore, by Lemma 1.4, the FHS set $Z$ with parameters $(v, f_1, e + 1; \frac{v-1}{e})$ is near-optimal with respect to the Peng-Fan bound when $v$ is composite.

With a slight modification of the above proof, we can get the proof when $v = ef + 1$ is prime. The proof is complete.

**Corollary 3.10.** Each FHS in the $Z$ generated by Construction $D$ is optimal with respect to the Lempel-Greenberger bound when $e$ is odd, and near-optimal with respect to the Lempel-Greenberger bound when $e$ is even.

**Proof.** We only give the proof when $e$ is odd since the other is completely parallel.

When $e$ is odd, each FHS generated by our construction has parameters $(v, \frac{v - 1}{e}, e)$ from the proof of Theorem 3.8. According to Lemma 1.2, the fact $v = e \frac{v - 1}{e} + 1$ implies that each FHS is optimal with respect to the Lempel-Greenberger bound.

**Example 3.11.** Let $v = 175 = 5^2 \times 7$, $e = 2$, $f_1 = 2$ and $f_2 = 3$. The set $A$ is defined by (26). Define $\psi_D^{(v_1)} = i - 1$ if $\frac{v}{v_1} D_{I_{v_1}}^{(v_1)}$ is the $i$th set in (26),
1 \leq i \leq 87$, and $\psi(\{0\}) = 0$. If $V = \{(0,1), (1,0)\}$ defined by (24), then the FHS set $Z = \{Z(I), Z(J)\}$, where $I = (0,1)$, $J = (1,0)$. By Magma calculation, we have

\[
H_{Z(I)}(\tau) = \begin{cases} 
175, & \text{if } \tau = 0 \\
3, & \text{if } \tau = 74, 101 \\
2, & \text{otherwise}
\end{cases}
\]

\[
H_{Z(J)}(\tau) = \begin{cases} 
175, & \text{if } \tau = 0 \\
3, & \text{if } \tau = 78, 97 \\
2, & \text{otherwise}
\end{cases}
\]

and

\[
H_{Z(I), Z(J)}(\tau) = \begin{cases} 
1, & \text{if } \tau = 0 \\
3, & \text{if } \tau = 74, 78, 97, 101 \\
2, & \text{otherwise}
\end{cases}
\]

Therefore, $Z$ is a near-optimal FHS set with parameters $(175, 2, 3; 87)$ and each FHS in $Z$ is a near-optimal FHS with parameters $(175, 87, 3)$.

**Remark 3.**
(1) In theorems 3.4 and 3.8, the Hamming correlation of the FHS sets $S$ and $Z$ are invariant under the selection of the index set $V$, respectively.
(2) When $v$ is an odd prime, the FHS sets generated by Construction D share the same parameters with those generated in Construction A of [8] by applying the classical cyclotomy. Furthermore, if $v = p_1p_2 \cdots p_k$ for $k$ different odd primes $p_i$, then the FHS sets generated by Construction D share the same parameters with those generated in Construction $A_1$ of [7] by applying $k$-fold cyclotomy. Yet, the length of the FHSs obtained by our construction can be any odd integer larger than 3.
(3) Based on the Zeng-Cai-Tang-Yang cyclotomy, Zeng et al. [27] obtained a class of optimal FHSs with parameters $(v, v^{-1}, e)$. Obviously, the FHS $S(i\vec{0})$ in our construction is equivalent to the FHS $W$ constructed in Construction B of [27], where $\vec{0}$ is the $k$-dimensional all-zeros vector.
(4) If $v = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k}$ for $k$ different odd primes $p_i$ and $V = \{iI_0 : 0 \leq i < f_1\}$, where $I_0$ is the $k$-dimensional all-ones vector, then Construction C is exactly the same as Construction A in [27]. In other words, compared with Construction A in [27], Construction C in our paper derives more optimal FHS sets by choosing appropriate index set $V$.
(5) Compared with Construction A in [27], Construction D slightly changes the alphabet size and obtained a lot of (near-) optimal FHSs and FHS sets which are not covered in the literature by choosing the appropriate set $V$.

### 4. Concluding remarks

Based on the Zeng-Cai-Tang-Yang cyclotomy, we present two constructions of FHSs and two constructions of FHS sets, where the length of sequences can be any odd integer larger than 3. The results show that the FHSs and FHS sets generated by our construction are optimal and (near-) optimal with respect to the Lempel–Greenberger bound and Peng–Fan bound, respectively. By choosing appropriate indexes and index sets, many new (near-) optimal FHSs and FHS sets can be obtained by our construction.
ACKNOWLEDGMENT

This work was partially supported by the National Natural Science Foundation of China (Grant No. 11771007, 11601177 and 61572027). The first author was also supported by the Open Project Program of Key Laboratory of Mathematics and Interdisciplinary Sciences of Guangdong Higher Education Institutes, Guangzhou University (Grant No. GDSXJCKXX2016-07) and the Funding of Nanjing Institute of Technology (Grant No. CKJB201606 and QKJ201804).

REFERENCES

[1] T. M. Apostol, Introduction to Analytic Number Theory, New York, NY, USA: Springer-Verlag, 1976.
[2] H. Cai, X. Zeng, T. Helleseth, X. Tang and Y. Yang, A new construction of zero-difference balanced functions and its applications, IEEE Trans. Inf. Theory, 59 (2013), 5008–5015.
[3] B. Chen, L. Lin, S. Ling and H. Liu, Three new classes of optimal frequency-hopping sequence sets, Des., Codes and Cryptogr., 83 (2017), 219–232.
[4] W. Chu and C. Colbourn, Optimal frequency-hopping sequences via cyclotomy, IEEE Trans. Inf. Theory, 51 (2005), 1139–1141.
[5] J. Chung, Y. Han and K. Yang, New classes of optimal frequency-hopping sequences by interleaving techniques, IEEE Trans. Inf. Theory, 55 (2009), 5783–5791.
[6] J. Chung and K. Yang, Optimal frequency-hopping sequences with new parameters, IEEE Trans. Inf. Theory, 56 (2010), 1685–1693.
[7] J. Chung and K. Yang, k-fold cyclotomy and its application to frequency-hopping sequences, IEEE Trans. Inf. Theory, 57 (2011), 2306–2317.
[8] J. Chung and K. Yang, New frequency-hopping sequence sets with optimal average and good maximum Hamming correlations, IET Commun., 6 (2012), 2048–2053.
[9] C. Ding, Y. Yang and X. Tang, Optimal sets of frequency hopping sequences from linear cyclic codes, IEEE Trans. Inf. Theory, 56 (2010), 3605–3612.
[10] C. Ding, D. Y. Pei and A. Salomaa, Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography, Singapore: World Scientific, 1996.
[11] C. Ding and T. Helleseth, New generalized cyclotomy and its applications, Finite Fields Appl., 4 (1998), 140–166.
[12] C. Ding, M. Miosio and J. Yuan, Algebraic constructions of optimal frequency hopping sequences, IEEE Trans. Inf. Theory, 53 (2007), 2606–2610.
[13] C. Ding and J. Yin, Sets of optimal frequency hopping sequences, IEEE Trans. Inf. Theory, 54 (2008), 3741–3745.
[14] 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, 55 (2009), 3297–3304.
[15] R. Fuji-Hara, Y. Miao and M. Mishima, Optimal frequency hopping sequences: A combinatorial approach, IEEE Trans. Inf. Theory, 50 (2004), 2408–2420.
[16] G. Ge, R. Fuji-Hara and Y. Miao, Further combinatorial constructions for optimal frequency-hopping sequences, J. Combinat. Theory A, 113 (2006), 1699–1718.
[17] G. Ge, Y. Miao and Z. Yao, Optimal frequency hopping sequences: Auto- and cross-correlation properties, IEEE Trans. Inf. Theory, 55 (2009), 867–879.
[18] Y. Han and K. Yang, On the Sidelnikov sequences as frequency-hopping sequences, IEEE Trans. Inf. Theory, 55 (2009), 4279–4285.
[19] P. Kumar, Frequency-hopping code sequence designs having large linear span, IEEE Trans. Inf. Theory, 34 (1988), 146–151.
[20] A. Lempel and H. Greenberger, Families of sequences with optimal Hamming correlation properties, IEEE Trans. Inf. Theory, 20 (1974), 90–94.
[21] D. Peng and P. Fan, Lower bounds on the Hamming auto-and cross-correlations of frequency-hopping sequences, IEEE Trans. Inf. Theory, 50 (2004), 2149–2154.
[22] W. Ren, F. Fu and Z. Zhou, New sets of frequency-hopping sequences with optimal Hamming correlation, Des. Codes Cryptogr., 72 (2014), 423–434.
[23] S. Xu, X. Cao and G. Xu, Recursive construction of optimal frequency-hopping sequences sets, IET Commun., 10 (2016), 1080–1086.
[24] S. Xu, X. Cao and G. Xu, Optimal frequency-hopping sequence sets based on cyclotomy, Int. J. Found. Comput. S., 27 (2016), 443–462.
[25] Y. Yang, X. Tang, U. Parampalli and D. Peng, New bound on frequency hopping sequence sets and its optimal constructions, IEEE Trans. Inf. Theory, 57 (2011), 7605–7613.
[26] X. Zeng, H. Cai, X. Tang and Y. Yang, A class of optimal frequency hopping sequences with new parameters, IEEE Trans. Inf. Theory, 58 (2012), 4899–4907.
[27] X. Zeng, H. Cai, X. Tang and Y. Yang, Optimal frequency hopping sequences of odd length, IEEE Trans. Inf. Theory, 59 (2013), 3237–3248.
[28] Z. Zhou, X. Tang, D. Peng and U. Parampalli, New constructions for optimal sets of frequency-hopping sequences, IEEE Trans. Inf. Theory, 57 (2011), 3831–3840.

Received for publication May 2017.

E-mail address: sdxzx11@163.com
E-mail address: xwcao@nuaa.edu.cn
E-mail address: mijiafu@163.com
E-mail address: ctang@gzhu.edu.cn