New Families of Optimal Frequency-Hopping Sequences of Composite Lengths

Jin-Ho Chung, Guang Gong, and Kyeongcheol Yang

Abstract

Frequency-hopping sequences (FHSs) are employed to mitigate the interferences caused by the hits of frequencies in frequency-hopping spread spectrum systems. In this paper, we present two new constructions for FHS sets. We first give a new construction for FHS sets of length nN for two positive integers n and N with $\gcd(n, N) = 1$. We then present another construction for FHS sets of length $(q-1)N$, where q is a prime power satisfying $\gcd(q-1, N) = 1$. By these two constructions, we obtain infinitely many new optimal FHS sets with respect to the Peng-Fan bound as well as new optimal FHSs with respect to the Lempel-Greenberger bound, which have length nN or $n(q-1)N$. As a result, a great deal of flexibility may be provided in the choice of FHS sets for a given frequency-hopping spread spectrum system.

Index Terms

Frequency-hopping spread spectrum, Frequency-hopping sequences, Hamming correlation, Lempel-Greenberger bound, Peng-Fan bound.

This work was supported in part by the year of 2013 Research Fund of the Ulsan National Institute of Science and Technology, in part by NSERC Discovery Grant and ORF-RE Grant, and in part by the National Research Foundation (NRF) of Korea under Grant 2011-0017396 funded by the Ministry of Science, ICT and Future Planning (MSIP) of the Korean Government.

J.-H. Chung is now with the Department of Electrical and Computer Engineering, University of Waterloo, on sabbatical leave from the School of Electrical and Computer Engineering, Ulsan National Institute of Science and Technology (UNIST), Ulsan Metropolitan City 689-798, Republic of Korea (e-mail: jinho@unist.ac.kr).

G. Gong is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1 Canada (e-mail: ggong@uwaterloo.ca).

K. Yang is with the Department of Electrical Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Gyungbuk 790-784, Korea (email: kcyang@postech.ac.kr).

I. Introduction

Frequency-hopping spread spectrum techniques have been widely used in ultrawideband communications, military applications, Wi-Fi, Bluetooth, and so on [1–6]. A frequency-hopping sequence (FHS) represents an ordered list of the frequencies assigned to a user at each time slot. In communication systems based on frequency-hopping, it is necessary to properly select an FHS or an FHS set in order to mitigate the interference caused by the hits of frequencies. For example, multiple access systems require FHS sets with low correlation and large size, while some systems such as Bluetooth need a single FHS with good autocorrelation. For these reasons, design of good FHS sets or FHSs has been a major issue in frequency-hopping spread spectrum systems.

The main purpose of FHS design is to find an FHS or an FHS set which is optimal under a given condition. In general, the optimality of an FHS set is measured by the Peng-Fan bound [7], whereas that of a single FHS is by the Lempel-Greenberger bound [8]. There are several algebraic or combinatorial constructions for optimal FHSs or FHS sets in the literature [8–27]. Moreover, some generic extension methods have been proposed [28,29], which generate several new families of optimal FHS sets. In the case that no mathematical structure which gives an optimal FHS set with some desired parameters has been found, extension of a given FHS set may be a good alternative to obtain new FHS sets with such parameters.

In this paper, we present two new extension methods for an FHS set, which increase its length and alphabet size, but preserve its maximum Hamming correlation. We first give a new construction for FHS sets of length nN for two positive integers n and N with $\gcd(n, N) = 1$. We then present another construction for FHS sets of length $(q-1)N$, where q is a prime power with $\gcd(q-1, N) = 1$. The two construction methods can be applied to any existing FHS sets or FHSs satisfying some constraints, as summarized in Table I. Moreover, by properly combining the two methods, it is possible to obtain infinitely many new optimal FHS sets with respect to the Peng-Fan bound as well as new optimal FHSs with respect to the Lempel-Greenberger bound, which have length nN or $n(q-1)N$. As a result, a great deal of flexibility may be provided in the choice of FHSs or FHS sets for a given frequency-hopping spread spectrum system.

The outline of the paper is as follows. In Section II, we give some preliminaries to FHSs. We give a new construction of FHS sets with length nN and provide some new optimal FHS sets and optimal FHSs as its example in Section III. We present a new construction of FHS sets with length $(q-1)N$ and obtain optimal FHS sets and optimal FHSs with new parameters in Section IV. Finally, we give some concluding remarks in Section V.

II. Preliminaries

Throughout this paper, the following notation will be used:

- $\langle x \rangle_y$: the least nonnegative residue of x modulo y for an integer x and a positive integer y;
- $\lfloor z \rfloor$: the largest integer less than or equal to z;
- $\lceil z \rceil$: the least integer greater than or equal to z;
- $\mathbb{Z}_n$: the ring of integers modulo n for a positive integer n.

Let $\mathcal{F} \triangleq \{f_0, f_1, \ldots, f_{M-1}\}$ be the set of available frequencies in a frequency-hopping multiple-access system. A sequence $X \triangleq \{X(t)\}_{t=0}^{N-1}$ is called an FHS of length N over $\mathcal{F}$ if $X(t) \in \mathcal{F}$ for all $0 \le t \le N-1$. For $f \in \mathcal{F}$, the number of occurrences of f within X, denoted by $N_X(f)$, can be written as

$$N_X(f) = |\{t : X(t) = f, \ 0 \le t \le N-1\}|.$$

For two FHSs X and Y of length N over $\mathcal{F}$, the (*periodic*) *Hamming correlation* between X and Y is defined as

$$H_{X,Y}(\tau) = \sum_{t=0}^{N-1} h[X(t), Y(\langle t+\tau \rangle_N)], \qquad 0 \le \tau \le N-1$$

where

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

If $X = Y$, it is called the *Hamming autocorrelation* of X, and is denoted by $H_X(\tau)$ for short. The following proposition can be easily derived.

Proposition 1. *The Hamming correlation between two FHSs $X \triangleq \{X(t)\}_{t=0}^{N-1}$ and $Y \triangleq \{Y(t)\}_{t=0}^{N-1}$ over $\mathcal{F}$ can be written as*

$$H_{X,Y}(\tau) = \sum_{t=0}^{N-1} \sum_{f \in \mathcal{F}} h[X(t), f] \cdot h[Y(\langle t+\tau \rangle_N), f].$$

The *maximum out-of-phase Hamming autocorrelation* of X is defined as

$$H(X) = \max_{1\leq\tau\leq N-1}\{H_X(\tau)\}.$$

If $H(X) = \lambda_{\mathrm{a}}$ for a nonnegative integer λ_{a}, X is called an $(N, M, \lambda_{\mathrm{a}})$-FHS. In general, the optimality of an FHS is measured by the Lempel-Greenberger bound.

Theorem 2 (Lempel-Greenberger Bound, [8]). *For an* $(N, M, \lambda_{\mathrm{a}})$*-FHS* X*, we have*

$$\lambda_{\mathrm{a}} \geq \left\lceil \frac{(N-b)(N+b-M)}{M(N-1)} \right\rceil \tag{1}$$

where $b = \langle N \rangle_M$.

The Lempel-Greenberger bound can be rewritten as follows.

Corollary 3 ([12]). *For any FHS* X *of length* N *over a frequency set of size* M*,*

$$H(X) \geq \begin{cases} a, & \textit{if } N \neq M \\ 0, & \textit{if } N = M \end{cases} \tag{2}$$

where $N = aM + b$*,* $0 \leq b \leq M-1$.

Let $\mathcal{X}$ be an FHS set consisting of L FHSs of length N over $\mathcal{F}$ with $|\mathcal{F}| = M$. For $f \in \mathcal{F}$, the number of appearances of f in $\mathcal{X}$ is defined as

$$N_{\mathcal{X}}(f) = \sum_{X\in\mathcal{X}} N_X(f).$$

For any two distinct FHSs X and Y of $\mathcal{X}$, let

$$H(X, Y) = \max_{0\leq\tau\leq N-1}\{H_{X,Y}(\tau)\}.$$

The *maximum out-of-phase Hamming autocorrelation* $H_{\mathrm{a}}(\mathcal{X})$ and the *maximum Hamming cross-correlation* $H_{\mathrm{c}}(\mathcal{X})$ of $\mathcal{X}$ are defined as

$$H_{\mathrm{a}}(\mathcal{X}) = \max_{X\in\mathcal{X}}\{H(X)\},$$
$$H_{\mathrm{c}}(\mathcal{X}) = \max_{X,Y\in\mathcal{X},\, X\neq Y}\{H(X, Y)\},$$

respectively. The *maximum Hamming correlation* of $\mathcal{X}$ is defined as

$$H(\mathcal{X}) = \max\{H_{\mathrm{a}}(\mathcal{X}), H_{\mathrm{c}}(\mathcal{X})\}.$$

If $H(\mathcal{X}) = \lambda$ for a certain nonnegative integer λ, then $\mathcal{X}$ is called an $(N, M, \lambda; L)$-FHS set. Peng and Fan established a bound on $H_{\rm a}(\mathcal{X})$ and $H_{\rm c}(\mathcal{X})$ of an FHS set in terms of frequency set size, length, and the number of FHSs.

Theorem 4 (Peng-Fan Bound, [7]). *Let $\mathcal{X}$ be an FHS set consisting of L FHSs of length N over $\mathcal{F}$ with $|\mathcal{F}| = M$. Then*

$$M(N-1)H_{\rm a}(\mathcal{X}) + NM(L-1)H_{\rm c}(\mathcal{X}) \geq N(NL-M). \tag{3}$$

The following corollary is frequently used as a simplified version of the Peng-Fan bound.

Corollary 5 ([7]). *An $(N, M, \lambda; L)$-FHS set $\mathcal{X}$ satisfies*

$$H(\mathcal{X}) \geq \left\lceil \frac{(NL-M)N}{(NL-1)M} \right\rceil \tag{4}$$

and

$$H(\mathcal{X}) \geq \left\lceil \frac{2INL-(I+1)IM}{(NL-1)L} \right\rceil$$

where $I = \lfloor \frac{NL}{M} \rfloor$.

In practical applications, the required length and alphabet size of an FHS or an FHS set are variable according to the specification of a given system or environment. Thus, it is very important to select FHSs or FHS sets with optimal Hamming correlation under the given condition. In the following sections, two new FHS construction methods will be presented, from which infinitely many new optimal FHSs or FHS sets can be obtained.

III. Construction of Frequency-Hopping Sequences of Length nN

Several optimal FHS sets were constructed from algebraic or combinatorial structures [8–27]. In the case that no mathematical structures for optimal FHS sets with some desirable parameters can be found, extension of a given FHS set may be a good solution to obtain new optimal FHS sets with such parameters. In [28], Chung *et al*. applied the interleaving technique [30,31] to the construction of FHS sets. As a result, an $(N, M, \lambda; L)$-FHS set can be extended to a

$(dN, M, d\lambda; \lfloor L/d \rfloor)$-FHS set for any integer d with $2 \leq d \leq L$. While the number of frequencies is fixed in this extension, the maximum correlation increases and the set size decreases. Later, Zeng *et al.* [29] presented another extension method of FHS sets by using the interleaving technique and field extension, in which the maximum correlation and the set size are preserved. These two extension methods are generic in the sense that they can be applied to any FHS set satisfying some constraints. In this section, we will give a new generic extension method which preserves the maximum correlation and the set size. We will also show that several infinite families of new optimal FHSs or FHS sets can be constructed from our extension.

A. New Construction of FHS Sets

The Chinese Remainder Theorem (CRT) [32] tells us that when V and W are positive integers such that $\gcd(V, W) = 1$, any integer t with $0 \leq t < VW$ can be uniquely represented as

$$t \triangleq (t_V, t_W)$$

where $t_V = \langle t \rangle_V$ and $t_W = \langle t \rangle_W$. By using the CRT, it is possible to extend an FHS set to another one in the following way.

Construction A: Let $\mathcal{X} \triangleq \{X_0, X_1, \ldots, X_{L-1}\}$ be an $(N, M, \lambda; L)$-FHS set over $\mathcal{F}$, where $X_i = \{X_i(t)\}_{t=0}^{N-1}$. Let $q_1 = p_1^{a_1}$ for a prime p_1 and a positive integer a_1, where p_1 satisfies $\gcd(p_1, N) = 1$ and $N_{\mathcal{X}}(f) \leq p_1 - 1$ for any $f \in \mathcal{F}$. For $0 \leq i \leq L-1$, let $Y_i \triangleq \{Y_i(t)\}_{t=0}^{q_1 N-1}$ be the FHS over $\mathbb{Z}_{q_1} \times \mathcal{F}$, defined as

$$Y_i(t) \triangleq Y_i(t_0, t_1) = (\, \langle \eta_i(t_1) t_0 \rangle_{q_1},\, X_i(t_1)\,)$$

where $t_0 = \langle t \rangle_{q_1}$, $t_1 = \langle t \rangle_N$, and η_i is the function given by

$$\eta_i(t_1) = \sum_{m=0}^{i-1} N_{X_m}(X_i(t_1)) + \left|\{u \,:\, X_i(u) = X_i(t_1),\ 0 \leq u \leq t_1\}\right|. \tag{5}$$

Construct an FHS set $\mathcal{Y}_A$ as

$$\mathcal{Y}_A = \{Y_i \,|\, 0 \leq i \leq L-1\}.$$

Remark: Define the $L \times N$ array associated with the FHS set $\mathcal{X}$ in Construction A as

$$\begin{bmatrix} X_0(0) & \cdots & X_0(t_1) & \cdots & X_0(N-1) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{i-1}(0) & \cdots & X_{i-1}(t_1) & \cdots & X_{i-1}(N-1) \\ X_i(0) & \cdots & X_i(t_1) & \cdots & X_i(N-1) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{L-1}(0) & \cdots & X_{L-1}(t_1) & \cdots & X_{L-1}(N-1) \end{bmatrix}.$$

The number $\eta_i(t_1)$ in Construction A is equal to the number of appearances of the symbol $f = X_i(t_1)$ in the subarray

$$\begin{matrix} X_0(0) & \cdots & X_0(t_1) & \cdots & X_0(N-1) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{i-1}(0) & \cdots & X_{i-1}(t_1) & \cdots & X_{i-1}(N-1) \\ X_i(0) & \cdots & X_i(t_1) & & \end{matrix}.$$

Clearly, $1 \leq \eta_i(t_1) \leq N_{\mathcal{X}}(f) \leq p_1 - 1$ for any $0 \leq i \leq L-1$ and any $0 \leq t_1 \leq N-1$. Furthermore, we have $\eta_i(t_1) \neq \eta_j(\langle t_1 + \tau_1 \rangle_N)$ if $i \neq j$ or $\tau_1 \neq 0$, when $X_i(t_1) = X_j(t_1 + \tau_1)$. These properties of η_i would be useful to prove the optimality of the FHS set $\mathcal{Y}_A$. ■

Each symbol of the FHSs in Construction A has a vector form with two components. However, the structure of the alphabet does not matter since each symbol is mapped into an available frequency by a one-to-one mapping. The Hamming correlation can be calculated by using the fact that a hit occurs only when both $Y_i(t)$ and $Y_j(t+\tau)$ in $\mathbb{Z}_{q_1} \times \mathcal{F}$ have the same components in each coordinate. The following lemma is useful to calculate the Hamming correlation of FHSs whose symbols are of a vector form with two components.

Lemma 6. *Let V and W are two positive integers with $\gcd(V, W) = 1$. Let $X \triangleq \{X(t)\}_{t=0}^{VW-1}$ and $Y \triangleq \{Y(t)\}_{t=0}^{VW-1}$ be two FHSs of length VW over $\mathcal{F}_1 \times \mathcal{F}_2$ such that $X(t) = (a(t_V), b(t_W))$, and $Y(t) = (c(t_V), d(t_W))$ with $t_V = \langle t \rangle_V$ and $t_W = \langle t \rangle_W$, where $\{a(t_V)\}$ and $\{c(t_V)\}$ are sequences of length V over $\mathcal{F}_1$, and $\{b(t_W)\}$ and $\{d(t_W)\}$ are sequences of length W over $\mathcal{F}_2$.*

The Hamming correlation between X and Y is given by

$$\begin{aligned} H_{X,Y}(\tau) &= \sum_{t_W=0}^{W-1} \sum_{f\in\mathcal{F}_2} h[b(t_W), f]\, h[d(\langle t_W+\tau_W\rangle_W), f] \\ &\qquad \cdot \sum_{t_V=0}^{V-1} h[a(t_V), c(\langle t_V+\tau_V\rangle_V) \end{aligned}$$

where $\tau_V = \langle \tau \rangle_V$ and $\tau_W = \langle \tau \rangle_W$.

Proof. Define two $V \times W$ arrays $\mathbf{X}$ and $\mathbf{Y}$ by

$$\mathbf{X} \triangleq \begin{bmatrix} (a(0), b(0)) & \cdots & (a(0), b(t_W)) & \cdots & (a(0), b(W-1)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ (a(t_V), b(0)) & \cdots & (a(t_V), b(t_W)) & \cdots & (a(t_V), b(W-1)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ (a(V-1), b(0)) & \cdots & (a(V-1), b(t_W)) & \cdots & (a(V-1), b(W-1)) \end{bmatrix}$$

and

$$\mathbf{Y} \triangleq \begin{bmatrix} (c(\tau_V), d(\tau_W)) & \cdots & (c(\tau_V), d(\langle t_W+\tau_W\rangle_W)) & \cdots & (c(\tau_V), d(\langle \tau_W-1\rangle_W)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ (c(\langle t_V+\tau_V\rangle_V), d(\tau_W)) & \cdots & (c(\langle t_V+\tau_V\rangle_V), d(\langle t_W+\tau_W\rangle_W)) & \cdots & (c(\langle t_V+\tau_V\rangle_V), d(\langle \tau_W-1\rangle_W)) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ (c(\langle \tau_V-1\rangle_V), d(\tau_W)) & \cdots & (c(\langle \tau_V-1\rangle_V), d(\langle t_W+\tau_W\rangle_W)) & \cdots & (c(\langle \tau_V-1\rangle_V), d(\langle \tau_W-1\rangle_W)) \end{bmatrix}$$

where each entry of $\mathbf{X}$ and $\mathbf{Y}$ is in $\mathcal{F}_1 \times \mathcal{F}_2$. It is clear that $H_{X,Y}(\tau)$ is equal to the number of the common entries of $\mathbf{X}$ and $\mathbf{Y}$ having the same elements in $\mathcal{F}_1 \times \mathcal{F}_2$. If $b(t_W) \neq d(\langle t_W+\tau_W\rangle_W)$, the t_W-th columns of $\mathbf{X}$ and $\mathbf{Y}$ have no such entries. Otherwise the number of such common entries in them is determined by comparing $\{a(t_V)\}_{t_V=0}^{V-1}$ and $\{c(\langle t_V+\tau_V\rangle_V)\}_{t_V=0}^{V-1}$. That is, we have

$$\begin{aligned} H_{X,Y}(\tau) &\triangleq H_{X,Y}(\tau_V, \tau_W) \\ &= \sum_{t_V=0}^{V-1} \sum_{t_W=0}^{W-1} h\left[\,(a(t_V), b(t_W)),\ (c(\langle t_V+\tau_V\rangle_V), d(\langle t_W+\tau_W\rangle_W))\right] \\ &= \sum_{t_V=0}^{V-1} \sum_{t_W=0}^{W-1} h\left[\,a(t_V), c(\langle t_V+\tau_V\rangle_V)\right]\, h\left[\,b(t_W), d(\langle t_W+\tau_W\rangle_W)\right] \\ &= \sum_{t_W=0}^{W-1} h\left[\,b(t_W), d(\langle t_W+\tau_W\rangle_W)\right] \cdot \sum_{t_V=0}^{V-1} h\left[\,a(t_V), c(\langle t_V+\tau_V\rangle_V)\right]. \end{aligned}$$

By applying Proposition 1, we get the assertion. □

Theorem 7. *The set $\mathcal{Y}_A$ in Construction A is a $(q_1N, q_1M, \lambda; L)$-FHS set. Furthermore, $H(Y_i) = H(X_i)$ for all $0 \le i \le L-1$.*

Proof. For $0 \le \tau \le q_1N-1$, let $\tau_0 = \langle \tau \rangle_{q_1}$ and $\tau_1 = \langle \tau \rangle_N$. By Lemma 6, the Hamming correlation $H_{i,j}(\tau)$ between Y_i and Y_j is given by

$$\begin{aligned} H_{i,j}(\tau) &:= H_{i,j}(\tau_0,\tau_1) \\ &= \sum_{t_1=0}^{N-1}\sum_{f\in\mathcal{F}} h[X_i(t_1), f\,]\cdot h[X_j(\langle t_1+\tau_1\rangle_N), f\,] \\ &\qquad \cdot \sum_{t_0=0}^{q_1-1} h[\langle\{\eta_i(t_1)-\eta_j(\langle t_1+\tau_1\rangle_N)\}\cdot t_0\rangle_{q_1},\ \langle\eta_j(\langle t_1+\tau_1\rangle_N)\cdot\tau_0\rangle_{q_1}]. \end{aligned}$$

In order to compute $H_{i,j}(\tau)$, we divide the problem into two cases.

Case i) $i=j$ and $\tau_1=0$. Since $\eta_i(t_1)=\eta_j(\langle t_1+\tau_1\rangle_N)$ in this case, we get

$$H_{i,i}(\tau_0,0)=\sum_{t_1=0}^{N-1}\sum_{f\in\mathcal{F}} h[X_i(t_1), f\,]\cdot h[X_i(t_1), f\,]\cdot\sum_{t_0=0}^{q_1-1} h[\,0,\ \langle\eta_i(t_1)\,\tau_0\rangle_{q_1}\,].$$

If $\tau_0=0$, then

$$\begin{aligned} H_{i,j}(0,0) &= \sum_{t_1=0}^{N-1}\sum_{f\in\mathcal{F}} h[X_i(t_1), f\,]\cdot\sum_{t_0=0}^{q_1-1} h[0,0] \\ &= \sum_{t_1=0}^{N-1} q_1 \\ &= q_1N. \end{aligned}$$

If $1\le\tau_0\le q_1-1$, then

$$\begin{aligned} H_{i,j}(\tau_0,0) &= \sum_{t_1=0}^{N-1}\sum_{f\in\mathcal{F}} h[X_i(t_1), f\,]\cdot\sum_{t_0=0}^{q_1-1} 0 \\ &= 0 \end{aligned}$$

where the first equality comes from the fact that $\eta_i(t_1)\tau_0 \ne 0 \mod q_1$ since $1\le\eta_i(t_1)\le p_1-1$. Therefore,

$$H_{i,i}(\tau_0,0) := \begin{cases} q_1N, & \text{if } \tau_0=0 \\ 0, & \text{otherwise.} \end{cases}$$

Case ii) $i\ne j$ or $\tau_1\ne0$. In this case, if $X_i(t_1)=X_j(\langle t_1+\tau_1\rangle_N)=f$ for some $f\in\mathcal{F}$, then

$$\eta_i(t_1)-\eta_j(\langle t_1+\tau_1\rangle_N)\ne 0 \mod p_1$$

since $1 \leq \eta_i(t_1) \neq \eta_j(\langle t_1 + \tau_1 \rangle_N) \leq p_1 - 1$. Hence,

$$\sum_{t_0=0}^{q_1-1} h[\langle \{\eta_i(t_1) - \eta_j(t_1 + \tau_1)\} \cdot t_0 \rangle_{q_1},\ \langle \eta_j(\langle t_1 + \tau_1 \rangle_N) \cdot \tau_0 \rangle_{q_1}] = 1$$

when $X_i(t_1) = X_j(\langle t_1 + \tau_1 \rangle_N)$. Then,

$$\begin{aligned} H_{i,j}(\tau_0, \tau_1) &= \sum_{t_1=0}^{N-1} \sum_{f \in \mathcal{F}} h[X_i(t_1), f\,]\, h[X_j(\langle t_1 + \tau_1 \rangle_N), f\,] \\ &= \sum_{t_1=0}^{N-1} h[X_i(t_1), X_j(\langle t_1 + \tau_1 \rangle_N)] \\ &= H_{X_i, X_j}(\tau_1) \\ &\leq \lambda \end{aligned}$$

since $i \neq j$ or $\tau_1 \neq 0$.

By summarizing the results of Cases i) and ii), we have

$$H_{i,i}(\tau) = \begin{cases} q_1 N, & \text{if } \tau = 0 \\ 0, & \text{if } \tau_0 \neq 0 \text{ and } \tau_1 = 0 \\ H_{X_i, X_i}(\tau_1), & \text{if } \tau_1 \neq 0 \end{cases}$$

for any $0 \leq i \leq L - 1$, and

$$H_{i,j}(\tau) = H_{X_i, X_j}(\tau_1) \leq \lambda$$

for any $0 \leq i \neq j \leq L - 1$ and any $0 \leq \tau \leq N - 1$. □

It is easily checked that $N_{\mathcal{Y}_A}((a, f)) = N_{\mathcal{X}}(f)$ for any $a \in \mathbb{Z}_{q_1}$ and any $f \in \mathcal{F}$ in Construction A. Therefore, it is possible to extend the length of $\mathcal{Y}_A$ by the factor $q_2 = p_2^{a_2}$, where a_2 is a positive integer and p_2 is a prime with $p_2 > p_1$ and $\gcd(p_2, N) = 1$. In this way, Construction A can be applied recursively infinitely many times.

Corollary 8. *Let $\mathcal{X}$ be an $(N, M, \lambda; L)$-FHS set over $\mathcal{F}$, where $X_i = \{X_i(t)\}_{t=0}^{N-1}$. For a positive integer k, let $q_i = p_i^{a_i}$ for $1 \leq i \leq k$, where $p_1, \ldots, p_k$ are primes with $p_1 < \cdots < p_k$ and $a_1, \ldots, a_k$ are positive integers. Assume that $n = q_1 \cdots q_k$ satisfies $\gcd(n, N) = 1$ and $N_{\mathcal{X}}(f) \leq p_1 - 1$ for any $f \in \mathcal{F}$. Then there exists an $(nN, nM, \lambda; L)$-FHS set over $\mathbb{Z}_{q_k} \times \cdots \times \mathbb{Z}_{q_1} \times \mathcal{F}$.*

If $\mathcal{X}$ in Corollary 8 is optimal with respect to the Peng-Fan bound, the resultant FHS set is also optimal whenever $\left\lceil \frac{(NL-M)N}{(NL-1)M} - \frac{1}{LM} \right\rceil = \left\lceil \frac{(NL-M)N}{(NL-1)M} \right\rceil$ since

$$\frac{(NL-M)N}{(NL-1)M} - \frac{1}{LM} < \frac{(nNL-nM)\cdot N}{(nNL-1)\cdot nM} < \frac{(NL-M)N}{(NL-1)M}.$$

For example, the $(9n, 3n, 3; 3)$-FHS set extended from the $(9, 3, 3; 3)$-FHS set given in [10] is always optimal as long as n satisfies the conditions in Corollary 8. Moreover, if each FHS of $\mathcal{X}$ is optimal with respect to the Lempel-Greenberger bound, it is guaranteed that each FHS in the resultant set is always optimal because $\left\lfloor \frac{nN}{nM} \right\rfloor = \left\lfloor \frac{N}{M} \right\rfloor$. Some new optimal FHS sets obtained by recursively applying Construction A are listed in Table II. Since Construction A can be applied to any existing FHS sets, it is expected that there exist some more classes of optimal FHS sets which can be obtained from our construction, but are not listed there.

Example 9. *Let* $\mathcal{X} \triangleq \{X_0, X_1, X_2\}$ *be the optimal* $(9, 3, 3; 3)$*-FHS set over* $\mathbb{Z}_3$ *given in [10], where*

$$\{X_0(t_1)\}_{t_1=0}^{8} = \{0, 0, 0, 0, 1, 2, 0, 2, 1\},$$
$$\{X_1(t_1)\}_{t_1=0}^{8} = \{1, 1, 1, 1, 2, 0, 1, 0, 2\},$$
$$\{X_2(t_1)\}_{t_1=0}^{8} = \{2, 2, 2, 2, 0, 1, 2, 1, 0\}.$$

It is easily checked that

$$\{\eta_0(t_1)\}_{t_1=0}^{8} = \{1, 2, 3, 4, 1, 1, 5, 2, 2\},$$
$$\{\eta_1(t_1)\}_{t_1=0}^{8} = \{3, 4, 5, 6, 3, 6, 7, 7, 4\},$$
$$\{\eta_2(t_1)\}_{t_1=0}^{8} = \{5, 6, 7, 8, 8, 8, 9, 9, 9\}.$$

Let $q_1 = p_1 = 11$ *in Construction A. The FHS* Y_0 *over* $\mathbb{Z}_{11} \times \mathbb{Z}_3$ *can be obtained from the* 11×9

array

$$\begin{bmatrix}
(0,0) & (0,0) & (0,0) & (0,0) & (0,1) & (0,2) & (0,0) & (0,2) & (0,1) \\
(1,0) & (2,0) & (3,0) & (4,0) & (1,1) & (1,2) & (5,0) & (2,2) & (2,1) \\
(2,0) & (4,0) & (6,0) & (8,0) & (2,1) & (2,2) & (10,0) & (4,2) & (4,1) \\
(3,0) & (6,0) & (9,0) & (1,0) & (3,1) & (3,2) & (4,0) & (6,2) & (6,1) \\
(4,0) & (8,0) & (1,0) & (5,0) & (4,1) & (4,2) & (9,0) & (8,2) & (8,1) \\
(5,0) & (10,0) & (4,0) & (9,0) & (5,1) & (5,2) & (3,0) & (10,2) & (10,1) \\
(6,0) & (1,0) & (7,0) & (2,0) & (6,1) & (6,2) & (8,0) & (1,2) & (1,1) \\
(7,0) & (3,0) & (10,0) & (6,0) & (7,1) & (7,2) & (2,0) & (3,2) & (3,1) \\
(8,0) & (5,0) & (2,0) & (10,0) & (8,1) & (8,2) & (7,0) & (5,2) & (5,1) \\
(9,0) & (7,0) & (5,0) & (3,0) & (9,1) & (9,2) & (1,0) & (7,2) & (7,1) \\
(10,0) & (9,0) & (8,0) & (7,0) & (10,1) & (10,2) & (6,0) & (9,2) & (9,1)
\end{bmatrix},$$

that is,

$$\begin{aligned}
\{Y_0(t)\}_{t=0}^{98} = \{&(0,0),(2,0),(6,0),(1,0),(4,1),(5,2),(8,0),(3,2),(5,1),(9,0),\\
&\cdots,(2,1),(2,0),(6,0),(1,0),(9,0),(6,1),(7,2),(7,0),(7,2),(9,1)\}.
\end{aligned}$$

Similarly,

$$\begin{aligned}
\{Y_1(t)\}_{t=0}^{98} = \{&(0,1),(4,1),(10,1),(7,1),(1,2),(8,0),(9,1),(5,0),(10,2),(5,1),\\
&\cdots,(4,2),(6,1),(1,1),(9,1),(8,1),(7,2),(9,0),(1,1),(8,0),(7,2)\};\\
\{Y_2(t)\}_{t=0}^{98} = \{&(0,2),(6,2),(3,2),(2,2),(10,0),(7,1),(10,2),(8,1),(6,0),(11,2),\\
&\cdots,(9,0),(10,2),(7,2),(6,2),(7,2),(4,0),(1,1),(6,2),(4,1),(2,0)\}.
\end{aligned}$$

For $0 \le i,j \le 2$*, the Hamming correlation* $H_{i,j}(\tau)$ *between* Y_i *and* Y_j *is easily computed as*

$$H_{i,j}(\tau) = \begin{cases} 99, & \textit{if} \;\; i=j \textit{ and } \tau = 0 \bmod 99 \\ 0, & \textit{if} \;\; i=j, \; 9\,|\tau \textit{ and } 11 \nmid \tau \\ 0, & \textit{if} \;\; i \neq j \textit{ and } 9|\,\tau \\ 3, & \textit{otherwise.} \end{cases}$$

Clearly, $\mathcal{Y}_A \triangleq \{Y_0, Y_1, Y_2\}$ *is an optimal* $(99,33,3;3)$*-FHS with respect to the Peng-Fan bound. Moreover, each FHS* Y_i *is an optimal* $(99,33,3)$*-FHS with respect to the Lempel-Greenberger* *bound. In a similar way, $\mathcal{X}$ can be extended to an optimal $(117, 39, 3; 3)$-FHS set, an optimal $(1287, 429, 3; 3)$-FHS set, or infinitely many optimal FHS sets.* ■

B. New Optimal Single FHS

Given a length and a frequency set size, the existence of an optimal FHS with respect to the Lempel-Greenberger bound is not always guaranteed. For instance, it is easily checked that neither a $(5, 2, 2)$-FHS nor a $(6, 2, 3)$-FHS exists. Thus, it is also an important problem to find an optimal FHS with respect to the Lempel-Greenberger bound, which has a length or an alphabet size not covered in the literature.

Construction A in the case of $L = 1$ leads to the construction of a new single FHS. Based on Construction A, it is possible to obtain new optimal FHSs with respect to the Lempel-Greenberger bound.

Corollary 10. *Assume that there exists an optimal $(N, M, \lambda_{\rm a})$-FHS X with respect to the Lempel-Greenberger bound, defined over $\mathcal{F}$. For positive integers k and $a_1, \ldots, a_k$, let $q_i = p_i^{a_i}$, $1 \leq i \leq k$, where $p_1, \ldots, p_k$ are primes with $p_1 < \cdots < p_k$. If $n = q_1 \cdots q_k$ satisfies $\gcd(n, N) = 1$ and $N_X(f) \leq p_1 - 1$ for any $f \in \mathcal{F}$, then there exists an optimal $(nN, nM, \lambda_{\rm a})$-FHS over $\mathbb{Z}_{q_k} \times \cdots \times \mathbb{Z}_{q_1} \times \mathcal{F}$.*

Proof. Let $N = aM + b$ with $0 \leq b \leq M - 1$. Then $\lambda_{\rm a} = a$ if $M \neq N$, and $\lambda_{\rm a} = 0$ if $M = N$ by Corollary 3. From Construction A, an $(nN, nM, \lambda_{\rm a})$-FHS Y can be obtained. Since $nN = a(nM) + nb$ with $0 \leq nb \leq n(M - 1)$, Y is optimal with respect to the Lempel-Greenberger bound by Corollary 3. □

Corollary 10 tells us that any optimal FHS with respect to the Lempel-Greenberger bound can be extended to an optimal FHS of a longer length over a larger set of available frequencies, if properly chosen. Some examples of new optimal FHSs are shown in Table III.

Example 11. *Let $X = \{X(t)\}_{t=0}^{18}$ be the $(19, 6, 3)$-FHS over $\mathbb{Z}_6$ given by*

$$\{X(t)\}_{t=0}^{18} = \{0, 0, 1, 1, 2, 4, 2, 0, 3, 2, 5, 0, 3, 5, 1, 5, 4, 4, 3\}$$

in [13]. By applying Construction A to X with $q_1 = p_1 = 5$, we obtain $Y = \{Y(t)\}_{t=0}^{94}$ over $\mathbb{Z}_5 \times \mathbb{Z}_6$ as

$$\begin{aligned}\{Y(t)\}_{t=0}^{94} = \{&00, 20, 21, 11, 42, 04, 22, 10, 33, 22, 05, 40, 43, 15, 21, 05, 24, 14, 43,\\ &40, 00, 11, 41, 32, 44, 02, 30, 23, 42, 45, 00, 23, 45, 41, 25, 04, 34, 13,\\ &30, 30, 01, 21, 22, 34, 32, 00, 13, 12, 35, 10, 03, 25, 11, 45, 34, 04, 33,\\ &20, 10, 41, 01, 12, 24, 12, 20, 03, 32, 25, 20, 33, 05, 31, 15, 14, 24, 03,\\ &10, 40, 31, 31, 02, 14, 42, 40, 43, 02, 15, 30, 13, 35, 01, 35, 44, 44, 23\}\end{aligned}$$

where (x, y) is simply denoted by xy for $x \in \mathbb{Z}_5$ and $y \in \mathbb{Z}_6$. It is easily checked that Y is an optimal $(95, 30, 3)$-FHS with respect to the Lempel-Greenberger bound. Similarly, X can be extended to an optimal $(133, 42, 3)$-FHS, an optimal $(665, 210, 3)$-FHS, or infinitely many optimal FHSs. ■

IV. Construction of Frequency-Hopping Sequences of Length $(q-1)N$

In [29], some new optimal $((q-1)N, qM - \Delta, \lambda; L)$-FHS sets obtained from an $(N, M, \lambda; L)$-FHS set were presented, where q is a prime power and Δ is determined by the properties of the given FHS set. In this section, we present a new construction for optimal FHS sets with similar parameters in a different approach. Let $\mathbb{F}_q$ be the finite field of q elements and α a primitive element of $\mathbb{F}_q$. For any nonzero element β of $\mathbb{F}_q$, we have $\beta = \alpha^l$ for an integer $0 \le l \le q-2$. By using the CRT and the finite field, it is possible to construct a new FHS set.

Construction B: Let $\mathcal{X} \triangleq \{X_0, X_1, \ldots, X_{L-1}\}$ be an $(N, M, \lambda; L)$-FHS set over $\mathcal{F}$, where $X_i = \{X_i(t)\}_{t=0}^{N-1}$. Assume that q is a prime power satisfying $\gcd(q-1, N) = 1$ and $N_{\mathcal{X}}(f) \le q$ for any $f \in \mathcal{F}$. Let ζ be a one-to-one function from $\{1, \ldots, q\}$ to $\mathbb{F}_q$. For $0 \le i \le L-1$, let $Y_i \triangleq \{Y_i(t)\}_{t=0}^{(q-1)N-1}$ be the FHS over $\mathbb{F}_q \times \mathcal{F}$, defined as

$$Y_i(t) \triangleq Y_i(t_0, t_1) = \left(\alpha^{t_0} + \zeta_i(t_1), X_i(t_1)\right)$$

where $t_0 = \langle t \rangle_{q-1}$, $t_1 = \langle t \rangle_N$, and $\zeta_i(t_1) = \zeta(\eta_i(t_1))$ with η_i defined in (5). Construct the FHS set $\mathcal{Y}_B$ as

$$\mathcal{Y}_B = \{Y_i \,|\, 0 \le i \le L-1\}.$$

Theorem 12. *The set $\mathcal{Y}_B$ in Construction B is a $((q-1)N, qM, \lambda; L)$-FHS set.*

Proof. For $0 \leq \tau \leq (q-1)N-1$, let $\tau_0 = \langle \tau \rangle_{q-1}$ and $\tau_1 = \langle \tau \rangle_N$. In a similar way to the Proof of Theorem 7, the Hamming correlation $H_{i,j}(\tau)$ between Y_i and Y_j is given by

$$\begin{aligned} H_{i,j}(\tau) &\triangleq H_{i,j}(\tau_0, \tau_1) \\ &= \sum_{t_1=0}^{N-1} \sum_{f \in \mathcal{F}} h[X_i(t_1), f\,] \cdot h[X_j(t_1+\tau_1), f\,] \\ &\qquad\qquad \cdot \sum_{t_0=0}^{q-2} h[\alpha^{t_0}\,(1-\alpha^{\tau_0})\,, \zeta_j(t_1+\tau_1) - \zeta_i(t_1)\,]. \end{aligned}$$

In order to compute $H_{i,j}(\tau)$, we divide the problem into two cases.

Case i) $\tau_0 = 0$. In this case,

$$\begin{aligned} H_{i,j}(\tau) &\triangleq H_{i,j}(\tau_0, \tau_1) \\ &= \sum_{t_1=0}^{N-1} \sum_{f \in \mathcal{F}} h[X_i(t_1), f\,]\, h[X_j(t_1+\tau_1), f\,] \cdot \sum_{t_0=0}^{q-2} h[0, \zeta_j(t_1+\tau_1) - \zeta_i(t_1)\,]. \end{aligned}$$

Note that

$$\sum_{t_0=0}^{q-2} h[0, \zeta_j(t_1+\tau_1) - \zeta_i(t_1)\,] = \begin{cases} q-1, & \text{if } i=j \text{ and } \tau_1 = 0 \\ 0, & \text{otherwise} \end{cases}$$

by the fact that $\eta_i(t_1) \neq \eta_j(\langle t_1 + \tau_1 \rangle_N)$ and ζ is one-to-one. Consequently,

$$H_{i,j}(\tau) = \begin{cases} (q-1)N, & \text{if } i=j \text{ and } \tau_1 = 0 \\ 0, & \text{otherwise.} \end{cases}$$

Case ii) $\tau_0 \neq 0$. Since α is a primitive element of $\mathbb{F}_q$, we have

$$\sum_{t_0=0}^{q-2} h[\alpha^{t_0}(1-\alpha^{\tau_0}),\, \zeta_j(t_1+\tau_1) - \zeta_i(t_1)\,] = \begin{cases} 0, & \text{if } i=j \text{ and } \tau_1 = 0 \\ 1, & \text{otherwise.} \end{cases}$$

Hence,

$$H_{i,j}(\tau) = \begin{cases} 0, & \text{if } i=j \text{ and } \tau_1 = 0 \\ H_{X_i,X_j}(\tau_1), & \text{otherwise.} \end{cases}$$

In summary,

$$H_{i,j}(\tau) \leq \begin{cases} (q-1)N, & \text{if } i=j \text{ and } \tau = 0 \\ \lambda, & \text{otherwise.} \end{cases}$$

Therefore, we get the assertion. □

Remark: Compared with the construction in [29], Construction B requires one additional condition that $\gcd(q-1, N) = 1$. However, the alphabet size of $\mathcal{Y}_B$ in Construction B is always exactly qM, while the alphabet size in [29] is given by $qM - |\Psi|$, where $\Psi = \{f \mid N_{\mathcal{X}}(f) = 1\}$. Moreover, the condition that $1 \leq N_{\mathcal{X}}(f) \leq q-1$ in [29] is also different from the condition that $1 \leq N_{\mathcal{X}}(f) \leq q$ in Construction B.

Note that $N_{\mathcal{Y}_B}((x, f)) \leq N_{\mathcal{X}}(f)$ for any $x \in \mathbb{F}_q$ and any $f \in \mathcal{F}$ in Construction B. Hence, it is possible to apply Construction A to $\mathcal{Y}_B$. By combining Construction B with Construction A in this way, other classes of optimal FHS sets and FHSs with new parameters can be obtained, as shown in the following corollaries and Tables III and IV.

Corollary 13. *Assume that there exists an optimal $(N, M, \lambda; L)$-FHS set $\mathcal{X}$ over $\mathcal{F}$. Let $q_i = p_i^{a_i}$ for $1 \leq i \leq k$ such that $p_1, \ldots, p_k$ are primes with $p_1 < \cdots < p_k$ and $\gcd(p_i, N) = 1$ for $1 \leq i \leq k$. Let q be a prime power satisfying $\gcd(q-1, q_1 \cdots q_k) = 1$ and $\gcd(q-1, N) = 1$. If $N_{\mathcal{X}}(f) \leq p_1 - 1$ and $N_{\mathcal{X}}(f) \leq q$ for all $f \in \mathcal{F}$, then there exists an $(n(q-1)N, nqM, \lambda; L)$-FHS set $\mathcal{Y}_{B'}$, where $n = p_1^{a_1} \cdots p_k^{a_k}$ with positive integers $a_1, \ldots, a_k$.*

Corollary 14. *Assume that there exist an optimal $(N, M, \lambda_{\mathrm{a}})$-FHS X over $\mathcal{F}$. Let $q_i = p_i^{a_i}$ for $1 \leq i \leq k$ such that $p_1, \ldots, p_k$ are primes with $p_1 < \cdots < p_k$ and $\gcd(p_i, N) = 1$ for $1 \leq i \leq k$. Let q be a prime power satisfying $\gcd(q-1, q_1 \cdots q_k) = 1$ and $\gcd(q-1, N) = 1$. If $N_X(f) \leq p_1 - 1$ and $N_X(f) \leq q$ for all $f \in \mathcal{F}$, then there exist an $(n(q-1)N, nqM, \lambda_{\mathrm{a}})$-FHS Y over $\mathbb{F}_q \times \mathcal{F}$. In particular, Y is optimal if $N = M$ or $bq \geq N$, where $N = aM + b$ with $0 \leq b \leq M$.*

Note that in Corollary 10, the optimality with respect to the Lempel-Greenberger bound is always preserved because $\frac{nN}{nM} = \frac{N}{M}$. However, an additional condition is needed in Corollary 14 since $\frac{(q-1)nN}{qnM} < \frac{N}{M}$.

V. Conclusion

We showed two new extension method for constructing FHS sets. We also proved that infinitely many families of new optimal FHS sets with respect to the Peng-Fan bound as well as new optimal FHSs with respect to the Lempel-Greenberger bound can be obtained from them. Compared with the previous extension methods in [28] and [29], our constructions give new optimal FHS sets for much more general cases, as shown in Table I. Moreover, several new classes of optimal FHSs or FHS sets are provided in Tables II–IV, whose parameters are not covered in the literature.

REFERENCES

[1] M. K. Simon, J. K. Omura, R. A. Scholtz, B. K. Levitt, *Spread Spectrum Communications Handbook*, (Revised Ed.). McGraw-Hill Inc. (1994).

[2] D. V. Sarwate, “Reed-Solomon codes and the design of sequences for spread-spectrum multiple-access communications,” *Reed-Solomon Codes and Their Applications*. edited by S. B. Wicker and V. K. Bharagava, Piscataway, NJ: IEEE Press (1994).

[3] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. Research Studies Press (RSP), John Wiley & Sons, London, UK, 1996.

[4] L. Yang and G. B. Giannakis, “Ultra-wideband communications: an idea whose time has come,” *IEEE Signal Proc. Mag.*, vol. 21, no. 6, pp. 26–54, Nov. 2004.

[5] Wi-Fi and Bluetooth - Interference Issues. [Online]. Available: http://www.hp.com

[6] Specification of the Bluetooth Systems-Core. The Bluetooth Special Interest Group (SIG). [Online]. Available: http://www.bluetooth.com

[7] 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, Sept. 2004.

[8] 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.

[9] G. Solomon, “Optimal frequency hopping for multiple access,” *Proc. 1977 Symp. Spread Spectrum Commun.*, San Diego, CA, USA, Mar. 13–16, 1977, pp. 33–35.

[10] P. V. Kumar, “Frequency-hopping code sequence designs having large linear span,” *IEEE Trans. Inf. Theory*, vol. 34, no. 1, pp. 146–151, Jan. 1988.

[11] 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, July 1998.

[12] 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.

[13] 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.

[14] Z. Cao, G. Ge, and Y. Miao, “Combinatorial characterizations of one-coincidence frequency-hopping sequences,” *Des. Codes Crypt.*, vol. 41, no. 2, pp. 177–184, Nov. 2006.

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

[16] 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.

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

[18] 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.

[19] 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.

[20] Y. K. Han and K. Yang, "On the Sidel'nikov sequences as frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4279–4285, Sep. 2009.

[21] 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.

[22] 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.

[23] 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.

[24] Y. Yang, X. Tang, U. Parampalli, 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.

[25] 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.

[26] J.-H. Chung and K. Yang, "A new class of balanced near-perfect nonlinear mappings and its application to sequence design," *IEEE Trans. Inf. Theory*, vol. 59, no. 2, pp. 1090–1097, Feb. 2013.

[27] 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.

[28] 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.

[29] 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.

[30] G. Gong, "Theory and applications of q-ary interleaved sequences," *IEEE Trans. Inf. Theory*, vol. 41, pp. 400–411, Mar. 1995.

[31] G. Gong, "New designs for signal sets with low cross correlation, balance property, and large linear span: GF(p) case," *IEEE Trans. Inf. Theory*, vol. 48, no. 11, pp. 2847–2867, Nov. 2002.

[32] C. Ding, D. Y. Pei, and A. Salomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1996.

TABLE I

EXTENSION METHODS OF AN $(N, M, \lambda; L)$-FHS SET $\mathcal{X}$. HERE, $p_1, \ldots, p_k$ ARE PRIMES WITH $p_1 < \cdots < p_k$ AND q IS A PRIME POWER.

References	Extended FHS set	Constraints
[28]	$(dN, M, d\lambda; \lfloor \frac{L}{d} \rfloor)$	$2 \leq d \leq L$
[29]	$((q-1)N, qM - \lvert\Psi\rvert, \lambda; L)$	$1 \leq N_{\mathcal{X}}(f) \leq q-1$ for all $f \in \mathcal{F}$, $\Psi = \{f \mid N_{\mathcal{X}}(f) = 1\}$
Construction A	$(nN, nM, \lambda; L)$	$1 \leq N_{\mathcal{X}}(f) \leq p_1 - 1$ for all $f \in \mathcal{F}$, $n = p_1^{a_1} \cdots p_k^{a_k}$, $\gcd(n, N) = 1$
Construction B	$((q-1)N, qM, \lambda; L)$	$1 \leq N_{\mathcal{X}}(f) \leq q$, for all $f \in \mathcal{F}$, $\gcd(q-1, N) = 1$
Combination of Constructions A and B	$(n(q-1)N,$ $n(q-1)M, \lambda; L)$	$1 \leq N_{\mathcal{X}}(f) \leq p_1 - 1$, $1 \leq N_{\mathcal{X}}(f) \leq q$ for all $f \in \mathcal{F}$, $n = p_1^{a_1} \cdots p_k^{a_k}$, $\gcd(n, q-1) = \gcd(q-1, N)$ $= \gcd(n, N) = 1$

TABLE II

Parameters of Some New Optimal FHS Sets with Respect to the Peng-Fan Bound Obtained from Construction A. Here, $p, p_1, \ldots, p_k$ are primes with $p_1 < \cdots < p_k$, $n = p_1^{a_1} \cdots p_k^{a_k}$, and r is a prime power.

New FHS Set $(N, M, \lambda; L)$	Individual FHS $(N, M, \lambda_{\mathrm{a}})$	Constraints
$\big(n(r^l-1), n\,r^m, r^{l-m}; r^m\big)$	$\big(n(r^l-1), n\,r^m, r^{l-m}-1\big)$ optimal	$1 \le m \le l$, $p_1 > r^l$
$\big(np^2, np, p; p\big)$	$\big(np^2, np, p\big)$ optimal	$p_1 > p^2$
$(np, n\,(e+1), g; e)$	$(np, n\,(e+1), g-1)$ optimal	$p = eg+1$, $2 \le g \le e$, $p_1 > p$
$(n(r-1), n\,(e+1), g; e)$	$(n(r-1), n\,(e+1),\ g-1)$ optimal	$r = eg+1$, $e(e+1) \ge r-1$, $p_1 > r$
$\Big(\frac{n(r^l-1)}{h}, n\,r^m, \frac{r^{l-m}-1}{h}; h\Big)$	$\Big(\frac{n(r^l-1)}{h}, n\,r^m, \frac{r^{l-m}-1}{h}\Big)$ optimal	$\gcd(l,h)=1$, $h \mid r-1$, $1 \le m \le l$, $p_1 > \frac{r^l-1}{h}$
$(nv, n\,(e+1), g; g_1)$	$(nv, n\,(e+1), g-1)$ optimal	$v = eg+1 = s_1^{m_1} \cdots s_k^{m_k}$, $s_1 < \cdots < s_k$: odd primes, $s_i = eg_i + 1$ for all i, $g_1 \ge e \ge 2,\ p_1 \ge eg_1$

TABLE III

PARAMETERS OF SOME NEW OPTIMAL FHSS WITH RESPECT TO THE LEMPEL-GREENBERGER BOUND OBTAINED FROM CONSTRUCTIONS A AND B. HERE, $p, p_1, \ldots, p_k$ ARE PRIMES WITH $p_1 < \cdots < p_k$, $n = p_1^{a_1} \cdots p_k^{a_k}$, AND BOTH q AND r ARE PRIME POWERS.

Parameters $(N, M, \lambda_{\mathrm{a}})$	Constraints
$(nv, n\,e, g)$	$v = eg + 1 = r_1^{m_1} \cdots r_k^{m_k}$, $r_1 < \cdots < r_k :$ odd primes, $r_i = eg_i + 1$ for all i, $2 \nmid g_i,\ p_1 > e + 1$
$(nv, n\,e, g)$	$v = eg + 1 = r_1^{m_1} \cdots r_k^{m_k}$, $r_1 < \cdots < r_k :$ odd primes, $r_i = eg_i + 1$ and $r_i \equiv 3 \bmod 4$ for all i, $2 \mid g_i,\ p_1 > e + 1$
$\big(np^2, np, p\big)$	$p_1 > 2p - 1$
$(n(r-1), n\,(e+1),\ g-1)$	$r = eg + 1$, $e(e+1) \geq r - 1, \quad p_1 > e$
$\big(n(r^l - 1), n\,r^m, r^{l-m} - 1\big)$	$1 \leq m \leq l, \quad p_1 > r^{l-m}$
$\Big(\frac{n(r^l-1)}{h}, n\,r^m, \frac{r^{l-m}-1}{h}\Big)$	$\gcd(n, h) = 1, \quad h \,\vert\, r - 1$, $1 \leq m \leq n, \quad p_1 > \frac{r^{l-m}-1}{h}$
$(n(q-1)v, nq\,e, g)$	$v = eg + 1 = r_1^{m_1} \cdots r_k^{m_k}$, $r_1 < \cdots < r_k :$ odd primes, $r_i = eg_i + 1$ for all i, $2 \nmid g_i,\ p_1 > e + 1$, $\gcd(n, q-1) = \gcd(q-1, v) = \gcd(v, n) = 1$
$(n(q-1)v, n\,e, g)$	$v = eg + 1 = r_1^{m_1} \cdots r_k^{m_k}$, $r_1 < \cdots < r_k :$ odd primes, $r_i \equiv 3 \bmod 4$ and $r_i = eg_i + 1$ for all i, $2 \mid g,\ p_1 > e + 1$, $\gcd(n, q-1) = \gcd(q-1, v) = \gcd(v, n) = 1$
$(n(q-1)v, n\,q(e+1), g-1)$	$v = eg + 1 = r_1^{m_1} \cdots r_k^{m_k}$, $r_1 < \cdots < r_k :$ odd primes, $r_i = eg_i + 1$ for all i, $2 \leq g \leq e,\ p_1 > e,\ (e - g + 2)q > v$, $\gcd(n, q-1) = \gcd(q-1, v) = \gcd(v, n) = 1$
$\big(n(q-1)\left(r^l - 1\right)\big), nqr^m, r^{l-m} - 1\big)$	$1 \leq m \leq n$, $p_1 > r^{l-m},\ q > \frac{r^l - 1}{r^m - 1}$, $\gcd(n, q-1) = \gcd(q-1, r^l - 1) = \gcd(r^l - 1, n) = 1$

TABLE IV

Parameters of Some New Optimal FHS Sets with Respect to the Peng-Fan Bound Obtained by Combining Constructions A and B. Here, $p, p_1, \ldots, p_k$ are primes with $p_1 < \cdots < p_k$, $n = p_1^{a_1} \cdots p_k^{a_k}$, and both q and r are prime powers.

New FHS Set $(N, M, \lambda; L)$	Individual FHS $(N, M, \lambda_{\mathrm{a}})$	Constraints
$\big(n(q-1)(r^l-1), nq\,r^m, r^{l-m}; r^m\big)$	$\big(n(q-1)(r^l-1), nq\,r^m, r^{l-m}-1\big)$ optimal	$1 \leq m \leq l,$ $p_1 > r^l,\ q > r^l$ $\gcd(n, q-1) = \gcd(q-1, r^l-1)$ $= \gcd(r^l-1) = 1$
$\big(n(q-1)p^2, nqp, p; p\big)$	$\big(n(q-1)p^2, nqp, p\big)$ near-optimal	$p_1 > p^2,\ q \geq p^2,$ $\gcd(n, q-1) = \gcd(q-1, p)$ $= \gcd(p, n) = 1$
$(n(q-1)p, nq\,(e+1), g; e)$	$(n(q-1)p, nq\,(e+1), g-1)$ optimal	$p = eg+1,$ $2 \leq g < e,$ $p_1 > p,\ q > p,$ $\gcd(n, q-1) = \gcd(q-1, p)$ $= \gcd(p, n) = 1$
$(n(q-1)(r-1), nq\,(e+1), g; e)$	$(n(q-1)(r-1), nq\,(e+1),\ g-1)$ optimal	$r = eg+1,$ $e(e+1) \geq r-1,$ $p_1 > r,\ q > q_1,$ $\gcd(n, q-1) = \gcd(q-1, r-1)$ $= \gcd(r-1, n) = 1$
$\Big(\frac{n(q-1)(r^l-1)}{h}, nq\,r^m, \frac{r^{l-m}-1}{h}; h\Big)$	$\Big(\frac{n(q-1)(r^l-1)}{h}, nq\,r^m, \frac{r^{l-m}-1}{h}\Big)$ optimal	$\gcd(n, h) = 1,$ $h \,\vert\, r-1,$ $1 \leq m \leq l,$ $p_1 > \frac{r^l-1}{h},\ q > \frac{r^l-1}{h},$ $\gcd(n, q-1) = \gcd(q-1, r^l-1)$ $= \gcd(r^l, n) = 1$
$(n(q-1)v, nq\,(e+1), g; g_1)$	$(n(q-1)v, nq\,(e+1), g-1)$ optimal	$v = eg+1 = s_1^{m_1} \cdots s_k^{m_k},$ $s_1 < \cdots < s_k :$ odd primes, $s_i = eg_i+1,\ g_1 < e \geq 2,$ $p_1 \geq eg_1,\ q(e+g-2) > v,$ $\gcd(n, q-1) = \gcd(q-1, v)$ $= \gcd(v, n) = 1$