Optimal Frequency Hopping Sequences: Auto- and Cross-Correlation Properties

doi: 10.1109/TIT.2008.2009856

Optimal Frequency Hopping Sequences: Auto- and Cross-Correlation Properties

Gennian Ge, Ying Miao, and Zhongxiang Yao

Abstract—**Frequency hopping (FH) sequences play a key role in frequency hopping spread spectrum communication systems. In order to evaluate the performance of FH sequences, Lempel and Greenberger (1974) and Peng and Fan (2004) derived lower bounds on their Hamming auto- and cross-correlations. In this paper, we construct families of FH sequences with Hamming correlations meeting those bounds by combinatorial and algebraic techniques. We first construct optimal families consisting of a single FH sequence with maximum Hamming correlation equal to 2 from a combinatorial approach. Then we investigate families consisting of multiple FH sequences. We provide a combinatorial characterization for such families, and present a recursive method to construct them by means of this characterization. We also describe two algebraic constructions for such families of FH sequences, generalizing those of Ding, Moisio, and Yuan (2007). As a consequence, many new optimal families of FH sequences are obtained.**

Index Terms—**Γ function, character sum, frequency hopping sequence, Hamming correlation, optimality, partition-type balanced nested difference packing, spread-spectrum communication, trace function.**

I. Introduction

LET $F = \{f_0, \ldots, f_{m-1}\}$ be a set of m available frequencies called a *frequency library*, and $\chi(v; F)$ be the set of all sequences $X = (x_0, \ldots, x_{v-1})$ of length v with $x_i \in F$ for $i = 0, \ldots, v-1$. Any element of $\chi(v; F)$ is called a *frequency hopping (FH) sequence* of length v over F. FH sequences are used in frequency hopping multi-access (FHMA) spread spectrum communication systems as data modulation technique to specify which frequency is used for transmission at any given time slot. Emerged from military communications for their antijamming, secure and multi-access properties, frequency hopping spread spectrum techniques are now widely used in civil communications such as "Bluetooth" and ultra-wideband (UWB) communications.

Manuscript received October 19, 2007; revised August 29, 2008. Current version published February 04, 2009. This work was supported by the National Outstanding Youth Science Foundation of China under Grant 10825103, National Natural Science Foundation of China under Grant 10771193, Zhejiang Provincial Natural Science Foundation of China, and Program for New Century Excellent Talents in University for the first author, and by JSPS Grant-in-Aid for Scientific Research (C) under Grant 18540109 for the second author.

G. Ge and Z. Yao are with the Department of Mathematics, Zhejiang University, Hangzhou 310027, Zhejiang, China (e-mail: gnge@zju.edu.cn; yaozhongxiang1@163.com).

Y. Miao is with the Department of Social Systems and Management, Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba, Ibaraki 305-8573, Japan (e-mail: miao@sk.tsukuba.ac.jp).

Communicated by G. Gong, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2008.2009856

In an FHMA spread spectrum communication system, each sender transmits a message along with switching frequencies in every time slot according to an FH sequence $X \in \mathcal{S}$ provided to him/her, where $\mathcal{S}$ is a subset of $\chi(v; F)$. FH sequences are often used periodically, i.e., they appear as $\ldots, x_{v-2}, x_{v-1}, x_0, x_1, \ldots$. The corresponding receiver then translates the received signals using the same FH sequence $X \in \mathcal{S}$. Suppose that another sender wants to transmit another message over the same frequency library F, using another FH sequence $Y = (y_0, \ldots, y_{v-1})$ from the same subset $\mathcal{S}$ of $\chi(v; F)$ starting at some time slot t. Then it may happen that the two senders transmit messages using the same frequency at the same time slot. If such signal interference occurs, then the messages transmitted at these time slots may be corrupted. Therefore it is generally desirable to keep the mutual interference, or the Hamming cross-correlations and the out-of-phase Hamming autocorrelations, as low as possible. In addition, it is also required that the frequency hopping signals have the in-phase Hamming autocorrelation as impulsive as possible so as to minimize any ambiguity about the source identity and the information in communication systems. For any two periodic FH sequences $X = (x_0, \ldots, x_{v-1}), Y = (y_0, \ldots, y_{v-1}) \in \chi(v; F)$, their Hamming correlation is defined by the number of *coincidences*, or *hits*, for relative time delay τ, i.e.

$$H_{X,Y}(\tau) = \sum_{0 \le i \le v-1} h(x_i, y_{i+\tau})$$

where

$$h(x_i, y_{i+\tau}) = \begin{cases} 0, & \text{if } x_i \neq y_{i+\tau} \\ 1, & \text{if } x_i = y_{i+\tau} \end{cases}$$

and all operations among position indices are performed modulo v. If $X \neq Y$, $H_{X,Y}(\tau)$ is the Hamming cross-correlation for relative time delay τ. If $X = Y$, $H_{X,Y}(\tau)$ is the out-of-phase Hamming autocorrelation for $\tau \not\equiv 0 \pmod v$ and the in-phase Hamming autocorrelation for $\tau \equiv 0 \pmod v$. Especially in military communications, FH sequences are also required to have large *linear span* [10], which is defined to be the length of the shortest linear feedback shift register that can produce the sequence.

In this paper, we will mainly consider the Hamming correlations of FH sequences instead of their linear spans. In Section II, we will review two known lower bounds on the Hamming correlations of FH sequences. In Section III-A, we focus on the constructions of optimal families consisting of a single FH sequence with the maximum Hamming correlations being 2 from a combinatorial approach. In Section III-B, we investigate families consisting of multiple FH sequences. We first provide a

combinatorial characterization of such families of multiple FH sequences, then present a general recursive method to construct such families by means of this characterization. We also provide two algebraic constructions for such families of FH sequences, using trace functions in Section IV-A and Γ functions in Section IV-B, respectively. Concluding remarks are listed in Section V.

II. Lower Bounds on the Hamming Correlations of FH Sequences

As is well known (see, for example, [4] and [10]), FH sequence design normally involves six parameters: the size m of the frequency library F, the sequence length v, the family size N of the subset $\mathcal{S} \subseteq \chi(v; F)$, the maximum out-of-phase Hamming autocorrelation H_a, the maximum Hamming cross-correlation H_c, and the linear span. It is generally desired that the family $\mathcal{S}$ of FH sequences has the following properties:

1) the maximum out-of-phase Hamming autocorrelation H_a should be as small as possible;
2) the maximum Hamming cross-correlation H_c should be as small as possible;
3) the family size $N = |\mathcal{S}|$ for given H_a, H_c, m and v should be as large as possible;
4) the linear span should be as large as possible.

In order to evaluate the theoretical performance of the FH sequences, it is important to find some theoretical bounds for these parameters. Given m, v and N of $\mathcal{S} \subseteq \chi(v; F)$, Lempel and Greenberger [11] and Peng and Fan [13] derived lower bounds on H_a and H_c of FH sequences in $\mathcal{S} \subseteq \chi(v; F)$. We restate their results in this section, which will be used later as the criteria to determine whether the new FH sequences constructed in this paper are optimal or not.

For any single FH sequence $X \in \chi(v; F)$, let

$$H_a(X) = \max_{1 \le \tau \le v-1} \{H_{X,X}(\tau)\}$$

be the maximum out-of-phase value of $H_{X,X}(\tau)$. If $H_a(X^*) \le H_a(X)$ for all $X \in \chi(v; F)$, then X^* is called an *optimal* FH sequence. In 1974, Lempel and Greenberger [11] developed the following lower bound on $H_a(X)$.

Theorem 2.1: [11] For any single FH sequence $X \in \chi(v; F)$ with $|F| = m$, we have

$$H_a(X) \ge \frac{(v-\epsilon)(v+\epsilon-m)}{m(v-1)}$$

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

Corollary 2.2: [7] For any single FH sequence $X \in \chi(v; F)$ with $|F| = m$, we have

$$H_a(X) \ge \begin{cases} k, & \text{if } v \ne m \\ 0, & \text{if } v = m \end{cases}$$

where $v = km + \epsilon$, $0 \le \epsilon < m$.

Corollary 2.2 implies that when $v > m$, if $H(X) = \lfloor \frac{v}{m} \rfloor$, then the single FH sequence $X \in \chi(v; F)$ is optimal.

For any two distinct FH sequences $X, Y \in \chi(v; F)$, define

$$H_c(X, Y) = \max_{0 \le \tau \le v-1} \{H_{X,Y}(\tau)\}$$

and

$$M(X, Y) = \max\{H_a(X), H_a(Y), H_c(X, Y)\}.$$

If $M(X^*, Y^*) \le M(X, Y)$ for all pairs of distinct FH sequences $\{X, Y\} \subseteq \chi(v; F)$, then $\{X^*, Y^*\} \subseteq \chi(v; F)$ is said to be an *optimal pair* of FH sequences. Lempel and Greenberger [11] also derived the following lower bound (called *Lempel–Greenberger bound*) on the value of $M(X, Y)$.

Theorem 2.3: [11] For any pair of distinct FH sequences $\{X, Y\} \subseteq \chi(v; F)$ with $|F| = m$, we have

$$M(X, Y) \ge \frac{\sum_{i=0}^{m-1}(d_i^2 + e_i^2 + d_i e_i) - 2v}{3v - 2}$$

where d_i, e_i, $0 \le i \le m-1$, denote the number of occurrences of the ith frequency $f_i \in F$ in one period of sequences X and Y, respectively. The right-hand side of the above inequality is minimized if the following conditions are satisfied:

$$d_0 \le d_1 \le \cdots \le d_{m-1} \text{ with } d_{m-1} - d_0 \le 1$$
$$e_0 \ge e_1 \ge \cdots \ge e_{m-1} \text{ with } e_0 - e_{m-1} \le 1.$$

Lempel and Greenberger [11] defined a family $\mathcal{S} \subseteq \chi(v; F)$ to be *optimal* if every pair of distinct FH sequences of $\mathcal{S}$ is an optimal pair of FH sequences. Peng and Fan [13] called such a family $\mathcal{S}$ a *Lempel–Greenberger optimal family of FH sequences.*

For any family $\mathcal{S} \subseteq \chi(v; F)$ consisting of N distinct FH sequences, define the maximum out-of-phase Hamming autocorrelation $H_a(\mathcal{S})$ and the maximum Hamming cross-correlation $H_c(\mathcal{S})$ as

$$H_a(\mathcal{S}) = \max\{H_a(X) : X \in \mathcal{S}\}$$
$$H_c(\mathcal{S}) = \max\{H_c(X, Y) : X, Y \in \mathcal{S}, X \ne Y\}$$

and the maximum nontrivial Hamming correlation $M(\mathcal{S})$ as

$$M(\mathcal{S}) = \max\{H_a(\mathcal{S}), H_c(\mathcal{S})\}.$$

In 2004, Peng and Fan [13] developed the following lower bound (called *Peng–Fan bound*) by taking into consideration the maximum values $H_a(\mathcal{S})$ and $H_c(\mathcal{S})$ separately (see also [15] for comments on [13]).

Theorem 2.4: [14], [13] For any family of FH sequences $\mathcal{S} \subseteq \chi(v; F)$ with $|F| = m$ and $|\mathcal{S}| = N$, we have

$$(v-1)NH_a(\mathcal{S}) + (N-1)NvH_c(\mathcal{S}) \ge 2IvN - (I+1)\text{Im}$$

where $I = \lfloor vN/m \rfloor$.

Peng and Fan [13] called such a family $\mathcal{S}$ *optimal* if $\{H_a(\mathcal{S}), H_c(\mathcal{S})\}$ is a pair of the minimum integer solutions of the inequality described in Theorem 2.4. They [13] showed some illustrative examples in which the Hamming correlations meet the Lempel–Greenberger bound [11] but do not meet the lower bound stated in Theorem 2.4. In order to distinguish the

optimality defined by Peng and Fan [13] from that derived from the Lempel–Greenberger bound [11], we say $\mathcal{S}$ is a *Peng–Fan optimal family of FH sequences* in this case.

When restricted to a pair of distinct FH sequences, say $X, Y \in \chi(v; F)$, Theorem 2.4 implies the following.

Theorem 2.5: [13], [14] For any pair of distinct FH sequences $\{X, Y\} \subseteq \chi(v; F)$ with $|F| = m$, we have

$$M(X, Y) \geq \frac{4Iv - (I+1)\mathrm{Im}}{4v - 2}$$

where $2v = \mathrm{Im} + r$ and $0 \leq r < m$.

We should note that the Lempel–Greenberger bound is inferior to the Peng–Fan bound for any family $\mathcal{S}$ of $\chi(v; F)$ of FH sequences. If $N = 1$, then $v = mI + \epsilon$, where $0 \leq \epsilon < m$. Substituting $I = (v - \epsilon)/m$ into Theorem 2.4, we immediately obtain Theorem 2.1, which implies that Theorem 2.1 is only a special case of Theorem 2.4. For the case $N = 2$, by a tedious verification, we can know that for any pair of distinct FH sequences $\{X, Y\} \subseteq \chi(v; F)$, the Peng-Fan bound on $M(X, Y)$ is always tighter than or equal to the Lempel–Greenberger bound on $M(X, Y)$. Therefore, when we consider the optimality of any pair of distinct FH sequences, we should use the Peng–Fan bound in Theorem 2.4.

III. Combinatorial Constructions

From now on, we consider the constructions of optimal FH sequences. As being witnessed in [7] and [9], combinatorial approach is very effective in the construction of optimal families consisting of a single FH sequence. In fact, as we will see in this section, this approach can also be used in the construction of optimal families consisting of multiple FH sequences.

A. Families Consisting of a Single Sequence

We first consider the case when the family $\mathcal{S}$ of FH sequences consists of only one sequence, i.e., $N = |\mathcal{S}| = 1$, or equivalently, we suppose that all senders use the same FH sequence, starting from different time slots. In this case, there is no ambiguity in the definition of optimality, so we can use the word "optimal" in the remainder of this paper for $|\mathcal{S}| = 1$. We will construct several new series of cyclic frames, and then use a known "frame construction" in [9] to produce new series of optimal families consisting of a single FH sequence.

We begin with some terminologies in combinatorial design theory. Let $\mathcal{P}$ be a collection of m subsets (called *blocks*) $B_0, \ldots, B_{m-1}$ of $\mathbf{Z}_v$, where $\mathbf{Z}_v$ is the residue ring of integers modulo v. $\mathcal{P} = \{B_0, \ldots, B_{m-1}\}$ is said to form a *difference packing* over $\mathbf{Z}_v$ and denoted by m-DP(v, K, λ), where K is the set of sizes of the blocks B_i, i.e., $K = \{|B_i| : 0 \leq i \leq m-1\}$, if, for each $d \in \mathbf{Z}_v \setminus \{0\}$, the ordered pairs $(a, b) \in B_i \times B_i$ such that $d \equiv a - b \pmod{v}$ appear at most λ times in $B_0, \ldots, B_{m-1}$. If each $d \in \mathbf{Z}_v \setminus \{0\}$ appears exactly λ times as the differences arising from $B_0, \ldots, B_{m-1}$, then $\mathcal{P}$ is called a *difference family*, denoted by (v, K, λ)-difference family. If every element of $\mathbf{Z}_v$ is contained in exactly one block of $\mathcal{P}$, then the m-DP(v, K, λ) is called a *partition-type difference packing*.

Fuji-Hara *et al.* [7] revealed a connection between FH sequences and partition-type difference packings.

Theorem 3.1: [7] There exists an FHS(v, m, λ) over a frequency library $F = \{0, \ldots, m-1\}$ if and only if there exists a partition-type m-DP(v, K, λ), $\mathcal{P} = \{B_0, \ldots, B_{m-1}\}$, over $\mathbf{Z}_v$, where $K = \{|B_i| : 0 \leq i \leq m-1\}$.

Lemma 3.2: [7] Let $v = km + m - 1$ with $k \geq 1$. Then there exists an optimal FHS(v, m, k) if and only if there exists a partition-type m-$(v, \{k, k+1\}, k)$-difference family in which $m-1$ blocks are of size $k+1$ and the remaining one is of size k.

If we take $k = 2$ in Lemma 3.2 for arbitrary $v = 3m - 1$, we would like to know whether there exists an optimal FHS$(3m - 1, m, 2)$. In FHMA communications, if the maximum number of coincidences or hits between any pair of FH sequences for any shift is 2, then the mutual interference is kept at a defined and low level, resulting in low-error probability. Meanwhile, if such FH sequences are assigned to users, then each frequency is used only twice or three times within the sequence period, which would facilitate a simple synchronization scheme.

In order to construct optimal FHS$(3m - 1, m, 2)$, or equivalently, partition-type m-$(3m - 1, \{2, 3\}, 2)$-difference families in which $m - 1$ blocks are of size 3 and the remaining one is of size 2, we need the concept of a cyclic frame. Let k be a positive integer. A *group divisible design* (k, λ)-GDD is a triple $(X, \mathbf{G}, \mathbf{B})$ where X is a finite set of elements called *points*, $\mathbf{G}$ is a set of subsets of X called *groups* which partition X, $\mathbf{B}$ is a collection of k-subsets of X called *blocks* such that every pair of points from distinct groups occurs in exactly λ blocks, and no pair of points belonging to a group occurs in any block. We use the usual exponential notation for the *type* of GDDs. Thus a GDD of type $1^i 2^j \cdots$ is one in which there are i groups of size 1, j groups of size 2, and so on. A (k, λ)-*frame* of type T is a (k, λ)-GDD $(X, \mathbf{G}, \mathbf{B})$ of type T in which the collection $\mathbf{B}$ of blocks can be partitioned into *holey resolution classes* each of which partitions $X \setminus G_i$ for some $G_i \in \mathbf{G}$.

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

In a $(k, k-1)$-frame of type h^n, it is well known (see [8] for example) that there are h holey resolution classes associated with each group, and there are altogether nh holey resolution

classes. If the underlying GDD of a $(k, k-1)$-frame of type h^n is cyclic with respect to an automorphism $\sigma : i \longmapsto i+1 \pmod{nh}$ of order $nh = |X|$, such that the blocks of the jth holey resolution class $\mathcal{R}_j$ are the jth translates of the blocks of the resolution class $\mathcal{R}_0$, i.e., $\mathcal{R}_j = \mathcal{R}_0^{\sigma^j} = \mathcal{R}_0 + j \pmod{nh}$ for all $j \in \mathbf{Z}_{nh}$, then the frame is said to be *cyclic* with respect to σ. The class $\mathcal{R}_0$ is an *initial holey resolution class* of this cyclic frame.

Now we state the following elementary but important result.

Lemma 3.3: For any integer $t \geq 0$, if there exists a cyclic $(3,2)$-frame of type 2^{3t+1}, then there also exist both a partition-type $(2t+1)$-$(6t+2, \{2,3\}, 2)$-difference family in which $2t$ blocks are of size 3 and the remaining one is of size 2, and an optimal $\mathrm{FHS}(6t+2, 2t+1, 2)$.

Proof: Let $\mathbf{B}_0$ be the initial holey resolution class of a cyclic $(3,2)$-frame of type 2^{3t+1} which partitions $\mathbf{Z}_{6t+2} \setminus (3t+1)\mathbf{Z}_2$. Then the $2t$ base blocks of $\mathbf{B}_0$ together with $\{0, 3t+1\}$ form the desired partition-type $(6t+2, \{2,3\}, 2)$-difference family. Apply Lemma 3.2. □

In the following two lemmas, we construct two new infinite series of cyclic $(3,2)$-frames, which immediately imply two new infinite series of optimal FH sequences.

Lemma 3.4: There exists a cyclic $(3,2)$-frame of type 2^p and thus an optimal $\mathrm{FHS}(2p, (2p+1)/3, 2)$ for any prime $p \equiv 1 \pmod 6$.

Proof: Let $p = 6s+1$ for some positive integer s, and let $\xi \in \mathbf{F}_p$ be a primitive element of the finite filed $\mathbf{F}_p$ of order p. Let $\theta = (\xi^s + 1)/2$. Define $X = \mathbf{F}_p \times \mathbf{Z}_2$. Then the desired $(3,2)$-frame of type 2^p can be obtained by taking the following base blocks over the additive group of $\mathbf{F}_q \times \mathbf{Z}_2$, which form an initial holey resolution class

$$\begin{aligned}
&\{(\xi^i, 0), (\xi^{i+s}, 0), (\theta\xi^i, 1)\},\\
&\quad 0 \leq i \leq s-1,\ 2s \leq i \leq 3s-1,\ 4s \leq i \leq 5s-1,\\
&\{(\theta\xi^{i+s}, 1), (\theta\xi^{i+3s}, 1), (\theta\xi^{i+5s}, 1)\},\\
&\quad 0 \leq i \leq s-1.
\end{aligned}$$

Then apply Lemma 3.3. □

As being described in [9], cyclic $(3,2)$-frames with other group size can also be used to obtain optimal FH sequences with maximum number of coincidences or hits between any pair of sequences for any shift being 2. Lemma 3.5 shows such an example. The interested reader is referred to [9] for more details.

Lemma 3.5: There exists a cyclic $(3,2)$-frame of type 8^p and thus an optimal $\mathrm{FHS}(8p, (8p+1)/3, 2)$ for any prime $p \equiv 7, 13 \pmod{18}$.

Proof: Let $p = 18s+7$ or $18s+13$, and let $\xi \in \mathbf{F}_p$ be a primitive element. Define $X = \mathbf{F}_p \times \mathbf{Z}_8$, and let $H_0 = \{\xi^0, \xi^3, \xi^6, \ldots, \xi^{p-4}\}$ be the subgroup of index 3 of the multiple group of $\mathbf{F}_p$. Then the desired $(3,2)$-frame of type 8^p can be obtained by taking the following $8(p-1)/3$ base blocks over the additive group of $\mathbf{F}_p \times \mathbf{Z}_8$, which form an initial holey resolution class:

$$\begin{aligned}
&\{(1,0), (\xi^{2s}, 0), (\xi^{4s}, 0)\} \times r, && r \in H_0\\
&\{(1,1), (\xi^{2s}, 2), (\xi^{4s}, 3)\} \times r, && r \in H_0\\
&\{(1,2), (\xi^{2s}, 3), (\xi^{4s}, 6)\} \times r, && r \in H_0\\
&\{(1,3), (\xi^{2s}, 6), (\xi^{4s}, 2)\} \times r, && r \in H_0\\
&\{(1,4), (\xi^{2s}, 7), (\xi^{4s}, 5)\} \times r, && r \in H_0\\
&\{(1,5), (\xi^{2s}, 1), (\xi^{4s}, 7)\} \times r, && r \in H_0\\
&\{(1,6), (\xi^{2s}, 4), (\xi^{4s}, 1)\} \times r, && r \in H_0\\
&\{(1,7), (\xi^{2s}, 5), (\xi^{4s}, 4)\} \times r, && r \in H_0.
\end{aligned}$$

Adding three new blocks $\{(0,0), (4,0)\}$, $\{(1,0), (6,0), (7,0)\}$ and $\{(2,0), (3,0), (5,0)\}$ to the above, we obtain a partition-type $(8p+1)/3$-$(8p, \{2,3\}, 2)$-difference family in which $(8p-2)/3$ blocks are of size 3 and the remaining one of size 2. Then apply Lemma 3.2. □

The first half of Lemma 3.5 can be generalized by introducing the notation of a *double difference matrix*. Let $\sum = (\sigma_{ij})$ be an $m \times n$ matrix with entries from $\mathbf{Z}_n$. If $\bigcup_{j=1}^{n} \sigma_{ij} = \mathbf{Z}_n$ for $i = 1, 2, \ldots, m$, and $\bigcup\{\pm(\sigma_{hj} - \sigma_{ij}) : j = 1, 2, \ldots, n\} = 2\mathbf{Z}_n$ for any $h \neq i$, where $1 \leq h, i \leq m$, then $\sum$ is called an (m,n)-double difference matrix (or (m,n)-DDM for short) over $\mathbf{Z}_n$. It can be easily checked that the matrix composed of the second components of points in the eight representative base blocks in Lemma 3.5, that is

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7\\ 0 & 2 & 3 & 6 & 7 & 1 & 4 & 5\\ 0 & 3 & 6 & 2 & 5 & 7 & 1 & 4 \end{pmatrix}$$

is in fact a $(3,8)$-DDM over $\mathbf{Z}_8$. We can also easily check that

$$\begin{pmatrix} 0 & 1 & 2 & 3\\ 0 & 2 & 3 & 1\\ 0 & 3 & 1 & 2 \end{pmatrix}$$

is also a $(3,4)$-DDM over $\mathbf{Z}_4$.

Replacing the $8(p-1)/3$ base blocks over the additive group of $\mathbf{F}_p \times \mathbf{Z}_8$ in Lemma 3.5 by the following $n(p-1)/3$ base blocks over the additive group of $\mathbf{F}_p \times \mathbf{Z}_n$:

$$\begin{aligned}
&\{(1, \sigma_{11}), (\xi^{2s}, \sigma_{21}), (\xi^{4s}, \sigma_{31})\} \times r, && r \in H_0\\
&\{(1, \sigma_{12}), (\xi^{2s}, \sigma_{22}), (\xi^{4s}, \sigma_{32})\} \times r, && r \in H_0\\
&\qquad\vdots && \qquad\vdots\\
&\{(1, \sigma_{1m}), (\xi^{2s}, \sigma_{2m}), (\xi^{4s}, \sigma_{3m})\} \times r, && r \in H_0
\end{aligned}$$

where $\sum = (\sigma_{ij})$ is a $(3,n)$-DDM, we easily obtain the following result.

Lemma 3.6: If there exists a $(3,n)$-DDM over $\mathbf{Z}_n$, then there exists a cyclic $(3,2)$-frame of type n^p for any prime $p \equiv 7, 13 \pmod{18}$ such that $\gcd(p, n) = 1$.

So it is also interesting to construct double difference matrices. To do this, we need the concept of a difference matrix.

Let $\Gamma = (\gamma_{ij})$ be a $t \times \lambda n$ matrix with entries from $\mathbf{Z}_n$. If each element of $\mathbf{Z}_n$ occurs exactly λ times in the multiset of differences $\{\gamma_{hj} - \gamma_{ij} : j = 1, 2, \ldots, \lambda n\}$ for any $h \neq i$, where $1 \leq h, i \leq t$, then Γ is called a $(t, n; \lambda)$-*difference matrix* (or $(t, n; \lambda)$-DM for short) over $\mathbf{Z}_n$. It is easy to see that the property of a difference matrix is preserved even if we add any element of $\mathbf{Z}_n$ to all entries in any row or column of the difference matrix. Then, without loss of generality, we can assume that all entries in the first row are zero. Such a difference matrix is said to be *normalized*. The difference matrix obtained from a normalized $(t, n; \lambda)$-DM by deleting the entries in its first row is said to be *homogeneous*. It is obvious that in a homogeneous difference matrix, any element of $\mathbf{Z}_n$ appears in every row λ times. The existence of a homogeneous $(t-1, n; \lambda)$-DM is equivalent to that of a $(t, n; \lambda)$-DM. The interested reader is referred to [2] for more detailed information on difference matrices.

Theorem 3.7: If there exist both a (t, m)-DDM over $\mathbf{Z}_m$ and a homogeneous $(t, n; 1)$-DM over $\mathbf{Z}_n$, then there also exists a (t, mn)-DDM over $\mathbf{Z}_{mn}$.

Proof: Assume that the (t, m)-DDM is

$$\mathbf{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \cdots & \vdots \\ a_{t1} & a_{t2} & \cdots & a_{tm} \end{pmatrix}$$

and the $(t, n; 1)$-DM is

$$\mathbf{B} = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ b_{t1} & b_{t2} & \cdots & b_{tn} \end{pmatrix}.$$

For every $i = 1, 2, \ldots, m$, denote

$$\mathbf{D}_i = \begin{pmatrix} a_{1i} + b_{11}m & a_{1i} + b_{12}m & \cdots & a_{1i} + b_{1n}m \\ a_{2i} + b_{21}m & a_{2i} + b_{22}m & \cdots & a_{2i} + b_{2n}m \\ \vdots & \vdots & \cdots & \vdots \\ a_{ti} + b_{t1}m & a_{ti} + b_{t2}m & \cdots & a_{ti} + b_{tn}m \end{pmatrix}$$

and define

$$\mathbf{D} = (\mathbf{D}_1 \quad \mathbf{D}_2 \quad \cdots \quad \mathbf{D}_m).$$

Then it is readily checked that $\mathbf{D}$ is the desired $(3, mn)$-DDM over $\mathbf{Z}_{mn}$. □

B. Families Consisting of Multiple Sequences

Families consisting of multiple FH sequences are more interesting than those consisting of only one FH sequence, at least for the reason that they allow more users to communicate in the FHMA spread spectrum communication systems. In this subsection, we focus on families consisting of multiple FH sequences. We first provide a combinatorial characterization of such families, then describe a general recursive method to construct optimal them by means of this characterization.

1) A Combinatorial Characterization: The central idea of the combinatorial approach used in Section III-A for designing FH sequences is to regard a single FH sequence as a partition-type difference packing. In fact, this idea can be extended to families consisting of multiple FH sequences by regarding a family consisting of multiple FH sequences as a family of partition-type difference packings with "nested" property. Combinatorial structures with such "nested" property were investigated in [6]. For convenience, a family of N FHS$(v, m, \Lambda_a, \Lambda_c)$ will denote a family of N FH sequences $\{X_1, \ldots, X_N\}$ with length v over a frequency library of size m having Hamming autocorrelations $\Lambda_a = \{H_a(X_1), \ldots, H_a(X_N)\}$ and Hamming cross-correlations $\Lambda_c = \{H_c(X_j, X_k) : 1 \leq j, k \leq N, j \neq k\}$.

Let P_j, $1 \leq j \leq N$, be a collection of m subsets (called *blocks*) $B_0^j, \ldots, B_{m-1}^j$ of $\mathbf{Z}_v$, respectively. The N collections $P_1, \ldots, P_N$ are said to form a *family of balanced nested difference packings* over $\mathbf{Z}_v$, denoted by N-BNDP$(v, m, K, \Lambda_a, \Lambda_c)$, where $K = \{K_1, \ldots, K_N\}$, $K_j = \{|B_i^j| : 0 \leq i \leq m-1\}$, $1 \leq j \leq N$, if for each $d \in \mathbf{Z}_v \setminus \{0\}$, the ordered pairs $(a, b) \in B_i^j \times B_i^j$ such that $d \equiv a - b \pmod v$ appear at most λ_j times in $B_0^j, \ldots, B_{m-1}^j$ for each j, and for each $d \in \mathbf{Z}_v$, the ordered pairs $(a, b) \in B_i^j \times B_i^k$ such that $d \equiv a - b \pmod v$ appear at most $\lambda_{j,k}$ times in all pairs $(B_0^j, B_0^k), \ldots, (B_{m-1}^j, B_{m-1}^k)$, where $\Lambda_a = \{\lambda_j : 1 \leq j \leq N\}$ and $\Lambda_c = \{\lambda_{j,k} : 1 \leq j, k \leq N, j \neq k\}$. If every element of $\mathbf{Z}_v$ is contained in exactly one block of P_j for each $j = 1, 2, \ldots, N$, then the N-BNDP$(v, m, K, \Lambda_a, \Lambda_c)$ is called a family of balanced nested difference packing of *partition-type*, or a partition-type N-BNDP$(v, m, K, \Lambda_a, \Lambda_c)$ for short.

Lemma 3.8: There exists a family of N FHS$(v, m, \Lambda_a, \Lambda_c)\{X_1, X_2, \ldots, X_N\}$ if and only if there exist N partitions of $\mathbf{Z}_v$

$$P_1 = \{B_0^1, \ldots, B_{m-1}^1\}, \ldots, P_N = \{B_0^N, \ldots, B_{m-1}^N\}$$

such that

$$\lambda_j = H_a(X_j) = \max_{1 \leq t < v} \{\sum_{i=0}^{m-1} |B_i^j \cap (B_i^j + t)|\}, \quad 1 \leq j \leq N$$

$$\lambda_{j,k} = H_c(X_j, X_k) = \max_{0 \leq t < v} \{\sum_{i=0}^{m-1} |B_i^j \cap (B_i^k + t)|\}, \quad 1 \leq j, k \leq N, \ j \neq k$$

where $B_i^j + t = \{b^j + t \pmod v : b^j \in B_i^j\}$.

Proof: Let the frequency library be $F = \{0, 1, \ldots, m-1\}$, and the support of $i \in F$ in $X_j = (x_0^j, \ldots, x_{v-1}^j)$ be $B_i^j = \{m : x_m^j = i, \ 0 \leq m \leq v-1\}$. By defining

$$h_i(x, y) = \begin{cases} 1, & \text{if } x = y = i, \\ 0, & \text{otherwise} \end{cases}$$

for $i \in F$, we have

$$|B_i^j \cap (B_i^k + t)| = \sum_{l=0}^{v-1} h_i(x_l^j, x_{l-t}^k),$$

which implies that

$$\begin{aligned}\sum_{i=0}^{m-1} |B_i^j \cap (B_i^k + t)| &= \sum_{i=0}^{m-1} \sum_{l=0}^{v-1} h_i(x_l^j, x_{l-t}^k) \\ &= \sum_{l=0}^{v-1} \sum_{i=0}^{m-1} h_i(x_l^j, x_{l-t}^k) \\ &= \sum_{l=0}^{v-1} h(x_l^j, x_{l-t}^k) \\ &= H_{X_j, X_k}(-t).\end{aligned}$$

Then if $j = k$, we have

$$\begin{aligned}\max_{1 \le t < v} \left\{ \sum_{i=0}^{m-1} |B_i^j \cap (B_i^k + t)| \right\} &= \max_{1 \le t < v} \{H_{X_j, X_k}(-t)\} \\ &= H_a(X_j) \\ &= \lambda_j,\end{aligned}$$

otherwise, we have

$$\begin{aligned}\max_{0 \le t < v} \left\{ \sum_{i=0}^{m-1} |B_i^j \cap (B_i^k + t)| \right\} &= \max_{0 \le t < v} \{H_{X_j, X_k}(-t)\} \\ &= H_c(X_j, X_k) \\ &= \lambda_{j,k}.\end{aligned}$$

□

Theorem 3.9: There exists a family of N FHS$(v, m, \Lambda_a, \Lambda_c)$ over a frequency library $F = \{0, 1, \ldots, m-1\}$ if and only if there exists a partition-type N-BNDP$(v, m, K, \Lambda_a, \Lambda_c)$ over $\mathbf{Z}_v$, $P_j = \{B_0^j, \ldots, B_{m-1}^j\}$, $1 \le j \le N$, where $K = \{K_1, \ldots, K_N\}$ and $K_j = \{|B_i^j| : 0 \le i \le m-1\}$.

Proof: Let $1 \le j, k \le N$. We first consider the case $j \ne k$. Let $B^j \in P_j$ and $B^k \in P_k$. For any $d \in \mathbf{Z}_v$, we prove that the number of ordered pairs $(a, b) \in B^j \times B^k$ such that $a - b \equiv d \pmod v$ is equal to $|B^j \cap (B^k + d)|$.

Let $(a_1, b_1), \ldots, (a_r, b_r)$ be all the ordered pairs in $B^j \times B^k$ whose ordered differences are d. Since $a_1, \ldots, a_r$ are all distinct and contained in $B^k + d$, so $|B^j \cap (B^k + d)| \ge r$. On the other hand, suppose $B^j \cap (B^k + d) = \{a_1, \ldots, a_l\}$. Then $b_1 = a_1 - d, \ldots, b_l = a_l - d$ are all contained in B^k, which implies that there exist at least l ordered pairs $(a_1, b_1), \ldots, (a_l, b_l) \in B^j \times B^k$ whose ordered differences are d. That is, $|B^j \cap (B^k + d)| = l \le r$. Hence, $|B^j \cap (B^k + d)| = r$.

Let $\lambda_d(B_i^j \times B_i^k)$ be the number of pairs in $B_i^j \times B_i^k$ whose ordered differences are d for each $B_i^j \in P_j, B_i^k \in P_k$. From the above consequence

$$\sum_{i=0}^{m-1} \lambda_d(B_i^j \times B_i^k) = \sum_{i=0}^{m-1} |B_i^j \cap (B_i^k + d)|.$$

So we have that $\sum_{i=0}^{m-1} \lambda_d(B_i^j \times B_i^k) \le \lambda_{j,k}$ for any $d \in \mathbf{Z}_v$ if and only if $\sum_{i=0}^{m-1} |B_i^j \cap (B_i^k + d)| \le \lambda_{j,k}$ for any $d \in \mathbf{Z}_v$.

The case $j = k$ can be proved in a similar way for any $d \in \mathbf{Z}_v \setminus \{0\}$. □

We note that there is some symmetry in differences. It can be easily checked that $\lambda_{j,k} = \lambda_{k,j}$ holds for any $1 \le j, k \le N$, $j \ne k$. Therefore, when we compute Λ_c, we need only compute $\lambda_{j,k}$ for $1 \le j < k \le N$.

This characterization builds a bridge between combinatorial designs and families of FH sequences, which would facilitate the construction for optimal families consisting of multiple FH sequences. There are several established construction methods in combinatorial design theory. We expect that some of them could be specified to work for these special families of balanced nested difference packings of partition-type, which would immediately imply families consisting of multiple FH sequences. The recursive construction described in the next subsection is one of such successful examples.

2) A Recursive Construction via Difference Matrices: Combinatorial direct constructions and algebraic constructions often produce families of FH sequences with restricted lengths related to prime powers, for the reason that they are mainly based on finite fields. Combinatorial recursive constructions, on the other hand, can produce families of FH sequences with composite lengths. All these construction methods are indispensable in constructing optimal families of FH sequences.

The combinatorial characterization in Section III-B1 enables us to develop a general recursive construction for families consisting of multiple FH sequences via difference matrices. Fujiwara and Fuji-Hara [5] described a similar but restrictive recursive construction which is stated only for families of FH sequences obtained via cyclotomy by Chu and Colbourn [1].

Theorem 3.10: Assume that $\mathcal{S}$ is a family of N FHS$(v, m, \Lambda_a, \Lambda_c)$ in which one frequency appears in a fixed position, say the 0th position, and each of the other frequencies appears in different non-0th positions of the N FH sequences of $\mathcal{S}$. Assume also that $\mathcal{T}$ is a family of N FHS$(w, n, \Lambda_a, \Lambda_c)$. If there exists a homogeneous difference matrix $(u, w; 1)$-DM over $\mathbf{Z}_w$, where u is the maximum number of total occurrences that frequencies appear in all the N FH sequences of $\mathcal{S}$, then there also exists a family $\mathcal{F}$ of N FHS$(vw, (m-1)w + n, \Lambda_a, \Lambda_c)$.

Proof: Without loss of generality, we may assume that the two families $\mathcal{S}, \mathcal{T}$ of FH sequences are defined over $F = \{0, 1, \ldots, m-1\}$ and $F' = \{0, 1, \ldots, n-1\}$, respectively, where $0 \in F$ appears in the 0th position and each $i \in F \setminus \{0\}$ appears in different non-0th positions of the N FH sequences of $\mathcal{S}$. By Theorem 3.9, $\mathcal{S}$ corresponds to a partition-type N-BNDP$(v, m, K, \Lambda_a, \Lambda_c)$ over $\mathbf{Z}_v$, $P_j = \{A_0^j, \ldots, A_{m-1}^j\}$, $1 \le j \le N$, where $A_0^j = \{0\}$, $A_i^j \cap A_i^{j'} = \emptyset$ for $i \in F \setminus \{0\}$ and $1 \le j \ne j' \le N$, $A_1^j \cup \cdots \cup A_{m-1}^j = \mathbf{Z}_v \setminus \{0\}$, and $K = \{K_1, \ldots, K_N\}$, $K_j = \{|A_i^j| : 0 \le i \le m-1\}$. Also, $\mathcal{T}$ corresponds to a partition-type N-BNDP$(w, n, K', \Lambda_a, \Lambda_c)$ over $\mathbf{Z}_w$, $Q_l = \{B_0^l, \ldots, B_{n-1}^l\}$, $1 \le l \le N$, where $K' =$

$K'_1, \ldots, K'_N\}$ and $K'_l = \{|B^l_i| : 0 \le i \le n-1\}$. Let $= (\gamma_{ij})$ be the homogeneous $(u, w; 1)$-DM over $\mathbf{Z}_w$, where $= \max_{0\le i\le m-1}\{\sum_{j=1}^{N} |A^j_i|\}$. For each collection of the following N mutually disjoint blocks

$$A^1_i = \{a^1_{i,1}, \ldots, a^j_{i,k_1}\}$$
$$A^2_i = \{a^2_{i,k_1+1}, \ldots, a^2_{i,k_2}\}$$
$$\vdots$$
$$A^N_i = \{a^N_{i,k_{N-1}+1}, \ldots, a^N_{i,k_N}\}$$

ere $1 \le i \le m-1$, we construct the following Nw new ıcks:

$$(k) = \{a^j_{i,k_{j-1}+1} + \gamma_{k_{j-1}+1,k}v, \ldots, a^j_{i,k_j} + \gamma_{k_j,k}v\}, \quad 1 \le j \le N,\ 1 \le k \le w.$$

en it can be readily checked that each element of $\mathbf{Z}_{vw} \setminus v\mathbf{Z}_w$ ı be represented as the difference $x - x'$ of two distinct elıents $x, x' \in A^j_i(k)$, $1 \le i \le m-1$, $1 \le k \le w$, in at ›st $\lambda_j \in \Lambda_a$ ways for any $1 \le j \le N$, and each element of $_w \setminus v\mathbf{Z}_w$ can be represented as the difference $y - y'$ of two ;tinct elements $y \in A^j_i(k)$, $y' \in A^{j'}_i(k)$, $1 \le i \le m-1$, $\le k \le w$, in at most $\lambda_{j,j'} \in \Lambda_c$ ways for any $1 \le j \ne \le N$. Meanwhile, it can also be readily checked that for any $\le j \le N$, the newly defined blocks $A^j_i(k)$, $1 \le i \le m-1$, $\le k \le w$, partition $\mathbf{Z}_{vw} \setminus v\mathbf{Z}_w$. By adding the collecn of blocks $\{vB^j_0, \ldots, vB^j_{n-1}\}$ to the collection of blocks $\mathrm{L}^j_i(k) : 1 \le i \le m-1,\ 1 \le k \le w\}$ for any $1 \le j \le N$, we tain a family of N FHS$(vw, (m-1)w + n, \Lambda_a, \Lambda_c)$. □

The optimality of the resultant family $\mathcal{F}$ of FH sequences can checked for any specified ingredients in Theorem 3.10. For ample, we can readily check that by applying Theorem 3.10, ; Lempel–Greenberger optimal families of FH sequences obned via cyclotomy (see [1]) satisfy all the conditions required Theorem 3.10 by a suitable permutation of frequencies, and ıs can be used to produce new optimal families of FH seences with longer length and larger frequency library but inriant Hamming correlations, where the required difference ıtrices can be found in, say, [2]. We omit the tedious verifition here.

IV. Algebraic Constructions

Families consisting of multiple FH sequences can also be nstructed from an algebraic approach. In this section, we scribe two algebraic constructions for optimal families con›sting of multiple FH sequences, which are generalizations of ose in [3].

A Construction via Trace Functions

Throughout this subsection, p will denote a prime and $q = p^r$ r some positive integer r. Suppose that m, l are two positive tegers satisfying $l \mid (q^m - 1)$ and $\gcd(\frac{q^m-1}{q-1}, l) = 1$. In this se, $l \mid (q-1)$. Let α be a primitive element of $\mathbf{F}_{q^m}$, s be a ›sitive integer with $\gcd(s, q^m - 1) = 1$, and let $\beta = \alpha^{ls}$. enote $n = \frac{q^m-1}{l}$.

In [3], Ding, Moisio, and Yuan constructed a Lempel–Greenberger optimal pair of FH sequences in the case that p and m are odd while $l = 2$ by defining the following sequence of length n over $\mathbf{F}_q$:

$$\mathbf{c}_g = (\mathrm{Tr}_{q^m/q}(g), \mathrm{Tr}_{q^m/q}(g\beta), \ldots, \mathrm{Tr}_{q^m/q}(g\beta^{n-1}))$$

for every $g \in \mathbf{F}_{q^m}$, where $\mathrm{Tr}_{q^m/q}$ denotes the trace function from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$.

In this subsection, we will generalize the above Ding, Moisio, and Yuan's construction. We need the following result in our proof, where G is the Gaussian sum defined by $G(\eta, \chi) = \sum_{g\in\mathbf{F}^*_{q^m}} \eta(g)\chi(g)$ for any multiplicative character η of $\mathbf{F}_{q^m}$ and any additive character χ of $\mathbf{F}_{q^m}$.

Lemma 4.1: ([12, Th. 5.30]) Let χ be a nontrivial additive character of $\mathbf{F}_q$, $n \in \mathbf{N}$, and λ a multiplicative character of $\mathbf{F}_q$ of order $d = \gcd(n, q-1)$. Then

$$\sum_{g\in\mathbf{F}_q} \chi(fg^n + h) = \chi(h)\sum_{j=1}^{d-1} \bar{\lambda}^j(f)G(\lambda^j, \chi)$$

for any $f, h \in \mathbf{F}_q$ with $f \ne 0$.

Lemma 4.2: The Hamming weight of $\mathbf{c}_g$ defined above is given by

$$w(\mathbf{c}_g) = \begin{cases} 0, & \text{if } g = 0, \\ \frac{q^m - q^{m-1}}{l}, & \text{if } g \in \mathbf{F}^*_{q^m}. \end{cases}$$

Proof: Our proof is a generalization of that for [3, Lemma 7]. If $g = 0$, then $\mathbf{c}_g$ is the all-zero sequence and thus $w(\mathbf{c}_g) = 0$. Now assume $g \ne 0$. Let $\tilde{\chi}$ and χ be the canonical additive character of $\mathbf{F}_q$ and $\mathbf{F}_{q^m}$, respectively, and $\tilde{\eta}$ and η be the lth multiplicative character of $\mathbf{F}_q$ and $\mathbf{F}_{q^m}$, respectively. Let $\mathrm{Tr}_{q/p}$ denote the trace function from $\mathbf{F}_q$ to $\mathbf{F}_p$. Then we have

$$\begin{aligned} n - w(\mathbf{c}_g) &= \sum_{j=0}^{n-1} \frac{1}{q} \sum_{c\in\mathbf{F}_q} \tilde{\chi}(cTr_{q^m/q}(g\beta^j)) \\ &= \sum_{j=0}^{n-1} \frac{1}{q} \sum_{c\in\mathbf{F}_q} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q/p}(cTr_{q^m/q}(g\beta^j))} \\ &= \frac{1}{q}(n + \sum_{c\in\mathbf{F}^*_q}\sum_{j=0}^{n-1} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q/p}(\mathrm{Tr}_{q^m/q}(gc\beta^j))}) \\ &= \frac{1}{q}(n + \sum_{c\in\mathbf{F}^*_q}\sum_{j=0}^{n-1} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(gc\alpha^{lsj})}) \\ &= \frac{1}{q}(n + \sum_{c\in\mathbf{F}^*_q}\frac{1}{l}\sum_{k=0}^{q^m-2} e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(gc\alpha^{lsk})}) \\ &= \frac{1}{q}(n + \sum_{c\in\mathbf{F}^*_q}\frac{1}{l}(\sum_{x\in\mathbf{F}_{q^m}} \chi(gcx^l) - 1)). \end{aligned}$$

By Lemma 4.1, we know that

$$\sum_{x\in\mathbf{F}_{q^m}} \chi(gcx^l) = \sum_{j=1}^{l-1} \tilde{\eta}^j(gc)G(\eta^j, \chi)$$

so we have

$$n - w(\mathbf{c}_g) = \frac{1}{q}(n + \sum_{c\in\mathbf{F}_q^*}\frac{1}{l}(\sum_{j=1}^{l-1}\bar{\eta}^j(gc)G(\eta^j,\chi) - 1))$$
$$= \frac{1}{q}(n - \frac{q-1}{l} + \frac{1}{l}\sum_{j=1}^{l-1}G(\eta^j,\chi)\sum_{c\in\mathbf{F}_q^*}\bar{\eta}^j(gc)).$$

Since α is a primitive element of $\mathbf{F}_{q^m}$, $\tilde{\alpha} = \alpha^{\frac{q^m-1}{q-1}}$ is obviously a primitive element of $\mathbf{F}_q$. Then for any $c = \tilde{\alpha}^k \in \mathbf{F}_q^*$ and any $j \in \{1,2,\ldots,l-1\}$

$$\eta^j(c) = \eta^j(\tilde{\alpha}^k) = \eta^j(\alpha^{\frac{q^m-1}{q-1}k}) = e^{2\pi i\frac{k}{l}\frac{q^m-1}{q-1}j}.$$

By the assumption that $\gcd(\frac{q^m-1}{q-1}, l) = 1$, we know that for any $j \in \{1,2,\ldots,l-1\}$, η^j is not the trivial multiplicative character $\tilde{\eta}_0$ when it is restricted on $\mathbf{F}_q$, where $\tilde{\eta}_0(c) = 1$ for any $c = \tilde{\alpha}^k \in \mathbf{F}_q^*$. Hence $\sum_{c\in\mathbf{F}_q^*}\eta^j(c) = 0$ for any $j \in \{1,2,\ldots,l-1\}$, which implies

$$\sum_{c\in\mathbf{F}_q^*}\eta^j(gc) = \sum_{c\in\mathbf{F}_q^*}\eta^j(g)\eta^j(c) = \eta^j(g)\sum_{c\in\mathbf{F}_q^*}\eta^j(c) = 0$$

and

$$n - w(\mathbf{c}_g) = \frac{1}{q}\left(n - \frac{q-1}{l} + \frac{1}{l}\sum_{j=1}^{l-1}G(\eta^j,\chi)\times\bar{0}\right)$$
$$= \frac{1}{q}\left(n - \frac{q-1}{l}\right)$$
$$= \frac{1}{q}\frac{q^m-q}{l}$$
$$= \frac{q^{m-1}-1}{l}.$$

Therefore,

$$w(\mathbf{c}_g) = n - \frac{q^{m-1}-1}{l} = \frac{q^m - q^{m-1}}{l}. \quad \square$$

In a way similar to that in [3], we can determine the autocorrelation values of $\mathbf{c}_g$.

Lemma 4.3: $H_a\mathbf{c}_g = \frac{q^{m-1}-1}{l}$ for any $g \in \mathbf{F}_{q^m}^*$.

Proof: For any t with $1 \le t < n$, if we cyclically shift $\mathbf{c}_g$ to the left for t times, we obtain

$$\mathbf{c}_{g\beta^t} = (\mathrm{Tr}_{q^m/q}(g\beta^t), \mathrm{Tr}_{q^m/q}(g\beta^{t+1}), \ldots, \mathrm{Tr}_{q^m/q}(g\beta^{t+n-1})).$$

Then by noting that for any $g, h \in \mathbf{F}_{q^m}$, $\mathbf{c}_g - \mathbf{c}_h = \mathbf{c}_{g-h}$, and for any $1 \le t < n$, $g - g\beta^t \ne 0$, we have

$$H_{\mathbf{c}_g,\mathbf{c}_g}(t) = n - d_H(\mathbf{c}_g, \mathbf{c}_{g\beta^t}) = \frac{q^m-1}{l} - w(\mathbf{c}_{g-g\beta^t})$$

where $d_H(\mathbf{c}_g, \mathbf{c}_h)$ denotes the Hamming distance between $\mathbf{c}_g$ and $\mathbf{c}_h$ for $g, h \in \mathbf{F}_{q^m}$. Then the result follows from Lemma 4.2. $\square$

Theorem 4.4: $\mathbf{c}_g$ is an optimal FHS($\frac{q^m-1}{l}, q, \frac{q^{m-1}-1}{l}$) for any $g \in \mathbf{F}_{q^m}^*$.

Proof: The conclusion follows from Corollary 2.2 and Lemma 4.3. $\square$

Now we consider a pair of FH sequences $\mathbf{c}_g$ and $\mathbf{c}_{\tilde{g}}$.

Theorem 4.5: If $g, \tilde{g}$ belong to distinct cyclotomic classes of order l in $\mathbf{F}_{q^m}$, then $\mathbf{c}_g$ and $\mathbf{c}_{\tilde{g}}$ constitute a Lempel-Greenberger optimal pair of FH sequences.

Proof: By Theorem 4.4, $H_a(\mathbf{c}_g) = H_a(\mathbf{c}_{\tilde{g}}) = \frac{q^{m-1}-1}{l}$. Now we compute the cross-correlation values of $\mathbf{c}_g$ and $\mathbf{c}_{\tilde{g}}$. From the definition of $\mathbf{c}_g$, we know that for any $t \in \{0,1,\ldots,n-1\}$, if we cyclically shift $\mathbf{c}_g$ to the left for t times, we obtain

$$\mathbf{c}_{g\beta^t} = (\mathrm{Tr}_{q^m/q}(g\beta^t), \mathrm{Tr}_{q^m/q}(g\beta^{t+1}), \ldots, \mathrm{Tr}_{q^m/q}(g\beta^{t+n-1})).$$

Then, by noting that $\mathbf{c}_g - \mathbf{c}_h = \mathbf{c}_{g-h}$ for any $g, h \in \mathbf{F}_{q^m}$, we have

$$H_{\mathbf{c}_{\tilde{g}},\mathbf{c}_g}(t) = n - d_H(\mathbf{c}_{\tilde{g}}, \mathbf{c}_{g\beta^t})$$
$$= \frac{q^m-1}{l} - w(\mathbf{c}_{\tilde{g}-g\beta^t}).$$

Since $g, \tilde{g}$ are in distinct cyclotomic classes of order l in $\mathbf{F}_{q^m}$, $\tilde{g} - g\beta^t$ can never be zero. It then follows from Lemma 4.2 that

$$H_{\mathbf{c}_{\tilde{g}},\mathbf{c}_g}(t) = \frac{q^{m-1}-1}{l}$$

for any $t \in \{0,1,\ldots,n-1\}$. Therefore we can conclude that $H_a(\{\mathbf{c}_g, \mathbf{c}_{\tilde{g}}\}) = H_c(\mathbf{c}_g, \mathbf{c}_{\tilde{g}}) = M(\mathbf{c}_g, \mathbf{c}_{\tilde{g}}) = \frac{q^{m-1}-1}{l}$.

We claim that $\mathbf{c}_g$ and $\mathbf{c}_{\tilde{g}}$ constitute a Lempel–Greenberger optimal pair of FH sequences if $g, \tilde{g}$ belong to distinct cyclotomic classes of order $l \ge 2$ in $\mathbf{F}_{q^m}$. In fact, for any two q-ary sequences X, Y of length $\frac{q^m-1}{l}$, since $2\times\frac{q^m-1}{l} = 2\times\frac{q^{m-1}-1}{l}q + 2\times\frac{q-1}{l}$, where $0 \le 2\times\frac{q-1}{l} < q$ when $l \ge 2$, Theorem 2.5 says that if we put $d = \frac{q^{m-1}-1}{l}$ and $e = \frac{q-1}{l}$, then

$$M(X,Y) \ge \frac{4dn - 2n + 4de + 2e}{4n-2}$$
$$= d - \frac{2n - 4de - 2d - 2e}{4n-2}.$$

A straightforward verification shows that

$$0 \le \frac{2n - 4de - 2d - 2e}{4n-2} < 1$$

which implies that

$$M(X,Y) = d = \frac{q^{m-1}-1}{l}.$$

This completes the proof. $\square$

Immediately, we have the following result.

Theorem 4.6: Let $\{g_0, g_1, \ldots\}$ be a subset of the complete set of representatives for the cyclotomic classes of order l in $\mathbf{F}_{q^m}$. Then $\{\mathbf{c}_{g_0}, \mathbf{c}_{g_1}, \ldots\}$ constitutes a Lempel–Greenberger optimal family of FH sequences.

The case $l = 2$ in the above theorem covers Ding, Moisio and Yuan's result [3] mentioned at the beginning of this subsection.

In fact, we can say more about $\mathbf{c}_g$ for $g \in \mathbf{F}_{q^m}^*$.

Theorem 4.7: Let $\{g_0, g_1, \ldots, g_{l-1}\}$ be a complete set of representatives for the cyclotomic classes of order l in $\mathbf{F}_{q^m}$. Then

$$\mathcal{S} = \{\mathbf{c}_{g_0}, \mathbf{c}_{g_1}, \ldots, \mathbf{c}_{g_{l-1}}\}$$

constitutes a Peng–Fan optimal family of l FH sequences.

Proof: We apply Theorem 2.4, where $I = \lfloor vN/m \rfloor = q^{m-1} - 1$. Since

$$\begin{aligned}
&(v-1)NH_a(\mathcal{S}) + (N-1)NvH_c(\mathcal{S}) \\
&\quad = (\frac{q^m-1}{l} - 1)l\frac{q^{m-1}-1}{l} + (l-1)l\frac{q^m-1}{l}\frac{q^{m-1}-1}{l} \\
&\quad = (q^m - l - 1)\frac{q^{m-1}-1}{l} + (l-1)(q^m-1)\frac{q^{m-1}-1}{l} \\
&\quad = (q^{m-1}-1)(q^m-2),
\end{aligned}$$

and

$$\begin{aligned}
&2IvN - (I+1)\mathrm{Im} \\
&\quad = 2(q^{m-1}-1)\frac{q^m-1}{l}l - q^{m-1}(q^{m-1}-1)q \\
&\quad = (q^{m-1}-1)(q^m-2)
\end{aligned}$$

we know that

$$(v-1)NH_a(\mathcal{S}) + (N-1)NvH_c(\mathcal{S}) = 2IvN - (I+1)\mathrm{Im}$$

which means that $\{H_a(\mathcal{S}) = \frac{q^{m-1}-1}{l}, H_c(\mathcal{S}) = \frac{q^{m-1}-1}{l}\}$ is a pair of the minimum integer solutions of the inequality described in Theorem 2.4, that is, $\mathcal{S}$ is a Peng–Fan optimal family of FH sequences. The proof is then completed. □

Summarizing the above, we obtain the main result of this subsection.

Theorem 4.8: Let q be a prime power and m, l be two positive integers such that $l | q^m - 1$ and $\gcd(\frac{q^m-1}{q-1}, l) = 1$. Then there exists a Peng–Fan optimal family of l FHS$(\frac{q^m-1}{l}, q, \frac{q^{m-1}-1}{l})$, in which each subset of the family is also a Lempel–Greenberger optimal family of FHS$(\frac{q^m-1}{l}, q, \frac{q^{m-1}-1}{l})$, and each sequence of the family is an optimal FHS$(\frac{q^m-1}{l}, q, \frac{q^{m-1}-1}{l})$.

Finally, we give an illustrative example below.

Example 4.9: Let $p = q = 7$, $m = 2$, $l = 3$, $s = 5$, and $n = 16$. Using the irreducible quadratic polynomial $f(x) = x^2 + x + 3 \in \mathbf{F}_7[x]$, we construct $\mathbf{F}_{49}$ as $\mathbf{F}_7[\alpha]/(f(\alpha))$ where $f(\alpha) = \alpha^2 + \alpha + 3 = 0$. The forty-nine elements of $\mathbf{F}_{49}$ can be given in the form $a_0 + a_1\alpha$, $a_0, a_1 \in \mathbf{F}_7$, and we can check that $1 + \alpha$ is a primitive element of $\mathbf{F}_{49}$, where the $l = 3$ cyclotomic classes are listed below:

$$\begin{aligned}
&\{1, 2+5\alpha, 6+2\alpha, 3+3\alpha, 3+6\alpha, 4\alpha, 3+2\alpha, 4+2\alpha \\
&\quad 6, 5+2\alpha, 1+5\alpha, 4+4\alpha, 4+\alpha, 3\alpha, 4+5\alpha, 3+5\alpha\} \\
&\{1+\alpha, 1+2\alpha, 6\alpha, 1+3\alpha, 6+3\alpha, 2, 4+3\alpha, 5+4\alpha \\
&\quad 6+6\alpha, 6+5\alpha, \alpha, 6+4\alpha, 1+4\alpha, 5, 3+4\alpha, 2+3\alpha\} \\
&\{5+\alpha, 2+\alpha, 3, 6+\alpha, 4+6\alpha, 2+2\alpha, 2+4\alpha, 5\alpha \\
&\quad 2+6\alpha, 5+6\alpha, 4, 1+6\alpha, 3+\alpha, 5+5\alpha, 5+3\alpha, 2\alpha\}.
\end{aligned}$$

Let $\beta = (\alpha+1)^{ls} = (\alpha+1)^{15} = 4\alpha$, $g_0 = 1$, $g_1 = (\alpha+1)^8 = 3$, and $g_2 = (\alpha+1)^{16} = 2$. Then g_0, g_1, g_2 are in distinct cyclotomic classes of order $l = 3$ in $\mathbf{F}_{49}$, and

$$\begin{aligned}
\mathbf{c}_{g_0} &= (2,3,4,1,0,1,3,3,5,4,3,6,0,6,4,4) \\
\mathbf{c}_{g_1} &= (6,2,5,3,0,3,2,2,1,5,2,4,0,4,5,5) \\
\mathbf{c}_{g_2} &= (4,6,1,2,0,2,6,6,3,1,6,5,0,5,1,1).
\end{aligned}$$

We can check that

$$\begin{aligned}
H_a(\mathbf{c}_{g_0}) &= H_a(\mathbf{c}_{g_1}) = H_a(\mathbf{c}_{g_2}) = H_c(\mathbf{c}_{g_0}, \mathbf{c}_{g_1}) \\
&= H_c(\mathbf{c}_{g_0}, \mathbf{c}_{g_2}) = H_c(\mathbf{c}_{g_1}, \mathbf{c}_{g_2}) = 2.
\end{aligned}$$

Then, each of $\mathbf{c}_{g_0}, \mathbf{c}_{g_1}, \mathbf{c}_{g_2}$ constitutes an optimal FH sequence, any two of them constitute a Lempel–Greenberger optimal pair of FH sequences, and altogether constitute a Peng–Fan and also a Lempel–Greenberger optimal family of 3 FH sequences, all of length 16 over the frequency library $\mathbf{F}_7$.

B. A Construction via Γ Functions

In [3], Ding, Moisio and Yuan also constructed a Lempel–Greenberger optimal family of FH sequences via norm functions. In this section, we will generalize their idea by introducing a new class Γ of functions from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$, where $q = p^r$ for some positive integer r, and p is a prime. Let $1 \le s \le q^m - 2$, and g be a function from $\mathbf{N}$ to $\mathbf{Z}_{q-1}$, where $\mathbf{N}$ is the set of all positive integers. We define Γ to be a class of functions $\Gamma_{s,g}$ from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$ satisfying the following properties (called Γ *property*):

1) $\Gamma_{s,g}(0) = 0$, and for any $x \in \mathbf{F}_{q^m}^*$, $\Gamma_{s,g}(x^s) \neq 0$;
2) $\Gamma_{s,g}(xy) = \Gamma_{s,g}(x)\Gamma_{s,g}(y)$ for any $x, y \in \mathbf{F}_{q^m}$;
3) $\Gamma_{s,g}(cx) = c^{g(m)}\Gamma_{s,g}(x)$ for any $c \in \mathbf{F}_q^*$ and any $x \in \mathbf{F}_{q^m}$.

Clearly, $\Gamma_{s,g}(1) = 1$. For any $d \in \mathbf{F}_{q^m}$, $a \in \mathbf{F}_q$, $b \in \mathbf{F}_{q^m}$, we define a function from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$

$$f_{da,b}(x) = \mathrm{Tr}_{q^m/q}(da\Gamma_{s,g}(x^s) + bx).$$

We also define the following periodic sequence of length $q^m - 1$ over $\mathbf{F}_q$:

$$\mathbf{c}_{da,b} = (f_{da,b}(\alpha^0), f_{da,b}(\alpha^1), \ldots, f_{da,b}(\alpha^{q^m-2}))$$

where α is a primitive element of $\mathbf{F}_{q^m}$.

Let $\chi(x)$ and $\varphi(x)$ be the canonical additive characters of $\mathbf{F}_q$ and $\mathbf{F}_{q^m}$, respectively. By the definition, we have

$$\begin{aligned}
\chi(x) &= e^{\frac{2\pi i}{p}\mathrm{Tr}_{q/p}(x)} \text{ for } x \in \mathbf{F}_q \\
\varphi(x) &= e^{\frac{2\pi i}{p}\mathrm{Tr}_{q^m/p}(x)} \text{ for } x \in \mathbf{F}_{q^m}.
\end{aligned}$$

Lemma 4.10: Assume $\gcd(1 - sg(m), q-1) = 1$. Then

$$w(\mathbf{c}_{da,b}) = \begin{cases} 0, & \text{if } \mathrm{Tr}_{q^m/q}(da) = b = 0 \\ q^m - 1, & \text{if } \mathrm{Tr}_{q^m/q}(da) \neq 0,\ b = 0 \\ (q-1)q^{m-1}, & \text{if } \mathrm{Tr}_{q^m/q}(da) = 0,\ b \neq 0 \\ (q-1)q^{m-1} - 1, & \text{if } \mathrm{Tr}_{q^m/q}(da) \neq 0,\ b \neq 0. \end{cases}$$

Proof: If $\mathrm{Tr}_{q^m/q}(da) = b = 0$, then for any $x \in \mathbf{F}_{q^m}$, since $\Gamma_{s,g}(x^s) \in \mathbf{F}_q$, we have

$$\begin{aligned}&\mathrm{Tr}_{q^m/q}(da\Gamma_{s,g}(x^s) + bx)\\ &\quad= \mathrm{Tr}_{q^m/q}(da\Gamma_{s,g}(x^s)) + \mathrm{Tr}_{q^m/q}(bx)\\ &\quad= \Gamma_{s,g}(x^s)\mathrm{Tr}_{q^m/q}(da) + \mathrm{Tr}_{q^m/q}(bx)\\ &\quad= 0\end{aligned}$$

so

$$w(\mathbf{c}_{da,b}) = 0.$$

If $\mathrm{Tr}_{q^m/q}(da) \neq 0$, $b = 0$, then

$$\begin{aligned}w(\mathbf{c}_{da,b}) &= q^m - 1 - \frac{1}{q}\sum_{x\in\mathbf{F}_{q^m}^*}\sum_{c\in\mathbf{F}_q}\chi(\mathrm{Tr}_{q^m/q}(da\Gamma_{s,g}(x^s))c)\\ &= q^m - 1 - \frac{1}{q}\sum_{x\in\mathbf{F}_{q^m}^*}\sum_{c\in\mathbf{F}_q}\chi(\mathrm{Tr}_{q^m/q}(da)\Gamma_{s,g}(x^s)c).\end{aligned}$$

Since

$$\mathrm{Tr}_{q^m/q}(da) \neq 0, \text{ and } \Gamma_{s,g}(x^s) \neq 0 \text{ for any } x \in \mathbf{F}_{q^m}^*$$

we have

$$\sum_{c\in\mathbf{F}_q}\chi(\mathrm{Tr}_{q^m/q}(da)\Gamma_{s,g}(x^s)c) = 0$$

which implies

$$w(\mathbf{c}_{da,b}) = q^m - 1.$$

If $\mathrm{Tr}_{q^m/q}(da) = 0$, $b \neq 0$, then

$$\begin{aligned}&w(\mathbf{c}_{da,b})\\ &= q^m - 1 - \frac{1}{q}\sum_{x\in\mathbf{F}_{q^m}^*}\sum_{c\in\mathbf{F}_q}\chi(\mathrm{Tr}_{q^m/q}(da\Gamma_{s,g}(x^s) + bx)c)\\ &= q^m - 1 - \frac{1}{q}\sum_{x\in\mathbf{F}_{q^m}^*}\sum_{c\in\mathbf{F}_q}\chi(\mathrm{Tr}_{q^m/q}(bcx))\\ &= \frac{1}{q}((q-1)(q^m-1) - \sum_{c\in\mathbf{F}_q^*}\sum_{x\in\mathbf{F}_{q^m}^*}\varphi(bcx))\\ &= \frac{1}{q}((q-1)(q^m-1) - \sum_{c\in\mathbf{F}_q^*}(-1))\\ &= (q-1)q^{m-1}.\end{aligned}$$

If $\mathrm{Tr}_{q^m/q}(da) \neq 0$, $b \neq 0$, then

$$\begin{aligned}&w(\mathbf{c}_{da,b})\\ &= q^m - 1 - \frac{1}{q}\sum_{x\in\mathbf{F}_{q^m}^*}\sum_{c\in\mathbf{F}_q}\chi(\mathrm{Tr}_{q^m/q}(da\Gamma_{s,g}(x^s) + bx)c)\\ &= q^m - 1 - \frac{1}{q}\sum_{c\in\mathbf{F}_q}\sum_{x\in\mathbf{F}_{q^m}^*}\varphi(cda\Gamma_{s,g}(x^s) + bcx)\\ &= \frac{1}{q}((q-1)(q^m-1) - \sum_{c\in\mathbf{F}_q^*}\sum_{x\in\mathbf{F}_{q^m}^*}\varphi(cda\Gamma_{s,g}(x^s) + bcx)).\end{aligned}$$

Replace cx by y. Since $\Gamma_{s,g}(cx) = c^{g(m)}\Gamma_{s,g}(x)$ for any $c \in \mathbf{F}_q^*$ and any $x \in \mathbf{F}_{q^m}$, we have

$$\begin{aligned}&w(\mathbf{c}_{da,b})\\ &= \frac{1}{q}((q-1)(q^m-1)\\ &\quad - \sum_{c\in\mathbf{F}_q^*}\sum_{y\in\mathbf{F}_{q^m}^*}\varphi(da\Gamma_{s,g}(y^s)c^{1-sg(m)} + by))\\ &= \frac{1}{q}((q-1)(q^m-1)\\ &\quad - \sum_{y\in\mathbf{F}_{q^m}^*}\varphi(by)\sum_{c\in\mathbf{F}_q^*}\chi(\mathrm{Tr}_{q^m/q}(da)\Gamma_{s,g}(y^s)c^{1-sg(m)})).\end{aligned}$$

By the assumption that $\gcd(1 - sg(m), q-1) = 1$, we know the mapping $c \mapsto c^{1-sg(m)}$ is a permutation of $\mathbf{F}_q^*$. Also, $\mathrm{Tr}_{q^m/q}(da) \neq 0$, and $\Gamma_{s,g}(y^s) \neq 0$ for any $y \in \mathbf{F}_{q^m}^*$. Therefore,

$$\begin{aligned}w(\mathbf{c}_{da,b}) &= \frac{1}{q}((q-1)(q^m-1) + \sum_{y\in\mathbf{F}_{q^m}^*}\varphi(by))\\ &= (q-1)q^{m-1} - 1.\end{aligned}$$

The proof is then completed. □

Lemma 4.11: Assume $\gcd(1 - sg(m), q-1) = 1$, $d \in \mathbf{F}_{q^m}$, $a \in \mathbf{F}_q$, and $b \in \mathbf{F}_{q^m}^*$. Then

1) If $a = 0$ or $\mathrm{Tr}_{q^m/q}(d) = 0$, we have $H_a(\mathbf{c}_{da,b}) = q^{m-1} - 1$.
2) Otherwise, we have $H_a(\mathbf{c}_{da,b}) \leq q^{m-1}$.

Proof: The length of the sequence $\mathbf{c}_{da,b}$ is $L = q^m - 1$. Let $\mathbf{c}_{da,b}(k)$ denote the kth element of $\mathbf{c}_{da,b}$ where $0 \leq k < L$. Since $\Gamma_{s,g}(xy) = \Gamma_{s,g}(x)\Gamma_{s,g}(y)$ for any $x, y \in \mathbf{F}_{q^m}$, we see that for any t with $1 \leq t \leq q^m - 2$,

$$(\mathbf{c}_{da,b}(t \bmod L), \mathbf{c}_{da,b}(t+1 \bmod L), \ldots, \mathbf{c}_{da,b}(t+L-1 \bmod L))$$

is equal to the sequence $\mathbf{c}_{da\Gamma_{s,g}(\alpha^{ts}),b\alpha^t}$. Then

$$\begin{aligned}H_{\mathbf{c}_{da,b},\mathbf{c}_{da,b}}(t) &= q^m - 1 - d_H(\mathbf{c}_{da,b}, \mathbf{c}_{da\Gamma_{s,g}(\alpha^{ts}),b\alpha^t})\\ &= q^m - 1 - w(\mathbf{c}_{da(1-\Gamma_{s,g}(\alpha^{ts})),b(1-\alpha^t)}).\end{aligned}$$

Since $b \in \mathbf{F}_{q^m}^*$, α is the primitive element of $\mathbf{F}_{q^m}$, and $1 \leq t \leq q^m - 2$, we know that

$$b(1 - \alpha^t) \neq 0.$$

By Lemma 4.10

$w(\mathbf{c}_{da(1-\Gamma_{s,g}(\alpha^{ts})),b(1-\alpha^t)}) = (q-1)q^{m-1} - 1$ or $(q-1)q^{m-1}$ according to whether $\mathrm{Tr}_{q^m/q}(da(1 - \Gamma_{s,g}(\alpha^{ts}))) \neq 0$ or not. But

$$\mathrm{Tr}_{q^m/q}(da(1 - \Gamma_{s,g}(\alpha^{ts}))) = a(1 - \Gamma_{s,g}(\alpha^{ts}))\mathrm{Tr}_{q^m/q}(d),$$

so 1) if $a = 0$ or $\mathrm{Tr}_{q^m/q}(d) = 0$, then $w(\mathbf{c}_{da(1-\Gamma_{s,g}(\alpha^{ts})),b(1-\alpha^t)}) = (q-1)q^{m-1}$ for any t with $1 \leq t \leq q^m - 2$, which implies $H_a(\mathbf{c}_{da,b}) = q^{m-1} - 1$; 2) otherwise $w(\mathbf{c}_{da(1-\Gamma_{s,g}(\alpha^{ts})),b(1-\alpha^t)}) \geq (q-1)q^{m-1} - 1$

for any t with $1 \le t \le q^m - 2$, which implies $H_a(\mathbf{c}_{da,b}) \le q^{m-1}$. □

Theorem 4.12: Assume $\gcd(1-sg(m), q-1) = 1, d \in \mathbf{F}_{q^m}$, $a \in \mathbf{F}_q$, and $b \in \mathbf{F}_{q^m}^*$. Then $\mathbf{c}_{da,b}$ is an optimal FHS$(q^m - 1, q, q^{m-1} - 1)$ provided that $a = 0$ or $\mathrm{Tr}_{q^m/q}(d) = 0$.

Proof: The conclusion follows from Corollary 2.2 and Lemma 4.11. □

In the following, we choose a fixed element $d \in \mathbf{F}_{q^m}^*$ with $\mathrm{Tr}_{q^m/q}(d) \neq 0$. We consider a set of sequences

$$\mathcal{R}_s = \{\mathbf{c}_{da,b} : (a,b) \in \mathbf{F}_q \times \mathbf{F}_{q^m}^*\}.$$

We claim that these $q(q^m - 1)$ sequences are pairwise distinct under the assumption $\mathrm{Tr}_{q^m/q}(d) \neq 0$. Since $\mathbf{c}_{da_1,b_1} - \mathbf{c}_{da_2,b_2} = \mathbf{c}_{d(a_1-a_2),b_1-b_2}$ for any $(a_1,b_1),(a_2,b_2) \in \mathbf{F}_q \times \mathbf{F}_{q^m}^*$, we only need to prove that if $\mathbf{c}_{da,b}$ is the all-zero sequence, then $a = b = 0$. Suppose $\mathbf{c}_{da,b} = (0,\ldots,0)$ for some $(a,b) \in \mathbf{F}_q \times \mathbf{F}_{q^m}$. Then $w(\mathbf{c}_{da,b}) = 0$, and $b = \mathrm{Tr}_{q^m/q}(da) = 0$ by Lemma 4.10. But $\mathrm{Tr}_{q^m/q}(da) = 0$ also implies $a = 0$ since $\mathrm{Tr}_{q^m/q}(d) \neq 0$.

Now we fix $b \in \mathbf{F}_{q^m}^*$ in $\mathcal{R}_s$ and denote such a subset of sequences by $\mathcal{R}_s(b) = \{\mathbf{c}_{da,b} : a \in \mathbf{F}_q\}$. We claim that any two distinct sequences in $\mathcal{R}_s(b)$ are not equivalent, that is, any one is not a cyclic shift of the other. Since

$$\begin{aligned} &H_{\mathbf{c}_{da_2,b_2},\mathbf{c}_{da_1,b_1}}(t) \\ &\quad = q^m - 1 - d_H(\mathbf{c}_{da_2,b_2}, \mathbf{c}_{da_1\Gamma_{s,g}(\alpha^{ts}),b_1\alpha^t}) \\ &\quad = q^m - 1 - w(\mathbf{c}_{d(a_2-a_1\Gamma_{s,g}(\alpha^{ts})),b_2-b_1\alpha^t}) \end{aligned}$$

for $0 \le t \le q^m - 2$, if $\mathbf{c}_{da_2,b_2}$ is a cyclic t-shift of $\mathbf{c}_{da_1,b_1}$, we should have

$$w(\mathbf{c}_{d(a_2-a_1\Gamma_{s,g}(\alpha^{ts})),b_2-b_1\alpha^t}) = 0.$$

It then follows from the discussions above, under the condition that $\mathrm{Tr}_{q^m/q}(d) \neq 0$, two sequences $\mathbf{c}_{da_1,b_1}$ and $\mathbf{c}_{da_2,b_2}$ are equivalent if and only if

$$a_2 - a_1\Gamma_{s,g}(\alpha^{ts}) = 0 \text{ and } b_2 - b_1\alpha^t = 0.$$

Since $b_2 = b_1 = b$ in $\mathcal{R}_s(b)$, if two distinct sequences in $\mathcal{R}_s(b)$ are equivalent, we should have $t = 0$, which implies $a_2 = a_1$ by the fact that $\Gamma_{s,g}(1) = 1$.

We can prove that $\mathcal{R}_s(b)$ is a Lempel–Greenberger optimal family of q FH sequences, in which the sequence $\mathbf{c}_{0,b}$ is optimal.

Let $\mathbf{c}_{da_1,b}$ and $\mathbf{c}_{da_2,b}$ be any two distinct sequences in $\mathcal{R}_s(b)$. Since $a_1 \neq a_2$ and $\mathrm{Tr}_{q^m/q}(d) \neq 0$, at least one of $\mathrm{Tr}_{q^m/q}(d(a_2 - a_1\Gamma_{s,g}(\alpha^{ts}))$ and $b(1-\alpha^t)$ is nonzero. By Lemma 4.10

$$\begin{aligned} &w(\mathbf{c}_{d(a_2-a_1\Gamma_{s,g}(\alpha^{ts})),b(1-\alpha^t)}) \\ &\qquad = (q-1)q^{m-1} - 1 \text{ or } (q-1)q^{m-1} \text{ or } q^m - 1 \end{aligned}$$

so

$$H_{\mathbf{c}_{da_2,b},\mathbf{c}_{da_1,b}}(t) = q^{m-1} \text{ or } q^{m-1} - 1 \text{ or } 0$$

hence

$$H_c(\mathbf{c}_{da_1,b}, \mathbf{c}_{da_2,b}) = \max_{0 \le t \le q^m-2}\{H_{\mathbf{c}_{da_2,b},\mathbf{c}_{da_1,b}}(t)\} = q^{m-1}.$$

Together with Lemma 4.11, we have

$$\begin{aligned} &M(\mathbf{c}_{da_1,b}, \mathbf{c}_{da_2,b}) \\ &\quad = \max\{H_a(\mathbf{c}_{da_1,b}), H_a(\mathbf{c}_{da_2,b}), H_c(\mathbf{c}_{da_1,b}, \mathbf{c}_{da_2,b})\} \\ &\quad = q^{m-1}. \end{aligned}$$

This implies the following theorem.

Theorem 4.13: Let $1 \le s \le q^m - 2$, g a function from $\mathbf{N}$ to $\mathbf{Z}_{q-1}$, $\gcd(1-sg(m), q-1) = 1$, and d an element of $\mathbf{F}_{q^m}^*$ with $\mathrm{Tr}_{q^m/q}(d) \neq 0$. Then for any $b \in \mathbf{F}_{q^m}^*$, $\mathcal{R}_s(b) = \{\mathbf{c}_{da,b} : a \in \mathbf{F}_q\}$ is a Lempel–Greenberger optimal family of q FH sequences of length $q^m - 1$ over $\mathbf{F}_q$, in which the sequence $\mathbf{c}_{0,b}$ is optimal.

Proof: Theorem 2.4 with $v = q^m - 1$, $N = 2$ and $|F| = q$ shows that for every pair of distinct FH sequences $X, Y \in \chi(v;F)$, we have $M(X,Y) \ge q^{m-1}$. This completes the proof of the first assertion. The second assertion comes from Theorem 4.12 with $a = 0$. □

Please note that for a pair of distinct FH sequences $\{\mathbf{c}_{da_1,b}, \mathbf{c}_{da_2,b}\} \subseteq \mathcal{R}_s(b)$, $\{H_a(\{\mathbf{c}_{da_1,b}, \mathbf{c}_{da_2,b}\}), H_c(\{\mathbf{c}_{da_1,b}, \mathbf{c}_{da_2,b}\})\}$ is usually not a pair of the minimum integer solutions of the inequality in Theorem 2.4 for $N = 2$. Also, $\mathcal{R}_s(b)$ is usually not a Peng-Fan optimal family of FH sequences. However, if we consider the parameter $M(\mathcal{R}_s(b))$, then from Theorem 2.4, we know that $M(\mathcal{R}_s(b))$ should be greater than or equal to q^{m-1}. Meanwhile, as we have already seen

$$\begin{aligned} H_a(\mathcal{R}_s(b)) &= \max\{H_a(\mathbf{c}_{da,b}) : a \in \mathbf{F}_q\} \le q^{m-1} \\ H_c(\mathcal{R}_s(b)) &= \max\{H_c(\mathbf{c}_{da_1,b}, \mathbf{c}_{da_2,b}) : a_1, a_2 \in \mathbf{F}_q, a_1 \neq a_2\} \\ &= q^{m-1} \end{aligned}$$

so $M(\mathcal{R}_s(b)) = q^{m-1}$. This means that $\mathcal{R}_s(b)$ has the minimum possible maximum value of auto- and cross-correlations.

Noting that the norm function $N_{q^m/q}(x) = x^{(q^m-1)/(q-1)}$ from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$ is an example of the functions in Γ with $g(m) = m \pmod{q-1}$ for any $m \in \mathbf{N}$ and $N_{q^m/q}(x^s) \neq 0$ for any $x \in \mathbf{F}_{q^m}^*$, where $1 \le s \le q^m - 2$, we obtain Ding, Moisio, and Yuan's third Lempel–Greenberger optimal family of FH sequences described in [3], which has the same number of sequences as the family of sequences constructed by Lempel and Greenberger in [11, Th. 2].

Now we consider the degenerated function $\Gamma_{s,g} \in \Gamma$ from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$ for $1 \le s \le q^m - 2$ such that for any $x \in \mathbf{F}_{q^m}^*$, $\Gamma_{s,g}(x) = 1$. Clearly, $\Gamma_{s,g}$ is a function in Γ with $g(m) = 0 \pmod{q-1}$, which can be denoted by $\Gamma_{s,g}^0$. In this case, by Theorem 4.13, for $d \in \mathbf{F}_{q^m}^*$ with $\mathrm{Tr}_{q^m/q}(d) \neq 0$, $\mathcal{R}_s^0(b) = \{\mathbf{c}_{da,b}^0 : a \in \mathbf{F}_q\}$ with

$$\begin{aligned} \mathbf{c}_{da,b}^0 = (&\mathrm{Tr}_{q^m/q}(da + b\alpha^0), \mathrm{Tr}_{q^m/q}(da + b\alpha^1) \\ &\ldots, \mathrm{Tr}_{q^m/q}(da + b\alpha^{q^m-2})) \end{aligned}$$

where α is a primitive element of $\mathbf{F}_{q^m}$, is a Lempel-Greenberger optimal family of q FH sequences of length $q^m - 1$ over $\mathbf{F}_q$ for any $b \in \mathbf{F}_{q^m}^*$. From the proof of Lemma 4.11, we can know that $H_a(\mathbf{c}_{da,b}^0) = H_a(\mathcal{R}_s^0(b)) = q^{m-1} - 1$ since we always

have $\mathrm{Tr}_{q^m/q}(da(1-\Gamma^0_{s,g}(\alpha^{ts})))=0$ in this case. Then it can be checked that $\mathcal{R}^0_s(b)$ is a Peng–Fan optimal family of FH sequences.

Corollary 4.14: Let α be a primitive element of $\mathbf{F}_{q^m}$. Then for any $b\in\mathbf{F}^*_{q^m}$ and any $d\in\mathbf{F}^*_{q^m}$ with $\mathrm{Tr}_{q^m/q}(d)\neq 0$, the following

$$\{(\mathrm{Tr}_{q^m/q}(da+b\alpha^0),\mathrm{Tr}_{q^m/q}(da+b\alpha^1)\ldots,\mathrm{Tr}_{q^m/q}(da+b\alpha^{q^m-2}):a\in\mathbf{F}_q\}$$

forms a Lempel-Greenberger and also a Peng–Fan optimal family of q FH sequences.

The following is an illustrative example.

Example 4.15: Let $p=q=5$, $m=2$, $b=d=1$, and s be any integer between1 and 23. Using the irreducible quadratic polynomial $f(x)=x^2+x+1\in\mathbf{F}_5[x]$, we construct $\mathbf{F}_{25}$ as $\mathbf{F}_5[\alpha]/(f(\alpha))$ where $f(\alpha)=\alpha^2+\alpha+1=0$. The twenty-five elements of $\mathbf{F}_{25}$ can be given in the form $a_0+a_1\alpha$, $a_0,a_1\in\mathbf{F}_5$, and we can check that $2+\alpha$ is a primitive element of $\mathbf{F}_{25}$. The five FH sequences of $\mathcal{R}^0_s(1)$ are

$$\mathbf{c}^0_{1\times 0,1}=(2,3,3,0,1,3,1,4,4,0,3,4,3,2,2,0,4,2,4,1,1,0,2,1)$$
$$\mathbf{c}^0_{1\times 1,1}=(4,0,0,2,3,0,3,1,1,2,0,1,0,4,4,2,1,4,1,3,3,2,4,3)$$
$$\mathbf{c}^0_{1\times 2,1}=(1,2,2,4,0,2,0,3,3,4,2,3,2,1,1,4,3,1,3,0,0,4,1,0)$$
$$\mathbf{c}^0_{1\times 3,1}=(3,4,4,1,2,4,2,0,0,1,4,0,4,3,3,1,0,3,0,2,2,1,3,2)$$
$$\mathbf{c}^0_{1\times 4,1}=(0,1,1,3,4,1,4,2,2,3,1,2,1,0,0,3,2,0,2,4,4,3,0,4).$$

We can check that $H_a(\mathbf{c}^0_{1\times a,1})=4$ and $H_c(\mathbf{c}^0_{1\times a,1},\mathbf{c}^0_{1\times a',1})=5$ for any $a\neq a'\in\mathbf{F}_5$. Then, each of the five FH sequences in $\mathcal{R}^0_s(1)$ is optimal, and all these five FH sequences constitute a Lempel-Greenberger optimal family of length 24 over $\mathbf{F}_5$. By a simple verification, we know that these five FH sequences even constitute a Peng–Fan optimal family.

Since $\mathrm{Tr}_{q^m/q}(\beta+\theta)=\mathrm{Tr}_{q^m/q}(\beta)+\mathrm{Tr}_{q^m/q}(\theta)$ for all $\beta,\theta\in\mathbf{F}_{q^m}$, we can see that the ith components of the q FH sequences with degenerated function $\Gamma^0_{s,g}$

$$\mathbf{c}^0_{da,b}=(\mathrm{Tr}_{q^m/q}(da+b\alpha^0),\mathrm{Tr}_{q^m/q}(da+b\alpha^1)\ldots,\mathrm{Tr}_{q^m/q}(da+b\alpha^{q^m-2}))$$

are obtained by adding $\mathrm{Tr}_{q^m/q}(da)$ to $\mathrm{Tr}_{q^m/q}(b\alpha^i)$ respectively with q distinct $a\in\mathbf{F}_q$. Moreover, each $\mathbf{c}_{0,b}$ with any function $\Gamma_{s,g}\in\Gamma$ reduces to the sequence

$$\mathbf{c}_g=(\mathrm{Tr}_{q^m/q}(g),\mathrm{Tr}_{q^m/q}(g\beta),\ldots,\mathrm{Tr}_{q^m/q}(g\beta^{n-1}))$$

defined in Section IV-A with $s=l=1$ and $b=g$. On the other hand, each $\mathbf{c}^0_{da,b}$ can be obtained from $\mathbf{c}_g$ by putting $s=l=1$. These show some connections between these two trace function constructions.

More generally, we can consider the following function $\Gamma_{s,g}\in\Gamma$ from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$ defined by

$$\Gamma_{s,g}(x)=N_{q^m/q}(x)^k=x^{\frac{q^m-1}{q-1}k}$$

for any $1\leq s\leq q^m-2$ and any positive integer k. $\Gamma_{s,g}$ satisfies the Γ property with $g(m)=mk \pmod{q-1}$, which can be denoted by $N^k_{q^m/q}$. By Theorem 4.13, for $d\in\mathbf{F}^*_{q^m}$ with $\mathrm{Tr}_{q^m/q}(d)\neq 0$ and $\gcd(1-smk,q-1)=1$, $\mathcal{R}_s(b)=\{\mathbf{c}_{da,b}:a\in\mathbf{F}_q\}$ is a Lempel–Greenberger optimal family of q FH sequences of length q^m-1 over $\mathbf{F}_q$. Obviously, when k is a multiplier of $q-1$, $N^k_{q^m/q}$ becomes $\Gamma^0_{s,g}$, which we have already discussed in the above. The following is an example with $k=2$.

Example 4.16: Let $p=q=5$, $k=m=2$, $s=b=d=1$. We construct $\mathbf{F}_{25}$ as $\mathbf{F}_5[\alpha]/(f(\alpha))$, where $f(x)=x^2+x+1\in\mathbf{F}_5[x]$ is an irreducible quadratic polynomial, and $2+\alpha$ is a primitive element of $\mathbf{F}_{25}$. The five FH sequences of $\mathcal{R}_s(1)$ are

$$\mathbf{c}_{1\times 0,1}=(2,3,3,0,1,3,1,4,4,0,3,4,3,2,2,0,4,2,4,1,1,0,2,1)$$
$$\mathbf{c}_{1\times 1,1}=(4,1,0,3,3,1,3,2,1,3,0,2,0,0,4,3,1,0,1,4,2,3,4,4)$$
$$\mathbf{c}_{1\times 2,1}=(1,4,2,1,0,4,0,0,3,1,2,0,2,3,1,1,3,3,3,2,0,1,1,2)$$
$$\mathbf{c}_{1\times 3,1}=(3,2,4,4,2,2,2,3,0,4,4,3,4,1,3,4,0,1,0,0,2,4,3,0)$$
$$\mathbf{c}_{1\times 4,1}=(0,0,1,2,4,0,4,1,2,2,1,1,1,4,0,2,2,4,2,3,4,2,0,3).$$

We can check that $H_a(\mathbf{c}_{1\times a,1})\leq 4$ and $H_c(\mathbf{c}_{1\times a,1},\mathbf{c}_{1\times a',1})=5$ for any $a,a'\in\mathbf{F}_5$, $a\neq a'$. So these five FH sequences of $\mathcal{R}_s(1)$ are a Lempel–Greenberger optimal family of length 24 over $\mathbf{F}_5$.

We make the final remark of this subsection. Since Γ functions are multiplicative homomorphisms from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$, they are determined by the images of any primitive element of $\mathbf{F}_{q^m}$, where the number of possible images is clearly q. The q examples of Γ functions described above are exactly the only possible Γ functions from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$.

V. Conclusion

In this paper, we considered the Hamming auto- and cross-correlations of FH sequences. We first reviewed the two known lower bounds on the Hamming correlations of FH sequences and the two concepts of optimality of FH sequences due to Lempel and Greenberger [11] and Peng and Fan [13], respectively. Then we constructed several new series of optimal families consisting of a single FH sequences from a combinatorial approach. We also provided a combinatorial characterization of families consisting of multiple FH sequences, and provided a general recursive construction via difference matrices by means of this characterization. Two algebraic constructions for such families of multiple FH sequences using trace functions and Γ functions were also described. However, there are still a lot of challenging problems left. More efforts are necessary for further research,

especially for those optimal families consisted of multiple FH sequences.

ACKNOWLEDGMENT

The authors thank Prof. Zhu Lie of Suzhou University for his important suggestions on this problem. The second author also wishes to thank Prof. Ryoh Fuji-Hara and Prof. Yoshitsugu Yamamoto of University of Tsukuba for their helpful discussions during the preparation of this paper, and Prof. Akihiro Munemasa of Tohoku University for confirming our assertion on the number of Γ functions. The authors express their gratitude to the two anonymous reviewers for their detailed and constructive comments which helped to improve the results and the technical presentation of this paper, and to Prof. Guang Gong, the Associate Editor, for her excellent editorial job.

REFERENCES

[1] W. Chu and C. J. Colbourn, "Optimal frequency-hopping sequences via cyclotomy," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1139–1141, 2005.

[2] C. J. Colbourn, "Difference matrices," in *Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz, Eds., Second ed. Boca Raton, FL: CRC, 2007, pp. 411–419.

[3] C. Ding, M. Moisio, and J. Yuan, "Algebraic constructions of optimal frequency hopping sequences," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2606–2610, 2007.

[4] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. Taunton, U.K.: Research Studies, 1996.

[5] Y. Fujiwara and R. Fuji-Hara, "Frequency hopping sequences with optimal auto- and cross-correlation properties and related codes," in *Proc. Tenth Int. Workshop Algebraic Combin. Coding Theory*, Zvenigorod, Russia, Sep. 2006, pp. 93–96.

[6] R. Fuji-Hara, K. Kuriki, and M. Miyake, "Cyclic orthogonal and balanced arrays," *J. Statist. Plan. Inference*, vol. 56, pp. 171–180, 1996.

[7] R. Fuji-Hara, Y. Miao, and M. Mishima, "Optimal frequency hopping sequences: A combinatorial approach," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2408–2420, 2004.

[8] S. Furino, Y. Miao, and J. Yin, *Frames and Resolvable Designs: Uses, Constructions, and Existence*. Boca Raton, FL: CRC, 1996.

[9] G. Ge, R. Fuji-Hara, and Y. Miao, "Further combinatorial constructions for optimal frequency-hopping sequences," *J. Combin. Theory, Series A*, vol. 113, pp. 1699–1718, 2006.

[10] P. V. Kumar, "Frequency hopping code sequence designs having large linear span," *IEEE Trans. Inf. Theory*, vol. 34, pp. 146–151, 1988.

[11] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming correlation properties," *IEEE Trans. Inf. Theory*, vol. 20, pp. 90–94, 1974.

[12] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge, U.K.: Cambridge University Press, 1997.

[13] D. Peng and P. Fan, "Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2149–2154, 2004.

[14] D. V. Sarwate, "Reed-Solomon codes and the design of sequences for spread-spectrum multiple-access communications," in *Reed-Solomon Codes and Their Applications*, S. B. Wicker and V. K. Bhargava, Eds. Piscataway, NJ: IEEE Press, 1994.

[15] D. V. Sarwate, "Comments on "Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 51, p. 1615, 2005.

Gennian Ge received the M.S. and Ph.D. degrees in mathematics from Suzhou University, Suzhou, Jiangsu, P. R. China, in 1993 and 1996, respectively. After that, he became a member of Suzhou University. He was a postdoctoral fellow in the Department of Computer Science at Concordia University, Montreal, QC, Canada, from September 2001 to August 2002, and a Visiting Assistant Professor in the Department of Computer Science at the University of Vermont, Burlington, Vermont, USA, from September 2002 to February 2004. Since then, he has been a full Professor in the Department of Mathematics at Zhejiang University, Hangzhou, Zhejiang, P. R. China. His research interests include the constructions of combinatorial designs and their applications to codes and crypts.

Dr. Ge is on the Editorial Boards of *Journal of Combinatorial Designs*, *The Open Mathematics Journal*, and *International Journal of Combinatorics*. He received the 2006 Hall Medal from the Institute of Combinatorics and its Applications.

Ying Miao received the D.Sci. degree in mathematics from Hiroshima University, Hiroshima, Japan, in 1997.

From 1989 to 1993, he worked for Suzhou Institute of Silk Textile Technology, Suzhou, Jiangsu, P. R. China. From 1995 to 1997, he was a Research Fellow of the Japan Society for the Promotion of Science. During 1997–1998, he was a Postdoctoral Fellow at the Department of Computer Science, Concordia University, Montreal, QC, Canada. In 1998, he joined the University of Tsukuba, Tsukuba, Ibaraki, Japan, where he is currently an Associate Professor at the Department of Social Systems and Management, Graduate School of Systems and Information Engineering. His research interests include combinatorics, coding theory, cryptography, DNA library screening, and their interactions.

Dr. Miao is on the Editorial Boards of both *Graphs and Combinatorics* and *Journal of Combinatorial Designs*. He received the 2001 Kirkman Medal from the Institute of Combinatorics and its Applications.

Zhongxiang Yao received the Master's degree from Zhejiang University, Hangzhou, Zhejiang, P. R. China, in 2007.

His research interests include combinatorial design theory, coding theory, cryptography, and their interactions.