

A Construction of Optimal Frequency Hopping Sequence Set via Combination of Multiplicative and Additive Groups of Finite Fields

Xianhua Niu * Chaoping Xing[†]

Abstract

In literatures, there are various constructions of frequency hopping sequence (FHS for short) sets with good Hamming correlations. Some papers employed only multiplicative groups of finite fields to construct FHS sets, while other papers implicitly used only additive groups of finite fields for construction of FHS sets. In this paper, we make use of both multiplicative and additive groups of finite fields simultaneously to present a construction of optimal FHS sets. The construction provides a new family of optimal $\left(q^m - 1, \frac{q^{m-t}-1}{r}, rq^t; \frac{q^{m-t}-1}{r} + 1\right)$ frequency hopping sequence sets archiving the Peng-Fan bound. Thus, the FHS sets constructed in literatures using either multiplicative groups or additive groups of finite fields are all included in our family. In addition, some other FHS sets can be obtained via the well-known recursive constructions through one-coincidence sequence set.

1 Introduction

In frequency-hopping multiple access (FHMA) communication systems, each user's wideband signal is generated by hopping over a large number of frequency slots. User's frequency slots used are chosen pseudo-randomly via a code called frequency hopping sequences. The degree of the mutual interference between users is clearly related to the Hamming correlation properties of the frequency hopping sequences, and the number of users allowed by the system for synchronous communication is determined by the number of frequency hopping sequences [6, 13]. In order to improve the system performance, it is desirable to employ frequency hopping sequences having low Hamming correlation to reduce the multiple-access interference (also called hits) of frequencies [7]. Moreover, the required sequence length and alphabet size of FHS set are variable according to the specification of a given system or environment. Thus, the design of FHS set with good Hamming correlation property and flexible parameters is an important problem.

*School of Computer and Software Engineering, Xihua University and National Key Laboratory of Science and Technology on Communications, University of Electronic Science and Technology of China. Research supported by the Youth Science and Technology Fund of Sichuan Province (No.2017JQ0059). Email: rurustef1212@gmail.com.

[†]School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. Email: xingcp@ntu.edu.sg.

In practical applications, the required length and alphabet size of an FHS or an FHS set vary depending on the specification of a given system or environment. Thus, it is very important to select FHS sets with optimal Hamming correlation under the given condition. In general, optimality of an FHS set is measured by the Peng-Fan bound [9], whereas that of a single FHS is by the Lempel-Greenberger bound [7]. It is of particular interest to construct FHS sets which meet Peng-Fan bound. There are several algebraic method, combinatorial and recursive constructions in the literature [7, 14, 3, 5, 20, 18, 19, 2, 10, 16, 1, 8, 17].

1.1 Known results

In literatures, there are various constructions of FHS sets with good Hamming correlations. Let us only recall the constructions relevant to our construction, namely those via either multiplicative or additive groups of finite fields.

- (1) Lempel et al. [7, 14, 20] showed that there is an optimal $(q^m - 1, q^{m-t}, q^t; q^{m-t})$ FHS set for a prime power q and integers $1 \leq t \leq m - 1$. This construction implicitly employed the additive group structure of a finite field.
- (2) Ding et al. [5] constructed optimal $(q - 1, \frac{q-1}{f}, f; \frac{q-1}{f} + 1)$ FHS set for a prime power q and integer f satisfying $f|(q - 1)$, and $2 \leq f \leq \frac{q-1}{f} - 1$. This construction used the multiplicative group structure of a finite field.

1.2 Our result

The optimal FHS sets given in Subsection 1.1 were constructed via either multiplicative or additive group structure of finite fields. By mixing both multiplicative and additive group structures of finite fields, we obtain the following result.

Theorem 1. *Let q be a prime power and let r be a divisor of $q-1$. Then for any $0 \leq t \leq m-1$, there is an FHS set \mathcal{S} with parameters*

$$\begin{cases} \left(q^m - 1, \frac{q^{m-t}-1}{r}, rq^t; \frac{q^{m-t}-1}{r} + 1 \right) & \text{if } r \geq 2 \\ \left(q^m - 1, 1 + \frac{q^{m-t}-1}{r}, rq^t; \frac{q^{m-t}-1}{r} + 1 \right) = (q^m - 1, q^{m-t}, q^t; q^{m-t}) & \text{if } r = 1 \end{cases}$$

In addition, if $q^m - 1 < e^2 + (e+1)q^t - 3e$ with $e = \frac{q^{m-t}-1}{r}$, then \mathcal{S} is optimal, i.e., it achieves the Peng-Fan bound.

It is easy to see that by taking $t = 0$, we get the FHS set given in Ding et al. [5]. By taking $r = 1$, we get the FHS set given in Lempel et al.[7, 14, 20]. Compared with the constructions in [5, 7, 14, 20], the FHS set in Theorem 1 allows more flexible parameters due to the free choice of t .

By applying the FHS sets in Theorem 1 to the standard recursive concatenation of FHS sets with one-coincidence (OC for short) sequence sets, we obtain the following new FHS sets.

Theorem 2. *Let q be a prime power and let $r \geq 2$ be a divisor of $q - 1$. Then for any $0 \leq t \leq m - 1$, we have FHS sets given in the following table.*

Table 1: Parameters of some new recursive constructions of optimal FHS Sets

| Length N | M | H_m | Alphabet Size ℓ | Constraints |
|---------------------|-----|--------|----------------------|---|
| $k(q^m - 1)$ | e | rq^t | $k(e + 1)$ | $er + 1 = q^{m-t}, 1 \leq t \leq m - 1,$ $q^m - q^t - 1 < \text{lpf}(k),$ $q^m - 1 < e^2 + (e + 1)p^t - 3e$ |
| $(p - 1)(q^m - 1)$ | e | rq^t | $p(e + 1)$ | $er + 1 = q^{m-t}, 1 \leq t \leq m - 1,$ $q^m - q^t - 1 \leq p,$ $q^m - 1 < e^2 + (e + 1)p^t - 3e$ |
| $k(p - 1)(q^m - 1)$ | e | rq^t | $kp(e + 1)$ | $er + 1 = q^{m-t}, 1 \leq t \leq m - 1,$ $q^m - q^t - 1 \leq \min\{\text{lpf}(k) - 1, p\},$ $q^m - 1 < e^2 + (e + 1)p^t - 3e$ |

In the above table, p denotes a prime power and $\text{lpf}(k)$ denotes the least prime factor of an integer $k > 1$.

1.3 Our techniques

Our approach is divided into four steps:

- (i) partition a finite field \mathbb{F}_{q^m} into ℓ disjoint subsets V_i for $i = 1, 2, \dots, \ell$;
- (ii) construct a polynomial $\phi(x)$ that is a constant polynomial in each V_i ;
- (iii) for every $b \in \mathbb{F}_{q^m}$, define an FHS $\mathbf{s}_b := (\phi(\theta^0 + b), \phi(\theta + b), \phi(\theta^2 + b), \dots, \phi(\theta^{q^m-2} + b))$, where θ is a primitive element of \mathbb{F}_{q^m} ;
- (iv) choose a suitable subset S of \mathbb{F}_{q^m} to form an FHS set $\{\mathbf{s}_b : b \in S\}$.

The key part of the above approach is partition of \mathbb{F}_{q^m} into ℓ disjoint subsets V_i for $i = 1, 2, \dots, \ell$. Although different languages were adopted to construct FHS sets in [5, 7, 14, 20], they implicitly used the above approach. More precisely speaking, Ding et al. [5] partitioned \mathbb{F}_{q^m} into disjoint cosets of a multiplicative group of \mathbb{F}_{q^m} , while Lempel et al. [7, 14, 20] partitioned \mathbb{F}_{q^m} into disjoint cosets of an \mathbb{F}_q -subspace of \mathbb{F}_{q^m} .

In this paper, we choose a multiplicative group G of \mathbb{F}_{q^m} and an \mathbb{F}_q -subspace V of \mathbb{F}_{q^m} , then partition \mathbb{F}_{q^m} into disjoint cosets of by mixing the structures of G and V . Thus, for the trivial group $G = \{1\}$, it degenerates to an \mathbb{F}_q -subspace V of \mathbb{F}_{q^m} , while for the trivial vector space $V = \{0\}$ and $m = 1$, it degenerates to a multiplication subgroup of \mathbb{F}_{q^m} .

1.4 Organization

The rest of this paper is organized as follows. In Section 2, we give some preliminaries to frequency hopping sequences. In Section 3, we present a construction of optimal FHS sets with new parameters by mixing both multiplicative and additive group structures of finite fields. In Section 4, we obtain some optimal FHS sets via the recursive construction through one-coincidence sequence sets. Finally, we conclude the paper in Section 5.

2 Preliminaries

Let $\mathcal{F} = \{f_1, f_2, \dots, f_\ell\}$ be a frequency slot set with size $|\mathcal{F}| = \ell$, and let \mathcal{S} be a set of M frequency hopping sequences of length N . For any two frequency hopping sequences $\mathbf{x} = (x_0,$

x_1, \dots, x_{N-1}) and $\mathbf{y}=(y_0, y_1, \dots, y_{N-1}) \in \mathcal{S}$, and any positive integer τ , $0 \leq \tau \leq N - 1$, the Hamming correlation function $H_{\mathbf{xy}}(\tau)$ of \mathbf{x} and \mathbf{y} at time delay τ is defined as follows:

$$H_{\mathbf{xy}}(\tau) = \sum_{i=0}^{N-1} h(x_i, y_{i+\tau}), \quad (1)$$

where $h(a, b) = 1$ if $a = b$, and $h(a, b) = 0$ otherwise.

For a given FHS set \mathcal{S} , the maximum Hamming autocorrelation $H_a(\mathcal{S})$, the maximum Hamming crosscorrelation $H_c(\mathcal{S})$ and the maximum Hamming correlation $H_m(\mathcal{S})$ are defined as follows, respectively:

$$\begin{aligned} H_a(\mathcal{S}) &= \max_{1 \leq \tau \leq N-1} \{H_{\mathbf{xx}}(\tau) : \mathbf{x} \in \mathcal{S}\}, \\ H_c(\mathcal{S}) &= \max_{0 \leq \tau \leq N-1} \{H_{\mathbf{xy}}(\tau) : \mathbf{x}, \mathbf{y} \in \mathcal{S}, \mathbf{x} \neq \mathbf{y}\}, \\ H_m(\mathcal{S}) &= \max\{H_a(\mathcal{S}), H_c(\mathcal{S})\}. \end{aligned}$$

In 2004, Peng and Fan [9] showed that the maximum Hamming correlation $H_m(\mathcal{S})$ of an FHS set \mathcal{S} of M sequences of length N over a frequency slot set of size ℓ must obey

$$H_m(\mathcal{S}) \geq \left\lceil \frac{(NM - \ell)N}{(NM - 1)\ell} \right\rceil. \quad (2)$$

In this paper, an FHS set \mathcal{S} is said *optimal* if it achieves the Peng-Fan bound with equality.

The one-coincidence sequence set is a special FHS set which was proposed firstly by Shaar and Davies [12] in 1984.

Definition 1. A one-coincidence sequence set is a set of nonrepeating sequences, for which the peak of the Hamming crosscorrelation function equals one for any pair of sequences belonging to the set.

Equivalently speaking, an OC sequence set is an FHS set with the maximum Hamming autocorrelation equal to 0 and maximum Hamming crosscorrelation at most 1.

The following notations will be used throughout this paper:

- $(N, M, \lambda; \ell)$ denotes an FHS set of M sequences of length N over a frequency slot set of size ℓ , with the maximum Hamming correlation equals to λ ;
- $(n, s; v)$ denotes an OC sequence set of s sequences of length n over a frequency slot set of size v , with the maximum Hamming autocorrelation equal to 0 and the maximum Hamming crosscorrelation at most 1;
- r is a divisor of $q - 1$;
- $0 \leq t \leq m - 1$ are integers;
- $\lceil z \rceil$ is the smallest integer larger than or equal to a real number z .

3 New construction of FHS Sets

Let G be a multiplicative subgroup \mathbb{F}_q^* with $|G| = r$. We label all elements of $G = \{g_1, g_2, \dots, g_r\}$. Let V be an \mathbb{F}_q -subspace of dimension t . Then $|V| = q^t$.

Lemma 1. *There exist $\alpha_1 = 0, \alpha_2, \dots, \alpha_\ell \in \mathbb{F}_{q^m}$ with $\ell = 1 + \frac{q^{m-t}-1}{r}$ such that V and $\{\alpha_i g + V : 2 \leq i \leq \ell, g \in G\}$ are $1 + (\ell - 1)r = q^{m-t}$ pairwise distinct cosets of V .*

Proof. Choose $\alpha_2 \in \mathbb{F}_{q^m} \setminus V$. We claim that $\alpha_2 g_1 + V, \dots, \alpha_2 g_r + V$ are pairwise distinct cosets of V . Suppose $\alpha_2 g_i + V = \alpha_2 g_j + V$ for some $1 \leq i \leq j \leq r$. Then, we have $\alpha_2(g_i - g_j) \in V$. Thus, $g_i - g_j = 0$, otherwise, one would have $\alpha_2 \in (g_i - g_j)^{-1}V = V$. This implies that $i = j$.

Next we choose $\alpha_3 \in \mathbb{F}_{q^m} \setminus V \cup (\bigcup_{g \in G} (\alpha_2 g + V))$. Then, in the same way, we can show that $\alpha_3 g_1 + V, \dots, \alpha_3 g_r + V$ are pairwise distinct cosets. Furthermore, we claim that $\alpha_2 g_i + V \neq \alpha_3 g_j + V$ for all $1 \leq i \leq j \leq r$. Suppose $\alpha_2 g_i + V = \alpha_3 g_j + V$ for a pair (i, j) with $1 \leq i \leq j \leq r$, then we would have $\alpha_2 g_i - \alpha_3 g_j \in V$, i.e., $\alpha_2 g_i g_j^{-1} - \alpha_3 \in g_j^{-1}V = V$. Thus, we have $\alpha_3 \in \alpha_2 g_i g_j^{-1} + V \subseteq \bigcup_{g \in G} \alpha_2 g + V$. This is a contradiction.

Continue this fashion to choose $\alpha_i \in \mathbb{F}_{q^m} \setminus V \cup (\bigcup_{2 \leq j \leq i-1} \bigcup_{g \in G} (\alpha_j g + V))$ for $i \geq 4$. Thus, we obtain all the desired cosets V and $\{\alpha_i g + V : 2 \leq i \leq \ell, g \in G\}$. \square

Lemma 2. *Define $\phi(x) = \prod_{g \in G} \prod_{\beta \in V} (x + g + \beta)$. Then $\phi(x)$ is a constant function on the set*

$$\bigcup_{i=1}^r (\gamma g_i + V) \text{ for any fixed } \gamma \in \mathbb{F}_{q^m}.$$

Proof. Let $\gamma \alpha + v \in \bigcup_{i=1}^r (\gamma g_i + V)$ for some $\alpha \in G$ and $v \in V$.

Then we have

$$\begin{aligned} \phi(\gamma \alpha + v) &= \prod_{g \in G} \prod_{\beta \in V} (\gamma \alpha + v + g + \beta) = \alpha^{|G||V|} \prod_{g \in G} \prod_{\beta \in V} (\gamma + g \alpha^{-1} + \beta \alpha^{-1}) \\ &= \alpha^{rq^t} \prod_{g \in G} \prod_{\beta \in V} (\gamma + g + \beta \alpha^{-1}) = \prod_{g \in G} \prod_{\beta \in V} (\gamma + g + \beta) = \phi(\gamma). \end{aligned}$$

Thus, $\phi(x)$ is a constant function on the set $\bigcup_{i=1}^r (\gamma g_i + V)$ for any fixed $\gamma \in \mathbb{F}_{q^m}$. This completes the proof. \square

Lemma 3. *If $1 \leq i \neq j \leq \ell$ with $\ell = 1 + \frac{q^{m-t}-1}{r}$, then $\phi(\alpha) \neq \phi(\beta)$ for all $\alpha \in \bigcup_{g \in G} (\alpha_i g + V)$, $\beta \in \bigcup_{g \in G} (\alpha_j g + V)$.*

Proof. Suppose $\phi(\alpha) = \phi(\beta)$. Let $c = \phi(\alpha)$. Consider the polynomial $\phi(x) - c$. Then all elements of $\left(\bigcup_{g \in G} (\alpha_i g + V) \right) \cup \left(\bigcup_{g \in G} (\alpha_j g + V) \right)$ are roots of $\phi(x) - c$. Thus, $\phi(x) - c$ has

at least $\left| \left(\bigcup_{g \in G} (\alpha_i g + V) \right) \cup \left(\bigcup_{g \in G} (\alpha_j g + V) \right) \right| \geq |V| + |G||V| = q^t + rq^t$ roots. On the other hand, the degree of $\phi(x) - c$ is rq^t . This forces that $\phi(x) - c$ is identical 0, i.e, $\phi(x) = c$. This contradiction completes the proof. \square

Construction of optimal FHS sets.

Step 1: Let r be a divisor of $q-1$. Let θ be a generator of $\mathbb{F}_{q^m}^*$. Let $G = \mathbb{F}_q^*$ be a multiplicative subgroup of \mathbb{F}_q with $|G| = r$. Let V be an \mathbb{F}_q -subspace of \mathbb{F}_{q^m} of dimension t with $0 \leq t \leq m-1$. Choose $\alpha_1 = 0, \alpha_2, \dots, \alpha_\ell \in \mathbb{F}_{q^m}$ with $\ell = 1 + \frac{q^{m-t}-1}{r}$ satisfying that $V, \{\alpha_i g + V : 2 \leq i \leq \ell, g \in G\}$ are q^{m-t} pairwise distinct cosets of V as defined in Lemma 1.

Step 2: Choose $\phi(x)$ as defined in Lemma 2. For every $\alpha_i \in \{\alpha_1, \alpha_2, \dots, \alpha_\ell\}$, we define a sequence

$$\mathbf{s}_i := (\phi(1 + \alpha_i), \phi(\theta + \alpha_i), \phi(\theta^2 + \alpha_i), \dots, \phi(\theta^{q^m-2} + \alpha_i)).$$

Step 3: The desired FHS set \mathcal{S} is a collection of \mathbf{s}_i , i.e.,

$$\mathcal{S} = \begin{cases} \{\mathbf{s}_i\}_{i=1}^\ell & \text{if } r = 1, \\ \{\mathbf{s}_i\}_{i=2}^\ell & \text{if } r \geq 2. \end{cases}$$

Theorem 3. *The FHS set \mathcal{S} constructed above is a $(q^m - 1, M, rq^t; \frac{q^{m-t}-1}{r} + 1)$ FHS set with*

$$M = \begin{cases} \ell = 1 + \frac{q^{m-t}-1}{r} = q^{m-t} & \text{if } r = 1, \\ \ell - 1 = \frac{q^{m-t}-1}{r} & \text{if } r \geq 2. \end{cases}$$

Proof. The sequence length of \mathcal{S} is clearly $q^m - 1$. The family size of \mathcal{S} is also clear. Furthermore, it follows from Lemmas 2 and 3 that the size of frequency slot set of \mathcal{S} is $\ell = 1 + \frac{q^{m-t}-1}{r}$.

Thus, it is sufficient to show that the maximum Hamming correlation of \mathcal{S} is rq^t . Given the facts: (i) the Hamming correlation $H_{\mathbf{s}_i, \mathbf{s}_j}(\tau)$ at time delay τ is the number of the roots of $\phi(\theta^\tau x + \alpha_i) - \phi(x + \alpha_j)$; and (ii) the degree of $\phi(\theta^\tau x + \alpha_i) - \phi(x + \alpha_j)$ is at most rq^t , it is equivalent to showing the following two inequalities.

- (a) $\phi(\theta^\tau x + \alpha_i) \neq \phi(x + \alpha_i), \quad \forall 1 \leq \tau \leq q^m - 2$ and $2 \leq i \leq \ell$ if $r \geq 2$ (and $1 \leq i \leq \ell$ if $r = 1$).
- (b) $\phi(\theta^\tau x + \alpha_i) \neq \phi(x + \alpha_j), \quad \forall 0 \leq \tau \leq q^m - 2$ and $1 \leq i < j \leq \ell$.

Let us prove (a) by contradiction. Suppose $\phi(\theta^\tau x + \alpha_i) = \phi(x + \alpha_i)$ for some $1 \leq \tau \leq q^m - 2$. Then, by comparing the leading coefficients of $\phi(\theta^\tau x + \alpha_i)$ and $\phi(x + \alpha_i)$, we have $(\theta^\tau)^r = 1$, i.e., $\theta^\tau \in G$. If $r = 1$, i.e., $G = \{1\}$, then $\theta^\tau = 1$. This is a contradiction since $\theta^\tau \neq 1$ for all $1 \leq \tau \leq q^m - 2$.

Now we assume that $r \geq 2$. Then $2 \leq i \leq \ell$ and we have

$$\phi(x + \alpha_i) = \phi(\theta^\tau x + \alpha_i) = (\theta^\tau)^r \phi(x + \alpha_i \theta^{-\tau}) = \phi(x + \alpha_i \theta^{-\tau}).$$

Choose $\gamma \in \mathbb{F}_{q^m}$ such that $\gamma + \alpha_i \in V$. By Lemma 3, we must have $\gamma + \alpha_i \theta^{-\tau} \in V$. This gives $(\gamma + \alpha_i \theta^{-\tau}) - (\gamma + \alpha_i) \in V$, i.e., $\alpha_i(\theta^{-\tau} - 1) \in V$. As $\theta^{-\tau} \neq 1$, i.e., $\theta^{-\tau} - 1 \in \mathbb{F}_q^*$, we have $\alpha_i \in (\theta^{-\tau} - 1)^{-1}V = V$. This is a contradiction by Lemma 1.

Again, we prove (b) by contradiction. Suppose $\phi(\theta^\tau x + \alpha_i) = \phi(x + \alpha_j)$ for some $0 \leq \tau \leq q^m - 2$ and $1 \leq i < j \leq \ell$. By comparing the leading coefficients with the same arguments given in the above proof of (a), we have $\theta^\tau \in G$ and $\phi(x + \alpha_i \theta^{-\tau}) = \phi(x + \alpha_j)$.

Choose $\gamma \in \mathbb{F}_{q^m}$ such that $\gamma + \alpha_j \in V$. By Lemma 3, we have $\gamma + \alpha_i \theta^{-\tau} \in V$. This gives $(\gamma + \alpha_i \theta^{-\tau}) - (\gamma + \alpha_j) \in V$, i.e., $\alpha_j \in \alpha_i \theta^{-\tau} + V \subseteq \bigcup_{g \in G} (\alpha_i g + V)$. This is a contradiction by Lemma 1. The proof is completed. \square

Proof of Theorem 1:

Proof. The first part of Theorem 1 was already proved in Theorem 3. Let us prove the second part only.

By the Peng-Fan bound, the FHS set \mathcal{S} is optimal if and only if the following inequality is satisfied.

$$\frac{e(q^m - 1) - (e + 1)}{e(q^m - 1) - 1} \cdot \frac{q^m - 1}{e + 1} > rq^t - 1. \quad (3)$$

The inequality (3) is equivalent to the following inequality.

$$e(q^m - 1)^2 - (e^3 + (e^2 + e)(q^t - 1) + 1)(q^m - 1) + (e + 1)(q^t - 1 + e) > 0. \quad (4)$$

The inequality (4) is always true if $q^m - 1 < e^2 + (e + 1)q^t - 3e$. This completes the proof. \square

We now illustrate our construction by the following examples.

Example 1. Let $q = 3$, $r = 2$, $m = 4$, and $t = 1$.

Let θ be a generator of $\mathbb{F}_{3^4}^*$. Let $G = \mathbb{F}_3^*$ be the multiplicative subgroup of \mathbb{F}_3 with $|G| = 2$. Let V be an \mathbb{F}_3 -subspace of \mathbb{F}_{3^4} of dimension $t = 1$.

Choose $\alpha = \{\alpha_i \in \mathbb{F}_{3^4} : 2 \leq i \leq 14\}$ satisfying that V , $\{\alpha_i g + V : 2 \leq i \leq 14, g \in G\}$ are 27 pairwise distinct cosets of V as defined in Lemma 1.

Choose $\phi(x)$ as defined in Lemma 2. For every $\alpha_i \in \{\alpha_2, \dots, \alpha_{14}\}$, we can obtain an FHS set $\mathcal{S}_1 = \{\mathbf{s}_i, 2 \leq i \leq 14\}$ with

$$\mathbf{s}_i = (\phi(1 + \alpha_i), \phi(\theta + \alpha_i), \phi(\theta^2 + \alpha_i), \dots, \phi(\theta^{79} + \alpha_i)).$$

It is easy to check that FHS set \mathcal{S}_1 is an optimal (80, 13, 6; 14) FHS set with new parameters.

Example 2. Let $q = 3$, $r = 2$, $m = 6$, and $t = 2$.

Let θ be a generator of $\mathbb{F}_{3^6}^*$. Let $G = \mathbb{F}_3^*$ be the multiplicative subgroup of \mathbb{F}_3 with $|G| = 2$. Let V be an \mathbb{F}_3 -subspace of \mathbb{F}_{3^6} of dimension $t = 2$.

Choose $\alpha = \{\alpha_i \in \mathbb{F}_{3^6} : 2 \leq i \leq 41\}$ satisfying that V , $\{\alpha_i g + V : 2 \leq i \leq 41, g \in G\}$ are 81 pairwise distinct cosets of V as defined in Lemma 1.

Choose $\phi(x)$ as defined in Lemma 2. For every $\alpha_i \in \{\alpha_2, \dots, \alpha_{41}\}$, we can obtain an FHS set $\mathcal{S}_2 = \{\mathbf{s}_i, 2 \leq i \leq 41\}$ with

$$\mathbf{s}_i = (\phi(1 + \alpha_i), \phi(\theta + \alpha_i), \phi(\theta^2 + \alpha_i), \dots, \phi(\theta^{727} + \alpha_i)).$$

It is easy to check that FHS set \mathcal{S}_2 is an optimal (728, 40, 18; 41) FHS set with new parameters.

Example 3. Let $q = 7$, $r = 3$, $m = 3$, and $t = 1$.

Let θ be a generator of $\mathbb{F}_{7^3}^*$. Let $G = \mathbb{F}_7^*$ be the multiplicative subgroup of \mathbb{F}_7 with $|G| = 3$. Let V be an \mathbb{F}_7 -subspace of \mathbb{F}_{7^3} of dimension $t = 1$.

Choose $\alpha = \{\alpha_i \in \mathbb{F}_{7^3} : 2 \leq i \leq 17\}$ satisfying that V , $\{\alpha_i g + V : 2 \leq i \leq 17, g \in G\}$ are 49 pairwise distinct cosets of V as defined in Lemma 1.

Choose $\phi(x)$ as defined in Lemma 2. For every $\alpha_i \in \{\alpha_2, \dots, \alpha_{17}\}$, we can obtain an FHS set $\mathcal{S}_3 = \{\mathbf{s}_i : 2 \leq i \leq 17\}$ with

$$\mathbf{s}_i = (\phi(1 + \alpha_i), \phi(\theta + \alpha_i), \phi(\theta^2 + \alpha_i), \dots, \phi(\theta^{341} + \alpha_i)).$$

It is easy to check that FHS set \mathcal{S}_3 is an optimal (342, 16, 21; 17) FHS set with new parameters.

4 Recursive Constructions of FHS sets with new parameters

Recursive constructions have been proposed in [2, 10, 16, 1, 8] to generate new families of optimal FHS sets under certain conditions. The framework of recursive constructions in [8] can be used to get FHS set with new parameters, which increase the length and alphabet size of the original FHS set, but preserve its family size and maximum Hamming correlation. In this section, by applying the FHS set \mathcal{S} in Theorem 3 to a recursive construction, we obtain some new classes of FHS sets.

Let us recall a recursive construction first. Denote by $m(\mathcal{S})$ the maximum appearance number of frequency slots of an FHS set \mathcal{S} .

Lemma 4. *Whenever there exist an $(N, M, H_m; l)$ FHS set \mathcal{S} and an $(n, s; v)$ OC sequence set \mathcal{C} with $s \geq m(\mathcal{S})$, there is an $(nN, M, H_m; vl)$ FHS set \mathcal{X} .*

To apply Lemma 4, we have to give an upper bound on $m(\mathcal{S})$.

Lemma 5. *For $r \geq 2$, the maximum appearance number $m(\mathcal{S})$ of frequency slots of the FHS set \mathcal{S} in Theorem 3 is upper bounded by $q^m - q^t - 1$.*

Proof. For $1 \leq i \leq \ell$, denote by A_i the set $\{\theta^k + \alpha_i : 0 \leq k \leq q^m - 2\}$. By Lemma 3, to count appearance of an element, we have to count the appearance number n_{ij} of elements of $\bigcup_{g \in G} (\alpha_i g + V)$ in A_j for all $1 \leq i \leq \ell$ and $2 \leq j \leq \ell$. Then we have $m(\mathcal{S}) = \max_{1 \leq i \leq \ell} \{\sum_{j=2}^{\ell} n_{ij}\}$.

For $i = 1$ and $2 \leq j \leq \ell$, every element in V appears in A_j once. Thus, the total appearance number of elements of $\bigcup_{g \in G} (\alpha_1 g + V)$ in $\bigcup_{j=2}^{\ell} A_j$ is $|V|(\ell - 1) = q^t \frac{q^{m-t} - 1}{r} < q^m - q^t - 1$ for $r \geq 2$.

For $2 \leq i \leq \ell$, every element in $\bigcup_{g \in G} (\alpha_i g + V)$ appears in A_j once for $j \neq i$. For $j = i$, every element in $\bigcup_{g \in G} (\alpha_i g + V)$ except for α_i appears in A_i once and α_i does not appear in A_i . Thus, the total appearance number of elements of $\bigcup_{g \in G} (\alpha_i g + V)$ in $\bigcup_{j=2}^{\ell} A_j$ is $r|V|(\ell - 1) - 1 = rq^t \left(\frac{q^{m-t} - 1}{r} \right) - 1 = q^m - q^t - 1$. The proof is completed. \square

The recursive constructions extend the FHS set \mathcal{S} in the above section by choosing different one-coincide sequence sets. There are some known constructions of OC sequence sets [12, 4, 15, 11, 8]. Based on the framework of the recursive construction in [8], we can obtain FHS sets with new parameters by combing the FHS set in Theorem 3 with OC sequence sets.

Let $e = \frac{q^{m-t} - 1}{r}$, then we have the following theorem and corollaries.

Theorem 4. *Put $e = \frac{q^{m-t} - 1}{r}$. Then whenever there is an $(n, s; v)$ OC sequence set with $s > q^m - q^t - 1$, there exists a $(n(q^m - 1), e, rq^t; v(e + 1))$ FHS set \mathcal{X} . Furthermore, \mathcal{X} is optimal if*

$$\left\lceil \frac{n(q^m - 1)e - v(e + 1)}{n(q^m - 1)e - 1} \frac{n(q^m - 1)}{v(e + 1)} \right\rceil = \left\lceil \frac{(q^m - 1)e - (e + 1)(q^m - 1)}{(q^m - 1)e - 1} \frac{(q^m - 1)}{e + 1} \right\rceil.$$

Proof. The desired result follows from Theorem 1 and Lemma 4. \square

Proof of Theorem 2:

Proof. By applying the $(k, \text{lpf}(k) - 1; k)$ OC sequence set given in [2, 1, 8], the $(p - 1, p; p)$ OC sequence set given in [2, 1, 8] and the $(k(p - 1), \min\{\text{lpf}(k) - 1, p\}; kp)$ OC sequence set given in [2, 8], respectively to Theorem 4, we obtain the desired FHS sets in Table 1. \square

We illustrate Theorem 2 by the following examples.

Example 4. Choose the optimal $(80, 13, 6; 14)$ FHS set \mathcal{S}_1 in Example 1. We can obtain the maximum appearance number of frequency slots in \mathcal{S}_1 is 77. Thus, the desired recursive result of FHS sets with new parameters are as follows.

- 1) There is an optimal $(79 \times 80, 13, 6; 79 \times 14)$ FHS set by applying the $(79, 78; 79)$ OC sequence set.
- 2) There is an optimal $(80 \times 80, 13, 6; 81 \times 14)$ FHS set by applying the $(80, 81; 81)$ OC sequence set.
- 3) There is an optimal $(79 \times 80 \times 80, 13, 6; 79 \times 81 \times 14)$ FHS set by applying the $(79 \times 80, 78; 79 \times 81)$ OC sequence set.

Example 5. Choose the optimal $(728, 40, 18; 41)$ FHS set \mathcal{S}_2 in Example 2. We can obtain the maximum appearance number of frequency slots in \mathcal{S}_2 is 719. Thus, the desired recursive result of FHS sets with new parameters are as follows.

- 1) There is an optimal $(727 \times 728, 40, 18; 727 \times 41)$ FHS set by applying the $(727, 726; 727)$ OC sequence set.
- 2) There is an optimal $(728 \times 728, 40, 18; 729 \times 41)$ FHS set by applying the $(728, 729; 729)$ OC sequence set.
- 3) There is an optimal $(727 \times 728 \times 728, 40, 18; 727 \times 729 \times 41)$ FHS set by applying the $(727 \times 728, 726; 727 \times 729)$ OC sequence set.

5 Conclusion

In this paper, we present new construction of optimal FHS sets by mixing both multiplicative and additive groups structures of finite fields simultaneously. The construction provides a new family of optimal $\left(q^m - 1, \frac{q^{m-t}-1}{r}, rq^t; \frac{q^{m-t}-1}{r} + 1\right)$ frequency hopping sequence sets archiving the Peng-Fan bound. Thus, the FHS sets constructed in literatures using either multiplicative groups or additive groups of finite fields are all included in our family. It should be noted that our construction not only includes some constructions in literatures as special cases, but also gives new and flexible parameters due to the free choice of t . In addition, some other FHS sets can be obtained via the well-known recursive constructions through one-coincidence sequence set. As a result, our constructions allow a great flexibility of choosing FHS sets for a given frequency-hopping spread spectrum system.

References

- [1] J. Bao, L. Ji, "New families of optimal frequency hopping sequence sets," *IEEE Trans. Inf. Theory*, vol. 62, no.9, pp.5209-5224, Sep. 2016.
- [2] J. Chung, G. Gong, K. Yang, "New families of optimal frequency-hopping sequences of composite lengths," *IEEE Trans. Inf. Theory*, vol. 60, no.6, pp.3688-3697, Jun. 2014.

- [3] W. Chu, C. Colbourn, "Optimal frequency-hopping sequences via cyclotomy," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1139-1141, Mar. 2005.
- [4] Z. Cao, G. Ge and Y. Miao, "Combinatorial characterizations of one-coincidence frequency-hopping sequences," *Des. Codes Cryptography*, vol.41, no.2, pp.177-184, Nov.2006.
- [5] C. Ding and J. Yin, "Sets of optimal frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3741-3745, Aug. 2008.
- [6] P. Fan and M. Darnell, "Sequence Design for Communications Applications. London," U.K.: Wiley, 1996.
- [7] A. Lempel, H. Greenberger, "Families sequence with optimal Hamming correlation properties," *IEEE Trans. Inf. Theory*, vol.IT-20, pp.90-94, Jan. 1974.
- [8] X. Niu and C. Xing, "New extension constructions of optimal frequency hopping sequence sets," arXiv:1806.09869, 2018.
- [9] 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. 2149C2154, Sep. 2004.
- [10] W. Ren, F. Fu, Z. Zhou, "New sets of frequency-hopping sequences with optimal Hamming correlation," *Des. Codes Cryptograph.*, vol. 72, no. 2, pp. 423-434, Nov. 2014.
- [11] W. Ren, F. Fu, F. Wang, et al., "A class of optimal one-coincidence frequency-hopping sequence sets with composite length," *IEICE Trans. Fund. of Elec. Comm. Comp. Sci.*, vol.E100-A, no.11, pp.2428-2533, Nov.2017.
- [12] A. Shaar and P. Davies, "A survey of one-coincidence sequences for frequency-hopped spread-spectrum systems," *IEE Proceeding F-Communciations, Radar and Signal Processing*, vol.131, no.7, pp.719-724, Dec.1984
- [13] M. Simon, J. Omura, R.A. Scholtz, and B.K. Levitt, "Spread Spectrum Communications Handbook." New York, NY, USA: McGraw-Hill, 1994.
- [14] P. Udaya and M. Siddiqi, "Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1492-1503, Jul. 1998.
- [15] H. Wang and P. Huang, "Construction of a one-coincidence frequency-hopping sequence set with optimal performance," Springer International Publishing Switzerland, pp.915-923, 2015.
- [16] X. Xu, X. Cao, G. Xu, "Recursive construction of optimal frequency-hopping sequence sets," *IET Communications*, vol. 10, no. 9, pp.1080-1086, Jun. 2016.
- [17] X. Xu, X. Cao, G. Xu, "Two classes of optimal frequency-hopping sequences with new parameters," *Applicable Algebra in Engineering, Communication and Computing*, <https://doi.org/10.1007/s00200-018-0356-0>, Apr. 2018.
- [18] 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.
- [19] 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.
- [20] 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.