doi:10.3934/amc.2022024

CONSTRUCTION OF THREE CLASSES OF STRICTLY OPTIMAL FREQUENCY-HOPPING SEQUENCE SETS

Xianhong Xie

Key Laboratory of Electromagnetic Space Information, CAS
School of Cyber Science and Technology
University of Science and Technology of China, Hefei, Anhui 230027, China

Yi Ouyang

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences
University of Science and Technology of China, Hefei, Anhui 230027, China

Honggang Hu

Key Laboratory of Electromagnetic Space Information, CAS
School of Cyber Science and Technology
University of Science and Technology of China, Hefei, Anhui 230027, China

Ming Mao

Beijing Electronic Science and Technology Institute, Beijing 100070, China

(Communicated by Zhengchun Zhou)

Abstract. In this paper, we construct three classes of strictly optimal frequency-hopping sequence (FHS) sets with respect to partial Hamming correlation and family size. The first and second classes are based on the trace map, the third class is based on a generic construction.

1. Introduction

With advantages such as secure properties, multiple-access, anti-jamming, and anti-fading, frequency-hopping multiple-access (FHMA) is now widely used in modern communication systems such as military communications, bluetooth, sonar echolocation systems and so on [26]. In FHMA systems, frequency-hopping sequences (FHSs) are used to control the frequency on which each sender transmits a message at any given time, so there exist two and more sender transmit their packet in the same frequency, it may cause a collision. But the collision can be measured by the Hamming correlation of FHS set. To reduce the multi-access interference due to the frequency collisions, the Hamming correlation of FHS set must be minimized. In fact, the parameters of FHS sets are not independent with each other, and they are subjected to limitation of some theoretic bounds, for example, the Lempel-Greenberger bound [19], the Peng-Fan bound [24], or the coding theory bound [8]. Therefore, it has received a lot of attention about constructing optimal

2020 *Mathematics Subject Classification:* 11B50, 94A55, 94A60.

Key words and phrases: Frequency-hopping sequences, partial Hamming correlation, difference-balanced functions.

Research is partially supported by Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200) and NSFC (Grant No. 11571328).

*Corresponding author: Yi Ouyang.

FHSs with respect to the bounds and much progress have been made (see [9]-[12], [27]-[17], [31, 23], [15] and the references therein).

The traditional Hamming correlation of FHSs can be divided into two types in general: the periodic Hamming correlation and the aperiodic Hamming correlation. Considering the correlation window, the Hamming correlation can be divided into the periodic partial Hamming correlation, and the aperiodic partial Hamming correlation. Compared with the traditional type, the results are relatively little known about the periodic partial and aperiodic partial ones. In the practical application scenarios, the length of a correlation window is usually shorter than the period of the chosen FHSs and may vary from time to time according to the channel conditions [10]. Consequently, the partial Hamming correlation begin to attract attention, and this paper shall focus on the construction of FHS sets with respect to the periodic partial Hamming correlation. Eun et al. [10] obtained a class of FHSs with optimal partial Hamming correlation from the m-sequence and GMW sequences over polynomial residue class ring. In 2012, Zhou et al. [32] derived FHS sets with optimal partial Hamming correlation from trace functions, and generalized the Peng-Fan bounds on the periodic Hamming correlation based on the array structure.

In 2014, Cai et al. [4] presented FHS sets with optimal partial Hamming correlation from generalized cyclotomy. Later, the authors gave some theoretic bounds of the size of FHS sets and presented a new class of FHSs with optimal partial Hamming correlation in [3]. Very recently, combinatorial constructions of FHSs with optimal partial Hamming correlation have been reported, see [1, 2, 11, 29, 21].

The purpose of this paper is to construct three classes of strictly optimal FHS sets with optimal partial Hamming correlation and optimal family sizes. We list the parameters of our construction and related known ones in Table 1, which gives a comparison of our construction and the constructions before us.

TABLE 1. Known Strictly Optimal FHS Sets

Length	Alphabet Size	$\mathcal{M}(\mathcal{F};L)$	Family Size	Constraints	Reference
$\frac{p^m-1}{r}$	p^{m-1}	$\lceil \frac{L}{T} \rceil$	r	$\psi(x)$ is identity, $r\|p-1$, $\gcd(r,m)=1$	[32]
$p^{2m}-1$	p^m	$\lceil \frac{L}{p^m+1} \rceil$	1		[32, 10]
$p(p^m-1)$	p^m	$\lceil \frac{L}{p^m-1} \rceil$	p^{m-1}	$\phi(x)$ is identity	[3]
$\frac{p^m-1}{r}$	p^{m-1}	$\lceil \frac{L}{T} \rceil$	r	$\psi(x)$, $r\|p-1$, $\gcd(r,m)=1$	Theorem 3.2 here
$\frac{p^{2m}-1}{r}$	p^m	$\lceil \frac{L}{p^m+1} \rceil$	r	$f(x)$, $r\|p-1$, $\gcd(r,2m)=1$	Theorem 3.4 here
$p(p^m-1)$	p^m	$\lceil \frac{L}{p^m-1} \rceil$	p^{m-1}	$\phi(x)$	Theorem 4.5 here

$T=\frac{q-1}{p-1}$, $q=p^m$ and $\gcd(d,p-1)=1$; $\psi(x)$ is $\mathbb{F}_p$-linear automorphism of $\mathbb{F}_q$; $\phi(x)$ can be found in Lemma 4.3; $f:\mathbb{F}_{q^2}\to\mathbb{F}_q$ is d-form difference-balanced function.

Compared with the constructions in [32, 10], our first and second constructions generate strictly optimal FHS sets by using the trace map, and it provides us a large number of choice for $\psi(x)$ and $f(x)$ (see Table 1). The third class is a generic construction, it can generate a great deal of strictly optimal FHS sets by using some sequence sets (satisfied **A1**) and sequences (satisfied **A2**).

2. Preliminaries

Throughout this paper we shall use the following notations.

- p is an odd prime and $q = p^m > 1$ is a p-power;
- $\mathbb{F}_q$ is the finite field of q elements, and $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ is the multiplicative group of $\mathbb{F}_q$;
- α is a primitive element of $\mathbb{F}_q$;
- $\mathrm{Tr}_{q^n/q}(x) = \sum_{i=0}^{n-1} x^{q^i}$ is the trace map from $\mathbb{F}_{q^n}$ to its subfield $\mathbb{F}_q$;
- For $t \in \mathbb{Z}$, $\langle t \rangle_n \in \{0, \cdots, n-1\}$ denotes the remainder of t by n.
- For all sequences $(x_t)_{t=0}^{n-1}$ indexed by a subscript $t \in \{0, \cdots, n-1\}$, we denote $x_t = x_{\langle t \rangle_n}$ for any $t \in \mathbb{Z}$.
- For X a finite set, $\#X$ denotes the cardinality of X. For the map $f : X \to Y$ and $y \in Y$, $f^{-1}(y) = \{x \in X : \ f(x) = y\}$ is the set of preimages of y.

2.1. Strictly optimal FHS sets.

Let N, M be two positive integers and $F = \{f_0, f_1, \dots, f_{d'-1}\}$ be an alphabet of d' available frequencies. Let $\mathcal{F}$ be a set of M frequency-hopping sequences of the form $(x_i)_{i=0}^{N-1}$ with $x_i \in F$. We also call $\mathcal{F}$ an $(N, M; d')$-FHS set. For $X = (x_t)_{t=0}^{N-1}$ and $Y = (y_t)_{t=0}^{N-1}$ in $\mathcal{F}$, the partial Hamming correlation of X and Y over a window of length $L \in \{1, \cdots, N\}$ starting from $j \in \{0, \cdots, N-1\}$ is

$$H_{X,Y}(\tau; j \mid L) := \sum_{t=j}^{j+L-1} h[x_t, y_{t+\tau}] \quad (\tau \in \{0, \cdots, N-1\}), \tag{1}$$

where $h[a, b] = 1$ if $a = b$ and 0 otherwise (i.e. the Kronecker δ-function). In other words,

$$H_{X,Y}(\tau; j \mid L) = \#\{t : \ j \le t \le j + L - 1, \ x_t = y_{t+\tau}\}. \tag{2}$$

If $X = Y$ (resp. $X \neq Y$), $H_{X,X}(\tau; j \mid L)$ (resp. $H_{X,Y}(\tau; j \mid L)$) is called the partial Hamming autocorrelation (resp. cross-correlation) of X (resp. X and Y). Define

$$H(X; L) := \max_{\substack{0 \le j < N \\ 1 \le \tau < N}} H_{X,X}(\tau; j \mid L) \quad (X \in \mathcal{F}), \tag{3}$$

$$H(X, Y; L) := \max_{\substack{0 \le j < N \\ 0 \le \tau < N}} H_{X,Y}(\tau; j \mid L) \quad (X \neq Y \in \mathcal{F}), \tag{4}$$

$$\mathcal{M}(\mathcal{F}; L) := \max_{\substack{X, Y \in \mathcal{F} \\ X \neq Y}} \{H(X; L), H(X, Y; L)\}. \tag{5}$$

In 2014, Cai et al. [4] obtained the following bounds on the maximum partial Hamming correlation of FHS sets: for any $(N, M; d')$-FHS set $\mathcal{F}$, for any window length $1 \le L \le N$,

$$\mathcal{M}(\mathcal{F}; L) \ge \left\lceil \frac{L}{N} \left\lceil \frac{(NM - d')N}{(MN - 1)d'} \right\rceil \right\rceil, \tag{6}$$

and

$$\mathcal{M}(\mathcal{F}; L) \ge \left\lceil \frac{[2IMN - (I + 1)Id']L}{(MN - 1)MN} \right\rceil, \tag{7}$$

where $I = \left\lfloor \frac{MN}{d'} \right\rfloor$. The partial Hamming correlation bound in (6) is the bound proved by Eun et al. [10] for the case $M = 1$, the Lempel-Greenberger bound by [19] for $L = N$ and $M = 1$, and the Peng-Fan bound by [24] for $L = N$. In fact, the bounds defined in Eqs. (6) and (7) are proved to be the same in [5, Theorem 1.3] if $NM > d'$.

In 2016, inspired by the idea of Ding et al. [8], Cai et al. [3] obtained the following results: for any $(N, M; d')$-FHS set $\mathcal{F}$,

$$M \leq \min_{2\leq L\leq N} \left\{ \left\lfloor \frac{1}{N} \left\lfloor \frac{(L-\mathcal{M}(\mathcal{F};L))d'}{L-d'\mathcal{M}(\mathcal{F};L)} \right\rfloor \right\rfloor : \ L > d'\mathcal{M}(\mathcal{F};L) \right\}, \tag{8}$$

and

$$M \leq \min_{2\leq L\leq N} \left\{ \left\lfloor \frac{d'^{\mathcal{M}(\mathcal{F};L)+1}}{N} \right\rfloor : \ L > \mathcal{M}(\mathcal{F};L) \right\}. \tag{9}$$

Definition 2.1. Let $\mathcal{F}$ be an $(N, M; d')$-FHS set.

(1) $\mathcal{F}$ is said to be strictly optimal with respect to the partial Hamming correlation if one of the bounds in (6) or (7) is achieved for any correlation window length $1 \leq L \leq N$.

(2) $\mathcal{F}$ is said to be strictly optimal with respect to family size if one of the bounds in (8) or (9) is achieved for any correlation window length $2 \leq L \leq N$.

2.2. DIFFERENCE-BALANCED FUNCTIONS.

Definition 2.2. A function $f(x) : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is called balanced if $\#f^{-1}(x) = q^{n-1}$ for each $x \in \mathbb{F}_q$. It is called difference-balanced if the difference function $f(\delta x) - f(x)$ is balanced for any $\delta \in \mathbb{F}_{q^n} \setminus \{0, 1\}$.

Remark 1. In the literature (see [25]), balanced and difference-balanced functions are defined over $\mathbb{F}_{q^n}^*$. However, the following is clear. If assigning $f(0) = 0$ to a balanced function f over $\mathbb{F}_{q^n}^*$, one gets a balanced function over $\mathbb{F}_{q^n}$; for a balanced function f over $\mathbb{F}_{q^n}$, then $f - f(0)$ is a balanced function over $\mathbb{F}_{q^n}^*$. If assigning $f(0) = b$ for any $b \in \mathbb{F}_q$ to a difference-balanced function f over $\mathbb{F}_{q^n}^*$, one gets a difference-balanced function over $\mathbb{F}_{q^n}$; for a difference-balanced function f on $\mathbb{F}_q$, the restriction of f on $\mathbb{F}_{q^n}^*$ is a difference-balanced function over $\mathbb{F}_{q^n}^*$.

Pott-Wang [25] tells us that a difference-balanced function f such that $f(0) = 0$ is always balanced. Moreover, the following is the list of all known difference-balanced functions from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ satisfying $f(0) = 0$:

(0) Functions which are surjective and $\mathbb{F}_q$-linear.

(1) Functions of the form

$$f(x) = \mathrm{Tr}_{q^n/q}(x^d), \tag{10}$$

where d is a positive integer prime to $q^n - 1$.

(2) Functions of Helleseth-Gong type, which was discovered in [16].

(3) Functions of Lin type

$$f(x) = \mathrm{Tr}_{3^n/3}(x + x^s), \tag{11}$$

where $q = 3$, $n = 2l + 1$ and $s = 2 \times 3^l + 1$. The difference balance property of functions of this type was a conjecture of Lin [20] and proved by Hu et al. [18].

(4) Functions which are composites of functions of the previous types (when the composition is legal).

Definition 2.3. Let d be an integer prime to $q - 1$. A function $f(x)$ from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$ is called a d-form function if

$$f(yx) = y^d f(x)$$

for any $y \in \mathbb{F}_q$ and $x \in \mathbb{F}_{q^n}$.

By definition, it is easy to see all the known difference-balanced functions are d-form functions: functions of type (0) are 1-form functions, of type (1) are d-form functions, and of type (2) and (3) are 1-form functions for the case $q = p$.

Lemma 2.4. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_q$ be a d-form difference-balanced function and $\delta \notin \{0, 1\}$, let $f_\delta(x) = f(\delta x) - f(x)$. Then $f_\delta^{-1}(0) = \mathbb{F}_q \cdot a_\delta$ for some $a_\delta \in \mathbb{F}_{q^2}^*$.*

Proof. On one hand $f_\delta^{-1}(0)$ is of order q as f_δ is balanced. On the other hand, $f(ca) = c^d f(a)$ if $c \in \mathbb{F}_q$, hence $f_\delta(a) = 0$ implies that $f_\delta(ca) = 0$ for any $c \in \mathbb{F}_q$. □

Remark 2. All known difference-balanced functions $f : \mathbb{F}_{q^2} \to \mathbb{F}_q$ such that $f(0) = 0$ are d-form functions belonging to one of the following two types: (i) a surjective $\mathbb{F}_q$-linear map; (ii) $(x \mapsto \psi(\mathrm{Tr}_{q^2/q}(x^d)))$ or $(x \mapsto \mathrm{Tr}_{q^2/q}(\psi(x^d)))$ where ψ is an $\mathbb{F}_q$-linear automorphism of $\mathbb{F}_{q^2}$.

3. CONSTRUCTION OF OPTIMAL FHS SETS VIA THE TRACE MAP

Let $q = p^m$ and α be a primitive root of $\mathbb{F}_q^*$. Let $T = \frac{q-1}{p-1}$. For a nonzero vector $\mathbf{w} = (a_0, a_1, \ldots, a_{k-1}) \in \mathbb{F}_q^k$, let $V_{\mathbf{w}} = \langle a_0, \cdots, a_{k-1} \rangle_{\mathbb{F}_p}$ be the $\mathbb{F}_p$-subspace of $\mathbb{F}_q$ generated by $\mathbf{w}$ and let $R(\mathbf{w}) = \dim_{\mathbb{F}_p} V_{\mathbf{w}}$. Define the map $\mathcal{T} = \mathcal{T}_{\mathbf{w}} : \mathbb{F}_q \to \mathbb{F}_p^k$ by

$$\mathcal{T}(x) = (\mathrm{Tr}_{q/p}(a_0 x), \mathrm{Tr}_{q/p}(a_1 x), \ldots, \mathrm{Tr}_{q/p}(a_{k-1} x)). \tag{12}$$

Lemma 3.1. *The map $\mathcal{T}$ is an $\mathbb{F}_p$-linear map whose kernel $\ker(\mathcal{T}) = V_{\mathbf{w}}^\perp$ where $V_{\mathbf{w}}^\perp$ is the orthogonal complementary of $V_{\mathbf{w}}$ via the nondegenerate bilinear map $\mathrm{Tr}_{q/p}$. In particular, $\dim_{\mathbb{F}_p} \ker(\mathcal{T}) = m - R(\mathbf{w})$ and $\dim_{\mathbb{F}_p} \mathrm{Im}(\mathcal{T}) = R(\mathbf{w})$.*

Proof. An element $x \in \ker(\mathcal{T})$ if and only if $\mathrm{Tr}_{q/p}(a_i x) = 0$, i.e., $x \perp a_i$ for all i, in other words, $x \in V_{\mathbf{w}}^\perp$. □

We construct optimal FHS sequences based on $\mathbf{w}$ with $R(\mathbf{w}) = m - 1$ or m.

3.1. FIRST CLASS OF OPTIMAL FHS SETS.

Theorem 3.2. *Fix $\mathbf{w} = (a_0, \cdots, a_{k-1}) \in \mathbb{F}_q^k$ such that $R(\mathbf{w}) = m-1$. Let $r \mid p-1$ such that $\gcd(r, m) = 1$ and $n' = \frac{q-1}{r}$. Let $v = (\alpha^{rt})_{0 \le t \le n'-1}$. Let $d \in \mathbb{Z}$ such that $\gcd(d, q-1) = 1$ and ψ be an $\mathbb{F}_p$-linear automorphism of $\mathbb{F}_q$. Define the sequence set*

$$\mathcal{F} = \mathcal{F}(\mathbf{w}; r, d, \psi) = \{S^i : 0 \le i \le r-1\}$$

where

$$S^i = (s_t^i)_{0 \le t \le n'-1} \text{ and } s_t^i = \mathcal{T} \circ \psi(\alpha^{d(i+rt)}). \tag{13}$$

Then $\mathcal{F}$ is an $(n', r; p^{m-1})$-FHS set and for each correlation window length $1 \le L \le n'$,

$$\mathcal{M}(\mathcal{F}; L) = \left\lceil \frac{L}{T} \right\rceil.$$

Moreover, $\mathcal{F}$ is a strictly optimal FHS set with optimal partial Hamming correlation with respect to the bound in (7) and with optimal family size with respect to the bound in (8).

Proof. As $\gcd(d, q-1) = 1$, α^d is still a primitive root of $\mathbb{F}_q^*$. Replacing α by α^d, we may assume $d = 1$.

The alphabet set $\{s_t^i :\ 0 \le i \le r-1,\ 0 \le t \le n'-1\}$ of $\mathcal{F}$ is nothing but $\mathrm{Im}(\mathcal{T})$, hence it is of order p^{m-1} by Lemma 3.1.

We are left to compute $\mathcal{M}(\mathcal{F}; L)$. Note that $\ker(\mathcal{T} \circ \psi) = \psi^{-1}\ker(\mathcal{T})$ is 1-dimensional $\mathbb{F}_p$-vector space, pick $0 \neq a \in \ker(\mathcal{T} \circ \psi)$, then $\ker(\mathcal{T} \circ \psi) = a\mathbb{F}_p$. Fix i, j and τ such that if $i = j$, then $\tau \not\equiv 0 \bmod n'$. The value $H_{S^i,S^j}(\tau; l \mid T)$ is nothing but the number of $t \in [l, l+L-1]$ such that $s_t^i = s_{t+\tau}^j$, in other words, $\alpha^{i+rt} - \alpha^{j+r(t+\tau)} = \alpha^{rt}(\alpha^i - \alpha^{j+r\tau}) \in a\mathbb{F}_p$. Note that $i - j - r\tau$ is not a multiple of $q-1$, hence $\alpha^i - \alpha^{j+r\tau} \neq 0$. Let $b = (\alpha^i - \alpha^{j+r\tau})^{-1}a$, then

$$s_t^i = s_{t+\tau}^j \iff \alpha^{rt} \in b\mathbb{F}_p^*.$$

Suppose we have $\alpha^{rt_0} \in b\mathbb{F}_p^*$ for some t_0 (otherwise $H_{S^i,S^j}(\tau; l \mid L) = 0$). Then

$$s_t^i = s_{t+\tau}^j \iff \alpha^{r(t-t_0)} \in \mathbb{F}_p^*.$$

Note that $\mathbb{F}_p^* = \{\alpha^{cT} : 0 \le c \le p-2\}$ and $\gcd(r, T) = \gcd(r, m) = 1$, then

$$s_t^i = s_{t+\tau}^j \iff t - t_0 \in T\mathbb{Z}.$$

This means that the number of $t \in [l, l+L-1]$ such that $s_t^i = s_{t+\tau}^j$ is at most $\lceil \frac{L}{T} \rceil$, i.e., $H_{S^i,S^j}(\tau; l \mid L) \le \lceil \frac{L}{T} \rceil$. Hence $\mathcal{M}(\mathcal{F}, L) \le \lceil \frac{L}{T} \rceil$.

On the other hand, the bound Eq. (7) gives

$$\begin{aligned} \mathcal{M}(\mathcal{F}; L) &\ge \left\lceil \frac{L}{N} \cdot \frac{[2INM - (I+1)Id']}{(NM-1)M} \right\rceil \\ &= \left\lceil \frac{Lr}{q-1} \cdot \frac{(p-1)(q-2)}{(q-2)r} \right\rceil = \left\lceil \frac{L}{T} \right\rceil. \end{aligned}$$

Thus $\mathcal{M}(\mathcal{F}, L) = \lceil \frac{L}{T} \rceil$ and $\mathcal{F}$ is optimal with respect to the bound in (7).

Set $L = \frac{q-1}{r}$, then $\mathcal{M}(\mathcal{F}; L) = \frac{p-1}{r}$ and $d'\mathcal{M}(\mathcal{F}; L) < L$. According to the bound in (8), we have

$$M \le \left\lfloor \frac{1}{N} \left\lfloor \frac{(L - \mathcal{M}(\mathcal{F}; L))d'}{L - d'\mathcal{M}(\mathcal{F}; L)} \right\rfloor \right\rfloor = \left\lfloor \frac{rq}{q-1} \right\rfloor = r.$$

Thus the family size of $\mathcal{F}$ is optimal with respect to the bound in (8). This completes the proof. □

Remark 3. In Theorem 3.2, from the choice of $\psi(x)$, we can see that $\mathcal{F}$ is equivalent with the ones constructed in [32], where two sequence sets are called equivalent if one can be obtained by the other from permuting the symbols of the corresponding alphabet (see [22]). However, the method of determining the Hamming correlation here is more straightforward and simple.

Example 3.3. *Let $p = 5$, $m = d = 3$, $r = 2$ and $(a_0, a_1) = (1, \alpha)$, where α is a primitive element of $\mathbb{F}_{5^3}$ over $\mathbb{F}_5$ generated by $\alpha^3 + \alpha + 1 = 0$. Suppose ψ is Frobenius automorphism of $\mathbb{F}_{5^3}$. Then the set $\mathcal{F}$ of (13) consists of the following two FHSs:*

$$\begin{aligned} S^0 = (&(3,0), (1,3), (1,2), (4,2), (0,0), (1,2), (0,4), (0,4), (1,1), (1,0), (1,4), (2,0), \\ &(3,0), (4,4), (1,4), (4,4), (3,3), (4,2), (3,1), (1,4), (0,1), (3,2), (4,1), (4,2), \cdots); \\ S^1 = (&(2,4), (1,4), (2,2), (4,1), (0,0), (2,2), (1,3), (1,3), (3,0), (4,3), (0,1), (3,1), \\ &(2,4), (2,0), (0,1), (2,0), (4,0), (4,1), (1,1), (0,1), (4,2), (0,3), (0,4), (4,1), \cdots). \end{aligned}$$

By computation,

$$\mathcal{M}(\mathcal{F};L)=\left\lceil\frac{L}{31}\right\rceil=\begin{cases}1, & \text{for } 1\le L\le 31,\\ 2, & \text{for } 31<L\le 62.\end{cases}$$

$\mathcal{F}$ is strictly optimal with respect to the bound in (7), and also has an optimal family size with respect to the bound in (8).

3.2. Second class of optimal FHS sets.

Theorem 3.4. *Fix $\mathbf{w}=(a_0,\cdots,a_{k-1})$ and assume $R(\mathbf{w})=m$. Let θ be a primitive element of $\mathbb{F}_{q^2}$, r be an odd factor of $q-1$, $n'=\frac{q^2-1}{r}$ and $v=(\theta^{rt})_{t=0}^{n'-1}$. Suppose $f:\mathbb{F}_{q^2}\to\mathbb{F}_q$ is a d-form difference-balanced function. Define a sequence set $\mathcal{F}=:\{S^i=(s_t^i)_{0\le t\le n'-1}:0\le i\le r-1\}$ by*

$$s_t^i=\mathcal{T}(f(\theta^{i+rt})). \tag{14}$$

Then $\mathcal{F}$ is an $(n',r;q)$-FHS set and for each correlation window length $1\le L\le n'$,

$$\mathcal{M}(\mathcal{F};L)=\left\lceil\frac{L}{q+1}\right\rceil.$$

Moreover, $\mathcal{F}$ is a strictly optimal FHS set with optimal partial Hamming correlation with respect to the bound in (7) and with optimal family size with respect to the bound in (8).

Proof. By Lemma 3.1, we know the alphabet size of $\mathcal{F}$ is p^m, and the map $\mathcal{T}$ is injective, hence

$$s_t^i=s_{t+\tau}^j\iff f(\theta^{i+rt})=f(\theta^{j+rt+r\tau}). \tag{15}$$

Fix i,j,τ such that if $i=j$ then $\tau\not\equiv 0 \bmod n'$. Then $\delta=\theta^{j-i+r\tau}\notin\{0,1\}$. By Lemma 2.4, the set $f_\delta^{-1}(0)$ of solutions of $f(\delta x)-f(x)=0$ is $a\mathbb{F}_q$ for some $a\neq 0$. If there exists an element $\theta^{i+rt_0}\in f_\delta^{-1}(0)$ (otherwise $H_{S^i,S^j}(\tau;l\mid L)=0$), then $\theta^{i+rt_0}\in a\mathbb{F}_q^*$ and

$$s_t^i=s_{t+\tau}^j\iff\theta^{i+rt}\in a\mathbb{F}_q^*\iff\theta^{r(t-t_0)}\in\mathbb{F}_q^*.$$

Any $c\in\mathbb{F}_q^*$ is of the form $c=\theta^{(q+1)s}$, since $(r,q+1)=1$, we have

$$s_t^i=s_{t+\tau}^j\iff t-t_0\in(q+1)\mathbb{Z}.$$

Therefore, we have $H_{S^i,S^j}(\tau;l\mid L)\le\left\lceil\frac{L}{q+1}\right\rceil$ and

$$\mathcal{M}(\mathcal{F};L)\le\left\lceil\frac{L}{q+1}\right\rceil.$$

We now check the strictly optimality of the sequence set $\mathcal{F}$, from (7),

$$\begin{aligned}\mathcal{M}(\mathcal{F};L)&\ge\left\lceil\frac{L}{N}\cdot\frac{[2INM-(I+1)Id']}{(NM-1)M}\right\rceil\\&=\left\lceil\frac{Lr}{q^2-1}\cdot\frac{(q-1)(q^2-2)}{(q^2-2)r}\right\rceil=\left\lceil\frac{L}{q+1}\right\rceil.\end{aligned}$$

Thus $\mathcal{M}(\mathcal{F};L)=\left\lceil\frac{L}{q+1}\right\rceil$.

Taking $L = \frac{q^2-1}{r}$, then $\mathcal{M}(\mathcal{F};L) = \frac{q-1}{r}$ and $d'\mathcal{M}(\mathcal{F};L) < L$. According to the bound in (8), we have

$$M \le \left\lfloor \frac{1}{N} \left\lfloor \frac{(L-\mathcal{M}(\mathcal{F};L))d'}{L-d'\mathcal{M}(\mathcal{F};L)} \right\rfloor \right\rfloor = \left\lfloor \frac{rq^2}{q^2-1} \right\rfloor = r.$$

Actually, the family size of $\mathcal{F}$ is exactly r. □

Remark 4. Compared with the known constructions in [32, 10], our construction in Theorem 3.4 is new and the FHS set is not equivalent to theirs, and it provides us a large number of choices from different $f(x)$.

Example 3.5. *Let $p = q = 7$, $r = 3$, $k = 1$ and $a_0 = 1$. Assume that θ is a primitive element of $\mathbb{F}_{7^2}$ over $\mathbb{F}_7$. Set*

$$f(x) = \mathrm{Tr}_{7^2/7}(x^5).$$

Then, $\mathcal{F}$ consists of the following three FHSs of length 16:

$$S^0 = (2,3,4,1,0,1,3,3,5,4,3,6,0,6,4,4);$$
$$S^1 = (3,0,3,2,2,1,5,2,4,0,4,5,5,6,2,5);$$
$$S^2 = (6,6,3,1,6,5,0,5,1,1,4,6,1,2,0,2).$$

By computer experiments,

$$\mathcal{M}(\mathcal{F};L) = \left\lceil \frac{L}{8} \right\rceil = \begin{cases} 1, & \textit{for } 1 \le L \le 8, \\ 2, & \textit{for } 9 \le L \le 16. \end{cases}$$

Thus, $\mathcal{F}$ is strictly optimal with respect to the bound in (7), and also has an optimal family size with respect to the bound in (8).

4. Second construction of optimal FHS sets

4.1. A generic construction. From now on, let $q = p^m$.

Definition 4.1. For an $(n, M; q)$-FHS set $\mathcal{U} := \{U^i = (u_t^i)_{t=0}^{n-1} : 0 \le i \le M-1\}$ and a function $\phi(x)$ over $\mathbb{F}_q$, for any given triple $(i,j,\tau) \in [0,M-1]^2 \times [0,n-1] - \{(i,i,0)\}$, we say that $(\mathcal{U},\phi)$ satisfies **A1** if

$$\phi(u_{t+\tau}^i) - \phi(u_t^j) = \text{constant } c(i,j,\tau) \in \mathbb{F}_q^* \text{ for all } 0 \le t \le n-1. \tag{16}$$

For a vector $v = (v_0, v_1, \ldots, v_{n'-1}) \in \mathbb{F}_q^{n'}$ and a function $\varphi(x)$ over $\mathbb{F}_q$, we say that (v,φ) satisfies **A2** if for $b \in \mathbb{F}_q$,

$$\max_{1 \le \tau \le n'-1} \#\{t : \varphi(v_{t+\tau}) - \varphi(v_t) = b, 0 \le t \le n'-1\} = 1. \tag{17}$$

Theorem 4.2. *Let $N = nn'$ with $\gcd(n,n') = 1$ and M be positive integers. Suppose $\mathcal{U}$ is an $(n,M;q)$-FHS set such that $(\mathcal{U},\phi)$ satisfies* **A1**. *Suppose $v \in \mathbb{F}_q^{n'}$ such that (v,φ) satisfies* **A2**. *Then the FHS set $\mathcal{F} := \{S^i : 0 \le i \le M-1\}$ with $S^i = (s_t^i)_{t=0}^{N-1}$ defined by*

$$s_t^i = \phi(u_t^i) + \varphi(v_t), \quad 0 \le t \le N-1, \tag{18}$$

is an $(N,M;q)$-FHS set and for each correlation window length $L \in \{1,\cdots,N\}$,

$$\mathcal{M}(\mathcal{F};L) \le \left\lceil \frac{L}{n'} \right\rceil.$$

Proof. For $0 \leq \tau \leq N-1$, $0 \leq i,j \leq M-1$ and $0 \leq l \leq N-1$ such that $\tau \neq 0$ if $i=j$, by Eq. (1) we have

$$\begin{aligned} H_{S^i,S^j}(\tau; l \mid L) &= \sum_{t=l}^{L+l-1} h[s_t^i, s_{t+\tau}^j] \\ &= \sum_{t=l}^{L+l-1} h[\phi(u_t^i)+\varphi(v_t), \phi(u_{t+\tau}^j)+\varphi(v_{t+\tau})] \\ &= \sum_{t=l}^{L+l-1} h[\phi(u_t^i)-\phi(u_{t+\tau}^j), \varphi(v_{t+\tau})-\varphi(v_t)]. \qquad (19) \end{aligned}$$

Note that $u_t^i := u_{\langle t\rangle_n}^i$, $v_t := v_{\langle t\rangle_{n'}}$ and $s_t^i := s_{\langle t\rangle_N}^i$ for $t \in \mathbb{Z}$ by our convention.

The triple (i,j,τ) belongs to two disjoint cases, either $i=j$ and $\langle\tau\rangle_n = 0$ or else. In both cases (the first case is trivial and the second follows from Eq. (16))

$$\phi(u_t^i) - \phi(u_{t+\tau}^j) = b \in \mathbb{F}_q \quad \text{for all} \quad t \in \mathbb{Z},$$

with $b=0$ if and only if $i=j$ and $\langle\tau\rangle_n = 0$. Note that if $i=j$, then $\tau \neq 0$, so one must have $\langle\tau\rangle_{n'} \neq 0$ or $b \neq 0$. Then by (17), one has

$$\sum_{t=l+n'z}^{l+n'z+n'-1} h[s_t^i, s_{t+\tau}^j] = \sum_{t=0}^{n'-1} h[b, \varphi(v_{t+\tau})-\varphi(v_t)] \leq 1 \qquad (20)$$

for any integers z and l. Write the correlation window length L as $L = m_1 n' + m_2$ where $0 \leq m_2 < n'$. From (19) and (20), if $m_2 = 0$, then

$$H_{S^i,S^j}(\tau; l \mid L) = \sum_{t=l}^{l+L-1} h[s_t^i, s_{t+\tau}^j] = \sum_{z=0}^{m_1-1} \sum_{t=l+n'z}^{l+n'z+n'-1} h[s_t^i, s_{t+\tau}^j] \leq m_1,$$

if $m_2 > 0$, then

$$H_{S^i,S^j}(\tau; l \mid L) = \sum_{z=0}^{m_1-1} \sum_{t=l+n'z}^{l+n'z+n'-1} h[s_t^i, s_{t+\tau}^j] + \sum_{t=l+m_1n'}^{l+m_1n'+m_2-1} h[s_t^i, s_{t+\tau}^j] \leq m_1 + 1.$$

In both cases, we have $H_{S^i,S^j}(\tau; l \mid L) \leq \lceil \frac{L}{n'} \rceil$. Hence

$$\mathcal{M}(\mathcal{F}; L) \leq \left\lceil \frac{L}{n'} \right\rceil,$$

which completes the proof of this theorem. □

Remark 5. The special case that $\phi(x) = \varphi(x) = x$, $(\mathcal{U}, \phi)$ and (v, φ) satisfying **A1** and **A2** was used in [3] to construct optimal FHS sets.

4.2. Third class of optimal FHS sets.

Lemma 4.3. *Let $R = \{a_0 = 0, a_1, \cdots, a_{p^{m-1}-1}\}$ be a set of additive coset representatives of $\mathbb{F}_p$ to $\mathbb{F}_q$. Construct p^{m-1} sequences $\mathcal{U} = \{U^i = (u_t^i)_{t=0}^{p-1} : 0 \leq i \leq p^{m-1}-1\}$ by*

$$u_t^i = a_i + t, a_i \in R. \qquad (21)$$

Then $\mathcal{M}(\mathcal{U}; L) = 0$ and $\mathcal{U}$ is an $(p, p^{m-1}, 0; p^m)$-FHS set. In particular, $\mathcal{U}$ is an $(p, 0; p)$-FHS if $m = 1$.

Suppose that $P(x) = x^e + c_{e-1}x^{e-1} + \cdots + c_0 \in \mathbb{F}_q[x]$ *is a polynomial prime to* $x^m - 1$*, and let* $\phi(x) = x^{p^e} + c_{e-1}x^{p^{e-1}} + \cdots + c_0 x : \mathbb{F}_q \to \mathbb{F}_q$*. Then for any* $(i, j, \tau) \in [0, p^{m-1} - 1]^2 \times [0, p-1] - \{(i, i, 0)\}$*, for any* $0 \le t \le p - 1$*,*

$$\phi(u^i_{t+\tau}) - \phi(u^j_t) = \phi(a_i - a_j + \tau) \in \mathbb{F}_q^*.$$

Hence $(\mathcal{U}, \phi)$ *satisfies* **A1***.*

Proof. This is because ϕ is additive and defines a bijection from $\mathbb{F}_q$ to itself, and $a_i - a_j + \tau \neq 0$ if $(i, j, \tau) \neq (i, i, 0)$. □

Lemma 4.4. *Let* α *be a primitive root of* $\mathbb{F}_q$ *and* $v = (\alpha^t)_{t=0}^{q-2}$*. For* $\gcd(d, q-1) = 1$*, set* $\varphi(x) = x^d$*, then* (v, φ) *satisfies* **A2***.*

Proof. For $\gcd(d, q-1) = 1$ and any fixed $1 \le \tau \le q-2$, $\{(\alpha^{d\tau} - 1)\alpha^{dt} : \ 0 \le t \le q-2\} = \mathbb{F}_q^*$, it is clear that

$$\max_{1 \le \tau \le q-2} \#\{t : \varphi(\alpha^{t+\tau}) - \varphi(\alpha^t) = b, 0 \le t \le q-2\} = 1.$$

□

Theorem 4.5. *Let* $(\mathcal{U}, \phi)$ *and* (v, φ) *be given by Lemmas 4.3 and 4.4 respectively. Then the FHS set* $\mathcal{F}$ *constructed from* $(\mathcal{U}, \phi)$ *and* (v, φ) *in Theorem 4.2 is an* $(p(p^m - 1), p^{m-1}; p^m)$*-FHS set such that for any correlation window length* $1 \le L \le p(p^m - 1)$*,*

$$\mathcal{M}(\mathcal{F}; L) = \left\lceil \frac{L}{p^m - 1} \right\rceil.$$

Moreover, $\mathcal{F}$ *is a strictly optimal FHS set with optimal partial Hamming correlation with respect to the bound in* (6) *and with optimal family size with respect to the bound in* (9)*.*

Proof. By Theorem 4.2, we know that $\mathcal{F}$ is an $(p(p^m - 1), p^{m-1}; p^m)$-FHS set and $\mathcal{M}(\mathcal{F}; L) \le \left\lceil \frac{L}{p^m - 1} \right\rceil$. We are left to check the equality and the optimality of the partial Hamming correlation and family size with respect to the bounds in Eqs.(6) and (9).

For $(N, M, d') = (p(p^m - 1), p^{m-1}, p^m)$,

$$\begin{aligned} \left\lceil \frac{(NM - d')N}{(NM - 1)d'} \right\rceil &= \left\lceil \frac{(p(p^m - 1)p^{m-1} - p^m)p(p^m - 1)}{(p(p^m - 1)p^{m-1} - 1)p^m} \right\rceil \\ &= \left\lceil \frac{(p^m - 2)p(p^m - 1)}{p^m(p^m - 1) - 1} \right\rceil = p. \end{aligned}$$

Then Niu et al.'s bound in Eq.(6) is that for any correlation window length $1 \le L \le p(p^m - 1)$, for any M FHS set $\mathcal{F}$ of length N and alphabet size d',

$$\mathcal{M}(\mathcal{F}; L) \ge \left\lceil \frac{L}{N} \left\lceil \frac{(NM - d')N}{(NM - 1)d'} \right\rceil \right\rceil = \left\lceil \frac{L}{p^m - 1} \right\rceil.$$

Hence $\mathcal{M}(\mathcal{F}; L) = \left\lceil \frac{L}{p^m - 1} \right\rceil$ and $\mathcal{F}$ has optimal partial Hamming correlation with respect to the bound in (6).

Take $L = p^m - 1$, then $\mathcal{M}(\mathcal{F}; L) = 1$. The bound (9) gives

$$M \le \left\lfloor \frac{p^{2m}}{p(p^m - 1)} \right\rfloor = \left\lfloor \frac{p^{m-1}p(p^m - 1) + p^m}{p(p^m - 1)} \right\rfloor = p^{m-1}.$$

Note that the actual family size of $\mathcal{F}$ is exactly p^{m-1}, hence $\mathcal{F}$ has an optimal family size with respect to the bound in (9). □

Example 4.6. *Let $p = 3$, $m = 2$, $d = 1$ and α be a primitive element of $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$ satisfying $\alpha^2 + \alpha + 2 = 0$. Take $a_i \in \{1, \alpha, \alpha^2\}$ with $0 \le i \le 2$. Suppose $\mathcal{U} = \{(1, 2, 0); (\alpha, \alpha + 1, \alpha + 2); (\alpha^2, \alpha^2 + 1, \alpha^2 + 2)\}$ and $v = (\alpha^t)_{t=0}^{7}$. Set*

$$\phi(x) = x^3 - \alpha x, \quad \varphi(x) = x.$$

Then the sequence set $\mathcal{F}$ in Theorem 4.5 consists of the following three FHSs of the length 24:

$$S^0 =(\alpha^3, \alpha^3, \alpha^2, \alpha, \alpha^7, \alpha^5, 0, \alpha^5, 1, 1, 0, \alpha^3, \alpha^5, \alpha^4, \alpha^6, \alpha^4, \alpha, \alpha, \alpha^6, 1, 2, \alpha^7, \alpha^2, \alpha^7);$$
$$S^1 =(2, 2, 1, \alpha^5, \alpha^2, 0, \alpha, 0, \alpha^7, \alpha^7, \alpha, 2, 0, \alpha^6, \alpha^3, \alpha^6, \alpha^5, \alpha^5, \alpha^3, \alpha^7, \alpha^6, \alpha^2, 1, \alpha^2);$$
$$S^2 =(\alpha^2, \alpha^2, \alpha^5, \alpha^6, \alpha, \alpha^3, 2, \alpha^3, 0, 0, 2, \alpha^2, \alpha^3, 1, \alpha^7, 1, \alpha^6, \alpha^6, \alpha^7, 0, 1, \alpha, \alpha^5, \alpha).$$

By computer experiments, $\mathcal{M}(\mathcal{F}; L) = \left\lceil \frac{L}{8} \right\rceil$ for any $1 \le L \le 24$. $\mathcal{F}$ is strictly optimal with respect to the bound in (6), and also has an optimal family size with respect to the bound in (9).

Example 4.7. *Let $p = 3$, $m = 3$, $d = 3$ and α be a primitive element of $\mathbb{F}_{3^3}$ over $\mathbb{F}_3$ satisfying $\alpha^3 - \alpha + 1 = 0$. Take $a_i \in \{0, \alpha, 2\alpha\}$ with $0 \le i \le 2$. Suppose $\mathcal{U} = \{(0, 1, 2); (\alpha, \alpha + 1, \alpha + 2); (2\alpha, 2\alpha + 1, 2\alpha + 2)\}$ and $v = (\alpha^t)_{t=0}^{25}$. Set*

$$\phi(x) = x, \quad \varphi(x) = x^3.$$

Then the sequence set $\mathcal{F}$ in Theorem 4.5 consists of the following three FHSs of the length 78:

$$\begin{aligned} S^0 =&(1, \alpha, \alpha^{10}, \alpha^9, \alpha^2, \alpha^8, \alpha^{18}, \alpha^{12}, \alpha^{23}, \alpha, \\ &\alpha^{18}, \alpha^{18}, \alpha^{10}, 0, \alpha^{14}, \alpha^{19}, \alpha^{14}, \alpha^{15}, \alpha^2, \alpha^{17}, \cdots); \\ S^1 =&(\alpha^9, \alpha^{14}, \alpha^4, \alpha^{16}, \alpha^{10}, \alpha^5, \alpha^{21}, \alpha^{11}, \alpha^{15}, \alpha^{14}, \\ &\alpha^{21}, \alpha^{21}, \alpha^4, \alpha, 0, \alpha^8, 0, \alpha^{17}, \alpha^{10}, \alpha^{23}, \cdots); \\ S^2 =&(\alpha^{16}, 0, \alpha^2, 1, \alpha^4, \alpha^{19}, \alpha^6, \alpha^7, \alpha^{17}, 0, \\ &\alpha^6, \alpha^6, \alpha^2, \alpha^{14}, \alpha, \alpha^5, \alpha, \alpha^{23}, \alpha^4, \alpha^{15}, \cdots). \end{aligned}$$

By computer experiments,

$$\mathcal{M}(\mathcal{F}; L) = \left\lceil \frac{L}{26} \right\rceil = \begin{cases} 1, & \textit{for } 1 \le L \le 26, \\ 2, & \textit{for } 27 \le L \le 52, \\ 3, & \textit{for } 53 \le L \le 78. \end{cases}$$

$\mathcal{F}$ is strictly optimal with respect to the bound in (6), and also has an optimal family size with respect to the bound in (9). Moreover, we can check that $\mathcal{F}$ is equivalent to FHS set in [3, Theorem 4].

5. CONCLUSION

In this paper, we construct three classes of strictly optimal FHS sets (given in Theorems 3.2, 3.4 and Theorem 4.5 respectively) with optimal partial Hamming correlation and optimal family size. Our main contribution is as follows: our second construction based on d-from difference-balanced functions (there are many) is new and not equivalent to the known constructions; our third construction is based on a generic approach (Theorem 4.2), which is inspired by and contains the one in [3]. It would be very interesting if one can find new examples satisfying the assumptions in Theorem 4.2 and we leave this as an open problem for future study.

References

[1] J. Bao, New families of strictly frequency hopping sequence sets, *Adv. Math. Commun.*, **12** (2018), 387–413.

[2] J. Bao and L. Ji, Frequency hopping sequences with optimal partial Hamming correlation, *IEEE Trans. Inf. Theory*, **62** (2016), 3768–3783.

[3] H. Cai, Y. Yang, Z. Zhou and X. Tang, Strictly optimal frequency-hopping sequence sets with optimal family sizes, *IEEE Trans. Inf. Theory*, **62** (2016), 1087–1093.

[4] H. Cai, Z. Zhou, Y. Yang and X. Tang, A new construction of frequency-hopping sequences with optimal partial Hamming correlation, *IEEE Trans. Inf. Theory*, **60** (2014), 5782–5790.

[5] B. Chen, L. Lin, S. Ling and H. Liu, Three new classes of optimal frequency-hopping sequence sets, *Des. Codes Cryptogr.*, **83** (2017), 219–232.

[6] W. Chu and C. J. Colbourn, Optimal frequency-hopping sequences via cyclotomy, *IEEE Trans. Inf. Theory*, **51** (2005), 1139–1141.

[7] J.-H. Chung, Y. K. Han and K. Yang, New classes of optimal frequency-hopping sequences by interleaving techniques, *IEEE Trans. Inf. Theory*, **55** (2009), 5783–5791.

[8] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo and M. Mishima, Sets of frequency hopping sequences: Bounds and optimal constructions, *IEEE Trans. Inf. Theory*, **55** (2009), 3297–3304.

[9] C. Ding, M. J. Moisio and J. Yuan, Algebraic constructions of optimal frequency-hopping sequences, *IEEE Trans. Inf. Theory*, **53** (2007), 2606–2610.

[10] Y. C. Eun, S. Y. Jin, Y. P. Hong and H. Y. Song, Frequency hopping sequences with optimal partial autocorrelation properties, *IEEE Trans. Inf. Theory*, **50** (2004), 2438–2442.

[11] C. Fan, H. Cai and X. Tang, A combinatorial construction for strictly optimal frequency-hopping sequences, *IEEE Trans. Inf. Theory*, **62** (2016), 4769–4774.

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

[13] G. Ge, R. Fuji-Hara and Y. Miao, Further combinatorial constructions for optimal frequency-hopping sequences, *J. Combin. Theory Ser. A*, **113** (2006), 1699–1718.

[14] G. Ge, Y. Miao and Z. Yao, Optimal frequency hopping sequences: Auto-and cross-correlation properties, *IEEE Trans. Inf. Theory*, **55** (2009), 867–879.

[15] H. Han, S. Zhang, L. Zhou and X. Liu, Decimated m-sequences families with optimal partial Hamming correlation, *Cryptogr. Commun.*, **12** (2020), 405–413.

[16] T. Helleseth and G. Gong, New nonbinary sequences with ideal two-level autocorrelation, *IEEE Trans. Inf. Theory*, **48** (2002), 2868–2872.

[17] H. Hu and G. Gong, New sets of zero or low correlation zone sequences via interleaving techniques, *IEEE Trans. Inf. Theory*, **56** (2010), 1702–1713.

[18] H. Hu, S. Shao, G. Gong and T. Helleseth, The proof of Lin's conjecture via the decimation-Hadamard transform, *IEEE Trans. Inf. Theory*, **60** (2014), 5054–5064.

[19] A. Lempel and H. Greenberger, Families of sequences with optimal Hamming-correlation properties, *IEEE Trans. Inf. Theory*, **20** (1974), 90–94.

[20] A. Lin, *From Cyclic Hadamard Difference Sets to Perfectly Balanced Sequences*, Ph.D thesis, Dept. Comput. Sci., Univ. in Southern California, Los Angeles, CA, USA, 1998.

[21] X. Liu, L. Zhou and S. Li, A new method to construct strictly optimal frequency hopping sequences with new parameters, *IEEE Trans. Inf. Theory*, **65** (2019), 1828–1844.

[22] S. L. Ng and M. B. Paterson, Disjoint difference families and their applications, *Des. Codes Cryptogr.*, **78** (2016), 103–127.

[23] X. Niu, D. Peng, F. Liu and X. Liu, Lower bounds on the maximum partial correlations of frequency hopping sequence set with low hit zone, *IEICE Trans. Fund.*, **E93-A** (2010), 2227–2231.

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

[25] A. Pott and Q. Wang, Some results on difference balanced functions, In *Arithmetic of Finite Fields, LNCS, Springer*, **9061** (2015), 111–120.

[26] M. K. Simon, J. K. Omura, R. A. Scholtz and B. K. Levitt, *Spread Spectrum Communication Handbook*, McGraw-Hill, New York, 2001.

[27] G. Solomn, Optimal frequency hopping sequences for multiple access, In *Pro. Symp. Spread Spectr. Commun.*, (1973), 33–35.

[28] H. Y. Song and S. W. Golomb, On the nonperiodic cyclic equivalence classes of Reed-Solomon codes, *IEEE Trans. Inf. Theory*, **39** (1993), 1431–1434.

[29] S. Xu, X. Cao, J. Gao and C. Tang, A kind of disjoint cyclic perfect Mendelsohn difference family and its applications in strictly optimal FHSs, *IEICE Trans. Fund.*, **E101-A** (2018), 2338–2343.

[30] X. Zeng, H. Cai, X. Tang and Y. Yang, A class of optimal frequency hopping sequences with new parameters, *IEEE Trans. Inf. Theory*, **58** (2012), 4899–4907.

[31] L. Zhou, D. Peng, H. Han and H. Liang, Construction of optimal low-hit-zone frequency hopping sequence sets under periodic partial Hamming correlation, *Adv. Math. Commun.*, **12** (2018), 67–79.

[32] Z. Zhou, X. Tang, X. Niu and U. Parampalli, New classes of frequency hopping sequences with optimal partial correlation, *IEEE Trans. Inf. Theory*, **58** (2012), 453–458.

[33] Z. Zhou, X. Tang, D. Peng and U. Parampalli, New constructions for optimal sets of frequency-hopping sequences, *IEEE Trans. Inf. Theory*, **57** (2011), 3831–3840.

Received October 2021; revised January 2022; early access April 2022.

E-mail address: xianhxie@mail.ustc.edu.cn
E-mail address: yiouyang@ustc.edu.cn
E-mail address: hghu2005@ustc.edu.cn
E-mail address: maomingDKY@163.com