IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 15, 2022, accepted January 24, 2022, date of publication February 11, 2022, date of current version February 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3151085

New Constructions for Near-Optimal Sets of Frequency-Hopping Sequences via the Gaussian Periods in Finite Fields

SHANDING XU[1,2] AND JIAFU MI[3]

[1]College of Liberal Arts and Science, National University of Defense Technology, Changsha 410073, China
[2]Department of Mathematics and Physics, Nanjing Institute of Technology, Nanjing 211167, China
[3]School of Mathematics and Statistic, Shandong University of Technology, Zibo 255000, China

Corresponding author: Shanding Xu (sdxzx11@njit.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 11771007, and in part by the Funding of Nanjing Institute of Technology under Grant ZKJ201909.

ABSTRACT Frequency-hopping sequences (FHSs) have been widely applied in frequency-hopping code-division multiple-access (FH-CDMA) systems, since they can be used for transmitting messages efficiently along with switching frequencies at set intervals by each sender. The performance of the FHSs has a great impact on the performance of FH-CDMA systems. The optimality achieving exactly the Peng-Fan bounds is an important performance measure. However, optimal sets of FHSs do not always exist for all lengths and alphabet sizes. Thus, it is meaningful to seek and design more near-optimal FHS sets whose parameters are near to achieving the Peng-Fan bounds. Let q be a power of a prime. In this paper, we present some classes of near-optimal sets of FHSs, whose parameters are $(\frac{3(q+1)}{2}, \frac{2(q-1)}{3}, 3; q)$ with $q \equiv 1 \pmod{12}$, $(\frac{q+1}{k}, k(q-1), 2; q)$ with even $\frac{q+1}{k}$, $(2(q^2+1), \frac{q^2-1}{2}, 2(q+1); q)$ with $q \equiv 3 \pmod 4$, $(19, 18, 4; 7)$, $(7, 9, 3; 4)$ and $(91, 45, 7; 16)$ respectively. Most importantly, these classes of near-optimal sets of FHSs have new parameters which are not covered in the foregoing literature.

INDEX TERMS Frequency-hopping sequence, Peng-Fan bound, cyclotomic class, Gaussian period, finite fields.

I. INTRODUCTION

Frequency-hopping multiple access (FHMA) spread systems play an important role in military radio communications, mobile communications, modern radar and sonar echolocation systems [1], [2]. In these systems, each user is represented by a sequence of hopping frequencies, which is called a frequency-hopping sequence (FHS). In general, we need to minimise the maximum of Hamming out-of-phase autocorrelation and Hamming crosscorrelation of the FHS sets, whose purpose is to discriminate their own signals from the others and reduce multiple access collisions by simultaneous transmission. To accommodate a great quantity of users, it is also preferred that the size of the FHS sets is as large as possible. All in all, it is imperative to find FHSs with long length, small available frequencies, large size of FHS set and low Hamming correlation simultaneously. As an inseparable whole, these parameters of the FHS sets are closely connected with each other. As a matter of fact, they are subjected to some theoretic bounds, for example, the Lempel-Greenberger bound [3] and the Peng-Fan bounds [4]. These bounds become standards of evaluating the performance of the FHSs.

Because of the specification of a given system or environment, the required length and alphabet size of an FHS set vary in practical applications. Hence it is very important to choose some FHS sets with (near-)optimal Hamming correlation under the given constraint condition. Generally speaking, (near-)optimality of an FHS set is measured by the Peng-Fan bounds. More specifically, we call an FHS set to be optimal if its maximum periodic Hamming correlation achieves exactly the Peng-Fan bounds, and we call an FHS set to be near-optimal if its maximum periodic Hamming correlation is bigger than the Peng-Fan bounds by one.

So far, both algebraic and combinatorial constructions of optimal sets of FHSs with respect to the Peng-Fan bound were provided (see, for example, [3], [5]–[23]). Generally speaking, optimal sets of FHSs do not always exist for all lengths and alphabet sizes. However, it is a difficult problem

The associate editor coordinating the review of this manuscript and approving it for publication was Khmaies Ouahada.

to verify whether an optimal FHS set exists for a given length and a given alphabet size. Hence it is also valuable to construct more near-optimal sets of FHSs. In 2011, Chung and Yang [24] introduced a class of near-optimal sets of FHSs via using k-fold cyclotomy. In 2012, Chung and Yang [16] presented a class of near-optimal sets of FHSs by using non-linear functions over $\mathbb{Z}_p$, where p is an odd prime. In 2013, Chung and Yang [25] got a near-optimal set of FHSs by applying the new class of balanced near-perfect nonlinear mappings. Except these constructions, Xu *et al.* [6], [21], [26] obtained some new classes of near-optimal sets of FHSs by means of interleaving technology and generalized cyclotomy.

Our purpose in this paper is to design more near-optimal sets of FHSs for some cases which are not covered in the literature. By means of the trace function and known Gaussian periods in finite fields, some classes of near-optimal sets of FHSs are presented, see Theorems 7, 9 and 11. In Table 2, we summarize some known near-optimal sets of FHSs, including the parameters obtained from this paper.

The rest of this paper is organized as follows. In Section II, we give some preliminaries to frequency-hopping sequence, the cyclotomic classes and Gaussian periods in finite fields. In Section III, we propose some constructions of near-optimal sets of FHSs. Finally, Section IV concludes this paper.

II. PRELIMINARIES

For the constructions of near-optimal sets of FHSs in the sequel, we need to recall the notions of frequency-hopping sequence, the cyclotomic classes and Gaussian periods in finite fields.

A. FREQUENCY-HOPPING SEQUENCE

Let $\mathcal{F} = \{f_0, f_1, \ldots, f_{l-1}\}$ be an alphabet of l available frequencies which are shared by numerous senders. A sequence $X = \{x_t\}_{t=0}^{n-1}$ is called a frequency-hopping sequence (FHS) of length n over $\mathcal{F}$ if $x_t \in \mathcal{F}$ for all $0 \le t \le n-1$. Given any two FHSs $X = \{x_t\}_{t=0}^{n-1}$ and $Y = \{y_t\}_{t=0}^{n-1}$ of length n over $\mathcal{F}$, their periodic Hamming correlation $H_{X,Y}$ at time delay τ is defined by

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

where $h[a, b] = 1$ if $a = b$ and 0 otherwise, and $t + \tau$ is performed modulo n.

The maximum periodic Hamming out-of-phase autocorrelation $H(X)$ of X and the maximum periodic Hamming crosscorrelation $H(X, Y)$ for two different FHSs X and Y are defined as

$$H(X) = \max_{1 \le \tau \le n-1} \{H_{X,X}(\tau)\};$$
$$H(X, Y) = \max_{0 \le \tau \le n-1} \{H_{X,Y}(\tau)\}.$$

Let $\mathcal{S}$ be a set of M FHSs of length n over an alphabet $\mathcal{F}$. The maximum periodic Hamming correlation of $\mathcal{S}$ is defined by

$$H(\mathcal{S}) = \max\{\max_{X \in \mathcal{S}}\{H(X)\}, \max_{\substack{X, Y \in \mathcal{S} \\ X \ne Y}} \{H(X, Y)\}\}.$$

Henceforth, we use $(n, M, \lambda; l)$ to denote a set $\mathcal{S}$ containing M FHSs of length n over an alphabet of size l with $H(\mathcal{S}) = \lambda$. In this case, we also say that a set $\mathcal{S}$ of FHSs has parameters $(n, M, \lambda; l)$.

In 2004, Peng and Fan established the following bounds on $H(\mathcal{S})$.

Lemma 1 ([4] The Peng-Fan Bounds): Let $\mathcal{S}$ be a set of M FHSs of length n over an alphabet of size l. Define $I = \lfloor \frac{nM}{l} \rfloor$. Then

$$H(\mathcal{S}) \ge \left\lceil \frac{(nM - l)n}{(nM - 1)l} \right\rceil \tag{1}$$

and

$$H(\mathcal{S}) \ge \left\lceil \frac{2InM - (I+1)Il}{(nM - 1)M} \right\rceil, \tag{2}$$

where $\lfloor z \rfloor$ denotes the largest integer less than or equal to z, and $\lceil z \rceil$ denotes the smallest integer not less than z.

In 2017, Chen *et al.* [5] proved that the two Peng-Fan bounds given above are actually identical. Furthermore, Xu *et al.* [6] in 2016 gave a simplified form of the Peng-Fan bounds as follows.

Lemma 2 ([5], [6]): Let $\mathcal{S}$ be a set of M FHSs of length n over an alphabet of size l and $a = \lfloor \frac{n}{l} \rfloor$. Then

$$\left\lceil \frac{(nM - l)n}{(nM - 1)l} \right\rceil = \left\lceil \frac{2InM - (I+1)Il}{(nM - 1)M} \right\rceil \in \{0, a, a+1\}.$$

An FHS set $\mathcal{S}$ is called optimal with respect to the Peng-Fan bound if the parameters of $\mathcal{S}$ meet the equality in (1) or (2), and an FHS set $\mathcal{S}$ is called near-optimal with respect to the Peng-Fan bound if $H(\mathcal{S})$ is bigger than the right-hand side of (1) or (2) by one.

B. CYCLOTOMIC CLASSES AND GAUSSION PERIODS

Throughout this paper, let p be a prime and $q = p^s$ for a positive integer s. Denote by $\mathbb{F}_q$ (or $\mathbb{F}_r$) the finite field with q (or r) elements, where $r = q^m$ and m is a positive integer. Let $\mathbb{F}_r^*$ be the multiplicative group consisting of all nonzero elements in $\mathbb{F}_r$ and θ be a fixed primitive element of $\mathbb{F}_r$ such that $\mathbb{F}_r^* = \langle\theta\rangle$. Let $\mathrm{Tr}_{r/q}$ denote the trace function from $\mathbb{F}_r$ to $\mathbb{F}_q$ defined by

$$\mathrm{Tr}_{r/q}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}, \quad x \in \mathbb{F}_r.$$

Let $r = nN + 1$ for two positive integers n, $N \ge 2$. The cyclotomic classes of order N in $\mathbb{F}_r$ are defined by

$$D_i^{(N,r)} = \theta^i \langle \theta^N \rangle = \{\theta^{i+tN} : 0 \le t < n\}, \quad 0 \le i < N.$$

In the remainder parts of this section, we shall introduce basic results on Gaussian periods. For more details, the reader is advised to refer to the paper [27] and the book [28].

Let $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ be the primitive p-th root of unity. The canonical additive character of $\mathbb{F}_r$ can be defined by

$$\begin{aligned}\chi : \mathbb{F}_r &\to \mathbb{C}^* \\ x &\mapsto \zeta_p^{\mathrm{Tr}_{r/p}(x)}\end{aligned}$$

where $\mathrm{Tr}_{r/p}$ denotes the absolute trace function from $\mathbb{F}_r$ to $\mathbb{F}_p$. According to the orthogonal property of additive characters, we have

$$\sum_{x\in\mathbb{F}_r}\chi(ax) = \begin{cases} r, & \text{if } a = 0 \\ 0, & \text{if } a \in \mathbb{F}_r^*. \end{cases}$$

Definition 3: Let χ be the canonical additive character of $\mathbb{F}_r$ and $D_i^{(N,r)}$ $(0 \le i < N)$ be the cyclotomic classes of order N in $\mathbb{F}_r$. The Gaussian periods of order N in $\mathbb{F}_r$ are defined by

$$\eta_i^{(N,r)} = \sum_{x\in D_i^{(N,r)}}\chi(x), \quad 0 \le i < N.$$

In general, it is very hard to calculate the values of Gaussian periods. However, they can be computed for several particular cases. In this paper, the following lemmas are important for determining the periodic Hamming correlation distributions of an FHS set in Section III.

Lemma 4: Let $r = q^m$, $q = p^s$ and $N = 2$. The Gaussian periods of order 2 in $\mathbb{F}_r$ are given by

$$\eta_0^{(2,r)} = \begin{cases} \dfrac{-1+(-1)^{ms-1}\sqrt{r}}{2}, & \text{if } p \equiv 1 \pmod 4 \\ \dfrac{-1+(-1)^{ms-1}(\sqrt{-1})^{ms}\sqrt{r}}{2}, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

and

$$\eta_1^{(2,r)} = -1 - \eta_0^{(2,r)}.$$

To present further known results about Gaussian periods in $\mathbb{F}_r$, we need to introduce the period polynomial $\Psi_{(N,r)}(X)$ defined as

$$\Psi_{(N,r)}(X) = \prod_{i=0}^{N-1}(X - \eta_i^{(N,r)}).$$

Lemma 5: Let $r = q^m$, $q = p^s$ and $N = 3$. If $p \equiv 1 \pmod 3$ and $ms \equiv 0 \pmod 3$, then the factorization of $\Psi_{(3,r)}(X)$ is given by

$$\begin{aligned}\Psi_{(3,r)}(X) = 3^{-3}(3X + 1 - cr^{\frac{1}{3}})(3X + 1 + \frac{1}{2}(c + 9d) \\ r^{\frac{1}{3}})(3X + 1 + \frac{1}{2}(c - 9d)\, r^{\frac{1}{3}}),\end{aligned}$$

where c and d are defined by $4p^{\frac{ms}{3}} = c^2 + 27d^2$, $c \equiv 1 \pmod 3$ and $\gcd(c, p) = 1$. These restrictions determine c uniquely, and d up to sign.

Lemma 6 (The Semiprimitive Case): Let p be a prime and N be a positive integer. Suppose that there exists a positive integer f such that $p^f \equiv -1 \pmod N$, where f is the least such positive integer. Write $r = p^{2f\gamma}$ for a positive integer γ. Then the Gaussian periods of order N in $\mathbb{F}_r$ are given below:
(1) If γ, p and $\frac{p^f+1}{N}$ are all odd, then

$$\eta_i^{(N,r)} = \begin{cases} \sqrt{r} - \dfrac{\sqrt{r}+1}{N}, & \text{if } i = \dfrac{N}{2} \\ -\dfrac{\sqrt{r}+1}{N}, & \text{otherwise}. \end{cases}$$

(2) In all the other cases,

$$\eta_i^{(N,r)} = \begin{cases} \dfrac{(-1)^{\gamma+1}(N-1)\sqrt{r}-1}{N}, & \text{if } i = 0 \\ \dfrac{(-1)^{\gamma}\sqrt{r}-1}{N}, & \text{otherwise}. \end{cases}$$

III. SOME CONSTRUCTIONS OF NEAR-OPTIMAL SETS OF FHSS

Let $r = q^m = nN + 1$ and θ be defined as Section II. The set $\mathcal{S} = \{s^{(0)}, s^{(1)}, \cdots, s^{(N-1)}\}$ of N FHSs of length n over $\mathbb{F}_q$ is defined by

$$s^{(i)} = (s_0^{(i)}, s_1^{(i)}, \cdots, s_{n-1}^{(i)}), \quad 0 \le i \le N-1$$

where

$$s_t^{(i)} = \mathrm{Tr}_{r/q}(\theta^{i+tN}), \quad 0 \le t \le n-1. \tag{3}$$

Up to now, the parameters of the set $\mathcal{S}$ of FHSs being optimal with respect to the Peng-Fan bound are listed in Table 1, where q is a power of a prime p. Our aim in this section is to present new constructions for such set being near-optimal with respect to the Peng-Fan bound. Specifically, these parameters with near-optimal Hamming correlation property are different from those parameters in [10, Theorem 4.8], [20, Theorem 2] and [23, Theorem 1], because $\gcd(N, \frac{q^m-1}{q-1}) \ne 1$ and $N \nmid (q-1)$. Furthermore, we also use the interleaving techniques in [13] to construct new near-optimal sets of FHSs with longer length and flexible maximum periodic Hamming correlation from old ones.

TABLE 1. Some relevant optimal sets of FHSs with parameters $(n, M, \lambda; I)$.

Parameters	Constraints	Ref.
$(\frac{q^m-1}{2}, 2, \frac{q^{m-1}-1}{2}; q)$	$2 \nmid q, m \ge 3$ is odd.	[8]
$(\frac{q^m-1}{q-1}, q-1, \frac{q^{m-1}-1}{q-1}; q)$	$\gcd(q-1, m) = 1$	[9]
$(\frac{q^m-1}{e}, e, \frac{q^{m-1}-1}{e}; q)$	$e\|(q-1), \gcd(e, m) = 1.$	[10]
$(q^2+1, q^2-1, q+1; q)$	$q = 2^s$ with $s \ge 1$	[11]
$(\frac{q+1}{2}, 2(q-1), 1; q)$	$q \equiv 1 \pmod 4$	[11]

A. THE FIRST CLASS OF NEAR-OPTIMAL SETS OF FHSS

In this subsection, let q be a power of an odd prime p and $r = q^2$. The set $\mathcal{A} = \{a^{(0)}, a^{(1)}, \cdots, a^{(\frac{2q-5}{3})}\}$ of $\frac{2(q-1)}{3}$ FHSs of length $\frac{3(q+1)}{2}$ over $\mathbb{F}_q$ is defined by

$$a^{(i)} = (a_0^{(i)}, a_1^{(i)}, \cdots, a_{\frac{3q+1}{2}}^{(i)}), \quad 0 \le i \le \frac{2q-5}{3}$$

where

$$a_t^{(i)} = \mathrm{Tr}_{r/q}(\theta^{i+\frac{2t(q-1)}{3}}), \quad 0 \le t \le \frac{3q+1}{2}. \tag{4}$$

Theorem 7: The set $\mathcal{A}$ of FHSs has the parameters $(\frac{3(q+1)}{2}, \frac{2(q-1)}{3}, 3; q)$ and is near-optimal with respect to the Peng-Fan bound, where q is a power of an odd prime with $q \equiv 1 \pmod{12}$.

Proof: Firstly, we have

$$\gcd(\frac{2(q-1)}{3}, q+1) = \frac{1}{3}\gcd(2(q-1), 3(q+1)) = 2$$

since $q \equiv 1 \pmod{12}$.

Secondly, for any two FHSs $a^{(i_1)}, a^{(i_2)} \in \mathcal{A}$ with $0 \le i_1, i_2 \le \frac{2q-5}{3}$, their periodic Hamming correlation at time delay τ is given as

$$\begin{aligned}
&H_{a^{(i_1)},a^{(i_2)}}(\tau) \\
&= |\{0 \le t \le \frac{3q+1}{2} : \\
&\qquad \mathrm{Tr}_{r/q}(\theta^{i_1+\frac{2t(q-1)}{3}}) = \mathrm{Tr}_{r/q}(\theta^{i_2+\frac{2(t+\tau)(q-1)}{3}})\}| \\
&= \frac{1}{q}\sum_{t=0}^{\frac{3q+1}{2}}\sum_{x\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{q/p}[x\cdot\mathrm{Tr}_{r/q}(\theta^{\frac{2t(q-1)}{3}}(\theta^{i_1}-\theta^{i_2+\frac{2\tau(q-1)}{3}}))]} \\
&= \frac{3(q+1)}{2q} + \frac{1}{q}\sum_{i=0}^{q-2}\sum_{t=0}^{\frac{3q+1}{2}} \\
&\qquad \zeta_p^{\mathrm{Tr}_{q/p}[\mathrm{Tr}_{r/q}(\theta^{\frac{2t(q-1)}{3}+i(q+1)}(\theta^{i_1}-\theta^{i_2+\frac{2\tau(q-1)}{3}}))]} \\
&= \frac{3(q+1)}{2q} + \frac{3}{q}\sum_{x\in D_0^{(2,q^2)}} \chi((\theta^{i_1}-\theta^{i_2+\frac{2\tau(q-1)}{3}})x) \\
&= \frac{3(q+1)}{2q} + \frac{3}{q}\sum_{x\in D_j^{(2,q^2)}} \chi(x) \\
&\qquad (\text{where } (\theta^{i_1}-\theta^{i_2+\frac{2\tau(q-1)}{3}}) \in D_j^{(2,q^2)},\ j=0,1) \\
&= \frac{3(q+1)}{2q} + \frac{3}{q}\eta_j^{(2,q^2)}, \qquad (5)
\end{aligned}$$

where (5) holds since $\frac{2t(q-1)}{3} + i(q+1)$ takes on each element of $2\mathbb{Z}_{\frac{q^2-1}{2}}$ exactly 3 times for $\gcd(\frac{2(q-1)}{3}, q+1) = 2$, when t and i range over $\mathbb{Z}_{\frac{3(q+1)}{2}}$ and $\mathbb{Z}_{q-1}$ respectively. Hence, we have

$$\eta_j^{(2,q^2)} \in \{\frac{q-1}{2}, -\frac{q+1}{2}\}, \quad j = 0, 1$$

by Lemma 4 and

$$H(\mathcal{A}) = \frac{3(q+1)}{2q} + \frac{3}{q}\frac{q-1}{2} = 3.$$

Furthermore,

$$\left\lceil \frac{(nM-l)n}{(nM-1)l} \right\rceil = \left\lceil \frac{(q^2-q-1)\frac{3(q+1)}{2}}{(q^2-2)q} \right\rceil$$

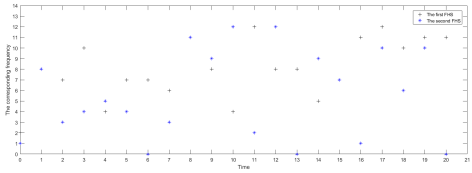

FIGURE 1. The time-frequency representation of an FHS set $\mathcal{A}$.

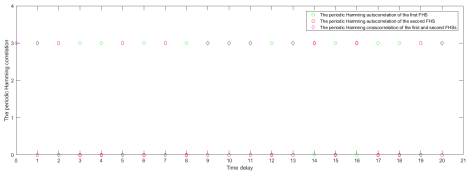

FIGURE 2. The periodic Hamming correlation of an FHS set $\mathcal{A}$.

$$= \left\lceil 2 - \frac{1}{2}(1 + \frac{3}{q^3-2q}) \right\rceil = 2.$$

Then we have

$$H(\mathcal{A}) = 3 = \left\lceil \frac{(nM-l)n}{(nM-1)l} \right\rceil + 1.$$

Therefore, $\mathcal{A}$ is near-optimal with respect to the Peng-Fan bound according to Lemma 1. □

Example 8: Let $q = p = 13$ and $r = q^2$. Let θ be the primitive element of $\mathbb{F}_r$ with $\theta^2 - \theta + 2 = 0$. Then the set $\mathcal{A} = \{a^{(0)}, a^{(1)}, \cdots, a^{(7)}\}$ defined by (4) consists of the following FHSs of length 21:

$$\begin{aligned}
a^{(0)} &= (2, 8, 7, 10, 4, 7, 7, 6, 11, 8, 4, 12, 8, 8, 5, 7, 11, 12, \\
&\quad 10, 11, 11), \\
a^{(1)} &= (1, 8, 3, 4, 5, 4, 0, 3, 11, 9, 12, 2, 12, 0, 9, 7, 1, 10, \\
&\quad 6, 10, 0), \\
a^{(2)} &= (10, 5, 2, 10, 10, 3, 12, 4, 2, 6, 4, 4, 9, 10, 12, 6, 5, \\
&\quad 12, 12, 1, 4), \\
a^{(3)} &= (8, 2, 9, 2, 0, 8, 12, 11, 6, 1, 6, 0, 11, 10, 7, 5, 3, 5, \\
&\quad 0, 7, 4), \\
a^{(4)} &= (1, 5, 5, 8, 6, 2, 1, 3, 2, 2, 11, 5, 6, 3, 9, 6, 6, 7, 2, \\
&\quad 5, 9), \\
a^{(5)} &= (11, 1, 0, 4, 6, 12, 3, 7, 3, 0, 12, 5, 10, 9, 8, 9, 0, 10, \\
&\quad 2, 4, 1), \\
a^{(6)} &= (9, 4, 3, 1, 7, 8, 1, 1, 12, 9, 3, 8, 11, 3, 3, 10, 1, 9, 11, \\
&\quad 7, 9), \\
a^{(7)} &= (0, 2, 3, 6, 8, 10, 8, 0, 6, 9, 5, 11, 4, 11, 0, 5, 1, 2, 7, \\
&\quad 12, 7).
\end{aligned}$$

By Matlab software, there are simulation results to validate Theorem 7 in Figures 1 and 2 as follows:

B. THE SECOND CLASS OF NEAR-OPTIMAL SETS OF FHSS

In this subsection, let p be an odd prime, $q = p^s$ with an odd integer s and $r = q^2$. Let k be a positive integer

satisfying that $p \equiv -1 \pmod{2k}$ and $\frac{q+1}{k}$ is even. The set $\mathcal{B} = \{b^{(0)}, b^{(1)}, \cdots, b^{(k(q-1)-1)}\}$ of $k(q-1)$ FHSs of length $\frac{q+1}{k}$ over $\mathbb{F}_q$ is defined by

$$b^{(i)} = (b_0^{(i)}, b_1^{(i)}, \cdots, b_{\frac{q+1}{k}-1}^{(i)}), \quad 0 \le i \le k(q-1)-1$$

where

$$b_t^{(i)} = \mathrm{Tr}_{r/q}(\theta^{i+kt(q-1)}), \quad 0 \le t \le \frac{q+1}{k} - 1. \tag{6}$$

Theorem 9: The set $\mathcal{B}$ of FHSs has the parameters $(\frac{q+1}{k}, k(q-1), 2; q)$ and is near-optimal with respect to the Peng-Fan bound, where $q = p^s$ with an odd integer s, $p \equiv -1 \pmod{2k}$ and $\frac{q+1}{k}$ is even.

Proof: Firstly, we have

$$\gcd(k(q-1), q+1) = k \cdot \gcd(q-1, \frac{q+1}{k}) = 2k$$

since $\frac{q+1}{k}$ is even.

Secondly, for any two FHSs $b^{(i_1)}, b^{(i_2)} \in \mathcal{B}$ with $0 \le i_1, i_2 < k(q-1)$, their periodic Hamming correlation at time delay τ is given as

$$\begin{aligned}
&H_{b^{(i_1)},b^{(i_2)}}(\tau) \\
&= |\{0 \le t < \frac{q+1}{k} : \\
&\qquad \mathrm{Tr}_{r/q}(\theta^{i_1+kt(q-1)}) = \mathrm{Tr}_{r/q}(\theta^{i_2+k(t+\tau)(q-1)})\}| \\
&= \frac{q+1}{kq} + \frac{1}{q}\sum_{i=0}^{q-2}\sum_{t=0}^{\frac{q+1}{k}-1} \\
&\qquad \zeta_p^{\mathrm{Tr}_{q/p}\left[\mathrm{Tr}_{r/q}(\theta^{kt(q-1)+i(q+1)}(\theta^{i_1}-\theta^{i_2+k\tau(q-1)}))\right]} \\
&= \frac{q+1}{kq} + \frac{2}{q}\sum_{x \in D_0^{(2k,q^2)}} \chi((\theta^{i_1} - \theta^{i_2+k\tau(q-1)})x) \\
&= \frac{q+1}{kq} + \frac{2}{q}\sum_{x \in D_j^{(2k,q^2)}} \chi(x) \\
&\qquad (\text{where } (\theta^{i_1} - \theta^{i_2+k\tau(q-1)}) \in D_j^{(2k,q^2)}, 0 \le j < 2k) \\
&= \frac{q+1}{kq} + \frac{2}{q}\eta_j^{(2k,q^2)},
\end{aligned} \tag{7}$$

where (7) holds since $kt(q-1) + i(q+1)$ takes on each element of $2k \cdot \mathbb{Z}_{\frac{q^2-1}{2k}}$ exactly 2 times for $\gcd(k(q-1), q+1) = 2k$, when t and i range over $\mathbb{Z}_{\frac{q+1}{k}}$ and $\mathbb{Z}_{q-1}$ respectively. For Lemma 6, p is an odd prime, $f = 1$ and $\gamma = s$. Hence, we have

$$\max_{0 \le j < 2k}\{\eta_j^{(2k,q^2)}\} = \frac{(2k-1)q-1}{2k}$$

by Lemma 6 and

$$H(\mathcal{B}) = \frac{q+1}{kq} + \frac{2}{q}\frac{(2k-1)q-1}{2k} = 2.$$

Furthermore,

$$\left\lceil \frac{(nM-l)n}{(nM-1)l} \right\rceil = \left\lceil \frac{(q^2-q-1)\frac{q+1}{k}}{(q^2-2)q} \right\rceil$$

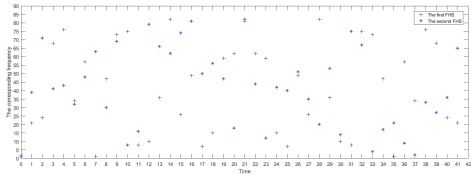

FIGURE 3. The time-frequency representation of an FHS set $\mathcal{B}$.

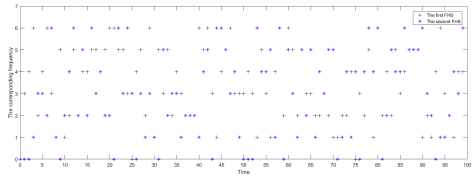

FIGURE 4. The periodic Hamming correlation of an FHS set $\mathcal{B}$.

$$= \left\lceil \frac{1}{k}(1 - \frac{1}{q^3-2q}) \right\rceil = 1.$$

Then we have

$$H(\mathcal{B}) = 2 = \left\lceil \frac{(nM-l)n}{(nM-1)l} \right\rceil + 1.$$

Therefore, $\mathcal{B}$ is near-optimal with respect to the Peng-Fan bound according to Lemma 1. □

Example 10: Let $q = p = 83$, $k = 2$ and $r = q^2$. Let θ be the primitive element of $\mathbb{F}_r$ with $\theta^2 - \theta + 2 = 0$. Then the set $\mathcal{B} = \{b^{(0)}, b^{(1)}, \cdots, b^{(163)}\}$ defined by (6) consists of the following FHSs of length 42:

$$\begin{aligned}
b^{(0)} &= (2, 21, 24, 68, 76, 34, 57, 1, 47, 73, 75, 8, 10, 36, \\
&\quad 82, 26, 49, 7, 15, 59, 62, 81, 62, 59, 15, 7, 49, 26, \\
&\quad 82, 36, 10, 8, 75, 73, 47, 1, 57, 34, 76, 68, 24, 21), \\
b^{(1)} &= (1, 39, 71, 41, 43, 32, 48, 63, 30, 69, 8, 16, 79, 66, \\
&\quad 62, 74, 81, 50, 56, 47, 18, 82, 44, 12, 42, 40, 51, 35, \\
&\quad 20, 53, 14, 75, 67, 4, 17, 21, 9, 2, 33, 27, 36, 65), \\
&\vdots \\
b^{(163)} &= (74, 18, 55, 58, 1, 46, 52, 50, 2, 75, 79, 7, 68, 10, \\
&\quad 59, 67, 20, 21, 6, 22, 41, 9, 65, 28, 25, 82, 37, 31, \\
&\quad 33, 81, 8, 4, 76, 15, 73, 24, 16, 63, 62, 77, 61, 42).
\end{aligned}$$

By Matlab software, there are simulation results to validate Theorem 9 in Figures 3 and 4 as follows:

C. THE THIRD CLASS OF NEAR-OPTIMAL SETS OF FHSS

In this subsection, let $q = p^s$ and $r = q^4$, where p is an odd prime with $p \equiv 3 \pmod 4$ and s is an odd integer. The set $\mathcal{C} = \{c^{(0)}, c^{(1)}, \cdots, c^{(\frac{q^2-3}{2})}\}$ of $\frac{q^2-1}{2}$ FHSs of length $2(q^2+1)$ over $\mathbb{F}_q$ is defined by

$$c^{(i)} = (c_0^{(i)}, c_1^{(i)}, \cdots, c_{2q^2+1}^{(i)}), \quad 0 \le i \le \frac{q^2-3}{2}$$

where

$$c_t^{(i)} = \mathrm{Tr}_{r/q}(\theta^{i+\frac{t(q^2-1)}{2}}), \quad 0 \le t \le 2q^2+1. \tag{8}$$

Theorem 11: The set $\mathcal{C}$ of FHSs has the parameters $(2(q^2+1), \frac{q^2-1}{2}, 2(q+1); q)$ and is near-optimal with respect to the Peng-Fan bound, where q is a power of an odd prime with $q \equiv 3 \pmod 4$.

Proof: Firstly, we have

$$\gcd(\frac{q^2-1}{2}, \frac{r-1}{q-1}) = \frac{q+1}{2} \cdot \gcd(2(q^2+1), q-1) = q+1$$

since $q \equiv 3 \pmod 4$.

Secondly, for any two FHSs $c^{(i_1)}, c^{(i_2)} \in \mathcal{C}$ with $0 \le i_1, i_2 \le \frac{q^2-3}{2}$, their periodic Hamming correlation at time delay τ is given as

$$\begin{aligned}
&H_{c^{(i_1)},c^{(i_2)}}(\tau) \\
&= |\{0 \le t \le 2q^2+1 : \\
&\qquad \mathrm{Tr}_{r/q}(\theta^{i_1+\frac{t(q^2-1)}{2}}) = \mathrm{Tr}_{r/q}(\theta^{i_2+\frac{(t+\tau)(q^2-1)}{2}})\}| \\
&= \frac{2(q^2+1)}{q} + \frac{1}{q}\sum_{i=0}^{q-2}\sum_{t=0}^{2q^2+1} \\
&\qquad \zeta_p^{\mathrm{Tr}_{q/p}[\mathrm{Tr}_{r/q}(\theta^{\frac{t(q^2-1)}{2}+i\frac{r-1}{q-1}}(\theta^{i_1}-\theta^{i_2+\frac{\tau(q^2-1)}{2}}))]} \\
&= \frac{2(q^2+1)}{q} + \frac{2}{q}\sum_{x \in D_0^{(q+1,q^4)}} \chi((\theta^{i_1}-\theta^{i_2+\frac{\tau(q^2-1)}{2}})x) \\
&= \frac{2(q^2+1)}{q} + \frac{2}{q}\sum_{x \in D_j^{(q+1,q^4)}} \chi(x) \\
&\qquad (\text{where } (\theta^{i_1}-\theta^{i_2+\frac{\tau(q^2-1)}{2}}) \in D_j^{(q+1,q^4)},\ 0 \le j \le q) \\
&= \frac{2(q^2+1)}{q} + \frac{2}{q}\eta_j^{(q+1,q^4)}, \qquad (9)
\end{aligned}$$

where (9) holds since $\frac{t(q^2-1)}{2} + i\frac{r-1}{q-1}$ takes on each element of $(q+1)\cdot\mathbb{Z}_{\frac{q^4-1}{q+1}}$ exactly 2 times for $\gcd(\frac{q^2-1}{2}, \frac{r-1}{q-1}) = q+1$, when t and i range over $\mathbb{Z}_{2(q^2+1)}$ and $\mathbb{Z}_{q-1}$ respectively. For Lemma 6, p is an odd prime, $f = s$ and $\gamma = 2$. Hence, we have

$$\max_{0 \le j \le q}\{\eta_j^{(q+1,q^4)}\} = \frac{q^2-1}{q+1} = q-1$$

by Lemma 6 and

$$H(\mathcal{C}) = \frac{2(q^2+1)}{q} + \frac{2}{q}(q-1) = 2(q+1).$$

Furthermore,

$$\begin{aligned}
\left\lceil \frac{(nM-l)n}{(nM-1)l} \right\rceil &= \left\lceil \frac{2(q^4-q-1)(q^2+1)}{(q^4-2)q} \right\rceil \\
&= \left\lceil 2q + \frac{2q^4-2q^3+2q^2-2q-2}{q^5-2q} \right\rceil \\
&= 2q+1
\end{aligned}$$

since $0 < \frac{2q^4-2q^3+2q^2-2q-2}{q^5-2q} < 1$.

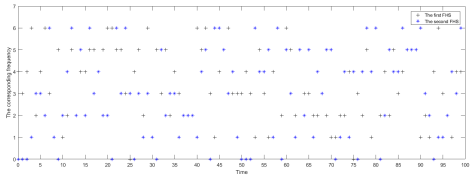

FIGURE 5. The time-frequency representation of an FHS set $\mathcal{C}$.

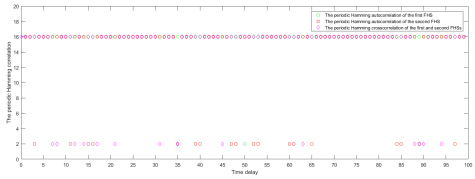

FIGURE 6. The periodic Hamming correlation of an FHS set $\mathcal{C}$.

TABLE 2. Some near-optimal sets of FHSs with parameters $(n, M, \lambda; l)$.

Parameters	Constraints	Ref.
$(p^2-p, p, p; p)$		[16], [25]
$(m(p^2-p), p, p; mp)$	$m = p_1^{e_1}p_2^{e_2}\cdots p_h^{e_h}$, $\gcd(m, p^2-p) = 1$ and $p^2-p < p_1$.	[6]
$(p, M, f+2; M)$	$p = Mf+1$ is an odd prime, $M \equiv 2 \pmod 4$ and f is even, or $4 \mid M$.	[16]
$(p, M, f+2; M)$	$p = Mf+1$ is an odd prime with $M > 1$ and $2 \nmid f$.	[21]
$(v, f_1, e+1; \frac{v-1}{e})$	$v = p_1^{m_1}p_2^{m_2}\cdots p_h^{m_h}$, $p_i = ef_i+1$ $(1 \le i \le h)$ and $f_1 > 1$.	[21]
$(N, M_1, f+1; M)$	$N = p_1p_2\cdots p_h = Mf+1$, $p_i = M_if+1$ $(1 \le i \le h)$ with $h \ge 2$ and f is even.	[24]
$(p^2, p, p; p+1)$	p is an odd prime	[26]
$(p^s, k, f+1; \frac{p^s-1}{f})$	$p = kf+1$ is an odd prime, $s \ge 2$ and f is odd.	[26]
$(p^s, k, f+1; \frac{p^s-1}{f})$	$p = kf+1$ is an odd prime, f is even.	[26]
$(\frac{3(q+1)}{2}, \frac{2(q-1)}{3}, 3; q)$	q is a power of an odd prime with $q \equiv 1 \pmod{12}$.	Theorem 3.1
$(\frac{q+1}{k}, k(q-1), 2; q)$	$q = p^s$ with an odd integer s, $p \equiv -1 \pmod{2k}$ and $\frac{q+1}{k}$ is even.	Theorem 3.3
$(2(q^2+1), \frac{q^2-1}{2}, 2(q+1); q)$	q is a power of an odd prime with $q \equiv 3 \pmod 4$.	Theorem 3.5
$(19, 18, 4; 7)$, $(7, 9, 3; 4)$, $(91, 45, 7; 16)$		Remark 3.7

Then we have

$$H(\mathcal{C}) = 2(q+1) = \left\lceil \frac{(nM-l)n}{(nM-1)l} \right\rceil + 1.$$

Therefore, $\mathcal{C}$ is near-optimal with respect to the Peng-Fan bound according to Lemma 1. □

Example 12: Let $q = p = 7$ and $r = q^4$. Let θ be the primitive element of $\mathbb{F}_r$ with $\theta^4 - 2\theta^2 - 3\theta + 3 = 0$. Then the set $\mathcal{C} = \{c^{(0)}, c^{(1)}, \cdots, c^{(23)}\}$ defined by (8) consists of the following FHSs of length 100:

$$c^{(0)} = (4, 3, 4, 6, 2, 4, 6, 3, 1, 5, 1, 2, 5, 2, 4, 4, 5, 5, 4, 5, 6,$$

$$
\begin{aligned}
& 6,5,5,3,0,4,5,2,6,1,5,3,5,2,4,3,2,2,2,\cdots),\\
c^{(1)} = {} & (0,0,0,1,3,3,2,6,1,0,2,4,6,2,5,2,6,3,4,2,2,\\
& 0,6,3,6,3,0,3,1,3,1,0,5,2,3,3,1,2,2,2,\cdots),\\
& \vdots\\
c^{(23)} = {} & (4,5,2,5,5,2,1,6,1,4,1,5,3,0,1,3,0,0,4,2,3,\\
& 6,4,0,4,1,3,5,4,0,0,4,1,0,3,2,1,3,1,1,\cdots).
\end{aligned}
$$

By Matlab software, there are simulation results to validate Theorem 11 in Figures 5 and 6 as follows:

Remark 13: Except these constructions given above, more near-optimal sets of FHSs can also be obtained from (3), Lemmas 5 and 6, whose parameters are $(19, 18, 4; 7)$, $(7, 9, 3; 4)$ and $(91, 45, 7; 16)$. Now we compare our parameters with some known parameters of near-optimal sets of FHSs in Table 2, where p is a prime, q is a power of an odd prime and $p_1, p_2, \cdots, p_h$ are h odd primes with $2 < p_1 < p_2 < \cdots < p_h$.

IV. CONCLUDING REMARKS

By means of the trace function and known Gaussian periods in finite fields, some algebraic constructions for near-optimal sets of FHSs were presented. As a comparison, we listed some parameters of near-optimal sets of FHSs, including our parameters in this paper. Inspired by this idea, more near-optimal sets of FHSs with new parameters may be obtained by virtue of new Gaussian periods and exponential sums in finite fields. Here we welcome the scholars to solve this problem together.

REFERENCES

[1] P. Fan and M. Darnell, *Sequence Design for Communications Applications*. London, U.K.: Wiley, 1996.

[2] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[3] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-20, no. 1, pp. 90–94, Jan. 1974.

[4] D. Peng and P. Fan, "Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2149–2154, Sep. 2004.

[5] B. Chen, L. Lin, S. Ling, and H. Liu, "Three new classes of optimal frequency-hopping sequence sets," *Designs, Codes Cryptogr.*, vol. 83, no. 1, pp. 219–232, Apr. 2017.

[6] S. Xu, X. Cao, and G. Xu, "Recursive construction of optimal frequency-hopping sequences sets," *IET Commun.*, vol. 10, no. 9, pp. 1080–1086, Feb. 2016.

[7] W. Chu and C. J. Colbourn, "Optimal frequency-hopping sequences via cyclotomy," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 1139–1141, Mar. 2005.

[8] C. Ding, M. J. Moisio, and J. Yuan, "Algebraic constructions of optimal frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2606–2610, Jul. 2007.

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

[10] G. Ge, Y. Miao, and Z. Yao, "Optimal frequency hopping sequences: Auto- and cross-correlation properties," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 867–879, Feb. 2009.

[11] C. Ding, R. Fuji-Hara, Y. Fujiwara, M. Jimbo, and M. Mishima, "Sets of frequency hopping sequences: Bounds and optimal constructions," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3297–3304, Jul. 2009.

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

[13] J.-H. Chung, Y. K. Han, and K. Yang, "New classes of optimal frequency-hopping sequences by interleaving techniques," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5783–5791, Dec. 2009.

[14] 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.

[15] 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.

[16] J.-H. Chung and K. Yang, "New frequency-hopping sequence sets with optimal average and good maximum Hamming correlations," *IET Commun.*, vol. 6, no. 13, pp. 2048–2053, Sep. 2012.

[17] 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.

[18] J.-H. Chung, G. Gong, and 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.

[19] W. Ren, F. Fu, and Z. Zhou, "New sets of frequency-hopping sequences with optimal Hamming correlation," *Designs, Codes Cryptogr.*, vol. 72, no. 2, pp. 423–434, Aug. 2014.

[20] H. Han, D. Peng, and U. Parampalli, "New sets of optimal low-hit-zone frequency-hopping sequences based on m-sequences," *Cryptogr. Commun.*, vol. 9, no. 4, pp. 511–522, Jul. 2017.

[21] S. Xu, X. Cao, J. M., and C. Tang, "More cyclotomic constructions of optimal frequency-hopping sequences," *Adv. Math. Commun.*, vol. 13, no. 3, pp. 373–391, Aug. 2019.

[22] X. Niu, C. Xing, Y. Liu, and L. Zhou, "A construction of optimal frequency hopping sequence set via combination of multiplicative and additive groups of finite fields," *IEEE Trans. Inf. Theory*, vol. 66, no. 8, pp. 5310–5315, Aug. 2020.

[23] H. Han, S. Zhang, L. Zhou, and X. Liu, "Decimated m-sequences families with optimal partial Hamming correlation," *Cryptogr. Commun.*, vol. 12, no. 3, pp. 405–413, May 2020.

[24] J.-H. Chung and K. Yang, "K-fold cyclotomy and its application to frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2306–2317, Apr. 2011.

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

[26] S. Xu, X. Cao, G. Xu, and G. Luo, "Two classes of near-optimal frequency-hopping sequence sets with prime-power period," *Cryptography Commun.*, vol. 10, no. 3, pp. 437–454, May 2018.

[27] G. Myerson, "Period polynomials and Gauss sums for finite fields," *Acta Arithmetica*, vol. 39, no. 3, pp. 251–264, 1981.

[28] C. Ding, *Codes From Difference Sets*. Singapore: World Scientific, 2015.