Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 8(12): 29158–29170.
DOI: 10.3934/math.20231493
Received: 13 August 2023
Revised: 09 October 2023
Accepted: 20 October 2023
Published: 26 October 2023

Research article

Optimal and near-optimal frequency-hopping sequences based on Gaussian period

Yan Wang[1], **Yanxi Fu**[1,*], **Nian Li**[2] **and Huanyu Wang**[1]

[1] School of Science, Xi'an University of Architecture and Technology, Caosi East Road, Xi'an, Shaanxi, 710311, China

[2] Hubei Key Laboratory of Applied Mathematics, School of Cyber Science and Technology, Hubei University, Wuhan, Hubei, 430062, China

* **Correspondence:** Email: fyx1998@xauat.edu.cn; Tel: 13468716034.

Abstract: Frequency-hopping sequences (FHSs) have a decisive influence on the whole frequency-hopping communication system. The Hamming correlation function plays an important role in evaluating the performance of FHSs. Constructing FHS sets that meet the theoretical bounds is crucial for the research and development of frequency-hopping communication systems. In this paper, three new classes of optimal FHSs based on trace functions are constructed. Two of them are optimal FHSs and the corresponding periodic Hamming autocorrelation value is calculated by using the known Gaussian period. It is shown that the new FHSs are optimal according to the Lempel-Greenberger bound. The third class of FHSs is the near-optimal FHSs.

Keywords: frequency-hopping sequence (FHS); trace function; Gaussian period; Lempel-Greenberger bound
Mathematics Subject Classification: 11T22, 94A60

1. Introduction

Frequency-hopping multiple-access is widely used in military radio communication, satellite communications, fiber-optic communications, underwater communications, microwave, and radar systems. The user's frequency slots used are chosen pseudo-randomly through a code called frequency-hopping sequences (FHS). The theoretical bound of the FHS gives the constraint relations that should be satisfied between different parameters.

Lempel and Greenberger [1] established a theoretical lower bound on the maximum Hamming autocorrelation of FHS for a given length and frequency set size, which is called the Lempel and

Greenberger bound, and the FHS satisfying the bound is called an optimal FHS. Constructing such optimal FHSs became a hot topic in FHS research [2,3].

Both algebraic and combinatorial constructions of optimal FHSs have been proposed in the literature (see [4–11]) and the references therein. Among all known constructions, cyclotomy [12] is one of the most useful techniques for coding theory and cryptography. Chung et al. [13] constructed several optimal FHSs of length from k-fold cyclotomic classes for distinct odd primes. A class of FHSs with flexible parameters was given based on the cyclotomic division of rings by Zeng [14]. In [15], Xu et al. constructed a family of FHSs based on the Zeng-Cai-Tang-Yang cyclotomy and the Chinese remainder theorem.

For a given sequence period and frequency set size, the optimal FHS does not always exist. Therefore, in the absence of the optimal parameters, the near-optimal FHS is a substitution of an optimal FHS. It is also important to construct a more near-optimal FHS with new parameters.

At present, the construction of near-optimal FHSs can be referred to in literature [16–19]. In 2008, Han et al. [20] first proposed the concept of near-optimal FHSs. In 2010, Chung et al. [21] generated two kinds of near-optimal FHSs by using the cyclotomic coset over finite fields. In 2014, Ren et al. [22] proposed a class of constructions of near-optimal FHSs by means of the Chinese remainder theorem and cyclotomic over finite fields. See Table 1 for more near-optimal FHSs.

Our purpose is to construct new optimal FHSs for some cases that are not covered in the literature. In this paper, we present three constructions for FHSs with optimal Hamming autocorrelation. The parameters of the optimal FHSs obtained in this paper are listed in Table 2, which gives a comparison of our constructions.

Table 1. Parameters of known near-optimal frequency sequences.

References	(n, l, λ)	Constraints	Lempel-Greenberger bound
[13]	$(p^2, p+1, p)$		near-optimal
[13]	$(p^n, \frac{p^n-1}{f}, k)$	$p = kf + 1, f$ is even.	near-optimal
[16]	$(q-1, e, f+1)$	$q = ef + 1$ is an odd prime power, f is odd.	near-optimal
[17]	$(\frac{q+1}{k}, \frac{q+2k+1}{2k}, 2)$	q is is odd prime power, $k \mid (q+1)$, $\dfrac{q+1}{k}$ is even.	near-optimal
[18]	$(pq, m, \frac{pq-1}{m}+1)$	p and q are distinct odd primes satisfying $p \equiv m + 1 (\bmod 2m)$ and $q \equiv 1 (\bmod 2m)$, and m is even common divisor of $p-1$ and $q-1$	near-optimal
[19]	$(q, e, f+1)$	$q = ef + 1$ is a prime power, f is even.	near-optimal
Theorem 3.3	$(\frac{q+1}{k^2}, \frac{q+2k^2+1}{2k^2}, 2)$	q is an odd prime power, $k^2 \mid (q+1)$, $\dfrac{q+1}{k^2}$ is even.	near-optimal

Table 2. Parameters of known optimal frequency sequences.

References	(n, l, λ)	Constraints	Lempel-Greenberger bound
[3]	(p^2, p, p)	p is a prime.	optimal
[5]	$(\frac{q+1}{k}, \frac{q+k+1}{2k}, 1)$	$k \mid (q+1)$, and $\dfrac{q+1}{k}$ is odd.	optimal
[6]	(p, M, f)	$p = Mf + 1$ is a prime, f is even, $p \equiv 3 \mod 4$,	optimal
[8]	$(\frac{q^n-1}{e}, q, \frac{q^{n-1}-1}{e})$	q is a prime power, $e \mid (q-1), \gcd(e, n) = 1$	optimal
[9]	$(\frac{q^m-1}{e}, q^k, \frac{q^{m-1}-1}{e})$	$1 \leqslant k \leqslant m$, $e \mid (q-1), \gcd(e, m) = 1$	optimal
[10]	$(q-1, e+1, f-1)$	$q = ef + 1$ is a prime power.	optimal
[12]	$(p, e+1, f+1)$	$p = ef + 1$, $e \geqslant 3f, f \geqslant 2$	optimal
Theorem 3.1	$\left(\frac{4(q+1)}{5}, \frac{4q+9}{10}, 1\right)$	$k^2 \mid (q+1)$, and $\dfrac{q+1}{k^2}$ is odd.	optimal
Theorem 3.2	$(\frac{q+1}{k^2}, \frac{q+k^2+1}{2k^2}, 1)$	$k^2 \mid (q+1)$, and $\dfrac{q+1}{k^2}$ is odd.	optimal

The rest of this paper is organized as follows. In section two, we present some notations and definitions about FHSs, as well as the cyclotomic class and Gaussian period. In section three, we propose two classes of optimal FHSs and prove they are optimal. In section four, we construct a class of near-optimal FHSs. The conclusions are provided in section five.

2. Preliminaries

For any positive integer $l \geqslant 2$, let $\mathbb{F} = \{f_0, f_1, \cdots, f_{l-1}\}$ be a set of l available frequencies, called an alphabet. A sequence $X = \{x(t)\}_{t=0}^{n-1}$ is called an FHS of length n over $\mathbb{F}$ if $x(t) \in \mathbb{F}$ for $0 \leqslant t \leqslant n-1$. For any FHS $X = \{x(t)\}_{t=0}^{n-1}$ of length n over $\mathbb{F}$, its Hamming autocorrelation H_X is defined by

$$H_X(\tau) = \sum_{t=0}^{n-1} h\left[x(t), x(t+\tau)\right], \quad 0 \leqslant \tau < n. \tag{2.1}$$

Where $h[a, b] = 1$ if $a = b$ and zero, the addition is performed modulo n. The maximum out-of-phase Hamming autocorrelation of X is defined as

$$H(X) = \max_{1 \leqslant \tau < n}\{H_X(\tau)\}.$$

Throughout this paper, let (n, l, λ) denote an FHS X of length n over an alphabet with size l with $\lambda = H(X)$. For a real number a, let $\lceil a \rceil$ denote the least integer no less than a and let $\lfloor a \rfloor$ denote the integer a part of a. A lower bound of $H(X)$ was established by Lempel and Greenberger as follows.

Lemma 2.1. *(Lempel-Greenberger bound [1], Lemma 4) For every FHS X of length n over an alphabet with size l,*

$$H(X) \geqslant \left\lceil \frac{(n-\epsilon)(n+\epsilon-l)}{l(n-1)} \right\rceil, \tag{2.2}$$

where ϵ is the least nonnegative residue of n modulo l.

Lemma 2.2. *([23], Corollary 1.2) Let X be any FHS of period n on a frequency set with size l,*

$$H(X) = \begin{cases} 0, & if\ n = l, \\ \lfloor n/l \rfloor, & if\ n > l. \end{cases} \tag{2.3}$$

We denote λ_{opt} as the righthand side in (2.2); that is, the value given by the Lempel-Greenberger bound. The following definitions will be used in this paper.

Definition 2.1. *An FHS X is optimal if $H(X) = \lambda_{opt}$, i.e. X is optimal with respect to the Lempel-Greenberger bound; an FHS X is near-optimal if $H(X) = \lambda_{opt} + 1$, i.e. X is near-optimal with respect to the Lempel-Greenberger bound.*

Let h be a positive integer, p be a prime number and $q = p^h$. Let n be a positive integer, $r = q^n$, $\mathbb{F}_r$ be a finite field containing r elements, and θ be the generator of the multiplicative group $\mathbb{F}^*_{q^m}$. Trace function Tr^r_q from finite field $\mathbb{F}_r$ to finite field $\mathbb{F}_q$ is defined as

$$Tr^r_q(x) = x + x^q + x^{q^2} + \cdots + x^{q^{n-1}},\ x \in \mathbb{F}_r.$$

Let $r - 1 = nN$, where n and N are positive integers greater than two. The Nth order of cyclotomic class $C^{(N,r)}_i$ of $\mathbb{F}_r$ is defined as

$$C^{(N,r)}_i = \{\alpha^{Nt+i} : 0 \leqslant t < N\},\ 0 \leqslant i < N.$$

Let $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ be the root of the primitive unit to the pth degree. The canonical addition feature χ over $\mathbb{F}_r$ is defined as

$$\chi(x) = \zeta_p^{Tr^r_p(x)},\quad x \in \mathbb{F}_r.$$

The orthogonal relation of addition characteristic is

$$\sum_{x\in\mathbb{F}_r} \chi(ax) = \begin{cases} r, & if\ a = 0, \\ 0, & if\ a \in \mathbb{F}^*_r. \end{cases} \tag{2.4}$$

The Gaussian period $\eta^{(N)}_i$ of order N over $\mathbb{F}_r$ is defined as

$$\eta^{(N)}_i = \sum_{x\in C^{(N)}_i} \chi(x),\ 0 \leqslant i < N.$$

Here's the convention:If $i \geqslant N$, then $\eta^{(N)}_i = \eta^{(N)}_{i(\bmod N)}$.

The following Gaussian period is from the conjugate case.

Lemma 2.3. *[24] Suppose j is the smallest positive integer such that $p^j \equiv -1\ (\bmod N)$. Let $r = p^{2j\gamma}$ and γ be a positive integer, then the Nth order Gaussian period $\eta^{(N)}_i$ over $\mathbb{F}_r$ satisfies*

1) when γ, p and $\frac{p^j+1}{N}$ are all odd,

$$\eta^{(N)}_i = \begin{cases} \dfrac{(N-1)\sqrt{r}-1}{N}, & if\ i = \dfrac{N}{2}, \\ \dfrac{-\sqrt{r}-1}{N}, & otherwise. \end{cases} \tag{2.5}$$

2) otherwise,

$$\eta_i^{(N)} = \begin{cases} \frac{(-1)^{\gamma+1}(N-1)\sqrt{r}-1}{N}, \ if\ i=0, \\ \frac{(-1)^{\gamma}\sqrt{r}-1}{N}, \ otherwise. \end{cases} \tag{2.6}$$

3. Results

Construction A. Let q be a power of an odd prime p and $r = q^2$. An FHS $X = \left(x_0, x_1, x_2, \cdots x_{\frac{4(q+1)}{5}-1}\right)$ of period $\frac{4(q+1)}{5}$ is defined as follows

$$X_t = Tr_q^{q^2}\left(\alpha^{\frac{5(q-1)}{4}t}\right),\ 1 \leqslant t < \frac{4(q+1)}{5}. \tag{3.1}$$

Lemma 3.1. *For*

$$0 \leqslant t_1 \leqslant t_2 < \frac{4(q+1)}{5},$$

we have

$$x_{t_1} = x_{t_2} \Leftrightarrow t_1 + t_2 = \frac{4(q+1)}{5}.$$

Proof. According to Eq (3.1),

$$\begin{aligned} x_t &= \alpha^{\frac{5}{4}(q-1)t} + \left(\alpha^{\frac{5}{4}(q-1)t}\right)^q \\ &= \alpha^{\frac{5}{4}(q-1)t} + \alpha^{-\frac{5}{4}(q-1)t}, \end{aligned}$$

thus

$$\begin{aligned} & x_{t_1} = x_{t_2} \\ \Leftrightarrow\ & \alpha^{\frac{5}{4}(q-1)t_1} + \alpha^{-\frac{5}{4}(q-1)t_1} = \alpha^{\frac{5}{4}(q-1)t_2} + \alpha^{-\frac{5}{4}(q-1)t_2} \\ \Leftrightarrow\ & \alpha^{\frac{5}{4}(q-1)t_1} - \alpha^{\frac{5}{4}(q-1)t_2} = \alpha^{-\frac{5}{4}(q-1)t_2} - \alpha^{-\frac{5}{4}(q-1)t_1} \\ \Leftrightarrow\ & \alpha^{\frac{5}{4}(q-1)(t_1+t_2)} = 1 \\ \Leftrightarrow\ & t_1 + t_2 = \frac{4(q+1)}{5}. \end{aligned}$$

□

Theorem 3.1. *Let the FHS X be given by Eq (3.1), then X has parameters* $\left(\frac{4(q+1)}{5}, \frac{4q+9}{10}, 1\right)$, *which is optimal with respect to the Lempel-Greenberger bound.*

Proof. First, from Lemma 3.1 we know that the frequency set size of the sequence X is $\frac{\frac{4(q+1)}{5}-1}{2} + 1 = \frac{4q+9}{10}$, then for $1 \leqslant \tau < \frac{4(q+1)}{5}$ we have

$$\begin{aligned} H_X(\tau) &= \left| \left\{ 0 \leqslant t < \frac{4(q+1)}{5} : Tr_q^{q^2}\left(\alpha^{\frac{5(q-1)t}{4}}\right) = Tr_q^{q^2}\left(\alpha^{\frac{5(q-1)(t+\tau)}{4}}\right) \right\} \right| \\ &= \frac{1}{q}\sum_{x\in F_q}\sum_{t=0}^{\frac{4(q+1)}{5}-1} \varsigma_p^{Tr_p^q\left[x\cdot Tr_q^{q^2}\left(\left(\alpha^{\frac{5(q-1)}{4}\tau}-1\right)\alpha^{\frac{5(q-1)t}{4}}\right)\right]} \end{aligned}$$

$$
\begin{aligned}
&= \frac{4(q+1)}{5q} + \frac{1}{q}\sum_{x\in F_q^*}\sum_{t=0}^{\frac{4(q+1)}{5}-1} \varsigma_p^{Tr_p^q\left[Tr_q^{q^2}\left(x\cdot\left(\alpha^{\frac{5(q-1)}{4}\tau}-1\right)\alpha^{\frac{5(q-1)t}{4}}\right)\right]}\\
&= \frac{4(q+1)}{5q} + \frac{1}{q}\sum_{t=0}^{\frac{4(q+1)}{5}-1}\sum_{i=0}^{q-2} \varsigma_p^{Tr_p^q\left[Tr_q^{q^2}\left(\left(\alpha^{\frac{5(q-1)}{4}\tau}-1\right)\alpha^{\frac{5(q-1)t+(q+1)i}{4}}\right)\right]}\\
&= \frac{4(q+1)}{5q} + \frac{1}{q}\sum_{t=0}^{\frac{4(q+1)}{5}-1}\sum_{i=0}^{q-2}\chi\left(\left(\alpha^{\frac{5(q-1)\tau}{4}}-1\right)\alpha^{\frac{5(q-1)t+(q+1)i}{4}}\right)\\
&= \frac{4(q+1)}{5q} + \frac{1}{q}\sum_{x\in C_0^{(\frac{5}{4})}}\chi\left(\left(\alpha^{\frac{5(q-1)\tau}{4}}-1\right)x\right)\\
&= \frac{4(q+1)}{5q} + \frac{1}{q}\sum_{x\in C_j^{(\frac{5}{4})}}\chi(x)\\
&= \frac{4(q+1)}{5q} + \frac{1}{q}\eta_j^{(\frac{5}{4})}.
\end{aligned}
$$

From Lemma 2.3, the minimum j is h while $\gamma = 1$. When $p = 2$, according to Eq (2.6),

$$H(X) \leqslant \frac{4(q+1)}{5q} + \frac{1}{q}\max_{0\leqslant j<\frac{5}{4}}\left\{\eta_j^{(\frac{5}{4})}\right\} = \frac{4(q+1)}{5q} + \frac{1}{q}\frac{(-1)^2 4(\frac{5}{4}-1)q-1}{5} = 1.$$

Similarly, when p is an odd prime number, it can be known from Eq (2.5) that

$$H(X) \leqslant \frac{4(q+1)}{5q} + \frac{1}{q}\max_{0\leqslant j<\frac{5}{4}}\left\{\eta_j^{(\frac{5}{4})}\right\} = \frac{4(q+1)}{5q} + \frac{1}{q}\frac{4(\frac{5}{4}-1)q-1}{5} = 1.$$

Thus, $H(X) \leqslant 1$ for all γ and p.

However,

$$H(X) \geqslant \left\lceil \frac{\left(\frac{4(q+1)}{5}-\frac{4q-1}{10}\right)\left(\frac{4(q+1)}{5}+\frac{4q-1}{10}-\frac{4q+9}{10}\right)}{\frac{4q+9}{10}\left(\frac{4(q+1)}{5}-1\right)}\right\rceil = 1.$$

Therefore, $H(X) = 1$, which is the Lempel-Greenberger bound. □

Construction B. Let $q = p^h$, p be a prime number and h be a positive integer. Let θ be the generator of the multiplication group $\mathbb{F}_{q^m}^*$ and m is even. The positive integer k is a factor of $q+1$, and $\frac{q+1}{k^2}$ is odd. An FHS $X = (x_0, x_1, \cdots, x_{\frac{q+1}{k^2}-1})$ of period $\frac{q+1}{k^2}$ is defined as follows

$$x_t = Tr_q^{q^m}(\theta^{k^2(q-1)t}),\quad 1 \leqslant t < \frac{q+1}{k^2}. \tag{3.2}$$

Lemma 3.2. *For*

$$0 \leqslant t_1 \leqslant t_2 < \frac{q+1}{k^2},$$

we have

$$x_{t_1} = x_{t_2} \Leftrightarrow t_1 + t_2 = \frac{q+1}{k^2}.$$

Proof. According to Eq (3.2),

$$\begin{aligned} x_t &= \left(\theta^{k^2(q-1)t} + (\theta^{k^2(q-1)t})^q + \cdots + \left(\theta^{k^2(q-1)t}\right)^{q^m}\right) \\ &= \left(\theta^{k^2(q-1)t} + (\theta^{k^2q(q-1)t}) + \cdots + \left(\theta^{k^2q^m(q-1)^t}\right)\right) \\ &= \frac{m}{2}\left(\theta^{k^2(q-1)t} + \theta^{-k^2(q-1)t}\right). \end{aligned}$$

Thus,

$$\begin{aligned} & x_{t_1} = x_{t_2} \\ \Leftrightarrow\ & \frac{m}{2}\left(\theta^{k^2(q-1)t_1} + \left(\theta^{-k^2(q-1)t_1}\right)\right) = \frac{m}{2}\left(\theta^{k^2(q-1)t_2} + \left(\theta^{-k^2(q-1)t_2}\right)\right) \\ \Leftrightarrow\ & \theta^{k^2(q-1)t_1} + \theta^{-k^2(q-1)t_1} = \theta^{k^2(q-1)t_2} + \theta^{-k^2(q-1)t_2} \\ \Leftrightarrow\ & \theta^{k^2(q-1)t_1} - \theta^{k^2(q-1)t_2} = \theta^{-k^2(q-1)t_2} - \theta^{-k^2(q-1)t_1} \\ \Leftrightarrow\ & \theta^{k^2(q-1)(t_1+t_2)} = 1 \\ \Leftrightarrow\ & t_1 + t_2 = \frac{q+1}{k^2}. \end{aligned}$$

Theorem 3.2. *Let the FHS X be given by Eq (3.2), then X has parameters* $\left(\frac{q+1}{k^2}, \frac{q+k^2+1}{2k^2}, 1\right)$*, which is optimal with respect to the Lempel-Greenberger bound, where* $k^2 \mid (q+1)$ *and* $\frac{q+1}{k^2}$ *is odd.*

Proof. First, from Lemma 3.2 we know that the frequency set size of the sequence X is $\frac{\frac{q+1}{k^2}-1}{2} + 1 = \frac{q+k^2+1}{2k^2}$, then for $1 \leqslant \tau < \frac{q+1}{k^2}$ we have

$$\begin{aligned} H_X(\tau) &= \left|\left\{0 \leqslant t < \frac{q+1}{k^2} : Tr_q^{q^m}(\theta^{k^2(q-1)t}) = Tr_q^{q^m}(\theta^{k^2(q-1)(t+\tau)})\right\}\right| \\ &= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\sum_{t=0}^{\frac{q+1}{k^2}-1} \zeta_p^{Tr_p^q[x\cdot Tr_q^{q^m}((\theta^{k^2(q-1)\tau}-1)\theta^{k^2(q-1)t})]} \\ &= \frac{q+1}{k^2q} + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\sum_{t=0}^{\frac{q+1}{k^2}-1} \zeta_p^{Tr_p^q[Tr_q^{q^m}(x(\theta^{k^2(q-1)\tau}-1)\theta^{k^2(q-1)t})]} \\ &= \frac{q+1}{k^2q} + \frac{1}{q}\sum_{t=0}^{\frac{q+1}{k^2}-1}\sum_{i=0}^{q-2} \zeta_p^{Tr_p^q[Tr_q^{q^m}((\theta^{k^2(q-1)\tau}-1)\theta^{k^2(q-1)t+(q+1)i})]} \\ &= \frac{q+1}{k^2q} + \frac{1}{q}\sum_{t=0}^{\frac{q+1}{k^2}-1}\sum_{i=0}^{q-2} \chi((\theta^{k^2(q-1)\tau}-1)\theta^{k^2(q-1)t+(q+1)i}) \\ &= \frac{q+1}{k^2q} + \frac{1}{q}\sum_{x\in C_0^{(k^2)}} \chi((\theta^{k^2(q-1)\tau}-1)x) \\ &= \frac{q+1}{k^2q} + \frac{1}{q}\sum_{x\in C_j^{(k^2)}} \chi(x) = \frac{q+1}{k^2q} + \frac{1}{q}\eta_j^{(k^2)}. \end{aligned}$$

From Lemma 2.3, the minimum j is h while $\gamma = 1$. When $p = 2$, according to Eq (2.6) we have

$$H(X) \leqslant \frac{q+1}{k^2 q} + \frac{1}{q} \max_{0 \leqslant j < k^2} \left\{ \eta_j^{(k^2)} \right\} = \frac{q+1}{k^2 q} + \frac{1}{q} \frac{(-1)^2 (k^2-1) q - 1}{k^2} = 1.$$

Similarly, when p is an odd prime number, it can be known from Eq (2.5) that

$$H(X) \leqslant \frac{q+1}{k^2 q} + \frac{1}{q} \max_{0 \leqslant j < k^2} \left\{ \eta_j^{(k^2)} \right\} = \frac{q+1}{k^2 q} + \frac{1}{q} \frac{(k^2-1) q - 1}{k^2} = 1.$$

Thus, $H(X) \leqslant 1$ for all γ and p.

However,

$$H(X) \geqslant \left\lceil \frac{\left(\frac{q+1}{k^2} - \frac{q-k^2+1}{2k^2}\right)\left(\frac{q+1}{k^2} + \frac{q-k^2+1}{2k^2} - \frac{q+k^2+1}{2k^2}\right)}{\frac{q+k^2+1}{2k^2}\left(\frac{q+1}{k^2} - 1\right)} \right\rceil = 1.$$

Therefore, $H(X) = 1$, which is the Lempel-Greenberger bound. □

Example 3.1. *Let $p = 211$, $h = 1$, $k = 2$ and $m = 2$, thus $q = p^h = 211$, $k^2 \mid (q+1)$ and $\frac{q+1}{k^2} = 53$ are odd. The FHS X defined by Eq (3.2) is*

$$\begin{aligned} X = (&2, 99, 93, 35, 207, 202, 168, 183, 14, 148, 79, 77, \\ &159, 50, 149, 142, 194, 74, 169, 199, 120, 76, 19, \\ &117, 170, 44, 177, 177, 44, 170, 117, 19, 76, 120, \\ &199, 169, 74, 194, 142, 149, 50, 159, 77, 79, 148, \\ &14, 183, 168, 202, 207, 35, 93, 99). \end{aligned}$$

It can be obtained by using Magma that the periodic Hamming autocorrelation $H_X(\tau)(1 \leqslant \tau \leqslant 52)$ of X is all one. Hence, the FHS X has parameters (53,27,1), and the Lempel-Greenberger bound is optimal. This is consistent with Theorem 3.2.

Example 3.2. *Let $p = 239$, $h = 1$, $k = 4$ and $m = 2$, thus $q = p^h = 239$, $k^2 \mid (q+1)$ and $\frac{q+1}{k^2} = 15$ are odd. The FHS X defined by Eq (3.2) is*

$$X = (2, 145, 230, 223, 79, 238, 15, 25, 25, 15, 238, 79, 223, 230, 145).$$

It can be obtained by using Magma that the periodic Hamming autocorrelation $H_X(\tau)(1 \leqslant \tau \leqslant 14)$ of X is all one. Hence, the FHS X has parameters (15,8,1), and the Lempel-Greenberger bound is optimal. This is consistent with Theorem 3.2.

Example 3.3. *Let $p = 107$, $h = 1$, $k = 2$ and $m = 2$, thus $q = p^h = 107$, $k^2 \mid (q+1)$ and $\frac{q+1}{k^2} = 27$ are odd. The FHS X defined by Eq (3.2) is*

$$\begin{aligned} X = (&2, 84, 99, 100, 62, 79, 47, 17, 97, 106, 33, 98, 67, 73, \\ &73, 67, 98, 33, 106, 97, 17, 47, 79, 62, 100, 99, 84). \end{aligned}$$

It can be obtained by using Magma that the periodic Hamming autocorrelation $H_X(\tau)(1 \leqslant \tau \leqslant 26)$ of X is all one. Hence, the FHS X has parameters (27,14,1), and the Lempel-Greenberger bound is optimal. This is consistent with Theorem 3.2.

Construction C. Let $q = p^h$, p be an odd prime number and h be a positive integer. Let θ be the generator of the multiplication group $\mathbb{F}_{q^m}^*$, and m is even. The positive integer k is a factor of $q+1$, and $\frac{q+1}{k^2}$ is even. An FHS $X = (x_0, x_1, \cdots, x_{\frac{q+1}{k^2}-1})$ of period $\frac{q+1}{k^2}$ is defined as follows

$$x_t = Tr_q^{q^m}(\theta^{k^2(q-1)t}),\ \ 1 \leqslant t < \frac{q+1}{k^2}. \tag{3.3}$$

Lemma 3.3. *For any* $1 \leqslant \tau < \frac{q+1}{k^2}$*, we have*

$$\theta^{k^2(q-1)\tau} - 1 \in \begin{cases} C_0^{(2k^2,q^2)}, \ \textit{if}\ \dfrac{q+1}{2k^2}\ \textit{and}\ \tau\ \textit{are parity}, \\ C_{k^2}^{(2k^2,q^2)}, \ \textit{otherwise}. \end{cases}$$

Proof.

$$\begin{aligned}
(\theta^{k^2(q-1)\tau} - 1)^{\frac{q^2-1}{2k^2}} &= ((\theta^{k^2(q-1)\tau} - 1)^{q-1})^{\frac{q+1}{2k^2}} \\
&= (\frac{(\theta^{k^2(q-1)\tau} - 1)^q}{\theta^{k^2(q-1)\tau} - 1})^{\frac{q+1}{2k^2}} \\
&= (\frac{\theta^{-k^2(q-1)\tau} - 1}{\theta^{k^2(q-1)\tau} - 1})^{\frac{q+1}{2k^2}} \\
&= (-1)^{\frac{q+1}{2k^2}-\tau} \\
&= \begin{cases} 1, & if\ \dfrac{q+1}{2k^2}\ and\ \tau\ are\ parity, \\ -1, & otherwise. \end{cases}
\end{aligned}$$

Consequently, the conclusion is proven. □

Lemma 3.4. *If* $\frac{q+1}{2k^2}$ *is odd, then*

$$\eta_0^{(2k^2,q^2)} = -\frac{q+1}{2k^2},\ \eta_{k^2}^{(2k^2,q^2)} = q - \frac{q+1}{2k^2};$$

if $\frac{q+1}{2k^2}$ *is even, then*

$$\eta_0^{(2k^2,q^2)} = q - \frac{q+1}{2k^2},\ \eta_{k^2}^{(2k^2,q^2)} = -\frac{q+1}{2k^2}.$$

Proof. If $\frac{q+1}{2k^2}$ is odd, then the smallest positive integer j satisfies $p^j \equiv -1 \pmod{2k^2}$ for h. For Lemma 3.2, $\Delta = 1$ and $\frac{p^j+1}{2k^2} = \frac{q+1}{2k^2}$ are odd. Therefore, $\eta_0^{(2k^2,q^2)} = \frac{-\sqrt{r}-1}{N} = \frac{-q-1}{2k^2} = -\frac{q+1}{2k^2}$ and $\eta_k^{(2k^2,q^2)} = \frac{(N-1)\sqrt{r}-1}{N} = \frac{(2k^2-1)q-1}{2k^2} = q - \frac{q+1}{2k^2}$. If $\frac{q+1}{2k^2}$ is even, the proof is similar to before. □

Theorem 3.3. *Let the FHS X be given by Eq (3.3), then X has parameters* $\left(\frac{q+1}{k^2}, \frac{q+2k^2+1}{2k^2}, 2\right)$*, and the Lempel-Greenberger bound is near-optimal.*

Proof. First, from Lemma 3.2, we know that the frequency set size of the sequence X is $\frac{\frac{q+1}{k^2}-2}{2} + 2 = \frac{q+2k^2+1}{2k^2}$, then for $1 \leqslant \tau < \frac{q+1}{k^2}$ we have

$$\begin{aligned}
H_X(\tau) &= |\left\{0 \leqslant t < \frac{q+1}{k^2} : Tr_q^{q^m}(\theta^{k^2(q-1)t}) = Tr_q^{q^m}(\theta^{k^2(q-1)(t+\tau)})\right\}| \\
&= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\sum_{t=0}^{\frac{q+1}{k^2}-1}\zeta_p^{Tr_p^q[x\cdot Tr_q^{q^m}((\theta^{k^2(q-1)\tau}-1)\theta^{k^2(q-1)t})]} \\
&= \frac{q+1}{k^2q} + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\sum_{t=0}^{\frac{q+1}{k^2}-1}\zeta_p^{Tr_p^q[Tr_q^{q^m}(x(\theta^{k^2(q-1)\tau}-1)\theta^{k^2(q-1)t})]} \\
&= \frac{q+1}{k^2q} + \frac{1}{q}\sum_{t=0}^{\frac{q+1}{k^2}-1}\sum_{i=0}^{q-2}\zeta_p^{Tr_p^q[Tr_q^{q^m}((\theta^{k^2(q-1)\tau}-1)\theta^{k^2(q-1)t+(q+1)i})]} \\
&= \frac{q+1}{k^2q} + \frac{1}{q}\sum_{t=0}^{\frac{q+1}{k^2}-1}\sum_{i=0}^{q-2}\chi((\theta^{k^2(q-1)\tau}-1)\theta^{k^2(q-1)t+(q+1)i}).
\end{aligned} \tag{3.4}$$

Since

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

we have Eq (3.4) as

$$\begin{aligned}
&= \frac{q+1}{k^2q} + \frac{2}{q}\sum_{x\in C_0^{(2k^2,q^2)}}\chi((\theta^{k^2(q-1)\tau}-1)x) \\
&= \begin{cases} \dfrac{q+1}{k^2q} + \dfrac{2}{q}\displaystyle\sum_{x\in C_0^{(2k^2,q^2)}}\chi(x), \ if \ \dfrac{q+1}{2k^2} \ and \ \tau \ are \ parity, \\ \dfrac{q+1}{k^2q} + \dfrac{2}{q}\displaystyle\sum_{x\in C_{k^2}^{(2k^2,q^2)}}\chi(x), \ otherwise. \end{cases} \\
&= \begin{cases} \dfrac{q+1}{k^2q} + \dfrac{2}{q}\eta_0^{(2k^2,q^2)}, \ if \ \dfrac{q+1}{2k^2} \ and \ \tau \ are \ parity, \\ \dfrac{q+1}{k^2q} + \dfrac{2}{q}\eta_{k^2}^{(2k^2,q^2)}, \ otherwise. \end{cases} \\
&= \begin{cases} 0, & if \ \tau \ is \ odd, \\ 2, & if \ \tau \ is \ even. \end{cases}
\end{aligned} \tag{3.5}$$

The penultimate row is derived from Lemma 3.3. Formula (3.5) is obtained from Lemma 3.4. Thus, $H(X) = 2$ and

$$\left\lfloor \frac{\frac{q+1}{k^2}}{\frac{q+2k^2+1}{2k^2}} \right\rfloor = \left\lfloor 1 + \frac{\frac{q+1}{2k^2}}{\frac{q+1}{2k^2}} \right\rfloor = 1.$$

Hence, $H(X) = 2 = \left\lfloor \frac{n}{l} \right\rfloor + 1$. That is, the FHS X is near-optimal with respect to the Lempel-Greenberger bound. □

Example 3.4. *Let $p = 167,\ h = 1,\ k = 2$ and $m = 2$, thus $q = p^h = 167$, $k^2 \mid (q+1)$ and $\frac{q+1}{k^2} = 42$ are even. The FHS X defined by Eq (3.3) is*

$$\begin{aligned} X = (&2, 21, 24, 68, 76, 34, 57, 1, 47, 73, 75, 8, 10, 36,\\ &82, 26, 49, 7, 15, 59, 62, 81, 62, 59, 15, 7, 49, 26,\\ &82, 36, 10, 8, 75, 73, 47, 1, 57, 34, 76, 68, 24, 21). \end{aligned}$$

It can be obtained by using Magma that the periodic Hamming autocorrelation is

$$H_X(\tau) = \begin{cases} 0, & if\ \tau\ is\ an\ odd,\\ 2, & if\ \tau\ is\ an\ even. \end{cases}$$

Therefore, the FHS X has parameters (42,22,2), and the Lempel-Greenberger bound is near-optimal. This is consistent with Theorem 3.3.

Example 3.5. *Let $p = 79,\ h = 1,\ k = 3$ and $m = 2$, thus $q = p^h = 79$, $k^2 \mid (q+1)$ and $\frac{q+1}{k^2} = 10$ are even. The FHS X defined by Eq (3.3) is*

$$X = (2, 80, 79, 10, 9, 87, 9, 10, 79, 80).$$

It can be obtained by using Magma that the periodic Hamming autocorrelation is

$$H_X(\tau) = \begin{cases} 0, & if\ \tau\ is\ an\ odd,\\ 2, & if\ \tau\ is\ an\ even. \end{cases}$$

Therefore, the FHS X has parameters (10,6,2), and the Lempel-Greenberger bound is near-optimal. This is consistent with Theorem 3.3.

Example 3.6. *Let $p = 499,\ h = 1,\ k = 5$ and $m = 2$, thus $q = p^h = 499$, $k^2 \mid (q+1)$ and $\frac{q+1}{k^2} = 20$ are even. The FHS X defined by Eq (3.3) is*

$$X = (2, 355, 275, 464, 274, 0, 225, 35, 224, 144, 497, 144, 224, 35, 225, 0, 274, 464, 275, 355).$$

It can be obtained by using Magma that the periodic Hamming autocorrelation is

$$H_X(\tau) = \begin{cases} 0, & \tau\ is\ an\ odd,\\ 2, & if\ \tau\ is\ an\ even. \end{cases}$$

Consequently, the FHS X has parameters (20,11,2), and the Lempel-Greenberger bound is near-optimal. This is consistent with Theorem 3.3.

4. Conclusions

In this paper, we proposed three classes of FHSs based on trace function, and showed they are optimal and near-optimal respectively according to the Lempel-Greenberger bound. Our construction was a discussion in the case of even numbers, though it would be interesting to discuss in the case of odd numbers. We leave this problem for one of our further works.

Use of AI tools declaration

The authors declare that they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The work of Yan Wang was supported by the National Natural Science Foundation of China under Grant 61902304 and Natural Science Basic Research Plan in Shaanxi Province of China 2021JQ-495. The work of Nian Li was supported in part by the Natural Science Foundation of Hubei Province of China under Grant 2021CFA079 and the Knowledge Innovation Program of Wuhan-Basic Research under Grant 2022010801010319.

Conflict of interest

The authors declare there is no conflict of interest.

References

1. A. Lempel, H. Greenberger, Families of sequences with optimal Hamming correlation properties, *IEEE Trans. Inform. Theory*, **20** (1974), 90–94. https://doi.org/10.1109/TIT.1974.1055169
2. X. Niu, C. Xing, New extension constructions of optimal frequency-hopping sequences sets, *IEEE Trans. Inform. Theory*, **65** (2019), 5846–5855. https://doi.org/10.1109/TIT.2019.2916362
3. G. Ge, R. Fuji-Hara, Y. Miao, Further combinatorial constructions for optimal frequency-hopping sequences, *J. Combin. Theory Ser. A*, **113** (2006), 1699–1718. https://doi.org/10.1016/j.jcta.2006.03.019
4. S. Xu, Optimal frequency-hopping sequences based on the decimated *m*-sequences, *Cryptogr. Commun.* **14** (2022), 983–998. https://doi.org/10.1007/s12095-022-00569-4
5. X. Zhou, Y. Li, A class of optimal frequency-hopping sequences with new parameters, *Math. Practice Theory*, **51** (2021), 216–221.
6. J. H. Chung, Y. K. Han, K. Yang, New classes of optimal frequency-hopping sequences by interleaving techniques, *IEEE Trans. Inform. Theory*, **55** (2009), 5783–5791. https://doi.org/10.1109/TIT.2009.2032742
7. X. Liu, L. Zhou, S. Li, A new method to construct strictly optimal frequency-hopping sequences with new parameters, *IEEE Trans. Inform. Theory*, **65** (2019), 1828–1844. https://doi.org/10.1109/TIT.2018.2864154
8. G. Ge, Y. Miao, Z. Yao, Optimal frequency-hopping sequences: Auto- and cross-correlation properties, *IEEE Trans. Inform. Theory*, **55** (2009), 867–879. https://doi.org/10.1109/TIT.2008.2009856
9. Z. Zhou, X. Tang, D. Peng, U. Parampalli, New constructions for optimal sets of frequency-hopping sequences, *IEEE Trans. Inform. Theory*, **57** (2011), 3831–3840. https://doi.org/10.1109/TIT.2011.2137290

10. C. Ding, J. Yin, Sets of optimal frequency-hopping sequences, *IEEE Trans. Inform. Theory*, **54** (2008), 3741–3745. https://doi.org/10.1109/TIT.2008.926410
11. C. Ding, M. J. Moisio, J. Yuan, Algebraic constructions of optimal frequency-hopping sequences, *IEEE Trans. Inform. Theory*, **53** (2007), 2606–2610. https://doi.org/10.1109/TIT.2007.899545
12. W. Chu, C. J. Colbourn, Optimal frequency-hopping sequences via cyclotomy, *IEEE Trans. Inform. Theory*, **51** (2005), 1139–1141. https://doi.org/10.1109/TIT.2004.842708
13. J. H. Chung, K. Yang, k-Fold cyclotomy and its application to frequency-hopping sequences, *IEEE Trans. Inform. Theory*, **57** (2011), 2306–2317. https://doi.org/10.1109/TIT.2011.2112235
14. X. Zeng, H. Cai, X. Tang, Y. Yang, Optimal frequency hopping sequences of odd length, *IEEE Trans. Inform. Theory*, **59** (2013), 3237–3248. https://doi.org/10.1109/TIT.2013.2237754
15. S. Xu, X. Cao, J. Mi, C. Tang, A new family of optimal FHS sets with composite lengths, *Discrete Math.*, **342** (2019), 1446–1455. https://doi.org/10.1016/j.disc.2019.01.026
16. Y. K. Han, K. Yang, On the Sidelnikov sequences as frequency-hopping sequences, *IEEE Trans. Inform. Theory*, **55** (2009), 4279–4285. https://doi.org/10.1109/TIT.2009.2025569
17. X. Zhou, Y. Li, Construction of near-optimal frequency-hopping sequences based on gaussian period, *J. Sichuan Normal Univ. Sci.*, **45** (2022), 654–659.
18. K. Yun, K. Yang, New near-optimal frequency-Hopping sequences of length pq, *IEEE Int. Symp. Inform. Theory*, 2008, 2593–2597. https://doi.org/10.1109/ISIT.2008.4595460
19. B. Huang, X. Zhang, Optimal construction of a class of frequency-hopping sequences sets, *Comput. Appl. Soft.*, **34** (2017), 123–127. https://doi.org/10.3969/j.issn.1000-386x.2017.03.022
20. X. Zeng, H. Cai, X. Tang, Y. Yang, A class of optimal frequency hopping sequences with new parameters, *IEEE Trans. Inform. Theory*, **58** (2012), 4899–4907. https://doi.org/10.1109/TIT.2012.2195771
21. J. H. Chung, K. Yang, Optimal frequency-hopping sequences with new parameters, *IEEE Trans. Inform. Theory*, **56** (2010), 1685–1693. https://doi.org/10.1109/TIT.2010.2040888
22. W. Ren, F. Fu, Z. Zhou, New sets of frequency-hopping sequences with optimal Hamming correlation, *Des. Codes Cryptogr.*, **72** (2014), 423–434. https://doi.org/10.1007/s10623-012-9774-3
23. R. Fuji-Hara, Y. Miao, M. Mishima, Optimal frequency-hopping sequences: A combinatorial approach, *IEEE Trans. Inform. Theory*, **50** (2004), 2408–2420. https://doi.org/10.1109/TIT.2004.834783
24. G. Myerson, Period polynomials and Gauss sums for finite fields, *Acta Arith.*, **39** (1981), 251–264.

AIMS Press