Optimal Sets of Frequency Hopping Sequences With Large Linear Spans

Qi Wang, *Student Member, IEEE*

***Abstract*—Frequency hopping (FH) is one of the basic spread coding technologies in spread spectrum communications. FH sequences are needed in FH code-division multiple access (CDMA) systems. For the anti-jamming purpose, FH sequences are required to have a large linear span. A few optimal sets of FH sequences are available in the literature. However, their sequences have very small linear spans. It is known that an optimal set of FH sequences could be transformed to another optimal set of FH sequences with large linear spans by a power permutation, if the power is chosen properly [see C. Ding and J. Yin, *IEEE Trans. Inf. Theory*, vol. IT-54, pp. 3741–3745, 2008]. The objective of this paper is to investigate this idea of C. Ding and J. Yin further, and determine the linear span of the FH sequences in the optimal sets obtained by applying a power permutation to some existing optimal sets of FH sequences.**

***Index Terms*—Frequency hopping sequence, linear span, optimal set of frequency hopping (FH) sequences, power permutation.**

I. Introduction

In spread spectrum communication systems, frequency hopping (FH) and direct sequence (DS) are two main spread coding technologies. Taking a basic modulation technique and changing the carrier frequency in some pseudorandom manner is the FH approach to generating a spread spectrum signal [2]. The carrier frequency is often determined by an *FH sequence*. FH sequences are an integral part of spread spectrum communication systems such as FH-CDMA systems (for a description of such systems, see [2]).

Throughout this paper, ℓ denotes a positive integer. Let $F = \{f_0, f_1, \dots, f_{\ell-1}\}$ be an abelian group (a set of available frequencies, also called the *alphabet*). Let $\mathcal{S}$ be the set of all FH sequences of length n over F. For two FH sequences $X, Y \in \mathcal{S}$, their Hamming correlation $H_{X,Y}$ is defined by

$$H_{X,Y}(t) = \sum_{i=0}^{n-1} h[x_i, y_{i+t}], \qquad 0 \le t < n \tag{1}$$

where $h[a,b] = 1$ if $a = b$, and 0 otherwise, and all operations among the position indices are performed modulo n. In an FH spread spectrum system, interference occurs when two distinct transmitters use the same frequency simultaneously. Hence the Hamming correlation between the two FH sequences X, Y being used by the transmitters is a measure of the quality of the sequence design.

Besides, for any distinct $X, Y \in \mathcal{S}$, we define the following three measures:

$$\begin{aligned} H(X) &= \max_{1 \le t < n} \{H_{X,X}(t)\} \\ H(X,Y) &= \max_{0 \le t < n} \{H_{X,Y}(t)\} \\ M(X,Y) &= \max\{H(X), H(Y), H(X,Y)\}. \end{aligned}$$

To judge whether an FH sequence is good, we need some bounds on its parameters. In 1974, Lempel and Greenberger developed the following lower bound for $H(X)$ [3].

Lemma 1: For every FH sequence X of length n over an alphabet of size ℓ, we have

$$H(X) \ge \left\lceil \frac{(n-\varepsilon)(n+\varepsilon-\ell)}{\ell(n-1)} \right\rceil$$

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

For a set of FH sequences, we define a measure on the quality of the set design as follows.

Let $\mathcal{F}$ be a subset of $\mathcal{S}$ containing N FH sequences. The maximum nontrivial Hamming correlation of the FH sequence set $\mathcal{F}$ is defined by

$$M(\mathcal{F}) = \max\left\{ \max_{X \in \mathcal{F}} H(X), \max_{X,Y \in \mathcal{F}, X \ne Y} H(X,Y) \right\}.$$

In this paper, let $(n, \lambda; \ell)$ denote an FH sequence X of length n over an alphabet of size ℓ where $\lambda = H(X)$; let $(n, N, \lambda; \ell)$ denote a set of N FH sequences $\mathcal{F}$ of length n over an alphabet of size ℓ where $\lambda = M(\mathcal{F})$.

To determine whether a set of FH sequences is good, some bounds are also needed on the parameters of the set. In 2004, Peng and Fan described the following bounds on $M(\mathcal{F})$, which take into consideration the number N of sequences in the set $\mathcal{F}$ [4].

Lemma 2: ([4, Corollary 1]) Let $\mathcal{F} \subseteq \mathcal{S}$ be a set of N FH sequences of length n over an alphabet of size ℓ. Define $I = \lfloor nN/\ell \rfloor$. Then

$$M(\mathcal{F}) \ge \left\lceil \frac{(nN-\ell)n}{(nN-1)\ell} \right\rceil \tag{2}$$

and

$$M(\mathcal{F}) \ge \left\lceil \frac{2InN-(I+1)I\ell}{(nN-1)N} \right\rceil. \tag{3}$$

Manuscript received May 18, 2009; revised October 09, 2009. Current version published March 17, 2010.

The author is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong (e-mail: wangq@cse.ust.hk).

Communicated by N. Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2010.2040874

0018-9448/$26.00 © 2010 IEEE

TABLE I
SOME KNOWN OPTIMAL SETS OF FREQUENCY HOPPING SEQUENCES

Length n	Alphabet size ℓ	H_{max}	Set size N	Linear span LS	Ref
p^r-1	p^u, $u \le r$	$p^{r-u}-1$	p^u		[3]
p^2	p	p	p	LS $> p$	[11]
p, odd prime	$e+1$, $e\|(p-1)$	$\frac{p-1}{e}$	e		[5]
$\frac{q^m-1}{2}$, m odd	q	$\frac{q^{m-1}-1}{2}$	2	m *	[6]

q^m-1	q	q^{m-1}	q	if $a=0$
				m *
				else
				$m+1$ *
					[6]

$q-1$, q is prime power	$e+1$, $e\|(q-1)$	$\frac{q-1}{e}$	e		[1]
$\frac{q^m-1}{d}$, q is prime power $\gcd(q-1,m)$ $=1$, $d\|(q-1)$	q	$\frac{q^{m-1}-1}{d}$	d	m *	[1] [9]

Hereafter, we use the following definitions:

1) A sequence $X \in \mathcal{S}$ is called *optimal* if the Lempel–Greenberger bound in Lemma 1 is met.
2) A subset $\mathcal{F} \subset \mathcal{S}$ is an *optimal set* if either of the bounds in Lemma 2 is met.

Lempel and Greenberger defined optimality for both single sequences and sets of sequences in other ways. A set of FH sequences meeting one of the bounds in Lemma 2 must be optimal in the Lempel–Greenberger sense.

It is relatively easy to construct single optimal FH sequences with respect to the Lempel–Greenberger bound of Lemma 1. Both algebraic and combinatorial constructions of such sequences were developed (for example, see [1], [3], [5]–[12]). However, only a few constructions of optimal sets of FH sequences are known. Table I describes the parameters of some known optimal sets of FH sequences, where the mark "$*$" means that the linear spans of the FH sequences in the optimal sets are discovered in this paper.

In engineering terms, the *linear span* of a sequence $\mathbf{s}$ is the length of the shortest linear feedback shift register (LFSR) that can output the sequence. Let $\mathbf{s} = (s_t)$ be a sequence over a field F. A polynomial of the form

$$f(X) = X^L + c_{L-1}X^{L-1} + \cdots + c_1X + c_0 \in F[X]$$

where $F[X]$ is the set of all polynomials in X over F, is called the *characteristic polynomial* of the sequence $\mathbf{s}$ if

$$s_{k+L} + c_{L-1}s_{k+L-1} + \cdots + c_1s_{k+1} + c_0s_k = 0, \quad \forall\, k \ge 0.$$

A characteristic polynomial of minimal degree L is called the *minimal polynomial* of $\mathbf{s}$ [13]. The minimal polynomial of a periodic sequence is uniquely defined. The linear span of a sequence $\mathbf{s}$ is defined as the degree of the minimal polynomial of $\mathbf{s}$, denoted by $\mathrm{LS}(\mathbf{s})$. The linear span implies, to some extent, the difficulty of reconstructing the sequence.

For some applications, FH sequences over a finite field are required to have a large linear span [2], [11], [14]. If the code sequence underlying the FH pattern has a small linear span, then the hopping pattern could possibly be exploited by a jammer attempting code sequence reconstruction [11]. Then a large linear span is desired for a more robust FH sequence design to baffle intelligent jammers. There are some optimal designs of FH sequences concerned with large linear spans. For example, see [11] and [12].

Three algebraic constructions of optimal sets of FH sequences were presented in [1] and [6]. These FH sequences are easy to implement using the arithmetic of finite fields. However, their linear spans are very small compared with their lengths. Ding and Yin mentioned in [1] that new optimal sets of FH sequences having large linear spans could be obtained by applying a proper power permutation to the optimal sets of FH sequences in [1]. In this paper, we investigate this idea further and determine the linear span of the FH sequences in the optimal sets obtained by applying a power permutation to the optimal sets in [1] and [6]. As a byproduct, we compute the linear spans and formulate the minimal polynomials of the FH sequences presented in [1] and [6].

II. THE FIRST ALGEBRAIC CONSTRUCTION

In this section, we first introduce the original construction of optimal sets of FH sequences presented in [6], and then investigate the linear span of the FH sequences in the transformed optimal sets. The transformed sets of FH sequences are still optimal with respect to the bounds in Lemma 2, and the linear span of the transformed sequences could be very large.

A. The Original Construction

Let p be an odd prime and $q = p^r$ for some positive integer r. Let $m \ge 3$ be an odd integer. For this construction, as described in Table I, the set of FH sequences has length $(q^m-1)/2$, set size 2 and $H_{\max} = (q^{m-1}-1)/2$.

The original construction of optimal sets of q-ary FH sequences of length $(q^m-1)/2$ is described as follows [6].

Let α be a generator of GF$(q^m)^*$, and let $n = (q^m-1)/2$. Let d be an integer with $\gcd(d, q^m-1) = 1$, and define $\beta = \alpha^{2d}$. For any $a \in$ GF(q^m), define a vector

$$\mathbf{s}_a = \left(\mathrm{Tr}_{q^m/q}(a), \mathrm{Tr}_{q^m/q}(a\beta), \ldots, \mathrm{Tr}_{q^m/q}(a\beta^{n-1})\right) \qquad (4)$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from GF(q^m) onto GF(q). Note that for any a, $a' \in$ GF(q^m), we have $\mathbf{s}_a - \mathbf{s}_{a'} = \mathbf{s}_{a-a'}$.

Theorem 3: [6] Let $m \ge 3$ be odd, then for $a \in$ GF$(q^m)^*$, $\mathbf{s}_a$ is an optimal $\left(\frac{q^m-1}{2}, \frac{q^{m-1}-1}{2}; q\right)$ FH sequence with respect to the bound of Lemma 1; let a be a square in GF$(q^m)^*$ and let a' be a nonsquare in GF$(q^m)^*$, then $\{\mathbf{s}_a, \mathbf{s}_{a'}\}$ constitutes a $\left(\frac{q^m-1}{2}, 2, \frac{q^{m-1}-1}{2}; q\right)$ optimal set of FH sequences with respect to the bound of (2).

Now we formulate the linear span and the corresponding minimal polynomial of the FH sequences aforedescribed.

Theorem 4: The linear span of FH sequences described in Theorem 3 is m, and the corresponding minimal polynomial of the FH sequences is

$$m(x) = \prod_{k=0}^{m-1} \left(x - \beta^{q^k}\right)$$

where $\beta = \alpha^{2d}$, $\gcd(d, q^m - 1) = 1$ and α is a generator of $\mathrm{GF}(q^m)^*$.

Proof: The FH sequences are defined by (4), that is, for $0 \le t \le n-1$

$$s_a(t) = \mathrm{Tr}_{q^m/q}(a\beta^t) = \mathrm{Tr}_{q^m/q}(a\alpha^{2dt}).$$

To compute the linear span, we first express $s_a(t)$ in terms of powers of α, and then obtain the linear span by counting the number of terms in this representation [15]. We have

$$s_a(t) = \mathrm{Tr}_{q^m/q}(a\alpha^{2dt}) = \sum_{j=0}^{m-1} (a^{q^j}\alpha^{2dq^j t}).$$

We now prove that all the exponents of α are pairwise distinct. Suppose that there exist j_1 and j_2, such that $0 \le j_1 < j_2 \le m-1$ and $\alpha^{2dq^{j_1}} = \alpha^{2dq^{j_2}}$. Then $\alpha^{2dq^{j_1}(q^{j_2-j_1}-1)} = 1$. Since $\mathrm{ord}(\alpha) = q^m - 1$, it follows that

$$(q^m - 1) \big| 2dq^{j_1}(q^{j_2-j_1} - 1). \tag{5}$$

Since $0 \le j_1 < j_2 \le m-1$, we get $q^{j_2-j_1} - 1 \le q^{m-1} - 1$. Note that $\gcd(q^m - 1, q^{j_1}) = 1$ and $\gcd(q^m - 1, d) = 1$, then $(q^m - 1)$ does not divide $2dq^{j_1}(q^{j_2-j_1} - 1)$, contradicting to (5). Therefore the number of terms in this representation is exactly m, which leads to the statement that the linear span of the FH sequences is m.

Suppose that $f(x) = x^m + \sum_{i=0}^{m-1} c_i x^i$ is an irreducible polynomial over $\mathrm{GF}(q)$. Let $\beta = \alpha^{2d}$ be a root of $f(x)$, that is, $\beta^m + \sum_{i=0}^{m-1} c_i\beta^i = 0$. We have

$$\begin{aligned} s_a(k+m) &+ \sum_{i=0}^{m-1} c_i s_a(k+i) \\ &= \mathrm{Tr}_{q^m/q}(a\beta^{k+m}) + \sum_{i=0}^{m-1} c_i \mathrm{Tr}_{q^m/q}(a\beta^{k+i}) \\ &= \mathrm{Tr}_{q^m/q}\left(a\beta^k\left(\beta^m + \sum_{i=0}^{m-1} c_i\beta^i\right)\right) \\ &= 0, \quad \forall\, k \ge 0. \end{aligned}$$

Thus $f(x)$ is a characteristic polynomial of $\mathbf{s}_a$, and β^{q^j} for $0 \le j \le m-1$ are all the m roots of $f(x)$. Thus the minimal polynomial of $\mathbf{s}_a$ is

$$m(x) = \prod_{k=0}^{m-1} (x - \beta^{q^k})$$

which leads to the desired result. ■

B. Transformed Optimal Sets of FH Sequences

According to Theorem 4, the linear span of the FH sequences is too small compared with their length $(q^m - 1)/2$. Now we transform $\{\mathbf{s}_a, \mathbf{s}_{a'}\}$ into another set of FH sequences using a power permutation of $\mathrm{GF}(q)$. The transformed set is still optimal with respect to the bounds of Lemma 2. We borrow the method in [14] to determine the linear span of the FH sequences in the transformed optimal sets.

Theorem 5: Let σ be a positive integer $0 < \sigma < q-1$ such that $\gcd(\sigma, q-1) = 1$. For $0 \le t \le n-1$ where $n = (q^m - 1)/2$, define

$$s_a^\sigma(t) = \left(\mathrm{Tr}_{q^m/q}(a\beta^t)\right)^\sigma$$

where $\beta = \alpha^{2d}$, $\gcd(q^m - 1, d) = 1$ and α is a generator of $\mathrm{GF}(q^m)^*$. Then

1) $\{\mathbf{s}_a^\sigma, \mathbf{s}_{a'}^\sigma\}$ constitutes a

$$\left(\frac{q^m - 1}{2}, 2, \frac{q^{m-1} - 1}{2}; q\right)$$

optimal set of FH sequences over the alphabet $\mathrm{GF}(q)$, meeting the bound of (2). Furthermore, either sequence of the set $\{\mathbf{s}_a^\sigma, \mathbf{s}_{a'}^\sigma\}$ is optimal with respect to the bound of Lemma 1.

2) The linear span of the transformed FH sequences is

$$\prod_{i=1}^{w} \binom{m + \sigma_i - 1}{\sigma_i},$$

where these σ_i's and w are determined by $\sigma = \sum_{i=1}^{w} \sigma_i p^{e_i}$, $q = p^r$, $0 \le e_i < r$, $e_i \ne e_j$ if $i \ne j$, and $\binom{x}{y} = x!/y!(x-y)!$ is the binomial coefficient.

Proof:

1) Since $\gcd(\sigma, q-1) = 1$, $\mathbf{s}_a^\sigma$ is a permutation sequence of $\mathbf{s}_a$. By the definition of Hamming correlation in (1), the first conclusion of this theorem follows obviously.

2) By definition, for $0 \le t \le n-1$,

$$s_a^\sigma(t) = \left(\mathrm{Tr}_{q^m/q}(a\beta^t)\right)^\sigma,$$

where $\gcd(\sigma, q-1) = 1$, $\sigma = \sum_{i=1}^{w} \sigma_i p^{e_i}$ and $\beta = \alpha^{2d}$.

By properties of the trace function,

$$s_a^\sigma(t) = \prod_{i=1}^{w} \left(\mathrm{Tr}_{q^m/q}(a^{p^{e_i}}\beta^{p^{e_i}t})\right)^{\sigma_i}. \tag{6}$$

Using the well-known multinomial formula

$$\left(\sum_{j=1}^{N} a_j\right)^t = \sum_{k_1+\cdots+k_N=t} \binom{t}{k_1, \ldots, k_N} {a_1}^{k_1} \ldots {a_N}^{k_N}$$

where

$$\binom{t}{k_1, \ldots, k_N} = \frac{t!}{k_1! \cdot \cdots \cdot k_N!},$$

we get

$$\begin{aligned} &\left(\mathrm{Tr}_{q^m/q}(a^{p^{e_i}}\beta^{p^{e_i}t})\right)^{\sigma_i} \\ &\quad= \left(\sum_{j=0}^{m-1} (a^{p^{e_i}}\beta^{p^{e_i}t})^{q^j}\right)^{\sigma_i} \\ &\quad= \sum_{\lambda_{i,0}+\cdots+\lambda_{i,m-1}=\sigma_i} \binom{\sigma_i}{\lambda_{i,0}, \ldots, \lambda_{i,m-1}} \\ &\qquad \cdot (a^{p^{e_i}}\beta^{p^{e_i}t})^{\sum_{j=0}^{m-1} q^j\lambda_{i,j}}. \end{aligned}$$

Then by (6)

$$s_a^\sigma(t) = \prod_{i=1}^{w} \sum_{\lambda_{i,0}+\cdots+\lambda_{i,m-1}=\sigma_i} \binom{\sigma_i}{\lambda_{i,0},\ldots,\lambda_{i,m-1}} \cdot \left(a^{p^{e_i}}\beta^{p^{e_i}t}\right)^{\sum_{j=0}^{m-1} q^j \lambda_{i,j}}.$$

Replacing the product by a w-fold sum, see (7) at the bottom of the page, where

$$g(\boldsymbol{\lambda}, \mathbf{e}) = \sum_{j=0}^{m-1} q^j \sum_{i=1}^{w} \lambda_{i,j} p^{e_i} \tag{8}$$

and

$$b = a^{g(\boldsymbol{\lambda}, \mathbf{e})}.$$

We now show that all the exponents of β in (7) are pairwise distinct modulo $q^m - 1$. Assume that two different $\boldsymbol{\lambda}$ and $\boldsymbol{\lambda}'$ produce the same exponent of β modulo $q^m - 1$, that is

$$g(\boldsymbol{\lambda}, \mathbf{e}) \equiv g(\boldsymbol{\lambda}', \mathbf{e}) \ (\bmod q^m - 1). \tag{9}$$

Since $\sigma = \sum_{i=1}^{w} \sigma_i p^{e_i}$ and $0 < \sigma < q - 1$, $g(\boldsymbol{\lambda}, \mathbf{e})$ is less than $q^m - 1$ and the modulo operation can be omitted.

With (8) and (9), we obtain

$$\begin{aligned} & q^0(\lambda_{1,0}p^{e_1} + \cdots + \lambda_{w,0}p^{e_w}) \\ & + q^1(\lambda_{1,1}p^{e_1} + \cdots + \lambda_{w,1}p^{e_w}) \\ & \quad \vdots \\ & + q^{m-1}(\lambda_{1,m-1}p^{e_1} + \cdots + \lambda_{w,m-1}p^{e_w}) \\ & = q^0(\lambda'_{1,0}p^{e_1} + \cdots + \lambda'_{w,0}p^{e_w}) \\ & + q^1(\lambda'_{1,1}p^{e_1} + \cdots + \lambda'_{w,1}p^{e_w}) \\ & \quad \vdots \\ & + q^{m-1}(\lambda'_{1,m-1}p^{e_1} + \cdots + \lambda'_{w,m-1}p^{e_w}). \end{aligned} \tag{10}$$

We consecutively reduce (10) modulo q^k for $k = 1, 2, \ldots, m-1$, and we have $\lambda_{i,j} = \lambda'_{i,j}$ for all $i \in \{1, 2, \ldots, w\}$ and $j \in \{0, 1, \ldots, m-1\}$. Thus we complete the proof that all the exponents of β in (7) are pairwise distinct.

Suppose that there exist $g_1 = g(\boldsymbol{\lambda_1}, \mathbf{e})$ and $g_2 = g(\boldsymbol{\lambda_2}, \mathbf{e})$ such that $\sigma \le g_1 < g_2 \le \sigma q^{m-1}$ and $\alpha^{2dg_1} = \alpha^{2dg_2}$. Then $\alpha^{2d(g_2 - g_1)} = 1$. Since $\mathrm{ord}(\alpha) = q^m - 1$, it follows that

$$(q^m - 1) \big| 2d(g_2 - g_1). \tag{11}$$

Since $\sigma \le g_1 < g_2 \le \sigma q^{m-1}$, we get

$$g_2 - g_1 \le \sigma(q^{m-1} - 1) < (q - 1)(q^{m-1} - 1).$$

Note that $\gcd(q^m - 1, d) = 1$ and $\gcd(q - 1, \sigma) = 1$, then $(q^m - 1)$ does not divide $2d(g_2 - g_1)$, contradicting to (11). Therefore the exponents of α are also pairwise distinct.

We now compute the linear span of $\mathbf{s}_a^\sigma$ by counting the number of terms in this representation. Since there are

$$\binom{m + \sigma - 1}{\sigma}$$

possibilities to represent σ as

$$\sigma = \sum_{j=0}^{m-1} l_j, \text{ for } 0 \le l_j \le \sigma$$

and by applying this result to all σ_i's, the linear span is

$$\mathrm{LS} = \prod_{i=1}^{w} \binom{m + \sigma_i - 1}{\sigma_i}$$

which completes the proof. ■

Corollary 6: If the exponent $\sigma = p^r - p^j - 1$ for $0 \le j < r$, the FH sequences transformed by the power permutation have the largest linear span, which is

$$\mathrm{LS} = \binom{m + p - 2}{p - 1}^{r-1} \binom{m + p - 3}{p - 2}.$$

Proof: According to Theorem 5, with a power permutation, the linear span of the transformed optimal FH sequences is

$$\mathrm{LS} = \prod_{i=1}^{w} \binom{m + \sigma_i - 1}{\sigma_i}.$$

For $0 < \sigma_i \le p - 1$, we have

$$\binom{m + \sigma_i - 1}{\sigma_i} \ge m.$$

And for $0 < \sigma_i < \sigma_j \le p - 1$, we have

$$\binom{m + \sigma_j - 1}{\sigma_j} > \binom{m + \sigma_i - 1}{\sigma_i}.$$

Therefore, to get the largest linear span, w and σ_i for $1 \le i \le w$ should be as large as possible. Since w and σ_i's are determined by $\sigma = \sum_{i=1}^{w} \sigma_i p^{e_i}$, LS is the largest when $w = r$, $r - 1$ σ_i's are $p - 1$ and the rest one σ_i is $p - 2$. It follows that $\sigma = p^r - p^j - 1$ where $0 \le j < r$. Note that

$$(p^{r-j} - 1)(p^r - 1) - p^{r-j}(p^r - p^j - 1) = 1$$

$$s_a^\sigma(t) = \sum_{\sum_{j=0}^{m-1} \lambda_{1,j} = \sigma_1} \sum_{\sum_{j=0}^{m-1} \lambda_{2,j} = \sigma_2} \cdots \sum_{\sum_{j=0}^{m-1} \lambda_{w,j} = \sigma_w} \prod_{i=1}^{w} \binom{\sigma_i}{\lambda_{i,0}, \ldots, \lambda_{i,m-1}} b \beta^{g(\boldsymbol{\lambda}, \mathbf{e}) \cdot t} \tag{7}$$

then we obtain $\gcd(\sigma, p^r - 1) = 1$, and the desired result follows. ■

Remark 1: In Corollary 6, if the power σ is chosen properly, the linear span of the sequences in the new optimal set could be very large. For example, let $q = 3^3$, $m = 3$, $d = 1$, $a = 1$ and $a' = -1$, the linear span of both sequences in $\{\mathbf{s}_a, \mathbf{s}_{a'}\}$ in only 3. However, if we choose $\sigma = 17$, the linear span of either sequence in $\{\mathbf{s}_a^\sigma, \mathbf{s}_{a'}^\sigma\}$ is 108.

III. The Second Algebraic Construction

In this section, we investigate another algebraic construction of optimal sets of FH sequences presented in [1]. This construction of optimal sets of FH sequences was generalized in [9]. In fact, the first construction investigated in Section II can be viewed as a special case of this construction. Using a proper power permutation, we obtain new sets of FH sequences having large linear spans. The transformed sets of FH sequences are still optimal with respect to the bounds in Lemma 2.

A. The Original Construction

Let p be a prime and $q = p^r$ for some positive integer r. Suppose that m, d are two positive integers satisfying $d|(q^m - 1)$ and $\gcd((q^m - 1)/(q - 1), d) = 1$, that is, $d|(q - 1)$. For this construction, the set of q-ary FH sequences has length $(q^m - 1)/d$, set size d and $H_{\max} = (q^{m-1} - 1)/d$.

The original construction of optimal sets of FH sequences is described as follows [1].

Let α be a generator of GF$(q^m)^*$. Define $\beta = \alpha^{cd}$ where c is a positive integer with $\gcd(c, q^m - 1) = 1$ and let $n = (q^m - 1)/d$. For each $0 \le i \le d - 1$, we define the following sequence:

$$s_i(t) = \mathrm{Tr}_{q^m/q}(\alpha^i \beta^t), \quad 0 \le t \le n - 1 \tag{12}$$

where $\mathrm{Tr}_{q^m/q}$ is the trace function from GF(q^m) onto GF(q). Each $\mathbf{s}_i$ is a sequence of length n over the alphabet GF(q). The set of FH sequences is defined as

$$\mathcal{S} = \{\mathbf{s}_i : 0 \le i \le d - 1\}.$$

Theorem 7: [1], [9] If $\gcd(d, \sum_{i=0}^{m-1} q^i) = 1$, then $\mathcal{S}$ is a $\left(\frac{q^m-1}{d}, d, \frac{q^{m-1}-1}{d}; q\right)$ optimal set of FH sequences over the alphabet GF(q), meeting the bound of (2). Furthermore, each sequence in $\mathcal{S}$ is optimal with respect to the bound of Lemma 1.

Now we calculate the linear span of the FH sequences in $\mathcal{S}$ and formulate the corresponding minimal polynomial.

Theorem 8: The linear span of the FH sequences described in Theorem 7 is m, and the corresponding minimal polynomial of the FH sequences is

$$m(x) = \prod_{k=0}^{m-1} (x - \beta^{q^k}),$$

where $\beta = \alpha^{cd}$ with $\gcd(c, q^m - 1) = 1$ and α is a generator of GF$(q^m)^*$.

Proof: The FH sequences are defined by (12), that is, for $0 \le t \le n - 1$

$$s_i(t) = \mathrm{Tr}_{q^m/q}(\alpha^i \beta^t) = \mathrm{Tr}_{q^m/q}(\alpha^i \alpha^{cdt}).$$

We first express $s_i(t)$ in terms of powers of α, and then compute the linear span by counting the number of terms in this representation [15]. We have

$$s_i(t) = \mathrm{Tr}_{q^m/q}(\alpha^i \alpha^{cdt}) = \sum_{j=0}^{m-1} (\alpha^{iq^j} \alpha^{q^j cdt})$$

for $0 \le i \le d - 1$. We now prove that all the exponents of α are pairwise distinct. Suppose that there exist j_1 and j_2, such that $0 \le j_1 < j_2 \le m - 1$ and $\alpha^{cdq^{j_1}} = \alpha^{cdq^{j_2}}$. Then $\alpha^{cdq^{j_1}(q^{j_2-j_1}-1)} = 1$. Since $\mathrm{ord}(\alpha) = q^m - 1$, it follows that

$$(q^m - 1) \big| cdq^{j_1}(q^{j_2-j_1} - 1). \tag{13}$$

Since $0 \le j_1 < j_2 \le m - 1$, we get $q^{j_2-j_1} - 1 \le q^{m-1} - 1$. Thus

$$d(q^{j_2-j_1} - 1) \le (q^{m-1} - 1)(q - 1) < q^m - 1.$$

Note that $\gcd(q^m - 1, q^{j_1}) = 1$ and $\gcd(c, q^m - 1) = 1$, it follows that $(q^m - 1)$ does not divide $cd(q^{j_2} - q^{j_1})$, contradicting to (13). Hence the number of terms in the representation is exactly m, leading to the desired result.

Similar to the proof of Theorem 4, the minimal polynomial of $\mathbf{s}_i$ is

$$m(x) = \prod_{k=0}^{m-1} (x - \beta^{q^k})$$

which completes the proof. ■

B. Transformed Optimal Sets of FH Sequences

According to Theorem 8, the linear span of the FH sequences above is too small compared with their length $(q^m - 1)/d$. Now we obtain optimal sets of FH sequences by a power permutation of GF(q).

Theorem 9: Let σ be a positive integer $0 < \sigma < q - 1$ such that $\gcd(\sigma, q - 1) = 1$. Define

$$\mathcal{S}^\sigma = \{s_i^\sigma : 0 \le i \le d - 1\}$$

where

$$s_i^\sigma(t) = \left(\mathrm{Tr}_{q^m/q}(\alpha^i \beta^t)\right)^\sigma, \quad 0 \le t \le n - 1$$

and $n = (q^m - 1)/d$.

1) If $\gcd\left(d, \sum_{i=0}^{m-1} q^i\right) = 1$, then $\mathcal{S}^\sigma$ is a

$$\left(\frac{q^m - 1}{d}, d, \frac{q^{m-1} - 1}{d}; q\right)$$

optimal set of FH sequences over the alphabet GF(q), meeting the bound of (2). Furthermore, each sequence in $\mathcal{S}^\sigma$ is optimal with respect to the bound of Lemma 1.

2) The linear span of the new FH sequences is

$$\prod_{i=1}^{w}\binom{m+\sigma_i-1}{\sigma_i},$$

where these σ_i's and w are determined by $\sigma = \sum_{i=1}^{w}\sigma_i p^{e_i}$, $q = p^r$, $0 \le e_i < r$, $e_i \ne e_j$ if $i \ne j$, and $\binom{x}{y} = x!/y!(x-y)!$ is the binomial coefficient.

Proof: Similar to the proof of Theorem 5, the conclusions follow. ■

Corollary 10: If the exponent $\sigma = p^r - p^j - 1$ for $0 \le j < r$, the FH sequences transformed by the power permutation have the largest linear span, which is

$$\mathrm{LS} = \binom{m+p-2}{p-1}^{r-1}\binom{m+p-3}{p-2}.$$

Proof: The conclusion of this corollary follows from that of Corollary 6. ■

Remark 2: According to Corollary 10, if the power σ is chosen properly, the linear span of the sequences in the new optimal set could be very large. For example, let $q = 5^3$, $m = 3$, the linear span of all sequences in $\mathcal{S}$ in only 3. However, if we choose $\sigma = 99$, the linear span of each sequence in $\mathcal{S}^\sigma$ is 2250.

IV. The Third Algebraic Construction

In this section, we first introduce an algebraic construction of optimal sets of FH sequences presented in [6], and then compute the linear span of the FH sequences in the transformed sets using a power permutation. The transformed sets of FH sequences are still optimal with respect to the bounds in Lemma 2.

A. The Original Construction

Let p be a prime and $q = p^r$ for some positive integer r. Suppose that $m \ge 1$ is an integer and $\mathrm{Norm}(x)$ denotes the norm function from $\mathrm{GF}(q^m)$ onto $\mathrm{GF}(q)$, which is defined by $\mathrm{Norm}(x) = x^{(q^m-1)/(q-1)}$, where $x \in \mathrm{GF}(q^m)$. For this construction, as described in Table I, the set of q-ary FH sequences has length $q^m - 1$, set size q and $H_{\max} = q^{m-1}$.

The original construction of optimal sets of q-ary FH sequences of length $q^m - 1$ is describe as follows [6].

Let α be a generator of $\mathrm{GF}(q^m)^*$, and let c be an integer with $1 \le c \le q-2$. For any $a, b \in \mathrm{GF}(q^m)$, we define a function from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$

$$f_{a,b}(x) = \mathrm{Tr}_{q^m/q}(a\mathrm{Norm}(x^c) + bx)$$

where $\mathrm{Tr}_{q^m/q}$ denotes the trace function from $\mathrm{GF}(q^m)$ onto $\mathrm{GF}(q)$.

For any $a, b \in \mathrm{GF}(q^m)$, we define the following vector:

$$\mathbf{s}_{a,b} = (f_{a,b}(\gamma_0), f_{a,b}(\gamma_1), \ldots, f_{a,b}(\gamma_{q^m-2})) \qquad (14)$$

where $\gamma_i = \alpha^i$ for $0 \le i \le q^m - 2$.

Theorem 11: [6] With the same notations as above, define

$$\mathcal{F}_s = \{\mathbf{s}_{da,1} : a \in \mathrm{GF}(q)\}.$$

Assume that $\gcd(cm-1, q-1) = 1$ for $1 \le c \le q-2$, and d is an element in $\mathrm{GF}(q^m)^*$ with $\mathrm{Tr}_{q^m/q}(d) \ne 0$. Then for $a \in \mathrm{GF}(q)$, $\mathbf{s}_{da,1}$ is a $(q^m-1, q^{m-1}; q)$ optimal FH sequence meeting the bound of Lemma 1; $\mathcal{F}_s$ is a $(q^m-1, q, q^{m-1}; q)$ optimal set of FH sequences with respect to the bound of (2).

To compute the linear span of FH sequences in Theorem 11, we first give the following lemma.

Lemma 12: [16] Let $\mathbf{s}$ be the sequence defined by the trace function $s(t) = \mathrm{Tr}_{q^m/q}(\alpha^t)$ (also known as m-sequence) where $q = p^r$ for p prime and r positive integer, and α is a generator of $\mathrm{GF}(q^m)^*$. Then the linear span of $\mathbf{s}$ is m and the corresponding minimal polynomial of $\mathbf{s}$ is an irreducible polynomial over $\mathrm{GF}(q)$ with the root of α.

The linear span and the corresponding minimal polynomial of the FH sequences in $\mathcal{F}_s$ are formulated in the following theorem.

Theorem 13: For the FH sequences in $\mathcal{F}_s$ in Theorem 11, the linear span of $\mathbf{s}_{da,1}$ is m for $a = 0$ and $m+1$ for $a \ne 0$. The corresponding minimal polynomial of the FH sequences is $m(x)$ and $m(x)\cdot(x - \alpha^{cv})$ where $v = (q^m-1)/(q-1)$, respectively, where $m(x)$ is an irreducible polynomial over $\mathrm{GF}(q)$ with the root of α.

Proof: The FH sequences are defined by (14), that is, for $0 \le t \le q^m - 2$

$$s_{da,1}(t) = \mathrm{Tr}_{q^m/q}\left(da\mathrm{Norm}(\alpha^{ct}) + \alpha^t\right).$$

We first represent $s_{da,1}(t)$ in terms of powers of α, and then compute the linear span by counting the number of terms in this representation [15]. We have

$$s_{da,1}(t) = \sum_{j=0}^{m-1}(\alpha^{q^j t}) + a\mathrm{Tr}_{q^m/q}(d)\alpha^{cvt}$$

where $v = (q^m-1)/(q-1)$. Since $q^j \ne cv = c\cdot(q^m-1)/(q-1)$ for $0 \le j \le m-1$, all the terms of the powers of α are pairwise distinct. Thus, the number of terms in the representation is exactly m for $a = 0$ and $m+1$ for $a \ne 0$, which leads to the desired result on the linear span.

If $a = 0$, we have $s_{da,1}(t) = \mathrm{Tr}_{q^m/q}(\alpha^t)$, which is actually an m-sequence.

If $a \ne 0$, we have

$$s_{da,1}(t) = \mathrm{Tr}_{q^m/q}(\alpha^t) + a\mathrm{Tr}_{q^m/q}(d)\alpha^{cvt} = s_1(t) + s_2(t)$$

where $s_1(t) = \mathrm{Tr}_{q^m/q}(\alpha^t)$ and $s_2(t) = a\mathrm{Tr}_{q^m/q}(d)\alpha^{cvt}$.

By [15, Theorem 6.2], $f(x) = f_1(x)f_2(x)$ is the minimal polynomial of the sequence $\mathbf{s}_{da,1}$, where $f_1(x) = m(x)$ for $m(x)$ is an irreducible polynomial over $\mathrm{GF}(q)$ with the root of α and $f_2(x) = x - \alpha^{cv}$. Thus the minimal polynomial is $m(x)\cdot(x - \alpha^{cv})$, which completes the proof. ■

B. Transformed Optimal Sets of FH Sequences

According to Theorem 13, the linear span of the FH sequences in the original construction is very small compared with their length $q^m - 1$. Hereafter we obtain new optimal sets of FH sequences with a power permutation of $\mathrm{GF}(q)$.

Theorem 14: Let σ be a positive integer $0 < \sigma < q-1$ such that $\gcd(\sigma, q-1) = 1$. Assume that $\gcd(cm-1, q-1) =$

1 for $1 \leq c \leq q-2$ and d is an element in GF$(q^m)^*$ with $\mathrm{Tr}_{q^m/q}(d) \neq 0$. For $0 \leq t \leq q^m - 2$, define

$$s^{\sigma}_{da,1}(t) = \left(\mathrm{Tr}_{q^m/q}(da\,\mathrm{Norm}(\alpha^{ct}) + \alpha^{t})\right)^{\sigma}$$

where α is a generator of GF$(q^m)^*$ and $a \in$ GF(q). Then

1) $\mathcal{F}^{\sigma}_{s} = \{\mathbf{s}^{\sigma}_{da,1} : a \in \mathrm{GF}(q)\}$ is a

$$\left(q^m - 1, q, q^{m-1}; q\right)$$

optimal set of FH sequences with respect to the bound of (2). Furthermore, each sequence of the set $\mathcal{F}^{\sigma}_{s}$ for $a \in$ GF(q) is optimal with respect to the bound of Lemma 1.

2) For the transformed FH sequences, if $a = 0$, the linear span is

$$\prod_{i=1}^{w} \binom{m + \sigma_i - 1}{\sigma_i}$$

and if $a \neq 0$, the linear span is

$$\prod_{i=1}^{w} \binom{m + \sigma_i}{\sigma_i}$$

where these σ_i's and w are determined by $\sigma = \sum_{i=1}^{w} \sigma_i p^{e_i}$, $q = p^r$, $0 \leq e_i < r$, $e_i \neq e_j$ if $i \neq j$, and $\binom{x}{y} = x!/y!(x-y)!$ is the binomial coefficient.

Proof:

1) Since $\gcd(\sigma, q-1) = 1$, $\mathbf{s}^{\sigma}_{da,1}$ is a permutation sequence of $\mathbf{s}_{da,1}$. By the definition of Hamming correlation $H(X,Y)$ in (1), the first conclusion of this theorem is obvious.

2) By definition, for $0 \leq t \leq q^m - 2$

$$s^{\sigma}_{da,1}(t) = \left(\mathrm{Tr}_{q^m/q}(\alpha^{t}) + a\mathrm{Tr}_{q^m/q}(d)\alpha^{cvt}\right)^{\sigma}$$

where $\gcd(\sigma, q-1) = 1$, $\sigma = \sum_{i=1}^{w} \sigma_i p^{e_i}$, and $v = (q^m - 1)/(q-1)$.

By properties of the trace function

$$s^{\sigma}_{da,1}(t) = \prod_{i=1}^{w} \left(\mathrm{Tr}_{q^m/q}(\alpha^{p^{e_i}t}) + a^{p^{e_i}}\mathrm{Tr}_{q^m/q}(d)^{p^{e_i}}\alpha^{cvp^{e_i}t}\right)^{\sigma_i}. \tag{15}$$

Using the well-known multinomial formula

$$\left(\sum_{j=1}^{N} a_j\right)^{t} = \sum_{k_1+\cdots+k_N=t} \binom{t}{k_1, \ldots, k_N} {a_1}^{k_1} \ldots {a_N}^{k_N}$$

for $a \neq 0$ we get

$$\begin{aligned}
&\left(\mathrm{Tr}_{q^m/q}(\alpha^{p^{e_i}t}) + a^{p^{e_i}}\mathrm{Tr}_{q^m/q}(d)^{p^{e_i}}\alpha^{cvp^{e_i}t}\right)^{\sigma_i} \\
&= \left(\sum_{j=0}^{m-1} (\alpha^{p^{e_i}t})^{q^j} + a^{p^{e_i}}\mathrm{Tr}_{q^m/q}(d)^{p^{e_i}}\alpha^{cvp^{e_i}t}\right)^{\sigma_i} \\
&= \sum_{\lambda_{i,0}+\cdots+\lambda_{i,m-1}+\lambda_{i,m}=\sigma_i} \binom{\sigma_i}{\lambda_{i,0}, \ldots, \lambda_{i,m-1}, \lambda_{i,m}} \\
&\quad \cdot (\alpha^{p^{e_i}t})^{\sum_{j=0}^{m-1} q^j \lambda_{i,j}} \cdot \left(a^{p^{e_i}}\mathrm{Tr}_{q^m/q}(d)^{p^{e_i}}\alpha^{cvp^{e_i}t}\right)^{\lambda_{i,m}}.
\end{aligned}$$

Then by (15)

$$\begin{aligned}
&s^{\sigma}_{da,1}(t) \\
&= \prod_{i=1}^{w} \sum_{\lambda_{i,0}+\cdots+\lambda_{i,m-1}+\lambda_{i,m}=\sigma_i} \binom{\sigma_i}{\lambda_{i,0}, \ldots, \lambda_{i,m-1}, \lambda_{i,m}} \\
&\quad \cdot (\alpha^{p^{e_i}t})^{\sum_{j=0}^{m-1} q^j \lambda_{i,j}} \cdot (a^{p^{e_i}}\mathrm{Tr}_{q^m/q}(d)^{p^{e_i}}\alpha^{cvp^{e_i}t})^{\lambda_{i,m}}.
\end{aligned}$$

Replacing the product by a w-fold sum, see (16) at the bottom of the page, where

$$\begin{aligned}
g(\boldsymbol{\lambda}, \mathbf{e}) &= \sum_{j=0}^{m-1} q^j \sum_{i=1}^{w} \lambda_{i,j} p^{e_i} + cv \sum_{i=1}^{w} \lambda_{i,m} p^{e_i} \\
&= \sum_{j=0}^{m-1} q^j \left(\sum_{i=1}^{w} (\lambda_{i,j} + c\lambda_{i,m}) p^{e_i}\right)
\end{aligned} \tag{17}$$

and

$$b = \left(a\mathrm{Tr}_{q^m/q}(d)\right)^{\sum_{i=1}^{w} \lambda_{i,m} p^{e_i}}.$$

We now show that all the exponents of α in (16) are pairwise distinct modulo $q^m - 1$. Assume that two different $\boldsymbol{\lambda}$ and $\boldsymbol{\lambda}'$ produce the same exponent of α modulo $q^m - 1$, that is

$$g(\boldsymbol{\lambda}, \mathbf{e}) \equiv g(\boldsymbol{\lambda}', \mathbf{e}) \ (\mathrm{mod} q^m - 1). \tag{18}$$

With (17) and (18), we obtain

$$\begin{aligned}
&\sum_{j=0}^{m-1} q^j \left(\sum_{i=1}^{w} (\lambda_{i,j} + c\lambda_{i,m}) p^{e_i}\right) \\
&\quad \equiv \sum_{j=0}^{m-1} q^j \left(\sum_{i=1}^{w} (\lambda'_{i,j} + c\lambda'_{i,m}) p^{e_i}\right) \ (\mathrm{mod} q^m - 1).
\end{aligned} \tag{19}$$

We consecutively reduce (19) modulo q^j for $j = 1, 2, \ldots, m-1$, then we have

$$\lambda_{i,j} + c\lambda_{i,m} = \lambda'_{i,j} + c\lambda'_{i,m} \tag{20}$$

for $1 \leq i \leq w$ and $0 \leq j \leq m-1$. Adding both sides of the m equations, we have

$$\sum_{j=0}^{m-1} \lambda_{i,j} + cm\lambda_{i,m} = \sum_{j=0}^{m-1} \lambda'_{i,j} + cm\lambda'_{i,m}$$

for $1 \leq i \leq w$. Then

$$\sigma_i - \lambda_{i,m} + cm\lambda_{i,m} = \sigma_i - \lambda'_{i,m} + cm\lambda'_{i,m}$$

therefore $\lambda_{i,m} = \lambda'_{i,m}$ for $1 \leq i \leq w$.

$$s^{\sigma}_{da,1}(t) = \sum_{\sum_{j=0}^{m} \lambda_{1,j}=\sigma_1} \sum_{\sum_{j=0}^{m} \lambda_{2,j}=\sigma_2} \cdots \sum_{\sum_{j=0}^{m} \lambda_{w,j}=\sigma_w} \prod_{i=1}^{w} \binom{\sigma_i}{\lambda_{i,0}, \ldots, \lambda_{i,m-1}, \lambda_{i,m}} \cdot b\alpha^{g(\boldsymbol{\lambda},\mathbf{e})\cdot t} \tag{16}$$

With (20), it follows that $\lambda_{i,j} = \lambda'_{i,j}$ for all $i \in \{1, 2, \ldots, w\}$ and $j \in \{0, 1, \ldots, m\}$. Hence, we complete the proof that all exponents of α in (16) are pairwise distinct.

We now compute the linear span of $\mathbf{s}_{da,1}(t)$ by counting the number of terms in this representation. Since there are

$$\binom{N+\sigma-1}{\sigma}$$

possibilities to represent σ as

$$\sigma = \sum_{j=0}^{N-1} l_j, \qquad \text{for } 0 \leq l_j \leq \sigma$$

and by applying this result to all σ_i's, the linear span is

$$\mathrm{LS} = \prod_{i=1}^{w} \binom{m+1+\sigma_i-1}{\sigma_i} = \prod_{i=1}^{w} \binom{m+\sigma_i}{\sigma_i},$$

which leads to the desired result. For the case $a = 0$, the proof is similar to the process above. ■

Corollary 15: If the exponent $\sigma = p^r - p^j - 1$ for $0 \leq j < r$, the FH sequences transformed by the power permutation have the possible largest linear span. More precisely, if $a = 0$, the linear span is

$$\mathrm{LS} = \binom{m+p-2}{p-1}^{r-1} \binom{m+p-3}{p-2}$$

and if $a \neq 0$, the linear span is

$$\mathrm{LS} = \binom{m+p-1}{p-1}^{r-1} \binom{m+p-2}{p-2}.$$

Proof: The conclusion of this corollary follows from that of Corollary 6. ■

Remark 3: According to Corollary 15, if the power σ is chosen properly, the linear span of the sequences in the transformed optimal set could be very large. For example, let $q = 3^3$, $m = 3$, $c = 4$ and $d = 1$, the linear span of the sequence in $\mathcal{F}_s$ when $a = 0$ is only 3, and the linear span of all the other sequences in $\mathcal{F}_s$ is only 4. However, if we choose $\sigma = 17$, the linear span of the sequence in $\mathcal{F}_s^{\sigma}$ when $a = 0$ is 108, and the linear span of all the other sequences in $\mathcal{F}_s^{\sigma}$ is 400.

V. Concluding Remarks

With proper power permutations, the transformed optimal sets of FH sequences from the three earlier constructions could have large linear spans. All the FH sequences in these transformed optimal sets are also easy to implement. It is also noted that other types of permutation polynomials over GF(q) may be employed in the same way for improving the linear spans of FH sequences in some optimal sets. But calculating the linear spans of the transformed sequences may not be easy.

Acknowledgment

The author is grateful to the three anonymous reviewers for their detailed suggestions and comments that much improved the presentation and quality of this paper.

References

[1] C. Ding and J. Yin, "Sets of optimal frequency hopping sequences," *IEEE Trans. Inf. Theory*, vol. IT-54, pp. 3741–3745, 2008.

[2] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*. New York: McGraw-Hill, 2002.

[3] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-20, pp. 90–94, 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. IT-50, pp. 2149–2154, 2004.

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

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

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

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

[9] G. Ge, Y. Miao, and Z. Yao, "Optimal frequency hopping sequences: Auto- and cross-correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-55, pp. 867–879, 2009.

[10] J. J. Komo and S. C. Liu, "Maximal length sequences for frequency hopping," *IEEE J. Sel. Areas Commun.*, vol. 5, pp. 819–822, 1990.

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

[12] P. Udaya and M. N. Siddiqi, "Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings," *IEEE Trans. Inf. Theory*, vol. IT-44, pp. 1492–1503, 1998.

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

[14] M. Antweiler and L. Bömer, "Complex sequences over $GF(p^M)$ with a two-level autocorrelation function and a large linear span," *IEEE Trans. Inf. Theory*, vol. IT-38, pp. 120–130, 1992.

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

[16] A. Pott, *Finite Geometry and Character Theory (Lecture Notes in Mathematics)*. Berlin, Germany: Springer-Verlag, 1995, vol. 1601.

Qi Wang (S'10) was born in Shandong, China, in 1985. He received the B.Eng. degree in information security from the University of Science and Technology of China in 2007. Currently, he is the Ph.D. degree candidate with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology.

His research interests include cryptography and coding theory.