Sets of Frequency Hopping Sequences: Bounds and Optimal Constructions

Cunsheng Ding, *Senior Member, IEEE*, Ryoh Fuji-Hara, Yuichiro Fujiwara, Masakazu Jimbo, and Miwako Mishima

***Abstract*—Frequency hopping spread spectrum and direct sequence spread spectrum are two main spread coding technologies in communication systems. Frequency hopping sequences are needed in frequency hopping code-division multiple-access (FH-CDMA) systems. In this paper, four algebraic and a combinatorial constructions of optimal sets of frequency hopping sequences with new parameters are presented, and a number of bounds on sets of frequency hopping sequences are described.**

***Index Terms*—Cyclotomy, direct sequence spread spectrum(DS-SS), frequency hopping sequence, frequency hopping spread spectrum.**

I. Introduction

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

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

where $h[a, b] = 1$ if $a = b$, and 0 otherwise, and all operations among the position indices are performed modulo n. For any distinct $X, Y \in \mathcal{S}$, we define the following three measures:

$$H(X) = \max_{1 \le t < n} \{H_{X,X}(t)\}$$

$$H(X,Y) = \max_{0 \le t < n} \{H_{X,Y}(t)\}$$

$$M(X,Y) = \max\{H(X), H(Y), H(X,Y)\}.$$

In 1974, Lempel and Greenberger developed the following lower bound for $H(X)$ [15].

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

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

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

Let $\mathcal{F}$ be a subset of $\mathcal{S}$ containing N sequences. The maximum nontrivial Hamming correlation of the 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, we use $(n, N, \lambda; \ell)$ to denote a set of N frequency hopping sequences $\mathcal{F}$ of length n over an alphabet of size ℓ, where $\lambda = M(\mathcal{F})$.

Peng and Fan described the following bounds on $M(\mathcal{F})$, which take into consideration the number of sequences in the set $\mathcal{F}$.

Lemma 2: [20, Corollary 1] Let $\mathcal{F} \subseteq \mathcal{S}$ be a set of N 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

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

In this paper, 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 one of the bounds in Lemma 2 or Section II-B is met.

Lempel and Greenberger defined optimality for both single sequences and sets of sequences in other ways. A set of frequency hopping sequences meeting one of the bounds in Lemma 2 must be optimal in the Lempel-Greenberger sense. In communication systems, frequency hopping spread spectrum and direct sequence spread spectrum are two main spread coding technologies. Both have advantages and disadvantages. Frequency hopping sequences are an integral part of spread-spectrum communication systems such as frequency hopping code-division

Manuscript received December 15, 2008. Current version published June 24, 2009. The work of C. Ding was supported by the Research Grants Council of the Hong Kong Special Administrative Region, China, Project No.612609. The work of M. Jimbo was supported in part by JSPS Scientific Research (B)18340024 and by Monbu Kagakusho Exploratory Research 20654012. The work of M. Mishima was supported in part by JSPS Scientific Research (C)19500236. The material in this paper was presented in part at the Tenth International Workshop on Algebraic and Combinatorial Coding Theory, Zvenigorod, Russia, September 2006.

C. Ding 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: cding@ust.hk).

R. Fuji-Hara and Y. Fujiwara with the Graduate School of System and Information Engineering, University of Tsukuba, Tsukuba, Ibaraki, Japan (e-mail: fujihara@sk.tsukuba.ac.jp; yuichiro.fujiwara@gmail.com).

M. Jimbo is in the Graduate School of Information Science, Nagoya University, Chikusa-ku, Nagoya, 464-8601, Japan (e-mail: jimbo@is.nagoya-u.ac.jp).

M. Mishima is with the Department of Information Science, Gifu University, Gifu 501-1193, Japan (e-mail: miwako@gifu-u.ac.jp).

Communicated by M. G. Parker, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2009.2021366

TABLE I
KNOWN OPTIMUM SETS OF FREQUENCY HOPPING SEQUENCES

Length v	Alphabet size	H_{max}	Set size	Ref
p^r-1	$p^u, 0<u\le r$	$p^{r-u}-1$	p^u	[15]
p^2	p	p	p	[14]
p, odd prime	$e+1$, where $e\|(p-1)$	$\frac{p-1}{e}$	e	[1]
$\frac{q^m-1}{2}$, m odd	q	$\frac{q^{m-1}-1}{2}$	2	[4]
q^m-1	q	q^{m-1}	q	[4]
$q-1$, where q prime power	$e+1$, where $e\|(q-1)$	$\frac{q-1}{e}$	e	[5]
$\frac{q^m-1}{q-1}$, where q prime power $\gcd(q-1,m)=1$	q	$\frac{q^{m-1}-1}{q-1}$	$q-1$	[5]

multiple-access (FH-CDMA) systems (for a description of such systems, see [21]). In multiple access frequency hopping packet radio networks each transmitter is assigned a unique signature sequence for controlling the frequencies used by the radios for consecutive packets within a frame. Assuming frame asynchronism and packet synchronism, whenever two or more radios transmit their packets simultaneously in the same frequency, the collided packets are capable of destroying each other. To maximize the throughput, we have to minimize the number of such coincidences between the signature sequences. As the number of such coincidences is the Hamming correlation, we need to use a set of signature sequences with good Hamming correlation and large size. Periodic Hamming correlation is considered in almost all papers, as this allows people to derive theoretical results, although aperiodic Hamming correlation matters in real applications.

It is relatively easy to construct single optimal frequency hopping sequences with respect to the bound of Lemma 1. Both algebraic and combinatorial constructions of such sequences were developed (see, for example, [1], [4], [5], [10], [11], [13]–[15], [25]). However, only a few constructions of optimal sets of frequency hopping sequences are known. Table I describes the parameters of known optimal sets of frequency hopping sequences. One objective of this paper is to present four algebraic constructions of optimal sets of frequency hopping sequences with new parameters.

The only bounds on sets of frequency hopping sequences documented in the literature are those of Lemma 2. Another objective of this paper is to describe other bounds on sets of frequency hopping sequences.

II. BOUNDS ON SETS OF FREQUENCY HOPPING SEQUENCES FROM CODING THEORY

In this section, we first make a connection between sets of frequency hopping sequences and cyclic error correcting codes, and then describe several bounds on sets of frequency hopping sequences. These bounds are different from the bounds of Lemma 2, and are not stated in the literature on frequency hopping sequences. The objective of this section is to make the bounds known to the reader, although they are easily obtained by modifying bounds on error correcting codes.

A. Some Bounds on Error Correcting Codes

Let $F=\{f_0,f_1,\ldots,f_{\ell-1}\}$ be an abelian group of size ℓ. Define

$$F^n=\{(s_0,s_1,s_2,\ldots,s_{n-1}): s_i\in F \text{ for all } i\}.$$

The Hamming weight of a vector in F^n is the total number of nonzero coordinates in the vector. The Hamming distance between two vectors in F^n is the total number of coordinate positions in which they differ.

An $(n,M,d;\ell)$ code is an M-subset of the space F^n with minimum Hamming distance d. An $(n,M,d,w;\ell)$ constant weight code is a code over an abelian group (alphabet) F of ℓ elements with length n, size M and minimum distance d such that the Hamming weight of each codeword is w. A code is called *equidistant* if the distance between every pair of distinct codewords is the same. An $[n,k,d;\ell]$ code is a linear subspace of GF$(\ell)^n$ with dimension k such that the minimum Hamming distance between all pairs of distinct codewords is d.

Let $A_\ell(n,d)$ denote the largest number of codewords in any ℓ-ary code of length n and minimum distance at least d. Let $A_\ell(n,d,w)$ denote the maximum number M of codewords in a constant weight code over an alphabet of size ℓ with length n, minimum distance at least d, and weight w (called an $(n,M,d,w;\ell)$ constant weight code). The first generalized Johnson bound on constant weight codes is the following:

$$A_\ell(n,d,w)\le\left\lfloor\frac{n(\ell-1)}{w}\left\lfloor\frac{(n-1)(\ell-1)}{w-1}\left\lfloor\cdots\right\rfloor\right\rfloor\right\rfloor. \tag{4}$$

The second generalized Johnson bound on constant weight codes is the following [7]:

$$A_\ell(n,d,w)\le\frac{n(\ell-1)d}{\ell w^2-2(\ell-1)nw+n(\ell-1)d} \tag{5}$$

provided that $\ell w^2-2(\ell-1)nw+n(\ell-1)d>0$. For nonbinary constant weight codes, we have the following known exact values of or lower bounds on $A_\ell(n,d,w)$:

- $A_3(n,3,3)=\frac{2n(n-1)}{3}$ for $n\equiv 0,1(\mathrm{mod}\ 3), n\ge 4$ [6].
- $A_3(n,3,3)=\frac{2n(n-1)-4}{3}$ for $n\equiv 2(\mathrm{mod}\ 3), n\ge 5$ [18].
- $A_3(n,3,4)\ge\lfloor\frac{n^3-5n^2+6n}{3}\rfloor$, if $n\ge 4$ [8].
- $A_3(n,3,w)\ge\frac{1}{2n+1}\binom{n}{w}2^w$ [23].
- $A_3(n,3,w)\ge\frac{1}{2n}\binom{n}{w}2^w$, if $n\equiv 0,1(\mathrm{mod}\ 4)$ [8].
- $A_3(2^r-1,3,2^r-2)=(2^r-1)2^{2^r-r-2}$ for $r\ge 2$ [24].
- $A_3(2^r-2,3,2^r-3)=(2^{r-1}-1)2^{2^r-r-2}$ for $r\ge 2$ [24].
- $A_3(2^r,3,2^r-1)=2^{2^r-1}$ for $r\ge 2$ [24].
- $A_3(q,\frac{q+3}{2},q-1)=q$, where q is a power of odd prime [7].
- $A_3(q\frac{q^m-1}{q-1},q^{m-1}\frac{q+3}{2},q^m-1)=q^m$, where q is a power of odd prime [7].
- $A_3(p^m+1,\frac{p^m+3}{2},p^m)=2p^m+2$, where $p\ge 3$ is a prime [19].
- $A_\ell(n,2,w)=\binom{n}{w}(\ell-1)^w$ [7].
- $A_q(\frac{q^m-1}{q-1},q^{m-1},q^{m-1})=q^m-1$, where q is a prime power [7].

- $A_q(q+1, \frac{q+1}{2}, q) \geq 2q+2$, where $q = p^m$ [7].
- $A_\ell(n, d, w) = 1$ if $d > 2w$ and $0 \leq w \leq n$.
- $A_\ell(n, 2w, w) = \lfloor \frac{n}{w} \rfloor$ [7].
- $A_\ell(n, d, n) = A_{\ell-1}(n, d)$ [19].

The Johnson bound for $A_\ell(n, d)$ is described in the following lemma [12].

Lemma 3: If $d = 2t+1$

$$A_\ell(n,d) \leq \frac{\ell^n}{\sum_{i=0}^{t} \binom{n}{i} (\ell-1)^i + \frac{\binom{n}{t+1}(\ell-1)^{t+1} - \binom{d}{t} A_\ell(n,d,d)}{A_\ell(n,d,t+1)}}. \quad (6)$$

If $d = 2t$

$$A_\ell(n,d) \leq \frac{\ell^n}{\sum_{i=0}^{t} \binom{n}{i} (\ell-1)^i + \frac{\binom{n}{t+1}(\ell-1)^{t+1}}{A_\ell(n,d,t+1)}}. \quad (7)$$

In the next section, we shall use those bounds to derive bounds on sets of FH sequences.

B. Coding Theory Bounds on Sets of FH Sequences

For any given set $\mathcal{F}$ of FH sequences with parameters $(n, N, \lambda; \ell)$, where $\lambda = M(\mathcal{F}) < n$, an $(n, nN, n-\lambda; \ell)$ code $\mathcal{C}_\mathcal{F}$ is obtained by putting all the sequences in $\mathcal{F}$ and all their cyclically shifted versions together. Hence bounds on error correcting codes give automatically bounds on sets of frequency hopping sequences.

The following bound follows from the Singleton bound on error correcting codes [16, p. 92].

Theorem 4: (The Singleton bound on FH sequences) For any set $\mathcal{F}$ of FH sequences with parameters $(n, N, \lambda; \ell)$; where $\lambda < n$ and $\ell > 1$, we have

$$N \leq \left\lfloor \frac{\ell^{\lambda+1}}{n} \right\rfloor. \quad (8)$$

In Section VI, we will present sets of FH sequences meeting this Singleton bound. The following bound follows from the Plotkin bound on error correcting codes [16, p. 95].

Theorem 5: (The Plotkin bound on FH sequences) For any set $\mathcal{F}$ of FH sequences with parameters $(n, N, \lambda; \ell)$, where $\ell\lambda < n$ and $\ell > 1$, we have

$$N \leq \left\lfloor \frac{1}{n} \left\lfloor \frac{\ell(n-\lambda)}{n-\ell\lambda} \right\rfloor \right\rfloor. \quad (9)$$

The following bound follows from the sphere-packing bound on error correcting codes [16, p. 83].

Theorem 6: (The sphere-packing bound on FH sequences) For any set $\mathcal{F}$ of FH sequences with parameters $(n, N, \lambda; \ell)$, where $\lambda < n$ and $\ell > 1$, we have

$$N \leq \left\lfloor \frac{\ell^n}{n\left(\sum_{i=0}^{\lfloor (n-\lambda-1)/2 \rfloor} \binom{n}{i} (\ell-1)^i\right)} \right\rfloor. \quad (10)$$

In Section VII, we will present sets of FH sequences meeting this sphere-packing bound. The following theorem describes the Johnson bounds on sets of FH sequences which follow from the bounds of Lemma 3.

Theorem 7: Let $\mathcal{F}$ be any set of FH sequences with parameters $(n, N, \lambda; \ell)$. If $n - \lambda = 2t+1$, see (11) at the bottom of the page.

If $n - \lambda = 2t$

$$N \leq \left\lfloor \frac{\ell^n}{\sum_{i=0}^{t} n \binom{n}{i} (\ell-1)^i + n\frac{\binom{n}{t+1}(\ell-1)^{t+1}}{A_\ell(n,2t,t+1)}} \right\rfloor. \quad (12)$$

The bounds in Theorem 7 involve $A_\ell(n, d, w)$ and are not specific. However, plugging the bounds on $A_\ell(n, d, w)$ described in Section II-A into the bounds of Theorem 7 yields various bounds on sets of FH sequences. We leave the details to the reader. The linear programming bound on error correcting codes yields similar bound on sets of frequency hopping sequences. We will demonstrate in subsequent sections that the bounds described in this section are useful, as they can be achieved by certain sets of FH sequences.

III. Cyclotomic Classes and Gaussian Periods

Throughout this section, let $q = p^s$ and $r = q^m$, where p is a prime, s and m are positive integers. Let $r - 1 = nN$ for two positive integers $n > 1$ and $N > 1$, and let α be a

$$N \leq \left\lfloor \frac{\ell^n}{\sum_{i=0}^{t} n \binom{n}{i} (\ell-1)^i + n\frac{\binom{n}{t+1}(\ell-1)^{t+1} - \binom{2t+1}{t} A_\ell(n,2t+1,2t+1)}{A_\ell(n,2t+1,t+1)}} \right\rfloor. \quad (11)$$

fixed generator of GF$(r)^*$. Define $C_i^{(N,r)} = \alpha^i\langle\alpha^N\rangle$ for $i = 0, 1, \ldots, N-1$, where $\langle\alpha^N\rangle$ denotes the subgroup of GF$(r)^*$ generated by α^N. The cosets $C_i^{(N,r)}$ are called the *cyclotomic classes* of order N in GF(r). The *cyclotomic numbers* of order N are defined by

$$(i,j)^{(N,r)} = \left|\left(C_i^{(N,r)} + 1\right) \cap C_j^{(N,r)}\right|$$

for all $0 \le i \le N-1$ and $0 \le j \le N-1$. The *Gaussian periods* are defined by

$$\eta_i^{(N,r)} = \sum_{x \in C_i^{(N,r)}} \chi(x), \quad i = 0, 1, \ldots, N-1$$

where χ is the canonical additive character of GF(r). In general, it is hard to determine the values of the Gaussian periods [22]. However, it can be done in certain cases. In the sequel, we will need the following lemma [17].

Lemma 8: Suppose there exists a positive integer j such that $p^j \equiv -1 (\mathrm{mod}\ N)$, and let j be the least such. Let $r = p^{ms}$, where $ms = 2j\gamma$. Then the Gaussian periods are given below.

1) If γ, p and $(p^j+1)/N$ are all odd, then $\eta_{N/2}^{(N,r)} = ((N-1)p^{j\gamma}-1)/N$ and $\eta_i^{(N,r)} = (-p^{j\gamma}-1)/N$ for all $i \ne N/2$.
2) In all other cases, $\eta_0^{(N,r)} = ((-1)^{\gamma+1}(N-1)p^{j\gamma}-1)/N$ and $\eta_i^{(N,r)} = ((-1)^{\gamma}p^{j\gamma}-1)/N$ for all $i \ne 0$.

IV. The First Construction of Optimal Sets of Frequency Hopping Sequences

In this section, let $p = 2, q = p^s$ and $r = q^4$, where s is a positive integer. Define $N = q^2 - 1$ and $n = q^2 + 1$. Let α be a generator of GF$(r)^*$. Define $g = \alpha^N$. For each $0 \le i \le N-1$, we define the following sequence;

$$S_i^{(q)}(t) = \mathrm{Tr}_{r/q}(\alpha^i g^t), \quad 0 \le t \le n-1 \tag{13}$$

where $\mathrm{Tr}_{r/q}$ is the trace function from GF(r) to GF(q). Each $S_i^{(q)}$ is a sequence of length n over the alphabet GF(q). We then define

$$\mathcal{S}^{(q)} = \left\{S_i^{(q)} : 0 \le i \le N-1\right\}. \tag{14}$$

Theorem 9: The $\mathcal{S}^{(q)}$ of (14) is a $(q^2+1, q^2-1, q+1; q)$ set of frequency hopping sequences over the alphabet GF(q), meeting the Peng–Fan bound of (3).

Proof: We first prove that

$$\cup_{y \in \mathrm{GF}(q)^*} yC_0^{(N,r)} = C_0^{(q+1,r)}.$$

Note that any $y \in$ GF$(q)^*$ can be expressed as

$$y = \alpha^{(q^3+q^2+q+1)t} = \alpha^{(q^2-1)(q+1)t+2(q+1)t}$$

for some t with $0 \le t \le q-2$. Hence

$$\cup_{y \in \mathrm{GF}(q)^*} yC_0^{(N,r)} \subseteq C_0^{(q+1,r)}.$$

On the other hand, since $\gcd(2, q-1) = 1$, we have

$$\mathrm{GF}(q)^* \cap C_0^{(N,r)} = \{1\}.$$

It then follows that $\cup_{y \in \mathrm{GF}(q)^*} yC_0^{(N,r)} = C_0^{(q+1,r)}$. By Lemma 8, we have

$$\eta_i^{(q+1,r)} = q-1 \text{ for all } i \ne 0, \quad \eta_0^{(q+1,r)} = -q^2+q-1.$$

Finally, define

$$\Delta_a = |\{i \in \mathbf{Z}_n : \mathrm{Tr}_{r/q}(ag^i) = 0\}|$$

for each nonzero $a \in \mathbf{Z}_n := \{0, 1, 2, \ldots, n-1\}$. Let $\chi(x) = (-1)^{\mathrm{Tr}_{r/p}(x)}$ be the additive character on GF(r). Furthermore, for any subset T of GF(r), we define

$$\chi(T) = \sum_{y \in T} \chi(y).$$

For any $0 \le \tau \le n-1$, using the results proved above we have then

$$\begin{aligned}
\Delta_a &= \frac{1}{q}\sum_{i=0}^{n-1}\sum_{y \in \mathrm{GF}(q)} (-1)^{\mathrm{Tr}_{q/p}[y\mathrm{Tr}_{r/q}(ag^i)]} \\
&= \frac{1}{q}\sum_{i=0}^{n-1}\sum_{y \in \mathrm{GF}(q)} \chi(yag^i) \\
&= \frac{1}{q}\left[n + \sum_{y \in \mathrm{GF}(q)^*} \chi\left(ayC_0^{(N,r)}\right)\right] \\
&= \frac{1}{q}\left[n + \chi\left(aC_0^{(q+1,r)}\right)\right] \\
&= \begin{cases} 1, & \text{if } a \in C_0^{(q+1,r)} \\ q+1, & \text{otherwise.} \end{cases}
\end{aligned} \tag{15}$$

For any $0 \le i \le N-1, 0 \le j \le N-1$ and $0 \le t \le n-1$, by (1) we have

$$H_{S_i^{(q)}, S_j^{(q)}}(t) = |\{k \in \mathbf{Z}_n : \mathrm{Tr}_{r/q}((\alpha^i - \alpha^j g^t)g^k) = 0\}|$$

where $1 \le t \le n-1$ if $i = j$ and $0 \le t \le n-1$ if $i \ne j$. These conditions on i, j and t guarantee that $\alpha^i - \alpha^j g^t \ne 0$. It then follows from (15) that $M(\mathcal{S}^{(q)}) = q+1$. This also proved that the size of $\mathcal{S}^{(q)}$ is $N = q^2 - 1$.

It is straightforward to check that the Peng–Fan bound of (3) is met. This completes the proof. □

Example 1: Let $q = 2^2$ and $r = q^4$. Let α be the generator of GF$(q^4)^*$ defined by $\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$, and define $u = \alpha^{85}$. Then u is a generator of GF$(2^2)^*$ defined by $u^2 + u + 1 = 0$. Then the set $\mathcal{S}^{(q)}$ consists of the following 15 frequency hopping sequences of length 17:

$$[0, u^2, u, 1, u^2, 1, 1, 1, u, u, 1, 1, 1, u^2, 1, u, u^2]$$
$$[1, 1, 1, 0, u^2, 0, u, u^2, u^2, 0, u^2, u^2, u, 0, u^2, 0, 1]$$
$$[1, 0, 1, u, 1, u, 0, u^2, u, 0, 0, u, u^2, 0, u, 1, u]$$
$$[1, u^2, u^2, 1, u^2, u, u, 0, 0, u^2, 0, u^2, 0, 0, u, u, u^2]$$

$[1,0,0,0,1,u^2,u^2,u,1,0,u^2,u^2,0,1,u,u^2,u^2]$
$[u^2,u^2,1,1,u^2,u^2,u^2,u,u^2,1,u,0,u,1,u^2,u,u^2]$
$[1,u,u,0,u,u,1,0,u,0,u^2,u^2,u^2,u^2,0,u,0]$
$[0,u,1,0,0,1,u,0,1,u^2,1,u^2,0,u^2,1,u^2,1]$
$[1,0,0,u,0,u,0,0,1,1,u,u^2,u,u,u^2,u,1]$
$[u,1,u^2,0,u,u,0,u^2,1,u,u,u^2,0,0,0,u^2,u]$
$[u,1,u,u^2,1,0,1,u^2,u,1,u,u,u,u^2,u^2,u,u]$
$[u^2,0,1,0,u,u,u,u,0,1,0,u^2,1,1,0,1,1]$
$[1,0,u^2,u,u^2,u,0,u,u^2,u,u^2,0,1,u^2,0,0,u^2]$
$[0,0,u^2,u^2,1,u,1,1,u,1,u^2,u^2,0,0,1,0,1]$
$[0,u,u^2,1,1,u,0,0,0,u,1,1,u^2,u,0,1,1].$

V. The Second Construction of Optimal Sets of Frequency Hopping Sequences

In this section, let p be an odd prime, $q=p^s$ and $r=q^m$, where s and m are positive integers. Let N be a positive divisor of $r-1$ and $n=(r-1)/N$. Let α be a generator of GF$(r)^*$. Define $g=\alpha^N$. For each $0\le i\le N-1$, we define the following sequence:

$$S_i^{(q,m)}(t)=\mathrm{Tr}_{r/q}(\alpha^i g^t),\quad 0\le t\le n-1 \tag{16}$$

where $\mathrm{Tr}_{r/q}$ is the trace function from GF(r) to GF(q). Each $S_i^{(q,m)}$ is a sequence of length n over the alphabet GF(q). We then define

$$\mathcal{S}^{(q,m)}=\left\{S_i^{(q,m)}: 0\le i\le N-1\right\}. \tag{17}$$

Theorem 10: If N is even, $\gcd(n,N)=1, q-1\equiv N/2 (\mathrm{mod}\ N)$ and $\gcd((r-1)/(q-1) \bmod N, N)=2$, the $\mathcal{S}^{(q,m)}$ of (17) is a $((r-1)/N, N, (r-q+(q-1)\sqrt{r})/(qN); q)$ set of frequency hopping sequences over the alphabet GF(q). Furthermore, if

$$N>\frac{q-1}{q}\sqrt{r} \tag{18}$$

the set $\mathcal{S}^{(q,m)}$ of FH sequences in (17) is optimal with respect to the Peng–Fan bound of (3).

Proof: Let $Z(r,a)$ denote the number of solutions $x\in$ GF(r) of the equation $\mathrm{Tr}_{r/q}(ax^N)=0$. Let $\epsilon_p=e^{2\pi\sqrt{-1}/p}$, and $\chi(x)=\epsilon_p^{\mathrm{Tr}_{r/p}(x)}$. Then χ is an additive character of GF(r). The following is well known [3]:

$$\chi\left(C_0^{(2,r)}\right)=\frac{-1\pm\sqrt{r}}{2},\ \chi\left(C_1^{(2,r)}\right)=\frac{-1\mp\sqrt{r}}{2}. \tag{19}$$

We have then

$$\begin{aligned}Z(r,a)&=\frac{1}{q}\sum_{y\in \mathrm{GF}(q)}\sum_{x\in\mathrm{GF}(r)}\epsilon_p^{\mathrm{Tr}_{q/p}(y\mathrm{Tr}_{r/q}(ax^N))}\\&=\frac{1}{q}\sum_{y\in \mathrm{GF}(q)}\sum_{x\in\mathrm{GF}(r)}\chi(yax^N)\\&=\frac{1}{q}\left[q+r-1+\sum_{y\in\mathrm{GF}(q)^*}\sum_{x\in\mathrm{GF}(r)^*}\chi(yax^N)\right]\\&=\frac{1}{q}\left[q+r-1+N\sum_{y\in\mathrm{GF}(q)^*}\sum_{x\in C_0^{(N,r)}}\chi(yax)\right].\end{aligned} \tag{20}$$

The condition that $\gcd((r-1)/(q-1) \bmod N, N)=2$ implies that m is even and q is odd. Let α be the generator of GF(r). Since $\gcd((r-1)/(q-1) \bmod N, N)=2$ and $q-1\equiv N/2 (\mathrm{mod}\ N)$, each cyclotomic class $C_{2i}^{(N,r)}$ contains exactly $2(q-1)/N$ elements of GF$(q)^*$, and each cyclotomic class $C_{2i+1}^{(N,r)}$ does not contain any element of GF$(q)^*$.

Let $a\in C_h^{(2,r)}$. It then follows from (20) and (19) that

$$\begin{aligned}Z(r,a)&=\frac{1}{q}\left[q+r-1+N\frac{2(q-1)}{N}\sum_{x_3\in C_0^{(2,r)}}\chi(ax_3)\right]\\&=\frac{1}{q}\left[q+r-1+2(q-1)\sum_{x_3\in C_h^{(2,r)}}\chi(x_3)\right]\\&=\frac{r\pm(q-1)\sqrt{r}}{q}.\end{aligned} \tag{21}$$

Hence, for any $\beta\in$ GF$(r)^*$ the Hamming weight of the vector

$$(\mathrm{Tr}_{r/q}(\beta),\mathrm{Tr}_{r/q}(\beta g),\ldots,\mathrm{Tr}_{r/q}(\beta g^{n-1}))$$

is equal to

$$n-\frac{Z(r,\beta)-1}{N}=\frac{(q-1)(r\mp\sqrt{r})}{qN}.$$

For any $0\le i\le N-1, 0\le j\le N-1$ and $0\le t\le n-1$, by (1)

$$H_{S_i^{(q,m)},S_j^{(q,m)}}(t)=|\{k\in\mathbf{Z}_n:\mathrm{Tr}_{r/q}((\alpha^i-\alpha^j g^t)g^k)=0\}|$$

where $1\le t\le n-1$ if $i=j$ and $0\le t\le n-1$ if $i\ne j$. These conditions on i,j and t guarantee that $\alpha^i-\alpha^j g^t\ne 0$. It then follows from (21) that $M(\mathcal{S}^{(q,m)})=(r-q+(q-1)\sqrt{r})/(qN)$. This also proved that the size of $\mathcal{S}^{(q,m)}$ is N.

It is straightforward to check that the Peng–Fan bound of (3) is met, if (18) is satisfied. □

The following example demonstrates that the construction of this section does produce optimal sets of FH sequences.

Example 2: Let $q\equiv 1(\mathrm{mod}\ 4), m=2, N=2(q-1)$. We have then $n=(q+1)/2$. It is easily checked that $\gcd(n,N)=1$ and

$$q-1\equiv\frac{N}{2}(\mathrm{mod}\ N),\quad \gcd((r-1)/(q-1),N)=2.$$

Then the $\mathcal{S}^{(q,m)}$ of (17) is a $((q+1)/2, 2(q-1), 1; q)$ set of frequency hopping sequences over the alphabet GF(q).

The condition of (18) is obviously satisfied. Hence this set of FH sequences is optimal with respect to the Peng–Fan bound of (3). Note that this set of FH sequences is also optimal with respect to the Singlton bound of (8).

VI. The Third Construction of Optimal Sets of Frequency Hopping Sequences

As made clear in Section II-B, any set $\mathcal{F}$ of FH sequences with parameters $(n, N, \lambda; \ell)$, where $\lambda = M(\mathcal{F}) < n$ gives automatically an $(n, nN, n-\lambda; \ell)$ cyclic code $\mathcal{C}_{\mathcal{F}}$. However, when a cyclic code is given, constructing a set of FH sequences using this cyclic code is not automatic and it varies from case to case. In this section, we use a subset of the Reed–Solomon code to construct a set of FH sequences meeting the Singleton bound of (8).

We first describe a subset of the Reed–Solomon code. Let q be a prime power, and let k be an integer with $1 \leq k \leq q-2$. Define

$$\mathrm{GF}(q)[x]_k = \left\{ \sum_{i=1}^{k} g_i x^i : g_i \in \mathrm{GF}(q), i = 0, 1, \ldots, k-1 \right\}. \tag{22}$$

Define $n = q-1$ and

$$\mathcal{C}_{\mathrm{RS}} = \{(g(1), g(\alpha), \ldots, g(\alpha^{n-1})) : g(x) \in \mathrm{GF}(q)[x]_k\}$$

where α is a generator of $\mathrm{GF}(q)^*$. It is well known that the code $\mathcal{C}_{\mathrm{RS}}$ has parameters $[n, k, d = n-k+1; q]$ and is cyclic.

Two codewords of $\mathcal{C}_{\mathrm{RS}}$ are said to be *equivalent* if one is the cyclic shift of the other. The codewords of $\mathcal{C}_{\mathrm{RS}}$ are now classified into equivalence classes. There is an equivalence classes $\{(0, 0, \ldots, 0)\}$ of

$$\{(a, a, \ldots, a)\}.$$

$a \in (q)$. Such equivalence class are said to be *trivial*. When $q-1$ is a prime number, it is easily seen that each of the remaining $(q^k-1)/(q-1)$ equivalence classes has exactly n codewords. Taking one and only one codeword from each of the remaining $(q^k-1)/(q-1)$ equivalence classes, we form a set $\mathcal{S}_{\mathrm{RS}}$ of $(q^k-1)/(q-1)$ FH sequences with parameters $(q-1, (q^k-q)/(q-1), k-1; q)$. This is because of the following:

- the code $\mathcal{C}_{\mathrm{RS}}$ has minimum distance $d = n-k+1$;
- $\mathcal{S}_{\mathrm{RS}}$ is a subset of the code $\mathcal{C}_{\mathrm{RS}}$; and
- any two sequences in $\mathcal{S}_{\mathrm{RS}}$ are not equivalent.

It is straightforward to verify that the set $\mathcal{S}_{\mathrm{RS}}$ of FH sequences meets the Singleton bound of (8). This proves the following theorem.

Theorem 11: Assume that q is a prime power and $q-1$ is a prime. The set $\mathcal{S}_{\mathrm{RS}}$ of FH sequences has parameters $(q-1, (q^k-1)/(q-1), k-1; q)$ and meets the Singleton bound of (8).

If $q-1$ is a prime, it must be of the format 2^s-1, where s is a positive integers. Primes of this format are called *Mersenne primes*. For example, 2^s-1 is a prime when $s = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257. The largest known Mersenne primes are $2^{43112609}-1$ and $2^{37156667}-1$.

VII. The Fourth Construction of Optimal Sets of Frequency Hopping Sequences

In this section, we use a subset of a cyclic code to construct a set of FH sequences meeting the sphere-packing bound of (10).

We first describe the cyclic linear code. Let q be a prime power, and let m be a positive integer such that $\gcd(m, q-1) = 1$. Define $n = (q^m-1)/(q-1)$. Let α be a generator of $\mathrm{GF}(q)^*$, and let $g = \alpha^{q-1}$. Define a cyclic linear code by

$$\mathcal{C}_{(q,m)} = \{c(x) : c(x) \in \mathrm{GF}(q)[x] \text{ and } c(g) = 0\}$$

where $\mathrm{GF}(q)[x]_n$ consists of all polynomials of degree at most $n-1$ over $\mathrm{GF}(q)$. It is known that $\mathcal{C}_{(q,m)}$ is equivalent to the $[n, n-m, 3; q]$ Hamming code [26, p. 92].

Two codewords of $\mathcal{C}_{(q,m)}$ are said to be *equivalent* if one is the cyclic shift of the other. The codewords of $\mathcal{C}_{(q,m)}$ are now classified into equivalence classes. There are clearly q trivial equivalence classes of the form $\{(a, a, \ldots, a)\}$. When n is a prime, it is easily seen that each of the remaining $(q^{n-m}-q)/n$ nontrivial equivalence classes has exactly n codewords. Taking one and only one codeword from each of the remaining $(q^{n-m}-q)/n$ equivalence classes, we form a set $\mathcal{S}_{(H,q,m)}$ of $(q^{n-m}-q)/n$ FH sequences with parameters

$$(n, (q^{n-m}-q)/n, n-3; q).$$

This is because of the following:

- the linear code $\mathcal{C}_{(q,m)}$ had minimum distance $d = 3$ and dimension $n-m$;
- $\mathcal{S}_{(H,q,m)}$ is a subset of the linear code $\mathcal{C}_{(q,m)}$; and
- any two sequences in $\mathcal{S}_{(H,q,m)}$ are not equivalent.

It is straightforward to verify that the set $\mathcal{S}_{(H,q,m)}$ of FH sequences meets the sphere-packing bound of (10). This proves the following theorem.

Theorem 12: If $\gcd(m, q-1) = 1$ and $n = (q^m-1)/(q-1)$ is a prime, the set $\mathcal{S}_{(H,q,m)}$ of FH sequences has parameters $(n, (q^{n-m}-q)/n, n-3; q)$ and meets the sphere-packing bound of (10).

The following pairs (q, m) satisfy the conditions in Theorem 12:

$$(2,2), (2,3), (2,5), (2,7), (3,3), (3,7), (4,2), (5,3), (5,7).$$

Regarding the construction of this section, we have the following open problem.

Open Problem 1: If the condition that $n = (q^m-1)/(q-1)$ is a prime in Theorem 12 is dropped, is it still true that every nontrivial equivalence class of codewords has size n?

If the answer to this open question is positive, then more optimal sets of FH sequences are obtained.

VIII. A Combinatorial Construction of Optimal Sets of Frequency Hopping Sequences

In this section, we present a combinatorial construction that produces an optimal set of frequency hopping sequences from another optimal set having different parameters, which appeared

in the conference proceedings [9]. The construction can be recursively applied to the resulting optimal set and generates infinitely many optimal examples of new parameters.

To this end, we utilize a type of combinatorial matrix. A *cyclic difference matrix* CDM$(m,n,1)$ is an $n\times m$ matrix $\sum=[\sigma_{i,j}]$ such that $\sigma_{i,j}\in \boldsymbol{Z}_m := \{0,1,\ldots,m-1\}$ and for each pair of two rows i and i' every element of $\boldsymbol{Z}_m$ occurs exactly once among the differences $\{(\sigma_{i,j}-\sigma_{i',j})(\mathrm{mod}\ m) : 0\le j\le m-1\}$. A CDM$(m,n,1)$ where every element of $\mathbf{Z}_n$ appears in every row exactly once is called *homogeneous*.

For a set $\mathcal{S}$ of FH sequences, we introduce the following two parameters:

$$\lambda_a=\max_{X\in\mathcal{S}}H(X),\lambda_c=\max_{X,Y\in\mathcal{S},X\neq Y}H(X,Y)$$

where λ_a and λ_c are maximum Hamming auto-correlation and maximum cross-correlation of the sequences in $\mathcal{S}$. By definition, $\lambda=\max\{\lambda_a,\lambda_c\}$. In the rest of this section, we will replace the parameters $(n,N,\lambda;l)$ of a set $\mathcal{S}$ of FH sequences with the more refined parameters $(n,N,\lambda_a,\lambda_c;l)$. We consider the case that for any sequence $S_i\in\mathcal{S}$ with parameters $(n,N,\lambda;l)$ there exists a frequency a such that $S_i(t)=a$ for $t=t_a$ and $S_i(t)\neq a$ for every $t\neq t_a$; that is, there exists a frequency that appears precisely once in each sequence of $\mathcal{S}$ at time t_a. Clearly, without loss of generality, we may assume that $f_0\in L$ and $t_{f_0}=0$.

For a frequency $a\in L$ of a set of sequences $\mathcal{S}$ over an alphabet set L, define also $a(S_i)$ as the number of occurrences of the frequency in the sequence S_i and $a(\mathcal{S})=\sum_i a(S_i)$. We define $\bar{\mathcal{S}}=\max_{a\in L}a(S)$.

Theorem 13: Assume that there exists a set $\mathcal{S}$ of FH sequences with parameters $(n,N,\lambda_a,\lambda_c;l)$ such that for any sequence $S_i\in\mathcal{S},S_i(0)=0,S_i(t)\neq 0$ for every $t\neq 0$, and for any pair of i and j with $1\le i\neq j\le N,S_i(t)\neq S_j(t)$ for every $t\neq 0$. Assume also that there exists another set $\mathcal{T}$ of FH sequences with parameters $(m,M,\lambda_a',\lambda_c';k)$. If there exists a homogeneous cyclic difference matrix CDM$(m,\bar{\mathcal{S}},1)$, then there exists a set $\mathcal{U}$ of FH sequences with parameters $(nm,\min\{N,M\},\max\{\lambda_a,\lambda_a'\},\max\{\lambda_c,\lambda_c'\};(l-1)m+k)$.

Proof: For $1\le j\le N$ and $1\le i\le l-1$, let A_i^j be the support set of f_i in S_j, that is, $A_i^j=\{w : 1\le w\le n-1,\ S_j(w)=f_i\}$. Then $\{A_1^j,A_2^j,\ldots,A_{l-1}^j\}$ is a partition of $\{1,2,\ldots,n-1\}$ for any $1\le j\le N$, and $A_i^1,A_i^2,\ldots,A_i^N$ are mutually disjoint for any $1\le i\le l-1$. Let $\Sigma=[\sigma_{ij}]$ be the homogeneous CDM$(m,\bar{\mathcal{S}},1)$. For any family of the following N support sets of $f_i\in L,1\le i\le l-1$

$$\begin{aligned}A_i^1&=\{a_{i,1}^1,\ldots,a_{i,k_1}^1\}\\ A_i^2&=\{a_{i,k_1+1}^2,\ldots,a_{i,k_2}^2\},\ \ldots\\ A_i^N&=\{a_{i,k_{N-1}+1}^N,\ldots,a_{i,k_N}^N\}\end{aligned}$$

construct the following Nw new support sets:

$$A_i^j(k)=\{a_{i,k_{j-1}+1}^j+\sigma_{k_{j-1}+1,k}v,\ldots,a_{i,k_j}^j+\sigma_{k_j,k}v\}\qquad 1\le j\le N,\ 1\le k\le w.$$

Similarly, for $1\le j\le M$ and $0\le i\le k-1$, let B_i^j be the support set of f_i' in $T_j\in\mathcal{T}$, that is, $B_i^j=\{w : 0\le w\le k-1,\ T_j(w)=f_i'\}$. Then similarly $\{B_0^j,B_1^j,\ldots,B_{k-1}^j\}$ is a partition of $\{0,1,\ldots,m-1\}$ for any $1\le j\le M$, and $B_i^1,B_i^2,\ldots,B_i^M$ are mutually disjoint for any $0\le i\le k-1$. Adding the family of support sets $\{vB_0^j,\ldots,vB_{k-1}^j\}$ to the family of support sets $\{A_i^j(k) : 1\le i\le l-1,\ 1\le k\le w\}$, we obtain the support sets of $(l-1)m+k$ frequencies of a new FH sequence for any $1\le j\le\min\{N,M\}$. It can be readily checked that these $\min\{N,M\}$ FH sequences form a set $\mathcal{U}$ of FH sequences with parameters $(nm,\min\{N,M\},\max\{\lambda_a,\lambda_a'\},\max\{\lambda_c,\lambda_c'\};(l-1)m+k)$. □

The following is an important application of Theorem 13.

Corollary 14: For each i let a_i be a nonnegative integer and $p_i\equiv 1(\mathrm{mod}\ f)$ a prime of the form $p_i=e_if+1$ with $e_i\ge 3$ and $f\ge 6$. There exists an optimal set of frequency hopping sequences with parameters $(n,N,\lambda_a,\lambda_c;l)$ meeting the Peng–Fan bound of (2), where $n=\prod_i p_i^{a_i},N=\min\{e_i\},\lambda_a=f-1,\lambda_c=f$, and $l=(\prod_i p_i^{a_i}+f-1)/f$.

Proof: Chu and Colbourn [1] constructed such a set $\mathcal{S}$ of frequency hopping sequences with parameters $(p_i,e_i,f-1,f;e_i+1)$ satisfying the condition of Theorem 14. Then the conclusion is followed by repeated applications of Theorem 14 to Chu and Colbourn's result and an easy verification of the Peng–Fan bound of (2), where the required homogeneous cyclic difference matrices in Theorem 13 are easily obtained from the multiplication tables of the finite fields GF(p_i) [2, Ch. XX] □

ACKNOWLEDGMENT

The authors would thank the two anonymous reviewers and the Associate Editor, M. Parker, for their comments that improved the presentation of this paper.

REFERENCES

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

[2] C. J. Colbourn and J. H. Dinitz, *CRC Handbook of CombinatorialDesigns*, 2nd ed. Boca Raton, FL: Champion and Hall/CRC, 2006.

[3] C. Ding, "Complex codebooks from combinatorial designs," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4229–4235, Sep. 2006.

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

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

[6] T. Etzion, "Optimal constant weight codes over Z_k and generalized designs," *Discrete Math.*, vol. 169, pp. 55–82, 1998.

[7] F.-W. Fu, A. J. Han Vinck, and S. Y. Shen, "On the construction of constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 328–333, 1998.

[8] F.-W. Fu, T. Kløve, Y. Luo, and W. Wei, "On the Svanström bound for ternary constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 2061–2064, 2001.

[9] Y. Fujiwara and R. Fuji-Hara, "Frequency hopping sequences with optimal auto- and cross-correlation properties and related codes," in *Proc. 10th Int. Workshop on Algebr. Combinator. Coding Theory*, Zvenigorod, Russia, Sep. 2006, pp. 83–96.

[10] 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.

[11] 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.

[12] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[13] J. J. Komo and S. C. Liu, "Maximal length sequences for frequency hopping," *IEEE J. Sel. Areas Commun.*, vol. 5, pp. 819–822, 1990.
[14] P. V. Kumar, "Frequency-hopping code sequence designs having large linear span," *IEEE Trans. Inf. Theory*, vol. IT-34, pp. 146–151, 1988.
[15] A. Lempel and H. Greenberger, "Families of sequences with optimal Hamming correlation properties," *IEEE Trans. Inf. Theory*, vol. IT-20, pp. 90–94, 1974.
[16] S. Lin and C. Xing, *Coding Theory: A First Course*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
[17] G. Myerson, "Period polynomials and Gauss sums for finite fields," *Acta Arithmetica*, vol. XXXIX, pp. 251–264, 1981.
[18] P. R. J. Östergaard, , M. Fossorier, H. Imai, S. Lin, and A. Poli, Eds., "On binary/ternary error-correcting codes with minimum distance 4," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*. Berlin, Germany: Springer, 1999, pp. 472–481, LNCS 1719.
[19] P. R. J. Östergaard and M. Svanström, "Ternary constant weight codes," *The Electron. J. Combinator.*, vol. 9, pp. 1–22, 2002.
[20] 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.
[21] R. A. Scholtz, "The spread spectrum concept," *IEEE Trans. Commun.*, vol. COM-25, pp. 748–755, 1977.
[22] T. Storer, *Cyclotomy and Difference Sets.*. Chicago, IL: Markham, 1967.
[23] M. Svanström, "A lower bound for ternary constant-weight codes," *IEEE Trans. Inf. Theory*, vol. 43, pp. 1630–1632, 1997.
[24] M. Svanström, "A class of perfect ternary constant-weight codes," *Designs, Codes and Cryptogr.*, vol. 18, pp. 223–229, 1999.
[25] 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.
[26] J. H. van Lint, *Introduction to Coding Theory*, 2nd ed. New York: Springer-Verlag, 1992.

Cunsheng Ding (M'98–SM'05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. degree in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992, he was a Lecturer of Mathematics with Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science with the National University of Singapore. His research fields are cryptography and coding theory. He has coauthored four research monographs.

Dr. Ding is a co-recipient of the State Natural Science Award of China in 1989. He served as a guest editor or editor for 10 journals.

Ryoh Fuji-Hara was born in Hyogo, Japan, on November 4, 1949. He received the M. Eng. degree from Waseda University, Tokyo, Japan, and the Ph.D. degree in combinatorics and optimization from the University of Waterloo, Waterloo, ON, Canada, in 1981.

From 1981 to 1983, he was a Postdoctoral Fellow with the University of Waterloo. He was an Assistant Professor from 1983 to 1988, an Associate Professor from 1988 to 1994, and is currently a Professor at the Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba, Ibaraki, Japan. With M. Jimbo, he coauthored the book *Mathematical Theory of Coding and Cryptography* (in Japanese) (Tokyo, Japan: Kyoritsu Shuppan, 1993).

Dr. Fuji-Hara is on the Editorial Board of the *Journal of Combinatorial Mathematics and Combinatorial Computing*.

Yuichiro Fujiwara received the B.S. and M.S. degrees in mathematics from Keio University, Japan, and the Ph.D. degree in information science from Nagoya University, Japan.

He is a Postdoctoral Fellow with the Graduate School of System and Information Engineering, Tsukuba University, Japan. His research interests include combinatorics, information theory, and their interactions.

Masakazu Jimbo received the a Dr. Science degree in information science from Tokyo Institute of Technology, Tokyo, Japan, in 1985.

He was an Assistant Professor with the Tokyo University of Science, a Lecturer with the University of Tsukuba, a professor with Gifu University, and a Professor with Keio University. He is currently a Professor in the Graduate School of Information Sciences, Nagoya University, Nagoya, Japan. His research interests cover the areas of discrete mathematics and statistics.

Miwako Mishima received the Ph.D. degree in science from Keio University, Yokohama, Japan, in 1999.

From 1993 to 1996, she was with Nippon Telegraph and Telephone Corporation (NTT), Japan. From 1996 to 2003, she was a Research Associate with Gifu University, Gifu, Japan, where she is currently an Associate Professor. Her research interests include design theory, graph theory, and their applications.