Optimal Sets of Frequency Hopping Sequences From Linear Cyclic Codes

Cunsheng Ding, *Senior Member, IEEE*, Yang Yang, *Student Member, IEEE*, and Xiaohu Tang, *Member, IEEE*

***Abstract*—In communication systems, frequency hopping spread spectrum and direct sequence spread spectrum are two main spread coding technologies. Frequency hopping sequences are used in FH-CDMA systems. In this paper, an earlier idea of constructing optimal sets of frequency hopping sequences is further investigated. New optimal parameters of sets of frequency hopping sequences are obtained with subcodes of the Reed–Solomon codes. Optimal sets of frequency hopping sequences are constructed with a class of irreducible cyclic codes. As a byproduct, the weight distribution of a subclass of irreducible cyclic codes is determined.**

***Index Terms*—Cyclic codes, direct sequence spread spectrum, frequency hopping sequence, frequency hopping spread spectrum, irreducible cyclic codes.**

I. Introduction

A. *Definitions and Notations*

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 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 FH-CDMA systems (for a description of such systems, see [27]).

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.

B. *Peng–Fan Bounds and Optimal Parameters With Respect to the Bounds*

Lempel and Greenberger developed the following lower bound for $H(X)$ [19].

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

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

In this paper, we use $(n,N,\lambda;\ell)$ to denote a set $\mathcal{F}$ of N frequency hopping sequences 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 $\mathcal{F}$.

Manuscript received July 02, 2009; revised July 06, 2009. Current version published June 16, 2010. The work of Y. Yang and X. H. Tang was supported in part by the National Science Foundation of China (NSFC) by Grant 60772086.

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clearwater Bay, Kowloon, Hong Kong (e-mail: cding@ust.hk).

Y. Yang and X. Tang are with the Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, Sichuan 610031, China (e-mail: yang_data@yahoo.cn; xhutang@ieee.org).

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

Digital Object Identifier 10.1109/TIT.2010.2048504

TABLE I
KNOWN OPTIMAL SETS OF FREQUENCY HOPPING SEQUENCES

Length n	Alphabet size	Correlation λ	Set size	Ref
p^r-1	p^u, $0<u\le r$	$p^{r-u}-1$	p^u	[19]
p^2	p	p	p	[17]
p, odd prime	$e+1$, where $e\|(p-1)$	$\frac{p-1}{e}$	e	[4]
$\frac{q^m-1}{2}$, m odd	q	$\frac{q^{m-1}-1}{2}$	2	[10]
q^m-1	q	q^{m-1}	q	[10]
$q-1$, where q prime power	$e+1$, where $e\|(q-1)$	$\frac{q-1}{e}$	e	[11]
$\frac{q^m-1}{d}$, where q prime power $\gcd(q-1,m) = 1$, $d\|(q-1)$	q	$\frac{q^{m-1}-1}{d}$	d	[11] [15]
q^2+1	$q=2^s$	$q+1$	q^2-1	[8]
$\frac{q+1}{2}$	$q\equiv 1 \pmod 4$	1	$2(q-1)$	[8]
$q-1$ prime	q	$k-1$	$\frac{q^k-1}{q-1}$	[8]
$n=\frac{q^m-1}{q-1}$ $\gcd(m,q-1)=1$	q	$n-3$	$\frac{q^{n-m}-q}{n}$	[8]

Lemma 2: ([26, 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

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

and

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

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, [4], [10], [11], [13], [14], [16], [17], [19], and [29]). Some of the parameters in Table I are optimal with respect to the Peng–Fan bounds.

C. Coding-Theory Bounds on Sets of FH Sequences and Optimal Constructions

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. 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 F^n with dimension k such that the minimum Hamming distance between all pairs of distinct codewords is d.

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 left-shifted versions together [8]. Hence bounds on error correcting codes give automatically bounds on sets of frequency hopping sequences. This connection between sets of FH sequences and cyclic linear codes was used to establish the following bounds on sets of FH sequences in [8].

Theorem 3: (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

$$N \leq \left\lfloor \frac{\ell^{\lambda+1}}{n} \right\rfloor. \tag{4}$$

Theorem 4: (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

$$N \leq \left\lfloor \frac{1}{n} \left\lfloor \frac{\ell(n-\lambda)}{n-\ell\lambda} \right\rfloor \right\rfloor. \tag{5}$$

Theorem 5: (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

$$N \leq \left\lfloor \frac{\ell^n}{n\left(\sum_{i=0}^{\lfloor (n-\lambda-1)/2 \rfloor} \binom{n}{i} (\ell-1)^i\right)} \right\rfloor. \tag{6}$$

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 this section or Lemma 2 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.

Let $F = \{f_0, f_1, \ldots, f_{\ell-1}\}$ be an abelian group of size ℓ. As pointed out before, any given set $\mathcal{F}$ of FH sequences with parameters $(n, N, \lambda; \ell)$ gives an $(n, nN, n-\lambda; \ell)$ cyclic code $\mathcal{C}_{\mathcal{F}}$ automatically.

An $(n, M, d; \ell)$ cyclic code $\mathcal{C}$ over F may be used to construct a set of FH sequences in different ways. However, it is open if the given cyclic code $\mathcal{C}$ could be used to construct optimal sets of FH sequences in some way. Even if this is possible, the way to use a given cyclic code to construct an optimal set of FH sequences may differ from case to case.

Two codewords of an $(n, M, d; \ell)$ cyclic code $\mathcal{C}$ over F are said *equivalent* if one is a cyclic left shift of the other. Using this equivalence relation, all the codewords of $\mathcal{C}$ are classified into equivalence classes $\{\mathbf{c}\}$. The number of elements in an equivalent class $\{\mathbf{c}\}$ is called the *cycle length* of all the codewords in the equivalence class. If the size of an equivalence class $\{\mathbf{c}\}$ is n, then $\{\mathbf{c}\}$ is called an *full-cycle* equivalence class. A general idea of constructing a set of FH sequences is to take one and only one codeword from each full-cycle equivalence class and put them together into a set $\mathcal{S}_{\mathcal{C}}$ [8]. Whether the set $\mathcal{S}_{\mathcal{C}}$ of FH sequences is optimal with respect to one of the bounds described before depends on the underlying cyclic code $\mathcal{C}$.

This idea was employed to obtain optimal sets of FH sequences using a few classes of cyclic linear codes in [8]. The parameters of the optimal sets of FH sequences obtained in [8] are included in Table I. The objective of this paper is to further explore this idea. We will prove that the construction of sets of FH sequences using the Reed–Solomon codes in [8] gives much more optimal parameters, and will present a construction of new optimal sets of FH sequences using a subclass of irreducible cyclic codes. As a byproduct, the weight distribution of a subclass of irreducible cyclic codes is determined.

II. More Optimal Sets of FH Sequences From the Reed–Solomon Codes

In [8], the Reed–Solomon code was employed to construct a set of FH sequences. It was shown in [8] that the set of FH sequences meets the Singleton bound of (4) when the length of the FH sequences is a prime. The objective of this section is to relax this condition and to obtain optimal sets of FH sequences with new parameters.

We now introduce the construction of sets of FH sequences with subcodes of the Reed–Solomon codes [8]. Let q be a prime power, and let k be an integer with $1 \le k \le q-1$. Define

$$\mathrm{GF}(q)[x]_k = \left\{ \sum_{i=1}^{k} g_i x^i : g_i \in \mathrm{GF}(q),\ i = 1, 2, \ldots, k \right\}. \tag{7}$$

Define $n = q - 1$ and

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

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

Two codewords of $\mathcal{C}_{RS}$ are said to be *equivalent* if one is the cyclic shift of the other. The codewords of $\mathcal{C}_{RS}$ are now classified into equivalence classes. The set

$$\{(0, 0, \ldots, 0)\}$$

is an equivalence class. Taking one and only one codeword from each of the remaining equivalence classes and putting them together, we form a set $\mathcal{S}_{\mathcal{C}_{RS}}$ of FH sequences.

The following result was proved in [8].

Theorem 6: [8] Assume that q is a prime power and $q-1$ is a prime. The set $\mathcal{S}_{\mathcal{C}_{RS}}$ of FH sequences has parameters $(q-1, (q^k-1)/(q-1), k-1; q)$ and meets the Singleton bound of (4).

Theorem 6 tells that the set $\mathcal{S}_{\mathcal{C}_{RS}}$ of FH sequences is optimal when $q-1$ is a Mersene prime of the form $2^s - 1$ for some positive integer s. The following is a generalization of Theorem [8] which shows that the set $\mathcal{S}_{RS}$ of FH sequences is also optimal in many other cases.

Theorem 7: Let $\Delta(q-1) = \min\{s : s \,|\, (q-1), s > 1\}$. For any k with $1 \le k < \Delta(q-1)$, the set $\mathcal{S}_{\mathcal{C}_{RS}}$ of FH sequences has parameters $(q-1, (q^k-1)/(q-1), k-1; q)$ and meets the Singleton bound of (4).

Proof: Let $n = q-1$. Suppose that $1 \le k < \Delta(q-1)$. Let

$$\mathbf{g} = (g(1), g(\alpha), \ldots, g(\alpha^{n-1}))$$

be a sequence in the set $\mathcal{S}_{\mathcal{C}_{RS}}$, where α is a generator of $\mathrm{GF}(q)^*$ and

$$g(x) = g_1 x + g_2 x^2 + \cdots + g_k x^k \in \mathrm{GF}(q)[x]_k.$$

We now prove that all the cyclic left shifts of the sequence $\mathbf{g}$ are pairwise distinct if the polynomial $g(x)$ is not the zero polynomial. Suppose on the contrary that the cyclic shift of $\mathbf{g}$ to the left for u positions is the same as $\mathbf{g}$, where $1 \le u < n$. In this case, u is a period of the sequence $\mathbf{g}$. The minimum value of such u is called the *cycle length* or the *least period* of the sequence $\mathbf{g}$. Here we assume that u is the cycle length of the sequence $\mathbf{g}$. Clearly, $\gcd(u, n)$ is also a period of the sequence $\mathbf{g}$. It follows from the minimality of the cycle length that $\gcd(u, n) = u$, i.e., $\Delta(q-1) \le u \le n/\Delta(q-1)$.

It is easily seen that $u \ne 1$. Otherwise $g(x)$ will be a constant polynomial. Hence we have $u > 1$. By the definition of u,

$$g(\alpha^{i+u}) = g(\alpha^i), \quad i = 0, 1, \ldots, u-1.$$

Hence

$$\sum_{j=1}^{k} g_j(\alpha^{uj} - 1)\alpha^{ij} = 0, \quad i = 0, 1, \ldots, u-1.$$

It follows that

$$\sum_{j=0}^{k-1} g_{j+1}\left(\alpha^{u(j+1)} - 1\right)\alpha^{ij} = 0, \quad i = 0, 1, \ldots, u-1.$$

This means that the polynomial $\sum_{j=0}^{k-1} g_{j+1}(\alpha^{u(j+1)} - 1)x^j$ has u roots α^i, where $i \in \{0, 1, \ldots, u-1\}$. Because any nonzero polynomial of degree at most $k-1$ has at most $k-1$ roots and $u > k-1$, we have

$$g_j(\alpha^{uj} - 1) = 0, \quad j = 1, 2, \ldots, k.$$

Note that $1 \le j \le k < \Delta(q-1) \le u$, and $u \le n/\Delta(q-1)$. It follows from $1 < uj < n$ that $\alpha^{uj} - 1 \ne 0$ for all j with $1 \le j \le k$. Therefore, $g_j = 0$ for all j with $1 \le j \le k$. This means that $g(x)$ is the zero polynomial. This is a contradiction.

The equivalence classes of the form $\{(a, a, \ldots, a)\}$ are called *trivial*. In summary, we have proved that every nontrivial equivalence class of codewords has exactly $n = q-1$ codewords of the code $\mathcal{C}_{RS}$. Hence, $\mathcal{S}_{\mathcal{C}_{RS}}$ is a set of $(q^k-1)/(q-1)$ FH sequences with parameters $(q-1, (q^k-1)/(q-1), k-1; q)$. It is straightforward to verify that the set $\mathcal{S}_{\mathcal{C}_{RS}}$ of FH sequences meets the Singleton bound of (4). This completes the proof. ■

Table II lists some of the parameters of the optimal set of FH sequences given in Theorem 7, where the remark "New" means that the parameters of the optimal set of FH sequences are discovered in this paper.

TABLE II
SOME OPTIMAL PARAMETERS OF THE SETS OF FH SEQUENCES IN THEOREM 7

Length n	k	Set size N	Correlation λ	Alphabet ℓ	Remark
7	$1 \le k \le 6$	$\frac{8^k-1}{7}$	$k-1$	8	[8]
15	$1 \le k \le 2$	$\frac{16^k-1}{15}$	$k-1$	16	New
31	$1 \le k \le 30$	$\frac{32^k-1}{31}$	$k-1$	32	[8]
63	$1 \le k \le 2$	$\frac{64^k-1}{63}$	$k-1$	64	New
127	$1 \le k \le 126$	$\frac{128^k-1}{127}$	$k-1$	128	[8]
255	$1 \le k \le 2$	$\frac{256^k-1}{255}$	$k-1$	256	New
511	$1 \le k \le 6$	$\frac{512^k-1}{511}$	$k-1$	512	New

III. OPTIMAL SETS OF FH SEQUENCES FROM A SUBCLASS OF IRREDUCIBLE CYCLIC CODES

A. Irreducible Cyclic Codes

Let $r = q^m$ with a positive integer m and let N be a positive integer dividing $r-1$. Put $n = (r-1)/N$. Let α be a primitive element of $\mathrm{GF}(r)$ and let $\theta = \alpha^N$. The set

$$\mathcal{C}(N, q^m) = \{\mathbf{c}(\beta) : \beta \in \mathrm{GF}(r)\} \tag{8}$$

where $\mathbf{c}(\beta) = (\mathrm{Tr}_{r/q}(\beta), \mathrm{Tr}_{r/q}(\beta\theta), \ldots, \mathrm{Tr}_{r/q}(\beta\theta^{n-1}))$, is called an *irreducible cyclic* $[n, m_0]$ *code* over $\mathrm{GF}(q)$, where $\mathrm{Tr}_{r/q}$ is the trace function from $\mathrm{GF}(r)$ onto $\mathrm{GF}(q)$ and m_0 divides m.

The weight distribution of irreducible cyclic codes is quite complicated in general [21]. However, in certain special cases the weight distribution is known. We summarize these cases here.

1) When $N \,|\, (q^j + 1)$ for some j being a divisor of $m/2$, which is called the *semi-primitive case*, the codes have two weights. These codes were studied by Delsarte and Goethals [5], McEliece [22], and Baumert and McEliece [1].
2) When $N = 2$, the weight distribution was found by Baumert and McEliece [1].
3) When $N = 3$ and $N = 4$, the weight distribution was described in [7].
4) When N is a prime with $N \equiv 3 \pmod 4$ and $\mathrm{ord}_q(N) = (N-1)/2$, the weight distribution was determined by Baumert and Mykkeltveit [2].
5) When $q \equiv 1 \pmod N$ and $\gcd(m, N) = 1$, the weight distribution was described in [7].
6) When N is even, $\gcd(n, N) = 1$ and $\gcd((r-1)/(q-1) \bmod N, N) = 2$, the weight distribution was described in [7].

McEliece also generalized some of these results [22] and showed that the weights of an irreducible cyclic code can be expressed as a linear combination of Gauss sums via the Fourier transform [23] (see also McEliece and Rumsey [24], Fitzgerald and Yucas [12], van der Vlugt [30], and the references therein).

Two-weight codes are a class of interesting codes which are closely related to combinatorial designs, finite geometry, and graph theory. Information on them can be found in Baumert and McEliece [1], Calderbank and Kantor [3], Wolfmann [32], Delsarte and Goethals [5], Langevin [18], Schmidt and White [28], Wolfmann [33], [34], and Vega and Wolfmann [31].

B. Subclass of Irreducible Cyclic Codes

Let p be a prime, $q = p^s$, $m = 2lk$, $r = q^m$, where s, l, and k are positive integers. Let h be a positive divisor of $q^k + 1$, and so of $(r-1)/(q-1)$, and let α be a primitive element of $\mathrm{GF}(r)$. Throughout this section we always assume $h < \sqrt{r} + 1$. Define the additive character χ on $\mathrm{GF}(r)$ by $\chi(x) = \zeta_p^{\mathrm{Tr}_{r/p}(x)}$, where $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ and $\mathrm{Tr}_{r/p} : \mathrm{GF}(r) \to \mathrm{GF}(p)$ is the absolute trace mapping. Let $\mathrm{Tr}_{r/q} : \mathrm{GF}(r) \to \mathrm{GF}(q)$ and $\mathrm{Tr}_{q/p} : \mathrm{GF}(q) \to \mathrm{GF}(p)$ be further trace mappings. Define

$$C_i = \left\{ \alpha^{i+jh} : 0 \le j < \frac{r-1}{h} \right\} \tag{9}$$

for each i with $0 \le i \le h-1$. These C_i $(0 \le i \le h-1)$ are called the *cyclotomic classes* of order h in $\mathrm{GF}(r)^*$.

For any $g \in \mathrm{GF}(r)$, define the exponential sum

$$S(g) = \sum_{x \in \mathrm{GF}(r)} \chi(gx^h).$$

Lemma 8: [25] Assume $h \,|\, (q^k + 1)$. Then for any $g \in \mathrm{GF}(r)^*$,

$$S(g) = \begin{cases} (-1)^l \sqrt{r} & \text{if } g \notin C_{h_0} \\ (-1)^{l-1}(h-1)\sqrt{r} & \text{if } g \in C_{h_0}, \end{cases}$$

where

$$h_0 = \begin{cases} h/2 & \text{if } p > 2,\ l \text{ odd, and } (q^k+1)/h \text{ odd} \\ 0 & \text{otherwise.} \end{cases}$$

Let $n = (r-1)/h(q-1)$, and let h be a divisor of $q^k + 1$. Define $d_i = \alpha^{h(q-1)(i-1)}$ for $i = 1, \ldots, n$. We are now ready to present the construction of the two-weight codes. For each $g \in \mathrm{GF}(r)$, define the vector

$$\mathbf{c}(g) = (\mathrm{Tr}_{r/q}(gd_1), \mathrm{Tr}_{r/q}(gd_2), \ldots, \mathrm{Tr}_{r/q}(gd_n)).$$

We then define the code

$$\mathcal{C}(q, h, l, k) = \{\mathbf{c}(g) : g \in \mathrm{GF}(r)\}. \tag{10}$$

It is easily seen that $\mathcal{C}(q, h, l, k)$ is an irreducible cyclic code over $\mathrm{GF}(q)$ with dimension being a divisor of m. Though h is a divisor of $q^k + 1$, $h(q-1)$ may not divide $q^j + 1$ for any positive integer j. The weight distribution of the irreducible cyclic code $\mathcal{C}(q, h, l, k)$ may be hard to determine, as this is not the semiprimitive case in general. The code $\mathcal{C}(q, h, l, k)$ may have only two nonzero weights or much more nonzero weights. The following examples illustrate this fact.

Example 1: Let $q = 2$, $l = 1$, $k = 3$, and $h = 3$. In this case, $\mathcal{C}(q, h, l, k)$ is a $[21, 6, 8]$ cyclic code over GF(2) with the weight distribution

$$1 + 21x^8 + 42x^{12}.$$

Its dual is a $[21, 15, 3]$ cyclic code over GF(2).

weight	frequency
$\frac{r+(-1)^l(h-1)\sqrt{r}}{qh}$	$\frac{r-1}{h}$
$\frac{r+(-1)^{l-1}\sqrt{r}}{qh}$	$\frac{(h-1)(r-1)}{h}$
0	1

Example 2: Let $q = 7$, $l = 1$, $k = 2$, and $h = 5$. In this case, $\mathcal{C}(q,h,l,k)$ is a $[80,4,56]$ cyclic code over GF(7) with the weight distribution

$$1 + 240x^{56} + 2160x^{70}.$$

Its dual is a $[80,76,2]$ cyclic code over GF(7).

Example 3: Let $q = 7$, $l = 1$, $k = 2$, and $h = 10$. In this case, $\mathcal{C}(q,h,l,k)$ is a $[40,4,28]$ cyclic code over GF(7) with the weight distribution

$$1 + 240x^{28} + 600x^{32} + 480x^{34} + 480x^{36} + 600x^{38}.$$

Its dual is a $[40,36,2]$ cyclic code over GF(7).

The code $\mathcal{C}(q,h,l,k)$ of (10) is different from the linear code defined in [9] due to the following:

1) The code $\mathcal{C}(q,h,l,k)$ of (10) is cyclic, while the one in [9] is not cyclic.
2) The code $\mathcal{C}(q,h,l,k)$ of (10) may have more than two nonzero weights, while the one in [9] is always a two-weight code.

We now determine the weight distribution of a subclass of the irreducible cyclic codes, and have the following conclusion.

Theorem 9: Assume that $h \mid (q^k+1)$ and $\gcd((r-1)/h(q-1),(q-1)) = 1$. The set $\mathcal{C}(q,h,l,k)$ of (10) is an $[n,m]$ two-weight cyclic linear code over $\mathrm{GF}(q)$ and has the following weight distribution:

Furthermore, the dual code $\mathcal{C}(q,h,l,k)^\perp$ of $\mathcal{C}(q,h,l,k)$ is an $[n, n-m, d^\perp]$ linear code with minimum distance $d^\perp \geq 3$.

Proof: Since $\gcd((r-1)/h(q-1), q-1) = 1$, we have that $\mathrm{GF}(q)^* \subset C_0$. We first prove that $\{d_1, d_2, \ldots, d_n\}$ is a complete set of coset representatives of $C_0/\mathrm{GF}(q)^*$. Note that

$$d_i d_j^{-1} = \alpha^{h(q-1)(i-j)}.$$

We need to prove that

$$(d_i d_j^{-1})^{q-1} = \alpha^{(q-1)^2 h(i-j)} \neq 1$$

for each pair of distinct i and j with $1 \leq i \leq n$ and $1 \leq j \leq n$. It follows from the assumption $\gcd((r-1)/h(q-1), q-1) = 1$ that

$$\gcd(r-1, h(q-1)^2) = \gcd(r-1, h(q-1)).$$

Hence, $\{d_1, d_2, \ldots, d_n\}$ is a complete set of coset representatives of $C_0/\mathrm{GF}(q)^*$.

Clearly, $\mathcal{C}(q,h,l,k)$ is a linear code over $\mathrm{GF}(q)$ of length n. We now determine the dimension and weight distribution of $\mathcal{C}(q,h,l,k)$. For any $g \in \mathrm{GF}(r)^*$, the Hamming weight $w_H(\mathbf{c}(g))$ of the codeword $\mathbf{c}(g) \in \mathcal{C}(q,h,l,k)$ is given by

$$\begin{aligned} w_H(\mathbf{c}(g)) &= n - |\{i : 1 \leq i \leq n, \mathrm{Tr}_{r/q}(gd_i) = 0\}| \\ &= n - \frac{1}{q}\sum_{i=1}^{n}\sum_{t\in\mathrm{GF}(q)} \zeta_p^{\mathrm{Tr}_{q/p}(t\mathrm{Tr}_{r/q}(gd_i))} \\ &= n - \frac{n}{q} - \frac{1}{q}\sum_{t\in\mathrm{GF}(q)^*}\sum_{i=1}^{n}\chi(gtd_i) \\ &= n - \frac{n}{q} - \frac{1}{q}\sum_{j=1}^{(r-1)/h}\chi(g\alpha^{jh}) \\ &= n - \frac{n}{q} - \frac{1}{qh}(S(g)-1), \end{aligned}$$

where the third equality holds by the transitivity of the trace (see [20, Th. 2.26]) and the fourth equality holds because $\{d_1, d_2, \ldots, d_n\}$ is a complete set of coset representatives of $C_0/\mathrm{GF}(q)^*$.

It then follows from Lemma 8 that

$$\begin{aligned} w_H(\mathbf{c}(g)) &= n - \frac{n}{q} - \frac{1}{qh}(S(g)-1) \\ &= \begin{cases} \frac{r+(-1)^l(h-1)\sqrt{r}}{qh} & \text{if } g \in C_{h_0}, \\ \frac{r+(-1)^{l-1}\sqrt{r}}{qh} & \text{otherwise.} \end{cases} \end{aligned}$$

Since $h < \sqrt{r}+1$, we have $w_H(\mathbf{c}(g)) \neq 0$ for all nonzero $g \in \mathrm{GF}(r)$. Hence the $\mathrm{GF}(q)$-linear map $g \in \mathrm{GF}(r) \mapsto \mathbf{c}(g)$ is injective. Then the conclusions about the dimension and weight distribution of $\mathcal{C}(q,h,l,k)$ follow.

For the dual code $\mathcal{C}(q,h,l,k)^\perp$, we only need to prove the lower bound for the minimum distance $d^\perp$. Suppose on the contrary that $d^\perp \leq 2$. By the well-known characterization of the minimum distance of a linear code in terms of a parity-check matrix (see [20, Lemma 9.14]), there exist a pair of integers $1 \leq i < j \leq n$ such that the ith column and the jth column of a parity-check matrix of $\mathcal{C}(q,h,l,k)^\perp$ (which is the same as a generator matrix of $\mathcal{C}(q,h,l,k)$) are linearly dependent over $\mathrm{GF}(q)$. If $\theta_1, \ldots, \theta_m$ form a $\mathrm{GF}(q)$-basis of $\mathrm{GF}(r)$, then $\mathbf{c}(\theta_1), \ldots, \mathbf{c}(\theta_m)$ form a $\mathrm{GF}(q)$-basis of $\mathcal{C}(q,h,l,k)$. It follows that there exists $(c_1, c_2) \in \mathrm{GF}(q)^2 \setminus \{(0,0)\}$ such that

$$c_1\mathrm{Tr}_{r/q}(\theta_u d_i) + c_2\mathrm{Tr}_{r/q}(\theta_u d_j) = 0 \quad \text{for } 1 \leq u \leq m.$$

This implies

$$\mathrm{Tr}_{r/q}(\theta_u(c_1 d_i + c_2 d_j)) = 0 \quad \text{for } 1 \leq u \leq m.$$

It follows now from [20, Th. 2.24] that

$$c_1 d_i + c_2 d_j = 0.$$

We may assume $c_1 \neq 0$. Hence $\frac{d_i}{d_j} = -\frac{c_2}{c_1} \in \mathrm{GF}(q)$, which is a contradiction to the fact that $\{d_1, d_2, \ldots, d_n\}$ is a complete set of coset representatives of $C_0/\mathrm{GF}(q)^*$. This completes the proof. ■

Even if the two conditions (i.e., $h \mid (q^k+1)$ and $\gcd((r-1)/h(q-1), q-1) = 1$) of Theorem 9 are not satisfied, it

weight	frequency
$\frac{r+(-1)^l q\sqrt{r}}{q(q+1)}$	$\frac{r-1}{q+1}$
$\frac{r+(-1)^{l-1}\sqrt{r}}{q(q+1)}$	$\frac{q(r-1)}{q+1}$
0	1

is still possible that the code $\mathcal{C}(q,h,l,k)$ has only two nonzero weights. However, the two nonzero weights may be different from those of Theorem 9. The following example demonstrates this.

Example 4: Let $q=3$, $l=1$, $k=3$, and $h=2$. In this case, $\mathcal{C}(q,h,l,k)$ is a $[182,6,108]$ cyclic code over GF(3) with the weight distribution

$$1+182x^{108}+546x^{126}.$$

Its dual is a $[182,176,2]$ cyclic code over GF(3).

Corollary 10: Let $k=1, h=q+1$. Let $\gcd(l,q-1)=1$. The set $\mathcal{C}(q,q+1,l,k)$ of (10) is an $[n,m]$ two-weight cyclic linear code over $\mathrm{GF}(q)$ and has the weight distribution in the table at the top of this column:

Furthermore, the dual code $\mathcal{C}(q,h,l,k)^\perp$ of $\mathcal{C}(q,h,l,k)$ is an $[n,n-m,d^\perp]$ linear code with minimum distance $d^\perp \geq 3$.

Proof: Note that

$$\begin{aligned}&\gcd((r-1)/h(q-1),q-1)\\&=\gcd\left(q^{2(kl-1)}+q^{2(kl-2)}+\cdots+q^2+1,q-1\right)\\&=\gcd(kl,q-1)\\&=1.\end{aligned}$$

The conclusion then follows from Theorem 9. ■

Example 5: Let $q=5, l=3, k=1$, and $h=q+1=6$. In this case, we have

$$\gcd((r-1)/h(q-1),q-1)=1.$$

So in this case $\mathcal{C}(q,h,l,k)$ is a $[651,6,500]$ cyclic code over GF(5) with the weight distribution

$$1+2604x^{500}+13020x^{525}.$$

Its dual is a $[651,645,3]$ cyclic code over GF(5).

Finally, we note that the code $\mathcal{C}(q,h,l,k)$ may be sometimes optimal. For example, when $l=k=1, h<q+1, h|(q+1)$ and $\gcd((q+1)/h,q-1)=1, \mathcal{C}(q,h,l,k)$ is a $[(q+1)/h,2,(q+1)/h-1]$ MDS code over $\mathrm{GF}(q)$.

C. Optimal Sets of FH Sequences From a Subclass of Irreducible Cyclic Codes

As before, let p be a prime, $q=p^s, m=2lk, r=q^m$, where s,l, and k are positive integers. Let h be a positive divisor of q^k+1, and so of $(r-1)/(q-1)$.

We are now ready to define a set $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$ of FH sequences using a subset of codewords in the linear code $\mathcal{C}(q,h,l,k)$. Define

$$\mathcal{S}_{\mathcal{C}(q,h,l,k)}=\left\{\mathbf{s}^{(a,i)}:a\in\mathrm{GF}(q)^*,\quad 0\leq i<h\right\}\tag{11}$$

where the sequence

$$\mathbf{s}^{(a,i)}=(a\mathrm{Tr}_{r/q}(\alpha^i d_1),a\mathrm{Tr}_{r/q}(\alpha^i d_2),\ldots,a\mathrm{Tr}_{r/q}(\alpha^i d_n)).$$

Theorem 11: Assume that $\gcd((r-1)/h(q-1),q-1)=1$. Then the set $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$ of FH sequences has parameters

$$\left(\frac{r-1}{h(q-1)},h(q-1),\lambda;q\right)$$

where

$$\lambda=\begin{cases}\frac{r-q+(h-1)(q-1)\sqrt{r}}{hq(q-1)} & l\text{ odd}\\ \frac{r-q+(q-1)\sqrt{r}}{hq(q-1)} & l\text{ even}\end{cases}.\tag{12}$$

Proof: The codeword $\mathbf{c}(g)$ is the zero codeword when and only when $g=0$. This follows from the fact that the dimension of the code $\mathcal{C}(q,h,l,k)$ is m (this is due to the condition that $h<\sqrt{r}+1$).

For any integer $1\leq u\leq n-1$ and any $g\in\mathrm{GF}(r)^*$, by cyclically shifting the codeword $\mathbf{c}(g)$ to the left for u positions, we obtain another codeword which has the expression $\mathbf{c}(g\alpha^{h(q-1)u})$. We now prove that the two codewords are distinct. The difference

$$\mathbf{c}\left(g\alpha^{h(q-1)u}\right)-\mathbf{c}(g)=\mathbf{c}\left(g\left(\alpha^{h(q-1)u}-1\right)\right),$$

which is another codeword in $\mathcal{C}(q,h,l,k)$. Note that $0<u<n=(r-1)/(h(q-1))$. We have that $0<uh(q-1)<r-1$. Hence $g(\alpha^{h(q-1)u}-1)\neq 0$ and $\mathbf{c}(g(\alpha^{h(q-1)u}-1))$ is not the zero codeword.

The foregoing discussions also showed that any two sequences in $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$ cannot be cyclically shifted versions of each other (inequivalent). This justifies the size of the set $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$. Finally, note that $\lambda=n-d$, where d is the minimum nonzero weight in $\mathcal{C}(q,h,l,k)$. The conclusion for λ follows from the weights of the code $\mathcal{C}(q,h,l,k)$ given in the table of Theorem 9. ■

The set $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$ of FH sequences is not optimal in general, but is optimal in the following special case.

Corollary 12: When l is odd, the set $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$ is optimal with respect to the Peng–Fan bound of (3) if and only if $r=q^2$ and $q+1\equiv h \pmod{2h}$. In this case, $\mathcal{S}_{\mathcal{C}(q,h,1,1)}$ has parameters

$$\left(\frac{q+1}{h},h(q-1),1;q\right),$$

and also meets the Singleton bound of (4).

When l is even, the set $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$ is optimal with respect to the Peng–Fan bound of (3) if and only if $p=2, q=p^s, r=q^4$ and $h=q+1$, where s is a positive integer. In this case, $\mathcal{S}_{\mathcal{C}(q,h,2,1)}$ has parameters

$$(q^2+1, q^2-1, q+1; q).$$

Proof: Applying the Peng–Fan bound of (3) to the FH sequence set $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$, we have that

$$M\left(\mathcal{S}_{\mathcal{C}(q,h,l,k)}\right) \geq \left\lceil \frac{r-q}{hq(q-1)} \right\rceil. \tag{13}$$

When l is odd, it follows from (13) that $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$ is optimal with respect to the Peng–Fan bound of (3) if and only if

$$\frac{r-q+(h-1)(q-1)\sqrt{r}}{hq(q-1)} = \left\lceil \frac{r-q}{hq(q-1)} \right\rceil,$$

which is equivalent to

$$\frac{(h-1)(q-1)\sqrt{r}}{hq(q-1)} < 1.$$

That is, $q^{lk} = \sqrt{r} < \frac{h}{(h-1)}q \leq 2q$, i.e., $k=l=1$ and $m=2$.

On the other hand, we have

$$\begin{aligned}\gcd&((r-1)/h(q-1), q-1)\\ &= \gcd((q+1)/h, q+1-2))\\ &= \gcd((q+1)/h, 2).\end{aligned}$$

Hence, $\gcd((r-1)/h(q-1), q-1) = 1$ if and only if $(q+1)/h$ is odd.

When $(q+1)/h$ is odd and $k=l=1$, the set $\mathcal{S}_{\mathcal{C}(q,h,1,1)}$ has parameters $((q+1)/h, h(q-1), 1; q)$. It is easily checked that the Singleton bound of (4) is also met in this case.

For the case that l is even, it follows from (13) that $\mathcal{S}_{\mathcal{C}(q,h,l,k)}$ is optimal with respect to the Peng–Fan bound of (3) if and only if

$$\frac{r-q+(q-1)\sqrt{r}}{hq(q-1)} = \left\lceil \frac{r-q}{hq(q-1)} \right\rceil.$$

This equality is equivalent to that

$$\frac{(q-1)\sqrt{r}}{hq(q-1)} < 1 \tag{14}$$

which implies $\sqrt{r} < hq \leq (q^k+1)q$ due to the fact that $h|(q^k+1)$. Since $\sqrt{r} = q^{lk}$ is a power of q, one has $q^{lk} \leq q^{k+1}$ and $k(l-1) \leq 1$, i.e., $l=2$ and $k=1$ since l is even. Then $r=q^4$ and $h|(q+1)$. Inequality (14) implies that $h>q$ and then $h=q+1$ because $h|(q+1)$. Note that

$$\begin{aligned}\gcd&\left(\frac{r-1}{h(q-1)}, q-1\right)\\ &= \gcd\left(\frac{r-1}{(q-1)(q+1)}, q-1\right)\\ &= \gcd(q^2+1, q-1).\end{aligned}$$

We have that $\gcd((r-1)/h(q-1), q-1) = 1$ if and only if $p=2$. This completes the proof. ■

For even l, the sufficient condition for the optimality of the set $\mathcal{S}_{\mathcal{C}(q,m,l,k)}$ has been obtained in [8]. While the necessary condition is further derived in Corollary 12. As for odd l, the result of Corollary 12 is new. Clearly, the construction of this section is a generalization of the one in [8, Sect. V].

Example 6: Let $q=3^2$ and let $h=2$. Let α be a generator of $\mathrm{GF}(q^2)^*$ defined by $\alpha^4+2\alpha^3+2=0$ and u be the generator of $\mathrm{GF}(q)^*$ defined by $u^2+2u+2=0$. Then the set $\mathcal{S}_{\mathcal{C}(q,h,1,1)}$ has parameters (5, 16, 1; 9) and consists of the following 16 sequences:

$$\begin{array}{ccc}(2,u^5,u^7,u^7,u^5), & (u^3,1,2,u^7,0), & (u^5,u^6,1,1,u^6)\\ (2,u,u^5,1,0), & (u^6,u^7,u,u,u^7), & (u^5,u^2,u^6,u,0)\\ (u^7,1,u^2,u^2,1), & (u^6,u^3,u^7,u^2,0), & (1,u,u^3,u^3,u)\\ (u^7,2,1,u^3,0), & (u,u^2,2,2,u^2), & (1,u^5,u,2,0)\\ (u^2,u^3,u^5,u^5,u^3), & (u,u^6,u^2,u^5,0), & (u^3,2,u^6,u^6,2)\\ (u^2,u^7,u^3,u^6,0). & & \end{array}$$

IV. Summary of Contributions

In this paper, we released the conditions of the construction of optimal sets of FH sequences using a subcode of the Reed–Solomon codes given in [8], and obtained new parameters of optimal sets of FH sequences. We described sets of FH sequences using a class of two-weight irreducible cyclic codes and proved that the sets of FH sequences are optimal under certain conditions. As a byproduct, we determined the weight distribution of a subclass of irreducible cyclic codes. All the constructions in this paper are either an extension or a generalization of some of the constructions in [8].

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] L. D. Baumert and R. J. McEliece, “Weights of irreducible cyclic codes,” *Inf. Contr.*, vol. 20, no. 2, pp. 158–175, 1972.

[2] L. D. Baumert and J. Mykkeltveit, “Weight distributions of some irreducible cyclic codes,” *DSN Progress Rep.*, vol. 16, pp. 128–131, 1073.

[3] R. Calderbank and W. M. Kantor, “The geometry of two-weight codes,” *Bull. London Math. Soc.*, vol. 18, pp. 97–122, 1986.

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

[5] P. Delsarte and J. M. Goethals, “Irreducible binary cyclic codes of even dimension,” in *Proc. 2nd Chapel Hill Conf. on Combinator. Math. Appl.*, 1970, pp. 100–113, Univ. North Carolina, Chapel Hill, NC.

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

[7] C. Ding, “The weight distribution of some irreducible cyclic codes,” *IEEE Trans. Inf. Theory*, vol. 55, no. 3, pp. 955–960, Mar. 2009.

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

[9] C. Ding, J. Luo, and H. Niederreiter, “Two-weight codes punctured from irreducible cyclic codes,” in *Proc. 1st Int. Workshop on Coding Theory and Cryptogr.*, Y. Li, S. Ling, H. Niederreiter, H. Wang, C. Xing, and S. Zhang, Eds., Singapore, 2008, pp. 119–124, World Scientific.

[10] 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.

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

[12] R. W. Fitzgerald and J. L. Yucas, "Sums of Gauss sums and weights of irreducible codes," *Finite Fields and Their Appl.*, vol. 11, pp. 89–110, 2005.

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

[14] 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.

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

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

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

[18] P. Langevin, "A new class of two weight codes," in *Finite Fields and Applications*, S. Cohen and H. Niederreiter, Eds. Cambridge, U.K.: Cambridge Univ. Press, 1996, pp. 181–187.

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

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

[21] F. MacWilliams and J. Seery, "The weight distributions of some minimal cyclic codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 6, pp. 796–806, 1981.

[22] R. J. McEliece, "A class of two-weight codes," *Jet Propulsion Lab. Space Program Summary 37–41*, vol. IV, pp. 264–266.

[23] R. J. McEliece, "Irreducible cyclic codes and Gauss sums," in *Combinatorics, Part 1: Theory of Designs, Finite Geometry and Coding Theory*, 1974, Math. Centre Tracts, no. 55, 179–96, Amsterdam, The Netherlands: Math. Centrum.

[24] R. J. McEliece and H. Rumsey Jr., "Euler products, cyclotomy, and coding," *J. Number Theory*, vol. 4, pp. 302–311, 1972.

[25] M. J. Moisio, "A note on evaluations of some exponential sums," *Acta Arith.*, vol. 93, pp. 117–119, 2000.

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

[27] R. A. Scholtz, "The spread spectrum concept," *IEEE Trans. Commun.*, vol. 25, pp. 748–755, 1977.

[28] B. Schmidt and C. White, "All two-weight irreducible cyclic codes?," *Finite Fields and Their Appl.*, vol. 8, pp. 1–17, 2002.

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

[30] M. van der Vlugt, "Hasse-Davenport curves, Gauss sums, and weight distributions of irreducible cyclic codes," *J. Number Theory*, vol. 55, pp. 145–159, 1995.

[31] G. Vega and J. Wolfmann, "New classes of 2-weight cyclic codes," *Des. Codes Cryptogr.*, vol. 42, pp. 327–334, 2007.

[32] J. Wolfmann, "Codes projectifs à deux poids, "caps" complets et ensembles de différences," *J. Comb. Theory Ser. A*, vol. 23, pp. 208–222, 1977.

[33] J. Wolfmann, "Are 2-weight projective cyclic codes irreducible?," *IEEE Trans. Inf. Theory*, vol. 51, pp. 733–737, 2005.

[34] J. Wolfmann, "Projective two-weight irreducible cyclic and constacyclic codes," *Finite Fields and Their Appl.*, vol. 14, no. 2, pp. 351–360, Apr. 2008.

[35] J. Yin, "A construction of optimal sets of FH sequences," in *Proc. 1st Int. Workshop on Coding and Cryptol.*, Y. Li, S. Lin, H. Niederreiter, H. Wang, C. Xing, and S. Zhang, Eds., Wuyi Mountain, China, Jun. 11–15, 2007, pp. 268–276.

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 was a corecipient of the State Natural Science Award of China in 1989. He has served as a guest editor or editor for 10 journals.

Yang Yang (S'09) was born in Hubei Province, China, on January 4, 1983. He received the B.S. and M.S. degrees from Hubei University, Wuhan, China, in 2005 and 2008, respectively.

He is currently working toward the Ph.D. degree with Southwest Jiaotong University, Chengdu, China. His research interest includes sequences and cryptography.

Xiaohu Tang (M'04) received the B.S. degree in applied mathematics from the Northwest Polytechnic University, Xi'an, China, the M.S. degree in applied mathematics from the Sichuan University, Chengdu, China, and the Ph.D. degree in electronic engineering from the Southwest Jiaotong University, Chengdu, in 1992, 1995, and 2001, respectively.

From 2003 to 2004, he was a Postdoctoral member with the Department of Electrical and Electronic Engineering, The Hong Kong University of Science and Technology. From 2007 to 2008, he was a Visiting Professor with the University of Ulm, Germany. Since 2001, he has been with the Institute of Mobile Communications, Southwest Jiaotong University, where he is currently a professor. His research interests include sequence design, coding theory, and cryptography.

Dr. Tang was the recipient of the National excellent Doctoral Dissertation award in 2003 (China) and the Humboldt Research Fellowship in 2007 (Germany).