Des. Codes Cryptogr.
DOI 10.1007/s10623-012-9652-z

A new frequency-hopping sequence set based upon generalized cyclotomy

Fang Liu · Daiyuan Peng · Zhengchun Zhou · Xiaohu Tang

Received: 7 May 2011 / Revised: 21 February 2012 / Accepted: 6 March 2012

Abstract In this paper, a new set of frequency-hopping sequences is proposed, and the Hamming correlation distribution of the new set is investigated. The construction of new frequency hopping sequences is based upon generalized cyclotomy. It is shown that the proposed frequency-hopping sequence set is optimal with respect to the average Hamming correlation bound.

Keywords Frequency-hopping sequence · Average Hamming correlation · Generalized cyclotomy

Mathematics Subject Classification 94A55 · 94B05

1 Introduction

Frequency-hopping code-division multiple-access (FH-CDMA) is widely used in modern communication systems such as Bluetooth, ultra-wideband (UWB), military or radar applications, etc. In a FH system, the wideband signal is generated by hopping from one frequency

Communicated by A. Pott.

F. Liu (✉) · D. Peng · X. Tang
Provincial Key Lab of Information Coding and Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, China
e-mail: hmimy5416@163.com

D. Peng
e-mail: dypeng@swjtu.edu.com

X. Tang
e-mail: xhutang@ieee.org

Z. Zhou
School of Mathematics, Southwest Jiaotong University, Chengdu, China
e-mail: zzc@home.swjtu.edu.cn

Published online: 10 April 2012

slot to another over a large number of frequency slots. The frequency slots used are chosen pseudorandomly by codes called frequency-hopping (FH) sequences. The receiver is confronted with the interference caused by undesired signals when it attempts to demodulate one of the signals from several transmitters in FH-CDMA systems. Generally, it is very desirable to keep the mutual interference, or the Hamming crosscorrelations and the out-of-phase Hamming autocorrelations of the FH sequences employed, as low as possible. On the other hand, it is also preferred to have more FH sequences accommodating more distinct users. As a consequence, the need for finding FH sequences which have simultaneously low Hamming correlation and large family size is therefore well motivated.

There are two kinds of measurement for the Hamming correlation of FH sequences: one is the maximum Hamming correlation [1,2] and another is the average Hamming correlation [3]. The design of FH sequences remains of great interest. Among of them, most have been devoted to the maximum Hamming correlation property. The average Hamming correlation (or average of hits) indicates the average error (or interference) performance of the FH-CDMA systems, the design of optimal FH sequences with respect to the optimal average Hamming correlation property is very meaningful as well.

A generalized cyclotomy with respect to $n = pq$ was introduced by Whiteman [4], where p and q are two different odd prime numbers. When n is a prime, it is referred to as classical cyclotomy. Some optimal or near-optimal FH sequence sets with respect to the maximum Hamming correlation bound were constructed based on classical cyclotomy [5–7]. Whiteman's generalized cyclotomy has been widely applied to design difference sets [4,8], as well as to construct binary sequences with good correlation properties (but, not Hamming correlation) [9–11]. In this paper, we construct a new set of FH sequences based on Whiteman's generalized cyclotomy and investigate the average Hamming correlation of the FH sequence set. It is shown that the set of FH sequences is an optimal average Hamming correlation set.

The outline of this paper is as follows. In Sect. 2, we give some preliminaries on FH sequences, and review some bounds on the maximum and average Hamming correlation, respectively. In Sect. 3, we introduce the definition and some fundamental properties of Whiteman's generalized cyclotomy and the corresponding cyclotomic numbers. In Sect. 4, we give some basic lemmas that are needed to prove our main results. In Sect. 5, we focus on a new construction of the FH sequence set, and determine the Hamming correlation value of the FH sequences.

2 Preliminaries

Let $\mathcal{F} = \{f_0, f_1, \ldots, f_{v-1}\}$ be a set of available frequencies called a frequency library. Let $\mathcal{U}$ be a set of M FH sequences of length L over $\mathcal{F}$. Given two sequences $X = \{x_0, x_1, \ldots, x_{L-1}\}$ and $Y = \{y_0, y_1, \ldots, y_{L-1}\}$ in $\mathcal{U}$, the periodic Hamming cross-correlation function of X and Y is defined by

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

where $h[x_t, y_{t+\tau}] = 1$ if $x_t = y_{t+\tau}$, and 0 otherwise, and the subscript addition is calculated modulo L. When $X = Y$, $H_{X,Y}(\tau)$ is called the Hamming autocorrelation function of X. In this case, we denote it by $H_X(\tau)$.

The maximum Hamming autocorrelation sidelobe $H(X)$ of X and the maximum Hamming crosscorrelation $H(X, Y)$ between X and Y are defined, respectively, by

$$H(X) = \max_{1 \le \tau < L} \{H_X(\tau)\},$$
$$H(X, Y) = \max_{0 \le \tau < L} \{H_{X,Y}(\tau)\}.$$

To estimate these measures for a single FH sequence or a pair of FH sequences, Lempel and Greenberger established the first bound in 1974, known as the Lempel-Greenberger bound.

Lemma 1 *(*The Lempel-Greenberger bound [1]*) For any FH sequence X of length L over $\mathcal{F}$ with $|\mathcal{F}| = v$,*

$$H(X) \ge \left\lceil \frac{(L-b)(L+b-v)}{v(L-1)} \right\rceil,$$

where b denotes the nonnegative residue of L modulo v, and $\lceil x \rceil$ denotes the smallest integer greater than or equal to x.

For any given FH sequence set $\mathcal{U}$, the maximum Hamming autocorrelation sidelobe $H_a(\mathcal{U})$ and the maximum Hamming crosscorrelation $H_c(\mathcal{U})$ are defined, respectively, by

$$H_a(\mathcal{U}) = \max_{X \in \mathcal{U}} \{H(X)\},$$
$$H_c(\mathcal{U}) = \max_{X,Y \in \mathcal{U}, X \ne Y} \{H(X, Y)\}.$$

In 2004, Peng and Fan took account of the number of sequences in the family and then developed the following bound.

Lemma 2 *(*The Peng-Fan bound [2]*) Let $\mathcal{U}$ be a set of M FH sequences of length L over a frequency slot set $\mathcal{F}$ with $|\mathcal{F}| = v$, and $I = \lfloor LM/v \rfloor$, where $\lfloor x \rfloor$ denotes the largest integer less than or equal to x. Then*

$$(L-1)vH_a + (M-1)LvH_c \ge (LM - v)L. \tag{1}$$

Another important performance indicator of the FH sequences is the average Hamming correlation defined as follows.

Definition 1 **([12])** Let $\mathcal{U}$ be a set of M FH sequences of length L over a given frequency slot set $\mathcal{F}$ with size v, we call

$$S_a(\mathcal{U}) = \sum_{X \in \mathcal{U}, 1 \le \tau < L} H_X(\tau),$$
$$S_c(\mathcal{U}) = \frac{1}{2} \sum_{X,Y \in \mathcal{U}, X \ne Y, 0 \le \tau < L} H_{X,Y}(\tau)$$

the overall number of Hamming autocorrelation and Hamming crosscorrelation of $\mathcal{U}$ respectively, and call

$$A_a(\mathcal{U}) = \frac{S_a(\mathcal{U})}{M(L-1)}, \tag{2}$$

$$A_c(\mathcal{U}) = \frac{2S_c(\mathcal{U})}{LM(M-1)} \tag{3}$$

the average Hamming autocorrelation and the average Hamming crosscorrelation of $\mathcal{U}$ respectively.

For simplicity, we denote $H_a = H_a(\mathcal{U})$, $H_c = H_c(\mathcal{U})$, $S_a = S_a(\mathcal{U})$, $S_c = S_c(\mathcal{U})$, $A_a = A_a(\mathcal{U})$ and $A_c = A_c(\mathcal{U})$.

In 2008, Peng et al. derived the following theoretical limit which gave a bounded relation among the parameters v, L, M, A_a and A_c.

Lemma 3 ([13]) *Let $\mathcal{U}$ be a set of M FH sequences of length L over a given frequency slot set $\mathcal{F}$ with size v, A_a and A_c be the average Hamming autocorrelation and the average Hamming crosscorrelation of $\mathcal{U}$, respectively. Then*

$$\frac{A_a}{L(M-1)} + \frac{A_c}{L-1} \geq \frac{LM-v}{v(L-1)(M-1)}. \tag{4}$$

Hereafter, we use the following definitions:

(1) A FH sequence $X \in \mathcal{U}$ is called optimal if the Lempel-Greenberger bound in Lemma 1 is met.
(2) A FH sequence set $\mathcal{U}$ is an optimal set with respect to the maximum Hamming correlation bound if H_a and H_c of $\mathcal{U}$ is a pair of the minimum integer solutions of inequality (1).
(3) A FH sequence set $\mathcal{U}$ is an optimal set with respect to the average Hamming correlation bound if A_a and A_c of $\mathcal{U}$ satisfy inequality (4) with equality.

Note that an optimal FH sequence set with respect to the maximum Hamming correlation bound is not necessarily optimal with respect to the average Hamming correlation bound. Similarly, an optimal FH sequence set with respect to the average Hamming correlation bound may not be optimal with respect to the maximum Hamming correlation bound [14]. In recent years, the constructions of optimal FH sequences with respect to the maximum Hamming correlation bound have been studied by many researchers [5,6,15–18]. Several FH sequence sets with optimal average Hamming correlation have been reported [3,12–14,19].

3 Generalized cyclotomy and cyclotomic number

Let p and q be two different odd primes with $\gcd(p-1, q-1) = e$. According to the Chinese Remainder Theorem, there exists a common primitive root of p and q, say g. Let x be an integer simultaneously satisfying the congruences

$$\begin{cases} x \equiv g (\mathrm{mod}\ p), \\ x \equiv 1 (\mathrm{mod}\ q). \end{cases}$$

Let $d = (p-1)(q-1)/e$, $f_1 = (p-1)/e$, $f_2 = (q-1)/e$, and $L = pq$. Thus, we can get a multiplicative subgroup of the residue ring $\mathbf{Z}_L$ as follows [4]

$$\mathbf{Z}_L^* = \{g^s x^i : s = 0, 1, \ldots, d-1; i = 0, 1, \ldots, e-1\}.$$

Let $\mathbf{Z}_L^*$ denote the set of all invertible elements of $\mathbf{Z}_L$. The Whiteman's generalized cyclotomic classes D_i, $0 \leq i \leq e-1$, of order e are defined by

$$D_i = \{g^s x^i : s = 0, 1, \ldots, d-1\},$$

where the multiplication is performed modulo L. Obviously, $\mathbf{Z}_L^* = \bigcup_{i=0}^{e-1} D_i$.

Define

$$P = \{p, 2p, \ldots, (q-1)p\},$$
$$Q = \{q, 2q, \ldots, (p-1)q\},$$
$$R = \{0\}.$$

Let H be a subset of $\mathbf{Z}_L$ and a be an element of $\mathbf{Z}_L$. Define

$$H + a = \{h + a : h \in H\}, \qquad a \cdot H = \{a \cdot h : h \in H\}.$$

For fixed i and j with $0 \le i, j \le e-1$, the corresponding generalized cyclotomic numbers of order e are defined by

$$(i, j) = |(D_i + 1) \cap D_j|. \tag{5}$$

Now we give two fundamental properties of the generalized cyclotomic numbers.

Lemma 4 *([8]) The cyclotomic numbers defined by (5) have the following properties:*

(1)

$$(i, j) = (e - i, j - i);$$

(2)

$$\sum_{i=0}^{e-1}(i, j) = \frac{(p-2)(q-2)-1}{e} + \varepsilon_j,$$

where

$$\varepsilon_j = \begin{cases} 1, & \text{if } j = 0 \\ 0, & \text{otherwise.} \end{cases}$$

4 Basic lemmas

In this section, we will give some useful lemmas for determining the Hamming correlation of our FH sequence set defined in the next section.

Lemma 5

$$\sum_{i=0}^{e-1}(k + i, i) = \begin{cases} \frac{(p-2)(q-2)-1}{e} + 1, & \text{if } k = 0 \\ \frac{(p-2)(q-2)-1}{e}, & \text{otherwise.} \end{cases}$$

Proof From item (1) of Lemma 4, we have

$$\sum_{i=0}^{e-1}(k + i, i) = \sum_{i=0}^{e-1}(e - k - i, -k) = \sum_{i=0}^{e-1}(i, -k)$$

Then the assertion follows from item (2) of Lemma 4. □

Lemma 6 ([4]) *For any $k \in \mathbf{Z}_e \backslash \{0\}$, we have*

(1) $\sum_{i=0}^{e-1} |(D_i + w) \cap D_i| = \begin{cases} ef_1(f_2 - 1), & \text{if } w \in P \\ ef_2(f_1 - 1), & \text{if } w \in Q \\ \frac{(p-2)(q-2)-1}{e} + 1, & \text{if } w \in \mathbf{Z}_L^*; \end{cases}$

(2) $\sum_{i=0}^{e-1} |(D_{i+k} + w) \cap D_i| = \begin{cases} ef_1f_2, & \text{if } w \in P \cup Q \\ \frac{(p-2)(q-2)-1}{e}, & \text{if } w \in \mathbf{Z}_L^*. \end{cases}$

Lemma 7

$$|((Q \cup R) + w) \cap (Q \cup R)| = \begin{cases} 0, & \text{if } w \in P \cup \mathbf{Z}_L^* \\ p, & \text{if } w \in Q \cup R \end{cases}$$

and

$$|(P + w) \cap P| = \begin{cases} q-2, & \text{if } w \in P \\ q-1, & \text{if } w = 0 \\ 0, & \text{otherwise.} \end{cases}$$

Proof This lemma is obvious, so we omit the proof. □

Lemma 8 *Given* $0 \le i \le e-1$, *then*

$$|(D_i + w) \cap (Q \cup R)| = \begin{cases} 0, & \text{if } w \in Q \\ f_1, & \text{if } w \in P \cup \mathbf{Z}_L^* \end{cases}$$

and

$$|(D_i + w) \cap (P \cup R)| = \begin{cases} 0, & \text{if } w \in P \\ f_2, & \text{if } w \in Q \cup \mathbf{Z}_L^*. \end{cases}$$

Proof We only prove the first equation since the second one is similar.

When $w \in Q$, $|(D_i + w) \cap (Q \cup R)| = 0$ is clear. As for $w \in P \cup \mathbf{Z}_L^*$, an element $z = g^s x^i + w \in (Q \cup R)$, $0 \le s < d$, $0 \le i \le e-1$, if and only if

$$g^s + w \equiv 0 (\text{mod } q) \tag{6}$$

in which we make use of the fact that $x \equiv 1 (\text{mod } q)$. Obviously, only one s_1 in $\mathbf{Z}_q$ satisfies (6). Then, there are f_1 solutions $0 \le s < d$ to (6), i.e., $s = s_1 + t(q-1)$, $0 \le t < f_1$, $0 \le s_1 < q$.

Lemma 9 ([11]) *Let* $m_1, \ldots, m_t$ *be positive integers. For a set of integers* $a_1, \ldots, a_t$, *the system of congruences*

$$y \equiv a_i (mod\ m_i) \text{ for } i = 1, \ldots, t$$

has solutions if and only if

$$a_i \equiv a_j (\text{mod } \gcd(m_i, m_j)), i \ne j, 1 \le i, j \le t. \tag{7}$$

If (7) *is satisfied, the solution is unique modulo* $lcm(m_1, \ldots, m_t)$. □

Lemma 10 *Let* $p = ef_1 + 1$ *and* $q = ef_2 + 1$, *then* $-1 \in D_0$ *if* $|f_1 - f_2|$ *is even, and* $-1 \in D_{e/2}$ *if* $|f_1 - f_2|$ *is odd.*

Proof Suppose that $-1 \in D_i$, where $0 \le i \le e-1$, then there exists an integer s with $0 \le s \le d-1$,

$$g^s x^i \equiv -1 (\text{mod } pq). \tag{8}$$

By the Chinese Remainder Theorem, (8) is equivalent to

$$g^{s+i} \equiv -1 (\text{mod } p) \text{ and } g^s \equiv -1 (\text{mod} q)$$

which further implies

$$s + i \equiv (p-1)/2 (\mathrm{mod}\ p-1) \text{ and } s \equiv (q-1)/2 (\mathrm{mod}\ q-1) \tag{9}$$

According to Lemma 9, (9) has a solution if and only if

$$i \equiv (p-q)/2 (\mathrm{mod}\ e) \Leftrightarrow i \equiv (f_1 - f_2)e/2 (\mathrm{mod}\ e).$$

Therefore, we have $-1 \in D_0$ if $|f_1 - f_2|$ is even and $-1 \in D_{e/2}$ otherwise. □

Lemma 11 *For any* $0 \le i \le e-1$, *we have*

(1)

$$|(D_i + w) \cap P| = \begin{cases} 0, & \text{if } w \in P \\ f_2, & \text{if } w \in Q \\ f_2 - 1, & \text{if } w \in D_i \text{ and } |f_1 - f_2| \text{ is even} \\ f_2, & \text{if } w \in \mathbf{Z}_L^* \backslash D_i \text{ and } |f_1 - f_2| \text{ is even} \\ f_2 - 1, & \text{if } w \in D_{e/2+i} \text{ and } |f_1 - f_2| \text{ is odd} \\ f_2, & \text{if } w \in \mathbf{Z}_L^* \backslash D_{e/2+i} \text{ and } |f_1 - f_2| \text{ is odd}; \end{cases}$$

(2)

$$|(P + w) \cap D_i| = \begin{cases} 0, & \text{if } w \in P \\ f_2, & \text{if } w \in Q \cup (\mathbf{Z}_L^* \backslash D_i) \\ f_2 - 1, & \text{if } w \in D_i. \end{cases}$$

Proof For (1), note that

$$|(D_i + w) \cap P| = |(D_i + w) \cap (P \cup R)| - |(D_i + w) \cap R|.$$

By Lemma 10, we have

$$|(D_i + w) \cap R| = \begin{cases} 0, \text{ if } w \in P \cup Q \\ 0, \text{ if } w \in \mathbf{Z}_L^* \backslash D_i \text{ and } |f_1 - f_2| \text{ is even} \\ 0, \text{ if } w \in \mathbf{Z}_L^* \backslash D_{e/2+i} \text{ and } |f_1 - f_2| \text{ is odd} \\ 1, \text{ if } w \in D_i \text{ and } |f_1 - f_2| \text{ is even} \\ 1, \text{ if } w \in D_{e/2+i} \text{ and } |f_1 - f_2| \text{ is odd} \end{cases} \tag{10}$$

Then the conclusion follows from Lemma 8 and Eq. (10).

For (2), we have

$$|(P + w) \cap D_i| = |P \cap (D_i - w)| = |(P \cup R) \cap (D_i - w)| - |R \cap (D_i - w)|.$$

Applying Lemma 8, we arrive at the conclusion. □

Lemma 12 ([11])

$$|(P + w) \cap (Q \cup R)| = \begin{cases} 0, & \text{if } w \in Q \\ 1, & \text{if } w \in P \cup \mathbf{Z}_L^*. \end{cases}$$

5 New construction of FH sequences based on Whiteman's generalized cyclotomy

In this section, we construct a new set of FH sequences with optimal average Hamming correlation property.

Let

$$\begin{aligned} C_0 &= D_0 \cup Q \cup R, \\ C_i &= D_i, \text{ for } 1 \le i < e \text{ and } i \ne e/2, \\ C_{e/2} &= D_{e/2} \cup P. \end{aligned}$$

Then, $\bigcup_{i=0}^{e-1} C_i = \mathbf{Z}_L$ and $C_i \cap C_j = \emptyset$ for $i \ne j$.

Let $X = \{x_0, x_1, \ldots, x_{L-1}\}$ be a sequence of length L over a frequency slot set $\mathcal{F}$. Then $supp_X(k) = \{t | x_t = k, 0 \le t \le L-1\}$ is called the support of $k \in \mathcal{F}$ in the sequence X.

Definition 2 Define a FH sequence set $\mathcal{U} = \{X^{(i)}, i = 0, 1, \ldots, e-1\}$ of length $L = pq$, where $X^{(i)} = \{x_0^{(i)}, x_1^{(i)}, \ldots, x_{L-1}^{(i)}\}$ is defined by

$$supp_{X^{(i)}}(j) = C_{j+i}, 0 \le j < e,$$

where $j + i$ is reduced modulo e.

Based on the lemmas in the last section, we are now ready to determine the Hamming correlation properties of the FH sequence set $\mathcal{U}$.

Theorem 1 *Let p and q be different odd primes with $\gcd(p-1, q-1) = e$. Define $p = ef_1 + 1$ and $q = ef_2 + 1$, then the FH sequence set $\mathcal{U}$ over $\mathcal{F}$ have the following properties:*

(1) *The family size is $M = e$, the sequence length $L = pq$, and $|\mathcal{F}| = e$;*
(2) *The Hamming autocorrelation function of $X^{(k)} \in \mathcal{U}$ for $0 \le k < e$ is given by*

$$H_{X^{(k)}, X^{(k)}}(w) = \begin{cases} \frac{pq-1}{e} + \frac{p-q}{e} + q - p - 1, & \text{if } w \in P \\ \frac{pq-1}{e} + \frac{q-p}{e} + p - q + 1, & \text{if } w \in Q \\ \frac{pq-1}{e} - 1, & \text{if } w \in D_{e/2} \text{ and } |f_1 - f_2| \text{ is even} \\ \frac{pq-1}{e}, & \text{if } w \in D_0 \cup D_{e/2} \text{ and } |f_1 - f_2| \text{ is odd} \\ \frac{pq-1}{e} + 1, & \text{if } w \in D_0 \text{ and } |f_1 - f_2| \text{ is even} \\ \frac{pq-1}{e} + 1, & \text{if } w \in D_i \text{ for } i \ne 0, e/2. \end{cases}$$

(3) *The Hamming crosscorrelation function of any two distinct FH sequences $X^{(k)}, X^{(l)} \in \mathcal{U}$ for $k \ne l$ is given by*

(3.1) When $l - k \equiv e/2 (mod\ e)$

$$H_{X^{(k)}, X^{(l)}}(w) = \begin{cases} 0, & \text{if } w = 0 \\ \frac{pq-1}{e} + \frac{p-q}{e} + 2, & \text{if } w \in P \\ \frac{pq-1}{e} + \frac{q-p}{e}, & \text{if } w \in Q \\ \frac{pq-1}{e} + 2, & \text{if } w \in D_{e/2} \text{ and } |f_1 - f_2| \text{ is even} \\ \frac{pq-1}{e} + 1, & \text{if } w \in D_0 \cup D_{e/2} \text{ and } |f_1 - f_2| \text{ is odd} \\ \frac{pq-1}{e}, & \text{if } w \in D_0 \text{ and } |f_1 - f_2| \text{ is even} \\ \frac{pq-1}{e} + 2, & \text{if } w \in D_i \text{ for } i \ne 0, e/2. \end{cases}$$

(3.2) When $2(l-k) \equiv e/2 (mod\ e)$,

$$H_{X^{(k)},X^{(l)}}(w) = \begin{cases} 0, & \text{if } w = 0 \\ \frac{pq-1}{e} + \frac{p-q}{e}, & \text{if } w \in P \\ \frac{pq-1}{e} + \frac{q-p}{e}, & \text{if } w \in Q \\ \frac{pq-1}{e} - 1, & \text{if } w \in D_{l-k} \cup D_{l-k+e/2} \text{ and } |f_1 - f_2| \text{ is even} \\ \frac{pq-1}{e} - 2, & \text{if } w \in D_{l-k} \text{ and } |f_1 - f_2| \text{ is odd} \\ \frac{pq-1}{e}, & \text{if } w \in D_{l-k+e/2} \text{ and } |f_1 - f_2| \text{ is odd} \\ \frac{pq-1}{e}, & \text{if } w \in D_i \text{ for } i \neq l-k, l-k+e/2. \end{cases}$$

(3.3) When $2(l-k) \neq e/2 (mod\ e)$ *and* $l-k \neq e/2 (mod\ e)$,

$$H_{X^{(k)},X^{(l)}}(w) = \begin{cases} 0, & \text{if } w = 0 \\ \frac{pq-1}{e} + \frac{p-q}{e}, & \text{if } w \in P \\ \frac{pq-1}{e} + \frac{q-p}{e}, & \text{if } w \in Q \\ \frac{pq-1}{e}, & \text{if } w \in D_{l-k} \text{ and } |f_1 - f_2| \text{ is even} \\ \frac{pq-1}{e} - 1, & \text{if } w \in D_{l-k} \text{ and } |f_1 - f_2| \text{ is odd} \\ \frac{pq-1}{e} - 1, & \text{if } w \in D_{l-k+e/2} \text{ and } |f_1 - f_2| \text{ is even} \\ \frac{pq-1}{e}, & \text{if } w \in D_{l-k+e/2} \text{ and } |f_1 - f_2| \text{ is odd} \\ \frac{pq-1}{e}, & \text{if } w \in D_i \text{ for } i \neq l-k, l-k+e/2, k-l+e/2 \\ \frac{pq-1}{e} - 1, & \text{if } w \in D_{k-l+e/2}. \end{cases}$$

Proof (1) is clear.

Concerning (2), the Hamming autocorrelation of $X^{(k)}$ at shift w is

$$\begin{aligned} H_{X^{(k)},X^{(k)}}(w) = &\sum_{i=0}^{e-1} |(D_i + w) \cap D_i| + |(D_0 + w) \cap (Q \cup R)| \\ &+ |((Q \cup R) + w) \cap D_0| + |(P + w) \cap P| + |(D_{e/2} + w) \cap P| \\ &+ |(P + w) \cap D_{e/2}| + |((Q \cup R) + w) \cap (Q \cup R)|. \end{aligned}$$

Then by Lemmas 6, 7, 8, and 11, the result follows.

Regarding (3), for any FH sequences $X^{(k)}, X^{(l)} \in \mathcal{U}$ with $k \neq l$ and $0 \leq k, l \leq e-1$, their Hamming crosscorrelation function at shift w is given by

$$H_{X^{(k)},X^{(l)}}(w) = \sum_{i=0}^{e-1} |(C_{i+l} + w) \cap C_{i+k}|.$$

When $l - k \equiv e/2 (\text{mod } e)$, we have

$$\begin{aligned} H_{X^{(k)},X^{(l)}}(w) = &\sum_{i=0}^{e-1} |(D_{i+e/2} + w) \cap D_i| + |((Q \cup R) + w) \cap D_{e/2}| \\ &+ |((Q \cup R) + w) \cap P| + |(D_0 + w) \cap P| + |(D_{e/2} + w) \cap (Q \cup R)| \\ &+ |(P + w) \cap (Q \cup R)| + |(P + w) \cap D_0|. \end{aligned}$$

Applying Lemmas 6, 8, 11 and 12 to the above equation, the conclusion in (3.1) follows.

While for any FH sequences $X^{(k)}$, $X^{(l)} \in \mathcal{U}$ with $l - k \neq e/2 (\mathrm{mod}\, e)$, their Hamming crosscorrelation function at shift w is given by

$$\begin{aligned} H_{X^{(k)},X^{(l)}}(w) = \sum_{i=0}^{e-1} & |(D_{i+l-k} + w) \cap D_i| + |(D_{l-k} + w) \cap (Q \cup R)| \\ & + |(D_{l-k+e/2} + w) \cap P| + |((Q \cup R) + w) \cap D_{k-l}| \\ & + |(P + w) \cap D_{k-l+e/2}|. \end{aligned}$$

When $2(l-k) \equiv e/2 (\mathrm{mod}\, e)$, it is easily verified that $|(P + w) \cap D_{k-l+e/2}| = |(P + w) \cap D_{l-k}|$. Therefore, the equation in (3.2) follows immediately from Lemmas 6, 8, and 11. Similarly, when $2(l-k) \neq e/2 (\mathrm{mod}\, e)$, from Lemmas 6, 8, and 11, the desired result in (3.3) follows, which completes the proof. □

Theorem 2 *The average Hamming autocorrelation and average Hamming crosscorrelation of the FH sequence set $\mathcal{U}$ are respectively as follows*

$$\begin{aligned} A_a(\mathcal{U}) &= \frac{S_a(\mathcal{U})}{M(L-1)} \\ &= \frac{(pq-1)^2 + e(q^2+p^2)}{e(pq-1)} + \frac{e(1-pq) - 2eq - (q-1)^2 - (p-1)^2}{e(pq-1)}, \end{aligned} \tag{11}$$

$$\begin{aligned} A_c(\mathcal{U}) &= \frac{2S_c(\mathcal{U})}{LM(M-1)} \\ &= \frac{(e-1)(pq-1)^2 + 2ep(q-1)}{pqe(e-1)} - \frac{(e-1)((q-1)^2 + (p-1)^2)}{pqe(e-1)}. \end{aligned} \tag{12}$$

The FH sequence set $\mathcal{U}$ is optimal with respect to the average Hamming correlation bound.

Proof When $|f_1 - f_2|$ is even, according to the definitions of S_a and S_c, we have

$$\begin{aligned} S_a &= \sum_{0 \le i \le e-1,\ 1 \le \tau \le L-1} H_{X^{(i)}}(\tau) \\ &= e\left\{(q-1)\left(\frac{pq-1}{e} + q - p + \frac{p-q}{e} - 1\right) + (p-1)\left(\frac{pq-1}{e} + p - q\right.\right. \\ &\quad \left.\left. + \frac{q-p}{e} + 1\right) + d\left(\frac{pq-1}{e} - 1\right) + d\left(\frac{pq-1}{e} + 1\right) + (e-2)d\left(\frac{pq-1}{e} + 1\right)\right\} \\ &= (pq-1)^2 + e(q^2+p^2) + e(1-pq) - 2eq - (q-1)^2 - (p-1)^2 \end{aligned}$$

and

$$\begin{aligned} 2S_c &= \sum_{\substack{0 \le i,j \le e-1, \\ 0 \le \tau \le L-1,\ i \neq j}} H_{X^{(i)},X^{(j)}}(\tau) \\ &= \sum_{\substack{0 \le i,j \le e-1,\ 0 \le \tau \le L-1, \\ i-j \equiv e/2 (\mathrm{mod}\, e)}} H_{X^{(i)},X^{(j)}}(\tau) + \sum_{\substack{0 \le i,j \le e-1,\ 0 \le \tau \le L-1, \\ 2(i-j) \equiv e/2 (\mathrm{mod}\, e)}} H_{X^{(i)},X^{(j)}}(\tau) \\ &\quad + \sum_{\substack{0 \le i,j \le e-1,\ 0 \le \tau \le L-1, 2(i-j) \\ \neq e/2 (\mathrm{mod}\, e),\ i-j \neq e/2 (\mathrm{mod}\, e)}} H_{X^{(i)},X^{(j)}}(\tau) \end{aligned}$$

From Theorem 1, then

$$\begin{aligned}
2S_c = & \sum_{\substack{0\le i,j\le e-1,\ 0\le\tau\le L-1,\\ i-j\equiv e/2 (\bmod e)}} \left\{(q-1)\left(\frac{pq-1}{e}+\frac{p-q}{e}+2\right)\right. \\
& +(p-1)\left(\frac{pq-1}{e}+\frac{q-p}{e}\right) \\
& \left.+d\left(\frac{pq-1}{e}+2\right)+d\frac{pq-1}{e}+(e-2)d\left(\frac{pq-1}{e}+2\right)\right\} \\
& + \sum_{\substack{0\le i,j\le e-1,\ 0\le\tau\le L-1,\\ 2(i-j)\equiv e/2 (\bmod e)}} \left\{(q-1)\left(\frac{pq-1}{e}+\frac{p-q}{e}\right)+(p-1)\left(\frac{pq-1}{e}+\frac{q-p}{e}\right)\right. \\
& \left.+2d\left(\frac{pq-1}{e}-1\right)+(e-2)d\frac{pq-1}{e}\right\} \\
& + \sum_{\substack{0\le i,j\le e-1,\ 0\le\tau\le L-1,\ 2(i-j)\\ \ne e/2 (\bmod e),\ i-j\ne e/2 (\bmod e)}} \left\{(q-1)\left(\frac{pq-1}{e}+\frac{p-q}{e}\right)\right. \\
& \left.+(p-1)\left(\frac{pq-1}{e}+\frac{q-p}{e}\right)+2d\left(\frac{pq-1}{e}-1\right)+(e-2)d\frac{pq-1}{e}\right\} \\
= & (e-1)(pq-1)^2+2epq-2ep-(e-1)(q-1)^2-(e-1)(p-1)^2.
\end{aligned}$$

Applying (2) and (3), we obtain (11) and (12).

Similarly, when $|f_1-f_2|$ is odd, we obtain the same average Hamming autocorrelation and average Hamming crosscorrelation. By applying (11) and (12) to (4), it follows that

$$\begin{aligned}
\frac{A_a}{L(M-1)}+\frac{A_c}{L-1} &= \frac{(pq-1)^2+e(q^2+p^2)+e(1-pq-2q)-(q-1)^2-(p-1)^2}{e(e-1)pq(pq-1)} \\
&\quad +\frac{(e-1)(pq-1)^2+2epq-2ep-(e-1)((q-1)^2+(p-1)^2)}{e(e-1)pq(pq-1)} \\
&= \frac{1}{e-1}\ge\frac{LM-v}{v(L-1)(M-1)}=\frac{pqe-e}{e(pq-1)(e-1)}=\frac{1}{e-1}.
\end{aligned}$$

Thus, the FH sequence set $\mathcal{U}$ is an optimal average Hamming correlation set. This finishes the proof. □

Example 1 For $p=5$, $q=17$, then $e=4$, $d=16$, $f_1=1$, $f_2=4$ and $|f_1-f_2|=3$. The FH sequences of $\mathcal{U}$ are

$X^{(0)}=\{00102210302121120010202232202123110222112113323300203312302021002223022330322123202 32\};$

$X^{(1)}=\{11213321013232231121313303313230221333223220030011310023013132113330133001033230313 03\};$

$X^{(2)}=\{22320032120303302232020010020301332000330331101122021130120203220001200112100301020 10\};$

$X^{(3)}=\{33031103231010013303131121131012003111001002212233132201231310331112311223211012131 21\}.$

The Hamming autocorrelation of $X^{(i)}$ for $i = 0, 1, 2, 3$ is

$$
\begin{aligned}
&H_{X^{(i)}} \\
&= \{85, 21, 22, 21, 21, 29, 22, 21, 22, 21, 29, 22, 21, 22, 22, 29, 21, 13, 22, 21, 29, 21, 21, \\
&\quad 21, 22, 29, 21, 21, 21, 22, 29, 22, 22, 22, 13, 29, 21, 21, 22, 22, 29, 22, 22, 22, 22, 29, \\
&\quad 22, 22, 21, 21, 29, 13, 22, 22, 22, 29, 22, 21, 21, 21, 29, 22, 21, 21, 21, 29, 21, 22, 13, \\
&\quad 21, 29, 22, 22, 21, 22, 29, 21, 22, 21, 22, 29, 21, 21, 22, 21\}.
\end{aligned}
$$

The Hamming crosscorrelation is

$$
\begin{aligned}
&H_{X^{(0)},X^{(1)}} \\
&= \{0, 21, 19, 21, 21, 18, 19, 21, 21, 21, 18, 19, 21, 19, 19, 18, 21, 24, 19, 21, 18, 21, \\
&\quad 21, 21, 21, 18, 21, 21, 21, 19, 18, 21, 19, 19, 24, 18, 21, 21, 19, 19, 18, 19, 19, 21, \\
&\quad 21, 18, 21, 21, 21, 21, 18, 24, 21, 21, 19, 18, 21, 21, 21, 21, 18, 19, 21, 21, 21, 18, \\
&\quad 21, 21, 24, 21, 18, 21, 21, 21, 21, 18, 21, 19, 21, 21, 18, 21, 21, 21, 21\}; \\
&H_{X^{(0)},X^{(2)}} \\
&= \{0, 22, 23, 22, 22, 20, 23, 22, 23, 22, 20, 23, 22, 23, 23, 20, 22, 24, 23, 22, 20, 22, \\
&\quad 22, 22, 23, 20, 22, 22, 22, 23, 20, 23, 23, 23, 24, 20, 22, 22, 23, 23, 20, 23, 23, 23, \\
&\quad 23, 20, 23, 23, 22, 22, 20, 24, 23, 23, 23, 20, 23, 22, 22, 22, 20, 23, 22, 22, 22, \\
&\quad 20, 22, 23, 24, 22, 20, 23, 23, 22, 23, 20, 22, 23, 22, 23, 20, 22, 22, 23, 22\}; \\
&H_{X^{(0)},X^{(3)}} \\
&= \{0, 21, 21, 21, 21, 18, 21, 21, 19, 21, 18, 21, 21, 21, 21, 18, 21, 24, 21, 21, 18, 21, \\
&\quad 21, 21, 19, 18, 21, 21, 21, 21, 18, 19, 21, 21, 24, 18, 21, 21, 21, 21, 18, 21, 21, 19, \\
&\quad 19, 18, 19, 19, 21, 21, 18, 24, 19, 19, 21, 18, 19, 21, 21, 21, 18, 21, 21, 21, 21, 18, \\
&\quad 21, 19, 24, 21, 18, 19, 19, 21, 19, 18, 21, 21, 21, 19, 18, 21, 21, 19, 21\}; \\
&H_{X^{(1)},X^{(2)}} \\
&= \{0, 21, 19, 21, 21, 18, 19, 21, 21, 21, 18, 19, 21, 19, 19, 18, 21, 24, 19, 21, 18, 21, \\
&\quad 21, 21, 21, 18, 21, 21, 21, 19, 18, 21, 19, 19, 24, 18, 21, 21, 19, 19, 18, 19, 19, 21, \\
&\quad 21, 18, 21, 21, 21, 21, 18, 24, 21, 21, 19, 18, 21, 21, 21, 21, 18, 19, 21, 21, 21, 18, \\
&\quad 21, 21, 24, 21, 18, 21, 21, 21, 21, 18, 21, 19, 21, 21, 18, 21, 21, 21, 21\}; \\
&H_{X^{(1)},X^{(3)}} \\
&= \{0, 22, 23, 22, 22, 20, 23, 22, 23, 22, 20, 23, 22, 23, 23, 20, 22, 24, 23, 22, 20, 22, \\
&\quad 22, 22, 23, 20, 22, 22, 22, 23, 20, 23, 23, 23, 24, 20, 22, 22, 23, 23, 20, 23, 23, 23, \\
&\quad 23, 20, 23, 23, 22, 22, 20, 24, 23, 23, 23, 20, 23, 22, 22, 22, 20, 23, 22, 22, 22, 20, \\
&\quad 22, 23, 24, 22, 20, 23, 23, 22, 23, 20, 22, 23, 22, 23, 20, 22, 22, 23, 22\}; \\
&H_{X^{(2)},X^{(3)}} \\
&= \{0, 21, 19, 21, 21, 18, 19, 21, 21, 21, 18, 19, 21, 19, 19, 18, 21, 24, 19, 21, 18, 21, \\
&\quad 21, 21, 21, 18, 21, 21, 21, 19, 18, 21, 19, 19, 24, 18, 21, 21, 19, 19, 18, 19, 19, 21, \\
&\quad 21, 18, 21, 21, 21, 21, 18, 24, 21, 21, 19, 18, 21, 21, 21, 21, 18, 19, 21, 21, 21, 18, \\
&\quad 21, 21, 24, 21, 18, 21, 21, 21, 21, 18, 21, 19, 21, 21, 18, 21, 21, 21, 21\}.
\end{aligned}
$$

The average Hamming auto- and cross-correlation are 473/21 and 5248/255 respectively. The sequence set $\mathcal{U}$ is optimal with respect to the average Hamming correlation bound. However, $\mathcal{U}$ is not optimal with respect to the maximum Hamming correlation bound.

Acknowledgments This work was supported by the National Science Foundation of China (Grant Nos. 60872015) and the Funds for the Excellent Ph.D. Dissertation of Southwest Jiaotong University, 2010.

References

1. Lempel A., Greenberger H.: Families of sequences with optimal Hamming correlation properties. IEEE Trans. Inf. Theory **20**, 90–94 (1974).
2. Peng D.Y., Fan P.Z.: Lower bounds on the Hamming auto- and cross-correlations of frequency-hopping sequences. IEEE Trans. Inf. Theory **50**, 2149–2154 (2004).
3. Peng D.Y., Niu X.H., Tang X.H., Chen Q.C.: The average Hamming correlation for the cubic polynomial hopping sequences. In: International Wireless Communications and Mobile Computing Conference (IWCMC 2008), Crete Island, Greece, pp. 464–469 (2008).
4. Whiteman A.L.: A family of difference sets. Ill. J. Math. **6**, 107–121 (1962).
5. Chu W.S., Colbourn C.J.: Optimal frequency-hopping sequences via cyclotomy. IEEE Trans. Inf. Theory **51**, 1139–1141 (2005).
6. Ding C., Yin J.: Sets of optimal frequency-hopping sequences. IEEE Trans. Inf. Theory **54**, 3741–3745 (2008).
7. Han Y.K., Yang K.: New near-optimal frequency-hopping sequences of length pq. In: Proceedings of the 2008 IEEE International Symposium on Information Theory (ISIT 2008), Toronto, Canada, pp. 2593–2597 (2008).
8. Storer T.: Cyclotomy and Difference Sets. Marham, Chicago (1967).
9. Bai E.J., Fu X.T., Xiao G.Z.: On the linear complexity of generalized cyclotomic sequences of order four over $\mathbf{Z}_{pq}$. IEICE Trans. Fundam. **E88-A**, 392–395 (2005).
10. Ding C.: Linear complexity of generalized cyclotomic binary sequences of order 2. Finite Fields Appl. **3**, 159–174 (1997).
11. Ding C.: Autocorrelation values of generalized cyclotomic sequences of order two. IEEE Trans. Inf. Theory **44**, 1699–1702 (1998).
12. Peng D.Y., Peng T., Fan P.Z.: Generalized class of cubic frequency-hopping sequences with large family size. IEE Proc. Commun. **152**, 897–902 (2005).
13. Peng D.Y., Peng T., Tang X.H., Niu X.H.: A class of optimal frequency hopping sequences based upon the theory of power residues. In: Sequences and Their Applications (SETA 2008), Lexington, KY, USA, September 14–18, pp. 188–196 (2008).
14. Chung J.H., Yang K.: On the average Hamming correlation of frequency-hopping sequence sets with good maximum Hamming correlation. In: The Fifth International Workshop on Signal Design and Its Applications in Communications (IWSDA'11), Guilin, China, pp. 118–121 (2011).
15. Ding C., Moisio M.J., Yuan J.: Algebraic constructions of optimal frequency-hopping sequences. IEEE Trans. Inf. Theory **53**, 2606–2610 (2007).
16. Ge G.N., Miao Y., Yao Z.X.: Optimal frequency hopping sequences: auto- and cross-correlation properties. IEEE Trans. Inf. Theory **55**, 867–879 (2009).
17. Ding C., Yang Y., Tang X.H.: Optimal sets of frequency hopping sequences from linear cyclic codes. IEEE Trans. Inf. Theory **56**, 3605–3612 (2010).
18. Zhou Z.C., Tang X.H., Peng D.Y., Udaya P.: New constructions for optimal sets of frequency-hopping sequences. IEEE Trans. Inf. Theory **57**, 3831–3840 (2011).
19. Peng D.Y., Niu X.H., Tang X.H.: Average Hamming correlation for the cubic polynomial hopping sequences. IET Commun. **4**, 1775–1786 (2010).