Research Article

Construction of Optimal Sets of Frequency Hopping Sequences

Bin Wen

Department of Mathematics, Changshu Institute of Technology, Changshu, Jiangsu 215500, China

Correspondence should be addressed to Bin Wen; wenbin9903@163.com

Received 18 December 2012; Accepted 3 January 2013

Academic Editors: C. da Fonseca and A. V. Kelarev

Copyright © 2013 Bin Wen. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Frequency hopping spread spectrum and direct sequence spread spectrum are two main spread coding technologies. Frequency hopping sequences are needed in FH-CDMA systems. In this paper, a construction of optimal sets of frequency hopping sequences is presented. The construction is based on the set-theoretic characterization of an optimal set of FH sequences.

1. Introduction

Frequency hopping spread spectrum and direct sequence spread spectrum are two main spread coding technologies. Frequency hopping sequences are an integral part of spread-spectrum communication systems such as FH-CDMA systems (for a description of such systems, see [1]). In modern radar and communication systems, frequency-hopping (FH) spread-spectrum techniques have become popular (see [2], for example).

Assume that \( F = \{ f_0, f_1, \ldots, f_{m-1} \} \) is a set of available frequencies, called an alphabet. Let \( \mathcal{X}(v; F) \) be the set of all sequences of length \( v \) over \( F \). Any element of \( \mathcal{X}(v; F) \) is called a frequency hopping sequence (FHS) of length \( v \) over \( F \). Given two FHS sequences, \( X = (x_0, x_1, \ldots, x_{v-1}) \) and \( Y = (y_0, y_1, \ldots, y_{v-1}) \), we define their Hamming correlation \( H_{X,Y}(w) \) to be

\[
H_{X,Y}(w) = \sum_{0 \leq s \leq v-1} h[x_i, y_{i+w}],
\]

where \( 0 \leq w < v \) if \( X \neq Y \) and \( 0 < w < v \) if \( X = Y \), and where

\[
h[x, y] = \begin{cases} 1, & \text{if } x = y, \\ 0, & \text{otherwise}, \end{cases}
\]

and all operations among position indices are performed modulo \( v \). If \( X = Y \), \( H_{X,Y}(w) \) is the Hamming autocorrelation. If \( X \neq Y \), \( H_{X,Y}(w) \) is the Hamming cross correlation.

2. Lower Bounds on the Correlations of FHSs

FH sequences for FH-CDMA systems are required to have good Hamming correlations and large linear span [3]; the linear span is defined to be the length of the shortest linear feedback shift register that can produce the sequence. FH sequences’ design normally involves six parameters: the size \( m \) of the frequency library \( F \), the sequence length \( v \), the family size \( N \) of the subset \( \mathcal{S}(v; F) \), the maximum out-of-phase Hamming autocorrelations \( H_a \), the maximum Hamming cross correlations \( H_c \), and the linear span. It is generally desired that the family \( \mathcal{S} \) of FH sequences has the following properties:

1. the maximum out-of-phase Hamming autocorrelations \( H_a \) should be as small as possible,

2. the maximum Hamming cross correlations \( H_c \) should be as small as possible,

3. the family size \( N = |\mathcal{S}| \) for given \( H_a, H_c, M, \) and \( v \) should be as large as possible,

4. the linear span should be as large as possible.

In order to evaluate the theoretical performance of the FH sequences, it is important to find some theoretical bounds for these parameters. Given \( m, v, \) and \( N \) of \( \mathcal{S} \), Lempel and Greenberger [4] and Peng and Fan [5] derived lower bounds on \( H_a \) and \( H_c \) of FH sequences in \( \mathcal{X}(v; F) \). We restate their results in this section, which will be used later as the criteria to determine whether the new FH sequences constructed in this paper are optimal or not.
For any single FH sequence $X \in \mathcal{X}(v; F)$, let $H_a(X) = \max_{1 \leq s \leq v-1} \{H_{Xs}(t)\}$ be the maximum out-of-phase value of $H_{Xs}(t)$. If $H_a(X^*) \leq H_a(X)$ for all $X \in \mathcal{X}(v; F)$, that is, if the value $H_a(X^*)$ is the least among all FH sequences of the same length $v$ and over the same frequency library $F$, $X^*$ is called an optimal FH sequence. Lempel and Greenberger [4] developed the following lower bound for $H_a(X)$.

**Lemma 1** (see [4]). For every FH sequence $X$ of length $v$ over a frequency alphabet $F$ of size $m$. One has

$$H_a(X) \geq \frac{(v-e)(v+e-m)}{m(v-1)}, \quad (3)$$

where $e$ is the least nonnegative residue of $v$ modulo $m$.

**Corollary 2.** For every FH sequence $X$ of length $v$ over a frequency alphabet $F$ of size $m$. One has

$$H_a(X) \geq \begin{cases} k, & \text{if } m \neq v, \\ 0, & \text{if } m = v, \end{cases} \quad (4)$$

where $v = km + e$ with $0 \leq e \leq m - 1$.

For any given subset $\delta \subseteq \mathcal{X}(v; F)$ containing $N$ FH sequences, any two $X, Y \in \delta, X \neq Y$, we write $H_c(X, Y) = \max_{0 \leq s \leq v-1} \{H_{Xs}(t)\}$. We define the maximum out-of-phase Hamming autocorrelations $H_a(\delta)$ and the maximum Hamming cross correlations $H_c(\delta)$ as

$$H_a(\delta) = \max \{H_a(X) : X \in \delta\},$$

$$H_c(\delta) = \max \{H_c(X, Y) : X, Y \in \delta, X \neq Y\}, \quad (5)$$

$$M(\delta) = \max \{H_a(\delta), H_c(\delta)\}.$$

Peng and Fan [5] developed the following bounds on $M(\delta)$, which take into consideration the number of FH sequences in the set.

**Lemma 3** (see [5]). Let $\delta \subseteq \mathcal{X}(v; F)$ be a set of $N$ sequences of length $v$ over an alphabet of size $m$. Define $I = \lfloor vN/m \rfloor$. Then

$$M(\delta) \geq \frac{(vN - m)v}{(vN - 1)m}, \quad (6)$$

$$M(\delta) \geq \frac{2(vN - (I + 1)m)l}{(vN - 1)N}. \quad (7)$$

A family $\delta \subseteq \mathcal{X}(v; F)$ is an optimal set if the Peng-Fan lower bound (2) or (3) in Lemma 3 is met. Let $N = m$, and we have the following corollary which is a useful tool to check the bound in Lemma 3.

**Corollary 4** (see [6]). Let $\delta \subseteq \mathcal{X}(v; F)$ be a set of $m$ sequences of length $v$ over an alphabet of size $m$. Then

$$M(\delta) \geq \begin{cases} a, & \text{if } m \mid v, \\ a + 1, & \text{if } m \nmid v, \end{cases} \quad (8)$$

where $v = am + b$ with $0 \leq b \leq m - 1$.

A number of authors have made contributions to the construction of optimal FH sequences. Both algebraic and combinatorial constructions of optimal FH sequences have been given (see, for example, [3, 4, 7–11]). Most of them are concentrated on single optimal FH sequences. The purpose of this paper is to present a construction of optimal sets of FH sequences based on the set-theoretic characterization of an optimal set of FH sequences. Throughout what follows, we use $(v, m, \lambda)$-FHS to denote an FH sequence $X$ of length $v$ over an alphabet of size $m$ whose Hamming autocorrelation

$$H_a(X) = \lambda. \quad (9)$$

We also call a set $\delta$ of $N$ FH sequences in $\mathcal{X}(v; F)$ a $(v, N, \lambda; m)$ set of FH sequences, where $\lambda = M(\delta)$.

### 3. Mixed Difference Functions

Fuji-Hara et al. [9] characterized a $(v, m, \lambda)$-FHS in terms of partition-type cyclic difference packings. Given a partition $\mathcal{D} = \{D_0, D_1, \ldots, D_{m-1}\}$ of $\mathbb{Z}_m$ into $m$ subsets (called base blocks), we can define a difference function on $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$ given by

$$\Gamma_\delta(w) = \sum_{i=0}^{m-1} |(D_i + w) \cap D_i|. \quad (10)$$

Let $\max \{\Gamma_\delta(w) : w \in \mathbb{Z}_m^* \} = \lambda$. Then $\mathcal{D}$ is called a $(v, K, \lambda)_m$-CPDP (partition-type cyclic difference packing). Here, $m$ is used in the notation to indicate the number of base blocks, and $K = \{\lfloor D_i \rfloor : 0 \leq i \leq m - 1\}$ is the list of the sizes of base blocks. This is to say that a $(v, K, \lambda)_m$-CPDP is a partition of $\mathbb{Z}_m^*$ into $m$ base blocks which satisfies the following property. For any fixed nonzero residue $w \in \mathbb{Z}_m^*$, the equation $x - y = w$ has at most $\lambda$ solutions $(x, y)$ in the multiset union $\bigcup_{D \in \mathcal{D}} (D \times D)$.

If we label the positions of a $(v, m, \lambda)$-FHS $X$ by the elements of $\mathbb{Z}_v$, then, by the above definition, the set of positions $\{v \in \mathbb{Z}_v : 0 \leq v \leq m - 1\}$ in $\mathcal{D}$ is a $v$-CPDP with $\Gamma_\delta(w) = H_{XX}(w)$ for any nonzero $w \in \mathbb{Z}_v$.

Conversely, if we label the $m$ base blocks of a $(v, K, \lambda)_m$-CPDP by the elements of $\mathbb{Z}_m^*$ and identify the frequency alphabet $F$ with $\mathbb{Z}_m$, then the PCDP gives a $(v, m, \lambda)$-FHS in $\mathcal{X}(v; F)$.

This fact reveals that a single FHS can be constructed by a PCDP. Apparently, the smaller the index $\lambda$ of a PCDP the lower the Hamming autocorrelation $H_a(X)$ of its corresponding FH sequence. For an optimal FH sequence, we need to construct a $(v, K, \lambda)_m$-CPDP so that its index $\lambda$ is as small as possible for any given value of $v$ and $m$. Based on Lempel-Greenberger bound on $H_a(X)$ in Lemma 1, Fuji-Hara et al. [9] proved the following result.

**Lemma 5** (see [9]). There exists a $(v, m, \lambda)$-FHS over the alphabet $F = \mathbb{Z}_m$ if and only if there exists a $(v, K, \lambda)_m$-CPDP in $\mathbb{Z}_v$. Furthermore, this FH sequence is optimal if $\lambda = \lfloor v/m \rfloor$ for $v > m$ and if $\lambda = 0$ for $v = m$.

The correspondence between an individual FH sequence and a PCDP can be naturally extended to give a set-theoretic interpretation of a set of FH sequences. Let $N$ be a positive integer. Let $\mathcal{C} = \{\mathcal{C}_0, \mathcal{C}_1, \ldots, \mathcal{C}_{N-1}\}$ be a collection of partitions of $\mathbb{Z}_v$ into $m$ subsets (called base blocks). Write

$$\mathcal{C}_r = \{D_0^r, D_1^r, \ldots, D_{m-1}^r\}, 0 \leq r \leq N - 1. \quad (12)$$

For any ordered pair $(i, j)$ with $0 \leq i < j \leq N - 1$, we define
a difference function on \( \mathbb{Z}_v \) given by \( \Gamma_{(r)}(w) = \sum_{k=0}^{m-1} |(D_k^r + w) \cap D_k^r| \). For any integer \( r \) with \( 0 \leq r \leq N - 1 \), we define a difference function on \( \mathbb{Z}_v \setminus \{0\} \), before given by \( \Gamma_{(r)}(w) = \sum_{k=0}^{m-1} |(D_k^r + w) \cap D_k^r| \). We refer to these \( N(N + 1)/2 \) difference functions defined above as "mixed difference functions" with respect to the given collection \( C \). Since each partition in \( C \) determines uniquely an FH sequence, the collection \( C \) gives a set of \( N \) FH sequences in \( \mathcal{X}(v, F) \), and vice versa, where the alphabet is regarded as \( \mathbb{Z}_m \). For the optimality of the derived set of FH sequences from \( C \), we define \( \lambda(r) = \max_{w \in C} \{\Gamma_{(r)}(w)\} \}, 0 \leq r \leq N - 1 \). \( \lambda(i, j) \) is the index of the \( \lambda \)-PCDPs so that its index \( \lambda \) is as small as possible. Since the index \( \lambda \) of \( C \) is the same as the Hamming correlation \( M(\delta) \), the Peng-Fan bounds in Lemma 3 can be employed as our benchmarks. As noted in [12], a set of FH sequences meeting one of the Peng-Fan bounds must be optimal. We have the following theorem.

**Theorem 6** (see [13]). Let \( N \geq 2 \) be an integer. Then there exists a \( (v, N, \lambda;\lambda) \) set of FH sequences in \( \mathcal{X}(v, F) \) if and only if there exists a \( \lambda \)-PCDPs in \( \mathcal{X}_v \) under our notations. This gives us an interpretation for a set of FH sequences from set-theoretic perspective. As with individual optimal FH sequence, for an \( \lambda \)-PCDPs in \( \mathcal{X}_v \), we refer to the bound of Lemma 1.

**Theorem 8.** Let \( p \) be an odd prime and \( m \) a positive integer. Define \( f : \mathbb{Z}_{p^m-1} \rightarrow \mathbb{Z}_p \) by \( f(x) = \text{Tr}_{p^m/p}(\alpha x^k) \), where \( \text{Tr}_{p^m/p} \) is the trace function from \( \mathbb{F}_{p^m} \) to \( \mathbb{F}_p \). \( \alpha \) is a generator of \( \mathbb{F}_{p^m}^* \).

Define

\[
D_j = f^{-1}(j) = \{ x \in \mathbb{Z}_{p^m-1} : f(x) = j \}, \quad 0 \leq j \leq p - 1,
\]

\[
D_j^{(r)} = D_{j+r}, \quad 0 \leq j \leq p - 1, \quad 0 \leq r \leq p - 1,
\]

\[
\mathcal{D}^{(r)} = \{ D_0^{(r)}, D_1^{(r)}, \ldots, D_{p-1}^{(r)} \}, \quad 0 \leq r \leq p - 1,
\]

where all operations among the subscripts are performed modulo \( p \). Then \( \mathcal{C} = \{ \delta^{(0)}, \delta^{(1)}, \ldots, \delta^{(p-1)} \} \) is an optimal \((p^{m-1}, p, p^{m-1}; p)\) set of FH sequences over \( \mathbb{Z}_p \) of length \( p^{m-1} \). Furthermore, each sequence of the set \( C \) is optimal with respect to the bound of Lemma 1.

**Proof.** For any \( r \) with \( 0 \leq r \leq e - 1 \) and any \( w \in \mathbb{Z}_{p^m-1} \), we have

\[
\Gamma_{(r)}^i(w) = \sum_{k=0}^{p-1} \left| (D_k^r + w) \cap D_k^r \right|
\]

\[
= \bigcup_{k=0}^{p-1} \left( (D_k^r + w) \cap D_k^r \right)
\]

\[
= \bigcup_{k=0}^{p-1} \left( (D_k^r + w) \cap D_k^r \right)
\]

\[
= \left| \{ x \in \mathbb{Z}_{p^m-1} : f(x + w) - f(x) = 0 \} \right|
\]

\[
= \left| \{ x \in \mathbb{Z}_{p^m-1} : \text{Tr}_{p^m/p}(\alpha^w - 1) = 0 \} \right|
\]

\[
p^{m-1} - 1,
\]

where the last equality follows from Lemma 7. Next we will show that \( \Gamma_{(r)}^i(w) = p^{m-1} \) for any \( i, j \) with \( 0 \leq i < j \leq p - 1 \) and any \( w \in \mathbb{Z}_{p^m-1} \). For any \( i, j \) with \( 0 \leq i < j \leq e - 1 \) and any \( w \in \mathbb{Z}_{p^m-1} \), we have

\[
\Gamma_{(r)}^i(w) = \sum_{k=0}^{p-1} \left| (D_k^r + w) \cap D_k^r \right|
\]

\[
= \sum_{k=0}^{p-1} \left| (D_{k+i} + w) \cap D_{k+j} \right|
\]

\[
= \sum_{k=0}^{p-1} \left| (D_{k+i} + w) \cap D_{k+j} \right|
\]

\[
= \sum_{k=0}^{p-1} \left| (D_k + w) \cap D_{k+j} \right| + b = j - i
\]
\[
\begin{align*}
\left\{ x \in \mathbb{Z}_{p^m-1} \mid f(x + \omega) - f(x) = b \right\} \\
\left\{ x \in \mathbb{Z}_{p^m-1} \mid \text{Tr}_{p^m/p} \left( (\alpha^u - 1) \alpha^x \right) = b \right\} \\
= p^{m-1},
\end{align*}
\]

(12)

where the last equality follows from Lemma 7. It follows that \( \mathcal{C} \) is a \((p^m - 1, \{K_0, K_1, \ldots, K_{p-1}\}, \{\lambda_0, \lambda_1, \ldots, \lambda_{p-1}\}; p^{m-1})_p \) collection of \( p \) PCDPs in \( \mathbb{Z}_{p^m} \), where \( \lambda_0 = \lambda_1 = \cdots = \lambda_{m-1} = p^{m-1} - 1 \). By Theorem 6, it derives a \((p^m - 1, p, p^{m-1}; p) \) set of FH sequences in \( \mathcal{Z}(w; F) \). For this set, we have \( N = p \) and both lower bounds in Lemma 3 are equal to \( p^{m-1} \) by Corollary 4. Hence, it is optimal. Furthermore, each sequence of the set \( \mathcal{C} \) is optimal with respect to the bound of Lemma 1. The proof is then complete.

Example 9. Take \( p = 3 \) and \( m = 2 \). It is readily calculated that
\[
D_0 = \{2, 6\}, \quad D_1 = \{1, 3, 4\}, \quad D_2 = \{0, 5, 7\}.
\]

(13)

We then have
\[
\begin{align*}
\mathcal{D}(0) &= \left\{ D_0^{(0)} = \{2, 6\}, D_1^{(0)} = \{1, 3, 4\}, D_2^{(0)} = \{0, 5, 7\} \right\}, \\
\mathcal{D}(1) &= \left\{ D_0^{(1)} = \{1, 3, 4\}, D_1^{(1)} = \{0, 5, 7\}, D_2^{(1)} = \{2, 6\} \right\}, \\
\mathcal{D}(2) &= \left\{ D_0^{(2)} = \{0, 5, 7\}, D_1^{(2)} = \{2, 6\}, D_2^{(2)} = \{1, 3, 4\} \right\}.
\end{align*}
\]

(14)

The family \( \mathcal{C} = \{\mathcal{D}(0), \mathcal{D}(1), \mathcal{D}(2)\} \) is a \((v, m, \{K_0, K_1, K_2\}; \{\lambda_0, \lambda_1, \lambda_2\})_3 \) collection of 3 PCDPs in \( \mathbb{Z}_9 \), where \( K_0 = \{2, 3, 3\}, K_1 = \{3, 3, 2\}, K_2 = \{3, 2, 3\}, \) and \( \lambda_0 = \lambda_1 = \lambda_2 = 2 \). By Theorem 6, it corresponds a \((8, 3, 3; 3)\) set \( \mathcal{S} \) consisting of the following 3 FH sequences over \( \mathcal{Z}_3 \):
\[
\begin{align*}
X &= (2, 1, 0, 1, 1, 2, 0, 2), \\
Y &= (1, 0, 2, 0, 0, 1, 2, 1), \\
Z &= (0, 2, 1, 2, 2, 0, 1, 0),
\end{align*}
\]

(15)

with \( M(\mathcal{C}) = 3 \). It is optimal meeting the lower bounds in Lemma 3.

Acknowledgment

The Paper was supported by the Tian Yuan Special Funds of the National Natural Science Foundation of China (Grant no. 11226282).

References
