

A construction of optimal sets of FH sequences

BIN WEN

*Department of Mathematics
Changshu Institute of Technology
Changshu 215500, Jiangsu
P. R. China
wenbin9903@yahoo.com.cn*

YANG LI CE SHI

*Department of Mathematics
Soochow University
Suzhou 215006, Jiangsu
P. R. China*

Abstract

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 via cyclotomy. The construction is based on the set-theoretic characterization of an optimal set of FH sequences. As a consequence, new optimal sets of FH sequences are obtained.

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 [10]). In modern radar and communication systems, frequency-hopping (FH) spread-spectrum techniques have become popular (see [4] for example).

Assume that $F = \{f_0, f_1, \dots, f_{m-1}\}$ 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 FH sequences, $X = (x_0, x_1, \dots, x_{v-1})$ and $Y = (y_0, y_1, \dots, y_{v-1})$, we define their Hamming correlation $H_{X,Y}(w)$ to be

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

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 $X = Y$, then $H_{X,Y}(w)$ is the Hamming auto-correlation. 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 [7], 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 $\mathcal{S} \subset \mathcal{X}(v; F)$, the maximum out-of-phase Hamming auto-correlations 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 auto-correlations 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 [8] and Peng and Fan [9] 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 $H_a(X) = \max_{1 \leq t \leq v-1} \{H_{X,X}(t)\}$ be the maximum out-of-phase value of $H_{X,X}(t)$. 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 , then X^* is called an optimal FH sequence. Lempel and Greenberger [8] developed the following lower bound for $H_a(X)$.

Lemma 2.1 [8] *For every FH sequence X of length v over a frequency alphabet F of size m , we have*

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

where ϵ is the least non-negative residue of v modulo m .

Corollary 2.2 *For every FH sequence X of length v over a frequency alphabet F of size m , we have*

$$H_a(X) \geq \begin{cases} k, & \text{if } m \neq v, \\ 0, & \text{if } m = v. \end{cases} \quad (1)$$

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

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

$$\begin{aligned} H_a(\mathcal{S}) &= \max\{H_a(X) : X \in \mathcal{S}\}, \\ H_c(\mathcal{S}) &= \max\{H_c(X, Y) : X, Y \in \mathcal{S}, X \neq Y\}, \\ M(\mathcal{S}) &= \max\{H_a(\mathcal{S}), H_c(\mathcal{S})\}. \end{aligned}$$

Peng and Fan [9] developed the following bounds on $M(\mathcal{S})$, which take into consideration of the number of FH sequences in the set.

Lemma 2.3 [9] *Let $\mathcal{S} \subseteq \mathcal{X}(v; F)$ be a set of N sequences of length v over an alphabet of size m . Define $I = \lfloor vN/m \rfloor$. Then*

$$M(\mathcal{S}) \geq \left\lceil \frac{(vN - m)v}{(vN - 1)m} \right\rceil \quad (2)$$

and

$$M(\mathcal{S}) \geq \left\lceil \frac{2IvN - (I + 1)mI}{(vN - 1)N} \right\rceil. \quad (3)$$

A family $\mathcal{S} \subseteq \mathcal{X}(v; F)$ is an optimal set if the Peng-Fan lower bound (2) or (3) in Lemma 2.3 is met. Let $N = m$, we have the following corollary which is a useful tool to check the bound in Lemma 2.3.

Corollary 2.4 *Let $\mathcal{S} \subseteq \mathcal{X}(v; F)$ be a set of m sequences of length v over an alphabet of size m . Then*

$$M(\mathcal{S}) \geq \begin{cases} a, & \text{if } m \mid v, \\ a + 1, & \text{if } m \nmid v. \end{cases} \quad (4)$$

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

Proof: Let $N = m$, then $I = \lfloor vN/m \rfloor = v$ and lower bounds (2) and (3) in Lemma 2.3 are equal. We have $\frac{(vN-m)v}{(vN-1)m} = \frac{(vm-m)v}{(vm-1)m} = \frac{v}{m} - \frac{m-1}{vm-1} \cdot \frac{v}{m}$. Since $\frac{m-1}{vm-1} < \frac{m}{vm} = \frac{1}{v}$ for any integer $v > 1$ and $m > 1$. Hence, $\frac{v}{m} - \frac{1}{m} < \frac{(vN-m)v}{(vN-1)m} < \frac{v}{m}$. If v is divisible by m , then $b = 0$ and $a - \frac{1}{m} < \frac{(vN-m)v}{(vN-1)m} < a$. Then $\left\lceil \frac{(vN-m)v}{(vN-1)m} \right\rceil = a$. If v is not divisible by m , then $1 \leq b \leq m-1$ and $a + \frac{b-1}{m} < \frac{(vN-m)v}{(vN-1)m} < a + \frac{b}{m}$. Then $\left\lceil \frac{(vN-m)v}{(vN-1)m} \right\rceil = a + 1$. \square

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, [1, 2, 5, 6, 7, 8, 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 using cyclotomy. Throughout what follows, we use (v, m, λ) -FHS to denote an FH sequence X of length v over an alphabet of size m whose Hamming auto-correlation $H_a(X) = \lambda$. We also call a set \mathcal{S} of N FH sequences in $\mathcal{X}(v; F)$ a $(v, N, \lambda; m)$ set of FH sequences, where $\lambda = M(\mathcal{S})$.

3 Mixed Difference Functions

Fuji-Hara, Miao and Mishima [5] characterized a (v, m, λ) -FHS in terms of partition-type cyclic difference packings. Given a partition $\mathcal{D} = \{D_0, D_1, \dots, D_{m-1}\}$ of \mathbb{Z}_v into m subsets (called *base blocks*), we can define a difference function on $\mathbb{Z}_v^* = \mathbb{Z}_v \setminus \{0\}$ given by $\Gamma_{\mathcal{D}}(w) = \sum_{i=0}^{m-1} |(D_i + w) \cap D_i|$. Let $\max\{\Gamma_{\mathcal{D}}(w) \mid w \in \mathbb{Z}_v \setminus \{0\}\} = \lambda$. Then \mathcal{D} is called a $(v, K, \lambda)_m$ -PCDP (*partition-type cyclic difference packing*). Here, m is used in the notation to indicate the number of base blocks and $K = \{|D_i| : 0 \leq i \leq m-1\}$ is the list of the sizes of base blocks. This is to say that a $(v, K, \lambda)_m$ -PCDP is a partition of \mathbb{Z}_v into m base blocks which satisfies the following property. For any fixed nonzero residue $w \in \mathbb{Z}_v$, the equation $x - y = w$ has at most λ solutions (x, y) in the multiset union $\bigcup_{D \in \mathcal{D}} (D \times D)$.

If we label the positions of a (v, m, λ) -FHS X by the elements of \mathbb{Z}_v , then, by the above definition, the sets of position indices of m frequencies in X form a $(v, K, \lambda)_m$ -PCDP \mathcal{D} with $\Gamma_{\mathcal{D}}(w) = H_{X,X}(w)$ for any nonzero $w \in \mathbb{Z}_v$. Conversely, if we label the m base blocks of a $(v, K, \lambda)_m$ -PCDP by the elements of \mathbb{Z}_m and identify the frequency alphabet F with \mathbb{Z}_m , then the PCDP gives a (v, m, λ) -FHS in $\mathcal{X}(v; F)$.

This fact reveals that a single FHS can be constructed by a PCDPs. Apparently, the smaller the index λ of a PCDP, the lower the Hamming auto-correlation $H_a(X)$ of its corresponding FH sequence. For an optimal FH sequence, we need to construct a $(v, K, \lambda)_m$ -PCDP so that its index λ is as small as possible for any given value of v and m . Based on Lempel-Greenberger bound on $H_a(X)$ in Lemma 2.1, Fuji-Hara, Miao and Mishima [5] proved the following result.

Lemma 3.1 [5] *There exists a (v, m, λ) -FHS over the alphabet $F = \mathbb{Z}_m$ if and only if there exists a $(v, K, \lambda)_m$ -PCDP 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 $\mathcal{C} = \{\mathcal{D}^{(0)}, \mathcal{D}^{(1)}, \dots, \mathcal{D}^{(N-1)}\}$ be a collection of partitions of \mathbb{Z}_v into m subsets (called *base blocks*). Write $\mathcal{D}^{(r)} = \{D_0^{(r)}, D_1^{(r)}, \dots, D_{m-1}^{(r)}\}$, $0 \leq r \leq N-1$. 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 $\Gamma_{\mathcal{C}}^{(i,j)}(w) = \sum_{k=0}^{m-1} \left| (D_k^{(i)} + w) \cap D_k^{(j)} \right|$. For any integer r with $0 \leq r \leq N-1$, we define a difference function on $\mathbb{Z}_v \setminus \{0\}$, as before, given by $\Gamma_{\mathcal{C}}^{(r,r)}(w) = \Gamma_{\mathcal{D}^{(r)}}(w) = \sum_{k=0}^{m-1} \left| (D_k^{(r)} + w) \cap D_k^{(r)} \right|$. We refer to these $N(N+1)/2$ difference functions defined above as *mixed difference functions* with respect to the given collection \mathcal{C} . Since each partition in \mathcal{C} determines uniquely an FH sequence, the collection \mathcal{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 \mathcal{C} , we define

$$\begin{aligned} \lambda(r) &= \max_{1 \leq w < v} \{ \Gamma_{\mathcal{C}}^{(r,r)}(w) \}, \quad 0 \leq r \leq N-1, \\ \lambda(i, j) &= \max_{0 \leq w < v} \{ \Gamma_{\mathcal{C}}^{(i,j)}(w) \}, \quad 0 \leq i < j \leq N-1, \\ \mu(i, j) &= \max \{ \lambda(i), \lambda(j), \lambda(i, j) \}, \quad 0 \leq i < j \leq N-1, \\ \lambda &= \max \left\{ \max_{0 \leq r \leq N-1} \lambda(r), \max_{0 \leq i < j \leq N-1} \lambda(i, j) \right\}. \end{aligned}$$

Then $\mathcal{D}^{(r)}$ is a $(v, K_r, \lambda_r)_m$ -PCDP, according to the above definition. We say that \mathcal{C} is a $(v, \{K_0, K_1, \dots, K_{N-1}\}, \{\lambda_0, \lambda_1, \dots, \lambda_{N-1}\}; \lambda)_m$ collection of N PCDPs. It turns out that there exists a $(v, N, \lambda; m)$ set of FH sequences in $\mathcal{X}(v; F)$ if and only if there exists a $(v, \{K_0, K_1, \dots, K_{N-1}\}, \{\lambda_0, \lambda_1, \dots, \lambda_{N-1}\}; \lambda)_m$ collection of N PCDPs in \mathbb{Z}_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 optimal $(v, N, \lambda; m)$ set of FH sequences, we are required to construct a $(v, \{K_0, K_1, \dots, K_{N-1}\}, \{\lambda_0, \lambda_1, \dots, \lambda_{N-1}\}; \lambda)_m$ collection \mathcal{C} of N PCDPs so that its index λ is as small as possible. Since the index λ of \mathcal{C} is the same as the Hamming correlation $M(\mathcal{S})$, the Peng-Fan bounds in Lemma 2.3 can be employed as our benchmarks. As noted in [3], a set of FH sequences meeting one of the Peng-Fan bounds must be optimal. We have the following theorem.

Theorem 3.2 [13] *Let $N \geq 2$ be an integer. Then there exists a $(v, N, \lambda; m)$ set of FH sequences in $\mathcal{X}(v; F)$ if and only if there exists a $(v, \{K_0, K_1, \dots, K_{N-1}\}, \{\lambda_0, \lambda_1, \dots, \lambda_{N-1}\}; \lambda)_m$ collection of N PCDPs in \mathbb{Z}_v . Furthermore, this set is optimal if λ meets one of the Peng-Fan lower bounds given in Lemma 2.3.*

4 The Construction of Optimal Sets of FH Sequences using Cyclotomy

Let p be an odd prime with $p - 1 = ef$. Given a primitive element x of \mathbb{F}_p , define $C_0^{(e,p)} = \langle x^e \rangle$, the multiplicative group generated by x^e , and $C_i^{(e,p)} = x^i C_0^{(e,p)}$ for $i = 1, 2, \dots, e - 1$. The $C_i^{(e,p)}$ are known as *cyclotomic classes* of order e with respect to \mathbb{F}_p . Wilson [12, Theorem 7] showed that the set $\mathcal{F} = \{C_i^{(e,p)} : 0 \leq i \leq e - 1\}$ of all cyclotomic classes of order e forms a $(p, f, f - 1)$ -difference family in \mathbb{F}_p . In the theory of cyclotomy, the number of solutions of $1 + X = Y, X \in C_i^{(e,p)}, Y \in C_j^{(e,p)}$ are called *cyclotomic numbers* of order e with respect to \mathbb{F}_p and denoted by $(i, j)_e$. The following formula about cyclotomic numbers is known (see [1]).

Lemma 4.1 *Let p be a prime power with $p - 1 = ef$. Then*

$$\sum_{u=0}^{e-1} (u, u+k)_e = \begin{cases} f-1, & \text{if } k=0, \\ f, & \text{if } k \neq 0. \end{cases}$$

Now we are able to establish our first result of this section.

Theorem 4.2 *Let $p = ef + 1$ be an odd prime with f even. Let $C_0^{(e,p)}, C_1^{(e,p)}, \dots, C_{e-1}^{(e,p)}$ be the cyclotomic classes of order e with respect to \mathbb{F}_p with an arbitrary primitive element x . Define*

$$\begin{aligned} D_0 &= C_0^{(e,q)} \cup \{0\}; \quad D_i = C_i^{(e,q)}, \quad 1 \leq i \leq e-1, \\ D_j^{(r)} &= D_{j+r}, \quad 0 \leq j \leq e-1, \quad 0 \leq r \leq e-1, \\ \mathcal{D}^{(r)} &= \{D_0^{(r)}, D_1^{(r)}, \dots, D_{e-1}^{(r)}\}, \quad 0 \leq r \leq e-1. \end{aligned}$$

where all operations among the subscripts are performed modulo e . Then $\mathcal{C} = \{\mathcal{D}^{(0)}, \mathcal{D}^{(1)}, \dots, \mathcal{D}^{(e-1)}\}$ is an optimal $(p, e, f + 1; e)$ set of FH sequences over \mathbb{Z}_e of length p .

Proof: Obviously, $\mathcal{D}^{(0)}$ is a partition of \mathbb{F}_p . As noted above, $\{C_i^{(e,p)} : 0 \leq i \leq e - 1\}$ forms a $(p, f, f - 1)$ -difference family in \mathbb{F}_p . Hence,

$$\Gamma_{\mathcal{C}}^{(r,r)}(w) = \sum_{k=0}^{m-1} \left| (D_k^{(r)} + w) \cap D_k^{(r)} \right| \leq f + 1$$

for any r with $0 \leq r \leq e - 1$ and any $w \in \mathbb{F}_p^*$. Next we will show that $\Gamma_{\mathcal{C}}^{(i,j)}(w) \leq f + 1$ for any i, j with $0 \leq i < j \leq e - 1$ and any $w \in \mathbb{F}_p^*$. To do this, we assume that $w^{-1} \in C_h^{(e,p)}$ for some h with $0 \leq h \leq e - 1$ for any given $w \in \mathbb{F}_p^*$. Then, making use

of Lemma 4.1, by a simple calculation similar to those in [3, Theorem 4] we have

$$\begin{aligned}
\Gamma_{\mathcal{C}}^{(i,j)}(w) &= \sum_{k=0}^{e-1} \left| (D_k^{(i)} + w) \cap D_k^{(j)} \right| \\
&= \sum_{k=0}^{e-1} \left| (D_{k+i} + w) \cap D_{k+j} \right| \\
&= \sum_{k=0}^{e-1} \left| (D_{k+i} + w) \cap D_{(k+i)+(j-i)} \right| \\
&= \sum_{k=0}^{e-1} \left| (D_k + w) \cap D_{k+t} \right|, \quad t = j - i \\
&= \left| \{w\} \cap C_t^{(e,p)} \right| + \left| (C_{e-t}^{(e,p)} + w) \cap \{0\} \right| + \sum_{k=0}^{e-1} \left| (C_k^{(e,p)} + w) \cap C_{k+t}^{(e,p)} \right| \\
&= \left| \{w\} \cap C_t^{(e,p)} \right| + \left| (C_{e-t}^{(e,p)} + w) \cap \{0\} \right| + \sum_{k=0}^{e-1} \left| \left(\frac{1}{w} C_k^{(e,p)} + 1 \right) \cap \frac{1}{w} C_{k+t}^{(e,p)} \right| \\
&= \left| \{w\} \cap C_t^{(e,p)} \right| + \left| (C_{e-t}^{(e,p)} + w) \cap \{0\} \right| + \sum_{k=0}^{e-1} \left| (C_{k+h}^{(e,p)} + 1) \cap C_{k+h+t}^{(e,p)} \right| \\
&= \begin{cases} f + 2, & w \in C_t^{(e,p)} \text{ and } -w \in C_{e-t}^{(e,p)}; \\ f + 1, & w \in C_t^{(e,p)} \text{ and } -w \notin C_{e-t}^{(e,p)} \text{ or } w \notin C_t^{(e,p)} \text{ and } -w \in C_{e-t}^{(e,p)}; \\ f, & \text{otherwise.} \end{cases}
\end{aligned}$$

By assumption, f is even, so we have $-1 \in C_0^{(e,p)}$. Therefore the first case never happens. It follows that $\max \left\{ \Gamma_{\mathcal{C}}^{(i,j)}(w) : 0 \leq t \leq e-1, w \in \mathbb{F}_p^* \right\} = f + 1$. It follows that \mathcal{C} is a $(p, \{K_0, K_1, \dots, K_{m-1}\}, \{\lambda_0, \lambda_1, \dots, \lambda_{m-1}\}; f+1)_e$ collection of e PCDDPs in \mathbb{Z}_p , where $\lambda_0 = \lambda_1 = \dots = \lambda_{m-1} \leq f+1$. By Theorem 3.2, it derives a $(p, e, f+1; e)$ set of FH sequences in $\mathcal{X}(v; F)$. For this set, we have $N = e$ and both lower bounds in Lemma 2.3 are equal to $f + 1$ by Corollary 2.4. Hence it is optimal. The proof is then complete. \square

Acknowledgments

The authors wish to extend their gratitude to the referees for their helpful comments in revising this paper.

References

- [1] W. Chu and C. J. Colbourn, Optimal frequency-hopping sequences via cyclotomy, *IEEE Trans. Inform. Theory* 51 (2005), 1139–1141.
- [2] C. Ding, M. Moisiso and J. Yuan, Algebraic Constructions of Optimal Frequency Hopping Sequences, *IEEE Trans. Inform. Theory* 53 (2007), 2606–2610.
- [3] C. Ding and J. Yin, Optimal Sets of Frequency Hopping Sequences, *IEEE Trans. Inform. Theory* 54 (2008), 3741–3745.
- [4] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Research Studies Press Ltd., Taunton, England, 1996.
- [5] R. Fuji-Hara, Y. Miao and M. Mishima, Optimal frequency hopping sequences: a combinatorial approach, *IEEE Trans. Inform. Theory* 50 (2004), 2408–2420.
- [6] G. Ge, R. Fuji-Hara and Y. Miao, Further combinatorial constructions for optimal frequency hopping sequences, *J. Combin. Theory Ser. A* 113 (2006), 1699–1718.
- [7] P. V. Kumar, Frequency-hopping code sequence designs having large linear span, *IEEE Trans. Inform. Theory* 34 (1988), 146–151.
- [8] A. Lempel and H. Greenberger, Families of sequences with optimal Hamming correlation properties, *IEEE Trans. Inform. Theory* 20 (1974), 90–94.
- [9] D. Peng and P. Fan, Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences, *IEEE Trans. Inform. Theory* 50 (2004), 2149–2154.
- [10] R. A. Scholtz, The spread spectrum concept, *IEEE Trans. Commun.* 25 (1977), 748–755.
- [11] P. Udaya and M. N. Siddiqi, Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings, *IEEE Trans. Inform. Theory* 44 (1998), 1492–1503.
- [12] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, *J. Number Theory* 4 (1972), 17–47.
- [13] J. Yin, *A construction of optimal sets of FH sequences*, Proc. Wuyi Mountain Workshop on Coding and Cryptology, World Scientific Co., 2008.