RAIRO-Theor. Inf. Appl. 46 (2012) 343–354
DOI: 10.1051/ita/2012007

Available online at:
www.rairo-ita.org

LINEAR SPANS OF OPTIMAL SETS OF FREQUENCY HOPPING SEQUENCES*

Gao Juntao[1,2], Hu Yupu[3] and Li Xuelian[4]

Abstract. Frequency hopping sequences sets are required in frequency hopping code division multiple access systems. For the anti-jamming purpose, frequency hopping sequences are required to have a large linear span. In this paper, by using a permutation polynomial $\delta(x)$ over a finite field, we transform several optimal sets of frequency hopping sequences with small linear span into ones with large linear span. The exact values of the linear span are presented by using the methods of counting the terms of the sequences representations. The results show that the transformed frequency hopping sequences are optimal with respect to the Peng-Fan bound, and can resist the analysis of Berlekamp-Massey algorithm.

Mathematics Subject Classification. 94A05, 94A55, 94A60.

1. Introduction

1.1. Optimal frequency-hopping sequences

In modern communication systems, frequency-hopping (FH) spread spectrum and direct sequence spread spectrum are two main spread spectrum techniques.

Keywords and phrases. Frequency hopping sequences, linear span, permutation polynomials, optimal sets.

* *This work is supported by 973 project under Grant No. 2007CB311201, Natural Science Foundation under Grant No. 60833008, the Fundamental Research Funds for the Central Universities under Grants No. K50511010007 and 111 project under Grant No. B08038.*

[1] Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an, Shaanxi province 710071, P.R. China. gjt_albert@163.com

[2] State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, 100049, P.R. China.

[3] School of Telecommunication and Engineering of Xidian University, Xi'an, Shaanxi province 710071, P.R. China.

[4] Department of Applied Mathematics of Xidian University, Xi'an, Shaanxi province 710071, P.R. China.

Article published by EDP Sciences

© EDP Sciences 2012

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

Frequency-hopping sequences are a very important part of FH Code Division Multiple Access (FH-CDMA) [16].

In an FH spread spectrum system, the interference occurs if two distinct transmitters use the same frequency simultaneously. To reduce the interference, we hope that both autocorrelation and crosscorrelation functions in an FH sequences set are as small as possible [7–9].

Let $F = \{f_0, f_1, \ldots, f_{\gamma-1}\}$ be a set of available frequencies with alphabet size γ. Let $\mathcal{F}$ be a set of N frequency sequences of length L over F. For any two sequences $X, Y \in \mathcal{F}$, where $X = (X(0), X(1), \ldots, X(L-1)), Y = (Y(0), Y(1), \ldots, Y(L-1))$, we can define their Hamming correlation $H_{X,Y}$ as follows

$$H_{X,Y}(\tau) = \sum_{i=0}^{L-1} h[X(i), Y(i+\tau)], \tag{1.1}$$

where $0 \leq \tau < L$, $h[X(i), Y(i+\tau)] = 1$ if $X(i) = Y(i+\tau)$, and 0 otherwise, and the addition operations are performed modulo L. If $X = Y$, $H_{X,X}(\cdot)$ is called the *autocorrelation function* of FH sequence X. $H_{X,Y}(\cdot)$ is the *crosscorrelation function* of X and Y if $X \neq Y$. For any distinct $X, Y \in \mathcal{F}$, we define

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

Lempel and Greenberger [13] developed the following lower bound for $H(X)$.

Lemma 1.1. *For every FH sequence of length L over an alphabet F of size γ, we have*

$$H(X) \geq \left\lceil \frac{(L-\varepsilon)(L+\varepsilon-\gamma)}{\gamma(L-1)} \right\rceil$$

where ε is the least nonnegative residue of L modulo γ.

The maximum nontrivial Hamming correlation of the FH sequence set $\mathcal{F}$ is defined by $M(\mathcal{F}) = max\{H(X), H(X,Y)\}$. In 2004, Peng and Fan [15] described the following bounds on $M(\mathcal{F})$.

Lemma 1.2. *Let $\mathcal{F}$ be a set containing N FH sequences of length L over an alphabet of size γ. Define $I = \lfloor LN/\gamma \rfloor$, Then*

$$M(\mathcal{F}) \geq \left\lceil \frac{(LN-\gamma)L}{(LN-1)\gamma} \right\rceil$$

and

$$M(\mathcal{F}) \geq \left\lceil \frac{2ILN - (I+1)I\gamma}{(LN-1)N} \right\rceil.$$

From Lemmas 1.1 and 1.2, we can define an optimal sequence and an optimal set as follows:

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

(1) an FH sequence $X \in \mathcal{F}$ is called optimal if the Lempel-Greenberger bound in Lemma 1.1 is met;
(2) an FH sequences set $\mathcal{F}$ is an optimal set if either of the bounds in Lemma 1.2 is met.

In this paper, let $(L, H(X); \gamma)$ denote an FH sequence X of length L over an alphabet F of size γ with the maximum nontrivial Hamming autocorrelation $H(X)$. Let $(L, N, M(\mathcal{F}); \gamma)$ denote a set of N FH sequences $\mathcal{F}$ of length L over an alphabet F of size γ with the maximum nontrivial Hamming correlation $M(\mathcal{F})$.

1.2. Linear span of a sequence

From the viewpoint of engineering, a linear span of a sequence is the length of the shortest linear feedback shift register (LFSR) which can produce the sequence [10]. Let p be a prime and $q = p^r$, r is a positive integer. F_q denotes the finite field with q elements. Let $s = (s_0, s_1, \ldots)$, $s_i \in F_q$, be a sequence produced by the LFSR and satisfy the following linear recurrence relation

$$s_{n+l} = c_1 s_{n+l-1} + c_2 s_{n+l-2} + \ldots + c_l s_n$$

where $n \geq 0$. $c(x) = c_l x^l + c_{l-1} x^{l-1} + \ldots + c_1 x + 1 \in F_q[x]$ is called the connection polynomial of the LFSR or a connection polynomial of sequence s. The connection polynomial of s with the least degree is called the minimal polynomial of s. The minimal polynomial of a periodic sequence s is uniquely defined. The linear span of a sequence s is defined as the degree of the minimal polynomial of s. If $c(x)$ is a primitive polynomial then the sequence s is called an m-sequence [11]. In this case, the linear span of s equals l.

In some applications, the FH sequences are required to have a large linear span, which ensures that the code sequences underlying the FH pattern can not be reconstructed by a vicious attacker. A large linear span is desired for a more robust FH sequence design and is a necessary condition for the security of sequences applied in cryptography. There are several optimal sets of FH sequences with large linear spans [12, 17].

1.3. Our contributions

In [18], the power permutation, $x \to x^\sigma$ over F_q, where $\gcd(\sigma, q-1) = 1$, was employed to improve the linear span of three classes of optimal sets of FH sequences. It was shown that the obtained FH sequences have much larger linear span compared with the primary ones. Wang [18] mentioned that '*the other type of permutation polynomials over F_q may be employed in the same way for improving the linear spans of FH sequences in some optimal sets, but calculating the linear spans of the transformed sequences may not be easy*'. The objective of this paper is to obtain new optimal sets of FH sequences with large linear span by using another type of permutation polynomials, which is different from power permutations. By using the method of counting terms in the root representation

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

of FH sequences, we give the exact values of the linear span of the transformed optimal sets of FH sequences. The obtained FH sequences have not only optimal Hamming correlations, but also large linear span to resist the Berlekamp-Massey algorithm. The results show that, besides the power permutation, the permutation polynomial used here can also be employed to improve the linear span of the optimal sets of FH sequences and we can calculating the exact values of the linear span.

2. Preliminaries

We begin this section by introducing some notations that will be used throughout this paper.

- p is an odd prime. $r \geq 1$ is a positive integer and $q = p^r$;
- F_{q^m}: the finite field with q^m elements, and $F_{q^m}^* = F_{q^m} - \{0\}$;
- α is a generator of $F_{q^m}^*$;
- m, n: two positive integers with $n|m$;
- $\mathrm{Tr}_n^m(x) = \sum_{i=0}^{\frac{m}{n}-1} x^{q^{ni}}$ for $x \in F_{q^m}$. $\mathrm{Tr}_n^m(\cdot)$ denotes the trace function from F_{q^m} to F_{q^n};
- $\mathcal{N}_n^m(x) = x^q \cdot x^{q^n} \ldots x^{q^{n(m/n-1)}}$ for $x \in F_{q^m}$. $\mathcal{N}_n^m(x)$ denotes the norm function from F_{q^m} to F_{q^n}. In this paper, we abbreviate the $\mathcal{N}_n^m(x)$ as $\mathcal{N}(x)$.

The following Theorem 2.1 comes from [14].

Theorem 2.1. *Let q be an odd integer, and $\delta(x) = x^{(q+1)/2} + bx \in F_q[x]$. $\delta(x)$ is a permutation polynomial over F_q if and only if $b = (c^2+1)(c^2-1)^{-1}$, where $c \in F_q$, $c \neq 0$ and $c^2 \neq 1$.*

Obviously, the permutation polynomial $\delta(x)$ is different from the power permutation. Note that $(q+1)/2$ may not be coprime with $q-1$.

Let $q > 3$, then $(q+1)/2 < q-1$. Let $s = \{s_i\}$ be a sequence over F_q, where s_i can be expressed as

$$s_i = \sum_{j=0}^{n-1} \lambda_j \alpha^{e_j i}$$

where $\lambda_j \neq 0$ for all j, and $0 \leq e_j < q-1$ for all j. The linear span of the sequence s is easily determined by n, *i.e.*, the number of nonzero coefficients in the powers-of-α representation [1,16]. In the following, we will determine the linear span of the transformed sequences by counting the terms of the powers-of-α representation of the transformed sequences.

3. Transformed optimal sets of FH sequences by $\delta(x)$

3.1. The first optimal class of FH sequences

In [4], Ding *et al.*, presented a construction of optimal set of q-ary FH sequences of length $q^m - 1$. It is described as follows.

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

Let d be a positive integer with $1 \leq d \leq q-2$. $\forall \quad u, v \in F_{q^m}$, we define a function $f_{u,v}(x)$ from F_{q^m} to F_q as follows

$$f_{u,v}(x) = \mathrm{Tr}_1^m \left(u\mathcal{N}\left(x^d\right) + vx\right) \tag{3.1}$$

we define the following vector

$$s_{u,v} = \left(f_{u,v}\left(\alpha^0\right), f_{u,v}\left(\alpha^1\right), \ldots, f_{u,v}\left(\alpha^{q^m-2}\right)\right). \tag{3.2}$$

The parameter d plays a role of determining different sequences. Given a specific value of d, we obtain a specific function $f_{u,v}(x)$, furthermore, the sequence $s_{u,v}$. If the parameter d satisfies some condition, the sequence $s_{u,v}$ will be an optimal frequency hopping sequence. The following theorem comes from [4].

Theorem 3.1. *With the same notation as above, define*

$$\mathcal{F} = \{s_{u'u,1} : u \in F_q\}. \tag{3.3}$$

Assume $gcd(dm-1, q-1) = 1$ *for* $1 \leq d \leq q-2$ *and* u' *is an element in* F_q^* *with* $Tr_1^m(u') \neq 0$. *Then for* $u \in F_q$, $s_{u'u,1}$ *is a* $(q^m-1, q^{m-1}; q)$ *optimal FH sequence meeting the bound in Lemma 1.1.* $\mathcal{F}$ *is a* $(q^m-1, q, q^{m-1}; q)$ *optimal FH sequence set with respect to the first bound of Lemma 1.2.*

In [18], Wang showed that the linear span of $s_{u'u,1}$ is equal to m for $u = 0$ and $m+1$ for $u \neq 0$. Obviously, the linear span of $s_{u'u,1}$ is very small compared with its length $q^m - 1$. Following the work in [18], we can significantly improve the linear span of the FH sequences in $\mathcal{F}$ by using the permutation polynomial in Theorem 2.1.

The following Theorem 3.3 gives the linear spans of the transformed sequences set by $\delta(x)$.

Theorem 3.2. *Let* $d = 1$, *then* $s_{u'u,1}(x) = \mathrm{Tr}_1^m(u'u\mathcal{N}(x) + x)$. *Let* p *be a prime,* $q = p^r$ *and* $q > 3$. *Assume that* $gcd(m-1, q-1) = 1$, u' *is an element of* $F_{q^m}^*$ *and* $Tr(u') \neq 0$. *For* $0 \leq t \leq q^m - 2$, *define*

$$\delta(s_{u'u,1}(t)) = \left(\mathrm{Tr}_1^m\left(u'u\mathcal{N}\left(\alpha^t\right) + \alpha^t\right)\right)^{(q+1)/2} + b\mathrm{Tr}_1^m\left(u'u\mathcal{N}\left(\alpha^t\right) + \alpha^t\right)$$

where α *is a generator of* $F_{q^m}^*$, $u \in F_q$ *and* b *is the parameter in* $\delta(x)$ *in Theorem 2.1. Then we have*

(1) $\delta(\mathcal{F}) = \{\delta(s_{u'u,1}) : u \in F_q\}$ *is a*

$$(q^m - 1, q, q^{m-1}; q)$$

optimal set of FH sequences with respect to the first bound of Lemma 1.2. Each sequence in $\delta(\mathcal{F})$ *for* $u \in F_q$ *is optimal with respect to the Lempel-Greenberg bound;*

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

(2) *for the transformed FH sequences, if* $u = 0$*, the linear span is*

$$\prod_{i=0}^{r-1} \binom{m+\eta_i-1}{\eta_i} + m$$

and if $u \neq 0$*, the linear span is*

$$\prod_{i=0}^{r-1} \binom{m+\eta_i}{\eta_i} + m + 1$$

where $(q+1)/2 = \sum_{i=0}^{r-1} \eta_i p^i$ *and* $\eta_0 = (p+1)/2$, $\eta_i = (p-1)/2$ *for* $i \in \{1, 2, \ldots, r-1\}$.

Proof. Let $d = 1$, then

$$s_{u'u,1}(t) = \mathrm{Tr}_1^m(u'u\mathcal{N}(\alpha^t) + \alpha^t)$$

for $0 \leq t \leq q^m - 2$. We have

$$\delta(s_{u'u,1}(t)) = \left(\mathrm{Tr}_1^m\left(u'u\mathcal{N}\left(\alpha^t\right) + \alpha^t\right)\right)^{(q+1)/2} + b\mathrm{Tr}_1^m\left(u'u\mathcal{N}\left(\alpha^t\right) + \alpha^t\right).$$

Note that $q = p^r$, according to the p-ary representation, $(q+1)/2$ can be uniquely written as follows

$$(q+1)/2 = \sum_{i=0}^{r-1} \eta_i p^i$$

where $\eta_0 = (p+1)/2$, $\eta_i = (p-1)/2$ for $i \in \{1, 2, \ldots, r-1\}$. Since $u \in F_q$, $\mathcal{N}(\alpha^t) = \alpha^{\frac{q^m-1}{q-1}t} \in F_q$, so we have

$$\begin{aligned}
\left(\mathrm{Tr}_1^m\left(u'u\mathcal{N}\left(\alpha^t\right) + \alpha^t\right)\right)^{(q+1)/2} &= \left(u\mathrm{Tr}_1^m(u')\left(\alpha^{\frac{q^m-1}{q-1}t}\right) + \mathrm{Tr}_1^m\left(\alpha^t\right)\right)^{(q+1)/2} \\
&= \left(u\mathrm{Tr}_1^m(u')\left(\alpha^{\frac{q^m-1}{q-1}t}\right) + \mathrm{Tr}_1^m\left(\alpha^t\right)\right)^{\sum_{i=0}^{r-1}\eta_i p^i} \\
&= \prod_{i=0}^{r-1}\left(u^{p^i}\mathrm{Tr}_1^m(u')^{p^i}\left(\alpha^{\frac{q^m-1}{q-1}p^i t}\right) + \mathrm{Tr}_1^m\left(\alpha^t\right)^{p^i}\right)^{\eta_i}.
\end{aligned}$$

According to the definition of the trace function, we have

$$\left(u^{p^i}\mathrm{Tr}_1^m(u')^{p^i}\left(\alpha^{\frac{q^m-1}{q-1}p^i t}\right) + \mathrm{Tr}_1^m\left(\alpha^t\right)^{p^i}\right)^{\eta_i} = \left(u^{p^i}\mathrm{Tr}_1^m(u')^{p^i}\left(\alpha^{\frac{q^m-1}{q-1}p^i t}\right) + \sum_{j=0}^{m-1}\left(\alpha^{p^i t}\right)^{q^j}\right)^{\eta_i}.$$

By using the multinomial formula,

$$\left(\sum_{i=1}^{r} a_i\right)^{\eta} = \sum_{k_1+k_2+\ldots+k_r=\eta} \binom{\eta}{k_1, \ldots, k_r} a_1^{k_1} \ldots a_r^{k_r}$$

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

where $0 \le k_i \le \eta$ for $i = 1, 2, \ldots, r$, and

$$\binom{\eta}{k_1, \ldots, k_r} = \frac{\eta!}{k_1! k_2! \ldots k_r!}.$$

For $u \neq 0$, we get

$$\left(u^{p^i} \mathrm{Tr}_1^m(u')^{p^i} \alpha^{\frac{q^m-1}{q-1} p^i t} + \sum_{j=0}^{m-1} \left(\alpha^{p^i t}\right)^{q^j} \right)^{\eta_i}$$
$$= \sum_{\lambda_{i,0}+\ldots+\lambda_{i,m}=\eta_i} \binom{\eta_i}{\lambda_{i,0}, \ldots, \lambda_{i,m}} \left(\alpha^{p^i t}\right)^{\sum_{j=0}^{m-1} q^j \lambda_{i,j}} \cdot \left(u^{p^i} \mathrm{Tr}_1^m(u')^{p^i} \alpha^{\frac{q^m-1}{q-1} p^i t} \right)^{\lambda_{i,m}}.$$

Then we get

$$\begin{aligned}
&\left(\mathrm{Tr}_1^m\left(u' u \mathcal{N}\left(\alpha^t\right) + \alpha^t\right)\right)^{(q+1)/2} \\
&= \prod_{i=0}^{r-1} \sum_{\lambda_{i,0}+\ldots+\lambda_{i,m}=\eta_i} \binom{\eta_i}{\lambda_{i,0}, \ldots, \lambda_{i,m}} \cdot \left(\alpha^{p^i t}\right)^{\sum_{j=0}^{m-1} q^j \lambda_{i,j}} \cdot \left(u^{p^i} \mathrm{Tr}_1^m\left(u'\right)^{p^i} \alpha^{\frac{q^m-1}{q-1} p^i t} \right)^{\lambda_{i,m}} \\
&= \sum_{\sum_{j=0}^{m} \lambda_{0,j} = \eta_0} \cdots \sum_{\sum_{j=0}^{m} \lambda_{r,j} = \eta_r} \prod_{i=0}^{r-1} \binom{\eta_i}{\lambda_{i,0}, \ldots, \lambda_{i,m}} \cdot \left(u \mathrm{Tr}_1^m\left(u'\right)\right)^{\sum_{i=0}^{r-1} \lambda_{i,m} p^i} \cdot \alpha^{g(\lambda, r) t}
\end{aligned} \tag{3.4}$$

where

$$g(\lambda, r) = \sum_{j=0}^{m-1} q^j \sum_{i=0}^{r-1} \lambda_{i,j} p^i + \frac{q^m - 1}{q-1} \sum_{i=0}^{r-1} \lambda_{i,m} p^i.$$

Since $\frac{q^m-1}{q-1} = \sum_{j=0}^{m-1} q^j$, we have

$$g(\lambda, r) = \sum_{j=0}^{m-1} q^j \left(\sum_{i=0}^{r-1} (\lambda_{i,j} + \lambda_{i,m}) p^i \right).$$

In the following, we show that the exponents $g(\lambda, r)$ of α in equation (3.4) are pairwise distinct. Assuming $\lambda \neq \lambda'$, however, they produce the same exponents of α mod $q^m - 1$, that is,

$$g(\lambda, r) \equiv g(\lambda', r) \mathrm{mod}(q^m - 1) \tag{3.5}$$

Since

$$\sum_{i=0}^{r-1} (\lambda_{i,j} + \lambda_{i,m}) p^i \le (q+1)/2 < q - 1$$

Obviously, $g(\lambda, r)$ is less than $q^m - 1$ and the modulo operation in equation (3.5) can be omitted.

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

The above equation (3.5) is equivalent to

$$\sum_{j=0}^{m-1} q^j \left(\sum_{i=0}^{r-1} (\lambda_{i,j} + \lambda_{i,m}) p^i \right) = \sum_{j=0}^{m-1} q^j \left(\sum_{i=0}^{r-1} (\lambda'_{i,j} + \lambda'_{i,m}) p^i \right). \tag{3.6}$$

Firstly, we reduce equation (3.6) modulo q, then we obtain

$$\sum_{i=0}^{r-1} (\lambda_{i,0} + \lambda_{i,m}) p^i \equiv \sum_{i=0}^{r-1} (\lambda'_{i,0} + \lambda'_{i,m}) p^i \bmod q. \tag{3.7}$$

Since both sides in equation (3.7) are less than q, and both $\lambda_{i,0} + \lambda_{i,m}$ and $\lambda'_{i,0} + \lambda'_{i,m}$ are less than $p-1$, we have $\lambda_{i,0} + \lambda_{i,m} = \lambda'_{i,0} + \lambda'_{i,m}$. Similarly, we reduce equation (3.6) modulo q^j for $j = 2, 3, \ldots, m-1$, then we have

$$\lambda_{i,j} + \lambda_{i,m} = \lambda'_{i,j} + \lambda'_{i,m} \tag{3.8}$$

for $0 \le i \le r-1$ and $0 \le j \le m-1$. Adding both sides of the m equations, we have

$$\sum_{j=0}^{m-1} \lambda_{i,j} + m\lambda_{i,m} = \sum_{j=0}^{m-1} \lambda'_{i,j} + m\lambda'_{i,m}$$

for $0 \le i \le r-1$. Therefore,

$$\eta_i + (m-1)\lambda_{i,m} = \eta_i + (m-1)\lambda'_{i,m}$$

so we have $\lambda_{i,m} = \lambda'_{i,m}$. From the equation (3.8), we have $\lambda_{i,j} = \lambda'_{i,j}$ for $0 \le i \le r-1$ and $0 \le j \le m-1$. Thus we have shown that all the exponents of α in equation (3.4) are pairwise distinct.

In the following, we show that the exponents of α in $\mathrm{Tr}_1^m(u'u\mathcal{N}(\alpha^t) + \alpha^t)$ are pairwise distinct to that of α in equation (3.4). Note that

$$\mathrm{Tr}_1^m(u'u\mathcal{N}(\alpha^t) + \alpha^t) = u\mathrm{Tr}_1^m(u')(\alpha^{\frac{q^m-1}{q-1}t}) + \sum_{j=0}^{m-1} \alpha^{q^j t}. \tag{3.9}$$

Since $q^j \neq \frac{q^m-1}{q-1}$ for $0 \le j \le m-1$, all the terms of the powers of α in equation (3.9) are pairwise distinct. Now we consider the exponent $g(\lambda, r)$ in equation (3.4) and the q^j for $0 \le j \le m-1$. Obviously, $g(\lambda, r) \neq 1$, and we only consider whether $g(\lambda, r) = q^k$ for $k \in \{1, 2, \ldots, m-1\}$. Assume that $g(\lambda, r)$ is equal to some q^k, $k \in \{1, 2, \ldots, m-1\}$, that is,

$$\sum_{j=0}^{m-1} q^j \left(\sum_{i=0}^{r-1} (\lambda_{i,j} + \lambda_{i,m}) p^i \right) = q^k.$$

Both sides of the above equation are taken modulo q^k, we get

$$\sum_{j=0}^{k-1} q^j \left(\sum_{i=0}^{r-1} (\lambda_{i,j} + \lambda_{i,m}) p^i \right) \equiv 0 \bmod q^k. \tag{3.10}$$

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

It implies that the left side of equation (3.10) is a multiple of q^k. However, $\sum_{i=0}^{r-1}(\lambda_{i,j}+\lambda_{i,m})p^i < q-1$, which implies that the left side of equation (3.10) is less than q^k, a contradiction. Therefore $g(\lambda,r)$ and all of the q^j for $0 \le j \le m-1$ are pairwise distinct.

In the following, we consider the exponents of $g(\lambda,r)$ and $\frac{q^m-1}{q-1} = \sum_{j=0}^{m-1} q^j$. Assume that

$$\sum_{j=0}^{m-1} q^j \left(\sum_{i=0}^{r-1} (\lambda_{i,j}+\lambda_{i,m})p^i \right) = \sum_{j=0}^{m-1} q^j.$$

Since $\sum_{i=0}^{r-1}(\lambda_{i,j}+\lambda_{i,m})p^i < q-1$, we know that $\sum_{i=0}^{r-1}(\lambda_{i,j}+\lambda_{i,m})p^i = 1$ for $0 \le j \le m-1$. It implies that

$$\begin{cases} \lambda_{0,j}+\lambda_{0,m} = 1 \ 0 \le j \le m-1 \\ \lambda_{i,j}+\lambda_{i,m} = 0 \ \ 0 \le j \le m-1 \text{ and } 1 \le i \le r-1. \end{cases}$$

Therefore, we have $\eta_0 = 1$, and $\eta_i = 0$ for $1 \le i \le r-1$, which is a contradiction to $\eta_0 = (p+1)/2$, $\eta_i = (p-1)/2$. It follows that the exponents of α in $\delta(s_{u'u,1}(t))$ are pairwise distinct. Since there are

$$\binom{m+\eta_i}{\eta_i}$$

possibilities to represent η_i as

$$\eta_i = \sum_{j=0}^{m} \lambda_{i,j}$$

for $0 \le \lambda_{i,j} \le \eta_i$. By applying the results to all η_i's, we have, if $u \neq 0$, the linear span of $\delta(s_{u'u,1}(t))$ is

$$LS = \prod_{i=0}^{r-1} \binom{m+\eta_i}{\eta_i} + m + 1.$$

If $u = 0$, then

$$\delta(s_{u'u,1}(t)) = \mathrm{Tr}_1^m(\alpha^t)^{(q+1)/2} + b\mathrm{Tr}_1^m(\alpha^t).$$

We have the linear span is

$$LS = \prod_{i=0}^{r-1} \binom{m+\eta_i-1}{\eta_i} + m$$

which completes the proof. □

Remarks 3.3. Our proof is similar with that in [18], and our Theorem is only suitable for the case of $d = 1$. If $d > 1$, from equations (3.7) and (3.8), we know that the exponents of α may be the same in (3.4), which leads to a decrease of the linear span of the transformed frequency hopping sequences. The permutation polynomial $\delta(x)$ also applies to other two classes of optimal sets of FH sequences presented by Ding *et al.* in [4].

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

3.2. Two other optimal classes of FH sequences with large linear span

Let $n = (q^m - 1)/2$, and let d be an integer with $gcd(d, q^m - 1) = 1$. Define $\beta = \alpha^{2d}$. For any $a \in F_{q^m}$, we define a vector

$$s_a = (\mathrm{Tr}_1^m(a), \mathrm{Tr}_1^m(a\beta), \ldots, \mathrm{Tr}_1^m(a\beta^{n-1})). \tag{3.11}$$

Note that for any a, $a' \in F_{q^m}$, we have $s_a + s_{a'} = s_{a+a'}$. The following theorem comes from [4].

Theorem 3.4. *Let $m \geq 3$ be odd, then for $a \in F_{q^m}^*$, s_a is an optimal $((q^m - 1)/2, (q^{m-1} - 1)/2; q)$ FH sequence with the bound of Lemma 1.1. Let a be a square in $F_{q^m}^*$ and a' be a nonsquare in $F_{q^m}^*$, then $\{s_a, s_{a'}\}$ consists of a $((q^m - 1)/2, 2, (q^{m-1} - 1)/2; q)$ optimal set of FH sequences with respect to the bound of Lemma 3.1.*

Though $\{s_a, s_{a'}\}$ consists of an optimal set of FH sequences, the linear span of each of sequence in $\{s_a, s_{a'}\}$ is equal to m, which is very small compared with with their length $(q^m - 1)/2$. We can improve the linear span of s_a and $s_{a'}$ by employing the permutation polynomial $\delta(x)$. The transformed set is still optimal with respect to the first bound of Lemma 1.2. By using a similar method to prove Theorem 3.3, we can obtain the following theorem.

Theorem 3.5. *Let s_a be defined by* (3.11) *and $b = (c^2 + 1)(c^2 - 1)^{-1}$, where $c \in F_q$, $c \neq 0$ and $c^2 \neq 1$. Let $\delta(x) = x^{(q+1)/2} + bx \in F_q[x]$. Define*

$$\delta(s_a(t)) = \mathrm{Tr}_1^m(a\beta^t)^{(q+1)/2} + b\mathrm{Tr}_1^m(a\beta^t).$$

Then

(1) *$(\delta(s_a), \delta(s_{a'}))$ constitutes a $((q^m - 1)/2, 2, (q^{m-1} - 1)/2; q)$ optimal set of FH sequences over F_q, meeting the first bound of Lemma 1.2. Furthermore, both sequences are optimal with respect to the bound of Lemma 1.1;*

(2) *the linear span of the transformed FH sequences is*

$$\binom{m + (p+1)/2 - 1}{(p+1)/2} \binom{m + (p-1)/2 - 1}{(p-1)/2}^{r-1} + m.$$

In the following, we discuss the linear span of the third optimal set of FH sequences. This construction can be viewed as a generalization of the second optimal set of FH sequences. The linear span is still very small compared with their lengths [18]. The original construction is as follows. Suppose that m and d are two positive integers satisfying $d|(q^m - 1)$ and $gcd(d, (q^m - 1)/(q - 1)) = 1$, which implies that $d|(q - 1)$. Define $\beta = \alpha^{\mu d}$, where μ is a positive integer with $gcd(\mu, q^m - 1) = 1$, and let $n = (q^m - 1)/d$. For each $0 \leq i \leq d - 1$, we define the following sequence,

$$s_i(t) = \mathrm{Tr}_1^m(\alpha^i \beta^t), \quad 0 \leq t \leq n - 1 \tag{3.12}$$

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

Each s_i is a sequence of length n over F_q. The set of FH sequences is defined as

$$\mathcal{F} = \{s_i : 0 \le i \le d-1\}.$$

Theorem 3.6 ([3,9]). *If* $gcd(d, \sum_{i=0}^{m-1} q^i) = 1$, *then* $\mathcal{F}$ *is a* $((q^m-1)/d, d, (q^{m-1}-1)/d; q)$ *optimal set of FH sequences over* F_q, *meeting the first bound of Lemma 1.2. Furthermore, each sequence is optimal with respect to the bound of Lemma 1.1.*

Similarly, we can obtain the following theorem by applying the permutation polynomial $\delta(x)$ to the sequence s_i.

Theorem 3.7. *Let* $s_i(t)$ *be defined by* (3.12) *and* $b = (c^2+1)(c^2-1)^{-1}$, *where* $c \in F_q$, $c \neq 0$ *and* $c^2 \neq 1$. *Let* $\delta(x) = x^{(q+1)/2} + bx \in F_q[x]$. *Define*

$$\delta(s_i(t)) = \mathrm{Tr}_1^m(\alpha^i\beta^t)^{(q+1)/2} + b\mathrm{Tr}_1^m(\alpha^i\beta^t).$$

Then

(1) *If* $gcd(d, \sum_{i=0}^{m-1} q^i) = 1$, *then* $\{\delta(s_i)|0 \le i \le d-1\}$ *constitutes a* $((q^m-1)/d, d, (q^{m-1}-1)/d; q)$ *optimal set of FH sequences over* F_q, *meeting the first bound of Lemma 1.2. Furthermore, each sequence is optimal with respect to the bound of Lemma 1.1.*

(2) *The linear span of the transformed FH sequences is*

$$\binom{m+(p+1)/2-1}{(p+1)/2}\binom{m+(p-1)/2-1}{(p-1)/2}^{r-1} + m.$$

Remarks 3.8. From Theorem 3.3, Theorems 3.5 and 3.7, we find that the linear spans of three classes of frequency hopping sequences are significantly improved. For example, for $q = 3^4$, $m = 5$ and $d = 2$, the linear span of the third class sequences is only 5. However, from Theorem 3.7, the linear span of the transformed sequences is 1880.

4. Conclusions

In this paper, we transform several classes of optimal sets of FH sequences with small linear span into ones with large linear span by applying a permutation polynomial $\delta(x)$ over the finite field F_q with $q > 3$. The transformed sequence sets are not only optimal for the Peng-Fan bound, but can also resist the cryptanalysis of the Berlekamp-Massey algorithm. Furthermore, our results confirm Wang's proposition, that other type of permutation polynomial different from the power permutation polynomial, can also be employed for improving the linear span of optimal sets of FH sequences. Note that the permutation polynomial $\delta(x)$ can be employed for other optimal sets of FH sequences, such as the optimal sets of FH sequences from linear cyclic codes considered in [5,6].

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press

References

[1] M. Antweiler and L. Bömer, Complex sequences over $GF(p^M)$ with a two-level autocorrelation function and a large linear span. *IEEE Trans. Inf. Theory* **38** (1992) 120–30.

[2] W. Chu and C.J. Colbourn, Optimal frequency-hopping sequences *via* cyclotomy, *IEEE Trans. Inf. Theory* **51** (2005) 1139–1141.

[3] C. Ding and J. Yin, Sets of optimal frequency hopping sequences, *IEEE Trans. Inf. Theory* **54** (2008) 3741–3745.

[4] C. Ding, M. Miosio and J. Yuan, Algebraic constructions of optimal frequency hopping sequences. *IEEE Trans. Inf. Theory* **53** (2007) 2606–2610.

[5] 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* **55** (2009) 3297–3304.

[6] C. Ding, Y. Yang and X. Tang, Optimal sets of frequency hopping sequences from linear cyclic codes. *IEEE Trans. Inf. Theory* **56** (2010) 3605–3612.

[7] R. Fuji-Hara, Y. Miao and M. Mishima, Optimal frequency hopping sequences: a combinatorial approach. *IEEE Trans. Inf. Theory* **50** (2004) 2408–2420.

[8] G. Ge, R. Fuji-Hara and Y. Miao, Further combinatorial constructions for optimal frequency hopping sequences. *J. Comb. Th. (A)* **113** (2006) 1699–1718.

[9] G. Ge, Y. Miao and Z. Yao, Optimal frequency hopping sequences: auto- and cross-correlation properties. *IEEE Trans. Inf. Theory* **55** (2009) 867–879.

[10] S.W. Golomb and G. Gong, *Signal Design for Good Correlation, for Wireless Communication, Cryptography, and Radar*. Cambridge University, Cambridge, UK Press (2005).

[11] J.J. Komo and S.C. Liu, Maximal length sequences for frequency hopping. *IEEE J. Select. Areas Commun.* **5** (1990) 819–822.

[12] P.V. Kumar, Frequency-hopping code sequence designs having large linear span. *IEEE Trans. Inf. Theory* **34** (1988) 146–151.

[13] A. Lempel and H. Greenberger, Families of sequences with optimal Hamming correlation properties. *IEEE Trans. Inf. Theory* **20** (1974) 90–94.

[14] R. Lidl and H. Niederreiter, Finite fields, *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, UK **20** (1997).

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

[16] M.K. Simon, J.K. Omura, R.A. Scholz and B.K. Levitt, *Spread Spectrum communications Handbook*. McGraw-Hill, New York (2002).

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

[18] Q. Wang, Optimal sets of frequency hopping sequences with large linear spans. *IEEE Trans. Inf. Theory* **56** (2010) 1729–1736.

[19] Z. Zhou and X. Tang, A new construction of optimal frequency hopping sequence sets. *IEEE Proc. of IWSDA'09* (2009) 92–95.

Communicated by N. Sendrier.
Received August 30, 2010. Accepted January 30, 2012.

https://doi.org/10.1051/ita/2012007 Published online by Cambridge University Press