Frequency/Time Hopping Sequences with Large Linear Complexities*

Yun-Pyo Hong and Hong-Yeop Song

CITY - Center for Information Technology of Yonsei University
Coding and Information Theory Lab.
Department of Electrical and Electronic Engineering, Yonsei University
134 Shinchon-dong Seodaemun-gu, Seoul, Korea, 120-749
{yp.hong, hy.song}@coding.yonsei.ac.kr

Abstract. In this paper, we discuss some methods of constructing frequency/time hopping (FH/TH) sequences over $GF(p^k)$ by taking successive k-tuples of given sequences over $GF(p)$. We are able to characterize those p-ary sequences whose k-tuple versions now over $GF(p^k)$ have the maximum possible linear complexities (LCs). Next, we consider the FH/TH sequence generators composed of a combinatorial function generator and some buffers. We are able to characterize the generators whose output FH/TH sequences over $GF(p^k)$ have the maximum possible LC for the given algebraic normal form.

1 Introduction

In a peer-to-peer frequency/time hopping (FH/TH) spread spectrum communication system, an interceptor may try to synthesize the entire FH/TH pattern from some frequency/time slots successively observed. That is, the interceptor may try to synthesize the linear feedback shift register (LFSR) [1][2] that can generate the next slots of the FH/TH pattern using, say, Berlekamp-Massey (BM) algorithm [3] over a finite field.

Let L be the linear complexity (LC) [4][5] of an FH/TH sequence. When the interceptor observes successive $2L$ frequency/time slots, he can successfully synthesize the next frequency/time slots as long as the same FH/TH sequence is used. Therefore, from the view point of the system designers, the system should change from one FH/TH sequence to another before $2L$ slots of the sequence are used, and the LC of the FH/TH sequences in use should be as large as possible.

Note that any FH/TH sequences are non-binary in general since there are usually more than 2 frequency/time slots available. In fact, an FH/TH communication systems using a few hundreds, or even a few thousands frequency/time slots are common in practice. It is well-known that the number of frequency/time slots affects directly the processing gain [2] of the FH/TH spread spectrum communication systems, at the price of the hardware complexity. Therefore, it is

* This work was supported by grant No.(R01-2003-000-10330-0) from the Basic Research Program of the Korea Science and Engineering Foundation.

Ø. Ytrehus (Ed.): WCC 2005, LNCS 3969, pp. 386–396, 2006.

necessary to design non-binary sequences (i) with “large” LC, and (ii) over “large” alphabet, but (iii) with “little” increase in the hardware complexity.

In this paper, we consider the simple way of constructing a non-binary (p^k-ary) sequence T over a large alphabet from a given (p-ary) sequence S over a small alphabet, simply reading its successive k-tuples. By increasing the parameter k, one may obtain a sequence over as large alphabet as one wishes. We believe that this method is so simple to construct a p^k-ary sequence compared with a construction over $GF(p^k)$ because the multiplications over $GF(p^k)$ is much more complex than those over $GF(p)$ in the LFSR constructions which is general methods in the hardware systems. In this view point, there will be no significant increase in the complexity in actual hardware design. Therefore, this method satisfies the last two conditions listed in the previous paragraph.

On the other hand, we have to be very careful in analyzing the LC of the new sequences, including the definition of the LC of T over k-tuples over $GF(p)$ which is not a field any more. One way to solve this problem is to interpret the k-tuples over $GF(p)$ as elements of $GF(p^k)$. In this case, it is not much surprising to observe that two different basis may result in two different LC of T (now over $GF(p^k)$), and hence, the LC of T depends on the choice of basis (of $GF(p^k)$ over $GF(p)$).

We are here trying to rule out any possibility that the decrease in its LC using some other basis than that used in the design might help the intercepter to track the FH/TH sequence, assuming that the FH/TH sequence T with its LC equal to L (using the basis used in the design process) is used for the duration of $2L-1$ slots.

Given any one basis, it is clear that the LC of T is at most that of S. We are able to characterize those p-ary sequences S whose k-tuple versions T now over $GF(p^k)$ have the same minimal polynomials [4][5] as S, and therefore, the same LC as S (that is the maximum possible), for any choice of basis of $GF(p^k)$ over $GF(p)$. This leads to the construction of p^k-ary sequences with minimal polynomials essentially over $GF(p)$.

We apply the above characterization into two sequences with as large as possible period when the number of registers, r, is given: binary de Bruijn sequences of period 2^r [6] and p-ary m-sequences of period p^r-1.

We consider the FH/TH sequence generators composed of a combinatorial function generator [7] and some buffers. We are able to characterize the FH/TH sequence generators which guarantee that a combinatorial function sequences, S, over $GF(p)$ have the maximum possible LC for the given algebraic normal form and that k-tuple versions T of S now over $GF(p^k)$ have the same minimal polynomials as S, and therefore, the same LC as S (that is the maximum possible) for any choice of basis of $GF(p^k)$ over $GF(p)$.

2 Constructions of Sequences over $GF(p^k)$ with Minimal Polynomials over $GF(p)$

Let $GF(q)$ be the finite field with q elements, and let p be a prime. Consider a given sequence $S=\{s_n|n=0,1,2,...\}$ over $GF(p)$. Let k be a positive integer, and define a new sequence (an FH/TH sequence) $T(k,S)=\{t_n|n=0,1,2,...\}$ based on S by the following:

$$t_n=(s_n,\ s_{n-1},\ \ldots,\ s_{n-k+1})\ . \tag{1}$$

Then, it is clear that the sequence $T(k,S)$ is over $GF(p)^k$, the k-tuple vector space over $GF(p)$. By using some but fixed basis such as a simple polynomial basis given by

$$\{\alpha^{k-1},\ \alpha^{k-2},\ \ldots,\ \alpha,\ 1\}, \tag{2}$$

where α is a primitive element of $GF(p^k)$, one can regard the sequence $T(k,S)$ being over a field $GF(p^k)$. This is a straightforward and simple way of enlarging the size of alphabet over which a sequence is.

Proposition 1. *The LFSR that generates a sequence $S=\{s_n\}$ over $GF(p)$ also generates $T(k,S)$ over $GF(p^k)$ as defined in* (1) *regardless of the choice of basis. The converse holds provided that the characteristic polynomial* [4][5] *that generates T over $GF(p^k)$ is essentially over $GF(p)$.*

Proof. Obvious. □

Example 1. A ternary sequence S with period 26 is given by

$$0\,0\,1\,1\,1\,0\,2\,1\,1\,2\,1\,0\,1\,0\,0\,2\,2\,2\,0\,1\,2\,2\,1\,2\,0\,2\,0\,0\ \ldots\ .$$

Then the sequences $T(3,S)$ and $T(4,S)$ according to (1) are given by the following:

$$T(3,S)=000\ \ 000\ \ 100\ \ 110\ \ 111\ \ 011\ \ 201\ \ 120\ \ 112\ \ 211\ \ \ldots,$$
$$T(4,S)=0002\ \ 0000\ \ 1000\ \ 1100\ \ 1110\ \ 0111\ \ 2011\ \ 1201\ \ 1120\ \ 2112\ \ \ldots\ .$$

Note that both T's as well as S are generated by the LFSR shown in Fig. 1 with connection coefficients over $GF(3)$.

Proposition 1 does not guarantee that the LFSR for $T(k,S)$ over $GF(p^k)$, $k\geq 2$, is necessarily the shortest possible even if it is the shortest for S over $GF(p)$, but that the LC of $T(k,S)$ is at most that of S. In fact, the shortest LFSR for $T(k,S)$ over $GF(p^k)$, $k\geq 2$, (and hence the LC of T) cannot be uniquely determined unless a basis of $GF(p^k)$ is fixed. Following example shows this.

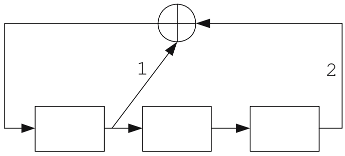

Fig. 1. The LFSR generating S and T's of Example 1

Example 2. (a) A binary sequence S_1 with period 63 is given by

$$110010000011111110101001001001101010111011011011101001111110010\ldots .$$

The LC of S_1 over $GF(2)$ is 62, but that of $T(3, S_1)$ over $GF(2^3)$ is 60 with respect to any polynomial basis as in (2). (b) A binary sequence S_2 with period 63 is given by

$$010111111100110000011011111101010011111100011001110100101001011\ldots .$$

The LC of $T(3, S_2)$ over $GF(2^3)$ is 55 or 53 with respect to the polynomial basis as in (2) using $x^3 + x + 1$ or $x^3 + x^2 + 1$, respectively.

A question at this point is the following: is it possible that the shortest LFSR that generates S over $GF(p)$ is indeed the shortest LFSR that generates $T(k, S)$ over $GF(p^k)$ with respect to some basis of $GF(p^k)$ over $GF(p)$ for $k \geq 2$? If it is possible to characterize such p-ary sequences S, then $T(k, S)$ over $GF(p^k)$ has the same minimal polynomial as S and hence it is over $GF(p)$.

Lemma 1. [4] (i) *The minimal polynomial of a sequence over $GF(q)$ divides any characteristic polynomial of the LFSR that generates the sequence over $GF(q)$. Therefore, it is uniquely determined up to the multiplication by a constant.* (ii) *An irreducible polynomial over $GF(q)$ of degree d remains irreducible over $GF(q^k)$ if and only if k and d are relatively prime.*

Theorem 1. *Let the minimal polynomial $C(x)$ of $S = \{s_n\}$ over $GF(p)$ be given by $C(x) = \prod_{i \in I}(f_i(x))^{m_i}$ for some irreducible polynomials $f_i(x)$ of degree d_i over $GF(p)$, some positive integers m_i, and some index set I. Let $T(k, S)$ over $GF(p^k)$ be defined as in* (1) *with respect to some but fixed basis for $k \geq 1$. Then,* (i) *the shortest LFSR that generates S is also the shortest LFSR that generates $T(k, S)$ over $GF(p^k)$, and therefore, their LCs are same, if k and d_i are relatively prime for all $i \in I$. Furthermore,* (ii) *it is also the shortest LFSR of $T(k, S)$ over $GF(p^m)$, and therefore, their LCs are same, for any $m \geq k$ such that m and d_i are relatively prime for all $i \in I$.*

Proof. (i) The LFSR with $C(x)$ also generate $T(k, S)$ over $GF(p^k)$ by Proposition 1. Suppose that the degree of $C(x)$ is not the least for $T(k, S)$. Then the shortest LFSR with characteristic polynomial $C'(x)$ exists and $C'(x)$ divides $C(x)$ by Lemma 1(i). $C'(x) = \prod_{i \in I}(f_i(x))^{s_i}$, where s_i is a non-negative integer, $0 \leq s_i \leq m_i$ for all $i \in I$, and $\sum_{i \in I} s_i < \sum_{i \in I} m_i$ by Lemma 1(ii). On the other hand, the polynomial $C'(x) = \prod_{i \in I}(f_i(x))^{s_i}$ is over $GF(p)$, and Proposition 1 (the converse part) implies that $C'(x)$ is also a characteristic polynomial for S over $GF(p)$ which is a desired contradiction. (ii) Furthermore, if we regard each term of $T(k, S)$ over $GF(p^m)$ for any $m \geq k$ such that m and d_i are relatively prime by inserting so many 0's at some fixed positions, all the previous arguments will be similarly applied. □

The converse of Theorem 1 is not generally true. We are able to construct p^k-ary FH/TH sequences as in Theorem 1 whose LC are the same as the original (that is the maximum possible) with respect to any basis from p-ary sequences. Thus, if the p-ary sequences have large LC, the resulting FH/TH sequences have the same large LC as the original with respect to any basis. We would like to emphasize the following two cases to which Theorem 1 applies.

Corollary 1. (i) *For a p-ary m-sequence S of period $p^r - 1$ with p a prime, the shortest LFSR that generates S is also the shortest LFSR that generates $T(k, S)$ over $GF(p^k)$ as defined in* (1) *with respect to any basis if k is relatively prime to r. Furthermore, it is also the shortest LFSR of $T(k, S)$ over $GF(p^m)$ for any $m \geq k$ which is relatively prime to r.* (ii) *If a binary sequence S has a period 2^r (for example, binary de Bruijn sequences), then the shortest LFSR that generates S is also the shortest LFSR that generates $T(k, S)$ over $GF(2^k)$ as defined in* (1) *for any positive integer k. Furthermore, it is also the shortest LFSR of $T(k, S)$ over $GF(2^m)$ for any $m \geq k$.*

Proof. (i) Obvious. (ii) We note that the minimal polynomial $C(x)$ of a binary sequence S with period 2^r is of the form $(1 + x)^\tau$ for some positive integer τ [6]. □

For a binary de Bruijn sequence, S, with period 2^r and large LC which is at least $2^{r-1} + r$ [6], $T(k, S)$ over $GF(2^k)$ as defined in (1) has the same large LC as S by Corollary 1(ii). In addition, the symbol distribution of the $T(k, S)$ in one period is uniform, that is any symbol of the $T(k, S)$ appears exactly 2^{r-k} times, $r \geq k$, in one period. In reality, the finite field of characteristic 2 would be a good choice for the algebraic structure of FH/TH sequences because the computations over characteristic 2 are most efficiently implemented as hardware systems and the usual practice follows this idea. In above three points, $T(k, S)$ from binary de Bruijn sequences would be good candidates for FH/TH sequences in a peer-to-peer FH/TH spread spectrum communication system.

Example 3. A binary sequence S with period 16 is given by

$$0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ \ldots\ .$$

An 8-ary sequence $T(3, S)$ with $k = 3$ over $GF(8)$ becomes

$$000\ 000\ 000\ 000\ 100\ 010\ 101\ 110\ 111\ 111\ 111\ 111\ \ldots\ .$$

An 8-ary sequence $T'(3, S)$ over $GF(16)$ becomes

$$0000\ 0000\ 0000\ 0000\ 0100\ 0010\ 0101\ 0110\ 0111\ 0111\ 0111\ 0111\ \ldots\ .$$

Here, the symbol 0 is padded at the leftmost position of the every term of $T(3, S)$, and the resulting 4-tuples are regarded as the elements of $GF(16)$. A 16-ary sequence $T(4, S)$ becomes

$$0001\ 0000\ 0000\ 0000\ 1000\ 0100\ 1010\ 1101\ 1110\ 1111\ 1111\ 1111\ \ldots\ .$$

All these sequences have the same minimal polynomial and the corresponding LFSR is shown in Fig. 2.

Remark 1. Some interesting discussions are given in [8] and [9] which are methods of constructing p^k-ary m-sequences using several p-ary m-sequences of the same period. We note that the resulting m-sequences over $GF(p^k)$ do not have the same minimal polynomial as the component p-ary m-sequences. In [9], for example, if the minimal polynomial $C(x)$ of the component p-ary m-sequence over $GF(p)$ has degree kn, then the minimal polynomial of resulting p^k-ary m-sequence over $GF(p^k)$ has degree n, and in fact, it is a factor of $C(x)$ over $GF(p^k)$.

Remark 2. Some interesting discussions are given in [10] which establish a lower bound on the LC of a multisequence over $GF(q^k)$ in terms of the joint LC of its k element sequences of period N over $GF(q)$. We note that he characterize the period, N, of which the LC of a multisequence is the same as the joint LC of element sequences.

Now, let $U = \{u_n | n = 0, 1, 2, ...\}$ be a p-ary k-tuple FH/TH sequence in general. In order to determine its minimal polynomial and therefore, LC of U over $GF(p^k)$, we need to fix one basis for BM algorithm. Following theorem characterizes those U which do not need this.

Theorem 2. *Let $U = \{u_n | n = 0, 1, 2, ...\}$ be a p-ary k-tuple sequence in general, where $u_n = (u_n^{(1)}, u_n^{(2)}, \ldots, u_n^{(k)})$. Let a basis of $GF(p^k)$ over $GF(p)$ be fixed, and the minimal polynomial $C(x)$ of U over $GF(p^k)$ using BM algorithm be determined to be of the form $\prod_{i \in I}(f_i(x))^{m_i}$, where $f_i(x)$ are irreducible polynomials of degree d_i over $GF(p)$, m_i are positive integers, and I is some index set. Then, $C(x)$ is a uniquely determined minimal polynomial of U over $GF(p^k)$ regardless of the choice of basis, if k and d_i are relatively prime for all $i \in I$. Furthermore, $C(x)$ is the unique minimal polynomial of U over $GF(p^m)$ for any $m \geq k$ using any basis such that m and d_i are relatively prime for all $i \in I$.*

Proof. Suppose $C'(x)$ is the corresponding minimal polynomial of U now over $GF(p^k)$ with respect to another basis. Then, $C'(x)$ must divide $C(x)$ over $GF(p^k)$ by Lemma 1(i), since $C(x)$ also generates U over $GF(p^k)$ with respect to another basis. Using the same arguments as in the proof of Theorem 1, we have a contradiction unless $C'(x) = C(x)$. □

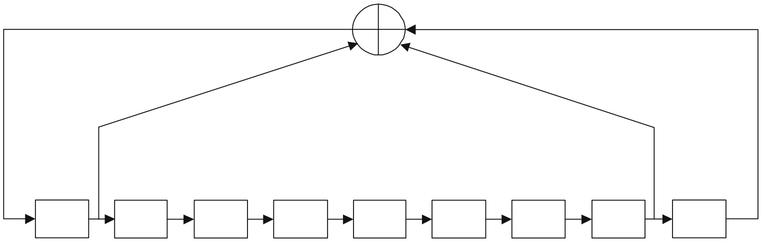

Fig. 2. The shortest LFSR generating S and three T's of Example 3

3 Frequency/Time Hopping Sequence Generators for Large Linear Complexities

We pay attention to the construction of S over $GF(p)$ with large LC. When $S^{(i)} = \{s_n^{(i)} | n = 0, 1, 2, ...\}$, $i = 1, 2, \ldots, N$, are sequences over $GF(p)$, a termwise product sequence $S = \prod_{i=1}^{N} S^{(i)} = \{s_n | n = 0, 1, 2, ...\}$ over $GF(p)$ based on $S^{(i)},\ i = 1, 2, \ldots, N$, is defined as

$$s_n = \prod_{i=1}^{N} s_n^{(i)} \ \ (\textit{multiplication in } GF(p)) \ . \tag{3}$$

It is well-known that the LC of a termwise product sequence defined above is at most the product of the LCs of multiplied sequences.

Lemma 2. [5] *Let $Y = \{y_n\}$ and $Z = \{z_n\}$ be sequences over $GF(p)$ with some irreducible minimal polynomials $C_Y(x)$ and $C_Z(x)$ of degree l and m, respectively. If l and m are relatively prime, then $S = YZ$ over $GF(p)$ as defined in* (3) *has the irreducible minimal polynomial of degree $l \times m$.*

Corollary 2. *Let $S = YZ$ be a sequence over $GF(p)$ as constructed in* Lemma 2. *If $l \times m$ and k are relatively prime, then $T(k, S)$ over $GF(p^k)$ as defined in* (1) *has the same minimal polynomial as S.*

Proof. It is obvious by Lemma 2 and Theorem 1. □

Example 4. The irreducible minimal polynomial of Y and Z over $GF(2)$ is $C_Y(x) = x^4+x+1$ and $C_Z(x) = x^3+x+1$, respectively. The irreducible minimal polynomial of $S = YZ$ over $GF(2)$ as defined in (3) is $x^{12}+x^9+x^5+x^4+x^3+x+1$ whose degree is $12 = 3 \times 4$ because $gcd(3, 4) = 1$. $T(k, S)$ over $GF(2^k)$ as defined in (1) has the same minimal polynomial as S for k relatively prime to 12.

We consider the general case of Lemma 2, that is the case of termwise product sequences based on arbitrary number of sequences with general minimal polynomials composed of irreducible factors.

Lemma 3. [5] *Let $S^{(i)},\ i = 1, 2, \ldots, N$, be sequence over $GF(p)$ with a minimal polynomial $C_{S^{(i)}}(x)$ of degree $M^{(i)}$, that divides $x^{p^{m^{(i)}}-1} - 1$ for some $m^{(i)}$ and contains no linear factor. For any pair of distinct roots, α and β, of $C_{S^{(i)}}(x),\ i = 1, 2, \ldots, N$, $\alpha\beta^{-1} \notin GF(p)$. If $m^{(i)},\ i = 1, 2, \ldots, N$, are pairwise relatively prime, then $S = \prod_{i=1}^{N} S^{(i)}$ over $GF(p)$ as defined in* (3) *has the minimal polynomial of degree $M = \prod_{i=1}^{N} M^{(i)}$.*

The above lemma characterizes those LFSRs whose termwise product sequence has the maximum possible LC, that is the product of the LCs of multiplied sequences. We note that $\alpha\beta^{-1}$ never be in $GF(p)$ for any pair of distinct roots, α and β, of a minimal polynomial $C_{S^{(i)}}(x),\ i = 1, 2, \ldots, N$, for the case of $p = 2$.

Corollary 3. *Let* $S = \prod_{i=1}^{N} S^{(i)}$ *be a sequence over* $GF(p)$ *as constructed in* Lemma 3*. If* $\prod_{i=1}^{N} m^{(i)}$ *and* k *are relatively prime, then* $T(k,S)$ *over* $GF(p^k)$ *as defined in* (1) *has the same minimal polynomial as* S*.*

Proof. Let $C_S(x)$ be the minimal polynomial of S, then the degree of any irreducible factor of $C_S(x)$ is of the form $\prod_{i=1}^{N} r^{(i)}$, where $r^{(i)}|m^{(i)}$, by Lemma 3 and Theorem 1 completes the proof. □

Example 5. The minimal polynomial of Y over $GF(2)$ is $C_Y(x) = x^3 + x^2 + 1$ that divides $x^{2^3-1} - 1$ and $C_Y(1) = 1$. The minimal polynomial of Z over $GF(2)$ is $C_Z(x) = x^6 + x^3 + x^2 + x + 1$ that divides $x^{2^4-1} - 1$ and $C_Z(1) = 1$. The minimal polynomial of $S = YZ$ over $GF(2)$ as defined in (3) is $x^{18} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^6 + x^4 + x^3 + x^2 + 1$ whose degree is $18 = 3 \times 6$ because $gcd(3,4) = 1$. $T(k,S)$ over $GF(2^k)$ as defined in (1) have the same minimal polynomial as S for k relatively prime to 3×4.

Now, we consider the FH/TH sequence generator composed of a combinatorial function generator [7] and k buffers shown in Fig. 3. Let a combinatorial function sequence, S, over $GF(p)$ by a combinatorial function, f, (that would make S have large LC) be represented in the algebraic normal form given by

$$\begin{aligned} s_n &= f(s_n^{(1)}, s_n^{(2)}, \ldots, s_n^{(N)}) \\ &= a_0 + \sum_{i=1}^{N} a_i s_n^{(i)} + \sum_{i=1}^{N} \sum_{j=i+1}^{N} a_{ij} s_n^{(i)} s_n^{(j)} + \ldots + a_{12\ldots N} s_n^{(1)} s_n^{(2)} \ldots s_n^{(N)}, \end{aligned} \tag{4}$$

where $S^{(i)}$, $i = 1, 2, \ldots, N$, are sequences over $GF(p)$ and the coefficients of f are elements of $GF(p)$. We note that the algebraic normal form as defined in (4) cannot represent all combinatorial functions. The maximum possible LC of a combinatorial function sequence, S, for the given algebraic normal form is given by

$$M = F(M^{(1)}, M^{(2)}, \ldots, M^{(N)}), \tag{5}$$

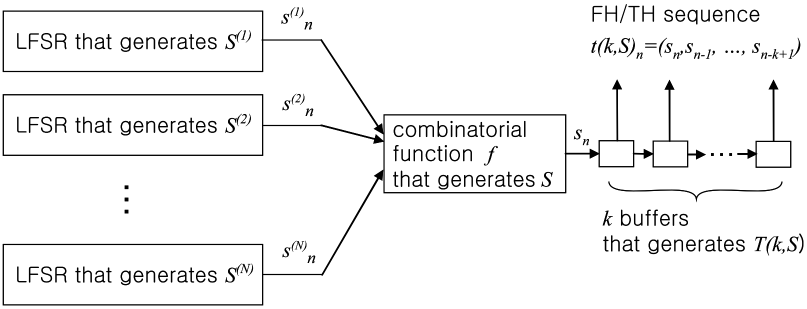
LFSR that generates $S^{(1)}$
LFSR that generates $S^{(2)}$
⋮
LFSR that generates $S^{(N)}$
$s^{(1)}{}_n$
$s^{(2)}{}_n$
$s^{(N)}{}_n$
combinatorial function f that generates S
s_n
FH/TH sequence
$t(k,S)_n=(s_n, s_{n-1}, \ldots, s_{n-k+1})$
k buffers that generates $T(k,S)$

Fig. 3. Frequency/Time hopping sequence generators for large linear complexities

where $F(M^{(1)}, M^{(2)}, \dots, M^{(N)})$ is defined as (4) with a coefficient being 0 if it is 0 or 1 otherwise and $M^{(i)}$ is the LC of $S^{(i)}$, $i = 1, 2, \dots, N$, and operations of F are over the integers.

R. A. Rueppel characterize those LFSRs such that a combinatorial function sequence, S, has the maximum possible LC for the given algebraic normal form [5]. In the previous section, we characterize those p-ary sequences, S, whose k-tuple versions, $T(k, S)$, now over $GF(p^k)$ have the maximum possible LCs. In this view point, we focus on the relations between the above two characterizations. We are able to characterize those LFSRs such that a resulting k-tuple sequence (an FH/TH sequence), $T(k, S)$, has the maximum possible LC, M as defined in (5). That is, we are able to construct FH/TH sequences with large LCs by the generators shown in Fig. 3.

Lemma 4. [5] *Let $S^{(i)}$, $i = 1, 2, \dots, N$, be sequences over $GF(p)$ with minimal polynomials $C_{S^{(i)}}(x)$ of degree $M^{(i)}$, that divide $x^{p^{m^{(i)}}-1} - 1$ for some $m^{(i)}$ and contain no linear factor. For any pair of distinct roots, α and β, of $C_{S^{(i)}}(x)$, $i = 1, 2, \dots, N$, $\alpha\beta^{-1} \notin GF(p)$. If $m^{(i)}$, $i = 1, 2, \dots, N$ are pairwise relatively prime, then S over $GF(p)$ as defined in* (4) *has the minimal polynomial of degree M as defined in* (5) *for the given algebraic normal form, f.*

Corollary 4. *Let S be a sequence over $GF(p)$ as constructed in* Lemma 4. *If $\prod_{i=1}^{N} m^{(i)}$ and k are relatively prime, then $T(k, S)$ over $GF(p^k)$ as defined in* (1) *has the same minimal polynomial as S.*

Proof. Let $C_S(x)$ be the minimal polynomial of S, then the degree of any irreducible factor of $C_S(x)$ is of the form $\prod_{i=1}^{N} r^{(i)}$, where $r^{(i)} | m^{(i)}$, by Lemma 4 and Theorem 1 completes the proof. □

Example 6. The minimal polynomial of X, Y, Z over $GF(2)$ is $C_X(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, $C_Y(x) = x^6 + x^3 + x^2 + x + 1$, $C_Z(x) = x^{10} + x^8 + x^7 + x^5 + x^3 + x^2 + 1$ that divides $x^{2^3-1} - 1$, $x^{2^4-1} - 1$, $x^{2^5-1} - 1$ respectively and contains no linear factor. The minimal polynomial of S over $GF(2)$ defined by $s_n = f(x_n, y_n, z_n) = 1 + x_n + y_n + z_n + x_n y_n + y_n z_n + z_n x_n + x_n y_n z_n$ as (4) is of degree $539 = M(6, 6, 10) = 1 + 6 + 6 + 10 + 6 \cdot 6 + 6 \cdot 10 + 10 \cdot 6 + 6 \cdot 6 \cdot 10$ as defined in (5) because 3, 4, and 5 are pairwise relatively prime. $T(k, S)$ over $GF(2^k)$ as defined in (1) have the same minimal polynomial as S for k relatively prime to $3 \cdot 4 \cdot 5$. For example, $T(7, S)$ is a 128-ary FH/TH sequence whose LC is 539.

We believe that FH/TH sequences as constructed in Corollary 4 must be a good candidates of FH/TH patterns in a peer-to-peer FH/TH spread spectrum communication system for the following good reasons: (i) with "large" LC, and (ii) over "large" alphabet, but (iii) with "little" increase in the hardware complexity.

4 Concluding Remarks

We believe that the finite field of characteristic 2 would be a good choice for the algebraic structure of FH/TH sequences because the computations over characteristic 2 are most efficiently implemented as hardware systems and the usual practice follows this idea.

We have tried several other options but failed to extract any further reasonable behavior of non-binary FH/TH sequences over $GF(p^k)$ whose minimal polynomial and therefore, LC are uniquely determined regardless of the choice of basis other than those given in Theorem 1. Theorem 2 is slightly more general in that the p-ary k-tuple FH/TH sequences are not necessarily constructed as a k-tuple version of a p-ary sequence.

We note that Corollary 4 characterize those FH/TH sequence generators such that a combinatorial function sequence, S, and a resulting k-tuple sequence (an FH/TH sequence), $T(k, S)$, has the maximum possible LC for any given algebraic normal form, f, to resist the only BM attack. So, it is proper that we use the algebraic normal form, f, that has desired cryptographic properties such as correlation immunity, resiliency, nonlinearity, and propagation [7][11][12][13] to resist other attacks than the BM attack.

We note that the sequence terms of $T(k, S)$ are highly correlated with each other because t_n is the right shifted version of t_{n-1} with the only new leftmost component. This correlation between consecutive terms must be a vulnerable point to some other attacks. But, Theorem 1 and all corollaries in this paper also apply equally well to $T(k, S)$ defined by

$$t_n = (s_{n-\sigma(0)}, s_{n-\sigma(1)}, \dots, s_{n-\sigma(k-1)}), \tag{6}$$

where σ is any permutation on $\{0, 1, \dots, k-1\}$. A further generalization is also possible by using any integers instead of $\sigma(i)$ for each i. Therefore, we are able to solve the correlation problem between consecutive terms by the above method.

References

1. S. W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, Laguna Hills, CA 92654, 1982.
2. M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications Handbook*, Revised Edition, McGraw-Hill, Inc., 1994.
3. J. L. Massey, "Shift-Register Synthesis and BCH decoding," *IEEE Transactions on Information Theory*, vol. IT-15, no. 1, pp. 122-127, Jan. 1969.
4. R. Lidl and H. Niederreiter, *Finite Fields*, Second Edition, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, 1997.
5. R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986.
6. A. H. Chan, R. A. Games, and E. L. Key, "On the Complexities of de Bruijn Sequences," *Journal of Combinatorial Theory*, Series A 33, pp. 233-246, 1982.
7. S. W. Golomb and G. Gong, *Signal Design for Good Correlation for Wireless Communication, Cryptography, and Radar*, Cambridge University Press, 2005.
8. W. J. Park and J. J. Komo, "Relationships Between m-Sequences over $GF(q)$ and $GF(q^m)$," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 183-186, Jan. 1989.
9. G. Gong and G. Z. Xiao, "Synthesis and Uniqueness of m-Sequences over $GF(q^n)$ as n-Phase Sequences over $GF(q)$," *IEEE Transactions on Communications*, vol. 42, no. 8, pp. 2501-2505, Aug. 1994.

10. W. Meidl, “Discrete Fourier Transform, Joint Linear Complexity and Generalized Joint Linear Complexity of Multisequences,” *Lecture Notes in Computer Science*, vol. 3486, pp. 101-112, Mar. 2005.
11. T. Siegenthaler, “Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications,” *IEEE Transactions on Information Theory*, vol. IT-30, no. 5, pp. 776-780, Sep. 1984.
12. W. Meier and O. Staffelbach, “Nonlinearity Criteria for Cryptographic Functions,” *Lecture Notes in Computer Science*, vol. 434, pp. 549-562, 1990.
13. B. Preneel, W. V. Leekwijck, and L. V. Linden “Propagation Characteristics of Boolean Functions,” *Lecture Notes in Computer Science*, vol. 473, pp. 161-173, 1990.