# 임의의 심볼 집합 상의 수열의 선형복잡도와 $GF(p)$상의 특성다항식을 갖는 $GF(p^k)$상의 수열 생성에 관한 연구

준회원 홍 윤 표*, 정회원 은 유 창*, 김 정 헌**, 종신회원 송 홍 엽*

# Linear Complexities of Sequences over Unknown Symbol Sets and Constructions of Sequences over $GF(p^k)$ whose Characteristic Polynomials are over $GF(p)$

Yun-Pyo Hong*, Yu-Chang Eun*, Jeong-Heon Kim**,
Hong-Yeop Song* *Regular Members*

요 약

본 논문에서는 임의의 심볼 집합 상의 수열의 선형복잡도를 정의한다. 또한 본 논문에서는 기저의 선택과 상관없이 자신의 $GF(p^k)$ 상의 $k$-tuple 수열이 자신과 같은 특성다항식을 갖는 $p$-ary 수열의 특성을 밝히며 이는 결과적으로 $GF(p)$ 상의 특성다항식을 갖는 $p^k$-ary 수열의 생성을 가능하게 한다. 마지막으로 심볼이 $GF(p)$ 상의 $k$-tuple로 표현될 때 기저의 선택과 무관하게 유일한 특성다항식을 갖는 $p^k$-ary 수열의 특성을 밝힌다.

**key Words** : Linear Complexity, Frequency-Hopping Patterns, Linear Feedback Shift Register, $p^k$-ary sequences

ABSTRACT

We propose an appropriate approach of defining the linear complexities (LC) of sequences over unknown symbol set. We are able to characterize those $p$-ary sequences whose $k$-tuple versions now over $GF(p^k)$ have the same characteristic polynomial as the original with respect to any basis. This leads to a construction of $p^k$-ary sequences whose characteristic polynomial is essentially over $GF(p)$. In addition, we can characterize those $p^k$-ary sequences whose characteristic polynomials are uniquely determined when symbols are represented as $k$-tuples over $GF(p)$ with respect to any basis.

## I. Introduction

In a peer-to-peer frequency hopping (FH) spread spectrum communication system, an interceptor who can observe full frequency band may try to synthesize the entire FH pattern from some frequency slots successively observed. Assume that he observes a frequency-hopping pattern (a FH sequence) $S=\{f_1 f_4 f_5 f_3 f_2 f_6 \cdots\}$ with 6 frequency slots. Then, one must decide the following two choices to synthesize the linear feedback shift register (LFSR) [2], [6] that can generate the next slots of the FH pattern. First, he/she must choose an underlying algebraic

* 연세대학교 대학원 전기전자공학과 (yp.hong@coding.yonsei.ac.kr), ** 삼성전자 (jeongheon.kim@samsung.com)
논문번호 : 030151-0407, 접수일자 : 2003년 4월 1일
※본 연구는 2000년 한국학술진흥재단 선도연구자 지원과제(2000-041-E00214)의 지원으로 수행되었습니다.

structure of the symbols of $S$. The symbols of $S$ can be regarded as elements of a finite field or an integer residue ring, of size at least 6. Second, he/she must choose a correspondence between the elements of the algebraic structure and the symbols of $S$. If he chooses $Z_6$ as an underlying algebraic structure, there will be 6! correspondences that he can choose. On the other hand, if he chooses $GF(8)$, there will be $8!/2!$ correspondences. After that, Berlekamp-Massey (BM) algorithm [4] can be used to synthesize the characteristic polynomial of $S$ over a finite field, and so can Reeds-Sloane (RS) algorithm [5] be used over an integer residue ring.

Let $L$ be the linear complexity of an FH pattern with specified algebraic structure and symbol correspondence. When the interceptor observes successive $2L$ frequency slots, and the choices are matched, then he can successfully synthesize the next FH slots forever as far as FH patterns are used in the same manner as the beginning. It is true in general, therefore, from the view point of system designers, that the FH pattern should be changed before $2L$ slots are used in order not to be tracked by others, and that the linear complexity of FH patterns should be as large as possible, with whatever choices on the underlying algebraic structures and symbol correspondence might be assumed by others.

Section II illustrates the fact that the linear complexity of a sequence over arbitrary symbols may vary according to the above-mentioned two choices. This leads to a way to define the linear complexity of sequences over arbitrary symbols.

In Section III, we discuss a construction of sequences over $GF(p^k)$ by taking successive $k$-tuples of a given sequence over $GF(p)$. Here, one concern is the choice of basis when we lift up every $k$-tuple over $GF(p)$ to $GF(p^k)$. Since the change of basis corresponds to a symbol permutation, the resulting sequences over $GF(p^k)$ may well have different characteristic polynomials and different complexities according to the choice of basis.

We are able to characterize in also Section III those $p$-ary sequences whose $k$-tuple versions now over $GF(p^k)$ have the same characteristic polynomial as the original with respect to any basis. This leads to a construction of $p^k$-ary sequences whose characteristic polynomial is essentially over $GF(p)$. In addition, we can characterize those $p^k$-ary sequences whose characteristic polynomials are uniquely determined when symbols are represented as $k$-tuples over $GF(p)$ with repect to any basis. In particular, we show that a binary sequence of period $2^r$ (including de Bruijn sequences) and any of its $k$-tuple versions over $GF(2^k)$ for any positive integer $k$ have the same characteristic polynomial that is over $GF(2)$. We also show that the binary $m$-sequence of period $2^r-1$ and any of its $k$-tuple versions over $GF(2^k)$ for $k$ relatively prime to $r$ have the same characteristic polynomial that is over $GF(2)$.

## II. Linear complexity of sequences over unknown symbol sets

Let $S=\{s_n\}$, where $n=1,2,\cdots$, be a sequence over an unknown symbol set of size $m$, whose linear complexity (and possibly, characteristic polynomial) is to be determined (and synthesized, respectively). Then the LC of $S$ may vary according to the following choices: (i) an underlying algebraic structure of the symbols of the sequence (ii) a correspondence between the elements of the alge-

braic structure and the symbols.

When we determine the LC of $S$ over $Z_m$, we first choose an ordering of elements of symbols of the sequence, and then correspond each term, $s_n$, to an element of $Z_m$ according to this ordering. This completes both choices, and RS algorithm can now be applied.

When we determine it over $GF(p^k)$, where $p$ is a prime and $p^k \geq m$, we need to set up the correspondence between the symbols and the elements of $GF(p^k)$. To this end, we first correspond each term of $S$ to an element of $Z_m$ as before, and then represent each non-negative integer as a $p$-ary $k$-tuple as

$$s_n \mapsto (v_1, v_2, \cdots, v_k) \quad so\ that \quad s_n = \sum_{i=1}^{k} v_i p^{k-i}. \tag{1}$$

Then, we interpret each $k$-tuple with respect to a fixed basis $\underline{\alpha} = (\alpha_1, \alpha_2, \cdots, \alpha_k)$ of $GF(p^k)$ over $GF(p)$. One choice could be so called a polynomial basis of the form

$$(1,\ \alpha,\ \alpha^2, \cdots,\ \alpha^{k-1}), \tag{2}$$

where $\alpha \in GF(p^k)$ is a primitive element. This completes the symbol correspondence. In this paper, we will primarily use this method given in Eq. (1) and any fixed basis for a correspondence between the set of non-negative integers from 0 to $m-1$. Selecting a polynomial basis would correspond to the choice of a primitive element $\alpha$, or equivalently, a primitive polynomial of degree $k$ over $GF(p)$.

When $k=1$, it is well known that both BM and RS algorithms produces the same result. When $k \geq 2$, BM algorithm with a choice of a basis must be used to determine the LC over $GF(p^k)$.

Note that selecting a different basis in the above discussion corresponds to taking a symbol permutation and using the same basis. Let $A$ be a $k \times k$ matrix over $GF(p^k)$ with non-zero determinant which transforms one basis into another. That is, we let $\underline{\alpha}^T = A\,\underline{\beta}^T$ for two basis $\underline{\alpha}$ and $\underline{\beta}$. Then a $k$-tuple $v = (v_1, \cdots, v_k)$ over $GF(p)$ can be regarded as an element of $GF(p^k)$ in two ways. Since $v\,\underline{\alpha}^T = vA\,\underline{\beta}$, lifting up $k$-tuples $v$ to $GF(p^k)$ with respect to $\underline{\alpha}$ corresponds to lifting up $vA$ (a permuted version by $A$) to $GF(p^k)$ with respect to $\underline{\beta}$.

***Example 1***: A sequence $S$ with period 64 is given by

0 2 2 1 2 1 2 2 0 1 1 1 1 2 2 0 0 1 2 1 1 2 0 2 2
1 1 2 0 0 0 0 1 0 1 0 1 1 0 1 1 1 0 2 0 0 0 1 0 0
1 0 2 2 1 2 0 0 2 2 0 0 1 2 ...

Table 1 shows the LC of $S$ assuming various algebraic structures of the symbols. ■

Table 1. The LC of $S$ of Example 1 over various algebraic structures.

| Over | $GF(3)$ | $GF(4)$ | $GF(5)$ | $Z_6$ | $GF(7)$ |
|---|---|---|---|---|---|
| LC | 60 | 64 | 61 | 63 | 64 |

***Example 2***: A sequence $S$ with period 8 is given by

0 1 3 7 6 5 2 4 ....

Assuming that $S$ is over $GF(8)$, we have applied BM algorithm to all the 8! symbol-permuted versions of $S$. Similarly, over $Z_8$, we have applied RS algorithm, and the results are summarized in Table 2. We note that, over $Z_8$, the LC can be as small as 2 for some symbol permutations. In fact, a sequence with LC=2 (which is a symbol-permuted version of $S$ over $Z_8$) turned out to be

7 6 1 0 3 2 5 4 .... ■

Table 2. The distribution of the LC of $S$ of Example 2.

| LC over $GF(8)$ | 2 | 3 | 4 | 5 | 6 | 7 | total |
|---|---|---|---|---|---|---|---|
| No. of sequences | 0 | 0 | 0 | 2688 | 5376 | 32256 | 8! |

| LC over $Z_8$ | 2 | 3 | 4 | 5 | 6 | 7 | total |
|---|---|---|---|---|---|---|---|
| No. of sequences | 128 | 256 | 768 | 5888 | 14848 | 18432 | 8! |

***Example 3***: An 8-ary sequence $S$ with period 63 is given by

1 3 6 4 1 4 6 6 2 0 1 1 1 3 1 3 3 6 3 4 7 4
6 1 4 6 5 4 6 7 7 6 3 2 5 0 3 3 3 6 7 3 2 5
1 0 5 7 5 4 3 4 6 5 5 3 3 5 1 2 4 3 6 ....

Each $s_n$ is represented as a binary 3-tuple as defined in Eq. (1), and lifted up to $GF(8)$ using only the polynomial basis as given in Eq. (2) with two different primitive elements. It turned out that the LC with $x^3+x^2+1$ is 59 and that with $x^3+x+1$ is 61. ■

***Example 4***: For a sequence over two-symbol alphabet, the LC based on BM algorithm may be changed by $\pm 1$ according to 2 different correspondences of the symbols with elements of $GF(2)$. Recall that the characteristic polynomial of the sequence would have (or not have) the factor $x+1$ according to the interpretation of 0 and 1 as they are (or as switched, respectively). ■

From all these observations, we see that the main concerns are the operations (addition and multiplication) of the symbols that are used in the LFSR. Fixing these two operations over the symbols is equivalent to fixing an algebraic structure with two operations and also a symbol correspondence.

***Definition 5***: The linear complexity (LC) of a sequence $S$ over an unknown symbol set is the minimum LC of $S$ over all possible algebraic structures and the symbol correspondences. ■

## Ⅲ. Construction of sequences over $GF(p^k)$ whose characteristic polynomial is over $GF(p)$

Let $S=\{s_n\}$, where $n=1,2,\cdots$, be a sequence over $GF(p)$ where $p$ is a prime, and let $k$ be a positive integer. Define a new sequence $T(k,S)=\{t_n\}$, where $n=1,2,\cdots$, from $S$ by regarding $k$ consecutive terms of $S$ as a $p$-ary $k$-tuple, $t_n$, as follows:

$$t_n=(s_n, s_{n+1}, \cdots, s_{n+k-1}). \quad (3)$$

Then these $p$-ary $k$-tuples are lifted up to $GF(p^k)$ with respect to some but fixed basis. One simple choice is the polynomial basis of $GF(p^k)$ as given in Eq. (2), but we will not stick to it.

***Proposition 6***: The LFSR that generates a sequence $S=\{s_n\}$ over $GF(p)$ also generates $T(k,S)$ over $GF(p^k)$ as defined in Eq. (3) regardless of the choice of basis. The converse holds provided that the connection polynomial that generates $T$ over $GF(p^k)$ is essentially over $GF(p)$.

***Proof***: With $c_i\,(i=1,2,\cdots,L)$ being constants over $GF(p)$, the first part is easily observed by the fact that the linear recurrence of $S$ over $GF(p)$ given by

$$s_n=\sum_{i=1}^{L} c_i s_{n-i}$$

directly applies to the same linear recurrence relation of $T(k,S)$ over $GF(p^k)$ where

$$(s_n, s_{n+1}, \cdots, s_{n+k-1})=\sum_{i=1}^{L} c_i (s_{n-i}, s_{n+1-i}, \cdots, s_{n+k-1-i}).$$

Here, the LFSR operations are only the vector addition and scalar multiplication of $GF(p^k)$ over $GF(p)$, and hence the choice of basis has nothing to do with the LFSR operations for $T$ over $GF(p^k)$. Conversely, the characteristic polynomial for $T$ should be

over $GF(p)$ for the choice of basis not to affect the LFSR operations. ■

***Example 7***: 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 ....

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

$T(3, S)$ = {001 011 111 110 102 021 211 112 121 210 ...},

$T(4, S)$ = {0011 0111 1110 1102 1021 0211 2112 1121 1210 2101 ...}.

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

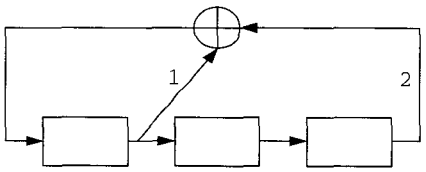



Fig. 1. The LFSR generating $S$ and $T$'s of Example 7.

Proposition 6 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 $GF(p)$. 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.

***Example 8***: (a) A binary sequence $S_1$ with period 63 is given by

1100100000111111101010010010011010101110110110111010011111110010....

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 Eq. (2). (b) A binary sequence $S_2$ with period 63 is given by

0101111111001100000110111111010100111111000110011101001010010 11....

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

***Proposition 9***: [3] The characteristic polynomial of a sequence over $GF(q)$ divides any connection polynomial of the LFSR that generates the sequence over $GF(q)$. Therefore, it is uniquely determined up to the multiplication by a constant.

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 characteristic polynomial as $S$ and hence it is over $GF(p)$.

***Theorem 10 (Main Theorem)***: Let the characteristic 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 Eq. (3) with respect to some but fixed basis for $k \geq 1$. Then, the shortest LFSR that generates $S$ is also the shortest LFSR that generates $T(k, S)$ over $GF(p^k)$, if $k$ and $d_i$ are relatively prime for all $i \in I$. Furthermore, it is also the shortest LFSR of $T(k, S)$ over $GF(p^m)$ for any $m \geq k$ such that $m$ and $d_i$ are relatively prime for all $i \in I$.

***Proof***: We know that the LFSR with

$C(x)$ also generate $T(k, S)$ over $GF(p^k)$ by Prop. 6. We now claim that $C(x)$ is the least degree connection polynomial for $T(k, S)$ over $GF(p^k)$. Suppose, on the contrary that the degree of $C(x)$ is not the least for $T(k, S)$. Then the shortest LFSR with connection polynomial $C'(x)$ exists and $C'(x)$ divides $C(x) = \prod_{i \in I}(f_i(x))^{m_i}$ by Prop. 9. We note that the necessary and sufficient condition for $f_i(x)$ over $GF(p^k)$ to be irreducible is that $k$ and $d_i$ are relatively prime [3, Corollary 3.47, page 107]. Therefore, $C'(x) = \prod_{i \in I}(f_i(x))^{s_i}$, where $s_i$ is a non-negative integer, $0 \le s_i \le m_i$ for all $i \in I$, and $\sum_{i \in I} s_i < \sum_{i \in I} m_i$. On the other hand, the polynomial $C'(x) = \prod_{i \in I}(f_i(x))^{s_i}$ is over $GF(p)$, and Prop. 6 (the converse part) implies that $C'(x)$ is also a connection polynomial for $S$ over $GF(p)$ which is a desired contradiction.

Furthermore, if we regard each term of $T(k, S)$ over $GF(p^m)$ for any $m \ge k$ 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 by the following example.

***Example 11***: A binary $m$-sequence $S$ with characteristic polynomial $C(x) = x^4 + x + 1$, is given by

1 1 1 1 0 1 0 0 1 0 0 1 0 0 0 ....

The 4-ary sequence $T(2, S)$ has the same characteristic polynomial as $S$ with respect to the polynomial basis in Eq. (2) even though the degree of $C(x)$ and $k = 2$ are not relatively prime. ∎

***Corollary 12 (Main Corollary)***: The linear complexity of $T(k, S)$ over $GF(p^k)$ as constructed in Theorem 10 is fixed regardless of the choice of basis when symbols are represented as $k$-tuples over $GF(p)$. Furthermore, so is the LC of $T(k, S)$ over $GF(p^m)$ for $m \ge k$, if $m$ and $d_i$ are relatively prime for all $i \in I$.

***Corollary 13***: 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 Eq. (3) 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 $m \ge k$ which is relatively prime to $r$.

For binary sequences, besides the case of $m$-sequences, we would like to pick up one additional case to which Theorem 10 applies.

***Corollary 14***: 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 Eq. (3) for any positive integer $k$. Furthermore, it is also the shortest LFSR of $T(k, S)$ over $GF(2^m)$ for any $m \ge k$.

***Proof***: We note that the characteristic polynomial $C(x)$ of a binary sequence $S$ with period $2^r$ is of the form $(1+x)^\tau$ for some positive integer $\tau$ [1]. ∎

***Example 15***: 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 ....

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

000 000 001 010 101 011 111 111 111 111 110 101 010 ....

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

0000 0000 0001 0010 0101 0011 0111 0111

0111 0111 0110 0101 0010 ....

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

0000 0001 0010 0101 1011 0111 1111 1111 1111 1110 1101 1010 0100 ....

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

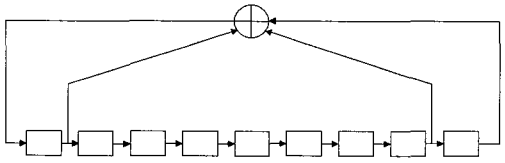


Fig. 2. The shortest LFSR generating $S$ and three $T$'s of Example 15.

***Example 16***: A ternary sequence $S$ in Ex. 7 is indeed an $m$-sequence with the characteristic polynomial $x^3+2x+1$ of degree 3. Therefore, the ternary 4-tuple sequence $T(4, S)$ in the example has the LFSR shown in Fig. 1 as the shortest LFSR over $GF(3^4)$. Theorem 10 implies that so does $T(k, S)$ over $GF(3^k)$ for any $k$ not divisible by 3. ■

***Remark 17***: Some interesting discussions are given in [7], [8] 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 characteristic polynomial as the component $p$-ary $m$-sequences. In [8], for example, if the characteristic polynomial $C(x)$ of the component $p$-ary $m$-sequence over $GF(p)$ has degree $kn$, then the characteristic polynomial of resulting $p^k$-ary $m$-sequence over $GF(p^k)$ has degree $n$, and in fact, it must be a factor of $C(x)$ over $GF(p^k)$. ■

Now, let $U=\{u_n\}$, where $n=1,2,\cdots$, be a $p$-ary $k$-tuple sequence in general. In order to determine its characteristic polynomial 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 18***: Let $U=\{u_n\}$, where $n=1,2,\cdots$, be a $p$-ary $k$-tuple sequence in general, where $u_n=(u_{n1}, u_{n2}, \cdots, u_{nk})$. Let a basis of $GF(p^k)$ over $GF(p)$ be fixed, and the characteristic 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 characteristic 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 characteristic polynomial of $U(p, k)$ 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 characteristic polynomial of $U$ now over $GF(p^k)$ with respect to another basis. Then, $C'(x)$ must divide $C(x)=\prod_{i\in I}(f_i(x))^{m_i}$ by Prop. 9 over $GF(p^k)$, since $C(x)$ also generates $U$ over $GF(p^k)$ with respect to another basis. This happens because the two operations, addition and multiplication, of the LFSR over $GF(p^k)$ corresponding to $C(x)$ are independent of the chosen basis since $C(x)$ is essentially over $GF(p)$. That is,

they are essentially the operations over $GF(p)$. Therefore, $C'(x)$ must divide $C(x)$ over $GF(p)$, and using the same arguments as in the proof of Theorem 10, we have a contradiction unless $C'(x) = C(x)$. ∎

## Ⅳ. Concluding Remarks

An observed FH pattern by an interceptor must be a non-binary sequence over some unknown symbol set, and this causes a problem of determining the LC of the pattern since some specific operations of the LFSR must be provided. Therefore, it is reasonable that the interceptor will use such choice that leads to the least LC over all possibilities, and the system designer on the other hand must consider the LC of the FH pattern over various algebraic structures and the symbol correspondences including the true choice of the system.

In reality, however, we believe that a good choice would be the smallest size finite field of characteristic 2 that can just cover all the symbols of the sequence, 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 sequences over $GF(p^k)$ whose characteristic polynomial is uniquely determined regardless of the choice of basis other than those given in Theorem 10 of Section III. Theorem 18 is slightly more general in that the $p$-ary $k$-tuple sequences are not necessarily constructed as a $k$-tuple version of a $p$-ary sequence.

We note that Theorem 10 and its corollaries also apply equally well to $T(k, S)$ defined by

$$t_n = (s_{n+\sigma(1)}, s_{n+\sigma(2)}, \cdots, s_{n+\sigma(k)}), \quad (4)$$

where $\sigma$ is any permutation on $\{1, 2, \cdots, k\}$. A further generalization is also possible by using any non-negative integers instead of $\sigma(i)$ for each $i$.

## REFERENCES


[1] A. H. Chan, R. A. Games, and E. L. Key, "On the Complexity of de Bruijn Sequences," J. Comb. Theory, Ser. A, vol. 33, pp. 233-246, Nov. 1972.

[2] S. W. Golomb, Shift Register Sequences, Revised Edition, Aegean Park Press, Laguna Hills, CA, 1982.

[3] R. Lidl and H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley, Reading, MA, 1983.

[4] J. L. Massey, "Shift-Register Synthesis and BCH decoding," IEEE Trans. Inform. Theory, vol. IT-15, pp. 122-127, Jan. 1969.

[5] J. A. Reeds and N. J. A. Sloane, "Shift Register Synthesis (modulo m)," Siam J. Comp., vol. 14, no. 3, pp. 505-513, Aug. 1985.

[6] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, Spread Spectrum Communications Handbook, Computer Science Press, Rockville, MD, 1985; revised edition, McGraw-Hill, 1994.

[7] W. J. Park, J. J. Komo, "Relationships Between $m$-Sequences over $GF(q)$ and $GF(q^m)$," IEEE Trans. Inform. Theory, vol. 35, no. 1, pp. 183-186, Jan. 1989.

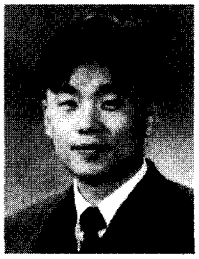
[8] G. Gong, G. Z. Xiao, "Synthesis and Uniqueness of $m$-Sequences over $GF(q^n)$ as $n$-Phase Sequences over $GF(q)$," IEEE Trans. Communications, vol. 42, no. 8, pp. 2501-2505, Aug. 1994.

홍 윤 표(Yun-Pyo Hong) 준회원

2000년 2월 : 연세대학교 전자공학과 졸업 (공학사)
2002년 2월 : 연세대학교 대학원 전기전자공학과 졸업 (공학석사)
2002년 3월~현재 : 연세대학교 대학원 전기전자공학과 박사과정

<주관심분야> Application of PN Sequences to Spread Spectrum and Crypto Systems, Block Codes and Convolutional codes

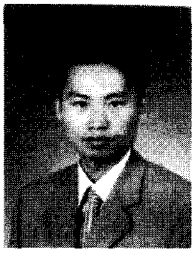
은 유 창(Yu-Chang Eun) 정회원



1998년 2월 : 연세대학교 전자공학과 졸업 (공학사)
2000년 2월 : 연세대학교 대학원 전기전자공학과 졸업 (공학석사)
2000년 3월~현재 : 연세대학교 대학원 전기전자공학과 박사과정

<주관심분야> Application of PN Sequences to Spread Spectrum and Crypto Systems, Block Codes and Convolutional codes

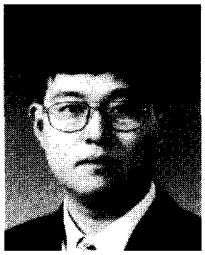
김 정 헌(Jeong-Heon Kim) 정회원



1996년 2월 : 연세대학교 전자공학과 졸업 (공학사)
1998년 2월 : 연세대학교 대학원 전기전자공학과 졸업 (공학석사)
2002년 2월 : 연세대학교 대학원 전기전자공학과 졸업 (공학박사)
2002년 3월~현재 : 삼성전자 선임연구원

<주관심분야> Application of PN Sequences to Spread Spectrum and Crypto Systems, Block Codes and Convolutional codes

송 홍 엽(Hong-Yeop Song) 종신회원



1984년 2월 : 연세대학교 전자공학과 졸업 (공학사)
1986년 5월 : USC 대학원 전자공학과 졸업 (공학석사)
1991년 12월 : USC 대학원 전자공학과 졸업 (공학박사)
1992년 ~ 1993년 : Post Doc., USC 전자공학과
1994년~1995년 : Qualcomm Inc., 선임연구원
1995년 9월~현재 : 연세대학교 전기전자공학과 교수

<주관심분야> PN Sequences, Error Correcting Codes, Spread Spectrum Communication Systems, Steam Cipher Systems