通信情報保護論文誌
第9券 第2號 1999. 06

선형 귀환 쉬프트 레지스터의 비선형적 결합에 관한 연구

김 철*

On the non-linear combination of the Linear Feedback Shift Register

Chul Kim*

요 약

본 논문에서는 선형 귀환 쉬프트 레지스터(LFSR)에 의하여 생성되는 수열의 복잡도를 고찰한 후, 이들의 비선형적 결합이 갖는 특성에 대하여 살펴본다. 이 비선형 결합의 구성 단위인 LFSR의 합과 곱을 중심으로 이들이 갖는 이론적인 면을 복잡도 측면에서 고찰한다.

ABSTRACT

We introduce feedback registers and definitions of complexity of a register or a sequence generated by it. In the view point of cryptography, the linear complexity of an ultimately periodic sequence is important because large one gives an enemy infeasible jobs. We state some results about the linear complexity of sum and product of two LFSRs.

I .Introduction

Let us consider sequences of elements of a finite fields. Those may be binary sequences. Shift register generators are used to produce binary sequences for various purposes. These devices are small, inexpensive, and offer a rich variety of sequences. In cryptographic applications, sequences produced by sequence generators should have the following properties:

1. It has the long period.
2. It is unpredictable. For example, it has the large linear complexity.
3. It has good statistical properties.

For the above cryptographical conditions, feedback shift registers are studied. Sequences generated by those may have maximum period or large linear complexity. We will state some results about the linear complexity in Section 5.

* 광운대학교 수학과 암호학 및 정보통신보호 연구실(kimch@daisy.kwangwoon.ac.kr)
※ 이 논문은 1998년도 광운대학교 학술연구비에 의하여 연구되었음.

We consider the linear complexity of functions of ultimately periodic sequences. Thus, we need concepts of feedback shift registers and minimal polynomials. In Section 2, we introduce feedback registers and some concepts on complexity of feedback registers or sequences generated by those. In Section 3, we describe some properties of the minimal polynomials of ultimately periodic sequences. In Section 4, we have results about the least period of sequence. In Section 5, some results about the linear complexity of sum and product of two ultimately periodic sequences are introduced. To avoid stream cipher attack, e.g., Meier-Staffelbach correlation attack, the nonlinear combination of feedback shift registers has to be done under the consideration of its linear complexity. Thus our results are useful to secure the nonlinearly combined stream cipher using the sum and multiplication of feedback shift registers.

2 Feedback Register

Let F_q denote the finite field. A feedback register (or simply register) of length n is a pair (F, g) where $F=(F_1, \cdots, F_n)$ is a function from F_q^n to F_q^n (the state transition function) and g is a function from F_q^n to F_q (the output or feedforward function). An initial loading of a register $F=(F, g)$ is an element $\alpha \in F_q^n$ F, with initial loading α, generates the sequence

$$F(\alpha) = (g(\alpha), g \cdot F(\alpha), g \cdot F^2(\alpha), \cdots).$$

The standard feedforward function) is $g(x_1, \cdots, x_n) = x_1$. A register (F, g) is a feedback shift register with feedforward function g if

$$F(x_1, \cdots, x_n) = (x_2, x_3, \cdots, x_n, f(x_1, \cdots, x_n))$$

for some function f from F_q^n to F_q, which is called the feedback function. A feedback shift register with the standard feedforward function is simply called a feedback shift register. A register is linear (resp., affine) if g and each F_i are linear polynomials (resp., affine polynomials). We introduce two notions of linear complexity.

Definition 2.1 The linear complexity of an ultimately periodic sequence of elements of F_q is the length of the shortest linear feedback shift register (LFSR) generating the sequence. The weak linear complexity of a register is the maximum of the linear complexities of sequences generated by the register.

Definition 2.2 The strong linear complexity of a register is the length of the smallest linear feedback shift register such that the LFSR generates all sequence generated by the register.

The linear complexity of a sequence measures the possibility which a sequence can reproduce by one. But the definitions of weak or strong linear complexity are related with a register itself. Those consider the worst case of linear complexities of sequences generated by a register. Obviously, the strong linear complexity of a register is greater than or equal to its weak linear complexity. For details about the above definitions, see [1].

3. Minimal Polynomial

Every ultimately periodic sequence can be generated by a LFSR. Thus, we will concentr ate on a LFSR. An ultimately periodic sequen ce is characterized by its minimal polynomial.

Now, we define a LFSR and aminimal polyno mial, rigorously.

Through Section 3, 4, 5, we use the following notations. Let F_q be a finite field.

Let L be a positive integer, let

$c_0, \cdots, c_{L-1}, a_0, \cdots, a_{L-1} \in F_q$, and let

$c_L = -1$.

Suppose that $\{a_n\}_{n=0}^{\infty}$ satisfies a linear rec urrence relation

$$a_n = \sum_{i=0}^{L-1} c_i a_{n-L+i} \text{ for } n \geq L$$

and r is the least period of $\{a_n\}$. Note that $\{a_n\}$ is ultimately periodic. We will assume that $\{a_n\}$ is a nonzero sequence. Put

1. $f(x) = x^L - c_{L-1}x^{L-1} - \cdots - c_1 x - c_0 = -\sum_{i=0}^{L} c_i x^i$

(It is called a characteristic polynomial of the linear recurring sequence $\{a_n\}$.),

2. $f^*(x) = x^L f\left(\frac{1}{x}\right) = -\sum_{i=0}^{L} c_i x^{L-i}$

(Note that $\deg(f^*) \leq L$.)

3. $a(x) = a_0 x^{r-1} + a_1 x^{r-2} + \cdots + a_{r-2}x + a_{r-1}$

$= \sum_{i=0}^{r-1} a_i x^{r-1-i}$,

4. $a^*(x) = x^{r-1} a\left(\frac{1}{x}\right) = \sum_{i=0}^{r-1} a_i x^i$,

5.

$$\begin{aligned} h(x) &= c_1 a_0 + c_2 a_1 + \cdots + c_L a_{L-1} \\ &\quad + x[c_2 a_0 + c_3 a_1 + \cdots + c_L a_{L-2}] \\ &\quad + x^2[c_3 a_0 + \cdots + c_L a_{L-3}] + \cdots \\ &\quad + x^{L-2}[c_{L-1} a_0 + c_L a_1] + x^{L-1} c_L a_0 \\ &= \sum_{i=0}^{L-1} \sum_{j=0}^{L-1-i} c_{1+i+j} a_i x^i, \text{ and} \end{aligned}$$

6. $h^*(x) = x^{L-1} h\left(\frac{1}{x}\right) = \sum_{i=0}^{L-1} \sum_{j=0}^{i} c_{L-i+j} a_i x^i$.

We will first state about generating functions of a given ultimately periodic sequence.

Let $G(x) = \sum_{n=0}^{\infty} a_n x^n$.

Consider the following equalities:

$$\begin{aligned} f^*(x)G(x) &= -\left(\sum_{i=0}^{L} c_i x^{L-i}\right)\left(\sum_{n=0}^{\infty} a_n x^n\right) \\ &= -[c_L a_0 + (c_{L-1}a_0 + c_L a_1)x \\ &\quad + (c_{L-2}a_0 + c_{L-1}a_1 + c_L a_2)x^2 \\ &\quad + \cdots + (c_1 a_0 + \cdots + c_L a_{L-1})x^{L-1}] \\ &\quad - [(c_0 a_0 + c_1 a_1 + \cdots + c_L a_L)x^L \\ &\quad + (c_0 a_1 + c_1 a_2 + \cdots + c_L a_{L+1})x^{L+1} \\ &\quad + \cdots] \end{aligned}$$

Then $G(x) = \frac{-h^*(x)}{f^*(x)}$ and, if $\{a_n\}$ is periodic,

$G(x) = \frac{a^*(x)}{1-x^r}$.

Hence we obtain a theorem.

Theorem 3.1

Let $k(x), c(x) \in F_q[x]$ be polynomials with $c(0) = 1$.

Let $\sum_{n=0}^{\infty} g_n x^n = \frac{k(x)}{c(x)}$. Then

$\{g_n\}$ is a sequence that generates by an d-stage LFSR where $d = \max(\deg(c), 1 + \deg(k))$.

In particular, if $k(x)$ and $c(x)$ are relatively prime, then $\{g_n\}$ is generated by the unique shortest d-stage LFSR.

Proof 3.1

Let $c(x) = \sum_{i=0}^{d} -c_i' x^{d-i}$ such that

$c_0' = \cdots = c'_{d-\deg(c)-1} = 0$ and $c_d' = -1$.

From above paragraph and $\sum_{n=0}^{\infty} g_n x^n = \frac{k(x)}{c(x)}$,

$\sum_{i=0}^{d} c'_i g_{n+i} = 0$ for $n \geq 0$.

Thus $\{g_n\}$ is a sequence that generates by an d-stage LFSR where

$d = \max(\deg(c), 1 + \deg(k))$.

Suppose that $k(x)$ and $c(x)$ are relatively prime.

If $\{g_n\}$ is generated by another LFSR such that $\sum_{n=0}^{\infty} g_n x^n = \frac{t(x)}{s(x)}$, then $s(x)k(x) = c(x)t(x)$.

Since $k(x)$ and $c(x)$ are relatively prime, $c(x)|s(x)$ and $k(x)|t(x)$.
If the LFSR is shortest, then $\deg(c)=\deg(s)$ and $\deg(k)=\deg(t)$. Then $c(x)=s(x)$ and so $k(x)=t(x)$.
The proof is complete.

The following fact follows Theorem 3.1.
Let $\{g_n\}$ be a ultimately periodic sequence of elements of F_q with the least period r and the preperiod n_0.

Then

$$\begin{aligned}\sum_{n=0}^{\infty} g_n x^n &= \sum_{n=0}^{n_0-1} g_n x^n + \sum_{n=n_0}^{\infty} g_n x^n \\ &= \sum_{n=0}^{n_0-1} g_n x^n + \frac{g_{n_0}x^{n_0}+\cdots+g_{n_0+r-1}x^{n_0+r-1}}{1-x^r} \\ &= \frac{\sum_{n=0}^{n_0+r-1} g_n x^n - \sum_{n=0}^{n_0-1} g_n x^{n+r}}{1-x^r},\end{aligned}$$

that is, $\{g_n\}$ is a sequence generated by an n_0+r-stage LFSR.

From Theorem 3.2, we define the minimal polynomial of a given sequence.

Theorem 3.2
There exists a uniquely determined minic polynomial $m(x)\in F_q[x]$ having the following property: a monic polynomial $c(x)\in F_q[x]$ of positive degree is a characterisitic polynomial of $\{a_n\}$ if and only if $m(x)$ divides $c(x)$.

Proof 3.2 Let $d(x)$ is the monic greatest common divisor of $f(x)$ and $h(x)$. Then $m(x)=f(x)/d(x)$ satisfies the statement of this theorem. For the complete proof, see [2].

Definition 3.1
In Theorem 3.2, $m(x)$ is called the minimal polynomial of the sequence.

In Theorem 3.1, if $k(x)$ and $c(x)$ are relatively prime, then $x^d c\left(\frac{1}{x}\right)$ is the minimal polynomial of $\{g_n\}$.

4. Period of Sequence

In this Section, we state some facts on the least periods of ultimately periodic sequences. It only depends on the finite field theory.

Put $A=\begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{L-1} \end{pmatrix}$ and

$a_n=(a_n, a_{n+1}, \cdots, a_{n+L-1})$.
Then $a_n=a_0A^n$ and, if $c_0\neq 0, A\in GL_L(F_q)$.

Lemma 4.1
If $c_0\neq 0$, then $\{a_n\}$ is periodic and its least period r divides the order of $A\in GL_L(F_q)$.

Proof 4.1. Let m be the order of A. Then $a_{n+m}=a_0A^{n+m}=a_0A^n=a_n$

Definition 4.1.
Let k(x) in $F_q[x]$. If $k(x)=x^n s(x)$ and $s(0)\neq 0$,then
ord($k(x)$) = min $\{e \mid s(x)$ *divides* $x^{e-1}\}$.
From Lemma 4.1 and the fact that $A^e=I$ if and only if $f(x)$ divides x^e-1, we see sufficient conditions that a sequence has the maximum least period.

Theorem 4.2.
1. *r divides ord(f).*
2. *If f is irreducible, then r is equal to ord(f)* and *r divides* q^L-1.
3. *If f is the* min*imal polynomial of* a_n *, then r is equal to ord(f).*

Proof 4.2.

1. If $c_0 \neq 0$, then it is clear.

Let $c_0 = 0$.

Then we write $f(x) = x^l c(x)$ *with* $c(0) \neq 0$.

Consider a sequence

$$\{b_n = a_{n+l} | n = 0, 1, 2, \cdots\}.$$

2. If $f(x) = x$, then $\mathrm{ord}(f) = 1$ and $r = 1$.

Otherwise, the results follow 1 and Corollary 3.4 in [2].

3. Let n_0 be the preperiod of $\{a_n\}$ such that $a_{n+r} = a_n$ for all $n \geq n_0$.

Then $x^{n_0+r} - x^{n_0}$ is acharacteristic polynomial of a_n and so $f(x)$ divides $x^{n_0}(x^r - 1)$.

Therefore $f(x)$ is of the form $f(x) = x^l c(x)$ with $l \leq n_0$ and $c(0) \neq 0$.

Hence $ord(f(x)) = ord(c(x)) \leq r$.

5 Linear Complexity of Sequence

First, if the linear complexity of a sequence is small, we show that one can easily reproduce the sequence under the assumption that one know a consecutive subsequence of length $2L$. This *means that a cryptographically* secure sequence should have the large linear complexity.

That $f(x)$ is the minimal polynomial of a_n is a necessary and sufficient condition of that $a_0, a_1, \cdots, a_{L-1}$ are linearly independent over F_q. Thus we obtain the following theorem.

Theorem 5.1

If $c_0 \neq 0$, then $f(x)$ is the minimal polynomial of a_n if and only if $a_n, a_{n+1}, \cdots, a_{n+L-1}$ are linearly independent over F_q for $n = 0, 1, 2, \cdots$.

If $c_0 = 0$, then Theorem 5.1 is false.

Let $c_0 = 0, c_1 = 1, c_2 = 1, a_0 = 0, a_1 = 0, a_2 = 1$ in F_2. Then the LFSR generates 0011011011$\cdots$. Since $f(x) = x^3 + x^2 + x$ and $h(x) = 1, f(x)$ is minimal. In this case, $(0,0,1), (0,1,1), (1,1,0)$ is an independent set and $(0,1,1), (1,1,0), (1,0,1)$ is a dependent set.

Theorem 5.1 implies that if one know a consecutive subsequence of length $2L$, then he can solve the linear equation system such that he finds a characteristic polynomial $f(x)$.

Now, we consider the linear complexity of sum and product of two ultimately periodic sequences.

Let us define vector spaces of ultimately periodic sequences.

Definition 5.1 Let $k(x) = -\sum_{i=0}^{m-1} b_i x^i + x^m$ be a nonconstant monic polynomial over F_q.

We define that

$$\Omega(k(x)) = \{\{g_n\} | g_n = \sum_{i=0}^{m-1} b_i g_{n-m+i} \text{ for } n \geq m\}.$$

Convetionally, $\Omega(1) = \{\{0\}\}$.

Note that $\Omega(k(x))$ is a vector space over F_q with the componentwise operations.

We need two lemmas.

Lemma5.2

Let $k(x)$ and $s(x)$ be monic polynomials over F_q. Then $\Omega(k(x)) \subset \Omega(s(x))$ if and only if $k(x) | s(x)$.

proof 5.2

If $k(x) = 1$, then it is clear. Let $k(x) \neq 1$.

Suppose that $\Omega(k(x)) \subset \Omega(s(x))$. Let $\{g_n\}$ be a

sequence in $\Omega(k(x))$ generated by an initial loaded vector $(0,\cdots,0,1)$. Then $k(x)$ is the minimal polynomial of $\{g_n\}$. Since $\{g_n\}\in\Omega(s(x))$,
$k(x)|s(x)$.

Conversely, suppose $k(x)|s(x)$. Let $\{g_n\}$ be a sequence in $\Omega(k(x))$ and let $m(x)$ be the minimal polynomial of $\{g_n\}$.
Then $m(x)$ divides $k(x)$ and $s(x)$. Hence $\{g_n\}\in\Omega(s(x))$.

Lemma 5.3
Let $k(x)$ and $s(x)$ be monic polynomials over F_q and let $d(x)=\gcd(k,s)$ and $l(x)=lcm(k,s)$ where $d(x)$ and $l(x)$ are monic. Then $\Omega(k)\cap\Omega(s)=\Omega(d)$ and $\Omega(k)+\Omega(s)=\Omega(l)$.

Proof 5.3
The result follows Lemma 5.2.

From the above two Lemmas, we have a result about the linear complexity and the least period of sum of two ultimately periodic sequences.

Let $\{g_n\}$ and $\{g_n'\}$ be ultimately periodic sequences of elements of F_q. Let $m(x)$ and $m'(x)$ be minimal polynomials of $\{g_n\}$ and $\{g_n'\}$, respectively. Then $\{g_n+g_n'\}$ is a ultimately periodic sequence
whose the minimal polynomial divides $lcm(m,m')$. In particular, if m and m' are relatively prime, then the minimal polynomial
of $\{g_n+g_n'\}$ is $m(x)m'(x)$ and so the least period of $\{g_n+g_n'\}$ is $\mathrm{ord}(mm')=\mathrm{lcm}(\mathrm{ord}(m),\mathrm{ord}(m'))$.

Proof 5.4 From Lemma 5.3, the first statement is true.

Let m and m' be relatively prime and let m^+ be the minimal polynomial of $\{g_n+g'_n\}$.
If $m^+(x)$ is 1, that is, $\{g_n+g_n'\}=\{0\}$, then $m(x)=m'(x)$. In this case, $m(x)=m'(x)=1$.
Suppose that
$$m^+(x) = x^L - b_{L-1}x^{L-1} - b_{L-2}x^{L-2} - \cdots - b_1x - b_0$$
and $L\geq 1$. Then

$$\begin{aligned} g_{L+n}+g'_{L+n} &= \sum_{i=0}^{L-1} b_i(g_{n+i}+g'_{n+i}) \\ &= \sum_{i=0}^{L-1} b_ig_{n+i} + \sum_{i=0}^{L-1} b_ig'_{n+i} \\ &\quad \text{for } n\geq 0. \end{aligned}$$

So $g_{L+n}-\sum_{i=0}^{L-1}b_ig_{n+i}$
$=-g'_{L+n}+\sum_{i=0}^{L-1}b_ig'_{n+i}$ for $n\geq 0$
that is,

$$\begin{aligned} \{v_n\} &= \{g_{L+n}\} - \sum_{i=0}^{L-1} b_i\{g_{n+i}\} \\ &= -\{g'_{L+n}\} + \sum_{i=0}^{L-1} b_i\{g'_{n+i}\} \end{aligned}$$

Since $\{g_{L+n}\}$, $\{g_{n+i}\}\in\Omega(m)$ and
$\{g'_{L+n}\}$, $\{g'_{n+i}\}\in\Omega(m')$,
$\{v_n\}\in\Omega(m)\cap\Omega(m')=\Omega(1)=\{\{0\}\}$.
Hence $\{g_n\}$, $\{g'_n\}\in\Omega(m^+)$ and so $m|m^+$, $m'|m^+$, i.e., the minimal polynomial of $\{g_n+g_n'\}$ is $m(x)m'(x)$.

The last statement follows Theorem 4.2-3.

The product of two sequences is more complicated. We start with the following criterion:

Let E be a set of sequences of elements of F_q. There exists
a monic polynomial $k(x)$ over F_q such that $E=\Omega(k(x))$ if and only if
E is a finite vector space, and
E is closed by the translation such that $\{g_n\}\in E$ implies $\{g_{n+i}\}\in E$ for any $i\geq 0$.

From the above criterion, we obtain Theorem 5.5.

Theorem 5.5
Let $k(x)$ and $s(x)$ be monic polynomials over F_q. There exists a monic polynomial $l(x)$ over F_q such that

$$\Omega((k(x))\cdot\Omega(s(x))t=\{\sum_{finite}\{g_n g_{n'}\}|,\{g_n\}\in\Omega(k(x)) \text{ and } \{g_n'\}\in\Omega(s(x))\}=\Omega(l(x)).$$

Thus, we can find a characteristic polynomial of a product sequence.
But, in Theorem 5.5, we do not have an explicit formula of $l(x)$.

If chracteristic polynomials of two sequences have only simple roots, we obtain an explicit formula of $l(x)$.

Definition 5.2
Let $k(x)$ and $s(x)$ be nonconstant polynomials over F_q. We define
that $k(x)\vee s(x)=\prod_{distinct\,\alpha\beta}(x-\alpha\beta)$
where α and β are roots of $k(x)$ and $s(x)$ in the splitting field of $k(x)s(x)$ over F_q, respectively.
Note that $k(x)\vee s(x)\in F_q[x]$.

Theorem 5.6
Let $k(x)$ and $s(x)$ be nonconstant monic polynomials over F_q without multiple roots.
Then $\Omega(k(x))\cdot\Omega(s(x))=\Omega(k(x)\vee s(x))$..

PROOF 5.4 See [2].

In general, the product of two sequences does not have maximum linear complexity such that the linear complexity may be not the product of two linear complexities. For example, let $k(x)=x^3+x+1$.and
$s(x)=x^6+x^4+x^2+x+1$
$k(x)$ and $s(x)$ are irreducible polynomials. Since
$k(x)\vee s(x)=x^{12}+x^{11}+x^9+x^8+x^6+x^4+x^3+x+1$,
the product of any two sequences generated by $k(x)$ and $s(x)$ does not have the maximum linear complexity 18.

From the results by Zierler and Gottfert, we can know that $k(x)\vee s(x)$ in Theorem may be the minimal polynomial of product of two sequences generated by the minimal polynomials $k(x)$ and $s(x)$.

Definition 5.3
Let n and m be positive integers and let F_q have the characteristic $p\neq 0$. We write

$$n-1=\sum j_\nu p^\nu, 0\leq j_\nu<p,$$
$$m-1=\sum i_\nu p^\nu, 0\leq i_\nu<p.$$

We let λ be the smallest nonnegative integer such that $j_\nu+i_\nu<p$ for all $\nu\geq\lambda$, and we set

$$n\vee m=p^\lambda+\sum_{\nu\geq\lambda}(j_\nu+i_\nu)p^\nu.$$

In Definition 5.3, $n\vee m$ has an equvalent definition.
For any positive integer n with p-ary expansion $n=\sum j_\nu p^\nu$,

$$(x+1)^n=(x+1)^{\sum j_\nu p^\nu}$$
$$\equiv\prod_\nu(x^{p^\nu}+1)^{j_\nu}(\mathrm{mod}\,p)$$

$$\equiv \prod_{\nu} \sum_{j=0}^{j_\nu} \binom{j_\nu}{j} x^{jp^\nu} (\mathrm{mod}\, p).$$

Therefore $\binom{n}{m} \equiv \prod \binom{j_\nu}{i_\nu} (\mathrm{mod}\, p)$ where $n = \sum j_\nu p^\nu$ and $m = \sum i_{nu} p^{nu}$ are p-ary expansions. Thus we get the following necessary and sufficient condition:

$\binom{n+m}{n} \not\equiv 0 (\mathrm{mod}\, p)$ if and only if $j_\nu + i_\nu <$ for *all* ν.

This implies that

$$n \vee m = \max \{i+j+1 | \binom{i+j}{i} \not\equiv 0 (\mathrm{mod}\, p), \\ 0 \le i \le n-1, 0 \le j \le m-1\}$$

We state an useful Lemma. Its proof is in [3].

Lemma 5.7

Let $0 \neq a \in F_q$ and $n, m \in Z^+$. Let $k(x)$ be a monic polynomial over F_q.

1. $\Omega((x-a)^n) = \Omega(x-a)\Omega((x-1)^n)$.
2. If k has distinct nonzero roots, then $\Omega(k^n) = \Omega(k)\Omega((x-1)^n)$.
3. $\Omega((x-1)^n)\Omega((x-1)^m) = \Omega((x-1)^{n \vee m})$.

Theorem 5.8 gives us an upper bound of the linear complexity of a product sequence.
It follows Lemma 5.7 and Lemma 5.3.

Theorem 5.8

Let $k(x)$, $s(x)$ be nonconstant monic polynomials over F_q

with irreducible decompositions $k(x) = \prod k_i^{n_i} x^n$ and $s(x) = \prod s_i^{m_i} x^m$ where k_i and s_i have nonzero roots. Then

$$\begin{aligned} \Omega(k)\Omega(s) &= \Omega(\prod k_i^{n_i} x^n)\Omega(\prod s_j^{m_j} x^m) \\ &= (\sum \Omega(k_i^{n_i} \Omega(x-1)) + \Omega(x^n))(\sum \Omega(s_j) \\ &\quad \Omega((x-1)^{m_j}) + \Omega(x^m)) \\ &= \sum_{i,j} \Omega(k_i \vee s_j)^{n_i \vee m_j} + \Omega(x^{\max(n,m)}) \\ &= \Omega(x^{\max(n,m)} \mathrm{lcm}_{i,j} \{(k_{i \vee ee} s_j)^{n_i \vee m_j}\}). \end{aligned}$$

Now, let us see a lower bound by R. Gottfert and H. Niederreiter.

Definition 5.4

Let $k(x)$ and $s(x)$ be nonconstant monic polynomials over F_q with only nonzero roots, let $\alpha_1, \cdots, \alpha_{t_1}$ be

roots of k with corresponding multiplicities $a_1, \cdots, a_{t_1}$, and let $\beta_1, \cdots, \beta_{t_2}$ be roots of s with corresponding multiplicities $b_1, \cdots, b_{t_2}$. We put

$C = \{(i,j) \in N^2 | 1 \le i \le t_1, 1 \le j \le t_2\}$, Let $\gamma_1, \cdots, \gamma_t$ be the distinct elements among the products $\alpha_i \beta_j$ with $(i,j) \in C$ and let C and let C.

$d = \{(i,j) \in C | \alpha_i \beta_j = \gamma_d\}$ for $1 \le d \le t$.

We define

$$A(k,s)(x) = \prod_{d=1}^{t}{}^{*} (x - \gamma_d)^{e_d} \in F_q[x]$$

where the asterisk indicates that the product is extended only over those d satisfying the following property:

the set C_d contains a pair (i,j) for which $\binom{a_{i+b_{j-2}}}{a_{i-1}} \not\equiv 0 (\mathrm{mod}\, p)$ and $a_{i'} \vee b_{j'} < a_i \vee b_j$ for all $(i',j') \in C_d$ with $(i',j') \neq (i,j)$.

Via this uniquely determined pair $(i,j) \in C_d$ we define

$e_d = a_i \vee b_j = a_i + b_j - 1$.

As usual, an empty product has the value 1.

One may be interested in the following theorem.

Theorem 5.9

Let k and $s \in F_q[x]$ be nonconstant monic polynomials with $k(0)s(0) \neq 0$ and let $\{a_n\}$ and $\{b_n\}$ be sequences generated by the minimal polynomials k and s, respectively. Then the minimal polynomial of $\{a_n b_n\}$ is divisible by $A(k, s)$.

Proof 5.9 ***see [2]***

With the notations in Definition 5.4 and Theorem 5.8,

$$\text{lcm}_{i,j}\{(k_i \vee s_j)^{n_i \vee m_j}\} = \prod_{d=1}^{t}(x-\gamma_d)^{z_d}$$

where $z_d = \max_{(i,j)\in C_d}(n_i \vee m_j)$ for $1 \le d \le t$.
Therefore we get the following fact:

If $k(x)$ and $s(x)$ are irreducible polynomials and every product of roots of $k(x)$ and roots of $s(x)$ is distinct
such that $\alpha_i \beta_j \neq \alpha_{i'} \beta_{j'}$ where $\alpha_i, \alpha_{i'}$
are any roots of $k(x)$ and
$\beta_j, \beta_{j'}$ are any roots of $s(x)$, then, by Theorem 5.8 and Theorem 5.9, the product of two sequences generated by $k(x)$ and $s(x)$ has the minimal polynomial $\prod_{i,j}(x-\gamma_{i,j})$ where
$\gamma_{i,j} = \alpha_i \beta_j$
are products of each roots of $k(x)$ and $s(x)$.
Thus in this case, the product has the maximum linear complexity.

6 Concluding Remarks

A sequence of elements of F_q generated by a LFSR with stage L may have the maximum least period $q^L - 1$.
From Theorem 4.2, if a characteristic polynomial of a sequence is primitive such that its order is $q^L - 1$,
then the least period of the sequence is $q^L - 1$.

Let $\{a_n\}$ and $\{b_n\}$ be sequences of elements of F_q generated by LFSRs with stage L_a and L_b,
respectively and let f_a and f_b be the minimul polynomials of $\{a_n\}$ and $\{b_n\}$, respectively.
If f_a is primitive, f_b is irreducible, and $\gcd(L_a, L_b) = 1$, then we have the following result:
$\deg(f_a \vee f_b) = L_a L_b$
Thus, by theorem 5.8 and Theorem 5.9, the product of the above two sequences has the maximum linear complexity.

To avoid Meier-Staffelbach correlation attack, the nonlinear combination of feedback shift registers has to be done under the consideration of its linear complexity. Thus our results are useful
to propose the nonlinearly combined stream cipher using the sum and multiplication of feedback shift registers.

References

[1] A. H. Chan, M. Goresky, and A. Klapper, On the Linear Complexity of Feedback Registers, IEEE Trans. Inform. Theory, vol. 36, no. 3, pp.~640--644, May 1990

[2] R. Lidl and H. Niederreiter, Finite Fileds, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1984

[3] N. Zierler and W. H. Mills, Products of linear recurring sequences, Journal of algebra, vol. 27, pp.~147--157, 1973

[4] R. G"ottfert and H. Niederreiter,

A general lower bound for the linear complexity of the product of shift-register sequences, Advances in Cryptology - EUROCRYPT '94, Lecture Notes in Computer Science, vol. 950, pp.~223--229, Springer-Verlag, Berlin, 1995

□ 著者紹介

김철(Chul Kim) **정회원**

1984년 2월 : 연세대학교 수학과 학사
1984년 3월 : 연세 대학교 대학원 수학과 입학
1989년 12월 : North Carolina 주립대 대학원 수학과 석, 박사

<관심분야> 암호학, 부호이론, 모의실험 이론, 계산이론, 응용 대수학