비선형 합성 함수를 이용한 랜덤 계열의 특성 분석

염 흥 열
순천향대학교 전자공학과

Analysis of Random Sequences using Nonlinear Combining Functions

HeungYoul Youm
Department of Electronics Engineering, SoonChunHyang Univ.

요약

본 논문에서는 비선형 합성 함수를 이용하여 생성된 난수 계열의 특성을 분석한다. 먼저 트레이스 함수 등을 정의하고, 선형 복잡도 및 생성기 구조 분석시 요구되는 관련 이론을 도출하고, 특정 난수 계열이 주어진 경우 이계열을 생성할 수 있는 최소 길이의 LFSR 을 합성할 수 있는 LFSR 합성 알고리듬을 제시한다. 동일한 계열을 위상 천이한 계열간의 비선형 결합으로 생성된 난수 계열과 다른 계열간의 비선형 결합으로 생성된 난수 계열에 대한 주기 및 선형 복잡도 등의 특성을 분석하고 생성기의 구조를 제시한다.

1. 서 론

LFSR (linear feedback shift register) 계열은 난수 계열을 생성하기 위한 기본 계열로 널리 이용되고 있다.[1,2,3,4,5] LFSR 계열은 암호학적으로 안전하지 않은 계열로 알려져 있다. 계열의 선형 복잡도(linear complexity) 는 해당 계열을 생성 할 수 있는 최소 길이의 LFSR의 단수를 의미한다. 특정 난수 계열이 주어졌을 경우, 이 계열을 생성할 수 있는 최소 길이의 LFSR 을 구하는 효율적인 알고리듬은 Berlekamp-Massey 에 의해 제시되었다.[6] LFSR 합성 알고리듬에 견딜 수 있는 방법으로 LFSR 계열을 비선형 함수로 결합하여 선형 복잡도를 키우는 방법이 널리 이용되어 왔다. LFSR 계열을 암호에 이용하기 위해서는 적어도 LFSR 합성 알고리듬의 계산량이 매우 큰 선형 복잡도를 갖는 난수 계열을 선택해야 한다. 일반적으로 비선형 함수를 적용하는 방법은 동일한 LFSR 계열을 위상 천이한 출력 계열들에 비선형 함수를 적용하는 방법과 서로 다른 LFSR 계열에 비선형 함수를 적용하는 방법이 있다.

본 논문에서는 주기 및 선형복잡도를 중심으로 한 비선형 난수 계열의 특성을 분석한다. 먼저 트레이스 함수을 정의하고, 선형복잡도 및 생성기 구조 분석시 요구되는 관련 이론을 도출하고, 특정 계열이 주어진 경우 최소 길이의 LFSR 을 합성할 수 있는 LFSR 합성 알고리듬을 제시한다. 그리고 동일한 LFSR 계열을 위상 천이한 계열들간의 비선형 결합으로 생성된 난수 계열과 다른 LFSR 계열간의 비선형 결합으로 생성된 난수 계열에 대한 선형 복잡도 등의 여러 특성을 분석하고 생성기의 구조를 제시한다. 이를 위하여 동일 계열을 위상 천이한 계열을 비선형 함수를 이용하여 결합한 계열의 특성방정식과 최소 다항식 등을 도출하고, 특정 원소의 특성방정식의 근 여부와 선형 복잡도의 상한값 및 하한값 그리고 임의로 선택된 비선형 함수가 최대의 선형복잡도를 갖을 확률 등과 관련된 바탕 이론을 제시한다. 그리고 다른 LFSR 계열 들간의 비선형 결합의 출력 계열의 특성을 분석하기 위한 선형 복잡도와 주기 관련 바탕 이론을 제시한다.

2. LFSR 계열과 합성 알고리듬

2.1 LFSR 계열

단수 (length) 가 r 인 LFSR 에서 가능한 귀환 계수의 전체 갯수는 2^r 이 되며, 이중 계열의 주기가 2^r-1 인 최대장 계열 (maximum length sequence) 의 갯수는 $\phi(2^r-1)/r$ 이다. 여기서 ϕ 는 Euler totient 함수이다. 키스트림 계열이 암호에 응용될 경우 비밀키는 LFSR 의 초기치와 귀환 계수 들이다. 최대장 계열의 최대 단점은 난수 계열의 $2n$ 비트만 알려지면, 이로부터 생성기의 초기치와 귀환 계수를 쉽게 구할 수 있다는 점이다. 따라서 최대장 계열은 암호학적으로 전혀 안전하지 않음을 의미한다. 난수 계열을 암호 시스템에 적용하기 위하여 계열이 가져야 할 조건은 심볼 0, 1 의 발생 빈도수가 거의 같아야 하고, 계열의 주기가 가능한 길어야 하며, 여러개의 계열을 조합한 경우 계열간이 서로 상관성 (correlation) 이 없어야 하고, 비선형성 함수를 도입하여 선형 복잡도를 증가시켜야 하며, 과거의 발생 심볼로 부터 현재의 계열을 예측할 수 없어야 한다는 것 등이다. 계열의 선형 복잡도는 해당 계열을 생성하기 위하여 요구되는 LFSR 의 최소 단수를 의미한다.

정수 M 이 J 에 의해 나누어 질 경우, 트레이스 함수 $tr_J^M(\alpha)$ 는 식 (2.1)과 $GF(2^M)$ 상의 원소 α 를 부분체 $GF(2^J)$ 상의 원소로 사상한다.

$$tr_J^M(\alpha) = \sum_{i=0}^{M/J-1} \alpha^{2^{iJ}} \qquad (2.1)$$

트레이스 함수는 다음 다섯가지 특성을 만족한다. [10,12]

① $GF(2^M)$ 상의 임의의 원소 α 에 대해 식 (2.2)가 만족한다. 즉 α 의 복소근 들의 트레이스 값은 동일함을 의미한다.

$$tr_J^M(\alpha) = tr_J^M(\alpha^{2^{Jk}}),\ k=1,\cdots,M-1 \qquad (2.2)$$

② $GF(2^M)$ 상의 임의의 원소 α, β, $GF(2^J)$ 상의 원소 a, b 에 대해, 식 (2.3)이 만족한다. 이는 트레이스 함수의 선형성을 의미한다.

$$tr_J^M(a\alpha+b\beta) = a\,tr_J^M(\alpha)+b\,tr_J^M(\beta) \qquad (2.3)$$

③ $GF(2^J)$ 상의 임의의 원소 b 가 주어진 경우, $tr_J^M(\alpha) = b$ 을 만족하는 $GF(2^M)$ 내의 원소의 갯수는 2^{M-J} 개 이다.

④ 실수 연산 상에서 $GF(2^M)$ 상의 0 이 아닌 임의의 원소 γ 에 대해, 식 (2.4)가 성립한다.

$$\sum_{\alpha\in GF(2^M)} (-1)^{tr_1^M(\gamma\alpha)} = 0 \qquad (2.4)$$

⑤ $GF(2^M)$ 상의 임의의 원소 α 에 대해, 식 (2.5)가 성립한다.

$$tr_1^M(\alpha) = tr_1^J(tr_J^M(\alpha)) \qquad (2.5)$$

LFSR 계열을 $\overline{a}$ 라 하고, 계열의 구성 요소를 a_n $(n=1,2,\cdots)$ 이라 하자. LFSR 계열의 재귀 귀환 다항식 (linear recursive equation) 과 이에 대응되는 특성 방정식 (characteristic equation) 은 식 (2.6)과 같다.

$$a_n + \sum_{i=1}^{r} c_i a_{n-i} = 0, \quad n \geq r \qquad (2.6)$$
$$x^r + \sum_{i=1}^{r} c_i x^{r-i} = 0$$

식 (2.6)과 같은 특성 방정식의 근을 α 라 가정하면 $\alpha^r + \sum_{i=1}^{r} c_i \alpha^{r-i} = 0$ 을 이용하여 유한체 $GF(2^r)$ 을 생성할 수 있다. 식 (2.6)은 $GF(2^r)$ 상에서 r 개의 근을 가지며, 특성 방정식이 원시다항식 (primitive polynomial) 이라고 가정하면 α 의 복소근 (conjugate roots) 을 r 개의 근으로 갖는다. 이의 일반해는 식 (2.7)과 같이 표현될 수 있다.

$$\begin{aligned} a_n &= tr_1^r(A\alpha^n) = \sum_{i=1}^{r} A_i (\alpha^{2^{i-1}})^n \\ &= A_1(\alpha)^n + A_2(\alpha^2)^n + \cdots + A_r(\alpha^{2^{r-1}})^n \end{aligned} \qquad (2.7)$$

여기서 계수 $A_i = A^{2^i}$ 는 난수 계열의 초기치 $a_0, \cdots, a_{r-1}$ 에 의해 유일하게 결정될 수 있다. 식 (2.7) 에서 알수 있듯이 선형 복잡도가 r 인 LFSR 계열의 요소는 r 개의 복소근들의 결합으로 표현된다. 따라서 계열의 원소가 임의의 l 개의 원소들로 표현된다면 이 계열의 선형 복잡도는 l 이 됨을 알 수 있다. 식 (2.7)에서 알수 있듯이 임의의 특성방정식에 의해 생성되는 계열요소 a_n 은 일반적으로 식 (2.8)과 같이 쓸수 있다.

$$a_n = \sum_{i=0}^{l-1} A_i \alpha^{e_i n} \qquad (2.8)$$

여기서 $A_i \in GF(2^r) \neq 0$ 이다. 식 (2.8) 과 같은 계열의 선형복잡도는 l 이 된다. 만약 계열 $\overline{a}$ 의 특성방정식 $c(x) = \sum_{i=0}^{l-1} c_i x^{l-i}$ 이라면 계열 요소와 계수와의 관계는 식 (2.9)와 같이 표현된다.

$$\sum_{i=0}^{l} c_i a_{n-i} = 0 \qquad (2.9)$$

여기서 $c_0 = 1$ 이다.

(정리 2.1) 식 (2.9) 에서의 l 개의 원소 $\alpha^{e_i} (i = 0, \cdots, l-1)$ 가 식 (2.8) 에서와 같이 계열 요소의 구성 원소일 경우, 계열 $\overline{a}$ 의 특성방정식은 식 (2.10) 과 같다.

$$c(x) = \prod_{i=0}^{l-1} (x - \alpha^{e_i}) \qquad (2.10)$$

(증명) $c(x)$ 의 차수는 l 이다. 식 (2.8)을 식 (2.9) 에 대입하면 식 (2.11) 이 된다.

$$\begin{aligned} \sum_{i=0}^{l} c_i a_{n-i} &= \sum_{i=0}^{l} c_i \sum_{j=0}^{l-1} A_j \alpha^{e_j(n-i)} \\ &= \sum_{i=0}^{l} c_i \sum_{j=0}^{l-1} A_j \alpha^{e_j(l-i+n-l)} \\ &= \sum_{j=0}^{l-1} A_j \alpha^{e_j(n-l)} \sum_{i=0}^{l} c_i \alpha^{e_j(l-i)} \\ &= \sum_{j=0}^{l-1} A_j \alpha^{e_j(n-l)} c(\alpha^{e_j}) \\ &= 0 \end{aligned} \qquad (2.11)$$

$c(\alpha^{e_j})$ 가 "0" 이 되어야 하므로 $c(x)$ 의 근은 α^{e_j} 가 된다. 따라서 식 (2.11)의 관계식을 만족

하는 계열 $\bar{a}$ 는 식 (2.10) 과 같은 특성방정식 $c(x)$ 를 갖는다.

(증명완료)

(정리 2.1) 로 부터 a_n 을 구성하는 원소들은 이 계열을 생성하는 특성방정식의 근이 됨을 알 수 있다. 그러므로 특성방정식의 차수가 계열의 선형복잡도이다.

LFSR 의 특성방정식이 원시다항식이고, 각 LFSR 의 길이가 r_i 인 경우, 원시다항식에 의해 생성된 최대장계열은 주기가 2^r-1 이고, "0" 또는 "1" 비트 발생 빈도가 등분포이며, 한 주기내에서 0 비트의 수는 1 비트의 수는 1 만큼 작은 특성이 있다.

2.2 LFSR 합성 알고리듬

본 절에서는 Berlekamp-Massey 가 제시한 LFSR 합성을 위한 기본 정리와 원리을 도출하고 LFSR 합성 알고리듬을 제시한다.[6] LFSR 의 귀환다항식 (connection polynomial) 을 지연변수 D 를 이용하여 표현하면 식 (2.12) 과 같다.

$$\begin{aligned} c(D) &= c_0 + c_1 D + \cdots + c_r D^r \\ &= 1 + c_1 D + \cdots + c_r D^r \end{aligned} \qquad (2.12)$$

계열 요소와 귀환 계수와의 관계는 식 (2.13) 과 같다.

$$\sum_{i=0}^{r} c_i a_{n-i} = 0, \quad \text{for } n \geq r \qquad (2.13)$$

식 (2.13) 를 지연요소를 이용하여 표현하면 식 (2.14) 와 같다.

$$a(D)c(D) = P(D) \qquad (2.14)$$

여기서 $\deg[P(D)] < r$ 이다. 앞으로 $<c(D),r>$ 은 계열을 생성하는 단수가 r 인 LFSR 을 나타낸다. 위의 결과로 부터 정리 2.2 가 유도될 수 있다.

(정리 2.2) LFSR $<c(D),r>$ 은 계열 $a_0, a_1, a_2, \cdots$ 를 생성하기 위한 필요충분 조건은 식 (2.15) 와 같다.

$$a(D) = \frac{P(D)}{c(D)} \qquad (2.15)$$

여기서 $\deg[P(D)] < r$ 이다.

(정리 2.3) $\gcd[P(D),c(D)] = 1$ 이고 $c_0 = 1$ 인 경우, $a(D) = P(D)/c(D)$ 라면 $<c(D),r>$ 은 계열 $a(D)$ 를 생성할 수 있는 최소 길이의 LFSR 이다. 여기서 $r = Max\{\deg[c(D)], \deg[P(D)]+1\}$ 이다.

(증명생략)

계열 $\tilde{a}^{(n)}$ 을 길이가 n 인 계열 요소로 구성된 $(a_0, \cdots, a_{n-1})$ 이라 정의한다.

(정리 2.4) $<c(D),r>$ 이 $\tilde{a}^{(n)}$ 을 생성하기 위한 필요충분 조건은 식 (2.16)과 같다.

$$\sum_{i=o}^{r} c_i a_{j-i} = 0, \quad \text{for } r \le j < n \tag{2.16}$$

(증명 자명)

정리 2.4의 의미는 $c(D)a(D)$ 의 D^n 차 미만의 항으로 구성되는 $R_{D^n}\{c(D)a(D)\}$ 의 r 에서 $n-1$ 까지의 차수의 계수는 "0" 됨을 의미한다.

(정리 2.5) $<c(D),r>$ 이 $\tilde{a}^{(n)}$ 을 생성하는 것은 식 (2.17)을 만족함을 의미한다.

$$R_{D^{n+1}}[c(D)a(D)] = P(D)+\delta_n D^n \tag{2.17}$$

여기서 $\deg[P(D)]<r$ 이고 $\delta_n = a_n + c_1 a_{n-1} + \cdots + c_r a_{n-r}$ 이다. 그리고 $<c(D),r>$ 이 $\tilde{a}^{(n)}$ 을 생성한다면 $<c(D),r>$ 이 $\tilde{a}^{(n+1)} = (a_0, a_1, \cdots, a_{n-1}, a_n)$ 을 생성하기 위한 필요충분 조건은 $\delta_n = 0$ 이다. (증명생략)

(정리 2.6) $<c_1(D),r_1>$ 가 계열 $\tilde{a}^{(n)}$ 을 생성하고, $<c_2(D),r_2>$ 가 계열 $\tilde{b}^{(n)}$ 을 생성하면 $<c_1(D)c_2(D), r_1+r_2>$ 는 $k_1\tilde{a}^{(n)}+k_2\tilde{b}^{(n)}$, $k_1,k_2 \in GF(2)$ 를 생성한다.

(증명) 가정으로 부터 식 (2.18) 을 구할 수 있다.

$$\begin{aligned} R_{D^n}[c_1(D)a(D)] &= P_1(D), \ \deg[P_1(D)]<r_1 \\ R_{D^n}[c_2(D)b(D)] &= P_2(D), \ \deg[P_2(D)]<r_2 \end{aligned} \tag{2.18}$$

식 (2.18)은 식 (2.19)을 의미한다.

$$\begin{aligned} & R_{D^n}[(c_1(D)c_2(D))\ (k_1a(D)+k_2b(D))] \\ &= R_{D^n}[k_1c_1(D)a(D)c_2(D) + k_2c_1(D)c_2(D)b(D)] \\ &= k_1P_1(D)c_2(D) + k_2c_1(D)P_2(D), \quad \text{for all } k_1,k_2 \in GF(2) \end{aligned} \tag{2.19}$$

식 (2.18) 의 좌변의 차수는 r_1+r_2 이하이다. (증명완료)

(정리 2.7) 동일한 계열 주기를 갖는 두 계열을 선형 결합한 계열의 선형복잡도는 두 계열의 선형 복잡도를 각각 합한 값보다 작다. 즉 (2.20)의 관계식을 만족한다.

$$\Lambda\{k_1\tilde{a}^{(n)}+k_2\tilde{b}^{(n)}\} \le \Lambda\{\tilde{a}^{(n)}\}+\Lambda\{\tilde{b}^{(n)}\} \tag{2.20}$$

정리 2.6을 이용하여 쉽게 증명된다.

(정리 2.8) $<c(D),r>$ 이 $\tilde{a}^{(n+1)}$ 을 생성하지 못하지만 $\tilde{a}^{(n)}$ 을 생성한다면 $\tilde{a}^{(n+1)}$의 선형복잡도 $\Lambda\{\tilde{a}^{(n+1)}\}$ 는 적어도 $n+1-r$ 이상이다.

(증명) 가정으로 부터 $<c(D),r>$ 은 $\tilde{a}^{(n)}a_n'$ 를 생성한다. 여기서 $a_n \neq a_n'$ 이다. 따라서 $\tilde{a}^{(n)}a_n'$ 의 선형복잡도는 $\Lambda\{\tilde{a}^{(n)}a_n'\}=r$ 이다. $\tilde{a}^{(n+1)} - \tilde{a}^{(n)}a_n' = \tilde{a}^{(n)}a_n - \tilde{a}^{(n)}a_n' = \tilde{0}^{(n)}\delta_n$이므로 $\Lambda\{\tilde{a}^{(n+1)} - \tilde{a}^{(n)}a_n'\} = \Lambda\{\tilde{0}^{(n)}\delta_n\} = n+1$ 이 된다. 여기서 $\delta_n = a_n - a_n' \neq 0$ 이다. 정리 2.7로 부터 $\Lambda[\tilde{a}^{(n)} - \tilde{a}^{(n)}a_n'] \le \Lambda(\tilde{a}^{(n+1)}) + \Lambda(\tilde{a}^{(n)}a_n')$ 의 관계식을 구할 수 있다. 따라서 식

(2.21) 을 구할 수 있다.

$$\begin{aligned} \Lambda\{\tilde{a}^{(n)} - \tilde{a}^{(n)}a_n'\} &\le \Lambda\{\tilde{a}^{(n+1)}\} + \Lambda\{\tilde{a}^{(n)}a_n'\} \\ n+1 &\le \Lambda\{\tilde{a}^{(n+1)}\} + r \\ \Lambda\{\tilde{a}^{(n+1)}\} &\ge (n+1) - r \end{aligned} \qquad (2.21)$$

(증명완료)

(정리 2.9) $0 \le m \le n$ 인 경우, $<c(D), r>$ 이 $\tilde{a}^{(n+1)}$ 을 생성하지 못하지만 $\tilde{a}^{(n)}$ 을 생성하고 ($\delta_n \neq 0$), $<c^*(D), r'>$ 이 $\tilde{a}^{(m+1)}$ 을 생성하지 못하지만 $\tilde{a}^{(m)}$ 을 생성 ($\delta_m \neq 0$) 할 수 있다면 $<c(D) - \frac{\delta_n}{\delta_m} D^{n-m} c^*(D)\ ,\ Max(r, r'+n-m)>$ 은 $\tilde{a}^{n+1}$ 을 생성한다.

(증명) 가정으로부터 식 (2.22) 의 관계식을 구할 수 있다.

$$\begin{aligned} R_{D^{n+1}}[c(D)a(D)\ ] &= P(D) + \delta_n D^n \\ R_{D^{n+1}}[c^*(D)a(D)\ ] &= P^*(D) + \delta_m D^m \\ R_{D^{n+1}}[D^{n-m}c^*(D)a(D)\ ] &= R_{D^{n+1}}[D^{n-m}(P^*(D) + \delta_m D^m)\ ] \\ &= [D^{n-m}P^*(D) + \delta_m D^n\ ] \end{aligned} \qquad (2.22)$$

식 (2.22) 로 부터 식 (2.23) 을 얻을 수 있다.

$$R_{D^{n+1}}\left\{\frac{\delta_n}{\delta_m} D^{n-m} c^*(D)a(D)\right\} = \frac{\delta_n}{\delta_m} D^{n-m} P^*(D) + \delta_n D^n \qquad (2.23)$$

식 (2.22)와 식 (2.23) 으로 부터 식 (2.24) 을 구할 수 있다.

$$\begin{aligned} & R_{D^{n+1}}\left\{c(D)a(D) - \frac{\delta_n}{\delta_m} D^{n-m} c^*(D)a(D)\ \right\} \\ &= R_{D^{n+1}}\left\{\left\{c(D) - \frac{\delta_n}{\delta_m} D^{n-m} c^*(D)\right\} a(D)\ \right\} \\ &= R_{D^{n+1}}\{c(D)a(D)\} - R_{D^{n+1}}\left\{\frac{\delta_n}{\delta_m} D^{n-m} c^*(D)a(D)\ \right\} \\ &= P(D) + \delta_n D^n - \left(\frac{\delta_n}{\delta_m} D^{n-m} P^*(D) + \delta_n D^n\right) \\ &= P(D) - \frac{\delta_n}{\delta_m} D^{n-m} P^*(D) \end{aligned} \qquad (2.24)$$

식 (2.24) 의 우변항의 차수는 $Max\{r, r'+n-m\}$ 이다. 그러므로 $<c(D) - \frac{\delta_n}{\delta_m} D^{n-m} c^*(D),\ Max(r, r'+n-m)>$ 은 계열 $\tilde{a}^{(n+1)}$ 을 생성한다.

(증명완료)

(정리 2.10) $<c(D), r>$ 이 $\tilde{a}^{(n+1)}$ 을 생성하지 못하지만 $\tilde{a}^{(n)}$ 을 생성하고 ($\delta_n \neq 0$), $0 \le m \le n$ 이고 $\Lambda\{\tilde{a}^{(m+1)}\} > \Lambda\{\tilde{a}^{(m)}\}$ 인 m 이 존재한다면 $\Lambda\{\tilde{a}^{(n+1)}\} \le Max[\Lambda\{\tilde{a}^{(n)}\}, \Lambda\{\tilde{a}^{(m)}\} + n - m]$ 이다. 정리 2.9의 결과를 적용하면 자명하다.

(정리 2.11) 단계 m 에서 복잡도가 증가하여 그후 n 까지 복잡도의 증가가 없다는 가정하에서, $r = \Lambda\{\tilde{a}^{(n)}\}$ 인 $<c(D), r>$ 이 $\tilde{a}^{(n+1)}$ 을 생성하지 못하지만 $\tilde{a}^{(n)}$ 을 생성하면 $\Lambda\{\tilde{a}^{(n+1)}\} = Max\{\Lambda\{\tilde{a}^{(n)}\},\ n+1-\Lambda\{\tilde{a}^{(n)}\}\}$ 이다.

(증명) $0 \le m \le n$ 이고 $\Lambda\{\tilde{a}^{(m+1)}\} > \Lambda\{\tilde{a}^{(m)}\}$ 인 m 이 존재하고, 정리 2.11 이 성립한다고 가정한다. 그러면 $\Lambda\{\tilde{a}^{(m+1)}\}$ 은 $\Lambda\{\tilde{a}^{(m+1)}\}$ 이 $m/2$ 보다 작기 때문에 식 (2.25) 와 같다.

$$\begin{aligned}\Lambda\{\tilde{a}^{(m+1)}\} &= Max\{\Lambda\{\tilde{a}^{(m)}\}, m+1-\Lambda\{\tilde{a}^{(m)}\}\} \\ &= m+1-\Lambda\{\tilde{a}^{(m)}\} \\ &= \Lambda\{\tilde{a}^{(n)}\}\end{aligned} \qquad (2.25)$$

따라서 식 (2.25) 로 부터 식 (2.26)을 구할 수 있다.

$$n+1-\Lambda\{\tilde{a}^{(n)}\} = \Lambda\{\tilde{a}^{(m)}\}+n-m \qquad (2.26)$$

한편 정리 2.10 에 의하여 식 (2.27) 이 만족한다.

$$\begin{aligned}\Lambda\{\tilde{a}^{(n+1)}\} &\le Max[\Lambda\{\tilde{a}^{(n)}\}, \Lambda\{\tilde{a}^{(m)}\}+n-m] \\ &= Max[\Lambda\{\tilde{a}^{(n)}\}, (n+1)-\Lambda\{\tilde{a}^{(n)}\}]\end{aligned} \qquad (2.27)$$

일반적으로 식 (2.28) 은 성립한다.

$$\Lambda\{\tilde{a}^{(n+1)}\} \ge \Lambda\{\tilde{a}^{(n)}\} \qquad (2.28)$$

정리 2.8에 의해 다음의 결과를 구할 수 있다.

$$\Lambda(\tilde{a}^{(n+1)}) \ge (n+1)-\Lambda(\tilde{a}^{(n)}) \qquad (2.29)$$

식 (2.27), (2.28), (2.29) 로 부터 $\Lambda\{\tilde{a}^{(n+1)}\} = Max\{\Lambda\{\tilde{a}^{(n)}\}, n+1-\Lambda\{\tilde{a}^{(n)}\}\}$ 을 구할 수 있다. (증명완료)

지금까지 기술된 정리들을 바탕으로 그림 2.1과 같은 LFSR 합성 알고리듬을 유도할 수 있다.

(예제 2.1) 그림 2.1과 같은 LFSR 합성알고리듬을 이용하여 $N=7$, $\tilde{a}^{(7)}=(1101001)$인 최소의 길이의 LFSR 은 표 2.1 과 같이 구할 수 있다. $N=7$, $\tilde{a}^{(7)}=(1101001)$을 생성하는 최소길이의 LFSR 은 $1+D+D^3$ 이고 초기치는 (110) 이다.

표 2.1 LFSR 합성알고리듬 적용예

n	a_n	δ	$T(D)$	$c(D)$	r	$c^*(D)$	δ^*	x
-	-	-	-	1	0	1	1	1
0	1	1	1	$1+D$	1	1	1	1
1	1	0	1	$1+D$	1	1	1	2
2	0	1	$1+D$	$1+D+D^2$	2	$1+D$	1	1
3	1	0	$1+D$	$1+D+D^2$	2	$1+D$	1	2
4	0	1	$1+D+D^2$	$1+D+D^3$	3	$1+D+D^2$	1	1
5	0	1	$1+D+D^2$	$1+D+D^3$	3	$1+D+D^2$	1	2
6	1	0	$1+D+D^2$	$1+D+D^3$	3	$1+D+D^2$	1	3

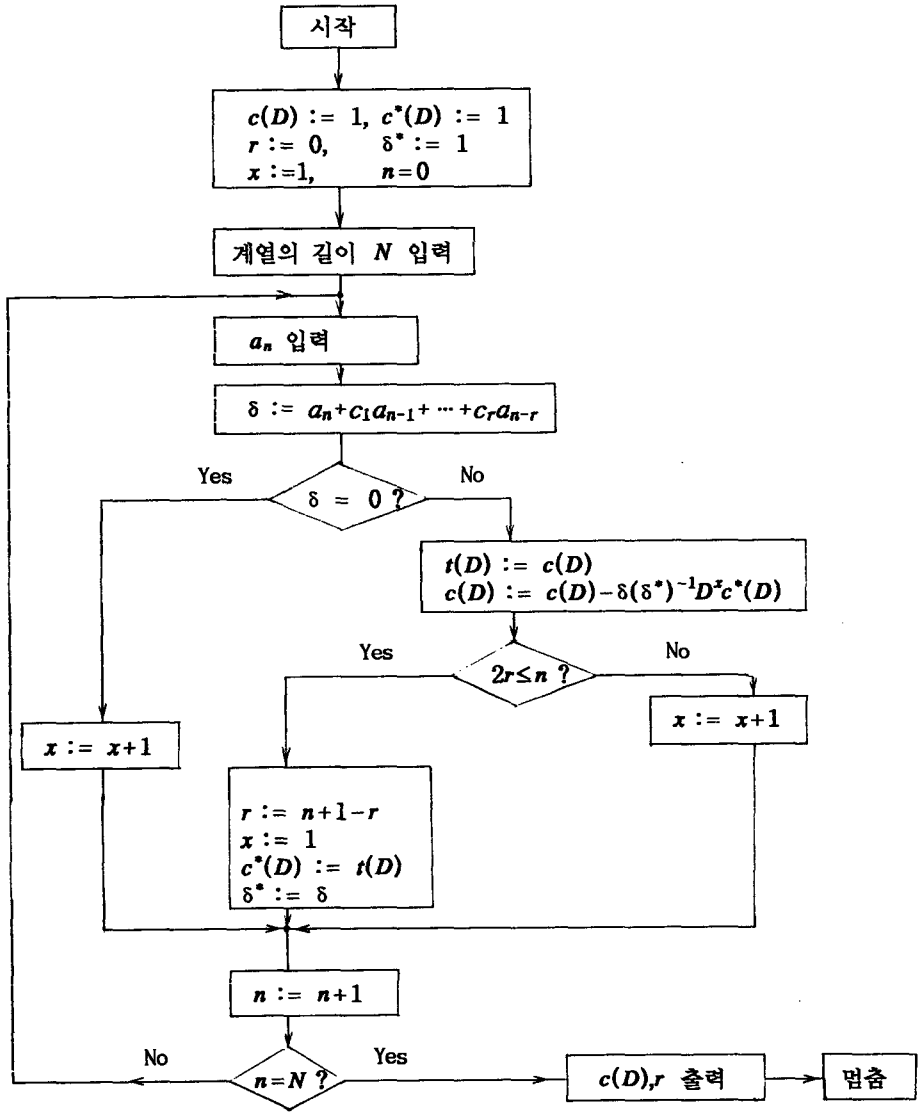

그림 2.1 Berlekamp-Massey LFSR 합성 알고리듬

3. 비선형 난수 계열의 특성

3.1 동일한 LFSR 계열을 위상 지연시킨 계열간의 비선형 결합에 의한 랜덤 계열

본 절에서는 동일한 LFSR 계열을 지연시킨 계열들을 비선형 함수를 이용하여 결합한 경우의 선형복잡도와 주기 등의 특성을 분석한다.[7] 동일한 LFSR 계열을 지연시킨 계열들을 비선형 함수를 이용하여 결합한 계열은 그림 3.1과 같다.

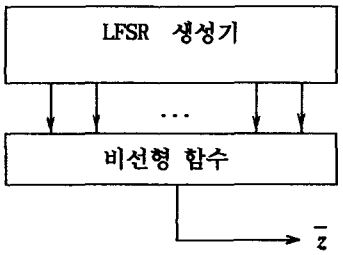

그림 3.1 비선형 함수를 이용한 출력 계열

LFSR 계열의 요소는 식 (2.8)과 같고, 이를 k 번 지연된 요소는 식 (3.1) 과 같다.

$$\begin{aligned} a_{n+k} &= \sum_{i=1}^{r-1} A_i(\alpha^{2^i})^{n+k} \\ &= \sum_{i=0}^{r-1} A_i(\alpha^{2^i})^k(\alpha^{2^i})^n \\ &= \sum_{i=0}^{r-1} A_i^*(\alpha^{2^i})^n \end{aligned} \tag{3.1}$$

(정리 3.1) 원래의 계열과 이를 k 번 지연한 계열을 논리 곱한 계열 $\bar{z}$ 의 선형 복잡도 $\Lambda(\bar{z})$ 는 식 (3.2)와 같다.

$$\begin{aligned} \Lambda(\bar{z}) &= \sum_{i=1}^{2}\binom{r}{i} \\ &= r+\frac{r(r-1)}{2} \\ &= \frac{r(r+1)}{2} \end{aligned} \tag{3.2}$$

(증명) 원래의 계열과 이를 k 번 지연한 계열을 논리 곱한 계열 $\bar{z}$ 의 요소 z_n 은 식 (3.3)과 같다.

$$\begin{aligned} z_n &= a_n a_{n+k} \\ &= \sum_{i=1}^{r-1}\sum_{j=1}^{r-1} A_iA_i^*(\alpha^{2^i+2^j})^n \end{aligned} \tag{3.3}$$

식 (3.3)의 α 의 지수부는 2^i+2^j 이고, 계수는 $A_iA_j^*$ 이다. 만약 $i=j$ 인 경우, 지수부는 2^{i+1} 이 되고 계수는 $A_iA_j^*=A_i^2(\alpha^{2^i})^k$ 이 되어 절대 0 이 되지 않는다. 만약 $i\neq j$ 인 경우, (i,j) 와 (j,i) 도 같은 지수부 2^i+2^j 가 되며 계수는 $A_iA_j^*+A_jA_i^*$ 이 된다. 그런데 $i\neq j$ 인 경우, $A_iA_j^*\neq A_jA_i^*$ 이 되어 절대 0 이 되지 않는다. 따라서 항의 수는 모두 $\sum_{1}^{2}\binom{l}{i} = \frac{r(r+1)}{2}$ 이

되므로 선형 복잡도는 식 (3.2)와 같다. (증명완료)

(예 3.1) 선형 재귀 방정식이 $a_n+a_{n-2}+a_{n-3}=0$, $n\geq 3$인 경우 특성 방정식은 x^3+x+1 이 된다. 이 특성방정식의 근을 α 라 하면 $\alpha^3+\alpha+1=0$을 이용하여 $GF(2^3)$ 을 생성할 수 있다. 따라서 계열 요소 a_n 은 다음과 같다.

$$a_n = A_1\alpha^n+A_2\alpha^{2n}+A_3\alpha^{4n}$$

LFSR 계열의 초기치를 $a_0=1, a_1=0, a_2=0$일 경우 다음의 관계식을 구할 수 있다.

$$\begin{aligned} a_0 &= A_1+A_2+A_3 &&= 1\\ a_1 &= A_1\alpha+A_2\alpha^2+A_3\alpha^4 &&= 0\\ a_2 &= A_1\alpha^2+A_2\alpha^4+A_3\alpha^8 &&= 0 \end{aligned}$$

윗식을 풀면 $A_1=A_2=A_3=1$ 을 구할 수 있다. 따라서 요소 a_n 은 다음과 같다.

$$a_n = \alpha^n+\alpha^{2n}+\alpha^{4n}$$

이 계열보다 시간적으로 1 뒤진 계열의 요소 a_{n+1} 은 다음과 같다.

$$a_{n+1} = \alpha\alpha^n+\alpha^2\alpha^{2n}+\alpha^4\alpha^{4n}$$

원래의 계열과 1 지연된 계열의 곱계열 $\overline{z}$ 의 요소 z_n 은 다음과 같다.

$$\begin{aligned} z_n &= (\alpha^n+\alpha^{2n}+\alpha^{4n})(\alpha\alpha^n+\alpha^2\alpha^{2n}+\alpha^4\alpha^{4n})\\ &= \alpha^4\alpha^n+\alpha\alpha^{2n}+\alpha^2\alpha^{4n}+\alpha^4\alpha^{3n}+\alpha\alpha^{6n}+\alpha^2\alpha^{5n} \end{aligned}$$

따라서 0 이 아닌 항의 갯수가 6 이 되어 정리 3.1의 이론치와 일치함을 알 수 있다. 한편 $\alpha^3,\alpha^5,\alpha^6$ 의 최소다항식 (minimum polynomial) 은 다음과 같다.

$$(x+\alpha^3)(x+\alpha^5)(x+\alpha^6) = x^3+x^2+1$$

따라서 곱계열 $\overline{z}$ 의 선형 등가 LFSR 은 다음과 같은 특성방정식 $m(x)$ 에 의해 생성될 수 있다.

$$(x^3+x^2+1)(x^3+x+1) = x^6+x^5+x^4+x^3+x^2+x+1$$

(정리 3.2) m ($<r$) 개의 지연 계열 모두를 곱하여 생성된 계열 $\overline{z}$ 의 최대 가능한 선형 복잡도는 식 (3.4)와 같으며, $m=r$ 인 경우의 계열의 최대 가능한 선형 복잡도는 계열의 주기 2^r-1 이하이다.

$$\Lambda(\overline{z}) = \sum_{i=1}^{m}\binom{r}{i} \qquad (3.4)$$

(증명) m 개의 지연 계열 모두를 곱하여 생성된 계열의 요소 z_n 은 식 (3.5) 와 같이 표현된다.

$$\begin{aligned} z_n &= a_{n+k_1}a_{n+k_2}\cdots a_{n+k_m}\\ &= \sum_{i_1=0}^{r-1}A_{i_1}(\alpha^{2^{i_1}})^n \cdots \sum_{i_m=0}^{r-1}A_{i_m}(\alpha^{2^{i_m}})^n\\ &= \sum_{i_1=0}^{r-1}\cdots\sum_{i_m=0}^{r-1}A_{i_1}(\alpha^{2^{i_1}})^n\cdots A_{i_m}(\alpha^{2^{i_m}})^n\\ &= \sum_{i_1=0}^{r-1}\cdots\sum_{i_m=0}^{r-1}A_{i_1}\cdots A_{i_m}(\alpha^{2^{i_1}+\cdots+2^{i_m}})^n \end{aligned} \qquad (3.5)$$

식 (3.5)의 지수부는 임의의 정수 l 로 표현될 수 있다.

$$l = 2^{t_1}+\cdots+2^{t_m} \qquad (3.6)$$

만약 식 (3.5)의 계수부가 모두 0 이 아니라면 서로 다른 항의 갯수는 식 (3.6) 의 r 개의 위치에서 최소 1 에서 m 개를 순서에 관계없이 고르는 경우의 수가 될 것이다. 따라서 곱계열의 최대 선형 복잡도는 식 (3.4)와 같음을 알 수 있다. 그리고 $m=r$ 인 경우 최대 가능한 선형복잡도는 $\Lambda(\bar{z}) = \sum_{i=1}^{r}\binom{r}{i} = 2^r-1$ 이 된다. (증명완료)

(예 3.2) 재귀 귀환 방정식이 $a_n+a_{n-3}+a_{n-4}=0,\ n\geq 4$인 경우 특성 방정식은 x^4+x+1 이 된다. 이 특성 방정식의 근을 α 라 하면 $\alpha^4+\alpha+1=0$을 이용하여 $GF(2^4)$ 을 생성할 수 있다. 따라서 계열 요소 a_n 은 다음과 같다.

$$a_n = A_1\alpha^n+A_2\alpha^{2n}+A_3\alpha^{4n}+A_4\alpha^{8n} \qquad (3.7)$$

LFSR 계열의 초기치를 $a_0=1,a_1=0,a_2=0,a_3=0$일 경우 다음의 관계식을 구할 수 있다.

$$\begin{aligned}
a_0 &= A_1+A_2+A_3+A_3 &&= 1\\
a_1 &= A_1\alpha+A_2\alpha^2+A_3\alpha^4+A_4\alpha^8 &&= 0\\
a_2 &= A_1\alpha^2+A_2\alpha^4+A_3\alpha^8+A_4\alpha^{16} &&= 0\\
a_3 &= A_1\alpha^3+A_2\alpha^6+A_3\alpha^{12}+A_4\alpha^9 &&= 0
\end{aligned}$$

윗식을 풀면 $A_1=\alpha^{14},A_2=\alpha^{13},A_3=\alpha^{11},A_4=\alpha^7$ 을 구할 수 있다. 따라서 요소 a_n 은 다음과 같다.

$$a_n = \alpha^{14}\alpha^n+\alpha^{13}\alpha^{2n}+\alpha^{11}\alpha^{4n}+\alpha^7\alpha^{8n}$$

이 계열보다 시간적으로 1 뒤진 계열의 요소 a_{n+1} 과 2 뒤진 계열의 요소 a_{n+2} 는 각각 다음과 같다.

$$\begin{aligned}
a_{n+1} &= \alpha^n+\alpha^{2n}+\alpha^{4n}+\alpha^{8n}\\
a_{n+3} &= \alpha^2\alpha^n+\alpha^4\alpha^{2n}+\alpha^8\alpha^{4n}+\alpha\alpha^{8n}
\end{aligned}$$

원래의 계열과 1 지연된 계열의 곱계열 $\bar{z}$ 의 요소 z_n 은 다음과 같다.

$$\begin{aligned}
z_n &= a_n a_{n+1} a_{n+3}\\
&= (\alpha^{14}\alpha^n+\alpha^{13}\alpha^{2n}+\alpha^{11}\alpha^{4n}+\alpha^7\alpha^{8n})(\alpha^n+\alpha^{2n}+\alpha^{4n}+\alpha^{8n})(\alpha^2\alpha^n+\alpha^4\alpha^{2n}+\alpha^8\alpha^{4n}+\alpha\alpha^{8n})\\
&= \alpha^{13}\alpha^n+\alpha^{11}\alpha^{2n}+\alpha^7\alpha^{4n}+\alpha^{14}\alpha^{8n}+\alpha^8\alpha^{5n}+\alpha\alpha^{7n}+\alpha^9\alpha^{10n}++\alpha^8\alpha^{11n}+\alpha^3\alpha^{13n}+\alpha^2\alpha^{14n}
\end{aligned}$$

따라서 0 이 아닌 항의 갯수가 10 이 되어 곱계열 $\bar{z}$ 의 선형복잡도는 10 이 된다. 따라서 이론적인 최대 복잡도 10 보다 4 작은 값이 된다.

한편 α^5,α^{10} 의 최소 다항식 (minimum polynomial) 과 $\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}$ 의 최소 다항식 (minimum polynomial) 은 각각 다음과 같다.

$$(x+\alpha^5)(x+\alpha^{10}) = x^2+x+1$$
$$(x+\alpha^7)(x+\alpha^{14})(x+\alpha^{13})(x+\alpha^{11}) = x^4+x^3+1$$

따라서 곱계열 $\bar{z}$ 의 선형 등가 LFSR 은 다음과 같은 식 (3.8) 에 의해 생성될 수 있다.

$$(x^4+x+1)(x^2+x+1)(x^4+x^3+1) = x^{10}+x^5+1 \qquad (3.8)$$

(정리 3.3) 차수가 r 인 원시다항식을 이용하여 생성된 LFSR 계열의 각단 신호를 $\bar{a}_1, \bar{a}_2, \cdots, \bar{a}_r$ 이라 하면, 각단의 출력을 모두 곱한 출력 계열의 선형 복잡도는 2^r-1 이다.
(증명생략)

(정리 3.4) 단수가 r 인 원시다항식에 의해 생성된 원래의 LFSR 계열을 $\bar{a}_0$ 라 하고, $\bar{a}_0$ 를 $t_i(i=1,\cdots,k)$ 회 지연시킨 계열을 $\bar{a}_{t_i}$ 라 할 경우, k 개의 서로 다른 위상을 k 차의 비선형 함수로 결합시켜서 생성된 출력 계열 $\bar{z}$ 의 선형복잡도 $\Lambda(\bar{z})$ 는 식 (3.9) 로 상한된다.

$$\Lambda(\bar{z}) \le \sum_{i=1}^{k}\binom{r}{i} \tag{3.9}$$

(증명) 최대장 계열을 지연한 계열 $\bar{a}_{t_i}$ 는 $\bar{a}_0, \bar{a}_1, \cdots, \bar{a}_{r-1}$ 의 선형 결합에 의해 표현될 수 있다. 따라서 출력계열은 식 (3.10)과 같다.

$$\begin{aligned}\bar{z} &= f(\bar{a}_{t_1}, \bar{a}_{t_2}, \cdots, \bar{a}_{t_k}) \\ &= f(\sum_{i=0}^{r-1} l_{1,i}\,\bar{a}_i, \cdots, \sum_{i=0}^{r-1} l_{k,i}\,\bar{a}_k) \\ &= f(\sum_{i=0}^{r-1} l_i'\,\bar{a}_i)\end{aligned} \tag{3.10}$$

여기서 $l_{j,i}$, l_i' 은 선형 결합 계수이다. 따라서 비선형함수의 차수가 k 이므로 (정리 3.2) 에 의하여 출력 계열 $\bar{z}$ 의 선형 복잡도는 식 (3.9)와 같다. (증명완료)

(정리 3.5) 계열 $\bar{a}$ 가 단수가 r 인 원시다항식에 의해 생성되는 LFSR 계열이며, $\bar{a}_0$ 를 $t_i(i=1,\cdots,k)$ 회 지연시킨 계열을 $\bar{a}_{t_i}$ 라 할 경우, 출력 계열 $\bar{z}(=\prod_{i=1}^{k}\bar{a}_{t_i})$ 는 k 개의 서로 다른 위상을 가진 출력 계열을 k 차의 논리곱으로 결합시켜서 얻어진다. 지수부 e 의 이진 중(binary weight) 이 k 인 $GF(2^r)$ 상의 임의의 원소 α^e 는 $\bar{z}$ 를 생성하는 특성방정식의 근일 필요충분 조건은 식 (3.11)과 같이 정의된 판별식 D_e 가 0 이 아닌 것이다.

$$D_e = \begin{vmatrix} \alpha^{t_1 2^{e_1}} & \cdots & \alpha^{t_k 2^{e_1}} \\ \alpha^{t_1 2^{e_2}} & \cdots & \alpha^{t_k 2^{e_2}} \\ & \cdots & \\ \alpha^{t_1 2^{e_k}} & \cdots & \alpha^{t_k 2^{e_k}} \end{vmatrix} \tag{3.11}$$

여기서 $e = 2^{e_1}+2^{e_2}+\cdots+2^{e_k}$, $0 \le e_1 < e_2 < \cdots < e_k < r$ 이다.

(증명) 출력 계열 $\bar{a}_0$ 의 요소 a_n 은 식 (3.12)와 같이 표현될 수 있다.

$$\begin{aligned}a_n &= tr_1^r(\alpha^n) \\ &= \alpha^n+\alpha^{2n}+\cdots+\alpha^{2^{r-1}n}\end{aligned} \tag{3.12}$$

이를 t_i 회 지연시킨 계열의 계열 요소 a_{n,t_i} 는 식 (3.13)과 같다.

$$a_{n,t_i} = tr_1^r(\alpha^{t_i}\alpha^n) = (\alpha^{t_i}\alpha)^n+(\alpha^{t_i}\alpha)^{2n}+\cdots+(\alpha^{t_i}\alpha)^{2^{r-1}n} \quad (3.13)$$

따라서 $\bar{z}$ 의 출력 요소 z_n 은 식 (3.14) 와 같이 표현될 수 있다.

$$z_n = a_{n,t_1}a_{n,t_2}\cdots a_{n,t_k} = \prod_{i=1}^{k} tr_1^r(\alpha^{t_i}\alpha^n) = \prod_{i=1}^{k}\left\{(\alpha^{t_i}\alpha)^n+(\alpha^{t_i}\alpha)^{2n}+\cdots+(\alpha^{t_i}\alpha)^{2^{r-1}n}\right\} \quad (3.14)$$

식 (3.14)은 중이 k 인 항들의 합과 k 이하인 항들의 합으로 구성된다. 이를 분리하여 구성하면 식 (3.15)와 같다.

$$z_n = \sum_{\{e:w_2(e)<k\}} A_e\alpha^{ej} + \sum_{\{e:w_2(e)=k\}} D_e\alpha^{ej} \quad (3.15)$$

식 (3.15)의 오른쪽 항에서 지수부의 항의 갯수는 $\binom{r}{k}$ 이므로 전체 항의 갯수도 $\binom{r}{k}$이다. 특정 지수부의 값이 결정된후 이 지수부에 기여하는 서로 다른 멱들의 갯수는 $k!$ 이다. 따라서 α^{en} 에 대응되는 계수 D_e 는 식 (3.16) 과 같이 표현될 수 있다.

$$D_e = \sum_{m\in\overline{P}} (\alpha^{t_1})^{2^{m_1}}(\alpha^{t_2})^{2^{m_2}}\cdots(\alpha^{t_k})^{2^{m_k}} \quad (3.16)$$

여기서 $e=(e_1,e_2,\cdots,e_k)$ 이고, $\overline{P}$ 는 중이 k 인 e 가 주어졌을 경우 모든 중들의 순열인 $k!$ 개의 집합 $\{(e_{1,1},e_{2,1},\cdots,e_{k,1}),\cdots,(e_{1,k!},e_{2,k!},\cdots,e_{k,k!})\}$ 을 의미한다. 식 (3.16) 은 식 (3.17) 과 등가이다.

$$D_e = \begin{vmatrix} \alpha^{t_1 2^{m_1}} & \cdots & \alpha^{t_k 2^{m_1}} \\ \alpha^{t_1 2^{m_2}} & \cdots & \alpha^{t_k 2^{m_2}} \\ & \cdots & \\ \alpha^{t_1 2^{m_k}} & \cdots & \alpha^{t_k 2^{m_k}} \end{vmatrix} \quad (3.17)$$

따라서 $D_e\neq 0$ 인 α^e 는 z_n 의 항으로 항으로 남게되어 $\bar{z}$ 의 특성방정식 $m_{\bar{z}}(x)$ 의 근이 되므로 선형복잡도에 기여한다.

(증명완료)

(예 3.3) 특성방정식이 $m(x)=x^4+x^3+1$ 인 LFSR 계열의 출력계열을 2번 지연시킨 계열과 원래 계열을 논리곱한 계열이 $GF(2^4)$ 상의 원소 α^3, α^5 을 갖는지 여부를 살펴보자.

α^3 의 지수부는 $e=3=2^0+2^1$이므로 판별식 D_3 은 다음과 같다.

$$D_3 = \begin{vmatrix} 1 & \alpha^2 \\ 1 & \alpha^4 \end{vmatrix} \neq 0$$

α^5 의 지수부는 $e=5=2^0+2^2$이므로 판별식 D_5 은 다음과 같다.

$$D_5 = \begin{vmatrix} 1 & \alpha^2 \\ 1 & \alpha^8 \end{vmatrix} \neq 0$$

따라서 α^3,α^5 은 논리곱 계열의 근이다. α^3 의 공액근은 $\{\alpha^6,\alpha^9,\alpha^{12}\}$ 이고, α^5 의 공액근이 $\{\alpha^{10}\}$ 임을 고려하면 곱계열의 특성방정식은 다음과 같고, 선형복잡도는 6 임을 알 수 있다.

$$\begin{aligned} m_{\bar{z}}(x) &= (x^4+x^3+x^2+x+1)(x^2+x+1) \\ &= x^6+x^4+x^3+x^2+1 \end{aligned} \tag{3.18}$$

(정리 3.6) 차수가 r 인 원시다항식에 의해 생성되는 최대장계열을 $\gcd(d,2^r-1)=1$ 인 등간격 d 로 지연한 계열을 k 차원 함수로 논리곱한 출력계열 $\bar{z}(=\bar{a}_t\ \bar{a}_{t+d}\cdots\bar{a}_{t+(k-1)d})$ 의 선형복잡도는 적어도 $\binom{r}{k}$ 이다. 즉, 중이 $w_2(e)=k$ 인 $GF(2^r)$ 상의 원소 α^e 는 계열의 특성방정식의 근이다.

(증명) 일반성의 결여없이 k 차의 논리곱 계열 $\bar{z}$ 는 식 (3.9) 와 같다.

$$\bar{z} = \bar{a}_t\ \bar{a}_{t+d}\cdots\bar{a}_{t+(k-1)d} \tag{3.19}$$

식 (3.19)와 같은 계열의 중이 k 인 지수부를 갖는 α^e 의 판별식은 식 (3.20)과 같다.

$$\begin{aligned} D_e &= \begin{vmatrix} \alpha^{t_1 2^{n_1}} & \cdots & \alpha^{t_k 2^{n_1}} \\ \alpha^{t_1 2^{n_2}} & \cdots & \alpha^{t_k 2^{n_2}} \\ \cdots & & \\ \alpha^{t_1 2^{n_k}} & \cdots & \alpha^{t_k 2^{n_k}} \end{vmatrix} = \begin{vmatrix} 1 & \cdots & \alpha^{(k-1)d 2^{n_1}} \\ 1 & \cdots & \alpha^{(k-1)d 2^{n_2}} \\ \cdots & & \\ 1 & \cdots & \alpha^{(k-1)d 2^{n_k}} \end{vmatrix} \\ &= \prod_{i=2}^{k-1}\prod_{j=1}^{i-1}(\alpha^{id2^{n_i}}-\alpha^{jd2^{n_j}}) \end{aligned} \tag{3.20}$$

식 (3.20)은 Vandermonde 의 행렬식이다. 따라서 $\gcd(d,2^r-1)=1$ 이고, $e_i\neq e_j,\ i\neq j$ 이므로 식 (3.20) 은 절대로 0 이 될 수 없다. 중이 $w_2(e)=k$ 인 $GF(2^r)$ 상의 원소 α^e 는 계열의 특성방정식의 근이다. 그러므로 출력 계열 $\bar{z}$ 의 선형복잡도는 적어도 $\binom{r}{k}$ 이다. (증명완료)

(정리 3.7) 차수가 r 인 원시다항식에 의해 생성되는 최대장계열을 $\gcd(d,2^r-1)=1$ 인 등간격 d 로 지연한 계열을 식 (3.21) 과 같이 선형 결합한 출력 계열 $\bar{z}$ 의 선형복잡도 $\Lambda(\bar{z})$ 는 최소로 $\binom{r}{k}-(N-1)$ 이상이다.

$$\bar{z}=\sum_{i=1}^{N-1} l_i\ \bar{a}_t\ \bar{a}_{t+d}\cdots\bar{a}_{t+(k-1)d} \tag{3.21}$$

여기서 N 은 정수이고 l_i 는 모두 0 이 아니다.

(증명) 식 (3.21)에서 하나의 차수가 k 인 곱항은 식 (3.22) 와 같이 표현될 수 있다.

$$\bar{z}^{(i)} = \bar{a}_t\ \bar{a}_{t+d}\cdots\bar{a}_{t+(k-1)d} \tag{3.22}$$

식 (3.22) 에서의 하나의 차수가 k 인 곱항의 계열요소는 식 (3.23) 과 같다.

$$z_n^{(i)} = \sum_{\{e:w_2(e)<k\}} A_e^{(i)}\alpha^{ej} + \sum_{\{e:w_2(e)=k\}} D_e^{(i)}\alpha^{ej} \tag{3.23}$$

식 (3.23) 에서 왼쪽항의 첫번째 계수는 식 (3.24)와 같다.

$$D_e^{(0)} = \begin{vmatrix} 1 & \cdots & \alpha^{(k-1)d2^m} \\ 1 & \cdots & \alpha^{(k-1)d2^m} \\ & \cdots & \\ 1 & \cdots & \alpha^{(k-1)d2^m} \end{vmatrix}_{k-1} = \prod_{i=2}^{k-1}\prod_{j=1}^{i-1}(\alpha^{id2^m} - \alpha^{jd2^m}) \tag{3.24}$$

식 (3.23)의 계수 $D_e^{(i)}$ 는 $D_e^{(0)}$ 로 식 (3.25)와 같이 표현된다.

$$D_e^{(i)} = \begin{vmatrix} \alpha^{i2^m} & \cdots & \alpha^{[i+(k-1)d]2^m} \\ \alpha^{i2^m} & \cdots & \alpha^{[i+(k-1)d]2^m} \\ & \cdots & \\ \alpha^{i2^m} & \cdots & \alpha^{[i+(k-1)d]2^m} \end{vmatrix} = \alpha^{i(2^m+\cdots+2^m)} D_e^{(0)} = \alpha^{ik} D_e^{(0)} \tag{3.25}$$

식 (3.23) 은 식 (3.25)을 이용하여 식 (3.26) 과 같이 변경될 수 있다.

$$z_n^{(i)} = \sum_{\{e:w_2(e)<k\}} A_e^{(i)} \alpha^{ed} + \sum_{\{e:w_2(e)=k\}} \alpha^{ik} D_e^{(0)} \alpha^{ed} \tag{3.26}$$

따라서 각 k 차 곱항들의 선형 합에 의해 계열 $\bar{z}$ 의 계열요소 z_n 은 식 (3.27) 과 같이 표현될 수 있다.

$$\begin{aligned} z_n &= \sum_{i=0}^{N-1} l_i z_n^{(i)} \\ &= \sum_{i=0}^{N-1} \sum_{\{e:w_2(e)<k\}} l_i A_e^{(i)} \alpha^{ed} + \sum_{i=0}^{N-1} \sum_{\{e:w_2(e)=k\}} l_i \alpha^{ik} D_e^{(0)} \alpha^{ed} \\ &= \sum_{i=0}^{N-1} \sum_{\{e:w_2(e)<k\}} l_i A_e^{(i)} \alpha^{ed} + \sum_{\{e:w_2(e)=k\}} D_e^{(0)} \alpha^{ed} \sum_{i=0}^{N-1} l_i \alpha^{ik} \end{aligned} \tag{3.27}$$

식 (3.27)에서 $D_e^{(0)}$ 는 절대로 0 이 될 수 없다. α^e 가 $\sum_{i=0}^{N-1} c_i \alpha^{ik}$ 의 근이라면 식 (3.27)의 두번째 항은 0이 된다. 이를 만족하는 근은 많아야 $N-1$ 이므로 중이 k 인 지수부는 적어도 전체 갯수에서 $N-1$ 를 뺀 갯수가 식 (3.27) 의 두번째 항으로 남게 된다. 따라서 $\bar{z}$ 의 선형복잡도의 하한값은 식 (3.28)과 같다.

$$\Lambda(\bar{z}) \geq \binom{r}{k} - (N-1) \tag{3.28}$$

(증명완료)

이상의 정리들을 종합하면 비선형함수 f 가 임의로 선택된 k 차원 비선형함수라고 하면 동일계열을 일정 비트 지연한 계열간의 논리곱의 선형합으로 생성된 계열의 최대가능한 선형복잡도 Λ_{max} 는 식 (3.29) 와 같이 주어진다.

$$\Lambda_{max} = \sum_{i=1}^{k} \binom{r}{k} \tag{3.29}$$

길이가 Λ_{max} 인 선형 등가회로에 의해 생성되는 임의의 계열 $z(D)$ 는 식 (3.30)과 같이 멱급수 전개로 표현된다.

$$z(D) = \frac{p(D)}{m(D)} \tag{3.30}$$

여기서 $p(D)$ 의 차수는 Λ_{max} 미만이고, 등가 LFSR 계열의 특성방정식 $m(D)$ 의 차수는 Λ_{max} 이다. $m(D)$ 는 차수가 Λ_{max} 또는 Λ_{max} 의 약수인 기약다항식 (irreducible polynomial) $m_i(D)$ 에 의해 인수분해된다. 따라서 식 (3.30)의 $z(D)$ 는 식 (3.31) 과 같이 변경될 수 있다.

$$z(D) = \frac{p_1(D)}{m_1(D)} + \cdots + \frac{p_t(D)}{m_t(D)} \tag{3.31}$$

여기서 $m(D) = m_1(D)m_2(D)\cdots m_t(D)$ 이고, $m_i(D)$ 는 $m(D)$ 의 기약다항식인 약수이며, $p_i(D)$ 의 차수는 $m_i(D)$ 의 차수보다 작다. 따라서 모두 식 (3.31)의 모든 분자부의 다항식이 0 이 아닐 경우 선형 등가 LFSR 의 선형복잡도가 최대가 된다. 최대의 선형복잡도를 갖는 계열의 갯수는 모든 0 이 아닌 가능한 모든 $p_i(D)$ 의 갯수와 같다.

(정리 3.8) 차수가 소수 r 인 원시다항식에 의해 생성되는 최대장계열을 차수가 k 인 비선형함수로 결합했을 경우 최대 획득 가능한 선형복잡도는 $\sum_{i=1}^{k}\binom{r}{k}$ 이다. 임의로 선택된 비선형함수가 최대 선형 복잡도를 갖을 확률 P_{nl} 은 식 (3.32) 와 같이 하한된다.

$$P_{nl} = e^{-\left[\frac{\Lambda_{max}}{r2^r}\right]} > e^{-\frac{1}{r}} \tag{3.32}$$

(증명) r 이 소수라면 $GF(2^r)$ 상의 "1" 을 제외한 모든 원소는 정확히 차수가 r 인 특성방정식만을 갖는다. 따라서 $m_i(D)$ 의 차수는 r 이므로 인수분해되는 특성방정식의 인수는 정확히 Λ_{max}/r 개이다. 각 $m_i(D)$ 에 대한 "0" 이 아닌 $p_i(D)$ 의 경우의 수는 2^r-1 이다. 그러므로 각 $m_i(D)$ 에 대한 "0" 이 아닌 분자부를 갖을 확률은 $(2^r-1)/2^r$ 이다. 임의로 선택된 비선형함수가 최대 선형 복잡도를 갖을 확률 P_{nl} 은 모든 $m_i(D)$ 가 확률 $(2^r-1)/2^r$ 을 갖을 확률이다.

$$\begin{aligned} P_{nl} &= (1-\frac{1}{2^r})^{\frac{\Lambda_{max}}{r}} = (1-\frac{1}{2^r})^{2^r\cdot\frac{\Lambda_{max}}{r2^r}} \\ &= (\frac{1}{e})^{\frac{\Lambda_{max}}{r2^r}} = e^{-\frac{\Lambda_{max}}{r2^r}} \\ &> e^{-\frac{1}{r}} \end{aligned} \tag{3.33}$$

임의로 선택된 비선형함수가 최대 선형 복잡도를 갖지 못할 확률 $1-P_{nl}$ 은 모든 $m_i(D)$ 가 확률 $1/2^r$ 을 갖을 확률이다.

$$1-P_{nl} = 1-(1-\frac{1}{2^r})^{\frac{\Lambda_{max}}{r}} < 1-e^{-\frac{1}{r}} \tag{3.34}$$

(증명완료)

(정리 3.9) 차수가 소수 r 인 원시다항식에 의해 생성되는 최대장계열을 차수가 k 인 비선형 함

수로 결합했을 경우, 임의로 선택된 비선형함수가 $\sum_{i=1}^{k}\binom{r}{k}-r$ 을 가질 확률 P_1 은 식 (3.35) 와 같이 근사된다.

$$P_1 = \frac{\Lambda_{max}}{r} 2^{\frac{1}{r}} e^{-[\frac{\Lambda_{max}}{r2^r}]} \tag{3.35}$$

(증명) 비선형함수가 $\sum_{i=1}^{k}\binom{r}{k}-r$ 을 가질 확률 P_1 은 Λ_{max}/r 개의 $m_i(D)$ 에 대응되는 분자부증 한개가 $2^{1/r}$ 확률로, 나머지 $\Lambda_{max}/(r-1)$ 개가 $(1-1/2^r)$ 확률을 가질 경우이다. 따라서 P_1 은 식 (3.36) 과 같다.

$$\begin{aligned} P_1 &= \binom{\Lambda_{max}/r}{1} 2^{\frac{1}{r}} (1-\frac{1}{2^r})^{\frac{\Lambda_{max}}{r}-1} = \binom{\Lambda_{max}/r}{1} 2^{\frac{1}{r}} (1-\frac{1}{2^r})^{2^r\frac{\Lambda_{max}}{r2^r}} \\ &= \binom{\Lambda_{max}/r}{1} 2^{\frac{1}{r}} (\frac{1}{e})^{\frac{\Lambda_{max}}{r2^r}} = \frac{\Lambda_{max}}{r} 2^{\frac{1}{r}} e^{-\frac{\Lambda_{max}}{r2^r}} \end{aligned} \tag{3.36}$$

따라서 임의로 선택된 k 차 비선형 함수의 선형복잡도가 최대 가능한 선형 복잡도를 갖거나 $\sum_{i=1}^{k}\binom{r}{k}-r$ 을 가질 확률 P_2 는 식 (3.37) 과 같이 구해질 수 있다.

$$\begin{aligned} P_2 &= P_{nd}+P_1 \\ &= e^{-\frac{1}{r}} + \frac{\Lambda_{max}}{r} 2^{\frac{1}{r}} e^{-\frac{\Lambda_{max}}{r2^r}} \end{aligned} \tag{3.37}$$

(증명완료)

3.2 다른 LFSR 계열간의 비선형 결합에 의한 랜덤 계열

동일한 계열을 지연한 계열들간의 선형 결합으로 생성된 계열의 최대 선형 복잡도는 LFSR 의 단수가 r 인 경우 최대 2^r-1 이 된다. 따라서 큰 선형 복잡도를 갖는 계열은 그림 3.2 와 같이 여러개의 LFSR 계열을 비선형 함수를 이용하여 생성할 수 있다. 비선형 출력 계열은 다음과 같은 특성을 가져야 한다. ① 주기가 가능한 길어야 한다. ② 2.2 절의 LFSR 합성 알고리듬에 의한 공격을 피하기 의하여 큰 선형 복잡도를 가져야 한다. ③ 랜덤성 : "0" 비트와 "1" 비트의 발생 빈도수는 같아야 한다. ④ 최대 상관 면역성(correlation immunity) 를 가져야 한다. [8,9,11]

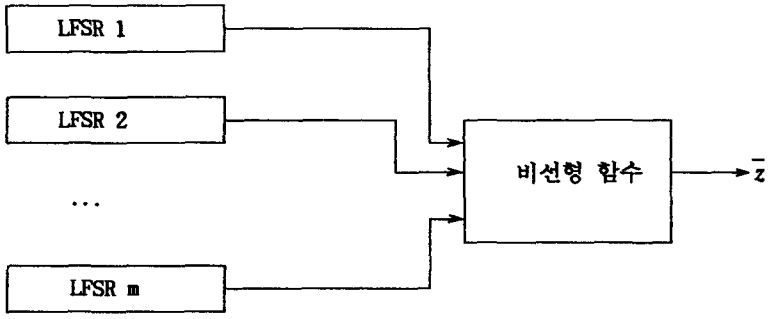

그림 3.2 다른 LFSR 계열간의 비선형 결합에 의한 랜덤 계열

(정리 3.10) LFSR 의 단수가 r,s 이고, 귀환다항식이 원시다항식이며, $\gcd(r,s)=1$ 인 경우, 각 LFSR 계열이 각각 $\overline{a},\overline{b}$ 라 하자. 두 계열의 곱계열 $\overline{z}$ 의 선형 복잡도 $\Lambda(\overline{z})$ 는 rs 이다.

(증명) $\gcd(r,s)=1$ 이므로 $GF(2^r)$ 과 $GF(2^s)$ 의 공통적인 부분체는 유일하게 $GF(2)$ 임을 알 수 있다. 만약 $\alpha_i(i=1,\cdots s)$ 를 계열 $\overline{a}$ 의 특성 다항식의 근이라 하고 $\beta_j(j=1,\cdots s)$ 를 계열 $\overline{b}$ 의 특성 다항식의 근이라 가정하자. 그러면 $\alpha_i(i=1,\cdots s)$, A_i 는 $GF(2^r)$ 에 포함되며, $\beta_j(j=1,\cdots s)$, B_j 는 $GF(2^s)$ 내에 포함된다. 계열 $\overline{a},\overline{b}$ 의 요소 a_n,b_n 는 식 (3.38) 과 같다.

$$\begin{aligned} a_n &= \sum_{i=1}^{r} A_i\alpha_i \\ &= A_1\alpha_1+A_2\alpha_2+\cdots+A_r\alpha_r \\ b_n &= \sum_{i=1}^{s} B_i\beta_i \\ &= B_1\beta_1+B_2\beta_2+\cdots+B_s\beta_s \end{aligned} \qquad (3.38)$$

곱계열 $\overline{z}$ 의 요소 z_n 은 식 (3.39)과 같다.

$$\begin{aligned} z_n &= a_nb_n \\ &= \sum_{i=1}^{r}\sum_{j=1}^{s} A_iB_j\alpha_i\beta_j \end{aligned} \qquad (3.39)$$

z_n 의 계수 A_iB_j 는 0 이 아니고, 각각의 $\alpha_i\beta_j$ 는 다음과 같은 이유로 서로 다르다. $GF(2^r)$ 상의 임의의 원소를 α 라 하고 $GF(2^s)$ 상의 임의의 원소를 β 라 가정한다. 만약 $\alpha\beta$ 가 $GF(2^r)$ 상의 원소라면 $\alpha^{-1}\alpha\beta=\beta\in GF(2^r)$ 이 되어 모순이 되며, 만약 $\alpha\beta$ 가 $GF(2^s)$ 상의 원소라면 $\beta^{-1}\alpha\beta=\alpha\in GF(2^r)$ 가 되어 모순이 된다. 따라서 $\alpha\beta$ 는 $GF(2^m)$ 상의 원소가 된다. 그리고 $\alpha_i\beta_j=\alpha_i\beta_{j'}(j\neq j')$ 이라면 양변에 α_i^{-1} 을 곱하면 $\beta_j=\beta_{j'}$ 이 되어 이는 모순이다. 따라서 곱해지는 모든 원소는 $GF(2^m)$ 상의 다른 원소들이 된다. 따라서 z_n 는 $GF(2^m)$ 상에서 rs 개의 항으로 표현된다. 그러므로 곱계열의 선형 복잡도는 rs 임을 알 수 있다. (증명완료)

(예 3.4) 두개의 특성 다항식이 각각 $x^2+x+1=0$, $x^3+x+1=0$이고, 첫번째 LFSR 의 초기치가 (10) 이고, 두번째 LFSR 의 초기치가 (100) 인 경우, 첫번째 LFSR 의 계열 요소 b_n 과 두번째 LFSR 의 계열 요소 a_n 은 다음과 같다.

$$\begin{aligned} b_n &= \beta^2\beta^n + \beta\beta^{2n} \\ a_n &= \alpha^n + \alpha^{2n} + \alpha^{4n} \end{aligned}$$

따라서 곱계열 $\overline{z}$ 의 요소 z_n 은 다음과 같다.

$$\begin{aligned} z_n &= a_nb_n \\ &= (\beta^2\beta^n+\beta\beta^{2n})(\alpha^n+\alpha^{2n}+\alpha^{4n}) \\ &= \beta^2(\alpha\beta)^n+\beta(\alpha\beta^2)^n+\beta^2(\alpha^2\beta)^n+\beta(\alpha^2\beta^2)^n+\beta^2(\alpha^4\beta)^n+\beta(\alpha^4\beta^2)^n \end{aligned}$$

따라서 곱계열의 근의 집합은 $\{\alpha\beta,\alpha\beta^2,\alpha^2\beta^2,\alpha^4\beta,\alpha^4\beta^2\}$ 이 된다. 이의 특성방정식을 구하면 다음과 같다.

$$\begin{aligned} m(x) &= (x+\alpha\beta)(x+\alpha\beta^2)(x+\alpha^2\beta)(x+\alpha^2\beta^2)(x+\alpha^4\beta)(x+\alpha^4\beta^2) \\ &= x^6+x^4+x^2+x+1 \end{aligned}$$

따라서 곱계열의 선형 등가 LFSR 은 $m(x) = x^6+x^4+x^2+x+1$ 로 실현되며, 초기치는 (100101) 이다.

(정리 3.11) 비선형 함수의 입력 계열 $\overline{a_i}$, (for $i=1,\cdots,m$) 의 특성다항식이 원시다항식이고, 원시다항식들의 차수와 지표들이 쌍으로 서로소 관계가 성립하면, 이들 계열의 이진합 계열과 논리곱 계열의 선형 복잡도는 식 (3.40) 과 같다.

$$\begin{aligned} \Lambda(\prod_{i=1}^{N}\overline{a_i}) &= \prod_{i=1}^{N}\Lambda(\overline{a_i}) \\ \Lambda(\sum_{i=1}^{N}\overline{a_i}) &= \sum_{i=1}^{N}\Lambda(\overline{a_i}) \end{aligned} \qquad (3.40)$$

(증명) 정리 3.10 을 적용하면 쉽게 증명된다.

(정리 3.12) 임의의 양의 정수 $q>1$, $m>0$, $n>0$ 에 대하여 식 (3.41) 의 관계가 만족한다.

$$\gcd(q^m-1, q^n-1) = q^{\gcd(m,n)}-1 \qquad (3.41)$$

(증명) 정수간의 관계가 $m>n$ 이라고 가정하자. 그러면 (3.42)의 관계식을 얻을 수 있다.

$$m = kn + r \qquad (3.42)$$

여기서 $0\le r<n$ 의 관계를 만족한다. 식 (3.42) 의 결과를 이용하여 다음의 관계식을 구할 수 있다.

$$\begin{aligned} q^m-1 &= q^{kn+r}-1 \\ &= q^r(q^{kn}-1)+q^r-1 \\ &= q^r(q^{(k-1)n}+q^{(k-2)n}+\cdots+q^n+1)(q^n-1) + q^r-1 \end{aligned} \qquad (3.43)$$

여기서 r 은 $m = kn + r$ 관계를 만족한다. $\gcd(q^m-1, q^n-1)$ 은 식 (3.43) 의 관계을 확장하면 구할 수 있다. 이를 수식으로 표현하면 식 (3.44) 와 같다.

$$\begin{aligned} q^m-1 &= q^r(q^{(k-1)n}+q^{(k-2)n}+\cdots+q^n+1)(q^n-1) + q^r-1 \\ &\quad : m=kn+r \\ q^n-1 &= l_2(q^n-1) + q^{r_1}-1 \\ &\quad : n=k_1n+r_1 \\ &\cdots \\ q^{r_{n-2}}-1 &= l_{n+1}(q^{r_{n-1}}-1) + q^{r_n}-1 \\ &\quad : r_{n-1}=k_nr_{n-1}+r_n \end{aligned} \qquad (3.44)$$

$\gcd(q^m-1, q^n-1)$ 는 $q^{r_n}-1$ 이 되며, 이는 $q^{\gcd(m,n)}-1$ 이 됨을 알 수 있다. (증명완료)

정리 3.12 는 계열의 주기를 계산할 때 이용될 수 있다.

(정리 3.13) 계열 $\overline{a}$, $\overline{b}$ 가 $GF(q)$ 상의 계열이며, $\overline{a}$ 는 차수가 m 인 $m_{\overline{a}}(x)$ 에 의해 생성되

고 $\bar{b}$ 는 차수가 n 인 $m_{\bar{b}}(x)$ 에 의해 생성된다. $m_{\bar{a}}(x)$ 의 order 가 T_1 이고, $m_{\bar{b}}(x)$ 의 order 가 T_2, $\gcd(m,n)=1$ 이라고 가정하자. $GF(q)$ 상의 가산 계열 $\bar{a}+\bar{b}$ 또는 곱 계열 $\bar{a}\bar{b}$ 인 $\bar{z}$ 의 주기는 식 (3.45) 의 관계식을 만족한다.

$$\frac{T_1T_2}{[\gcd(T_1,T_2)]^2} \le T \le T_1T_2 \qquad (3.45)$$

(증명) 계열 $\bar{z}$ 의 최대 가능한 주기는 T_1T_2 이다. 따라서 $T \le T_1T_2$ 의 관계가 만족된다. 그리고 $d_1 \le T_1$ 인 d_1 이 T_1 을 나누고 $d_2 \le T_2$ 인 d_2 이 T_2 을 나누면 주기의 최소 가능한 값은 $T_{\min}=d_1d_2$ 가 된다. $\bar{z}$ 는 d_1T_2 에서 주기적이므로 $T_1 | d_1T_2$ 의 관계식이 만족한다. 따라서 $\{T_1/\gcd(T_1,T_2)\} | kd_1$ 이 되어 $\{T_1/\gcd(T_1,T_2)\}$ 은 d_1 의 약수이다. 마찬가지 방법으로 $\{T_2/\gcd(T_1,T_2)\} | kd_2$ 가 되어 $\{T_2/\gcd(T_1,T_2)\}$ 은 d_2 의 약수이다. 따라서 다음과 같은 관계식을 구할 수 있다.

$$\frac{T_1T_2}{[\gcd(T_1,T_2)]^2} \le d_1d_2 \le T \le T_1T_2$$

한편 $\gcd(m,n)=1$ 이므로 $\gcd(T_1,T_2)=q-1$ 이 된다. 따라서 윗 식은 식 (3.46) 과 같이 변경될 수 있다.

$$\frac{T_1T_2}{(q-1)^2} \le T \le T_1T_2 \qquad (3.46)$$

만약 $q=2$ 라면 $T=T_1T_2$ 가 된다. (증명완료)

(정리 3.14) $\gcd(m,n)=1$ 인 관계가 만족하고 α 가 $GF(q^m)$ 상의 원소이고 β 가 $GF(q^n)$ 상의 원소라고 가정하면 식 (3.47) 의 관계식이 만족한다.

$$tr_1^m(\alpha)\,tr_1^n(\beta) = tr_1^{mn}(\alpha\beta) \qquad (3.47)$$

(증명) $GF(q^m)$ 과 $GF(q^n)$ 은 $GF(q^{mn})$ 의 부분체이다. $\alpha\beta$ 가 $GF(q^m)$ 상의 원소라면 $\alpha^{-1}\alpha\beta=\beta\in GF(q^m)$ 이 되어 이는 가정을 모순한다. 따라서 $\alpha\beta$ 가 $GF(q^m)$ 상의 원소가 아니다. 같은 이유로 $\alpha\beta$ 가 $GF(q^n)$ 상의 원소가 아니다. 그러므로 $\alpha\beta$ 가 $GF(q^{mn})$ 상의 원소다. 그리고 $\gcd(m,n)=1$ 이므로, 중국인의 잉여 정리에 의해 i 가 0 에서 $mn-1$ 사이의 정수라면 i 는 $(i \bmod m,\ i \bmod n) = (j,k)$, $(0 \le j < m,\ 0 \le k < n)$ 로 쓸수 있다. 따라서 식 (3.48) 과 같은 관계식을 유도할 수 있다.

$$\begin{aligned} tr_1^{mn}(\alpha\beta) &= \sum_{i=0}^{mn-1} \alpha^{q^i}\beta^{q^i} \\ &= \sum_{j=0}^{m-1}\sum_{k=0}^{n-1} \alpha^{q^j}\beta^{q^k} \\ &= (\alpha+\cdots+\alpha^{q^{m-1}})(\beta+\cdots+\beta^{q^{n-1}}) \\ &= tr_1^m(\alpha)\,tr_1^n(\beta) \end{aligned} \qquad (3.48)$$

(증명완료)

(정리 3.15) 계열 $\bar{a}$, $\bar{b}$ 가 $GF(q)$ 상의 계열이며, $\bar{a}$ 는 특성다항식의 차수가 m 인 $m_{\bar{a}}(x)$ 에

의해 생성되고 $\overline{b}$ 는 다항식의 차수가 n 인 $m_{\overline{b}}(x)$ 에 의해 생성된다. $\gcd(m,n)=1$ 이라고 가정하자. $GF(q)$ 상의 곱 계열 $\overline{ab}$ 인 $\overline{z}$ 는 차수가 mn 인 $GF(q)$ 상의 특성방정식 $m_{\overline{z}}(x)$ 에 의해 생성된다.

(증명) 계열 $\overline{a}$ 의 요소 a_n, 계열 $\overline{b}$ 의 요소 b_n 는 각각 식 (3.49) 와 같다.

$$\begin{aligned} a_n &= tr_1^m(A\alpha^n) \\ b_n &= tr_1^n(B\alpha^n) \end{aligned} \qquad (3.49)$$

여기서 계수 A,B 는 각 계열의 초기치에 의해 결정된다. 따라서 다음의 관계식이 만족된다.

$$\begin{aligned} tr_1^{mn}(\alpha\beta) &= \sum_{i=0}^{mn-1}(\alpha\beta)^{q^i} \\ &= \sum_{i=0}^{mn-1}\alpha^{q^i}\beta^{q^i} \end{aligned} \qquad (3.50)$$

한편 $\alpha\in GF(q^m)$, $\beta\in GF(q^n)$ 은 식 (3.51)의 관계식을 만족한다.

$$\begin{aligned} \alpha^{q^i} &= \alpha^{q^{i \bmod m}} \\ \beta^{q^i} &= \beta^{q^{i \bmod n}} \end{aligned} \qquad (3.51)$$

$\gcd(m,n)=1$ 이므로, 중국인의 잉여 정리에 의해 i 가 0 에서 $mn-1$ 사이의 정수라면 i 는 $(i \bmod m,\ i \bmod n) = (j,k)$, $(0\le j<m,\ 0\le k<n)$ 로 쓸수 있다. 따라서 식 (3.51) 의 지수부는 각각 다른 값 (j,k) 를 갖게 된다. 한편 계열 요소 z_n 은 식 (3.52) 와 같이 쓸수 있다.

$$\begin{aligned} z_n &= a_n b_n \\ &= tr_1^m(A\alpha^n)tr_1^n(B\beta^n) \\ &= tr_1^{mn}(AB(\alpha\beta)^n) \end{aligned} \qquad (3.52)$$

여기서 $AB\in GF(q^{mn})$, $\alpha\beta\in GF(q^{mn})$ 이다. $\alpha\beta$ 의 복소근의 차수는 mn 이므로, 차수가 mn 이고 $\alpha\beta$ 의 복소근을 근으로 갖는 $m_{\overline{z}}(x)$ 는 계열 $\overline{z}$ 을 생성한다. (증명완료)

(정리 3.16) 차수가 M 이고 $GF(q)$ 상의 특성방정식 $m_{\overline{a}}(x)$ 에 의해 생성되는 계열 $\overline{a}$ 와 차수가 N 이고 $GF(q)$ 상의 특성방정식 $m_{\overline{b}}(x)$ 에 의해 생성되는 계열 $\overline{b}$ 가 있다. $m_{\overline{a}}(x)$ 의 근들은 $GF(q^m)-GF(q)$ 상에 존재하고 $m_{\overline{b}}(x)$ 의 근들은 $GF(q^n)-GF(q)$ 상에 존재한다고 가정하자. $\gcd(m,n)=1$ 이고 $\alpha_i\alpha_j^{-1}\notin GF(q)$, $\beta_i\beta_j^{-1}\notin GF(q)$ 라고 가정한다. 그러면 곱계열 $\overline{z}=\overline{ab}$ 를 생성하는 특성방정식 $m_{\overline{z}}(x)$ 는 $GF(q^{mn})-[GF(q^m)\cup GF(q^n)]$ 에서 MN 개의 단순근 (simple root) 을 갖는다.

(증명) $\overline{a}$, $\overline{b}$ 의 역급수 전개식 $a(D)$, $b(D)$ 는 식 (3.53) 과 같다.

$$\begin{aligned} a(D) &= \sum_i \frac{P_i(D)}{F_i(D)} \\ &= \frac{P_1(D)}{F_1(D)} + \frac{P_2(D)}{F_2(D)} + \cdots \\ b(D) &= \sum_k \frac{Q_k(D)}{G_k(D)} \\ &= \frac{Q_1(D)}{G_1(D)} + \frac{Q_2(D)}{G_2(D)} + \cdots \end{aligned} \tag{3.53}$$

여기서 $\deg[P_i(D)]<m_i=\deg[F_i(D)]$, $\deg[Q_i(D)]<n_k=\deg[G_i(D)]$ 이고, n_k 는 n 또는 n 의 약수이며 m_i 는 m 또는 m 의 약수이다. 계열 $\bar{a}$ 의 구성 계열 $\bar{a}^{(i)}$ 라고 하고 계열 $\bar{b}$ 의 구성 계열 $\bar{b}^{(k)}$ 라고 하자. 그러면 각 구성 계열과 멱급수 전개식 간의 관계식은 식 (3.54) 와 같다.

$$\begin{aligned} \bar{a}^{(i)}(D) &= \frac{P_i(D)}{F_i(D)} \\ \bar{b}^{(k)}(D) &= \frac{Q_k(D)}{G_k(D)} \end{aligned} \tag{3.54}$$

따라서 계열 $\bar{a}$ 는 모든 구성 계열 $\bar{a}^{(i)}$ 의 합으로 구성되며, 계열 $\bar{b}$ 는 모든 구성 계열 $\bar{b}^{(k)}$ 의 합이다. 따라서 계열 $\bar{a}$, $\bar{b}$ 는 식 (3.55) 로 표현될 수 있다.

$$\begin{aligned} \bar{a} &= \sum_i \bar{a}^{(i)} \\ \bar{b} &= \sum_k \bar{b}^{(k)} \end{aligned} \tag{3.55}$$

그러므로 곱계열 $\bar{z}$ 는 식 (3.56) 과 같다.

$$\begin{aligned} \bar{z} &= \overline{ab} = \sum_i \sum_k \bar{a}^{(i)}\ \bar{b}^{(k)} \\ &= \sum_i \sum_k \bar{z}^{(ik)} \end{aligned} \tag{3.56}$$

$\gcd(m,n)=1$ 이므로 $\gcd(m_1m_2\cdots, n_1n_2\cdots)=1$ 이다. 따라서 $\gcd(m_i,n_k)=1$ 의 관계식이 만족된다. 여기서 $\bar{z}^{(ik)}$ 는 차수가 m_in_k 인 기약 특성방정식에 의해 생성된다. 구성계열 $\bar{z}^{(ik)}$ 의 계열 요소 $z_n^{(ik)}$ 는 식 (3.57) 과 같다.

$$z_n^{(ik)} = tr_1^{m_in_k}(A_iB_k(\alpha_i\beta_k)^n) \tag{3.57}$$

여기서 $A_i\in GF(q^m)$, $B_k\in GF(q^n)$ 이다. 한편 $\alpha_1,\alpha_2\in GF(q^m)$, $\beta_1,\beta_2\in GF(q^n)$ 인 원소에 대해 $\alpha_1\beta_1=\alpha_2\beta_2$ 라고 가정하자. 양변에 $\alpha_2^{-1}\beta_1^{-1}$ 를 곱하면 $\alpha_1\alpha_2^{-1}=\beta_2\beta_1^{-1}$ 이 된다. $\alpha_1\alpha_2^{-1}\in GF(q^m)$, $\beta_2\beta_1^{-1}\in GF(q^n)$, $\gcd(m,n)=1$, $GF(q^m)\cap GF(q^n)=GF(q)$ 등을 고려하면, $\alpha_1\alpha_2^{-1}$, $\beta_2\beta_1^{-1}\in GF(q)$ 이 되어야 한다. 따라서 $\alpha_1=c_1\alpha_2$, $\beta_2=c_2\beta_1$ 이 되어 정리의 가정을 모순한다. 따라서 $\alpha_1\beta_1\neq\alpha_2\beta_2$ 가 성립한다. 이는 모든 구성 계열의 특성방정식의 근이 모두 다름을 의미한다. 각 구성 계열들간의 곱계열의 근들이 서로 다르고, 각 구성 계열의 근이 다르므로 $m_{\bar{z}}(x)$ 의 근은 MN 개의 단순근으로 구성된다. (증명완료)

정리 3.16 에서 $\alpha_i\alpha_j^{-1} \notin GF(q)$, $\beta_i\beta_j^{-1} \notin GF(q)$ 라는 조건은 $q=2$ 인 경우 $GF(2)$ 내의 0 이 아닌 원소는 "1" 이 되어 $\alpha_i \neq \alpha_j^{-1}$, $\beta_i \neq \beta_j$ 라는 조건으로 귀착된다.

(정리 3.17) 차수가 M_i 이고 $GF(q)$ 상의 특성방정식 $m_{\bar{a}^{(i)}}(x)$ 에 의해 생성되는 계열 $\bar{a}^{(i)}$ 가 있다. $m_{\bar{a}^{(i)}}(x)$ 의 근 $\alpha_{i,n}$ $(i=1,\cdots,N,\ n=1,\cdots,M_i)$ 들은 $GF(q^{m_i})-GF(q)$ 상에 단일근으로 존재한다. $\gcd(m_i,n_j)=1$ 이고 $\alpha_{i,n}\alpha_{j,n}^{-1} \notin GF(q)$ 라고 가정한다. 그러면 $m = \prod_{i=1}^{N} m_i$ 인 경우, N 개의 $\bar{a}^{(i)}$ 들의 곱계열 $\bar{z} = \bar{a}^{(1)} \cdots \bar{a}^{(N)}$ 를 생성하는 특성방정식 $m_{\bar{z}}(x)$ 는 $GF(q^m) - [\bigcup_k GF(q^k)]$ 에서 $M=\prod_{i=1}^{N} M_i$ 개의 단일근 (simple root) 을 갖는다. 여기서 k 는 가능한한 N 개의 $N-1$ 차의 m_i 들의 곱을 의미한다.

(증명) 계열 $\bar{b}_{(1)}= \bar{a}^{(1)}\ \bar{a}^{(2)}$ 를 생성하는 특성방정식 $m_{\bar{b}_1}(x)$ 의 차수는 정리 3.16 에 의하여 M_1M_2 이고 근은 $GF(q^{m_1m_2})-[GF(q^{m_1}) \cup GF(q^{m_2})]$ 상에 존재한다. 또한 $\gcd(m_3,m_1m_2)=1$ 이므로 계열 $\bar{b}_{(2)} = \bar{b}_{(1)}\ \bar{a}^{(3)}$ 을 생성하는 특성방정식 $m_{\bar{b}_2}(x)$ 의 차수는 정리 3.16 에 의하여 $M_1M_2M_3$ 이고, 근은 $GF(q^{m_1m_2m_3})-[GF(q^{m_1m_2}) \cup GF(q^{m_1m_3}) \cup GF(q^{m_2m_3})]$ 상에 존재한다. 이를 확대하면 정리의 증명이 완료될 수 있다. (증명완료)

(정리 3.18) 차수가 M_i 이고 $GF(q)$ 상의 특성방정식 $m_{\bar{a}^{(i)}}(x)$ 에 의해 생성되는 계열 $\bar{a}^{(i)}$ 가 있다. $m_{\bar{a}^{(i)}}(x)$ 의 근 $\alpha_{i,n}$ $(i=1,\cdots,N,\ n=1,\cdots,M_i)$ 들은 $GF(q^{m_i})-GF(q)$ 상에 단일근으로 존재한다. $\gcd(m_i,n_j)=1$ 이고 $\alpha_{i,n}\alpha_{j,n}^{-1} \notin GF(q)$ 라고 가정한다. 비선형 합성함수 $f(x_1,\cdots,x_N)$ 는 식 (3.58) 과 같이 주어진다.

$$f(x_1,\cdots,x_N) = a_0 + \sum_i a_i x_i + \sum_{ij} a_{ij} x_i x_j + \cdots + a_{12\cdots N} x_1 x_2 \cdots x_N \qquad (3.58)$$

여기서 $a_i, a_{ij}, \cdots \in GF(q)$ 이다. 그러면 비선형 합성함수의 출력 계열 $\bar{z}$ 는 차수 $M=f'(M_1,\cdots,M_N)$ 인 특성방정식 $m_{\bar{z}}(x)$ 에 의해 생성된다. $m = \prod_{i=1}^{N} m_i$ 인 경우, 특성방정식 $m_{\bar{z}}(x)$ 는 $GF(q^m)-GF(q)$ 에서 단일근 (simple root) 을 갖는다. 여기서 $f'(x_1,\cdots,x_N)$ 은 $a_i, a_{ij}, \cdots$ 가 0 이 아닐 경우, $a_i=1, a_{ij}=1, \cdots$ 하여 실수상에서 계산된 값을 의미한다.

(증명) k 차의 곱항 $\bar{a}_1\ \bar{a}_2 \cdots \bar{a}_k$ 는 차수 $M_k' = \prod_{i=1}^{k} M_i$ 인 특성 방정식과 연관된다. 특정의 주기 계열에 임의의 상수를 곱하여 생성된 계열은 원래의 계열과 동일한 선형복잡도와 특성방정식을 갖는다. 계열 $\bar{z}$ 의 특성방정식은 여러개의 기약다항식으로 인수분해된다. 위의 정리들을 이용하면 $\gcd(m_i,m_j)=1, i\neq j$ 이므로 임의의 두 계열의 곱계열의 원소 $\alpha_1\beta_1, \alpha_2\beta_2$ 는 계열 $\bar{z}$ 의 특

성방정식의 서로 다른 기약다항식의 근이 된다. 따라서 $f(x_1,\cdots,x_N)$ 내의 모든 곱항의 근 들을 더하면 이의 갯수는 $M=f'(M_1,\cdots,M_N)$ 이 됨은 쉽게 알수 있다. 그러므로 비선형 합성함수의 출력 계열 $\bar{z}$ 는 차수 $M=f'(M_1,\cdots,M_N)$ 인 특성방정식 $m_{\bar{z}}(x)$ 에 의해 생성된다. (증명완료)

4. 결 론

통신망이 고속화됨에 따라 속도 측면에서 여타의 암호 알고리듬에 비해 강점이 있는 스트림 암호 방식이 널리 적용될 예정이다. 스트림 암호시스팀의 암호 강도 측정 요소의 하나는 계열을 생성하는 선현 복잡도이다. 일반적으로 선형복잡도가 큰 계열은 Berlekamp-Massey 가 제시한 LFSR 합성알고리듬이 견딜 수 있다. LFSR 계열은 선형 복잡도가 일반적으로 낮으므로 LFSR 계열에 비선형 함수를 도입하여 선형복잡도를 높이는 기법이 널리 적용되어 왔다. LFSR 계열에 비선형함수를 적용하는 방법은 하나의 LFSR 계열을 지연시켜 비선형함수를 적용하는 방법과 서로 다른 LFSR 계열에 비선형 함수를 적용하는 방법이 있다.

본 논문에서는 기본적으로 LFSR 계열의 분석을 위해 요구되는 기본 이론을 도출하고 이를 바탕으로 LFSR 합성 알고리듬의 근간이 되는 여러 관련 정리들을 유도하였으며, 실제로 LFSR 합성 알고리듬을 이용하여 계열의 특성방정식과 선형복잡도가 구해짐을 보였다. 그리고 하나의 LFSR 계열을 지연시켜서 비선형함수에 적용한 여러 관련 이론 등을 제시하였고, 선형 복잡도 및 주기 특성 등의 구체적인 예를 제시하였다. 서로 다른 LFSR 계열을 비선형함수로 결합한 계열의 선형 복잡도 등의 특성을 제시하였다.

본 논문의 결과는 LFSR 계열을 이용한 비선형 랜덤 계열을 생성하기 위한 생성기의 바탕 이론이 될수 있으며, CDMA 이동통신망 또는 고속 디지틀 전송망 특히 SONET (synchronous optical network) 에서의 정보보호 기법으로 활용될 수 있을 것이다.

참 고 문 헌

(1) S.W. Golomb, Shift Register Sequences, Hoden-day, 1982.

(2) R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986.

(3) J.L. Massey, Coding and Cryptography, Advanced technology seminars, 1985.

(4) M.Y. Rhee, Cryptography and Secure Communications, McGraw-Hill, 1993.

(5) S.Tsujii, M.O. Kasahara, Cryptography and Information Security, 昭晃堂, 1990.

(6) J.L. Massey, "Shift-Register Synthesis and BCH Decoding," IEEE Tr. on Inform. Theory, Vol.IT-15, No.1, Jan. 1969, pp. 122-127

(7) E.L. Key, "An Analysis of the Structure and Complexity of Non-linear Binary Sequence Generator," IEEE Transactions on Information Theory, Vol.IT-22, No.6, pp.732-736, 1976.

(8) T.Siegenthaler, "Design of Combiners to Prevent Divide and Conquer Attacks," Proceedings of Crypto 85, Santa Barbara, August 18-22, 1985.

(9) M. Tatebayashi, N. Matsuzaki and D.B. Newrman Jr, "A Cryptosystem Using Signal Processors for Mobile Communication," ICC, pp.1145-1148, Sep, 1989.

(10) R.A. Scholtz, L.R.Welch, "GMW Sequences," IEEE Tr. on Inform. Theory, Vol.IT-30, No.3, pp. 548-553, May 1984.

(11) R.A.Rueppel, O.J.Staffelbach, "Products of Linear Recurring Sequences with Maximum

Complexity," IEEE Tr. on Inform. Theory, Vol.IT-33, No.2, pp.122-131, Jan. 1987.

(12) M.Antweiler, L.Bomer, "Complex Sequences over GF(P^M) with a Two-level Autocorrelation Function and Large Linear Span," IEEE Tr. on Inform. Theory, Vol.IT-38, No.1, pp.120-130, Jan. 1992.