이 학 석 사 학 위 논 문

최대무게다항식에 대응하는 난수생성기에 대한 연구

2019년 2월

부경대학교 대학원

응 용 수 학 과

강 성 원

이 학 석 사 학 위 논 문

최대무게다항식에 대응하는 난수생성기에 대한 연구

지도교수 조 성 진

이 논문을 이학석사 학위논문으로 제출함.

2019년 2월

부경대학교 대학원

응 용 수 학 과

강 성 원

강성원의 이학석사 학위논문을 인준함.

2019년 2월 22일

주 심 이학박사 표 용 수 (인)

위 원 이학박사 박 진 한 (인)

위 원 이학박사 조 성 진 (인)

목 차

표 목차

그림 목차

Study on PRNG Corresponding to the Maximum Weight Polynomial

Sung-Won Kang

Department of Applied Mathematics, Graduate School

Pukyong National University

Abstract

In order to design the pseudorandom number generator(PRNG) directly on the hardware, it should be possible to make it using the logic circuit. A linear finite state machine(FSM), which can be fabricated based on linear recurrence, facilitates fabrication using logic circuits. A linear FSM typically includes a linear feedback shift register(LFSR) and a linear cellular automata(CA).

A linear FSM can represent a state using a state transition matrix, and the characteristics of a linear FSM can also be analyzed by analyzing this state transition matrix. What is used to analyze the state transition matrix is the characteristic polynomial corresponding to the state transition matrix. Since the characteristics of the linear FSM depend on what the characteristic polynomial is, it is important to determine the appropriate characteristic polynomial for the linear FSM suitable for the application.

In this thesis, we analyze the characteristics of the PRNG, especially the CA corresponding to the maximum weight polynomial which is a polynomial with all coefficients 1 over GF(2). The results of the algorithm for the synthesis method for 90/150 CA corresponding to the maximum weight polynomial are also introduced.

Ⅰ. 서 론

Von Neumann에 의하여 수소폭탄 실험의 컴퓨팅 과정 도중 제안된 Middle-square 방법은 하드웨어 기반의 난수생성기의 발상의 시발점이다[1]. 1949년 Lehmer에 의해 연구된, 선형 합동식을 기반으로 한 난수 생성 구조는 현재까지도 하드웨어 기반 난수생성기의 바탕으로써 사용되고 있다[2].

난수생성기를 VLSI, ULSI, 3D-IC 등과 같은 집적회로로 구성된 하드웨어에 직접 설계하기 위해 선형 유한상태기계(Finite State Machine; 이하 FSM)의 구조를 이용한다[3].

선형 FSM의 구조를 이용하여 하드웨어로 제작가능한 난수생성기는 입력값에만 의존하여 수열을 생성하므로 의사난수생성기(Pseudorandom Number Generator) 또는 결정론적 난수 비트 생성기(Deterministic random bit generator)라고 부른다[4].

의사난수생성기로 사용하기 적합한 선형 FSM으로 선형 피드백 시프트 레지스터(이하 LFSR)와 선형 셀룰라 오토마타(이하 CA)가 존재한다[5].

LFSR은 컴퓨팅에서 사용되는 대표적인 구조로써 출력값이 다시 입력값으로 되먹임(feedback)하는 순차적 연결 구조를 가지고 있다[6,7].

CA는 Von Neumann에 의해 1950년대 초, 스스로의 상태를 인접 상태에 의존하여 이산시간에 따라 재생성 가능한 구조로써 소개되었다. Wolfram에 의하여 분류된 선형 CA의 수학적 모델은 이러한 의사난수생성기로 사용되기에 적합하다[8].

위와같은 선형 FSM들을 이용하여 제작한 의사난수생성기는 대표적으로

암호, 계수기(counter), 서킷 테스트(circuit test), 시뮬레이션(simulation), 디지털 통신 등 다양한 분야에서 사용된다[6-8,12].

사용처에 적합한 의사난수생성기를 제작하는데에 있어서 어떤 구조에 따라 제작할지를 택하는 것은 중요한 문제이다.

의사난수생성기 구조를 분석할때 쓰이는 대표적인 수학적 도구는 기계에 대응하는 상태전이행렬과 이 행렬에 대응하는 특성다항식 및 최소다항식인데, 이것들의 분석은 사용처에 적합한 의사난수생성기를 제작하는데 도움이 된다. 그러므로 의사난수생성기 구조에 대응하는 다양한 다항식들의 성질들을 면밀히 분석하는 것은 중요하다.

본 논문에서는 유한체 GF(2) 위에서 최고차항 이하의 모든 계수가 1인 다항식 '최대무게다항식'과 최대무게다항식을 특성다항식으로 갖는 LFSR과 90/150 CA에 초점을 맞추어 각 구조로 생성한 의사난수생성기의 특성들을 분석하고 비교한다. 선형 FSM의 주기는 초기상태와 최소다항식으로 인해 결정이 되는데, LFSR과 90/150 CA는 최소다항식과 특성다항식이 동일한 선형 FSM이기 때문에 본 논문에서 집중하는 주제로 삼게되었다.

2장에서는 의사난수생성기와 선형 FSM에 관한 기본지식에 대하여 기술하고 기존 연구에 대해서 알아본다. 그리고 GF(2)위에서의 최대무게다항식과 이것의 특성에 대해서도 알아본다.

3장과 4장에서는 최대무게다항식에 대응하는 LFSR의 성질과 최대무게다항식에 대응하는 90/150 CA의 성질을 각각 분석해보고, 특히 4장에서는 최대무게다항식에 대응하는 90/150 CA를 생성하는 알고리즘 또한 제안한다.

5장에서는 최대무게다항식에 대응하는 LFSR과 90/150 CA의 성질에 대하여 각각의 특징들을 비교해본 뒤, 6장에서 결론을 짓는다.

Ⅱ. 배경지식

이 장에서는 본 논문에서 사용하는 의사난수생성기, FSM, 유한체 위에서의 최대무게다항식과 관련된 기초지식에 대하여 기술하고 기존 연구에 대해서 알아본다.

2.1 의사난수생성기

의사난수생성기는 수학적 생성기(Mathematical generator)라고도 불리운다. 수학적 모델로 합성하에 제작한 알고리즘을 일컫는다.

의사난수생성기로는 Middle-Square Method, 선형합동 생성기(Linear Congruential Generator; 이하 LCG), Mersenne Twister 등과 같이 다양한 구조들이 존재한다[10].

이 구조 중에서도 특히 LCG는 1949년 Lehmer에 의해 연구된 대표적인 의사난수생성기로써 오늘날에도 널리 쓰이고 있는 의사난수생성기의 구조이다[2]. LCG는 아래와 같은 식으로 구성되는 의사난수 생성함수이다.

$$X_{n+1} = (aX_n + c) \mod m$$

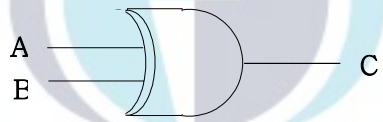
여기서 X_n은 n번째 수열의 상태를 의미한다.

2.2 FSM

FSM(Finite State Machine)은 유한 자동기계(Finite Automaton)라고도 불리운다.

FSM은 다음 상태와 출력을 결정하는 두 개의 조합 논리 블록과 상태를 저장하는 레지스터, 클럭 에지 등으로 구성된다.

조합 논리 블록은 신호가 전달되는 노드와 연산을 수행하는 게이트로 구성되어 있다. <그림 2.2.1>에서는 XOR게이트를 그림으로 나타낸 것이다. XOR게이트는 입력받은 이진 신호 A, B에 대하여 부울대수 진리표를 나타내고 있는 [표 2.2.1]과 같이 이진 신호 C를 출력하는 조합회로이다. 여기서 회로에 신호가 들어오는 경우를 T, 들어오지 않는 경우를 F라고 한다.



<그림 2.2.1> XOR게이트의 개략도 표현

[표 2.2.1] XOR게이트의 전이규칙

A	B	C
T	T	F
T	F	T
F	T	T
F	F	F

FSM은 대표적으로 무어 기계(Moore Machine)와 밀리 기계(Mealy Machine)가 존재하며 기계의 구별은 출력 신호가 기계의 현재 입력 신호에 의존하는가에 따라서 결정된다.

FSM은 이진부호화를 할당받아 값이 입력 및 출력이 이루어지고 있기 때문에, 상태를 이진수로 나타내며 적용되는 관계를 부울함수를 이용하여 나타내는 것이 가능하다. 회로에 신호가 들어오는 경우를 1로 두고, 들어오지 않는 경우를 0이라고 두면 [표 2.2.1]에서 나타내고있는 게이트의 수행상태는 유한체인 GF(2) 위에서의 덧셈을 수행하는 것과 같은 의미를 가지게 된다. 이러한 FSM을 기반으로 한 의사난수생성기는 하드웨어로 제작이 가능하기때문에 특별히 Hardware PRNG(HPRNG) 또는 Programmable PRNG라고도 부른다[10].

2.3 선형 FSM

선형 FSM은 모든 상태에 관여하는 연산이 XOR만으로 이루어져 있는 FSM를 말한다. 이 때 선형 FSM은 상태전이 규칙과 상태를 각각 유한체 GF(2) 위의 행렬과 벡터의 곱으로 표현가능하다.

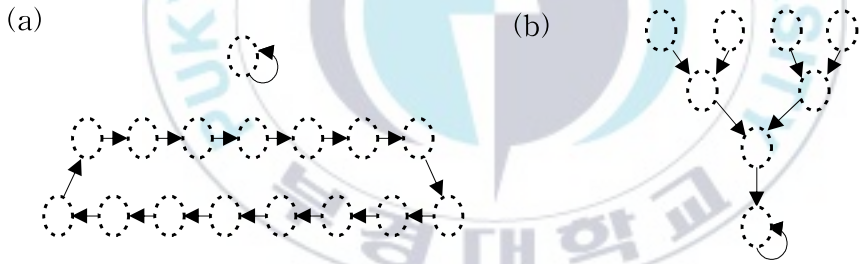
시간 t의 상태를 나타내는 벡터를 $\boldsymbol{s}_t$, 상태전이규칙을 나타내는 행렬을 T라고 하자. 그러면 선형 FSM에 의한 전이규칙은 아래와 같은 식으로 나타낼 수 있다.

$$\boldsymbol{s}_{t+1} = T\boldsymbol{s}_t$$

선형 FSM의 성질을 분석하기 위해서는 상태전이행렬의 특성다항식(characteristic polynomial)과 최소다항식(minimal polynomial)을 분석하면 된다.

선형 FSM의 $n \times n$ 상태전이행렬 T에 대하여 특성다항식 $c_T(x)$은 $GF(2) = \{0,1\}$상에서 $c_T(x) = |T \oplus xI|$이다. 여기서, I는 n차 단위행렬이다. 그리고 선형 FSM의 상태전이행렬 T에 대한 특성다항식 $c_T(x)$의 인수 중 T를 해로 가지는 다항식들 중 차수가 가장 낮은 다항식을 특별히 최소다항식이라 하고 $m_T(x)$로 나타낸다.

임의의 선형 FSM으로 인하여 발생하는 상태전이의 형태는 <그림 2.3.1>과 같이 두 가지로 분류가 가능하다.



<그림 2.3.1> 선형 FSM에 따라 전이되는 상태의 형태

<그림 2.3.1(a)>와 같이 나타나는 형태를 Cycle형이라고 하며, <그림 2.3.1(b)>와 같이 나타나는 형태를 Tree형이라고 한다.

<정리 2.3.1> 선형 FSM M의 상태전이행렬을 T라고 하고, 특성다항식을 $c_T(x)$라고 하자.

$c_T^*(x) = x^n c_T(\frac{1}{x})$를 $c_T(x)$의 상반다항식이라고 하면(이 때 n은 $c_T(x)$의 차수이다.) 아래와 같은 성질들을 만족한다.

(a) $\deg c_T^*(x) = \deg c_T(x)$이면 M으로 인하여 발생하는 상태전이의 형태는 Cycle형이다.

(b) $\deg c_T^*(x) \neq \deg c_T(x)$이면 M으로 인하여 발생하는 상태전이의 형태는 Tree형이다.

선형 FSM에서 상태의 주기는 $\boldsymbol{s}_{t+m} = T^m \boldsymbol{s}_t = I\boldsymbol{s}_t = \boldsymbol{s}_t$를 만족하는 가장 작은 양의 정수 m이다. 즉, 현재 상태와 선형 FSM을 m번 적용한 상태가 동일하게 된다는 것이다.

<정리 2.3.2> 선형 FSM에 의해 생성되는 수열의 주기는 초기상태와 최소다항식 두 가지에 의존한다.

케일리-헤밀턴 정리에 따라 상태전이행렬 T는 $c_T(T) = O$를 만족하기 때문에, 최소다항식은 반드시 특성다항식의 인수이다. 정리 2.2에 따르면 수열의 주기는 최소다항식에 의존하는데 특성다항식의 인수라는 것은 최소다항식의 주기가 특성다항식의 주기의 인수중에서 결정된다는 것을 의미한다.

본 논문에서 다루는 LFSR과 CA는 최소다항식과 특성다항식이 동일하기 때문에, 선형 FSM 중에서도 이러한 특별한 성질을 만족하는 구조로써 다루게 되었다.

2.4 GF(2) 위의 최대무게다항식

GF(2) 위에서의 n차 최대무게다항식이란 $x^n+x^{n-1}+\cdots+x+1$로 나타나는 모든 계수가 1인 다항식이다. 본 논문에서는 f_n을 GF(2) 위에서의 n차 최대무게다항식이라고 할 것이다.

f_n의 기본적인 성질들은 다음과 같다[13].

<정리 2.4.1> $\deg f_n^* = \deg f_n$

<정리 2.4.2> $f_n \cdot (x+1) = x^{n+1}+1$

정리 2.3.1(a), 정리 2.4.1, 정리 2.4.2에 따라서 최대무게다항식에 대응하는 선형 FSM은 항상 Cycle형 구조를 이룬다는 것을 알 수 있으며, 또한 수열의 주기는 항상 $n+1$의 약수인 것 또한 알 수 있다.

이는 어떠한 최대무게다항식에 대응하는 선형 FSM의 상태전이행렬을 고려하더라도 항상 갖게되는 성질이다. 즉, 본 논문에서 다루는 LFSR과 CA 역시 이와 동일한 성질을 반드시 가지게 된다.

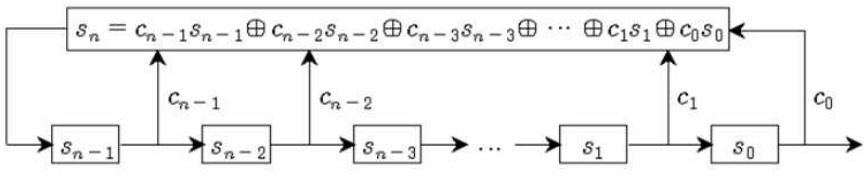
Ⅲ. 최대무게다항식에 대응하는 LFSR

3.1 LFSR(Linear Feedback Shift Register)

LFSR은 선형 FSM의 한가지로써 가장 잘 알려진 구조이며 하드웨어 제작에서도 유용하게 쓰이는 HPRNG로써 <그림 3.1.1>과 같이 입력값을 레지스터에 시프트하여 출력값을 결정하도록 하는 구조이다. n차 LFSR의 구조는 <그림 3.1.1>과 같이 레지스터에 할당된 n개의 비트셀과 식 (3.1.1)와 같은 선형 피드백 함수(linear feedback function) $f(s_0, s_1, .., s_{n-1})$에 의해 점화관계가 결정되는 조합 논리 블럭으로 구성된다[11].

$$f(s_0, s_1, .., s_{n-1}) = c_0 s_0 \oplus c_1 s_1 \oplus \cdots \oplus c_{n-1} s_{n-1} \tag{3.1.1}$$

여기서 $c_0, c_1, c_2, .., c_{n-1} \in GF(2)$는 조합 논리에 적용된 XOR게이트에 노드가 연결되었는지를 알려주는 값이며, $s_0, s_1, s_2, .., s_{n-1}$는 레지스터에 입력되는 초깃값이다.



<그림 3.1.1> LFSR의 구조도

식 (3.1.1)에 대한 다항식 $c_T(x)=x^k+c_{k-1}x^{k-1}+\cdots+c_0$은 LFSR의 상태 전이행렬에 대한 특성다항식과 동일하다[7,8]. 만약 LFSR의 초기값이 모두 '0'이면 출력값은 모두 '0'이 된다. 초기값 중 적어도 하나가 '0'이 아니라고 할 경우 LFSR이 가질 수 있는 상태는 2^k-1가지보다 작거나 같다.

3.2 동반행렬(Companion matrix)

<정의 3.2.1> $f(x)=x^n+c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0$ $(0 \le i \le n-1)$ 에 대해 아래와 같은 $n\times n$ 행렬들을 $f(x)$의 동반행렬(companion matrix)이라고 한다.

$$\text{(i)}\quad T_1=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ c_0 & c_1 & c_2 & \cdots & c_{n-2} & c_{n-1} \end{pmatrix}=\begin{pmatrix} O_{(n-1)\times 1} & I_{n-1} \\ c_0 & C \end{pmatrix}$$

$$\text{(ii)}\quad T_2=\begin{pmatrix} c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_1 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}=\begin{pmatrix} C & c_0 \\ I_{n-1} & O_{(n-1)\times 1} \end{pmatrix}$$

여기서 I_{n-1}은 $(n-1)\times(n-1)$단위행렬이고, $C=(c_1, c_2, \ldots, c_{n-1})^t$이다.

(i)에서 만든 동반행렬 T_1은 $(a_1, a_2, \ldots, a_{n-1}, a_n)^T$라는 상태의 요소들을

오른쪽에서 왼쪽으로 쉬프트하여 $(a_2, a_3, \ldots, a_n, a_{n+1})^T$라는 다음 상태를 만드는 동반행렬이고, (ii)에서 만든 동반행렬 T_2는 $(a_n, a_{n-1}, \ldots, a_2, a_1)^T$라는 상태의 요소들을 왼쪽에서 오른쪽으로 쉬프트하여 $(a_{n+1}, a_n, \ldots, a_3, a_2)^T$라는 다음 상태를 만드는 동반행렬이다. 여기서 $a_{n+1} = c_{n-1}a_n + c_{n-2}a_{n-1} + \cdots + c_1a_2 + c_0a_1$라는 점화관계가 성립한다.

동반행렬의 특성다항식은 $f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1x + c_0$로 나타난다. 따라서 어떤 다항식에 대응하는 LFSR의 상태전이행렬은 동반행렬을 이용하여 아주 간단하게 나타내는 것이 가능하다.

3.3 최대무게다항식에 대응하는 LFSR

최대무게다항식 f_n에 대응하는 LFSR에 대한 상태전이행렬 T_n은 아래의 두 가지 방법으로 표현할 수 있다.

$$\text{(i)}\ T_n = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad \text{(ii)}\ T_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix}$$

3.2절에서 살펴본 것과 같이 (i)에 대응하는 LFSR은 현재상태가 우측으로 쉬프트되는 구조이며, (ii)에 대응하는 LFSR은 현재상태가 좌측으로 쉬프트되는 구조이다.

다음 예제를 통하여 실제로 현재 상태가 LFSR을 통해 어떻게 변화하는지를 살펴본다.

<예제 3.3.1> $f_4(x)$에 대응하는 LFSR의 동반행렬 T가 다음과 같이 주어졌다고 하자.

$$T=\begin{pmatrix}1&1&1&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}$$

$\mathbf{s}_t=(0,0,0,1)^t$를 시간 t의 상태라 하고 $T\mathbf{s}_t, T^2\mathbf{s}_t, \cdots, T^4\mathbf{s}_t, T^5\mathbf{s}_t$를 구해보자. 여기서 $\mathbf{s}_t$를 십진수로 나타내면 1이다. 이것을 $\mathbf{s}_t=1$로 표시할 것이다. $T\mathbf{s}_t=(1,0,0,0)^t=8$이 된다. 그리고 LFSR을 계속 적용한 결과는 아래의 식과 같이 나타난다.

$$T^2\mathbf{s}_t=(1,1,0,0)^t=12,\ T^3\mathbf{s}_t=6,\ T^4\mathbf{s}_t=3,\ T^5\mathbf{s}_t=1$$

여기서, 주어진 상태에 LFSR을 5번 적용하는 것으로 처음 상태인 1로 되돌아 간다는 것 또한 알 수 있다.

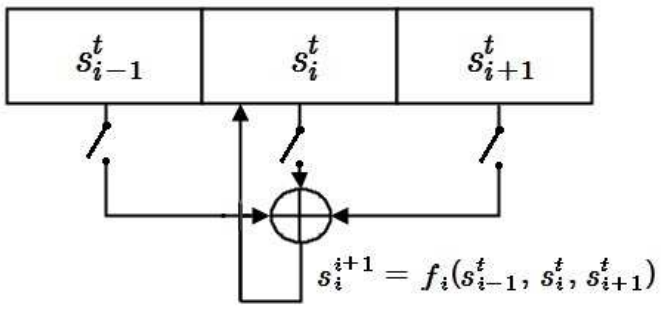
$f_4(x)=x^4+x^3+x^2+x+1 \mid x^5+1$가 성립하기 때문에 $f_4(x)$의 주기는 5이며 실제로도 $T^5\mathbf{s}_t=\mathbf{s}_t$를 만족한다.

Ⅳ. 최대무게다항식에 대응하는 90/150 CA

이 장에서는 본 논문에서 사용하는 CA의 용어와 기본성질에 대하여 기술하고 기존의 연구 및 제안된 방법들을 살펴보고, 최대무게다항식에 대응하는 90/150 CA에 대한 합성방법에 대하여 살펴본다.

4.1 셀룰라 오토마타(Cellular Automata)

셀룰라 오토마타(Cellular Automata; CA)는 이산 시간에 따라 다른 상태로 갱신되는 동적 시스템으로써, 셀이라는 기본 단위 메모리의 배열로 이루어져 있다[8]. 1차원 CA(One dimensional CA) 중에서도 국소적 상호작용이 세 개의 셀, 즉 자기 자신과 인접한 두 개의 셀에 의해서만 이루어지는 CA를 3-이웃 선형 CA(3-neighborhood linear CA)라고 한다. 3-이웃 선형 CA의 셀 구조는 <그림 4.1.1>과 같다.



<그림 4.1.1> 3-이웃 선형 CA 구조

이 구조에서 셀의 다음 상태는 어떤 규칙에 따라 정해진다. 즉, 각 셀들은 자기 자신과 이웃 셀의 함숫값에 의해 다음 상태가 결정되어 동시에 갱신되는데, 3-이웃 CA에 대한 상태전이함수(state-transition function)는 다음 식 (4.1.1)과 같다.

$$q_i(t+1) = f\left[q_i(t), q_{i+1}(t), q_{i-1}(t)\right] \tag{4.1.1}$$

여기서 $q_i(t)$은 시간 t에서 i번째 셀의 상태를 의미한다.

여기서 f는 결합 논리를 가지는 국소전이 함수이다. GF(2)상에서 3-이웃 CA에는 서로 다른 2^3개의 이웃의 배열상태가 있으며 그러한 CA에는 255개의 상태전이함수가 있게 되며, 이를 CA의 전이규칙(transition rule)이라고 한다.

이러한 전이규칙 중에서도 HPRNG로 구현 가능한 CA들만을 특별히 PCA(Programmable CA)라고 부른다. PCA에서도 XOR게이트만을 이용하여 제작가능한 규칙은 크게 선형규칙과 여원규칙으로 나뉜다. 특히 선형규칙 60, 90, 102, 150, 240에 대한 전이함수는 [표 4.1.1]과 같다.

본 논문에서 사용하는 선형규칙 90, 150에 대한 상태전이는 [표 4.1.2]와 같이 나타난다.

3-이웃 선형 CA가 n개의 셀에 적용되는 경우, 이러한 CA를 n-셀 CA라고 부른다. n-셀 CA에 의한 상태의 변화를 LFSR과 마찬가지 상태전이행렬로 나타낼 수 있다.

선형규칙 90과 150만을 이용한 CA $\mathbb{C}$의 상태전이행렬이 T라고 하자. 이 때, 상태전이행렬 T는 식 (4.1.2)와 같은 삼중대각행렬로 나타난다 [9,10].

[표 4.1.1] 3-이웃 CA의 선형 전이규칙

전이규칙	전이함수
60	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$
90	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
102	$q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$
150	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$
170	$q_i(t+1) = q_{i-1}(t)$
204	$q_i(t+1) = q_i(t)$
240	$q_i(t+1) = q_{i+1}(t)$

[표 4.1.2] 전이규칙 90과 150의 상태전이 표

이웃상태	111	110	101	100	011	010	001	000	전이규칙
다음상태	0	1	0	1	1	0	1	0	90
다음상태	1	0	0	1	0	1	1	0	150

$$T=\begin{pmatrix} d_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & d_2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & d_3 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & d_4 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & d_{n-2} & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & d_{n-1} & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & d_n \end{pmatrix} \tag{4.1.2}$$

본 논문에서는 상태전이행렬 T를 식 (4.1.3)처럼 간단히 나타내기로 한다.

$$T =< d_1\, d_2\, \ldots\, d_{n-1}\, d_n > \tag{4.1.3}$$

식 (4.1.4)와 같이 전이규칙이 90이면 '0'으로 150이면 '1'로 나타낸다.

$$d_i = \begin{cases} 0, & i\text{번째 셀의 전이규칙} = 90 \\ 1, & i\text{번째 셀의 전이규칙} = 150 \end{cases} \tag{4.1.4}$$

<정리 4.1.1 [8]> 상태전이행렬이 T인 n-셀 90/150 CA에서는 특성다항식과 최소다항식이 같다.

특히 n셀 90/150 CA R_n=<$a_1 a_2 \ldots a_n$>의 특성다항식을 Δ_n이라고 할 때, 아래의 점화식 (4.1.5)이 성립한다.

$$\Delta_{n+1} = (x + a_{n+1})\Delta_n + \Delta_{n-1} \tag{4.1.5}$$

LFSR과 다르게 임의의 다항식에 대응하는 90/150 CA는 항상 존재한다는 보장이 없다. 그렇기 때문에 임의의 다항식에 대응하는 90/150 CA 존재성 판별법에 관한 연구는 계속 진행되고 있다[10].

90/150 CA의 전이규칙은 상태전이행렬의 대각성분을 읽는 것으로 표현할 수 있는데, Choi 등에 의해 이러한 전이규칙을 하나의 블록, 즉 전이규칙 블록으로 보고 다른 전이규칙 블록과 연결하여 새로운 90/150 CA를 합성하는 방법이 제안되었다[14].

Cattell 등에 의해 임의의 기약다항식에 대응하는 90/150 CA 합성 알고리즘이 제안되었다[5]. 이후, Cho 등에 의해 임의의 다항식에 대응하는 효율적인 90/150 CA 합성 알고리즘이 제안되었다[9]. Cattell 등에 의해 제안된 합성 알고리즘의 시간복잡도는 $O(n^7)$이었지만, Cho 등에 의해 제안된

합성 알고리즘의 시간복잡도는 $O(n^2)$로 크게 개선되었다[9]. 또한 Cho 등이 제안한 합성 알고리즘을 통해 임의의 다항식에 대응하는 90/150 CA의 규칙도 찾을 수 있기 때문에, 본 논문에서 다루는 최대무게다항식에 대응하는 CA 또한 이 합성 알고리즘을 통해 얻는 것이 가능하다. 그리고 최대무게다항식에 대응하는 90/150 CA를 합성하려 할 때 알고리즘의 계산 시간을 더욱 단축시키는 것이 가능하며 이에 따라 개선된 알고리즘을 다음 절에서 소개한다.

4.2 최대무게다항식에 대응하는 90/150 CA

최대무게다항식은 언제 기약인지 가약인지에 대해 알려져 있지 않기 때문에 대응하는 90/150 CA가 항상 존재한다는 보장을 할 수가 없다. 따라서 이 절에서는 최대무게다항식에 대응하는 90/150 CA에 대하여 존재하는지 판정하고, 존재한다면 합성하는 알고리즘과 정리에 대하여 논한다.

최대무게다항식에 대응하는 90/150 CA를 합성하는 방법은 홀수차인가 짝수차인가에 따라서 구별되며 그에 따른 정리도 각각 주어져 있다. Choi 등에 의해 홀수차 최대무게다항식이 CA다항식인지 아닌지와 CA다항식을 합성하는 방법에 대하여 알려져있다[15]. 하지만 짝수차의 경우는 기존에 알려져 있지 않다.

아래에 주어진 정리는 짝수차 최대무게다항식이 CA다항식인 경우에 관한 정리이며, 이 정리를 토대로 짝수차 최대무게다항식에 대응하는 90/150 CA 합성 알고리즘을 더욱 효율적으로 제작할수 있음을 보일 것이다.

<정리 4.2.1> $2n+2$셀 90/150 CA $<R_n01R_n^*>$의 특성다항식을 U_{2n+2}라고 할 때, 다음 조건들은 동치관계이다.

(a) $U_{2n+2} = f_{2n+2}(x)$

(b) $(\Delta_{n+1}\Delta_n)' = \{f_n(x)\}^2$

(c) $f_n(x) = \sum_{i=0}^{n} \Delta_i$

짝수차 최대무게다항식에 대응하는 90/150 CA의 규칙을 상태전이 블록에는 반드시 $<R_n01R_n^*>$의 모양이 존재한다[16]. 정리 4.2.1은 짝수차 최대무게다항식이 CA다항식이라면 짝수셀 90/150 CA의 상태전이 블록 중에서 반드시 $<R_n01R_n^*>$와 같은 형태가 존재한다는 것을 보여준다. 따라서 이러한 형태의 최대무게다항식에 대응하는 90/150 CA 규칙을 효율적으로 합성하기 위해, [9]에서 소개된 알고리즘을 개선한 알고리즘을 아래에서 소개한다.

우선 입력값은 $f_{2n}(x)$의 차수인 $2n$이며, 출력값은 $f_{2n}(x)$에 대응하는 $2n$-셀 90/150 CA $< R_{n-1}01R_{n-1}^* >$인 알고리즘이다.

Step 1. 각 열이 아래의 식 (4.2.1)로 구성된 $2n \times 2n$ 행렬 D를 생성:

$$\boldsymbol{d}_i = \begin{cases} x^{i-1} + x^{2i-1} + x^{2i} & , 1 \le i \le n-1 \\ \sum_{i=0}^{n-2} (x^i + x^{n+i}) & , i = n \\ x^{2(i-n-1)} + x^{2(i-n)-1} + x^{i-1} & , n+1 \le i \le 2n-1 \\ x^{2n-2} & , i = 2n \end{cases} \quad (4.2.1)$$

여기서 $\boldsymbol{d}_i$에서 나타나는 x^j는 행렬 D의 i행 j열의 값이 1이라는 것을 의미한다.

Step 2. 방정식 $D\boldsymbol{v}=\boldsymbol{e}_{2n}$의 해 $\boldsymbol{v}$를 구한다. 여기서 $\boldsymbol{e}_i$는 i번째 요소만 1인 단위벡터이다. 만약 해 $\boldsymbol{v}$가 존재하지 않으면 $f_{2n}(x)$는 CA다항식이 아니다. STOP.

Step 3. 행렬의 각 성분이 아래의 식 (4.2.2)와 같이 구성된 $(n-1)\times(n-1)$ 행렬 $K'=(k_{ij}')$를 생성:

$$k_{ij}' = v_{i+j-1} \ (1 \le i \le n-1, 1 \le j \le n-1) \qquad (4.2.2)$$

여기서 벡터 $\boldsymbol{v}$는 Step 2에서 구한 $D\boldsymbol{v}=(0,\cdots,0,1)^T$의 해 $\boldsymbol{v}$이다.

Step 4. Step 3에서 구한 K'에 가우스 소거법을 하여 상삼각행렬인 U를 생성한다. 만약 가우스 소거법으로 얻어낸 행렬 U가 상삼각행렬이 아니라면 $f_{2n}(x)$는 CA다항식이 아니다. STOP.

Step 5. Step 4에서 구한 행렬 $U=(u_{i,j})$로부터 아래의 식 (4.2.3)을 이용하여 $R_{n-1}=< d_1\, d_2 \cdots\ d_{n-1} >$을 구한다.

$$d_i = \begin{cases} u_{1,2} & , i=1 \\ u_{i-1,i}+u_{i,i+1} & , 2 \le i \le n-2 \\ u_{i-1,i} & , i=n-1 \end{cases} \qquad (4.2.3)$$

[9]에서 제안한 알고리즘의 Step 1에서는 D를 얻기위해 모듈연산 $x^{i-1}+x^{2i-1}+x^{2i} \bmod f(x)$ $(i=1,\cdots,2n)$을 수행해야 한다.

하지만 $f(x)$가 최대무게다항식이 되는 경우에는, $GF(2)$위에서 $(x^n+x^{n-1}+\cdots+x+1)(x+1)=x^{n+1}+1$ 이기 때문에 $x^{i-1}+x^{2i-1}+x^{2i} \bmod f_n(x)$로 구성된 행렬 D를 이루는 요소들의 규칙성을 찾을 수 있다. 따라서 모듈연산을 시행하지 않고도 행렬 D를 구하는 것이 가능하게 된다.

예를 들어, $f_{10}(x)$에 대응하는 행렬 D는 다음과 같다.

$$D=\begin{pmatrix}
1&1&1&0&0&0&0&0&0&0\\
0&1&0&1&1&0&0&0&0&0\\
0&0&1&0&0&1&1&0&0&0\\
0&0&0&1&0&0&0&1&1&0\\
1&1&1&1&0&1&1&1&1&0\\
1&1&0&0&0&1&0&0&0&0\\
0&0&1&1&0&0&1&0&0&0\\
0&0&0&0&1&1&0&1&0&0\\
0&0&0&0&0&0&1&1&1&0\\
0&0&0&0&0&0&0&0&1&0
\end{pmatrix}$$

행렬 D의 i번째 행 $\boldsymbol{d}_i$ $(i=1,\cdots,2n)$은 식 (4.2.1)과 같다.

식 (4.2.1)에 따라, 모듈연산 $x^{i-1}+x^{2i-1}+x^{2i} \bmod f_{2n}(x)$ $(i=1,\cdots,2n)$을 수행 하지 않고도 행렬 D를 얻을 수 있다.

[9]에서 제안한 알고리즘의 Step 3에서는 동반행렬 C와 $D\boldsymbol{v}=(0,\cdots,0,1)^T$의 해 v를 이용하여 Krylov 행렬 K을 구해야 한다. 이어서 Step 4에서 Krylov 행렬 K로부터 가우스 소거법을 거쳐 U를 얻어낸 뒤, Step 5의 과정을 거쳐 상태전이규칙을 얻을 수 있다.

최대무게다항식 $f_{2n}(x)$의 경우, 이에 대응하는 상태전이 규칙이 $< R_{n-1}01R_{n-1}^{*} >$의 형태이며, $c_{n-1}=1$이므로 a_{n-1}=0임을 유도할 수 있다. $i=1, \cdots, n-2$에 대하여 $a_i = u_{i,i+1}$가 행렬의 $(i, i+1)$항의 원소라고 할 때, 오로지 이 원소들만을 이용하여 상태전이 규칙 R_{n-1}을 구할 수 있다. $a_i (i=1, \cdots, n-2)$는 $(2n)\times(2n)$ Krylov 행렬 K의 $(n-1)\times(n-1)$ 좌측 상단 부분행렬인 K'로부터 얻을 수 있다.

예를 들어, $f_{10}(x)$에 대응하는 Krylov 행렬 K와 K의 좌측 상단 부분행렬인 K'는 아래와 같다.

$$K=\begin{pmatrix}1&1&0&0&1&0&0&1&1&0\\1&0&0&1&0&0&1&1&0&1\\0&0&1&0&0&1&1&0&1&1\\0&1&0&0&1&1&0&1&1&1\\1&0&0&1&1&0&1&1&1&0\\0&0&1&1&0&1&1&1&0&0\\0&1&1&0&1&1&1&0&0&1\\1&1&0&1&1&1&0&0&1&0\\1&0&1&1&1&0&0&1&0&0\\0&1&1&1&0&0&1&0&0&1\end{pmatrix} \quad K'=\begin{pmatrix}1&1&0&0\\1&0&0&1\\0&0&1&0\\0&1&0&0\end{pmatrix} \quad U'=\begin{pmatrix}1&1&0&0\\0&1&0&1\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

$D\boldsymbol{v}=\boldsymbol{e}_{2n}$의 해가 $\boldsymbol{v}=(v_1, v_2, \cdots, v_{2n})^T$일 때, 동반행렬 C와 $\boldsymbol{v}$로 생성한 $(2n)\times(2n)$ Krylov 행렬 K의 $(n-1)\times(n-1)$ 좌측 상단 부분행렬인 $K'=(k_{ij}')_{(n-1)\times(n-1)}$는 식 (4.2.2)를 통하여 구성된다.

식 (4.2.2)를 통해, Krylov 행렬을 구하지 않고도 Step 4, Step 5를 진행할 수 있다. $f_{2n}(x)$에 대응하는 상태전이규칙 $< R_{n-1}01R_{n-1}^{*} >$을 얻기 위해서는, 식 (4.2.2)로 생성한 K'를 통해 R_{n-1}를 구하면 된다.

[표 4.2.1]은 제안된 알고리즘으로 최대무게다항식 $f_{2n}(x)$에 대응하는 90/150 CA를 구하는데 걸리는 시간을 기존의 알고리즘[9]과 비교한 결과이다. 두 알고리즘에 대하여 동일한 컴퓨터로 MAPLE 프로그램을 이용하여 산출한 결과이다.

[표 4.2.1] 알고리즘 시간 비교(시간 : 초)

차수	Previous[9]	New
40	0.406	0.218
100	1.451	0.905
250	32.526	6.786
350	132.851	20.498
450	384.059	48.235

이어서 다음 정리는 홀수차 최대무게다항식에 대응하는 CA의 합성법에 대한 정리이며, 본 논문에서 제안한 알고리즘과 함께 모든 차수 최대무게다항식에 대응하는 CA를 합성할 수 있음을 보인다.

<정리 4.2.2 [15]> $f_m(x)$가 CA다항식이면 $f_{2m+1}(x)$도 CA다항식이다. 또한 $f_m(x)$에 대응하는 CA가 $< a_1\, a_2 \cdots\ a_m >$인 경우, 90/150 CA 규칙 $< a_1\, a_2 \cdots\ a_m\ 1\ a_m \cdots\ a_2 a_1 >$가 $f_{2m+1}(x)$에 대응한다.

예를 들어 $f_{39}(x)$에 대응하는 90/150 CA를 구하려하는 경우, $f_4(x)$에 대응하는 90/150 CA가 $R_4 = < 0010 >$라고 하면, 정리 4.2.2를 통하여 $f_9(x)$에 대응하는 90/150 CA $R_9 = < R_4 1 R_4^* >$, 같은 방법을 반복하여 $R_{19} = < R_9 1 R_9^* >$ 그리고 $R_{39} = < R_{19} 1 R_{19}^* >$를 구할 수 있다. 즉 홀수차

인 높은 차수의 최대무게다항식에 대응하는 90/150 CA를 구하려는 경우, 낮은 차수의 최대무게다항식에 대응하는 90/150 CA 전이규칙 블록을 이용하여 구하는 것이 가능하다.

이에 따라 모든 차수 n에 대하여 $f_n(x)$가 CA다항식이라면 $f_n(x)$에 대응하는 CA 규칙을 합성하는 것이 가능함을 보였다.

Ⅴ. 의사난수생성기 비교

이 장에서는 최대무게다항식에 대응하는 LFSR과 90/150 CA로 생성한 의사난수생성기의 특징을 비교한다.

최대무게다항식에 대응하는 두 종류의 선형 FSM인 LFSR과 90/150 CA는 공통점과 차이점들을 가지고 있다.

같은 최소다항식에 대응하는 LFSR과 CA로 생성한 수열의 구조는 동형이다[8]. LFSR과 CA은 입력값에 따라 변이되는 상태는 비록 다르지만, 같은 특성다항식에 대응하여 생성하였다면 반드시 동형인 상태전이를 가진다는 것을 알 수 있다.

하지만 최대무게다항식에 대응하는 LFSR은 오로지 동반행렬이라고 하는 정해진 상태전이 형태를 가지지만, 90/150 CA는 존재하는 경우도 있고, 존재한다면 반드시 한 가지 이상의 상태전이 형태를 가진다는 특징을 가진다. [표 5.1.1]에서 LFSR과 90/150 CA에 따른 의사난수생성기 특징들을 비교하였다.

[표 5.1.1] f_n에 대응하는 선형 FSM으로 생성한 의사난수생성기

특성	LFSR	90/150 CA
주기	$n+1$의 약수	$n+1$의 약수
존재성	항상 존재	특성다항식이 가약인 경우 존재성 보장 불가능
FSM형태	동반행렬	존재한다면 복수형태 존재

Ⅵ. 결론

사용처에 적합한 의사난수생성기를 제작하기 위해 어떤 구조와 특성을 기반으로 해야하는지를 선택하는 것은 중요한 문제이다. 따라서 본 논문에서는 잘 알려진 선형 FSM인 LFSR과 90/150 CA에 초점을 맞추어 각 구조의 특성다항식이 '최대무게다항식'이 되는 경우에 대한 의사난수생성기를 연구하였다.

최대무게다항식 f_n에 대응하는 LFSR는 반드시 동반행렬이라는 형태로 상태전이행렬이 결정된다. 그에반해 최대무게다항식 f_n에 대응하는 90/150 CA는 항상 존재한다는 보장도 없고, 만약 존재한다고 해도 어떠한 형태의 상태전이행렬로 결정되는지에 대해서 알기 어렵다는 문제점이 존재하고 있었다.

본 논문에서는 짝수차 최대무게다항식 f_{2n}에 대응하는 90/150 CA를 효율적으로 생성하는 알고리즘을 제안하였다. 또한 홀수차 최대무게다항식에 대응하는 90/150 CA도 전이규칙 블록을 이용하여 간단히 합성할 수 있음을 살펴보았으며 이와같은 방법은 기존에 알려진 90/150 CA 합성법보다 더욱 빠른 수행속도를 가진다는 것을 살펴보았다.

참 고 문 헌

[1] J. Von Neumann, “Various techniques used in connection with random digits,” in A.S. Householder, G.E. Forsythe, and H.H. Germond, eds., Monte Carlo Method, National Bureau of Standards Applied Mathematics Series, Vol. 12, U.S. Government Printing Office, Washington, D.C., pp. 36-38, 1951.

[2] S.K. Park, and K.W. Miller, “Random Number Generators: Good Ones Are Hard To Find,” Communications of the ACM. Vol. 31, No. 10, pp. 1192-1201, 1988.

[3] D. Harris, and S. Harris, “Digital Design and Computer Architecture 2nd Edition,” Morgan Kaufmann, 2012.

[4] B. Elaine, B. William, B. William, P. William, and S. Miles, “Recommendation for Key Management,” NIST Special Publication 800-57. NIST. Retrieved 19 August 2013.

[5] K. Cattell, and J.C. Muzio, “Synthesis of one-dimensional linear hybrid cellular automata”, IEEE Trans. Comput-Aided Design Integr. Circuits Syst., Vol. 19, No. 2, pp. 325-335, 1996.

[6] S. Golomb, *Shift Register Sequences,* Aegean Park Press, California, 1967.

[7] A. Klein, “Linear Feedback Shift Registers,” Stream Ciphers, Springer, London, 2013.

[8] P.P. Chaudhuri, D.R. Chowdhury, S. Nandy, and C. Chattopadhyay, *Additive Cellular Automata: Theory and Applications*, Vol. 1, IEEE Computer Society Press, California, 1997.

[9] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim, and S. H. Heo,

"New synthesis of one-dimensional 90/150 linear hybrid group cellular automata," IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., Vol. 26, No. 9, pp. 1720-1724, 2007.

[10] Stepan Bilan, *Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities,* IGI Global, 2017.

[11] C. Krishna, A. Jas, and N.A. Touba, "Achieving high encoding efficiency with partial dynamic LFSR reseeding," *ACM Trans.* Design Automation of Electronic Systems, Vol. 9, pp. 500-516, 2004.

[12] C.C. Krishna and N.A. Touba, "Reducing test data volume using LFSR reseeding with seed compression," in Proceeding IEEE ITC, pp. 321-330, 2002.

[13] R. Lidl and H. Niederreiter, *Finite Fields,* Cambridge University, 1997.

[14] U.S. Choi and S.J. Cho, "Characteristic Polynomial of 90 UCA and Synthesis of CA using Transition Rule Blocks," Journal of the Korea Institute of Electronic Communication Sciences, Vol. 13, No. 3, pp. 593-600, 2018.

[15] U.S. Choi, S.J. Cho, H.D. Kim, and J.G. Kim, "90/150 CA Corresponding to Polynomial of Maximum Weight," Journal of Cellular Automata, Vol. 13, pp. 347-358, 2018.

[16] U.S. Choi, S.J. Cho, H.D. Kim, J.G. Kim, and S.W. Kang, "Synthesis of even-cell 90/150 MWCA," Submitted.