카오스적인 랜덤신호 발생에 관한 연구
(A Study on the Chaotic Random Signal Generator)

구 인 수, 김 환 우

한국원자력연구소, 충남대학교

요약

기존 의사 랜덤순서 발생회로에서 존재하는 출력이 일치할 가능성을 없애고, 출력이 전 계에 골고루 이상적으로 분포시켜 랜덤성을 높일 필요가 있다.

본 논문은 기존의 의사 랜덤순서 발생회로에 결정론적 카오스 함수의 특성을 덧 붙임으로써 보다 랜덤성이 뛰어난 랜덤순서 신호를 발생시켰다.

결정론적 카오스 함수는 이미 카오스 특성이 입증된 텐트함수를 이용하였으며, 카오스적인 랜덤신호는 예측가능하면서, 혼돈적 특성으로 인해 보다 랜덤한 카오스적인 랜덤신호 발생회로와 개념을 제시하였다.

I. 서 론

혼돈(chaos)이라고 믿는 수많은 현상을 결정론적 혼돈(deterministic chaos)으로 해석하고, 이를 응용하여 과학과 기술의 새로운 차원을 열고 있다. 혼돈과정(chaos process)에서 초기조건의 미미한 변화가 출력(outcome)에서 아주 크게 달라지므로, 작은 섭동(fluctution)이나 잡음의 증폭에 기인해서 새로움과 다양함을 가지면서 자연계에 존재하는 계를 자연계 혹은 혼돈계라 한다.[1],[4]

어떤 비선형 역학계인 혼돈계는 혼란한 랜덤과정을 거치는데, 실제는 예측 가능한 결정론적 과정이다. 결정론적 과정의 의미있는 랜덤변화는 여전히 혼돈 매커니즘 통제하에 있으며, 과도상태 후에는 끌림의 구역에 수렴한다. 랜덤변화가 발생하는 혼돈 발생기인 비선형 연속함수를 이용하는 연속 혼돈발생기와 표본을 표현하는 비트를 이용하는 논리 혼돈 발생기, 양쪽 모두가 랜덤과정이나 순서를 거친다.[3] 즉, 혼돈력학을 컴퓨터에 응용하는데는 랜덤 숫자나 랜덤이진파형이 필요하다. 따라서, 본 논문은 의사이진순서를 발생하는 여러 방법중에서 쉬프트 레지스터와 결정론적 혼돈함수를 이용하여 다양한 부호화 랜덤순서를 발생하는 방안을 나타낸다.

본 논문에서 제시하는 혼돈 랜덤순서발생은 쉬프트 레지스터와 modulo-2 가산기에 의해 불규칙 순서를 발생하는 랜덤순서 발생기의 의사랜덤변환 개념에 혼돈력학의 개념이 가미된 것이다.

II. 기존 랜덤순서 발생기와 결정론적 혼돈순서 발생

가. 기존 랜덤순서 발생기[2]

1) 원리

선형 쉬프트 레지스터는 단순히 modulo-2 가산기와 쉬프트 레지스터로 구성한다. 이진 가산기의 진치표는 배타적 합의 논리와 일치하므로 배타적 합의 게이트라고도 한다. 이 배타적 합의 게이트를 여러 단의 레지스터에 연결하여 하나 이상의 폐루프를 만들고, 폐루프 쉬프트 레지스터 회로에 펄스를 인가하면 레지스

터 회로의 출력은 이진 순서로 나타나는 데, 이 디지틀 순서는 궤환연결과 초기 부하치에 따라 다르다.기존의 좌 쉬프트 레지스터를 이용한 의사 랜덤 순서발생의 기본적인 예시는 아래그림 1과 같다.

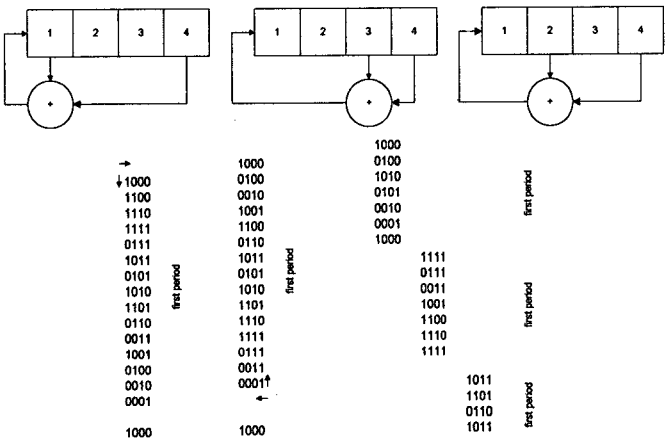


그림 1 좌 쉬프트 레지스터에 의한 의사랜덤순서 발생

Fig. 1. Left shift-register generation of psedo-random sequences

그림1 에서 쉬프트 레지스터의 길이 $n=4$이며, 좌측에서 첫째 비트, 둘째 비트 혹은 첫째 단, 둘째 단 등으로 부른다. 상기 그림중 첫째 레지스터와 둘째 레지스터는 순서 발생이 서로 역의 관계인 궤환련결이다. 그림에서 임의의 m단에서 $n-m$ 단으로 궤환련결을 이동하면, 역 순서를 만들 수 있다

n	m or $n-m$	2^n-1	n	m or $n-m$	2^n-1
3	1	7	18	7	262,143
4	1	15	19	none	-
5	2	31	20	3	1,048,575
6	1	63	21	2	2,097,151
7	1 or 3	127	22	1	4,194,303
8	none	-	23	5 or 9	8,388,607
9	4535	511	24	none	-
10	3	1,023	25	3 or 7	33,554,431
11	2	2,047	26	none	-
12	none	-	27	none	-
13	none	-	28	3, 9 or 13	268,435,455
14	none	-	29	2	536,870,911
15	1, 4 or 7	32,767	30	none	-
16	none	-	31	3,6,7 or 13	2,147,483,647
17	3, 5 or 6	131,071	32	none	-
			33	13	8,589,934,591

Table 1. Maximum length generated and feedback connection for maximum length

셋째 레지스터는 사단 좌측 쉬프트 레지스터에서 발생할 수 있는 또 다른 디지틀 순서(이진순서)를 나타낸다.상기 세 개의 레지스터를 통해 출력순서를 최대 길이 순서와 최대 길이가 아닌 순서로 나눌 수 있다. 단을 갖는 n쉬프트 레지스터의 최대 길이 순서는 2^n-1이며, 궤환련결방법에 따라 최대 길이 순서가 발생하거나, 발생하지 않는다.

다음은 하나의 배타적 합 게이트 만을 연결하여 최대 길이를 갖는 궤환련결방법에 관한 사항이다.

표 1. 최대 길이를 갖는 궤환연결과 발생하는 최대길이

표 1. 에서 파악된 각각의 이진 최대 길이 순서는 배타적 합 게이트를 이용한 궤환에 의해 발생하는 데, 실존하는 랜덤순서로 여길수 있을 만큼 확실하게 의사 랜덤 특징을 갖는다.

그림 1에서 살펴보면 좌측 쉬프트 레지스터에서 발생한 의사 랜덤순서가 초기상태에 종속함을 보인다. 즉, 최대 길이를 위한 궤환련결 경우 쉬프트 레지스터에 주어진 초기상태가 다르더라도 결국은 같은 상태를 만들게 되며, 한 주기를 이루는 출력의 순서가 다를 뿐이다. 최대 길이를 갖지않는 궤환련결 경우 초기상태가 다르면 다른 순서를 발생한다. 참고로 최대 길이 순서의 주기 비트 수는 2^n-1개이고, 0의 비트 수는 1의 비트 수보다 정확히 하나가 작다.

기존의 배타적 합 게이트를 궤환연결로 갖는 n 비트(혹은 n단) 쉬프트 레지스터는 $\frac{\delta(p)}{n}$개의 서로 다른 최대 길이의 순서를 발생시킬 수 있음이 밝혀졌다. (여기서, $\delta(p)$는 n보다 작은 양의 정수이고, 오일러 수(Euler's number)라 한다.

간혹, 몇몇 랜덤순서발생에 두 개이상의 배타적 합 게이트를 궤환련결로 이용하는 데, 상기 표의 경우 오직 하나의 궤환련결(하나의 배타적 합 게이트)만을 사용하여 발생된 최대 길이 의사 랜덤순서라는 것에 주목하면, 결정론적 카오스함수를 구현하는 궤환련결을 이용하여 보다 랜덤하며 보다 긴 최대 길이를 갖는 이진순서를 발생시킬 수 있음을 고려한다.

2) 기존 랜덤순서 변환의 개념

전자회로내에서 회로변수의 변화를 의미하는 신호를 기술자(descriptor)라 부르는 디지틀 수로 표현 가능하다.

거의 모든 기술자는 다음의 다항식으로 표현할 수 있다.

$$D(x) = a_d\, x^d + a_{d-1}\, x^{d-1} + \cdots + a_1\, x + a_0$$

여기서, $a_0, a_1, a_2, \cdots, a_d$ 는 갈로이스계(Galois field) $GF(2)$의 요소이고, 0 이나 1 중 하나를 갖는다. 예를 들면, $D_5 = 000\cdots101$이면, 십진값은 5이며, 다항식의 계수는 $a_0 = a_2 = 1$, $a_1 = a_3 = a_4 = \cdots = a_d = 0$이 된다. 이 다항식의 차수는 d이다.

그리고, 차수 d 인 다항식 $D(x)$에 상기 수 5인 정의된 또 다른 다항식 $S(x)$를 곱하면, 차수가 $d+s$인 다항식 $M(x)$를 얻는다. 이때 곱하는 다항식 $S(x)$의 모든 계수, $b_{s-1}, b_{s-2}, \cdots, b_1, b_0$가 모두 0 이고 오직 $b_s = 1$이면, 다항식 $M(x)$는 다음과 같이 표현 가능하다.

$$D(x)\cdot S(x) = (a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0)(b_s x^s + b_{s-1}x^{s-1} + \cdots + b_1 x + b_0) = M(x) \quad \text{------ (1)}$$

$$M(x) = c_m x^{d+s} + c_{m-1}x^{d+s-1} + \cdots + a_1 b_0 x + b_1 a_0 x + a_0 b_0 \quad \text{----------(2)}$$

여기서 $m = d+s$ 이다.

식 (1)에서 오직 $b_s = 1$ 이므로, 식 (2) 는 다음과 같이 다시 쓸 수 있다.

$$M(x) = c_d x^{s+d} + \cdot \cdot \cdot + c_1 x^{s+1} + c_0 x^s \quad \text{--- (3)}$$

식 (3)에서, $c_d = a_d$이므로, $c_0, c_1, \cdot \cdot \cdot, c_d$도 역시 갈로이스계 $GF(2)$의 요소이며, 0 이나 1 값을 갖는다. 결국 다항식 $M(x)$는 s위치에 대해 왼쪽으로 편이(shift)한 기술자이다.

다음으로 다항식 $M(x)$를 다항식 $T(x)$로 나누면, (이때 차수 관계는 $s \geq t$ 이다)

$$M(x) = Q(x)T(x) + R(x) \quad \text{---------- (4)}$$

라는 식을 얻으며, 나머지인 다항식 $R(x)$는 다항식 $T(x)$의 차수 t 보다 작은 차수를 갖는다.

기존의 랜덤순서 변환과정에서는 식 (4)에서의 다항식 $R(x)$를 기술자의 번지 수로 사용한다.

이는 물리적 계안에 있는 근접한 서로 다른 기술자는 차수가 t 인 거의 모든 다항식에 대해 나머지인 서로 다른 다항식 $R(x)$를 만들기 때문이다.

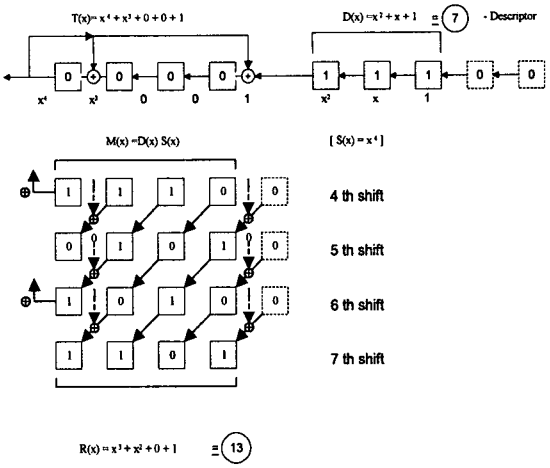


그림 2. 의사 랜덤 디지틀 변환

Fig. 2. Pseduo-random digital transformation

즉, 기술자는 물리적인 계의 임의의 지점에서 발생 가능하며, 기술자를 표현하는 다항식에서 만들어지는 나머지 다항식은 2^t개의 서로 다른 메모리 번지 중 하나를 표현할 수 있다. 원시 기술자에 관한 다항식 $D(x)$가 t 보다 작은 차수를 갖는 경우 $T(x)$ 로 나눈 나머지 $R(x) = D(x)$ 일 것이다.

이런 기술자의 변환은 랜덤화 효과(randomizing effect)가 없으므로 먼저 $S(x)$를 곱해야 한다. 이와 같이 t보다 작은 차수인 기술자는 $S(x)$를 곱하는 것은 기술자간의 거리를 멀리하고, 물리적인 계를 증가시키는 데도 필요하다. 그림 2는 이와 같은 랜덤변화의 예로 갈로이스계 코드(Galois field code)로 수를 세는 회로이다.

그림 2 에서 기술자 다항식 $D(x)$는 십진수 7에 해당하며, 변환에 관계하는 $T(x)$의 차수는 4이다. 처음 4개의 쉬프트 레지스터는 $S(x) = x^4$에 의한 곱을 의미하고, 4번째에서 7번째 쉬프트까지는 궤환 연결로 결정되는 변환 다항식 $T(x)$에 의해 다항식 $M(x) = D(x) \cdot S(x)$를 나눈 나머지, $R(x)$이다.

$R(x)$의 차수는 $t-1$이하이며, 기술자 $D(x)$번지를 t 승(t-tuple)으로 표현한다. 즉 번지수는 변환 식 $T(x)$의 차수에 종속이며, 최대 2^t 개의 다른 번지를 가질 수 있다. 또한, 변환에 이용하는 다항식의 처음과 끝의 계수 값이 모두 1, $a_t = a_0 = 1$ 을 가져야하므로, 차수 t인 경우에 2^{t-1}개의 서로 다른 변환 식이 존재할 수 있다.

다음 식은 구현 가능한 변환 식 $T(x)$의 수 ($2^{t-1} = 2^3 = 8$)에 대한 것이다.

$$T_0(x) = x^4 + 0 + 0 + 0 + 1$$

$T_1(x) = x^4 + 0 + 0 + x + 1$

$T_2(x) = x^4 + 0 + x^2 + 0 + 1$

$T_3(x) = x^4 + 0 + x^2 + x + 1$

$T_4(x) = x^4 + x^3 + 0 + 0 + 1$

$T_5(x) = x^4 + x^3 + 0 + x + 1$

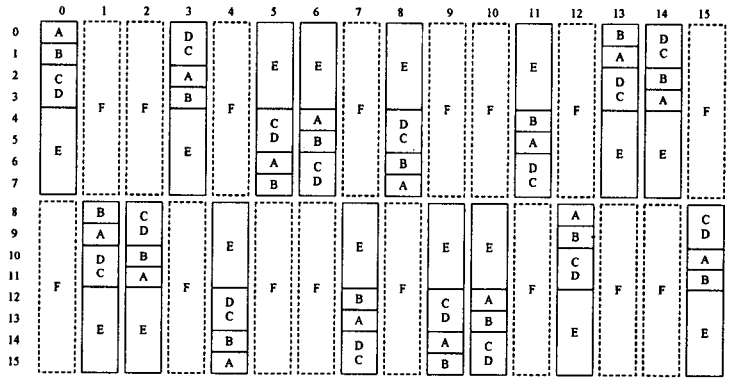
$T_6(x) = x^4 + x^3 + x^2 + 0 + 1$

$T_7(x) = x^4 + x^3 + x^2 + x + 1$

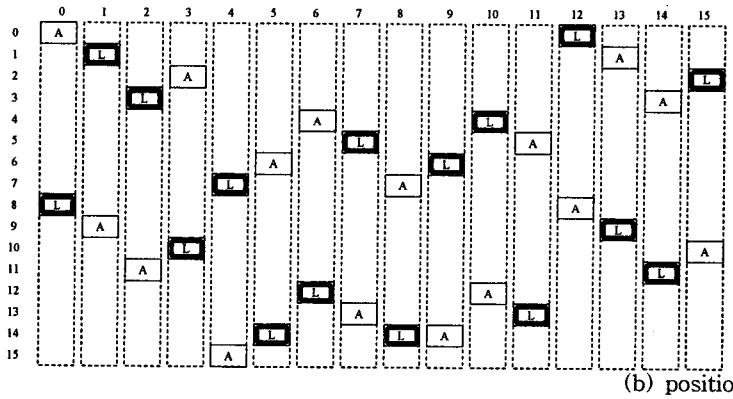
3) 다항식의 나눔에 의한 의사 랜덤변환의 성질

그림 3에서 크기가 16 x 16 인 기술자의 계(field of descriptors)에 의해 만들어지는 256개 번지의 계는 (a)에 표현하였고, 똑같은 번지 A 혹은 L을 만드는 기술자의 위치는 (b)에 나타냈다.

이와 같이 번지와 위치가 일치하는 기술자를 일치모듈로(congruent modulo), $T(x)$라 부르며, $T(x)$는 똑같은 잔여 층(residue class)을 형성한다. 서로 다른 잔여 층의 총수도 $2t$ 개로 계산할 수 있으며, 잔여 층에 해당하는 똑같은 번지를 갖는 기술자는 랜덤하게 256개의 잔여 층내에 분포된다.



(a) address



(b) position

그림 3 번지와 위치가 같은 기술자

Fig. 3 Position of the descriptors producing the same address

일치 모듈로 $T(x)$의 계수, a^{t-1}, a^{t-2}, $\cdot\cdot\cdot$, a_1을 변경하여 다항식으로 만든다 하더라도, 서로 다른 번지의 개수는 변하지 않으며, 2^t 개이지만, 혹시 몇 몇 다항식은 닮은 형태를 만들 수도 있다.

따라서, 이런 조그만 가능성조차도 없게끔 다항식을 선택한다. 이 다항식의 선택은 컴퓨터 모의실험으로, 갈로이스계 코드로 수를 세는 회로이며 최대주기 2^t를 갖는 차수 t의 다항식을 얻는다.

이런 회로의 예가 그림 2 이며, 배타적 합 게이트로 궤환연결된 4단 쉬프트 레지스터이다. 이 4단 쉬프트 레지스터는 최상의 궤환연결로 갈로이스계 $GF(2^4)$의 요소, 16가지의 다른 번지를 발생시키며 최대 주기의 크기는 16이다.

일반적으로 2^t개의 요소를 갖는 갈로이스계 $GF(2^t)$는 $GF(2)$ modulo $a_t x^t + a_{t-1}x^{t-1} + \cdot\cdot\cdot + a_1 x + a_0$의 전반에 걸친 다항식의 계와 흡사하게 형성가능하며, 이때의 계는 2^t개의 다른 번지에 해당한다.

변환 다항식 $T(x)$는 갈로이스계 코드 안에서 수를 세는 회로에 최대주기를 마련하기 위한 의사 랜덤 형태를 만드는, 랜덤 형태의 잔여 층에 속하는 기술자도 필연적으로 의사 랜덤하게 분포한다.

표 2 는 크기가 32x32인 기술자 계를 변환 다항식 $T(x)$로 나누어 발생시킨 1024개의 번지에 관한 의사 랜덤 형태를 나타낸다.

이때 변환 다항식은

$T(x) = x^5 + x^4 + 0 + x^2 + x + 1$의 형태이다.

표 2에서 행은 기술자 0-31로 인해 만들어진 1차 형태이며, 2차 형태를 형성하는 2t=32개의 또 다른 1차 형태는 열이다.

표에서 R은 같은 잔여 층에 속하는 몇 개의 기술자를 의미하므로, 0과 27번지는 잔여 층에 속한다.

지금까지 살펴본 바와 같이 변환은 인터럽트 루틴을 갖는 컴퓨터 데이터의 한 부분으로 실제화될 수 있거나, 아나로그-디지틀 변환의 하드웨어 한 부분으로 구현 가능하다.

즉, 변환회로를 통과함으로써, 각 기술자가 저장될 의사 랜덤 번지가 생성되는데, 이때 특정형태를 갖는 기술자의 번지가 전체 메모리에 걸쳐 골고루 분포한다면 이상적이지만, 실제는 같은 번지로 변환되는 두 개이상의 기술자가 있을 가능성이 있다. 이런 연유로 변환의 주목적은 목록의 탐색을 시작 번지 발생에 두어야 한다.

변환의 주목적으로 시작번지를 발생하는 방법은 기존 변환 모드 분석기에서처럼 직접 번지 지정이 가능하여 메모리 공간의 높은 이용을 가능케 한다.

표 2 32x32 기술자 계에서 발생한 1024개 번지의 형태

III. 결정론적 혼돈 순서 발생[5],[6],[7],[8]

다양한 함수가 결정론적 혼돈역학을 보이지만, 널리 알려진 톱니함수(saw-tooth function or Baker's function)를 이용하여 혼돈적인 거동을 나

타낸다.[5]

톱니함수 변환의 정량적인 현상은 전형적인 혼돈으로 판명되었고, 수식적으로 완전한 해석이 가능하므로 결정론적 혼돈역학을 살피는 데 유용하다.

톱니함수의 수식적인 정의는 다음과 같이 표현된다.

$$S(x) = \begin{cases} 2x, & x < \frac{\text{단위구간}}{2} \text{ 인 경우} \\ 2x-1, & x \geq \frac{\text{단위구간}}{2} \text{ 인 경우} \end{cases}$$

윗 식에서 단위구간의 범위는 [0,1)이다. 수식의 오른쪽 항은 2진수에 보다 쉽게 적용하기 위해 다음 식을 정의하면,

$Frac(x) = x - k$

(여기서 $k \leq x < k+1$이며, k는정수이다)

이제, 톱니함수의 새로운 수식적인 정의는 다음과 같다.

$S(x) = Frac(2x)$

(여기서 x의 범위는 $0 \leq x \leq 1$이다.)

위 식에 의해 단위간격에서 임의의 실수 x 에 대한 2진수 표현은 새롭게 해석할 수 있는 데, 예를 들면,

$\frac{1}{2} = 0.1$, $\frac{3}{4} = 0.11$, $\frac{1}{3} = 0.0101 \cdots = 0.\dot{0}\dot{1}$

등으로 표현하며, 방정식 $S(x) = Frac(2x)$에서 변수 x에 곱해지는 2는 임의의 실수에 관한 2진수 $0.a_1a_2a_3 \cdots a_k$

($a_1, a_2, a_3, \cdots a_k$는 0이나 1을 갖는다.)를 $a_1.a_2a_3 \cdots a_k$로 변환하는 것을 의미한다.

톱니함수의 변환은 2진비트의 왼쪽 이동 동작으로 간주할 수 있으며, 어떤 변수의 이진전개가 $x = a_1a_2a_3 \cdots a_k$라 할 때, 이 값을 k단 왼쪽 쉬프트 레지스터의 초기 값으로 놓으면, 주기는 k가 되며, k번보다 작은 몇 번의 왼쪽 이동에 의해 초기 값은 아주 다른 값으로 바뀐다.

예로, 임의의 두 변수의 이진전개를 각각 $x = a_1a_2a_3 \cdots a_{n-1}a_n$이고, $y = a_1a_2a_3 \cdots a_{k-1}a_k^*$이라 한다면 (여기서 $n = k$이며 a_k^*는 이중 이진수이다.), 두 변수 x와 y는 기껏해야 2^1정도의 크기 차이가 있으나 $k-1$번의 왼쪽 쉬프트 동작 후에는, 두 변수중 어느 한쪽의 값은 0이고 다른 한쪽은 1이 되어, 크기 차이는 극단적으로 되므로 혼돈역학의 초기조건에의 민감성(sensitive dependence on initial condition)이라는 특성을 보여준다.[6]

톱니함수변환의 또 다른 성질로 주기점의 밀집성(density of periodic points)을 들 수 있는데 앞의 예에서 살펴본 두 변수 x와 y의 차이는 기껏해야 2^1정도뿐이며, 왼쪽 이동순환(left shift rotation) 했을 경우, 주기 k를 갖고 순환하며 주기점은 밀집하게됨을 알 수 있다.

그리고, 적절한 두 변수의 이진전개가 임의의 주기를 갖고 순환할 때, 톱니함수변환의 적절한 반복에 의해서 한 변수에서 다른 변수로 바꿀 수 있다는 사실, 즉 혼돈역학에서는 혼합특성에 해당하는 성질도 내재되어 있음을 간접적으로 알 수 있다.

이와 같이 혼돈적인 거동을 나타내는 톱니함수

변환은 레지스터의 왼쪽이동 순환동작에 의해 쉽게 실현되므로, 혼돈순서 발생을 위한 결정론적 혼돈함수로써 톱니함수를 응용할 수 있다.[7],[8]

기존의 의사 랜덤순서를 발생시키기 위한 의사 랜덤 디지틀 변환에 관계된 회로를 보이고 있는 그림 2로 다시 돌아가 본다. 이 회로에서 다항식 $S(x)$만의 변경으로 결정론적인 혼돈순서를 발생시킬 수 있음을 쉽게 짐작할 수 있다. 다항식 $S(x)=x^4$대신에 톱니함수 $S(x)=Frac(2x)$를 이용한다면 그림 2는 다음 그림 4와 같이 변경되어야 할 것이다.

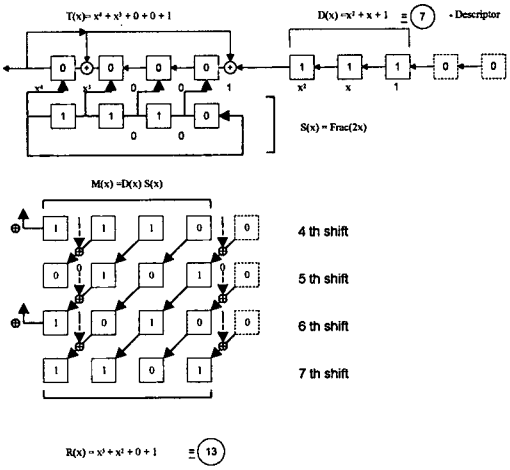


그림 4. 기술자 $D(x)$에 톱니함수 $S(x)$를 곱한 후, 4차 다항식 $T(x)$로 나누어 발생시킨 혼돈 순서 $R(x)$

Fig. 4 Generation of chaotic sequence $R(x)$, multiplying descriptor $D(x)$ by saw-tooth function $S(x)$ and dividing by polynomial $T(x)$ with degree 4.

그림 4의 예와 그림 2의 차이는 다항식 $S(x)=x^4$대신에 톱니함수 $S(x)=Frac(2x)$가 사용되었다는 것이다.

톱니함수에 의한 변환은 초기 값(기술자의 값을 이용할 수도 있으며, 임의의 톱니함수 값을 사용할 수도 있다)에 따라 달라지지만, 그림 2에서처럼 변환다항식 $T(x)$가 4차라면, 4단 왼쪽 쉬프트 레지스터에 의해 쉽게 실현될 수 있다.

따라서, $D(x)$에 $S(x)$를 곱하여 얻어지는 $M(x)$의 차수도 $d+s$로 구해지지만, 의사 랜덤 디지틀 변환의 경우에는 $S(x)$의 계수, b_{s-1}, b_{s-2}, $\cdot\cdot\cdot$, b_1, b_0이 모두 0이고 오직 $b_s=1$이었던 반면, 톱니함수 변환의 경우에서는 $S(x)$의 계수는 모두가 0이나 1이 아니어야 한다.

그림 2에서와 같이 4차 변환다항식 $T(x)$를 함께 이용했을 때, $S(x)=Frac(2x)$의 초기 값을 1110이라 한다면 (그림 4 참조), 초기 값에 따라 톱니함수변환은 1110, 1101, 1011, 0111과 같은 순서의 주기 4를 가지므로, 그림 2의 회로에서 발생하는 2^t개의 의사 랜덤순서보다 4배 많은 혼돈순서를 그림 4의 회로를 발생시킨다. 변환다항식 $T(x)$의 차수가 커질수록 혼돈순서는 보다 혼돈적이며 결정론적일 것이다.

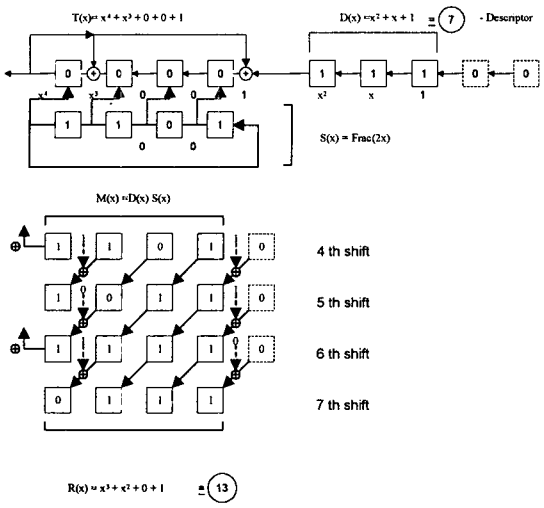


그림 5. 1110에 관한 톱니함수, 둘째 주기인 1101에 의해 발생한 혼돈순서 $R(x)$

그림 4의 나머지 $R(x)$의 값이 그림 2의 나머지 값과 동일해야함이 당연하며, 톱니함수 변환에 의하여 두 번째로 발생하는 값 1101로 초기 값으로 사용될 때에는 다른 나머지 값이 발생할 것이다. 그림 5는 값 1101에 의한 다른 나머지 값의 계산의 예다.

IV. 결론

임의의 신호에 대한 기술자의 다항식을 이용하여, 의사 랜덤 수나 순서를 만드는 기존의 디지틀 변환을 개선하기 위한 방안을 제안하였다.

기존의 의사 랜덤 디지틀 변환방법은 기술자 다항식을 다른 다항식으로 곱하고, 나누어 랜덤순서를 발생시키는 데, 곱하는 다항식, S(x)를 혼돈거동이 나타나는 톱니함수로 대치함으로서 보다 랜덤한 순서, 즉, 결정론적 혼돈순서발생에 관한 방안을 제시하였다. 또한, 혼돈순서발생을 구현할 회로를 기존 의사랜덤순서발생회로에 준하여 나타내었으므로, 기존 방식에 비해 랜덤성이 보다 뛰어남을 쉽게 비교할 수 있다.

후기

본 연구는 과학기술부의 원자력연구 개발사업의 일환으로 수행되었음.

참고문헌

1. Denny Gulick, Encounters with chaos, McGraw-Hill, New York, pp. 96-103, 1992.
2. V. Bonacic, B. Soucek and K. Culjat, Pseudo-random digital transformation, Nuclear Instr. Meth. 66, 213, 1968.
3. B. Soucek and the IRIS Group, Dynamic, genetic and chaotic programming, John Wiley & Sons, Inc., pp. 456-469, 1992.
4. Heinz Georg Schuster, Deterministic chaos, Verlags gesellschaft mbH, pp. 1, pp. 21-36, 1989.
5. Heinz-Otto Peitgen, Hartmut Jurgens and Dietmar Saupe, Chaos and fractals, Springer-Verlag, New York, pp. 509-583, 1992.
6. K. H. Park, J. S. Hwang and C. E. Chung, Implementation of chaotic state machine using deterministic chaos function, JEEIS, vol. 3, no. 2, April 1998.
7. 구 인수 외, 결정론적 카오스함수를 이용한 상태머신, 대한전자공학회 추계학술대회, 1995.

8. 정 종은 외, 카오스 상태머신의 구현, 회로 및 시스템 연구회, 전력연구회 학술대회, 대한전자공학회, 1995.