

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

구인수* 김환우**
(In-Soo Koo) (Hwan-Woo Kim)

요약 디지털 의사 랜덤변환의 출력이 같은 랜덤성을 갖는 것을 방지하기 위해서 카오스적인 처리과정이라 부르는 보다 랜덤하고 결정론적인 변환과정을 소개하였다. 카오스적인 변환과정을 거치면, 카오스적인 랜덤순서가 발생하는 데, 이 카오스 변환은 결정론적 카오스함수를 기본으로 설계하였으며, 쉬프트 레지스터와 같은 간단한 하드웨어로 구현할 수 있었다. 본 논문에서는 쉬프트 레지스터로 구현한 카오스변환 회로를 제시하였고, 제시한 회로의 카오스적인 거동은 카오스 거동을 갖는 톱니함수 특성으로 설명하였다.

Abstract To prevent the congruent output of the digital psuedo-random transformation from giving the same randomness, a transformation of seemingly random deterministic process, called Chaotic transformation, is introduced. Passing through a Chaotic transformation, each event(descriptor) will produce chaotic random sequences. Chaotic transformation is designed on the basis of deterministic chaos function and also can be realized by simple hardware like shift registers. The circuit of chaotic transformation implemented with the shift registers is presented and the chaotic behavior of suggested circuit is explained with the characteristics of saw-tooth function with the chaotic behavior.

1. 서론

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(fluctuation)이나 잡음의 증폭에 기인해서 새로움과 다양함을 가지면서 자연계에 존재하는 계를 자연계 혹은 혼돈계라 한다.[1],[4]

어떤 비선형 역학계인 혼돈계는 혼란한 랜덤과정을 거치는데, 실제로는 예측 가능한 결정론적 과정이다. 결정론적 과정의 의미있는 랜덤변화는 여전히 혼돈 매커니즘 통제하

에 있으며, 과도상태 후에는 끌림의 구역에 수렴한다. 랜덤 변화가 발생하는 혼돈 발생기인 비선형 연속함수를 이용하는 연속 혼돈발생기와 표본을 표현하는 비트를 이용하는 논리 혼돈 발생기, 양쪽 모두가 랜덤과정이나 순서를 거친다.[3] 즉, 혼돈역학을 컴퓨터에 응용하는 데는 랜덤 숫자나 랜덤이진과형이 필요하다. 따라서, 본 논문은 의사이진 순서를 발생하는 여러 방법중에서 쉬프트 레지스터와 결정론적 혼돈함수를 이용하여 다양한 부호화 랜덤순서를 발생하는 방안을 나타낸다. 본 논문에서 제시하는 혼돈 랜덤 순서발생은 쉬프트 레지스터와 modulo-2 가산기에 의해 불규칙 순서를 발생하는 랜덤순서 발생기의 의사랜덤변환 개념에 혼돈역학의 개념이 가미된 것이다.

* 한국원자력연구소

** 충남대학교

† 본 연구는 과학기술부의 원자력연구 개발사업의 일환으로 수행되었음.

2. 기존 랜덤순서 발생기와 결정론적 혼돈순서

발생

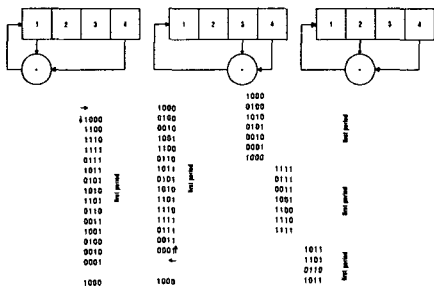
2.1. 기존 랜덤순서 발생기[2]

2.1.1 원리

선형 쉬프트 레지스터는 단순히 modulo-2 가산기와 쉬프트 레지스터로 구성한다. 이진 가산기의 진리표는 배타적 합의 논리와 일치하므로 배타적 합의 게이트라고도 한다. 이 배타적 합의 게이트를 여러 단의 레지스터에 연결하여 하나 이상의 페루프를 만들고, 페루프 쉬프트 레지스터 회로에 펄스를 인가하면 레지스터 회로의 출력은 이진 순서로 나타나는 데, 이 디지털 순서는 케환 연결과 초기 부하치에 따라 다르다.

기존의 좌 쉬프트 레지스터를 이용한 의사 랜덤순서 발생의 기본적인 예시는 아래 <그림 1>과 같다.

<그림 1>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 케환 연결이다. 그림에서 임의의 m 단에서 $n-m$ 단으로 케환 연결을 이동하면, 역 순서를 만들 수 있다. 셋째 레지스터는 사단 좌측 쉬프트 레지스터에서 발생할 수 있는 또 다른 디지털 순서(이진 순서)를 나타낸다.



<그림 1> 좌 쉬프트 레지스터에 의한 의사랜덤순서 발생

상기 세 개의 레지스터를 통해 출력순서를 최대 길이 순서와 최대 길이가 아닌 순서로 나눌 수 있다. n 단을 갖는 쉬프트 레지스터의 최대 길이 순서는 2^n-1 이며, 케환 연결방법에 따라 최대 길이 순서가 발생하거나, 발생하지 않는다.

다음은 하나의 배타적 합 게이트만을 연결하여 최대 길이를 갖는 케환 연결방법에 관한 사항이다.

<표 1> 최대 길이를 갖는 케환 연결과 발생하는 최대 길이

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 or 3	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

<표 1>에서 파악된 각각의 이진 최대 길이 순서는 배타적 합 게이트를 이용한 케환에 의해 발생하는 데, 실존하는 랜덤순서로 여길 수 있을 만큼 확실하게 의사 랜덤 특성을 갖는다.

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

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

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

2.1.2 기존 랜덤순서 변환의 개념

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

거의 모든 기술자는 다음의 다항식으로 표현할 수 있다.

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

여기서, $a_0, a_1, a_2, \dots, a_d$ 는 갈로이스계(Galois field) $GF(2)$ 의 요소이고, 0 이나 1 중 하나를 갖는다. 예를 들면, $D_5 = 000\dots101$ 이면, 십진값은 5이며, 다항식의 계수는

$a_0 = a_2 = 1, a_1 = a_3 = a_4 = \dots = a_d = 0$ 이 된다. 이 다항식의 차수는 d 이다.

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, $b_{s-1}, b_{s-2}, \dots, b_1, b_0$ 가 모두 0 이고 오직 $b_s=1$ 이면, 다항식 $M(x)$ 는 다음과 같이 표현 가능하다.

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

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

여기서 $m = d + s$ 이다.

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

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

식 (3)에서, $c_d = a_d$ 이므로, c_0, c_1, \dots, c_d 도 역시 갈로이스계 $GF(2)$ 의 요소이며, 0 이나 1 값을 갖는다. 결국 다항식 $M(x)$ 는 s 위치에 대해 왼쪽으로 편이(shift)한 기술자이다. 여기서, $c_d = a_d$ 를 일반식으로 확장하면, $c_i = a_i$ 로 표현할 수 있다.

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

$$M(x) = Q(x)T(x) + R(x) \quad (4)$$

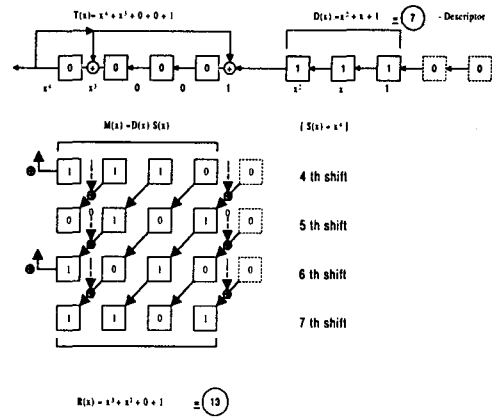
라는 식을 얻으며, 나머지인 다항식 $R(x)$ 는 다항식 $T(x)$ 의 차수 t 보다 작은 차수를 갖는다.

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.

즉, 기술자는 물리적인 계의 임의의 지점에서 발생 가능하며, 기술자를 표현하는 다항식에서 만들어지는 나머지 다항식은 2^t 개의 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 t 보다 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> 의사 랜덤 디지털 변환

<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 t 인 경우에 2^{t-1} 개의 서로 다른 변환 식이 존재할 수 있다.

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

- $T_0(x) = x^4 + 0 + 0 + 0 + 1$
- $T_1(x) = x^4 + 0 + 0 + x + 1$
- $T_2(x) = x^4 + 0 + x^2 + 0 + 1$
- $T_3(x) = x^4 + 0 + x^2 + x + 1$
- $T_4(x) = x^4 + x^3 + 0 + 0 + 1$
- $T_5(x) = x^4 + x^3 + 0 + x + 1$
- $T_6(x) = x^4 + x^3 + x^2 + 0 + 1$
- $T_7(x) = x^4 + x^3 + x^2 + x + 1$

2.1.3 다항식의 나눔에 의한 의사 랜덤변환의 성질[9]

크기가 16×16 인 기술자의 계(field of descriptors)에 의해 만들어지는 256개 번지 중 번지와 위치가 일치하는 기술자를 일치모듈로(congruent modulo), $T(x)$ 라 부르며,

$T(x)$ 는 똑같은 잔여 층(residue class)을 형성한다.

일치 모듈로 $T(x)$ 의 계수, $a^{t-1}, a^{t-2}, \dots, a_1$ 을 변경하여 다항식으로 만든다 하더라도, 서로 다른 번지의 개수는 변하지 않으며, 2^t 개이지만, 혹시 몇 몇 다항식은 낮은 형태를 만들 수도 있다.

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

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

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

2.2 결정론적 혼돈 순서 발생[5],[6],[7],[8]

2.2.1 결정론적 혼돈함수

다양한 함수가 결정론적 혼돈역학을 보이지만, 널리 알려진 톱니함수(saw-tooth function or Baker's function)를 이용하여 혼돈적인 거동을 나타낸다.[5]

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

톱니함수의 수식적인 정의는 다음과 같이 표현된다.

$$S(x) = 2x, \quad x < \frac{\text{단위구간}}{2} \text{인 경우}$$

$$2x - 1, \quad x \geq \frac{\text{단위구간}}{2} \text{인 경우}$$

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

$$\text{Frac}(x) = x - k \quad (\text{여기서 } k \leq x < k+1 \text{이며, } k \text{는 정수이다})$$

이제, 톱니함수의 새로운 수식적인 정의는 다음과 같다.

$$S(x) = \text{Frac}(2x) \quad (\text{여기서 } x \text{의 범위는 } 0 \leq x < 1 \text{이다.})$$

위 식에 의해 단위간격에서 임의의 실수 x 에 대한 2진

수 표현은 새롭게 해석할 수 있는 데, 예를 들면, $\frac{1}{2} = 0.1$, $\frac{3}{4} = 0.11$, $\frac{1}{3} = 0.0101 \dots = 0.0\dot{1}$ 등으로 표현하며, 방정식 $S(x) = \text{Frac}(2x)$ 에서 변수 x 에 곱해지는 2는 임의의 실수에 관한 2진수 $0.a_1 a_2 a_3 \dots a_k$ ($a_1, a_2, a_3, \dots, a_k$ 는 0이나 1을 갖는다.)를 $a_1 a_2 a_3 \dots a_k$ 로 변환하는 것을 의미한다.

톱니함수의 변환은 2진비트의 왼쪽 이동 동작으로 간주할 수 있으며, 어떤 변수의 이진진수가 $x = a_1 a_2 a_3 \dots a_k$ 라 할 때, 이 값을 k 단 왼쪽 쉬프트 레지스터의 초기 값으로 놓으면, 주기는 k 가 되며, k 번보다 작은 몇 번의 왼쪽 이동에 의해 초기 값은 아주 다른 값으로 바뀐다.

예로, 임의의 두 변수의 이진진개를 각각 $x = a_1 a_2 a_3 \dots a_{n-1} a_n$ 이고, $y = a_1 a_2 a_3 \dots a_{k-1} a_k^*$ 이라 한다면 (여기서 $n = k$ 이며 a_k^* 는 이중 이진수이다.), 두 변수 x 와 y 는 기껏해야 2^t 정도의 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 초기조건에 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 x 와 y 의 차이는 기껏해야 2^t 정도뿐이며, 왼쪽 이동순환(left shift rotation)했을 경우, 주기 k 를 갖고 순환하며 주기점은 밀집하게됨을 알 수 있다.

그리고, 적절한 두 변수의 이진진개가 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 톱니함수변환은 레지스터의 왼쪽이동 순환동작에 의해 쉽게 실현되므로, 혼돈순서 발생을 위한 결정론적 혼돈함수로서 톱니함수를 응용할 수 있다.[7],[8]

2.2.2 혼돈적인 랜덤순서 발생개념

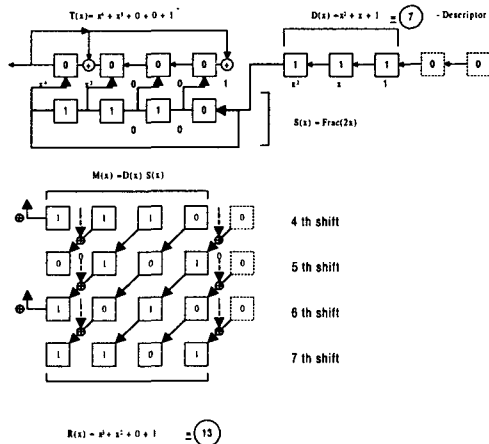
기존의 의사 랜덤순서를 발생시키기 위한 의사 랜덤 디지털 변환에 관계된 회로를 보이고 있는 그림 2로 다시 돌아가 본다. 이 회로에서 다항식 $S(x)$ 부분 만의 변경으로 결정론적인 혼돈순서를 발생시킬 수 있음을 쉽게 짐작할 수 있다. 다항식 $S(x) = x^2$ 와 톱니함수 $S(x) = \text{Frac}(2x)$ 를 함께 이용한다면 <그림 2>는 다음 <그림 3>과 같이 변경되어야 할 것이다.

<그림 2>에 대해 <그림 3>의 차이점은 4차다항식 는

점이다.

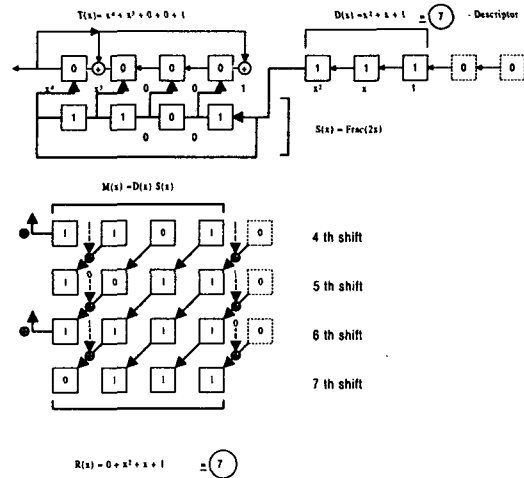
$S(x) = x^4$ 와 톱니함수 $S(x) = \text{Frac}(2x)$ 가 함께 사용되었다. 톱니함수에 의한 변환은 초기 값(기술자의 값을 이용할 수도 있으며, 임의의 톱니함수 값을 사용할 수도 있다)에 따라 달라지지만, <그림 2>에서처럼 변환다항식 $T(x)$ 가 4차라면, 4단 왼쪽 쉬프트 레지스터에 의해 쉽게 실현될 수 있다.

<그림 3>에서와 같이 $S(x) = \text{Frac}(2x)$ 의 초기값을 1110이라한다면 초기값에 따른 톱니함수 변환을 4단 왼쪽 이동레지스터(four stage shift-left register)에 의해 표현했을 경우, 1110, 1101, 1011, 0111과 같은 순서와 주기 4를 가지므로, <그림 2>의 회로에서 발생하는 2'개의 의사 랜덤순서보다 4배 많은 혼돈순서를 <그림 3>의 회로를 발생시킨다. 변환다항식 $T(x)$ 의 차수가 커질수록 혼돈순서는 보다 혼돈적이며 결정론적일 것이다.



<그림 3> 기술자 $D(x)$ 에 톱니함수 $S(x)$ 를 곱한 후, 4차 다항식 $T(x)$ 로 나누어 발생시킨 혼돈 순서 $R(x)$

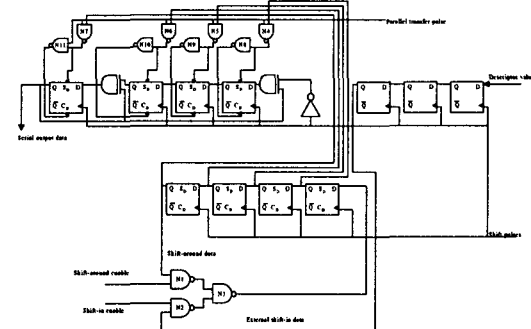
<그림 4>의 나머지 $R(x)$ 의 값이 <그림 2>의 나머지 값과 동일해야함이 당연하며, 톱니함수 변환에 의하여 두 번째로 발생하는 값 1101로 초기 값으로 사용될 때에는 다른 나머지 값이 발생할 것이다. <그림 4>는 값 1101에 의한 다른 나머지 값의 계산의 예다.



<그림 4> 1110에 관한 톱니함수, 둘째 주기인 1101에 의해 발생한 혼돈순서 $R(x)$

2.2.3 카오스적인 랜덤순서 발생회로 설계

<그림 3>과 <그림 4>에서 수행하는 혼돈적인 랜덤순서 발생에 관한 변환을 실제 논리 게이트를 이용하여 <그림 5>와 같이 간단하게 설계하였다.



<그림 5> 논리게이트로 설계한 혼돈 랜덤순서 발생회로

<그림 5>의 회로에서 톱니함수변환을 수행하는 하단부의 4단 shift-left 레지스터에서 shift-in에 관한 procedure는 다음과 같다

- shift-in enable 신호를 논리값 1로한다. 이때 shift-around enable 신호는 논리값 0으로 설정한다.
- 4개의 shift 펄스에 의해 descriptor value를 저장하고 있는 쉬프트 레지스터로부터 톱니함수 변환을 위한 4단 shift-left 레지스터 속으로 data value를 옮긴다.(이때, data가 동기되어 이동하도록 두 레지스터에 똑 같은 4개의 shift pulse를 사용한다.)
- 네 번째 shift pulse발생 후, shift-in enable신호를 논리값 0으로하여 shift-in cycle를 끝낸다.

또한 shift-around cycle에 관한 procedure는 다음과 같이 요약할 수 있다.

- shift-around enable신호를 논리값 1로 한다.(이때, shift-in enable신호는 계속 논리값 0이어야 한다.)
- 세 번째의 shift pulse후, shift-around enable신호를 논리값 0으로 한다.(이때, shift-in enable신호도 논리값 0이어야 하며, high parallel transfer pulse가 주어진다.)

3. 결 론

입력의 (전기적) 신호에 관한 기술자의 다항식을 이용하여 의사 랜덤수나 순서를 발생시키는 기존의 디지털 변환(digital transformation)을 개선하기 위한 방안으로 제안하였다.

기존의 의사 랜덤 디지털 변환방법(conservative method of pseudo-random digital transformation)은 기술자를 표현하는 다항식을 변형시키는 방법, 즉 물리적거리를 더 멀리하기 위해 다른 다항식을 곱하고, 나누어 랜덤한 순서를 발생시키는 방법이다.

이에 반해, 본 논문은 혼돈거동(chaotic dynamics)을 나타내는 톱니함수의 특성(characteristics of saw-tooth function)을 기존의 의사 랜덤 디지털 변환방법에 덧붙임으로써 보다 다양한 물리적 거리에 위한 보다 랜덤한 순서의 발생-결정론적 혼돈 특성을 갖는순서(sequence including the characteristics of deterministic chaos)의 발생에 관한 개념을 제시하고, 간단한 하드웨어 회로를 설계하였다.

또한 제시된 결정론적 혼돈순서발생 개념과 하드웨어 회로가 기존의 의사 랜덤 순서발생 개념과 회로를 개선하는 차원에서 설계하였으므로 기존방식에 비해 랜덤성이 뛰어난 쉽게 비교할 수 있을 것이며, 상용부품들을 이용한 확장된 다단 회로설계 및 모의실험(simulation)은 연속연구로써 진행중이다.

참 고 문 헌

[1] Denny Gulick, Encounters with chaos, pp. 96-103, McGraw-Hill, New York, 1992.

[2] V. Bonacic, B. Soucek and K. Culjat, "Pseudo-random digital transformation," Nuclear Instr. Meth. 66, 1968, pp213.

[3] B. Soucek and the IRIS Group, Dynamic, genetic and chaotic programming, pp. 456-469, John Wiley & Sons, Inc., 1992.

[4] Heinz Georg Schuster, "Deterministic chaos," Verlags gesellschaft mbH, pp. 21-36, 1989.

[5] Heinz-Otto Peitgen, Hartmut Jurgens and Dietmar Saupe, Chaos and fractals, pp. 509-583, Springer-Verlag, New York, 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 인 수 외, 결정론적 카오스함수를 이용한 상태머신, 대한전자공학회 추계학술대회, 1995.

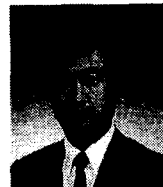
[8] 정 종은 외, 카오스 상태머신의 구현, 회로 및 시스템 연구회, 전력연구회 학술대회, 대한전자공학회, 1995.

구 인 수



1977.2 경북대학교 전자공학과 졸업
 1998.5. 현재 한국원자력연구소 책임 연구원
 1988.8 전자기술사 (공업계측제어)
 1995.8 청주대학교 대학원, 공학석사
 1999.2 충남대학교 대학원 박사과정 수료
 1999.8 한국원자력학회 계측제어 전문 위원장

김 환 우



1977.2 서울대학교 전자공학과 졸업
 1979.2 한국과학기술원 전자공학과 (공학석사)
 1983.9-1988.6 University of Utah (공학박사)
 1980.6. 현재 충남대학교 교수
 1995.1-1996.12 한국통신학회 신호처리연구회 전문위원장
 1998.1. 현재 한국전자공학회 음향 및 신호처리연구회 전문위원장