혼돈맵을 사용한 난수성 2진 순서발생기의 설계

Design of Random Binary Sequence Generator using the Chaotic Map

박광현*, 백승재**
충주대학교 전기전자정보공학부*, 청주대학교 전자정보공학부**

Kwang-Hyeon Park(pkh-2001@hanmail.net)*, Seung-Jae Baek(bsj3386@empal.com)**

요약

본 논문에서는 1차원 혼돈맵들 중의 하나인 톱니맵을 16비트의 유한정밀도로 이산화시켜 설계하였고, 이 이산화된 톱니맵을 사용한 혼돈 2진 순서 발생기의 회로도도 제시하였다. 설계된 혼돈맵의 실제 구현은 이산화된 진리표로부터 얻어진 출력변수의 간략화된 부울함수에 따른 입력선과 출력선들의 정확한 연결에 의해 실현하였다. 최대길이를 발생시키는 선형궤환이동레지스터(mLFSR)에 의해 발생되는 난수성 2진 출력 순서들을 이산화된 톱니맵의 입력순서로 사용함으로써 결과적으로 최소 16배 더 긴 주기를 갖는 혼돈 2진 순서들을 발생시켰다.

■ 중심어 : | 혼돈맵 | 난수성2진 | 2진순서발생기 |

Abstract

The discretized saw-tooth map with the 16-bit finite precision which is one of the 1-dimensional chaotic maps is designed, and the circuit of chaotic binary sequence generator using the discretized saw-tooth map is presented also in this brief.

The real implementation of designed chaotic map is accomplished by connecting the input and output lines exactly according to the simplified Boolean functions of output variables obtained from truth table which is discretized.

The random binary output sequences generated by mLFSR generator were used for the inputs of descretized saw-tooth map, and, by the descretized map, chaotic binary sequence which has more long period of 16 times minimally is generated as a results.

■ keyword : | Chaotic map | Random Binary | Binary Sequence Generator |

I. 서 론

본 논문에서는 보다 더 긴 주기와 양질의 난수성 2진 순서를 발생시키기 위해 많은 연구나 노력들이 있어왔고 그 중 하나가 혼돈맵을 이용하는 것이다. 이 논문에서는 대표적인 1차원의 혼돈맵들인 톱니맵(saw-tooth map)과 텐트맵(tent map)중에서 톱니맵을 활용한 난수성 2진 순서발생기의 설계와 톱니맵회로의 설계를 통해 이산화된 혼돈맵(discretized chaotic map)의 구현도 제시하였다.

16차의 원시다항식(primitive polynomial)을 궤환함수로 갖는 16비트 길이의 mLFSR (maximum- length

접수번호 : #080318-002
접수일자 : 2008년 03월 18일
심사완료일 : 2008년 06월 16일
교신저자 : 백승재, e-mail : bsj3386@empal.com

Linear Feedback Shift Registor)로부터 주기 2^{16}-1인 난수성 2진 순서를 발생시켰고, 발생된 이 난수성 2진 순서들을 이산화된 톱니맵의 입력으로 사용하였다. 입력된 16자리의 2진수열(상태)마다 톱니맵에 의해 다시 주기 16인 16비트의 혼돈 2진 순서를 발생시키도록 톱니맵에 관련된 궤환회로(feedback circuit)에는 16비트 길이의 병렬 이동레지스터(parallel shift register)를 사용하였다.

이산화된 톱니맵을 이용한 난수성 순서 2진 발생기에 사용한 디지털 소자들로는, 17개의 16비트 이동레지스터와 카운터(counter), 3상태버퍼(three static buffer) 만으로 구성된다.

II. 이산화된 16비트 톱니맵 회로의 설계

톱니맵으로 사용할 톱니함수(Saw-Tooth function)는 그에 의한 반복적인 곱셈 중에 발생하는 1이상인 정수 부분을 항상 제거시키는 알고리즘(algorithm)을 갖는 함수이며 다음 식(1)과 [그림 1]에 의해, 수치적이고 기하학적으로 정의할 수 있다.

$$S(x)=\begin{cases}2x, & 0.0 \le x < 0.5 \\ 2x-1, & 0.5 \le x < 1.0\end{cases} \quad (1)$$

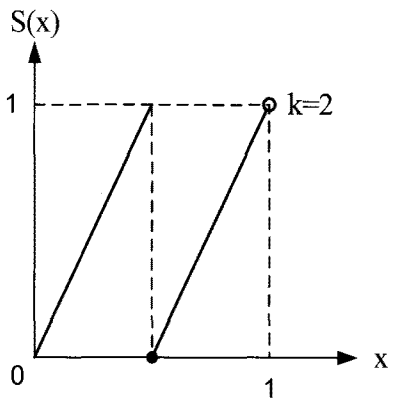


그림 1. 기울기 k=2인 톱니함수의 그래프(구간은 [0,1))

구간 [0, 1)을 갖는 톱니함수의 기능을 맵의 해당구간 (0 , 1)내에서 반복하기위한 이산화된 톱니맵을 설계하고 디지털 소자로 구현하기 위해 우선 톱니맵에 의해 혼돈거동(chaotic behavior)을 내보이는 기울기 k > 1인 경우들 중에서, k=2인 경우, 구간에 임의의 점 x_0의 Liapunov지수 $\lambda(x_0)$

$$\lambda(x_0)=\log 2 \cdot |\overline{\Delta I}| \quad (2)$$

와 정보의 평균손실(the mean less of information) $|\overline{\Delta I}|$

$$|\overline{\Delta I}|=-\lim_{n\to\infty}\frac{1}{N}\sum_{i=0}^{N-1} ld\,|S'(x_i)| \quad (3)$$

에 의해, Liapunov 지수 $\lambda(x_0)$의 일반식은

$$\lambda(x_0)=\log 2 \quad (4)$$

로 구해진다 [1].

기울기 k=2인 혼돈맵을 사용하므로, 맵의 구간 (0, 1)내에 분포하는 임의의 점들의 값들, 그 모두는 한 번의 변환에 의해 배수가 되고, n번의 반복에 대한 기울기는 다음 식 (5)의 관계가 성립된다.

$$k=\left|\frac{d}{dx}S^n(x)\right|=2n\ ,(n=0,1,2,3\cdots) \quad (5)$$

식 (1)과 같이 두 개의 부구간에 대하여 각기 다른 수식으로 표현하는 것에 비해 구간 (0, 1)내의 임의의 한 점 x_n를 톱니맵에 의한 한 번의 반복을 표현하는 식 (6)으로 정의하면, 식 (1)보다 간결해지며, 톱니맵 변환의 개념이 보다 명확해진다[2-5].

$$x_{n+1}\equiv F[x_n]=k\cdot x_n-\lfloor k\cdot x_n\rfloor = k\cdot x_n \bmod 1 \quad (6)$$

식 (6)에서 k는 기울기이고, n=0, 1, 2, 3,… 이며, 함수$F[x_n]$은 x_{n+1}의 비정수 부분을 의미한다. 따라서

$\lfloor \ \rfloor$ 의 연산으로 얻어지는 정수를 $k \bullet x_n$에서 빼면 결국 소수점 이하의 값만을 갖는 x_{n+1}을 계산 할 수 있다.

16비트의 난수성 2진수를 입력으로 하는 이산화된 톱니맵의 경우는 궤환회로를 이용하여 16번의 반복적인 톱니맵 변환에 의해 주기 16인 순서를 발생시킬 수가 있다. 따라서 먼저 식 (6)에 의해 설계할 이산화된 16비트 톱니맵의 진리표를 다음과 같이 작성하였다.

표 1. 이산화된 톱니맵에대해 부분적으로 보인 진리표

	입력변수	출력변수
	$S_{15}S_{14}S_{13}S_{12}S_{11}S_{10}S_9S_8S_7S_6S_5S_4S_3S_2S_1S_0$	$C_{15}C_{14}C_{13}C_{12}C_{11}C_{10}C_9C_8C_7C_6C_5C_4C_3C_2C_1C_0$
1	0000000000000001	0000000000000010
2	0000000000000010	0000000000000100
3	0000000000000011	0000000000000110
4	0000000000000100	0000000000001000
5	0000000000000101	0000000000001010
6	0000000000000110	0000000000001100
7	0000000000000111	0000000000001110
8	0000000000001000	0000000000010000
9	0000000000001001	0000000000010010
10	0000000000001010	0000000000010100
⋮	⋮ ⋮	⋮ ⋮
32766	0111111111111110	1111111111111100
32767	0111111111111111	1111111111111110
32768	1000000000000000	0000000000000001
32769	1000000000000001	0000000000000011
32770	1000000000000010	0000000000000101
⋮	⋮ ⋮	⋮ ⋮
65526	1111111111110110	1111111111101101
65527	1111111111110111	1111111111101111
65528	1111111111111000	1111111111110001
65529	1111111111111001	1111111111110011
65530	1111111111111010	1111111111110101
65531	1111111111111011	1111111111110111
65532	1111111111111100	1111111111111001
65533	1111111111111101	1111111111111011
65534	1111111111111110	1111111111111101
65535	1111111111111111	1111111111111111

작성한 [표 1]의 진리표로부터 출력변수들에 관한 간략화된 부울함수(simplified Boolean function)는 다음식으로 구해졌다.

$$\begin{aligned} &C_0 = S_{15}, C_1 = S_0, C_2 = S_1, C_3 = S_2, C_4 = S_3, \\ &C_5 = S_4, C_6 = S_5, C_7 = S_6, C_8 = S_7, C_9 = S_8, \\ &C_{10} = S_9, C_{11} = S_{10}, C_{12} = S_{11}, C_{13} = S_{12}, \\ &C_{14} = S_{13}, C_{15} = S_{14} \end{aligned} \quad (7)$$

이산화된 톱니맵에 입력되는 16비트 난수성 2진수의 입력은 소숫점 이하 16자리의 2진수를 의미하고, 임의의 지점 x_n에서 이산화된 톱니맵과 톱니함수의 차이는 $\left|\frac{1}{2^{16}}\right|$에 불과하다는 것을 의미한다. 즉, 16비트의 유한 정밀도(finite precision)을 갖는 경우, FIPS(Federal Information Processing Standard)테스트의 통과율이 100%였다는 것을 이미 발표된 논문[6]에서 입증하였으므로, 다음 [그림 2]와 같이 설계한 이산화된 혼돈맵 회로에서, 임의의 점 x_n과 임의의 시각 τ에 발생하는 다음식 (8)로 표현되는 이산화된 상태 S_n의 순서는 난수적이다.

$$\begin{aligned} S_n &= (0.x_1x_2x_3\cdots x_{16})_2 \\ &= \sum_{i=1}^{16} x_i 2^{-i} \end{aligned} \quad (8)$$

식 (6), [표 1], 식 (8)을 구현하는 이산화된 16비트 톱니맵회로 [그림 2]는 궤환회로에 의해 출력회로에 연결되고, 톱니맵은 간략화된 부울식(7)에 의해 간단한 배선으로만 꾸며졌다.

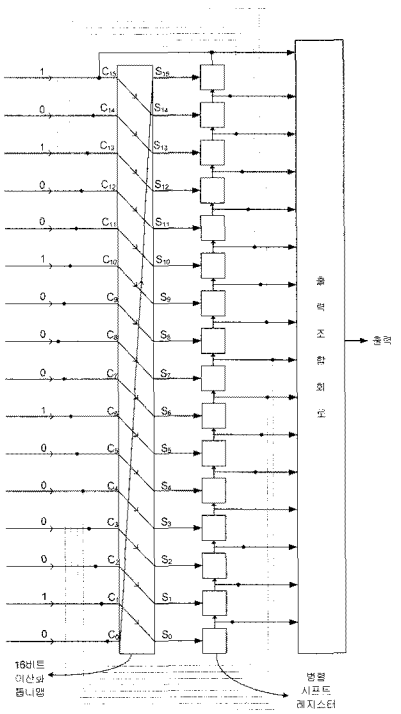


그림 2. 출력조합회로를 포함하는 이산화된 톱니맵과 궤환회로

그리고 이산화된 톱니맵의 초기입력으로 상태벡터 (1010010001000010)를 입력할 경우, 톱니맵의 반복에 의해 [표 2]와 같은 주기 16인 혼돈상태들을 발생시킨다.

표 2. 주기16인 16개의 혼돈상태들

	상태값	십진수값
①	0101001000100001	0.320816040
②	1010100100010000	0.660400391
③	0101010010001000	0.330200195
④	0010101001000100	0.165100098
⑤	0001010100100010	0.082550049
⑥	0000101010010001	0.041275024
⑦	1000010101001000	0.520629883
⑧	0100001010100100	0.260314941
⑨	0010000101010010	0.130157471
⑩	0001000010101001	0.065078735
⑪	1000100001010100	0.532531738
⑫	0100010000101010	0.266265869
⑬	0010001000010101	0.133132935
⑭	1001000100001010	0.566558838
⑮	0100100010000101	0.283279419
⑯	1010010001000010	0.641632080

발생한 16개의 혼돈상태들의 옆 괄호 안에 계산해 놓은 십진수 값에 의해 발생한 상태들이 난수성을 가졌음을 보다 확실하게 파악할 수 있다. 이산화된 톱니맵에 의해 발생한 혼돈상태들의 주기성을 기하학적으로 살펴보면 [그림 3]과 같다.

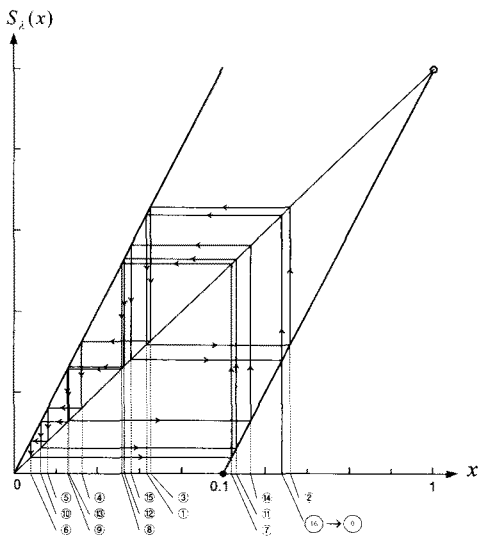


그림 3. 이산화된 톱니맵 회로에 의한 상태들의 주기에 관한 거동

III. 난수성 2진 순서발생기 설계

궤환함수(feedback function)로 16차의 원시다항식 $x^{16}+x^5+x^3+x^2+1$을 갖는 16비트의 mLFSR과 [그림 2]의 이산화 16비트 톱니맵을 사용하여 [그림 4]와 같은 난수성 2진 순서 발생기를 설계하였다. [그림 4]에 보인 m-LFSR에 초기입력으로 무리수에 근접하게 정한 16비트의 유리수 0.1010010001000010의 소숫점 이하 16비트로 된 상태벡터, (1010010001000010)를 입력하면, 16비트의 m-LFSR에서는 주기 2^{16}-1인 난수성 2진 순서(혹은 상태)가 발생하게 된다. [그림 4]에서 살펴 볼 수 있는 바와 같이, 이 초기 입력상태는 직접 이산화된 16비트 혼돈맵의 초기입력으로도 이용할 수 있다. 이산화 혼돈맵에 입력된 초기상태는, [표 2]와 같은 16개의 난수성 상태를 발생시키므로 mLFSR에서 발생하는 2^{16}-1개의 한 상태마다 주기 16인 혼돈 2진 발생기와 같은 역할을 할 것이다. 결국 mLFSR과 이산화된 톱니맵에 의해 길이 65K×16인 난수성 순서가 발생하고, 그 이후 출력 조합회로의 출력순서 중 16비트를 입력으로 재사용 한다면, 필요에 따라서는 반복하지 않는 무한에 가까운 난수성 2진 순서를 얻을 수 있다.

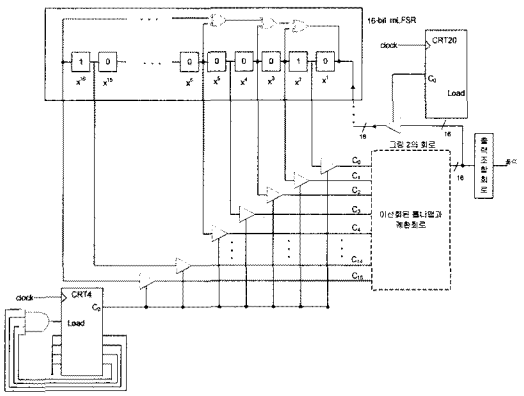


그림 4. 난수성 2진 순서 발생기의 회로 설계

IV. 결 론

혼돈맵의 이산화 과정 중에서는 혼돈특성이 변하지 않고 이산화된 톱니맵의 설계와 구현이 용이하도록 [표

1]에 보인 이산화 진리표를 작성한 결과 배선만으로도 하드웨어 구현이 용이하였다. 뿐만 아니라 이산화된 혼돈맵 회로에 의해 [표 2]처럼 주기 16인 완벽한 혼돈순서를 발생시켰다. 서론에서 이미 사용한 디지털소자의 갯수와 종류를 언급하였고, [그림 4]에서 보인 난수성 2진 순서 발생회로로부터 직접 살펴볼 수 있는 바와 같이 기존의 어느 난수성 2진 순서발생기나 유한상태머신(finite state machine)보다 간단하며 효율적으로 양질의 긴 주기를 갖는 난수성 2진 순서를 발생시켰다. 또한 설계 절차(혹은 설계개념)의 단순함과 선로의 변경만으로 구현한 이산화 톱니맵회로의 간결함 때문에 상관성(correlativity)을 무시할 수도 있지만 FIPS테스트를 통한 확실한 난수성(randomness)의 증명은 다음 연구과제로 남겨놓는다.

참 고 문 헌

[1] G. S. Heinz, "Deterministic chaos," Weinhem, Germany : VCH Verlagstesellschaft, pp.24-27, 1989.

[2] H. O. Peitgen, H. Jürgens, and D. Saupe, "Chaos and Fractals," in New Frontiers of Science, NewYork : Springes-Verlag, 1992.

[3] J. Argyris, G. Faust, and M. Haase, "An exploration of chaos," in Texts on Computaional Mathematics, NewYork : Elevier, Vol.VII., Elsevier science B. V. 1994.

[4] M. Jessa, "The Period of Sequences Generated by Tent-Like Maps," IEEE Trans, Circuits Syst.I, Vol.49, No.1, pp.84-89, 2002(1).

[5] M. Jessa, "Designing Security for Number Sequences Generated by Means of the Saw-tooth chatotic Map," IEEE Trans, Circuits Syst.I, Vol.53, No.5, pp.1140-1150, 2006(5).

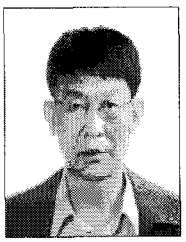
[6] M. Alioto, S. Bernardi, A. Fort, Rocchis, and V. Vignoli, "Analysis and design of digital PRNGS based on the discretized saw-tooth map," proc. conf. Electron Circuits syst, Vol.2, pp.427-430, 2003.

[7] S. W. Galomb, "Shift Register sequences," Aeglean Park Press, Revised Edition, 1992.

[8] 박광현, "비선형 난수성 순서발생기의 설계", 충주대학교 논문집, 제40집, 제2호, pp.85-88, 2005(12).

저 자 소 개

박 광 현(Kwang-Hyeon Park) 정회원



- 1996년 8월 : 청주대학교 전자공학과(공학박사)
- 1997년 1월 : 충주대학교 전기전자정보공학부 교수

<관심분야> : 카오스역학, 스트림암호

백 승 재(Seung-Jae Baek) 정회원

- 1997년 2월 : 청주대학교 전자공학과(공학사)
- 1999년 2월 : 청주대학교 전자공학과(공학석사)
- 1999년 2월 ~ 2002년 : 청주대학교 전자공학과(박사수료)
- 2004년 ~ 현재 : 한국폴리텍IV청주캠퍼스 정보통신홈네트워크과 IT교수

<관심분야> : 스트림암호, 부호이론, 정보이론, 디지털통신