# 톱니맵을 이용한 상태머신의 설계

***서용원**, *서은미, **박광현, ***Ala Eldin Abdallah Awouda
*(주)이씨엠, **충주대학교 전자통신과, ***University Technology Malaysia

# Design of The State machine using the Saw-Tooth Map

*Yong-Won Seo, *Eun-Mi Seo, **Kwang-Hyeon Park, ***Ala Eldin Abdallah Awouda
*Inc. ECM, **Chungju National University, ***University Technology Malaysia

**Abstract** - 이 논문에서는 1차원 혼돈맵들 중의 하나인 톱니맵을 8비트의 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 연결만에 의해 실현하였다. 최대길이를 발생시키는 선형궤환시프트레지스터(mLFSR)에 의해 발생되는 난수성 2진 출력 순서들을 이산화된 톱니맵의 입력순서로 사용함으로써 결과적으로 최소 8배 더 긴 주기를 갖는 혼돈 2진 순서들을 발생시켰다.

## 1. 서 론

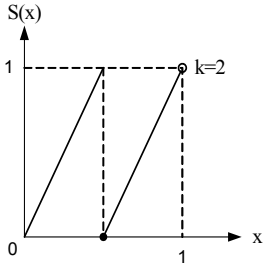
보다 더 긴 주기와 양질의 난수성 2진 순서를 발생시키기 위해 많은 연구나 노력들이 있어왔고 그 중 하나로 혼돈맵을 이용하는 것이다. 이 논문에서는 대표적인 1차원의 구분적선형 혼돈맵들인 톱니맵(saw-tooth map)과 텐트맵(tent map)중에서 이산화된 혼돈맵(discretized chaotic map)의 구현과 이산화된 톱니맵 회로의 설계를 통해 혼돈 2진 순서 발생회로 설계를 제시하였다.
8차의 원시다항식(primitive polynomial)을 궤환함수로 갖는 8비트 길이의 mLFSR (maximum- length Linear Feedback Shift Registor)로부터 주기 $2^8$-1인 난수성 2진 순서를 발생시켰고, 발생된 이 난수성 2진 순서들을 이산화된 톱니맵의 입력으로 사용하였다. 입력된 8자리의 2진수열(상태)마다 톱니맵에 의해 다시 주기 8인 8비트의 혼돈 2진 순서를 발생시키도록 톱니맵에 관련된 궤환회로(feedback circuit)에는 8비트 길이의 병렬 시프트레지스터(parallel shift register)를 사용하였다.
이산화된 톱니맵 회로를 이용한 혼돈 순서 2진 발생기에 사용한 디지털 소자들로는, 8비트 시프트레지스터와 카운터(counter), 3상태버퍼(three static buffer)만으로 구성된다.

## 2. 본 론

### 2.1 이산화된 8비트 톱니맵 회로의 설계

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

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




<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

본 연구는 충북테크노파크 (맞춤형과제 "인휠 모터 기반의 미니 전기차 제어시스템 개발", 주관기업 (주) 이씨엠) 지원에 의한 것입니다.

우선 톱니맵에 의해 혼돈거동(chaotic behavior)을 내보이는 기울기 k=2 (k>1)인 경우, 구간에 임의의 점 $x_0$의 Liapunov지수 $\lambda(x_0)$

$$\lambda(x_0)=\log 2 \bullet |\overline{\Delta I}| \qquad (2)$$

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

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

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

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

로 구해진다 [1].

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

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

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

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

식 (6)에서 k는 기울기이고, n=0, 1, 2, 3,… 이며, 함수$F[x_n]$은 $x_{n+1}$의 비정수 부분을 의미한다. 따라서 ⌊ ⌋의 연산으로 얻어지는 정수를 $k \bullet x_n$에서 빼면 결국 소수점 이하의 값만을 갖는 $x_{n+1}$을 계산 할 수 있다.
8비트의 난수성 2진수를 입력으로 하는 이산화된 톱니맵의 경우는 궤환회로를 이용하여 8번의 반복적인 톱니맵 변환에 의해 주기 8인 순서를 발생시킬 수가 있다. 따라서 먼저 식 (6)에 의해 설계한 이산화된 8비트 톱니맵의 진리표를 다음과 같이 작성하였다.

<표 1> 이산화된 톱니맵에대해 부분적으로 보인 진리표

| | 입력변수 | 출력변수 |
|---|---|---|
| | $S_7S_6S_5S_4S_3S_2S_1S_0$ | $C_7C_6C_5C_4C_3C_2C_1C_0$ |
| 1 | 00000001 | 00000010 |
| 2 | 00000010 | 00000100 |
| 3 | 00000011 | 00000110 |
| 4 | 00000100 | 00001000 |
| 5 | 00000101 | 00001010 |
| 6 | 00000110 | 00001100 |
| 7 | 00000111 | 00001110 |
| 8 | 00001000 | 00010000 |
| 9 | 00001001 | 00010010 |
| 10 | 00001010 | 00010100 |
| ⋮ | ⋮ ⋮ | ⋮ ⋮ |
| 126 | 01111110 | 11111100 |
| 127 | 01111111 | 11111110 |
| 128 | 10000000 | 00000001 |
| 129 | 10000001 | 00000011 |
| 130 | 10000010 | 00000101 |
| ⋮ | ⋮ ⋮ | ⋮ ⋮ |
| 252 | 11111100 | 11111001 |
| 253 | 11111101 | 11111011 |
| 254 | 11111110 | 11111101 |
| 255 | 11111111 | 11111111 |

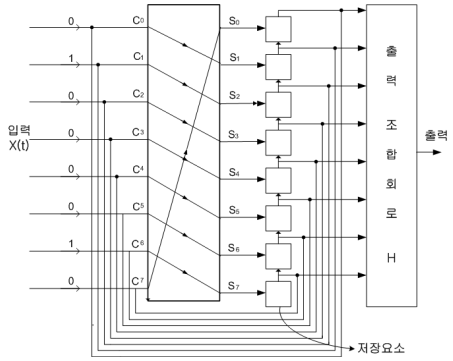
작성한 [표 1]의 진리표로부터 출력변수들에 관한 간략화된 부울함수(simplified Boolean function)는 다음 식으로 구해졌다.

$$C_0 = S_7,\ C_1 = S_0,\ C_2 = S_1,\ C_3 = S_2,\ C_4 = S_3,$$
$$C_5 = S_4,\ C_6 = S_5,\ C_7 = S_6, \qquad (7)$$

이산화된 톱니맵에 입력되는 8비트 난수성 2진수의 입력은 소숫점 이하 8자리의 2진수를 의미하고, 임의의 지점 $x_n$에서 이산화된 톱니맵과 톱니함수의 차이는 $\left|\frac{1}{2^8}\right|$에 불과하다는 것을 의미한다. 즉, 8비트의 유한정밀도(finite precision)을 갖는 경우에도, 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 $x_n$과 임의의 시각 $\tau$에 발생하는 다음식 (8)로 표현되는 이산화된 상태 $S_n$의 순서는 필히 난수적이다.

$$S_n = (0.x_1x_2x_3\cdots x_8)_2 \qquad (8)$$
$$= \sum_{i=1}^{8} x_i 2^{-i}$$

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




**<그림 2> 이산화된 톱니맵과 궤환회로**

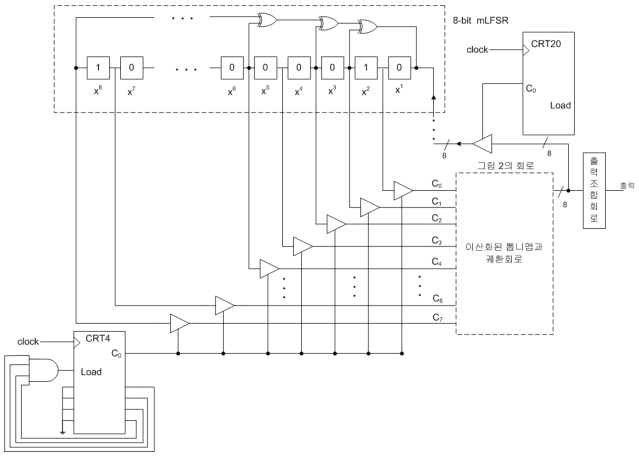
그리고 이산화된 톱니맵의 초기입력으로 상태벡터 (10100100)를 입력할 경우, 톱니맵의 반복에 의해 [표 2]와 같은 주기 8인 혼돈상태들을 발생시킨다.

**<표 2> 주기 8인 8개의 혼돈상태들**

| | 상태값 | 십진수값 |
|---|---|---|
| ① | 01010010 | 0.320816040 |
| ② | 10101001 | 0.660400391 |
| ③ | 01010100 | 0.330200195 |
| ④ | 00101010 | 0.165100098 |
| ⑤ | 00010101 | 0.082550049 |
| ⑥ | 00001010 | 0.041275024 |
| ⑦ | 10000101 | 0.520629883 |
| ⑧ | 01000010 | 0.260314941 |

### 2.2 난수성 2진 순서발생기 설계

궤환함수(feedback function)로 8차의 원시다항식 을 갖는 8비트의 mLFSR과 [그림 2]의 이산화 8비트 톱니맵을 사용하여 [그림 3]와 같은 난수성 2진 순서 발생기를 설계하였다. [그림 3]에 보인 m-LFSR에 초기입력으로 무리수에 근접하게 정한 8비트의 유리수 0.1010010의 소숫점 이하 8비트로 된 상태벡터, (1010010)를 입력하면, 8비트의 m-LFSR에서는 주기 $2^8$-1인 난수성 2진 순서(혹은 상태)가 발생하게 된다. [그림 3]에서 살펴 볼 수 있는 바와 같이, 이 초기 입력상태는 직접 이산화된 8비트 혼돈맵의 초기입력으로도 이용할 수 있다. 이산화 혼돈맵에 입력된 초기상태는, [표 2]와 같은 8개의 난수성 상태를 발생시키므로 mLFSR에서 발생하는 $2^8$-1개의 한 상태마다 주기 8인 혼돈 2진 발생기와 같은 역할을 할 것이다. 결국 mLFSR과 이산화된 톱니맵에 의해 길이 256×8인 난수성 순서가 발생하고, 그 이후 출력 조합회로의 출력 순서 중 8비트를 입력으로 재사용 한다면, 필요에 따라서는 반복하지 않는 무한에 가까운 혼돈 2진 순서를 얻을 수 있다.




**<그림 3> 혼돈 2진 순서 발생기의 회로 설계**

## 3. 결 론

가혼돈맵의 이산화 과정 중에서는 혼돈특성이 변하지 않고 이산화된 톱니맵의 설계와 구현이 용이하도록 [표 1]에 보인 이산화 진리표를 작성하여 간략화된 부울함수를 구한 결과 배선 변경만으로도 하드웨어 구현이 가능하였다. 뿐만 아니라 이산화된 혼돈맵 회로에 의해 [표 2]처럼 주기 8인 완벽한 혼돈순서를 발생시켰다. 서론에서 이미 사용한 디지털소자의 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 간단하게 설계되었고 효율적으로 양질의 긴 주기를 갖는 혼돈 2진 순서를 발생시켰다. 또한 설계 절차(혹은 설계개념)의 단순함과 선형복잡도(linear complexity)의 변화없이 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. Jurgens, 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, No1, 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, Vol53, No.5, pp.1140-1150, 2006(5).

[6] M. Alioto, S. Bernardi, A. Fort, Rocchis, 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).