한국산학기술학회논문지
Vol. 10, No. 12, pp. 3688-3693, 2009

혼돈맵들에 기반한 합성 상태머신의 설계

서용원[1*], 박진수[1]
[1]청주대학교 전자공학과

Design of the composition state machine based on the chaotic maps

Yong-Won Seo[1*] and Jin-Soo Park[1]
[1]**Department of Electronics rading, Cheongju University**

요 약 본 논문에서는 두 가지 혼돈맵들 -톱니맵 $S_2(x)$ 와 텐트맵 $T_2(x)$- 을 연결시킨 하나의 합성맵을 기초로 사용하는 독립된 하나의 합성상태머신을 설계하는 방법 및 그 결과을 제시하였다. 두 가지 다른 혼돈맵들 -톱니맵과 텐트맵- 의 합성 논리를 이용하여 설계된 독립된 하나의 합성상태머신에서 발생하는 혼돈적인 상태들을 그래프적으로 보였으며, 발생하는 의사 난수적인 상태들의 주기는 이산화된 진리표의 정밀도에 따른 길이를 갖는다는 것도 보였다.

Abstract In this paper the design methode of a separated composition state machine based on the compositive map with connecting two chaotic maps together - sawtooth map $S_2(x)$ and tent map $T_2(x)$ and the result of that is proposed. this paper gives a graph of the chaotic states generated by the composition state machine using the compositive logic of two different chaotic maps - sawtooth map and tent map and also shows that the period of pseudo-random states has the length according to the precision of the discreet truth table.

Key Words : Chaotic map, Random Binary, Binary Sequence Generator

1. 서론

본 논문에서는 보다 난수적인 상태(random states)들을 발생시키는 합성상태머신(composi tion state machine)을 설계하고자, 혼돈역학의 난수성(randomness)을 디지털 회로의 상태머신(state machine)에 활용하여, 이산화된 혼돈맵들(discretized chaotic maps)을 사용하는 혼돈합성머신(chaotic composition machine)을 설계하였다. 디지털 회로나 시스템들은 그동안 출력에 관여하는 변수들의 종류에 따라 크게 Mealy state machine과 Moore state machine으로 대별되어져 왔으며, 이 두 상태머신들은 조합논리회로부분(part of combinational logic circuit)의 설계에 따라 다양한 다음상태들과 출력을 발생시키고 있다.

이 논문에서는 상태머신의 조합회로 부분으로 혼돈함수(chaotic function)의 변환을 수행하는 두 가지 혼돈맵들(chaotic maps)을 연결하여 [1-3] 보다 혼돈적인 상태(chaotic state)들을 발생시키는 독립된 하나의 합성상태머신을 설계하여 제시하였다.

사용한 두 가지 혼돈맵들은 이산화된 톱니맵(discretized saw-tooth map)과 이산화된 텐트맵(tent map)이며[4,5], 두 가지 혼돈맵들을 연결시킨 독립된 하나의 합성상태머신으로부터 발생하는 상태들은 16비트의 2진수(binary number) 값으로 그 랜덤성을 보이도록 하였다.

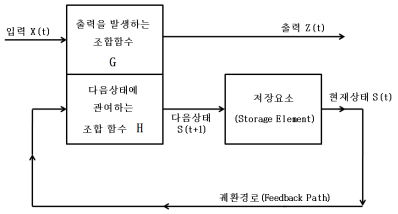
2. 상태머신과 혼합맵들

2.1 상태머신

다음 [그림 1]의 디지털 회로와 시스템의 블록도(block diagram)에 보인 디지털순차회로(digital sequential circuit)에 관련시킬 수 있는 Mealy 와 Moore 상태머신들, 두 상태머신들의 상태전이함수(state transition function)

*교신저자 : 서용원(ds3dhy@hotmail.com)
접수일 09년 10월 16일 수정일 09년 11월 20일 게재확정일 09년 12월 16일

나 출력함수(output function)은 각각 다음 식들 (1), (2)로 정의 할 수 있었다.[6]



[그림 1] 전형적인 디지털 회로 블록도

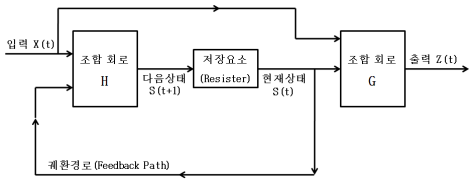
[Mealy 상태 머신의 상태전이함수와 출력함수]

$$\begin{aligned} &\text{상태전이함수 : } S(t+1) = H(\ S(t),\ X(t)\ ) \\ &\text{출력함수 : } \quad Z(t) \quad = G(\ S(t),\ X(t)\ ) \end{aligned} \tag{1}$$

[Moore 상태 머신의 상태전이함수와 출력함수]

$$\begin{aligned} &\text{상태전이함수 : } S(t+1) = H(\ S(t),\ X(t)\ ) \\ &\text{출력함수 : } \quad Z(t) \quad = G(\ S(t)\ ) \end{aligned} \tag{2}$$

따라서 식 (1)과 (2)에 의해 그림 2와 같이 두 개의 조합회로로도 분리될 수 있다.



[그림 2] 두 개의 조합회로로 표현된 블록도

2.2 이산화된 톱니맵

기울기 S=2를 갖는 다음 식 (3)으로 정의되는 톱니맵을 16비트로 이산화 시킨다면

$$S(x)=\begin{cases} 2x, & 0.0 < x \le 0.5 \\ 2x-1, & 0.5 < x \le 1.0 \end{cases} \tag{3}$$

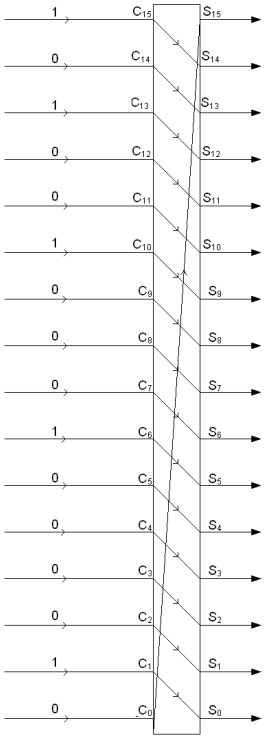
십진수값 x=0.0(이진수 표현은 00000000000000 00)을 제외한 다음 표 1과 같이 2진수(binary number)의 16비트 유리수들(16-bit rational number)로 이산화된 진리표(discretized truth table)를 얻을 수 있고, 이 진리표로부터

[표 1] 이산화된 톱니맵에 대해 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

식 (4)와 같은 간략화 된 부울 함수(simplified boolean algibra)를 찾아냄으로써 그림 3 과 같이 입력과 출력의 관계를 배선의 변경만으로 참고문헌[4]에서는 설계 하였었다. [4]

$$\begin{aligned} &C_0 = S_{15}, C_1 = S_0, C_2 = S_1, C_3 = S_2, C_4 = S_3, \\ &C_5 = S_4, C_6 = S_5, C_7 = S_6, C_8 = S_7, C_9 = S_8, \\ &C_{10} = S_9, C_{11} = S_{10}, C_{12} = S_{11}, C_{13} = S_{12}, \\ &C_{14} = S_{13}, C_{15} = S_{14} \end{aligned} \tag{4}$$



[그림 3] 이산화된 톱니맵의 조합논리회로

이렇게 16비트로 이산화 시킨 경우, 톱니함수와 이산화 된 톱니맵과의 오차는 구간 [0, 1)을 갖는 톱니함수의 기능을 맵의 해당구간 [0, 1)내에서 반복하기위한 이산화된 톱니맵과의 오차는 $\left|\frac{1}{2^{16}}\right|$에 불과하다는 것을 진리표에 통해서도 확인할 수 있었고, 식(5)에 의해 표현 할 수 있는 이산화된 상태 S_n의 순서들도

$$S_n = (0.x_1x_2x_3\cdots x_{16})_2 = \sum_{i=1}^{16} x_i 2^{-i} \quad (5)$$

으로 나타낼 수 있고 역시 난수성(randomness)을 갖는 것이 입증되었다.

2.3 이산화된 텐트맵

톱니 함수의 경우와 마찬가지로 다음 식 (6)으로 정의되는 텐트함수의 이산화된 텐트맵도

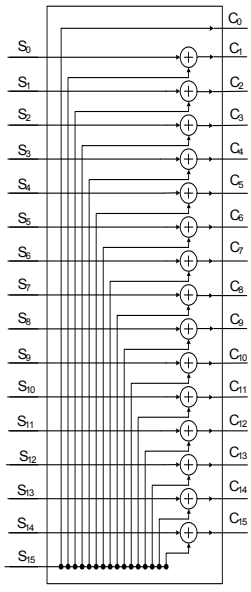
$$T(x) = \begin{cases} 2x, & 0.0 < x \le 0.5 \\ 2(1-x), & 0.5 < x \le 1.0 \end{cases} \quad (6)$$

역시 십진수값 X = 0.0은 제외한 다음 표 2와 같이 이산화된 진리표에 의해 식 (7)과 같이 간략화 된 부울식을 구한 다음 그림 4처럼 오직 배타적합논리게이트(exclusive-OR logic gate)만을 사용하여, 간략화 된 부울식에 일치하는 선 연결만으로 설계하였었다.[5]

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

[표 2] 이산화 텐트맵의 부분적 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	1111111111111111
32769	1000000000000001	1111111111111101
32770	1000000000000010	1111111111111011
⋮	⋮ ⋮	⋮ ⋮
65526	1111111111110110	0000000000001011
65527	1111111111110111	0000000000010001
65528	1111111111111000	0000000000001111
65529	1111111111111001	0000000000001101
65530	1111111111111010	0000000000001011
65531	1111111111111011	0000000000001001
65532	1111111111111100	0000000000000111
65533	1111111111111101	0000000000000101
65534	1111111111111110	0000000000000011
65535	1111111111111111	0000000000000001



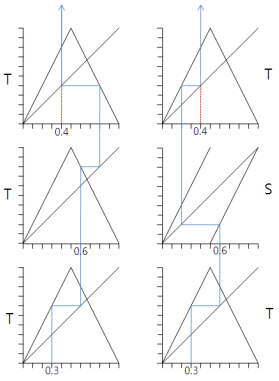
[그림 4] 이산화된 텐트맵의 조합논리회로

3. 톱니맵과 텐트맵의 합성논리

텐트맵 변환을 n회 반복하는 것은 톱니맵 변환을 n-1회 반복한 후에 마지막 일회만을 텐트맵 변환으로 수행한 결과와 같다는 것이 다음 수식 (8)에 의해 정의되어졌고 [1,8],

$$T^n(x) = T(S^{n-1}(x)) \qquad (8)$$

더 나아가, 텐트맵과 톱니맵이 뒤섞이는 경우 일지라도, 마지막 일회변환이 텐트맵이라면 역시 같은 결과가 나온다는 사실을 다음 그림 5를 통해서도 알 수 있다.



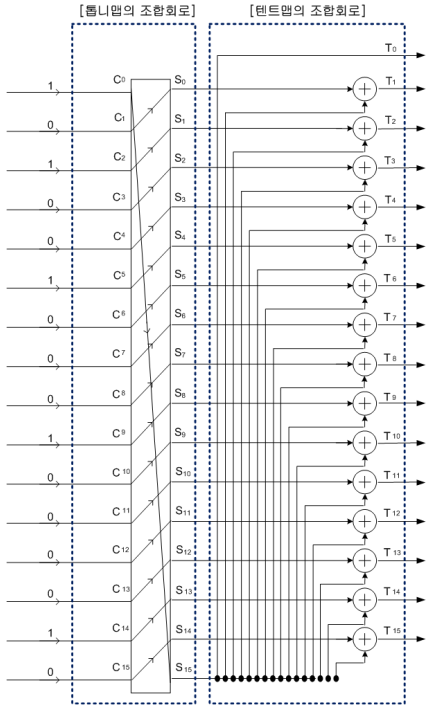
[그림 5] T(T(T(x))) = T(S(T(x))) 인 경우

4. 합성상태머신의 설계

4.1 합성맵의 설계

앞 절의 합성논리와 부합하게 두 가지 혼돈맵을 합성한 맵의 조합회로를 다음 그림 6처럼 설계하였다.

상태머신 [그림 2 참조]의 조합회로 H에 해당하는 그림 6에 보인 합성맵 조합회로에 입출력 관계를 살펴 보기 위해, 표 1의 입력변수항의 첫 번째 행에 있는 2진상태 (binary state) 0000000000000001을 $C^0 \sim C^{15}$ 입력선에 인가한다면, 출력선 $T^0 \sim T^{15}$에 발생하는 2진 상태는 0000000000000100이며, 또 다른 입력으로 2진상태 1111111111111101을 인가한다면 00000000 00001001의 2진상태가 출력으로 발생되는 것을 표 1과 표 2를 통해 확인함으로써 2회의 혼돈맵 반복을 수행하는 혼돈 합성맵임을 입증 할 수 있었다.



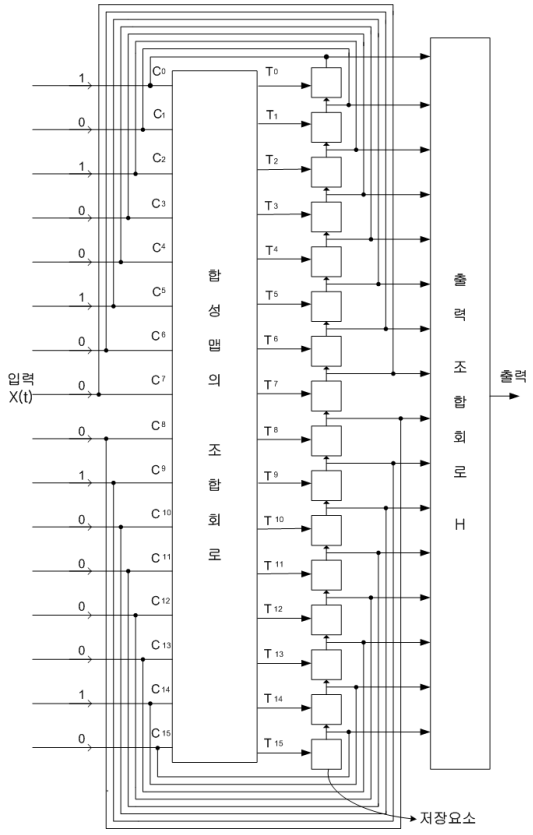
[그림 6] 혼돈 합성맵의 조합회로

4.2 혼돈의 합성상태머신

앞의 그림 2에 보인 블록도와 일치하도록 설계한 합성상태머신을 다음 그림 7에 제시하였다.

혼돈적인 궤적을 발생시키는 톱니맵 $S_2(x)$와 텐트맵 $T_S(x)$의 연결은, 기울기 S=2일 경우, 다음의 표현식 (9)와 같은 항등관계를 갖는다. [8]

$$T_2(T_2^n(x)) = T_2(S_2^n(x)) \quad (9)$$

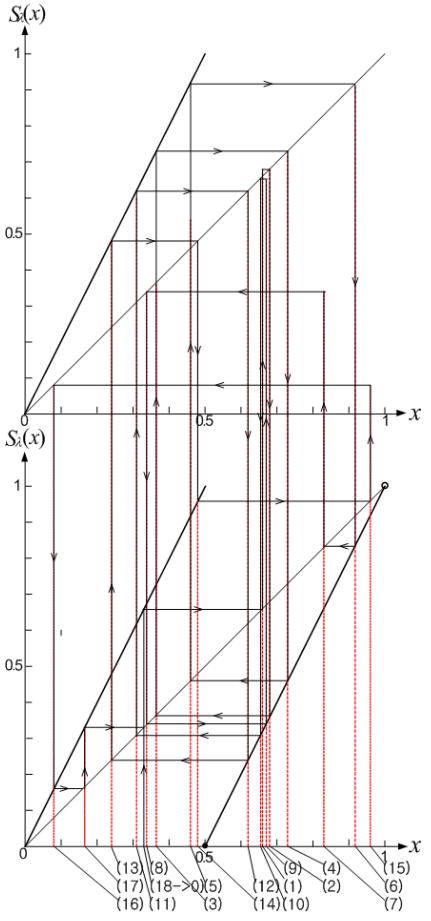


[그림 7] 합성상태머신

수식에서, n = 1,2,3,… 은 혼돈맵들-$S_2(x)$와 $T_2(x)$-의 n번째 합성(the n-th composition)을 의미한다. 이 논문에서 설계한 합성상태머신에 의해 수행할 수 있는 혼돈맵의 변환들은 다음식 (10)으로 표현할 수 있다.

$$T_2^2(x)) = T_2(T_2(x)) = T_2(S_2(x)) \quad (10)$$

그리고 발생하는 상태의 주기 P는, 이산화과정에서 16비트의 왼쪽 이동 레지스터(left shift resister : LSR)을 사용하였으므로, 하나의 입력마다 16개의 상태를 발생시키는 주기 P=15의 길이를 갖는다. (그림 8에 한 입력마다 주기 15인 발생하는 상태의 혼돈적인 주기성을 보인다.)



[그림 8] 발생 상태의 혼돈적인 주기성

5. 결론

디지털회로나 시스템에 관한 분류의 한 방법으로 두 가지 상태머신-Mealy머신과 Moore머신-을 정의하였고, 사용용도에 따라 두 종류중 하나나, 혼합된 형태를 설계하여 사용해왔다.

대부분, 기존의 상태머신들이 정해진 상태들을 발생시키는 데에 목표를 두었다면, 이 논문에서 설계하여 제시한 합성상태머신은 혼돈맵들의 변환에 의한 비선형적인 거동(nonlinear behavior)을 이용하여 난수적인 상태, 즉 혼동적인 상태(chaotic state)를 발생시키고자 하였다. 두 가지의 혼돈맵 [4~5] 을 결합한 독립된 하나의 혼돈맵이 주기성이 있는 의사 난수적인 상태를 발생하는 것을 보았으며 이러한 난수적인 상태 발생에 대한 시스템을 디지털 회로의 상태머신(state machine)에 활용하여 회로로 구현이 가능한 것을 보았다. 이 논문에서 보인 시스템을

활용하여 다양한 암호화기법들이나 시스템들 중에서 혼돈역학을 적용하는 스트림 암호시스템(stream cipher system)에 적용 시 시스템의 단순하면서 복잡한 암호화 시스템의 설계가 가능 할 것으로 보인다.

그림 5에 의해 합성상태 머신에서 발생되는 혼돈적인 상태들을 기하학적으로 입증하였고, 사용된 이산화진리표들에 따라 혼돈적인 상태들의 주기도 확인할 수 있었다. 물론, 두 혼돈맵들의 이산화진리표들을 어떻게 작성하느냐에 따라 발생하는 주기의 길이가 바뀔 수 있다. 향후 연구에서는 이에 대한 연구가 추가적으로 이루어져야 한다.

참고문헌

[1] Heinz-Otto Peitgen, Hartmut Jurgens, Dietmar Saupe, Evan Maletsky, Terry Percianate and Lee Yunker, "Fractals for the classroom", Springer-verlag(New York), 1991.

[2] Heinz Georg Schuster, "Deterministic Chaos", VCH Verlags gesellschaft revised edition, 1989.

[3] Joseph L.Mccauley, "Chaos, Dynamics, and Fractals (An Algorithmic approach to deterministic chaos)", Cambrige University Press, 1993.

[4] 박광현, 백승재, “혼돈맵을 사용한 난수성 2진 순서 발생기의 설계”, 한국콘텐트학회논문지 제8권 제7호 별쇄, 논문08-08-07-7, 2008년 07월.

[5] 백승재, 박진수, "이산화된 텐트맵의 설계", 한국콘텐트학회논문지 ‘04 Vol. 4 No.

[6] Milos D.Ercegovac and Tomas Lang, " Digital Systems and Hardware / Firmward Algorithms", John Wiley & Sons, 1985.

[7] Kwang-Hyeon Park, Jong-Sun Hwang and Chong-Eun Chung, "Implementation of Chaotic State Machine using Deterministic Chaos Function", Journal of Electrical Engineering and Information Science, Vol. 3, No. 2, 1998.

[8] Mieczyslaw Jessa, "The period of Sequences Generated by Tent-Like Maps" IEEE Trans. Circuits Syst. I, Vol. 49, pp.84-89, Jan. 2002

서 용 원(Won-Yong Seo) **[정회원]**

- 2002년 2월 : 청주대학교 전자공학과 (공학사)
- 2004년 2월 : 청주대학교 전자공학과 (공학석사)
- 2008년 9월 ~ 현재 : 청주대학교 전자공학과 (박사과정)
- 2006년 3월 ~ 현재 : (주)이씨엠 대표이사

<관심분야>
스트림암호, 부호이론, 정보이론, 디지털통신

박 진 수(Jin-Soo Park) **[정회원]**

- 1975년 2월 : 한양대학교 전자공학과(공학사)
- 1977년 2월 : 한양대학교 전자통신과(공학석사)
- 1985년 2월 : 한양대학교 전자통신과(공학박사)
- 1999년 3월 ~ 2008년 2월 : RRC 정보통신연구센터 소장
- 1978년 3월 ~ 현재 : 청주대학교 전자정보공학부 교수
- 2008년 3월 ~ 현재 : 청주대학교 학술정보처 처장

<관심분야>
이동통신, 디지털 통신, 부호이론, 스프레드스펙트럼, 스트림암호