LSB 확장 기법이 적용된 의사 혼돈 수열의 주기와 상관특성

최효정, 송홍엽
연세대학교
{hjchoi3022, hysong}@yonsei.ac.kr,

Period and autocorrelation properties of pseudo chaotic sequences generated by LSB extension method

Hyojeong Choi and Hong-Yeop Song
Yonsei Univ.

요 약

본 논문은 LSB(Least Significant Bit) 확장 기법이 적용된 이진 시프트 혼돈 맵(Binary Shift Chaotic Map, BSCM)의 출력 실수 수열의 주기와 상관 특성을 분석한다. 본 논문에서 BSCM의 LSB 확장은 하나의 LFSR을 사용하여 확장하는 경우와 두 개의 LFSR을 사용하여 확장하는 M-BSCM(modified BSCM)의 경우를 고려하여 출력 실수 수열들의 특성을 비교한다.

Ⅰ. 서 론

혼돈 맵(Chaotic map)은 초기값에 민감한 특성을 가지고 있어 미세한 초기값의 차이만으로도 완전히 다른 수열이 도출되는 비선형 함수이며, 서로 다른 무한한 수열을 쉽게 생성할 수 있으므로 의사 잡음 코드(PN code)를 사용하는 직접 수열 대역 확산 시스템에서 혼돈 수열의 사용이 고려되어왔다[1].

디지털 시스템에서 혼돈 수열을 고정 또는 부동 소수점 산술을 사용하여 구현하면 반올림 오류 등 연산의 오차가 발생하여 수열이 임의의 값으로 수렴하거나 짧은 주기성이 나타날 수 있다[2, 3]. 최근에는 이러한 디지털 구현 문제를 해결하기 위해 고정 또는 부동 소수점 산술에 의존하지 않고 AND, OR, NOT 등과 같은 간단한 논리 연산을 사용하여 반올림 오류에서 자유로운 LSB 확장 기법이 제안되었다[2, 3].

[2]에서 제안된 BSCM에대한 LSB 확장 기법은 의사 난수 생성기(Pseudo Random Number Generator, PRNG)를 사용하여 의사 혼돈 수열을 생성한다. 이 방식은 혼돈 맵의 초기값 뿐만 아니라 PRNG의 초기값도 출력 수열의 비밀키가 될 수 있다. 여기서 BSCM은 곱셈이 이진 시프트 연산이고, 덧셈 연산 중에 오버플로우가 발생하지 않는 혼돈 맵으로 정의된다. [2]에서는 BSCM으로 Bernoulli 맵, Tent 맵, Backer's 맵이 고려되었으며, 유의할 점은 이러한 BSCM에 대한 LSB 확장 기법 또한 유한 정밀도를 가진 디지털 구현에서의 산술이기 때문에 실제로 완전한 혼돈 수열이 아닌 의사 혼돈 수열이다.

[2]에서 제안한 기법에서 PRNG에 임의의 초기값을 적용하여 생성된 출력 수열과, 그 초기값의 시프트된 버전을 초기값으로 갖는 출력 수열은 시프트 관계에 있다. 따라서 [3]에서는 두 수열 간의 상호상관 특성이 좋지 않음을 보이고 하나의 LFSR 대신 두 개의 LFSR을 사용하여 변형된 BSCM (modified BSCM, M-BSCM)을 제안하였다.

본 논문에서는 BSCM으로 베르누이맵(Bernoulli map)과 텐트맵(Tent map)을 고려하여 [2]와 [3]에서 제안한 두 기법의 출력 수열들의 자기 상관 특성과 주기성을 비교 분석한다.

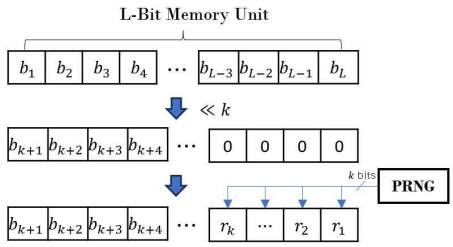


그림 1. PRNG를 사용한 LSB 확장 기법

Ⅱ. 본론

A. 이진 시프트 혼돈 맵(BSCM)

본 논문에서는 BSCM으로 베르누이맵과 텐트맵을 고려한다.
베르누이맵 S는 다음 식 (1)로 정의되는 함수이다.

$$S(x) = 2x \pmod 1 = \begin{cases} 2x, & 0 \le x \le 1/2 \\ 2x-1, & 1/2 \le x < 1 \end{cases} \quad (1)$$

베르누이맵은 최상위 비트(Most Significant Bit, MSB)를 버리고 왼쪽으로 한 비트 이동하는 연산으로 설명될 수 있다. 즉, $S(.b_1\, b_2\, b_3\, \cdots)_2 = (.b_2\, b_3\, b_4\, \cdots)_2$이다. 텐트맵 T는 다음 식 (2)로 정의되는 함수이다.

$$T(x) = \begin{cases} 2x, & 0 \le x < 1/2 \\ 2(1-x), & 1/2 \le x \le 1 \end{cases} \quad (2)$$

텐트맵의 구현은 베르누이맵과 비슷하며, 유일한 차이점은 $(1-x)$가 곱해지므로 보수 연산을 취하는 연산이 추가 된다. 자세한 구현 알고리즘은 [2]에 나와있다.

B. LSB 확장 기법

LSB 확장 방법의 주요 아이디어는 [2]의 2장에 자세히 설명되어있다. 그림 1과 같이 이 방법에서 모든 연산은 L비트 메모리 단위에서 수행된

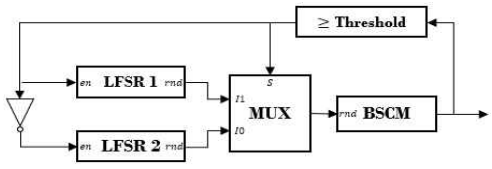


그림 2. M-BSCM의 구성

다. k비트 왼쪽 시프트를 수행할 때, k개의 LSB들은 0이 되고, 그 k개의 LSB들을 PRNG의 출력 비트들로 대체한다. II-A에서 설명한 BSCM들은 메모리 단위의 L비트를 단순히 왼쪽으로 한 칸 시프트 연산을 수행하거나 보수를 취하는 것으로 구현할 수 있다. 이렇게 L비트 메모리 유닛에서 해당 맵에 대한 연산이 수행된 후 이를 다시 L비트 부호없는 정수로 읽은 뒤 이 정수에 2^{-L}를 곱하여 0과 1사이의 실수가 생성된다.

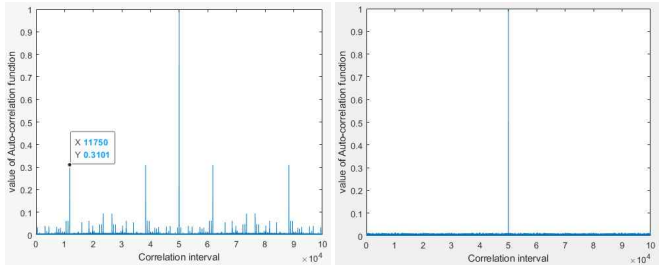
[2]에서는 이러한 BSCM의 연산 과정에 LSB 확장 기법을 적용할 때 하나의 LFSR을 적용하였다. [3]에서는 그림 2와 같이 두 개의 LFSR을 적용한 M-BSCM을 제안하였다. M-BSCM은 임계값을 설정하여 BSCM의 실수 출력값이 임계값을 넘으면 1, 넘지 않으면 0을 출력하여 MUX와 두 LFSR의 활성화를 위해 사용된다. 만약 BSCM의 실수 출력값이 임계값을 넘어 1이 출력되면 LFSR1이 활성화가 되고 NOT게이트를 지나 0으로 바뀌면서 LFSR2는 비활성화가 되면서 MUX에서 LFSR1의 출력이 BSCM의 LSB를 확장하는데 사용된다.

C. 실험 환경 및 의사 혼돈 수열의 특성 분석

본 논문에서는 BSCM으로 베르누이맵과 텐트맵을 고려하여, [2]에서 제안한 하나의 LFSR로 LSB가 확장 되는 기법을 통한 실수 출력 수열과 [3]에서 제안하는 두 개의 LFSR로 LSB가 확장 되는 기법을 통한 실수 출력 수열의 상관 특성을 먼저 분석한다. 수열의 길이는 50000으로 고정하여 실험하였으며, 16비트 메모리 유닛을 사용하였으며, 혼돈 맵의 초기값은 모두 0.7로 설정하였다. 16비트 메모리 유닛을 사용하였으므로 출력 실수 값이 0과 1사이를 2^{16}으로 양자화된 실수가 출력되기 때문에 자기 상관 특성을 확인하기 위해 2^{16}-th root of unity로 맵핑하여 2^{16}-ary 수열로 변환하여 자기 상관을 계산하였다. PRNG로는 16비트, 32비트 LFSR로 생성된 m-수열을 사용하였다.

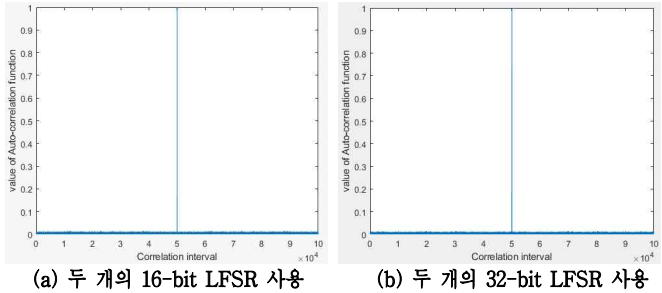
먼저, 그림 3은 BSCM으로 베르누이맵을 고려하여 LFSR로 주기 2^{16}-1, 주기 2^{32}-1인 m-수열을 사용한 경우의 실수 출력 수열을 2^{16}-ary 수열로 변환한 수열의 자기 상관 특성을 보여준다. 주기 2^{16}-1인 m-수열을 적용한 경우에는 사이드로브에 잦은 피크가 발생하고 가장 큰 피크 값은 0.31으로 좋지 않은 상관 특성을 갖는 것을 보여주며, 주기 2^{32}-1인 m-수열을 적용한 경우에는 사이드로브의 평균값이 약 0.003으로 좋은 상관 특성을 갖는 것을 확인했다. 또한, 이 경우의 출력 수열은 m-수열의 주기와 동일한 주기를 갖는 것을 확인했다. 그림 4는 베르누이맵을 M-BSCM에 적용한 경우이며, 하나의 LFSR을 적용한 경우보다 모두 좋은 상관 특성을 갖는 것을 확인했다.

그림 5는 BSCM으로 텐트맵을 고려하여 LFSR로 주기 2^{16}-1, 주기 2^{32}-1인 m-수열을 사용한 경우를 보여준다. 이들 모두 사이드로브의 가장 끝에 0.4정도의 하나의 피크값이 발생하는 것을 확인했고, 그 이외의 나머지 사이드로브들은 평균 약 0.004 정도로 낮은 상관 영역(Low correlation zone)에 속한다. 또한, 이 경우의 출력 수열은의 주기는 m-수열의 주기와 메모리 유닛의 개수를 곱한 것으로 매우 긴 주기를 갖는 것을 확인하였다. 그림 6의 M-BSCM에 텐트맵을 적용한 수열의 경우에도 그림 5의 경우와 유사한 자기 상관 특성을 갖는다.



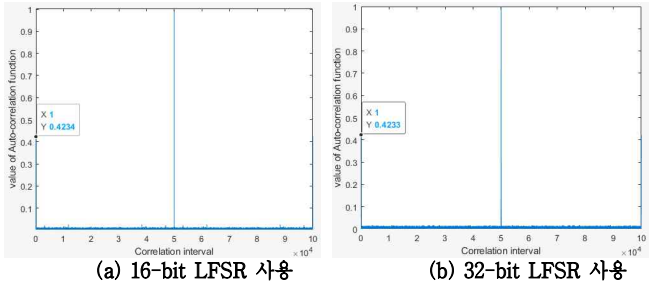
(a) 16-bit LFSR 사용 (b) 32-bit LFSR 사용

그림 3. 베르누이맵을 BSCM으로 고려한 수열의 자기 상관 특성



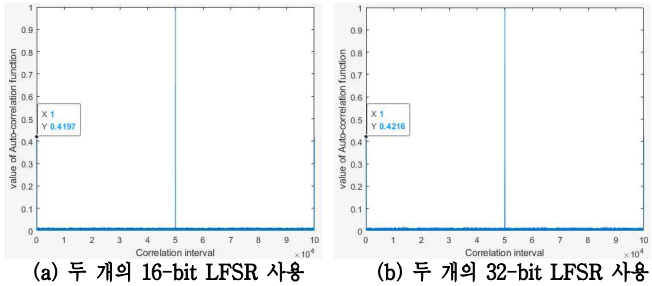
(a) 두 개의 16-bit LFSR 사용 (b) 두 개의 32-bit LFSR 사용

그림 4. 베르누이맵을 M-BSCM에 적용한 수열의 자기 상관 특성



(a) 16-bit LFSR 사용 (b) 32-bit LFSR 사용

그림 5. 텐트맵을 BSCM으로 고려한 수열의 자기 상관 특성



(a) 두 개의 16-bit LFSR 사용 (b) 두 개의 32-bit LFSR 사용

그림 6. 텐트맵을 M-BSCM에 적용한 수열의 자기 상관 특성

ACKNOWLEDGMENT

이 (성과)는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.RS-2023-00209000).

참 고 문 헌

[1] R. L. Devaney, An introduction to chaotic dynamical systems, CRC press, 2003.

[2] I. Öztürk and R. Kilic, "Digitally generating true orbits of binary shift chaotic maps and their conjugates," *Communications in Nonlinear Science and Numerical Simulation*, vol. 62, pp. 395 - 408, Sep. 2018.

[3] I. Öztürk and R. Kilic, "Utilizing true periodic orbits in chaos-based cryptography," *Nonlinear Dynamics*, vol.103, pp. 2805-2818, 2021.