x^2+ax+c를 이용한 수열 생성 방법의 특성화†

조성진* · 황윤희* · 최언숙** · 허성훈*** · 김진경*

*부경대학교, **동명대학교, ***김해대학

Characteristic of Method of generation sequence using x^2+ax+c

Sung-jin Cho* · Yoon-Hee Hwang* · Un-Sook Choi**· Seong-hun Heo***· Jin-Gyoung Kim*

*Pukyong National University, **Tongmyong University, ***Gimhae College

E-mail : sjcho@pknu.ac.kr*

요 약

최대 주기를 갖는 의사 난수열을 생성하기 위하여 다양한 방법들이 시도되어 왔다. 가장 일반적인 방법은 원시다항식을 특성다항식으로 갖는 LFSR을 생성기로 이용하는 방법, LFSR보다 랜덤성이 우수한 셀룰라 오토마타를 생성기로 이용하는 방법과 이차함수를 이용하여 최대 주기 수열을 생성하는 방법이 있다. 본 논문에서는 보다 긴 주기를 갖는 수열을 생성하기 위하여 이차함수를 이용한 수열 생성 방법에 관하여 분석하고 특성화한다.

ABSTRACT

Many researchers had made a diversity of attempts for generating pseudorandom sequences such as the method of using LFSR whose characteristic polynomial is a primitive polynomial, of using Cellular Automata and of using quadratic functions.

In this paper, we can analyze and characterize the methods for generating maximal period pseudorandom sequences constructed by quadratic functions.

키워드

의사 난수 생성, 이차함수, LFSR, 원시다항식, 셀룰라 오토마타

Ⅰ. 서 론

컴퓨터 네트워크는 많은 다른 개체들 간에 많은 양의 정보를 전달하는 등, 넓은 영역의 서비스를 제공한다. 이때, 현금 자동 지급기에서 예금·출자금 등의 인출하거나 네트워크 상에서 신용카드를 사용한 결제등과 같은 쉽게 노출될 수 있는 중요한 데이터의 관리에 대한 문제점이 발생하였다. 따라서 오늘날 정보보안은 매우 중요하며, 요구되는 보안 서비스들을 수행하기 위해서 많은 암호 기술들이 개발되어왔다. 의사난수열은 스트림 암호에 기반이 되는 암호시스템이다([1]-[4]). 스트림 암호는 매우 긴 주기의 의사 난수열을 발생시켜서 키로 사용한다. 이 때 만들어진 키는 평문과 더해져서 암호문으로 생성되는데 이렇게 생성된 암호문의 수열이 난수와 구별이 불가능해야만 안전하다고 할 수 있다. 스트림 암호를 설계하는데 다양한 방법들이 도입되었다. 그 중 LFSR과 Cellular Automata를 이용하는 방법은 최대주기 수열을 얻을 수 있으며 수학적 분석이 쉬운 장점이 있다. 하지만 출력 수열 중 적당한 길이의 연속된 출력값을 알면 그 다음에 출력될 값을 알 수 있듯이 패턴을 나타내는 단점이 있다.

이차함수는 암호학에서 매우 중요하다. 이차함수는 다른 유한 영역에서 연구되고 적용되었다([5], [6]). Z_{pq} (p와 q는 소수)에서 이러한 함수의 범위는 [5]에서 사용되었다. 그리고 $GF(2^n)$에서 정의된 이차함수는 [7]에서 사용되었다.

본 논문에서는 보다 긴 수열을 생성하기 위해서 이차함수를 이용한 수열의 생성방법에 대하여 분석하고 특성화한다. 특히 이차 다항식의 일차항의

†이 논문은 2009년도 정부재원(교육과학기술부 인문사회연구역량강화사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음(KRF-2009-371-B00008)

성분과 특성다항식과의 관계를 분석하고, 일차항의 성분이 α일 때 B 의 형태를 분석하여 특성다항식을 알아보고 또한 최대 길이를 생성하기 위한 일차항의 성분과 $B \cdot Q(B)$의 영공간 $N(B \cdot Q(B))$와 관계도 분석한다.

II. 이차함수를 이용한 의사난수 생성

[7]에서 $Tr\left(\frac{c}{\alpha^2+1}\right)=0$ 또는 $Tr\left(\frac{c}{\alpha^2+1}\right)=1$ 이냐에 따라서 상태들의 구조가 두 가지 형태로 나뉘어졌으며 상태전이 다이어그램을 사용한 이차함수 $f(x)=x^2+\alpha x+c$에 대한 α와 c를 특성화하였다.

본 논문에서는 trace 함수 없이 α와 c를 특성화한다.

이차함수 $f(x)=x^2+\alpha x$에 의한 다음상태의 계산은

$$f(1)=1^2+\alpha \cdot 1$$
$$f(1)=1^2+\alpha \cdot 1$$
$$f(\alpha)=(\alpha)^2+\alpha \cdot (\alpha)$$
$$f(\alpha^2)=(\alpha^2)^2+\alpha \cdot (\alpha^2)$$
$$\vdots$$
$$f(\alpha^n)=(\alpha^n)^2+\alpha \cdot (\alpha^n)$$

와 같이 선형이므로 행렬 B로 대신할 수 있고 B는 다음과 같이 구성할 수 있다. 이 때 B의 계수(rank)는 $n-1$이다.

$$B=\begin{bmatrix}\alpha^{n-1}(\alpha^{n-1}+\alpha)\\ \vdots \\ \alpha^2(\alpha^2+\alpha)\\ \alpha(\alpha+\alpha)\\ (1+\alpha)\end{bmatrix}^T$$

<예제1> 이차함수를 $f(x)=x^2+\alpha x$이라고 하자. 여기서 α는 원시다항식 $p(x)=x^7+x^3+x^2+x+1$의 근이며 행렬 B는 다음과 같다.

$$B=\begin{bmatrix}\alpha^6(\alpha^6+\alpha)\\ \alpha^5(\alpha^5+\alpha)\\ \alpha^4(\alpha^4+\alpha)\\ \alpha^3(\alpha^3+\alpha)\\ \alpha^2(\alpha^2+\alpha)\\ \alpha(\alpha+\alpha)\\ (1+\alpha)\end{bmatrix}^T=\begin{bmatrix}1\,0\,0\,1\,0\,0\,0\\ 1\,1\,1\,0\,0\,0\,0\\ 1\,1\,1\,1\,1\,0\,0\\ 1\,1\,1\,0\,1\,0\,0\\ 1\,0\,1\,0\,0\,0\,0\\ 1\,0\,1\,0\,0\,0\,1\\ 0\,0\,0\,0\,0\,0\,1\end{bmatrix}.$$

여기서 행렬 B의 계수는 3이다.

다음 정리는 행렬 B의 특성다항식에 대한 정확한 공식을 제공한다. 여기서 $a=\alpha$는 $GF(2^n)$ 상에서 정의된 원시근이다.

행렬 B의 $(n-1)$열 B_{n-1}과 n열 B_n은 각각 다음과 같으므로 보조정리 1을 얻을 수 있다.

$$B_{n-1}=(0,\cdots,0,0)^T$$
$$B_n=(0,\cdots,0,1,1)^T$$

<보조정리1> 이차함수 $f(x)=x^2+\alpha x$에 의해서 구성된 행렬 B의 형태는 다음과 같다.

$$B=\begin{bmatrix}\alpha^{n-1}(\alpha^{n-1}+\alpha)\\ \vdots \\ \alpha^2(\alpha^2+\alpha)\\ \alpha(\alpha+\alpha)\\ (1+\alpha)\end{bmatrix}^T=\begin{bmatrix}\vdots & \vdots & \vdots & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \vdots & \vdots & \vdots & 0 & 0\\ \vdots & \vdots & \vdots & 0 & 1\\ \vdots & \vdots & \vdots & 0 & 1\end{bmatrix}$$

보조정리1에 의하여 정리1을 얻을 수 있다.

<정리2> 이차함수 $f(x)=x^2+\alpha x$에 의해서 구성된 행렬 B의 특성다항식은

$$c(x)=|B\oplus xI|=x(x+1)Q(x)$$

이다.

<예제2> 예제1에와 같이 이차함수를 $f(x)=x^2+\alpha x$이라고 하자. 여기서 α는 원시다항식 $p(x)=x^7+x^3+x^2+x+1$의 근이라 하면, 행렬 B의 특성다항식은 다음과 같다.

$$c(x)=x(x+1)(x^5+x^4+x^3+x^2+1)$$

[7]에서 행렬 B의 특성다항식은 $p(x)+1$이며 $p(x)$는 $GF(2^n)$에서 정의된 기약다항식이다. $Q(x)=x^4+x+1$에 대하여 $x(x+1)Q(x)+1:=p(x)=(x^2+x+1)^3$은 기약다항식이 아니므로 행렬 B를 구성하는 것이 불가능하다.

<정리3> $f(x)=x^2+ax+c$가 $b,c\in GF(2^n)$를 갖는 $GF(2^n)$상에서 정의된 이차함수이고 α가 $GF(2^n)$의 원시근이라고 하자. B는 x^2+ax에 의해서 구성된 행렬이고 B의 특성다항식이 $c(x)$라 하자. 그러면 $x^2+a^{2^k}x$ 에 의해서 구성된 B'

의 특성다항식은 $c(x)$이다.

<예제3> 이차함수를 $f(x)=x^2+ax$이라고 하자. 여기서 α는 원시다항식 $p(x)=x^7+x^3+x^2+x+1$의 근이며 a를 다음과 같이 두면 특성다항식은 표 1과 같다.

표 1. b에 대한 특성다항식 $c(x)$

$a=\alpha^i$의 i값	특성다항식 $c(x)$
0	$x(x^3+x^2+1)(x^3+x+1)$
1,2,4,8, 16,32,64	$x(x+1)(x^5+x^4+x^3+x^2+1)$
3,6,12,24, 48,96,65	$x(x+1)^2(x^4+x+1)$
5,10,20,40, 80,33,66,	$x(x+1)^4(x^2+x+1)$
7,14,28,56, 67,97,112	$x^2(x+1)^2(x^3+x^2+1)$
9,18,36,72, 17,34,68	$x(x+1)^3(x^3+x+1)$
11,22,44,88, 49,98,69	$x^2(x+1)^2(x^3+x+1)$
13,26,52,104, 81,35,70	$x(x+1)^6$
15,30,60,120, 113,99,71	$x(x+1)(x^2+x+1)(x^3+x+1)$
19,38,76,25,50 ,100,73	$x^6(x+1)$
21,42,84,41, 82,37,74	$x^4(x+1)(x^2+x+1)$
23,46,92,57, 114,101,75	$x^2(x+1)(x^4+x+1)$
27,54,108,89, 51,102,77	$x(x+1)^2(x^2+x+1)^2$
29,58,116,105, 83,39,78,	$x^3(x+1)(x^3+x^2+1)$
31,62,124,121, 115,103,79	$x^2(x+1)(x^2+x+1)^2$
43,86,45,90, 53,106,85	$x^3(x+1)^4$
47,94,61,122, 117,107,87	$x(x+1)(x^5+x^3+1)$
55,110,93,59, 118,109,91,55	$x(x+1)(x^2+x+1)(x^3+x^2+1)$
63,126,125, 123,119	$x^4(x+1)^3$

이차함수에 의해서 생성되는 긴 주기의 난수를 생성하기 위해서는 $Q(x)$가 원시다항식이 되어야 한다. [7]에서 $Q(x)$가 원시다항식일 때 $x(x+1)Q(x)+1$가 $GF(2^n)$을 생성하는 원시다항식 $p(x)$가 되어야 한다고 했지만 $p(x)$와 $Q(x)$를 찾는 것은 매우 어렵고 어떤 차수에 대해서는 존재하지 않는 경우도 있다. 이러한 문제점을 보완하기 위해서 다음 정리는 긴 수열을 생성하는 효과적인 이차함수의 조건을 제시한다. 보다 긴 주기를 갖는 수열을 생성하기 위하여 비선형 함수인 이차식 $f(x)=x^2+\alpha x+c$를 이용한다.

<정리4> $f(x)=x^2+\alpha x+c$가 $c\in GF(2^n)$를 갖는 $GF(2^n)$상에서 정의된 이차함수이고 α가 $GF(2^n)$의 원시근이라고 하자. B는 $x^2+\alpha x$에 의해서 구성된 행렬이고 $N(B\cdot Q(B))$이 $B\cdot Q(B)$의 영공간이라고 하자. $c\notin N(B\cdot Q(B))$라면, $f(x)$에 의해서 생성된 상태전이 다이어그램의 최대주기 길이는 $2l$이다. 여기서 l은 $x^2+\alpha x$에 의해서 생성된 최대주기 길이를 나타낸다.

<예제4> $f(x)=x^2+\alpha x$가 $GF(2^4)$에서 정의된 이차함수이고 α가 $p(x)=x^4+x+1$의 원시근이라 하자. 그림1은 $f(x)$에 대한 상태전이 다이어그램을 보여준다.

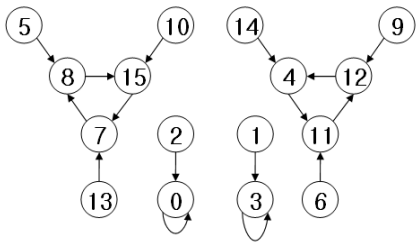
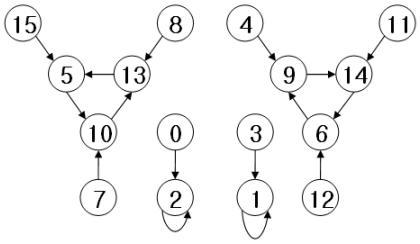


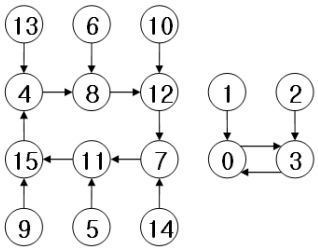
그림 1. $f(x)=x^2+\alpha x$에 대한 상태전이 다이어그램

$N(B\cdot Q(B))=B^3+B^2+B$은 $[2,5,8]$이며, $[2,5,8]$은 상태 2,5와 8에 의해서 생성된 부분공간 $\{0,2,5,7,8,10,13,15\}$이다. 그림2는 $c=2(\in N(B\cdot Q(B)))$와 $c=3(\notin N(B\cdot Q(B)))$인

경우에 대한 상태전이 다이어그램이다. 이차함수에 의해서 생성된 수열이 최대주기를 갖는다면, $Q(x)$는 반드시 원시다항식이어야 한다.



(a) $c=2(=\alpha)$



(b) $c=3(=\alpha^4)$

그림 2. $c=2,3$에 대한 상태전이 다이어그램

Ⅲ. 결론

본 논문에서는 보다 긴 수열을 생성하기 위해서 이차함수를 이용한 수열의 생성방법에 대하여 분석하고 특성화하였다. 특히 이차 다항식의 일차항의 성분과 특성다항식과의 관계를 분석하였고, 일차항의 성분이 α일 때 B 의 형태를 분석하여 특성다항식을 특성화하였으며 또한 최대 길이를 생성하기위한 일차항의 성분이 $N(B \cdot Q(B))$의 원소가 아니어야 함을 분석하였다.

참고문헌

[1] D. de la Guia and A. Fuster-Sabater, Cryptographic design based on cellular automata, IEEE international Symposium on Information Theory, pp. 180, 1997.

[2] S.J. Cho, U.S, Choi, Y.H. Hwang, Y.S. Pyo, H.D. Kim, K.S. Kim and S.H. Heo, Computing phase shifts of maximum-length 90/150 cellular automata sequences, In Proc. ACRI 2004, LNCS, 3305, pp. 31-39, 2004.

[3] S. Nandi, B.K. Kar and P.P. Chaudhuri, Theoty and application of cellular automata in cryptography, IEEE Trans. Computer vol. 43, pp. 1346-1357, 1994.

[4] A.K. Das and P.P. Chaudhuri, Vector space theoretic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation, IEEE Trans. Comput., vol. 42, pp. 340-352, 1993.

[5] L. Blum, M. Blum and S. Shub, A simpler unpredictable pseudorandom number generator, SIAM Journal on Computing, vol. 15, pp. 364-383, 1986.

[6] M. Blum and S. Goldwasser, An efficient probabilistic public key encryption scheme which hides all partial information, Proceeding of Advances in Cryptology-CRYPTO'84, LNCS, 196, pp. 289-299, 1985.

[7] D. de la Guia Martinez an A. Peinado Dominguez, Pseudorandom number generation based on nongroup cellular automata, Security Technology, Proceedings, IEEE 33rd Annual 1999 International Carnahan Conference, vol. 45, pp. 370-376, 1999.