通信情報保護學會論文誌
第7卷 第4號, 1997. 12

FCSR의 선형 복잡도 하한에 관하여

서 창 호*, 이 상 진*, 김 용 대*, 임 종 인**

On the Lower Bound of Linear Span of FCSR

Changho Seo, Sangjin Lee, Yongdae Kim, Jongin Lim

요 약

본 논문은 유한체 $GF(p)$에서 $r=2p+1$이 2-prime이고, p에 대한 2의 위수(order) m을 가질때, $q=r^e(e\geq 2)$를 연결 정수로 갖는 FCSR의 생성된 출력수열에 대한 선형 복잡도의 하한을 구한다.

Abstract

In this paper, we derive a lower bound of linear span of the sequences generated by FCSR with connection integer q, when q is of the form $r^e(e\geq 2)$ of a 2-prime integer $r=2p+1$ and m is the order of 2 modulo p.

1. 서 론

암호 기술 측면에서 이진 난수 발생기로서 여러 방면에서 응용이 가능한 LFSR(Linear Feedback Shift Register)[4]은 H/W로 구현하기가 용이하며, 출력 수열의 특성다항식에 대한 성질을 분석하면 출력 수열의 주기, 통계적 특성,선형 복잡도 등을 알 수 있어 스트림 암호 개발에 널리 활용되고 있다. 임의의 주기가 있는 이진 수열을 하나의 멱급수로 보면 그에 대응되는 유리다항식 $\frac{p(x)}{q(x)}$가 존재하며 이 유리다항식이 기약으로 표시되었다면, $q(x)$에 대응하는 LFSR로 그 수열을 생성할 수 있다. 이때 $q(x)$의 차수를 선형복잡도(linear span)라 한다.

1994년 A. Klapper 와 M. Goresky[5]가 FCSR(Feedback with Carry Shift Register)이라는 난수 발생기의 새로운 유형을 제안하였다. LFSR이 유한체 위의 다항식에 근거하여 설계

* 한국전자통신연구원
* * 고려대학교 수학과

↑ 이 논문은 1996년도 한국학술진흥재단의 공모과제 연구비에 의하여 연구되었음

되었다면 FCSR는 2-adic 수에 근거하여 설계되었다고 할 수 있다. 이 경우 주기가 있는 이진 수열을 2-adic 수로 생각하면, 그에 대응하여 하나의 유리수 $\frac{p}{q}$가 있고, 이 유리수가 기약이면 q에 대응되는 FCSR로 그 수열을 생성할 수 있다.

이 때 FCSR를 구성하는데 소요되는 단의 갯수를 2-adic 복잡도(2-adic span)라 한다. FCSR은 메모리를 사용하고 있기 때문에 LFSR에 비해 구현시 약간의 어려움이 있으나 생성 수열의 주기 및 선형복잡도 관점에서 많은 장점을 가지고 있다. 그러므로 최적 연결수를 사용한 FCSR로 부터 생성된 수열의 선형복잡도의 상한를 이론적인 증명 하였으며[9], FCSR을 이용하면 LFSR 사용할 때 보다 선형복잡도가 큰 난수열을 생성할 수 있는 방법이 있다.

본 논문에서는 유한체 $GF(p)$에서 $r=2p+1$이 2-prime이고 p에 대한 2의 위수(order)가 m일 경우, $q=r^e(e\geq 2)$를 연결 정수로 갖는 FCSR에 의하여 생성된 출력수열의 선형 복잡도 하한을 구하였다. 2절에서는 FCSR에 대하여 살펴보고 3절에서는 FCSR의 특성 및 선형복잡도에 대하여 기술하였다. 4절은 본 논문의 결론부이다.

2. FCSR

2가 아닌 소수 q에 대해서 $q+1=q_1 2+q_2 2^2+q_3 2^3+\ldots+q_t 2^t$, $q_i\in\{0,1\}$과 같은 이진 전개가 주어졌다고 하자. 이때 q를 연결수(connection number)로 하는 FCSR은 t개의 레지스터(register)와 메모리(memory) m으로 구성되어 있다. (그림 1)에서와 같이 레지스터의 초기치가 $(a_{t-1}, a_{t-2},\ldots, a_1, a_0)$이고 메모리가 m이면 FCSR의 동작은 다음과 같다.

1. 정수합 $\sigma=\sum_{k=1}^{t} q_k a_{t-k}+m$을 구한다.
2. 최하위 비트 a_0를 출력하고, 레지스터의 content들을 오른쪽으로 한 칸씩 이동한다.
3. $a_t\equiv\sigma(mod\ 2)$를 쉬프트 레지스터의 최상위 cell에 대치시킨다.
4. 메모리 m을 $(\sigma-a_t)/2$로 바꾼다.

정의 1 주기 수열 $a=(a_0, a_1, a_2,\ldots)$을 생성하는 가장 작은 FCSR의 크기를 수열의 2-adic span이라 한다.

정의 2 2가 $GF(q)$의 원시원(primitive element) 일때 q는 2-prime이라 한다.

2-prime인 소수 q를 FCSR의 연결 정수로 사용하면 FCSR의 동작에 필요한 단의 갯수는 $t=\log_2 q$이고 주기는 $q-1$이다. 그러므로 $2^t\leq q<2^{t+1}$이다. FCSR은 LFSR에 없는 메모리가 동작에 필요한다. 이진 주기 수열을 2-adic 수로 생각하면 하나의 기약 유리수 $\frac{p}{q}$를 대응시킬 수 있고, 이때 q를 연결수로 하는 FCSR을 이용

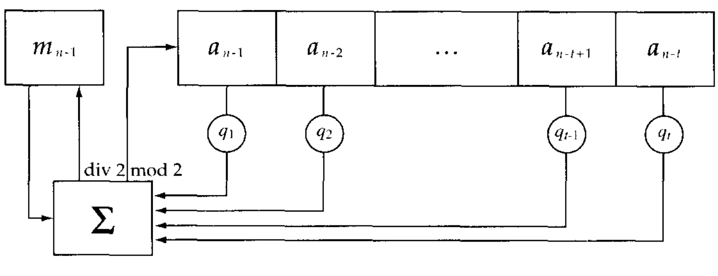


그림 1 : FCSR의 동작도

하여 주어진 이진 주기 수열을 생성할 수 있다[5].

3. FCSR의 선형 복잡도

본 절에서는 유한체 $GF(p)$에서 $r=2p+1$이 2-prime 이고, p에 대한 2의 위수(order) m을 가질때, $q=r^e(e\geq2)$를 연결 정수로 갖는 FCSR에 의하여 생성된 수열에 대한 선형복잡도 하한에 대하여 살펴본다.

주기 수열 $a=(a_0, a_1, a_2, \ldots)$가 연결수 q인 FCSR에 의해 생성되었다고 가정하자. 그리고, $\gamma=2^{-1}(\in Z/(q))$라 하자. 그러면, 적당한 $A\in Z/(q)$가 존재하여 모든 $i=0, 1, 2, \ldots$에 대해서

$$a_i \equiv A\gamma^i(q)(2)$$

이 된다. 여기에서, 표기 $(q)(2)$는 먼저 q로 나눈 나머지를 다시 2로 나눈 나머지이다.

정리 1 [7] 주기 수열 $a=(a_0, a_1, a_2, \ldots)$가 연결수 q인 FCSR에 의해 생성되었다고 가정하자. 만약 p가 2-prime이고, 연결 정수 q가 p^e이면, 모든 $i=0, 1, 2, \ldots$에 대해서

$$a_i+a_{i+\frac{\varphi(q)}{2}}=1.$$

여기서 $\varphi(q)=\varphi(p^e)=p^{e-1}(p-1)$이다.

정리 2 FCSR의 연결수 q가 2-prime이면 이러한 FCSR로부터 생성된 수열의 선형복잡도는 $\frac{q+1}{2}$ 보다 작거나 같다.

증명: 정리1에 의해서 FCSR의 출력 수열은 $a=(s, \bar{s}, s, \bar{s}, \ldots)$와 같은 형태의 수열이다. 여기서, $s=(a_0, a_1, \ldots, a_{\frac{q-1}{2}-1})$이고 $\bar{s}$는 s의 보수(complement)수열이다. 이때 다항식

$$1+x+x^{\frac{q-1}{2}}+x^{\frac{q+1}{2}}$$

은 수열 a의 특성 다항식이다. 그런데 선형 복잡도는 최소 다항식(minimal polynomial)[6]의 차수이고, 최소 다항식은 특성 다항식을 항상 나누므로 선형 복잡도는 $\frac{q+1}{2}$ 보다 작거나 같다.

주의 1[9] p와 $q=2p+1$이 2-prime이라 하자. 그러면 q을 연결수로 사용한 FCSR의 선형복잡도는 $p+1$이다.

정의 3 만약 p와 $q=2p+1$이 2-prime이라 할 때, 정수 q을 strong 2-prime 연결수(strong 2-prime connection integer)라고 한다.

strong 2-prime 연결수 q로 FCSR를 구성하면 FCSR의 출력 수열의 선형복잡도는 $\frac{q+1}{2}$가 된다. p에 대한 2의 위수 m를 갖고, 연결 정수 q가 $2p+1$ 또는 $q=r^e(r=2p+1)$ 형태를 사용하여 출력하는 수열의 선형 복잡도의 하한에 대하여 알아본다.

정리 3 만약 p에 대하여 2의 위수를 m을 갖고 $(2^m\equiv1(\bmod\ p))$, $q=2p+1$이 2-prime이라 하자. 그러면 q을 연결수로 사용한 FCSR의 선형복잡도의 하한은 $m+2$이다.

증명: 정리2에 의해서 FCSR의 출력 수열의 특성 다항식은

$$1+x+x^p+x^{p+1}=(1+x)(1+x^p) \tag{1}$$

이다.

그런데, $Q_i(x)$가 i번째 cyclotomic 다항식(i-th cyclotomic polynomial)[6]일때 아래의 식은 다음과 같이 성립한다.

$$x^p - 1 = \prod_{d|p} Q_d(x)$$
$$= Q_1(x) \times Q_p(x).$$

만약 m이 p에 대하여 2의 위수이면, $Q_p(x)$는 차수가 m인 기약다항식 $r_i(x)$의 곱 형태로 표현된다.

$$Q_p(x) = \prod_{i=1}^{\varphi(p)/m} r_i(x)$$

여기서 $\varphi(p)=p-1$이고 $r_i(x)$는 차수 m를 갖는 기약 다항식이다. 따라서 식(1)은

$$1+x+x^p+x^{p+1} = (1+x)(1+x^p)$$
$$= (1+x)(1+x) \times \prod_{i=1}^{\varphi(p)/m} r_i(x)$$
$$= (1+x^2) \times \prod_{i=1}^{\varphi(p)/m} r_i(x)$$

이다. 그런데 출력 수열의 주기가 $2p$이므로 위수가 $2p$이면서 식(1)의 약수인 최저차 다항식은 $(1+x^2)r_i(x)$이다. 그러므로 선형복잡도의 하한은 $m+2$이다.

주의 2 일반적으로 p에 대하여 2의 위수를 m일때 선형 복잡도(**Linear Span**)의 하한은 $m+2$이고, p가 2-prime이고 연결 정수 q가 strong 2-prime인 경우에는 선형 복잡도는 $p+1$이다.(즉 $m+2 \le LS \le p+1$)

주의 3 $q=r^e$($e>2$인 정수)에 대하여 r이 2-prime이라 하면 q을 연결수로 사용한 FCSR의 출력 수열의 주기는 $\varphi(q)=r^{e-1}(r-1)$이다.

정리 4 만약 $r=2p+1$이고 p에 대한 2의 위수가 m일 경우($2^m \equiv 1(\bmod p)$)에 $q=r^e$연결수로 사용한 FCSR로부터 생성된 수열의 선형 복잡도의 하한은 $lcm(m, \varphi(q)/r)+2$이다.

(증명): 정리 3과 마찬가지로, $Q_i(x)$가 i-th cyclotomic 다항식(cyclotomic polynomial)일때 아래의 식은 다음과 같이 성립한다.여기서, n은 $r^{e-1} \times p$이다.

$$x^{n-1} = \prod_{d|p} Q_d(x)$$
$$= \prod_{d|r^{e-1} \times p} Q_d(x)$$
$$= Q_1(x) \times Q_r(x) \times \ldots \times Q_{r^{e-1}}(x) \times Q_{rp}(x)$$
$$\times \ldots \times Q_{r^{e-1} \times p}(x).$$

$2^m \equiv 1(\bmod p)$, $2^{r^{e-2} \times (r-1)} \equiv 1(\bmod r^{e-1})$이므로, $n=r^{e-1} \times p$에 대한 2의 위수는 $b=lcm(m, r^{e-2} \times (r-1))$이다.

$$Q_{r^{e-1} \times p}(x) = \prod_{i=1}^{\varphi(n)/b} r_i(x)$$

여기서 $r_i(x)$ 다항식은 b차 기약 다항식이며, 위수는 $r^{e-1} \times p$이다.

그런데 출력 수열의 주기가 $r^{e-1}(r-1)$이므로 FCSR의 최소 다항식은 적당한 i에 대해서 $(1+x^2) \times r_i(x)$를 약수로 갖는다. 그러므로 선형복잡도의 하한은 $b+2$이다.

따름정리 1 $r=2p+1$이고, $q=r^e$($e>2$인 정수)이면서 r이 strong 2-prime인 경우에 선형복잡도의 하한은 $r^{e-2} \times p \times (p-1)+2$이다.

(증명): 정리 4에 의해서, $2^{p-1} \equiv 1(\bmod p)$, $2^{r^{e-2} \times (r-1)} \equiv 1 (\bmod r^{e-1})$이므로 선형 복잡도의 하한은 $lcm(p-1, r^{e-2} \times (r-1))+2$이다. 한편, $lcm((p-1), r^{e-2} \times (r-1))$의 최소 공배수는 $r^{e-2} \times p \times (p-1)$이다. 그러므로 p와 $q=r^e$이 2-prime 인 경우 선형복잡도의 하한은 $(r^{e-2} \times p \times (p-1))+2$이다.

FCSR의 연결 정수로 사용되는 2-prime의 정확한 밀도와 존재성에 대한 증명은 아직 없으나, 소수 중에서 2-prime인 소수는 약 $\frac{1}{3}$

표 1: 2-primes과 strong 2-prime의 개수

	2	3	4	5	6	7	8	9	10
2-prime	1	1	2	3	6	11	20	36	70
strong 2 prime	0	0	1	1	0	1	2	1	1

	14	15	16	17	18	19	20	21	22
2-prime	814	1521	2861	5395	10179	19424	36912	70499	134766
strong 2 prime	17	32	62	97	172	295	542	924	1748

정도 존재한다고 알려져 있다[3]. 컴퓨터 실험에 의해서, FCSR의 연결 정수로 사용할 만한 2-prime을 구하였고, 표 1에서와 같이 2 비트부터 비트를 증가하면 2-prime과 strong 2-prime의 갯수는 증가함을 알수 있었다.

4. 결 론

FCSR는 LFSR보다 선형 복잡도 관점에서 암호학적으로 우수한 스트림 암호의 구성 논리 소자이다. 본 논문에서는 strong 2-prime을 연결수로 사용하면 적은 단으로 구성된 FCSR의 선형복잡도는 주기의 반이라는 사실을 보였다. 그리고 p에 대한 2의 위수가 m이고 $r=2p+1$이 2-prime일때 연결 정수 $q=r^e$인 FCSR의 선형 복잡도 하한을 구하였다.

참 고 문 헌

[1] D.E. Knuth, The Art of Computer Programming, Vol.2: Seminumberical Algorithms, Addison-Wesley.1981.

[2] J. M. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Trans. Info. Theory, Vol. IT-15, 1969, 122-127.

[3] Hua Loo Keng, Introduction to Number Theory, Springer-Verlag, 1982, 406-422.

[4] R. A. Rueppel, Analysis and design of stream Ciphers, Springer-Verlag, 1986.

[5] A. Klapper and M. Goresky, "2-adic Shift Registers", private communication.

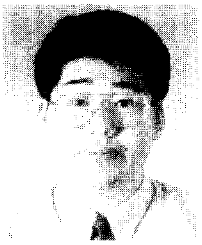
[6] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge Univ. Press, 1986.

[7] A. Klapper and M. Goresky, "Arithmetic Crosscorrelations of FCSR Sequences", IEEE Trans. Info. Theory, Vol. IT-43, 1997, 1342-1345.

[8] A. Klapper and M. Goresky, "Large Period Nearly deBruijn FCSR Sequences", Advances in Cryptology-EUROCRYPTO'95, pp. 263-273, 1995.

[9] 임종인, 이상진, 서창호, 엄봉식, "2-adic 수상에서 케리를 갖는 쉬프트 레지스터에 관한 연구", 한국통신정보보호학회 논문지, Vol.6, pp.33-40, 1996.

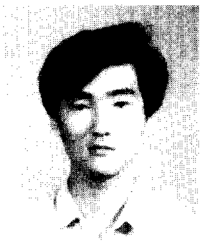
□ 著者紹介



서 창 호

1990년 2월 고려대학교 수학과 학사
1992년 8월 고려대학교 대학원 수학과 석사
1996년 8월 고려대학교 대학원 수학과 박사
1996년 ~ 현재 한국전자통신연구원 선임연구원

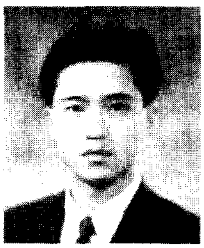
※ 주관심 분야 : 응용대수학 및 정수론, 암호론



이 상 진

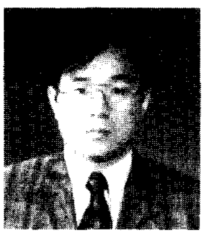
1987년 2월 고려대학교 이과대학 수학과(이학사)
1989년 2월 고려대학교 대학원 수학과(이학석사)
1994년 8월 고려대학교 대학원 수학과(이학박사)
1989년 ~ 현재 한국전자통신연구원 선임연구원

※ 주관심 분야 : 응용대수학 및 정수론, 암호론



김 용 대

1991년 2월 연세대학교 이과대학 수학과(이학사)
1993년 2월 연세대학교 대학원 수학과(이학석사)
1993년 2월 ~ 현재 한국전자통신연구원 연구원



임 종 인

1980년 2월 고려대학교 수학과 학사
1982년 2월 고려대학교 대학원 수학과 석사
1986년 2월 고려대학교 대학원 수학과 이학박사
1986년 8월 ~ 현재 고려대학교 수학과 교수

※ 주관심 분야 : 응용대수학 및 정수론, 암호론