M진 Sidel'nikov 수열의 F_p 상에서의 선형복잡도와 1-오류 선형복잡도

준회원 정 진 호*, 종신회원 양 경 철*

Linear Complexity and 1-Error Linear Complexity over F_p of M-ary Sidel'nikov Sequences

Jin-Ho Chung* ***Associate Member***, Kyeongcheol Yang* ***Lifelong Member***

요 약

본 논문에서는 $M \geq 3$이고 $p \equiv \pm 1 \bmod M$인 경우에 대해서 주기가 $p^m - 1$인 M진 Sidel'nikov 수열의 F_p 상에서의 선형복잡도의 하계와 1-오류 선형복잡도의 상계를 유도한다. 특히 $m \geq 4$이고 $p \equiv -1 \bmod 3$인 경우에는 3진 Sidel'nikov 수열의 정확한 1-오류 선형복잡도를 계산한다. 이 결과들을 바탕으로 선형복잡도와 1-오류 선형복잡도의 주기에 대한 비율의 근사적 특성을 제시한다.

Key Words : linear complexity, k-error linear complexity, Sidel'nikov sequences, M-ary sequences

ABSTRACT

In this paper we derive some lower bounds on the linear complexity and upper bounds on the 1-error linear complexity over F_p of M-ary Sidel'nikov sequences of period $p^m - 1$ when $M \geq 3$ and $p \equiv \pm 1 \bmod M$. In particular, we exactly compute the 1-error linear complexity of ternary Sidel'nikov sequences when $p \equiv -1 \bmod 3$ and $m \geq 4$. Based on these bounds we present the asymptotic behavior of the normalized linear complexity and the normalized 1-error linear complexity with respect to the period.

Ⅰ. 서 론

Sidel'nikov 수열은 1969년에 Sidel'nikov에 의해 처음 제안되었다[1]. 그리고 Lempel 등도 이와 독립적으로 이진 Sidel'nikov 수열을 제안하고 최적의 자기상관(autocorrelation) 특성을 가진다는 것을 증명하였다[2]. 선형복잡도(linear complexity)와 k-오류 선형복잡도(k-error linear complexity)는 수열의 암호학적 성능을 평가하는 중요한 척도이다. 주기(period)가 N인 수열 $S = \{s(t) | t = 0, 1, \cdots, N-1\}$의 선형복잡도 $LC(S)$는 다음과 같이 정의된다:

$$LC(S) = N - \deg(\gcd(x^N - 1, S(x))),$$

여기서 $S(x) = s(0) + s(1)x + s(2)x^2 \cdots + s(N-1)x^{N-1}$이다. 그리고 S의 k-오류 선형복잡도 $LC_k(S)$는 다음과 같이 정의된다[3]:

$$LC_k(S) = \min\{LC(S+E) | 0 \leq w_H(E) \leq k\},$$

여기서 E는 주기가 N인 수열이고 $w_H(E)$는 E의 한 주기에 해당하는 해밍 무게(Hamming weight)이다.

Sidel'nikov 수열의 선형복잡도에 관한 연구는 Helleseth와 Yang에 의해 시작되었다[4]. 이후에

※ 본 연구는 한국과학재단 특정기초 연구지원(R01-2003-000-10330-0)으로 수행되었습니다.
* 포항공과대학교 전자전기공학과 통신 및 신호설계 연구실 (kcyang@postech.ac.kr)
논문번호 : KICS2006-05-234, 접수일자 : 2006년 5월 26일, 최종논문접수일자 : 2006년 12월 4일

Helleseth 등에 의해 이진 Sidel'nikov 수열의 F_p 상에서의 선형복잡도에 대한 공식이 유도되었다[5],[6]. 그리고 Eun 등은 이진 Sidel'nikov 수열의 F_p 상에서의 1-오류 선형복잡도를 정확하게 계산하였다[7]. 또한 최근에 Kim 등에 의해 M진 Sidel'nikov 수열의 F_p 상에서의 선형복잡도에 관한 연구결과들이 발표되기 시작하였다[8],[9].

본 논문에서는 $M\geq 3$인 경우에 M진 Sidel'nikov 수열의 F_p 상에서의 선형복잡도의 하계(lower bound)와 1-오류 선형복잡도의 상계(upper bound)를 구하고 각각의 주기에 대한 비율의 근사적 특성을 서술한다.

본 논문의 구성은 다음과 같다. II장에서는 M진 Sidel'nikov 수열에 대해 소개하고 $M\geq 3$이고 $p\equiv\pm 1 \bmod M$인 경우에 F_p 상에서의 선형복잡도의 하계를 유도한다. III장에서는 같은 경우에 대해서 1-오류 선형복잡도의 상계를 구하고 $p\equiv -1 \bmod 3$이고 $m\geq 4$인 경우에 대해서 3진 Sidel'nikov 수열의 1-오류 선형복잡도를 정확하게 계산한다. 그리고 IV장에서는 얻어진 결과들에 대한 예제를 제시하고 V장에서 결론을 맺는다.

Ⅱ. M진 Sidel'nikov 수열의 선형복잡도

$M\geq 3$이고 p는 M보다 큰 소수이며 $M|p^m-1$이라 가정하자. 또한, F_{p^m}의 원시원소(primitive element) α와 $r=0,1,\ldots,M-1$에 대해서 다음 집합을 정의하자:

$$R_r=\{\alpha^{Ml+r}-1|0\leq l\leq (p^m-1)/M-1\}.$$

이 때, 주기가 p^m-1인 M진 Sidel'nikov 수열 $S=\{s(t)|t=0,1,\ldots,p^m-2\}$는 다음과 같이 정의된다[1]:

$$s(t)=\begin{cases} r, & \alpha^t\in R_r \\ r_0, & \alpha^t=-1, \end{cases}$$

여기서 $r_0=0$일 때 S는 균형성(balancedness)를 만족한다. 본 논문에서는 $r_0=0$인 경우를 다룬다.

수열 S의 F_p 상에서의 선형복잡도는 이산 푸리에 변환(discrete Fourier transform)의 해밍 무게와 같다[10]. S의 주기가 n일 때 이산 푸리에 변화은 다음과 같이 정의된다:

$$A_i=\frac{1}{n}\sum_{t=0}^{n-1}s(t)\alpha^t.$$

Kim 등은 M진 Sidel'nikov 수열의 이산 푸리에 변환을 다음과 같이 유도했다.

<u>정리 1.</u>[8],[9] 소수 p에 대해서 $L=(p^m-1)/M$이고 $p>M$이라 하자. 주기가 p^m-1인 M진 Sidel'nikov 수열 S의 이산 푸리에 변환은 다음과 같이 유도 된다.

$$A_{-i}=\frac{M-1}{2}(-1)^i-(-1)^i\sum_{v=1}^{M-1}\frac{B_v(i)}{1-\alpha^{vL}}, \tag{1}$$

여기서 $B_v(i)=\binom{i}{vL}(-1)^{vL}$, $0\leq i\leq p^m-2$이다.

2.1 $p\equiv -1 \bmod M$인 경우

주어진 조건에서 L이 자연수가 되기 위해서 m은 2 이상의 짝수여야 한다. $M=3$인 경우에 $\binom{i}{L}$과 $\binom{i}{2L}$을 Lucas 정리[11]에 따라 모듈로 p에서 전개하면 규칙적인 형태를 얻는다[8],[9]. 이것을 다음과 같이 3 이상의 M에 대해 일반화할 수 있다.

<u>보조정리 2.</u> 소수 p에 대해서 $p=Md-1$, $d\geq 2$이고 m은 2 이상의 짝수일 때, $L=(p^m-1)/M$이라 하자. $0\leq i\leq p^m-2$, $1\leq v\leq M-1$에 대해 $\binom{i}{vL}$은 다음과 같이 전개할 수 있다:

$$\binom{i}{vL}=\binom{i_{m-1}}{vd-1}\binom{i_{m-2}}{(M-v)d-1}\cdots\binom{i_1}{vd-1}\binom{i_0}{(M-v)d-1} \bmod p$$

여기서 $i=\sum_{k=0}^{m-1}i_kp^k$, $0\leq i_k\leq p-1$이다. $\square$

<u>정리 3.</u> 소수 p에 대해서 $p=Md-1$, $d\geq 2$이고 m은 2 이상의 짝수일 때, 주기가 p^m-1인 M진 Sidel'nikov 수열 S의 F_p 상에서의 선형복잡도 $LC(S)$는 다음을 만족한다.

(a) M이 홀수인 경우,

$$LC(S)\geq p^m-d^m\sum_{j=2}^{M-1}\{(M-j)^{m/2}-(M-1-j)^{m/2}\}(j-1)^{m/2};$$

(b) M이 짝수인 경우,

$$LC(S)\geq p^m-d^m\sum_{j=2}^{M-1}\{(M-j)^{m/2}-(M-1-j)^{m/2}\}(j-1)^{m/2} -d^m\{(M/2)^{m/2}-(M/2-1)^{m/2}\}^2$$

증명) (1)에서 모든 $v\in\{0,1,\dots,M-1\}$에 대해 $B_v(i)=0$이면 $A_{-i}=(-1)^i(M-1)/2\neq 0$이다. 또한 어떤 v_0, $1\le v_0\le M-1$에 대해 $B_{v_0}(i)\neq 0$, $\alpha^{v_0L}\notin F_p$이고 모든 $v\neq v_0$에 대해서 $B_v(i)=0$이면

$$A_{-i}=(-1)^i\frac{M-1}{2}-(-1)^i\frac{B_{v_0}(i)}{1-\alpha^{v_0L}}\neq 0$$

이다. $\alpha^{vL}\in F_p$에 대한 필요충분조건은 $(\alpha^{vL})^{p-1}=1$이고, 이 조건은 $p^m-1|vL(p-1)$이 성립할 때만 만족된다. $vL(p-1)=(p^m-1)\cdot v(p-1)/M$이므로 M이 홀수인 경우에는 모든 v에 대해 $\alpha^{vL}\notin F_p$이고, M이 짝수인 경우에는 $v=M/2$일 때만 $\alpha^{vL}\in F_p$이다.

$|\{v|B_v(i)\neq 0, 1\le v\le M-1\}|\ge 2$인 i의 개수를 C라 하고 $i_a=\min\{i_{m-1},i_{m-3},\dots,i_1\}$, $i_b=\min\{i_{m-2},i_{m-4},\dots,i_0\}$라 하자. $1\le j\le M-1$일 때 $jd-1\le i_a\le M-1$일 때 $jd-1\le i_a\le(j+1)d-1$이 성립하도록 $(i_{m-1},i_{m-3},\dots,i_1)$을 선택하는 경우의 수는 $[(M-j)d]^{m/2}-[(M-j-1)d]^{m/2}$이다. 이러한 $(i_{m-1},i_{m-3},\dots,i_1)$에 대해서 $|\{v|B_v(i)\neq 0,1\le v\le M-1\}|\ge 2$가 성립할 조건은 $j\ge 2$이고 $i_b\ge(M-j+1)d-1$를 만족하는 것이다. 이러한 $(i_{m-2},i_{m-4},\dots,i_0)$를 선택하는 방법의 수는 $[(j-1)d]^{m/2}$이다. 여기서 $i=p^m-1$인 경우를 배제하면

$$C=d^m\sum_{j=2}^{M-1}\{(M-j)^{m/2}-(M-1-j)^{m/2}\}(j-1)^{m/2}-1$$

이다. 그리고 M이 짝수일 때 $B_{M/2}(i)\neq 0$이고 $v\neq M/2$에 대해서는 $B_v(i)=0$인 i의 개수를 C'라 하면 C'은 $(M/2)d-1\le i_a,i_b\le(M/2+1)d-1$인 i의 개수와 같으므로

$$C'=d^m\{(M/2)^{m/2}-(M/2-1)^{m/2}\}$$

이다. 따라서 M이 홀수인 경우에

$$LC(S)\ge p^m-1-C$$

이고 M이 짝수인 경우에

$$LC(S)\ge p^m-1-C-C'$$

이다. □

정리 3의 결과에서 M이 홀수일 때

$$\sum_{j=2}^{M-1}(M-j)^{m/2}(j-1)^{m/2}\le(M-2)\left(\frac{M-1}{2}\right)^m,$$

$$\sum_{j=2}^{M-1}(M-1-j)^{m/2}(j-1)^{m/2}\ge(M-3)^{m/2+1}$$

이 성립하므로

$$LC(S)\ge p^m-d^m\left[(M-2)\left(\frac{M-1}{2}\right)^m-(M-3)^{m/2+1}\right]$$

임을 알 수 있다.

다음과 같이 4진 Sidel'nikov 수열에 대해서 더욱 엄밀한 선형복잡도의 하계를 얻을 수 있다.

정리 4. $p=4d-1$, $d\ge 2$인 소수 p에 대해서 m이 2 이상의 짝수일 때, 주기가 p^m-1인 M진 Sidel'nikov 수열 S_4의 F_p 상에서의 선형복잡도 $LC(S_4)$는 다음을 만족한다.

$$LC(S_4)\ge p^m-(2^m-2^{m/2+1}+2)d^m.$$

증명) 정리 1에 의해 $A_{-i}=0$에 대한 필요충분조건은

$$3=\left(\binom{i}{L}-\binom{i}{3L}\right)\alpha^L+\binom{i}{L}+\binom{i}{2L}+\binom{i}{3L}$$

이 성립하는 것이다. 따라서 모든 $v\in\{1,2,3\}$에 대해서 $B_v(i)=0$이면 $A_{-i}=0$이다. 그리고 $\alpha^L,\alpha^{3L}\notin F_p$이므로 $B_1(i)$와 $B_3(i)$ 중 하나만 0인 경우에도 $A_{-i}\neq 0$이다. 따라서

$$\begin{aligned}LC(S_4)&\ge p^m-1-(d^m-1)-((2d)^{m/2}-d^{m/2})^2\\&=p^m-(2^m-2^{m/2+1}+2)d^m\end{aligned}$$

이므로 주어진 식이 성립한다. □

2.2 $p\equiv +1 \bmod M$인 경우

이 경우에 모든 자연수 m에 대해서 L은 자연수이다. M이 $p-1$을 나누기 때문에 α^{vL}은 모든 v에 대해서 F_p의 원소이다. $p=Md+1$이라 두면 $\binom{i}{vL}$을 모듈로 p에서 다음과 같이 전개할 수 있다.

$$\binom{i}{vL}=\binom{i_{m-1}}{vd}\binom{i_{m-2}}{vd}\cdots\binom{i_1}{vd}\bmod p.$$

이 식을 이용해서 다음 결과를 유도할 수 있다.

정리 5. 어떤 소수 p에 대해서 $p=Md+1$, $d\geq 1$이고 m은 양의 정수라 하자. 주기가 p^m-1인 M진 Sidel'nikov 수열 S의 F_p 상에서의 선형복잡도 $LC(S)$는 다음을 만족한다.

$$LC(S)\geq p^m-[(M-1)d+1]^m.$$

증명) $i=\sum_{k=0}^{m-1}i_kp^k$에 대해 $i_c=\min\{i_{m-1},i_{m-2},\cdots,i_0\}$라 하자. $i_c<d$이면 모든 v에 대해 $B_v(i)=0$이므로 $A_{-i}\neq 0$이다. 이러한 i의 개수를 C'이라 하면

$$C'=p^m-1-\{[(M-1)d+1]^m-1\}$$

이고 다음이 성립한다.

$$LC(S)\geq C^*. \qquad \square$$

정리 3, 4, 5를 통해 $p\equiv\pm 1 \bmod M$일 때 주기가 p^m-1인 M진 Sidel'nikov 수열의 F_p 상에서의 선형복잡도를 주기로 나눈 값은 m이 커질 때 근사적으로 1에 수렴한다는 것을 알 수 있다.

Ⅲ. M진 Sidel'nikov 수열의 1-오류 선형복잡도

Eun 등은 원래의 수열에 1비트 이하의 오류가 더해진 수열의 이산 푸리에 변환을 써서 이진 Sidel'nikov 수열의 1-오류 선형복잡도를 정확하게 계산하였다[7]. 길이가 p^m-1이고 해밍무게가 0 또는 1인 오류수열은 $\lambda\in F_p$, $0\leq\tau\leq p^m-2$에 대해 다음과 같이 나타낼 수 있다.

$$E(\lambda,\tau)=\{\lambda I(\alpha^{t-\tau}+1)\,|\,0\leq t\leq p^m-2\},$$

여기서 $I(x)$는 $I(0)=1$이고 $x\neq 0$에 대해서 $I(x)=0$이다. 원래의 수열에 1비트 이하의 오류가 더해진 수열 $S(\lambda,\tau)$의 이산 푸리에 변환을 이용해서 다음 결과들을 얻을 수 있다.

3.1 $p\equiv -1 \bmod M$인 경우

정리 1과 보조정리 2를 이용해서 다음 결과를 얻을 수 있다.

정리 6. 소수 p에 대해서 $p=Md-1$, $d\geq 2$이고 m은 2 이상의 짝수일 때, 주기가 p^m-1인 M진 Sidel'nikov 수열 S의 F_p 상에서의 1-오류 선형복잡도 $LC_1(S)$는 다음을 만족한다.

$$LC_1(S)\leq d^m\sum_{j=1}^{M-1}\{(M-j)^{m/2}-(M-1-j)^{m/2}\}j^{m/2}-1.$$

증명) 1비트 이하의 오류가 더해진 수열 $S(\lambda,\tau)$의 이산 푸리에 변환 $A_{-i}(\lambda,\tau)$는 다음과 같다.

$$A_{-i}(\lambda,\tau)=\left(\frac{M-1}{2}-\lambda\alpha^{\tau i}\right)(-1)^i-(-1)^i\sum_{v=1}^{M-1}\frac{B_v(i)}{1-\alpha^{vL}}.$$

따라서

$$A_{-i}\left(\frac{M-1}{2},0\right)=-(-1)^i\sum_{v=1}^{M-1}\frac{B_v(i)}{1-\alpha^{vL}}$$

이다. $A_{-i}\left(\frac{M-1}{2},0\right)\neq 0$에 대해한 필요조건은 적어도 하나의 v에 대해서 $B_v(i)\neq 0$이 성립하는 것이다. $1\leq j\leq M-1$이고 $jd-1\leq i_a<(j+1)d-1$일 때 $B_v(i)\neq 0$인 v가 적어도 하나 존재하기 위해서는 $j\geq 1$이고 $i_b\geq (M-j)d-1$이 성립해야 한다. 그러한 i의 개수를 C''라 하면

$$C''=d^m\sum_{j=1}^{M-1}\{(M-j)^{m/2}-(M-1-j)^{m/2}\}j^{m/2}-1$$

이고 $S\left(\frac{M-1}{2},0\right)$의 선형복잡도는 C''보다 작거나 같다. 따라서 1-오류 선형복잡도의 정의에 의해 주어진 정리가 성립한다. $\square$

특수한 경우로서 3진 Sidel'nikov 수열에 대해서는 다음과 같이 1-오류 선형복잡도를 정확하게 계산할 수 있다.

정리 7. 소수 p에 대해서 $p=3d-1$, $d\geq 2$이고 m은 4 이상의 짝수일 때, 주기가 p^m-1인 3진 Sidel'nikov 수열 S_3의 F_p 상에서의 1-오류 선형복잡도 $LC_1(S)$는 다음을 같다.

$$LC_1(S)=(2^{m/2+1}-1)d^m-1.$$

증명) $M=3$인 경우에 $S_3(\lambda,\tau)$의 이산 푸리에 변환 $A_{-i}(\lambda,\tau)$는 다음과 같이 주어진다.

$$A_{-i}(\lambda,\tau)=(-1)^i(1-\lambda\alpha^{\tau i}) - \frac{(-1)^i}{3}\left\{\left(\binom{i}{L}-\binom{i}{2L}\right)\alpha^L+2\binom{i}{L}+\binom{i}{2L}\right\}.$$

각각의 (λ,τ)에 따른 $S_3(\lambda,\tau)$의 선형복잡도를 다음과 같은 경우들에 대해서 비교해 본다.

i) $(\lambda,\tau)=(1,0)$인 경우

$A_{-i}(\lambda,\tau)=0$에 대한 필요충분조건은 $\binom{i}{L}=\binom{i}{2L}=0$이다. 따라서 $LC(S_3(1,0))$는 $\binom{i}{L}\neq 0$이거나 $\binom{i}{2L}\neq 0$인 i의 개수와 같으므로 보조정리 2에 의해

$$LC(S_3(1,0))=(2^{m/2+1}-1)d^m-1$$

이다.

ii) $\lambda=0$인 경우

이 경우에는 원래의 수열 S_3가 유지되므로 $m\geq 4$에 대해서

$$LC(S_3(0,\tau))\geq p^m-d^m\geq LC(S_3(1,0))$$

이 성립한다.

iii) $\lambda\neq 0$, $\alpha^\tau\in F_p$이고 $(\lambda,\tau)\neq(1,0)$인 경우

$A_{-i}(\lambda,\tau)=0$을 만족하는 i의 개수를 C_3라 하자. $\alpha^L\notin F_p$이고 $\alpha^\tau\in F_p$이므로

$$\begin{aligned}C_3&=\left|\left\{i\,\middle|\,\binom{i}{L}=\binom{i}{2L}=0 \text{ and } \binom{i}{L}=1-\lambda\alpha^{\tau i}\right\}\right|\\&\leq\left|\left\{i\,\middle|\,\binom{i}{L}=\binom{i}{2L}=0 \text{ and } \lambda\alpha^{\tau i}=1\right\}\right|\\&\quad+\left|\left\{i\,\middle|\,\binom{i}{L}=\binom{i}{2L}\neq 0 \text{ and } \lambda\alpha^{\tau i}\neq 1\right\}\right|\\&\leq|\{i|\lambda\alpha^{\tau i}=1\}|+\left|\left\{i\,\middle|\,\binom{i}{L}\neq 0 \text{ and } \binom{i}{2L}\neq 0\right\}\right|\\&\leq\frac{p^m-1}{2}+d^m-1\end{aligned}$$

이 성립한다. 따라서

$$LC(S_3(\lambda,\tau))=p^m-1-C_3\geq(p^m-1)/2-d^m+1$$

이므로 $m\geq 4$일 때

$$LC(S_3(\lambda,\tau))\geq LC(S_3(1,0))$$

이다.

iv) $\lambda\neq 0$, $\alpha^\tau\notin F_p$인 경우

$\lambda\alpha^{\tau i}=1$을 만족하는 i에 대해서 $A_{-i}(\lambda,\tau)=0$에 대한 필요충분조건은 $\binom{i}{L}=\binom{i}{2L}=0$이다. $\lambda\alpha^{\tau i}\neq 1$인 i에 대해서 $A_{-i}(\lambda,\tau)=0$이 성립하기 위해서는 $\binom{i}{L}\neq 0$이거나 $\binom{i}{2L}\neq 0$을 만족해야 한다. 따라서 다음 식을 얻을 수 있다.

$$\begin{aligned}C_3&\leq|\{i|\lambda\alpha^{\tau i}=1\}|+\left|\left\{i\,\middle|\,\binom{i}{L}\neq 0 \text{ or } \binom{i}{2L}\neq 0\right\}\right|.\\&\leq\frac{p^m-1}{3}+(2^{m/2+1}-1)d^m-1.\end{aligned}$$

따라서

$$LC(S_3(\lambda,\tau))\geq\frac{2(p^m-1)}{3}-(2^{m/2+1}-1)d^m+1$$

이므로 $m\geq 4$일 때

$$LC(S_3(\lambda,\tau))\geq LC(S_3(1,0))$$

이다.

그러므로 i), ii), iii), iv)의 결과에 의해 주어진 정리가 성립함을 알 수 있다. □

3.2 $p\equiv+1 \bmod M$인 경우

정리 5의 증명 과정으로부터 다음을 얻을 수 있다.

따름정리 8. 어떤 소수 p에 대해서 $p=Md+1$, $d\geq 1$이고 m은 양의 정수라 하자. 주기가 p^m-1인 M진 Sidel'nikov 수열 S의 F_p 상에서의 1-오류 선형복잡도 $LC_1(S)$는 다음을 만족한다.

$$LC(S)\leq[(M-1)d+1]^m-1. \qquad \square$$

정리 6, 7과 따름정리 8로부터 $p\equiv\pm 1 \bmod M$일 때 주기가 p^m-1인 M진 Sidel'nikov 수열의 F_p 상에서의 1-오류 선형복잡도의 주기에 대한 비율은 m이 커질 때 근사적으로 0에 가까워진다는 것을 알 수 있다.

Ⅳ. 예 제

정리 3과 정리 7에 의해 $p=5$일 때 $LC(S_3)$의 하계 L_3와 $LC_1(S_3)$의 상계 U_3는 각각 다음과 같다.

$$L_3 = 5^m - 2^m,$$
$$U_3 = (2^{m/2+1} - 1)2^m - 1.$$

마찬가지로 $p = 11$일 때는 다음을 얻을 수 있다:

$$L_3 = 11^m - 4^m,$$
$$U_3 = (2^{m/2+1} - 1)4^m - 1.$$

표 1은 m이 변화할 때 이러한 값들의 주기에 대한 비율을 나타낸다.

표 1. $p = 5, 11$일 때 주어진 경계의 비교 ($M = 3$).

m	$p=5$		$p=11$	
	$L_3/(p^m-1)$	$U_3/(p^m-1)$	$L_3/(p^m-1)$	$U_3/(p^m-1)$
2	0.8750	0.4583	0.8750	0.3917
4	0.9760	0.1779	0.9826	0.1223
6	0.9960	0.0614	0.9977	0.0347
8	0.9993	0.0203	0.9997	0.0095

정리 4와 정리 6에 의해 $p = 11$인 경우에 $LC(S_4)$의 하계 L_4와 $LC_1(S_4)$의 상계 U_4는 각각 다음과 같다:

$$L_4 = 11^m - (2^m - 2^{m/2+1} + 2)3^m,$$
$$U_3 = (2 \cdot 3^{m/2} - 2^{m/2+1} + 2^m)3^m - 1.$$

표 2는 서로 다른 M에 대해서 주어진 선형복잡도의 하계와 1-오류 선형복잡도의 상계의 주기에 대한 비율을 나타낸다.

표 2. $M = 3, 4$일 때 주어진 경계의 비교 ($p = 11$).

m	$M=3$		$M=4$	
	$L_3/(p^m-1)$	$U_3/(p^m-1)$	$L_3/(p^m-1)$	$U_3/(p^m-1)$
2	0.8750	0.3917	0.8583	0.4417
4	0.9826	0.1223	0.9447	0.1438
6	0.9977	0.0347	0.9794	0.0420
8	0.9997	0.0095	0.9931	0.0118

V. 결 론

$M \geq 3$이고 $p \equiv \pm 1 \bmod M$인 경우에 대해서 주기가 $p^m - 1$인 M진 Sidel'nikov 수열의 F_p 상에서의 선형복잡도의 하계와 1-오류 선형복잡도의 상계를 구하였다. m이 커짐에 따라 선형복잡도의 주기에 대한 비율은 1에 수렴하지만 1-오류 선형복잡도의 주기에 대한 비율은 0에 가까워진다는 것을 알 수 있었다. 또한 $p \equiv -1 \bmod 3$이고 $m \geq 4$일 때 3진 Sidel'nikov 수열의 1-오류 선형복잡도를 정확하게 계산하였다.

참 고 문 헌

〔1〕 V. M. Sidel'nikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, no. 1, pp. 12-16, Jan. 1969.

〔2〕 A. Lempel, M. Cohn and W. L. Eastman, "A class of balanced binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. 23, no. 1, pp. 38-42, Jan. 1977.

〔3〕 M. Stamp and C. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2^n," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1398-1401, July 1993.

〔4〕 T. Helleseth and K. Yang, "On binary sequences of period $p^m - 1$ with optimal autocorrelation," *Sequences and Their Applications 2001, Discrete Mathematics and Theoretical Computer Science*, Springer, pp. 209-217, Aug. 2001.

〔5〕 T. Helleseth, S.-H. Kim, and J.-S. No, "Linear complexity over F_p and trace representation of Lempel-Cohn-Eastman sequences," *IEEE Trans. Inform. Theory,* vol. 49, no, 6, pp. 1548-1552, June 2003.

〔6〕 T. Helleseth, M Maas, J. E. Mathiassen, and T. Segers, "Linear complexity over F_p of Sidel'nikov sequences," *IEEE Trans. Inform. Theory,* vol. 50, no, 10, pp. 2468-2472, Oct. 2004.

〔7〕 Y.-C. Eun, H.-Y. Song, and G. Kyureghyan, "1-Error linear complexity over F_p of Sidelnikov sequences," *Lecture Notes in Computer Science*, vol. 3486, *Sequences and Their Applications 2004*, Springer, pp. 154-165, Mar. 2005.

〔8〕 Y.-S. Kim, J.-S. Chung, J.-S. No, and H.

Chung, "Linear complexity over F_p of M-ary Sidel'nikov sequences," *제 15회 통신정보 합동학술대회 (JCCI 2005) 논문집*, 대구, 2005년 4월, 제 15권, pp. 100.

[9] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the linear complexity over F_p of M-ary Sidel'nikov sequences," in *Proc. 2005 IEEE Inter. Symp. Inform. Theory*, Adelaide, Australia, Sep. 2005, pp. 2007-2011.

[10] R. E. Blahut, "Transform techniques for error control codes," *IBM J. Res. Develop.*, vol. 23, pp. 299-315, May 1979.

[11] P. J. Cameron, *Combinatorics: topics, techniques, algorithms*, Cambridge University Press, 1994.

정 진 호 (Jin-Ho Chung) 준회원

2005년 2월 포항공과대학교 전자전기공학과 졸업

2005년 2월~현재 포항공과대학교 정보통신대학원 석사과정

<관심분야> 신호설계, 정보보호, 부호이론, 디지털 통신

양 경 철 (Kyeongcheol Yang) 종신회원

1986년 2월 서울대학교 전자공학과 졸업

1988년 2월 서울대학교 전자공학과 석사

1992년 12월 University of Southern California 전기공학과 박사

1993년 3월~1999년 2월 한양대학교 전자통신공학과 조교수

1999년 2월~현재 포항공과대학교 전자전기공학과 교수

<관심분야> 디지털 통신, 부호이론, 다중 안테나 시스템, 신호설계, 정보보호