

Sidel'nikov 수열로부터 생성한 새로운 M -진 수열군

정회원 김 영 식*, 정 정 수*, 종신회원 노 종 선**, 정 하 봉**

A New M -ary Sequence Family Constructed From Sidel'nikov Sequences

Young-Sik Kim*, Jung-Soo Chung**, *Regular Members*,
Jong-Seon No**, Ha-Bong Chung*** *Lifelong Members*

요 약

이 논문에서는 $M|p^n - 1$ 를 만족하는 양의 정수 M 과 소수 p 에 대해서 주기가 $p^n - 1$ 인 M -진 Sidel'nikov 수열을 사용해서 M -진 수열 군을 생성하였다. 이 수열군은 상관 값의 최대값이 $3\sqrt{p^n} + 6$ 을 상한으로 갖고 수열군의 크기는 $p=2$ 일 때 $(M-1)^2(2^{n-1}-1)+M-1$ 이거나 p 가 홀수인 소수일 때는 $(M-1)^2(p^n-3)/2+M(M-1)/2$ 가 된다.

Key Words : Autocorrelation, Cross-correlation, Family of M -ary sequences, M -ary sequences, PN sequences, Sidel'nikov sequences

ABSTRACT

In this paper, for a positive integer M and a prime p such that $M|p^n - 1$, families of M -ary sequences using the M -ary Sidel'nikov sequences with period $p^n - 1$ are constructed. The family has its maximum magnitude of correlation values upper bounded by $3\sqrt{p^n} + 6$ and the family size is $(M-1)^2(2^{n-1}-1)+M-1$ for $p=2$ or $(M-1)^2(p^n-3)/2+M(M-1)/2$ for an odd prime p .

I. 서 론

오늘날 고속 데이터 통신을 위해서 M -진 변조 방식들이 표준에 적용되고 있다. 이에 따라서 좋은 상관 특성을 갖는 M -진 수열군을 생성하는 것 또한 중요한 문제가 되고 있다. 그 동안 낮은 상관 특성을 갖는 수열군에 대해서 많은 연구가 진행되어 왔다. 그러나 현재까지 알려진 수열군의 알파벳 크기는 소수 p 이거나 4로 한정되어 있었다. 최근에 Kim, Chung, No, 그리고 Chung은 Sidel'nikov 수

열을 사용해서 최대의 상관 값의 상한이 $2\sqrt{p^n} + 6$ 인 수열군을 생성하였다^[5].

이 논문에서는 $M|p^n - 1$ 를 만족하는 양의 정수 M 과 소수 p 에 대해서 주기가 $p^n - 1$ 인 M -진 Sidel'nikov 수열을 사용해서 M -진 수열 군을 생성하였다. 이것은 최근의 연구^[5]를 더 확장시킨 것으로 이 수열군은 상관 값의 최대 크기가 항상 $3\sqrt{p^n} + 6$ 보다 작거나 같으며 수열군의 크기는 $p=2$ 일 때는 $(M-1)^2(2^{n-1}-1)+M-1$ 이고, p 가 홀수인 소수일 때 $(M-1)^2(p^n-3)/2 + M(M-1)/2$ 가 된다.

* 본 연구는 교육인적자원부, 산업자원부, 노동부의 출연금으로 수행한 최우수실용실지원사업의 연구결과입니다.

* 삼성전자(kingsi@ccl.snu.ac.kr), ** 서울대학교 전기·컴퓨터공학부 및 뉴미디어통신공동연구소(integer@ccl.snu.ac.kr, jsno@snu.ac.kr)

*** 홍익대학교 전자전기공학부(habchung@hongik.ac.kr)

논문번호 : KICS2007-06-253, 접수일자 : 2007년 6월 9일, 최종논문접수일자 : 2007년 10월 2일

II. 사전 지식

α 가 p^n 개의 원소를 갖는 유한체 F_{p^n} 의 원시원이라고 하자. Sidel'nikov는 다음과 같이 좋은 자기상관특성을 갖는 M -진 수열을 도입하였다^[1].

정의 1. [2] p 가 소수이고 α 가 F_{p^n} 의 원시원이라고 하자. M 은 $Mp^n - 1$ 을 만족하는 양의 정수이다. $S_k, k=0,1,\dots,M-1$ 는 다음과 같은 F_{p^n} 의 중복되지 않은 부분집합이라 하자.

$$S_k = \left\{ \alpha^{Mi+k} - 1 \mid 0 \leq i < \frac{p^n - 1}{M} \right\} \quad (1)$$

그러면 주기가 $p^n - 1$ 인 M -진 Sidel'nikov 수열 $s(t)$ 는 다음과 같이 정의된다.

$$s(t) = \begin{cases} k, & \text{if } \alpha^t \in S_k, 0 \leq k \leq M-1 \\ k_0, & \text{if } \alpha^t = -1 \end{cases} \quad (2)$$

여기서 k_0 는 modulo M 을 취한 정수이다. \square

정의 2. [3] F_{p^n} 에서 차수가 M 인 곱의 character $\psi(\cdot)$ 는 다음과 같이 정의된다.

$$\psi(\alpha^t) = e^{j2\pi t/M}, \quad 0 \leq t \leq p^n - 2 \\ \psi(0) = 0$$

여기서 α 는 F_{p^n} 의 원시원이고 $Mp^n - 1$ 이다. \square

위의 정의로부터 다음이 성립함을 알 수 있다.

$$\sum_{x \in F_p} \psi(x) = 0. \quad (3)$$

지시 함수를 다음과 같이 정의하자.

$$I(x) = \begin{cases} 1, & \text{if } x = 0 \\ 0, & \text{if } x \neq 0. \end{cases}$$

M -진 Sidel'nikov 수열은 다음과 같이 지시 함수와 곱의 character 사용해서 나타낼 수 있다.

$$\omega^s(t) = \psi(\alpha^t + 1) + \omega^{k_0} I(\alpha^t + 1). \quad (4)$$

여기서 ω 는 1의 복소 M 차 근이다.

주기가 $p^n - 1$ 인 두 개의 M -진 수열 $u(t)$ 와 $v(t)$ 의 상호상관 함수는 다음과 같이 정의된다.

$$C(\tau) = \sum_{t=0}^{p^n-2} \omega^{u(t)-v(t+\tau)}. \quad (5)$$

(4)에서의 표현을 보면 Sidel'nikov 수열들 간의 상관 값을 계산할 때에는 주어진 유한체 상에서 곱의 character들의 곱의 합을 구할 필요가 있음을 알 수 있다. 다음의 정리가 곱의 character들의 곱의 합의 상한 값을 제공해 준다.

정리 3. [4] $f_1(z), \dots, f_l(z)$ 가 l 개의 두쌍 씩 서로 소인 $F_{p^n}[z]$ 에서의 monic 다항식이라고 하자. 이 다항식의 가장 큰 squarefree 약수의 차수는 d_1, \dots, d_l 을 갖는다. 이제 χ_1, \dots, χ_l 이 F_p 의 자명하지 않은 곱의 character라 하자. 그리고 $1 \leq i \leq l$ 에 대해서 다항식 $f_i(z)$ 는 $g(z)^{\text{ord}(\chi_i)}$ 의 형태가 아니라고 가정하자. 여기에서 $\text{ord}(\chi)$ 는 $\chi^d = 1$ 를 만족하는 가장 작은 양의 정수 d 이고 $g(z)$ 는 $F_{p^n}[z]$ 상에서의 다항식이다. 그러면 다음 식이 성립한다.

$$\left| \sum_{z \in F_p} \chi_1(f_1(z)) \cdots \chi_l(f_l(z)) \right| \\ \leq \left(\sum_{i=1}^l d_i - 1 \right) p^{\frac{n}{2}} \quad (6)$$

\square

III. M 진 수열군의 생성

$s(t)$ 가 (2)에서 정의된 주기가 $p^n - 1$ 인 M -진 Sidel'nikov 수열이라 하자. $T = \lceil (p^n - 1)/2 \rceil$ 라 하자. 여기서 $\lceil x \rceil$ 은 x 보다 크거나 같은 최소의 정수를 의미한다. L 이 다음과 같이 주어지는 주기가 $p^n - 1$ 인 M -진 수열의 집합이라 하자.

i) $p=2$ 인 경우,

$$L = \{v_{0,c_1}(t) \mid 1 \leq c_1 \leq M-1\} \\ \cup \{v_{i,c_1,c_2}(t) \mid 1 \leq c_1, c_2 \leq M-1, \\ 1 \leq i \leq T-1\} \quad (7)$$

ii) 홀수 p 인 경우,

$$L = \{v_{0,c_1}(t) \mid 1 \leq c_1 \leq M-1\} \\ \cup \{v_{i,c_1,c_2}(t) \mid 1 \leq c_1, c_2 \leq M-1, \\ 1 \leq i \leq T-1\} \\ \cup \{v_{T,c_1,c_2}(t) \mid 1 \leq c_1, c_2 \leq M-1\} \quad (8)$$

여기서 $v_{0,c_1}(t) = c_1 s(t)$ 이고 $i \neq 0$ 이면

$v_{i, c_1, c_2}(t) = c_1 s(t) + c_2 s(t+i)$ 이다. L 의 크기는 $p=2$ 일 때 $(M-1)^2 T - (M-1)(M-2)$ 이고 홀수 p 일 때 $(M-1)^2 T - (M-1)(M-2)/2$ 이다. 이 논문에서는 $p=2$ 인 경우에서도 동일하게 증명할 수 있기 때문에 홀수 p 인 경우에 대해서만 증명할 것이다.

먼저 i 의 구간이 $0 \leq i \leq (p^n - 3)/2$ 이고 $c_1 < c_2$ 에 대해서 $i = (p^n - 1)/2$ 이기 때문에 L 에서의 각각의 수열이 서로 순회적으로(cyclically) 다르다는 것을 쉽게 알 수 있다. 그렇지 않은 경우에는 $1 \leq i \leq T$ 일 때 $v_{i, c_1, c_2}(t) = v_{p^n - 1 - i, c_2, c_1}(t+i)$ 가 된다.

(4)를 사용해서, $1 \leq i \leq T$ 에 대해서 L 에서의 수열 $v_{i, c_1, c_2}(t)$ 는 다음과 같이 나타낼 수 있다.

$$\begin{aligned} \omega^{v_{i, c_1, c_2}(t)} &= \omega^{c_1 s(t) + c_2 s(t+i)} \\ &= [\psi^{c_1}(\alpha^t + 1) + \omega^{c_1 k_0} I(\alpha^t + 1)] \\ &\quad \times [\psi^{c_2}(\alpha^{t+i} + 1) + \omega^{c_2 k_0} I(\alpha^{t+i} + 1)] \quad (9) \\ &= \psi^{c_1}(\alpha^t + 1) \psi^{c_2}(\alpha^{t+i} + 1) \\ &\quad + \omega^{c_1 k_0} I(\alpha^t + 1) \psi^{c_2}(\alpha^{t+i} + 1) \\ &\quad + \omega^{c_2 k_0} I(\alpha^{t+i} + 1) \psi^{c_1}(\alpha^t + 1) \end{aligned}$$

여기서 (9)의 두 번째 항과 세 번째 항에는 지지 함수가 포함되어 있고 이로 인해 $t = T$ 와 $t = T - i$ 를 제외하고는 0이 된다.

정리 4. (7)과 (8)에 정의된 L 에 속한 임의의 두 개의 수열의 상관값의 크기는 다음과 같은 상한을 갖는다.

$$|\mathcal{C}(\tau)| \leq 3\sqrt{p^n} + 6.$$

증명: 여기서는 홀수 p 인 경우만 증명할 것이다. 먼저 두 개의 수열이 $v_{i, c_1, c_2}(t)$ 와 $v_{j, c'_1, c'_2}(t)$ 라 하자.

경우 1) $i \neq 0$ 이고 $j \neq 0$;

두 수열의 상관값은 다음과 같이 쓸 수 있다.

$$\begin{aligned} \mathcal{C}(\tau) &= \sum_{t=0}^{p^n-2} \omega^{v_{i, c_1, c_2}(t) - v_{j, c'_1, c'_2}(t+\tau)} \\ &= \sum_{t=0}^{p^n-2} \omega^{c_1 s(t) + c_2 s(t+i) - c'_1 s(t+\tau) - c'_2 s(t+j+\tau)} \end{aligned}$$

이 때 (9)에 의해 위의 상관함수는 다음과 같이 (10)처럼 총 9개의 덧셈 항으로 표현할 수가 있다.

$$\begin{aligned} \mathcal{C}(\tau) &= \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{c_2}(\alpha^{t+i} + 1) \psi^{-c'_1}(\alpha^{t+\tau} + 1) \psi^{-c'_2}(\alpha^{t+j+\tau} + 1) \\ &\quad + \omega^{-c'_1 k'_1} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{c_2}(\alpha^{t+i} + 1) \psi^{-c'_1}(\alpha^{t+j+\tau} + 1) I(\alpha^{t+\tau} + 1) \\ &\quad + \omega^{-c'_2 k'_2} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{c_2}(\alpha^{t+i} + 1) \psi^{-c'_1}(\alpha^{t+\tau} + 1) I(\alpha^{t+j+\tau} + 1) \\ &\quad + \omega^{c_1 k_1} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{-c'_1}(\alpha^{t+\tau} + 1) \psi^{-c'_2}(\alpha^{t+j+\tau} + 1) I(\alpha^t + 1) \\ &\quad + \omega^{(c_1 - c'_1) k_1} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{-c'_1}(\alpha^{t+j+\tau} + 1) I(\alpha^t + 1) I(\alpha^{t+\tau} + 1) \\ &\quad + \omega^{(c_1 - c'_2) k_1} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{-c'_1}(\alpha^{t+\tau} + 1) I(\alpha^t + 1) I(\alpha^{t+j+\tau} + 1) \\ &\quad + \omega^{c_2 k_2} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{-c'_1}(\alpha^{t+\tau} + 1) \psi^{-c'_2}(\alpha^{t+j+\tau} + 1) I(\alpha^{t+i} + 1) \\ &\quad + \omega^{(c_2 - c'_1) k_2} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{-c'_1}(\alpha^{t+j+\tau} + 1) I(\alpha^{t+i} + 1) I(\alpha^{t+\tau} + 1) \\ &\quad + \omega^{(c_2 - c'_2) k_2} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{-c'_1}(\alpha^{t+j+\tau} + 1) \psi^{c'_2}(\alpha^{t+i} + 1) I(\alpha^{t+\tau} + 1) \end{aligned} \quad (10)$$

먼저 네 개의 곱의 character만으로 구성된 첫 번째 항은 다음과 같이 나타낼 수 있다.

$$\begin{aligned} &\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{c_2}(\alpha^{t+i} + 1) \\ &\quad \times \psi^{-c'_1}(\alpha^{t+\tau} + 1) \psi^{-c'_2}(\alpha^{t+j+\tau} + 1) \\ &= \sum_{z \in F_p} \psi^{c_1}(z+1) \psi^{c_2}(\alpha^i z + 1) \\ &\quad \times \psi^{-c'_1}(\alpha^\tau z + 1) \psi^{-c'_2}(\alpha^{j+\tau} z + 1) - 1 \end{aligned}$$

그러면 정리 3으로부터 다음 식이 성립한다.

$$\begin{aligned} &|\sum_{z \in F_p} \psi^{c_1}(z+1) \psi^{c_2}(\alpha^i z + 1) \\ &\quad \times \psi^{-c'_1}(\alpha^\tau z + 1) \psi^{-c'_2}(\alpha^{j+\tau} z + 1) - 1| \quad (11) \\ &\leq 3\sqrt{p^n} + 1 \end{aligned}$$

(10)에서의 두 번째 항은 다음과 같이 주어진다.

$$\begin{aligned} &\omega^{-c'_1 k'_1} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t + 1) \psi^{c_2}(\alpha^{t+i} + 1) \\ &\quad \times \psi^{-c'_2}(\alpha^{t+j+\tau} + 1) I(\alpha^{t+\tau} + 1) \\ &= \omega^{-c'_1 k'_1} \psi^{c_2}(\alpha^{t+i} + 1) \psi^{c_1}(\alpha^t + 1) \psi^{-c'_2}(\alpha^{t+j+\tau} + 1) \\ &\quad \times \psi^{-c'_1}(\alpha^{t+\tau} + 1) \quad (12) \\ &= \begin{cases} 0, & \text{if } \tau=0 \text{ or } \tau=i \\ \omega^{-c'_1 k'_1} \psi^{c_2} \left(\frac{(1-\alpha^\tau)^{c_1} (1-\alpha^{i-\tau})^{c_2}}{(1-\alpha^j)^{c'_2}} \right), & \text{otherwise} \end{cases} \end{aligned}$$

세 번째 항은 다음과 같이 주어진다.

$$\begin{aligned} & \omega^{-c_2 k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1) \psi^{c_2}(\alpha^{t+i}+1) \\ & \times \psi^{-c_1'}(\alpha^{t+\tau}+1) I(\alpha^{t+j+\tau}+1) \\ & = \begin{cases} 0, & \text{if } \tau=-j \text{ or } \tau=i-j \\ \omega^{-c_2 k_0} \psi\left(\frac{(1-\alpha^{-j-\tau})^{c_1} (1-\alpha^{j-\tau})^{c_2}}{(1-\alpha^{-j})^{c_1}}\right), & \text{otherwise} \end{cases} \end{aligned} \quad (13)$$

네 번째 항은 다음과 같다.

$$\begin{aligned} & \omega^{c_1 k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^t+1) \psi^{-c_1'}(\alpha^{t+\tau}+1) \\ & \times \psi^{-c_2'}(\alpha^{t+j+\tau}+1) I(\alpha^t+1) \\ & = \begin{cases} 0, & \text{if } \tau=0 \text{ or } \tau=-j \\ \omega^{c_1 k_0} \psi\left(\frac{(1-\alpha^t)^{c_2}}{(1-\alpha^\tau)^{c_1} (1-\alpha^{j+\tau})^{c_2}}\right), & \text{otherwise} \end{cases} \end{aligned} \quad (14)$$

다섯 번째 항은 다음과 같다.

$$\begin{aligned} & \omega^{(c_1-c_1')k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^t+1) \psi^{-c_2'}(\alpha^{t+j+\tau}+1) \\ & \times I(\alpha^t+1) I(\alpha^{t+\tau}+1) \\ & = \begin{cases} \omega^{(c_1-c_1')k_0} \psi\left(\frac{(1-\alpha^t)^{c_2}}{(1-\alpha^t)^{c_2}}\right), & \text{if } \tau=0 \\ 0, & \text{otherwise} \end{cases} \end{aligned} \quad (15)$$

여섯 번째 항은 다음과 같다.

$$\begin{aligned} & \omega^{(c_1-c_2')k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^t+1) \psi^{-c_1'}(\alpha^{t+\tau}+1) \\ & \times I(\alpha^t+1) I(\alpha^{t+j+\tau}+1) \\ & = \begin{cases} \omega^{(c_1-c_2')k_0} \psi\left(\frac{(1-\alpha^t)^{c_2}}{(1-\alpha^j)^{c_1}}\right), & \text{if } \tau=-j \\ 0, & \text{otherwise} \end{cases} \end{aligned} \quad (16)$$

일곱 번째 항은 다음과 같다.

$$\begin{aligned} & \omega^{c_2 k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1) \psi^{-c_1'}(\alpha^{t+\tau}+1) \\ & \times \psi^{-c_2'}(\alpha^{t+j+\tau}+1) I(\alpha^{t+i}+1) \\ & = \begin{cases} 0, & \text{if } \tau=i \text{ or } \tau=i-j \\ \omega^{c_2 k_0} \psi\left(\frac{(1-\alpha^{-i})^{c_1}}{(1-\alpha^{-i+\tau})^{c_1} (1-\alpha^{-i+j+\tau})^{c_2}}\right), & \text{otherwise} \end{cases} \end{aligned} \quad (17)$$

여덟 번째 항은 다음과 같다.

$$\begin{aligned} & \omega^{(c_2-c_1')k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1) \psi^{-c_2'}(\alpha^{t+j+\tau}+1) \\ & \times I(\alpha^{t+i}+1) I(\alpha^{t+\tau}+1) \\ & = \begin{cases} \omega^{(c_2-c_1')k_0} \psi\left(\frac{(1-\alpha^{-i})^{c_1}}{(1-\alpha^t)^{c_2}}\right), & \text{if } \tau=i \\ 0, & \text{otherwise} \end{cases} \end{aligned} \quad (18)$$

아홉 번째 항은 다음과 같다.

$$\begin{aligned} & \omega^{(c_2-c_2')k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1) \psi^{-c_1'}(\alpha^{t+\tau}+1) \\ & \times I(\alpha^{t+i}+1) I(\alpha^{t+j+\tau}+1) \\ & = \begin{cases} \omega^{(c_2-c_2')k_0} \psi\left(\frac{(1-\alpha^{-i})^{c_1}}{(1-\alpha^{-j})^{c_1}}\right), & \text{if } \tau=i-j \\ 0, & \text{otherwise} \end{cases} \end{aligned} \quad (19)$$

그래서 (11)-(19)로부터 다음과 같은 부등식을 얻게 된다.

$$|C(\tau)| \leq \begin{cases} 3\sqrt{p^n}+5, & \text{if } \tau=0, i, i-j, -j \\ 3\sqrt{p^n}+6, & \text{otherwise} \end{cases}$$

다음으로 $v_{i, c_1, c_2}(t)$ 와 $v_{0, c_1}(t)$ 두 개의 상관값을 구 하자.

경우 2) $i \neq 0$ 이고 $j=0$ (또는 $i=0$ 이고 $j \neq 0$)

이 경우에 상관함수는 다음과 같이 (20)처럼 쓸 수 있다.

$$\begin{aligned} C(\tau) &= \sum_{t=0}^{p^n-2} \omega^{c_2 s(t)+c_2 s(t+i)-c_1 s(t+\tau)} \\ &= \sum_{t=0}^{p^n-2} \psi^{-c_1'}(\alpha^{t+\tau}+1) \psi^{c_2}(\alpha^t+1) \psi^{c_2}(\alpha^{t+i}+1) \\ &+ \omega^{c_1 k_0} \sum_{t=0}^{p^n-2} \psi^{-c_1'}(\alpha^{t+\tau}+1) \psi^{c_2}(\alpha^{t+i}+1) I(\alpha^t+1) \\ &+ \omega^{c_2 k_0} \sum_{t=0}^{p^n-2} \psi^{-c_1'}(\alpha^{t+\tau}+1) \psi^{c_2}(\alpha^{t+i}+1) I(\alpha^{t+i}+1) \\ &+ \omega^{-c_1' k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1) \psi^{c_2}(\alpha^{t+i}+1) I(\alpha^{t+\tau}+1) \\ &+ \omega^{(c_1-c_1')k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^{t+i}+1) I(\alpha^t+1) I(\alpha^{t+\tau}+1) \\ &+ \omega^{(c_2-c_2')k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1) I(\alpha^{t+i}+1) I(\alpha^{t+\tau}+1) \end{aligned} \quad (20)$$

(20)에서의 첫 번째 항은 다음과 같다.

$$\begin{aligned} & \sum_{t=0}^{p^n-2} \psi^{-c_1'}(\alpha^{t+\tau}+1) \psi^{c_2}(\alpha^t+1) \psi^{c_2}(\alpha^{t+i}+1) \\ &= \sum_{z \in F_p} \psi^{-c_1'}(\alpha^z+1) \psi^{c_2}(z+1) \psi^{c_2}(\alpha^z+1) - 1 \end{aligned}$$

정리 3으로부터 위의 합은 $2\sqrt{p^n}+1$ 을 상한으로 갖는다. 다른 항들의 경우는 지시 함수를 포함하고 있기 때문에 τ 에 따라서 0을 갖거나 단일한 곱의 character로 표현할 수 있다. 따라서 경우 1)에서와 마찬가지로 다음과 같은 부등식을 얻을 수 있다.

$$|C(\tau)| \leq 2\sqrt{p^n} + 4$$

끝으로 $v_{0,c_1}(t)$ 와 $v_{0,c_2}(t)$ 사이의 상관값의 크기가 $\sqrt{p^n} + 3$ 을 상한으로 갖는다는 것을 동일한 방식으로 증명할 수가 있다. □

다음의 예에서는 4진 수열군을 생성한다.

예제 1. $M=4$, $p=7$, 그리고 $n=4$ 인 경우에 주기가 $N=2400$ 인 4진 수열군을 생성할 수가 있다. $s(t)$ 가 4진 Sidel'nikov 수열이라 하자. 그러면 수열군 L 에는 총 10,797개의 수열이 다음과 같이 포함되어 있다.

$$L = \{s(t), 2s(t), 3s(t)\} \\ \cup \{s(t) + 2s(t+1200), s(t) + 3s(t+1200), \\ 2s(t) + 3s(t+1200)\} \\ \cup \{c_1s(t) + c_2(t+i) \mid 1 \leq c_1, c_2 \leq 3, 1 \leq i \leq 1199\}$$

L 에서의 수열들의 상호 상관값들의 크기는 $3 \times 49 + 6 = 153$ 을 상한으로 갖는다. □

IV. 결론

이 논문에서는 $M|p^n - 1$ 를 만족하는 양의 정수 M 과 소수 p 에 대해서 주기가 $p^n - 1$ 인 M -진 Sidel'nikov 수열을 사용해서 M -진 수열 군을 생성하였다. 이 수열군은 상관값의 최대값이 $3\sqrt{p^n} + 6$ 을 상한으로 갖고 수열군의 크기는 $p=2$ 일 때 $(M-1)^2(2^n - 1) + M - 1$ 이거나 p 가 홀수인 소수일 때는 $(M-1)^2(p^n - 3)/2 + M(M-1)/2$ 가 된다.

참고 문헌

[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, 1969.

[2] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "On the autocorrelation distributions of Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3303 - 3307, Sep. 2005.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its*

Applications. Reading, MA: Addison-Wesley, 1983.

[4] D. Wan, "Generators and irreducible polynomials over finite fields," *Mathematics of Computations*, vol. 66, no. 219, pp. 1195-1212, July 1997.

[5] 김영식, 정정수, 노종선, 정하봉, "New constructions of the family of M -ary sequences with low correlation," 한국통신학회 추계종합학술대회 논문집, vol. 34, 2006년 11월, p.56.

[6] P. V. Kumar, T. Helleseth, A. R. Calderbank, and A. R. Hammons, Jr., "Large families of quaternary sequences with low correlation," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 579-592, Mar. 1996.

[7] P. V. Kumar, T. Helleseth, and A. R. Calderbank, "An upper bound for Weil exponential sums over Galois rings and applications," *IEEE Trans. Inf. Theory*, vol. 41, no. 2, pp. 456-468, Mar. 1995.

[8] S.-C. Liu and J. F. Komo, "Nonbinary Kasami sequences over $GF(p)$," *IEEE Trans. Inf. Theory*, vol. 38, pp. 1409-1412, July 1992.

[9] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions," *IEEE Trans. Inf. Theory*, vol. 14, pp. 154-156, Jan. 1968.

[10] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences," Ph.D. dissertation, Univ. of Southern California, Los Angeles, CA, 1970.

김영식 (Young-Sik Kim)

정희원



2001년 2월 서울대학교 전기공학부 공학사

2003년 2월 서울대학교 전기컴퓨터공학부 석사

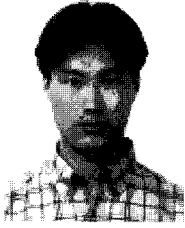
2007년 2월 서울대학교 전기컴퓨터공학부 박사

2007년 3월~현재 삼성전자

<관심분야> 시퀀스, 오류정정부호, 디지털통신

정 정 수 (Jung-Soo Chung)

정회원



2003년 2월 서울대학교 전기공학
부 공학사

2003년 3월~현재 서울대학교 대
학원 전기·컴퓨터공학부 석
·박사 통합과정

<관심분야> 시퀀스, 오류정정부호, 디지털통신

정 하 봉 (Ha-Bong Chung)

종신회원



1981년 2월 서울대학교 전자공학
과 졸업 공학학사

1985년 미국 University of
Southern California, 전기공학
과 공학석사

1988년 미국 University of
Southern California, 전기공학

과 공학박사

1988년~1991년 미국 뉴욕주립대 전기공학과 조교수

1991년~현재 홍익대학교 전자전기공학부 교수

<관심분야> 부호 이론, 조합수학, 시퀀스 설계

노 종 선 (Jong-Seon No)

종신회원



1981년 2월 서울대학교 전자공
학과 공학사

1984년 2월 서울대학교 대학원
전자공학과 석사

1988년 5월 University of
Southern California, 전기공학
과 공학박사

1988년 2월~1990년 7월 Hughes Network Systems,
Senior MTS

1990년 9월~1999년 7월 건국대학교 전자공학과 부교수

1999년 8월~현재 서울대학교 전기컴퓨터공학부 교수

<관심분야> 시퀀스, 시공간부호, LDPC 부호, OFDM,
이동통신, 암호학