Sidel'nikov 수열로부터 생성된 새로운 M-진 수열군

*정정수, *최성태O, *노종선, **정하봉
*서울대학교 전기컴퓨터공학부, 뉴미디어통신공동연구소
**홍익대학교 전자전기공학부

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

*Jung-Soo Chung, *Sung-Tai ChoiO, *Jong-Seon No, and **Habong Chung
*Department of EECS, INMC, Seoul National University
**School of Electronics and Electrical Engineering, Hongik University,
{integer, stchoi}@ccl.snu.ac.kr, jsno@snu.ac.kr, habchung@hongik.ac.kr

요약

이 논문에서는, 주기가 p^n-1인 M-진 수열군을 제시한다. 이 수열군의 크기는 크고 좋은 상관 특성을 가진다. 이 수열군의 상한은 $4\sqrt{p^n}+5$이다.

1. 서론

양의 정수 n과 M, 소수 p에 대해서 Sidel'nikov는 주기가 p^n-1인 M-진 수열(*Sidel'nikov* 수열이라 부름)을 제시하였다 [1]. 여기서 M은 p^n-1의 약수이다. 이 수열의 자기 상관값은 상한 값이 4이다.

Krone와 Sarwate는 유한체 F_q상에서 주기가 $q-1$인 4-진 Sidel'nikov 수열로부터 수열군을 제안하였다 [2]. 이 수열군의 최대상관값은 $3\sqrt{q}+5$로 상한되고 수열군의 크기는 $2(q+1)$이다. Kim과 Chung, No, Chung은 주기가 p^n-1인 M-진 Sidel'nikov 수열로부터 M-진 수열군을 제안하였다 [3]. 이 수열군의 최대상관값은 $3\sqrt{p^n}+5$로 상한되고 홀수인 소수 p에 대해서 수열군의 크기는 $(M-1)^2(\frac{p^n-3}{2})+\frac{M(M-1)}{2}$이다. 특히 $M=4$인 경우, [3]에서 제시한 수열군의 크기는 [2]에서 제시한 수열군 크기의 2배보다 더 크다. 이 때 두 수열군의 상한값은 같다.

이 논문에서는, 주기가 p^n-1인 M-진 수열군을 제시한다. 수열군의 상한은 $4\sqrt{p^n}+5$이고 수열군의 크기는 [3]에서 제시된 크기보다 대략 2배 크다.

2. 사전지식

주기가 N인 M-진 수열 $s_i(t)$과 $s_j(t)$에 대해서, 상관함수 $R_{s_i,s_j}(\tau)$는 다음과 같이 정의된다.

$$R_{s_i,s_j}(\tau)=\sum_{t=0}^{N-1}\omega_M^{s(t)-s(t+\tau)}, \quad 0\le\tau\le N-1 \quad (1)$$

여기서 $\omega_M=e^{j2\pi/M}$이다.

정의 1 ([4]): p를 소수라 하고 α는 유한체 F_{p^n}의 원시원이라 하자. M은 p^n-1의 약수이며 2보다 큰 양수라 하자. F_{p^n}의 공통 원소를 가지지 않는 부분 집합(disjoint subsets)을 S_k, $k=0,1,\cdots,M-1$, 라 하고 다음과 같이 정의한다.

$$S_k=\left\{\alpha^{Mi+k}-1 \mid 0\le i<\frac{p^n-1}{M}\right\}. \quad (2)$$

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

$$s(t)=\begin{cases}k, & \text{if } \alpha^t\in S_k,\ 0\le k\le M-1\\ k_0, & \text{if } \alpha^t=-1\end{cases} \quad (3)$$

여기서 $0\le k_0\le M-1$이다. □

식 (3)에서 M-진 Sidel'nikov 수열 $s(t)$는 유한체 F_{p^n}상에서 위수(order)가 M인 multiplicative character $\psi_M(\cdot)$와 지시 함수 $I(\cdot)$로 표현할 수 있다.

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

여기서 지시 함수는 다음과 같다.

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

Multiplicative character $\psi_M(\cdot)$은 $\psi_M(\alpha^t)=e^{j2\pi t/M}$이고 $\psi_M(0)=0$이다.

Sidel'nikov 수열들 간의 상호 상관값을 계산하기 위해서는 multiplicative character의 곱의 합을 계산해야 한다. 다음 정리는 multiplicative character의 곱들의 합에 대한 상한을 말해준다.

정리 2 ([5]): $F_{p^n}[z]$ 상에서 각 차수에서 거듭제곱 약수를 가지지 않는 최고 차수가 $h_1, h_2, \cdots, h_l$인 다항식을 $f_1(z), f_2(z), \cdots, f_l(z)$라 하자. $\chi_1, \chi_2, \cdots, \chi_l$는 trivial하지 않은 F_{p^n}의 multiplicative characters라 하자. $1 \le i \le l$인 i에 대해서 다항식 $f_i(z)$는 $F_{p^n}[z]$상에서 $g(z)^{ord(\chi_i)}$의 형태가 될 수 없다고 가정하자. 여기서 $ord(\chi)$는 $\chi^h = 1$를 만족하는 가장 작은 양수 h이다. 그리고 $g(z)$는 $F_{p^n}[z]$ 상의 다항식이다. 그러면,

$$\Big| \sum_{z \in F_{p^n}} \chi_1(f_1(z))\chi_2(f_2(z)) \cdots \chi_l(f_l(z)) \Big| \le (\sum_{i=1}^{l} h_i - 1)p^{n/2}. \tag{5}$$

□

3. M-진 수열군의 생성

Kim과 Chung, No, Chung는 M-진 수열의 수열군을 제안하였고 수열군의 크기와 상관값의 상한을 제시하였다 [3].

정리 3 ([3]): $s(t)$는 (3)와 (4)에서 정의된 주기가 $p^n - 1$인 M-진 Sidel'nikov 수열이다. $T = \lceil \frac{p^n-1}{2} \rceil$이라 하자. 여기서 $\lceil a \rceil$는 a보다 작거나 같은 최대 정수이다. 수열군 $\mathcal{L}$를 다음과 같이 정의하자.

1) $p = 2$일 때;

$$\begin{aligned}\mathcal{L} =& \{u_{0,c_1}(t) \mid 1 \le c_1 \le M-1\} \\ & \cup \{u_{i,c_1,c_2}(t) \;\Big|\; 1 \le c_1, c_2 \le M-1, 1 \le i \le T-1\}.\end{aligned} \tag{6}$$

2) 홀수인 소수 p일 때;

$$\begin{aligned}\mathcal{L} =& \{u_{0,c_1}(t) \mid 1 \le c_1 \le M-1\} \\ & \cup \{u_{i,c_1,c_2}(t) \;\Big|\; 1 \le c_1, c_2 \le M-1, 1 \le i \le T-1\} \\ & \cup \{u_{T,c_1,c_2}(t) \;\Big|\; 1 \le c_1 < c_2 \le M-1\}.\end{aligned} \tag{7}$$

여기서 $u_{0,c_1}(t) = c_1 s(t)$이고 $u_{i,c_1,c_2}(t) = c_1 s(t) + c_2 s(t+i)$이다. 수열군 크기는 $p = 2$일 때 $(M-1)^2(T-1) + (M-1)$이고 홀수인 소수 p일 때 $(M-1)^2(T-1) + (M-1)(M-2)/2 + (M-1)$ 이다. 수열군 $\mathcal{L}$에서 임의의 두 수열 사이의 상관값의 상한은 다음과 같다.

$$|R(\tau)| \le 3\sqrt{p^n} + 5.$$

□

정리 3의 생성방법을 수정하여 $s(t)$의 역수열인 $s(-t)$를 이용하여 다음 정리에서 수열군 $\mathcal{K}$를 생성해 보자.

정리 4: $s(t)$는 주기가 $N = p^n - 1$인 M-진 Sidel'nikov 수열이라 하고 $T = \lceil \frac{p^n-1}{2} \rceil$이라 하자. 수열군 $\mathcal{K}$는 다음과 같이 정의된다.

1) $p = 2$일 때;

$$\begin{aligned}\mathcal{K} =& \{v_{0,a_1}(t) \mid 1 \le a_1 \le M-1\} \\ & \cup \{v_{1,a_1}(t) \mid 1 \le a_1 \le M-1\} \\ & \cup \{v_{i,a_1,a_2}(t) \;\Big|\; 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\}.\end{aligned} \tag{8}$$

2) 홀수인 소수 p일 때;

$$\begin{aligned}\mathcal{K} =& \{v_{0,a_1}(t) \mid 1 \le a_1 \le M-1\} \\ & \cup \{v_{1,a_1}(t) \mid 1 \le a_1 \le M-1\} \\ & \cup \{v_{i,a_1,a_2}(t) \;\Big|\; 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\} \\ & \cup \{v_{T,a_1,a_2}(t) \;\Big|\; 1 \le a_1, a_2 \le M-1, a_1 \ne a_2\}.\end{aligned} \tag{9}$$

여기서

$$\begin{aligned}v_{0,a_1}(t) =& a_1 s(t), \\ v_{1,a_1}(t) =& a_1 s(-t) \\ v_{i,a_1,a_2}(t) =& a_1 s(t) + a_2 s(-t+i).\end{aligned}$$

수열군 $\mathcal{K}$에서 임의의 두 수열 사이의 상관값의 상한은 다음과 같다.

$$|R(\tau)| \le 4\sqrt{p^n} + 5$$

수열군의 크기는 $p = 2$인 경우 $(M-1)^2(T-1) + 2(M-1)$이고 홀수인 소수인 경우 $(M-1)^2(T-1) + M(M-1)$이다.

Proof: $v_{i,a_1,a_2}(t)$와 $v_{N-i,a_1,a_2}(t)$의 상호 상관값이 주기 N에 근접하는 경우가 있기 때문에 i는 T보다 작아야 한다. 여기서는 홀수인 소수 p에 대해서만 증명을 한다. $p = 2$인 경우도 홀수인 경우와 유사하다.

경우 1) $v_{i,a_1,a_2}(t)$와 $v_{j,a_3,a_4}(t)$의 상관값;

두 $v_{i,a_1,a_2}(t)$와 $v_{j,a_3,a_4}(t)$의 상호 상관값을 정리하면 다음과 같다.

$$\begin{aligned}& R_{v_{i,a_1,a_2}, v_{j,a_3,a_4}}(\tau) \\ =& \sum_{t=0}^{N-1} \omega^{v_{i,a_1,a_2}(t+\tau) - v_{j,a_3,a_4}(t)} \\ =& \sum_{t=0}^{N-1} [\psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1) \\ & \quad + \psi_M^{a_1}(\alpha^{t+\tau}+1)\omega^{a_2 k_0} I(\alpha^{-t-\tau+i}+1) \\ & \quad + \omega^{a_1 k_0} I(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)] \\ & \times [\psi_M^{-a_3}(\alpha^{t}+1)\psi_M^{-a_4}(\alpha^{-t+j}+1) \\ & \quad + \psi_M^{-a_3}(\alpha^{t}+1)\omega^{-a_4 k_0} I(\alpha^{-t+j}+1) \\ & \quad + \omega^{-a_3 k_0} I(\alpha^{t}+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)] \\ =& \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1) \\ & \quad \times \psi_M^{-a_3}(\alpha^{t}+1)\psi_M^{-a_4}(\alpha^{-t+j}+1) \\ & + \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1) \\ & \quad \times \psi_M^{-a_3}(\alpha^{t}+1)\omega^{-a_4 k_0} I(\alpha^{-t+j}+1) \\ & + \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\end{aligned}$$

$$\times \omega^{-a_3k_0} I(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)$$
$$+\sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\omega^{a_2k_0} I(\alpha^{-t-\tau+i}+1)$$
$$\times \psi_M^{-a_3}(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)$$
$$+\sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\omega^{a_2k_0} I(\alpha^{-t-\tau+i}+1)$$
$$\times \psi_M^{-a_3}(\alpha^t+1)\omega^{-a_4k_0} I(\alpha^{-t+j}+1)$$
$$+\sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\omega^{a_2k_0} I(\alpha^{-t-\tau+i}+1)$$
$$\times \omega^{-a_3k_0} I(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)$$
$$+\sum_{t=0}^{N-1} \omega^{a_1k_0} I(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)$$
$$\times \psi_M^{-a_3}(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)$$
$$+\sum_{t=0}^{N-1} \omega^{a_1k_0} I(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)$$
$$\times \psi_M^{-a_3}(\alpha^t+1)\omega^{-a_4k_0} I(\alpha^{-t+j}+1)$$
$$+\sum_{t=0}^{N-1} \omega^{a_1k_0} I(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)$$
$$\times \omega^{-a_3k_0} I(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1).$$

$R_{v_{i,a_1,a_2},v_{j,a_3,a_4}}(\tau)$는 9개의 합으로 표현되고 이를 $A_1, A_2, \cdots, A_9$로 다음과 같이 정리할 수 있다.

첫 번째는

$$\begin{aligned}A_1 &= \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\\ &\quad\times \psi_M^{-a_3}(\alpha^t+1)\psi_M^{-a_4}(\alpha^{-t+j}+1)\\ &= \sum_{z\in F_{p^n}} \psi_M^{a_1}(\alpha^\tau z+1)\psi_M^{a_2}(\alpha^{i-\tau}z^{-1}+1)\\ &\quad\times \psi_M^{-a_3}(z+1)\psi_M^{-a_4}(\alpha^j z^{-1}+1)-1\\ &= \sum_{z\in F_{p^n}} \psi_M^{a_1}(\alpha^\tau z+1)\psi_M^{a_2}(\alpha^{i-\tau}+z)\\ &\quad\times \psi_M^{-a_3}(z+1)\psi_M^{-a_4}(\alpha^j+z)\psi_M^{-a_2+a_4}(z)-1.\end{aligned}$$

정리 2로부터 z에 대한 최고 차수는 $h_1=h_2=h_3=h_4=h_5=1$이다. 따라서 간단하게 다음을 구할 수 있다. $|A_1|\le 4\sqrt{p^n}+1$.

두 번째 합은 지시 함수 성질을 이용하여 $t=N/2+j$인 경우에만 $I(\alpha^{-t+j}+1)=1$이 되는 것을 활용한다.

$$\begin{aligned}A_2 &= \sum_{t=0}^{N-1} \psi_M^{a_1}(\alpha^{t+\tau}+1)\psi_M^{a_2}(\alpha^{-t-\tau+i}+1)\\ &\quad\times \psi_M^{-a_3}(\alpha^t+1)\omega^{-a_4k_0} I(\alpha^{-t+j}+1)\\ &= \begin{cases}0, & \text{if } \tau=i-j \\ & \text{or } \tau=-j\\ \omega^{-a_4k_0}\psi_M^{a_1}(-\alpha^{j+\tau}+1) & \\ \times\psi_M^{a_2}(-\alpha^{-j-\tau+i}+1)\psi_M^{-a_3}(-\alpha^j+1), & \text{otherwise.}\end{cases}\end{aligned}$$

마찬가지로 $t=N/2$일 때 $I(\alpha^t+1)=1$이므로 세 번째 합은

$$A_3 = \begin{cases}0, & \text{if } \tau=0\\ & \text{or } \tau=i\\ \omega^{-a_3k_0}\psi_M^{a_1}(-\alpha^\tau+1)\psi_M^{a_2}(-\alpha^{-\tau+i}+1) & \\ \quad\times\psi_M^{-a_4}(-\alpha^j+1), & \text{otherwise.}\end{cases}$$

A_4부터 A_9도 지시 함수 성질을 이용하여 다음과 같이 정리할 수 있다.

$$A_4 = \begin{cases}0, & \text{if } \tau=i-j\\ & \text{or } \tau=i\\ \omega^{a_2k_0}\psi_M^{a_1}(-\alpha^i+1)\psi_M^{-a_3}(-\alpha^{-\tau+i}+1) & \\ \quad\times\psi_M^{-a_4}(-\alpha^{\tau-i+j}+1), & \text{otherwise.}\end{cases}$$

$$A_5 = \begin{cases}\omega^{(a_2-a_4)k_0}\psi_M^{a_1}(-\alpha^i+1)\psi_M^{-a_3}(-\alpha^j+1), & \text{if } \tau=i-j\\ 0, & \text{otherwise.}\end{cases}$$

$$A_6 = \begin{cases}\omega^{(a_2-a_3)k_0}\psi_M^{a_1}(-\alpha^i+1)\psi_M^{-a_4}(-\alpha^j+1), & \text{if } \tau=i\\ 0, & \text{otherwise.}\end{cases}$$

$$A_7 = \begin{cases}0, & \text{if } \tau=0\\ & \text{or } \tau=-j\\ \omega^{a_1k_0}\psi_M^{a_2}(-\alpha^i+1)\psi_M^{-a_3}(-\alpha^{-\tau}+1) & \\ \quad\times\psi_M^{-a_4}(-\alpha^{\tau+j}+1), & \text{otherwise.}\end{cases}$$

$$A_8 = \begin{cases}\omega^{(a_1-a_4)k_0}\psi_M^{a_2}(-\alpha^i+1)\psi_M^{-a_3}(-\alpha^j+1), & \text{if } \tau=-j\\ 0, & \text{otherwise.}\end{cases}$$

$$A_9 = \begin{cases}\omega^{(a_1-a_3)k_0}\psi_M^{a_2}(-\alpha^i+1)\psi_M^{-a_4}(-\alpha^j+1), & \text{if } \tau=0\\ 0, & \text{otherwise.}\end{cases}$$

위의 9개의 합을 정리하면

$$\begin{aligned}&|R(\tau)|\\ &= \begin{cases}|A_1+A_2+A_4+A_9|\le 4\sqrt{p^n}+4, & \text{if } \tau=0\\ |A_1+A_3+A_4+A_8|\le 4\sqrt{p^n}+4, & \text{if } \tau=-j\\ |A_1+A_2+A_6+A_7|\le 4\sqrt{p^n}+4, & \text{if } \tau=i\\ |A_1+A_3+A_5+A_7|\le 4\sqrt{p^n}+4, & \text{if } \tau=i-j\\ |A_1+A_2+A_3+A_4+A_7|\le 4\sqrt{p^n}+5, & \text{otherwise.}\end{cases}\end{aligned}$$

따라서, $v_{i,a_1,a_2}(t)$와 $v_{j,a_3,a_4}(t)$의 상호 상관값의 상한이 $4\sqrt{p^n}+5$임을 알 수 있다.

경우 2) $v_{1,a_1}(t)$와 $v_{j,a_3,a_4}(t)$의 상관값;

경우 3) $v_{T,a_1,a_2}(t)$와 $v_{j,a_3,a_4}(t)$의 상관값;

경우 4) $v_{0,a_1}(t)$와 $v_{1,a_2}(t)$의 상관값;

경우 1)의 증명과 비슷한 방법으로 각 합들의 최대값을 정리하면 각각의 상한은 $4\sqrt{p^n}+5$보다 크지 않다. 그러므로 모든 경우에 대해서 $4\sqrt{p^n}+5$가 상한이다.

수열군의 크기는 i와 a_1, a_2 따라 $p=2$인 경우 $(M-1)^2(T-1)+2(M-1)$ 이고 홀수인 소수인 경우 $(M-1)^2(T-1)+M(M-1)$이다. □

수열군의 상관값 상한이 주기보다 작아야 제안한 생성 방법과 같은 특정 수열군을 생성한 의미가 있는 것이므로 정리 4는 $p^n \geq 4\sqrt{p^n}+5$을 만족해야 한다.

4. 두 수열군의 결합

수열군 $\mathcal{K}$는 $\mathcal{L}$에 비해서 상관값의 상한이 $3\sqrt{p^n}+5$에서 $4\sqrt{p^n}+5$로 악화되었다. 이 두 수열군을 결합하면 크기가 더 커진 수열군을 다음과 같이 만들 수 있다. 주기가 $N=p^n-1$인 M-진 수열군 $\mathcal{M}$은 다음과 같이 주어진다.

1) $p=2$일 때;

$$\begin{aligned}\mathcal{M} = &\{v_{0,a_1}(t) \mid 1 \leq a_1 \leq M-1\} \\ &\cup \{v_{1,a_1}(t) \mid 1 \leq a_1 \leq M-1\} \\ &\cup \{v_{i,a_1,a_2}(t) \mid 1 \leq a_1, a_2 \leq M-1, 1 \leq i \leq T-1\} \\ &\cup \{u_{i,a_1,a_2}(t) \mid 1 \leq a_1, a_2 \leq M-1, 1 \leq i \leq T-1\}.\end{aligned} \tag{10}$$

2) 홀수인 소수 p일 때;

$$\begin{aligned}\mathcal{M} = &\{v_{0,a_1}(t) \mid 1 \leq a_1 \leq M-1\} \\ &\cup \{v_{1,a_1}(t) \mid 1 \leq a_1 \leq M-1\} \\ &\cup \{v_{i,a_1,a_2}(t) \mid 1 \leq a_1, a_2 \leq M-1, 1 \leq i \leq T-1\} \\ &\cup \{v_{T,a_1,a_2}(t) \mid 1 \leq a_1, a_2 \leq M-1, a_1 \neq a_2\} \\ &\cup \{u_{i,a_1,a_2}(t) \mid 1 \leq a_1, a_2 \leq M-1, 1 \leq i \leq T-1\} \\ &\cup \{u_{T,a_1,a_2}(t) \mid 1 \leq a_1 < a_2 \leq M-1\}.\end{aligned} \tag{11}$$

여기서

$$\begin{aligned}v_{0,a_1}(t) &= a_1 s(t) \\ v_{1,a_1}(t) &= a_1 s(-t) \\ v_{i,a_1,a_2}(t) &= a_1 s(t) + a_2 s(-t+i) \\ u_{i,a_1,a_2}(t) &= a_1 s(t) + a_2 s(t+i).\end{aligned}$$

다음 정리에서 수열군의 상한을 구해 보자.

정리 5: 식 (10)과 (11)에서 정의된 수열군 $\mathcal{M}$의 상관값의 상한은 다음과 같다.

$$|R(\tau)| \leq 4\sqrt{p^n}+5.$$

수열군의 크기는 $p=2$인 경우 $2(M-1)^2(T-1)+2(M-1)$이고 홀수인 소수인 경우 $2(M-1)^2(T-1)+2(M-1)+3(M-1)(M-2)/2$이다.

Proof: 홀수인 소수 p에 대해서만 증명을 할 것이다. $i \neq 0$와 $j \neq 0$에 대해서 $u_{i,a_1,a_2}(t)$와 $v_{j,a_3,a_4}(t)$를 유도하자. 정리 4에서의 증명과 비슷한 방법으로 B_i의 9개의 합으로 정리가 된다. $u_{i,a_1,a_2}(t)$가 정리 4의 $v_{i,a_1,a_2}(t)$로 생각할 수 있다. 이를 정리하면 다음과 같다.

$$\begin{aligned}&|R(\tau)| \\ &= \begin{cases} |B_1+B_2+B_4+B_9| \leq 4\sqrt{p^n}+4, & \text{if } \tau = 0 \\ |B_1+B_3+B_4+B_8| \leq 4\sqrt{p^n}+4, & \text{if } \tau = -j \\ |B_1+B_2+B_6+B_7| \leq 4\sqrt{p^n}+4, & \text{if } \tau = i \\ |B_1+B_3+B_5+B_7| \leq 4\sqrt{p^n}+4, & \text{if } \tau = i-j \\ |B_1+B_2+B_3+B_4+B_7| \leq 4\sqrt{p^n}+5, & \text{otherwise.} \end{cases}\end{aligned}$$

$u_{i,a_1,a_2}(t)$와 $v_{j,a_3,a_4}(t)$의 상호 상관값의 상한이 $4\sqrt{p^n}+5$임을 보였다. 수열군 $\mathcal{M}$에 속한 다른 수열들 간의 상관값도 정리하면 상한이 $4\sqrt{p^n}+5$이다. □

이 방법은 상관 값의 상한은 $3\sqrt{p^n}+5$에서 $4\sqrt{p^n}+5$로 악화되는 단점이 있지만 수열군 크기 $|\mathcal{M}|$는 $|\mathcal{L}|$의 약 2배가 되는 장점을 가지고 있다.

5. 결론

Kim과 Chung, No, Chung은 수열군의 상관값이 $3\sqrt{p^n}+5$로 상한되는 M-진 수열군을 제안하였다. 이 논문에서는, 주기가 p^n-1인 M-진 수열군을 제시하였다. 이 수열군의 상한은 $4\sqrt{p^n}+5$이다. 제안된 수열군은 상관값의 상한을 비교했을 때 Kim과 Chung, No, Chung이 제안한 수열군의 상관 값의 상한보다 큰 것이 단점이지만 수열군 크기 약 2배가 되는 장점을 가지고 있다.

6. 감사의 글

본 연구는 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원 [No. 2009-0081441]과 지식경제부 및 정보통신연구진흥원의 IT핵심기술개발사업의 일환으로 수행하였음 [2008-F-007-02, 3차원 환경에서의 지능형 무선통신 시스템].

7. 참고문헌

[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] S. M. Krone and D. V. Sarwate, "Quadriphase sequences for spread-spectrum multiple-access communication," *IEEE Trans. Inf. Theory*, vol. 30, no. 4, pp. 520–529, May 1984.

[3] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "New families of M-ary sequences with low correlation constructed from Sidel'nikov sequences," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3768–3774, Aug. 2008.

[4] 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.

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

[6] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and Its Applications.* Reading, MA: Addison-Wesley, 1983.

[7] T. Storer, *Cyclotomy and Difference Sets, Lectures in Advanced Mathematics.* Chicago, IL: Markham, 1967.