Sidel'nikov 수열로부터 생성한 새로운 M진 수열군

*김영식O, *정정수, *노종선, **정하봉
*서울대학교 전기컴퓨터공학부 & INMC, **홍익대학교 전자전기공학부

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

*Young-Sik Kim, *Jung-Soo Chung, *Jong-Seon No, and **Habong Chung
*School of EECS & INMC, Seoul National University
**School of Electronics and Electrical Engineering, Hongik University
{kingsi, integer}@ccl.snu.ac.kr, jsno@snu.ac.kr, habchung@hongik.ac.kr

요약

이 논문에서는 $M|p^n-1$를 만족하는 양의 정수 M과 소수 p에 대해서 주기가 p^n-1인 M진 Sidel'nikov 수열을 사용해서 M진 수열군을 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 p가 홀수일 때는 $(M-1)^2(p^n-3)/2+M(M-1)/2$가 된다.

1. 도입

오늘날 고속 데이터 통신을 위해서 M진 변조 방식들이 표준에 적용되고 있다. 이에 따라서 좋은 상관 특성을 갖는 M진 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 p이거나 4로 한정되어 있었다. 최근에 Kim, Chung, No, 그리고 Chung은 M진 Sidel'nikov 수열을 사용해서 최대의 상관 값의 상한이 $2\sqrt{p^n}+6$인 M진 수열군을 생성하였다 [5] .

이 논문에서는 $M|p^n-1$를 만족하는 양의 정수 M과 소수 p에 대해서 주기가 p^n-1인 M진 Sidel'nikov 수열을 사용해서 M진 수열군을 생성하였다. 이것은 최근의 연구를 [5] 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, p가 홀수일 때는 $(M-1)^2(p^n-3)/2+M(M-1)/2$가 된다.

2. 사전지식

α가 p^n개의 원소를 갖는 유한체 F_{p^n}의 원시원이라 하자. Sidel'nikov는 [1] 다음과 같이 좋은 자기상관특성을 갖는 M진 수열을 도입하였다.

정의 1 [1] p가 소수이고 α가 F_{p^n}의 원시원이라 하자. M은 $M|p^n-1$을 만족하는 양의 정수이다. S_k, $k=0,1,\cdots,M-1$는 다음과 같은 F_{p^n}의 중복되지 않은 부분집합이라 하자.

$$S_k=\{\alpha^{Mi+k}-1|\ 0\le i<\frac{p^n-1}{M}\}. \tag{1}$$

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

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

여기서 k_0는 modulo M을 취한 정수이다. □

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

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

여기서 α는 F_{p^n}의 원시원이고 $M|p^n-1$이다. □

위의 정의로부터 다음이 성립함을 알 수 있다.

$$\sum_{x\in F_{p^n}}\psi(x)=0. \tag{3}$$

지시 함수를 다음과 같이 정의하자.

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

이제 M진 Sidel'nikov 수열을 다음과 같이 지시 함수와 곱의 character를 사용해서 나타낼 수 있다.

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

여기서 ω는 1의 복소 M차 근이다.

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

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

(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] $f_1(z), \cdots, f_l(z)$가 l개의 두쌍 씩 서로소인 $F_{p^n}[z]$에서의 monic 다항식이라고 하자. 이 다항식의 가장 큰 squarefree 약수의 차수를 $d_1, \cdots, d_l$라 하자. 이제 $\chi_1 \cdots, \chi_l$이 F_{p^n}의 자명하지 않은 곱의 character라 하자. 그리고 $1 \leq i \leq l$에 대해서 다항식 $f_i(z)$는 $g(z)^{ord(\chi_i)}$의 형태가 아니라고 가정하자. 여기에서 $ord(\chi)$는 $\chi^d = 1$를 만족하는 가장 작은 양의 정수 d이고 $g(z)$는 $F_{p^n}[z]$상에서의 다항식이다. 그러면 다음 식이 성립한다.

$$\Big| \sum_{z \in F_{p^n}} \chi_1(f_1(z)) \cdots \chi_l(f_l(z)) \Big| \leq (\sum_{i=1}^{l} d_i - 1) p^{n/2}. \tag{6}$$

□

3. M진 수열군의 생성

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

i) $p = 2$인 경우;

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

ii) 홀수 p인 경우;

$$\begin{aligned} L = &\{v_{0,c_1}(t) \mid 1 \leq c_1 \leq M-1\} \\ &\cup \{v_{i,c_1,c_2}(t) \;\Big|\; 1 \leq c_1, c_2 \leq M-1, 1 \leq i \leq T-1\} \\ &\cup \{v_{T,c_1,c_2}(t) \;\Big|\; 1 \leq c_1 < c_2 \leq M-1\} \end{aligned} \tag{8}$$

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. L의 크기는 $p = 2$일 때 $(M-1)^2 T - (M-1)(M-2)$이고 홀수 p일 때 $(M-1)^2 T - (M-1)(M-2)/2$이다. 이 논문에서는 $p = 2$인 경우에서도 동일하게 증명할 수 있기 때문에 홀수 p인 경우에 대해서만 증명할 것이다.

먼저 i의 구간이 $0 \leq i \leq (p^n - 3)/2$이고 $c_1 < c_2$에 대해서 $i = (p^n - 1)/2$이기 때문에 L에서의 각각의 수열이 서로 순회적으로(cyclically) 다르다는 것을 어렵지 않게 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 L에서의 수열 $v_{i,c_1,c_2}(t)$는 다음과 같이 나타낼 수 있다.

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

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

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

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

증명: 여기서는 홀수 p인 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 $j \neq 0$;

이 때 (9)에 의해 두 수열의 상관 함수는 다음과 같이 총 9개의 덧셈 항으로 표현할 수가 있다.

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

$$
\begin{aligned}
&= \sum_{t=0}^{p^n-2} \Big[\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1) + \omega^{c_1k_0} I(\alpha^t+1) \\
&\quad \times \psi^{c_2}(\alpha^{t+i}+1) + \omega^{c_2k_0} I(\alpha^{t+i}+1)\psi^{c_1}(\alpha^t+1)\Big] \\
&\quad \times \Big[\psi^{-c_1'}(\alpha^{t+\tau}+1)\psi^{-c_2'}(\alpha^{t+j+\tau}+1) \\
&\quad + \omega^{-c_1'k_0} I(\alpha^{t+\tau}+1)\psi^{-c_2'}(\alpha^{t+j+\tau}+1) \\
&\quad + \omega^{-c_2'k_0} I(\alpha^{t+j+\tau}+1)\psi^{-c_1'}(\alpha^{t+\tau}+1)\Big] \\
&= \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) \\
&\quad \times \psi^{-c_2'}(\alpha^{t+j+\tau}+1) + \omega^{-c_1'k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1) \\
&\quad \times \psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_2'}(\alpha^{t+j+\tau}+1) I(\alpha^{t+\tau}+1) \\
&\quad + \omega^{-c_2'k_0} \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) I(\alpha^{t+j+\tau}+1) \\
&\quad + \omega^{c_1k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_1'}(\alpha^{t+\tau}+1) \\
&\quad \times \psi^{-c_2'}(\alpha^{t+j+\tau}+1) I(\alpha^t+1) \\
&\quad + \omega^{(c_1-c_1')k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_2}(\alpha^{t+j+\tau}+1) \\
&\quad \times I(\alpha^t+1) I(\alpha^{t+\tau}+1) \\
&\quad + \omega^{(c_1-c_2')k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_1'}(\alpha^{t+\tau}+1) \\
&\quad \times I(\alpha^t+1) I(\alpha^{t+j+\tau}+1) \\
&\quad + \omega^{c_2k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1)\psi^{-c_1'}(\alpha^{t+\tau}+1) \\
&\quad \times \psi^{-c_2'}(\alpha^{t+j+\tau}+1) I(\alpha^{t+i}+1) \\
&\quad + \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) \\
&\quad \times I(\alpha^{t+i}+1) I(\alpha^{t+\tau}+1) \\
&\quad + \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) \\
&\quad \times I(\alpha^{t+i}+1) I(\alpha^{t+j+\tau}+1). \qquad (10)
\end{aligned}
$$

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

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

그러면 정리 3으로부터 다음 식이 성립한다.

$$
\Big| \sum_{z\in F_{p^n}} \psi^{c_1}(z+1)\psi^{c_2}(\alpha^i z+1)\psi^{-c_1'}(\alpha^\tau z+1) \times \psi^{-c_2'}(\alpha^{j+\tau} z+1) - 1 \Big| \le 3\sqrt{p^n} + 1. \qquad (11)
$$

(10)에서의 두 번째 항은 다음과 같이 주어진다.

$$
\begin{aligned}
&\omega^{-c_1'k_0} \sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_2'}(\alpha^{t+j+\tau}+1) \\
&\quad \times I(\alpha^{t+\tau}+1) \\
&= \omega^{-c_1'k_0}\psi^{c_1}(1-\alpha^{-\tau})\psi^{c_2}(1-\alpha^{i-\tau})\psi^{-c_2'}(1-\alpha^j) \\
&= \begin{cases} 0, & \text{if } \tau = 0 \text{ or} \\ & \tau = i \\ \omega^{-c_1'k_0}\psi\big(\frac{(1-\alpha^{-\tau})^{c_1}(1-\alpha^{i-\tau})^{c_2}}{(1-\alpha^j)^{c_2'}}\big), & \text{otherwise.} \end{cases} \qquad (12)
\end{aligned}
$$

세 번째 항은 다음과 같이 주어진다.

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

네 번째 항은 다음과 같다.

$$
\begin{aligned}
&\omega^{c_1k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_1'}(\alpha^{t+\tau}+1) \\
&\quad \times \psi^{-c_2'}(\alpha^{t+j+\tau}+1) I(\alpha^t+1) \\
&= \begin{cases} 0, & \text{if } \tau = 0 \text{ or } \tau = -j \\ \omega^{c_1k_0}\psi\big(\frac{(1-\alpha^i)^{c_2}}{(1-\alpha^\tau)^{c_1'}(1-\alpha^{j+\tau})^{c_2'}}\big), & \text{otherwise.} \end{cases} \qquad (14)
\end{aligned}
$$

다섯 번째 항은 다음과 같다.

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

여섯 번째 항은 다음과 같다.

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

일곱 번째 항은 다음과 같다.

$$\begin{aligned}&\omega^{c_2k_0}\sum_{t=0}^{p^n-2}\psi^{c_1}(\alpha^t+1)\psi^{-c_1'}(\alpha^{t+\tau}+1)\psi^{-c_2'}(\alpha^{t+j+\tau}+1)\\&\quad\times I(\alpha^{t+i}+1)\\&=\begin{cases}0, & \text{if } \tau=i \text{ or}\\ & \tau=i-j\\ \omega^{c_2k_0}\psi\Big(\frac{(1-\alpha^{-i})^{c_1}}{(1-\alpha^{-i+\tau})^{c_1'}(1-\alpha^{-i+j+\tau})^{c_2'}}\Big), & \text{otherwise.}\end{cases}\end{aligned}\tag{17}$$

여덟 번째 항은 다음과 같다.

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

아홉 번째 항은 다음과 같다.

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

따라서 (11)-(19)로부터 다음과 같은 부등식을 얻게 된다.

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

다음으로 $v_{i,c_1,c_2}(t)$와 $v_{0,c_1'}(t)$ 두 개의 상관 값을 구하자.

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

이 경우에 상관 함수는 다음과 같이 쓸 수 있다.

$$\begin{aligned}C(\tau)&=\sum_{t=0}^{p^n-2}\omega^{c_1s(t)+c_2s(t+i)-c_1's(t+\tau)}\\&=\sum_{t=0}^{p^n-2}\Big[\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\\&\qquad+\omega^{c_1k_0}\psi^{c_2}(\alpha^{t+i}+1)I(\alpha^t+1)\\&\qquad+\omega^{c_2k_0}\psi^{c_1}(\alpha^t+1)I(\alpha^{t+i}+1)\Big]\\&\qquad\times\Big[\psi^{-c_1'}(\alpha^{t+\tau}+1)+\omega^{-c_1'k_0}I(\alpha^{t+\tau}+1)\Big]\\&=\sum_{t=0}^{p^n-2}\psi^{-c_1'}(\alpha^{t+\tau}+1)\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\\&+\omega^{c_1k_0}\sum_{t=0}^{p^n-2}\psi^{-c_1'}(\alpha^{t+\tau}+1)\psi^{c_2}(\alpha^{t+i}+1)I(\alpha^t+1)\\&+\omega^{c_2k_0}\sum_{t=0}^{p^n-2}\psi^{-c_1'}(\alpha^{t+\tau}+1)\psi^{c_1}(\alpha^t+1)I(\alpha^{t+i}+1)\\&+\omega^{-c_1'k_0}\sum_{t=0}^{p^n-2}\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)I(\alpha^{t+\tau}+1)\\&+\omega^{(c_1-c_1')k_0}\sum_{t=0}^{p^n-2}\psi^{c_2}(\alpha^{t+i}+1)I(\alpha^t+1)I(\alpha^{t+\tau}+1)\\&+\omega^{(c_2-c_1')k_0}\sum_{t=0}^{p^n-2}\psi^{c_1}(\alpha^t+1)I(\alpha^{t+i}+1)I(\alpha^{t+\tau}+1).\end{aligned}\tag{20}$$

(20)에서의 첫 번째 합은 다음과 같다.

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

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

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

끝으로 $v_{0,c_1}(t)$와 $v_{0,c_1'}(t)$ 사이의 상관 값의 크기가 $\sqrt{p^n}+3$을 상한으로 갖는다는 것을 동일한 방식으로 증명할 수가 있다. □

다음의 예에서는 4진 수열군을 생성한다.

예제 5 $M=4$, $p=7$, 그리고 $n=4$인 경우에 주기가 $N=2400$인 4진 수열군을 생성할 수가 있다. $s(t)$가 4진 Sidel'nikov 수열이라 하자. 그러면 수열군 L에는

총 10,797개의 수열이 다음과 같이 포함되어 있다.

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

L에서의 수열들의 상호 상관 값들의 크기는 $3 \times 49 + 6 = 153$을 상한으로 갖는다. □

4. 감사의 글

본 연구는 정보통신부의 출연금으로 수행하고 있는 ITRC 과제와 교육인적자원부, 산업자원부, 노동부의 출연금으로 수행한 최우수실험실 지원 사업에 의한 연구 결과입니다.

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.