New Construction of M-ary Sequence Family From Sidel'nikov Sequences

Young-Sik Kim
Samsung Electronics, Co., Ltd.
Yongin, Gyeonggi-do, Korea
mypurist@gmail.com

Jung-Soo Chung, Sung-Tai Choi, Jong-Seon No
Department of EECS
Seoul National University,
Seoul, Korea
{integer, stchoi}@ccl.snu.ac.kr, jsno@snu.ac.kr

Habong Chung
School of EEE,
Hongik University, Seoul, Korea
habchung@hongik.ac.kr

***Abstract*— In this paper, for a positive integer M and a prime p such that $M|p^n-1$, a family of M-ary sequences using the M-ary Sidel'nikov sequences with period p^n-1 is constructed. This 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. Introduction

Especially for the high speed data transmission, M-ary phase shift keying (PSK) modulation schemes are frequently adopted as a standard. Accordingly, it becomes more important to find M-ary codes with good error correctability as well as the family of M-ary sequences with good correlation property.

There have been lots of research results on the families of sequences with low correlation [3]–[16]. However, the alphabet sizes of the known families of sequences are restricted to a prime p or 4.

In this paper, for a positive integer M and a prime p such that $M|p^n-1$, a family of M-ary sequences using the M-ary Sidel'nikov sequences with period p^n-1 is constructed. This 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.

II. Preliminaries

Let α be a primitive element of the finite field F_{p^n} with p^n elements. Sidel'nikov [1] introduced the following M-ary sequences called Sidel'nikov sequences with good autocorrelation property.

Definition 1: [2] Let p be a prime and α a primitive element of F_{p^n}. Let M be a positive integer such that $M|p^n-1$. Let S_k, $k=0,1,\cdots,M-1$, be the disjoint subsets of $F_{p^n}\backslash\{-1\}$ defined as

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

Then, the M-ary Sidel'nikov sequence $s(t)$ of period p^n-1 is defined as

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

where k_0 is some integer modulo M. □

Definition 2: [18] A multiplicative character $\psi(\cdot)$ of order M in F_{p^n} is defined as

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

where α is a primitive element in F_{p^n} and $M|p^n-1$. □

From the above definition, it is obvious that

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

The indicator function is defined as

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

The M-ary Sidel'nikov sequences can be expressed using the indicator function and the multiplicative character as [2]

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

where ω is a complex M-th root of unity.

The cross-correlation function between two M-ary sequences $u(t)$ and $v(t)$ of period p^n-1 is defined as

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

Due to the expression in (4), the evaluation of the correlation between Sidel'nikov sequences may require that of a summation of products of multiplicative characters over the given field. The following theorem provides us an upper bound on a sum of products of multiplicative characters.

Theorem 3: [19] Let $f_1(z),f_2(z),\cdots,f_l(z)$ be l monic pairwise prime polynomials in $F_{p^n}[z]$ whose largest squarefree divisors have degrees $d_1,d_2,\cdots,d_l$. Let $\chi_1,\chi_2,\cdots,\chi_l$ be non-trivial multiplicative characters of F_{p^n}. Assume that for any $1\le i\le l$, the polynomial $f_i(z)$ is not of the form $g(z)^{ord(\chi_i)}$ in $F_{p^n}[z]$, where $ord(\chi)$ is the smallest positive integer d such that $\chi^d=1$ and $g(z)$ is a polynomial in $F_{p^n}[z]$. Then, we have

$$\Big|\sum_{z\in F_{p^n}}\chi_1(f_1(z))\chi_2(f_2(z))\cdots\chi_l(f_l(z))\Big|\le(\sum_{i=1}^{l}d_i-1)p^{n/2}. \tag{6}$$

If $\chi_i^{d_i} = 1$ for all i, then the right side of (6) can be improved to

$$(\sum_{i=1}^{l} d_i - 2)p^{n/2} + 1.$$

□

III. Constructions of the Families of M-ary Sequences

Let $s(t)$ be an M-ary Sidel'nikov sequence of period p^n-1 defined in (2). Let $T = \lceil (p^n-1)/2 \rceil$, where $\lceil x \rceil$ denotes the least integer larger than or equal to x. Let $\mathcal{L}$ be the set of M-ary sequences of period p^n-1 given as:

i) For the case of $p = 2$;

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

ii) For the case of odd prime p;

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

where $v_{0,c_1}(t) = c_1 s(t)$ and $v_{i,c_1,c_2}(t) = c_1 s(t) + c_2 s(t+i)$ for $i \ne 0$. It is clear that the family size of $\mathcal{L}$ is $(M-1)^2 T - (M-1)(M-2)$ for $p = 2$ or $(M-1)^2 T - (M-1)(M-2)/2$ for an odd prime p. In the rest of the paper, we will restrict our discussion on $\mathcal{L}$ to the case of odd prime p because similar statements can be made for the case of even prime.

It is not difficult to see that each sequence in $\mathcal{L}$ is cyclically distinct to one another, since the range of i is restricted to $0 \le i \le (p^n-3)/2$ and $i = (p^n-1)/2$ for $c_1 < c_2$. Otherwise, we may have $v_{i,c_1,c_2}(t) = v_{p^n-1-i,c_2,c_1}(t+i)$ for $1 \le i \le T$.

Using (4), for $1 \le i \le T$, a sequence $v_{i,c_1,c_2}(t)$ in $\mathcal{L}$ can be represented as

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

Note that each of the second term and the third term in (9) contains the indicator function and thus vanishes except for the specific t, namely $t = T$ and $t = T - i$, respectively.

Theorem 4: The magnitude of the correlation values of any two M-ary sequences in the large family $\mathcal{L}$ in (7) and (8) is upper bounded by

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

Proof: We will prove only for the case of odd prime p. Let us first consider the case when the two sequences are $v_{i,c_1,c_2}(t)$ and $v_{j,c_1',c_2'}(t)$, that is, neither i nor j is zero.

Case 1) $i \ne 0$ and $j \ne 0$;

Using (9), the correlation of two sequences $v_{i,c_1,c_2}(t)$ and $v_{j,c_1',c_2'}(t)$ in $\mathcal{L}$ can be written as

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

$$+\,\omega^{(c_2-c_2')k_0}\sum_{t=0}^{p^n-2}\psi^{c_1}(\alpha^t+1)\psi^{-c_1'}(\alpha^{t+\tau}+1)$$
$$\times I(\alpha^{t+i}+1)I(\alpha^{t+j+\tau}+1). \tag{10}$$

There are nine summations in (10) and now we are going to evaluate each by turns.

The first summation in (10) is given as

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

From Theorem 3, we have

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

The second summation in (10) is given as

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

The third summation in (10) is given as

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

The fourth summation in (10) is given as

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

The fifth summation in (10) is given as

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

The sixth summation in (10) is given as

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

The seventh summation in (10) is given as

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

The eighth summation in (10) is given as

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

The ninth summation in (10) is given as

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

Thus we have

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

Next, let us consider the case when the two sequences are $v_{i,c_1,c_2}(t)$ and $v_{0,c_1'}(t)$ or vice versa.

Case 2) $i\neq 0$ and $j=0$ (or $i=0$ and $j\neq 0$);

In this case, the correlation function can be written as

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

The first summation in (20) is given as

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

From Theorem 3, the above sum is upper bounded by $2\sqrt{p^n}+1$. Since the other summations contain the indicator function, they can be represented by single multiplicative character or zero with respect to phase shift τ. Similarly to Case 1), we have

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

Finally, it can be proved that the magnitudes of correlation between $v_{0,c_1}(t)$ and $v_{0,c_1'}(t)$ are upper bounded by $\sqrt{p^n}+3$ in the similar way. □

From the cross-correlation properties in Theorem 4, it is clear that the sequences in the family $\mathcal{L}$ are cyclically distinct. The following example gives the family of quaternary sequences.

Example 5: For $M = 4$, $p = 7$, and $n = 4$, we can construct a family of quaternary sequences of period $N = 2400$. Let $s(t)$ be a quaternary Sidel'nikov sequence. Then, the family $\mathcal{L}$ contains 10,797 sequences as

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

The magnitude of cross-correlation values of sequences in $\mathcal{L}$ is upper bounded by $3\times 49+6 = 153$. □

ACKNOWLEDGMENT

This research was supported by the MEST, the MKE, and the MOLAB, Korea, through the fostering project of the Laboratory of Excellency.

REFERENCES

[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] T. Kasami, "Weight distribution formular for some class of cyclic codes," Technical Report R-285 (AD 632574), Coordinated Science Laboratory, Univ. of Illinois, Urbana, Apr. 1966.

[4] T. Kasami, "Weight distribution of Bose-Chaudhuri-Hocquenghem codes," in *Cambinatorial Mathematics and Its Applications.* Chapel Hill, NC: Univ. of North Carolina Press, 1969.

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

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

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

[8] V. M. Sidel'nikov, "On mutual correlation of sequences," *Soviet Math. Dokl.*, vol. 12, no. 1, pp. 197–201, 1971.

[9] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discrete Math.*, vol. 16, pp. 209–232, 1976.

[10] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inf. Theory,* vol. 28, pp. 858–864, Nov. 1982.

[11] J.-S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal correlation properties and large linear span," *IEEE Trans. Inf. Theory,* vol. 35, pp. 371–379, Mar. 1989.

[12] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," *IEEE Trans. Inf. Theory,* vol. 37, pp. 603–616, May 1991.

[13] T. Moriuchi and K. Imamura, "Balanced nonbinary sequences with good periodic correlation properties obtained from modified Kumar-Moreno sequences," *IEEE Trans. Inf. Theory*, vol. 41, pp. 572–576, Mar. 1995.

[14] J.-W. Jang, Y.-S. Kim, J.-S. No, and T. Helleseth, "New family of p-ary sequences with optimal correlation property and large linear span," *IEEE Trans. Inf. Theory,* vol. 50, no. 8, pp. 1839–1844, Aug. 2004.

[15] S. Boztas, R. Hammons, and P. V. Kumar, "4-phase sequences with near-optimum correlation properties," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 1101–1113, May 1992.

[16] 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.

[17] 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.

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

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