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 \( (M-1)^2(2^{M-1}-1)+M-1 \) 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 \( (M-1)^2(2^{M-1}-1)+M-1 \) for \( p=2 \) or \( (M-1)^2(p^n-3)/2+M(M-1)/2 \) for an odd prime \( p \).

II. PRELIMINARIES

Let \( \alpha \) 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 \( \alpha \) 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

\[
S_k = \{ \alpha^{M+i-k} \mid 0 \leq i < \frac{p^n-1}{M} \}. \tag{1}
\]

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

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

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

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

\[
\psi(0) = 0
\]

where \( \alpha \) 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

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

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 \( \omega \) 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

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

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 \( f_1(z), f_2(z), \ldots, f_l(z) \) be \( l \) monic pairwise prime polynomials in \( F_{p^n}[z] \) whose largest squarefree divisors have degrees \( d_1, d_2, \ldots, d_l \). Let \( \chi_1, \chi_2, \ldots, \chi_l \) be non-trivial multiplicative characters of \( F_{p^n} \). Assume that for any \( 1 \leq i \leq l \), 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

\[
\left| \sum_{z \in F_{p^n}} \chi_1(f_1(z))\chi_2(f_2(z))\cdots\chi_l(f_l(z)) \right| \leq \sum_{i=1}^{l} d_i - 1)^{p^n/2}. \tag{6}
\]
If $\chi_i^{d_i} = 1$ for all $i$, then the right side of (6) can be improved to

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

III. CONSTRUCTIONS OF THE FAMILIES OF $M$-ARY SEQUENCES

Let $s(t)$ be an $M$-ary Sidelnikov 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 $p = 2$;

$$\mathcal{L} = \{ v_{0,c_1}(t) \mid 1 \leq c_1 \leq M - 1 \}$$

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

ii) For the case of odd prime $p$;

$$\mathcal{L} = \{ v_{0,c_1}(t) \mid 1 \leq c_1 \leq M - 1 \}$$

$$\cup \{ v_{i,c_1,c_2}(t) \mid 1 \leq c_1, c_2 \leq M - 1, 1 \leq i \leq T - 1 \}$$

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

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 $i \neq 0$. 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 $0 \leq i \leq (p^n - 3)/2$ 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 $1 \leq i \leq T$.

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

$$\omega^{v_{i,c_1,c_2}(t)} = \omega^{c_1 s(t) + c_2 s(t + i)}$$

$$= \left[ \psi_{c_1}(a^t + 1) + \omega^{c_2 k_0} I(a^t + 1) \right]$$

$$\times \left[ \psi_{c_2}(a^{t + i} + 1) + \omega^{c_1 k_0} I(a^{t + i} + 1) \right]$$

$$= \psi_{c_1}(a^t + 1) \psi_{c_2}(a^{t + i} + 1)$$

$$+ \omega^{c_1 k_0} I(a^t + 1) \psi_{c_2}(a^{t + i} + 1)$$

$$+ \omega^{c_2 k_0} I(a^{t + i} + 1) \psi_{c_1}(a^t + 1). \quad (9)$$

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

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

**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** $i \neq 0$ and $j \neq 0$;

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

$$C(\tau) = \sum_{t=0}^{p^n-2} \omega^{v_{i,c_1,c_2}(t) - v_{j,c_1,c_2}(t + \tau)}$$

$$= \sum_{t=0}^{p^n-2} \omega^{c_1 s(t) + c_2 s(t + i) - c_1 s(t + \tau) - c_2 s(t + j + \tau)}$$

$$= \sum_{t=0}^{p^n-2} \left[ \psi_{c_1}(a^t + 1) \psi_{c_2}(a^{t+i} + 1) + \omega^{c_1 k_0} I(a^t + 1) \times \psi_{c_2}(a^{t+i} + 1) + \omega^{c_2 k_0} I(a^{t+i} + 1) \psi_{c_1}(a^t + 1) \right]$$

$$\times \left[ \psi_{c_1}(a^{t+\tau} + 1) \psi_{c_2}(a^{t+j+\tau} + 1) + \omega^{c_1 k_0} I(a^{t+\tau} + 1) \psi_{c_2}(a^{t+j+\tau} + 1) + \omega^{c_2 k_0} I(a^{t+j+\tau} + 1) \psi_{c_1}(a^t + 1) \right]$$

$$= \sum_{t=0}^{p^n-2} \psi_{c_1}(a^t + 1) \psi_{c_2}(a^{t+i} + 1) \psi_{c_1}(a^{t+j+\tau} + 1)$$

$$\times \psi_{c_1}(a^{t+\tau} + 1) \psi_{c_2}(a^{t+j+\tau} + 1) + \omega^{c_1 k_0} I(a^t + 1) \psi_{c_2}(a^{t+i} + 1) \psi_{c_1}(a^{t+\tau} + 1)$$

$$\times \psi_{c_1}(a^{t+j+\tau} + 1) \psi_{c_2}(a^{t+i} + 1) I(a^{t+j+\tau} + 1)$$

$$+ \omega^{c_1 k_0} \sum_{t=0}^{p^n-2} \psi_{c_1}(a^t + 1) \psi_{c_2}(a^{t+i} + 1) I(a^{t+\tau} + 1)$$

$$+ \omega^{c_1 k_0} \sum_{t=0}^{p^n-2} \psi_{c_1}(a^{t+\tau} + 1) \psi_{c_2}(a^{t+i} + 1) I(a^{t+j+\tau} + 1)$$

$$+ \omega^{c_1 k_0} \sum_{t=0}^{p^n-2} \psi_{c_1}(a^{t+j+\tau} + 1) \psi_{c_2}(a^{t+i} + 1) I(a^{t+\tau} + 1)$$

$$+ \omega^{c_1 k_0} \sum_{t=0}^{p^n-2} \psi_{c_1}(a^{t+i} + 1) \psi_{c_2}(a^{t+j+\tau} + 1) I(a^{t+\tau} + 1)$$

$$+ \omega^{c_1 k_0} \sum_{t=0}^{p^n-2} \psi_{c_1}(a^{t+\tau} + 1) \psi_{c_2}(a^{t+j+\tau} + 1) I(a^{t+j+\tau} + 1).$$

Note that $\psi_{c_1}(a^t + 1)$ and $\psi_{c_2}(a^{t+i} + 1)$ are not zero if $i < j$ and $c_1 < c_2$. Therefore, the correlation is upper bounded by

$$|C(\tau)| \leq 3\sqrt{p^T} + 6.$$
There are nine summations in (10) and now we are going to evaluate each by turns.

The first summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1)\psi^{-c_1}(\alpha^{t+\tau}+1) \times I(\alpha^{t+i}+1)I(\alpha^{t+j+\tau}+1). \tag{10}
\]

The second summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_2}(\alpha^{t+j+\tau}+1)
\times I(\alpha^{t+i}+1) = \sum_{z \in F_p} \psi^{c_1}(z+1)\psi^{c_2}(\alpha^t z+1)
\times \psi^{-c_1}(\alpha^t z+1)\psi^{-c_2}(\alpha^t z+1)+1 - 1. \tag{11}
\]

The third summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_3}(\alpha^t+1)\psi^{-c_3}(\alpha^{t+j+\tau}+1)
\times I(\alpha^{t+i}+1)
\times I(\alpha^{t+i}+1) = \left\{ \begin{array}{ll}
\omega^{-c_3}_k \psi \frac{(1-\alpha^{-\tau})(1-\alpha^{-j})}{(1-\alpha^{-i})^2}, & \text{if } \tau = 0 \text{ or } \tau = i \\
0, & \text{otherwise.} \end{array} \right. \tag{12}
\]

The fourth summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^{t+i}+1)\psi^{-c_1}(\alpha^{t+j+\tau}+1)\psi^{-c_2}(\alpha^{t+j+\tau}+1)
\times I(\alpha^{t+i}+1) = \left\{ \begin{array}{ll}
0, & \text{if } \tau = -j \text{ or } \tau = i-j \\
\omega^{-c_2}_k \psi \frac{(1-\alpha^{-i})(1-\alpha^{-i-j})}{(1-\alpha^{-i})^2}, & \text{otherwise.} \end{array} \right. \tag{13}
\]

The fifth summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^{t+i}+1)\psi^{-c_2}(\alpha^{t+j+\tau}+1)I(\alpha^{t+i}+1)
\times I(\alpha^{t+i}+1) = \left\{ \begin{array}{ll}
\omega^{-c_2}_k \psi \frac{(1-\alpha^{-i})(1-\alpha^{-i-j})}{(1-\alpha^{-i})^2}, & \text{if } \tau = 0 \\
0, & \text{otherwise.} \end{array} \right. \tag{15}
\]

The sixth summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^{t+j+\tau}+1)\psi^{-c_2}(\alpha^{t+j}+\tau+1)I(\alpha^{t+j}+\tau+1)
\times I(\alpha^{t+i}+1) = \left\{ \begin{array}{ll}
\omega^{-c_2}_k \psi \frac{(1-\alpha^{-i})(1-\alpha^{-i-j})}{(1-\alpha^{-i})^2}, & \text{if } \tau = -j \\
0, & \text{otherwise.} \end{array} \right. \tag{16}
\]

The seventh summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^{t+i}+1)\psi^{-c_2}(\alpha^{t+j+\tau}+1)\psi^{-c_2}(\alpha^{t+j+\tau}+1)
\times I(\alpha^{t+i}+1) = \left\{ \begin{array}{ll}
0, & \text{if } \tau = i \text{ or } \tau = i-j \\
\omega^{-c_2}_k \psi \frac{(1-\alpha^{-i})(1-\alpha^{-i-j})}{(1-\alpha^{-i})^2}, & \text{otherwise.} \end{array} \right. \tag{17}
\]

The eighth summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^{t+i}+1)\psi^{-c_2}(\alpha^{t+j}+\tau+1)I(\alpha^{t+i}+1)
\times I(\alpha^{t+i}+1) = \left\{ \begin{array}{ll}
\omega^{-c_2}_k \psi \frac{(1-\alpha^{-i})(1-\alpha^{-i-j})}{(1-\alpha^{-i})^2}, & \text{if } \tau = i \\
0, & \text{otherwise.} \end{array} \right. \tag{18}
\]

The ninth summation in (10) is given as
\[
\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^{t+i}+1)\psi^{-c_2}(\alpha^{t+j}+\tau+1)I(\alpha^{t+i}+1)
\times I(\alpha^{t+j}+\tau+1) = \left\{ \begin{array}{ll}
\omega^{-c_2}_k \psi \frac{(1-\alpha^{-i})(1-\alpha^{-i-j})}{(1-\alpha^{-i})^2}, & \text{if } \tau = i-j \\
0, & \text{otherwise.} \end{array} \right. \tag{19}
\]

Thus we have
\[
|C(\tau)| \leq \begin{cases} 3\sqrt{p^n+5}, & \text{if } \tau = 0, i, i-j, \text{ or } -j \\ 3\sqrt{p^n+6}, & \text{otherwise.} \end{cases}
\]

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
\[
C(\tau) = p^{n-2} \sum_{\ell=0}^{p^n-2} \omega^{c_1 s(\tau) + c_2 (s(\tau+t) - c_i s(t + \tau))} \\
= p^{n-2} \left[ \psi^{c_1}(\alpha^t + 1)\psi^{c_2}(\alpha^{t+i} + 1) \\
+ \omega^{c_1 k_0} \psi^{c_2}(\alpha^{t+i} + 1)(\alpha^t + 1) \\
+ \omega^{c_2 k_0} \psi^{c_1}(\alpha^t + 1)(\alpha^{t+i} + 1) \\
\times \left[ \psi_{c_1}(\alpha^{t+i} + 1) + \omega^{c_1 k_0} I(\alpha^{t+i} + 1) \right] \right] \\
= p^{n-2} \sum_{t=0}^{\psi^{c_1}(\alpha^{t+i} + 1)} \left[ \psi^{c_1}(\alpha^t + 1)\psi^{c_2}(\alpha^{t+i} + 1) \\
+ \omega^{c_1 k_0} \psi^{c_2}(\alpha^{t+i} + 1)(\alpha^t + 1) \\
+ \omega^{c_2 k_0} \psi^{c_1}(\alpha^t + 1)(\alpha^{t+i} + 1) \\
\times \left[ \psi_{c_1}(\alpha^{t+i} + 1) + \omega^{c_1 k_0} I(\alpha^{t+i} + 1) \right] \right].
\]

The first summation in (20) is given as
\[
\sum_{t=0}^{p^{n-2}} \psi^{c_1}(\alpha^{t+i} + 1)\psi^{c_1}(\alpha^t + 1)\psi^{c_2}(\alpha^{t+i} + 1) \\
= \sum_{z \in F_p} \psi^{c_1}(\alpha^t + 1)\psi^{c_2}(\alpha^{t+i} + 1) - 1.
\]

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 \(\tau\). Similarly to Case 1), we have
\[
|C(\tau)| \leq 2\sqrt{p^n + 4}.
\]

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
\[
\mathcal{L} = \{s(t), 2s(t), 3s(t)\} \\
\cup \{s(t) + 2s(t + 1200), s(t) + 3s(t + 1200), s(t) + 3s(t + 1200)\} \\
\cup \{c_1 s(t) + c_2 s(t + i) \mid 1 \leq c_1, c_2 \leq 3, 1 \leq i \leq 1199\}.
\]

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**


