A Construction of a New Family of M-ary Sequences With Low Correlation From Sidel'nikov Sequences

Jung-Soo Chung, Jong-Seon No, *Senior Member, IEEE*, and Habong Chung, *Member, IEEE*

***Abstract*—In this paper, a new family of M-ary sequences of period $p^n - 1$ is proposed. The proposed family is constructed by the addition of cyclic shifts of an M-ary Sidel'nikov sequence and its reverse sequence. The number of sequences contained in this family is about $(M-1)^2$ times of their period and the maximum magnitude of their correlation values is upper bounded by $4\sqrt{p^n}+5$.**

***Index Terms*—Autocorrelation, cross-correlation, family of M-ary sequences, Legendre sequences, M-ary sequences, power residue sequences, Sidel'nikov sequences.**

I. Introduction

FOR POSITIVE integers n, M, and a prime p such that $M|p^n-1$, Sidel'nikov [1] constructed M-ary sequences, called *Sidel'nikov sequences* of period p^n-1, the out-of-phase autocorrelation magnitude of which is upper bounded by 4.

Like Legendre sequences, the Sidel'nikov sequences can be expressed by multiplicative characters over the given finite field. Recently, a series of constructing methods for a family of M-ary sequences using these character sequences have been proposed. Rushanan [2] proposed the family of Weil sequences of an odd prime length p whose correlation magnitude is upper bounded by $2\sqrt{p}+5$. The family size is $(p-1)/2$ and each sequence is constructed by a shift-and-add of a single quadratic-residue-based Legendre sequence. Kim *et al.* [3] constructed a family of M-ary Sidel'nikov sequences of period p^n-1 such that $M|p^n-1$, whose maximum magnitude of correlation values is upper bounded by $3\sqrt{p^n}+5$. The size of this sequence family is $(M-1)^2(\frac{p^n-3}{2})+\frac{M(M-1)}{2}$ for an odd prime p. When $M=4$, this family contains more than twice as many sequences as the family in [4] while keeping the maximum correlation magnitude the same. Han and Yang [5], [6] constructed M-ary sequence families using the shift and addition of power residue sequences, whose correlation magnitudes are upper bounded by $2\sqrt{p}+5$ or $3\sqrt{p}+4$, where p is the period. They also proposed that M-ary sequence families of period p^n-1 have correlation values upper bounded by $2\sqrt{p^n}+6$. Yu and Gong [7] introduced notion of partitioning an M-ary sequence family into $(M+1)$ disjoint subsequence families. They showed more generalized constructions by the addition of multiple cyclic shifts of power residue and Sidel'nikov sequences.

In this paper, a new family of M-ary sequences of period p^n-1 is constructed from M-ary Sidel'nikov sequences. This family whose maximum correlation magnitude is upper bounded by $4\sqrt{p^n}+5$ contains roughly twice as many sequences as the one by Kim *et al.* [3].

II. Preliminaries

For M-ary sequences $s_i(t)$ and $s_j(t)$ of period N, the correlation function $R_{s_i,s_j}(\tau)$ is defined as

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

where $\omega=e^{j2\pi/M}$.

Definition 1 ([8]): Let p be a prime and α a primitive element in the finite field $\mathbb{F}_{p^n}$. Let M be an integer greater than 1 such that $M|p^n-1$. Let S_k, $k=0,1,\cdots,M-1$, be the disjoint subsets of $\mathbb{F}_{p^n}$ defined by

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

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

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

where k_0 is some integer modulo M. ■

The M-ary Sidel'nikov sequence $s(t)$ in (1) can be expressed in terms of the multiplicative character $\psi_M(\cdot)$ of order M in $\mathbb{F}_{p^n}$ and the indicator function $I(\cdot)$ as

$$\omega^{s(t)}=\omega^{k_0}I(\alpha^t+1)+\psi_M(\alpha^t+1) \tag{2}$$

where

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

and the multiplicative character $\psi_M(\cdot)$ is defined as $\psi_M(\alpha^t)=e^{j2\pi t/M}$ and $\psi_M(0)=0$.

From (2), it is manifest that the correlation function between Sidel'nikov sequences can be expressed as sums of products

Manuscript received February 16, 2010; revised August 04, 2010; accepted November 03, 2010. Date of current version March 16, 2011. This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) under Grant 2010-0000867 and in part by the IT R&D program of MKE/KEIT (KI001809, Intelligent Wireless Communication Systems in Three-Dimensional Environment). The material in this paper was presented in part at the International Symposium on Information Theory and its Applications (ISITA 2010), Taichung, Taiwan, October 2010.

J.-S. Chung is with the Department of Electrical Engineering and Computer Science, INMC, Seoul National University, Seoul 151-744, Korea (e-mail: integer@ccl.snu.ac.kr).

J.-S. No is with the Department of Electrical Engineering and Computer Science, INMC, Seoul National University, Seoul 151-744, Korea (e-mail: jsno@snu.ac.kr).

H. Chung is with the School of Electronics and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea (e-mail: habchung@hongik.ac.kr).

Communicated by N. Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2011.2110750

of multiplicative characters over the given finite field. The following theorem provides us an upper bound on a sum of products of multiplicative characters.

Theorem 2 ([9]): Let $f_1(z), f_2(z), \ldots, f_l(z)$ be l monic pairwisely prime polynomials in $\mathbb{F}_{p^n}[z]$ whose highest-degree squarefree divisors have degrees $h_1, h_2, \ldots, h_l$. Let $\chi_1, \chi_2, \ldots, \chi_l$ be non-trivial multiplicative characters of $\mathbb{F}_{p^n}$. 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 $\mathbb{F}_{p^n}[z]$, where $ord(\chi)$ is the smallest positive integer h such that $\chi^h = 1$ and $g(z)$ is a polynomial in $\mathbb{F}_{p^n}[z]$. Then, we have

$$\Big| \sum_{z \in \mathbb{F}_{p^n}} \chi_1(f_1(z))\chi_2(f_2(z)) \cdots \chi_l(f_l(z)) \Big| \le \Big(\sum_{i=1}^{l} h_i - 1\Big)\sqrt{p^n}.$$

■

III. Constructions of the Families of M-ary Sequences

Kim *et al.* [3] constructed the families of M-ary sequences and derived the upper bound on the maximum magnitude of correlation values.

For a given M-ary Sidel'nikov sequence $s(t)$ of period $p^n - 1$, let $\mathcal{L}$ be the set of M-ary sequences of period $p^n - 1$ given as in [3]

1) For $p = 2$;

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

2) For an odd prime p;

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

where $u_{c_1,c_2;i}(t) = c_1 s(t) + c_2 s(t+i)$. Let $T = \lceil \frac{p^n-1}{2} \rceil$, where $\lceil a \rceil$ denotes the least integer larger than or equal to a. Then the following theorem can be stated.

Theorem 3 ([3]): Let $s(t)$ be an M-ary Sidel'nikov sequence of period $p^n - 1$ defined in (1) and (2). The family size of $\mathcal{L}$ is $(M-1)^2(T-1) + (M-1)$ for $p = 2$ or $(M-1)^2(T-1) + M(M-1)/2$ for an odd prime p. The magnitude of the correlation values of any two M-ary sequences in the family $\mathcal{L}$ is upper bounded by

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

■

Now, we can slightly modify the construction in Theorem 3 by introducing the reverse sequence $s(-t)$ to construct a new sequence family $\mathcal{K}$. Let $\mathcal{K}$ be the set of M-ary sequences of period $p^n - 1$ defined as:

1) For $p = 2$;

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

2) For an odd prime p;

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

where $v_{a_1,a_2;i}(t) = a_1 s(t) + a_2 s(-t+i)$.

Then the maximum correlation magnitude and the size of the sequence family $\mathcal{K}$ can be derived as in the following theorem.

Theorem 4: The magnitude of the correlation values of any two M-ary sequences in the family $\mathcal{K}$ is upper bounded by

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

and the family size is given as

$$|\mathcal{K}| = \begin{cases} (M-1)^2(T-1) + 2(M-1), & \text{for } p = 2 \\ (M-1)^2(T-1) + M(M-1), & \text{for an odd prime } p. \end{cases}$$

Proof: We will prove the theorem for an odd prime p. The case of $p = 2$ can be done similarly. The cross-correlation of two sequences $v_{a_1,a_2;i}(t)$ and $v_{a_3,a_4;j}(t)$ in the family $\mathcal{K}$ can be written as

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

As one can notice immediately, $R_{v_{a_1,a_2;i},v_{a_3,a_4;j}}(\tau)$ is expressed as the sum of nine summations over t of the product of multiplicative characters and possibly of indicator functions.

The first summation, namely A_1, is written as

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

Certainly, for some τ, i, and j, $\alpha^{\tau} z + 1, \alpha^{i-\tau} + z, z + 1$, and $\alpha^{j} + z$ become pairwisely prime so that $h_1 = h_2 = h_3 = h_4 = h_5 = 1$ defined in Theorem 2. If they are not pairwisely

TABLE I
PARAMETERS OF SOME KNOWN FAMILIES OF SEQUENCES

Family of Sequence	Alphabet	Period N	Family Size	$R_{\max}$
Kasami [10]–[12]	p	p^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
Gold (n odd) [13]	2	2^n-1	$N+2$	$\sqrt{2(N+1)}+1$
Gold (n even) [13]	2	2^n-1	$N+2$	$2\sqrt{(N+1)}+1$
Trachtenberg [14]	odd p	p^n-1	$N+1$	$\sqrt{p(N+1)}+1$
Sidel'nikov [15]	odd p	p^n-1	$N+1$	$\sqrt{N+1}+1$
Helleseth [16]	odd p	p^n-1	$N+1$	$2\sqrt{N+1}+1$
Bent [17]	p	p^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
No [18]	2	2^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
$S(0)$ [19]	4	2^n-1	$N+2$	$\sqrt{N+1}+1$
$S(1)$ [19]	4	2^n-1	$\geq N^2+3N+2$	$2\sqrt{N+1}+1$
$S(2)$ [19]	4	2^n-1	$\geq N^3+4N^2+5N+2$	$4\sqrt{N+1}+1$
KHC ($N_e=2$) [20]	4	2^n-1	$N+1$	$\sqrt{N}+1$
KHC ($N_e=3$), odd n [20]	4	2^n-1	N^2+3N+3	$2\sqrt{N}+1$
KHC ($N_e=3$), even n [20]	4	2^n-1	N^2+3N+2	$2\sqrt{N}+1$
KS [4]	4	p^n-1	$2(N+2)$	$3\sqrt{N+1}+5$
$\mathcal{W}$ [2]	2	p	$\frac{p-1}{2}$	$2\sqrt{p}+5$
$\mathcal{S}_{c_1}$[3]	M	p^n-1	$\frac{N}{2}+M-2$	$2\sqrt{N+1}+6$
$\mathcal{S}_{c_1,c_2}$[3]	M	p^n-1	$N+M-2$	$2\sqrt{N+1}+6$
$\mathcal{L}$ ($p=2$) [3]	M	2^n-1	$(M-1)^2(\frac{N-1}{2})+M-1$	$3\sqrt{N+1}+5$
$\mathcal{L}$ (p odd prime) [3]	M	p^n-1	$(M-1)^2(\frac{N}{2}-1)+\frac{M(M-1)}{2}$	$3\sqrt{N+1}+5$
$\mathcal{F}_{\mathbf{r}}^{(a)}$ [6]	M	p	$\frac{N-1}{2}+M-1$	$2\sqrt{N}+5$
$\mathcal{F}_{\mathbf{r}}$ [6]	M	p	$\frac{(M-1)^2(N-1)}{2}+M-1$	$3\sqrt{N}+4$
$\tilde{\mathcal{F}}_{\mathbf{s}}$ [6]	M	p^n-1	$\frac{(M-1)}{2}N+\lfloor\frac{M-1}{2}\rfloor$	$2\sqrt{N+1}+6$
$\mathcal{G}_{\mathbf{r}}^{(\delta,2)}, \delta\neq 0$ [7]	M	p	$(M-1)+(\frac{N-1}{2})(M-1)^2$ $+\frac{(N-1)(N-3)}{8}(M^2-3M+3)$	$4\sqrt{N}+7$
$\mathcal{H}_{\mathbf{r}}^{(2)}$ [7]	M	p	$(M-1)+(\frac{N-1}{2})(M-1)^2$ $+\frac{(N-1)(N-3)}{8}(M-1)^3$	$5\sqrt{N}+6$
$\mathcal{G}_{\mathbf{s}}^{(\delta,2)}, \delta\neq 0$ [7]	M	p^n-1	$(M-1)+(\frac{N-2}{2})(M-1)^2$ $+\frac{(N-2)(N-4)}{8}(M^2-3M+3)$	$4\sqrt{N+1}+8$
$\mathcal{H}_{\mathbf{s}}^{(2)}$ [7]	M	p^n-1	$(M-1)+(\frac{N-2}{2})(M-1)^2$ $+\frac{(N-2)(N-4)}{8}(M-1)^3$	$5\sqrt{N+1}+7$
$\mathcal{K}$ ($p=2$)	M	2^n-1	$(M-1)^2(\frac{N-1}{2})+2(M-1)$	$4\sqrt{N+1}+5$
$\mathcal{K}$ (p odd prime)	M	p^n-1	$(M-1)^2(\frac{N}{2}-1)+M(M-1)$	$4\sqrt{N+1}+5$
$\mathcal{M}$ ($p=2$)	M	2^n-1	$2(M-1)^2(\frac{N-1}{2})+2(M-1)$	$4\sqrt{N+1}+5$
$\mathcal{M}$ (p odd prime)	M	p^n-1	$2(M-1)^2(\frac{N}{2}-1)$ $+2(M-1)+\frac{3(M-1)(M-2)}{2}$	$4\sqrt{N+1}+5$

* p is a prime number, M is an integer greater than or equal to 2, and N is a period. $R_{\max}$ denotes the maximum magnitude of correlation value. N_e denotes weighted degree.

prime for other values of τ, i, and j, some $\psi_M(\cdot)$ can be merged, since they are all of degree one. Thus it is easy to check $|A_1| \leq 4\sqrt{p^n}+1$ from Theorem 2.

In the second summation A_2, $I(\alpha^{-t+j}+1)=1$ only when $t=N/2+j$ and thus we have

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

In each of the remaining seven summations, the summand contains either one or two indicator functions so that the magnitude of each summation is either one or zero. Thus, we can prove that $|R_{v_{a_1,a_2;i},v_{a_3,a_4;j}}(\tau)| \leq 4\sqrt{p^n}+5$.

Similarly, we can prove that the cross-correlation magnitude of any two sequences in the family $\mathcal{K}$ is less than or equal to $4\sqrt{p^n}+5$. ■

IV. MAIN CONSTRUCTION

Certainly the sequence family $\mathcal{K}$ itself has no merit compared to the family $\mathcal{L}$ in [3] because the family size is almost the same but the maximum correlation magnitude is deteriorated from $3\sqrt{p^n}+5$ to $4\sqrt{p^n}+5$. But combining $\mathcal{K}$ and $\mathcal{L}$ can give us a larger family.

Let $\mathcal{M}(=\mathcal{K}\cup\mathcal{L})$ be the set of M-ary sequences of period p^n-1 defined as:

1) For $p = 2$;

$$\begin{aligned}\mathcal{M} = &\{v_{a_1,0;0}(t) \mid 1 \le a_1 \le M-1\}\\ &\cup \{v_{0,a_1;0}(t) \mid 1 \le a_1 \le M-1\}\\ &\cup \left\{v_{a_1,a_2;i}(t) \,\middle|\, 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\right\}\\ &\cup \left\{u_{a_1,a_2;i}(t) \,\middle|\, 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\right\}. \quad (3)\end{aligned}$$

2) For an odd prime p;

$$\begin{aligned}\mathcal{M} = &\{v_{a_1,0;0}(t) \mid 1 \le a_1 \le M-1\}\\ &\cup \{v_{0,a_1;0}(t) \mid 1 \le a_1 \le M-1\}\\ &\cup \left\{v_{a_1,a_2;0}(t) \,\middle|\, 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\right\}\\ &\cup \left\{v_{a_1,a_2;T}(t) \,\middle|\, 1 \le a_1, a_2 \le M-1, a_1 \ne a_2\right\}\\ &\cup \left\{u_{a_1,a_2;i}(t) \,\middle|\, 1 \le a_1, a_2 \le M-1, 1 \le i \le T-1\right\}\\ &\cup \left\{u_{a_1,a_2;T}(t) \,\middle|\, 1 \le a_1 < a_2 \le M-1\right\} \quad (4)\end{aligned}$$

where $v_{a_1,a_2;i}(t) = a_1 s(t) + a_2 s(-t+i)$ and $u_{a_1,a_2;i}(t) = a_1 s(t) + a_2 s(t+i)$.

Then we have the following theorem regarding the upper bound on the correlation values for the family $\mathcal{M}$.

Theorem 5: The magnitude of the correlation values of any two M-ary sequences in the large family $\mathcal{M}$ in (3) and (4) is upper bounded by

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

and their family size is given as

$$|\mathcal{M}| = \begin{cases} 2(M-1)^2(T-1) + 2(M-1), & \text{for } p = 2\\ 2(M-1)^2(T-1) + 2(M-1) & \\ +3(M-1)(M-2)/2, & \text{for an odd prime } p. \end{cases}$$

Proof: We will sketch the proof for the case of an odd prime p. It is enough to show that the magnitude of the cross-correlation between a sequence from $\mathcal{K}$ and a sequence from $\mathcal{L}$ is upper bounded by $4\sqrt{p^n}+5$. Here, we will take $u_{a_1,a_2;i}(t)$ from $\mathcal{L}$ and $v_{a_3,a_4;j}(t)$ from $\mathcal{K}$. For the other sequences, the proof goes similarly. Just similar to the proof of Theorem 4, the cross-correlation of $u_{a_1,a_2;i}(t)$ and $v_{a_3,a_4;j}(t)$ can be expressed as the sum of nine summations among which only one summation does not contain the indicator function. Thus, we can prove that the cross-correlation magnitude of two sequences $u_{a_1,a_2;i}(t)$ and $v_{a_3,a_4;j}(t)$ is less than or equal to $4\sqrt{p^n} + 5$. ■

Note that with a little sacrifice in maximum correlation magnitude from $3\sqrt{p^n}+5$ to $4\sqrt{p^n}+5$, the family size $|\mathcal{M}|$ is almost double of $|\mathcal{L}|$.

Some known families of sequences are listed in Table I.

V. Conclusion

In this paper, we proposed a new family of M-ary sequences of period $p^n - 1$ from Sidel'nikov sequences whose maximum correlation magnitude is upper bounded by $4\sqrt{p^n} + 5$. The sequence family constructed in this paper can be considered as an extension of the one in [3] by additionally introducing the reverse version of a Sidel'nikov sequence.

Acknowledgment

The authors wish to thank the anonymous reviewers for their valuable comments and suggestions that much improved the presentation of this paper.

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] J. J. Rushanan, "Weil sequences: A family of binary sequences with good correlation properties," in *Proc. 2006 IEEE Int. Symp. Inf. Theory (ISIT 2006)*, Seattle, WA, Jul. 2006, pp. 311–315.

[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] 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.

[5] Y.-K. Han and K. Yang, "New M-ary power residue sequence families with low correlation," in *Proc. 2007 IEEE Int. Symp. Inf. Theory (ISIT 2007)*, Nice, France, Jun. 2007, pp. 2616–2620.

[6] Y.-K. Han and K. Yang, "New M-ary sequence families with low correlation and large size," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1815–1823, Apr. 2009.

[7] N. Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6376–6387, Dec. 2010.

[8] 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.

[9] D. Wan, "Generators and irreducible polynomials over finite fields," *Math. Comput.*, vol. 66, no. 219, pp. 1195–1212, Jul. 1997.

[10] T. Kasami, Weight Distribution Formula for Some Class of Cyclic Codes Coordinated Science Laboratory, Univ. Illinois, Urbana, IL, Tech. Rep. R-285 (AD 632574), 1966.

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

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

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

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

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

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

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

[18] 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.

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

[20] 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.

Jung-Soo Chung received the B.S. and Ph.D. degrees from the Department of Electrical Engineering and Computer Science, Seoul National University, Seoul, Korea, in 2003 and 2010, respectively.

He is with the Department of Electrical Engineering and Computer Science, Seoul National University, Seoul, Korea. His research interests include pseudo-random sequences, error-correcting codes, and communications theory.

Jong-Seon No (S'80–M'88–SM'10) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988.

He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, from September 1990 to July 1999. He joined the faculty of the Department of Electrical Engineering and Computer Science, Seoul National University, in August 1999, where he is currently a Professor. His area of research interests includes error-correcting codes, sequences, cryptography, space-time codes, LDPC codes, and wireless communication systems.

Habong Chung (S'86–M'89) received the B.S. degree from Seoul National University, Seoul, Korea, in 1981 and the M.S. and the Ph.D. degrees from the University of Southern California, Los Angeles, in 1985 and 1988, respectively.

From 1988 to 1991, he was an Assistant Professor in the Department of Electrical and Computer Engineering, State University of New York at Buffalo. Since 1991, he has been with the School of Electronic and Electrical Engineering, Hongik University, Seoul, where he is a Professor. His research interests include coding theory, combinatorics, and sequence design.