REFERENCES

[1] R. G. Gallager, *Low Density Parity Check Codes*. Cambridge, MA: MIT Press, 1963.

[2] T. J. Richardson and R. Urbanke, "The capacity of low-density parity-check codes under message-passing algorithm," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[3] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, pp. 619–637, 2001.

[4] D. MacKay and M. Postol, "Weaknesses of margulis and ramanujan-margulis low-density parity check codes," *Electron. Notes Theoret. Comput. Sci.*, vol. 74, 2003.

[5] N. Wiberg, "Codes and Decoding on General Graphs," Ph.D. dissertation, Linköping University, Linköping, Sweden, 1996.

[6] J. K. Moura, J. Lu, and H. Zhang, "Structured LDPC codes with large girth," *IEEE Signal Proc. Mag.*, vol. 21, no. 1, pp. 42–55, Jan. 2004.

[7] C. Di *et al.*, "Finite length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, Jun. 2002.

[8] C. Wang, S. R. Kulkarni, and H. V. Poor, "Upper bounding the performance of arbitrary finite ldpc codes on binary erasure channels," in *Proc. Int. Symp. Inf. Theory*, Seattle, WA, USA, Jul. 9–14, 2006.

[9] T. J. Richardson, "Error floors of LDPC codes," in *Proc. 41st Annu. Allerton Conf. Commun., Contr. Comput.*, 2003.

[10] M. Stepanov and M. Chertkov, "Instanton analysis of low-density parity-check codes in the error-floor regime," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Seattle, WA, Jul. 9–14, 2006.

[11] Z. Zhang, L. Dolecek, B. Nikolić, V. Anantharam, and M. Wainwright, "Investigation of Error Floors of Structured Low- Density Parity-Check Codes by Hardware Emulation," presented at the Proc. IEEE GLOBECOM, San Francisco, CA, 2006.

[12] P. O. Vontobel and R. Koetter, Graph-Cover Decoding and Finite-Length Analysis of Message-Passing Iterative Decoding of Ldpc Codes [Online]. Available: http://www.arxiv.org/

[13] R. Smarandache and P. O. Vontobel, Pseudo-Codeword Analysis of Tanner Graphs from Projective and Euclidean Planes [Online]. Available: http://arxiv.org/

[14] R. Smarandache, A. E. Pusane, P. O. Vontobel, D. J. Costello, and Jr., Pseudo-Codeword Performance Analysis for LDPC Convolutional Codes [Online]. Available: http://arxiv.org/

[15] A. E. Pusane, R. Smarandache, P. O. Vontobel, and D. J. Costello Jr., "On deriving good LDPC convolutional codes from OC LDPC Block Codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 24–29, 2007, pp. 1221–1225.

[16] G. D. Forney, Jr., R. Koetter, F. R. Kschischang, and A. Reznik, "On the effective weights of pseudocodewords for codes defined on graphs with cycles," in *Codes, Systems, and Graphical Models*, B. Marcus and J. Rosenthal, Eds. New York: Springer Verlag, 2001, pp. 101–112.

[17] S. K. Chilappagari, S. Sankaranarayanan, and B. Vasic, "Error Floors of LDPC Codes on the Binary Symmetric Channel," presented at the Proc. Int. Conf. Commun., ICC 2006, Istanbul, Turkey, Jun. 2006.

[18] N. Varnica and M. Fossorier, "Improvements in belief-propagation decoding based on averaging information from decoder and correction of clusters of nodes," *IEEE Communications Letters*, vol. 10, no. 12, pp. 846–848, Dec. 2006.

[19] S. Laendner, T. Hehn, O. Milenković, and J. Huber, "When does one redundant parity-check equation matter?," presented at the Proc. IEEE GLOBECOM, San Francisco, CA, 2006.

[20] C. Wang, "Code annealing and the suppressing effect of the cyclically lifted LDPC code ensemble," presented at the 2006 IEEE Information Theory Workshop, Chengdu, China, Oct. 22–26, 2006, unpublished.

[21] R. M. Tanner, D. Sridhara, and T. Fuja, "A class of Group-Structured LDPC codes," *Proc. ISCTA*, 2001.

[22] J. Rosenthal and P. O. Vontobel, "Constructions of LDPC codes using ramanujan graphs and ideas from margulis," in *Proc. 38th Allerton Conf. Commun., Contr. Comput.*, 2000.

[23] D. J. C. MacKay, Encyclopedia of Sparse Graph Codes [Online]. Available: http://www.interference.phy.cam.ac.uk/mackay/codes/data.html

[24] J. Thorpe, Low Density Parity Check (LDPC) Codes Constructed from Protographs JPL INP Progress, Pasadena, CA, Rep. 42–154, Aug. 15, 2003.

[25] D. Divsalar and C. Jones, "Protgraph LDPC Codes with Node Degrees at Least 3," presented at the Proc. IEEE GLOBECOM, San Francisco, CA, 2006.

[26] C. Kelley, D. Sridhara, and J. Rosenthal, Tree-Based Construction of LDPC Codes Having Good Pseudocodeword Weights [Online]. Available: http://arxiv.org/

New Families of M-Ary Sequences With Low Correlation Constructed From Sidel'nikov Sequences

Young-Sik Kim, Jung-Soo Chung, Jong-Seon No, *Member, IEEE*, and Habong Chung, *Member, IEEE*

***Abstract*—In this correspondence, for a positive integer M and a prime p such that $M|p^n-1$, three families of M-ary sequences using the M-ary Sidel'nikov sequences with period p^n-1 are constructed. Two small families contain $\lceil (p^n-1)/2 \rceil + M - 2$ or $p^n + M - 3$ M-ary sequences, and both of their maximum magnitudes of correlation values are upper bounded by $2\sqrt{p^n}+6$. The largest family has its maximum magnitude of correlation values upper bounded by $3\sqrt{p^n}+5$ 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.**

***Index Terms*—Autocorrelation, cross-correlation, family of M-ary sequences, M-ary sequences, pseudonoise (PN) sequences, Sidel'nikov sequences.**

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.

For a prime p and a positive integer M such that $M|p-1$, Sidel'nikov [1] introduced the M-ary power residue sequences of period p with the magnitudes of out-of-phase autocorrelation values upper bounded by $\sqrt{5}$ or 3. For a positive integer M such that $M|p^n-1$, he also constructed M-ary sequences (called *Sidel'nikov sequences*) of period p^n-1, the out-of-phase autocorrelation magnitudes of which are upper bounded by 4 [1]. It is known that the autocorrelation distribution of M-ary Sidel'nikov sequences can be expressed in terms of the cyclotomic numbers of order M [2].

There have been many research results on the families of sequences with low correlation. Kasami sequence family [3]–[5], Gold sequence family [6], Trachtenberg [7], Sidel'nikov [8], Helleseth [9], bent sequence family [10], No sequence family [11], prime phase sequence family by Kumar and Moreno [12], family by Moriuchi and Imamura [13], and Helleseth–Gong sequence family [14] are well-known families of p-ary sequences with low correlation for a prime p. For the alphabet size of other than prime, Boztas, Hammons, and Kumar [15] proposed quaternary sequences with near-optimum cross-correlation properties. Kumar, Helleseth, Calderbank, and Hammons [16] constructed the large families of quaternary sequences with low cross correlation. For a prime p and an integer e, Kumar, Helleseth, and Calderbank [17] introduced the family of p^e-ary sequences on a Galois ring. Up to now, the alphabet sizes of the known families of sequences are restricted to prime power.

Manuscript received October 17, 2006; revised December 17, 2007. This work was supported by the MEST, the MKE, and the MOLAB, Korea, under the fostering project of the Laboratory of Excellency.

Y.-S. Kim is with Samsung Electronics, Co., Ltd., Yongin, Gyeonggi-do 446-711, Korea (e-mail: kingsi@ccl.snu.ac.kr).

J.-S. Chung and J.-S. No are with the Department of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea (e-mail: integer@ccl.snu.ac.kr; 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 G. Gong, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2008.926428

In this correspondence, for a positive integer M and a prime p such that $M|p^n-1$, three families of M-ary sequences using the M-ary Sidel'nikov sequences with period p^n-1 are constructed. Two small families contain $\lceil (p^n-1)/2\rceil+M-2$ or p^n+M-3 M-ary sequences, and both of their maximum magnitudes of correlation values are upper bounded by $2\sqrt{p^n}+6$. The largest family has its maximum magnitude of correlation values upper bounded by $3\sqrt{p^n}+5$ 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 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 $S_k, k=0,1,\ldots,M-1$, be the disjoint subsets of $F_{p^n}\backslash\{-1\}$ defined as

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

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: A multiplicative character $\psi_M(\cdot)$ of order M in F_{p^n} is defined as

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

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

From the above definition, it is obvious that

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

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]

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

where ω is a complex Mth 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 $f_1(z), f_2(z),\ldots,f_l(z)$ be l monic pairwise prime polynomials in $F_{p^n}[z]$ whose highest degree square-free divisors have degrees $d_1,d_2,\ldots,d_l$. Let $\chi_1,\chi_2,\ldots,\chi_l$ be nontrivial 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 $g(z)^{\mathrm{ord}(\chi_i)}$ in $F_{p^n}[z]$, where $\mathrm{ord}(\chi)$ 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

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

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

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

□

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 follows.

1) For the case of $p=2$

$$\mathcal{L}=\{v_{0,c_1}(t)|1\le c_1\le M-1\}\cup\{v_{i,c_1,c_2}(t)|1\le c_1,c_2\le M-1, 1\le i\le T-1\}. \tag{7}$$

2) For the case of odd prime p

$$\mathcal{L}=\{v_{0,c_1}(t)|1\le c_1\le M-1\}\cup\{v_{i,c_1,c_2}(t)|1\le c_1,c_2\le M-1, 1\le i\le T-1\}\cup\{v_{T,c_1,c_2}(t)|1\le c_1<c_2\le M-1\} \tag{8}$$

where $v_{0,c_1}(t)=c_1s(t)$ and $v_{i,c_1,c_2}(t)=c_1s(t)+c_2s(t+i)$ for $i\ne 0$. It is clear that the family size of $\mathcal{L}$ is $(M-1)^2T-(M-1)(M-2)$ for $p=2$ or $(M-1)^2T-(M-1)(M-2)/2$ for an odd prime p. In the rest of this correspondence, 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, because 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

$$\begin{aligned}\omega^{v_{i,c_1,c_2}(t)}&=\omega^{c_1s(t)+c_2s(t+i)}\\&=[\psi^{c_1}(\alpha^t+1)+\omega^{c_1k_0}I(\alpha^t+1)]\\&\quad\times[\psi^{c_2}(\alpha^{t+i}+1)+\omega^{c_2k_0}I(\alpha^{t+i}+1)]\\&=\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\\&\quad+\omega^{c_1k_0}I(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\\&\quad+\omega^{c_2k_0}I(\alpha^{t+i}+1)\psi^{c_1}(\alpha^t+1)\end{aligned} \tag{9}$$

where $\psi(\cdot)$ is $\psi_M(\cdot)$ defined in Definition 2. 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

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

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

$$\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} [\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1) + \omega^{c_1 k_0} I(\alpha^t+1) \\
&\qquad \times \psi^{c_2}(\alpha^{t+i}+1) + \omega^{c_2 k_0} I(\alpha^{t+i}+1)\psi^{c_1}(\alpha^t+1)] \\
&\quad \times [\psi^{-c_1'}(\alpha^{t+\tau}+1)\psi^{-c_2'}(\alpha^{t+j+\tau}+1) \\
&\qquad + \omega^{-c_1' k_0} I(\alpha^{t+\tau}+1)\psi^{-c_2'}(\alpha^{t+j+\tau}+1) \\
&\qquad + \omega^{-c_2' k_0} I(\alpha^{t+j+\tau}+1)\psi^{-c_1'}(\alpha^{t+\tau}+1)] \\
&= \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) \\
&\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}$$

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

The first summation in (10) is given as

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

From Theorem 3, we have

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

The second summation in (10) is given as

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

The third summation in (10) is given as (13) shown at the bottom of the page. The fourth summation in (10) is given as

$$\begin{aligned}
&\omega^{c_1 k_0} \sum_{t=0}^{p^n-2} \psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_1'}(\alpha^{t+\tau}+1)\psi^{-c_2'}(\alpha^{t+j+\tau}+1) \\
&\quad \times I(\alpha^t+1) = \omega^{c_1 k_0} \psi^{c_2}(1-\alpha^i)\psi^{-c_1'}(1-\alpha^\tau)\psi^{-c_2'}(1-\alpha^{j+\tau}) \\
&\quad = \begin{cases} 0, & \text{if } \tau = 0 \text{ or } \tau = -j \\ \omega^{c_1 k_0} \psi\left(\frac{(1-\alpha^i)^{c_2}}{(1-\alpha^\tau)^{c_1'}(1-\alpha^{j+\tau})^{c_2'}}\right), & \text{otherwise.} \end{cases}
\end{aligned} \qquad (14)$$

The fifth summation in (10) is given as

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

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

$$= \begin{cases} 0, & \text{if } \tau = -j \text{ or } \tau = i-j \\ \omega^{-c_2' k_0} \psi\left(\frac{(1-\alpha^{-j-\tau})^{c_1}(1-\alpha^{i-j-\tau})^{c_2}}{(1-\alpha^{-j})^{c_1'}}\right), & \text{otherwise.} \end{cases} \qquad (13)$$

TABLE I
MAGNITUDES OF EACH TERM IN (10)

Term	$\tau=0$	$\tau=i$	$\tau=-j$	$\tau=i-j$	otherwise
1st	$\le 3\sqrt{p^n}+1$				
2nd	0	0	≤ 1	≤ 1	≤ 1
3rd	≤ 1	≤ 1	0	0	≤ 1
4th	0	≤ 1	0	≤ 1	≤ 1
5th	≤ 1	0	0	0	0
6th	0	0	≤ 1	0	0
7th	≤ 1	0	≤ 1	0	≤ 1
8th	0	≤ 1	0	0	0
9th	0	0	0	≤ 1	0
Sum	$\le 3\sqrt{p^n}+4$	$\le 3\sqrt{p^n}+4$	$\le 3\sqrt{p^n}+4$	$\le 3\sqrt{p^n}+4$	$\le 3\sqrt{p^n}+5$

The sixth summation in (10) is given as

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

The seventh summation in (10) is given as (17) shown at the bottom of the page. The eighth summation in (10) is given as

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

The ninth summation in (10) is given as

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

Magnitudes of each term in (10) are tabulated in Table I. Thus, we have

$$|C(\tau)|=\begin{cases}|(11)+(13)+(15)+(17)|\le 3\sqrt{p^n}+4, & \text{if } \tau=0\\ |(11)+(13)+(14)+(18)|\le 3\sqrt{p^n}+4, & \text{if } \tau=i\\ |(11)+(12)+(14)+(19)|\le 3\sqrt{p^n}+4, & \text{if } \tau=i-j\\ |(11)+(12)+(16)+(17)|\le 3\sqrt{p^n}+4, & \text{if } \tau=-j\\ |(11)+(12)+(13)+(14)+(17)|\le 3\sqrt{p^n}+5, & \text{otherwise.}\end{cases}$$

Thus, we have

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

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

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

The first summation in (20) is given as

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

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

TABLE II
MAGNITUDES OF EACH TERM IN (20)

Term	$\tau=0$	$\tau=i$	otherwise
1st	$2\sqrt{p^n}+1$		
2nd	0	≤ 1	≤ 1
3rd	≤ 1	0	≤ 1
4th	0	0	≤ 1
5th	≤ 1	0	0
6th	0	≤ 1	0
Sum	$\le 2\sqrt{p^n}+3$	$\le 2\sqrt{p^n}+3$	$\le 2\sqrt{p^n}+4$

From Theorem 3, the above sum is upper bounded by $2\sqrt{p^n}+1$. The second summation in (20) is given as

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

The third summation in (20) is given as

$$\omega^{c_2k_0}\sum_{t=0}^{p^n-2}\psi^{-c_1'}(\alpha^{t+\tau}+1)\psi^{c_1}(\alpha^{t}+1)I(\alpha^{t+i}+1)=\begin{cases}0, & \text{if } \tau=i\\ \omega^{c_2k_0}\psi^{-c_1'}(1-\alpha^{\tau-i})\psi^{c_1}(1-\alpha^{-i}), & \text{otherwise.}\end{cases}$$

The fourth summation in (20) is given as

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

The fifth summation in (20) is given as

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

The sixth summation in (20) is given as

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

Magnitudes of each term in (20) are tabulated in Table II. 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. □

By selecting some subset in the large family $\mathcal{L}$ in (8), we can construct a small family with better correlation property than $\mathcal{L}$. Let

$$\mathcal{S}_{c_1}=\{v_{0,c}(t)|1\le c\le M-1\}\cup\{v_{i,c_1,c_1}(t)|1\le i\le T-1\} \quad (21)$$

for $1\le c_1\le M-1$. The family S_{c_1} contains $T+M-2$ sequences and it can be shown that the maximum correlation magnitude is upper bounded by $2\sqrt{p^n}+6$ in Theorem 5.

We can also construct another family with better correlation property than $\mathcal{L}$ by fixing c_1 and c_2 in $\mathcal{L}$ but enlarging the range of i instead. Let

$$\mathcal{S}_{c_1,c_2}=\{v_{0,c}(t)|1\le c\le M-1\}\cup\{v_{i,c_1,c_2}(t)|1\le i\le p^n-2\} \quad (22)$$

for $1\le c_1\ne c_2\le M-1$. The maximum correlation magnitude for S_{c_1,c_2} is also upper bounded by $2\sqrt{p^n}+6$, but it contains p^n+M-3 sequences, which has almost double size of S_{c_1}.

Theorem 5: The magnitudes of the correlation values of two sequences in either of the small families $\mathcal{S}_{c_1}$ and $\mathcal{S}_{c_1,c_2}$ are upper bounded by

$$|C(\tau)|\le 2\sqrt{p^n}+6.$$

Proof: We will prove only for $\mathcal{S}_{c_1,c_2}$. The case of $\mathcal{S}_{c_1}$ can be done similarly. By the same way as in the proof of Theorem 4, for $i\ne j, i\ne 0$, and $j\ne 0$, we can obtain (10) with the replacement of c_1' and c_2' by c_1 and c_2, respectively. Then, for nonzero $i\ne j$, we only have to consider the first summation in (10) as follows. If $\tau=0$, then the first summation in (10) becomes

$$\begin{aligned}&\sum_{t=0}^{p^n-2}\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_1}(\alpha^t+1)\psi^{-c_2}(\alpha^{t+j}+1)\\ &=\sum_{t=0,t\ne\frac{p^n-1}{2}-j}^{p^n-2}\psi^{c_2}\left(\frac{\alpha^{t+i}+1}{\alpha^{t+j}+1}\right)\\ &=\sum_{z\in F_{p^n}}\psi^{c_2}(z)-\psi^{c_2}(1)-\psi^{c_2}(\alpha^{i-j})\\ &=-\psi^{c_2}(1)-\psi^{c_2}(\alpha^{i-j}).\end{aligned}$$

If $\tau=i-j$, then the first summation in (10) becomes

$$\begin{aligned}&\sum_{t=0}^{p^n-2}\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_1}(\alpha^{t+i-j}+1)\psi^{-c_2}(\alpha^{t+i}+1)\\ &=\sum_{t=0,t\ne\frac{p^n-1}{2}-i+j}^{p^n-2}\psi^{c_1}\left(\frac{\alpha^{t}+1}{\alpha^{t+i-j}+1}\right)\\ &=\sum_{z\in F_{p^n}}\psi^{c_1}(z)-\psi^{c_1}(1)-\psi^{c_1}(\alpha^{j-i})\\ &=-\psi^{c_1}(1)-\psi^{c_1}(\alpha^{j-i}).\end{aligned}$$

If $\tau=i$, from Theorem 3, the first summation in (10) becomes

$$\begin{aligned}&\left|\sum_{t=0}^{p^n-2}\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\right.\\ &\qquad\left.\times\ \psi^{-c_1}(\alpha^{t+i}+1)\psi^{-c_2}(\alpha^{t+i+j}+1)\right|\\ &=\left|\sum_{t=0,t\ne\frac{p^n-1}{2}-i}^{p^n-2}\psi^{c_1}(\alpha^t+1)\psi^{c_2-c_1}(\alpha^{t+i}+1)\right.\\ &\qquad\left.\times\ \psi^{-c_2}(\alpha^{t+i+j}+1)\right|\le 2\sqrt{p^n}+2.\end{aligned}$$

If $\tau=-j$, the first summation in (10) becomes

$$\begin{aligned}&\left|\sum_{t=0}^{p^n-2}\psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_1}(\alpha^{t-j}+1)\psi^{-c_2}(\alpha^t+1)\right|\\ &=\left|\sum_{t=0,t\ne\frac{p^n-1}{2}}^{p^n-2}\psi^{c_1-c_2}(\alpha^t+1)\psi^{-c_1}(\alpha^{t-j}+1)\psi^{c_2}(\alpha^{t+i}+1)\right|\\ &\le 2\sqrt{p^n}+2.\end{aligned}$$

Otherwise, the first summation in (10) can be rewritten as

$$\begin{aligned}
&\sum_{t=0}^{p^n-2} \psi^{c_1}(\alpha^t+1)\psi^{c_2}(\alpha^{t+i}+1)\psi^{-c_1}(\alpha^{t+\tau}+1)\psi^{-c_2}(\alpha^{t+j+\tau}+1)\\
&\quad=\sum_{z\in F_{p^n}} \psi^{c_1}(z+1)\psi^{c_2}(\alpha^i z+1)\\
&\qquad\times \psi^{-c_1}(\alpha^\tau z+1)\psi^{-c_2}(\alpha^{j+\tau} z+1)-1\\
&\quad=\sum_{z\in F_{p^n}\setminus\{-\alpha^{-\tau},-\alpha^{-j-\tau}\}} \psi^{c_1}\left(\frac{z+1}{\alpha^\tau z+1}\right)\psi^{c_2}\left(\frac{\alpha^i z+1}{\alpha^{j+\tau} z+1}\right)-1\\
&\quad=\sum_{x\in F_{p^n}\setminus\{0,1-\alpha^{-j}\}} \psi^{c_1}\left(\frac{x+\alpha^\tau-1}{\alpha^\tau x}\right)\psi^{c_2}\left(\frac{\alpha^{i-\tau}(x-1)+1}{\alpha^j(x-1)+1}\right)-1\\
&\quad=\sum_{y\in F_{p^n}\setminus\left\{0,\frac{\alpha^j}{\alpha^j-1}\right\}} \psi^{c_1}\left(\left(\frac{\alpha^\tau-1}{\alpha^\tau}\right)y+\frac{1}{\alpha^\tau}\right)\\
&\qquad\times \psi^{c_2}\left(\frac{\alpha^{i-\tau}(1-y)+y}{\alpha^j(1-y)+y}\right)-1\\
&\quad=A\left[\sum_{y\in F_{p^n}\setminus\left\{0,\frac{\alpha^j}{\alpha^j-1}\right\}} \psi^{c_1}\left(y+\frac{1}{\alpha^\tau-1}\right)\right.\\
&\qquad\left.\times\ \psi^{c_2}\left(y+\frac{\alpha^i}{\alpha^\tau-\alpha^i}\right)\times\psi^{-c_2}\left(y+\frac{\alpha^j}{1-\alpha^j}\right)\right]-1\\
&\quad=A\left[\sum_{y\in F_{p^n}} \psi^{c_1}\left(y+\frac{1}{\alpha^\tau-1}\right)\psi^{c_2}\left(y+\frac{\alpha^i}{\alpha^\tau-\alpha^i}\right)\right.\\
&\qquad\left.\times\ \psi^{-c_2}\left(y+\frac{\alpha^j}{1-\alpha^j}\right)\right]-\psi(\alpha^{-\tau})\psi^{c_2}(\alpha^{i-j-\tau})-1 \qquad (23)
\end{aligned}$$

where $A=\psi^{c_1}(\frac{\alpha^\tau-1}{\alpha^\tau})\psi^{c_2}(\frac{1-\alpha^{i-\tau}}{1-\alpha^j})$, $x=\alpha^\tau z+1$, and $y=1/x$. Let

$$B=A\left[\sum_{y\in F_{p^n}} \psi^{c_1}\left(y+\frac{1}{\alpha^\tau-1}\right)\times\psi^{c_2}\left(y+\frac{\alpha^i}{\alpha^\tau-\alpha^i}\right)\psi^{-c_2}\left(y+\frac{\alpha^j}{1-\alpha^j}\right)\right].$$

Since $\chi_1(\cdot)=\psi^{c_1}(\cdot)$, $\chi_2(\cdot)=\psi^{c_2}(\cdot)$, and $\chi_3(\cdot)=\psi^{-c_2}(\cdot)$ are nontrivial multiplicative characters in F_{p^n} and $f_1(y)=y+\frac{1}{\alpha^\tau-1}$, $f_2(y)=y+\frac{\alpha^i}{\alpha^\tau-\alpha^i}$, and $f_3(y)=y+\frac{\alpha^j}{1-\alpha^j}$ are three monic pairwise prime polynomials in $F_{p^n}[y]$ whose highest degree square-free divisors have degree one, the above summation B in the first term is upper bounded from Theorem 3 by

$$\begin{aligned}
|B|&=\left|\sum_{y\in F_{p^n}} \psi^{c_1}\left(y+\frac{1}{\alpha^\tau-1}\right)\right.\\
&\qquad\left.\times\ \psi^{c_2}\left(y+\frac{\alpha^i}{\alpha^\tau-\alpha^i}\right)\psi^{-c_2}\left(y+\frac{\alpha^j}{1-\alpha^j}\right)\right|\\
&=\left|\sum_{y\in F_{p^n}} \chi_1(f_1(y))\chi_2(f_2(y))\chi_3(f_3(y))\right|\\
&\le(1+1+1-1)\sqrt{p^n}=2\sqrt{p^n}. \qquad (24)
\end{aligned}$$

Then, we have

$$|C_{ij}(\tau)|=\begin{cases}
|(23)+(13)+(15)+(17)|\le 2\sqrt{p^n}+5, & \text{if } \tau=0\\
|(23)+(13)+(14)+(18)|\le 2\sqrt{p^n}+5, & \text{if } \tau=i\\
|(23)+(12)+(14)+(19)|\le 2\sqrt{p^n}+5, & \text{if } \tau=i-j\\
|(23)+(12)+(16)+(17)|\le 2\sqrt{p^n}+5, & \text{if } \tau=-j\\
|(23)+(12)+(13)+(14)+(17)|\le 2\sqrt{p^n}+6, & \text{otherwise.}
\end{cases}$$

For $i=j\neq 0$ or $j=0$ and $i\neq 0$, we can similarly prove that the upper bound is $2\sqrt{p^n}+6$. □

Note that achieving the upper bounds in Theorems 4 and 5 is impossible for odd M. Even for even M, it seems quite rare.

Some known families of sequences are listed in Table III. No claim is made that the list in Table III is exhaustive. The following examples give the families of quaternary and 8-ary sequences, respectively.

Example 6: 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

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

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

Example 7: For $M=8, p=5$, and $n=4$, we can construct a family of 8-ary sequences of period $N=624$. Let $s(t)$ be an 8-ary Sidel'nikov sequence. Then, the family $\mathcal{S}_{2,3}$ contains 630 sequences as

$$\mathcal{S}_{2,3}=\{s(t),2s(t),\ldots,7s(t)\}\cup\{2s(t)+3s(t+i)|1\le i\le 623\}.$$

Although the magnitude of cross-correlation values of sequences in $\mathcal{L}$ is upper bounded by $2\times 25+6=56$ from Theorem 5, but the actual maximum magnitude shows 55.3 from exhaustive search. □

Remark 1: The proposed families of M-ary sequences are not optimal with respect to any of Welch, Sidel'nikov, and Levenshtein bounds.

Remark 2 (Generalized Construction): Note that the proposed construction of the sequence family can be generalized as

$$u_{\mathbf{i}}(t)=c_0 s(t)+c_1 s(t+i_1)+c_2 s(t+i_2)+\cdots+c_n s(t+i_n)\bmod M$$

where $\mathbf{i}=(i_1,i_2,\ldots,i_n)$. It is not difficult to derive that the cross-correlation magnitude between $u_{\mathbf{i}}(t)$ and $u_{\mathbf{j}}(t)$ is upper bounded by $(2n+1)p^{n/2}+(n+2)^2$.

IV. Symbol Balancedness of Proposed M-ary Sequence Families

In the M-ary sequence, $u_i(t)=c_1 s(t)+c_2 s(t+i)$, some of the symbols may not occur if $\gcd(c_1,c_2)$ is not relatively prime to M. Otherwise, all of M symbols in an alphabet occur. The Sidel'nikov sequence $s(t)$ is balanced when $k_0=0$. Then, what can we say about the symbol balancedness of the sequence in our family?

In the case when $\gcd(c_1,c_2,M)=1$, we can derive the lower and upper bounds of the number of occurrences of a given symbol. Let $N_j, 0\le j\le M-1$, be the number of occurrences of each symbol j in one period of a sequence. Then, we can determine the bound of N_j's as follows.

Theorem 8: Let $\gcd(c_1,c_2,M)=1$. Then, we have

$$\frac{p^n-1}{M}-\frac{(M-1)(p^{n/2}+1)}{M}\le N_j\le\frac{p^n-1}{M}+\frac{(M-1)(p^{n/2}+1)}{M}.$$

TABLE III
PARAMETERS OF SOME KNOWN FAMILIES OF SEQUENCES

Family	alphabet	period N	family size	$C_{\max}$
Kasami [3]–[5]	p	p^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
Gold (n odd) [6]	2	2^n-1	$N+2$	$\sqrt{2(N+1)}+1$
Gold (n even) [6]	2	2^n-1	$N+2$	$2\sqrt{(N+1)}+1$
Trachtenberg [7]	odd p	p^n-1	$N+1$	$\sqrt{p(N+1)}+1$
Sidel'nikov [8]	odd p	p^n-1	$N+1$	$\sqrt{N+1}+1$
Helleseth [9]	odd p	p^n-1	$N+1$	$2\sqrt{N+1}+1$
Bent [10]	p	p^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
No [11]	2	2^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
Kumar and Moreno [12]	odd p	p^n-1	$N+1$	$\sqrt{N+1}+1$
Moriuchi and Imamura [13]	odd p	p^n-1	$\sqrt{N+1}$	$\sqrt{N+1}+1$
Helleseth and Gong [14]	odd p	p^n-1	$N+1$	$\sqrt{N+1}+1$
$S(0)$ [16]	4	2^n-1	$N+2$	$\sqrt{N+1}+1$
$S(1)$ [16]	4	2^n-1	$\geq N^2+3N+2$	$2\sqrt{N+1}+1$
$S(2)$ [16]	4	2^n-1	$\geq N^3+4N^2+5N+2$	$4\sqrt{N+1}+1$
KHC ($N_e=2$) [17]	4	2^n-1	$N+1$	$\sqrt{N}+1$
KHC ($N_e=3$), odd n [17]	4	2^n-1	N^2+3N+3	$2\sqrt{N}+1$
KHC ($N_e=3$), even n [17]	4	2^n-1	N^2+3N+2	$2\sqrt{N}+1$
KHC ($N_e=4$), odd n [17]	8	2^n-1	N^3+4N^2+6N+4	$3\sqrt{N}+1$
KHC ($N_e=4$), even n [17]	8	2^n-1	N^3+4N^2+6N+3	$3\sqrt{N}+1$
KHC ($N_e=5$) [17]	8	2^n-1	$\geq (N+1)^4$	$4\sqrt{N}+1$
$\mathcal{S}_{c_1}$	M	p^n-1	$\lceil \frac{N}{2} \rceil + M-2$	$2\sqrt{N+1}+6$
$\mathcal{S}_{c_1,c_2}$	M	p^n-1	$N+M-2$	$2\sqrt{N+1}+6$
$\mathcal{L}$ ($p=2$)	M	2^n-1	$(M-1)^2(2^{n-1}-1)+M-1$	$3\sqrt{N+1}+6$
$\mathcal{L}$ (p odd prime)	M	p^n-1	$(M-1)^2\frac{(N-2)}{2}+\frac{M(M-1)}{2}$	$3\sqrt{N+1}+6$

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

Proof: Since ω is a complex Mth root of unity, we have

$$\sum_{a=0}^{M-1} \omega^{a(u_i(t)-j)} = \begin{cases} 0, & \text{if } u_i(t) \neq j \\ M, & \text{if } u_i(t) = j. \end{cases}$$

Thus, we have

$$\begin{aligned} N_j &= \frac{1}{M} \sum_{t=0}^{p^n-2} \sum_{a=0}^{M-1} \omega^{a(u_i(t)-j)} \\ &= \frac{1}{M} \left(\sum_{t=0}^{p^n-2} \sum_{a=1}^{M-1} \omega^{a(u_i(t)-j)} + p^n - 1 \right) \\ &= \frac{p^n-1}{M} + \frac{1}{M} \sum_{a=1}^{M-1} \sum_{t=0}^{p^n-2} \omega^{a(u_i(t)-j)}. \end{aligned} \tag{25}$$

For $a \neq 0$, from Theorem 3, we have

$$\begin{aligned} \left| \omega^{-ja} \sum_{t=0}^{p^n-2} \omega^{a u_i(t)} \right| &= \left| \sum_{z \in F_{p^n}} \psi^a(z+1)\psi^a(\alpha^i z+1) - 1 \right| \\ &\leq p^{n/2}+1. \end{aligned} \tag{26}$$

From (25) and (26), we have

$$|MN_j - p^n + 1| \leq (M-1)(p^{n/2}+1).$$

□

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," Coordinated Science Lab., Univ. Illinois, Urbana, IL, Tech. Rep. R-285 (AD 632574), Apr. 1966.

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

[5] S.-C. Liu and J. F. Komo, "Nonbinary Kasami sequences over $GF(p)$," *IEEE Trans. Inf. Theory*, vol. 38, no. 4, pp. 1409–1412, Jul. 1992.

[6] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions," *IEEE Trans. Inf. Theory*, vol. IT-14, no. 1, pp. 154–156, Jan. 1968.

[7] H. M. Trachtenberg, "On the cross-correlation functions of maximal recurring sequences," Ph.D. dissertation, Dept. Electr. Eng., Univ. 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. IT-28, no. 6, 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, no. 2, 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, no. 3, 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, no. 2, 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," *Math. Comput.*, vol. 66, no. 219, pp. 1195–1212, Jul. 1997.