Punctured Sidelnikov Sequences with Better Correlation Properties

Min Hyung Lee, Gangsan Kim, and Hong-Yeop Song*

School of Electrical and Electronic Engineering
Yonsei University, Seoul, Korea
{mhlee95, gs.kim, hysong}@yonsei.ac.kr

Abstract

Let q be a power of a prime and let k be a divisor of $q-1$. We propose a construction of an almost-polyphase (punctured) sequence set of size $k-1$ and of period $q-1$ using a k-ary Sidelnikov sequence of period $q-1$. We prove that the out-of-phase autocorrelation magnitude of the sequences in the set is upper-bounded by 2 and the crosscorrelation magnitude is upper bounded by $\sqrt{q}+1$.

1 Introduction

In code-division multiple-access (CDMA) communication systems, the signature sequences must have good autocorrelation and crosscorrelation properties. [1] Most of the research on sequences, therefore, have focused on the low out-of-phase autocorrelation property as well as their low crosscorrelation properties.

The binary m-sequences is well-known to have the ideal autocorrelation [2]. The polyphase Power Residue sequences (PRS) and Sidelnikov sequences were initially proposed to have very good autocorrelation property [3]. Kim *et. al.* in 2007 proposed a family consisting of a Sidelnikov sequence and its all possible constant mulptiples, and showed that the out-of-phase autocorrelation magnitude of the sequences in the set is upper-bounded by 4 and the crosscorrelation magnitude is upper bounded by $\sqrt{q}+3$ [4]. Later, some families using Sidelnikov sequences (and/or PRS sequences) were constructed with good autocorrelation and crosscorrealtion properties [5, 6, 7, 8, 9].

Shi *et. al.* proposed in 2019 punctured polyphase PRS sequences of period p by replacing a single term of 1 with 0, and showed that the maximum autocorrelation magnitude is reduced (in fact, from 3 to 1) [15]. The resulting sequences are polyphase and contain some zero (not zero phase, which corresponds to 1). These sequences are sometimes called "almost-polyphase." We note that the terms "almost-polyphase" and "punctured polyphase" can be used interchangeably.

*This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government.

In this paper, we have applied the similar technique [15] to a k-ary Sidelnikov sequence of period $q-1$ and all its constant multiples [4], and now we report the result is interesting enough. Let q be a power of a prime and let k be a divisor of $q-1$. We propose a construction of an almost-polyphase sequence set of size $k-1$ and of period $q-1$ using a k-ary Sidelnikov sequence of period $q-1$. We prove that the out-of-phase autocorrelation magnitude of the sequences in the set is upper-bounded by 2 (reduced from 4) and the crosscorrelation magnitude is upper bounded by $\sqrt{q}+1$ (reduced from $\sqrt{q}+3$).

We will introduce almost-polyphase sequences and some basic notions in Section 2, and present the main result in Section 3. We conclude the paper in Section 4 with some interesting discussion and a conjecture.

2 Sidelnikov sequences

We fix the following notation throughout the paper.

- p is an odd prime number.
- $q = p^m$ is an odd prime power, with positive integer m.
- $\mathbf{F}_q$ is the finite field of size q, and μ is a primitive element of $\mathbf{F}_q$.
- k is a positive divisor of $q-1$.
- $\mathbf{Z}_k$ is the set of integers mod k.

Definition 1 ([3])**.** Let $q = kf+1$ for some positive integers k, f, and

$$D_0 = \{\mu^{kl} \mid l = 0, 1, ..., f-1\},$$

be the set of all the powers of μ^k in $\mathbf{F}_q$, where μ is a primitive element of $\mathbf{F}_q$. For $i = 0, 1, , ..., k-1$, we let $D_i = \mu^i D_0$. Then a k-ary Sidelnikov sequence $\mathbf{s}$ of period $q-1$ is defined as

$$s(n) = \begin{cases} 0 & \text{if } \mu^n + 1 = 0, \\ i & \text{if } \mu^n + 1 \in D_i. \end{cases}$$

The k-ary Sidelnikov sequence $\mathbf{s}$ defined in Definition 1 is a phase sequence. Let $\omega = e^{j\frac{2\pi}{k}}$ be a complex primitive k-th root of unity, then we can transform $\mathbf{s}$ to complex polyphase sequence $\mathbf{t}$ whose n-th term is given as

$$t(n) = \omega^{s(n)}, \qquad n = 0, 1, 2, ... \tag{1}$$

Let c be a positive integer such that $1 \le c \le k-1$. We can multiply the constant c to k-ary Sidelnikov sequence $\mathbf{s}$ so that the n-th term of the result is $c \cdot s(n)$. The corresponding complex polyphase sequence is denoted by $\mathbf{t}_c$ and its n-th term is given as

$$t_c(n) = \omega^{c \cdot s(n)}, \qquad n = 0, 1, 2, ... \tag{2}$$

Alternatively, the sequence $t_c(n)$ is obtained by using ω^c instead of ω from $\mathbf{s}$.

The k-ary sidelnikov sequence $\mathbf{s}$ in Definition 1 can be conveniently represented by the following function, called Power Residue function from $\mathbf{F}_q$ to $\mathbf{Z}_k$.

Definition 2. Let q, k, μ, D_i be as given in *Definition 1.* We define a **Power Residue** function $g : \mathbf{F}_q \mapsto \mathbf{Z}_k$ as follows:

$$g(x) = \begin{cases} 0 & \text{if } x = 0, \\ i & \text{if } x \in D_i. \end{cases}$$

Now, we can represent the k-ary Sidelnikov sequences $\mathbf{s}$ of period $q-1$ as follows:

$$s(n) = g(\mu^n + 1), \qquad n = 0, 1, 2, ...$$

Since μ has order $q-1$, we have $\mu^{\frac{q-1}{2}} = -1$. Therefore,

$$s\left(\frac{q-1}{2}\right) = g(0) = 0,$$

and hence,

$$t\left(\frac{q-1}{2}\right) = \omega^0 = 1. \tag{3}$$

The following properties of Sidelnikov sequence $\mathbf{s}$ is well-known.

Lemma 3 (Correlation of Sidelnikov Sequences [4])**.** *Let* $\mathbf{s}$ *be a* k*-ary Sidelnikov sequence of period* $q-1$ *as defined in Definition 1 and* $\mathbf{t}_c$ *be a complex polyphase sequence given in* (2)*. Then the following holds:*

(i) For any $\tau \neq 0$*, and an integer* c*, with* $1 \leq c \leq k-1$*, the autocorrelation of* $\mathbf{t}_c$ *is given as follows:*

$$\begin{aligned} R_{\mathbf{t}_c}(\tau) &= \sum_{x=0}^{q-2} t_c(x+\tau) t_c(x)^* \\ &= -\omega^{c \cdot g(\mu^\tau)} - 1 + \omega^{c \cdot g(-\mu^\tau + 1)} + \omega^{-c \cdot g(-\mu^{-\tau} + 1)}. \end{aligned}$$

Therefore,

$$|R_{\mathbf{t_c}}(\tau)| \leq 4.$$

(ii) Let a, b *are integers with* $1 \leq a \neq b \leq k-1$*. The crosscorrelation of* $\mathbf{t}_a$ *and* $\mathbf{t}_b$ *is given as follows:*

If $\tau = 0$*,*

$$C_{\mathbf{t}_a, \mathbf{t}_b}(0) = 0.$$

If $\tau \neq 0$,

$$C_{\mathbf{t}_a,\mathbf{t}_b}(\tau) = \omega^{a\cdot g(-\mu^\tau+1)} + \omega^{b\cdot g(-\mu^{-\tau}+1)} + \sum_{x\in\mathbf{F}_q\setminus\{0,-1,-\mu^{-\tau}\}} \omega^{a\cdot g(\mu^\tau x+1)-b\cdot g(x+1)}.$$

This leads to

$$|C_{\mathbf{t}_a,\mathbf{t}_b}(\tau)| \leq \sqrt{q}+3.$$

3 Main Result

Definition 4. Let $\mathbf{s}$ be a k-ary Sidelnikov sequence of period $q-1$ defined in Definition 1 and $\omega = e^{j\frac{2\pi}{k}}$.

(i) The almost-polyphase sequence $\mathbf{t}^+$ is defined as

$$t^+(n) = \begin{cases} 0, & \text{if } n = \frac{q-1}{2}, \\ \omega^{s(n)} & \text{otherwise.} \end{cases}$$

(ii) For a positive integer c such that $1 \leq c \leq k-1$, almost-polyphase sequence $\mathbf{t}_c^+$ is defined as

$$t_c^+(n) = \begin{cases} 0, & \text{if } n = \frac{q-1}{2}, \\ \omega^{c\cdot s(n)} & \text{otherwise.} \end{cases}$$

(iii) Almost-polyphase sequence set T of size $k-1$ is defined as

$$T = \{\mathbf{t}_c^+ \mid c = 1, 2, ..., k-1\}.$$

Note that the family T above consists exactly of a sidelnikov sequence and all its constant multiples with the term at position $(q-1)/2$ punctured to be zero.

Theorem 5. *Let* $\mathbf{t}_c^+$ *be defined in Definition 4. The magnitude of autocorrelation of* $\mathbf{t}_c^+$ *is upper bounded by 2, i.e.*

$$|R_{\mathbf{t}_c^+}(\tau)| \leq 2.$$

Proof. Assume $\tau \neq 0$,

$$\begin{aligned} R_{\mathbf{t}_c^+}(\tau) &= \sum_{x=0}^{q-2} t_c^+(x+\tau)t_c^+(x)^* \\ &= R_{\mathbf{t}_c}(\tau) - t_c\left(\frac{q-1}{2}+\tau\right)t_c\left(\frac{q-1}{2}\right)^* \\ &\quad - t_c\left(\frac{q-1}{2}\right)t_c\left(\frac{q-1}{2}-\tau\right)^*. \end{aligned}$$

By (3), $\mu^{\frac{q-1}{2}} = -1$, $t_c(\frac{q-1}{2}) = 1$ for any c. Using the result of Lemma 3-(i),

$$R_{\mathbf{t}_c^+}(\tau) = R_{\mathbf{t}_c}(\tau) - \omega^{c\cdot g(-\mu^\tau+1)} - \omega^{-c\cdot g(-\mu^{-\tau}+1)}$$

$$= -\omega^{c\cdot g(\mu^\tau)} - 1.$$

Therefore,

$$|R_{\mathbf{t}_\mathbf{c}^+}(\tau)| \le 2.$$

□

Theorem 6. *Let T be the set of almost-polyphase sequence of size $k-1$ defined in Definition 4. For any $\mathbf{t}_a^+$ and $\mathbf{t}_b^+$ in T with $1 \le a \ne b \le k-1$, the crosscorrelation magnitude of the almost-polyphase sequences $\mathbf{t}_a^+$ and $\mathbf{t}_b^+$ is upper-bounded by $\sqrt{q}+1$, i.e.,*

$$|C_{\mathbf{t}_a^+,\mathbf{t}_b^+}| \le \sqrt{q}+1.$$

Proof. Assume $\tau = 0$,

$$C_{\mathbf{t}_a^+,\mathbf{t}_b^+}(0) = C_{\mathbf{t}_a,\mathbf{t}_b}(0) - t_a\left(\frac{q-1}{2}\right)t_b\left(\frac{q-1}{2}\right)^*$$
$$= -1.$$

Assume $\tau \ne 0$,

$$C_{\mathbf{t}_a^+,\mathbf{t}_b^+}(\tau) = C_{\mathbf{t}_a,\mathbf{t}_b} - t_a\left(\frac{q-1}{2}+\tau\right)t_b\left(\frac{q-1}{2}\right)^*$$
$$-t_a\left(\frac{q-1}{2}\right)t_b\left(\frac{q-1}{2}-\tau\right)^*.$$

By (3), $\mu^{\frac{q-1}{2}} = -1$, $t_c(\frac{q-1}{2}) = 1$ for any c. Using the result of Lemma 3-(ii),

$$C_{\mathbf{t}_a^+,\mathbf{t}_b^+}(\tau) = C_{\mathbf{t}_a,\mathbf{t}_b}(\tau) - \omega^{a\cdot g(-\mu^\tau+1)} - \omega^{b\cdot g(-\mu^{-\tau}+1)}$$

$$= \sum_{x\in\mathbf{F}_q\setminus\{0,-1,-\mu^{-\tau}\}} \omega^{a\cdot g(\mu^\tau x+1)-b\cdot g(x+1)}. \tag{4}$$

From Lemma 3, the magnitude of (4) is upper-bounded by $\sqrt{q}+1$. Therefore,

$$|C_{\mathbf{t}_a^+,\mathbf{t}_b^+}| \le \sqrt{q}+1.$$

□

Table 1: Max. Correlation when a single 1 on n_1-th position is replaced with 0

n_1	Max Autocorr.	n_1	Max Autocorr.
0	5.950	**364**	**2.000**
28	5.177	392	5.441
56	5.569	420	5.493
84	5.509	448	5.435
112	5.531	476	5.653
140	5.817	504	5.769
168	5.200	532	5.638
196	5.638	560	5.200
224	5.769	588	5.817
252	5.653	616	5.531
280	5.435	644	5.509
308	5.493	672	5.569
336	5.441	700	5.177

4 Conclusion and some discussion

In this paper, we propose a construction of an almost-polyphase sequence set T of size $k-1$ and of period $q-1$ by replacing a single term of 1 with 0 from the complex polyphase sequence $\mathbf{t}_c$ corresponding to the phase sequence given by the k-ary Sidelnikov sequence. The member sequences of T have better correlation properties (than those given in [4]): the out-of-phase autocorrelation magnitude is upper-bounded by 2 and the crosscorrelation magnitude of any two sequences is upper-bounded by $\sqrt{q}+1$.

The proofs of the main results depends heavily on those of [4] and the imporvement seems to be marginal. Here, the key technique is to choose a single term of 1 at some position n_1 and replace it with 0. We suspect this technique may apply to a single term of 1 at ANY position of the sequence $\mathbf{t}_c$. However, it turned out that it is not true in general. What is even more surprising is that, for some sequences, there exists ONLY one position of the sequence such that the technique essentially improves the correlation property.

To show this case, we choose $q-1 = 3^6 - 1 = 728 = 28 \times 26$ and $k = 28$. Now, the sequence $\mathbf{s}$ is a 28-ary Sidelnikov sequence of period 728, and the sequence $\mathbf{t}_c$ is a polyphase sequence given by $t_c(n) = \omega^{cs(n)}$ for $n = 0, 1, ..., 727$, where ω is a complex primitive 28-th root of unity. The results are shown in Table 1. Here, the value is the maximum autocorrelation magnitude of the sequences when the single term of 1 at position n_1 is replaced with 0. Observe that there is ONLY one position that essentially improves the

autocorrelation property, i.e., $n_1 = (q-1)/2 = 364$ which is shown in bold, corresponding to the proposed sequences $\mathbf{t}_c^+$ in Definition 4.

We suspect that this might happen for all other k-ary Sidelnikov sequences, which is a topic of future study. That is, we conjecture the following: for any k-ary Sidelnikov sequence of period $q-1$, puncturing a single term 1 into 0 will not improve the correlation property unless the punctured position is $(q-1)/2$.

References

[1] P. Z. Fan, M. Darnell, *Sequence design for communications applications,* Exter: John Wiley & Sons Inc., 1996.

[2] S.W. Golomb, Shift register sequences, CA, Holden-Day, San Francisco, 1967; 2nd edition, Aegean Park Press, Laguna Hills, CA, 1982; 3rd edition, World Scientific, Hackensack, NJ, 2017.

[3] V. M. Sidelnikov, "Some k-valued Pseudo-Random Sequences and Nearly Equidistance Codes," *Problemy Peredachi Informatsil,* Vol. 5, No. 1, pp.16-22, 1969.

[4] Y.-J. Kim and H.-Y. Song, "Cross correlation of Sidelnikov sequences and their constant multiples," *IEEE Trans. Inf. Theory,* vol. 53, no. 3, pp. 1220-1224, Mar. 2007.

[5] Y.-S. Kim, J.-S. Chung, J.-S. No, and H. Chung, "New families of M-ary sequences with low correlation constructed from Sidelnikov sequences," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3768-3774, Aug. 2008.

[6] N. Y. Yu and G. Gong, "New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 4061-4070, Aug. 2010.

[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.-T. Kim, D. S. Kim, and H.-Y. Song, "New M-ary sequence families with low correlation from the array structure of Sidelnikov sequences," *IEEE Tans. Inf. Theory*, vol. 61, no. 1, pp. 655-670, Jan. 2015.

[9] Min Kyu Song and Hong-Yeop Song, "Correlation of column sequences from the arrays of Sidelnikov sequences of different periods," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E102-A, no. 10, pp. 1333-1339, Oct. 2019.

[10] E I. Krengel, "Some Constructions of Almost-Perfect, Odd-Perfect and Perfect Polyphase and Almost-Polyphase Sequences," *SETA 2010,* Sep. 2010.

[11] H.D. Luke, H.D. Schotten, "Odd-perfect, almost binary correlation sequences," *IEEE Trans. Aerospace and Electronic Systems,* Sep. 2010.

[12] A. Ali, E. Ali, A. Habib, Nadim, T. Kusaka, Y. Nogami, "Pseudo Random Ternary Sequence and Its Autocorrelation Property Over Finite Field," *International Journal of Computer Network and Information Security,* vol.11, no. 9, Sep. 2017.

[13] M. K. Song, H-Y. Song, "A generalized Milewski construction for perfect sequences," *Sequences and Their Applications (SETA 2018),* Oct. 2018.

[14] M. K. Song, G. Kim, H-Y. Song, "Punctured Bent Function Sequences for Watermarked DS-CDMA," *IEEE Comm. Letters,* vol. 23, no. 7, July. 2019.

[15] X. Shi, X. Zhu, X. Huang and Q. Yue, "A Family of M -Ary σ -Sequences With Good Autocorrelation," *IEEE Comm. Letters,* vol. 23, no. 7, pp. 1132-1135, May. 2019.