Polyphase Sequences with Almost Perfect Autocorrelation and Optimal Crosscorrelation

2020 KICS-NA Workshop

Hong-Yeop Song
hysong@yonsei.ac.kr

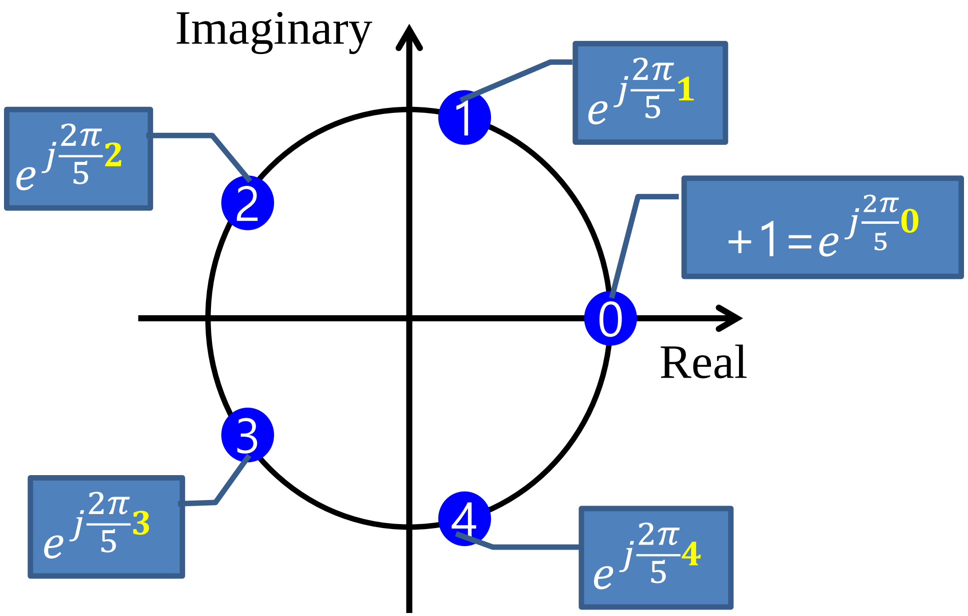
YONSEI UNIVERSITY, SEOUL, KOREA

Contents

- Introduction
- Some historical reviews on
  - the design of polyphase sequences family with GOOD (complex) correlation properties based on **Sidelnikov sequences** of period $q-1$
  - the design of polyphase sequences family with GOOD (complex) correlation properties based on **Partial Residue sequences** of period p (**another type of Sidelnikov sequences**)
- Recent development on **Partial Residue sequences**
- Main Result on **Sidelnikov sequences**
- Some discussion and Conclusion

Polyphase sequences

Alphabet of a polyphase sequence



$\{x(n)\}_{n=0}^{L-1}$ be ***k*-ary polyphase sequences** of length L

$\Updownarrow$

$x(n)$ belongs to the integers mod ***k*** for each $n = 0,1,\ldots$

Equivalent representations

A complex-valued polyphase sequence

$$e^{j\frac{2\pi}{5}1},\ e^{j\frac{2\pi}{5}3},\ e^{j\frac{2\pi}{5}0},\ e^{j\frac{2\pi}{5}2},\ e^{j\frac{2\pi}{5}4},\ldots$$

$\Updownarrow$

1, 3, 0, 2, 4, …

Corresponding **phase sequence** over the integers **modulo 5**

Correlation of sequences

- Let $\boldsymbol{x} = \{x(n)\}_{n=0}^{L-1}$ and $\boldsymbol{y} = \{y(n)\}_{n=0}^{L-1}$ be two ***k*-ary polyphase sequences** of length L. (over the integers mod $\boldsymbol{k}$)
- The (periodic) correlation between $\boldsymbol{x}$ and $\boldsymbol{y}$ at time shift τ is computed over the complex:

$$\mathrm{C}_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{n=0}^{L-1} \omega^{x(n)} \left(\omega^{y(n+\tau)}\right)^* = \sum_{n=0}^{L-1} \omega^{x(n)-y(n+\tau)}$$

where $\omega = e^{-j\frac{2\pi}{k}}$ is a complex primitive k-th root of unity.

  - It is called autocorrelation if $\boldsymbol{y} = \boldsymbol{x}$.
  - It is called cross-correlation **otherwise.**

In the beginning

- (Sidelnikov-69) Sidelnikov introduced two different types of non-binary (k-ary polyphase) sequences with

  very good non-trivial autocorrelation (ONLY)

  - **Power Residue sequences** (PRS in short) **of period p**
  - **Sidelnikov sequences of period $q-1$**

  ✓ V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, pp. 12-16, 1969.

- (Lempel-Cohn-Eastman-77) re-discovered binary "Sidelnikov sequences" of period $q-1$

  ✓ A. Lempel, M. Cohn, and W.L. Eastman, "A class of binary sequences with optimal **autocorrelation** properties," *IEEE* Trans. *Inform. Theory,* vol. *23,* No. 1, pp. 38-42, Jan. 1977.

Cosets of k-th powers in F_q^*

- p = odd prime, $q = p^m$ and F_q = finite field of size q
- μ = primitive element of F_q
- k is a divisor of $q-1$ so that $q = kf + 1$ for some f
- Coset Partition
  - ✓ D_0 = set of k-th powers in F_q^*

    $$= \{\mu^{k0} = 1,\ \mu^{2k},\ \mu^{3k},\ \dots,\ \mu^{(f-1)k}\}$$
  - ✓ $D_i = \mu^i D_0$ for $i = 0,1,\dots,k-1$

    $$= \{\mu^{k0+i} = \mu^i, \mu^{2k+i}, \mu^{3k+i}, \dots, \mu^{(f-1)k+i}\}$$
- Well-known that

$$F_q^* = \bigcup_{i=0}^{k-1} D_i \quad \text{is a disjoint union}$$

and

$$|D_i| = f \ \text{ for all } i = 0,1,\dots,k-1.$$

Example

- Let $q = 13$ and the finite field $F_q = F_{13}$ has $\mu = 2$ *(primitive)* since

$$\{\mu^n | n = 1,2,\dots,11,12\}$$
$$= \{\mu^1, \mu^2, \mu^3, \mu^4, \dots, \mu^{12}\}$$
$$= \{2,4,8,3,6,12,11,9,5,10,7,1\} = F_{13}^*$$

- A divisor $k = 3$ of $q - 1 = 12 = 3 \times 4$ with $f = 4 = (q-1)/k$

and $$D_0 = \{2^3, 2^{3\cdot 2}, 2^{3\cdot 3}, 2^{3\cdot 4}\} = \{8,\ 12,\ 5,\ 1\}$$

is the set of all the k-th (3rd) powers of F_{13}^*.

- All its cosets are

$$D_0 = 2^0 D_0 = \{\mathbf{8, 12,\ 5,\ 1}\}$$
$$D_1 = 2^1 D_0 = \{\mathbf{3, 11, 10,\ 2}\}$$
$$D_2 = 2^2 D_0 = \{\mathbf{6,\ 9,\ 7,\ 4}\}$$

each of size $f = 4$, and

$F_{13}^* = D_0 \cup D_1 \cup D_2$ is a disjoint union

Two sequences from Sidelnikov

- Let p must be an **odd prime** and $q = p^m$
  - Let $k \geq 2$ be a **divisor** of $q-1$
  - Let μ be a primitive element of F_q^*
  - D_0 = set of all the k-th powers of F_q^* (for Sidel S)
  - $D_i = \mu^i D_0$ = coset of D_0 for $i = 0,1,\ldots,k-1$

- A k-ary power residue sequence (PRS) of **period $q = p$**

  ($q = p$ =prime):

$$s(n) = \begin{cases} 0, & \textbf{if} \quad n = 0 \\ i, & \textbf{if} \quad n \in D_i \end{cases}$$

- A k-ary sidelnikov sequence of **period $q-1$**

  ($q - 1 = p^m - 1$ = one less than a prime or a power of a prime)

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

$p = q = 13$ *and* $\boldsymbol{k} = \mathbf{3}$

- $D_0 = 2^0 D_0 = \{8, 12, 5, 1\}$
- $D_1 = 2^1 D_0 = \{3, 11, 10, 2\}$
- $D_2 = 2^2 D_0 = \{6, 9, 7, 4\}$

- A k-ary PR S of period p:

$$s(n) = \begin{cases} 0, & \textbf{if} \quad n = 0 \\ i, & \textbf{if} \quad n \in D_i \end{cases}$$

- A k-ary Sidel. sequence of period $q-1$:

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

$\boldsymbol{n}$	0	1	2	3	4	5	6	7	8	9	10	11	12
PRS	0	0	1	1	2	0	2	2	0	2	1	1	0
μ^n	1	2	4	8	3	6	12	11	9	5	10	7	
μ^n+1	2	3	5	9	4	7	0	12	10	6	11	8	
Sidel S	1	1	0	2	2	2	0	0	1	2	1	0	X
$\log_\mu (\mu^n+1)$	1	4	9	8	2	11	*	11	10	5	7	3	X
$\log_\mu (\mu^n+1)$ **mod 3**	1	1	0	2	2	2	0	0	1	2	1	0	X

equivalent presentation: $s(n) = \log_\mu (\mu^n+1) \bmod \boldsymbol{k}$ - **GONG-10**

QUESTIONs

Can we construct a set of sequences with

GOOD cross-correlation

as well as

GOOD non-trivial autocorrelation

from any of these sequences?

Up until 2006, **only** the **autocorrelation** properties of these sequences are known (original paper Sidelnikov-69):

The non-trivial autocorrelation magnitude is upper bounded by 3 (for PRS) or 4 (for Sidel. sequences).

First Attempt (2006-2007)

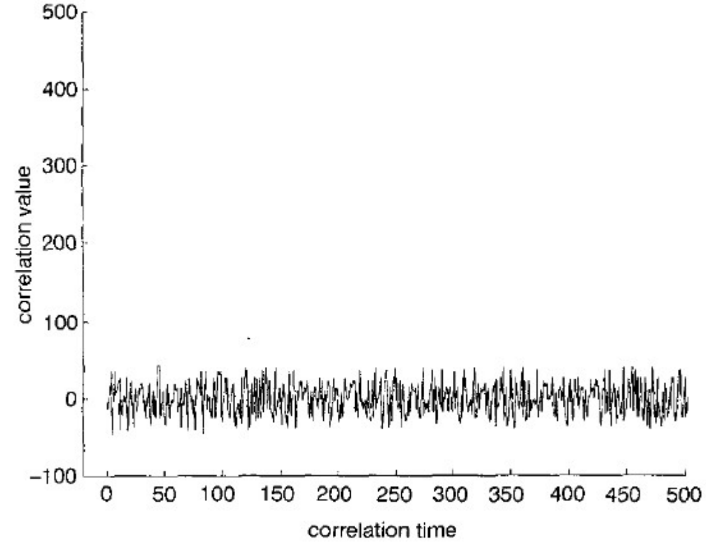
- Construct a family from a given sequence by changing the primitive element in the definition.
- It turned out that the same family can be obtained by multiplying a constant term-by-term.
- Results are
  - PRS (period p): **Song-06** (ISIT)
    - $Max \leq \sqrt{p} + 2$

      Crosscorrelation of q-ary power residue sequences of period p
  - SS (period q-1): **Song-07** (IT Trans.)
    - $Max \leq \sqrt{q} + 3$

      Crosscorrelation of Sidel'nikov Sequences and Their Constant Multiples
- Note that the size of the family is $k-1$ for k-ary sequences. It is only $\varphi(k)$ when we need to maintain k distinct values.

An improvement begins by some observations and a conjecture

- Z. Guohua and Z. Quan, "Pseudonoise codes constructed by Legendre sequence," IEE Electronic Letters, vol. 38, no. 8, pp. 376-377, 2002.
- The technique of shift-and-add (as in the construction of GOLD sequences using an m-sequence) is introduced.
- They used a Legendre sequence and the technique of shift-and-add to construct a family with good crosscorrelation, where the crosscorrelation is (conjectured to be) upper bounded by $4\lfloor 2\sqrt{p}/4 \rfloor + 1$



It is proved by Rushanan at ISIT-06

- J. Rushanan, "Weil Sequences: A Family of Binary Sequences with Good orrelation Properties," *Proc. of IEEE Int. Symp. Information Theory(ISIT2006)*, Seattle, WA, USA, July 2006.

- Crosscorrelation of the sequence family containing a Legendre sequence and its shift-and-add sequences is upper bounded by $\mathbf{2\sqrt{p}+5}$.

- Major Technique:

quartic polynomial (product of 4 linear polynomials)

$$\left|\sum_{x=0}^{p-1}\left(\frac{(x+a_1)\cdots(x+a_4)}{p}\right)\right| \le 2\sqrt{p}+1$$

quadratic character

Results of No-Chung/Yang/Gong (2008-2010)

Shift-and-add techniques

to construct larger family of sequences from a Sidelnikov sequence or a power-residue sequence

➕

Weil Bound on character sums

to prove crosscorrelation bound of the family constructed

Sidelnikov sequences only

- **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**.

Both Sidelnikov sequences and PRS

- **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**.
- **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**.

Note that the size of the family becomes $\approx \boldsymbol{kq/2}$ for $\boldsymbol{k}$-ary sequences of period $\boldsymbol{q-1}$.

Array structure of Sidelnikov sequences

For a k-ary **Sidelnikov sequence** $s(t)$ of period $\boldsymbol{q^d - 1}$, make an array as

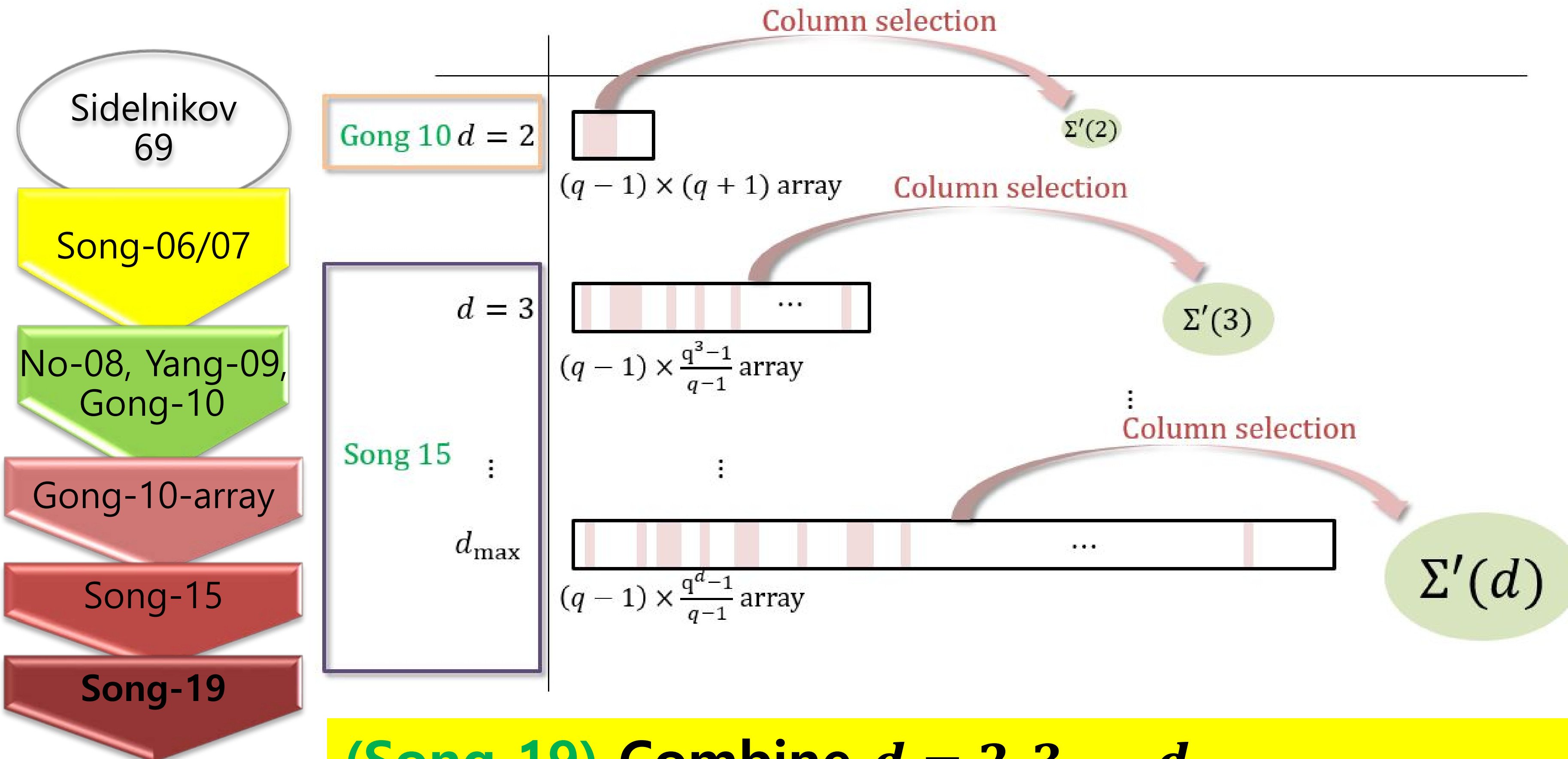
$$\begin{pmatrix} s(0) & s(1) & \cdots & s(\frac{q^d-1}{q-1}-1) \\ s(\frac{q^d-1}{q-1}) & s(\frac{q^d-1}{q-1}+1) & \cdots & s(2\times\frac{q^d-1}{q-1}-1) \\ \vdots & \vdots & \ddots & \vdots \\ s((q-2)\times\frac{q^d-1}{q-1}) & s((q-2)\times\frac{q^d-1}{q-1}+1) & \cdots & s(q^d-2) \end{pmatrix}$$

and **choose some columns** to construct a set of k-ary sequences of period $\boldsymbol{q-1}$.

(Gong 10) when $\boldsymbol{d = 2}$
(Song 15) when $\boldsymbol{3 \le d < \sqrt{q}/2}$ with $q \geq 27$

The **family size** now becomes $\approx \boldsymbol{kq^d/d}$

Array structure of **Sidelnikov sequences**



(Song 19) Combine $d = 2, 3, \dots, d_{max}$,

The **family size** now becomes $\approx k \sum q^d / d$

References

1) P. Z. Fan, M. Darnell, Sequence design for communications applications, 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 Sidel'nikov 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, October 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.