Polyphase Sequences with Almost Perfect Autocorrelation and Optimal Crosscorrelation

2020 Information Theory and Applications Workshop

Hong-Yeop Song

hysong@yonsei.ac.kr

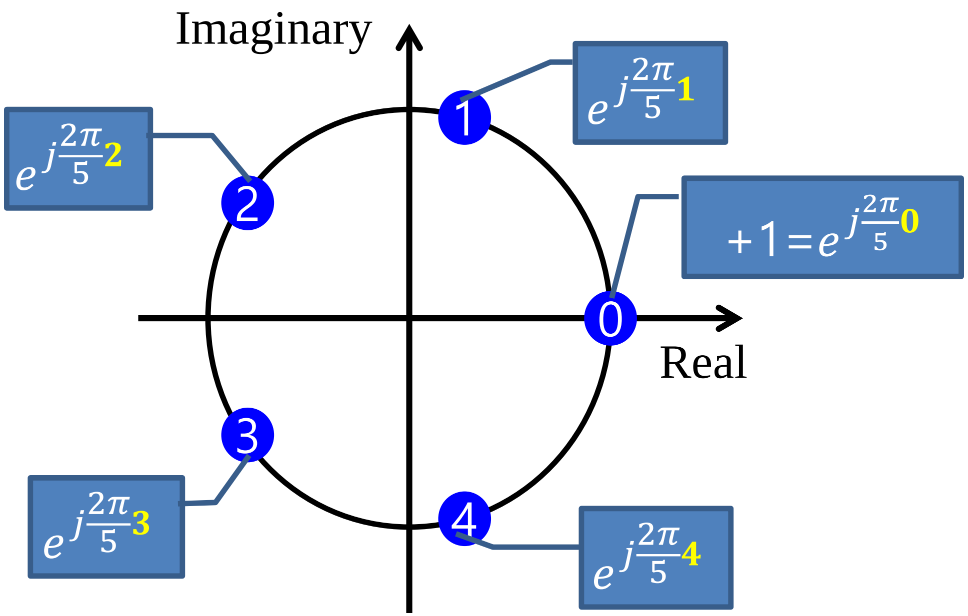
YONSEI UNIVERSITY, SEOUL, KOREA

Contents

- Introduction to Sidelnikov sequences
  - ✓ There are two different types, now called **Sidelnikov sequences** and **Power Residue sequences**
- Historical Review on the construction for polyphase sequences family with good correlation property
  - ✓ Original paper only discusses **only their autocorrelation properties**
- Main contribution (very brief)
  - ✓ Almost-polyphase sequences

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 $\boldsymbol{k}$ 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 **$\boldsymbol{k}$-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

- **Power Residue sequences** (PRS in short) **of period p**
  - Max non-trivial autocorrelation magnitude ≤ 3
- **Sidelnikov sequences of period $q-1$**
  - Max non-trivial autocorrelation magnitude ≤ 4

✓ 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 $q-1$

Cosets of k-th powers in F_q^*

- $p =$ odd prime, $q = p^m$ and $F_q =$ finite field of size q
- $\mu =$ 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

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

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^*
  - $D_i = \mu^i D_0$ = 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)

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

Examples - continued

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

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

- A k-ary PR S of period p:

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

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

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

$\boldsymbol{n}$	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

QUESTION

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)

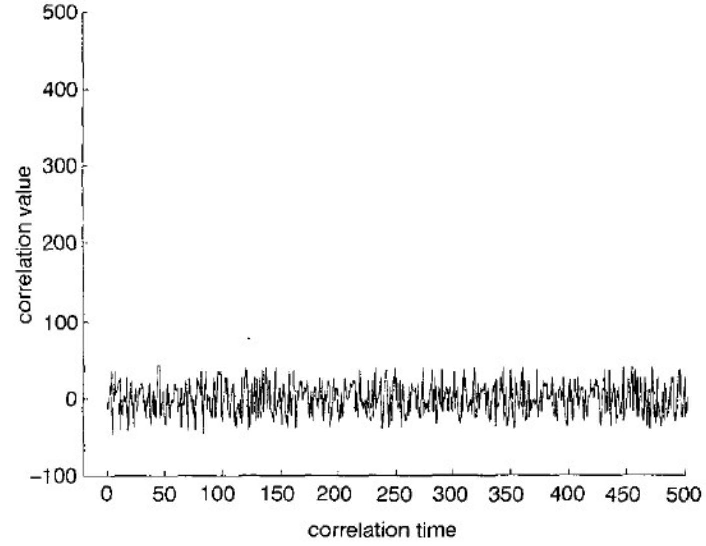
- Construct a family from a given sequence by changing the primitive element in the definition.
- It turned out that the same family can be obtained by multiplying a constant term-by-term.
- Results are
  - PRS (period p): **Song-06** (ISIT)
    - $Max \leq \sqrt{p} + 2$

      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 $\boldsymbol{k-1}$ for $\boldsymbol{k}$-ary sequences. It is only $\boldsymbol{\varphi(k)}$ 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

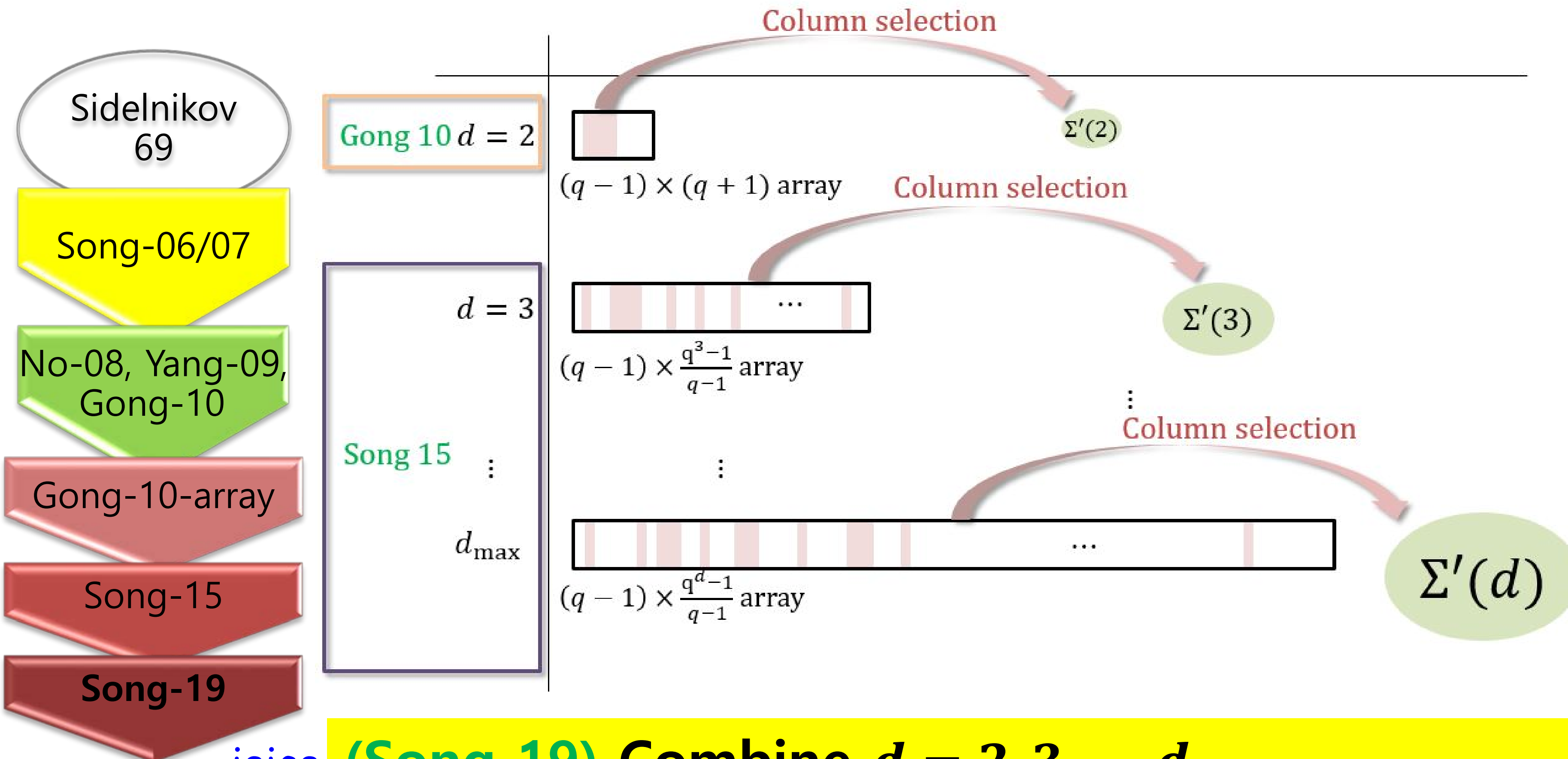
$$\begin{pmatrix} s(0) & s(1) & \cdots & s(\frac{q^d-1}{q-1}-1) \\ s(\frac{q^d-1}{q-1}) & s(\frac{q^d-1}{q-1}+1) & \cdots & s(2\times\frac{q^d-1}{q-1}-1) \\ \vdots & \vdots & \ddots & \vdots \\ s((q-2)\times\frac{q^d-1}{q-1}) & s((q-2)\times\frac{q^d-1}{q-1}+1) & \cdots & s(q^d-2) \end{pmatrix}$$

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 $q \ge 27$

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

Array structure of **Sidelnikov sequences**



ieice

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

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

MAIN CONTRIBUTION

PRS with single ZERO

In 2019, **Xiaoping Shi et al** proposed an **almost-polyphase** sequence of period p, by **replacing a single term of 1 to zero from PRS.**

X. Shi et al, "A family of M-ary σ-sequences with good autocorrelation," ***IEEE Comm. Letters***, vol. 23, no. 7, pp. 1132-1135, May. **2019**.

Key Contribution:

The **max autocorrelation magnitude** of this sequence is **reduced from 3 to 1.**

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

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

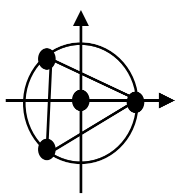
- A k-ary PR S of period p:

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

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

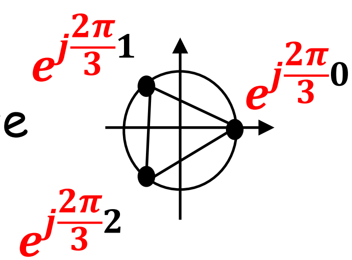
$$s(n) = \begin{cases} 0, & \text{if } \mu^n + 1 = 0 \\ i, & \text{if } \mu^n + 1 \in D_i \end{cases}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12
PRS (phase)	**0**	0	1	1	2	0	2	2	0	2	1	1	0
complex	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}0}$



Almost-polyphase

polyphase



Shi et al (2019)	**0**	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}0}$

Main Contribution

- We have applied **similar technique to a k-ary Sidelnikov sequences** of period $q-1$ and all its constant multiples.
- We can make a sequence set of size $k-1$ with better correlation properties in both **auto** and **cross-correlation**.

	Auto	Cross	alphabet
Sidelnikov	4	$\sqrt{q}+3$	k-ary polyphase
Proposed Seq. set	2	$\sqrt{q}+1$	k-ary polyphase and ZERO

Proof is almost the same as those in **Song-2007**

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

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

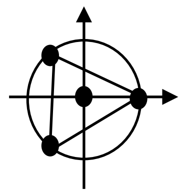
- A k-ary PR S of period p:

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

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

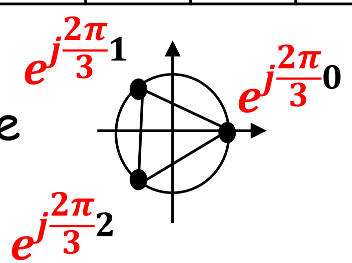
$$s(n) = \begin{cases} \mathbf{0}, & \textbf{if} \quad \boldsymbol{\mu^n + 1 = 0} \\ i, & \text{if} \quad \mu^n + 1 \in D_i \end{cases}$$

n	0	1	2	3	4	5	6	7	8	9	10	11	
Sidel S	1	1	0	2	2	2	**0**	0	1	2	1	0	X
complex	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}0}$	X



Almost-polyphase

polyphase



Song (2020)	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}2}$	**0**	$e^{j\frac{2\pi}{3}0}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}2}$	$e^{j\frac{2\pi}{3}1}$	$e^{j\frac{2\pi}{3}0}$	X

Some Discussion

We suspect that the main result is an easy (and almost trivial) consequence of replacing the value $\mathbf{1 = e^{j\frac{2\pi}{k}0}}$ (phase 0) at **only one position** with the value **0** (not phase 0).

Question:
Could we have the same result if we replace the value $\mathbf{1 = e^{j\frac{2\pi}{k}0}}$ at **ANY one position** with the value **0** ?

The answer is NO.

Some Discussion

- For an experiment, we choose $q-1=3^6-1=728=28\times 26.$
- We construct a 28-ary Sidelnikov sequence $\{s(n)\}$ of period 728.
- We multiply a constant 2 to every term: $\{2s(n)\}$
- Complex polyphase sequence $\{\omega^{2s(n)}\}$ of period 728
- The table shows that **the maximum autocorrelation magnitude** of the sequences when **the single term** of **1 at position n_1** is replace with **0** from this sequence

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

Some Discussion

Conjecture.

This happens for all other k-ary Sidelnikov sequences.

That is,

Replacing a value 1 with 0 will reduce the max autocorrelation magnitude ONLY when the position is $(q-1)/2$.

Some Discussion

The conjecture was confirmed for **all odd prime powers** q with $1000 \leq q \leq 10000$ and **all the divisors** $\boldsymbol{k}$ of $q-1$ and **constants** $\boldsymbol{c}$ **from 2 to** $\boldsymbol{k-1}$.

We have just completed the proof!
(4 days ago)

Theorem:

The change of no other single element with the value 0 will reduce the max non-trivial autocorrelation magnitude **unless the position is** $\boldsymbol{(q-1)/2}$.

q		
3^7	37^2	71^2
3^8	41^2	73^2
5^5	43^2	79^2
7^4	47^2	83^2
11^3	53^2	89^2
13^3	59^2	97^2
17^3	61^2	
19^3	67^2	

Summary

- **A k-ary Sidelnikov sequence and all its constant multiples** (of period $q-1$) will have a **slightly better correlation performance** (both autocorrelation and crosscorrelation) when the single term **at the position $(\boldsymbol{q}-\mathbf{1})/\mathbf{2}$** is replaced with the value 0.

- No other position will work for the same improvement at all (for Sidelnikov sequences).

- **Conjecture:**

  We guess that the same is true for PRS sequences.