Punctured Sidelnikov Sequences with Better Correlation Properties

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

Channel Coding Lab.

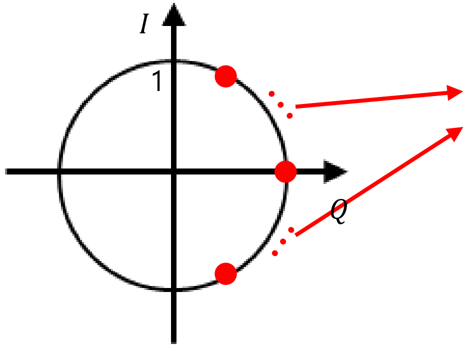
Yonsei University
{gs.kim, hysong}@yonsei.ac.kr

Contents

Polyphase sequence

A sequence consisting of **Roots of unity**

$e^{j\frac{2\pi a_1}{N}}$	$e^{j\frac{2\pi a_2}{N}}$	$e^{j\frac{2\pi a_3}{N}}$	$\cdots$	$e^{j\frac{2\pi a_{L-2}}{N}}$	$e^{j\frac{2\pi a_{L-1}}{N}}$	$e^{j\frac{2\pi a_L}{N}}$



$N-\text{th}$ roots of unity

$$e^{j\frac{2\pi a_i}{N}}, \qquad a_i \in Z_N$$

Perfect sequence

Even-periodic autocorrelation value is always 0

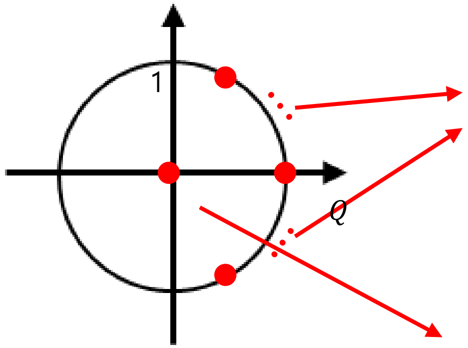
- **Zadoff-Chu sequence**
- **Frank sequence**
- **Milewski sequence**
- **Popovic sequence**

Well-known polyphase sequence with good correlation property

- **M-sequence**
  Even-periodic autocorrelation value is always 1
- **Sidelnikov sequence**
  Even-periodic autocorrelation value is upperbounded by 4
  Even-periodic crosscorrelation value is upperbounded by $\sqrt{L}+2$
- **Power Residue sequence**
  Even-periodic autocorrelation value is upperbounded by 3
  Even-periodic crosscorrelation value is upperbounded by $\sqrt{L+1}+3$

Almost-polyphase sequence

$e^{j\frac{2\pi b_1}{N}}$	0	$e^{j\frac{2\pi b_3}{N}}$	$\cdots$	0	$e^{j\frac{2\pi b_{L-1}}{N}}$	$e^{j\frac{2\pi b_L}{N}}$



$N-$th roots of unity

$e^{j\frac{2\pi a_i}{N}}, \qquad a_i \in Z_N$

Zero

A sequence consisting of
Roots of unity and **zero**

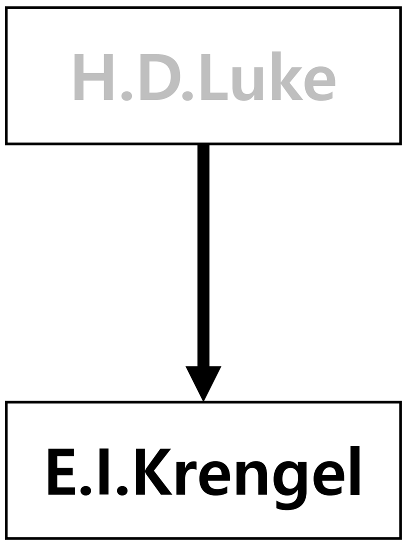
History of almost-polyphase sequence

H.D.Luke

- Odd-perfect sequence is created by putting 0 instead of the complex binary symbol at **one specific position** in the **complex binary sequence** (2003)
- First use of the word **'Almost-binary sequence'**

H.D. Luke, H.D. Schotten, "Odd-perfect almost binary correlation sequences". IEEE Trans. Aerosp. Electron. Syst. 31, 495–498 (1996)

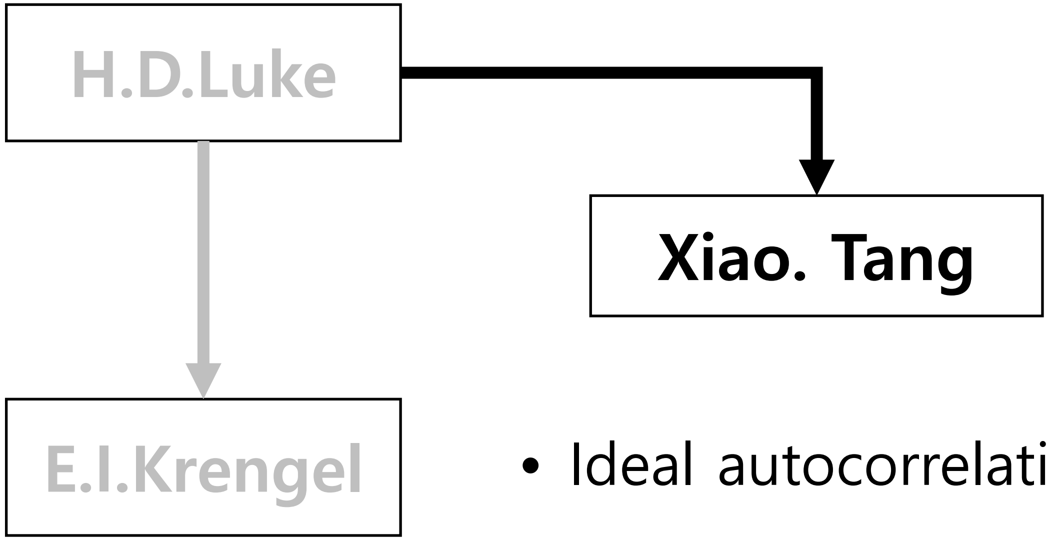
History of almost-polyphase sequence



- Almost perfect sequence is created by putting 0 instead of the complex symbol at **some specific positions** in the **polyphase sequence** (2010)
- First use of the word **‘Almost-polyphase sequence**’

E I. Krengel, ”Some Constructions of Almost-Perfect, Odd-Perfect and Perfect Polyphase and Almost-Polyphase Sequences,” SETA 2010, Sep.2010.

History of almost-polyphase sequence



- Ideal autocorrelation sequence is created by putting 0 instead of the complex symbol at **one specific position** in the **complex 2, 4-ary sequence** (2009)

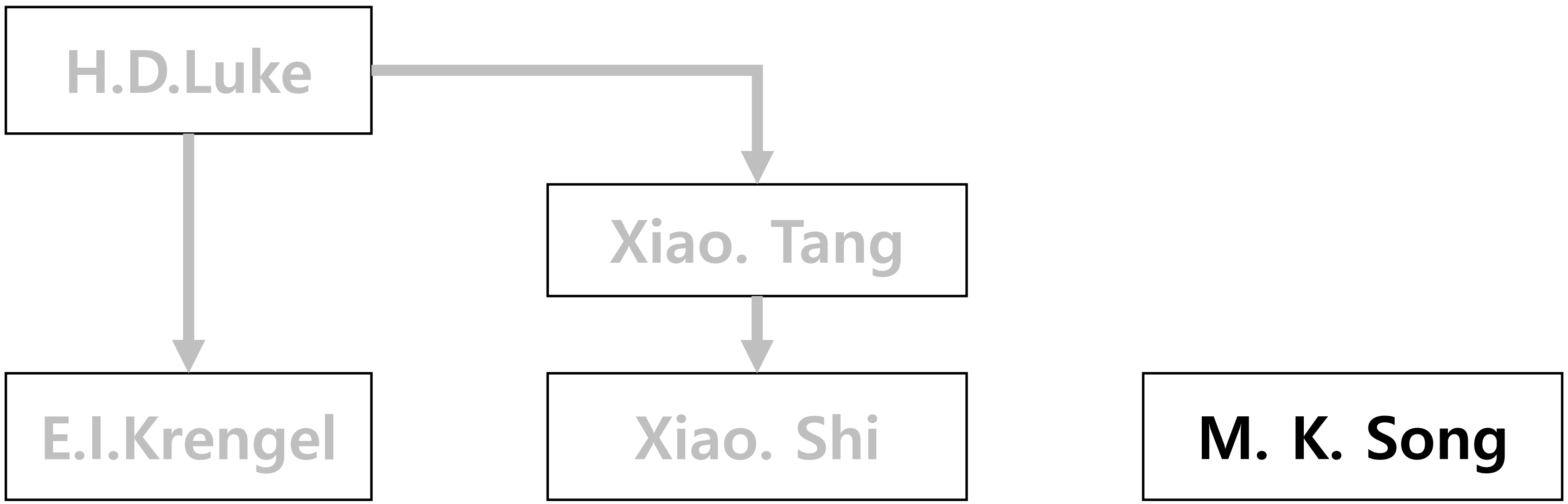
X. Tang and C. Ding, “New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value,” IEEE Trans. Inf. Theory, vol. 56, no. 12, pp. 6398–6405, Dec. 2010

History of almost-polyphase sequence

- Shi extend Tang's almost-polyphase sequence to ***k*-ary**(2019)

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.

History of almost-polyphase sequence



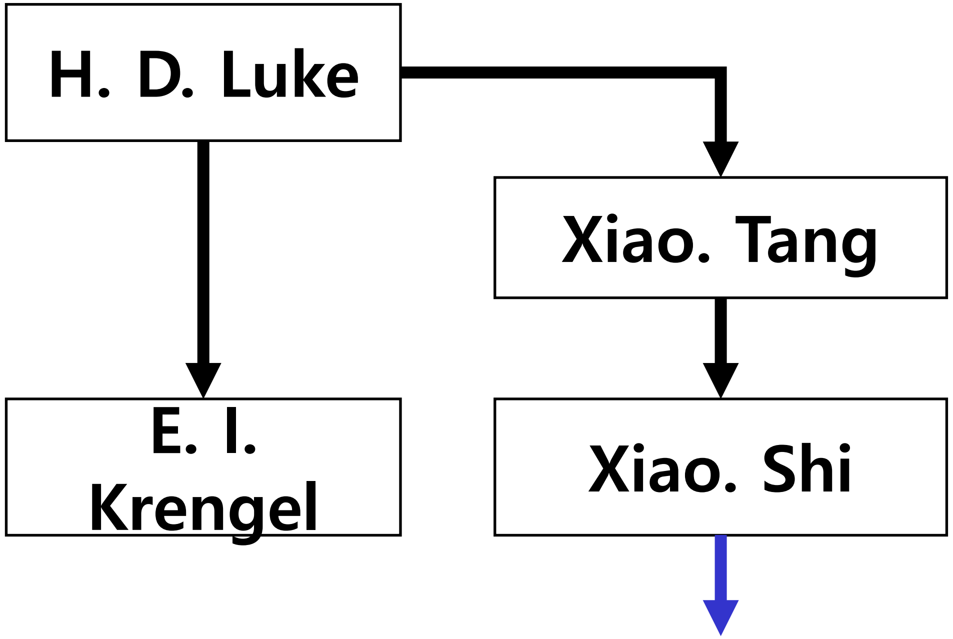
- Almost-polyphse sequence is created by Generalized Milweski construction (2018)
- Perfect sequence

Min Kyu Song and Hong-Yeop Song, "A generalized Milewski construction for perfect sequences," Sequences and Their Applications (SETA 2018), Hong Kong, China, Oct. 1-7, 2018

Almost-polyphase sequence

A sequence consisting of
Roots of unity and **zero**

$e^{j\frac{2\pi b_1}{N}}$	0	$e^{j\frac{2\pi b_3}{N}}$	$\cdots$	0	$e^{j\frac{2\pi b_{L-1}}{N}}$	$e^{j\frac{2\pi b_L}{N}}$



2,4 – ary almost-polyphase sequence

Ideal autocorrelation sequence is created by putting 0 instead of the complex symbol at **one specific position** in the **complex 2, 4-ary sequence** (2009)

k – ary almost-polyphase sequence

- Shi Extend Tang's almost-polyphase sequence to **k-ary**(2019)

Proposed New constructions

Sidelnikov sequences

Definition 1. sidelnikov sequence

Let $q = kf + 1$ be an odd prime power for some positive integers k, f and

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

with a primitive element μ of $\boldsymbol{F}_q$. For $i = 0,1,\dots,k-1$, we let $D_i = \mu^i D_0$.
Then a k-ary Sidelnikov sequence **s** of period $q-1$ is defined as

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

We can transform $\boldsymbol{s}$ to complex polyphase sequence $\boldsymbol{t}$ is given as

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

where $\omega = e^{j\frac{2\pi}{k}}$. We can multiply the constant c to k-ary sequence $\boldsymbol{s}$ and corresponding polyphase sequence is denoted by $\boldsymbol{t}_c$, $t_c(n) = \omega^{c \cdot s(n)}, n = 0,1,2,\dots$

Proposed punctured sidelnikov sequence

Definition 4.(proposed)

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

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

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

$$t_{\mathrm{c}}^{+}(n)=\begin{cases}0 & \text{if } n=\dfrac{q-1}{2},\\ \mathrm{t_c(n)} & \text{otherwise.}\end{cases}$$

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

$$\mathrm{T}=\{\boldsymbol{t}_{\mathrm{c}}^{+} \mid \mathrm{c}=1,2,\ldots,\text{k-1}\}$$

Sidelnikov's and proposed sequences

	Length	Alphabet size	Family size
Sidelnikov Sequence (& constant multiple family)	Odd prime power-1 $q-1=kf$	k	$k-1$
Proposed punctured sidelnikov sequences	Odd prime power-1 $q-1=kf$	k	$k-1$

Sidelnikov's two polyphase sequences

	Example
4-ary Sidelnikov Sequence $\boldsymbol{t}$ $(q-1=8)$	1 | -1 | $e^{j\frac{3}{2}\pi}$ | -1 | 1 | $e^{j\frac{3}{2}\pi}$ | $e^{j\frac{1}{2}\pi}$ | $e^{j\frac{1}{2}\pi}$
4-ary Proposed punctured sidelnokov sequence $\boldsymbol{t}^{+}$ $(q-1=8)$	1 | -1 | $e^{j\frac{3}{2}\pi}$ | -1 | 0 | $e^{j\frac{3}{2}\pi}$ | $e^{j\frac{1}{2}\pi}$ | $e^{j\frac{1}{2}\pi}$

Sidelnikov's two polyphase sequences

	Correlation upperbound	
	Auto	Cross (with constant multipl e)
Sidelnikov Sequence (& constant multiple family)	4	$\sqrt{q}+3$
Proposed punctured sidelnikov sequences	2	$\sqrt{q}+1$

Proof of correlation upperbound

<u>Definition 2. power residue function</u>

Let $\mathrm{q}, k, \mu, \mathrm{D_i}$ be given in *Definition 1*. We define a **Power Residue** function $\mathrm{g}: \mathrm{F_q} \rightarrow \mathrm{Z_k}$ as flows:

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

Note that

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

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

Proof of correlation upperbound

<u>Lemma 3-(i): autocorrelation of Sidelnokov sequence</u>

For any $\tau \neq 0$, an integer c, with $1 \leq \mathrm{c} \leq \mathrm{k}-1$, the autocorrelation of $\mathrm{t_c}$ is given as follows:

$$\mathrm{R}_{\boldsymbol{t}_{\mathrm{c}}}(\tau) = \sum_{x=0}^{q-2} t_c(x+\tau) t_c(x)^*$$

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

Therefore

$$\left|\mathrm{R}_{\boldsymbol{t}_{\mathrm{c}}}(\tau)\right| \leq 4.$$

Proof of correlation upperbound

<u>Theorem 5: autocorrelation of proposed punctured sidelnokov sequence</u>

For $\tau \neq 0$,

$$\left|R_{t_c^+}(\tau)\right| \leq 2.$$

Proof)

Assume $\tau \neq 0$,

$$R_{t_c^+}(\tau) = \sum_{x=0}^{q-2} t_c^+(x+\tau)t_c^+(x)^*$$

$$= R_{t_c}(\tau) - t_c\left(\frac{q-1}{2}+\tau\right)t_c\left(\frac{q-1}{2}\right)^* - t_c\left(\frac{q-1}{2}\right)t_c\left(\frac{q-1}{2}-\tau\right)^*$$

Note that $\mu^{\frac{q-1}{2}} = -1$, $t_c\left(\frac{q-1}{2}\right) = 1$. By Lemma 3-(i)

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

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

Proof of correlation upperbound

Lemma 3-(ii),(iii): crosscorrelation of Sidelnokov sequence

Let a, b be integers with $1 \le a \ne b \le \mathrm{k}-1$. The crosscorrelation of $\boldsymbol{t}_\mathrm{a}$ and $\boldsymbol{t}_\mathrm{b}$ is given as follows:

(ii) If $\tau = 0$,

$$\mathrm{C}_{\boldsymbol{t}_a,\boldsymbol{t}_b}(0) = \sum_{x=0}^{q-2} t_a(x) t_b(x)^* = 0\,.$$

(iii) If $\tau \ne 0$,

$$\mathrm{C}_{\boldsymbol{t}_a,\boldsymbol{t}_b}(\tau) = \sum_{x=0}^{q-2} t_c(x+\tau) t_c(x)^*$$

$$= \omega^{a\cdot \mathrm{g}(-\mu^{\tau}+1)} + \omega^{b\cdot \mathrm{g}(-\mu^{-\tau}+1)} + \sum_{x \in F_q \backslash \{0,-1,-\mu^{-\tau}\}} \omega^{a\cdot g(\mu^{\tau}x+1) - b\cdot g(x+1)}$$

This leads to

$$\left|C_{\boldsymbol{t}_a,\boldsymbol{t}_b}(\tau)\right| \le \sqrt{q} + 3$$

Proof of correlation upperbound

<u>Theorem 5: autocorrelation of proposed punctured sidelnokov sequence</u>

For $1 \le a \ne b \le k-1$

$$\left|C_{t_a^+,t_b^+}(\tau)\right| \le \sqrt{q}+1.$$

Proof)

Note that $\mu^{\frac{q-1}{2}} = -1$, $t_c\left(\frac{q-1}{2}\right) = 1$. Assume $\tau = 0$, by Lemma 3-(ii),

$$C_{t_a^+,t_b^+}(0) = \sum_{x=0}^{q-2} t_a^+(x) t_b^+(x)^* = C_{t_a,t_b}(0) - t_a\left(\frac{q-1}{2}\right) t_b\left(\frac{q-1}{2}\right)^* = -1.$$

Assume $\tau \ne 0$,

$$\begin{aligned} C_{t_a^+,t_b^+}(\tau) &= C_{t_a,t_b}(\tau) - t_a\left(\frac{q-1}{2}+\tau\right) t_b\left(\frac{q-1}{2}\right)^* - t_a\left(\frac{q-1}{2}\right) t_b\left(\frac{q-1}{2}-\tau\right)^* \\ &= C_{t_a,t_b}(\tau) - \omega^{a\cdot g(-\mu^{\tau}+1)} - \omega^{b\cdot g(-\mu^{-\tau}+1)} \\ &= \sum_{x\in F_q \setminus\{0,-1,-\mu^{-\tau}\}} \omega^{a\cdot g(\mu^{\tau}x+1)-b\cdot g(x+1)} \end{aligned}$$

Conclusion remarks

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

- The key technique: a single term of 1 at some position n_1 and replace it with 0
- There exists ONLY one position of sequence such that key technique improves the correlation property.
- To show this case, we choose $q-1=3^6-1=728=28\times 26$ and $k=28$.
- How about other parameters? It is a topic of future study