Balanced Binary Sequences with Favourable Autocorrelation from Cyclic Relative Difference Sets

Gangsan Kim and Hong-Yeop Song

Channel Coding Lab.
School of Electrical and Electronic Engineering, Yonsei Univ.

2024 SEquences and Their Applications

Introduction

In this talk, by using cyclic relative difference sets, we introduce construction of two types of binary sequences with favourable autocorrelation.

1. Balanced binary sequence s with **5-level even autocorrelation**

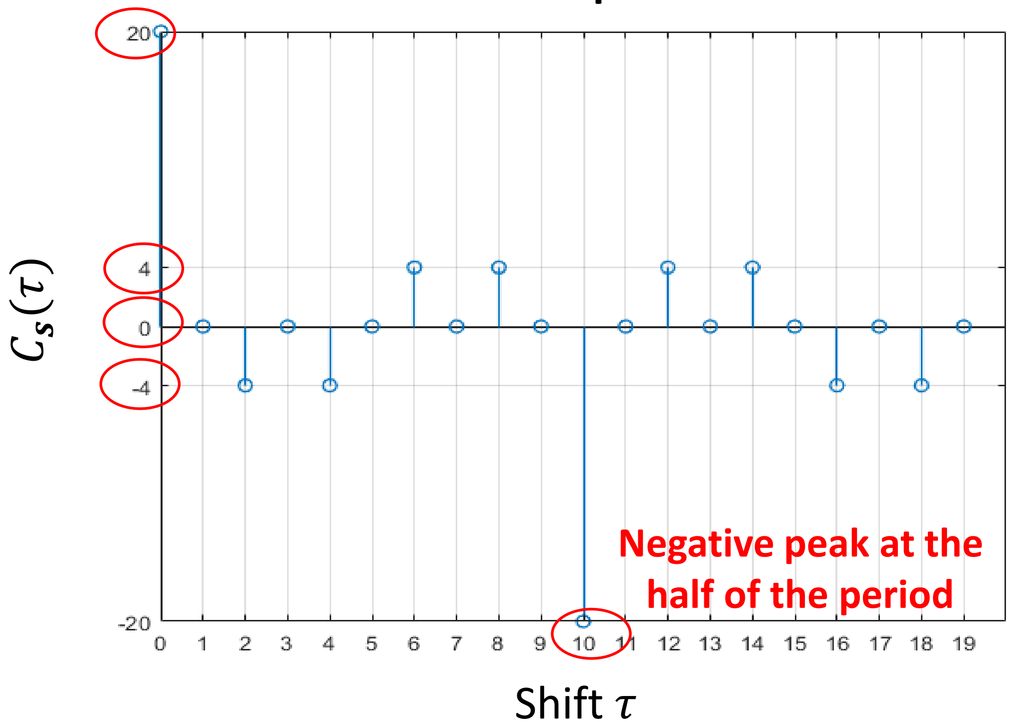
Example

Introduction

In this talk, by using cyclic relative difference sets, we introduce construction of two types of binary sequences with favourable autocorrelation.

1. Balanced binary sequence s with **5-level even autocorrelation**

Example

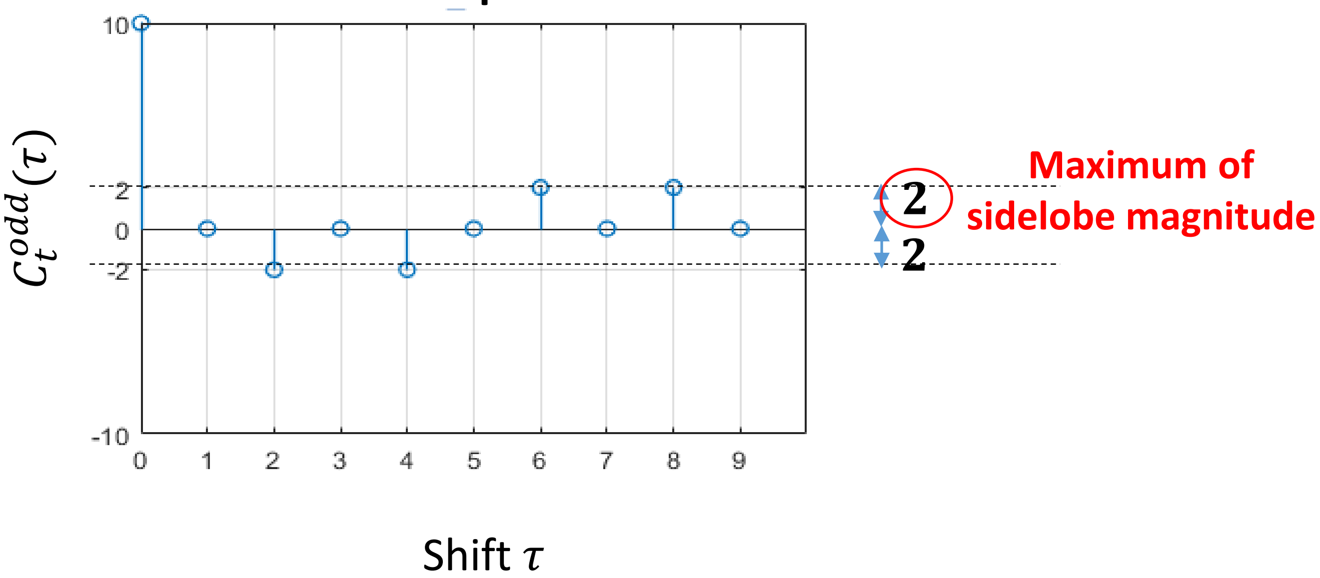


Introduction

In this talk, by using cyclic relative difference sets, we introduce construction of two types of binary sequences with favourable autocorrelation.

2. Binary sequence $\boldsymbol{t}$ with **optimal odd autocorrelation property** (optimal in terms of minimizing maximum of sidelobe magnitude).

Example



Relative Difference Set

Def. Relative Difference Set (RDS)

Let u, v, k, λ be positive integers.

A (u, v, k, λ)-RDS D is a k-subset $\{d_1, d_2, \dots, d_k\} \subset \mathbb{Z}_{uv}$

satisfying the following: For $d \in \mathbb{Z}_{uv}$,

$$|D \cap (d + D)| = \begin{cases} \lambda & \text{if } d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}, \\ 0 & \text{if } d \in u\mathbb{Z}_{uv} \backslash \{0\}, \\ k & \text{if } d = 0. \end{cases}$$

Relative Difference Set

Def. Relative Difference Set (RDS)

Let u, v, k, λ be positive integers.

A (u, v, k, λ)-RDS D is a k-subset $\{d_1, d_2, \dots, d_k\} \subset \mathbb{Z}_{uv}$

satisfying the following: For $d \in \mathbb{Z}_{uv}$,

$$|D \cap (d + D)| = \begin{cases} \lambda & \text{if } d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}, \\ 0 & \text{if } d \in u\mathbb{Z}_{uv} \backslash \{0\}, \\ k & \text{if } d = 0. \end{cases}$$

Partition from Relative Difference Set

In this talk, we are interested in $\left(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1\right)$-RDSs

Prop.

Let D be a $(u, 2, u - 1, \frac{u}{2} - 1)$-RDS, Then, $\mathbb{Z}_{2u}$ can be decomposed into the following disjoint union:

$$\mathbb{Z}_{2u} = D \cup (u + D) \cup \{z\} \cup \{u + z\},$$

for some z.

Partition from Relative Difference Set

In this talk, we are interested in $\left(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1\right)$-RDSs

Prop.

Let D be a $(u, 2, u - 1, \frac{u}{2} - 1)$-RDS. Then, $\mathbb{Z}_{2u}$ can be decomposed into the following **disjoint union**:

$$\mathbb{Z}_{2u} = D \cup (u + D) \cup \{z\} \cup \{u + z\},$$

for some $z \notin D \cup (u + D)$.

Proof) $D \cap (u + D)$ is empty by definition.

Partition from Relative Difference Set

In this talk, we are interested in $\left(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1\right)$-RDSs

Prop.

Let D be a $(u, 2, u-1, \frac{u}{2} - 1)$-RDS. Then, $\mathbb{Z}_{2u}$ can be decomposed into the following **disjoint union**:

$$\mathbb{Z}_{2u} = \underbrace{D}_{\substack{u-1\\\text{elements}}} \cup (u + \underbrace{D}_{\substack{u-1\\\text{elements}}}) \cup \{\underbrace{z}_{\text{1 element}}\} \cup \{u \underbrace{+}_{\text{1 element}} z\},$$

for some $z \notin D \cup (u + D)$.

Proof) $D \cap (u + D)$ is empty by definition.

Example

Consider $(10,2,9,4)$-RDS

$$D = \{0,1,2,3,6,7,9,14,18\}$$

$$\mathbb{Z}_{20} = D \cup (10 + D) \cup \{z\} \cup \{10 + z\},$$

$\mathbb{Z}_{20}$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19

Example

Consider $(10,2,9,4)$-RDS

$$D = \{0,1,2,3,6,7,9,14,18\}$$

$$\mathbb{Z}_{20} = D \cup (10 + D) \cup \{z\} \cup \{10 + z\},$$

$\mathbb{Z}_{20}$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19

Example

Consider $(10,2,9,4)$-RDS

$$D = \{0,1,2,3,6,7,9,14,18\}$$

$$\mathbb{Z}_{20} = D \cup (10 + D) \cup \{z\} \cup \{10 + z\},$$

$\mathbb{Z}_{20}$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19

Example

Consider $(10,2,9,4)$-RDS

$$D = \{0,1,2,3,6,7,9,14,18\}$$

$$\mathbb{Z}_{20} = D \cup (10 + D) \cup \{z\} \cup \{10 + z\},$$

$\mathbb{Z}_{20}$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19

Example

Consider $(10,2,9,4)$-RDS

$$D = \{0,1,2,3,6,7,9,14,18\}$$

$$\mathbb{Z}_{20} = D \cup (10 + D) \cup \{z\} \cup \{10 + z\},$$

$\mathbb{Z}_{20}$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19

Example

Consider $(10,2,9,4)$-RDS

$D = \{0,1,2,3,6,7,9,14,18\}$

To make binary sequence, let assign

0 1

$$\mathbb{Z}_{20} = D \cup (10 + D) \cup \{z\} \cup \{10 + z\},$$

$\mathbb{Z}_{20}$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19

Main construction

Let D be a $(u, 2, u-1, \frac{u}{2}-1)$-RDS. Then

$$\mathbb{Z}_{2u} = D \cup (u+D) \cup \{z\} \cup \{u+z\}.$$

Construct a binary sequence $\boldsymbol{s} = \{s(i) \mid i = 0,1,\dots,2u-1\}$ as follows:

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

Thm. the periodic (even) autocorrelation of $\boldsymbol{s}$ becomes:

$$C_s(\tau) = \begin{cases} 2u, & \tau = 0 \\ -2u, & \tau = u \\ 4, & \tau \in (-z+u+D) \cap (z-u-D) \\ -4, & \tau \in (-z+D) \cap (z-D) \\ 0, & \text{otherwise.} \end{cases}$$

Main construction

Let D be a $(u, 2, u-1, \frac{u}{2}-1)$-RDS. Then

$$\mathbb{Z}_{2u} = D \cup (u+D) \cup \{z\} \cup \{u+z\}.$$

Construct a binary sequence $\boldsymbol{s} = \{s(i) \mid i = 0,1,\ldots,2u-1\}$ as follows:

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

Thm. the periodic (even) autocorrelation of $\boldsymbol{s}$ becomes:

$$C_s(\tau) = \begin{cases} 2u, & \tau = 0 \\ -2u, & \tau = u \\ 4, & \tau \in (-z+u+D) \cap (z-u-D) \\ -4, & \tau \in (-z+D) \cap (z-D) \\ 0, & \text{otherwise.} \end{cases}$$

Main construction

Let D be a $(u, 2, u-1, \frac{u}{2}-1)$-RDS. Then

$$\mathbb{Z}_{2u} = D \cup (u+D) \cup \{z\} \cup \{u+z\}.$$

Construct a binary sequence $\boldsymbol{s} = \{s(i) \mid i = 0,1,\ldots,2u-1\}$ as follows:

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

Thm. The periodic (even) autocorrelation of $\boldsymbol{s}$ becomes:

$$C_{\boldsymbol{s}}(\tau) = \begin{cases} 2u, & \tau = 0 \\ -2u, & \tau = u \\ 4, & \tau \in (-z+u+D) \cap (z-u-D) \\ -4, & \tau \in (-z+D) \cap (z-D) \\ 0, & \text{otherwise.} \end{cases}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

$$C_s(\tau) = \sum_{i \in \mathbb{Z}_{2u}} (-1)^{s(i)+s(i+\tau)}$$

$$= \sum_{i \in D} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in (u+D)} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

$$C_s(\tau) = \sum_{i \in \mathbb{Z}_{2u}} (-1)^{s(i)+s(i+\tau)}$$

$$= \boxed{\sum_{i \in D} (-1)^{s(i)+s(i+\tau)}} + \sum_{i \in (u+D)} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

$$\boxed{\sum_{i \in D} (-1)^{s(i)+s(i+\tau)}} = \sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{s(i)+s(i+\tau)} + \sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{s(i)+s(i+\tau)} + \sum_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

$$\sum_{i \in D} (-1)^{s(i)+s(i+\tau)} = \boxed{\sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{s(i)+s(i+\tau)}} + \boxed{\sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{s(i)+s(i+\tau)}} + \sum_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)}$$

$$\sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{s(i)+s(i+\tau)} = \sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^0 = |\boldsymbol{D} \cap (-\boldsymbol{\tau} + \boldsymbol{D})| = |(\boldsymbol{\tau} + \boldsymbol{D}) \cap \boldsymbol{D}| \triangleq \boldsymbol{\Delta}_{\mathbf{D}}(\boldsymbol{\tau})$$

$$\sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{s(i)+s(i+\tau)} = \sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^1 = -|\boldsymbol{D} \cap (-\boldsymbol{\tau} + \boldsymbol{u} + \boldsymbol{D})| = -\Delta_D(u-\tau)$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u + D) \cup \{u + z\} \end{cases}$$

$$\sum_{i \in D} (-1)^{s(i)+s(i+\tau)} = \boxed{\sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{s(i)+s(i+\tau)}} + \boxed{\sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{s(i)+s(i+\tau)}} + \sum_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)}$$

$$\sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{s(i)+s(i+\tau)} = \sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{0} = |D \cap (-\tau + D)| = |(\tau + D) \cap D| \triangleq \Delta_D(\tau)$$

$$\sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{s(i)+s(i+\tau)} = \sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{1} = -|D \cap (-\tau + u + D)| = -\Delta_D(u - \tau)$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

$$\sum_{i \in D} (-1)^{s(i)+s(i+\tau)} = \boxed{\sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{s(i)+s(i+\tau)}} + \boxed{\sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{s(i)+s(i+\tau)}} + \sum_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)}$$

$$\sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{s(i)+s(i+\tau)} = \sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{0} = |D \cap (-\tau + D)| = |(\tau + D) \cap D| \triangleq \Delta_D(\tau)$$

$$\sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{s(i)+s(i+\tau)} = \sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{1} = -|D \cap (-\tau + u + D)| = -\Delta_D(u - \tau)$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

$$\sum_{i \in D} (-1)^{s(i)+s(i+\tau)} = \Delta_D(\tau) - \Delta_D(u-\tau) + \sum_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)}$$

$$\sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^{s(i)+s(i+\tau)} = \sum_{\substack{i \in D \\ i+\tau \in D}} (-1)^0 = |D \cap (-\tau + D)| = |(\tau + D) \cap D| \triangleq \Delta_D(\tau)$$

$$\sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^{s(i)+s(i+\tau)} = \sum_{\substack{i \in D \\ i+\tau \in (u+D)}} (-1)^1 = -|D \cap (-\tau + u + D)| = -\Delta_D(u-\tau)$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

Recall that

$$C_s(\tau) = \boxed{\left\{ \sum_{i \in D} (-1)^{s(i)+s(i+\tau)} \right\}} + \left\{ \sum_{i \in (u+D)} (-1)^{s(i)+s(i+\tau)} \right\} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

$$C_s(\tau) = \boxed{\left\{ \begin{array}{c} \Delta_D(\tau) - \Delta_D(u-\tau) \\ + \sum\limits_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} \end{array} \right\}} + \left\{ \sum_{i \in (u+D)} (-1)^{s(i)+s(i+\tau)} \right\} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

Similarly,

$$C_s(\tau) = \left\{ \begin{array}{c} \Delta_D(\tau) - \Delta_D(u-\tau) \\ + \sum_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} \end{array} \right\} + \boxed{\left\{ \sum_{i \in (u+D)} (-1)^{s(i)+s(i+\tau)} \right\}} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

Similarly,

$$C_s(\tau) = \left\{ \begin{array}{c} \Delta_D(\tau) - \Delta_D(u-\tau) \\ + \displaystyle\sum_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} \end{array} \right\} + \boxed{\left\{ \begin{array}{c} \Delta_D(\tau) - \Delta_D(u+\tau) \\ + \displaystyle\sum_{\substack{i \in (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} \end{array} \right\}} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

Rearrange it as a simple form

$$C_s(\tau) = \boxed{\left\{ \begin{array}{c} \Delta_D(\tau) - \Delta_D(u-\tau) \\ + \displaystyle\sum_{\substack{i \in D \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} \end{array} \right\} + \left\{ \begin{array}{c} \Delta_D(\tau) - \Delta_D(u+\tau) \\ + \displaystyle\sum_{\substack{i \in (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} \end{array} \right\}} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

Rearrange it as a simple form

$$C_s(\tau) = \boxed{2\Delta_D(\tau) - \Delta_D(u-\tau) - \Delta_D(u+\tau) + \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)}} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

$$C_s(\tau) = 2\Delta_D(\tau) - \Delta_D(u-\tau) - \Delta_D(u+\tau) + \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

We omit the proof of trivial case where $\tau = 0$ or $\tau = u$.

Now we consider the case where $\tau \neq 0, u$.

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\boldsymbol{\tau \neq 0, u}$

$$C_s(\tau) = 2\Delta_D(\tau) - \Delta_D(u-\tau) - \Delta_D(u+\tau) + \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\boldsymbol{\tau \neq 0, u}$

$$C_s(\tau) = \underbrace{2\Delta_D(\tau)}^{(=\mathbf{2}\boldsymbol{\lambda})} - \overbrace{\Delta_D(u-\tau)}^{(=\boldsymbol{\lambda})} - \overbrace{\Delta_D(u+\tau)}^{(=\boldsymbol{\lambda})} + \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Recall that

$$\Delta_D(d) = \begin{cases} \lambda & \text{if } d \in \mathbb{Z}_{uv} \backslash u\mathbb{Z}_{uv}, \\ 0 & \text{if } d \in u\mathbb{Z}_{uv} \backslash \{0\}, \\ k & \text{if } d = 0 \end{cases}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\boldsymbol{\tau \neq 0, u}$

$$C_s(\tau) = \underbrace{2\Delta_D(\tau)}_{(=2\lambda)} - \underbrace{\Delta_D(u-\tau)}_{(=\lambda)} - \underbrace{\Delta_D(u+\tau)}_{(=\lambda)} + \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

$$= \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\boldsymbol{\tau \neq 0, u}$

$$C_s(\tau) = 2\Delta_D(\tau) - \Delta_D(u-\tau) - \Delta_D(u+\tau) + \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

$$= \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Note that

$\{z-\tau, u+z-\tau\} \subset (D \cap (u+D))$

$$= \sum_{i+\tau \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

Proof

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\tau \neq 0, u$

$$C_s(\tau) = 2\Delta_D(\tau) - \Delta_D(u-\tau) - \Delta_D(u+\tau) + \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

$$= \sum_{\substack{i \in D \cup (u+D) \\ i+\tau \in \{z, u+z\}}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)}$$

$$= \sum_{i+\tau \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)} + \sum_{i \in \{z, u+z\}} (-1)^{s(i)+s(i+\tau)} = \sum_{i \in \{z, u+z, z-\tau, u+z-\tau\}} (-1)^{s(i)+s(i+\tau)}$$

QED

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\boldsymbol{\tau \neq 0, u}$

$$C_s(\tau) = \sum_{i \in \{z, u+z, z-\tau, u+z-\tau\}} (-1)^{s(i)+s(i+\tau)}$$

$$= (-1)^{s(z)+s(z+\tau)} + (-1)^{s(u+z)+s(u+z+\tau)} + (-1)^{s(z-\tau)+s(z)} + (-1)^{s(u-z-\tau)+s(u+z)}$$

QED

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\boldsymbol{\tau \neq 0, u}$

$$C_s(\tau) = \sum_{i \in \{z, u+z, z-\tau, u+z-\tau\}} (-1)^{s(i)+s(i+\tau)}$$

$$= (-1)^{s(z+\tau)} + (-1)^{s(u+z+\tau)+1} + (-1)^{s(z-\tau)} + (-1)^{s(u-z-\tau)+1}$$

QED

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\boldsymbol{\tau \neq 0, u}$

$$C_s(\tau) = \sum_{i \in \{z, u+z, z-\tau, u+z-\tau\}} (-1)^{s(i)+s(i+\tau)}$$

$$= (-1)^{s(z+\tau)} + (-1)^{s(u+z+\tau)+1} + (-1)^{s(z-\tau)} + (-1)^{s(u-z-\tau)+1}$$

The above value is depend on whether

each $z+\tau, u+z+\tau, z-\tau$, or $\mathrm{u}-\mathrm{z}-\tau$ is in D or $(u+D)$.

Note that each of them is not equal to z or $u+z$.

We calculate each case and it is summarized as shown on the next page.

QED

$$s(i) = \begin{cases} 0, & i \in D \cup \{z\} \\ 1, & i \in (u+D) \cup \{u+z\} \end{cases}$$

For the case when $\boldsymbol{\tau \neq 0, u}$

$$C_s(\tau) = \sum_{i \in \{z, u+z, z-\tau, u+z-\tau\}} (-1)^{s(i)+s(i+\tau)}$$

$$= (-1)^{s(z+\tau)} + (-1)^{s(u+z+\tau)+1} + (-1)^{s(z-\tau)} + (-1)^{s(u-z-\tau)+1}$$

$$= \begin{cases} -4, & z-\tau, z+\tau \in D \\ 4, & z-\tau, z+\tau \in (u+D) \\ 0, & \text{otherwise} \end{cases}$$

$\blacksquare$

Example

Consider $(10,2,9,4)$-RDS

$D = \{0,1,2,3,6,7,9,14,18\}$

To make binary sequence, let assign

$0 \quad 1$

$\mathbb{Z}_{20} = D \cup (10 + D) \cup \{z\} \cup \{10 + z\},$

0	1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18	19

Example

Consider $(10,2,9,4)$-RDS

$D = \{0,1,2,3,6,7,9,14,18\}$

To make binary sequence, let assign

0 1

$$\mathbb{Z}_{20} = D \cup (10+D) \cup \{z\} \cup \{10+z\},$$

$\boldsymbol{s} = \{$ 0, 0, 0, 0, 1, 0, 0, 0, 1, 0,

1, 1, 1, 1, 0, 1, 1, 1, 0, 1 $\}$

Example

Consider $(10,2,9,4)$-RDS

$D = \{0,1,2,3,6,7,9,14,18\}$

To make binary sequence,
let assign

$0 \quad 1$

$\mathbb{Z}_{20} = D \cup (10 + D) \cup \{\boldsymbol{z}\} \cup \{\mathbf{10} + \boldsymbol{z}\}$,

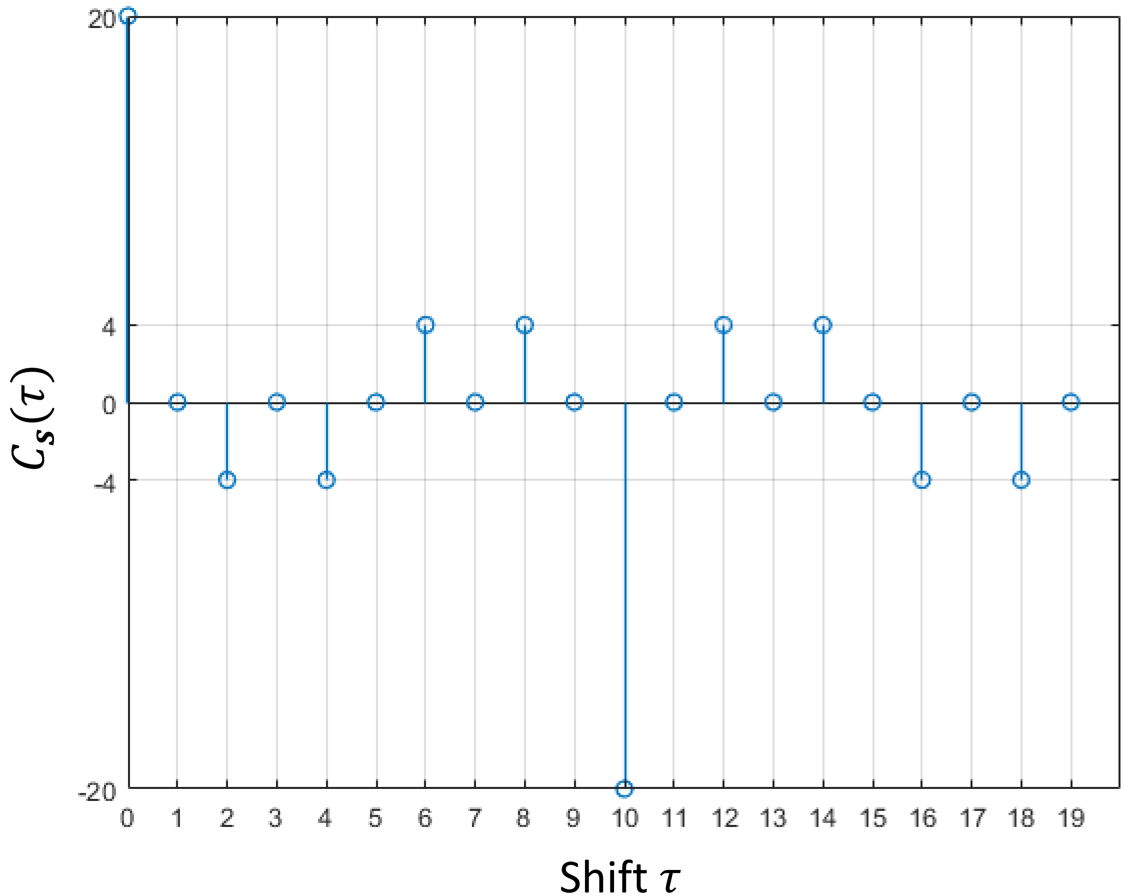
Note that these two symbols can be interchanged depending on whether $z = 5$ or 15.

$\boldsymbol{s} = \{$ 0, 0, 0, 0, 1, **0,** 0, 0, 1, 0,
1, 1, 1, 1, 0, **1,** 1, 1, 0, 1 $\}$

Example

$$\boldsymbol{s} = \{\ 0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,$$
$$1,\ 1,\ 1,\ 1,\ 0,\ 1,\ 1,\ 1,\ 0,\ 1\ \}$$

5-level

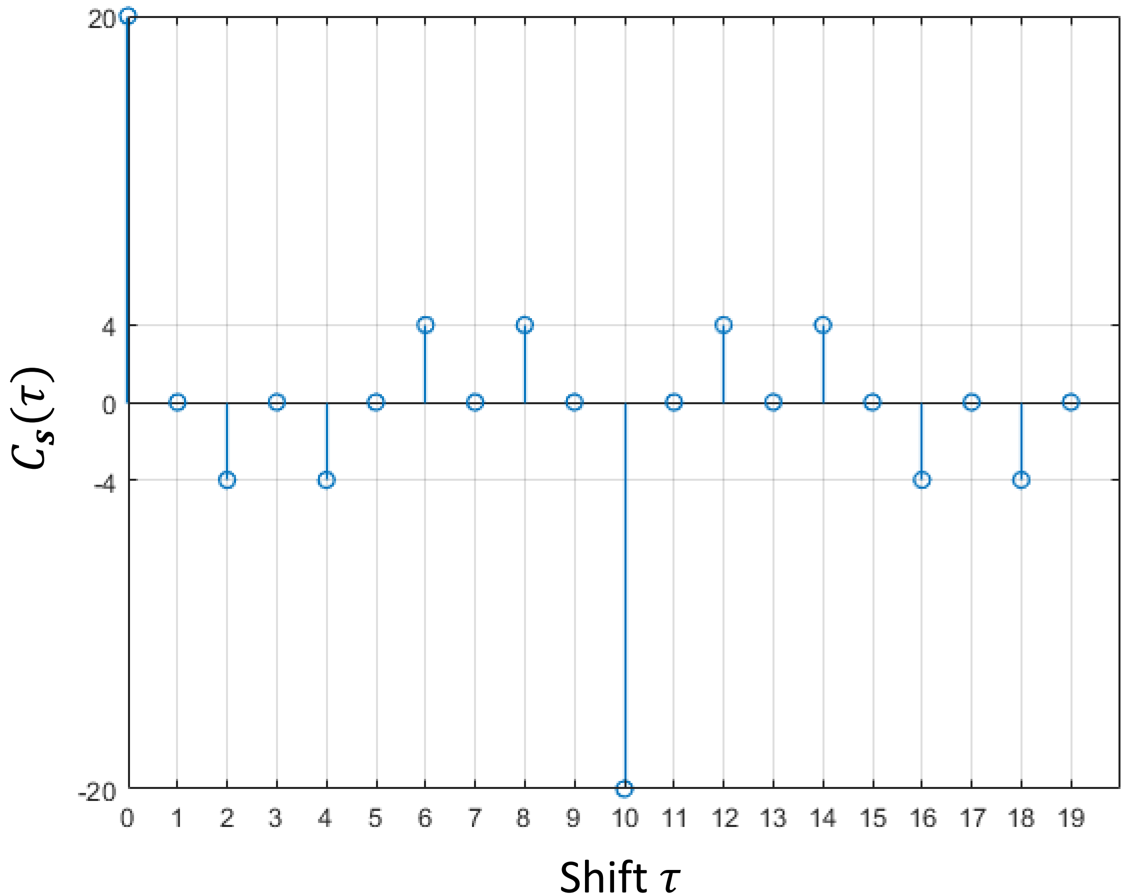


Example

$\boldsymbol{s} = \{$ 0, 0, 0, 0, 1, 0, 0, 0, 1, 0,
1, 1, 1, 1, 0, 1, 1, 1, 0, 1 $\}$

Observation:
Complement

5-level

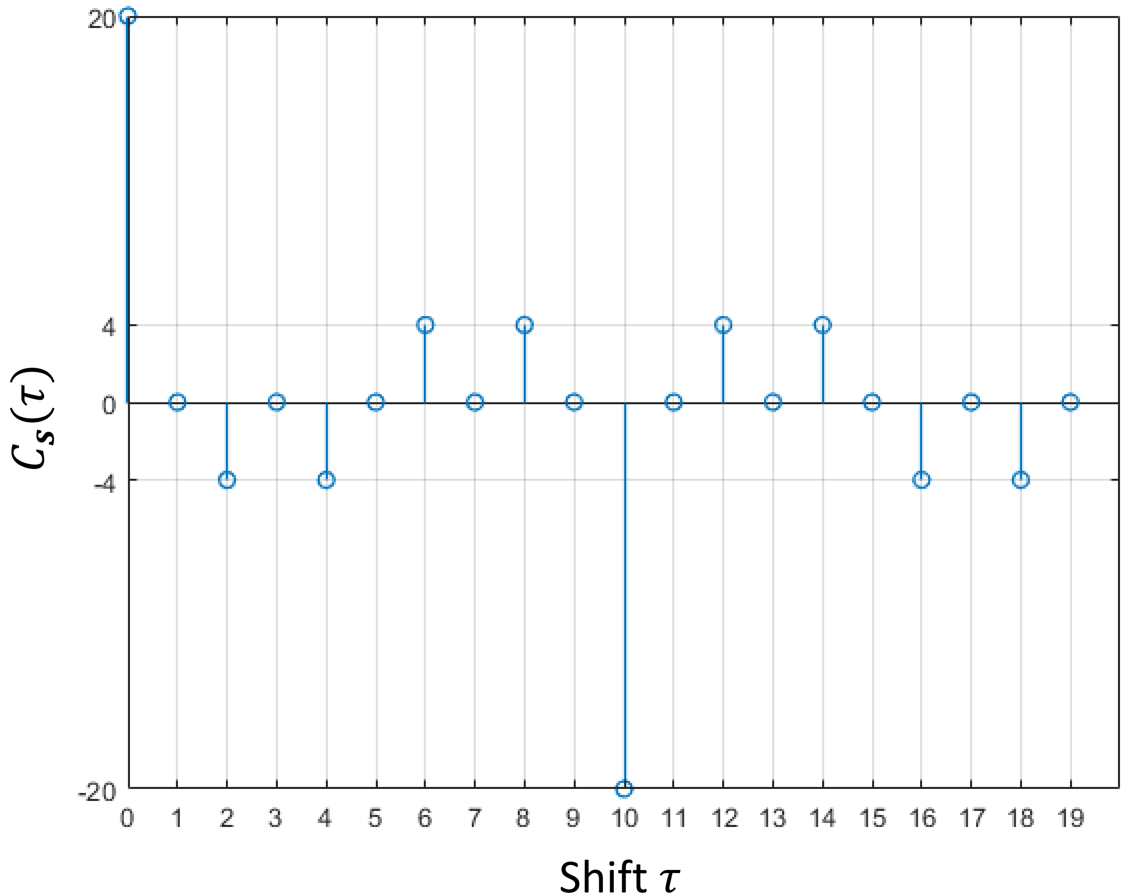


Example

$\boldsymbol{s} = \{$ $\boxed{0,\ 0,\ 0,\ 0,\ 1,\ 0,\ 0,\ 0,\ 1,\ 0,}$
$1,\ 1,\ 1,\ 1,\ 0,\ 1,\ 1,\ 1,\ 0,\ 1\ \}$

Let's observe **the sequence consisting of only one side**

5-level



Main construction

From the previous sequence $\boldsymbol{s}$ of period $2u$,

construct a sequence $\boldsymbol{t}$ of period u as follows: For $i = 0, 1, \dots, u-1$

$$t(i) = s(i).$$

Thm. The periodic odd autocorrelation of t becomes:

$$C_{\boldsymbol{t}}^{odd}(\tau) = \begin{cases} u, & \tau = 0 \\ 2, & \tau \in (-z+u+D) \cap (z-u-D) \\ -2, & \tau \in (-z+D) \cap (z-D) \\ 0, & \text{otherwise.} \end{cases}$$

Main construction

From the previous sequence $\boldsymbol{s}$ of period $2u$,

construct a sequence $\boldsymbol{t}$ of period u as follows: For $i = 0, 1, \dots, u-1$

$$t(i) = s(i).$$

Thm. The periodic odd autocorrelation of t becomes:

$$C_{\boldsymbol{t}}^{odd}(\tau) = \begin{cases} u, & \tau = 0 \\ 2, & \tau \in (-z+u+D) \cap (z-u-D) \\ -2, & \tau \in (-z+D) \cap (z-D) \\ 0, & \text{otherwise.} \end{cases}$$

Main construction

From the previous sequence $\boldsymbol{s}$ of period $2u$,

construct a sequence $\boldsymbol{t}$ of period u as follows: For $i = 0, 1, \dots, u-1$

$$t(i) = s(i).$$

Thm. The periodic odd autocorrelation of t becomes:

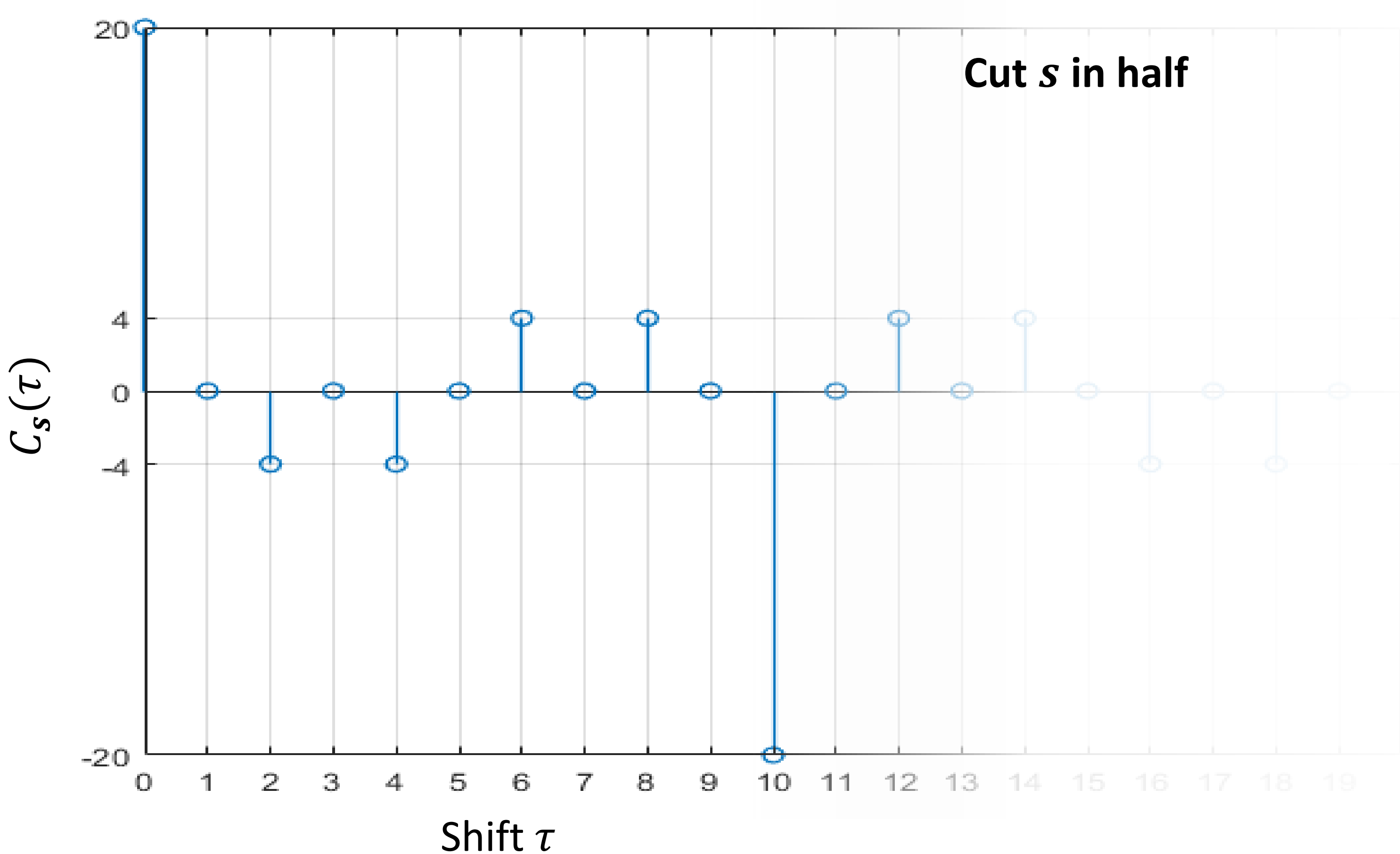
$$C_{\boldsymbol{t}}^{odd}(\tau) = \begin{cases} u, & \tau = 0 \\ 2, & \tau \in (-z+u+D) \cap (z-u-D) \\ -2, & \tau \in (-z+D) \cap (z-D) \\ 0, & \text{otherwise.} \end{cases}$$

Recall that

$$C_{\boldsymbol{s}}(\tau) = \begin{cases} 2u, & \tau = 0 \\ -2u, & \tau = u \\ 4, & \tau \in (-z+u+D) \cap (z-u-D) \\ -4, & \tau \in (-z+D) \cap (z-D) \\ 0, & \text{otherwise.} \end{cases}$$

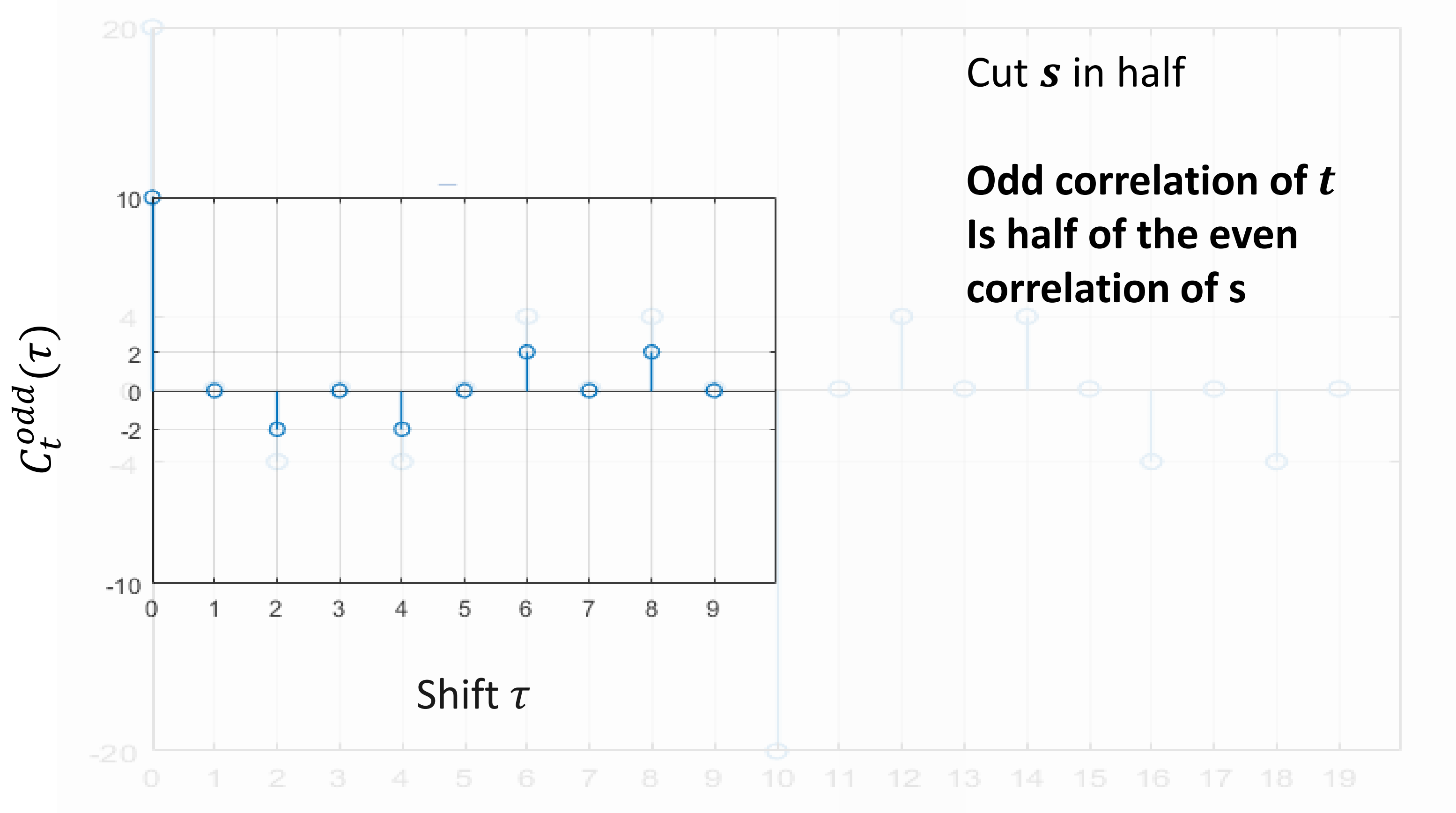
Example

$\boldsymbol{s} = \{$ 0, 0, 0, 0, 1, 0, 0, 0, 1, 0,
1, 1, 1, 1, 0, 1, 1, 1, 0, 1 $\}$



Example

$t = \{$ 0, 0, 0, 0, 1, 0, 0, 0, 1, 0 $\}$



Cut s in half

Odd correlation of t
Is half of the even
correlation of s

Relation between our construction and other known construction

For odd prime power q, **the modified Krengel sequence** [12,14] is the following binary sequence $\boldsymbol{x}$ of period $(q+1)$

$$x(i) = \begin{cases} 1, & \log_\beta \mathrm{Tr}(\alpha^i) \text{ is odd} \\ 0, & \mathrm{Tr}(\alpha^i) = 0 \text{ or else } \log_\beta \mathrm{Tr}(\alpha^i) \text{ is even.} \end{cases}$$

*** Tr: trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$**

*** $\boldsymbol{\beta}$: primitive element of $\mathbb{F}_q$**

This binary sequence $\boldsymbol{x}$ can be constructed by our construction from the following $(q+1, 2, q, \frac{q-1}{2})$-RDS

$$D \triangleq \left\{ i \in \mathbb{Z}_{2(q+1)} \,\middle|\, \mathrm{Tr}(\alpha^i) \neq 0 \text{ and } \log_\beta \mathrm{Tr}(\alpha^i) \text{ is even} \right\}$$

[12] E. I. Krengel, “Almost-perfect and odd-perfect ternary sequences,” SETA 2004.
[14] H.D. Luke, H. D. Schotten and H. Hadinejad-Mahram, “Binary and quadriphase sequences with optimal autocorrelation properties,” IEEE Trans. Inf. Theory, 2003

Relation between our construction and other known construction

For odd prime power q, the modified Krengel sequence [12,14] is the following binary sequence $\boldsymbol{x}$ of period $(q+1)$

$$x(i)=\begin{cases}1, & \log_\beta \mathrm{Tr}(\alpha^i) \text{ is odd} \\ 0, & \mathrm{Tr}(\alpha^i)=0 \text{ or else } \log_\beta \mathrm{Tr}(\alpha^i) \text{ is even.}\end{cases}$$

*** Tr: trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_{q}$**

*** $\boldsymbol{\beta}$: primitive element of $\mathbb{F}_{q}$**

This binary sequence $\boldsymbol{x}$ can be constructed by our construction from the following $(q+1, 2, q, \frac{q-1}{2})$-RDS

$$D \triangleq \{i \in \mathbb{Z}_{2(q+1)} \mid \mathrm{Tr}(\alpha^i) \neq 0 \text{ and } \log_\beta \mathrm{Tr}(\alpha^i) \text{ is even}\}$$

[12] E. I. Krengel, “Almost-perfect and odd-perfect ternary sequences,” SETA 2004.
[14] H.D. Luke, H. D. Schotten and H. Hadinejad-Mahram, “Binary and quadriphase sequences with optimal autocorrelation properties,” IEEE Trans. Inf. Theory, 2003

Relation between our construction and other known construction

For odd prime power q, the modified Krengel sequence [12,14] is the following binary sequence $\boldsymbol{x}$ of period $(\boldsymbol{q}+\mathbf{1})$

$$x(i)=\begin{cases}1, & \log_\beta \mathrm{Tr}(\alpha^i) \text{ is odd} \\ 0, & \mathrm{Tr}(\alpha^i)=0 \text{ or else} \log_\beta \mathrm{Tr}(\alpha^i) \text{ is even.}\end{cases}$$

*** Tr: trace function from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$**

*** $\boldsymbol{\beta}$: primitive element of $\mathbb{F}_q$**

Another variation: Binary NTU sequence $\boldsymbol{y}$ of period $\mathbf{2}(\boldsymbol{q}+\mathbf{1})$ [16]

$$y(i)=\begin{cases}1, & \log_\beta \mathrm{Tr}(\alpha^i) \text{ is odd} \\ 0, & \mathrm{Tr}(\alpha^i)=0 \text{ or else} \log_\beta \mathrm{Tr}(\alpha^i) \text{ is even.}\end{cases}$$

[16] Y. Nogami, K. Tada, and S. Uehara, “A geometric sequence binarized with Legendre symbol over odd characteristic field and its properties,” IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 2014.

Concluding Remarks

All the known parameters of the $(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1)$-RDS are $u = q + 1$ for odd prime power q.

Indeed, our construction gives some binary sequences of period $q + 1$ with optimal odd autocorrelation.

By exhaustive search, we confirm that all binary sequences of period $q + 1$ with optimal odd autocorrelation property for $q = 3,5,7,11,13,17,19$.

We conjecture that it is the only way of getting a binary sequence of period $q + 1$ with optimal odd autocorrelation for odd prime power q.

Concluding Remarks

All the known parameters of the $(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1)$-RDS are $u = q + 1$ for odd prime power q.

Indeed, our construction gives some binary sequences of period $q + 1$ with optimal odd autocorrelation.

By exhaustive search, we confirm that all binary sequences of period $q + 1$ with optimal odd autocorrelation property for $q = 3,5,7,11,13,17,19$.

We conjecture that it is the only way of getting a binary sequence of period $q + 1$ with optimal odd autocorrelation for odd prime power q.

Concluding Remarks

All the known parameters of the $(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1)$-RDS are $u = q + 1$ for odd prime power q.

Indeed, our construction gives some binary sequences of period $q + 1$ with optimal odd autocorrelation.

By exhaustive search, we confirm that all binary sequences of period $q + 1$ with optimal odd autocorrelation property for $q = 3,5,7,11,13,17,19$.

We conjecture that it is the only way of getting a binary sequence of period $q + 1$ with optimal odd autocorrelation for odd prime power q.

Concluding Remarks

All the known parameters of the $(u, v = 2, k = u - 1, \lambda = \frac{u}{2} - 1)$ -RDS are $u = q + 1$ for odd prime power q.

Indeed, our construction gives some binary sequences of period $q + 1$ with optimal odd autocorrelation.

By exhaustive search, we confirm that all binary sequences of period $q + 1$ with optimal odd autocorrelation property for $q = 3,5,7,11,13,17,19$.

We conjecture that it is the only way of getting a binary sequence of period $q + 1$ with optimal odd autocorrelation for odd prime power q.