Some construction of optimal ZCZ sequence families with suppressed side-lobe outside ZCZ

CSDL

Min Kyu Song
and Hong-Yeop Song
Yonsei University

Jang Yong Lee
Agency for Defense Development

SETA 2016, October 9-14

Orthogonal codes with good out-of-phase correlations

Orthogonal codes

A set Θ of mutually orthogonal vectors of length l is called an orthogonal code. It is well-known that

$$|\Theta| \leq l.$$

We call Θ maximal orthogonal code when the equality holds.

Maximal orthogonal codes can be obtained from:

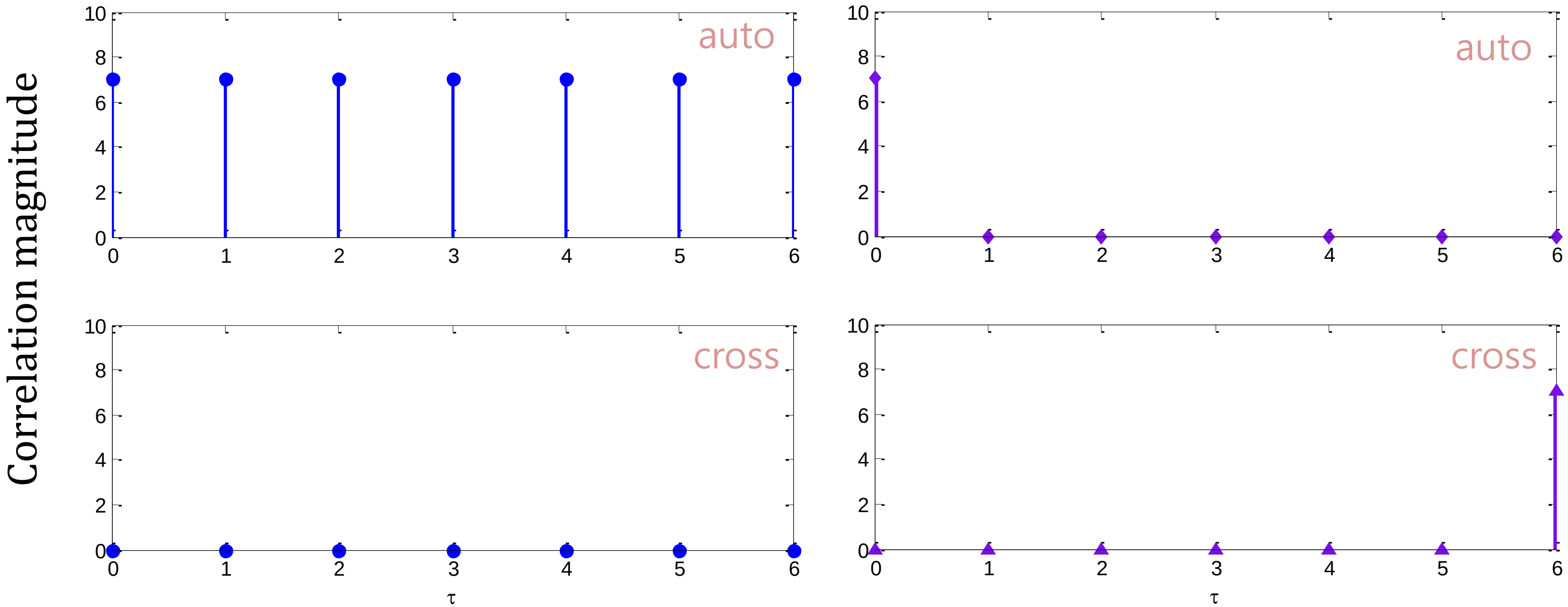
1. DFT matrices
2. circulant matrices generated by perfect sequences
3. (generalized) Hadamard matrices

only consider mutually orthogonality

don't consider out-of-phase correlation.

Example: correlations of such codes

Maximal orthogonal codes of length 7 over Z_7



DFT matrix　　　　perfect sequence

Not good out-of-phase correlation

Lower bound on out-of-phase correlation of orthogonal codes

(Fan96, **approximated lower bound**) Let Θ be a set of l sequences of length l over the integers modulo q and assume that $l \gg 1$.

Then the maximum non-trivial correlation is lower bounded by

- $\sqrt{l}$ if $q > 2$.
- $\sqrt{2l}$ if $q = 2$.

Do there exist such orthogonal codes?

How can we construct?

ANS) Fortunately, we can construct them for **odd prime lengthes**.

Main Construction
- a class of orthogonal codes -

For odd prime p, using Zadoff-Chu sequences $z = \{z_{u,k}(t)\}_{t=0}^{p-1}$ defined

$$z_{u,k}(t) = ut(t+1+2k)/2 \ \ mod \ \ l.$$ (Chu72)

Definition. For odd prime $p > 3$ and a non-zero element c in Z_p, let $z(t)$ be a Zadoff-Chu sequence of period p. Define a set K of p sequences $k_0, k_1, \ldots, k_{p-1}$ of length p over Z_p as

$$\boldsymbol{k_i = \{k_i(t) = z(t+i) + ct^3 \bmod p\}_{t=0}^{p-1}}$$

Theorem. The set K is a maximal orthogonal code and the magnitude of out-of-phase correlation of any two sequences in K is $\sqrt{p}$. In other words, ***K* is a maximal orthogonal code which meets the approximated lower bound.**

Proof of the theorem

For simplicity, consider the case when $z(t) = t(t+1)/2$. $(u = 1, k = 0)$

For $k_i, k_j \in K$,

$$C_{k_i,k_j}(\tau) = \sum_{t=0}^{p-1} \omega_p^{z(t+i)+t^3-z(t+\tau+j)-(t+\tau)^3}$$

$$C_{k_i,k_j}(\tau) = \sum_{t=0}^{p-1} \omega_p^{-3\tau t^2-3\tau^2 t+\tau^3+ct+d}$$

$$C_{k_i,k_j}(0) = \sum_{t=0}^{p-1} \omega_p^{z(t+i)-z(t+j)} = \begin{cases} p, \text{if } i = j \\ 0, \text{if } i \neq j \end{cases}$$

Mutually orthogonality

$$\left|C_{k_i,k_j}(\tau)\right|^2 = \sum_{t=0}^{p-1} \omega_p^{-3\tau t^2-3\tau^2 t+\tau^3+ct+d} \sum_{t'=0}^{p-1} \omega_p^{3\tau t'^2+3\tau^2 t'-\tau^3-ct'-d}$$

$$= \sum_{t=0}^{p-1} \omega_p^{-3\tau t^2-3\tau^2 t+\tau^3+ct+d} \sum_{e=0}^{p-1} \omega_p^{3\tau(t+e)^2+3\tau^2(t+e)-\tau^3-c(t+e)-d}$$

$$= \sum_{e=0}^{p-1} \omega_p^{3\tau e^2+3\tau^2 e-ce} \sum_{t=0}^{p-1} \omega_p^{6\tau et}$$

※The constants c, d are determined by i, j, τ.

$$\left|C_{k_i,k_j}(\tau)\right|^2 = \sum_{e=0}^{p-1} \omega_p^{3\tau e^2+3\tau^2 e-ce} \sum_{t=0}^{p-1} \omega_p^{6\tau et}.$$

Since

$$\sum_{t=0}^{p-1} \omega_p^{6\tau et} = \begin{cases} p, & \text{if } e = 0 \\ 0, & \text{otherwise,} \end{cases}$$

it becomes

$$\left|C_{k_i,k_j}(\tau)\right|^2 = p,$$

for $\tau \not\equiv 0 \bmod p$.

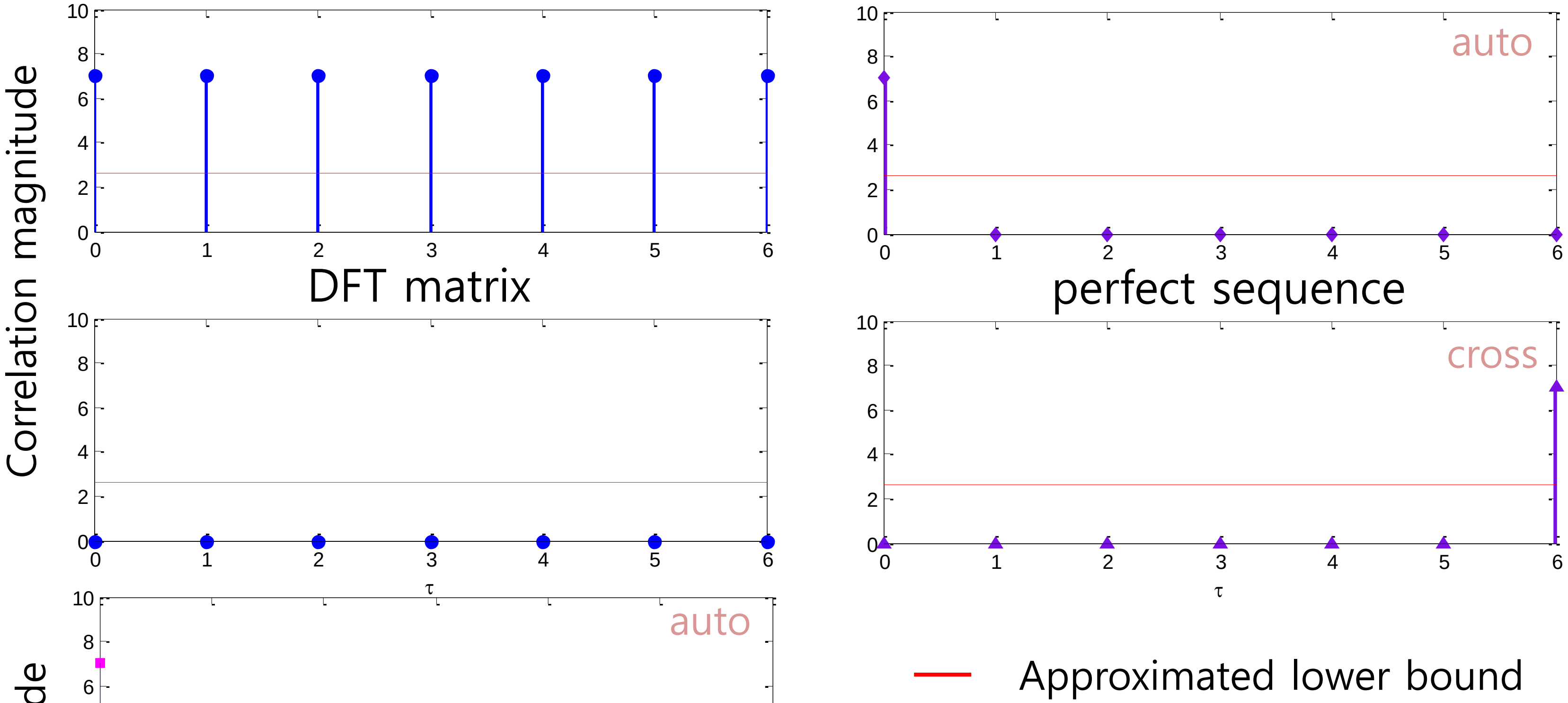
Therefore, for any $0 < \tau < p$,

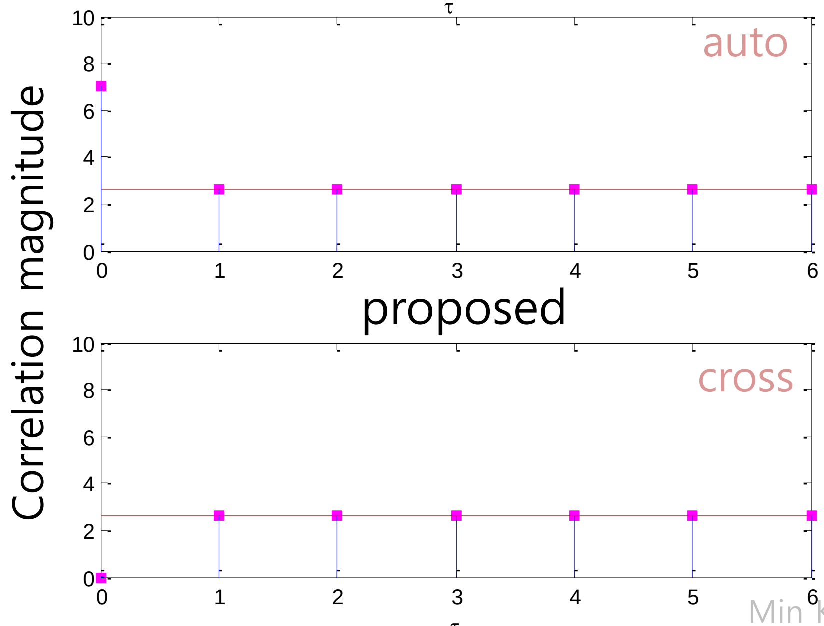
$$\left|C_{k_i,k_j}(\tau)\right| = \sqrt{p},$$

regardless of i and j.

The proof is similar for other case.

Comparison with others





Maximal orthogonal codes of length 7 over Z_7

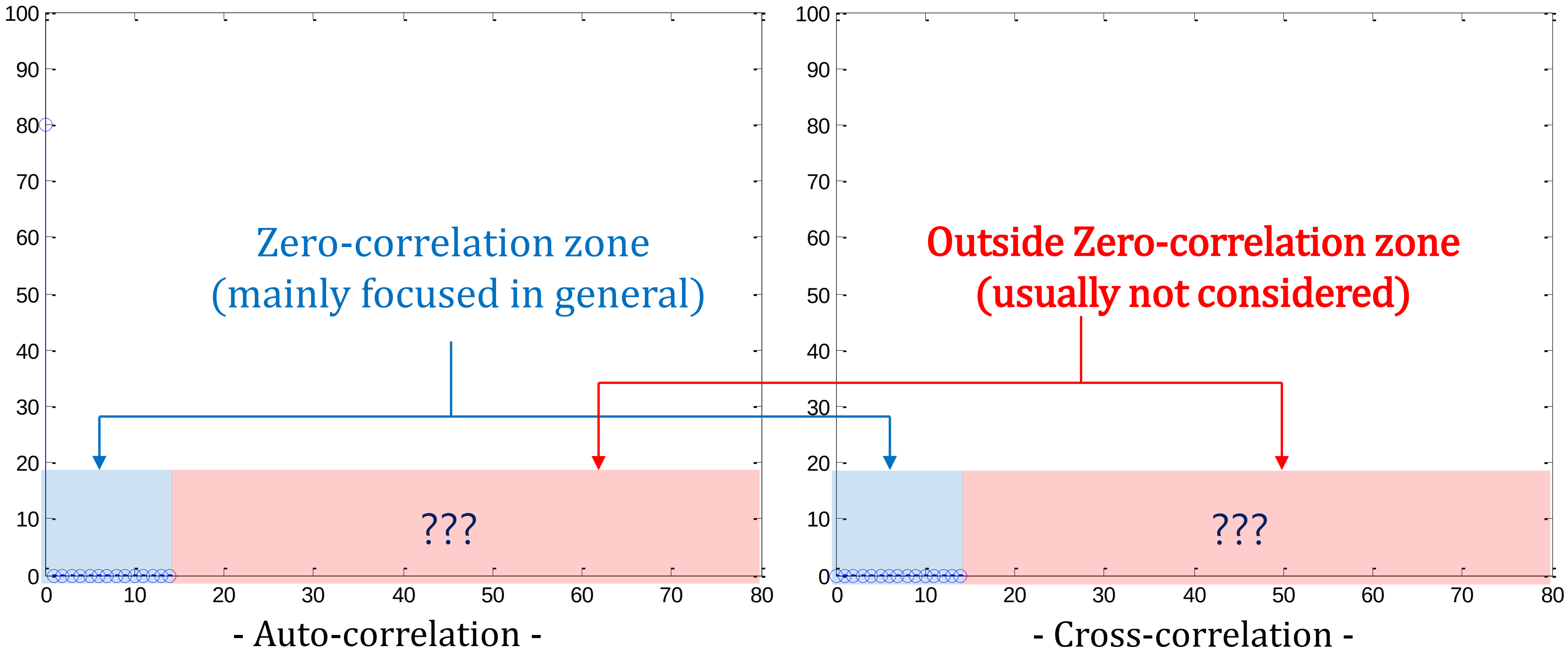
Approximated lower bound: $\sqrt{7}$

Application of the orthogonal code:

ZCZ sequence family construction
with suppressed side-lobes outside ZCZ

What we will consider here

Side-lobes of zero-correlation zone (ZCZ) sequences
outside zero-correlation zone



An example of auto- and cross-correlation of ZCZ sequences

- sequence length : 80
- zero-correlation zone length : 15

ZCZ Sequences

Let $S = \{s_0, s_1, \ldots, s_{m-1}\}$ be a set of sequences of period l. Then, we call S a **(l, m, z) zero-correlation zone (ZCZ) sequence family** if their non-trivial correlation is zero for τ in ZCZ, that is,

$$C_{s_i}(\tau) = 0, \qquad \text{for } 0 < |\tau| < z$$
$$C_{s_i, s_j}(\tau) = 0, \qquad \text{for } 0 \leq |\tau| < z.$$

(bound for zero-correlation zone size)

For a (l, m, z) ZCZ sequence family S, it is always true that

$$z - 1 \leq \frac{l}{m}.$$

S is called **optimal when the equality holds.**

ZCZ sequence family construction

- Many constructions for optimal families have been proposed by using
  - Mutually orthogonal complementary sequence sets (Deng00, Appusewamy06, Liu14, Liu13)
  - Perfect sequences (**Matsufuji03**, Hu10, Tang08, Takatsukasa08, Zhou08)

    By using term-by-term product of a perfect sequence and a maximal orthogonal code.

Term-by-Term product (TBTP)

(Titsworth62)

Let

$a = \{a(t)\}_{t=0}^{l_1-1}$ be an m_1-ary sequence of period l_1 and

$b = \{b(t)\}_{t=0}^{l_2-1}$ be an m_2-ary sequence of period l_2.

The term-by-term product (TBTP) of a and b, denoted by $a \circ b$, is

$$(a \circ b)(t) = \frac{m_2}{\gcd(m_1, m_2)} a(t) + \frac{m_1}{\gcd(m_1, m_2)} b(t) \mod \operatorname{lcm}(m_1, m_2)$$

for $t = 0,1,2, \ldots, l_1 l_2 - 1$.

ZCZ sequence family based on TBTP

(Matsufuji03) **ZCZ sequence family construction based on TBTP**
Let $a = \{a(t)\}_{t=0}^{l_1-1}$ is a perfect sequence over Z_{m_1} and Θ is a maximal orthogonal code of length l_2 over Z_{m_2}. If $\gcd(l_1, l_2) = 1$,

$$a \circ \Theta = \{a \circ \mathrm{b} | b \in \Theta\}$$

forms an $\mathrm{lcm}(m_1, m_2)$-ary optimal $(l_1 l_2, l_2, l_1)$ ZCZ sequence family.

For any two ZCZ sequences $u = a \circ b_1, v = a \circ \mathrm{b}_2$ where $b_1, b_2 \in \Theta$, the cross-correlation between them is of the form

$$C_{u,v}(\tau) = C_a(\tau) C_{b_1,b_2}(\tau) = \begin{cases} z C_{b_1,b_2}(\tau), & \text{if } \tau \equiv 0 \mod z \\ 0, & \text{if } \tau \not\equiv 0 \mod z \end{cases}$$

⇒ To minimize non-zero side-lobes outside ZCZ, we need to design orthogonal codes with good out-of-phase correlation.

ZCZ sequence family with minimized side-lobe outside ZCZ

Construction. Let p be an odd prime greater than 3 and K be the proposed maximal p-ary orthogonal code of period p.
Let a be an m-ary perfect sequence of period l such that $\gcd(p, l) = 1$. Then,

$$\boldsymbol{a} \circ \boldsymbol{K}$$

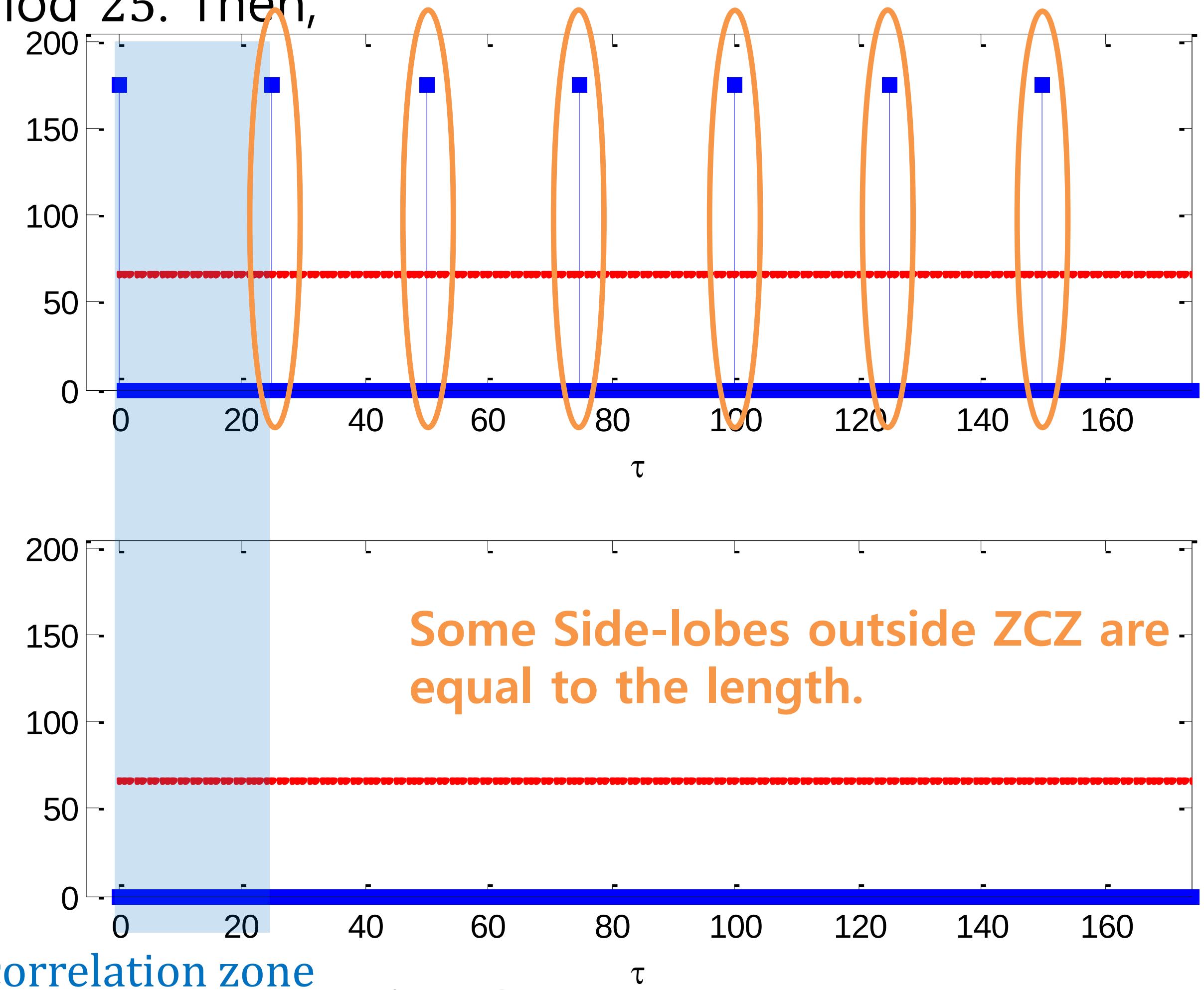
is an optimal (mp)-ary (lp, p, l) ZCZ sequence family whose the maximum magnitude of side-lobe outside ZCZ meets the approximated lower bound.
In other words, **it has minimized side-lobe level outside ZCZ.**

When use ordinary orthogonal code

(Matsufuji03) For example, let Θ be the maximal orthogonal code from the 7×7 DFT matrix. And Let q be the Fermat-quotient sequence of period 25. Then,

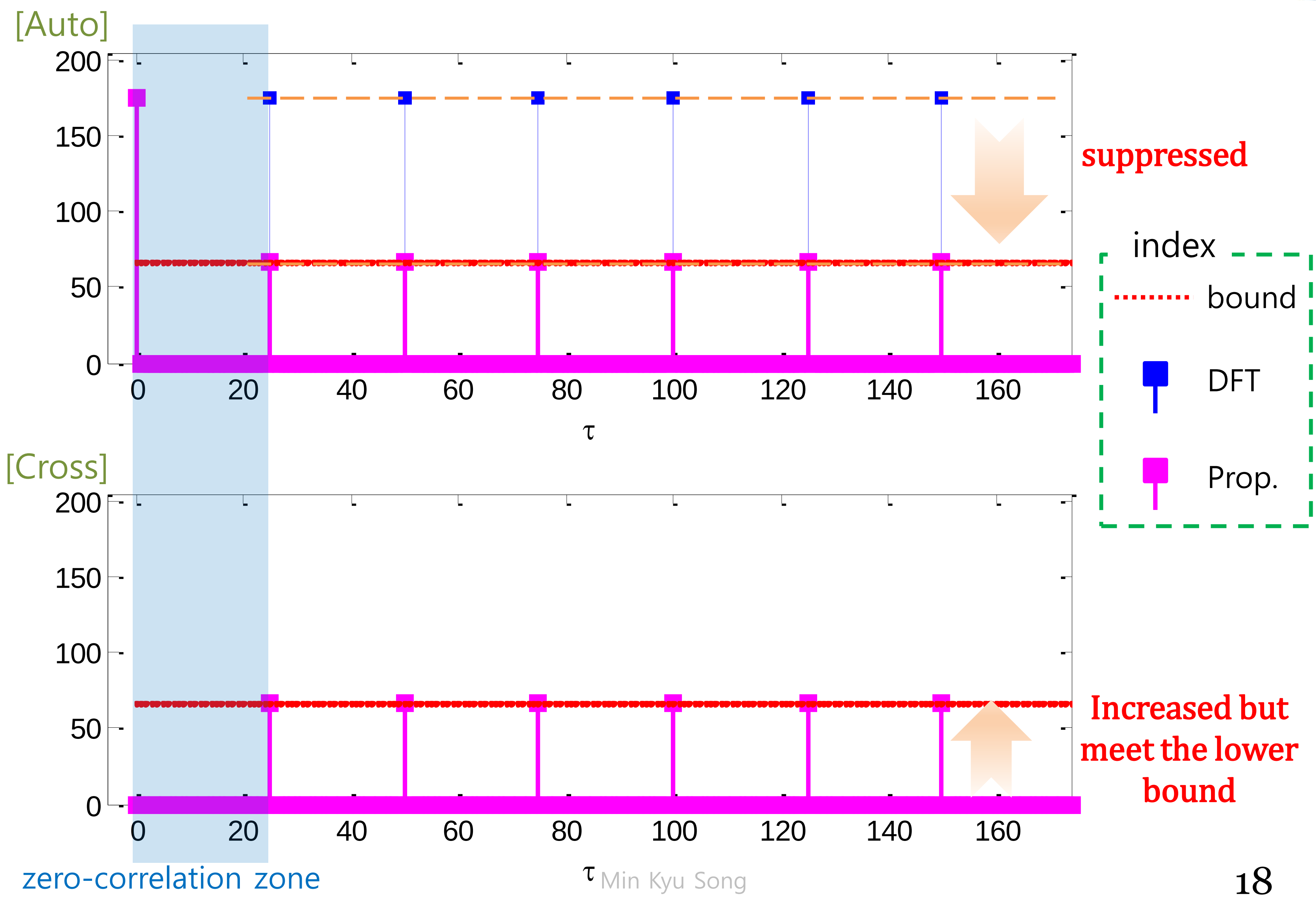
Auto-correlation

Cross-correlation



zero-correlation zone

Comparison



[Auto]
200
150
100
50
0
0
20
40
60
80
100
120
140
160
τ
suppressed
index
bound
DFT
Prop.
[Cross]
200
150
100
50
0
0
20
40
60
80
100
120
140
160
τ
Increased but meet the lower bound
zero-correlation zone

Concluding remarks

- Some orthogonal code of length odd prime may play the role of the Zadoff-Chu sequence in our orthogonal code construction.

Definition. For odd prime $p > 3$ and a non-zero element c in Z_p, let $z(t)$ be a Zadoff-Chu sequence of period p. Define a set K of p sequences $k_0, k_1, \dots, k_{p-1}$ of length p over Z_p as

$$\boldsymbol{k_i} = \{\boldsymbol{k_i(t)} = \boldsymbol{z(t+i)} + \boldsymbol{ct^3} \mathbf{\ mod\ } \boldsymbol{p}\}_{\boldsymbol{t=0}}^{\boldsymbol{p-1}}$$

This can be replaced with codewords in other orthogonal codes