The Investigation on Zero-Correlation Zone among Golay Complementary Pairs

Dian Li

UNIVERSITY OF BERGEN

Contents

Contents

Aperiodic sequences

- An aperiodic sequence of length L:
  $\mathbf{s}_i = (s_i(0), s_i(1), \ldots, s_i(L-1)) = s_i(t)_{t=0}^{L-1}$, where each $s_i(t)$ is a complex number.
  - binary case: $s_i(t) \in \{\pm 1\}$;
  - ternary case: $s_i(t) \in \{\pm 1, 0\}$;
  - N-polyphase case: $s_i(t) \in \{exp(j2\pi i/N), 0 \leq j < N\}$;
- A set $\mathbf{S} = \{\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_{M-1}\}$ is a family of M sequences of length L.
- In this work, we mainly focus on sequence pairs, that is $M = 2$.

Correlation function of sequences

Cross-correlation function

For two length-L complex-valued sequences $\mathbf{a} = (a_0, a_1, \ldots, a_{L-1})$, $\mathbf{b} = (b_0, b_1, \ldots, b_{L-1})$, the aperiodic cross-correlation function of **a** and **b** at a displacement u is

$$\rho(\mathbf{a}, \mathbf{b})(u) = \begin{cases} \sum_{t=0}^{L-u-1} a_{i+u} b_u^*, & 0 \le u < L; \\ \sum_{t=0}^{L+u-1} a_i b_{i-u}^*, & -L < u < 0; \\ 0, & \text{otherwise}, \end{cases}$$

where b^* is the complex conjugate of b.

- If $\mathbf{a} = \mathbf{b}$, $\rho(\mathbf{a}, \mathbf{b})(u)$ is called aperiodic auto-correlation (simply denoted by $\rho(\mathbf{a})(u)$.

Golay complementary pair

- First introduced by Marcel J. E. Golay in 1949[1].
- Pair of sequences with their out-of-phase aperiodic auto-correlation coefficients sum to zero.
- $\rho(\mathbf{a})(u) + \rho(\mathbf{b})(u) = 0, u \neq 0.$
- Existing known binary GCPs only have even-lengths in the form of $2^{\alpha}10^{\beta}26^{\gamma}$ where α, β, γ are non-negative integers[2].
- For odd-length binary pairs. There exists possible zero-correlation zone (ZCZ) width and minimum possible out of zone aperiodic auto-correlation sums[3].
- $\rho(\mathbf{a})(u) + \rho(\mathbf{b})(\tau) = 0$ for $1 \leq u \leq Z$.

---

[1] Marcel JE Golay. 'Multi-slit spectrometry'. In: *JOSA* 39.6 (1949), pp. 437–444.

[2] Matthew G Parker, Kenneth G Paterson and Chintha Tellambura. 'Golay complementary sequences'. In: *Encyclopedia of telecommunications* (2003), pp. 1–18.

[3] Zilong Liu, Udaya Parampalli and Yong Liang Guan. 'Optimal Odd-Length Binary Z-Complementary Pairs'. In: *IEEE Transactions on Information Theory* 60.9 (2014), pp. 5768–5781. ISSN: 0018-9448 1557-9654. DOI: 10.1109/tit.2014.2335731.

Z-Complementary sequences

For a set **S** of M length-L sequences and be represented as

$$\mathbf{S} = \{\mathbf{s}_0, \mathbf{s}_1, \ldots, \mathbf{s}_k, \ldots, \mathbf{s}_{M-1}\}$$

S is called a set of Z-complementary sequences if

$$\sum_{i=0}^{M-1} \rho(\mathbf{s}_i)(u) = \begin{cases} ML, & u = 0 \\ 0, & 1 \leq u \leq Z \end{cases}$$

Z is called **zero correlation zone**(ZCZ).

When $Z = L$ the above definition includes the conventional complementary set as a special case.

We say another set

$$T = \{\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_k, \ldots, \mathbf{t}_{M-1}\}$$

is a Z-complementary mate of S if

$$\sum_{i=0}^{M-1} \rho(\mathbf{s}_i, \mathbf{t}_i)(u) = 0, 0 \leq u \leq Z-1.$$

We say T is the complemenatary mate of S if $Z = L$.

It is shown that the maximum number N of distinct Z-complementary mates is bounded by $N \leq M\lfloor L/Z \rfloor$ which is normally larger than the number of conventional complementary mates.[4]

[4] Pingzhi Fan, Weina Yuan and Yifeng Tu. 'Z-complementary binary sequences'. In: *IEEE Signal Processing Letters* 14.8 (2007), pp. 509–512.

Generalized Boolean Function

A generalized Boolean function $f\colon \mathbb{Z}_2^m \rightarrow \mathbb{Z}_{2^h}$ of m variables $x_1, x_2, \ldots, x_m$ where $h \geq 1$.

Define the monomial of degree r as a product of r variables of the form $x_{j_1} x_{j_2} \ldots x_{j_r}$ where $1 \leq j_1 < j_2 < \cdots < j_r \leq m$.
Then all the monomials are as follows:

$$1, x_1, x_2, \ldots, x_m, x_1x_2, x_1x_3, \ldots, x_{m-1}x_m, \ldots, x_1x_2, \ldots, x_m.$$

Any generalized Boolean function f can be uniquely expressed as a linear combination of these 2^m monomials, where the coefficient of each monomial belongs to $\mathbb{Z}_q$.

For a generalized Boolean function f, we identify a sequence $\mathbf{f} = (f_0, f_1, \ldots, f_{2^m-1})$ of length 2^m corresponding to f where $f_i = f(i_1, i_2, \ldots, i_m)$ and $(i_1, i_2, \ldots, i_m)$ is the binary representation of the integer $i = \sum_{j=1}^{m} i_j 2^{j-1}$.

For example, if we consider $m = 3$, we have

$$\begin{aligned}\mathbf{f} =&(f(0,0,0), f(1,0,0), f(0,1,0), f(1,1,0)\\ &f(0,0,1), f(1,0,1), f(0,1,1), f(1,1,1)).\end{aligned}$$

and so $\mathbf{x_1} = (01010101)$,$\mathbf{x_2} = (00110011)$.

- The construction from generalized Boolean functions has algebraic structure and hence can be friendly for efficient hardware generations.

Contents

Construction of GCP

Theorem

For any integer $m \geq 2$, let π be the permutation of the symbols $\{1, 2, \cdots, m\}$, we denote the generalized boolean function

$$f(x_1, x_2, \cdots, x_m) = \frac{q}{2} \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{m} c_k x_k$$

where q is an even integer and $c_k \in \mathbb{Z}_q$. For any choice $d, d' \in \mathbb{Z}_q$, the pair

$$(\mathbf{a}_0, \mathbf{a}_1) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2} \mathbf{x}_{\pi(1)} + d')$$

is a Golay complementary pair over $\mathbb{Z}_q$ of length 2^m.

[5] James A Davis and Jonathan Jedwab. 'Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes'. In: *IEEE Transactions on information theory* 45.7 (1999), pp. 2397–2417.

Motivation

Based on Davis's construction, let

$$f'(x_1, x_2, \cdots, x_m) = \frac{q}{2} \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{m} c'_k x_k,$$

where π_m is the same as f and $c'_k \in \mathbb{Z}_q$.

Another Goaly sequence pair $(\mathbf{b_0}, \mathbf{b_1}) = (\mathbf{f}' + d, \mathbf{f}' + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ where $c_{\pi_(m-1)} - c_{\pi_(m-1)'} = \frac{q}{2}$ and $c_{\pi_(i)} = c_{\pi_(i)'}$ for $0 \leq i < m-1$. Then $(\mathbf{a_0}, \mathbf{a_1})$ and $(\mathbf{b_0}, \mathbf{b_1})$ have aperiodic cross-correlation ZCZ of $2^{\pi_m(m)-1}$.

Moreover if $c_{\pi_(m)} - c_{\pi_(m)'} = \frac{q}{2}$, then $(\mathbf{a_0}, \mathbf{a_1})$ and $(\mathbf{b_0}, \mathbf{b_1})$ are Golay complementary mates.

- Consider arbitrary two Golay complementary pairs with different coefficients c_i in f and f', how about their ZCZ width?

Main results

Theorem

Let $m \geq 2$ be a integer and π is a permutation on $\{1, 2, \ldots, m\}$ same as f. We denote the generalized boolean function

$$g(x_1, x_2, \cdots, x_m) = \frac{q}{2} \sum_{k=1}^{m-1} x_{\pi(k)} x_{\pi(k+1)} + \sum_{k=1}^{m} c'_k x_k$$

where $c_{\pi(r)} = c'_{\pi(r)}$ for $1 \leq r < t$ and $c_{\pi(t)} - c'_{\pi(t)} = q/2$. Then the pair $(\mathbf{b_0}, \mathbf{b_1})$ given by $(\mathbf{g} + d, \mathbf{g} + \frac{q}{2}\mathbf{x}_{\pi(1)} + d')$ is a ZCP mate of $(\mathbf{a}_0, \mathbf{a}_1)$ with the ZCZ width

$$Z = 2^{\pi(t+1)-1} - \sum_{\substack{k=t+2 \\ \pi(k)<\pi(t+1)}}^{m} 2^{\pi(k)-1}$$

- Given any two Golay complementary pairs based on Davis' construction, the inter set ZCZ width can be determined.
- The lower bound on the ZCZ width of the different Golay complementary pairs is only related to the permutation π in the corresponding function.
- When $\mathcal{S}$ contains only the GCPs and their GCP mates. According to the bound when $Z = L$, the the set size $M \leq 2$.
- Consider a set of Golay complementary pairs with the set size $M \geq 2$, what is the ZCZ among different pairs? Can we construct such a set with maximum ZCZ width among each pairs?

Definition

For a set of Golay complementary pairs $\mathcal{S} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_M\}$, where each $\mathbf{C}_i$ is a $2 \times L$ matrix for $1 \leq i \leq M$. Let $Z_{i,j}$ be the mutual ZCZ width between between $\mathbf{C}_i$ and $\mathbf{C}_j$ for $1 \leq i, j \leq M$. The average ZCZ of the set $\mathcal{S}$ is

$$Z_{avg} = \frac{\sum_{i=1}^{M} \sum_{j=1}^{M} Z_{i,j}}{M^2}.$$

We consider the set $\mathcal{S}$ composed by the GCPs corresponding to all possible coefficients c_i where $1 \leq i \leq m$.

- The set generated by f with all possible coefficients c if of size 2^m.
- Z_{avg} is related to the permutation π only.

Average zero correlation zone

We first consider a group of cyclic shift permutations:

Property

Let $\Pi^t = (t+1, t+2, \ldots, m, 1, 2, \ldots, t)$ be a cyclic shift permutaion with $0 \leq t \leq m-1$. For any choice $d, d' \in \mathbb{Z}_q$, the set $\mathcal{C}^t$ consists all 2^m sequence pairs generated by $(\mathbf{a}, \mathbf{b}) = (\mathbf{f} + d, \mathbf{f} + \frac{q}{2}\mathbf{x}_{\Pi^t(1)} + d')$. Denoted the average ZCZ of any two sequence pairs in $\mathcal{C}^t$ by Z_{avg} then

$$Z_{avg} = 2^t(m-t-2) + 3 + \frac{2^{t+1} + t - 2}{2^{m-t}}.$$

- When m increasing, the ratio of the maximum average ZCZ over whole sequence length decreases.
- The maximum average ZCZ achieves at $t = m - 3$.

For all possible permutations on $\{1, \ldots, m\}$, on which permutation the set $\mathcal{S}$ has the largest average ZCZ width?

Theorem

Let σ_m the permutation such that $\mathcal{S}$ has largest Z_{avg}. Then $\sigma_m = \{m-2, m-1, m, i_1, \ldots, i_m\}$ where $(i_1, i_2, \ldots, i_{m_3}) = \sigma_{m-3}$ and $m \geq 4$. $\sigma_1 = (1), \sigma_2 = (1, 2), \sigma_1 = (1, 2, 3)$

Future work

- How about the ZCZ width of GCPs generated by different permutaions.
- Construct a set of more GCPs for a given Z_{avg}.
- Derive new bound towards the average ZCZ width.

Thank You

Reference

[1] Marcel JE Golay. 'Multi-slit spectrometry'. In: *JOSA* 39.6 (1949), pp. 437–444.

[2] Matthew G Parker, Kenneth G Paterson and Chintha Tellambura. 'Golay complementary sequences'. In: *Encyclopedia of telecommunications* (2003), pp. 1–18.

[3] Zilong Liu, Udaya Parampalli and Yong Liang Guan. 'Optimal Odd-Length Binary Z-Complementary Pairs'. In: *IEEE Transactions on Information Theory* 60.9 (2014), pp. 5768–5781. ISSN: 0018-9448 1557-9654. DOI: 10.1109/tit.2014.2335731.

[4] Pingzhi Fan, Weina Yuan and Yifeng Tu. 'Z-complementary binary sequences'. In: *IEEE Signal Processing Letters* 14.8 (2007), pp. 509–512.

[5] James A Davis and Jonathan Jedwab. 'Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes'. In: *IEEE Transactions on information theory* 45.7 (1999), pp. 2397–2417.