Pair of Binary Sequences with Ideal Two-Level Crosscorrelation

Seok-Yong Jin and Hong-Yeop Song

{sy.jin, hysong}@yonsei.ac.kr
Coding and Crypto Lab
Yonsei University, Seoul, KOREA

2008 IEEE International Symposium on Information Theory
Toronto, Canada
July 6-11, 2008

Outline

Definition of Correlation

- $\mathbf{a} = (a_0, \cdots, a_{v-1})$ and $\mathbf{b} = (b_0, \cdots, b_{v-1})$: binary $(0,1)$-sequences of length v
- Periodic correlation function

$$\theta_{a,b}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i + b_{i+\tau}}$$

Ideal 2-level Correlation: Single Sequence

- 2-level (auto)-correlation of a sequence ($\Leftrightarrow$ **cyclic difference set**)

$$\theta_{a,a}(\tau) = \begin{cases} v & ,\tau = 0 \\ \gamma(\neq v) & ,otherwise. \end{cases}$$

- Ideal 2-level (auto)-correlation
  - Small $|\gamma|$ is desirable for various applications
  - $\gamma = 0$: currently no such example found, except for $v = 4$
  - $\gamma = -1$: called ideal 2-level autocorrelation (m-sequences, GMW sequences, 3-term and 5-term sequences, etc.)

Ideal 2-level Correlation: Sequence Pair

- Generalization to pair of binary sequences
- Binary sequence pair $(\mathbf{a}, \mathbf{b})$ has 2-level correlation if

$$\theta_{a,b}(\tau) = \begin{cases} \Gamma_1 & , \tau = 0 \\ \Gamma_2 (\neq \Gamma_1) & , \tau \neq 0 \pmod{v}, \end{cases}$$

- $\Gamma_2 = 0$: Ideal 2-level correlation

$$\theta_{a,b}(\tau) = \begin{cases} \Gamma(\neq 0) & , \tau = 0 \\ 0 & , \text{else.} \end{cases}$$

Notations

$\mathbf{s} = (s_0, s_1, \cdots, s_{v-1})$: binary sequence of period v

- Support set and characteristic sequence
  - Support set: $supp(\mathbf{s}) = \{i | s_i = 1, 0 \le i \le v-1\} \subset \mathbb{Z}_v$ ($\mathbf{s}$ is called the characteristic sequence)
  - Weight: $wt(\mathbf{s}) = |\{i | s_i = 1, 0 \le i \le v-1\}| = \left| supp(\mathbf{s}) \right|$
- Operations on binary sequences
  - Cyclic shift: $\rho^i(\mathbf{s}) = (s_i, s_{i+1}, \cdots, s_{i+v-1})$
  - Decimation: $\mathbf{s}^{(d)} = \left(s_{d\cdot 0}, s_{d\cdot 1}, \cdots, s_{d\cdot (v-1)} \right)$
  - Negation: $\mathbf{s}' = \left(s'_0, \cdots, s'_{v-1} \right)$, where $s'_i = 1$ if $s_i = 0$ and $s'_i = 0$ if $s_i = 1$
  - Alternation at even positions: $\mathbf{s}_E = \left(s'_0, s_1, s'_2, s_3, \cdots \right)$

Notations

$\mathbf{s} = (s_0, s_1, \cdots, s_{v-1})$: binary sequence of period v

- Support set and characteristic sequence
- Operations on binary sequences
- Hall polynomial: $h_s(z) = s_0 + s_1 z^1 + \cdots + s_{v-1} z^{v-1} \pmod{z^v - 1}$
- Canonical form of circulant matrix associated with $\mathbf{s}$:

$$M_s = \begin{bmatrix} s_0 & s_{v-1} & s_{v-2} & \dots & s_1 \\ s_1 & s_0 & s_{v-1} & \dots & s_2 \\ s_2 & s_1 & s_0 & \dots & s_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{v-1} & s_{v-2} & s_{v-3} & \dots & s_0 \end{bmatrix}$$

The sequence $\mathbf{s}$ is called the defining array of M_s.

Correlation Coefficients by Set Notation

- $(\mathbf{a}, \mathbf{b})$: binary sequence pair of length v
  $A := supp(\mathbf{a})$, $B := supp(\mathbf{b})$, $k_a := wt(\mathbf{a})$, $k_b := wt(\mathbf{b})$
  $k := |A \cap B|$, $d_{A,B}(\tau) = |A \cap (\tau + B)|$
- Calculation of correlation coefficients of binary sequences

$$
\begin{array}{rcccc}
\mathbf{a}: & 1\cdots1 & 1\cdots1 & 0\cdots0 & 0\cdots0 \\
\rho^{\tau}(\mathbf{b}): & \underbrace{1\cdots1} & \underbrace{0\cdots0} & \underbrace{1\cdots1} & \underbrace{0\cdots0} \\
\#\text{ of times}: & d_\tau & k_a - d_\tau & k_b - d_\tau & v - (k_a + k_b) + d_\tau
\end{array}
$$

$$
\boxed{\theta_{a,b}(\tau) = v - 2(k_a + k_b) + 4d_{A,B}(\tau)}
$$

- For a sequence pair $(\mathbf{a}, \mathbf{b})$ with ideal 2-level correlation:

$$
\begin{array}{lcl}
d_{A,B}(0) = k & \Rightarrow & \Gamma = v - 2(k_a + k_b) + 4k \\
d_{A,B}(\tau) = \lambda, \forall \tau \neq 0 & \Rightarrow & 0 = v - 2(k_a + k_b) + 4\lambda
\end{array}
$$

Cyclic Difference Pair (CDP)

- Binary sequence with 2-level correlation ⇔ cyclic difference set
- Binary sequence pair with 2-level correlation ⇔ ?

Definition (Cyclic Difference Pair)

- X and Y: k_x-subset and k_y-subset of $\mathbb{Z}_v$ with $|X \cap Y| = k$
- (X, Y) is a $(v, k_x, k_y, k, \lambda)$-cyclic difference pair (CDP) if
- For every nonzero $w \in \mathbb{Z}_v$, w is expressed in exactly λ ways in the form $w = x - y \pmod{v}$ where $x \in X$ and $y \in Y$.
- Especially when $v = 2(k_1 + k_2) - 4\lambda$ and $k \neq \lambda$, it is called an ideal cyclic difference pair.

Relation: CDP and Binary Sequence Pair

Theorem (Existence and Relation)

- $(\mathbf{a}, \mathbf{b})$*: binary sequence pair of period* v *with 2-level correlation such that*
  - *In-phase correlation coefficient:* Γ
  - *Out-of-phase correlation coefficients:* γ
  - $wt(\mathbf{a}) = k_a$ *and* $wt(\mathbf{b}) = k_b$
- *Their support set pair* (A, B) *forms a* $(v, k_a, k_b, k, \lambda)$*-cyclic difference pair, where*
  - $k = |A \cap B|$ *satisfies* $\Gamma = v - 2(k_a + k_b) + 4k$
  - λ *is such that* $\gamma = v - 2(k_a + k_b) + 4\lambda$.
- *Moreover, any cyclic difference pair arises in this way.*

Characterization: Three Equations

1. Inphase and out-of-phase correlation coefficient:

$$v - 2(k_a + k_b) + 4k = \Gamma \tag{e-I}$$

$$v - 2(k_a + k_b) + 4\lambda = 0 \tag{e-II}$$

2. Counting the number of elements of $A \times B$:

$$k_a k_b = \lambda v + (k - \lambda) \tag{e-III}$$

- If there exists a binary sequence pair of period v having ideal 2-level correlation, then v is even.
- $\Gamma = 4(k - \lambda)$

Characterization: using Hall Polynomial

- A, B: k_a-subset and k_b-subset of $\mathbb{Z}_v$ with $|A \cap B| = k$
- $\mathbf{a}, \mathbf{b}$: the characteristic binary sequences of A and B of period v

Theorem

- *Let $h_a(z)$ and $h_b(z)$ denote the associated hall polynomial of* $\mathbf{a}$ *and* $\mathbf{b}$*, respectively.*
- *Then (A, B) is a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair if and only if*

$$h_a(z)\, h_b(z^{-1}) = (k - \lambda) + \lambda(1 + z + \cdots + z^{v-1})$$

Characterization: using Circulant Matrix

Under the same notations: A, B, (k_a and k_b-subset), $k = |A \cap B|$, and $\mathbf{a}$ and $\mathbf{b}$

Theorem

- *M_a, M_b: canonical form of the circulant matrix associated with* $\mathbf{a}$ *and* $\mathbf{b}$
- *(A, B) is a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair, if and only if*

$$M_a {M_b}^T = (k - \lambda)I + \lambda J$$

- *Matrices are viewed over the integers or over the reals.*

Necessary Condition: Determinants

- (A, B): $(v, k_a, k_b, k, \lambda)$-cyclic difference pair
- $(\mathbf{a}, \mathbf{b})$: the corresponding characteristic binary sequence pair

Theorem

Let M_a and M_b be the canonical form of circulant matrices associated with $\mathbf{a}$ *and* $\mathbf{b}$*, respectively. Then*

$$det(M_a) \cdot det(M_b) = k_a k_b (k - \lambda)^{v-1}$$

Property Preserving Transformations

If (A, B) is an ideal $(v, k_a, k_b, k, \lambda)$-cyclic difference pair:

Cyclic Difference Pair	Parameters
$(\tau + A, \tau + B)$, $\tau = 0, 1, \ldots$	$(v, k_a, k_b, k, \lambda)$
$\left(A^{(d)}, B^{(d)}\right)$, $gcd(d, v) = 1$	$(v, k_a, k_b, k, \lambda)$
(B, A) (A, B^C) (A^C, B) (A^C, B^C)	$(v, k_b, k_a, k, \lambda)$ $(v, k_a, v - k_b, k_a - k, k_a - \lambda)$ $(v, v - k_a, k_b, k_b - k, k_b - \lambda)$ $(v, v - k_a, v - k_b, k', \lambda')$, $k' = v - (k_a + k_b) + k$, $\lambda' = v - (k_a + k_b) + \lambda$
(A_E, B_E)	$(v, k''_a, k''_b, k'', \lambda'')$, $k''_a = k_a + (v/2 - 2e_a)$, $k''_b = k_b + (v/2 - 2e_b)$, $k'' = k + (v/2 - (e_a + e_b))$, $\lambda'' = \lambda + (v/2 - (e_a + e_b))$

Parameterizations

For any $(v, k_a, k_b, k, \lambda)$-cyclic difference pair, we assume without loss of generality:

$$v/2 \geq k_a \geq k_b \geq k > \lambda, \text{ and}$$

$$\lambda > 0 \text{ for } v > 4$$

- $4(k - \lambda) = (v - 2k_a)(v - 2k_b)$
- $\Gamma = 4(k - \lambda) \neq 0 \Rightarrow k \gneq \lambda.$
- If $\lambda = 0$: $k_a = k_b = k = 1$, $\mathbf{a} = \mathbf{b} = (1000)$.

Ideal CDP with $k-\lambda=1$: Parameterizations

Theorem

If an ideal (v,k_a,k_b,k,λ)-cyclic difference pair with $k-\lambda=1$ exists, then

$$(v,k_a,k_b,k,\lambda)=(4t,\ 2t-1,\ 2t-1,\ t,\ t-1)$$

Note:

- $(v,k,\lambda)=(4t-1,2t-1,t-1)$: cyclic difference set with Hadamard parameters
- $(v,k_a,k_b,k,\lambda)=(4t,2t-1,2t-1,t,t-1)$: cyclic difference pair with “Hadamard" parameters

Ideal CDP with $k-\lambda=1$: Construction

$$det(M_a)\cdot det(M_b) = k_a k_b (k-\lambda)^{v-1}$$

$$k-\lambda=1 : det(M_a)\cdot det(M_b) = k_a \cdot k_b$$

Q: **a** and **b** with $det(M_a) = k_a$ and $det(M_b) = k_b$??

- One part: If the sequence **a** is such that

$$\mathbf{a} = (\ \underbrace{\overbrace{11\cdots1}^{2t-1}\overbrace{00\cdots0}^{2t+1}}_{4t}\ )\ ,$$

  then $$det(M_a) = 2t-1 = wt(\mathbf{a}).$$

- The other part: even position negation and shift of **a**

Ideal CDP with $k - \lambda = 1$: Construction

Theorem (cyclic Hadamard difference pair)

- *Let $v = 4t$ and $k_a = k_b = 2t - 1$.*
- *Define k_a-subset A and k_b-subset B of $\mathbb{Z}_v$ as*

$$A = \{0, 1, \cdots, 2t-2\}$$
$$B = \{0, 2, \cdots, 2t-2,\ 2t+1, 2t+3, \cdots, 4t-3\}.$$

- *(A, B) is a $(4t, 2t-1, 2t-1, t, t-1)$-CDP with $k - \lambda = 1$.*

Example ($v = 12$)

	0	1	2	3	4	5	6	7	8	9	10	11
a	**1**	1	**1**	1	**1**	0	**0**	0	**0**	0	**0**	0
b	**1**	0	**1**	0	**1**	0	**0**	1	**0**	1	**0**	0

Parameters for exhaustive search

Table I. $4 < v \leq 30,\ v \equiv 2 \pmod 4$

v	k_a	k_b	k	λ	$k-\lambda$
6	-	-	-	-	-
10	4	3	3	1	2
14	6	5	4	2	2
18	8	7	5	3	2
22	10	9	6	4	2
	10	7	7	3	4
26	12	11	7	5	2
	12	9	8	4	4
	11	10	10	4	6
30	14	13	8	6	2
	14	11	9	5	4
	13	12	11	5	6

Table II. $4 < v \leq 30,\ v \equiv 0 \pmod 4$

v	k_a	k_b	k	λ	$k-\lambda$
8	3	3	2	1	1
12	5	5	3	2	1
16	7	7	4	3	1
	7	5	5	2	3
	6	6	6	2	4
20	9	9	5	4	1
	9	7	6	3	3
	8	8	7	3	4
24	11	11	6	5	1
	11	9	7	4	3
	10	10	8	4	4
28	13	13	7	6	1
	13	11	8	5	3
	12	12	9	5	4
	13	9	9	4	5

Search Results for $v \leq 30$

- If $v \equiv 2 \pmod 4$, there is NO ideal cyclic difference pair of period $v \leq 30$.
- If there exists an ideal $(v, k_a, k_b, k, \lambda)$-cyclic difference pair of period $v \equiv 0 \pmod 4$, it has Hadamard parameters $k - \lambda = 1$, for $v \leq 30$.
- Moreover, every cyclic Hadamard difference pair found by exhaustive computer search is equivalent to that by the construction given in our Theorem under the combination of transformations introduced.

Concluding Remarks

Our expectation ("Conjecture") concerning the existence and uniqueness of cyclic difference pair:

If an ideal $(v, k_a, k_b, k, \lambda)$*-cyclic difference pair exists,*

1. $v = 0 \pmod 4$
2. $|k - \lambda| = 1$ *(*$\Rightarrow \Gamma = 4(k - \lambda) = 4$*)*
3. *By some combination of transformations, it can be transformed to the cyclic Hadamard difference pair introduced.*

Note that the second statement imply
Circulant Hadamard matrix conjecture.