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

1. Introduction
2. Structure and Property of Associated Cyclic Difference Pair
3. Ideal Cyclic Difference Pair with $k - \lambda = 1$: Parameterizations and Construction
4. Exhaustive Search for Short Lengths
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

\[
\theta_{a,b}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i + b_{i+\tau}}
\]
2-level (auto)-correlation of a sequence (↔ cyclic difference set)

\[
\theta_{a,a}(\tau) = \begin{cases} 
  v, & \tau = 0 \\
  \gamma (\neq v), & \text{otherwise}
\end{cases}
\]

**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.)
Generalization to pair of binary sequences

Binary sequence pair \((a, b)\) has 2-level correlation if

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

\(\Gamma_2 = 0: \text{Ideal 2-level correlation}\)

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

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

- **Support set and characteristic sequence**
  - Support set: \( \text{supp}(s) = \{i|s_i = 1, 0 \leq i \leq v - 1\} \subset \mathbb{Z}_v \) (\( s \) is called the characteristic sequence)
  - Weight: \( \text{wt}(s) = |\{i|s_i = 1, 0 \leq i \leq v - 1\}| = |\text{supp}(s)| \)

- **Operations on binary sequences**
  - Cyclic shift: \( \rho^i(s) = (s_i, s_{i+1}, \cdots, s_{i+v-1}) \)
  - Decimation: \( s^{(d)} = (s_{d \cdot 0}, s_{d \cdot 1}, \cdots, s_{d \cdot (v-1)}) \)
  - Negation: \( s' = (s'_0, \cdots, s'_{v-1}) \), where \( s'_i = 1 \) if \( s_i = 0 \) and \( s'_i = 0 \) if \( s_i = 1 \)
  - Alternation at even positions: \( s_E = (s'_0, s_1, s'_2, s_3, \cdots) \)
Notations

\( s = (s_0, s_1, \cdots, s_{v-1}) \): 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 \( s \):

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

The sequence \( s \) is called the **defining array** of \( M_s \).
(\(a, b\)): binary sequence pair of length \(v\)

\[ A := supp(a), B := supp(b), k_a := wt(a), k_b := wt(b) \]
\[ k := |A \cap B|, d_{A,B}(\tau) = |A \cap (\tau + B)| \]

Calculation of correlation coefficients of binary sequences

\[
\begin{align*}
\text{a} & : \quad 1 \cdots 1 \quad 1 \cdots 1 \quad 0 \cdots 0 \quad 0 \cdots 0 \\
\rho^\tau(b) & : \quad 1 \cdots 1 \quad 0 \cdots 0 \quad 1 \cdots 1 \quad 0 \cdots 0 \\
\text{# of times:} & \quad d_\tau \quad k_a - d_\tau \quad k_b - d_\tau \quad v - (k_a + k_b) + d_\tau
\end{align*}
\]

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

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

\[
d_{A,B}(0) = k \quad \Rightarrow \quad \Gamma = v - 2(k_a + k_b) + 4k \\
d_{A,B}(\tau) = \lambda, \forall \tau \neq 0 \quad \Rightarrow \quad 0 = v - 2(k_a + k_b) + 4\lambda
\]
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 $\lambda$ 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.
Theorem (Existence and Relation)

- \((a, b)\): binary sequence pair of period \(v\) with 2-level correlation such that
  - In-phase correlation coefficient: \(\Gamma\)
  - Out-of-phase correlation coefficients: \(\gamma\)
  - \(wt(a) = k_a\) and \(wt(b) = k_b\)

- Their support set pair \((A, B)\) forms a \((v, k_a, k_b, k, \lambda)\)-cyclic difference pair, where
  - \(k = |A \cap B|\) satisfies \(\Gamma = v - 2(k_a + k_b) + 4k\)
  - \(\lambda\) 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:

\[ v - 2(k_a + k_b) + 4k = \Gamma \]  \hspace{2cm} (e-I)

\[ v - 2(k_a + k_b) + 4\lambda = 0 \]  \hspace{2cm} (e-II)

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

\[ k_a k_b = \lambda v + (k - \lambda) \]  \hspace{2cm} (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 $|A \cap B| = k$
- $a, b$: 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 $a$ and $b$, 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 $a$ and $b$

**Theorem**

- $M_a$, $M_b$: canonical form of the circulant matrix associated with $a$ and $b$
- $(A, B)$ is a $(v, k_a, k_b, k, \lambda)$-cyclic difference pair, if and only if
  \[M_aM_b^T = (k - \lambda)I + \lambda J\]

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

Let $M_a$ and $M_b$ be the canonical form of circulant matrices associated with $a$ and $b$, 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:

<table>
<thead>
<tr>
<th>Cyclic Difference Pair</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>((\tau + A, \tau + B),\ \tau = 0, 1, \ldots)</td>
<td>((v, k_a, k_b, k, \lambda))</td>
</tr>
<tr>
<td>((A^{(d)}, B^{(d)}),\ \gcd(d, v) = 1)</td>
<td>((v, k_a, k_b, k, \lambda))</td>
</tr>
<tr>
<td>((B, A))</td>
<td>((v, k_b, k_a, k, \lambda))</td>
</tr>
<tr>
<td>((A, B^C))</td>
<td>((v, k_a, v - k_b, k_a - k, k_a - \lambda))</td>
</tr>
<tr>
<td>((A^C, B))</td>
<td>((v, v - k_a, k_b, k_b - k, k_b - \lambda))</td>
</tr>
<tr>
<td>((A^C, B^C))</td>
<td>((v, v - k_a, v - k_b, k', \lambda')), (k' = v - (k_a + k_b) + k), (\lambda' = v - (k_a + k_b) + \lambda)</td>
</tr>
<tr>
<td>((A_E, B_E))</td>
<td>((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)))</td>
</tr>
</tbody>
</table>
For any \((v, k_a, k_b, k, \lambda)\)-cyclic difference pair, we assume without loss of generality:

\[
\frac{v}{2} \geq k_a \geq k_b \geq k > \lambda, \text{ and } \\
\lambda > 0 \text{ for } v > 4
\]

- \(4(k - \lambda) = (v - 2k_a)(v - 2k_b)\)
- \(\Gamma = 4(k - \lambda) \neq 0 \Rightarrow k \geq \lambda.\)
- If \(\lambda = 0\): \(k_a = k_b = k = 1, \ a = b = (1000).\)
**Theorem**

If an ideal \((v, k_a, k_b, k, \lambda)\)-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: \textbf{a} and \textbf{b} with \( \det(M_a) = k_a \) and \( \det(M_b) = k_b \)?

- **One part**: If the sequence \textbf{a} is such that

\[
\begin{pmatrix}
2t - 1 & 2t + 1 \\
11 \cdots 1 & 00 \cdots 0 \\
4t
\end{pmatrix},
\]

then

\[
\det(M_a) = 2t - 1 = \text{wt}(\textbf{a}).
\]

- **The other part**: even position negation and shift of \textbf{a}
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 ($v = 12$)

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>b</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Parameters for exhaustive search

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

<table>
<thead>
<tr>
<th>$v$</th>
<th>$k_a$</th>
<th>$k_b$</th>
<th>$k$</th>
<th>$\lambda$</th>
<th>$k - \lambda$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>14</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>18</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>22</td>
<td>10</td>
<td>9</td>
<td>6</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>7</td>
<td>7</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>26</td>
<td>12</td>
<td>11</td>
<td>7</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>9</td>
<td>8</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>10</td>
<td>10</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>30</td>
<td>14</td>
<td>13</td>
<td>8</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>11</td>
<td>9</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>12</td>
<td>11</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>$v$</th>
<th>$k_a$</th>
<th>$k_b$</th>
<th>$k$</th>
<th>$\lambda$</th>
<th>$k - \lambda$</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>12</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>7</td>
<td>7</td>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>5</td>
<td>5</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>20</td>
<td>9</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>7</td>
<td>6</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>8</td>
<td>7</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>24</td>
<td>11</td>
<td>11</td>
<td>6</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>9</td>
<td>7</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>10</td>
<td>8</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>28</td>
<td>13</td>
<td>13</td>
<td>7</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>11</td>
<td>8</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>12</td>
<td>9</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>9</td>
<td>9</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>
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. \(|k - \lambda| = 1 \implies \Gamma = 4(k - \lambda) = 4\)
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.