Problems in Cyclic Hadamard Difference Sets: Introduction and Current Results

송홍엽
연세대학교 전기전자공학부
hy.song@coding.yonsei.ac.kr

School of Electrical and Electronics Engineering,
Yonsei University, Seoul, Korea.
Contents

- Introduction to cyclic Hadamard difference sets (CHDS, in short)
- Some applications of CHDS or balanced binary sequences with ideal autocorrelation
- Description of “known” CHDS (Conjecture on the characterization on m-sequences)
- Brief history and results on the existence of CHDS (Main conjecture)
- Summary
- Reference
I. Introduction

Definition 1 A \((v, k, \lambda)\) cyclic difference set \(D\) is a \(k\)-subset of \(\mathbb{Z}_v \triangleq \mathbb{Z}/v\mathbb{Z}\) such that for all non-zero \(d \in \mathbb{Z}_v\) the equation

\[ x - y \equiv d \pmod{v} \]

has exactly \(\lambda\) solution pairs \((x, y)\) with \(x, y \in D\).

Example 1 The set \(\{1, 3, 4, 5, 9\}\) is a \((11, 5, 2)\)-CDS, since

\[ \begin{array}{cccccc}
- & 1 & 3 & 4 & 5 & 9 \\
1 & 0 & 9 & 8 & 7 & 3 \\
3 & 2 & 0 & 10 & 9 & 5 \\
4 & 3 & 1 & 0 & 10 & 6 \\
5 & 4 & 2 & 1 & 0 & 7 \\
9 & 8 & 6 & 5 & 4 & 0 \\
\end{array} \]
Some Basic Theory

1. [Lemma] Let $D = \{d_1, d_2, ..., d_k\}$ be a $(v, k, \lambda)$-cyclic difference set. Then, so are

   (Cyclic) Shift: $s + D \triangleq \{ s + d_i \mid 1 \leq i \leq k \}$ for any integer $s$, and

   Decimation: $tD \triangleq \{ td_i \mid 1 \leq i \leq k \}$ for any integer $t$ with $(t, v) = 1$.

2. [Definition] Let $t$ be an integer with $(t, v) = 1$. Then $t$ is called a “multiplier” of $D$ if there exists $s$ such that

   $$tD = D + s.$$ 

3. [Theorem] If $D$ is a $(v, k, \lambda)$-cyclic difference set with a multiplier $t$, then there exists a shift $D'$ of $D$ such that

   $$tD' = D'.$$

   $\implies$ this gives an easy “constructive test” for the existence of a $(v, k, \lambda)$-CDS.

4. [Theorem] Let $D$ be a $(v, k, \lambda)$-cyclic difference set. If $p$ is a prime such that

   $$p \mid k - \lambda, \quad p \nmid v, \quad p > \lambda$$

   then $p$ is a multiplier of $D$. 

Hong-Yeop Song  School of E.& E. Engineering, Yonsei Univ.
Example 2 Does there exist a \((13, 3, 1)\)-CDS?

Find a multiplier of the potential CDS \(D\):

\[ p = 2 | 2 = k - \lambda, \quad 2 \nmid 13, \quad \text{and} \quad 2 > \lambda = 1. \]

Therefore, \( t = 2 \) must be a multiplier of such \( D \) (if it exists).

\[ \implies \text{There must exist a shift } D' \text{ that is fixed by } 2, \text{ that is } 2D' = D'. \]

\[ \implies \text{If } a \in D' \text{ then } 2a \in D'. \]

\[ \implies \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\} \subset D'. \]

\[ \implies D' = \{0\} \text{ or } D' = \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\} = \mathbb{Z}_{13}\backslash\{0\}. \]

Since \( D' \) is of size 3, we conclude that no such CDS exists.
Example 3 Does there exist a \((13, 4, 1)\)-CDS?

Find a multiplier of the potential CDS \(D\):

\[
p = 3|k - \lambda, \quad 3 \nmid 13, \quad \text{and} \quad 3 > \lambda = 1.
\]

Therefore, \(t = 3\) must be a multiplier of such \(D\) (if it exists).

\(\Rightarrow\) There must exist a shift \(D'\) that is fixed by 3, that is \(3D' = D'\).

\(\Rightarrow\) If \(a \in D'\) then \(3a \in D'\).

Therefore, \(D'\) must be a union of some of the following:

\[
\begin{align*}
\{0\} & \quad - & \quad 0 & \quad 1 & \quad 3 & \quad 9 \\
\{1, 3, 9\} & & 0 & 12 & 10 & 4 \\
\{2, 6, 5\} & \Rightarrow \text{try one choice as} & 1 & 1 & 0 & 11 & 5 \\
\{4, 12, 10\} & & 3 & 3 & 2 & 0 & 7 \\
\{7, 8, 11\} & & 9 & 9 & 8 & 6 & 0
\end{align*}
\]

\(\Rightarrow\) Therefore, \(\{0, 1, 3, 9\}\) is a \((13, 4, 1)\)-CDS.
**Why are we doing this?**

- Construct a binary sequence of period \( v = 13 \) from \((13, 4, 1)\)-CDS found earlier, which is \( \{0, 1, 3, 9\} \), as:

\[
\begin{align*}
i & : \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \\
\downarrow & \quad \downarrow \quad \downarrow \\
\text{s}(i) & : \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \\
\text{s}(i+1) & : \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \\
\text{s}(i+2) & : \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \\
\end{align*}
\]

- In reality, we calculate the dot-product of the following:

\[
\begin{align*}
(-1)^{\text{s}(i)} & : \quad +1 \quad +1 \quad -1 \quad +1 \quad -1 \quad -1 \quad -1 \quad +1 \quad -1 \quad -1 \quad -1 \\
(-1)^{\text{s}(i+1)} & : \quad +1 \quad -1 \quad +1 \quad -1 \quad -1 \quad -1 \quad -1 \quad +1 \quad -1 \quad -1 \quad +1 \\
(-1)^{\text{s}(i+2)} & : \quad -1 \quad +1 \quad -1 \quad -1 \quad -1 \quad -1 \quad +1 \quad -1 \quad -1 \quad -1 \quad +1 \quad +1 \\
\end{align*}
\]

\[
\phi(1) = \sum_{0\leq i<13} (-1)^{\text{s}(i)+\text{s}(i+1)} = (+7) + (-6) = 1.
\]

\[
\phi(2) = \sum_{0\leq i<13} (-1)^{\text{s}(i)+\text{s}(i+2)} = (+7) + (-6) = 1.
\]
• Define the un-normalized autocorrelation $\phi(\tau)$ of ANY binary sequence of period $v$ as

$$\phi(\tau) = \sum_{0 \leq i < v} (-1)^{s(i) + s(i+\tau)}$$

• [Theorem] The characteristic sequence of a $(v, k, \lambda)$-CDS of period $v$ has 2-level autocorrelation values, given as

$$\phi(\tau) = \begin{cases} 
v & \tau \equiv 0 \pmod{v} \\
v - 4(k - \lambda) & \tau \not\equiv 0 \pmod{v} \end{cases}$$

Proof: For $\tau = 0$, we have $\phi(0) = v$, obviously. Assume $\tau \neq 0$. When you compare $s(i)$ and $s(i + \tau)$ term by term for $i = 0, 1, 2, \ldots, v - 1$, there are four possibilities:

<table>
<thead>
<tr>
<th>$s(i)$</th>
<th>0 0 1 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s(i + \tau)$</td>
<td>0 1 0 1</td>
</tr>
<tr>
<td>number</td>
<td>$a$ $b$ $c$ $d$</td>
</tr>
</tbody>
</table>

Then, $a = \lambda$ for any $\tau \neq 0$. Also, $b = c = k - \lambda$, and $d = v - (a + b + c) = v - (\lambda + 2(k - \lambda)) = v - 2k + \lambda$. Therefore,

$$\phi(\tau) = a + d - (b + c) = v - 2(k - \lambda) - 2(k - \lambda) = v - 4(k - \lambda)$$
• **It is desired (in most engineering problems) that**
  1. these two values are as far apart as possible
     ⇒ **called “optimal autocorrelation”**,  
  2. the number of 1’s is as much the same as the number of 0’ in one period
     ⇒ **called “balanced”** if the difference is minimal, i.e., 0 or 1.

• **Cyclic Hadamard Difference Sets** have parameters
  
  \[ v = 4n - 1, \quad k = 2n - 1, \quad \lambda = n - 1, \quad (\text{note that } n = k - \lambda) \]

  so that its characteristic sequence has
  
  \[ \phi(\tau) = \begin{cases} 
  v & \tau \equiv 0 \pmod{v} \\
  v - 4n = -1 & \tau \not\equiv 0 \pmod{v}, 
  \end{cases} \]

  and is balanced since it contains \( k = (v - 1)/2 \) zero’s and \((v + 1)/2\) one’s.

• **[Theorem]** These are equivalent:
  1. a \((v, (v - 1)/2, (v - 3)/4)\)-CHDS
  2. a balanced binary sequence of period \(v\) with ideal autocorrelation
  3. a \((v + 1) \times (v + 1)\) Hadamard matrix of cyclic type

Hong-Yeop Song  School of E.& E. Engineering, Yonsei Univ.
**Example 4** Consider a \((15, 7, 3)\)-CDS, which is CHDS: \{0, 5, 7, 10, 11, 13, 14\}.

![Cyclic Hadamard Difference Set Example](image)
$H_{16} = \begin{bmatrix}
+ & + & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
+ & + & + & + & + & + & + & + & + & + & + & + & + & + \\
\end{bmatrix}$
II. Applications

- **Synchronization**
  - Almost every digital communication systems have it.

- **Position Location and Navigation Systems**
  - Geostationary Positioning Satellite use it.

- **Signature sequences in CDMA Communications**
  - Your hand-phone has it and will have it for at least 10 more years.

- **Various powerful “Error-Correcting Codes” construction**
  - Hadamard matrix of cyclic type.

- **Randomization algorithms in many application**
  - Experiment design - psychology and manufacturing.

- **Key streams for Streamcipher Systems**
  - Encryption systems.

- Many more...
Example 5 The transmitter of an $M$-ary digital communication modem transmits, for each incoming symbol out of $M$ symbols, a corresponding waveform of $T$ sec interval out of $M$ waveforms. The receiver has to decide which waveform has been transmitted for each symbol interval.

- One has to design a set of $M$ waveforms $\{s_i(t)|i = 1, 2, ..., M, 0 \leq t \leq T\}$ that can be ”best” distinguishable in terms of ”correlation”.
  - consider waveforms with a constant energy: $\int_0^T s_i(t)^2 dt = E_s$ for all $i$.
  - correlation matrix $\Gamma = (\gamma_{ij})$ of the waveforms where $\gamma_{ij} = \frac{1}{E_s} \int_0^T s_i(t)s_j(t)dt$.
  - when $M = 2$ (binary signaling), some famous signal sets are $\Gamma_{\text{antipodal}} = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ or $\Gamma_{\text{orthogonal}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

- When $M = 4$ (quaternary signaling), one may dream of the following: (will it be possible?)

$$\Gamma_{\text{dream}} = \begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & 1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$
• Simplex Bound says:

\[
\min_{\text{all possibilities}} \max_{i \neq j} \gamma_{ij} \geq \frac{-1}{M - 1}
\]

• The best one can achieve:

\[
\Gamma_{\text{simplex}} = \begin{pmatrix}
1 & -\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} \\
-\frac{1}{3} & 1 & -\frac{1}{3} & -\frac{1}{3} \\
-\frac{1}{3} & -\frac{1}{3} & 1 & -\frac{1}{3} \\
-\frac{1}{3} & -\frac{1}{3} & -\frac{1}{3} & 1
\end{pmatrix}
\]

or

\[
\Gamma_{\text{bi-orthogonal}} = \begin{pmatrix}
1 & 0 & -1 & 0 \\
0 & 1 & 0 & -1 \\
-1 & 0 & 1 & 0 \\
0 & -1 & 0 & 1
\end{pmatrix}
\]
III. Description of Known CHDS

◇ Equivalence of binary sequences

Let $\mathcal{S}$ be the set of the binary sequences of period $v$. Define three operations on $a = \{a(t)|t = 0, 1, 2, \ldots\} \in \mathcal{S}$ as:

1. (Cyclic shifts) $L(a) = b$ where $b(t) = a(t + 1)$ for all $t$.
2. (Complement) $C(a) = b$ where $b(t) = a(t) + 1$ for all $t$.
3. (Decimation) For $d$ with $(d, v) = 1$, $D_d(a) = b$ where $b(t) = a(dt)$ for all $t$.

Then the group $G = \langle L, C, D_d \rangle$ acts on $\mathcal{S}$, and partitions it into “equivalence classes”.

We say $a, b \in \mathcal{S}$ are equivalent if there exist $g \in G$ such that $g(a) = b$. 
Summary

1. \( v = p \equiv 3 \pmod{4} \) is a prime:
   (a) Quadratic residue construction works for all such \( p \).
   (b) Hall's sextic residue construction works for \( p = 4x^2 + 27 \).

2. \( v = p(p+2) \) is a product of twin primes:
   (a) Generalization of "Quadratic residue construction" works.

3. \( v = 2^t - 1 \) for \( t = 1, 2, 3, \ldots \)
   (a) m-sequence (or maximal LFSR sequence) construction works for all such \( t \).
   This is 1-term trace sequence.
   (b) GMW construction works for all "composite" \( t \).
   (c) Recent addition ('97 and later):
      i. 3-term trace sequences, 5-term trace sequences
      ii. hyperoval type (Glynn's Type I and Type II)
      iii. What else ??
Quadratic Residue Construction

Let $v = p$ be a prime congruent to $3 \mod 4$, and $a = \{a(i) | i = 0, 1, 2, \ldots, p - 1\ldots \} \in \mathbb{S}$. Then it is called “Legendre” sequence (or quadratic residue sequence) if

$$a(i) = \begin{cases} 
1, & \text{if } i \equiv 0 \pmod{p} \\
0, & \text{if } i \text{ is a “quadratic residue mod } p” \\
1, & \text{otherwise}
\end{cases}$$

Note, the same construction for $p \equiv 1 \pmod{4}$ gives also “Legendre sequences” but they do not correspond to CHDS, i.e., they do not have 2-level “ideal” auto-correlation, though they are balanced.
Hall’s Sextic Residue Construction

Let $p$ be an odd prime of the form $p = 4x^2 + 27$ for some integer $x$. Then $p \equiv 1 \pmod{6}$ and we may write it as $p = 6f + 1$ for some integer $f$. Let $g$ be a primitive root modulo $p$ such that $3 \in C_1$ where

$$C_i = \{g^{6i+l} \mid i = 0, 1, \ldots, f - 1\}.$$ 

Then, Hall’s sextic residue sequence $s = \{s(t) \mid t = 0, 1, 2, \ldots\}$ of period $p$ is defined as

$$s(t) = \begin{cases} 0 & \text{if } t \in C_0 \cup C_1 \cup C_3 \\ 1 & \text{otherwise} \end{cases}$$

- Note that the subset $D = C_0 \cup C_1 \cup C_3$ of the integers mod $p$ is a $(v = p, k = (p - 1)/2, \lambda = (p - 3)/4)$-cyclic Hadamard difference set, called Hall’s sextic residue difference set.

- The subset $C_0 \cup C_2 \cup C_4$ is a quadratic residue difference set, used in the previous page.
Example 6 *Binary sequences of period* $31 = 4 \cdot 1^2 + 27$. *Note that 3 is a generator of* $\mathbb{Z}_{31}^*$ *and we have*

<table>
<thead>
<tr>
<th>Cosets</th>
<th>Legendre</th>
<th>Hall’s sextic</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_0 = {1, 2, 4, 8, 16}$</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>$C_1 = {3, 6, 12, 24, 17}$</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>$C_2 = {9, 18, 5, 10, 20}$</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>$C_3 = {27, 23, 15, 30, 29}$</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>$C_4 = {19, 7, 14, 28, 25}$</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>$C_5 = {26, 21, 11, 22, 13}$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| $i$ : | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| $a(i)$ : | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| $b(i)$ : | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |

- *The Hall’s sextic residue sequence* $\{b(i)\}$ *of period 31 turns out to be equivalent to m-sequence of period* $31 = 2^5 - 1$.  

Hong-Yeop Song  
School of E.& E. Engineering, Yonsei Univ.
Jacobi Construction

Let \( p, q \) be two distinct odd primes. We define a binary sequence \( J_{p,q} = \{ J_{p,q}(i) | i \geq 0 \} \) of period \( pq \) as

\[
J_{p,q}(i) = \begin{cases} 
0 & i \equiv 0 \pmod{pq} \\
1 & i \equiv 0 \pmod{p}, \ i \not\equiv 0 \pmod{q} \\
0 & i \not\equiv 0 \pmod{p}, \ i \equiv 0 \pmod{q} \\
\sigma \left( \left( \frac{i}{p} \right) \left( \frac{i}{q} \right) \right) & (i, pq) = 1,
\end{cases}
\]

where \( \sigma(1) = 0 \) and \( \sigma(-1) = 1 \), and \( \left( \frac{i}{p} \right) \) is the legendre symbol of the integer \( i \) mod \( p \), taking the value \(+1\) or \(-1\) according to whether \( i \) is a quadratic residue mod \( p \) or not. It is clear that

\[
\sigma \left( \left( \frac{i}{p} \right) \left( \frac{i}{q} \right) \right) = \sigma \left( \frac{i}{p} \right) + \sigma \left( \frac{i}{q} \right).
\]

\( \bullet \) Note that \( J_{p,p+2} \) whenever both \( p \) and \( p + 2 \) are prime gives a twin-prime sequence of period \( v = p(p + 2) \).
Example 7 Twin-prime sequence of period $15 = 3 \cdot 5$.

<table>
<thead>
<tr>
<th>$i$</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>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(i/3)$</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(i/5)$</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$(i/3)(i/5)$</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\cdot$</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\cdot$</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- It turns out that, for the period 15, this is equivalent the m-sequence of period $2^4 - 1 = 15$. 

Hong-Yeop Song School of E.& E. Engineering, Yonsei Univ.
Type (iii) Construction for \( v = 2^t - 1 \)

1. The maximal length linear feedback shift register sequences (shortly, \( m \)-sequences) for all values of \( t > 1 \).

\[
s(i) = Tr^n_1(\alpha^i)
\]

where the trace function \( Tr^n_\cdot \) is a linear mapping from \( GF(2^n) \) to \( GF(2^m) \), defined as

\[
Tr^t_m(\alpha) = \alpha + \alpha^{2^m} + \alpha^{2^{2m}} + \cdots + \alpha^{2^{m(t/m-1)}}
\]

where \( m \mid t, \alpha \in GF(2^t) \).

2. Some Properties of \( m \)-sequences of period \( 2^t - 1 \)

- balance property: “0” appears \( 2^{t-1} - 1 \) times, and “1” appears \( 2^{t-1} \) times.
- span-property: every \( t \)-tuple (except for all-zero) appears exactly once
- ideal-autocorrelation property: already discussed
- cycle-and-add property: An \( m \)-sequence and all of its cyclic shifts together with all-zero sequence of length \( 2^t - 1 \) form an additive group with respect to the component-wise mod-2 addition. (necessary and sufficient)
- worst linear complexity: it has the minimum linear complexity among all the balanced binary sequences of length \( 2^t - 1 \).
3. The GMW sequences of period $2^t - 1$ for composite values of $t$. Let $t = JK$.

$$s(i) = Tr_1^J([Tr_J^K(\alpha^i)]^r)$$

where $\alpha$ primitive in $GF(2^t)$ and $(2^J - 1, r) = 1, 0 < r < 2^J - 1$.

4. 3-term and 5-term trace sequences (No-Golomb-Gong-Lee-Gaal, '98): Let $\alpha$ be a primitive element of $GF(2^t)$.

- For $n = 2k + 1$ where $k$ is a positive integer,

$$s(i) = Tr_1^n(\alpha^i) + Tr_1^n(\alpha^{(2k+1)i}) + Tr_1^n(\alpha^{(2k+2k-1+1)i}).$$

- For $n = 3k - 1$ where $k$ is a positive integer,

$$s(i) = Tr_1^n(\alpha^i) + Tr_1^n(\alpha^{(2k+1)i}) + Tr_1^n(\alpha^{(2k+2k-1+1)i}) + Tr_1^n(\alpha^{(2k-2k-1+1)i}) + Tr_1^n(\alpha^{(2k+2k-1+1)i}).$$

- For $n = 3k - 2$ where $k \geq 2$

$$s(i) = Tr_1^n(\alpha^i) + Tr_1^n(\alpha^{(2k-1+1)i}) + Tr_1^n(\alpha^{(2k-2+2k-1+1)i}) + Tr_1^n(\alpha^{(2k-2-2k-1+1)i}) + Tr_1^n(\alpha^{(2k-1-2k-1)i}).$$

- Welch-Gong Transformation of all three above.

5. Hyperoval type (I and II) - much more complicated but they are all represented as a sum of some traces, similarly.
Open problem on the characterization of $m$-sequences

- Every $m$-sequence is balanced and has both span property and ideal autocorrelation property.

- (’82, Golomb) Is it true that a balanced binary sequence of period $2^t - 1$ must be an $m$-sequence if it has both properties?

- (Equivalent Formulation) Is it true that a balanced binary sequence of period $2^t - 1$ must have the cycle-and-add property if it has both span and ideal autocorrelation properties?

- Partial Answer: Yes, for $t \leq 10$.

- Neither counterexample for $t > 10$ has been found, nor any theoretical proof has been completed.
Exhaustive search for type (iii)

m: \(m\)-sequence
G: GMW sequence but not an \(m\)-sequence
L: Legendre sequence
H: Hall’s sextic residue sequence
M: miscellaneous type belonging to none of the above.

<table>
<thead>
<tr>
<th>(n)</th>
<th>m</th>
<th>G</th>
<th>L</th>
<th>H</th>
<th>M</th>
<th>Total</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>6</td>
<td>Baumert ’67</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>Cheng ’83</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>5</td>
<td>Drier ’92 (Song ’97)</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>10</td>
<td>Gaal ’98</td>
</tr>
</tbody>
</table>
IV. Existence of Cyclic Hadamard Difference Sets

◇ Summary

• If a \((v, (v - 1)/2, (v - 3)/4)\)-CHDS exists, then \(v \equiv 3 \pmod{4}\).

• All “known” CHDS has \(v\) that is one of the following:
  
  (i) \(v = p \equiv 3 \pmod{4}\) is a prime.
  
  (ii) \(v = p(p + 2)\) is a product of twin primes.
  
  (iii) \(v = 2^t - 1\) for \(t = 1, 2, 3, \ldots\).

• Current status of computer check:

  No CHDS exists for \(v\) other than those listed above, for \(v < 10000\), except possibly for the following 7 values:

  \[
  3439, \quad 4355, \quad 8591, \quad 8835, \quad 9135, \quad 9215, \quad 9423.
  \]
Conjecture 1 (Main) If a CHDS exists, then $v$ must be one of the following three types:

(i) $v = p \equiv 3 \pmod{4}$ is a prime.

(ii) $v = p(p + 2)$ is a product of twin primes.

(iii) $v = 2^t - 1$ for $t = 1, 2, 3, \ldots$.

• It is interesting to note that the above three types of integers have those “common” property.
Search History

Baumert (1971) Conjecture was confirmed up to \( v < 1000 \) except for the six cases \( v = 399, 495, 627, 651, 783, \) and 975, not fully investigated.

Song and Golomb (1994) Conjecture was confirmed up to \( v < 10000 \) except “possibly” for the following 17 cases: 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423.

- 619 = Number of primes up to 10000
- 8 = Number of products of twin primes
- 12 = Number of numbers of the form \( 2^t - 1 \)
- 1867 = 2500 - 619 - 8 - 12 + 5 + 1 = Total number to check.

Kim and Song (1999) The values 1295, 1599, 1935, 3135 are ruled out.

Baumert and Gordon (2003) Six values 4623, 5775, 7395, 7743, 8227, 8463 were recently ruled out by Necessary condition by Landers.

Left-overs (as of June 2003)

3439, 4355, 8591, 8835, 9135, 9215, 9423.
Main Tools

(Baumert ’71) If a \((v, k, \lambda)\)-cyclic difference set exists, then for every divisor \(w\) of \(v\), there exist integers \(b_i \ (i = 0, 1, 2, \cdots, w - 1)\) satisfying the diophantine equations

\[
\begin{align*}
\sum_{0 \leq i < w} b_i &= k \\
\sum_{0 \leq i < w} b_i^2 &= k - \lambda + v\lambda/w \\
\sum_{0 \leq i < w} b_ib_{i-j} &= v\lambda/w, \text{ for } 1 \leq j \leq w - 1
\end{align*}
\]

Here, the subscript \(i - j\) is taken modulo \(w\).

And, some other necessary conditions scattered throughout papers...
Summary and Open Problems

1. We believe there are MORE undiscovered examples of type (iii) for larger values of $t$ where $v = 2^t - 1$.

2. Trace function representation for CHDS of all the known types have been “almost” completed.

3. (Conjecture)
   - If a CHDS exists, then $v$ must be one of the three types:
     (i) $v = p = 3 \pmod{4}$,
     (ii) $v = p(p + 2)$ is a product of twin primes, or
     (iii) $v = 2^n - 1$ some $n$.
   - Computer Checks: The conjecture is true for $v < 10000$ except possibly for the following 7 cases: 3439, 4355, 8591, 8835, 9135, 9215, and 9423.

4. (Conjecture)
   - If a balanced binary sequence has both span and ideal autocorrelation properties then it must be an $m$-sequence.
   - Exhaustive search for $v = 2^t - 1$ gives an answer “YES” for $t \leq 10$. 
참고 문헌


Hong-Yeop Song  School of E.& E. Engineering, Yonsei Univ.


What comes next?

1. About the MAIN CONJECTURE:
   - If it is false, there should be a CHDS with \( n \) not of the above 3 types.
     - Various extensive computer search shows NONE exists for \( n < 3149 \)
       - None for \( n < 10000 \) except possibly for 13 cases
   - If it is true, we believe that the three types of integer \( n \) must have "some" common property to answer (prove) the question.
     - or, at least, there should be "some" common or consistent way to describe CHDS for three different types of \( n \).

2. Type A when it is of the form \( 2^t - 1 \) (Mersenne prime) can be described as a sum of traces

   A.1. \( G_c = \sum_{j=0}^{p^t-1} tr_n \left( \alpha^j i \right) \) \( \text{if } p = 2^t - 1 \)

   A.2. \( G_c = \sum_{j=0}^{p^{t-1}-1} tr_n \left( \alpha^j i \right) \) \( \text{if } p = \frac{2^t - 1}{31}, \frac{2^t - 1}{127}, \frac{2^t - 1}{131071} \) \( \text{and } n = 4A + 1 \)

2. For other values of Type A ???
2. Type A provides much more abundant examples, but Type C is more interesting in the sense of applying them to communication engineering.

→ Classification & Exhaustive determination of Hadamard sequences of period

\[ V = 2^t - 1 \]

<table>
<thead>
<tr>
<th>( t )</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>
</tr>
</thead>
<tbody>
<tr>
<td># of inequiv. examples</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>4</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

Braun & Fredriksen '67
Friedrichsen '83
Dreier & Gaal '92
Cheng (independently) '97
Song '97

2. The structure of some sporadic examples of period 127, 255, 511 is now fully identified as sum of some traces, and based on empirical observations, several new constructions are recently proposed (without proof). Most of

- These new constructions have been checked by computer up to around \( 2^{20} - 1 \). (97)
- Some constructions were proved recently. (98)
Hadamard sequences of period $2^n - 1$

$m$: $m$-sequence

$G$: GMW sequence but not an $m$-sequence

$L$: Legendre sequence

$H$: Hall's sextic residue sequence

$M$: miscellaneous type belonging to none of the above.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
<th>$G$</th>
<th>$L$</th>
<th>$H$</th>
<th>$M$</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

The number of inequivalent binary sequences of period $2^n - 1$ with ideal autocorrelation.
• For $n = 3$

1. $m$-sequence:

$$s(t) = \text{Tr}(\alpha^t)$$

where $\alpha$ is a primitive element of $GF(2^3)$.

• For $n = 4$

1. $m$-sequence:

$$s(t) = \text{Tr}(\alpha^t)$$

where $\alpha$ is a primitive element of $GF(2^4)$.

• For $n = 5$

Let $\alpha$ be a primitive element of $GF(2^5)$.

1. $m$-sequence: $s(t) = \text{Tr}(\alpha^t)$.

2. Legendre sequence:

$$s(t) = \text{Tr}(\alpha^t + \alpha^{5t} + \alpha^{7t}).$$
Trace function representation of Legendre sequences

**Theorem 3** Let $p = 2^n - 1$ be a prime for some integer $n \geq 3$ and $u$ be a primitive element of $Z_p$, the set of integers mod $p$. Let $\alpha$ be a primitive element of $GF(2^n)$ such that

$$\sum_{i=0}^{\frac{n-1}{2n}-1} Tr_1^n(\alpha^{u2^i}) = 0$$

Then the sequence $s(t)$ for $t = 0, 1, 2, \cdots, p-1$ of period $p$ given by

$$s(t) = \sum_{i=0}^{\frac{n-1}{2n}-1} Tr_1^n(\alpha^{u2^i t})$$

is the “Legendre” sequence.

• For $n = 6$

1. $m$-sequence: $s(t) = Tr(\alpha^t)$.

2. GMW-sequence: $s(t) = Tr(\alpha^t + \alpha^{15t})$

• For $n = 7$ \(^5\)

1. $m$-sequence: $s_1(t) = Tr(\alpha^t)$.

2. Legendre sequence:

$$s(t) = Tr(\alpha^t + \alpha^{9t} + \alpha^{11t} + \alpha^{13t} + \alpha^{15t} + \alpha^{19t} + \alpha^{21t} + \alpha^{31t} + \alpha^{47t})$$

3. Hall’s sextic residue sequence:

$$s(t) = Tr(\alpha^t + \alpha^{19t} + \alpha^{47t}).$$

4. Miscellaneous sequences:

(a) $s(t) = Tr(\alpha^t + \alpha^{11t} + \alpha^{15t})$.

(b) $s(t) = Tr(\alpha^t + \alpha^{3t} + \alpha^{7t} + \alpha^{19t} + \alpha^{29t})$.

(c) $s(t) = Tr(\alpha^t + \alpha^{5t} + \alpha^{13t} + \alpha^{21t} + \alpha^{29t})$.

Trace function representation of Hall’s sextic residue sequences of Mersenne prime period

There are only three Mersenne primes, 31, 127, 131071 which are of the form $4A^2 + 27$ for some integer $A$. Let $p$ be any one of 31, 127, 131071, and $u$ be a primitive root mod $p = 2^n - 1$ and $\alpha$ be a primitive element of the finite field $GF(2^n)$.

Then Hall’s sextic residue sequence can be expressed as

$$h(t) = \sum_{i=0}^{\frac{p-1}{6m} - 1} Tr_1^n(\alpha^{6i^t}).$$

For $p = 127 = 2^7 - 1$, since 3 is a primitive root mod 127,

$$h(t) = \sum_{i=0}^{2} Tr_1^7(\alpha^{36i^t})$$

$$= Tr_1^7(\alpha^t) + Tr_1^7(\alpha^{19t}) + Tr_1^7(\alpha^{47t})$$

---

*Hwan-Keun Lee, Jong-Seon No, Habong Chung, Kyeongcheol Yang, Jeon-Heon Kim, and Hong-Yeop Song, “Trace function representation of Hall’s sextic residue sequences and some new sequences with ideal autocorrelation,” APCC’97.*
• For $n = 8$ \(^\text{7}\)

1. $m$-sequence: $s(t) = Tr(\alpha^t)$.

2. GMW-sequence:
$$s(t) = Tr(\alpha^t + \alpha^{19t} + \alpha^{53t} + \alpha^{91t})$$

3. Miscellaneous sequences:
   
   (a) $s(t) = Tr(\alpha^t + \alpha^{11t} + \alpha^{19t} + \alpha^{27t} + \alpha^{87t})$.

   (b) $s(t) = Tr(\alpha^t + \alpha^{3t} + \alpha^{43t} + \alpha^{91t} + \alpha^{111t})$.

• For $n = 9$ \(^\text{8}\)

1. $m$-sequence: $s(t) = Tr(\alpha)$

2. GMW-sequence:
$$s(t) = Tr(\alpha^t + \alpha^{11t} + \alpha^{43t})$$

3. Miscellaneous sequences:
   
   (a) $s(t) = Tr(\alpha^t + \alpha^{23t} + \alpha^{31t})$.

   (b) $s(t) = Tr(\alpha^t + \alpha^{51t} + \alpha^{57t} + \alpha^{83t} + \alpha^{111t} + \alpha^{125t} + \alpha^{183t})$.


(c) \( s(t) = Tr(\alpha^t + \alpha^{7t} + \alpha^{57t} + \alpha^{77t} + \alpha^{83t} + \alpha^{103t} + \alpha^{111t} + \alpha^{127t} + \alpha^{183t}). \)

- For \( n = 10^9 \)

Let \( \alpha \) be a primitive element of \( GF(2^{10}) \).

1. \( m \)-sequence: \( s(t) = Tr(\alpha^t). \)

2. GMW-sequences:

   (a) \( s(t) = Tr(\alpha^t + \alpha^{63t}). \)

   (b) \( s(t) = Tr(\alpha^t + \alpha^{219t}). \)

   (c) \( s(t) = Tr(\alpha^t + \alpha^{101t} + \alpha^{159t} + \alpha^{221t}). \)

   (d) \( s(t) = Tr(\alpha^t + \alpha^{39t} + \alpha^{157t} + \alpha^{221t}). \)

   (e) \( s(t) = Tr(\alpha^t + \alpha^{39t} + \alpha^{47t} + \alpha^{63t} + \alpha^{109t} + \alpha^{125t} + \alpha^{159t} + \alpha^{187t}). \)

3. Miscellaneous sequences

   (a) \( s(t) = Tr(\alpha^t + \alpha^{11t} + \alpha^{15t} + \alpha^{39t} + \alpha^{127t}). \)

   (b) \( s(t) = Tr(\alpha^t + \alpha^{39t} + \alpha^{47t} + \alpha^{63t} + \alpha^{109t} + \alpha^{125t} + \alpha^{159t} + \alpha^{187t}). \)

---

(c) \( s(t) = \text{Tr}(\alpha^t + \alpha^{41t} + \alpha^{47t} + \alpha^{63t} + \alpha^{87t} + \alpha^{125t} + \alpha^{205t}). \)

(d) \( s(t) = \text{Tr}(\alpha^t + \alpha^{5t} + \alpha^{9t} + \alpha^{49t} + \alpha^{63t} + \alpha^{71t} + \alpha^{111t} + \alpha^{121t} + \alpha^{253t} + \alpha^{237t} + \alpha^{191t} + \alpha^{183t} + \alpha^{205t} + \alpha^{245t}). \)