ON THE EXISTENCE OF SOME CYCLIC HADAMARD DIFFERENCE SETS

Jeong-heon Kim, Hong-Yeop Song, Kyu Tae Park
Electronic Engineering Dept. Yonsei Univ.

제 8 회 통신 정보 합동 학술 대회
1998년 4월 22일 ~ 24일

Two-level ideal autocorrelation

Definition A balanced binary sequence $\{b_i\}$ of length v has two-level ideal autocorrelation if it satisfy the following equation ($b_i \in \{0,1\}$) :

$$\sum_{i=0}^{v-1} (-1)^{b_i + b_{i+\tau}} = \begin{cases} v & \tau = 0 \\ -1 & otherwise \end{cases}$$

Example 1

(7,3,1)-cyclic difference set

binary sequence of period 7 with ideal autocorrelation

	1	2	4
1	0	1	3
2	6	0	2
4	4	5	0

t	0	1	2	3	4	5	6
$s(t)$	1	0	0	1	0	1	1

	3	5	6
3	0	2	3
5	5	0	1
6	4	6	0

t	0	1	2	3	4	5	6
$s(t)$	1	1	1	0	1	0	0

(v, k, λ)-cyclic difference sets

Definition : Given a positive integer v, let U denote the set of nonnegative integers smaller than v. Let D be a subset of U. One calls D a (v, k, λ)-cyclic difference set if D contains k elements of U, and for any $d \in U$, $d \neq 0$, there are exactly λ pairs of (x, y), $x, y \in D$ such that $d \equiv x - y \pmod{v}$.

Definition : D is called a cyclic Hadamard difference set if $v = 4n - 1$, $k = 2n - 1$, $\lambda = n - 1$ for some n.

Classification of (v, k, λ)-CHDS

a) $v = 4n - 1$ is prime.

b) $v = p(p+2)$, where both p and $p+2$ are prime.

c) $v = 2^t - 1$, for $t = 2, 3, 4, \cdots$.

Is there a cyclic Hadamard difference set with v none of the above three types?

Search results up to 1994.

- $v < 1000$ are confirmed except for the six cases v = 399, 495, 627, 651, 783, 975 by Baumert (1971).

- $v < 10000$ are confirmed except for the 17 cases v = 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423 by Song and Golomb (1994).

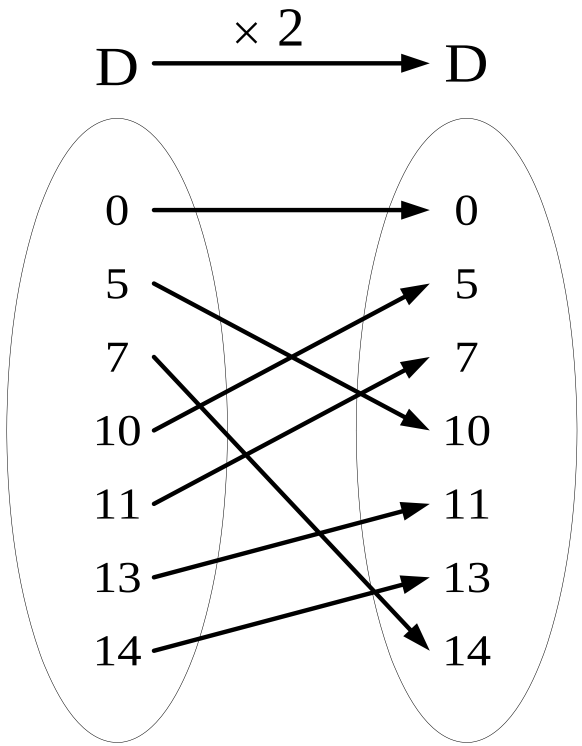
- The cases v = 1295, 1599, 1935, 3135 are confirmed.

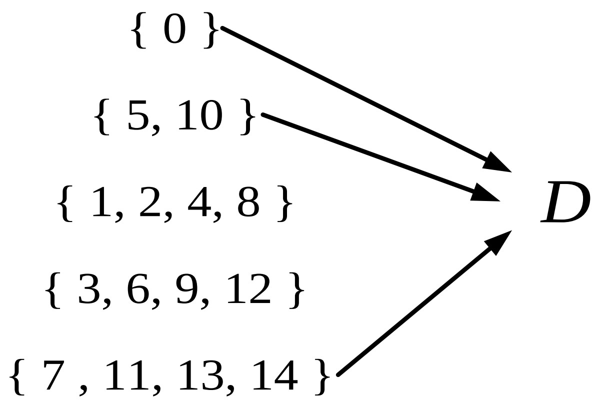
Multiplier of a (v, k, λ)-CDS

If two cyclic difference sets $D = \{d_1, d_2, \cdots, d_k\}$ and $D' = \{td_1, td_2, \cdots, td_k\}$ are the same set, D is said to be fixed by t. If $D' = \{d_1 + s, d_2 + s, d_3 + s, \cdots, d_k + s\}$ for some s, t is called a multiplier of D.

Known : If a (v, k, λ)-CDS with multiplier t exists, then there is some shift D'' of D such that D'' is fixed by t.

Multiplier of (15,7,3)-CDS





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

$$\sum_{i=0}^{w-1} b_i = k$$

$$\sum_{i=0}^{w-1} b_i^2 = k - \lambda + v\lambda/w$$

$$\sum_{i=0}^{w-1} b_i b_{i-j} = v\lambda/w \qquad \text{for} \quad 1 \le j \le w-1$$

Here, the subscript $i-j$ is taken modulo w.

Fact : b_i denotes the number of residues $i \mod w$ that must belong to D if D exists.

Basic procedure for non-existence proof

1. Find a multiplier and cyclotomic cosets for each divisor of v.
2. For each prime divisor, find solutions for the three equations in Theorem 1.
3. For each composite divisor, find solutions which satisfy the three equations and relations with its prime divisors.

Non-existence proof of (175,87,43)-CDS

- Multiplier is 11.
- $175 = 5^2 \times 7$.

$$
\begin{aligned}
C_0^5 &= \{0\} \\
C_1^5 &= \{1\} \\
C_2^5 &= \{2\} \\
C_3^5 &= \{3\} \\
C_4^5 &= \{4\}
\end{aligned}
$$

$$
\begin{aligned}
C_0^7 &= \{0\} \\
C_1^7 &= \{1, 2, 4\} \\
C_2^7 &= \{3, 5, 6\}
\end{aligned}
$$

$$
\begin{aligned}
C_0^{35} &= \{0\} \\
C_1^{35} &= \{5, 10, 20\} \\
C_2^{35} &= \{15, 25, 30\} \\
C_3^{35} &= \{21\} \\
C_4^{35} &= \{6, 26, 31\} \\
C_5^{35} &= \{1, 11, 16\} \\
C_6^{35} &= \{7\} \\
C_7^{35} &= \{12, 17, 27\} \\
C_8^{35} &= \{2, 22, 32\}
\end{aligned}
$$

$$
\begin{aligned}
C_{9}^{35} &= \{28\} \\
C_{10}^{35} &= \{3, 13, 33\} \\
C_{11}^{35} &= \{8, 18, 23\} \\
C_{12}^{35} &= \{14\} \\
C_{13}^{35} &= \{19, 24, 34\} \\
C_{14}^{35} &= \{4, 9, 29\}
\end{aligned}
$$

For the divisor $w = 5$:

$$\sum_{i=0}^{4} b_i = 87,$$

$$\sum_{i=0}^{4} b_i^2 = 1549,$$

$$\sum_{i=0}^{4} b_i b_{i+j} = 1505, \quad \text{where} \quad 1 \le j \le$$

,

and $0 \le b_i \le 35$.

Solutions :

b_0	b_1	b_2	b_3	b_4
13	17	17	19	21
13	17	21	17	19
17	13	19	17	21
17	13	21	19	17
19	13	17	21	17
21	13	17	17	19

For the divisor $w = 7$:

$$\sum_{i=0}^{6} c_i = 87,$$

$$\sum_{i=0}^{6} c_i^2 = 1119,$$

$$\sum_{i=0}^{6} c_i c_{i+j} = 1075, \quad \text{where} \quad 1 \le j \le$$

,

and $0 \le c_{0,} c_{1,} c_2, \cdots, c_6 \le 25.$

Solution :

c_0	c_1	c_2	c_3	c_4	c_5	c_6
9	11	11	15	11	15	15
12	10	10	12	10	12	12
18	11	11	12	11	12	12

For the divisor $w = 7 \times 5 = 35$:

$$\sum_{i=0}^{34} d_i = 87, \quad \sum_{i=0}^{34} d_i^2 = 259,$$

$$\sum_{i=0}^{34} d_i d_{i+j} = 215, \qquad \text{where} \quad 1 \leq j \leq 34,$$

and $0 \leq d_0, d_1, \cdots, d_{34} \leq 5.$

$$\begin{aligned}
b_0 &= d_0 + 3(d_5 + d_{15}) \\
b_1 &= d_{21} + 3(d_6 + d_1) \\
b_2 &= d_7 + 3(d_{12} + d_2) \\
b_3 &= d_{28} + 3(d_3 + d_8) \\
b_4 &= d_{14} + 3(d_{19} + d_4)
\end{aligned}$$

$$\begin{aligned}
c_0 &= d_0 + d_{21} + d_7 + d_{28} + d_{14} \\
c_1 &= d_5 + d_6 + d_{12} + d_3 + d_{19} \\
c_2 &= d_{15} + d_1 + d_2 + d_8 + d_{14}
\end{aligned}$$

There is **no solution** for d_i's !!!

Search results

v	Multiplier	# of cyclotomic cosets	# of solutions for divisors
1295	16	155	w = 5 : 2 w = 37 : 1 w = 5×37 = 185 : 0
1599	25	176	w = 3 : 2 w = 41 : 1 w = 3×41 = 123 : 0
1935	16	175	w = 3 : 1 w = 43 : 10 w = 3×43 = 129 : 0
3135	49	189	w = 3 : 5 w = 5 : 1 w = 3×5 = 15 : 0

Conclusion

● It is confirmed that there is no CHDS with $v < 3000$ none of three types.

● remaining cases : 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423.