ON THE EXISTENCE OF SOME CYCLIC HADAMARD DIFFERENCE SETS

Jeong-Heon Kim, Hong-Yeop Song

Computer & Electrical Engineering Dept. Yonsei Univ.

APCC/OECC'99

October 19 - 21 1999, Beijing, China

(v, k, λ)-cyclic difference sets

Definition : Let D be a k-subset of Z_v. One calls D a (v, k, λ)-cyclic difference set if for any non-zero $d \in Z_v$, there are exactly λ pairs of (x, y), where $x, y \in D$ such that $d \equiv x - y \pmod{v}$.

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

Remark : If a CHDS is given, one can obtain a balanced binary sequence with ideal autocorrelation (so called, Hadamard sequence).

Hadamard sequences

Definition If a binary sequence $\{b(t)\}$ of length v has the following property, it is called a Hadamard sequence.

1. Balanced property : **# of 1's − # of 0's = 1.**
2. Ideal autocorrelation property :

$$\sum_{t=0}^{v-1} (-1)^{b(t)+b(t+\tau)} = \begin{cases} v & \text{if } \tau = 0 \mod v \\ -1 & \text{otherwise} \end{cases}$$

Example 1 : (11,5,2)-CHDS

D = {1, 3, 4, 5, 9}

1 = 4 - 3 = 5 - 4

2 = 3 - 1 = 5 - 3

5 = 3 - 9 = 9 - 4

etc.

-	1	3	4	5	9
1	0	2	3	4	8
3	9	0	1	2	6
4	8	10	0	1	5
5	7	9	10	0	4
9	3	5	6	7	0

t	0	1	2	3	4	5	6	7	8	9	10
s(t)	1	0	1	0	0	0	1	1	1	0	1

Classification of CHDS

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

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

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

Main conjecture : If a CHDS exists, v must be one of the above three types.

Summary of recent results

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

- **Song & Golomb (1994) :** $v < 10000$ 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.

- **In this paper :** The smallest four cases v = 1295, 1599, 1935, 3135 are confirmed that none exists with these values of v.

Multiplier of a (v, k, λ)-CDS

Let $D = \{d_1, d_2, \cdots, d_k\}$ be a (v, k, λ)-CDS.

Then so is $s + D = \{s + d_i \mid 1 \le i \le k\}$ for any $s \in Z_v$

and if $(t, v) = 1$, so is $tD = \{t \cdot d_i \mid 1 \le i \le k\}$.

If $tD = D + s$ for some $s \in Z_v$, then t is called a **multiplier** of D.

Remark : If a (v, k, λ)-CDS with multiplier t exists, then there exists some shift $D' = D + s$ of D such that $D' = tD'$.

==> There exists a CDS which is a union of some cyclotomic cosets of integers mod v.

Multiplier of (15,7,3)-CDS

- Assume there exists a (15,7,3)-CDS.
- Hypothetical multiplier is 2.

Cyclotomic cosets

$C_1 = \{0\}$

$C_2 = \{5,10\}$

$C_3 = \{1,2,4,8\}$

$C_4 = \{3,6,9,12\}$

$C_5 = \{7,11,13,14\}$

Candidates for CDS :
CDS is a union of some cosets

$D_1 = C_1 \bigcup C_2 \bigcup C_3$

$D_2 = C_1 \bigcup C_2 \bigcup C_4$

$D_3 = C_1 \bigcup C_2 \bigcup C_5$

They are CDSs

Theorem 1 [Baumert] If a (v, k, λ)-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

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

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

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

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

Remark : By this theorem, we can give a restriction to the number of residues modulo each divisor that must belong to D if D exists.

Basic procedure of 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.

●

mod 5	mod 7	mod 35	
		$C_0^{35} = \{0\}$	
		$C_1^{35} = \{5,10,20\}$	
		$C_2^{35} = \{15,25,30\}$	
		$C_3^{35} = \{21\}$	$C_9^{35} = \{28\}$
$C_0^{5} = \{0\}$		$C_4^{35} = \{6,26,31\}$	$C_{10}^{35} = \{3,13,33\}$
$C_0^{5} = \{1\}$		$C_5^{35} = \{1,11,16\}$	$C_{11}^{35} = \{8,18,23\}$
$C_0^{5} = \{2\}$	$C_0^{7} = \{0\}$	$C_6^{35} = \{7\}$	$C_{12}^{35} = \{14\}$
$C_0^{5} = \{3\}$	$C_0^{7} = \{1,2,4\}$	$C_7^{35} = \{12,17,27\}$	$C_{13}^{35} = \{19,24,34\}$
$C_0^{5} = \{4\}$	$C_0^{7} = \{3,5,6\}$	$C_8^{35} = \{2,22,32\}$	$C_{14}^{35} = \{4,9,29\}$

< cyclotomic cosets mod divisors >

$175 = 5^2 \times 7.$

For the divisor $w = 5$:

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

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

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

,

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 $w = 7$:

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

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

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

,

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 $w = 7 \times 5 = 35$:

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

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

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

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

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

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

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

==> There is no (175,87,43)-CDS.

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 $v < 3439$ none of the three types.

● remaining 14 cases : 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423.