Exhaustive Construction of (511,255,127)-Cyclic Hadamard Difference Sets*

김 정 헌, 송 홍 엽, 박 규 태
연세대학교 전자공학과

1997년 5월 24일

’97 2nd Workshop
Coding & Information Theory Society

* 본 연구는 정보통신연구관리단의 대학기초연구 지원사업의 연구비지원에 의한 결과입니다.

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

1 0 0 1 0 1 1

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

1 1 1 0 1 0 0

Ideal Autocorrelation

- **Definition**

  Binary sequence $\{b_i\}$ of period $2^n - 1$ has ideal autocorrelation

  if it satisfies following property :

$$\sum_{i=0}^{2^n-2} (-1)^{b_i + b_{i+\tau}} = -1 \quad \text{for} \quad 1 \le \tau \le 2^n - 2$$

(v,k,λ)-Cyclic Difference Sets

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 as 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 (d_1,d_2), $d_1,d_2 \in D$ such that

$$d \equiv d_1 - d_2 \bmod v$$

Example 2

(15,7,3)-cyclic difference set

	0	5	7	10	11	13	14
0	0	5	7	10	11	13	14
5	10	0	2	5	6	8	9
7	8	13	0	3	4	6	7
10	5	10	12	0	1	3	4
11	4	9	11	14	0	2	3
13	2	7	9	12	13	0	1
14	1	6	8	11	12	14	0

⟺

binary sequence of period 15
with ideal autocorrelation

0 1 1 1 1 0 1 0 1 1 0 0 1 0 0

Definition of m-sequences

Let a be a generator of the multiplicative group of non zero elements of $GF(2^n)$.
Then $\{Tr(a^i)|i = 0,1,2,\cdots,2^n - 2\}$ gives a binary sequence of period $2^n - 1$, called an m-sequence, where

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \cdots + \alpha^{2^{n-1}}$$

Properties of m-sequences

- Balance property
- Constant-on-the-coset property
- Span-n property
- Ideal autocorrelation
- Cycle and Add property

Main Conjecture

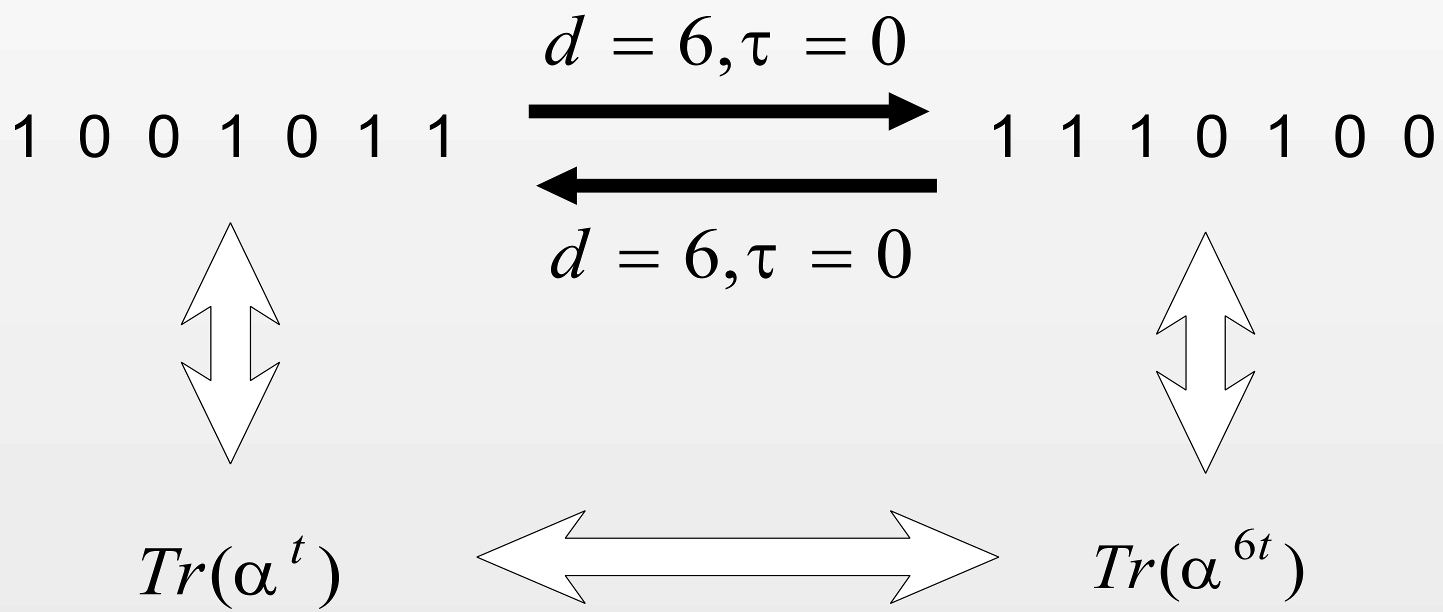
If a balanced binary sequence of period $2^n - 1$ has the span-n property and the ideal autocorrelation, then it is an m-sequence.

Equivalence of two sequences

Let $\{a_i\}$ and $\{b_i\}$ be two binary sequences of period $2^n - 1$. Then $\{a_i\}$ and $\{b_i\}$ are said to be equivalent if there exist d with $\gcd(d, 2^n - 1) = 1$ and τ with $0 \le \tau \le 2^n - 2$ such that $b_i = a_{di+\tau}$ for $i = 0, 1, 2, \cdots, 2^n - 2$, where the subscript is taken mod $2^n - 1$.

Example of equivalence

Let α be the primitive element of $GF(2^3)$ which satisfies $\alpha^3 + \alpha + 1 = 0$.



The results up to 1996

n	m	G	L	H	M	Total	having span-n properpty	
3	1	0	0	0	0	1	1	-
4	1	0	0	0	0	1	1	-
5	1	0	1	0	0	2	1	-
6	1	1	0	0	0	2	1	-
7	1	0	1	1	3	6	1	Baumert & Fredricksen ('67)
8	1	1	0	0	2	4	1	Cheng ('82)
9	1	1	0	0	2	4	1	Dreier ('92)
10	1	5	0	0	3 or more	9 or more	1 or more	-

+ Conjecture is still open!!!

(511,255,127) CDS

- Roland Dreier ('92)
  - 4 inequivalent examples
  - 1 of Singer type and 3 of non-Singer type
- New results ('97)
  - 5 inequivalent examples
  - 1 of Singer type and 4 of non-Singer type

Results in detail (use $\alpha \in GF(2^9)$ with $\alpha^9 + \alpha^4 + 1 = 0$)

m - sequence : $Tr(\alpha^{255t})$

1000000001000100011001000111010101101100011100010010101000110110011111001
1110001011011100101001000001001100111010001111101111000001111111110000111
1011100001011001101101111010000111001100001001000101011101011110010010111
0011100000011101110100111101010010100000010101010111110101101000001101110
1101101011000000101110111110001111001101001101011100011010001011111101001
0110001010011000110000000110011001010110010011111101101001001001101111110
0101101010000101000100111011001011110110000110101010011100100001100010000

GMW sequence : $Tr(\alpha^{19t}) + Tr(\alpha^{45t}) + Tr(\alpha^{83t})$

1000000101010110001001100111100100001100001010000010101011000010010100011
1110001010111001101010100001100100010011010010101001101001101100100001010
1011110100011101100111111101011010011100110110010100001111000010000101110
0011110001001011101110011010111110010000111100010110100100000000010001101
1101111011110010000100111011011010000011101110111111001101101100110000111
0110001111101111100011000110000000011111011000101011000010101110110101001
0101111110100100001101011100111110001111100100111101100110101110100100100

↑ ↑↑ ↑ ↑ ↑ ↑ ↑ ↑

Results (continued)

$M_1 : \; Tr(\alpha^{37t}) + Tr(\alpha^{85t}) + Tr(\alpha^{125t})$

1 0 0 0 0 1 0 0 0 1 1 0 0 0 0 1 0 0 1 1 1 1 0 0 0 0 0 1 0 1 1 1 0 0 0 0 1 0 1 0 1 1 1 1 0 0 0 0 0 0 0 1 0 0 1 1 0 0 1 1 1 0 1 0 0 1 0 0 0 1 0 0 1

1 001001101011110001000101010010000010110000111011011101011001010010000011

1 001001000011111001101111111101000111010101110011011100011001000000101110

0 111000001010010111100101101101110011000101001011001110000110001010100101 0

1 001001101011100000100101111101100001010001110111111101111110111010100111

0 100110011001101010000110110010111000010111100100110100000101110111111101

0 010101000010100100111010110011111111000001100111101111000101111000110100

$M_2 : \; Tr(\alpha^{25t}) + Tr(\alpha^{31t}) + Tr(\alpha^{55t}) + Tr(\alpha^{59t}) + Tr(\alpha^{79t}) + Tr(\alpha^{127t}) + Tr(\alpha^{191t})$

1 000010001110000000101110000100010000110010101100000010010010100100100000 11

1 110001110110001111000100010110000111010010011001001101011001000101001010

1 010100101011111110001110000000110111011000101110101001101111100010100111 11

0 011100001000000111100001101001111011100101100001001010010001001001100100 1

1 101110011010110011100101011101011000000111110010001010101111101111011011

0 110000001100110111100100011000010100111101110110001001000110101111111101 1

0 100101011000100001101010100011111101100010100111101110101101111110111111

Results (continued)

Newly Found

$$M_3 : \; Tr(\alpha^{t}) + Tr(\alpha^{7t}) + Tr(\alpha^{57t}) + Tr(\alpha^{77t}) + Tr(\alpha^{83t})$$
$$+ Tr(\alpha^{103t}) + Tr(\alpha^{111t}) + Tr(\alpha^{127t}) + Tr(\alpha^{183t})$$

1 0 0 1 0 1 1 0 0 0 1 0 1 1 0 1 0 1 0 1 1 1 0 1 1 0 1 0 0 1 1 0 0 1 1 0 0 0 1 0 1 1 1 1 0 1 1 0 1 0 0 1 1 0 0 0 0 1 1 1 1 0 0 1 0 0 1 0 1 1 0 1 0
1 011001101010100111110111010011100000000011111011010111010111011011001001
1 000111000011111001001100010000110101010100010101001110101101111000000010
0 000001001010111010011010001101101011011000111111001010001110010011010011
1 101000011111101000000110111111110100100100111001000010000000000111101100001
0 001000100100011001100111000010101101110011110010111110010101000000011100
0 000010101011000011101100110111000110001111001110101001011011110011101111

This sequence does not have the span-n property.

⟶ Therefore, the conjecture is still alive !!

Some Analysis for (1023,511,255) CDS

- # of cosets = 107

Size of Coset	1	2	5	10
# of cosets	1	1	6	99
# of cosets to be included	1	0	6	48

- Total # of binary sequences $= 2^{1023}$ ($\because$ length 1023)
- Total # of balanced examples = $\binom{1023}{511}$
- Above table shows that # of examples to check is $\binom{99}{48} \approx 4.8 \times 10^{28}$
- All these are partitioned into 197 subsets each of which may take about 74 years($\approx 2 \times 10^{9}$ sec) in PentiumPro.
  - 197 x 74 years = 14578 years of CPU time
  - It is equivalent to the computing power of checking $\frac{10^{26}}{10^{9}} = 10^{17}$ examples per sec.