

최적 상관 특성을 갖는 주기 **511**의 모든 이진수열*

김 정 현, 송 홍 엽, 박 규 태
연세대학교 전자공학과

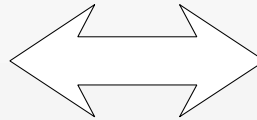
'97 한국 통신학회 하계 학술 대회

본 연구는 정보통신연구관리재단의 대학기초연구 지원사업의 연구비지원에 의한 결과입니다.

Example 1

(7,3,1)-cyclic
difference set

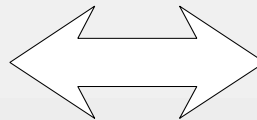
	1	2	4
1	0	1	3
2	6	0	2
4	4	5	0



binary sequence of
period 7 with ideal
autocorrelation

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

λ Definition

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

if it satisfies following property :

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

(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

$$d \equiv d_1 - d_2 \pmod{v}$$

Example 2

(15,7,3)-cyclic difference set

binary sequence of period 15
with ideal autocorrelation

	0	5	7	10	11	13	14	
0	0	5	7	10	11	13	14	$\longleftrightarrow$ 0 1 1 1 1 0 1 0 1 1 0 0 1 0 0
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	

Definition of m -sequences

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

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

Properties of m -sequences

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

Main Conjecture

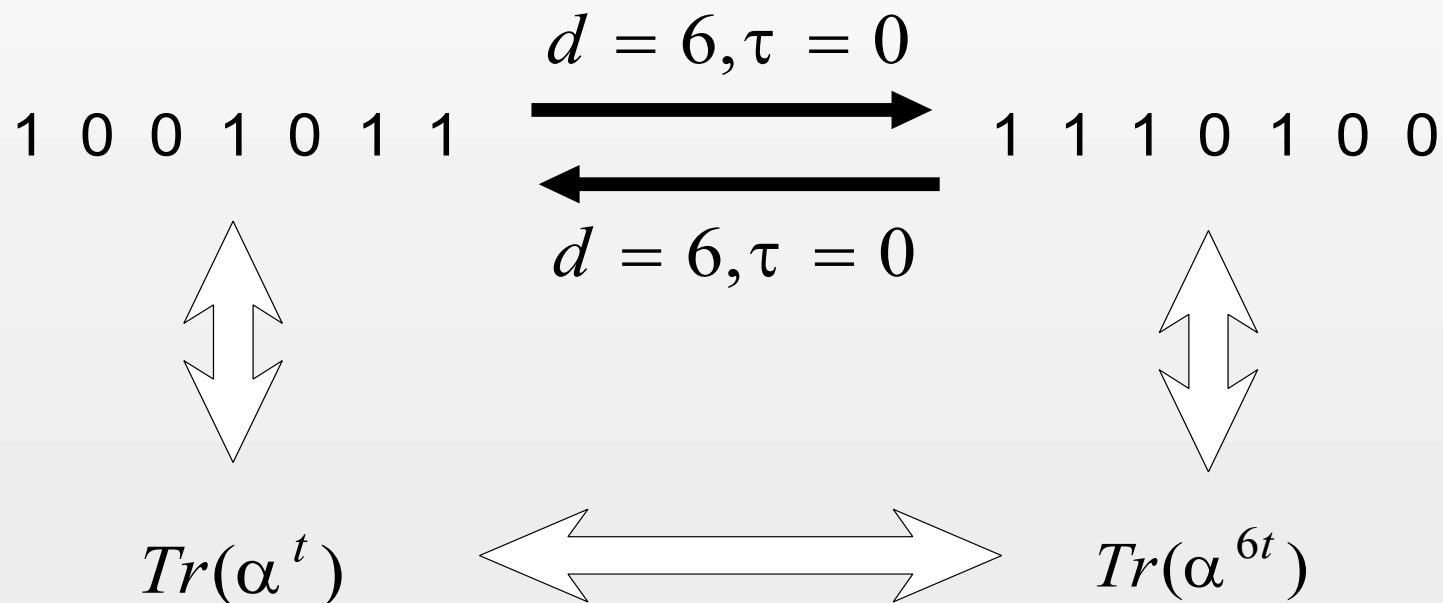
If a balanced binary sequence of period $2^n - 1$ has the span- n property and the ideal autocorrelation, then it is an m -sequence.

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 $0 \leq \tau \leq 2^n - 2$ such that $b_i = a_{di+\tau}$ for $i = 0, 1, 2, \dots, 2^n - 2$, 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 property	
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

λ Roland Dreier ('92)

- ✓ 4 inequivalent examples
- ✓ 1 of Singer type and 3 of non-Singer type

λ 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 : $Tr(\alpha^{255t})$

```
1 0 0 0 0 0 0 0 0 1 0 0 0 1 0 0 0 1 1 0 0 1 0 0 0 1 1 1 0 1 0 1 0 1 1 1 0 1 1 0 0 0 1 1 1 0 0 0 1 0 0 1 0 1 0 1 0 0 0 1 1 0 1 1 0 0 1 1 1 1 1 0 0 1
1 1 1 0 0 0 1 0 1 1 0 1 1 1 0 0 1 0 1 0 0 1 0 0 0 0 0 1 0 0 1 1 0 0 1 1 1 0 1 0 0 0 1 1 1 1 1 0 1 1 1 1 0 0 0 0 1 1 1
1 0 1 1 1 0 0 0 0 1 0 1 1 0 0 1 1 0 1 1 0 1 1 1 1 0 1 0 0 0 0 1 1 1 0 0 1 1 0 0 0 0 1 0 0 1 0 0 0 1 0 1 0 1 1 1 0 1 0 1 1 1 1 0 0 1 0 0 1 0 1 1 1
0 0 1 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 0 1 0 0 1 1 1 1 0 1 0 1 0 0 1 0 1 0 0 0 0 0 0 1 0 1 0 1 0 1 1 1 1 1 0 1 0 1 1 0 1 0 0 0 0 0 1 1 0 1 1 1 0
1 1 0 1 1 0 1 0 1 1 0 0 0 0 0 1 0 1 1 1 0 1 1 1 1 1 0 0 0 1 1 1 1 0 0 1 1 0 1 0 0 1 1 0 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 1 0 1 1 1 1 1 1 1 0 1 0 0 1
0 1 1 0 0 0 1 0 1 0 0 1 1 0 0 0 1 1 0 0 0 0 0 0 0 1 1 0 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 0 1 1 1 1 1 1 1 0 1 1 0 1 0 0 1 0 0 1 0 0 1 1 0 1 1 1 1 1 1 0
0 1 0 1 1 0 1 0 1 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 1 0 1 1 0 0 1 0 1 1 1 1 0 1 1 0 0 0 0 1 1 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 0 0 0 1 1 0 0 0 1 0 0 0 0
```

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

```
1 0 0 0 0 0 0 1 0 1 0 1 0 1 1 0 0 0 1 0 0 1 1 0 0 1 1 1 1 0 0 1 0 0 0 0 1 1 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 1 0 0 0 0 1 0 0 1 0 1 0 0 0 1 1
1 1 1 0 0 0 1 0 1 0 1 1 1 0 0 1 1 0 1 0 1 0 1 0 0 0 0 1 1 0 0 1 0 0 0 1 0 0 1 1 0 1 0 0 1 0 1 0 1 0 0 1 1 0 1 1 0 0 1 0 0 0 0 1 0 1 0
1 0 1 1 1 1 0 1 0 0 0 1 1 1 0 1 1 0 0 1 1 1 1 1 1 0 1 0 1 1 0 1 0 0 1 1 1 0 0 1 1 0 1 1 0 0 1 0 1 0 0 0 0 1 1 1 1 0 0 0 0 1 0 0 0 0 1 0 1 1 1 0
0 0 1 1 1 1 0 0 0 1 0 0 1 0 1 1 1 0 1 1 1 0 0 1 1 0 1 0 1 1 1 1 1 0 0 1 0 0 0 0 1 1 1 1 0 0 0 1 0 1 1 0 1 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 0 1 1 0 1
1 1 0 1 1 1 1 0 1 1 1 1 0 0 1 0 0 0 0 1 0 0 1 1 1 0 1 1 0 1 1 0 1 0 0 0 0 0 1 1 1 0 1 1 1 0 1 1 1 1 1 1 0 0 1 1 0 1 1 0 1 1 0 0 1 1 0 0 0 0 1 1 1
0 1 1 0 0 0 1 1 1 1 1 0 1 1 1 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 0 1 1 0 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 0 1 1 1 0 1 1 0 1 0 1 0 0 1
0 1 0 1 1 1 1 1 1 0 1 0 0 1 0 0 0 0 1 1 0 1 0 1 1 1 0 0 1 1 1 1 1 0 0 0 1 1 1 1 1 0 0 1 0 0 1 1 1 1 0 1 1 0 0 1 1 1 0 1 0 0 1 1 0 1 0 0 1 0 0 1 0 0
```

↑

↑↑

↑

↑

↑

↑

↑↑

↑↑

Results (continued)

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

```
1000010001100001001111000001011100001010111100000001001100111010010001001
1001001101011110001000101010010000010110000111011011101011001010010000011
1001001000011111001101111111110100011101010111001101110001100100000101110
0111000010100101111001011011011100110001010010110011100001100010101001010
1001001101011100000100101111101100001010001110111111101111110111010100111
0100110011001101010000110110010111000010111100100110100000101110111111101
0010101000010100100111010110011111111000001100111101111000101111000110100
```

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

```
1000010001110000001011100001000100001100101011000001001001010010010000011
1110001110110001111000100010110000111010010011001001101011001000101001010
1010100101011111100011100000011011101100010111010100110111110001010011111
0011100001000001111000011010011110111001011000010010100100010010011001001
1101110011010110011100101011101011000000111110010001010101111101111011011
0110000011001101111001000110000101001111011101100010010001101011111111011
0100101011000100001101010100011111101100010100111101110101101111110111111
```

Results (continued)

Newly Found

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

```
1001011000101101010111011010011001100010111101101001100001111001001011010
1011001101010100111110111010011100000000011111011010111010111011011001001
1000111000011111001001100010000110101010100010101001110101101111000000010
0000001001010111010011010001101101011011000111111001010001110010011010011
1101000011111101000001101111111101001001001110010000100000000011110110001
0001000100100011001100111000010101101110011110010111110010101000000011100
0000010101011000011101100110111000110001111001110101001011011110011101111
```

This sequence does not have the span-n property.
→ Therefore, the conjecture is still alive !!

Some Analysis for (1023,511,255) CDS

λ # 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

λ Total # of binary sequences = 2^{1023} ($\because$ length 1023)

λ Total # of balanced examples = $\binom{1023}{511}$

λ Above table shows that # of examples to check is $\binom{99}{48} \approx 4.8 \times 10^{28}$

λ 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.