# Relative Difference Set Design for Binary Three-level Autocorrelation Sequence Using Legendre Symbol and Trace Function



제 28회 통신정보 합동학술대회

김강산, 송민규, 송홍엽

연세대학교

# 자기상관

- 주기가 $L$인 이진 수열 $a_t$의 자기상관(Autocorrelation)

$$C_a(\tau) = \sum_{t=0}^{L-1} (-1)^{a_t + a_{t+\tau}}$$

- 자기상관 특성이 좋은 이진 수열
  - 대부분의 시간 지연 $\tau$에 대하여 자기상관의 크기(magnitude)가 작게 나오는 수열
  - 대표적으로 m-sequence 등이 있다.(한 주기 내에서 $\tau$=0을 제외하고 자기상관 값이 -1이 나옴)

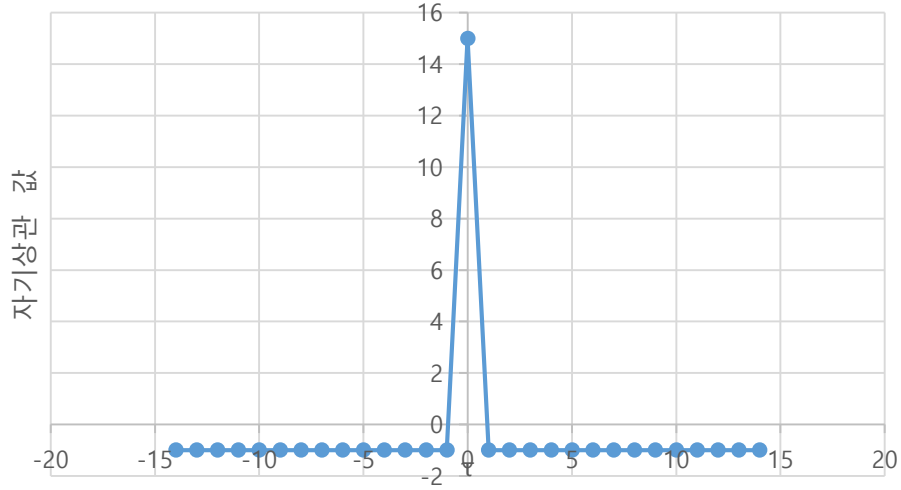


그림 1. 길이 15인 m-sequence의 시간지연 τ에 따른 자기상관 값

# Notation

- $q$ is a odd prime power.
- $F_q$ is a finite field of size q
- $F_{q^n}$ is a finite field of size $q^n$
- $\alpha$ is a primitive element of $F_{q^n}$
- $\beta$ is a primitive element of $F_q$
- $Tr_1^n(x) \in F_q$ is the trace of $x \in F_{q^n}$ defined by

$$Tr_1^n(x) = \sum_{i=0}^{n-1} x^{q^i}$$

- $(\frac{\cdot}{F_q})$ is a function from $F_q$ to the complex numbers defined by

$$(\frac{x}{F_q}) = \begin{cases} 1 & If\ \ x \neq 0\ \ is\ \ a\ quadratic\ element\ of\ F_q \\ -1 & If\ \ x \neq 0\ \ is\ \ not\ a\ quadratic\ element \\ 0 & If\ x = 0 \end{cases}$$

# Relative Difference Set

- Definition1

Let $u,w,k,\lambda$ be positive integers. A $(u,w,k,\lambda)$ relative difference set (RDS) D $=\{d_1, d_2, \ldots, d_k\}$ is a $k$-subset of $Z_{uw}$ satisfying the following conditions:

- $\{d_i - d_j | d_i \neq d_j$, for $d_i$, $d_j \in$ D $\} = Z_{uw} \backslash \mathrm{u} Z_{uw}$
- For any $d$ in $Z_{uw} \backslash \mathrm{u} Z_{uw}$, the congruence $d_i - d_j \equiv d$ (mod uw) has exactly $\lambda$ solution pairs $(d_i, d_j)$ with $d_i, d_j \in$ D.

- Example1

D={1, 2, 4}, uw=7

| $d_j \backslash d_i$ | 1 | 2 | 4 |
|---|---|---|---|
| 1 | 0 | 1 | 3 |
| 2 | 6 | 0 | 2 |
| 4 | 4 | 5 | 0 |

표 1. D={1, 2, 4}, uw=7일때 $d_i - d_j$ 값

- $\{d_i - d_j | d_i \neq d_j$, for $d_i$, $d_j \in$ D $\}$ $=\{1, 2, 3, 4, 5, 6\}=Z_7 \backslash \{0\}$
- $d_i - d_j \equiv$ d (mod 12) in $Z_7 \backslash \{0\}$ has exactly 1 solution pair $(d_i, d_j)$

=> D is a (7,1,3,1) RDS

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

6 없음

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

# Relative Difference Set

- Example 2

D={1,4,5,6,8}, uw=12

| $d_j \backslash d_i$ | 1 | 4 | 5 | 6 | 8 |
|---|---|---|---|---|---|
| 1 | 0 | 3 | 4 | 5 | 7 |
| 4 | 9 | 0 | 1 | 2 | 4 |
| 5 | 8 | 11 | 0 | 1 | 3 |
| 6 | 7 | 10 | 11 | 0 | 2 |
| 8 | 5 | 8 | 9 | 10 | 0 |

표 2. D={1,4,5,6,8}, uw=12일때 $d_i - d_j$ 값

- $\{d_i - d_j | d_i \neq d_j$, for $d_i$, $d_j \in$ D $\}$={1,2,3,4,5,7,8,9,10,11}=$Z_{12} \backslash 6Z_{12}$
- $d_i - d_j \equiv d \ (mod\ 12)$ in $Z_{12} \backslash 6Z_{12}$has exactly 2 solution pair $(d_i, d_j)$

=> D is (6,2,5,2) RDS

# Characteristic Sequence of RDS

- (u,w,k,$\lambda$) RDS인 D에 대해 주기가 uw인 이진 수열 $s_t$를 다음과 같이 정의하자

$$s_t = \begin{cases} 1 & for\ \ t \in D \\ 0 & for\ t \notin D \end{cases}$$

그렇다면 수열 $s_t$는 항상 다음과 같은 자기상관을 갖는다.

$$C_s(\tau) = \begin{cases} uw & \tau = 0 \\ uw - 4(k-\lambda) & \tau \in Z_{uw} \backslash \mathrm{u} Z_{uw} \\ uw - 4k & otherwise \end{cases}$$

# Characteristic Sequence of RDS

- Example 3
  - D={1,4,5,6,8}: (6,2,5,2) RDS
  - $s_t$={0,1,0,0,1,1,1,0,1,0,0,0,…}

- $\tau = 1,2,3,4,5,$
  $C_s(\tau)$ =agreement-disagreement=6-6=0,
  $uw$ -4(k-$\lambda$)=0
- $\tau$=6,
  $C_s(\tau)$ =agreement-disagreement=2-10=-8,
  $uw - 4k$=-8

| | | |
|---|---|---|
| $s_t$ | 0 1 0 0 1 1 1 0 1 0 0 0 | |
| $s_{t+1}$ | 1 0 0 1 1 1 0 1 0 0 0 0 | |
| $s_t$ | 0 1 0 0 1 1 1 0 1 0 0 0 | |
| $s_{t+2}$ | 0 0 1 1 1 0 1 0 0 0 0 1 | |
| $s_t$ | 0 1 0 0 1 1 1 0 1 0 0 0 | |
| $s_{t+3}$ | 0 1 1 1 0 1 0 0 0 0 1 0 | |
| $s_t$ | 0 1 0 0 1 1 1 0 1 0 0 0 | |
| $s_{t+4}$ | 1 1 1 0 1 0 0 0 0 1 0 0 | |
| $s_t$ | 0 1 0 0 1 1 1 0 1 0 0 0 | |
| $s_{t+5}$ | 1 1 0 1 0 0 0 0 1 0 0 1 | |
| $s_t$ | 0 1 0 0 1 1 1 0 1 0 0 0 | |
| $s_{t+6}$ | 1 0 1 0 0 0 0 1 0 0 1 1 | |

# Elliott-Butson RDS

- Theorem 1 (J. Elliott and A. Butson, "Relative difference sets," *Illinois Journal of Mathematics*, 1966)

$$\{t | Tr_1^n(\alpha^t) = 1, 0 \le t < q^n - 1\} \pmod{2\frac{q^n-1}{q-1}}$$

is a $(\frac{q^n-1}{q-1}, 2, q^{n-1}, q^{n-2}(\frac{q-1}{2}))$-RDS.

# Elliott-Butson RDS

- Theorem 2

$$\{\, t \mid \left(\frac{Tr_1^n(\alpha^t)}{F_q}\right) = 1,\ 0 \le t < 2\frac{q^n-1}{q-1}\}$$

is an Elliott-Butson RDS with parameters

$$(\frac{q^n-1}{q-1},\ 2,\ q^{n-1}, q^{n-2}(\frac{q-1}{2})).$$

*Proof) Let* $U=\{\, t \mid \left(\frac{Tr_1^n(\alpha^t)}{F_q}\right) = 1,\ 0 \le t < 2\frac{q^n-1}{q-1}\}$ *and*

$V= \{t | Tr_1^n(\alpha^t) = 1, 0 \le t < q^n - 1\}$ (mod $2\frac{q^n-1}{q-1}$) .

For any $t_1$ in U, there exists integer b with $0 \le b < \frac{q-1}{2}$ such that

$Tr(\alpha^{t_1}) = \beta^{2b}$. Then $Tr_1^n(\alpha^{t_1+(q-1-2b)\frac{q^n-1}{q-1}})$=1. So $t_1$ *is in* $V$ and U$\subset V$.

# Elliott-Butson RDS

Since the ternary sequence $Tr_1^n(\alpha^t)$ has period $2\frac{q^n-1}{q-1}$, then the cardinality of U can be written as,

$$|U|=\frac{2}{q-1}\left|\{\, t \mid \left(\frac{Tr_1^n(\alpha^t)}{F_q}\right)=1,\ 0 \le t < q^n-1\}\right|$$

$$=q^{n-1}$$

It equals the cardinality of V. So U=V.

# Binary sequence with 3-level autocorrelation

- Definition 2 (A. M. Arshad et al, IWSDA, 2017 )

$$s_t = \begin{cases} 1 & if \left(\frac{Tr_1^{\mathrm{n}}(\alpha^{\mathrm{t}})}{\mathrm{F_q}}\right) = 1 \\ 0 & Otherwise \end{cases}$$

- 위 이진 수열 $s_t$는 $2\frac{q^n-1}{q-1}$의 주기를 갖고. 다음과 같은 자기상관을 갖는 것으로 잘 알려져 있다.

$$C_s(\tau) = \begin{cases} 2\dfrac{q^n-1}{q-1} & \text{for } \tau = 0 \\ 2\dfrac{q^n-1}{q-1} - 4q^{n-1} & \text{for } \tau = \dfrac{q^n-1}{q-1} \\ 2\dfrac{q^{n-2}-1}{q-1} & Otherwise. \end{cases}$$

# Binary sequence with 3-level autocorrelation

- 사실 이 수열 $s_t$는 Theorem 2의 $(\frac{q^n-1}{q-1}, 2, q^{n-1}, q^{n-2}(\frac{q-1}{2}))$-RDS인

$$\{ t \mid \left(\frac{Tr_1^n(\alpha^t)}{F_q}\right) = 1,\ 0 \le t < 2\frac{q^n-1}{q-1} \}$$

의 characteristic sequence 이다. 따라서 아래와 같은 3-level 자기 상관 특성도 사실 RDS의 characteristic sequence의 성질에 기인한 것이다.

$$C_s(\tau) = \begin{cases} 2\dfrac{q^n-1}{q-1} & \text{for } \tau = 0 \\ 2\dfrac{q^n-1}{q-1} - 4q^{n-1} & \text{for } \tau = \dfrac{q^n-1}{q-1} \\ 2\dfrac{q^{n-2}-1}{q-1} & Otherwise. \end{cases}$$

# 결론

- RDS를 이용하여 수열을 설계하면 대부분의 시간지연 $\tau$에서 0에 가까운 값이 나오는 3-레벨 자기상관을 갖게된다.
- 실제로 A. M. Arshad이 설계한 수열이 3-level 자기상관을 갖게 되는건 RDS의 characteristic sequence의 성질에 기인한것이다.