주기 $q^d - 1$을 가지는 **Sidelnikov** 수열의 **2**차원 배열구조의 특징

2013년 통신정보 합동학술대회

10000001000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

2013.05.02

연세대학교

부호 및 암호 연구실

김영태, 송홍엽

서 론

- Sidelnikov 수열은 좋은 자기상관특성에 대해 연구되었고, 이를 이용한 수열군에 대한 연구가 2000년대 중반에 이르러 시작됨.

- 현재 상수배, shift-and-add 등의 방식이 사용되었고, Sidelnikov 수열의 2차원 배열구조를 활용되고 있음.

- 주기 $q^d - 1$을 가지는 수열의 2차원 배열구조에서 $(d, q-1) = 1$ 조건이 필요하여 적용 가능한 d의 수가 적다.

- 이를 개선하기 위해, $(d, q-1) = 1$ 조건이 필요 없는 방법을 제안한다.

Notation

- p : prime, $q = p^n$: prime power
- $GF(q)$: finite field of order q
- β : primitive element of $GF(q)$, α : primitive element of $GF(q^d)$
- ω_M : complex M^{th} root of unity where $M|q-1$
- ψ : the **multiplicative character of order *M*** from $GF(q)$ to complex, defined by $\psi(x) = \exp(2\pi i \log_\beta x\,/M) = \omega_M^{\log_\beta x}$ and $\psi(0) = 1$.
- **Correlations** and **Sequence Families**

  Let $a(t), b(t)$ be M-ary sequences of period L. A (periodic) correlation of sequences $a(t), b(t)$ is defined by

$$C_{a,b}(\tau) = \sum_{t=0}^{L-1} \omega_M{}^{a(t)-b(t+\tau)}.$$

  For a sequence set $\mathcal{S}$, $C_{\max}(\mathcal{S})$ is the maximum magnitude of all nontrivial correlations of pairs of sequences in $\mathcal{S}$.

Weil bound

- **Refined Weil bound** Gong-10

Let $f_1(x), \ldots, f_l(x)$ be l monic and irreducible polynomial over $GF(q)$ which have positive degrees $d_1, \ldots, d_l$, respectively. Let d be the number of distinct roots of $f(x) = \prod_{i=1}^{l} f_i(x)$ in its splitting field over $GF(q)$. Let $\psi_1, \ldots, \psi_l$ be multiplicative characters of $GF(q)$. Assume that the product character $\prod_{i=1}^{l} \psi_i(f_i(x))$ is nontrivial. Let e_i be the number of distinct roots in $GF(q)$ of $f_i(x)$. If $\psi_i(0) = 1$, then for every $a_i \in \mathbb{F}_q \backslash \{0\}$,

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_l(a_l f_l(x)) \right| \leq (d-1)\sqrt{q} + \sum_{i=1}^{l} e_i \, .$$

Sidelnikov Sequences

- **Definition** Sidelnikov-69
  - Let $D_k = \{\beta^{Mi+k} - 1 | 0 \le i < \frac{q-1}{M}\}$ for $0 \le k \le M-1$. $(M|q-1)$
  - The $\boldsymbol{M}$**-ary Sidelnikov sequence of period** $\boldsymbol{q-1}$ is defined by

$$s(t) = \begin{cases} 0, & \text{if } \beta^t = -1 \\ k, & \text{if } \beta^t \in D_k \end{cases}$$

  - Equivalently, $s(t)$ is defined by

$$\boldsymbol{s(t) \equiv \log_\beta(\beta^t + 1) \mod M,\ 0 \le t \le q-2}$$

Example of Sidelnikov Sequence

- Consider $q = 7, M = 6$. A primitive element of $GF(7)$ is 3. So we can define 6-ary Sidelnikov sequence of period 6.

t	β^t	$\beta^t + 1$	$s(t)$
0	1	2	2
1	3	4	4
2	2	3	1
3	6	0	0
4	4	5	5
5	5	6	3

2차원 배열 구조와 기존 결과 (1)

- Sidelnikov sequence of length $q^d - 1$ is written in an array of size $(q-1) \times (\frac{q^d-1}{q-1})$.
- **Theorem** (Kim-10)

  Column sequences of array $v_l(t)$ can be represented as

  $$\boldsymbol{v_l(t) = \log_\beta f_l(\beta^t)}$$

  where $f_l(x) = N(\alpha^l x + 1)$.

  - **Proof** A Theorem is equivalent to $s(t) \equiv \log_\beta(N(\alpha^t + 1)) \bmod M$.

  Let $\beta^{x(t)} = N(\alpha^t + 1)$. Then $\frac{q^d-1}{q-1} s(t) \equiv \log_\alpha(\alpha^t + 1)^{\frac{q^d-1}{q-1}} \equiv$

  $\log_\alpha N(\alpha^t + 1) \equiv \log_\alpha \alpha^{\frac{q^d-1}{q-1}x(t)} \equiv \frac{q^d-1}{q-1} x(t) \bmod M \cdot \frac{q^d-1}{q-1}$. This implies that $x(t) \equiv s(t) \bmod q - 1$ and hence that, as $M | q - 1$, $s(t) \equiv x(t) \equiv \log_\beta N(\alpha^t + 1) \bmod M$.

2차원 배열 구조와 기존 결과 (2)

- **Theorem** (Kim-10)

  Assume that $(\boldsymbol{d}, \boldsymbol{q}-\mathbf{1}) = \mathbf{1}, \boldsymbol{d} < \frac{\sqrt{\boldsymbol{q}} - \frac{\mathbf{2}}{\sqrt{\boldsymbol{q}}} + \mathbf{1}}{\mathbf{2}}$. For family

  $$\boldsymbol{\Sigma} = \{\boldsymbol{c}\boldsymbol{v}_{\boldsymbol{l}}(\boldsymbol{t}) | \mathbf{1} \leq \boldsymbol{c} < \boldsymbol{M}, \boldsymbol{l} \in \boldsymbol{\Lambda} \backslash \{\mathbf{0}\}\}$$

  where Λ is the set of all integers $k \left(0 \leq k \leq \frac{q^d - 1}{q-1} - 1\right)$ consisting of the smallest q-cyclotomic coset representative from each q-cyclotomic coset mod $\frac{q^d-1}{q-1}$, we have

① $|C_{max}(\Sigma)| \leq (2d-1)\sqrt{q} + 1$.

② The asymptotic size is $\frac{(M-1)q^{d-1}}{d}$ as $q \to \infty$.

Main Result

- Let Λ be the subset of $\{l|0 \leq l < \frac{q^d-1}{q-1}\}$ consisting of the smallest q-cyclotomic coset representative from each q-cyclotomic coset mod $\frac{q^d-1}{q-1}$.
- Consider $C_l = \{l, ql, \cdots, q^{m_l-1}l\}$ for arbitrary l where m_l is minimum positive integer such that $q^{m_l}l \equiv l \bmod \frac{q^d-1}{q-1}$.

  We define $\Lambda' = \{l \in \Lambda | m_l = d\}$.

- **Main Theorem**
  - For $d < \frac{\sqrt{q}-\frac{2}{\sqrt{q}}+1}{2}$, the sequences in the family

    $$\Sigma' = \{cv_l(t)|1 \leq c < M, l \in \Lambda' \backslash \{0\}\}$$

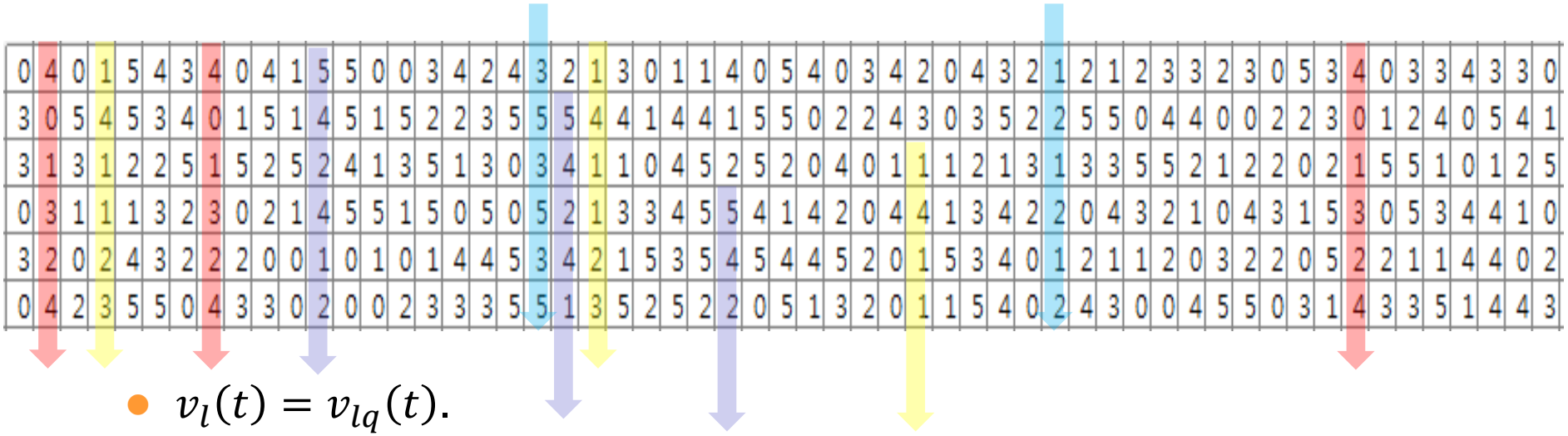
    are cyclically inequivalent.

- $(q-1, d) = 1$ 이 아닌 배열 구조의 예

  Let $q = 7, M = 6, d = 3$. Consider finite field $GF(343)$.

  Then 6-ary Sidelnikov sequence $s(t)$ of period 48 is represented by 6×57 array as follows:

$$s(t) = [v_0(t), v_1(t), \cdots, v_{55}(t), v_{56}(t)]$$



  - $v_l(t) = v_{lq}(t)$.
  - In above figure, $v_{19}(t)$ and $v_{38}(t)$ are sequences of period 2.
  - In general, we can not use all column sequences for $(q-1, d) \neq 1$.

Λ와 Λ'의 크기 비교

q	d	$(q-1, d)$	$\lvert\Lambda\rvert$	$\lvert\Lambda'\rvert$
49	3	3	818	816
121	3	3	4922	4920
121	4	4	446643	446520
169	3	3	9578	9576
169	4	4	1213971	1213800
243	3	1	19764	19764
243	4	2	3602172	3601928
256	3	3	21932	21930
256	4	1	4210816	4210688
289	3	3	27938	27936
289	4	4	6055491	6055200
343	3	3	39332	39330
343	4	2	10118072	10117728

Proof of Main Theorem

- Let $c_1 v_{l_1}(t) = c_2 v_{l_2}(t+\tau)$ for some τ $(o \le \tau < q-1)$.
- Hence,

$$q-1 = \sum_{t=0}^{q-2} \omega_M^{c_1 v_{l_1}(t) - c_2 v_{l_2}(t+\tau)} = \sum_{t=0}^{q-2} \psi^{c_1}\left(f_{l_1}(\beta^t)\right)\psi^{M-c_2}\left(f_{l_2}(\beta^{t+\tau})\right)$$

$$= \sum_{x \in GF(q)} \psi_1\left(\beta^{l_1} p_{l_1}(x)\right)\psi_2\left(\beta^{l_2} \cdot \beta^{\tau d} \cdot \beta^{-\tau d} p_{l_2}(\beta^{\tau} x)\right) - 1$$

where $\psi_1 = \psi^{c_1}$ and $\psi_2 = \psi^{M-c_2}$ and $p_l(x) = \beta^{-l} f_l(x)$.

- **Claim**

$$\sum_{x \in GF(q)} \psi_1\left(\beta^{l_1} p_{l_1}(x)\right)\psi_2\left(\beta^{l_2} \cdot \beta^{\tau d} \cdot \beta^{-\tau d} p_{l_2}(\beta^{\tau} x)\right)$$

$$\le (d + d - 1)\sqrt{q} = (2d-1)\sqrt{q}.$$

- If claim is true, then $q - 1 \le (2d-1)\sqrt{q} + 1$.
- This is impossible in view of our assumption $d < \frac{\sqrt{q} - \frac{\sqrt{q}}{2} + 1}{2}$.

- For proof of claim, we have to show that following statement.

  - Let l_1, l_2 be elements in $\Lambda' \backslash \{0\}$, and let $\tau (0 \leq \tau < q-1)$ be an integer. Then $p_{l_1}(x)$ and $\beta^{-\tau d} p_{l_2}(\beta^{\tau} x)$ are distinct irreducible polynomials over $GF(q)$, unless $l_1 = l_2$ and $\tau = 0$.

  - $p_l(x)$ is alternative form of $f_l(x) = N(\alpha^l x + 1)$.

    For each $l \left(0 \leq l < \frac{q^d - 1}{q-1}\right)$,

    $$\begin{aligned} f_l(x) &= \beta^l N(x + \alpha^{-l}) \\ &= \beta^l (x + \alpha^{-l})(x + \alpha^{-lq}) \cdots (x + \alpha^{-lq^{d-1}}) \\ &= \beta^l p_l(x)^{d/d_l} \end{aligned}$$

    where $p_l(x)$ is the minimal polynomial over $GF(q)$ of $-\alpha^{-l}$ of degree d_l. And if $l \in \Lambda'$, then $d = d_l = m_l$. So, $f_l(x) = \beta^l p_l(x)$.

- **Proof of statement**
  - ✓ Assume that they are the same.
  - ✓ $\beta^{-\tau d} p_{l_2}(\beta^{\tau} x) = \left(x + \alpha^{-l_2}\beta^{-\tau}\right)\left(x + \alpha^{-l_2 q}\beta^{-\tau}\right) \cdots \left(x + \alpha^{-l_2 q^{d-1}}\beta^{-\tau}\right)$ imply $\alpha^{-l_1} = \alpha^{-l_2 q^s}\beta^{-\tau}$ for some nonnegative integer s $(s < d)$.
  - ✓ Hence $l_1 \equiv l_2 q^s + \tau\left(\frac{q^d-1}{q-1}\right) \bmod q^d - 1$.
  - ✓ So, $l_1 \equiv l_2 q^s \bmod \frac{q^d-1}{q-1}$, and $\boldsymbol{l_1 = l_2}$.
  - ✓ Now $l_1 \equiv l_1 q^s \bmod \frac{q^d-1}{q-1}$, and hence $s = 0$ since $m_{l_1} = d$.
  - ✓ In all, $l_1 \equiv l_1 + \tau\left(\frac{q^d-1}{q-1}\right) \bmod q^d - 1$.
  - ✓ This implies $q - 1 | \tau$, and therefore $\boldsymbol{\tau = 0}$.

결 론

- 기존의 방식의 단점을 보완하여 $(d, q-1)=1$ 조건을 완화할 수 있었고, 그 결과 사용 가능한 d의 범위가 크게 늘어남.

참고 문헌

1. V. M. Sidelnikov, "*Some k-valued pseudo-random sequences and nearly equidistant codes*," Probl. Inf. Transm., vol. 5, pp. 12-16, 1969
2. N. Y. Yu, G. Gong, "*New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences*," IEEE Trans. Inf. Theory, vol. 56, no. 8, pp. 4061-4070, 2010
3. D. S. Kim, "*A family of sequences with large size and good correlation property arising from M-ary Sidelnikov sequences of period* $q^d - 1$," arXiv:1009.1225v1, 2010