Frequency-hopping sequences from the array structure of Sidelnikov sequences

Hong-Yeop Song

Yonsei University

2017 Sino-Korea conference on coding theory and its related topics

July 10-15, 2017

NIMS, KOREA

What we will concern

- Introduction and **array structure** of Sidelnikov sequences under the complex correlation properties
- **Hamming correlation** properties of Sidelnikov sequences
- **A construction** for set of frequency-hopping sequences from the array structure of Sidelnikov sequences
- Discuss **optimality** and their relationship to RS codes

A full version of this presentation was recently submitted to
IEEE Trans. Information Theory (2017. 05)

Toward

array structure

of Sidelnikov sequences

Complex correlation

Let $\{a(t)\}_{t=0}^{L-1}$ and $\{b(t)\}_{t=0}^{L-1}$ be two ***M*-ary sequences** of period L.

A complex (periodic) correlation between $\{a(t)\}$ and $\{b(t)\}$ is defined by

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

For a set of sequences (or a sequence family) Ω, we denote the **maximum magnitude** of all the non-trivial complex correlations of any two pair of sequences in Ω as $\mathbf{C_{max}(\Omega)}$.

We consider only the **PHASE sequences** of **complex root-of-unity-sequences**

$$\text{M-ary} = \text{M-phase}$$

Complex correlation of Sidelnikov sequence

- Sidelnikov showed that magnitude of any out-of-phase complex **auto-correlation** of a Sidelnikov sequence is less than or equal to 4.
- That is,

$$\max_{\tau \neq 0} |C(\tau)| \leq 4$$

for any M -ary Sidelnikov sequence of period $q-1$

$q =$ *any prime power*

$M =$ *any divisor of q-1,* $M>1$

History on this line
(complex correlation and array structure)

Sidelnikov 69

First construction for set of sequences with good complex correlation by using Sidelnikov sequences.

Song 07

No 08 and Yang 09

First use of shift-and-add (Gold-like) to increase the family size **and use Weil bound** to prove the correlation bound

Gong 10

First analyzed $(q-1)\times(q+1)$ **array** of Sidelnikov sequences of period q^2-1. Here, $d=2$ ONLY.

Song 15

Analyzed $(q-1)\times\frac{q^d-1}{q-1}$ **array** of Sidelnikov sequences of period q^d-1 where $2\le d<\frac{1}{2}\left(\sqrt{q}-\frac{2}{\sqrt{q}}+1\right)$.

Song 16

Combined column sequences from $(q-1)\times\frac{q^d-1}{q-1}$ **arrays** of Sidelnikov sequences of periods $\boldsymbol{q^2-1, q^3-1, \ldots, q^d-1}$ where $2\le d<\frac{1}{2}\left(\sqrt{q}-\frac{2}{\sqrt{q}}+1\right)$.

Song 2007

- Complex crosscorrelation of a set which consists of $\boldsymbol{M}$-ary Sidelnikov sequence $\boldsymbol{s} = \{\boldsymbol{s(t)}\}_{\boldsymbol{t=0}}^{\boldsymbol{q-2}}$ of length $q-1$ and its constant multiple sequence $\{\boldsymbol{c} \cdot s(t)\}_{t=0}^{q-2}$ is upper bounded by $\boldsymbol{\sqrt{q}+3}$.
  - When $\gcd(c, M) \neq 1$, the resulting sequence is NOT a Sidelnikov sequence in general.
  - Otherwise, the resulting sequence is another Sidelnikov sequence obtained by using another primitive element of GF(q).

- This gives a family of M-ary sequences of period $q-1$ containing at most $M-1$ cyclically distinct sequences.
- The exact size is given as $\varphi(M)$.

No 2008, Yang 2009

Shift-and-add

- Main Theorem (No-08, Yang-09)

  Let $s(t)$ be an M-ary Sidelnikov sequence of period $q-1$, with p odd.

  Let $T = \lceil (q-1)/2 \rceil$.

  Let $\mathcal{L}$ be the set of M-ary sequences of period $q-1$ given as follows.

$$\mathcal{L} = \{c_1 s(t) | 1 \le c_1 \le M-1\} \quad \cup$$
$$\{c_1 s(t) + c_2 s(t+l) | 1 \le c_1, c_2 \le M-1, 1 \le l \le T-1\}$$
$$\cup \{c_1 s(t) + c_2 s(t+T) | 1 \le c_1, c_2 \le M-1\}$$

  Then,

  ① Correlations of the family $\mathcal{L}$ is upper bounded by

$$|\boldsymbol{C(\tau)}| \le \mathbf{3}\sqrt{\boldsymbol{q}} + \mathbf{5}.$$

  ② Family size is $\frac{\boldsymbol{(M-1)^2(q-3)}}{\mathbf{2}} + \frac{\boldsymbol{M(M-1)}}{\mathbf{2}}$.

Array structure (Gong10)

- Let $q = 7,\ M = 6$. A 6-ary Sidelnikov sequence $s(t)$

of period $\boldsymbol{q^2 - 1 = 48}$

is represented by 6×8 array as follows:

$$s(t) = [v_0(t), v_1(t), v_2(t), v_3(t), v_4(t), v_5(t), v_6(t), v_7(t)]$$

$$= \begin{bmatrix} 4 & 1 & 5 & 0 & 5 & 1 & 5 & 1 \\ 2 & 4 & 4 & 2 & 2 & 2 & 5 & 4 \\ 2 & 4 & 3 & 3 & 1 & 0 & 4 & 4 \\ 0 & 5 & 0 & 3 & 5 & 2 & 3 & 5 \\ 4 & 1 & 3 & 1 & 2 & 3 & 0 & 1 \\ 0 & 0 & 5 & 2 & 1 & 3 & 3 & 0 \end{bmatrix}.$$

array size

$$(q-1) \times \frac{q^2 - 1}{q - 1}$$

$$(q-1) \times (q+1)$$

- $v_l(t) = s\big((q+1)t + l\big)$ for $0 \le t \le q-2$ and each $l = 0,1,2,\dots,q$.
  - $v_0(t) = 2s'(t)$, where $\boldsymbol{s'(t) = (2,4,1,0,5,3)}$ is a 6-ary Sidelnikov sequence.
  - $v_l(t) = v_{q+1-l}(t+1-l)$ for $0 \le t \le q-2$ and each $l = 1,2,\dots,q$.

Song 2015 – further generalization

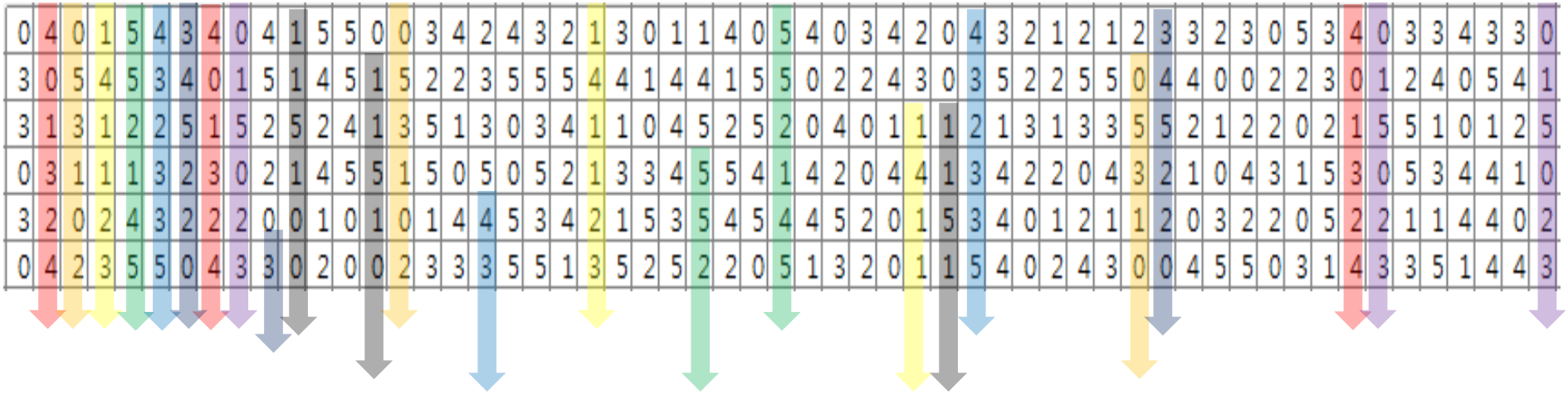
- $(q-1)\times\frac{q^{d}-1}{q-1}=(q-1)\times(q^{d-1}+q^{d-2}+\cdots+1)$

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

Then 6-ary Sidelnikov sequence $s(t)$ of period 342 is represented by 6×57 array as follows:

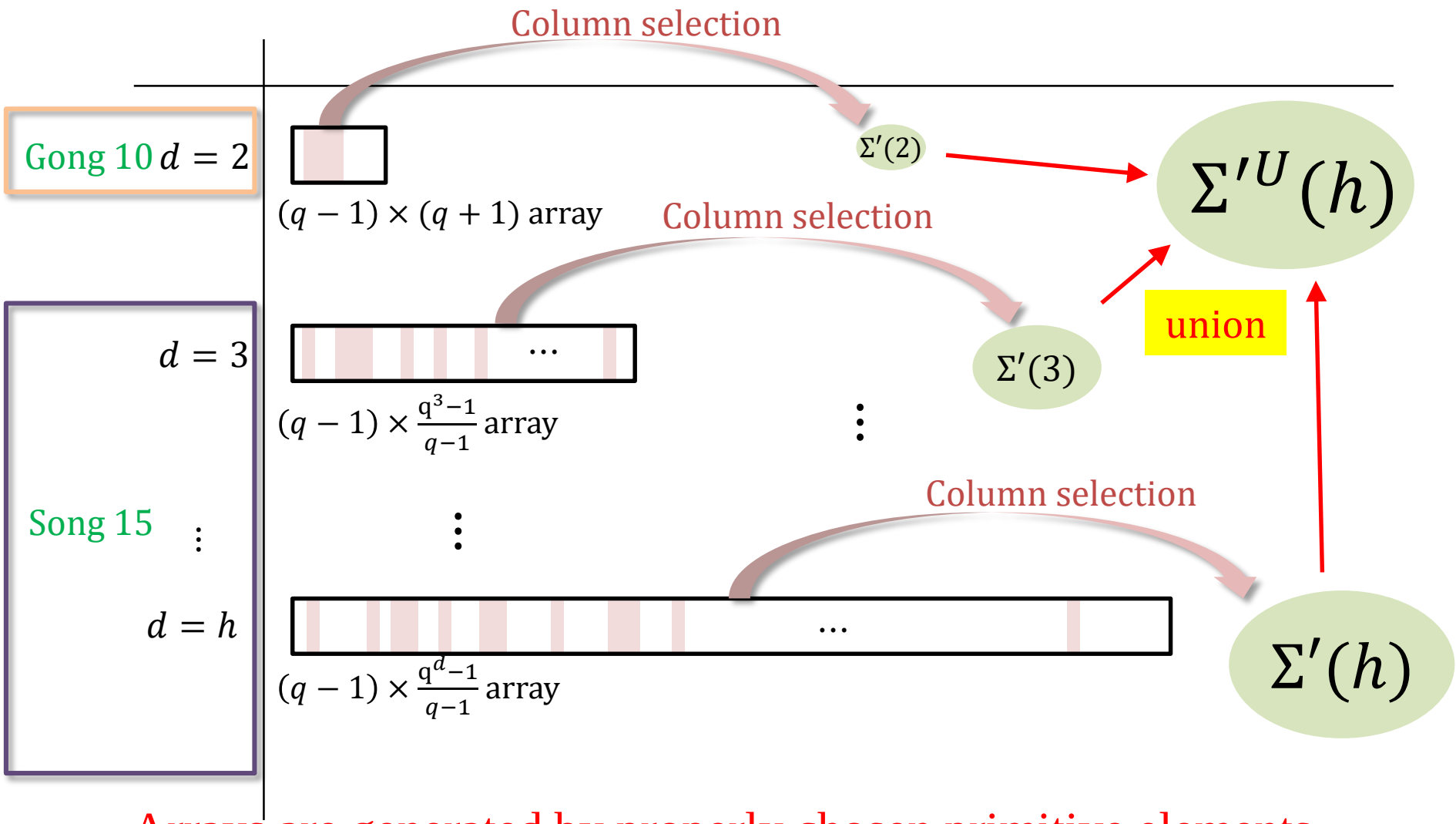
$$s(t)=[v_0(t), v_1(t), \cdots, v_{55}(t), v_{56}(t)]$$

012345678901234567890123456789012345678901234567890123456



- $v_l(t)=v_{lq}(t)$.
- For nonnegative integers l_1, l_2, with $l_1\equiv l_2 \bmod \frac{q^{d}-1}{q-1}$, $v_{l_1}(t)$ and $v_{l_2}(t)$ are cyclically equivalent.

Song 2016 (ISIT) – combine all d



Arrays are generated by properly chosen primitive elements.

Hamming correlation property

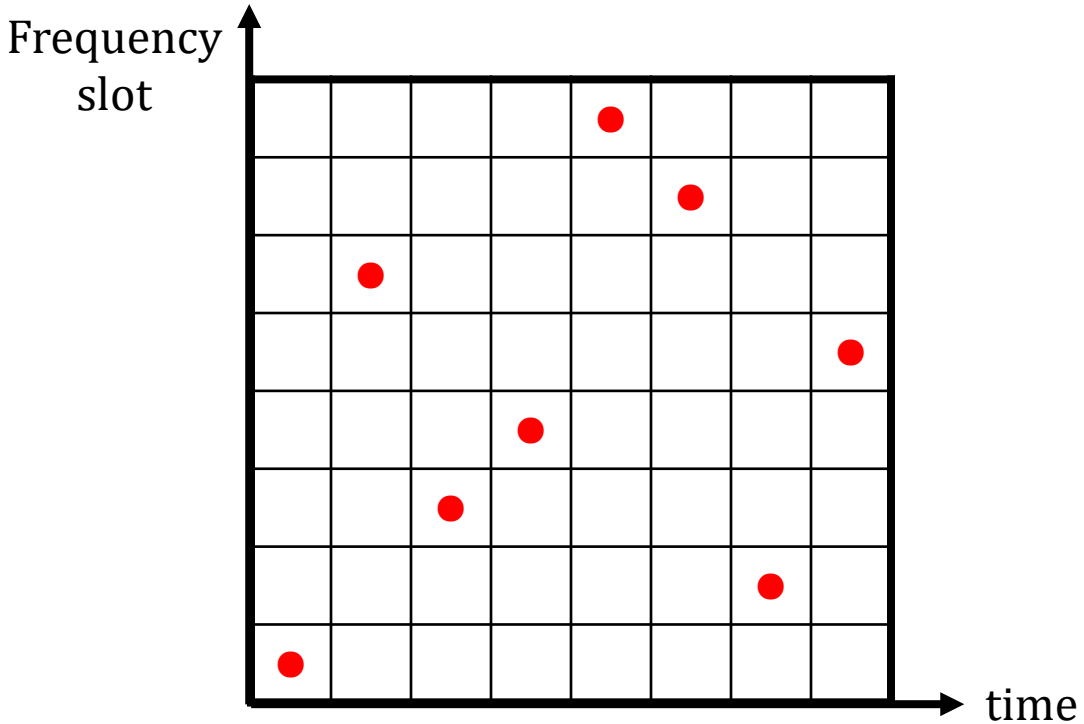
of

Sidelnikov sequences

for frequency-hopping codes

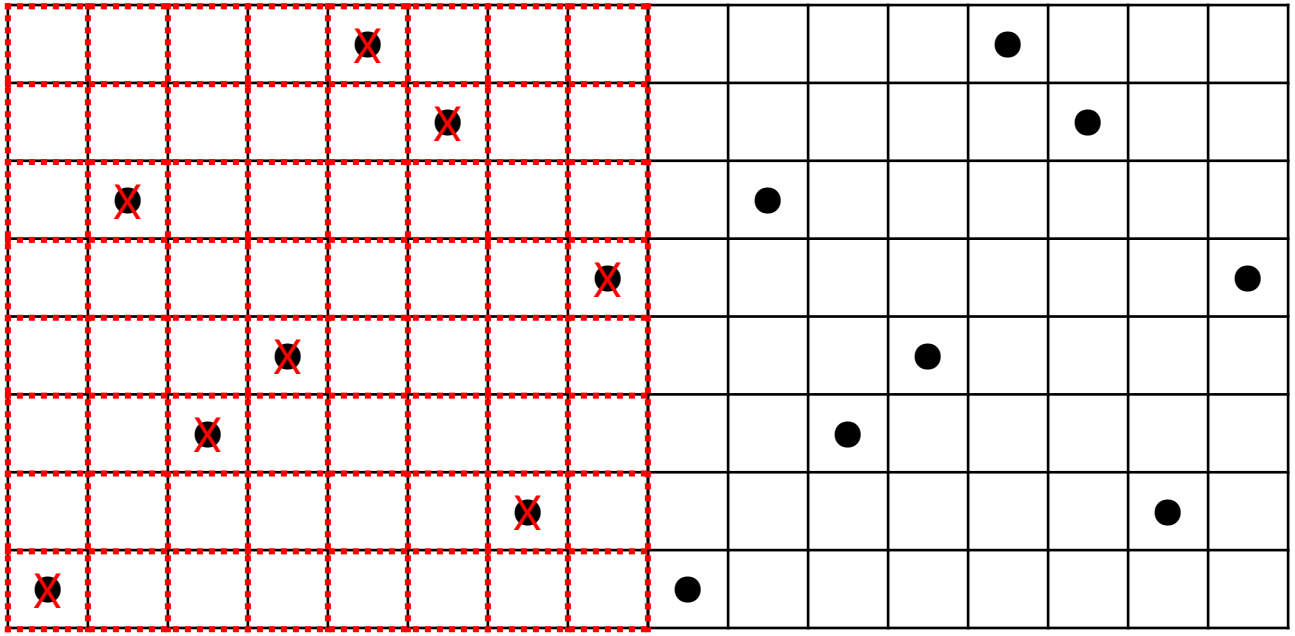
Frequency-hopping

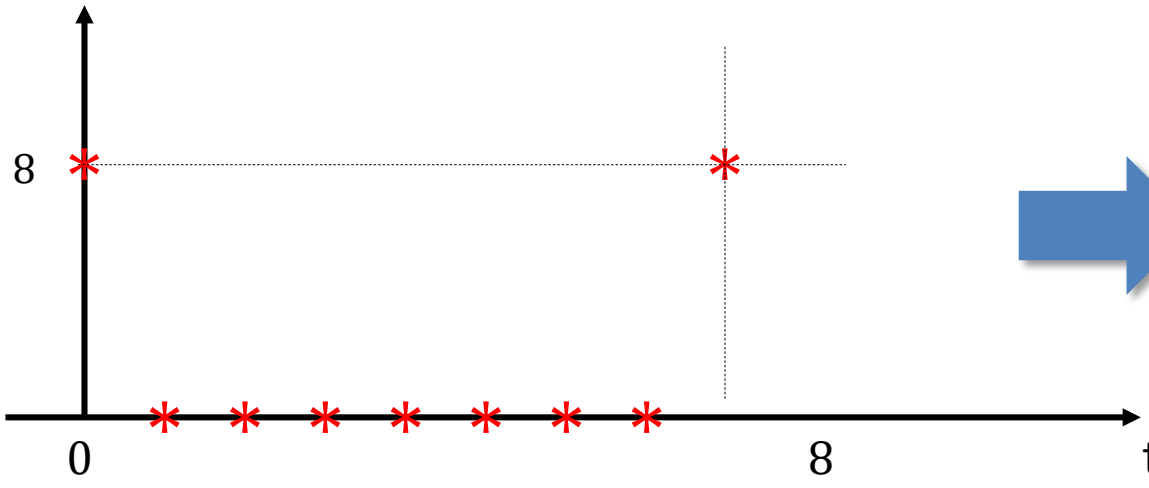
- A technique of transmitting signals for
  - covert communication
  - serving multiple users with the same resource (multiple access)
  - Radar systems



- Frequency-hopping transmission -

At the receiver…





Correlation

Correlation

- Hamming correlation is the measure of similarity between hopping sequences

(mathematical definition of hamming correlation)

Let $\boldsymbol{a} = \{a(n)\}_{n=0}^{L-1}$, $\boldsymbol{b} = \{b(n)\}_{n=0}^{L-1}$ be two sequences of period L. Then, the hamming correlation between $\boldsymbol{a}$ and $\boldsymbol{b}$ at the delay τ is given by

$$H_{\boldsymbol{a},\boldsymbol{b}}(\tau) = \sum_{t=0}^{L-1} h\big(a(t+\tau), b(t)\big),$$

where

$$h(x,y) = \begin{cases} 1, & \text{if } x = y \\ 0, & \text{otherwise.} \end{cases}$$

H_{max} = max of non-trivial hamming correlations

Relation with Coding Theory

Frequency-hopping	Coding theory
$H_{\boldsymbol{a},\boldsymbol{b}}(\tau) = \sum_{t=0}^{L-1} h\big(a(t+\tau), b(t)\big)$ where $h(x,y) = \begin{cases} 1, & \text{if } x = y \\ 0, & \text{otherwise.} \end{cases}$	$L - \mathrm{wt}(\boldsymbol{a}' - \boldsymbol{b})$ where $\boldsymbol{a}'$ is the τ-left cyclic shift of $\boldsymbol{a}$

Many of the results in **coding theory** can be applied for construction and analysis of **frequency-hopping sequences**, because, **a set E' of frequency-hopping sequences** can be obtained from **an (n=L,k) cyclic code E with large minimum distance d** by

1. **Identifying cyclic equivalence classes of E, and**
2. **Picking up one codeword from each and every class of period n=L.**

Then, **hopefully**, we have

$|E'|$ = number of cyclic equivalence classes

and

$H_{max} = L - d$

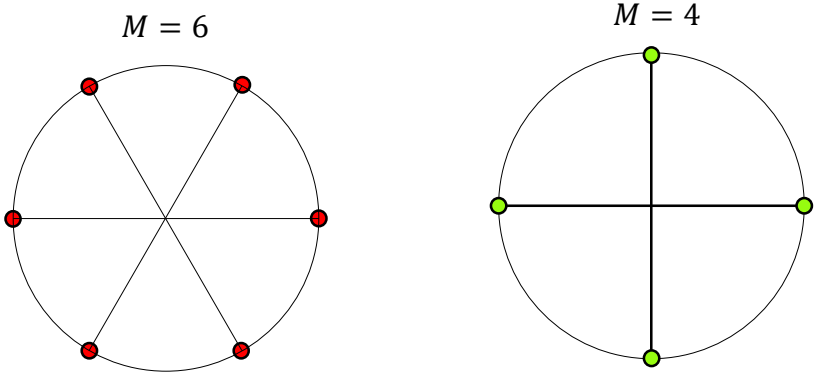
Alternative form

- The hamming correlation between $\boldsymbol{a}$ and $\boldsymbol{b}$ can also be written as

$$H_{\boldsymbol{a},\boldsymbol{b}}(\tau) = \frac{1}{M}\sum_{t=0}^{L-1}\sum_{k=0}^{M-1}\left(\omega_M^{a(t+\tau)-b(t)}\right)^k,$$

since

$$\frac{1}{M}\sum_{k=0}^{M-1}(\omega_M^x)^k = \begin{cases}1, & \text{if } x = 0\\ 0, & \text{otherwise}\end{cases} \quad = \quad h(x,0)$$



Sidelnikov sequences of period $q-1$

- Introduced by V. M. Sidelnikov in 1969.
  - q : a prime power
  - M : a divisor of $q-1$ with $M \geq 2$
  - β : a primitive element of $GF(q)$

(original definition, Sidelnikov 69)

A Sidelnikov sequence is an M-ary sequence $\boldsymbol{s} = \{s(t)\}_{t=0}^{q-2}$ of period $q-1$ defined by

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

where $D_k = \left\{\beta^{Mi+k} \mid 0 \leq i < \frac{q-1}{M}\right\}, k = 0,1,2,\ldots,M-1$

(alternative definition, Gong 10)

$$s(t) = \log_\beta(\beta^t + 1) \mod M,$$

where $\log_\beta(0) = 0$.

- Example when $q = 11, \beta = 2, M = 10$

t	β^t	$\beta^t + 1$	$s(t)$
0	1	2	**1**
1	2	3	**8**
2	4	5	**4**
3	8	9	**6**
4	5	6	**9**
5	10	0	**0**
6	9	10	**5**
7	7	8	**3**
8	3	4	**2**
9	6	7	**7**

$$\boldsymbol{s} = \{1, 8, 4, 6, 9, 0, 5, 3, 2, 7\}$$

Sidelnikov sequences of period $q^d - 1$

- Let
  - q : a prime power
  - d : a positive integer
  - M : a divisor of $q-1$ with $M \geq 2$
  - α : a primitive element of $GF(q^d)$
  - $\beta = \alpha^{\frac{q^d-1}{q-1}}$: the primitive element of $GF(q)$ fixed by α

- Then,

$$s(t) = \log_{\alpha}(\alpha^t + 1) \mod M$$

$$s(t) = \log_{\beta}\left[N_1^d(\alpha^t + 1)\right] \mod M$$

4-ary Sidelnikov sequence of period 24

$q = 5, d = 2$, and α is a primitive element of F_{25} with $\alpha^2 = 4\alpha + 3$.

Then, $\beta = \alpha^{\frac{5^2-1}{5-1}} = \alpha^6 = 2 \in F_5$ is primitive.

If $\alpha^t + 1 = \alpha^l$ then $N_1^2(\alpha^t + 1) = N(\alpha^l) = (\alpha^l)^6 = \alpha^{6l}$. Therefore, we have

t	α^t	$N_1^2(\alpha^t+1)$	$\log_\beta N_1^2(\alpha^t+1)$	t	α^t	$N_1^2(\alpha^t+1)$	$\log_\beta N_1^2(\alpha^t+1)$
0	1	$\alpha^{12} = \beta^2 = 4$	**2**	12	4	0	**0**
1	α	$\alpha^6 = \beta = 2$	**1**	13	4α	$\alpha^{12} = \beta^2 = 4$	**2**
2	$4\alpha + 3$	$\alpha^6 = \beta = 2$	**1**	14	$\alpha + 2$	$\alpha^{18} = \beta^3 = 3$	**3**
3	$4\alpha + 2$	$\alpha^{12} = \beta^2 = 4$	**2**	15	$\alpha + 3$	$\alpha^{12} = \beta^2 = 4$	**2**
4	$3\alpha + 2$	$\alpha^{18} = \beta^3 = 3$	**3**	16	$2\alpha + 3$	$\alpha^0 = \beta^0 = 1$	**0**
5	$4\alpha + 4$	$\alpha^6 = \beta = 2$	**1**	17	$\alpha + 1$	$\alpha^{12} = \beta^2 = 4$	**2**
6	2	$\alpha^{12} = \beta^2 = 4$	**2**	18	3	$\alpha^0 = \beta^0 = 1$	**0**
7	2α	$\alpha^6 = \beta = 2$	**1**	19	3α	$\alpha^0 = \beta^0 = 1$	**0**
8	$3\alpha + 1$	$\alpha^0 = \beta^0 = 1$	**0**	20	$2\alpha + 4$	$\alpha^{18} = \beta^3 = 3$	**3**
9	$3\alpha + 4$	$\alpha^{18} = \beta^3 = 3$	**3**	21	$2\alpha + 1$	$\alpha^{18} = \beta^3 = 3$	**3**
10	$\alpha + 4$	$\alpha^6 = \beta = 2$	**1**	22	$4\alpha + 1$	$\alpha^{18} = \beta^3 = 3$	**3**
11	$3\alpha + 3$	$\alpha^6 = \beta = 2$	**1**	23	$2\alpha + 2$	$\alpha^0 = \beta^0 = 1$	**0**

Some history
(frequency-hopping sequences)

Sidelnikov 69

Constructed nearly equidistance (non-linear) cyclic codes by using Sidelnikov sequences. (optimal minimum distance with respect to the Plotkin bound.)

Ding & Yin 08

Constructed a set of optimal frequency-hopping sequences by using the discrete logarithm

Han & Yang 09

Showed that **the set of hopping sequences by Ding & Yin is actually a subcode of Sidelnikov's cyclic codes.**

Hamming correlation property of sequences from 2-D array structure of a Sidelnikov sequence

Notations

- p : a prime
- q : a power of a prime p
- $GF(q^d)$: the finite field with q^d elements
- α : a primitive element over $GF(q^d)$
- $\beta = \alpha^{\frac{q^d-1}{q-1}}$: the primitive element over $GF(q)$
- M : a divisor of $q-1$ with $2 \le M \le q-1$
- d : a positive integer with $2 \le d < \max\left\{M + \frac{1}{q-1}, \frac{1}{2}\left(\sqrt{q} - \frac{2}{\sqrt{q}} + 1\right)\right\}$

- $p_l(x)$: the minimal polynomial of $-\alpha^{-l}$ over $GF(q)$
- ω_M : a complex primitive M-th root of unity
- ψ : a multiplicative character of $GF(q)$ of order M defined by

$$\psi(x) = \omega_M^{\log_\beta(x)}.$$

For simplicity, we keep $\psi(0) = 1$.

2-D Array structure

- Let $\boldsymbol{s_d}$ be a M-ary Sidelnikov sequence of period $q^d - 1$ where ***M* is a divisor of $q - 1$** with $M \geq 2$.

- Write $\boldsymbol{s_d}$ row-by-row, i.e.,

$$\begin{pmatrix} s_d(0) & s_d(1) & \cdots & s_d(\frac{q^d-1}{q-1} - 1) \\ s_d(\frac{q^d-1}{q-1}) & s_d(\frac{q^d-1}{q-1} + 1) & \cdots & s_d(2 \times \frac{q^d-1}{q-1} - 1) \\ \vdots & \vdots & \ddots & \vdots \\ s_d((q-2) \times \frac{q^d-1}{q-1}) & s_d((q-2) \times \frac{q^d-1}{q-1} + 1) & \cdots & s_d(q^d - 2) \end{pmatrix}$$

- The l-th column sequence $\boldsymbol{v_l}$ is given by

$$\boldsymbol{v_l} = \left\{ v_l(t) = s_d\left(\frac{q^d - 1}{q - 1} t + l\right) \right\}_{t=0}^{q-2}.$$

Known Properties

- Let $\hat{C}_l(d)$ be a q-cyclotomic coset **mod** $\frac{q^d-1}{q-1}$ defined by

$$\hat{C}_l(d) = \{l, lq, \dots, lq^{m_l-1}\}$$

where m_l is the cardinality of $\hat{C}_l(d)$.

- Let $\boldsymbol{v_l}$ be the l-th column of the array. Then,
  1. $v_0(t) \equiv d \log_\beta(\beta^t + 1) \pmod{M}$.
  2. If $l_2 \in \hat{C}_{l_1}$, then $\boldsymbol{v_{l_2}}$ is a cyclic shift of $\boldsymbol{v_{l_1}}$.
  3. If $m_l = d$, then $\boldsymbol{v_l}$ is of period $q-1$ for any M.

Known Properties (cont')

- Let $\Lambda'(d)$ be the set of smallest non-zero representatives of all the $\hat{C}_l(d)$s such that $m_l = d$.

- For $l \in \Lambda'(d)$,

$$\boldsymbol{v_l} = \left\{ \boldsymbol{v_l(t) \equiv log_\beta \left(\beta^l p_l(\beta^t) \right) \mod M} \right\}_{t=0}^{q-2}$$

where $p_l(x)$ is the minimal polynomial of $-\alpha^{-l}$ over $GF(q)$.

- For $l, k \in \Lambda'(d)$, let $p_l(x)$, $p_k(x)$ be two minimal polynomials over $GF(q)$ of $-\alpha^{-l}$ and $-\alpha^{-k}$, respectively. Then, $\beta^{-\tau d} p_l(\beta^\tau x)$ and $p_k(x)$ are distinct monic irreducible polynomials over $GF(q)$, unless $l = k$ and $\tau = 0$.

Known Properties (cont')

- Let $l_1, l_2 \in \Lambda'(d)$. Then,

$$\left| \sum_{t=0}^{L-1} \omega_M^{v_{l_1}(t+\tau) - v_{l_2}(t)} \right| \leq (2d-1)\sqrt{q} + 1,$$

except for $l_1 = l_2$ and $\tau = 0$.

Hamming correlation of columns

(Definition)

For $d \geq 2$, let $\Gamma(d)$ be the set of column sequences of the $(q-1) \times \frac{q^d-1}{q-1}$ array of M-ary Sidelnikov sequence of period $q^d - 1$ given by

$$\Gamma(d) = \{v_l(t) | l \in \Lambda'(d)\}.$$

(Theorem)

The maximum non-trivial hamming correlation of $\Gamma(d)$, denoted by $H_{\max}(\Gamma(d))$, is

$$H_{\max}(\Gamma(d)) \leq \min\left\{\frac{(q-1)d}{M} - 1, \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q}+1]\right\}.$$

※Note: When $M = q-1$, $H_{\max}(\Gamma(d)) \leq d-1$

when $d = 2$

- Let $q = 7$, $M = 6$. Then, the array is given by

0	1	2	3	4	5	6	7
4	1	5	0	5	1	5	1
2	4	4	2	2	2	5	4
2	4	3	3	1	0	4	4
0	5	0	3	5	2	3	5
4	1	3	1	2	3	0	1
0	0	5	2	1	3	3	0

$$\Lambda'(2) = \{1, 2, 3\}$$

$$\Gamma'(2) = \{s_1, s_2, s_3\}$$

$$s_1 = \{1, 4, 4, 5, 1, 0\}$$

$$s_2 = \{5, 4, 3, 0, 3, 5\}$$

$$s_3 = \{0, 2, 3, 3, 1, 2\}$$

Pairwise maximum non-trivial hamming correlation

	$M = 6$	$M = 3$
$\max H_{s_1,s_2}$	**1**	**3**
$\max H_{s_1,s_2}$	**1**	**3**
$\max H_{s_1,s_2}$	**1**	**3**
(The bound) $\min\left\{\frac{(q-1)d}{M} - 1, \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q}+1]\right\}$	**1**	**3**

Proof of the bound

Assume that $l_1 \neq l_2$ or $\tau \neq 0$.

We first claim that

$$H_{\max}\big(\Gamma(d)\big) \leq \frac{(q-1)d}{M} - 1.$$

Observe that

$$H_{v_{l_1}, v_{l_2}}(\tau) = \frac{1}{M}\sum_{t=0}^{q-1}\sum_{k=0}^{M-1}\left[\omega_M^{v_{l_1}(t+\tau)-v_{l_2}(t)}\right]^k$$

..... the alternative form

$$\omega_M^{k\, v_l(t)} = \psi^k\left(\beta^l p_l(\beta^t)\right)$$

$$= \frac{1}{M}\sum_{t=0}^{q-1}\sum_{k=0}^{M-1}\psi^k\left(\beta^{l_1-l_2}p_{l_1}(\beta^{t+\tau})p_{l_2}(\beta^t)^{-1}\right)$$

$$= \sum_{t=0}^{q-1}\frac{1}{M}\sum_{k=0}^{M-1}\psi^k\left(\beta^{l_1-l_2}p_{l_1}(\beta^{t+\tau})p_{l_2}(\beta^t)^{-1}\right)$$

Focus on this part

$$\frac{1}{M}\sum_{k=0}^{M-1}\psi^k\left(\beta^{l_1-l_2}p_{l_1}(\beta^{t+\tau})p_{l_2}(\beta^t)^{-1}\right)$$

1. Observe that

$$\frac{1}{M}\sum_{k=0}^{M-1}\psi^k(x)=\begin{cases}1, & \text{if } x=0\\ 1, & \text{if } x=(\beta^M)^e \text{ for some } e\in\left\{0,1,\dots,\frac{q-1}{M}-1\right\}\\ 0, & \text{otherwise}\end{cases}.$$

2. Since $p_{l_1}(x)$ and $p_{l_2}(x)$ are minimal polynomials of degree $d\geq 2$,
$$\beta^{l_1-l_2}p_{l_1}(\beta^{t+\tau})p_{l_2}(\beta^t)^{-1}=0$$
is impossible from any t.

3. Therefore,
$$\frac{1}{M}\sum_{k=0}^{M-1}\psi^k(x)=1$$
when $\beta^{l_1-l_2}p_{l_1}(\beta^{t+\tau})p_{l_2}(\beta^t)^{-1}=\beta^{eM}$ for some integer e.

$$\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau}) p_{l_2}(\beta^t)^{-1} = \beta^{eM}$$

$$\Leftrightarrow \left[\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau}) p_{l_2}(\beta^t)^{-1}\right]^{\frac{q-1}{M}} = 1$$

$$\Leftrightarrow \underbrace{\left[\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau})\right]^{\frac{q-1}{M}} - \left[p_{l_2}(\beta^t)\right]^{\frac{q-1}{M}}}_{\triangleq f(x)} = 0$$

Then, the calculation becomes simple!

$$H_{v_{l_1}, v_{l_2}}(\tau) = \sum_{t=0}^{q-1} \frac{1}{M} \sum_{k=0}^{M-1} \psi^k\left(\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau}) p_{l_2}(\beta^t)^{-1}\right)$$

$$= \#\text{ of roots of } f(x) \text{ in } GF(q)^*.$$

$$H_{v_{l_1}, v_{l_2}}(\tau) = \#\text{ of roots of } f(x) \text{ in } GF(q)^*.$$

$$\text{where } f(x) = \left[\beta^{l_1 - l_2} p_{l_1}(\beta^{t+\tau})\right]^{\frac{q-1}{M}} - \left[p_{l_2}(\beta^t)\right]^{\frac{q-1}{M}}$$

- For any $l_1, l_2 \in \Lambda'(d)$, and τ except for $l_1 = l_2$ and $\tau = 0$, $f(x)$ is a non-zero polynomial and

$$\deg f(x) \leq \frac{q-1}{M} d,$$

Since, in that case, $\beta^{-\tau d} p_{l_1}(\beta^{\tau} x)$ and $p_{l_1}(\beta^t)$ are two distinct monic irreducible polynomials of degree d over $GF(q)$.

- Since f(x) has no constant term, we have

$$H_{\max}\big(\Gamma(d)\big) \leq \frac{(q-1)d}{M} - 1.$$

Second claim:

$$H_{\max}\big(\Gamma(d)\big) \le \frac{q-1}{M} + \frac{M-1}{M}\left[(2d-1)\sqrt{q}+1\right]$$

is easily obtained as follows:

$$H_{v_{l_1}, v_{l_2}}(\tau) = \frac{1}{M}\sum_{t=0}^{q-1}\sum_{k=0}^{M-1}\left[\omega_M^{v_{l_1}(t+\tau)-v_{l_2}(t)}\right]^k$$

$$= \frac{q-1}{M} + \frac{1}{M}\sum_{t=0}^{q-1}\sum_{k=1}^{M-1}\left[\omega_M^{v_{l_1}(t+\tau)-v_{l_2}(t)}\right]^k$$

$$\le \frac{q-1}{M} + \frac{1}{M}\sum_{k=1}^{M-1}\left|\sum_{t=0}^{q-1}\left[\omega_M^{v_{l_1}(t+\tau)-v_{l_2}(t)}\right]^k\right|$$

triangular inequality

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

$$\left|\sum_{t=0}^{L-1}\omega_M^{v_{l_1}(t+\tau)-v_{l_2}(t)}\right| \le (2d-1)\sqrt{q}+1$$

$$H_{\max}(\Gamma(\mathbf{d})) \le \min\left\{\frac{(q-1)d}{M} - 1,\ \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q}+1]\right\}$$

Upper-Bound on Maximum nontrivial Hamming correlation ($q = 101, \boldsymbol{d = 2}$)

M	$H_1 = \frac{q-1}{M}d - 1$	$H_2 = \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q}+1]$	$\min(H_1, H_2)$
100	1	31	1
50	3	32	3
25	7	33	7
20	9	34	9
10	19	38	19
5	39	44	39
4	49	48	48
2	99	65	65

H_1 ↑ (M = 100, 50, 25, 20, 10, 5)

H_2 ↓ (M = 4, 2)

$\frac{\sqrt{q}}{2}$??

The bound and true maximum

	$d = 2, \lvert\Gamma(d)\rvert = 50$			$d = 3, \lvert\Gamma(d)\rvert = 3434$		
M	$H_{a,max}$	$H_{c,max}$	bound	$H_{a,max}$	$H_{c,max}$	bound
100	1	1	1	2	2	2
50	3	3	3	5	5	5
25	7	7	7	11	11	11
20	9	9	9	14	14	14
10	18	19	19	25	25	29
5	32	33	39	38	39	59
4	36	37	48	46	46	63
2	58	59	65	68	69	75

The region where true maximum meets the bound

Is that good?

- To determine whether the proposed set of frequency-hopping sequence is good or not, we will use the Singleton bound.

(Signleton bound for sets of frequncy-hopping sequence)
Let K be a set of N frequency-hopping sequences of length L over the integers modulo M. Then,

$$H_{\max}(K) \geq \lceil \log_M(NL) - 1 \rceil$$

It directly comes from the singleton bound for (non-linear) codes

$$N \leq M^{n-d+1}$$

The Size of $\Gamma(d)$

- To apply the Singleton bound, we need knowledge about the size of $\Gamma(d)$. For $d = 2$, the exact size is already known by Yu & Gong as

$$|\Gamma(d)| = |\Lambda'(d)| = \left\lfloor \frac{q}{2} \right\rfloor.$$

(Lemma, the size of $\Gamma(d)$)

For $3 \leq d < M$,

$$|\Gamma(d)| = |\Lambda'(d)| \geq \frac{q^{d-1}}{d}.$$

Proof of the Size of $\Gamma(d)$

We can write

$$|\Lambda'(d)| = \frac{1}{d}\left(\frac{q^d - 1}{q-1} - k - 1\right),$$

Where

$$k = \sum_{\substack{r|d \\ r\neq 1, r\neq d}} \left|\left\{ l \,\middle|\, 1 \le l < \frac{q^d-1}{q-1}, m_l = r \right\}\right|.$$

Following is a condition on m_l and it is useful:

(Kim, Kim, Song 15)

For a fixed $l \in \{1,\ 2, \dots,\ \frac{q^d-1}{q-1} - 1\}$, m_l is the least positive integer which satisfies

$$\frac{q^d - 1}{(q^{m_l} - 1)\gcd\left(\frac{d}{m_l}, q-1\right)} \,\middle|\, l.$$

There are

$$\frac{(q^r-1)\gcd\left(\frac{d}{r},q-1\right)}{q-1}$$

elements in $\Lambda'(d)$ which can be divided by

$$\frac{q^d-1}{(q^r-1)\gcd\left(\frac{d}{r},q-1\right)},$$

where $2 \le r \le d$.

Therefore,

$$k < \sum_{\substack{r|d \\ r\neq 1, r\neq \mathrm{d}}} \frac{(q^r-1)\gcd\left(\frac{d}{r},q-1\right)}{q-1}.$$

Denote the greatest proper positive divisor of d by δ. Then,

$$\delta \leq \left\lfloor \frac{d}{2} \right\rfloor.$$

Observe that

$$k \leq \sum_{\substack{r|d \\ r\neq 1, r\neq \mathrm{d}}} \frac{(q^r-1)\gcd\left(\frac{d}{r}, q-1\right)}{q-1}$$

$$\leq \sum_{r=2}^{\left\lfloor \frac{d}{2} \right\rfloor} \frac{(q^r-1)\gcd\left(\frac{d}{r}, q-1\right)}{q-1}$$

$$\leq \sum_{r=2}^{\left\lfloor \frac{d}{2} \right\rfloor} \frac{q^{r+1}}{q-1} = \frac{q^{\left\lfloor \frac{d}{2} \right\rfloor+1}-q^3}{q-1} < \frac{q^{\left\lfloor \frac{d}{2} \right\rfloor+1}-1}{q-1} - 1$$

Therefore,

$$|\Lambda'(d)| = \frac{1}{d}\left(\frac{q^d - 1}{q - 1} - k - 1\right)$$

$$> \frac{1}{d}\left(\frac{q^d - 1}{q - 1} - \frac{q^{\lfloor d/2 \rfloor + 1} - 1}{q - 1}\right)$$

$$> \frac{1}{d}\left[q^{d-1} + \sum_{y=0}^{d-2} q^y - \sum_{z=0}^{\lfloor d/2 \rfloor} q^z\right]$$

$$> \frac{1}{d}[q^{d-1}]$$

Since

$$\sum_{y=0}^{d-2} q^y - \sum_{z=0}^{\left\lfloor \frac{d}{2} \right\rfloor} q^z \geq 0$$

when $d \geq 3$.

Optimality of the set

(Theorem, optimality of the proposed set of frequency hopping sequences)
Let $M = q - 1$ and $2 \leq d \leq q - 1$. Then, the frequency hopping sequence family $\Gamma(d)$ is **optimal with respect to the Singleton bound for sets of frequency-hopping sequences**.

Proof)
For $d = 2$,

$$H_{\max}(\Gamma(2)) \geq \left\lceil \log_{q-1} \left\lfloor \frac{q}{2} \right\rfloor (q-1) - 1 \right\rceil$$
$$\geq \left\lceil 2 \log_{q-1}(q-1) - \log_{q-1} 2 - 1 \right\rceil = 1.$$

For $d \geq 3$,

$$H_{max}(\Gamma(d)) \geq \left\lceil \log_{q-1} \frac{(q-1)q^{d-1}}{d} - 1 \right\rceil$$
$$\geq \left\lceil d - 1 - \log_{q-1} d \right\rceil = d - 1.$$

Relation with Reed's k-th order near orthogonal code

- In 1971, Reed proposed a set of frequency-hopping sequences by using q-ary Reed-Solomon (RS) code of length $q-1$.
  - In 1993, Song gave a way to construct $\boldsymbol{k}$-th order near orthogonal codes in which all the sequences are of period $q-1$.

Note that

$\{\beta^l p_l(\beta^t)\}_{t=0}^{q-2}$: a q-ary RS codeword which has no zero term.

↓ **Applying $\log_\beta(\cdot)$.**

$\boldsymbol{v_l} = \left\{v_l(t) \equiv \log_\beta\left(\beta^l p_l(\beta^t)\right) \mod q-1\right\}_{t=0}^{q-2}$: a $(q-1)$-ary column sequence.

The hamming distance among such codewords **remains the same even though** we apply **the discrete logarithm,**
because each codeword has no zero term.
Obviously, **their hamming correlation also remains the same.**

(Corollary)

If $M = q - 1$, then a sequence $\boldsymbol{v_l} \in \Gamma(2)$ has one of the following Hamming auto-correlation profiles:

1) If q is even, then

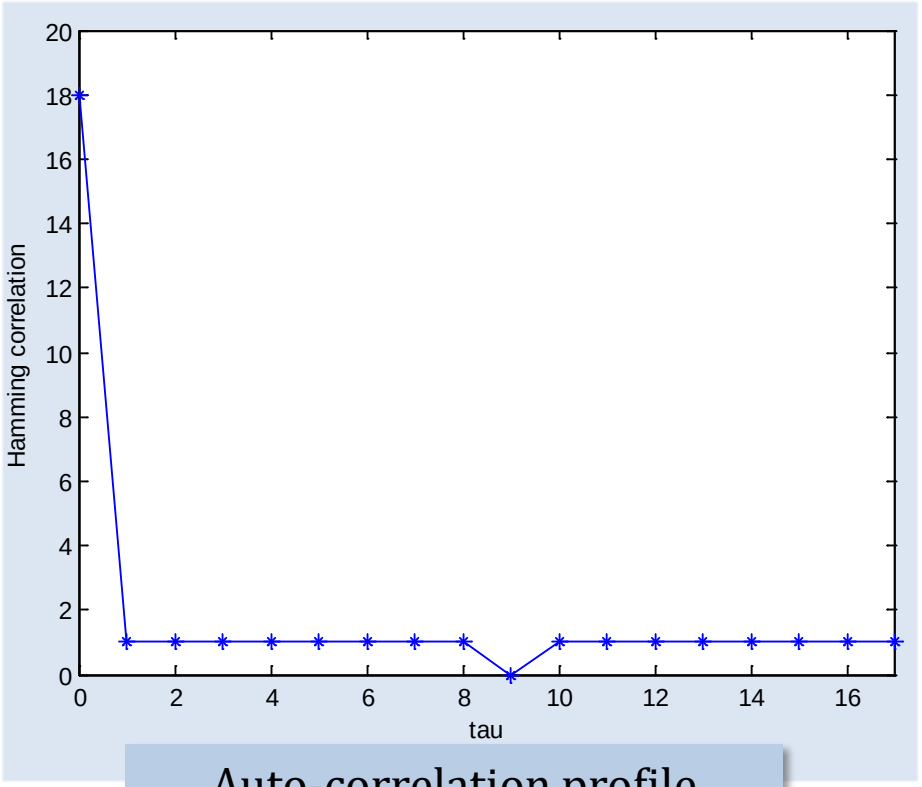
$$H_l(\tau) = \begin{cases} q-1, & \text{if } \tau = 0 \\ 1, & \text{otherwise.} \end{cases}$$

2) If q is odd, then

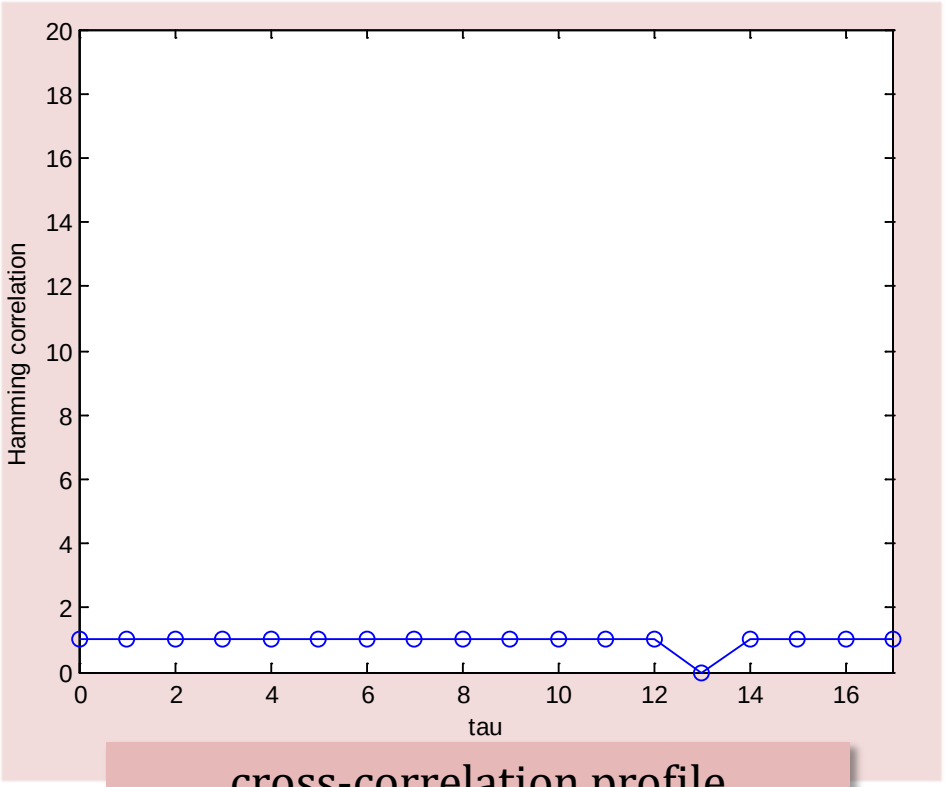
$$H_l(\tau) = \begin{cases} q-1, & \text{if } \tau = 0 \\ 0, & \text{if } \tau = \dfrac{q-1}{2} \\ 1, & \text{otherwise.} \end{cases}$$

Example: correlation profile

$q = 19, d = 2, M = q - 1 = 18$



Auto-correlation profile



cross-correlation profile

A extention – constant addition

(definition)

For $2 \le d \le q-2$, let $\Delta(d)$ be a set of M-ary frequency-hopping sequences such that

$$\Delta(d) = \{\boldsymbol{v_l} + \boldsymbol{c} | \boldsymbol{v_l} \in \Gamma(d), 0 \le c < M\},$$

where $M \ge 2$ is a positive divisor of $q-1$.

(theorem)

For the set $\Delta(d)$,

$$H_{\max}\big(\Delta(d)\big) \le \min\left\{\frac{(q-1)d}{M}, \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q}+1]\right\},$$

and $|\Delta(d)| \ge M\frac{q^{d-1}}{d}$.

When $M = q-1$, $\Delta(d)$ is also optimal with respect to the Singleton bound for sets of frequency-hopping sequences.

Especially, when $M = q-1$,

$$H_{\max}\big(\Delta(d)\big) \le d.$$

Comparison with previous results

	length	Alphabet size	$H_{\max}$	Set size
Sidelnikov '69	$q-1$	M $M \mid q-1$ q or $\frac{q-1}{M}$ is even	$\frac{q-1}{M}+1$	$2M$
Lempel & Greenberger '74	p^r-1	p^u $(0<u\le r)$	$p^{r-u}-1$	p^u
Song, Reed and Golomb '93	$q-1$	q	$k \le B(q)$ $B(q)$ is determined by $q-1$	$\frac{1}{n}\sum_{d\mid n}\mu(d)q^{1+\lfloor\frac{k}{d}\rfloor}$ $(n=q-1)$
Ding '08 (Yang '09)	$q-1$	M $(M \mid q-1)$	$\frac{q-1}{M}$ (if q or $(q-1)$ is even) $\frac{q-1}{M}+1$ (if q and $(q-1)$ is odd)	M
$\Gamma(d)$ in this talk	$q-1$	M $(M \mid q-1)$	$\min\{\frac{q-1}{M}d-1, 1\frac{q-1}{M}+\frac{M-1}{M}\alpha\}$	$\geq \boldsymbol{q^{d-1}/d}$
$\Delta(d)$ in this talk	$q-1$	M $(M \mid q-1)$	$\min\{\frac{q-1}{M}d, \quad 1\frac{q-1}{M}+\frac{M-1}{M}\alpha\}$	$\geq \boldsymbol{M\frac{q^{d-1}}{d}}$

p : prime, q : prime power

$\alpha = [(2d-1)\sqrt{q}+1]$

Conclusion

- From the array structure of Sidelnikov sequences,
  - we define a new set of frequency-hopping sequences, and
  - analyze their hamming correlation properties.

- When $M = q - 1$, the proposed set is optimal with respect to the Singleton bound for sets of frequency hopping sequences.

- Optimality of the proposed set seems to be highly related to maximum distance separable (MDS) property of RS codes.

- The method which combines all the set of column sequences from Sidelnikov sequences of period $q^2 - 1, q^3 - 1, \ldots, q^h - 1$ can also be applied.