Constructions for favorable sequences family using Sidelnikov sequences

100000010000001100001010001111001000101100111010100111110100001110001001001101101011011110110001101001011101110011001010101111111

ITA 2014

Feb. 10-14

Hong-Yeop Song
Yonsei University
Seoul, Korea

Dae San Kim
Sogang University
Seoul, Korea

Motivation

- Synchronization, Distinguishing users, Interference minimization, Higher resolution RADAR,…
- 1969 – Sidelnikov (autocorrelation property only)
- 2007~Present – Sequence families from Sidelnikov sequences
- **Purpose**
  - Sequence families with larger size
  - Sequence families with lower correlation magnitude

Brief History and Main Contribution

(SONG-07) Sequence family constructions from Sidelnikov sequences have been considered, **by using constant multiples**

(NO-08, YANG-09) Family size increased **by additionally using shift-and-adds**

(GONG-10) **2-D array** structure of size $(q-1) \times \left(\frac{q^2-1}{q-1}\right)$

(KIM-10) 2-D array structure of size $(q-1) \times \left(\frac{q^d-1}{q-1}\right)$ with $(d, q-1) = 1$

(This paper) **2-D array structure of size $(\mathbf{q}-\mathbf{1}) \times \left(\frac{\mathbf{q}^{\mathbf{d}}-\mathbf{1}}{\mathbf{q}-\mathbf{1}}\right)$**

without $(\mathbf{d}, \mathbf{q}-\mathbf{1}) = \mathbf{1}$

maintaining the family size "comparable" to the above

and the correlation bound the same as the above

Notation

- p : prime
- $q = p^n$:   prime power or prime
- $GF(q)$: finite field of order q
- $GF(q^d)$: finite field of order q^d with $2 \le d < (\sqrt{q} - \frac{2}{\sqrt{q}} + 1)/2$
- α : arbitrary but fixed primitive element of $GF(q^d)$
- $\beta = \alpha^{(q^d-1)/(q-1)}$: the primitive element of $GF(q)$
- ω_M : complex M^{th} root of unity, where $M|q-1$
- ψ : the **multiplicative character of order M** from $GF(q)$, defined by

$$\psi(x) = \exp(\frac{2\pi i}{M} \log_\beta x) = \omega_M^{\log_\beta x}$$

and

$$\psi(0) = 1.$$

Sidelnikov Sequences of period q-1

- $GF(q)$ = finite field of size q where $q = p^n$
- β = primitive element of $GF(q)$
- M = a divisor of $q - 1$
- **Coset Partition**
  - ✓ D_0 : the set of M-th powers in $GF(q)^*$
  - ✓ $D_k = \beta^k \cdot D_0$ for $0 \leq k \leq M-1$

- **An M-ary Sidelnikov sequence of period $q - 1$** is defined as, **for t = 0, 1, 2,…, q-2,**

Sidelnikov-69

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

(Example) $p = q = 13$, $\mathbf{M = 3}$, $\beta = 2$

- $D_0 = 2^0 \cdot D_0$ = {**1,5,8,12**} = cubic residues mod 13
- $D_1 = 2^1 \cdot D_0$ = {**2,10,3,11**}
- $D_2 = 2^2 \cdot D_0$ = {**4,7,6,9**}

t	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
$\beta^t = 2^t$	1	2	4	8	3	6	**12**	11	9	5	10	7
$\beta^t + 1$	2	3	5	9	4	7	**0**	12	10	6	11	8
belongs to	D_1	D_1					**?**		D_1		D_1	
S(t)	**1**	**1**	**0**	**2**	**2**	**2**	**0**	**0**	**1**	**2**	**1**	**0**

$$\mathbf{s(t) \equiv \log_{\beta}(\beta^{t} + 1) \pmod{12}}$$

Is this ADDONE table of the finite field GF(13)?

t	β^t	$\beta^t + 1$	$\log_\beta(\beta^t + 1)$ (mod 12)	(mod 3)
*	0	1	0	0
0	1	2	1	1
1	$\beta = 2$	3	4	1
2	$\beta^2 = 4$	5	9	0
3	$\beta^3 = 8$	9	8	2
4	$\beta^4 = 16 = 3$	4	2	2
5	$\beta^5 = 6$	7	11	2
6	$\beta^6 = 12$	0		
7	11	12	6	0
8	9	10	10	1
9	5	6	5	2
10	10	11	7	0
11	7	8	3	0

Sidelnikov Sequences (alternative definition)

The M-ary Sidelnikov sequence $s(t)$ of period $q-1$ is defined by, for $0 \le t \le q-2$,

$$s(t) \equiv \log_{\beta}(\beta^{t} + 1) \quad \mathbf{mod}\, \mathrm{M},$$

where we assume that $\log_{\beta}(0) = 0$.

2-D array structure of size $(q-1) \times \left(\frac{q^2-1}{q-1}\right)$

Gong-10

Write a **Sidelnikov sequence of period** $\mathbf{q^2-1}$ as an array of size $(q-1) \times (q+1)$.

1) the first column sequence is always a **constant-multiple** of a **Sidelnikov sequence of period** $\mathbf{q-1}$.
2) other column sequences of period $\mathbf{q-1}$ (not necessarily Sidelnikov sequences) have GOOD correlations
   - NOT ONLY with each other
   - BUT ALSO with previously constructed family members of period $\mathbf{q-1}$

if they are not cyclically equivalent to each other.

→ **Nontrivial increase in the family size**

Theorem (Gong-10)

Let $\mathcal{U}$ be the set of sequences of period $q-1$ given as follows:

$$\mathcal{U} = \{cs(t) | 1 \le c \le M-1\}$$
$$\cup \left\{c_0 s(t) + c_1 s(t+l_1) \middle| 1 \le l_1 \le \left\lfloor \frac{q-1}{2} \right\rfloor \right\}$$
$$\cup \left\{c_2 v_{l_2}(t) \middle| 1 \le l_2 \le \left\lfloor \frac{q}{2} \right\rfloor \right\}.$$

Then,

① The maximum correlation of $\mathcal{U}$ is upper bounded by $3\sqrt{q}+5$.

② This family have size $\frac{M(M-1)(q-2)}{2} + M - 1$.

If $v_l(t)$ is the column sequence of the (q-1) x (q+1) array of a Sidelnikov sequence of period $\mathbf{q^2-1}$ given by

$$\log_\alpha(\alpha^t + 1) \mod M,$$

Then $s(t)$ must be the Sidelnikov sequence of period $\mathbf{q-1}$ given by

$$\log_\beta(\beta^t + 1) \mod M \quad \textbf{where } \boldsymbol{\beta = \alpha^{(q^2-1)/(q-1)} = \alpha^{q+1}}.$$

Kim's Generalization

D.S. Kim, 2010: 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 [cs.IT]

- Why not considering a sidelnikov sequence of period $q^3 - 1,\ q^4 - 1$ or $q^d - 1$ in general in the first place and then using **an array of size** $\mathbf{(q-1)} \times (\frac{\mathbf{q^d-1}}{\mathbf{q-1}})$?

Key Observation – Theorem and remark

- To analyze the column sequences of the array, one has to represent **the Sidelnikov sequence of period $q^d - 1$** using a **primitive element of** GF(q).
- THEOREM:

  Let α be a primitive element of GF(q^d).

  $\beta = \alpha^{(q^d-1)/(q-1)}$: the primitive element of $\mathrm{GF}(q)$

  For period $q^d - 1$, we have

  $$s(t) \equiv \log_\beta N(\alpha^t + 1) \mod M.$$

- REMARK: when $d = 2$, it becomes that

$$N(\alpha^t + 1) = (\alpha^t + 1)^{\frac{q^2-1}{q-1}} = (\alpha^t + 1)^{q+1} = (\alpha^t + 1)^q(\alpha^t + 1)$$
$$= \alpha^{(q+1)t} + \alpha^{qt} + \alpha^t + 1 = \beta^t + 1 + \mathrm{Tr}(\alpha^t)$$

Key Observation - proof

- Let α be a primitive element of GF(q^d).
- For period $q^d - 1$, denote $y(t) \equiv \log_\alpha(\alpha^t + 1) \bmod q^d - 1$.
- Assume that $N(\alpha^t + 1) \neq 0$. Then $N(\alpha^t + 1) = \beta^{x(t)}$.
- This gives:

$$\frac{q^d-1}{q-1} y(t) \equiv \frac{q^d-1}{q-1} \log_\alpha(\alpha^t + 1) \equiv \log_\alpha(\alpha^t + 1)^{\frac{q^d-1}{q-1}}$$

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

$$\equiv \frac{q^d-1}{q-1} x(t) \quad \bmod q^d - 1$$

- Since $\left(\frac{q^d-1}{q-1}, q^d - 1\right) = \frac{q^d-1}{q-1}$, we have:

$x(t) \equiv y(t) \equiv \log_\beta N(\alpha^t + 1) \bmod q - 1$ (and hence, mod M).

Columns of the Array Structure

Kim-10

Let $d \geq 2$, and write a Sidelnikov sequence of period $q^d - 1$ as an array of size $(q-1) \times (\frac{q^d-1}{q-1})$. Then, the column sequences $v_l(t)$ of the array can be represented as

$$\mathbf{v}_{\boldsymbol{l}}(\mathbf{t}) \equiv \mathbf{log}_{\boldsymbol{\beta}}\, \mathbf{f}_{\boldsymbol{l}}(\boldsymbol{\beta}^{\mathbf{t}}) \quad \textbf{(mod M)}$$

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

- Proof:

$$v_l(t) \equiv s\left(\frac{q^d - 1}{q - 1} t + l\right) \equiv \log_\beta N(\alpha^{\frac{q^d-1}{q-1}t+l} + 1) \equiv \log_\beta N(\alpha^l \beta^t + 1)$$

YONSEI UNIVERSITY

Cyclic Equivalence of Columns

Kim-10

Let $\mathrm{d} \geq 2$, and write a Sidelnikov sequence of period $\mathrm{q}^{\mathrm{d}} - 1$ as an array of size $(\mathrm{q}-1) \times (\frac{\mathrm{q}^{\mathrm{d}}-1}{\mathrm{q}-1})$. The column sequences are denoted by $\mathrm{v}_{l}(\mathrm{t})$ for $l = 0,1,2, \ldots, \frac{\mathrm{q}^{\mathrm{d}}-1}{\mathrm{q}-1} - 1$.

Then,

(1) For $l = 0$, $\mathrm{v}_0(\mathrm{t}) \equiv \mathrm{d} \log_{\beta}(\beta^{\mathrm{t}} + 1) \mod \mathrm{M}$

(2) For $l \neq 0$, $\mathrm{v}_{l}(\mathrm{t}) \equiv \mathrm{v}_{lq}(\mathrm{t}) \mod \mathrm{M}$

where lq is computed mod $\frac{\mathrm{q}^{\mathrm{d}}-1}{\mathrm{q}-1}$

Family of Column Sequences

Kim-10

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

Construct a family

$$\Sigma = \{\, c v_l(t) \mid \ 1 \le c < M \text{ and } \ l \ \in \Lambda \backslash \{0\} \ \}$$

where Λ is the set of all the representatives

of q-cyclotomic cosets mod $\frac{q^d - 1}{q - 1}$.

Then

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

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

Importance of $\gcd(d, q-1)$

q	$\gcd(q-1,3)$	$\gcd(q-1,4)$	q	$\gcd(q-1,3)$	$\gcd(q-1,4)$
31	3	X	61	3	4
37	3	X	64	3	1
41	1	X	67	3	2
43	3	X	71	1	2
47	1	X	73	3	4
49	3	X	79	3	2
53	1	4	81	1	4
59	1	2	83	1	2

Can we remove the condition (d,q-1)=1 ?

- q-cyclotomic coset mod $q^d - 1$ ⇨ Natural
- q-cyclotomic coset mod $\frac{q^d-1}{q-1}$ ⇨ Define $\Lambda\backslash\{0\}$ Kim-10
- q-cyclotomic coset mod $\frac{q^d-1}{q-1}$ **with full size d** ⇨ Define $\Lambda'\backslash\{0\}$
  Key Idea
- Example ($q = 7, \ \ d = 2$)
  - 7-cyclotomic coset mod 48
    - ✓ There exists 23 cosets of size 2 except {0}, {7}
  - 7-cyclotomic coset mod 8
    - ✓ {0}, {1,7}, {2,6}, {3,5}, {4} ⇨ $\Lambda\backslash\{0\} = \{1,2,3,4\}$
  - 7-cyclotomic coset mod 8 of size $d(= 2)$
    - ✓ {1,7}, {2,6}, {3,5} ⇨ $\Lambda'\backslash\{0\} = \{1,2,3\}$

MAIN THEOREM

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

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

are cyclically inequivalent.

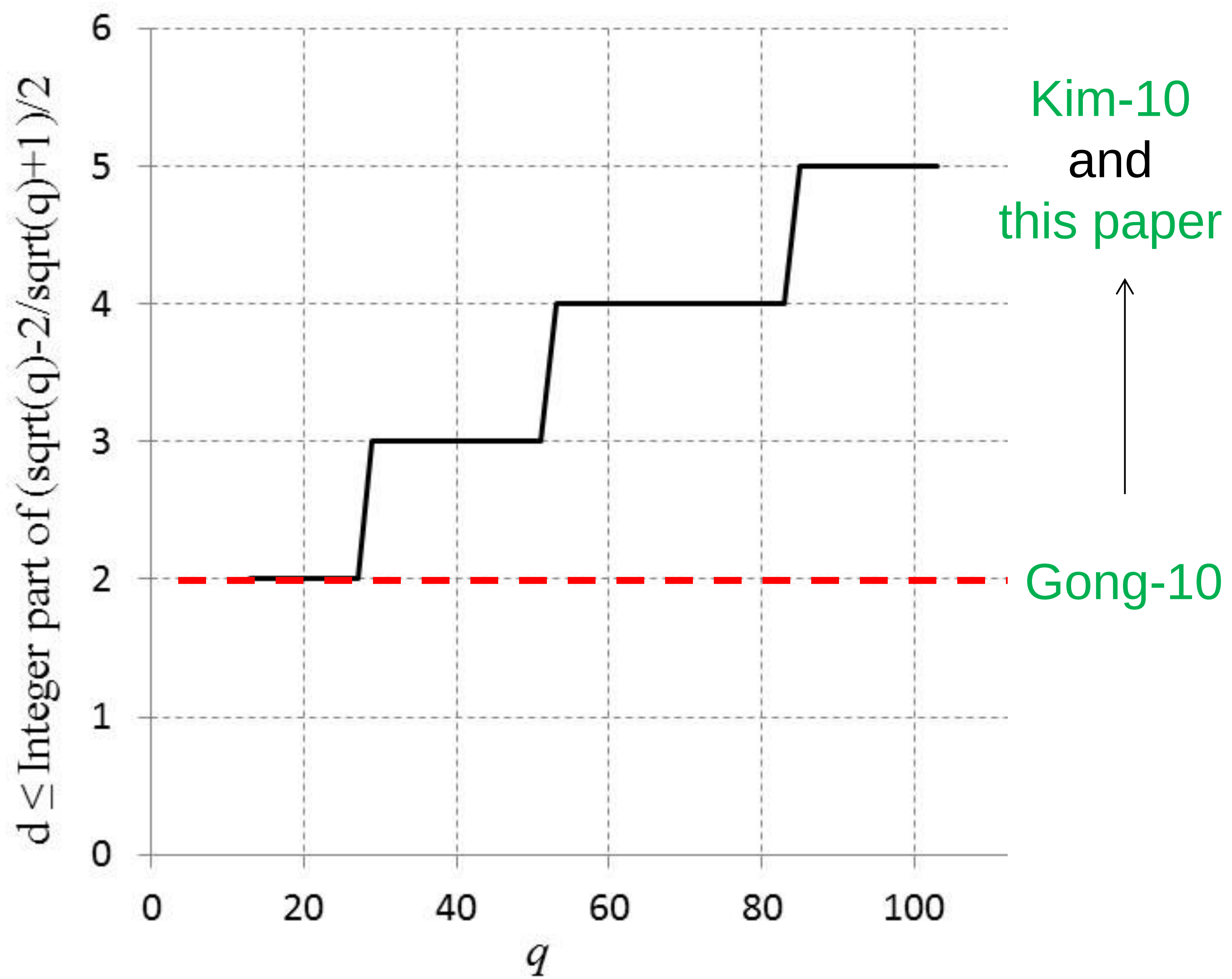
Further, we have

$$|C_{max}(\Sigma')| \le (2d - 1)\sqrt{q} + 1,$$

and

$$(M - 1)|\Lambda'| = \quad |\Sigma'| \cong |\Sigma| \quad = (M - 1)|\Lambda|$$

Range of d



d ≤ Integer part of (sqrt(q)-2/sqrt(q)+1)/2
0
1
2
3
4
5
6
0
20
40
60
80
100
q
Kim-10
and
this paper
Gong-10

Example for case $(q-1,d) \neq 1$

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:

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

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

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

Proof of Main Theorem

Suppose that $c_1 v_{l_1}(t) = c_2 v_{l_2}(t+\tau)$ **for some** τ $(o \leq \tau < q-1)$.

Then,

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

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

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

- **Claim**

Weil bound

$$\left| \sum_{x \in GF(q)} \psi_1\big(\beta^{l_1} p_{l_1}(x)\big)\psi_2\big(\beta^{l_2} \cdot \beta^{\tau d} \cdot \beta^{-\tau d} p_{l_2}(\beta^\tau x)\big) \right| \overset{??}{\leq} (2d-1)\sqrt{q}$$

If the above claim is true, then $q-1 \leq (2d-1)\sqrt{q} + 1$.

This is impossible because of our assumption $d < (\sqrt{q} - \frac{\sqrt{q}}{2} + 1)/2$.

Weil bound

Wan-97/Gong-10/Kim-10

Let $f_1(x), \dots, f_m(x)$ be **distinct monic irreducible** polynomial over $GF(q)$ with degrees $d_1, \dots, d_m$, with e_j the **number of distinct roots** in $GF(q)$ of $f_j(x)$.

Let $\psi_1, \dots, \psi_m$ be **nontrivial multiplicative characters** of $GF(q)$, with $\psi_j(0) = 1$.

Then **for every** $a_i \in \mathbb{F}_q \backslash \{0\}$, we have the estimate

$$\left| \sum_{x \in \mathbb{F}_q} \psi_1(a_1 f_1(x)) \cdots \psi_m(a_m f_m(x)) \right| \leq \left(\sum_{i=1}^{m} d_i - 1 \right) \sqrt{q} + \sum_{i=1}^{m} e_i \,.$$

For the proof of claim, we have to show that the following statement is true:

- Let l_1, l_2 be elements in $\Lambda'\backslash\{0\}$, and let $\tau (0 \le \tau < q-1)$ 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 $\tau = 0$.

Note that $p_l(x)$ **is alternative form of** $f_l(x) = N\left(\alpha^l x + 1\right)$.

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

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

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 the 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 $l_1 = l_2$.
- 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 $\tau = 0$.

Remaining steps for the family construction are straightforward

$$\Lambda \longrightarrow \Lambda'$$

by removing the representatives of the cosets of size **smaller** than d

$$\begin{tikzcd}
\Sigma \arrow[r] \arrow[d] & \Sigma' \arrow[d] \\
\Sigma^{\mathrm{ext}} \arrow[r] & \Sigma'^{\,\mathrm{ext}}
\end{tikzcd}$$

by adding **the constant multiples** of **the Sidelnikov sequence of period q-1 using β** as well as some of their **shift-and-add's**

EXAMPLE FOR $q = 199$, $L = q - 1 = 198$ FOR $M = 2$ AND $M = 198$

M	d	$(d, q-1)$	$\lvert\Lambda\rvert$ or $\lvert\Lambda'\rvert$	$\lvert\Sigma\rvert$ or $\lvert\Sigma'\rvert$	$\lvert\Sigma^{ext}\rvert$ or $\lvert\Sigma'^{ext}\rvert$	$(2d-1)\sqrt{q}+1$ or $3\sqrt{q}+3$
2	2	2	99	99	198	45.32
	3	3	13266	13266	13365	71.53
	4	2	1980000	1980000	1980099	99.75
	5	1	315231920	315231920	315232019	127.96
	6	6	52275946734	52275946734	52275946833	156.17
198	2	2	99	19503	3842288	45.32
	3	3	13266	2613402	6436187	71.53
	4	2	1980000	390060000	393882785	99.75
	5	1	315231920	62100688240	62104511025	127.96
	6	6	52275946734	10298361506598	10298365329383	156.17

Summary

Author	Family size	Correlation bound	Method
Sidelnikov '69	1	4 (regardless of q and M)	By construction
Song '07	$M-1$	$\sqrt{q}+3$	Constant Multiple
No & Yang '08-'09	$M-1+\frac{(M-1)^2(q-1)}{2}+0$	$3\sqrt{q}+5$	+ Shift-and-add
Gong '10	$\left(M-1+\frac{(M-1)^2(q-1)}{2}\right)+\frac{(M-1)(q-1)}{2}$	$3\sqrt{q}+5$	+ Column sequence
Kim '10	$\approx\left(M-1+\frac{(M-1)^2(q-1)}{2}\right)+\frac{(M-1)q^{d-1}}{d}$	$(2d-1)\sqrt{q}+1$	Extension of Gong, **With (d,q-1)=1**
IT Trans submission	comparable	comparable	Variation of Kim, **Without (d,q-1)=1**

Thanks for your attention…

Any questions?