Correlation properties of sequences from the 2-D array structure of Sidelnikov sequences of different lengths and their union

CSDL

Min Kyu Song
and **Hong-Yeop Song**
Yonsei University

Dae San Kim
Sogang University

Jang Yong Lee
Agency for Defense Development

ISIT 2016, July 10-15

Correlation among sequences

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

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

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 $C_{\max}(\Omega)$.

Notations

- p : a prime
- $q = p^r$: a prime power with a positive integer r
- $GF(q^d)$: the finite field with q^d elements
- α : a primitive elements 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 $M \geq 2$
- d : a positive integer with $2 \leq d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$
- $p_l(x)$: 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 $\psi(0) = 1$.

Brief history

Sidelnikov 69	Introduced a class of sequences called Sidelnikov sequences
Song 07	Constructed sequence families by using constant multiple
No 08 and Yang 09	Constructed sequence families by using shift-and-add
Gong 10	First analyzed 2-D array structure of Sidelnikov sequences and combining previous results
Song 15	Extended Gong's results by increasing size of the array
This paper	**Analyze the relations among arrays of different lengths**

Enlarging family size with small correlation magnitude

Sidelnikov sequences

Sidelnikov 69

Song 07

No 08 and Yang 09

Gong 10

Song 15

This paper

(Sidelnikov 69) Original definition

For a primitive element α of $GF(q)$, Sidelnikov sequence is an M-ary sequence $\{s(t)\}_{t=0}^{q-2}$ of period $q-1$ defined as

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

where $D_k = \left\{\beta^{Mi+k} - 1 \mid 0 \le i < \frac{q-1}{M}\right\}$.

(Gong 10) Alternative definition

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

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

Simple and easy to manipulate!

Array structure of Sidelnikov sequences

Sidelnikov 69

Song 07

No 08 and Yang 09

Gong 10

Song 15

This paper

For an M-ary Sidelnikov sequence $s(t)$ of period $q^d - 1$, make an array as

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

and choose some columns to construct a set of M-ary sequences of period $q-1$.

(Song 15) Column sequence representation

For a primitive element α of $GF(q^d)$ and the primitive element $\beta = \alpha^{\frac{q^d-1}{q-1}}$ of $GF(q)$, the l-th column can be represented as

$$v_l(t) = \log_\beta N_1^d(\alpha^l \beta^t + 1) \mod M,$$

where N_1^d is the norm function from $GF(q^d)$ to $GF(q)$.

How to choose columns?

use cyclotomic cosets to choose columns

(Song 15) Column selection

- Define two different cyclotomic cosets as

  1) A q-cyclotomic coset $C_l(d)$ containing l mod $q^d - 1$:

  $$C_l(d) = \{l, lq, \ldots, lq^{d_l - 1} \pmod{q^d - 1}\}.$$

  2) A q-cyclotomic coset $\tilde{C}_l(d)$ containing l mod $\frac{q^d-1}{q-1}$:

  $$\tilde{C}_l(d) = \left\{l, lq, \ldots, lq^{m_l - 1} \left(\bmod \frac{q^d - 1}{q - 1}\right)\right\}.$$

- Choose the smallest representative l of each and every $\tilde{C}_l(d)$ except for 0 such that

  $$m_l = d_l.$$

- Denote by $\Lambda'(d)$ the set of such representatives.

Sequence family construction

(Song 15)

1) For any $l \in \Lambda'(d)$ $N_1^d\left(\alpha^l \beta^t + 1\right) = \beta^l p_l(x)$ where $p_l(x)$ is a minimal polynomial of degree d which has $-\alpha^{-l}$ as a root.
   Thus, all the roots are distinct.

2) Let $\Sigma'(d)$ be a set of column sequences:

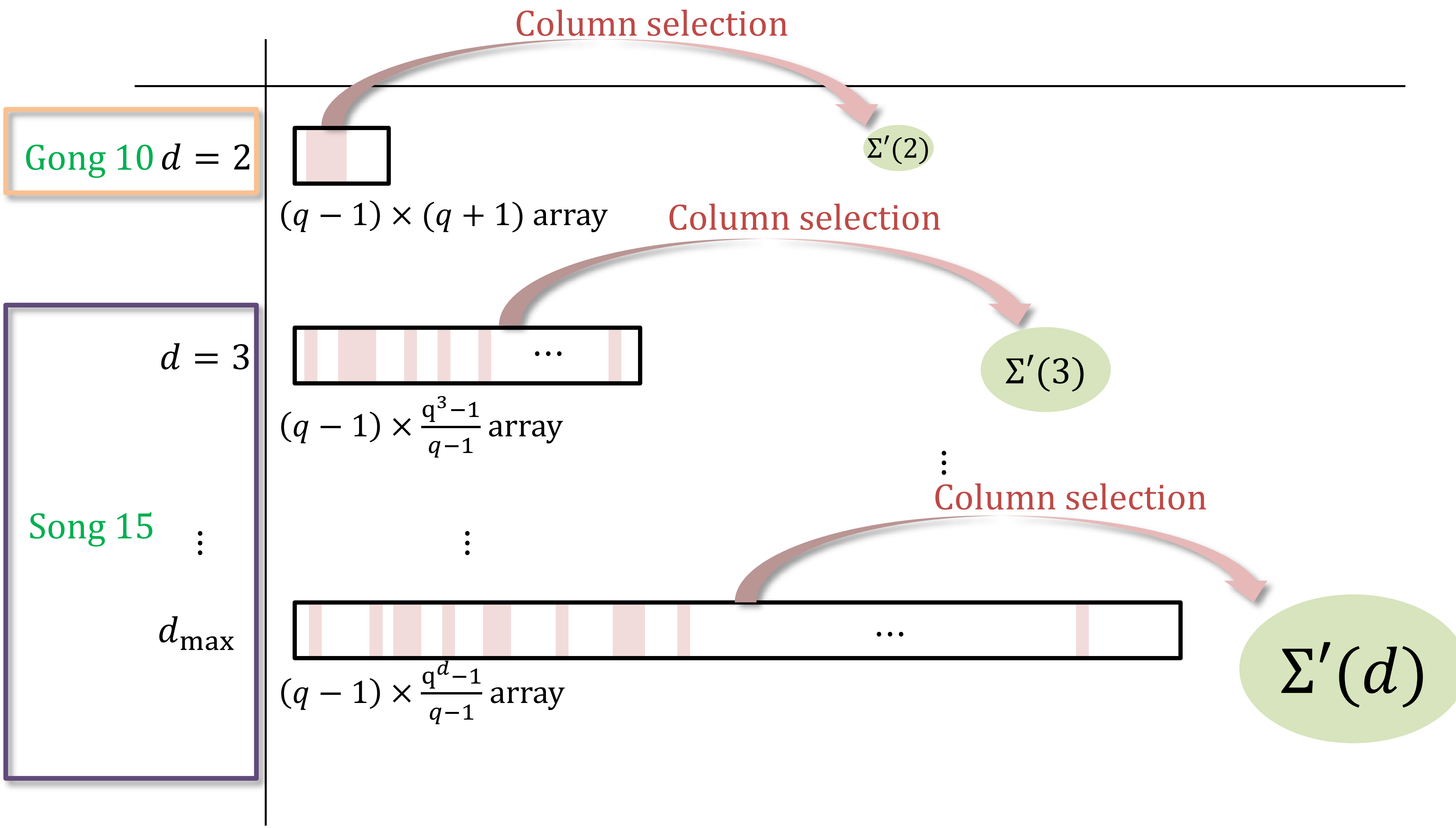
$$\Sigma'(d) = \{\, c v_l(t) \mid l \in \Lambda'(d), 1 \le c < M \,\}.$$

Then,

- $\mathrm{C}_{\max}\left(\Sigma'(d)\right) \le (2d-1)\sqrt{q} + 1.$
- The size of $|\Sigma'(d)| \sim \frac{(M-1)q^{d-1}}{d}$ as $q \to \infty$.

The upper-bound is obtained by using Weil bound.

Sequence Family construction



※ $d_{\max} = \left\lfloor \frac{1}{2}\left(\sqrt{q} - \frac{2}{\sqrt{q}} + 1\right) \right\rfloor$

Weil Bound

Let $f_1(x), \ldots, f_k(x)$ be k distinct monic irreducible polynomials over $GF(q)$ with positive degrees $m_1, \ldots, m_k$, respectively.

Let $\psi_1, \ldots, \psi_k$ be non-trivial multiplicative characters of $GF(q)$ with $\psi_i(0) = 1$ for $\mathrm{i} = 1, \ldots, k$.

Then, if the product character $\prod_{i=1}^{k} \psi_i\,(f_i(x))$ is non-trivial for some $x \in GF(q)$, then

$$\left| \sum_{x \in GF(q)} \psi_1\big(a_1 f_1(x)\big) \cdots \psi_k\big(a_k f_k(x)\big) \right| \leq \left(\sum_{i=1}^{l} d_i - 1 \right) \sqrt{q}$$

for any $a_i \in GF(q) \backslash \{0\}$, $i = 1, \ldots, k$.

Brief proof of the bound

Sidelnikov 69

Song 07

No 08 and Yang 09

Gong 10

Song 15

This paper

Since, for any $l \in \Lambda'(d)$, $p_l(x)$ is of degree d with d distinct roots and

$$p_{l_1}(x) \neq p_{l_2}(x)$$

for two distinct $l_1, l_2 \in \Lambda'(d)$, the magnitude of the correlation between $c_1 v_{l_1}(t)$ and $c_2 v_{l_2}(t)$ is

$$\left| \sum_{t=0}^{q-2} \psi^{c_1}\left(\beta^{l_1} p_{l_1}(\beta^t)\right) \psi^{M-c_2}\left(\beta^{l_2} p_{l_2}(\beta^t)\right) \right| + 1 \leq (2d-1)\sqrt{q}$$

Note: $(2d-1)\sqrt{q} < q - 1$ when

$$2 \leq d \leq \frac{1}{2}\left(\sqrt{q} - \frac{2}{\sqrt{q}} + 1\right).$$

The reason why they have the upper-bound!

Key observation

For $2 \le e < f < \frac{1}{2}\left(\sqrt{q} - \frac{2}{\sqrt{q}} + 1\right)$,

A Sidelnikov sequence of period $q^e - 1$	A Sidelnikov sequence of period $q^f - 1$
↓	↓
Array of size $(q-1) \times \frac{q^e-1}{q-1}$	Array of size $(q-1) \times \frac{q^f-1}{q-1}$
↓	↓
$\Sigma'(e) = \{cv_l(t) \mid l \in \Lambda'(e), 1 \le c < M\}$.	$\Sigma'(f) = \{cv_l(t) \mid l \in \Lambda'(f), 1 \le c < M\}$.
↓	↓
$c_1 v_{l_1}(t) = c_1 \log_\beta(\beta^{l_1} p_{l_1}(\beta^t)) \mod M$	$c_2 v_{l_2}(t) = c_2 \log_\beta(\beta^{l_2} p_{l_2}(\beta^t)) \mod M$

① $p_{l_1}(\beta^t)$ and $p_{l_2}(\beta^t)$ are of degree e and d and have all distinct roots.
② They are distinct polynomials since they are minimal and of different degree.
③ But, βs in two representations may denote different primitive elements over $GF(q)$. → If **we make them same**, **we can obtain upper bound** of the magnitude of their cross-correlation **by applying Weil bound in the same way of Song's result**.

Key observation (2)

Theorem. (relation of sequences from arrays of different size)
Let e and f be two integers with $2 \le e < f < \frac{1}{2}\left(\sqrt{q} - \frac{2}{\sqrt{q}} + 1\right)$. If we construct $\Sigma'(e)$ and $\Sigma'(f)$ **by choosing primitive elements properly**, then any two sequences $a(t) \in \Sigma'(e)$ and $b(t) \in \Sigma'(f)$ are **cyclically inequivalent** regardless of their column indices. Furthermore,

$$\mathrm{C}_{\max}\left(\Sigma'(e) \cup \Sigma'(f)\right) \le (e + f - 1)\sqrt{q} + 1.$$

How to choose:
Consider $GF(q^h)$ where $h = \mathrm{lcm}(e, f)$.
Let α be a primitive element of $GF(q^h)$. Then,

$$\alpha_e = \alpha^{(q^h-1)/(q^e-1)},$$
$$\alpha_f = \alpha^{(q^h-1)/(q^f-1)},$$

are two primitive elements over $GF(q^e)$ and $GF(q^f)$, respectively.
Obviously,

$$\beta = \alpha_e^{(q^e-1)/(q-1)} = \alpha_f^{(q^f-1)/(q-1)}.$$

So, we can easily obtain above theorem by applying Weil bound.

Union of sequence families from arrays of different size

Definition. (Extended sequence families)

Two M-ary sequence families of period $q-1$.

1) $\Sigma'^{U}(d) = \bigcup_{e=2}^{d} \Sigma'(e)$.

2) $\Sigma'^{D}(d) = \bigcup_{\substack{e|d \\ e\neq 1}} \Sigma'(e)$.

Computation over $GF(q^h)$

where $h = \mathrm{lcm}(2,3,\ldots,d)$

where $h = d$

Corollary. (Upper bound of maximum non-trivial correlation)

1) The Non-trivial complex correlation of $\Sigma'^{U}(d)$ is bounded by

$$C_{\max}(\Sigma'^{U}(d)) \leq (2d-1)\sqrt{q}+1,$$

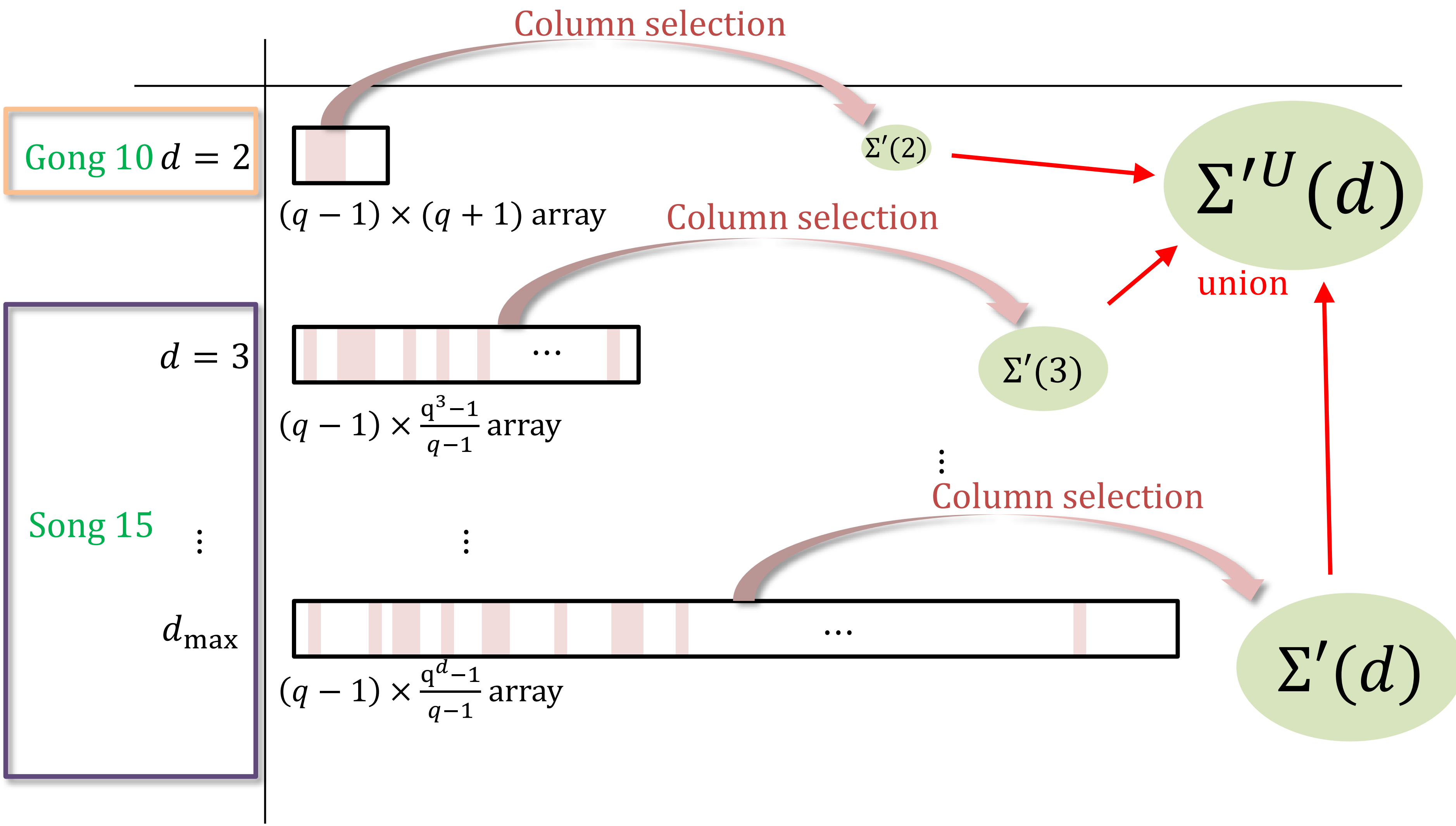
and

$$C_{\max}(\Sigma'^{D}(\mathrm{d})) \leq (2d-1)\sqrt{q}+1.$$

2) The sizes $|\Sigma'^{U}(d)|$ and $|\Sigma'^{D}(d)|$ are asymptotic to, as $q\to\infty$,

$$(M-1)\frac{q^{d-1}}{d}.$$

$\Sigma'^{U}(d)$ construction



※ $d_{\max} = \left\lfloor \frac{1}{2}\left(\sqrt{q} - \frac{2}{\sqrt{q}} + 1\right) \right\rfloor$

Comparison

q	64					
M	7			63		
d	2	3	4	2	3	4
$\lvert\Lambda'\rvert$	32	1386	66560	32	1386	66560
$(M-1)q^{(d-1)}/d$	192	8192	393216	1984	84651	4063232
$\lvert\Sigma'(d)\rvert$ (Song 15)	192	8316	399360	1984	85932	4126720
$\lvert\Sigma'^{U}(d)\rvert$	192	8508	407868	1984	87916	4214636
$\mathrm{C_{max}}(\Sigma'(d)) = \mathrm{C_{max}}(\Sigma'^{U}(d))$	25	41	57	25	41	57

Combining further previous results

For a Sidelnikov sequence $s(t)$ of period $q-1$,

Sidelnikov 69

$$I_S = \{cs(t) | 1 \leq c < M\}$$

Song 07

No 08 and Yang 09

$$A_S = \{c_0 s(t) + c_1 s(t+\delta) | 1 \leq \delta < \lfloor (q-1)/2 \rfloor\}$$

where $1 \leq c_0, c_1 < M$ if $1 \leq \delta \leq \lfloor (q-1)/2 \rfloor$

and $c_0 < c_1$ if $\delta = \frac{q-1}{2}$ for odd prime power q.

Gong 10

Song 15

$$\Sigma'^{ext}(d) = I_S \cup A_S \cup \Sigma'(d)$$

This paper

$$I_S \cup A_S \cup \Sigma'^{U}(d)$$

Question?