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

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) \( \Omega \), we denote the maximum magnitude of all the non-trivial complex correlations of any two pair of sequences in \( \Omega \) as \( C_{\text{max}}(\Omega) \).
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
- $\alpha$: a primitive elements over $GF(q^d)$
- $\beta = \frac{q^d - 1}{q - 1}$: 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 $GF(q)$
- $\omega_M$: a complex primitive $M$-th root of unity
- $\psi$: 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) Original definition
For a primitive element $\alpha$ 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 $D_k = \{\beta^{Mi+k} - 1 | 0 \leq i < \frac{q-1}{M}\}$.

(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

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

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

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

**Column sequence representation**

For a primitive element $\alpha$ of $GF(q^d)$ and the primitive element $\beta = \alpha^{q^{-1}}$ 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 $l \mod \frac{q^d - 1}{q - 1}$:
     $$\tilde{C}_l(d) = \left\{l, lq, \ldots, lq^{m_l-1} \left( \frac{q^d - 1}{q - 1} \mod q^d - 1 \right) \right\}.$$  

- 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.
(Song 15)

1) For any $l \in \Lambda'(d)$, $N_1^d(\alpha^l \beta^t + 1) = \beta^l p_l(x)$ 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:

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

Then,

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

\[ \Sigma'(d) \]

\[ (q - 1) \times (q + 1) \text{ array} \]

\[ (q - 1) \times \frac{q^d - 1}{q - 1} \text{ array} \]

\[ d = 2 \]

\[ d = 3 \]

\[ d_{\text{max}} \]

\[ d_{\text{max}} = \left\lfloor \frac{1}{2} \left( \sqrt{q} - \frac{2}{\sqrt{q}} + 1 \right) \right\rfloor \]
Weil Bound

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

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

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

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

for any $a_i \in GF(q) \backslash \{0\}$, $i = 1,...,k$. 
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 $2 \leq e < f < \frac{1}{2}\left(\sqrt{q} - \frac{2}{\sqrt{q}} + 1\right)$,

A Sidelnikov sequence of period $q^e - 1$

Array of size $(q - 1) \times \frac{q^{e-1}}{q-1}$

$\Sigma'(e) = \{cv_1(t) | l \in \Lambda'(e), 1 \leq c < M\}$.

$c_1v_1(t) = c_1 \log_\beta(\beta^{l_1}p_{l_1}(\beta^t)) \mod M$

A Sidelnikov sequence of period $q^f - 1$

Array of size $(q - 1) \times \frac{q^{f-1}}{q-1}$

$\Sigma'(f) = \{cv_1(t) | l \in \Lambda'(f), 1 \leq c < M\}$.

$c_2v_2(t) = c_2 \log_\beta(\beta^{l_2}p_{l_2}(\beta^t)) \mod M$

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, $\beta$'s 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.
**Theorem.** (relation of sequences from arrays of different size)

Let $e$ and $f$ be two integers with $2 \leq e < f < \frac{1}{2} \left( \sqrt{q} - \frac{2}{\sqrt{q}} + 1 \right)$. 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,

$$C_{\text{max}}(\Sigma'(e) \cup \Sigma'(f)) \leq (e + f - 1) \sqrt{q} + 1.$$

**How to choose:**

Consider $GF(q^h)$ where $h = \text{lcm}(e, f)$.

Let $\alpha$ 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) \[ \Sigma'^D(d) = \bigcup_{e | d \text{ and } e \neq 1} \Sigma'(e) \]

Computation over $GF(q^h)$

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

where \( h = d \)

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

1) The Non-trivial complex correlation of \( \Sigma'^U(d) \) is bounded by
\[ C_{\text{max}}(\Sigma'^U(d)) \leq (2d - 1)\sqrt{q} + 1, \]
and
\[ C_{\text{max}}(\Sigma'^D(d)) \leq (2d - 1)\sqrt{q} + 1. \]

2) The sizes \(|\Sigma'^U(d)|\) and \(|\Sigma'^D(d)|\) are asymptotic to, as $q \to \infty$,
\[ (M - 1) \frac{q^{d-1}}{d} \]
\[ \sum' \cup (d) \text{ construction} \]

\[ d = 2 \]
\[ (q - 1) \times (q + 1) \text{ array} \]

\[ d = 3 \]
\[ (q - 1) \times \frac{q^3 - 1}{q - 1} \text{ array} \]

\[ \vdots \]

\[ d_{\text{max}} \]
\[ (q - 1) \times \frac{q^{d-1} - 1}{q - 1} \text{ array} \]

\[ \star d_{\text{max}} = \left[ \frac{1}{2} (\sqrt{q} - \frac{2}{\sqrt{q}} + 1) \right] \]

Song 15

Gong 10 \( d = 2 \)

\[ \Sigma'(2) \]

Column selection

\[ \Sigma'(3) \]

\[ \Sigma'(d) \]

\[ \sum' \cup (d) \]

Column selection

union
## Comparison

<table>
<thead>
<tr>
<th>q</th>
<th>64</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>7</td>
</tr>
<tr>
<td>d</td>
<td>2</td>
</tr>
<tr>
<td>$</td>
<td>\Lambda'</td>
</tr>
<tr>
<td>$(M-1)q^{(d-1)}/d$</td>
<td>192</td>
</tr>
<tr>
<td>$</td>
<td>\Sigma'(d)</td>
</tr>
<tr>
<td>$</td>
<td>\Sigma'U(d)</td>
</tr>
<tr>
<td>$C_{\text{max}}(\Sigma'(d)) = C_{\text{max}}(\Sigma'U(d))$</td>
<td>25</td>
</tr>
</tbody>
</table>
Combining further previous results

For a Sidelnikov sequence $s(t)$ of period $q - 1$,\[
I_S = \{cs(t)|1 \leq c < M\}
\]
\[
A_S = \{c_0s(t) + c_1s(t + \delta)|1 \leq \delta < \lfloor(q - 1)/2\rfloor\}
\]
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 $q$.

\[
\Sigma'^\text{ext}(d) = I_S \cup A_S \cup \Sigma'(d)
\]

\[
I_S \cup A_S \cup \Sigma'^U(d)
\]
Question?