Properties and Crosscorrelation of Decimated Sidelnikov Sequences

IWSDA 2013
Oct. 27 – Nov. 1

Young-Tae Kim,
Ki-Hyeon Park,
Hong-Yeop Song

and
Dae San Kim

Sogang University

Yonsei University
Introduction

- Sidelnikov sequence: $M$-ary sequence of period $q - 1$
  - Will use all the notations from the previous presentation

- Decimation is a well-known method for constructing new sequences from the given sequence.

- Goal
  - Properties of decimations of a Sidelnikov sequence
  - Find the maximal correlation magnitude between two decimations
Decimation and Constant multiple

Definition

(1) \( b(t) = a(dt) \) for \( t = 0,1, \ldots \) is called the \textit{d-decimation} of \( a(t) \)

(2) \( c(t) = d \cdot a(t) \) for \( t = 0,1, \ldots \) is called the \textit{d-multiple} of \( a(t) \)

REMARK

Let \( a(t) \) be an \( M \)-ary sequence of period \( L \).

- Period of \( d \)-decimation of \( a(t) \) becomes \( \frac{L}{\gcd(d,L)} \).
  - Must choose \( d \) with \( (d, L) = 1 \)
- Alphabet size of \( d \)-multiple of \( a(t) \) becomes \( \frac{M}{\gcd(d,M)} \).
  - Must choose \( d \) with \( (d, M) = 1 \)
Theorem 1

- Let \( q = p^m \) and \( \gcd(\delta, q - 1) = 1 \).
- \( s(t) \equiv \log_\beta (\beta^t + 1) \mod M, \beta \) is primitive in \( \text{GF}(q) \).
- \( s'(t) \equiv \log_\gamma (\gamma^t + 1) \mod M, \gamma \) is primitive in \( \text{GF}(q) \).
- Then, \( s(\delta t) \equiv \delta \cdot s'(t) \mod M \) if and only if \( \gamma = \beta^\delta \).

Example \((q = 11, M = 10, \beta = 2, \gamma = 8, \delta = 3)\)

\[
\begin{align*}
\beta = 2 &: 1 8 4 6 9 0 5 3 2 7 \\
s(t) &\equiv \log_\beta (\beta^t + 1) \\
\text{Change } \beta &\rightarrow \gamma \\
s'(t) &\equiv \log_\gamma (\gamma^t + 1) \\
\gamma = 2^3 &: 7 2 5 9 8 0 4 6 3 1
\end{align*}
\]

\[
\begin{align*}
&\quad 1 6 5 7 4 0 2 8 9 3 \\
&\quad \text{\( \delta \)-Decimation} \\
&\quad 1 6 5 7 4 0 2 8 9 3 \\
&\quad \text{\( \delta \)-Multiple} \\
&\quad 1 6 5 7 4 0 2 8 9 3
\end{align*}
\]
When $d = p^l$ is prime power

**Corollary 1**
- If $d = p^l$ for $l \geq 0$, then $s(dt) = ds(t)$ for all $t$.
- Its converse is also true and the proof is not at all trivial.

**Theorem 2 (Converse of above)**
- Let $q = p^m$, $s(t)$ be a Sidelnikov sequence of period $q - 1$.
- If for some $d$ we have $s(dt) = ds(t)$ for all $t$, then $d = p^l$ for some $l$. 

\[ s(t) \equiv \log_\beta (\beta^t + 1) \quad \text{or} \quad s(p^k t) \equiv \log_\beta (\beta^{p^k t} + 1) \]
Correlation between two decimations

- Let $s(t)$ be an M-ary Sidelnikov sequence of period $q - 1$.
- Assume that $d, d'$ are relatively prime to $q - 1$.
- **Goal:** find the max correlation between $c_1 s(dt)$ and $c_2 s(d't)$.

- If $p$ divides $d$, i.e. $d = p^l q$ with $(d, q) = 1$, then we can replace $s(dt) = s(p^l qt)$ with $p^l s(qt)$ by Corollary 1.
- If $d = p^l$ and $d' = p^{l'}$ then $s(dt) = s(p^l t) = p^l s(t)$ and $s(d't) = s(p^{l'} t) = p^{l'} s(t)$.
  - Correlation between two distinct multiples of a Sidelnikov sequence.
  - This case has been studied by Song-07, No-09, Gong-10.

- Enough to consider the case where $p$ divides neither $d$ nor $d'$.  

Correlation between two decimations

Theorem 3

- Let \( s(t) \) be an M-ary Sidelnikov sequence of period \( q - 1 \).
- Assume that \( d, d' \) are relatively prime to \( q - 1 \).
- Let \( a(t) = c_1 s(dt), b(t) = c_2 s(d't) \) be cyclically inequivalent.
- Then we have

\[
| \max_{\tau} \{ C_{a,b}(\tau) \} | \leq (d + d' - 1) \sqrt{q} + 3
\]

where \( \tau \) runs over the integers \( 0 \leq \tau \leq q - 2 \).
When $d' = 1$

**Corollary 2**

- Assume that $(d, q - 1) = 1$ and $p$ does not divide $d$.
- Let $s(t)$ be a Sidelnikov sequence of period $q - 1$.
- Let $b(t) = s(dt)$ and $a(t) = s(t)$.
- Then we have

$$| \max_{\tau} \{ C_{a,b}(\tau) \} | \leq d \sqrt{q} + 3$$

where $\tau$ runs over the integers $0 \leq \tau \leq q - 2$. 
Example: Correlation function

- Correlation of the Sidelnikov sequence of period $3^5 - 1 = 242$ and its 5-decimation.

- Red line indicates the correlation bound which is about 81.

- True max is about 42, showing some gap.
Example: Correlation bound

<table>
<thead>
<tr>
<th>q</th>
<th>d</th>
<th>M</th>
<th>Max</th>
<th>Bound (= d√q + 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>5</td>
<td>7</td>
<td>17.62</td>
<td>43.00</td>
</tr>
<tr>
<td>243</td>
<td>3</td>
<td>11</td>
<td>17.95</td>
<td>49.76</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>11</td>
<td>41.78</td>
<td>80.94</td>
</tr>
<tr>
<td>256</td>
<td>7</td>
<td>15</td>
<td>40.26</td>
<td>115.00</td>
</tr>
<tr>
<td>289</td>
<td>5</td>
<td>8</td>
<td>45.12</td>
<td>88.00</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>8</td>
<td>35.52</td>
<td>122.00</td>
</tr>
<tr>
<td>343</td>
<td>5</td>
<td>9</td>
<td>42.23</td>
<td>95.60</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>9</td>
<td>21.00</td>
<td>132.64</td>
</tr>
<tr>
<td>512</td>
<td>5</td>
<td>7</td>
<td>50.80</td>
<td>68.88</td>
</tr>
<tr>
<td>1024</td>
<td>5</td>
<td>3</td>
<td>72.06</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>11</td>
<td>87.14</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>31</td>
<td>97.39</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>33</td>
<td>106.24</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>93</td>
<td>86.23</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>341</td>
<td>86.15</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1023</td>
<td>91.48</td>
<td></td>
</tr>
</tbody>
</table>

- This table shows the exact maximal correlation magnitude between \( s(t) \) and \( s(dt) \) and the correlation bound for given \( q, d, m \).
Conclusion

- Apply the decimation to Sidelnikov sequences.

- Main result 1
  - Deriving a relation between decimations and primitive elements. (known earlier by others)
  - $d$-decimation is equal to $d$-multiple if and only if $d = p^l$ for some $l \geq 0$.

- Main result 2
  - The max correlation between two decimations is dependent on the sum of two decimation factors.
Thanks for your attention...

Any questions?