Properties and Crosscorrelation of Decimated Sidelnikov Sequences

1000000100000110000101000111100100010110011101010011111010000111000100100110110101101111011000110100101110111001100101010111111

IWSDA 2013
Oct. 27 – Nov. 1

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

and Dae San Kim
Sogang 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 ***d*-decimation** of $a(t)$

(2) $c(t) = d \cdot a(t)$ for $t = 0,1, \ldots$is called the ***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 $(d, M) = 1$

Changing the primitive element

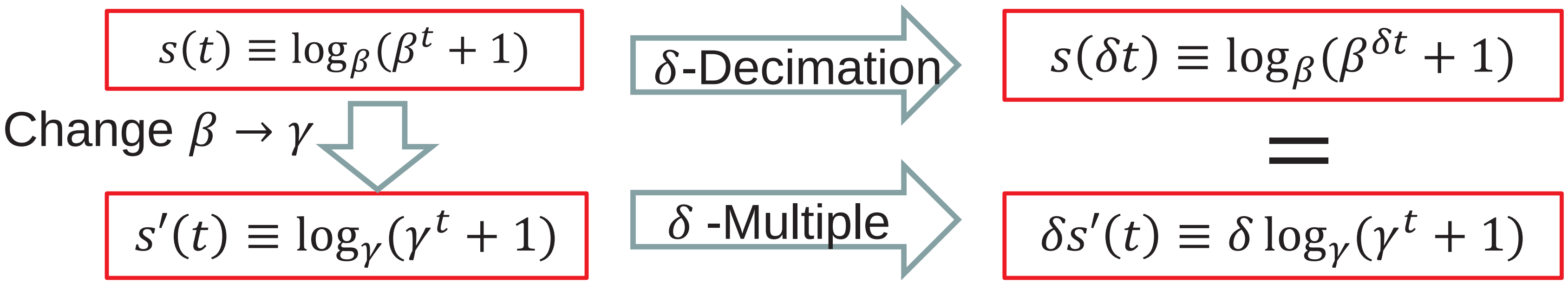
No-09

- **Theorem 1**
  - Let $q = p^m$ and $\gcd(\delta, q-1) = 1$.
  - $s(t) \equiv \log_\beta(\beta^t + 1) \bmod M$, β is primitive in GF(q).
  - $s'(t) \equiv \log_\gamma(\gamma^t + 1) \bmod M$, γ is primitive in GF(q).
  - Then, $s(\delta t) \equiv \delta \cdot s'(t) \bmod M$ if and only if $\gamma = \beta^\delta$.

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

$\beta = 2$: 1 8 4 6 9 0 5 3 2 7

1 6 5 7 4 0 2 8 9 3



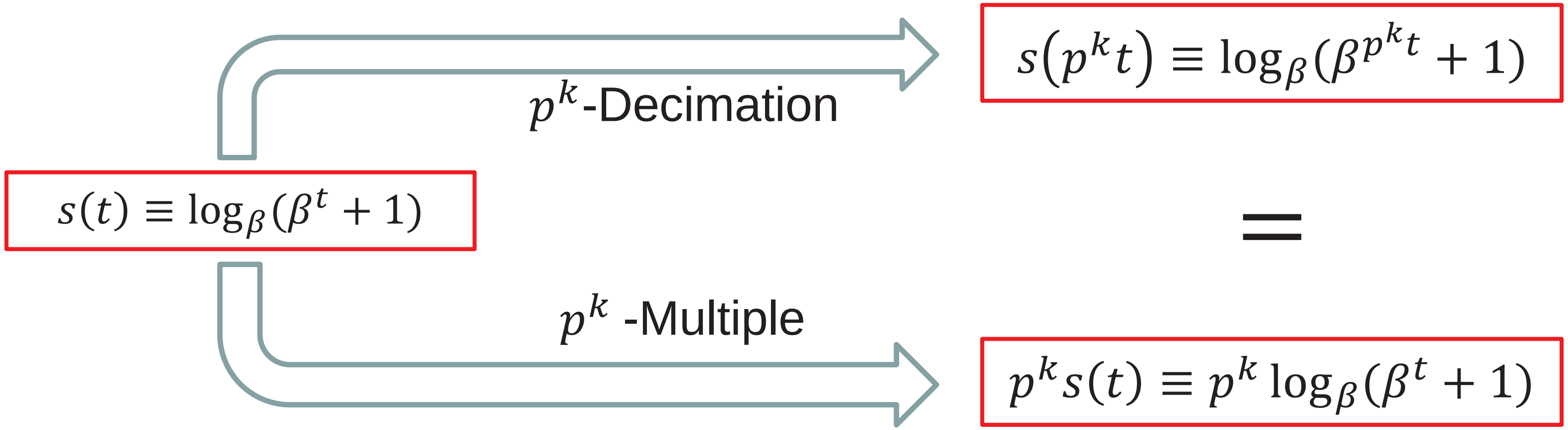
$\gamma = 2^3$: 7 2 5 9 8 0 4 6 3 1

1 6 5 7 4 0 2 8 9 3

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.



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 $s(dt) = s\left(p^l q t\right)$ with $p^l s(qt)$ by Corollary 1.
- If $d = p^l$ and $d' = p^{l'}$ then $s(dt) = s\left(p^l t\right) = p^l \mathrm{s}(\mathrm{t})$ and $s(d't) = s\left(p^{l'} t\right) = p^{l'} \mathrm{s}(\mathrm{t})$.
  - 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 τ runs over the integers $0 \leq \tau \leq q-2$.

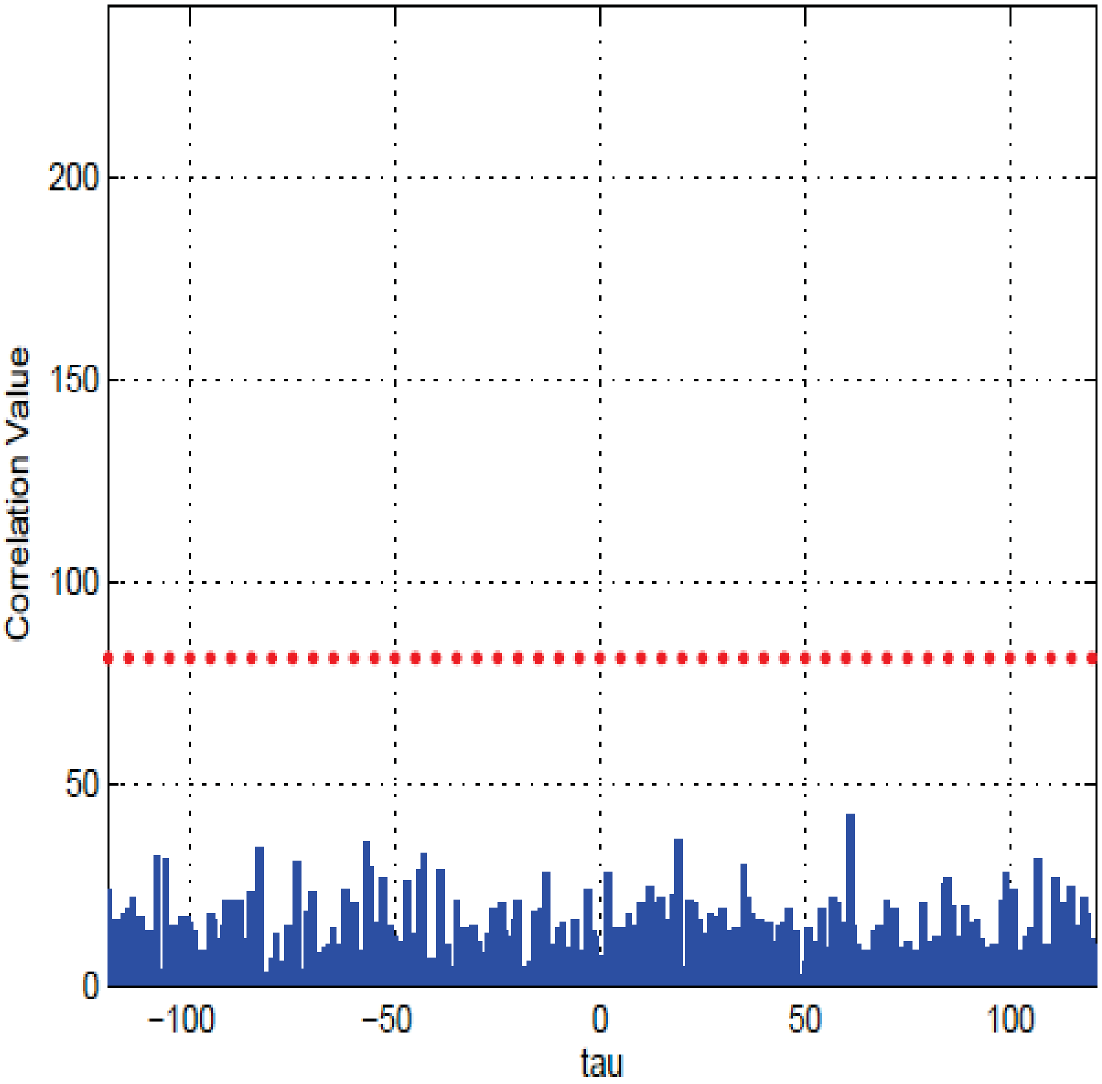
When $d' = 1$

- **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 τ 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

q	d	M	Max	Bound $(= d\sqrt{q}+3)$
64	5	7	17.62	43.00
243	3	11	17.95	49.76
	5	11	41.78	80.94
256	7	15	40.26	115.00
289	5	8	45.12	88.00
	7	8	35.52	122.00
343	5	9	42.23	95.60
	7	9	21.00	132.64
512	5	7	50.80	68.88
1024	5	3	72.06	163.00
		11	87.14	
		31	97.39	
		33	106.24	
		93	86.23	
		341	86.15	
		1023	91.48	

- This table shows the exact maximal correlation magnitude between $s(t)$ and $s(dt)$ and

  the correlation bound

  for given q, d, m.

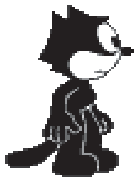
Conclusion

- 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?