Linear Complexity of Generalized NTU Sequences

1 Kazuyoshi Tsuchiya  2 Chiaki Ogawa  2 Yasuyuki Nogami
   3 Satoshi Uehara

1Koden Electronics Co., Ltd.
2Graduate School of Natural Science and Technology, Okayama University
3Faculty of Environmental Engineering, the University of Kitakyushu

September 24, 2017 – September 28, 2017
Hokkaido University, Sapporo, Japan
Session 4 : Sequence design and analysis of sequences (1)
IWSDA ‘17
Motivation

Geometric sequences and generalized NTU sequences

Linear complexity of generalized NTU sequences
1. Motivation

1. Motivation
2. Geometric sequences and generalized NTU sequences
3. Linear complexity of generalized NTU sequences
Motivation

In cryptography, PRNGs are required to generate PRNs which have good statistical properties as well as unpredictability. M-sequences are well-distributed sequences with long period, however, we must nonlinearize these sequences for cryptographic purposes.

A geometric sequence is a sequence given by applying a nonlinear feedforward function to an m-sequence. Nogami et al. proposed a geometric sequence whose nonlinear feedforward function is given by the Legendre symbol, and showed the period, periodic autocorrelation and linear complexity of the geometric sequence.

Furthermore, Nogami et al. proposed a generalization of the geometric sequence (referred to as the generalized NTU sequence), and showed the period and periodic autocorrelation.

The purpose of our work
To investigate the linear complexity of the generalized NTU sequences
Linear Complexity

Linear Complexity of a sequence \( S \)
The shortest length of an LFSR that generates \( S \).

Definition of Linear Complexity
For a sequence \( S = (s_n)_{n \geq 0} \) over a finite field \( \mathbb{F}_\ell \), the linear complexity \( L(S) \) of \( S \) is the length \( L \) of the shortest linear recurrence relation
\[
s_{n+L} = a_{L-1}s_{n+L-1} + \cdots + a_0s_n, \quad n \geq 0
\]
for some \( a_0, \ldots, a_{L-1} \in \mathbb{F}_\ell \), and the minimal polynomial \( m(x) \) of \( S \) is the polynomial
\[
x^L - a_{L-1}x^{L-1} - \cdots - a_0 \in \mathbb{F}_\ell[x].
\]

Properties of Linear Complexity
Assume that \( S \) is a periodic sequence of period \( N \) and 
\[S(x) := s_0 + s_1x + \cdots + s_{N-1}x^{N-1} \in \mathbb{F}_\ell[x].\]
Then
\[L(S) = N - \deg (\gcd (x^N - 1, S(x))).\]
In particular, \( L(S) \leq N \).
2. Geometric sequences and generalized NTU sequences

1. Motivation
2. Geometric sequences and generalized NTU sequences
3. Linear complexity of generalized NTU sequences
Geometric sequences

A geometric sequence is a sequence given by applying a nonlinear feedforward function to an m-sequence.

Definition of geometric sequences (Chan–Games)

- Let $p$ be an odd prime number, $m > 1$ an integer, $\omega$ a primitive element in $\mathbb{F}_{p^m}$.
- $R = (R_n)_{n \geq 0}$ an m-sequence defined as $R_n = \text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\omega^n)$, $n \geq 0$.
- Let $\rho : \mathbb{F}_p \rightarrow \mathbb{F}_2$ be a (nonlinear) map.
- $S = (S_n)_{n \geq 0}$, $S_n = \rho(R_n)$, $n \geq 0$ is called a geometric sequence.
- $g = \omega^{(p^m-1)/(p-1)} \in \mathbb{F}_p$.
- $s = (s_n)_{n \geq 0}$, $s_n = \rho(g^n)$, $n \geq 0$.

Examples of geometric sequences
GMW sequences, cascaded GMW sequences, ...
Definition of generalized NTU sequences

Generalized NTU sequences

- For $A \in \mathbb{F}_p$, we define a map $\rho_A^{\text{NTU}} : \mathbb{F}_p \to \mathbb{F}_2$ as

$$\rho_A^{\text{NTU}}(x) = \begin{cases} 
1 & \text{if } \left( \frac{x+A}{p} \right) = -1 \\
0 & \text{otherwise}
\end{cases}$$

- Let $S_A^{\text{NTU}} = (S_{A,n}^{\text{NTU}})_{n \geq 0}$, $S_{A,n}^{\text{NTU}} = \rho_A^{\text{NTU}}(R_n)$, $n \geq 0$. $S_A^{\text{NTU}}$ is called a generalized NTU sequence.

- Let $s_A^{\text{NTU}} = (s_{A,n}^{\text{NTU}})_{n \geq 0}$, $s_{A,n}^{\text{NTU}} = \rho_A^{\text{NTU}}(g^n)$, $n \geq 0$.

NTU sequence

If $A = 0$, then $S_0^{\text{NTU}}$ is an NTU sequence.

Sidel’nikov sequence

If $A = 1$, then $s_1^{\text{NTU}}$ is a Sidel’nikov sequence.
Motivation
Geometric sequences and generalized NTU sequences
Linear complexity of generalized NTU sequences

Equivalence on generalized NTU sequences

Example

\( p = 5, \ m = 2, \ f(x) = x^2 + 2x + 3 \in \mathbb{F}_5[x] : \) primitive polynomial.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|   | 2 | 3 | 3 | 0 | 1 | 3 | 1 | 4 | 4 | 0 | 3 | 4 | 3 | 2 | 2 | 0 | 4 | 2 | 4 | 1 | 1 | 0 | 2 | 1 |
| \( S_{1,n}^{\text{NTU}} \) | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| \( S_{2,n}^{\text{NTU}} \) | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 |
| \( S_{3,n}^{\text{NTU}} \) | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 |
| \( S_{4,n}^{\text{NTU}} \) | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 |

Lemma (Equivalence on generalized NTU sequences)

Let \( A_1, A_2 \in \mathbb{F}_p - \{0\} \).

If \( (A_1/p) = (A_2/p) \), then \( S_{A_1,n}^{\text{NTU}} \) and \( S_{A_2,n}^{\text{NTU}} \) are shift-equivalent to each other.

\[ \Rightarrow S_{A}^{\text{NTU}} \] can be classified into three types: \( A = 0 \), \( A \) is QR and \( A \) is QNR.
### NTU sequences vs Generalized NTU sequences

<table>
<thead>
<tr>
<th></th>
<th>NTU ((A = 0))</th>
<th>Generalized NTU ((A \neq 0))</th>
</tr>
</thead>
<tbody>
<tr>
<td>period</td>
<td>(\frac{2(p^m - 1)}{(p - 1)})</td>
<td>(p^m - 1)</td>
</tr>
<tr>
<td>autocorrelation</td>
<td>have been explicitly obtained</td>
<td></td>
</tr>
<tr>
<td>linear complexity</td>
<td>(\frac{2(p^m - 1)}{(p - 1)})</td>
<td>???</td>
</tr>
</tbody>
</table>

|                      | ↑ maximal                                 | ↑ to be maximal?                    |
|                      | conditions to have large LC?             |                                     |

### Our strategy

1. Applying a formula for general geometric sequences
2. Considering the sequence of complement numbers
3. Using the Hasse derivative and cyclotomic classes
3. Linear complexity of generalized NTU sequences
Chan–Games formula

Strategy 1
Applying a formula for general geometric sequences

Lemma (Chan–Games formula)
Assume that $\rho(0) = 0$. Then

$$L(S) = \frac{p^m - 1}{p - 1} L(s).$$

1. Case of $(A/p) = 1$:
   - Since $\rho_A^{\text{NTU}}(0) = 0$,
   - $L(S_A^{\text{NTU}}) = L(S_1^{\text{NTU}}) = \frac{p^m - 1}{p - 1} L(s_1^{\text{NTU}})$.
   $\uparrow$ LC of a Sidel’nikov seq.

2. Case of $(A/p) = -1$:
   - Since $\rho_A^{\text{NTU}}(0) = 1$,
   - we can not apply the Chan–Games formula.
Sequence of complement numbers

Strategy 2

Considering the sequence of complement numbers

Sequence of complement numbers and Chan–Games formula

- We define a map \( \rho_A^{\text{NTU}} : \mathbb{F}_p \to \mathbb{F}_2 \) as
  \[
  \rho_A^{\text{NTU}}(x) = \rho_A^{\text{NTU}}(x) + 1.
  \]
- Let \( S_A^{\text{NTU}} = (S_{A,n}^{\text{NTU}})_{n \geq 0}, \quad S_{A,n}^{\text{NTU}} = \rho_A^{\text{NTU}}(R_n), \quad n \geq 0, \)
  and \( s_A^{\text{NTU}} = (s_{A,n}^{\text{NTU}})_{n \geq 0}, \quad s_{A,n}^{\text{NTU}} = \rho_A^{\text{NTU}}(g^n), \quad n \geq 0. \)
- Assume that \( (A/p) = -1. \)
  Since \( \rho_A^{\text{NTU}}(0) = 0, \) we can apply the Chan–Games formula to \( S_A^{\text{NTU}}. \)

Question

What is the relationship between \( L(S_A^{\text{NTU}}) \) and \( L(S_A^{\text{NTU}}) \) ?
Case of \((A/p) = -1, p \equiv 1 \text{ mod } 4\)

**Lemma (See Lidl–Niederreiter Theorem 8.62)**

<table>
<thead>
<tr>
<th>the multiplicity of 1</th>
<th>linear complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>(m_1(x^N - 1) \leq m_1(S(x)))</td>
<td>(L(\tilde{S}) = L(S) + 1)</td>
</tr>
<tr>
<td>(m_1(x^N - 1) = m_1(S(x)) + 1)</td>
<td>(L(\tilde{S}) = L(S) - 1)</td>
</tr>
<tr>
<td>(m_1(x^N - 1) &gt; m_1(S(x)) + 1)</td>
<td>(L(\tilde{S}) = L(S))</td>
</tr>
</tbody>
</table>

**Theorem**

*Assume that \((A/p) = -1, p \equiv 1 \text{ mod } 4\). Then*

\[
L(S_{A_{NTU}}^N) = \frac{p^m - 1}{p - 1} L(s_{A_{NTU}}^N). \quad \leftarrow \text{the same eq. as in Chan–Games formula}
\]

In fact, \(m_1(x^{p^m-1} - 1) \geq 2\) and \(m_1(x^{p-1} - 1) \geq 2\).
On the other hand, \(m_1(S_{A_{NTU}}^N(x)) = m_1(s_{A_{NTU}}^N(x)) = 0\).
**Note:** \((A/p) = -1, p \equiv 3 \text{ mod } 4 \implies m_1(S_{A_{NTU}}^N(x)) \geq 1, m_1(s_{A_{NTU}}^N(x)) \geq 1\).
Hasse derivative and cyclotomic classes

**Strategy 3**

Using the Hasse derivative and cyclotomic classes

**Hasse derivative**
For \( S(x) = a_0 + a_1x + \cdots + a_{N-1}x^{N-1} \),

\[
S^{(k)}(x) = a_k + \binom{k+1}{k}a_{k+1}x + \cdots + \binom{N-1}{k}a_{N-1}x^{N-1-k}
\]

is called the \( k \)th Hasse derivative of \( S(x) \).

Let \( \xi \) be a root of \( S(x) \). Then

\[
m_\xi(S(x)) = \nu \iff S(\xi) = S^{(1)}(\xi) = \cdots = S^{(\nu-1)}(\xi) = 0, \quad S^{(\nu)}(\xi) \neq 0.
\]

**Cyclotomic classes and difference parameter**

\( D_0 = \{ a \in \mathbb{F}_p \mid (a/p) = 1 \} \), \( D_1 = \{ a \in \mathbb{F}_p \mid (a/p) = -1 \} \) are called cyclotomic classes of order 2. For \( a \in \mathbb{F}_p \), the difference parameter is defined as

\[
d(i,j;a) = \#(D_i \cap (D_j - a)), \quad i,j \in \{0,1\}, \quad a \in \mathbb{F}_p.
\]

If \( a = 1 \), then \( d(i,j;1) \) is nothing but the cyclotomic number \((i,j)_2\) of order 2.
Case of \((A/p) = -1, p \equiv 3 \mod 4\)

**Lemma**

Assume that \((A/p) = -1, p \equiv 3 \mod 4\) and \(m \equiv 1 \mod 2\). Then

\[
S_{NTU}^{(1)}(1) = \sum_{i=0}^{\frac{p^m - 3}{2}} S_{NTU}^{(1)}_{A,2i+1} = \begin{cases} 
0 & \text{if } p \equiv 3 \mod 8 \\
1 & \text{if } p \equiv 7 \mod 8.
\end{cases}
\]

**Theorem**

Assume that \((A/p) = -1, p \equiv 3 \mod 4\) and \(m \equiv 1 \mod 2\). Then

\[
L(S_{NTU}^{(1)}) = \begin{cases} 
\frac{p^m - 1}{p - 1} (L(S_{NTU}^{(1)})+1) - 1 & \text{if } p \equiv 3 \mod 8 \\
\frac{p^m - 1}{p - 1} (L(S_{NTU}^{(1)})-1) + 1 & \text{if } p \equiv 7 \mod 8.
\end{cases}
\]

**Remark**

In the case of \(m \equiv 0 \mod 2\), Heguri et al. obtained a formula of LC by numerical experiments (See Remark 11 in the proceeding).
Sketch of the proof of Lemma

Interleaved structure of an m-sequence $R = (R_n)_{n \geq 0}$

$$\nu = (p^m - 1)/(p - 1)$$

$R_j \neq 0$  

$R_j = 0$  

$$\mathbb{F}_p^\times$$  

$$\mathbb{F}_p^\times$$  

$(0)$  

$\cdots$  

$$\mathbb{F}_p^\times$$  

$g^0 R_0$  

$g^1 R_0$  

$\cdots$  

$g^{p-2} R_0$  

$g^0 R_1$  

$g^1 R_1$  

$\cdots$  

$g^{p-2} R_1$  

$0$  

$0$  

$\cdots$  

$0$  

$g^0 R_{\nu-1}$  

$g^1 R_{\nu-1}$  

$\cdots$  

$g^{p-2} R_{\nu-1}$
Sketch of the proof of Lemma (cont.)

The number of terms satisfying $S_{A,i
u+j}^{\text{NTU}} = 1$ and $i\nu + j \equiv 1 \mod 2$

\[
\begin{array}{cccc}
g^0 R_0 & g^0 R_1 & 0 & \cdots & g^0 R_{\nu-1} \\
g^1 R_0 & g^1 R_1 & 0 & \cdots & g^1 R_{\nu-1} \\
g^2 R_0 & g^2 R_1 & 0 & \cdots & g^2 R_{\nu-1} \\
g^3 R_0 & g^3 R_1 & 0 & \cdots & g^3 R_{\nu-1} \\
g^4 R_0 & g^4 R_1 & 0 & \cdots & g^4 R_{\nu-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
g^{p-2} R_0 & g^{p-2} R_1 & 0 & \cdots & g^{p-2} R_{\nu-1} \\
D_0 \text{ or } D_1 & D_0 \text{ or } D_1 & (0) & \cdots & D_0 \text{ or } D_1 \\
\end{array}
\]

\[
\sum_{i=0}^{(p^m-3)/2} S_{A,2i+1}^{\text{NTU}} = \frac{p^m - 1}{p - 1} \times \frac{p - 1}{2} + \left\{ \nu - \frac{p^m - 1}{p - 1} \right\} \times \frac{p - 3}{4}
\]

# of "(0)"s  # of "0"s in (0)  # of "D_0 or D_1"s  $d(0, 1; A)$ or $d(1, 1; A)$
### Conditions to have a large linear complexity

#### Descriptions of \( L(S_A^{NTU}) \) using \( L(s_A^{NTU}) \)

<table>
<thead>
<tr>
<th>( \left( \frac{A}{p} \right) = 1 )</th>
<th>( \left( \frac{A}{p} \right) = -1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( p \equiv 1 \mod 4 )</td>
<td>( p \equiv 3 \mod 4, m \equiv 1 \mod 2 )</td>
</tr>
</tbody>
</table>
| \( \frac{p^m - 1}{p - 1} L(s_A^{NTU}) \) | \( \frac{p^m - 1}{p - 1} \left( L(s_A^{NTU}) + 1 \right) - 1 \)
| \( \frac{p^m - 1}{p - 1} \left( L(s_A^{NTU}) - 1 \right) + 1 \) | \( \frac{p^m - 1}{p - 1} \left( L(s_A^{NTU}) - 1 \right) + 1 \) |

#### Conditions to have a large linear complexity

\( p = 2^s r + 1 \) (\( r \): odd prime number, \( 2 \in \mathbb{F}_r \): primitive root, \( r \geq \sqrt{p} + 1 \)).

<table>
<thead>
<tr>
<th>( \left( \frac{A}{p} \right) = 1 )</th>
<th>( \left( \frac{A}{p} \right) = -1 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( s = 1 )</td>
<td>( s \geq 2 )</td>
</tr>
<tr>
<td>( L(s_A^{NTU}) = p - 1 ) ( \leftarrow ) max</td>
<td>( L(s_A^{NTU}) = p - 2 )</td>
</tr>
<tr>
<td>( L(S_A^{NTU}) = p^m - 1 ) ( \leftarrow ) max</td>
<td>( L(S_A^{NTU}) = \frac{p^{m+1} - 3p^m + 2}{p - 1} )</td>
</tr>
</tbody>
</table>

This table is obtained by the result of Meidl–Winterhof (Brandstatter–Meidl).
Conclusion

We investigate linear complexity of generalized NTU sequences.

We describe $L(S_{NTU}^A)$ using $L(s_{NTU}^A)$ with the following strategy:

1. Applying a formula for general geometric sequences
2. Considering the sequence of complement numbers
3. Using the Hasse derivative and cyclotomic classes

We can ensure that generalized NTU sequences have large linear complexity from the results on linear complexity of Sidel’nikov sequences.

Future work

- Theoretical estimation in the case of $m \equiv 0 \mod 2$.
- Estimation of linear complexity profile.
- Applications to cryptography.
Acknowledgment

Thank you for your attention.