One-Error Linear Complexity over F_p of S-LCE Sequences

SETA'04 (Oct. 24 ∼ 28)

Yu-Chang Eun and Hong-Yeop Song

Yonsei University

Seoul, Korea

Outline

- Introduction
  - Sidelnikov-Lempel-Cohn-Eastman sequences
  - k-error linear complexity
- One-error linear complexity over F_p of a S-LCE sequence
  - Linear complexity computation by Fourier transform
  - Special case (Upper bound on one-error L.C.)
  - Proof of the theorem
- Conjecture

Introduction

◇ Sidelnikov-Lempel-Cohn-Eastman sequences

- Definition of a S-LCE sequence

$$s(t) = \begin{cases} 1 & \text{if } \alpha^t + 1 \in QNR \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

where $QNR = \{\alpha^{2t+1} | t = 0, 1, ..., \frac{p^m-1}{2} - 1\}$ over F_{p^m}

- Let $\chi(x)$ denote the quadratic character of $x \in F_{p^m}$ defined by

$$\chi(x) = \begin{cases} +1, & \text{if } x \text{ is a quadratic residue} \\ 0, & \text{if } x = 0 \\ -1, & \text{if } x \text{ is a quadratic nonresidue.} \end{cases}$$

Then [*Helleseth and Yang '01*],

$$s(t) = \frac{1}{2}\big(1 - I(\alpha^t + 1) - \chi(\alpha^t + 1)\big) \tag{2}$$

where $I(x) = 1$ if $x = 0$ and $I(x) = 0$ otherwise.

- [*Helleseth, Kim, and No '03*]

  The linear complexity over F_p (not F_2) of a S-LCE sequence of length $p^m - 1$ and its trace representation were derived when $p = 3$, 5, and 7.

◇ k-error linear complexity

- Denote the linear complexity of a sequence S by $L(S)$.
- Let $Z = \{z(t)\}$ belong to the set of all the sequences withe the same length as S.
- The k-error linear complexity of S

$$L_k(S) = \min_{0 \leq \mathsf{WH}(Z) \leq k} L(S + Z). \tag{3}$$

One-error linear complexity over F_p of a S-LCE sequence

- Assume $z^{(\tau,\lambda)}(t) = \frac{\lambda}{2} I(\alpha^{t-\tau}+1)$ for $0 \le \tau < p^m - 1$ and $\lambda \in F_p$.
- Then the sequence $Z^{(\tau,\lambda)} = \{z^{(\tau,\lambda)}(t)\}$ is able to represent all the sequences over F_p such that WH$(Z^{(\tau,\lambda)}) \le 1$.

- The one-error allowed S-LCE sequence $S_Z^{(\tau,\lambda)} = \{s_z^{(\tau,\lambda)}(t)\}$

$$\begin{aligned} s_z^{(\tau,\lambda)}(t) &\triangleq s(t) + z^{(\tau,\lambda)}(t) \\ &= \frac{1}{2}\left(1 - I(\alpha^t+1) - \chi(\alpha^t+1)\right) + \frac{\lambda}{2} I(\alpha^{t-\tau}+1). \end{aligned} \tag{4}$$

- The one-error linear complexity of a S-LCE sequence S

$$L_1(S) = \min_{0 \le \tau \le p^m - 2,\ \lambda \in F_p} L(S_Z^{(\tau,\lambda)}). \tag{5}$$

◇ Linear complexity computation (Blahut's theorem)

- Fourier transform for a p-ary sequence $Y = \{y(t)\}$ of period $n = p^m - 1$

$$A_i = \frac{1}{n}\sum_{t=0}^{n-1} y(t)\alpha^{-it} \in F_{p^m} \tag{6}$$

where α is a primitive element of F_{p^m}

- The linear complexity of Y

$$\begin{aligned} L(Y) &= |\{\ i \mid A_i \neq 0,\ 0 \leq i \leq n-1\ \}| \\ &= p^m - 1 - |\{\ i \mid A_i = 0,\ 0 \leq i \leq n-1\ \}|\,. \end{aligned} \tag{7}$$

Lemma 1 [*Helleseth, Kim, and No '03*] *Let the p-adic expansion of i be given as*

$$i = \sum_{n=0}^{m-1} i_a p^a$$

where $0 \le i \le p-1$. Then, the Fourier coefficient $A_{-i}(\in F_{p^m})$ of the S-LCE sequence defined in (2) is given as

$$A_{-i} = \frac{1}{p-1}\left(-(-1)^i - (-1)^{i-\frac{p^m-1}{2}} \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}}\right). \tag{8}$$

Lemma 2 *The Fourier coefficient $A_{-i}(\tau, \lambda)$ of the one-error allowed S-LCE sequence $S_Z^{(\tau,\lambda)}$ defined in (4) is given as*

$$\begin{aligned} A_{-i}(\tau,\lambda) =& \frac{1}{p-1}\Bigg(- (-1)^i \\ & + \lambda(-\alpha^\tau)^i - (-1)^{i-\frac{p^m-1}{2}} \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}}\Bigg) \in F_{p^m} \end{aligned} \tag{9}$$

where i_a is defined in Lemma 1.

◇ Special case (Upper bound on one-error L.C.)

- When $\alpha^{\tau} = 1$ (or $\tau = 0$) and $\lambda = 1$ in the one-error allowed S-LCE sequence $s_z^{(\tau,\lambda)}(t) = \frac{1}{2}\left(1 - I(\alpha^t + 1) - \chi(\alpha^t + 1)\right) + \frac{\lambda}{2} I(\alpha^{t-\tau} + 1)$

$$s_z^{(0,1)}(t) = \frac{1}{2}(1 - \chi(\alpha^t + 1)).$$

- Then,

$$\begin{aligned} L\left(S_Z^{(0,1)}\right) &= \left|\{\ i \mid A_{-i}(0,1) \neq 0,\ 0 \le i \le p^m - 2\ \}\right| \\ &= |I| = \left(\frac{p+1}{2}\right)^m - 1. \end{aligned} \tag{10}$$

where

$$\begin{aligned} I &= \left\{\ i \mid\ \textstyle\prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}} \neq 0,\ 0 \le i \le p^m - 2 \right\} \\ &= \left\{\ i \mid\ i_a \in \left\{ \frac{p-1}{2}, \frac{p+1}{2}, \cdots, p-1 \right\},\ 0 \le i \le p^m - 2 \right\} \end{aligned} \tag{11}$$

- Without calculating $A_{-i}(0,1)$,

$$
\begin{aligned}
s_z^{(0,1)}(t) &= \frac{1}{2}\big(1-\chi(\alpha^t+1)\big) = \frac{1}{2}\left(1-(\alpha^t+1)^{\frac{p^m-1}{2}}\right) \\
&= \frac{1}{2}\left(1-(\alpha^t+1)^{\sum_{k=0}^{m-1}\frac{p-1}{2}p^k}\right) \\
&= \frac{1}{2}\left(1-\prod_{k=0}^{m-1}(\alpha^t+1)^{\frac{p-1}{2}p^k}\right) \\
&= \frac{1}{2}\left(1-\prod_{k=0}^{m-1}(a_0+a_1\alpha^t+\cdots+a_{\frac{p-1}{2}}\alpha^{\frac{p-1}{2}t})^{p^k}\right).
\end{aligned}
\tag{12}
$$

where $a_i = \binom{\frac{p-1}{2}}{i}$. Since the characteristic is p and $a_i \not\equiv 0 \pmod{p}$ we obtain the same linear complexity as (10) by just counting all the sum-terms.

- This indicates

$$
L_1(S) \le \left(\frac{p+1}{2}\right)^m - 1. \tag{13}
$$

Theorem 1 (main) *Let S be an S-LCE sequence of period $p^m - 1$, where p is an odd prime and m is a positive integer. Assume that m is even, or $p = 3$ and $m > 1$. Then*

$$L_1(S) = \left(\frac{p+1}{2}\right)^m - 1. \tag{14}$$

Table 1: Comparison of L_0 and L_1 when $p = 3$

m	L_0	L_1	n	$\frac{L_0}{n}(\%)$	$\frac{L_1}{n}(\%)$
2	7	3	8	87.5	37.5
4	73	15	80	91.3	18.8
6	697	63	728	95.7	8.7
8	6433	255	6560	98.1	3.9

Table 2: Comparison of L_0 and L_1 when $p = 5$

m	L_0	L_1	n	$\frac{L_0}{n}(\%)$	$\frac{L_1}{n}(\%)$
2	21	8	24	87.5	33.3
4	608	80	624	97.4	12.8
6	15501	728	15624	99.2	4.7
8	389248	6560	390624	99.6	1.7

◇ Proof of the theorem

- We will distinguish two cases for

$$A_{-i}(\tau,\lambda) = \frac{1}{p-1}\Bigg(-(-1)^i + \lambda(-\alpha^\tau)^i - (-1)^{i-\frac{p^m-1}{2}} \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}} \Bigg) \in F_{p^m}$$

as follows:

Case I . $\alpha^\tau \notin F_p$ and $\lambda \neq 0$

Case II. $\alpha^\tau \in F_p$

◇ Case I. $\alpha^{\tau} \notin F_p$ and $\lambda \neq 0$

- Since $A_{-i}(\tau, \lambda) \neq 0$ if $\alpha^{\tau i} \notin F_p$,

$$L(S_Z^{(\tau,\lambda)}) \geq \left| \left\{ \ i \mid \alpha^{\tau i} \notin F_p, \ 0 \leq i \leq p^m - 2 \ \right\} \right| \triangleq N. \tag{15}$$

- Since

$$N = (p^m - 1)\left(1 - \frac{1}{d}\right) \geq \frac{p^m - 1}{2} \geq \left(\frac{p+1}{2}\right)^m - 1 \tag{16}$$

  where d is the least positive integer such that $\alpha^{\tau d} \in F_p$,

- Therefore,

$$L(S_Z^{(\tau,\lambda)}) \geq \left(\frac{p+1}{2}\right)^m - 1. \tag{17}$$

◇ Case II. $\alpha^\tau \in F_p$

- When $C = \{\, i \mid A_{-i}(\tau,\lambda) = 0,\ 0 \le i \le n-1 \,\}$,

$$L(S_Z^{(\tau,\lambda)}) = n - |C|\,. \tag{18}$$

- Let $\beta = \alpha^\tau (\in F_p)$,

$$C = \left\{\, i \mid \ \prod_{a=0}^{m-1} \binom{i_a}{\frac{p-1}{2}} = (-1)^{\frac{p^m-1}{2}}(1-\lambda\beta^i),\ 0 \le i \le n-1 \,\right\}. \tag{19}$$

- Let e denote the order of β thus $e|(p-1)$. Then we can consider two subcases in terms of β as follows.

◇ When $\beta = 1$ (or $\tau \equiv 0 \pmod e$)

- $\lambda = 1$ yields the special case as

$$L\left(S_Z^{(0,1)}\right) = |I| = \left(\frac{p+1}{2}\right)^m - 1.$$

- Since $1-\lambda\beta^i \neq 0$ for any $\lambda \in F_p \setminus \{1\}$,

$$|C| \leq |I^c| = n - |I| = n + 1 - \left(\frac{p+1}{2}\right)^m. \tag{20}$$

- Thus,

$$\begin{aligned} L(S_Z^{(\tau,\lambda)}) &= n - |C| \\ &\geq \left(\frac{p+1}{2}\right)^m - 1. \end{aligned} \tag{21}$$

◇ When $\beta \neq 1$ (or $\tau \not\equiv 0 \pmod{e}$)

- If $\lambda = 0$, $S_Z^{(\tau,0)}$ = the S-LCE sequence S for any τ. Then,

$$|C| \leq |I^c| \quad \text{as (20)}$$

- If $\lambda \neq 0$,

$$|C| \leq \left|\{\, i \mid \ \beta^i = \lambda^{-1}\} \cap I^c\right| + \left|\{\, i \mid \ \beta^i \neq \lambda^{-1}\} \cap I\right|. \tag{22}$$

- Let u denote some integer such that $\lambda^{-1} = \beta^u$ and $0 \leq u \leq e$. If u does not exist,

$$|C| \leq |I| \leq |I^c|. \tag{23}$$

- Otherwise, if such u exists (22) becomes

$$\begin{aligned}|C| \leq & \left|\left\{ i \mid \sum_{a=0}^{m-1} i_a \equiv u \pmod e \right\} \cap I^c\right| \\ & + \left|\left\{ i \mid \sum_{a=0}^{m-1} i_a \not\equiv u \pmod e \right\} \cap I\right|\end{aligned} \tag{24}$$

since $i = \sum_{a=0}^{m-1} i_a p^a \equiv \sum_{a=0}^{m-1} i_a \pmod e$.

- Now the RHS of (24) can be upper bounded by $|I^c|$ when m is even: Let H denote

$$H = \left\{ i \mid i_a \in \left\{0, 1, \cdots, \frac{p-1}{2}\right\}, 0 \leq i \leq n-1,\ i \neq \frac{n}{2} \right\}. \tag{25}$$

Then

$$\left|\left\{ i \mid \sum_{a=0}^{m-1} i_a \not\equiv u \pmod e \right\} \cap I\right| = \left|\left\{ i \mid \sum_{a=0}^{m-1} i_a \not\equiv u \pmod e \right\} \cap H\right| \tag{26}$$

where $I = \left\{ i \mid i_a \in \left\{\frac{p-1}{2}, \frac{p+1}{2}, \cdots, p-1\right\},\ 0 \leq i \leq p^m - 2\right\}$, since

$$\begin{aligned}\sum_{a=0}^{m-1} i_a &= \sum_{a=0}^{m-1}\left(i_a - \frac{p-1}{2}\right) + \frac{m}{2}(p-1) \\ &\equiv \sum_{a=0}^{m-1}\left(i_a - \frac{p-1}{2}\right) \pmod{e}.\end{aligned} \tag{27}$$

- Since $H \subset I^c$, the second term of (24) is upper bounded by $|\{\ i \mid \sum_{a=0}^{m-1} i_a \not\equiv u \pmod{e}\} \cap I^c|$.

- When m is odd, we are only able to finish this case when $p = 3$.
  - $m = 1$ is the trivial case yielding $L_1(S)$=0.
  - if $m > 1$, we observe
$$|I| = 2^m - 1 \text{ and} |I^c| = 3^m - 2^m.$$
  - Assume $\beta = 2$ and $\lambda = 1$. Since $e = 2$,
$$\begin{aligned} |C| \leq & \left| \left\{ i \mid \sum_{a=0}^{m-1} i_a \equiv 0 \pmod 2 \right\} \cap I^c \right| \\ & + \left| \left\{ i \mid \sum_{a=0}^{m-1} i_a \equiv 1 \pmod 2 \right\} \cap I \right| . \end{aligned} \tag{28}$$
  - Let $N_0(X)$ (or $N_1(X)$) denote the number of zero (or one) $\pmod 2$ in a set of integers X. Then,
$$\begin{aligned} |C| \leq N_0(I^c) + N_1(I) = \frac{3^m + 1}{2} \\ \leq 3^m - 2^m = |I^c|. \end{aligned} \tag{29}$$

    Similarly, the same is true when $\beta = 2$ and $\lambda = 2$.

Conjecture

Conjecture 1 *Let S be an S-LCE sequence of period $p^m - 1$, where $p > 3$ is prime and $m \geq 1$, or $p = 3$ and $m > 1$. Then*

$$L_1(S) = \left(\frac{p+1}{2}\right)^m - 1. \tag{30}$$

$\Rightarrow$ it seems true in general for all odd prim p and $m \leq 1$ except the trivial case when $p = 3$ and $m = 1$.