How to Evaluate the Linear Complexity of Sequences

Yun-Pyo Hong, Yu-Chang Eun, Hong-Yeop Song

yphong@eve.yonsei.ac.kr

Oct. 13. 2001

Coding & Information Theory Lab.
Department of Electrical and Electronic Engineering, Yonsei Univ.

Contents

1. Introduction (1)

- Linear Complexity(LC) of a sequence
  ; The size of the shortest Linear Feedback Shift Register(LFSR) which can generate the sequence

  ⇒ The difficulty of generating or analyzing the sequence, from a few successively observed symbols

  ⇒ Important factor in the field of security (i.e. stream cipher systems, military frequency hopping communications, etc.)

1. Introduction (2)

- Assume that we observe $S = \{A\ D\ E\ C\ F\ B \cdots\}$ with 6 symbols, then we must decide the following three choices

1) Set of the symbols of S

$\Rightarrow$ Field $(GF(7), GF(8), GF(8), \cdots)$ or Integer residue ring $(Z_6, Z_7, Z_8, \cdots)$

2) Mapping method from a symbol to an element of the set

$\Rightarrow$ If the set is Z_6, there are 6! mapping methods

3) When the set is an extension field, Generator polynomial of the field

$\Rightarrow$ If the set is $GF(8)$, there are 2 generator polynomials

- After above three choices is decided, we can synthesize the characteristic polynomial of S
  - ✓ Over field by Berlekamp-Massey (BM) algorithm
  - ✓ Over integer residue ring by Reeds-Sloane (RS) algorithm

1. Introduction (3)

- It may be possible that the characteristic polynomial and therefore, the LC of S is changed, when one of the above three choices is changed

2. How to Evaluate the LC of Sequences (1)

- $S = \{s_n\}$: a sequence of non-negative integers

- Mapping method that we use to evaluate the LC of S
  - ✓ LC over Z_m

    ; $s_n \mapsto s_n$ (just an integer s_n, an element of Z_m)

  - ✓ LC over $GF(p^k)$

    ; $s_n \mapsto (v_1, v_2, \cdots, v_k)$ (p-ary k-tuple, an element of $GF(p^k)$)

    $$s_n = \sum_{i=1}^{k} v_n p^{k-i}$$

- We use
  - ✓ BM algorithm to evaluate LC of S over a field with characteristic 2
  - ✓ RS algorithm to evaluate LC of S over an integer residue ring and an odd prime field

2. How to Evaluate the LC of Sequences (2)

Example 1) S with period $64 = \{0\ 2\ 2\ 1\ 2\ 1\ 2\ 2\ 0\ 1\ 1\ 1\ 1\ 2\ 2\ 0\ 0\ 1\ 2\ 1\ 1\ 2\ 0\ 2\ 2\ 1\ 1\ 2\ 0$
$0\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 2\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 2\ 2\ 1\ 2\ 0\ 0\ 2\ 2\ 0\ 0\ 1\ 2 \cdots\}$

TABLE I

THE LINEAR COMPLEXITY OF S OF EXAMPLE 1.

Over	$GF(3)$	$GF(4)$	$GF(5)$	Z_6	$GF(7)$
LC	60	64	61	63	64

- LC of a sequence may be changed, when the set of the symbols of the sequence is changed

2. How to Evaluate the LC of Sequences (3)

- Mapping method is equivalent to a permutation of symbols of a sequence
  ⇒ Evaluate the distribution of the LC of a sequence for permutations of the symbols

Example 2) S with period $8 = \{0\ 1\ 3\ 7\ 6\ 5\ 2\ 4\ \cdots\}$

TABLE II

THE DISTRIBUTION OF THE LINEAR COMPLEXITY OF S OF EXAMPLE 2 OVER $GF(8)$.

LC	5	6	7
No. of sequences	2688	5376	32256

TABLE III

THE DISTRIBUTION OF THE LINEAR COMPLEXITY OF S OF EXAMPLE 2 OVER Z_8.

LC	2	3	4	5	6	7
No. of sequences	128	256	768	5888	14848	18432

- LC of a sequence may be changed, when the mapping method from a symbol of the sequence to an element of the set of the symbols is changed

2. How to Evaluate the LC of Sequences (4)

Example 3) S with period $64 = \{1\ 3\ 6\ 4\ 1\ 4\ 6\ 6\ 2\ 0\ 1\ 1\ 1\ 3\ 1\ 3\ 3\ 6\ 3\ 4\ 7\ 4\ 6\ 1\ 4\ 6\ 5\ 4\ 6$
$7\ 7\ 6\ 3\ 2\ 5\ 0\ 3\ 3\ 3\ 6\ 7\ 3\ 2\ 5\ 1\ 0\ 5\ 7\ 5\ 4\ 3\ 4\ 6\ 5\ 5\ 3\ 3\ 5\ 1\ 2\ 4\ 3\ 6 \cdots\}$

TABLE IV

THE LINEAR COMPLEXITY OF S OF EXAMPLE 3.

Over	$GF(8)$ with gen. poly. x^3+x^2+1	$GF(8)$ with gen. poly. x^3+x+1
LC	59	61

- LC of a sequence over an extension field may be changed, when the generator polynomial of the field is changed

$\because$ The change of the generator polynomial of an extension field is equivalent to the change of the mapping method from a symbol of a sequence to an element of the field

2. How to Evaluate the LC of Sequences (5)

- LC of a sequence should be evaluated, after the following three choices are decided

  1) Set of the symbols of a sequence

  2) Mapping method from a symbol to an element of the set

  3) When the set is an extension field, Generator polynomial of the field

Example 4) Two 16-ary random sequences of Figure 1 and Figure 2

Fig. 1. S_1 with period 255

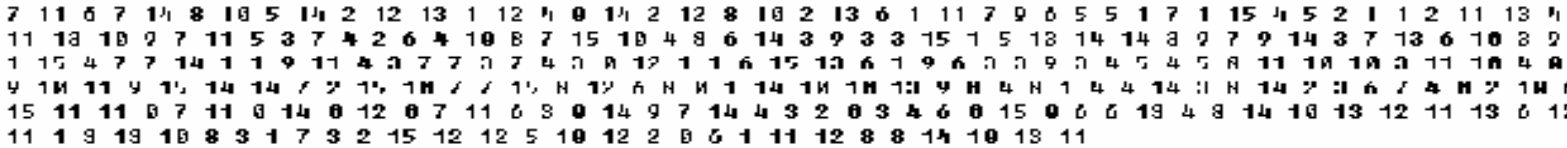

Fig. 2. S_2 with period 255

TABLE V

THE LINEAR COMPLEXITY OF TWO 16-ARY RANDOM SEQUENCES OF EXAMPLE 4 ($GF(16)_3$: $GF(16)$ WITH A GENERATOR POLYNOMIAL x^4+x+1, $GF(16)_9$: WITH x^4+x^3+1).

	Z_{16}	$GF(16)_3$	$GF(16)_9$	$GF(17)$	Z_{18}	$GF(19)$	Z_{20}
LC of S_1	255	253	253	255	254	254	255
LC of S_2	255	252	250	255	255	254	255

3. Construction of a Non-Binary sequence with Unique Linear Complexity Over Some Fields (1)

- $S = \{s_n\}$: a sequence of non-negative integers
  - ✓ k : positive integer
  - ✓ p : least prime, $p > Max[s_n]$

$\Rightarrow$ A new sequence $T = \{t_n\}$ from S

- ✓ $t_n = (s_n, s_{n+1}, \cdots, s_{n+k-1})$

- We regard
  - ✓ s_n as an integer (an element of $GF(p)$) in $GF(p)$
  - ✓ t_n as a p-ary k-tuple (an element of $GF(p^k)$) in $GF(p^k)$

Lemma 1 *The LFSR generating a sequence* $S = \{s_n\}$ *of non-negative integers over* $GF(p)$, *where* p *is the least prime that satisfies* $p > Max[s_n]$, *also generates* $T = \{t_n\}$, *where* $t_n = (s_n, s_{n+1}, \cdots, s_{n+k-1})$, *over* $GF(p^k)$.

Example 5) S with period 26 $= \{0\ 0\ 1\ 1\ 1\ 0\ 2\ 1\ 1\ 2\ 1\ 0\ 1\ 0\ 0\ 2\ 2\ 2\ 0\ 1\ 2\ 2\ 1\ 2\ 0\ 2\ 0\ 0$ $\cdots\}$

i) p=3, k=3

$T = \{001\ 011\ 111\ 110\ 102\ 021\ 211\ 112\ 121\ 210\ \cdots\}$

ii) p=3, k=4

$T = \{0011\ 0111\ 1110\ 1102\ 1021\ 0211\ 2112\ 1121\ 1210\ 2101\ \cdots\}$

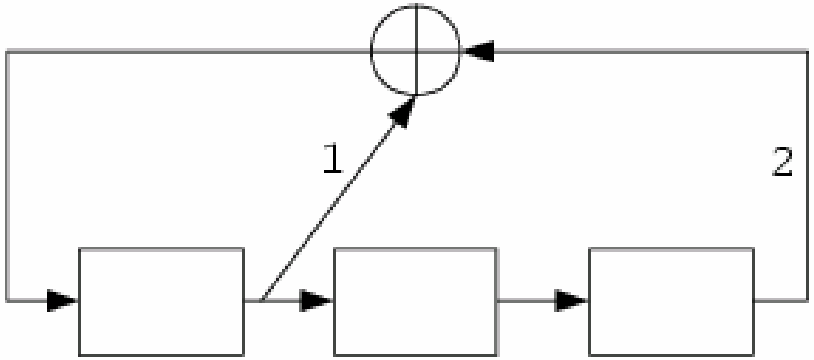

Fig. 3. The LFSR generating S and T of Example 5.

- From Lemma 1, the shortest LFSR generating S over $GF(p)$ also generates T over $GF(p^k)$
- It is not always the shortest LFSR generating T over $GF(p^k)$
- Furthermore, the linear complexity of T over $GF(p^k)$ cannot be uniquely determined unless a generator polynomial of $GF(p^k)$ is fixed

Example 6) The period of S is 63 and p=2.

i) $S = \{1\,1\,0\,0\,1\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,1\,0\,1\,0\,1\,0\,1\,1\,1\,0\,1\,1\,0$
$1\,1\,0\,1\,1\,1\,0\,1\,0\,0\,1\,1\,1\,1\,1\,1\,0\,0\,1\,0\cdots\}$

$\Rightarrow$ LC of S over $GF(2) = 62$,
But, LC of T (k=3) over $GF(2^3) = 60$ regardless of a generator polynomial

ii) $S = \{0\,1\,0\,1\,1\,1\,1\,1\,1\,0\,0\,1\,1\,0\,0\,0\,0\,0\,1\,1\,0\,1\,1\,1\,1\,1\,1\,0\,1\,0\,1\,0\,0\,1\,1\,1\,1\,1\,1\,0\,0\,0$
$1\,1\,0\,0\,1\,1\,1\,0\,1\,0\,0\,1\,0\,1\,0\,0\,1\,0\,1\,1\cdots\}$

$\Rightarrow$ LC of T (k=3) over $GF(2^3) = 55$ with a generator polynomial, $x^3 + x + 1$
But, LC of T (k=3) over $GF(2^3) = 53$ with a generator polynomial, $x^3 + x^2 + 1$

Fact 1 *The characteristic polynomial of* $G = \{g_n\}$ *over* $GF(q)$ *divides any connection polynomial of the LFSR generating* G *over* $GF(q)$.

Fact 2 *The characteristic polynomial of* $G = \{g_n\}$ *over* $GF(q)$ *is uniquely determined up to a multiplication by a constant.*

Theorem 1 *The shortest LFSR generating a binary sequence* $S = \{s_n\}$ *of integer 0 and 1 with period* 2^r *over* $GF(2)$ *is also the shortest LFSR generating a binary k-tuple sequence* $T = \{t_n\}$, *where* $t_n = (s_n, s_{n+1}, \cdots, s_{n+k-1})$, *over* $GF(2^k)$.

Theorem 2 *Let* $S = \{s_n\}$ *be a binary sequence of integer 0 and 1 with period* 2^r. *Then, The linear complexity of a binary k-tuple sequence* $T = \{t_n\}$, *where* $t_n = (s_n, s_{n+1}, \cdots, s_{n+k-1})$, *over* $GF(2^k)$ *is uniquely determined regardless of a choice of a generator polynomial of* $GF(2^k)$.

Example 7) A binary sequence S with period 16 $= \{0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0 \cdots\}$.

i) Binary 3-tuple sequence $T = \{000\ 000\ 001\ 010\ 101\ 011\ 111\ 111\ 111\ 111\ 110\ 101\ 010\ 100\ 000\ 000 \cdots\}$

ii) Binary 4-tuple sequence $T = \{0000\ 0001\ 0010\ 0101\ 1011\ 0111\ 1111\ 1111\ 1111\ 1110\ 1101\ 1010\ 0100\ 1000\ 0000\ 0000 \cdots\}$

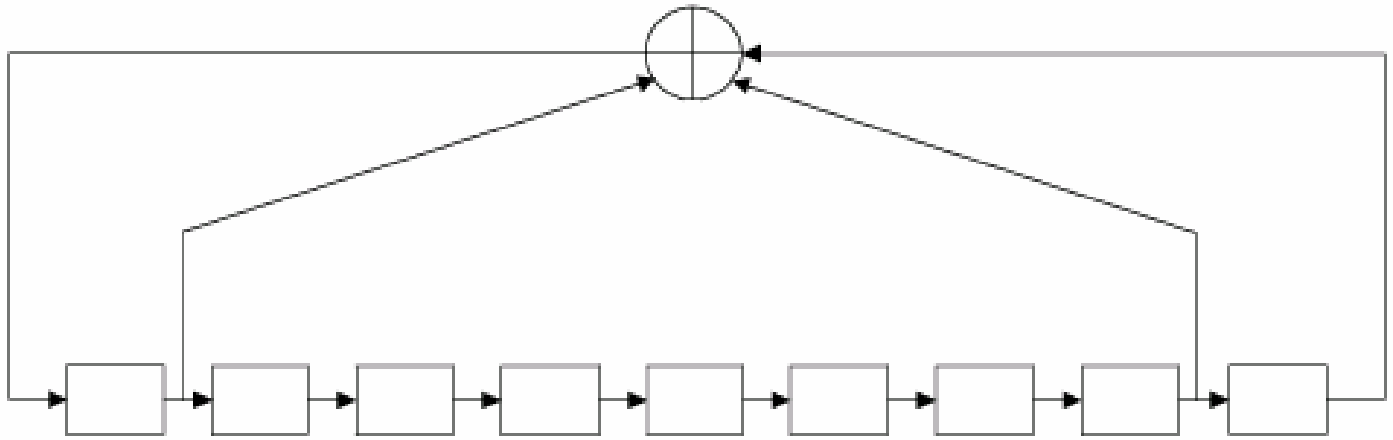

Fig. 4. The shortest LFSR generating S and T of Example 7.

♦ Theorem 1 and Theorem 2 is true when $GF(2^k)$ is $GF(2^m)$, where $m > k$

- The shortest LFSR generating a binary sequence $S = \{s_n\}$ of integer 0 and 1 with period 2^r over $GF(2)$ is also the shortest LFSR generating a binary k-tuple sequence $T = \{t_n\}$ over $GF(2^m)$, where $t_n = (s_n, s_{n+1}, \cdots, s_{n+k-1})$ and $m \geq k$

- LC of T over $GF(2^m)$ is uniquely determined regardless of a choice of a generator polynomial

4. Acknowledgement

- LC of a sequence should be evaluated, after the following three choices are decided
  1) Set of the symbols of a sequence
  2) Mapping method from a symbol to an element of the set
  3) When the set is an extension field, Generator polynomial of the field
- The shortest LFSR generating a binary sequence $S = \{s_n\}$ of integer 0 and 1 with period 2^r over $GF(2)$ is also the shortest LFSR generating a binary k-tuple sequence $T = \{t_n\}$ over $GF(2^m)$, where $t_n = (s_n, s_{n+1}, \cdots, s_{n+k-1})$ and $m \geq k$
- LC of T over $GF(2^m)$ is uniquely determined regardless of a choice of a generator polynomial

5. Reference

[1] J. L. Massey, “Shift-Register Synthesis and BCH decoding,” IEEE Trans. Inform. Theory, IT-15, pp. 122-127, Jan. 1969.

[2] J. A. Reed, N. J. A. Sloane, “Shift Register Synthesis (modulo m),” Siam J. Comp., vol. 14, no. 3, pp. 505-513, Aug. 1985.

[3] S. W. Golomb, “Shift Register Sequences,” Revised Edition, Aegean Park Press, 1982.

[4] A. H. Chan, R. A. Games, and E. L. Key, “On the Complexity of de Bruijn Sequences,” J. Comb. Theory, Ser. A, vol. 33, pp. 233-246, Nov. 1972.