Handout 2 - Linear complexity

Let $S = z_0, z_1, z_2, z_3, \ldots$ be a finite or infinite sequence. We say that the linear complexity LC(S) of S is the length of the shortest LFSR which generates it.

Linear complexity of a finite sequence does not decrease if new terms are added to the sequence, but it may remain the same.

<u>Examples 5.</u>

a) S = 000…01 (with n - 1 zeroes); LC(S) = n; one feedback polynomial of the LFSR is $x^n + 1$; indeed, any polynomial of degree n can be taken as feedback polynomial.

b) S = 111..10 (with n ones); LC(S) = n; one feedback polynomial of the LFSR is x^n+x+1; indeed, any polynomial of degree n with odd number of terms can be taken as feedback polynomial.

c) By example 3 (Handout 1), the linear complexity of 0111001011 is less than or equal to 3, since the polynomial f has degree 3. From b) above it follows that the linear complexity is exactly 3.

Handout 2 - Linear complexity

Theorem 4. Let LC(S) = L . Consider the LFSR of length L which generates the sequence S of length n (where n can be infinite). Then

a) The L subsequent states of the the LFSR are linearly independent.

b) The L + 1 subsequent states are linearly dependent.

c) If moreover, at least 2L terms of the sequence are given, that is, $n \geq 2L$, then the connection polynomial of the generating LFSR is uniquely determined (cf. Stinson: Section 1.2.5).

Proof. Let the connection coefficients be $c_0\, c_1\; c_2\; c_3\; . . . c_{L\text{-}1}$. Writing the recursion equation

$$z_{k+L} = c_0\, z_k + c_1\, z_{k+1} + c_2\, z_{k+2} + . . . + c_{L\text{-}1}\, z_{k+L\text{-}1}$$

in vector form we get

$$(c_0\; c_1\; c_2\; c_3\; . . . c_{L\text{-}1})\, \mathrm{Z} = (z_L\; z_{L+1}\; z_{L+2}\; z_{L+3}\; . . .\; z_{2L\text{-}1}) \qquad (*)$$

where the rows (and columns) of the matrix Z are vectors $(z_k\ z_{k+1}\ z_{k+2}\ z_{k+3}\ .\ .\ .\ z_{k+L-1})$, for $k = 0,1,\ldots,L - 1$. Claim b) follows immediately from this representation. Further, if L subsequent states are linearly dependent, the sequence satisfies a linear recursion relation of length (at most) L -1, and can be generated using a LFSR of length less than L . This gives a).

Finally, if at least $2L$ terms of the sequence are given, then the vectors

$$(z_k\ z_{k+1}\ z_{k+2}\ z_{k+3}\ .\ .\ .\ z_{k+L-1}),\quad k = 0,1,\ldots,L$$

that determine the columns of the matrix Z in equation (*) are known. By a), the matrix Z is invertible. This gives a unique solution for the tap constants $(c_0\ c_1\ c_2\ c_3\ .\ .\ .c_{L-1})$.

Handout 2 -- Linear Complexity

Now we know:

1. Any finite or periodic sequence has finite linear complexity. Linear complexity is less than or equal to the length of the sequence and less than the period of it.
2. If we know the linear complexity of the sequence we can compute the feedback polynomial. The feedback polynomial is unique if the length of the available sequence is at least twice the linear complexity.

Question:

How can we determine linear complexity for any sequence?

Answer:

Using Berlekamp-Massey Algorithm

Denote: $S = z_0, z_1, z_2, z_3, \ldots$

$S^{(k)} = z_0, z_1, z_2, \ldots, z_{k-1}$

$L_k = \mathrm{LC}(S^{(k)})$

$f^{(k)}(x) =$ polynomial of degree L_k such that $S^{(k)}$ can be generated using an LFSR with feedback polynomial $f^{(k)}(x)$

Then the "LC change lemma" holds:

Lemma. If LFSR with $f^{(k)}(x)$ does not generate $S^{(k+1)}$ then

$$L_{k+1} \geq \max\{L_k, k+1-L_k\}$$

Proof. $f^{(k)}(x)$ generates $S^{(k+1)} + \underbrace{00\ldots01}_{k+1}$, hence LC $(S^{(k+1)} + 00\ldots01) = L_k$.

Then

$k + 1 = \mathrm{LC}\,(00\ldots01) = \mathrm{LC}\,((S^{(k+1)} + 00\ldots01) + S^{(k+1)}) \leq$

$\mathrm{LC}\,(S^{(k+1)} + 00\ldots01) + \mathrm{LC}(S^{(k+1)}) = L_k + L_{k+1}$, from where the claim follows. □

Berlekamp-Massey: If $f^{(k)}(x)$ does not generate $S^{(k+1)}$ then

$$L_{k+1} = \max\{L_k, k+1- L_k\}$$

and

$$\boxed{f^{(k+1)}(x) = x^{L_{k+1}-L_k} f^{(k)}(x) + x^{L_{k+1}-k+m-L_m} f^{(m)}(x)}$$

where m is the largest index such that $L_m < L_k$. That is, m the previous index at which the linear complexity changed.

Notes: (1) BM algorithm may give feedback polynomials with $c_0 = 0$.

(2) Polynomial $f^{(k)}(x)$ is not unique unless degree of $f^{(k)}(x)$ is $\leq k/2$.

Example.

k	z_{k-1}	L_k	$f^{(k)}$
0		0	1
1	1	$k=1$	$x^k+1 = x+1$ (Example 5a)
2	1	1	$x+1$
3	0	2	$x(x+1)+1 = x^2+x+1$
4	0	2	x^2
5	1	3	x^3+x+1
6	0	3	x^3+x+1
7	1	3	x^3+x+1
8	1	3	x^3+x+1

initialisation

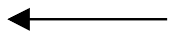
the first 1

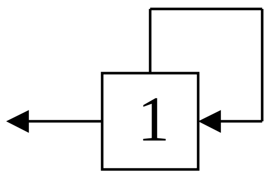
the first jump:
$k=2$, $L_k=1$
$k+1=3$, $L_{k+1}=2$
$m=0$, $L_m=0$

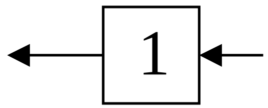
$$z_{k+m} = c_0 z_k + c_1 z_{k+1} + c_2 z_{k+2} + c_3 z_{k+3} + \ldots + c_{m-1} z_{k+m-1}$$

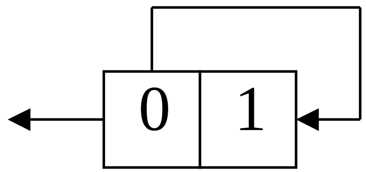
for all $k = 0,1,2,\ldots$

<u>Examples 1.</u>

a) $z_i = 0$, $i = 0,1,2,\ldots$ shortest LFSR:  (no contents, length = 0)

b) $z_i = 1$, $i = 0,1,2,\ldots$ shortest LFSR: 

or 

c) sequence 010101… ; shortest LFSR: 

(length $m = 2$)

$z_0 = 0$, $z_1 = 1$, $z_{k+2} = z_k$, $k = 0,1,2,\ldots$

d) sequence 000000100000010… LFSR: