Linear Complexity

Now we know:

1. Any finite or periodic sequence has a finite linear complexity. Linear complexity is less than or equal to the length and the period of the sequence.
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 as much as the linear complexity.

Question:

How can we determine the linear complexity for a sequence?

Answer:

Using Berlekamp-Massey Algorithm

Linear Complexity Change Lemma

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 $f^{(k)}(x)$

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 $S^{(k+1)} + \{00\ldots01\}$, that is, $S^{(k+1)}$ with the last bit flipped , hence $\mathrm{LC}(S^{(k+1)} + \underbrace{\{00\ldots01\}}_{k+1}) = L_k$. 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.

□

Linear Complexity: Berlekamp-Massey

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

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

and

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

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

Comments:

(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 $\leq k/2$.

Berlekamp-Massey Algorithm

k = number of terms observed

z_{k-1} = k^{th} term observed

1. Intialize $k = 0$, $L_k = 0$, $f^{(k)}(x) = 1$. If all $z_k = 0$, output $L = 0$, $f(x) = 1$.
2. Else, set r to be the least index such that $z_{r-1} = 1$. Then set $m = r - 1$, $L_m = 0$, $f^{(m)}(x) = 1$, and set $L_r = r$, $f^{(r)}(x) = 1 + x^r$.
3. Set $k = r$.
4. Check if $f^{(k)}(x)$ generates z_k from the preceeding terms of the sequence. If yes, set $f^{(k+1)}(x) = f^{(k)}(x)$ and $L_{k+1} = L_k$.
5. Else use Berlekamp-Massey theorem to compute L_{k+1} and $f^{(k+1)}(x)$. If $L_{k+1} > L_k$ set $m = k$, $L_m = L_k$ and $f^{(m)}(x) = f^{(k)}(x)$.
6. If z_k the last term, output $f(x) = f^{(k+1)}(x)$ and $L = L_{k+1}$.
7. Else set $k = k+1$, and go to 4.

Berlekamp-Massey: Example

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

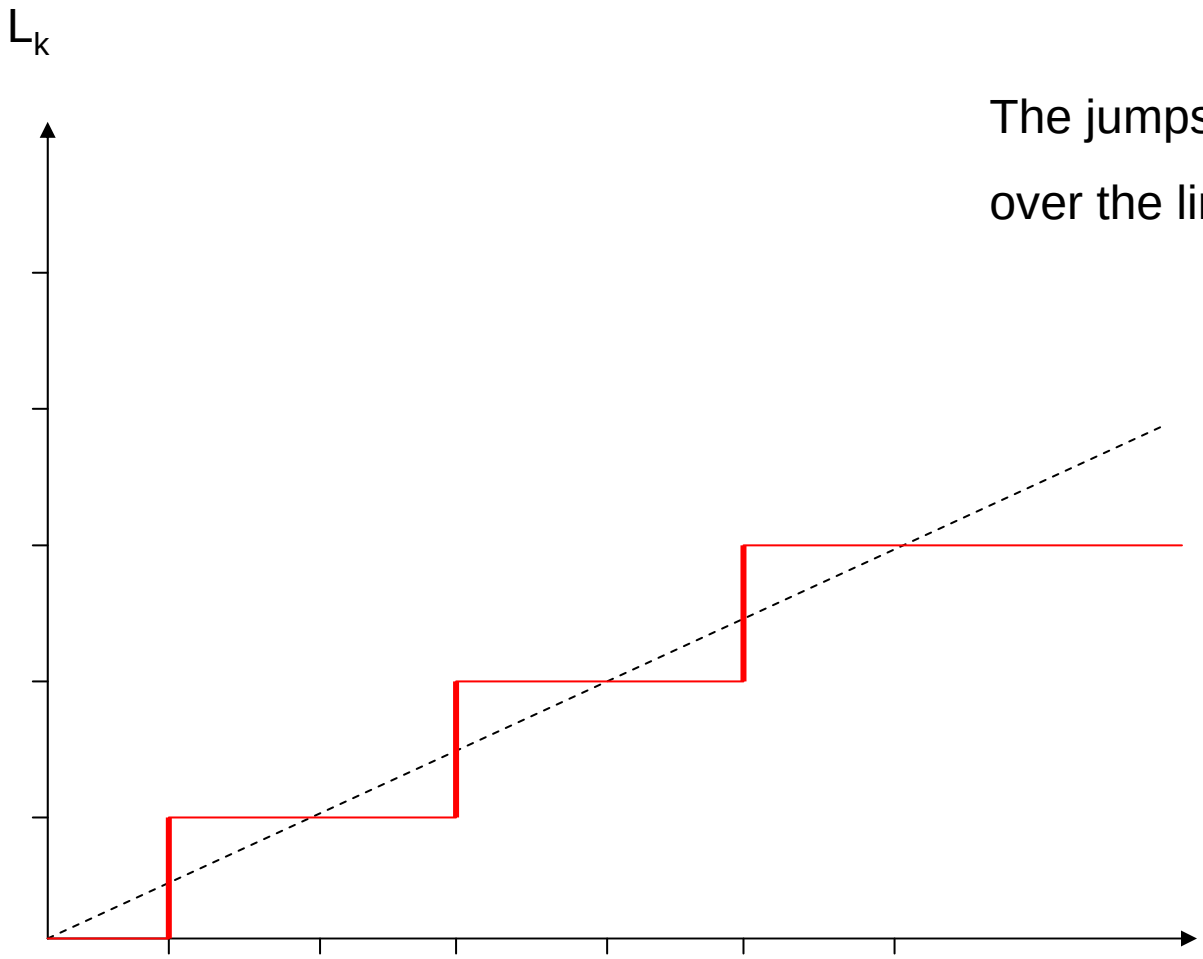
initialisation

the first index such that $z_{r-1}=1$

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

a jump:
k=4, L_k =2
m=2, L_m =1
k+1=5, L_{k+1}=3

LC profile



The jumps are symmetric

over the line $L_k = k/2$