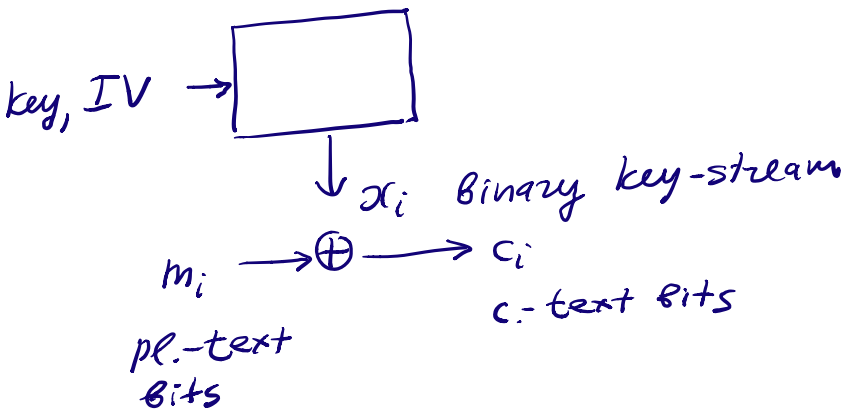
Linear Complexity of Binary sequences and Berlekamp-Massey Algorithm.

motivation

stream cipher



known pl-text attack

$c_0 \dots c_{N-1}\ c_N\ c_{N+1} \dots$

$m_0 \dots m_{N-1}$ | $m_N\ m_{N+1}$ unknown

$x_0 \dots x_{N-1}\ \underbrace{x_N\ x_{N+1} \dots}_{\text{predict (find, compute)}}$

$\Rightarrow$ decrypt the rest of the pl.-text $m_N\ m_{N+1} \dots$

can be done efficiently if the key-stream is of a low linear complexity.
(by Berlekamp-Massey Algorithm).

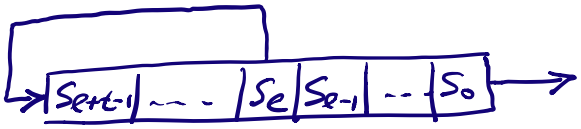
Linear Complexity

Binary sequence

$$s = \underbrace{s_0 \dots s_{e-1}}_{\text{tail}}\ \underbrace{s_e s_{e+1} \dots s_{e+t-1}}_{\text{period}}\ \underbrace{s_e s_{e+1} \dots s_{e+t-1}}\ \dots$$

ultimately periodic

construct an LFSR to generate S.



generating polynomial for LFSR:

$$X^{l+t} + X^{l}$$

if it is possible to construct a shorter LFSR?

Definition non-zero sequence S

1) S finite sequence of length n denoted $S^n = s_0 s_1 \dots s_{n-1}$
2) S infinite but ultimately periodic

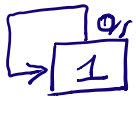
$L(S)$ linear complexity = length of the shortest LFSR that generates S.

By agreement 1) $S^0 = \emptyset$, $L(S^0) = 0$
generating polynomial is 1.

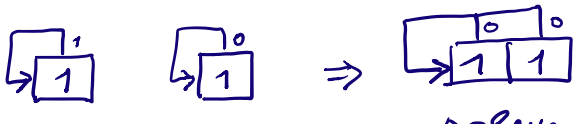
2) S all 0-sequence (finite or infinite)

$L(S) = 0$, generating polynomial is 1.

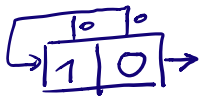
Examples.

$S^n = 10\dots0$  gen. pol. is $X + \underline{0}\cdot 1 = X$

$\Rightarrow L(10\dots0) = 1$.

$S^n = \underline{11}0\dots0$ 

polyn. is $X^2 + 0\cdot X + 0\cdot 1 = X^2$

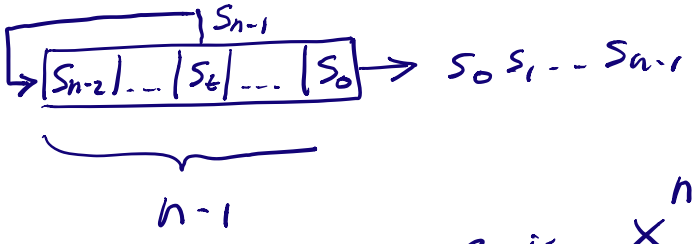
$s^n = 010\ldots0$  gen. pol. is x^2

Lemma. $L(s^n) = n \iff s^n = \underbrace{0\ldots0}_{n-1}1$

Proof. $\Rightarrow$ assume $L(s^n) = n$

$s^n = s_0 s_1 \ldots s_{n-1} \neq 0\ldots01$

$t < n-1$ s.t. $s_t = 1$

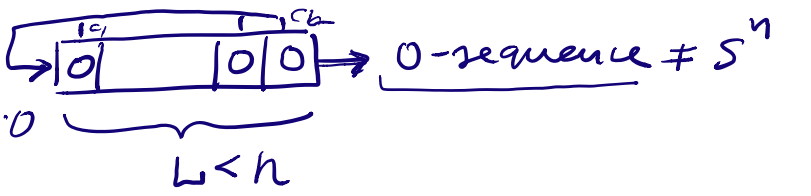


gen. polynomial is $x^{n-1} + s_{n-1}x^t$

contradiction

$\Leftarrow$ assume $s^n = \underbrace{0\ldots0}_{n-1}1$

if $L = L(s^n) < n$



$0 = c_1 \cdot 0 + \ldots + c_{L-1} 0 + c_L 0$ $\quad L < n$

contradiction.

$s^n = s_0 s_1 \ldots s_{n-1}$ $\quad L_1 = L(s^n)$

$t^n = t_0 t_1 \ldots t_{n-1}$ $\quad L_2 = L(t^n)$

$s^n + t^n = s_0 + t_0, s_1 + t_1, \ldots, s_{n-1} + t_{n-1}$ (+ : XOR)

$L(s^n + t^n) = ? \leq L_1 + L_2$.

some notation

$s = s_0 s_1 s_2 \ldots$ infinite

shifts of s

$s^{(0)} = s_0 s_1 s_2 \ldots$

$s^{(1)} = s_1 s_2 s_3 \ldots$

$\ldots$

$s^{(i)} = s_i s_{i+1} s_{i+2} \ldots$

$\ldots$

polynomial

$$R(x) = d_0 x^M + d_1 x^{M-1} + \ldots + d_M$$

$(d_0 = 1)$

define action of $R(x)$ on s

$$R(s) = \sum_{i=0}^{M} d_{M-i}\, s^{(i)}$$ infinite sequence.

linear combination of shifts $s^{(0)}, \ldots, s^{(M)}$.

e.g. $R(x) = 1$ $\quad R(s) = s^{(0)} = s$

$R(x) = x$ $\quad R(s) = s^{(1)}$

$R(x) = x^2$ $\quad R(s) = s^{(2)}$

$\ldots$

Lemma. $R(x)$ is a generating polynomial for s $\Leftrightarrow$ $R(s) = 0$-sequence.

$R(x) = 1 \cdot x^M + d_1 x^{M-1} + \ldots + d_M$

Proof.

$d_M \quad s^{(0)} = s_0\ s_1\ s_2 \ldots$

$d_{M-i} \quad s^{(1)} = s_1\ s_2\ s_3 \ldots$

$d_1 \quad s^{(M-1)} = s_{M-1}\ s_M\ s_{M+1} \ldots$

$1 = d_0 \quad s^{(M)} = s_M\ s_{M+1}\ s_{M+2} \ldots$

$R(S) = 0\ 0\ 0 \ldots$

$$S_M = d_1 \cdot S_{M-1} + \ldots + d_{M-1} S_1 + d_M \cdot S_0$$
$$S_{M+1} = d_1 S_M + \ldots + d_{M-1} S_2 + d_M S_1$$
$$\ldots$$

linear recurrence defined by $R(x)$ $\Leftrightarrow$ $R(x)$ generating polynomial for S.

Theorem S, t infinite sequences

1. $R(x)$ any polynomial, then
$R(S+t) = R(S) + R(t)$
(+ = xor)

2. R, g any polynomials, then
$(R+g)(S) = R(S) + g(S)$

3. $(R \cdot g)(S) = R(g(S))$

without proof.

Corollary. S, t infinite sequences with generating polynomials $f(x)$ and $g(x)$ respectively.

Then $f \cdot g$ is generating pol. for $S+t$.

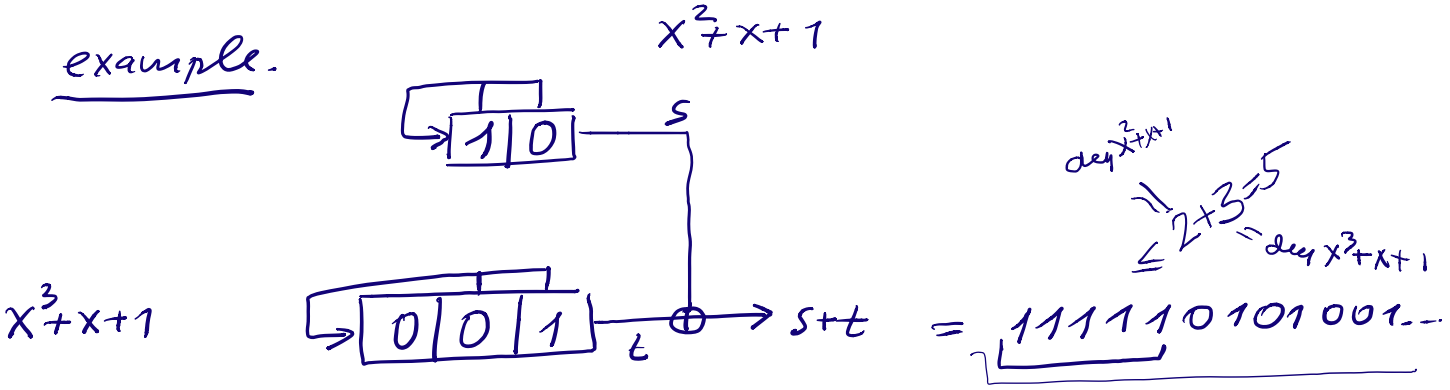
Proof. $(f \cdot g)(S+t) = (fg)(S) + (fg)(t) =$ (by Theorem)

$= g(f(S)) + f(g(t)) = g(0\text{-seq}) + f(0\text{-seq}) = 0\text{-seq}.$

0-seq. 0-seq

$\Rightarrow$ by Lemma p.g is a generating pol. for $s+t$.

example.

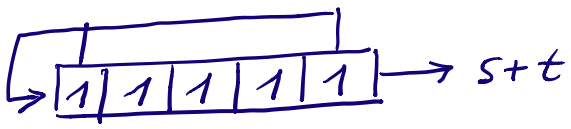


construct LFSR to generate $s+t$.

$s+t$ is generated by

$$(x^2+x+1)(x^3+x+1) = x^5+x^4+1$$

LFSR :



Corollary. s^n, t^n non-zero

$$\Rightarrow L(s^n+t^n) \leq L(s^n)+L(t^n)$$

Proof. s^n gen. by pol. $f(x)$ of degree $L(s^n)$

t^n $g(x)$ $L(t^n)$

S expansion of s^n with $f(x)$

t t^n $g(x)$

f.g generating pol. for $s+t$

s^n+t^n interval of $s+t$

$\Rightarrow$ f.g gen. for s^n+t^n

$$L(s^n + t^n) \leq \deg f + \deg g = L(s^n) + L(t^n).$$

e.g. $L(s^n + s^n) = L(0^n) = 0 < L(s^n) + L(s^n)$.

Corollary s infinite sequence (non-zero)

$f(x)$ gen. polynomial of smallest degree ≥ 1.

$g(x)$ any gen. polyn.

Then. $f(x) \mid g(x)$.

Proof. divide $g(x)$ by $f(x)$ with remainder

$$g(x) = h(x) \cdot f(x) + g_1(x)$$

$$\deg g_1(x) < \deg f(x).$$

assume $g_1(x) \neq 0$-polyn.

$f(x)$ gen. for s. $\Rightarrow$ 0-seq. as

$$g(s) = (h \cdot f + g_1)(s) = h(f(s)) + g_1(s)$$

$g(s)$: 0-seq.; $h(f(s))$: 0-seq.

$\uparrow$ By Theorem.

$\Rightarrow g_1(s) = 0$-sequence $\Rightarrow$ $g_1(x)$ gen. polyn. By Lemma.

Contradiction with $f(x)$ gen. pol. of smallest degree.

This statement is not correct for finite sequences.

Linear Complexity Profile.

$S = s_0 s_1 \ldots$

$s^N = s_0 s_1 \ldots s_{N-1}$ $\quad L_N = L(s^N)$

$f_N(x)$ gen. polyn. of degree L_N for s^N.

sequence of integers

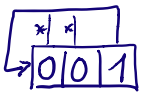
$L_0, L_1, L_2 \ldots$

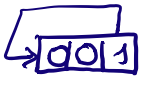
linear complexity profile for S.

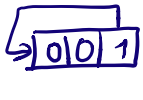
Example. $s^{10} = 1001001111$

construct lin. compl. profile for s^{10}

N	s^N	f_N	L_N
0	$\emptyset$	1	0
1	1	$x, x+1$	1
2	10	x	1
3	100	x	1
4	1001	$x^3+1,\ x^3+x+1,\ x^3+x^2+1,$ x^3+x^2+x+1	3
5	10010	$x^3+1,\ x^3+x+1$	3
6	100100	x^3+1	3
7	1001001	x^3+1	3
8	10010011	?	?







reg. length 8

$4, 5 \to 2^5 = 32$

$2^4 = 16$