Time Complexity of Berlekamp-Massey Algorithm.

$S^N = s_0 s_1 \dots s_{N-1}$

BM finds $L_N = L(S^N)$ and $f_N(x)$

Number of bit operations.

$S^i = s_0 s_1 \dots s_{i-1}$ $\quad f_i(x)$

$S^{i+1} = s_0 s_1 \dots s_{i-1} s_i$ $\quad f_{i+1}(x) = ?$

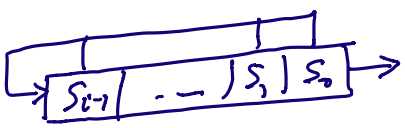
two cases

$f_{i+1} = f_i \quad (d_i = 0)$

$$f_{i+1} = \begin{cases} f_i + x^{2-L_i-i-1} \cdot f_m, & L_i > i/2 \\ x^{i+1-2L_i} \cdot f_i + f_m, & L_i \le i/2 \end{cases}$$

m largest s.t. $L_m < L_i$. $(d_i = 1)$

$L_i \le i$ $\Longleftarrow$



add polynomials of degree $\le i+1$

costs $\le i+2$ XORs

$1 \le i \le N-1$

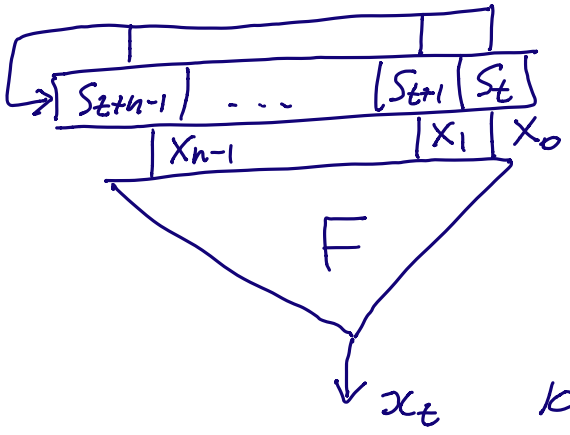
overall cost is $\sum_{i=1}^{N-1} i+2 =$

$$= \sum_{i=1}^{N-1} i + 2\cdot(N-1) = \frac{(N-1)N}{2} + 2\cdot(N-1) \approx \underline{\frac{N^2}{2}}$$

Asymptotically fast BM Algorithm

$O(N \cdot \log^{2+\varepsilon} N)$ ε small.

Linear Complexity of Filter Generator.



$f(X) = X^n + c_1 X^{n-1} + \cdots + c_n$

$x = x_0 x_1 \cdots$ $L(x)$?

One needs $2 \cdot L(x)$ key-stream bits to apply BM Algorithm to find generating polynomial for x. and then predict the rest of the key-stream.

Theorem $F(X_{n-1} \cdots X_0)$ is of algebraic degree d. Then

$$L(x) \leq D = \sum_{i=0}^{d} \binom{n}{i} \approx n^{d/2}$$

(e.g. if $d=2$ $\Rightarrow$ $L(x) \leq 1 + \binom{n}{1} + \binom{n}{2} = 1 + n + \frac{n(n-1)}{2}$.)

Proof.

LFSR current state at time $t = 0, 1, \ldots$

$$s(t) = (s_{n-1} \cdots s_1 s_0) = (s_{n-1}(t) \cdots s_1(t) s_0(t))$$

s_1: skip (t)

LFSR initial state is $s(0)$.

Monomial state.

$S(t)$ vector of length D

entries are products (monomials) of $s(t) = (s_{n-1} \cdots s_1 s_0)$ of degree $\leq d$.

order the entries according to a total monomial ordering

$$S(t) = (1, \underbrace{s_{n-1}, \ldots, s_1, s_0}, \underbrace{s_{n-1}s_0, \ldots, s_1 s_0}, \ldots \underbrace{s_{n-1}s_{n-2}\cdots s_{n-d}})$$

1: monomial of degree 0; $s_{n-1}, \ldots, s_1, s_0$: degree 1; $s_{n-1}s_0, \ldots, s_1 s_0$: degree 2; $s_{n-1}s_{n-2}\cdots s_{n-d}$: degree d

$$D = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{d}$$

$$F(X_{n-1}, \ldots, X_0) = \sum_{\substack{\{i_1 i_2 \cdots i_t\} \subseteq \{n-1, \ldots, 0\} \\ t \leq d}} b_{(i_1 i_2 \cdots i_t)} X_{i_1} \cdot X_{i_2} \cdots X_{i_t}$$

$t \leq d$: $\deg F \leq d$.

if $F(0 \ldots 0) = 0$

$$B_F = (\underbrace{b_\emptyset}_{=0}, \underbrace{b_{(n-1)}, \dots, b_{(0)}}, \underbrace{b_{(n-1,0)} \cdots b_{(1,0)}}, \dots \underbrace{\quad\quad})$$

coeff. at 1 — coeff. at x_i — coef. at $x_i x_j$ — coeff. at $x_{i_1} x_{i_2} \cdots x_{i_d}$

$$D = 1 + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{d}$$

Represent key-stream

$$x_t = F(S_{n-1}(t), \dots, S_1(t), S_0(t)) =$$

$$= \underbrace{S(t) \cdot B_F}_{\text{row} \quad \text{column}} = (1, *, \dots, *) \begin{pmatrix} 0 \\ * \\ \vdots \\ * \end{pmatrix}$$

$S(t)$ current monomial state

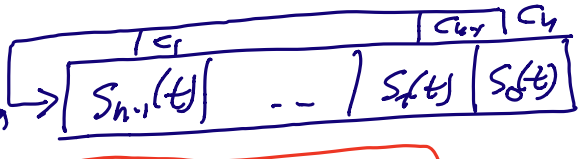
$S(t+1)$ next monomial state

$S(t) \longrightarrow S(t+1)$

linear transform

$$S_i(t+1) = S_{i+1}(t) \qquad i = 0, \dots, n-2$$

$$S_{n-1}(t+1) = c_1 S_{n-1}(t) + \dots + c_n S_0(t)$$



$$\Rightarrow \quad \boxed{S(t+1) = S(t) \cdot R}$$

of size 1])

R is $D \times D$ - matrix.

$$S(t) = S(0) \cdot R^t$$

$$\Rightarrow \boxed{x_t = S(t) \cdot B_F = S(0) \cdot R^t \cdot B_F}$$

$$G(X) = \sum_{i=0}^{D} a_i X^{D-i}, \quad a_0 = 1$$

characteristic polynomial of R.

$G(R) = 0$-matrix.

We construct a recurrence for x_t ($t \geq D$)

$$\sum_{i=0}^{D} a_i x_{t-i} = \sum_{i=0}^{D} a_i \underbrace{S(0) \cdot R^{t-i} \cdot B_F}_{x_{t-i}} =$$

(a_i: user (GA); x_{t-i}: key-stream bits)

$$= S(0) \cdot R^{t-D} \left(\sum_{i=0}^{D} a_i R^{D-i} \right) \cdot B_F$$

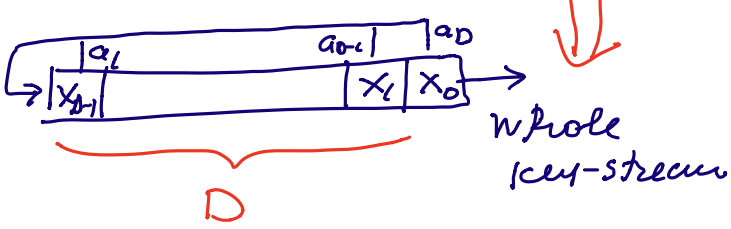
$G(R) = 0$-matrix

$$= 0$$

as $a_0 = 1$

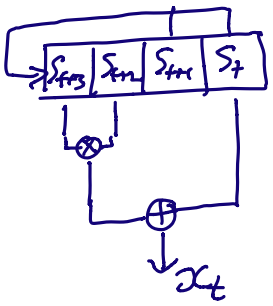
$$x_t = a_1 \cdot x_{t-1} + \dots + a_D \cdot x_{t-D}, \quad t \geq D$$

construct LFSR



$\Rightarrow L(x) \leq D$.

Example.



$X^4 + X + 1 = f(x)$

$s(t) = (s_3 s_2 s_1 s_0) = (s_3(t), s_2(t), s_1(t), s_0(t))$

$F(x_3 x_2 x_1 x_0)$ of alg. degree 2.

monomial state of degree 2.

$$S(t) = (\underbrace{1}, \underbrace{s_3, s_2, s_1, s_0}, \underbrace{s_3 s_0, s_3 s_1, s_3 s_2, s_2 s_0, s_2 s_1, s_1 s_0})$$

$$1 + \binom{4}{1} + \binom{4}{2} = D = 11.$$

$$S(t+1) = (1, s_0+s_1, s_3, s_2, s_1, (s_0+s_1)-s_1, (s_0+s_1)s_2, (s_0+s_2)s_3, s_3 s_1, s_3 s_2, s_2 s_1) =$$

$$= (1, s_0+s_1, s_3, s_2, s_1, s_0 s_1 + s_1, s_0 s_2 + s_1 s_2, s_0 s_3 + s_1 s_3, s_3 s_1, s_3 s_2, s_2 s_1)$$

$$S(t+1) = S(t) \cdot R$$

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \vdots & & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}_{11\times 11}$$

char. polynomial of R :

$$X^{11}+X^{10}+X^9+X^8+X^6+X^4+X^3+1$$

$$\Rightarrow L(x) \leq 11.$$

$$= (X+1)(X^4+X+1)(X^6+X^4+X^3+X^2+1)$$

as $F(0000) = 0$

key-stream may be generated by $X^{10}+X^8+X^5+X^4+X^2+X+1$

Construct LFSR