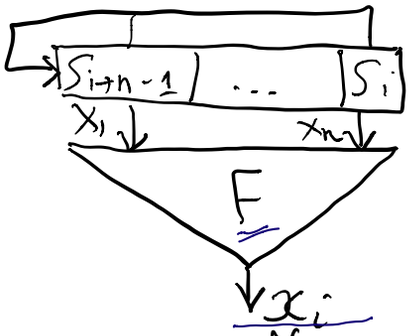
1. Problem
2. How to construct a linearized equation system
3. Example
4. How to solve lin. equation systems
5. Example



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

$\deg F = 2$

$N = 491$

given $x^N = x_0 \dots x_{N-1}$

find LFSR initial state $S_0 = (s_{n-1} \dots s_1 s_0)$

(*) $x_i = F(S_0 A^i)$ $i = 0 \dots N-1$

where A "companion" matrix for $f(x)$

$$A = \begin{pmatrix} c_1 & 1 & & \\ \dots & & \ddots & \\ & & & \ddots \\ c_{n-1} & & & 1 \\ c_n & & & \end{pmatrix}$$

2. fix ordering on the variables

$$\underbrace{S_{n-1} \cdots S_1 S_0}_{1 \qquad n-1 \; n}$$

monomial ordering

$1, 2, \ldots, n, 12, 13, \ldots, 1n, 23, 24, \ldots, n-1\,n$

monomial state

$$\bar{S}_0 = (\overbrace{S_{n-1}, \ldots, S_1, S_0}^{1 \qquad n-1 \; n}, \overbrace{S_{n-1}S_{n-2}}^{12}, \overbrace{S_{n-1}S_{n-3}}^{13}, \ldots, \overbrace{S_{n-1}S_0}^{1n}, \overbrace{S_{n-2}S_{n-3}}^{23}, \ldots)$$

vector of length $n + \frac{n(n-1)}{2} = m$

Boolean function. Assume $F(0\ldots0) = 0$

ANF $\quad F = F_1 X_1 + \ldots + F_n X_n + F_{12} X_1 X_2 + \ldots + F_{n-1\,n} X_{n-1} X_n$

coefficient vector

$$F = (F_1, \ldots, F_n, F_{12}, \ldots, F_{n-1\,n})$$

column vector

Then $\quad x_0 = \bar{S}_0 \cdot F = F_1 \cdot S_{n-1} + \ldots + F_n \cdot S_0 + F_{12} \cdot S_{n-1} S_{n-2} + \cdots$

Similarly, $x_1 = \bar{S}_1 \cdot F = F_1 \cdot S_n + \ldots + F_n \cdot S_1 + F_{12} \cdot S_n \cdot S_{n-1} + \cdots$

($\bar{S}_1$ monomial state after one LFSR clock)

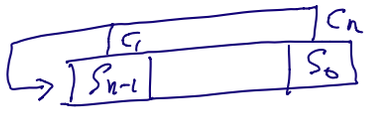
Find $m \times m$ matrix U s.t. $\quad \bar{S}_1 = \bar{S}_0 \cdot U$

$x_i = \bar{S}_i \cdot F$, $0 \le i \le N-1$.

By definition

$$\bar{S}_1 = (S_n, \ldots S_2, S_1, S_n S_{n-1}, \ldots, S_n S_1, S_{n-1} S_{n-2}, \ldots, S_2 S_1)$$

LFSR state after 1 clock.



$$s_n = c_1 \cdot s_{n-1} + \dots + c_n s_0$$

Then $\bar{S}_1 = (\underbrace{c_1 s_{n-1} + \dots + c_n s_0}_{=s_n}, s_{n-1}, \dots, s_1, \underbrace{(c_1 s_{n-1} + \dots + c_n s_0)}_{=s_n} s_{n-1}, \dots$

expand and simplify

$s_i^2 = s_i$ as $s_i \in \{0,1\}$

thus we construct the matrix U as $\bar{S}_1$ is a lin. f. of $\bar{S}_0$

$(*)$ may be written

$$\begin{cases} x_0 = \bar{S}_0 \cdot F \\ x_1 = \bar{S}_0 \cdot U \cdot F \\ \dots \\ x_{N-1} = \bar{S}_0 U^{N-1} \cdot F \end{cases}$$

$s_{n-1} \dots s_1 s_0$: $s_i \cdot s_0$

$0 \dots 0 1$: 1

Into a matrix form. Denote

$$V = (F, U \cdot F, \dots, U^{N-1} F)$$

$M \times N$-matrix

the system is now written as

$$\bar{S}_0 \cdot V = (x_0 \dots x_{N-1})$$

columns of V are known

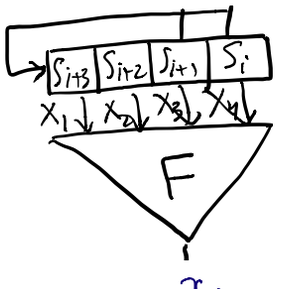
$x_0 \dots x_{N-1}$ known

system of N lin. equations in M variables

find $\bar{S}_0$ $\Rightarrow$ deduce S_0

3. Example (LN Section 2.10.1)

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



$F(x_1, x_2, x_3, x_4) = x_1 + x_2 + x_1 x_4$

x_3 irrelevant

$\downarrow x_i$

given $x^{10} = 0\,1\,1\,0\,0\,0\,1\,0\,1\,1$

find $S_0 = (S_3, S_2, S_1, S_0)$ — $1\ 2\ 3\ 4$

ordering $S_3\ S_2\ S_1\ S_0$

monomial state — deg 1 | deg 2 | deg 3 | deg 4 — $m = 4 + \binom{4}{2} = 10$

$\overline{S_0} = (S_3, S_2, S_1, S_0, S_3S_2, S_3S_1, S_3S_0, S_2S_1, S_2S_0, S_1S_0)$

matrix U

$\overline{S_1} = (S_4, S_3S_4, S_2S_4, S_1S_4, S_3S_2, S_3S_1, S_2S_1) =$

$S_4 = S_1 + S_0$ — S_4: 1 | S_2 | S_1 | S_0

$= (S_1 + S_0, S_3S_2S_1, S_3S_1 + S_3S_0, S_2S_1 + S_2S_0, S_1 + S_1S_0, S_3S_2, S_3S_1, S_2S_1)$

$S_1^2 = S_1$

matrix U s.t. $\overline{S_1} = S_0 \cdot U$

$m = 10$

$$U = \begin{array}{c|cccc|cccccc} & & & & & S_3 & S_2 & S_1 & S_0 & S_3S_2 & \cdots \\ \hline S_3 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\ S_2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \\ S_1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \\ S_0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \\ \hline S_3S_2 & & & & & 0 & 0 & 0 & 1 & 0 & 0 \\ S_3S_1 & & & & & 1 & 0 & 0 & 0 & 1 & 0 \\ \vdots & & & & & 1 & 0 & 0 & 0 & 0 & 0 \\ & & & & & 0 & 1 & 0 & 0 & 0 & 1 \\ & & & & & 0 & 1 & 0 & 0 & 0 & 0 \\ S_1S_0 & & & & & 0 & 0 & 1 & 0 & 0 & 0 \end{array}$$

Boolean function

$F = (1\,1\,0\,0\,0\,0\,1\,0\,0\,0)$ — $1\ 2\ 3\ 4\ 12\ 13\ 14\ 23\ 24\ 34$

$= X_1 + X_2 + X_1X_4$

Construct columns

$$V = (F, U\cdot F, \ldots, U^{9}\cdot F)$$

10×10

$$= \begin{pmatrix} 1 & 1 & & 1 \\ 1 & 0 & & 0 \\ 0 & 0 & & 1 \\ 0 & 1 & & 1 \\ 0 & 0 & & 1 \\ 0 & 0 & & 0 \\ 1 & 0 & & 1 \\ 0 & 0 & & 1 \\ 0 & 0 & & 0 \\ 0 & 1 & \cdots & 1 \end{pmatrix}$$

$N = 491$

$m = 496$

solution $\geq 2^{m-N} = 2^{5} = 32$

Solve $\overline{S_0}\, V = x^{10}$ ← key-stream.

a system of 10 linear equations in 10 variables

solution $\overline{S_0} = (\underbrace{0001}_{S_0}000000)$

Answer $S_0 = (0001)$

4. How to solve linear equations modulo 2

notation

A $m \times n$-matrix with entries $0, 1$

a column n-vector

x column n-vector of unknowns

$x = (x_1, \ldots, x_n)$

solve (find all solutions)

$$A \cdot X = a$$

A_i — i-th row of A

A_{ij} — (i,j)-entry of A

definition

A is in a row echelon form if

$0 \le r \le n$ and numbers

$$0 = t_0 < t_1 < t_2 < \dots < t_r < t_{r+1} = n+1$$

s.t. 1) $A_{ij} = 0 \quad 1 \le j < t_i$

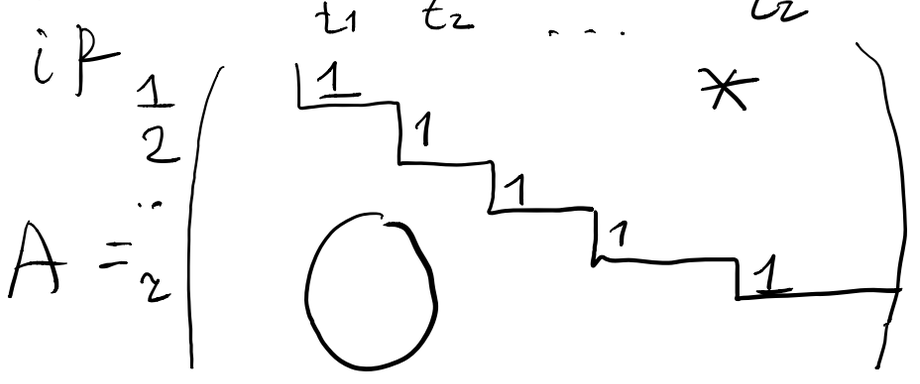
$A_{i t_i} = 1$

2) $A_{ij} = 0 \quad r+1 \le i \le m$

$1 \le j \le n$

matrix A is in a row echelon form

if



$r = \operatorname{rank}(A)$

Solving Algorithm

1. Augment A with column a and get

$$M = A_1 a$$

$m \times (n+1)$ - matrix

2. Reduce M to a row echelon form (in the first n columns)

2.1 initialize $r = 0$, $t_r = 0$

2.2. For j from $t_r + 1$ to n do
For i from $r+1$ to m do

(a) if $M_{ij} = 1$ then

$$M_{r+1} \longleftrightarrow M_i$$

For u from $r+2$ to m do

$$M_u \leftarrow M_u + M_{uj} \cdot M_{r+1}$$

Break j and i - loops

(B) if $M_{ij} = 0$, then continue

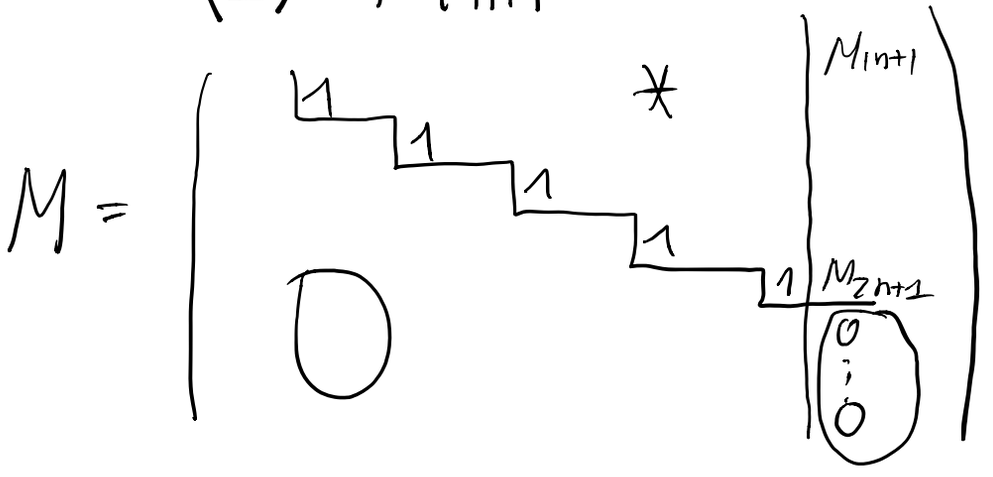
(c) if $M^{\circ}_{ij} = 0$ $t_{r+1} \le j \le n$
$r+1 \le i \le m$

terminate 2

2.3 If $r = n$, then terminate 2,
else $r \leftarrow r+1$ and $t_r \leftarrow j$,
repeat 2.2

3. Construct all solutions

3.1. The system has a solution
$\Leftrightarrow M_{i\,n+1} = 0$ $r+1 \le i \le m$

$M =$ 

3.2 The variables x_j $t_i < j < t_{i+1}$
$0 \le i \le r$ may have any values

One computes the rest $x_{t_1}, x_{t_2}, \ldots, x_{t_2}$

For i from r to 1 do

$$x_{t_i} = M_{i\,n+1} + \sum_{j=t_i+1}^{n} x_j \cdot M_{ij}$$

5. Example.

$$\underset{A}{\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}} \underset{x}{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}} = \underset{a}{\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}}$$

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

t_1 t_2 t_3

$$\rightarrow \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$r=3$ #solutions $2^{4-3}=2$

x_3 may have any value

1) $x_3=0$ $x_4=1$, $x_2=1+x_4\cdot 1+x_3\cdot 1=0$

$x_1=1+x_4\cdot 1+x_3\cdot 1=0$

solution (0001)

2) $x_3=1$ $x_4=1$, $x_2=1+x_4\cdot 1+x_3\cdot 1=1$

$x_1=1+x_4\cdot 1+x_3\cdot 1=1$

solution (1111)

That is all for today!

Questions?