LFSR:

Linear-feedback shift register.

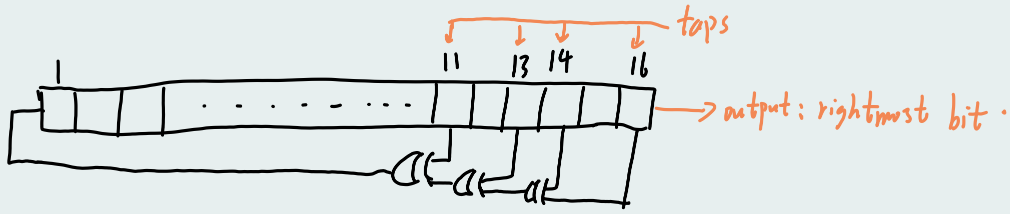
- a shift register whose input bit is a linear function of its previous state.

using XOR as the linear function

seed: the initial value of the LFSR.

Fibonacci LFSRs

taps: the bit positions that affect the next state.



In GF(2), the feedback polynomial:

$$S(x) = x^{16} + x^{14} + x^{13} + x^{11} + 1$$

GF field: $GF(p) \Rightarrow \bmod p$

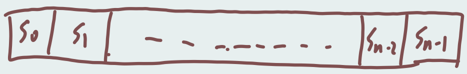
$GF(2) = XOR$

$1+1 = 0 \pmod 2$ $\quad 1 = -1$

$1-1 = 0 \pmod 2$

$0+1 = 1 \pmod 2$

n-bit register



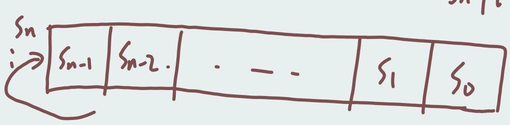
$$S(x) = s_0 + s_1 x + s_2 x^2 + \dots + s_{n-1} x^{n-1}$$

$\Rightarrow x^k = k$th bit of the register.

shift $= S(x) \cdot x$ $\quad s_0 \to s_1, \; s_1 \to s_2.$

$$x \cdot S(x) = s_0 x + s_1 x^2 + \dots + s_{n-1} x^n$$

In LFSR:



$$s_n = c_1 s_{n-1} + c_2 s_{n-2} + \dots + c_n s_0 \pmod 2$$

$s_n + c_1 s_{n-1} + c_2 s_{n-2} + \dots + c_n s_0 = 0$, as $s_k = x^k s_0$

$$x^n s_0 + c_1 x^{n-1} s_0 + c_2 x^{n-2} s_0 + \dots + c_n s_0 = 0$$

$$(x^n + c_1 x^{n-1} + c_2 x^{n-2} + \dots + c_n) s_0 = 0$$

$$f(x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \dots + c_n$$