MATH 314 Fall 2023 - Class Notes

02/19/2024

Scribe: Demontez Chin

LFSRs

Notes:

- Every random number generator repeats eventually
- The number of times it takes between repetitions called the period
- Generally bigger periods are better
- LCRNGs (mod n)

  -Period is always at most n
- LFSRS

  -Linear feedback shift registers
- Produce one pseudorandom bit at a time
- Store last m bits, m is called the degree
- Pick m feedback coefficients

  Examples:
- $P_0, P_1, P_m - 1$

  – All 0's and 1's
- Generate new bits
- $S_m = P_m - 1, S_m - 1 + P_m - 2S_m - 2P_0S_0 \pmod 2$
- $S_m + 1 = P_m - 1S_m + P_m - 2S_m - 1P_0S_1 \pmod 2$
- $S_i =$ State bits
- $S_0, S_1S_m - 1$ — initial seed
- $S_m, S_m + 1$ — random bits
- $S_{m+j} = P_m - 1S_{m+j} - 1 + P_{m-2}S_{m+j} - 2P_0S_j \pmod 2)$

- Think of the bits being shifted after every step, called clocking
- Ex: $m = 4, P_0 = 1, P_1 = 1, P_2 = 0, P_3 = 1$
- $S_m = P_3 * S_m - 1 + P_2 * S_m - 2 + P_1 S_m - 3 + P_0 S_m - 4$
- stream: 11000111000111000111000
- $S_0 = 1; S_1 = 1; S_2 = 0; S_3 = 0$
- $S_4 = S_3 + S_1 + S_0 \pmod 2$
  $0 + 1 + 1 = 0 \pmod 2$
- $S_5 = S_4 + S_2 + S_1$
  $0 + 0 + 1 = 1 \pmod 2$
- $S_6 = S_5 + S_3 + S_2$
  $1 + 0 + 0 = 1 \pmod 2$
- $S_7 = S_6 + S_4 + S_3$
  $= 1 + 0 + 0 = 1 \pmod 2$
- $S_8 = S_7 + S_5 + S_4$
  $1 + 1 + 0 = 0 \pmod 2$
- $S_9 = S_8 + S_6 + S_5$
  $0 + 1 + 1 = 0 \pmod 2$
- A degree m LFSR has maximum period $2^m - 1$
  Example: m = 3
- $P_0 = 1; P_1 = 0; P_2 = 1$
- $S_0 = 1; S_1 = 1; S_2 = 1$
- $S_3 = S_2 + S_0$
  $1 + 1 \equiv 0 \pmod 2$
- $S_4 \equiv S_3 + S_1$
  $\equiv 0 + 1 = 1 \pmod 2$
- $S_5 = S_4 + S_2 = 1 + 1 \equiv 0 \pmod 2$
- $S_6 = S_5 + S_3 = 0 + 0 \equiv 0 \pmod 2$

- $S_7 = S_6 + S_4 = 0 + 1 \equiv 1 \pmod 2$
- $S_8 = S_7 + S_5 = 1 + 0 \equiv 1 \pmod 2$
- $S_9 = S_8 + S_6 = 1 + 0 \equiv 1 \pmod 2$

Continued Notes:

- The connection polynomial of an LFSR of degree m is
  $Cx = x^m + P_{m-1}x^{m-1} + P_{m-2} * x^{m-2} + ... + P_1x + P_0$
- If an LFSR has maximum degree then its connection polynomial is irreducible

Last Example:

- Bluetooth uses a cipher called EO which has 4 LFSRs with connection polynomials
  : $x^{25} + x^{20} + x^{12} + x^8 + 1$
  : $x^{31} + x^{24} + x^{16} + x^{12} + 1$
  : $x^{33} + x^{28} + x^{24} + x^4 + 1$
  : $x^{39} + x^{36} + x^{28} + x^4 + 1$
- These equal 1 bit of output and is used as a key stream for the stream cipher