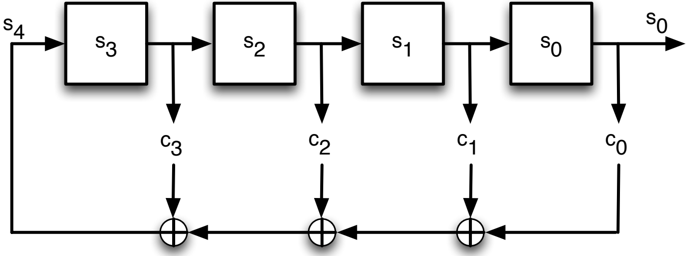
Linear Complexity



Linear Complexity

- The length n of the minimal length LFSR that produces the given sequence of length m is called **linear complexity** of the sequence
- The Berlekamp-Massey algorithm computes the length and the connection polynomial of the the minimal length LFSR that produces the given sequence
- We expect that $1 \leq n \leq m$

Linear Complexity

- Linear complexity is proposed as a measure of randomness of the given sequence
- Higher values of n imply that the RNG that produced is more complex, or less linear or more nonlinear
- The linear complexity of a sequence is the measure of complexity of **the given sequence**, **not** necessarily the **RNG** that produced the sequence
- At another time the same RNG may produce a sequence whose linear complexity is different

Linear Complexity

- An LFSR with $n = 1$ can only produce the sequences $000\cdots$ or $111\cdots$, i.e., the linear complexity of these sequences is 1
- Similarly, the linear complexity of the sequence $010101\cdots$ can be shown to be equal 2, regardless of its length
- The period of a sequence and its linear complexity are related, but they will not be the same
- An n-bit maximal LFSR produces a sequence with period $2^n - 1$ and the linear complexity is n

Linear Complexity

- What is the linear complexity of an arbitrary sequence of length m ?
- The smallest value of linear complexity for a sequence of length will be 1 (if the sequence happens to be all-zero or all-one)
- The largest possible value of linear complexity for a sequence of length m will be $n = m$
- The value of $n = m$ essentially indicates our failure to find a smaller LFSR producing the sequence, and thus, we just build a m-bit LFSR and set the initial state as the bits of the given sequence, which produces the sequence by right shift in m clock cycles
- Otherwise, we will obtain a value between 1 and m

Linear Complexity

- Higher value of the linear complexity **does not imply** randomness
- It is quite easy to construct a sequence of length m whose linear complexity is m, which is the highest possible value
- Consider the sequence which consists of $m-1$ consecutive zeros followed by a single 1

$$0^{m-1}1 = 00\cdots001$$

- It has the highest linear complexity which is $n = m$
- Its linear complexity is equal to its length, however, it is not statistically random and highly predictable,

Linear Complexity

- On the hand, randomness **must imply** higher linear complexity
- We expect a truly random source to produce sequences whose linear complexity is unbounded