Pseudo-Random Binary Sequences

- Voice-Band Modem Functions
  - Modulator and Demodulator (MODEM)
  - Data compression
  - Error detection and correction
  - Clock and carrier tracking
  - Automatic dialing, etc
- Testing of digital communication systems
  - Sequences that approximate ideal binary random sequences are required.
- Generate Pseudo-random binary sequences using linear feedback shift registers
- Data scrambler and descrambler
  - To break up long strings of 1’s and 0’s to allow tracking loops in the receiver to maintain lock, rather than secrecy.

Linear Feedback Shift Registers

- Ideal binary random sequence
  - Infinite, identically distributed, random variables, each taking on the values 0 and 1 with probability 0.5
- Approximations to binary random sequences
  - Generated by linear feedback shift registers
- The resulting sequences are called
  - Pseudo-random, Pseudo-noise (PN), Maximal length or M-sequences
- The scrambler input and output relation

\[
y(n) = x(n) + \sum_{k=1}^{m} h_k y(n-k)
\]
Sequence Generation

- Connection polynomial
- Simulation of binary random sequences
  - Maximum possible period is $2^{m-1}$
  - These are called maximal length sequences
- If the connection polynomial is primitive polynomial
- Primitive polynomials are irreducible
  - Cannot be factored into the product of polynomials

Properties of PN Sequences

- Frequency of occurrence of 1’s ($2^{m-1}$) and 0’s ($2^{m-1}-1$)
- Frequency of Runs of 1’s and 0’s
- Correlation property
  - Transform sequences of 0’s and 1’s as
    $0 \rightarrow 1$ and $1 \rightarrow -1$
  - The periodic autocorrelation function is defined to be
    $$R(n) = \frac{1}{N} \sum_{k=0}^{N-1} \hat{y}(n) \hat{y}(n+k)$$
- $N=2^{m-1}$ and $R(n)$
  $$R(n) = \begin{cases} -1/N & \text{for } n \text{ not a multiple of } N \\ 1 & \text{for } n \text{ a multiple of } N \end{cases}$$
Scrambler and Descrambler

- Scrambler randomizes long strings of 0’s and 1’
- ITU Standard Modem’s connection polynomial
  - \( h(D) = 1 + D^{18} + D^{23} \)
  - \( Y(D) = X(D) / h(D) \)
- Descrambler recovers the received sequence by inverting
  - \( X(D) = Y(D) h(D) \)