Linear Feedback Shift Registers

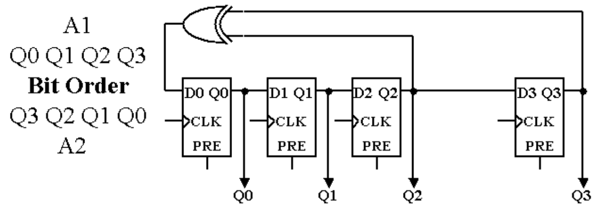

Figure 1

Sequence
A1 - 15,14,12,8,1,2,4,9,3,6,13,10,5,11,7...

The Linear Feedback Shift Register LFSR

Figure 1 shows a linear feedback shift register (LFSR). The exclusive-OR gates and shift register act to produce a pseudo-random binary sequence (PRBS) at each of the flip-flop outputs. By correctly choosing the points at which we take the feedback from an n -bit shift register, we can produce a PRBS of length $2^n - 1$, a maximal-length sequence that includes all possible patterns (or vectors) of n bits, excluding the all-zeros pattern. The diagram shows a 4 bit linear feedback shift register (LFSR). A 4-bit maximal-length LFSR produces a repeating string of 15 pseudo-random binary numbers.

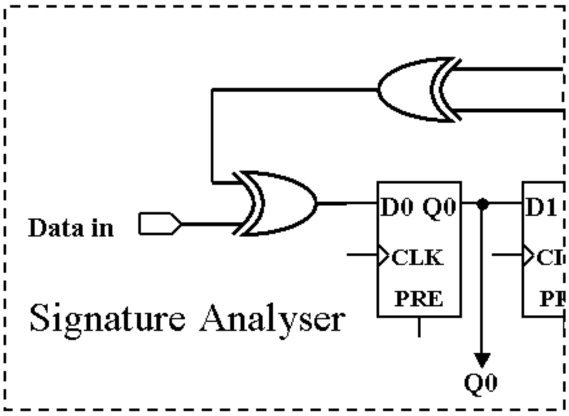

Figure 2

Signature Analysis

Figure 2 shows the LFSR of **Figure 1** with an additional XOR gate used in the first stage of the shift register. If we apply a binary input sequence to IN , the shift register will perform data compaction (or compression) on the input sequence. At the end of the input sequence the shift-register contents, Q0Q1Q2Q3 , will form a pattern that we call a signature. If the input sequence and the serial-input signature register (SISR) are long enough, it is unlikely (though possible) that two different input sequences will produce the same signature. If the input sequence comes from data that we wish to check, an error in the data will cause the input sequence to change. This causes the signature to change from the known good expected value..

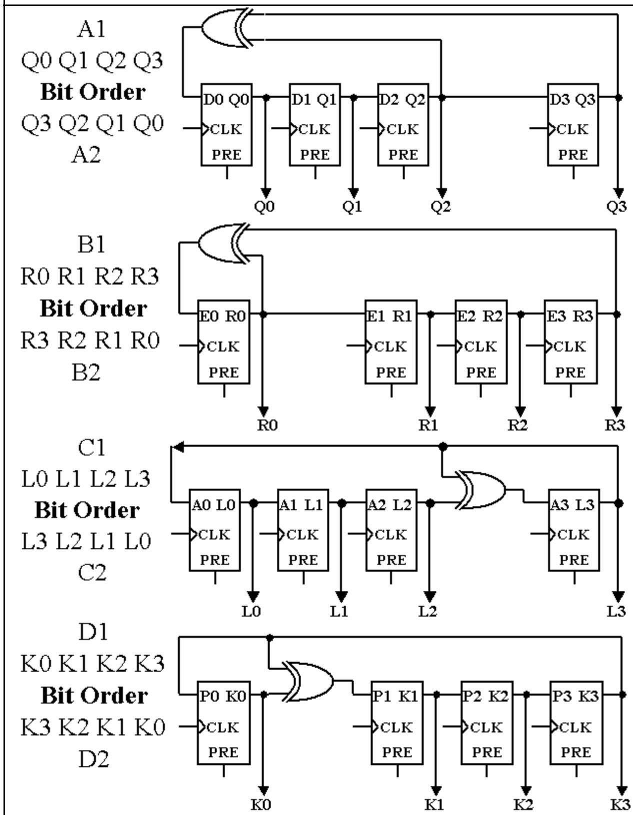

Figure 3

LFSR Types

Finally for every primitive polynomial there are in fact four linear feedback shift registers (LFSRs) that may be implemented.- either by using XOR gates in series with each flip-flop output, or with the XOR gates external to the shift register in the feedback path. The external-XOR LFSR is called a type 1 LFSR (i.e. A and B in **Figure 3**) and the internal-XOR LFSR is called a type 2 LFSR (i.e. C and D in **Figure 3**)

Within each type of LFSR the positions of the feedback points may be defined by numbering from either one end of the register, or the other.

Each LFSR produces a different pseudo-random sequence with the register initialised to '1111', hex F as a starting point giving eight different sequences. (A1, A2; B1, B2; C1, C2; and D1, D2 in **Figure 3)**

Each form of the LFSR can be made a Signature Analyser by the addition of the input XOR to the first D-type

[Internet search "LFSR" "pseudo random binary sequence" "PRBS" "Signature Analysis" "BIST" "build in self test"] Note: detailed LFSR/polynomial theory is **NOT** required in this unit!