Linear Feedback Shift Registers (LFSRs)

- Efficient design for Test Pattern Generators & Output Response Analyzers (also used in CRC)
  - FFs plus a few XOR gates
  - better than counter
    - fewer gates
    - higher clock frequency
- Two types of LFSRs
  - External Feedback
  - Internal Feedback
    - higher clock frequency
- Characteristic polynomial
  - defined by XOR positions
  - $P(x) = x^4 + x^3 + x + 1$ in both examples

C. Stroud, Dept. of ECE, Auburn
Univ. 10/04
LFSRs (cont)

Characteristic polynomial of LFSR

- \( n = \# \) of FFs = degree of polynomial
- XOR feedback connection to FF \( i \) \( \iff \) coefficient of \( x^i \)
  - coefficient = 0 if no connection
  - coefficient = 1 if connection
  - coefficients always included in characteristic polynomial:
    - \( x^n \) (degree of polynomial & primary feedback)
    - \( x^0 = 1 \) (principle input to shift register)

- Note: state of the LFSR \( \iff \) polynomial of degree \( n-1 \)
- Example: \( P(x) = x^3 + x + 1 \)
LSFRs (cont)

• An LFSR generates periodic sequence
  – must start in a non-zero state,

• The maximum-length of an LFSR sequence is $2^n - 1$
  – does not generate all 0s pattern (gets stuck in that state)

• The characteristic polynomial of an LFSR generating a maximum-length sequence is a \textit{primitive polynomial}

• A maximum-length sequence is \textit{pseudo-random}:
  – number of 1s = number of 0s + 1
  – same number of runs of consecutive 0s and 1s
  – 1/2 of the runs have length 1
  – 1/4 of the runs have length 2
  – … (as long as fractions result in integral numbers of runs)
LFSRs (cont)

- Example: Characteristic polynomial is $P(x) = x^3 + x + 1$

- Beginning at all 1s state
  - 7 clock cycles to repeat
  - maximal length = $2^n - 1$
  - polynomial is primitive

- Properties:
  - four 1s and three 0s
  - 4 runs:
    - 2 runs of length 1 (one 0 & one 1)
    - 1 run of length 2 (0s)
    - 1 run of length 3 (1s)

- Note: external & internal LFSRs with same primitive polynomial do not generate same sequence (only same length)
LFSRs (cont)

- Reciprocal polynomial, $P^*(x)$
  - $P^*(x) = x^n P(1/x)$
    - example: $P(x) = x^3 + x + 1$
    - then: $P^*(x) = x^3 (x^{-3} + x^{-1} + 1) = 1 + x^2 + x^3 = x^3 + x^2 + 1$
    - if $P(x)$ is primitive, $P^*(x)$ is also primitive
      - same for non-primitive polynomials

- Polynomial arithmetic
  - modulo-2 ($x^n + x^n = x^n - x^n = 0$)

<table>
<thead>
<tr>
<th>Addition/Subtraction</th>
<th>Multiplication</th>
<th>Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x^5 + x^2 + 1) + (x^4 + x^2)$</td>
<td>$(x^2 + x + 1) \times (x^2 + 1)$</td>
<td>$x^2 + 1$</td>
</tr>
<tr>
<td>$x^5$ $x^2$ $1$</td>
<td>$x^2 + x + 1$</td>
<td>$x^4 + x^3 + x + 1$</td>
</tr>
<tr>
<td>$+ x^4$ $x^2$</td>
<td>$\times x^2 + 1$</td>
<td>$x^4 + x^2$</td>
</tr>
<tr>
<td>$x^5$ $x^4$ $1$</td>
<td>$= x^4 + x^3 + x + 1$</td>
<td>$x^3 + x^2 + x + 1$</td>
</tr>
<tr>
<td>$= x^5 + x^4 + 1$</td>
<td></td>
<td>$x^3 + x^2 + x + 1$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$x^3 + x + x$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$= x^2 + 1$</td>
</tr>
</tbody>
</table>

C. Stroud, Dept. of ECE, Auburn
Univ. 10/04
LFSRs (cont)

- Non-primitive polynomials produce sequences < $2^n-1$
  - Typically primitive polys desired for TPGs & ORAs
- Example of non-primitive polynomial
  - $P(x) = x^3 + x^2 + x + 1$
LFSRs (cont)

- Primitive polynomials with minimum # of XORs

<table>
<thead>
<tr>
<th>Degree ($n$)</th>
<th>Polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,3,4,6,7,15,22</td>
<td>$x^n + x + 1$</td>
</tr>
<tr>
<td>5,11,21,29</td>
<td>$x^n + x^2 + 1$</td>
</tr>
<tr>
<td>8,19</td>
<td>$x^n + x^6 + x^5 + x + 1$</td>
</tr>
<tr>
<td>9</td>
<td>$x^n + x^4 + 1$</td>
</tr>
<tr>
<td>10,17,20,25,28</td>
<td>$x^n + x^3 + 1$</td>
</tr>
<tr>
<td>12</td>
<td>$x^n + x^7 + x^4 + x^3 + 1$</td>
</tr>
<tr>
<td>13,24</td>
<td>$x^n + x^4 + x^3 + x + 1$</td>
</tr>
<tr>
<td>14</td>
<td>$x^n + x^{12} + x^{11} + x + 1$</td>
</tr>
<tr>
<td>16</td>
<td>$x^n + x^5 + x^3 + x^2 + 1$</td>
</tr>
<tr>
<td>18</td>
<td>$x^n + x^7 + 1$</td>
</tr>
<tr>
<td>23</td>
<td>$x^n + x^5 + 1$</td>
</tr>
<tr>
<td>26,27</td>
<td>$x^n + x^8 + x^7 + x + 1$</td>
</tr>
<tr>
<td>30</td>
<td>$x^n + x^{16} + x^{15} + x + 1$</td>
</tr>
</tbody>
</table>