

Galois LFSR shift/XOR truth table (1-bit output, 8-bits wide, polynomial x^8 + x^4 + x^3 + x^2 + 1):

0: ‘0’⊕ 7

1: 0

2: 1 ⊕ 7

3: 2 ⊕ 7

4: 3 ⊕ 7

5: 4

6: 5

7: 6

Unrolling the LFSR Logic so we can generate multiple bits per clock (these are the state bits):

SEE Galois\_LFSR\_Calculations.xlsx

(0 bits per clock is not valid, but included to illustrate the pattern)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Bit** | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| **Bits/Clk** |  |  |  |  |  |  |  |  |
| 0 | **7** | **6** | **5** | **4** | **3** | **2** | **1** | **0** |
| 1 | **6** | **5** | **4** | 7 ⊕ **3** | 7 ⊕ **2** | 7 ⊕ **1** | **0** | **7** |
| 2 | **5** | **4** | 7 ⊕ **3** | 7 ⊕ (6 ⊕ **2**) | 7 ⊕ (6 ⊕ **1**) | 6 ⊕ **0** | **7** | **6** |
| 3 | **4** | 7 ⊕ **3** | 7 ⊕ (6 ⊕ **2**) | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) | 6 ⊕ (**5** ⊕ **0**) | **5** ⊕ **7** | **6** | **5** |
| 4 | 7 ⊕ **3** | 7 ⊕ (6 ⊕ **2**) | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) | (**5** ⊕ (**4** ⊕ **7** )) | **4** ⊕ **6** | **5** | **4** |
| 5 | 7 ⊕ (6 ⊕ **2**) | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) | (7 ⊕ **3**) ⊕ (**5** ⊕ (**4** ⊕ **7**)) | (7 ⊕ **3**) ⊕ (**4** ⊕ **6**) | (7 ⊕ **3**) ⊕ **5** | **4** | 7 ⊕ **3** |
| 6 | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) | (7 ⊕ **3**) ⊕ (**5** ⊕ (**4** ⊕ **7**)) | 7 ⊕ (6 ⊕ **2**) ⊕ ((7 ⊕ **3**) ⊕ (**4** ⊕ **6**)) | 7 ⊕ (6 ⊕ **2**) ⊕ ((7 ⊕ **3**) ⊕ **5**) | 7 ⊕ (6 ⊕ **2**) ⊕ **4** | 7 ⊕ **3** | 7 ⊕ (6 ⊕ **2**) |
| 7 | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) | (7 ⊕ **3**) ⊕ (**5** ⊕ (**4** ⊕ **7**)) | 7 ⊕ (6 ⊕ **2**) ⊕ ((7 ⊕ **3**) ⊕ (**4** ⊕ **6**)) | (7 ⊕ (6 ⊕ (**5** ⊕ **1**))) ⊕ (7 ⊕ (6 ⊕ **2**) ⊕ ((7 ⊕ **3**) ⊕ **5**)) | (7 ⊕ (6 ⊕ (**5** ⊕ **1**))) ⊕ (7 ⊕ (6 ⊕ **2**) ⊕ **4**) | (7 ⊕ (6 ⊕ (**5** ⊕ **1**))) ⊕ (7 ⊕ **3**) | 7 ⊕ (6 ⊕ **2**) | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) |
| 8 | (7 ⊕ **3**) ⊕ (**5** ⊕ (**4** ⊕ **7**)) | 7 ⊕ (6 ⊕ **2**) ⊕ ((7 ⊕ **3**) ⊕ (**4** ⊕ **6**) ) | (7 ⊕ (6 ⊕ (**5** ⊕ **1**))) ⊕ (7 ⊕ (6 ⊕ **2**) ⊕ ((7 ⊕ **3**) ⊕ **5**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) ⊕ ( (7 ⊕ (6 ⊕ (**5** ⊕ **1**))) ⊕ (7 ⊕ (6 ⊕ **2**) ⊕ **4**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) ⊕ ((7 ⊕ (6 ⊕ (**5** ⊕ **1**))) ⊕ (7 ⊕ **3**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) ⊕ (7 ⊕ (6 ⊕ **2**)) | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) |

CURRENT INCORRECT from here down

**LFSR Contents and Output – 1 bit/clock**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | **6** | **5** | **4** | 7 ⊕ **3** | 7 ⊕ **2** | 7 ⊕ **1** | **0** | **7** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clock | Check Program  (Binary) | Simulation  (Binary) | Register  (Hex) | Output (1 bit/clock – bit 7) |
| 0 | 00000001 |  | 1 | 0 |
| 1 | 00000010 |  | 2 | 0 |
| 2 | 00000100 |  | 4 | 0 |
| 3 | 00001000 |  | 8 | 0 |
| 4 | 00010000 |  | 10 | 0 |
| 5 | 00100000 |  | 20 | 0 |
| 6 | 01000000 |  | 40 | 0 |
| 7 | 10000000 |  | 80 | 1 |
| 8 | 00011101 |  | 1d | 0 |
| 9 | 00111010 |  | 3a | 0 |
| 10 | 01110100 |  | 74 | 0 |
| 11 | 11101000 |  | e8 | 1 |
| 12 | 11001101 |  | cd | 1 |
| 13 | 10000111 |  | 87 | 1 |
| 14 | 00010011 |  | 13 | 0 |
| 15 | 00100110 |  | 26 | 0 |
| 16 | 01001100 |  | 4c | 0 |

0000 0001 0001 1100 0

**LFSR Contents and Output – 2 bit/clock**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | **5** | **4** | 7 ⊕ **3** | 7 ⊕ (6 ⊕ **2**) | 7 ⊕ (6 ⊕ **1**) | 6 ⊕ **0** | **7** | **6** |

|  |  |  |  |
| --- | --- | --- | --- |
| Clock | Register  (Binary) | Register  (Hex) | Output (1 bit/clock – bit 7) |
| 0 | 00000001 | 1 | 0 |
| 1 | 00000100 | 4 | 0 |
| 2 | 00010000 | 10 | 0 |
| 3 | 01000000 | 40 | 0 |
| 4 | 00011101 | 1d | 1 |
| 5 | 01110100 | 74 | 0 |
| 6 | 11001101 | cd | 1 |
| 7 | 00010011 | 13 | 3 |
| 8 | 01001100 | 4c | 0 |
| 9 |  | 2d | 1 |
| 10 |  | b4 | 0 |
| 11 |  | ea | 2 |
| 12 |  | 8f | 3 |
| 13 |  | 06 | 2 |
| 14 |  | 18 | 0 |
| 15 |  | 60 | 0 |
| 16 |  | 9d | 1 |

0000 0001 0001 1100 0100 1011 1000 0001

**LFSR Contents and Output – 4 bit/clock**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 7 ⊕ **3** | 7 ⊕ (6 ⊕ **2**) | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) | (**5** ⊕ (**4** ⊕ **7** )) | **4** ⊕ **6** | **5** | **4** |

|  |  |  |  |
| --- | --- | --- | --- |
| Clock | Register  (Binary) | Register  (Hex) | Output (1 bit/clock – bit 7) |
| 0 | 00000001 | 1 | 0 |
| 1 | 00010000 | 10 | 0 |
| 2 | 00011101 | 1d | 1 |
| 3 | 11001101 | cd | 1 |
| 4 | 01001100 | 4c | c |
| 5 |  | b4 | 4 |
| 6 |  | 8f | b |
| 7 |  | 18 | 8 |
| 8 |  | 9d | 1 |
| 9 |  | 25 | 9 |
| 10 |  | 6a | 2 |
| 11 |  | ee | 6 |
| 12 |  | 46 | e |
| 13 |  | 14 | 4 |
| 14 |  | 5d | 1 |
| 15 |  | b9 | 5 |
| 16 |  | 5f | b |

0000 0001 0001 1100 0100 1011 1000 0001 1001 0010 0110 1110 0100 0001 0101 1011

**LFSR Contents and Output – 6 bit/clock**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 6 | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) | **5** ⊕ (**4** ⊕ (**3** ⊕ **7** )) | **4** ⊕ (**3** ⊕ (**2** ⊕ **6**)) | **3** ⊕ (**2** ⊕ **5**) | **2** ⊕ **4** | 7 ⊕ **3** | 7 ⊕ (6 ⊕ **2**) |

|  |  |  |  |
| --- | --- | --- | --- |
| Clock | Register  (Binary) | Register  (Hex) | Output (1 bit/clock – bit 7) |
| 0 | 00000001 | 1 | 00 |
| 1 |  | 40 | 00 |
| 2 |  | d1 | 10 |
| 3 |  | 46 | 34 |
| 4 |  | 4c | 11 |
| 5 |  | f6 | 13 |
| 6 |  |  |  |
| 7 |  |  |  |
| 8 |  |  |  |
| 9 |  |  |  |
| 10 |  |  |  |
| 11 |  |  |  |
| 12 |  |  |  |
| 13 |  |  |  |
| 14 |  |  |  |
| 15 |  |  |  |
| 16 |  |  |  |

0000 0001 0000 1101 0001 0001 0100 11

**LFSR Contents and Output – 8 bit/clock**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | **5** ⊕ (**4** ⊕ (**3** ⊕ **7** )) | **4** ⊕ (**3** ⊕ (**2** ⊕ **6**)) | **3** ⊕ (**2** ⊕ (**1** ⊕ **5**)) | **2** ⊕ (**1** ⊕ (**0** ⊕ **4**)) | 7 ⊕ (**1** ⊕ (**0** ⊕ **3**)) | 7 ⊕ (6 ⊕ (**0** ⊕ **2**)) | 7 ⊕ (6 ⊕ (**5** ⊕ **1**)) | 6 ⊕ (**5** ⊕ (**4** ⊕ **0**)) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clock | Check Program  (Binary) | Simulation Output | Register  (Hex) | Output (1 bit/clock – bit 7) |
| 0 | 00000000 | 00000000 |  |  |
| 1 | 00000001 | 00000001 |  |  |
| 2 | 00000000 | 00000000 |  |  |
| 3 | 00011101 | 00011101 |  |  |
| 4 | 00000001 | 00000000 |  |  |
| 5 | 01010001 |  |  |  |
| 6 | 00011011 |  |  |  |
| 7 | 10001100 |  |  |  |
| 8 | 00010001 |  |  |  |
| 9 | 00011101 |  |  |  |
| 10 | 11001100 |  |  |  |
| 11 | 01011000 |  |  |  |
| 12 | 01011010 |  |  |  |
| 13 | 01111110 |  |  |  |
| 14 | 01000111 |  |  |  |
| 15 | 10010001 |  |  |  |
| 16 | 00011100 |  |  |  |