Tony Majestro

Problem Set 3

1. Consider the linear recurrence of degree 5. For each of the 32 possible initialization vectors (i.e. the 32 initial fills), determine the period of the resulting keystream.

To find the period of each keystream for the LFSR, we can model the registers as a list of values 0 or 1. We can then emulate the LFSR by adding a new value according to the recurrence relation to the end of the register list. Finally, we can remove the first value from the register list. This process can be repeated until the list of registers is equal to the original initialization vector’s list of vectors. The number of cycles it took for this to happen will be the period of its keystream. We can model the recurrence relation as an XOR of the first two values in the list of registers:



To solve the problem, we can generate each of the possible 32 seeds and print its key period. The following code generates each seed as a list of integers:



Using this code, we can get the period for each of the 32 initialization vectors:



This gives the following output:

|  |  |
| --- | --- |
| 00000 1 | 10000 21 |
| 00001 21 | 10001 21 |
| 00010 21 | 10010 21 |
| 00011 21 | 10011 7 |
|  |  |
| 00100 21 | 10100 7 |
| 00101 21 | 10101 21 |
| 00110 21 | 10110 3 |
| 00111 7 | 10111 21 |
|  |  |
| 01000 21 | 11000 21 |
| 01001 7 | 11001 21 |
| 01010 21 | 11010 7 |
| 01011 21 | 11011 3 |
|  |  |
| 01100 21 | 11100 21 |
| 01101 3 | 11101 7 |
| 01110 7 | 11110 21 |
| 01111 21 | 11111 21 |

1. Suppose we build a linear feedback shift register (LFSR) machine that works mod 3 instead of mod 2. It uses a recurrence of length 2 of the form to generate the sequence 1, 1, 0, 2, 2, 0, 1, 1. Set up and solve the matrix equation to find the coefficients and .

From the sequence, we have that , , , and . From the recurrence relation, we have that and . To find the values, we can combine the two equations to form the matrix equation:

We can then solve this matrix equation to get the values for and by substituting in values for , , , and :

|  |
| --- |
|  |
|  |
|  |
|  |

To solve the matrix, must find the inverse matrix . We have that the determinate of the matrix is (0 – 1) = -1. Then, the inverse matrix is:

|  |
| --- |
|  |
|  |
|  |
|  |

Now that we have the inverse, we can solve the matrix equation:

|  |
| --- |
|  |
|  |
|  |
|  |
|  |

So we have that and . To verify, we can check that and for and . This gives

and

, which is correct.