

## Solutions to Assignment 1

### Question 1

**Solution.**

(a) The state diagram of the FSR is shown in Figure 1.

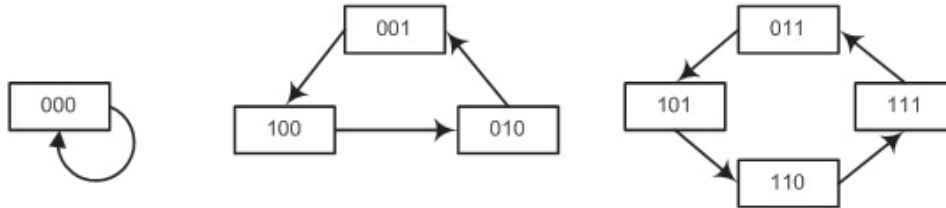


Figure 1: The state diagram of the FSR (Question 1)

(b) If the initial state is set as  $(a_0, a_1, a_2) = (011)$ , the output sequence would be 011101110111... . And the period of the sequence is 4.

### Question 2

**Solution.**

The cycles in the state diagram have no branch points if and only if two distinct state vectors have distinct successors. If  $(a_0, a_1, \dots, a_{n-1})$  and  $(b_0, b_1, \dots, b_{n-1})$  differ in any component other than the first, then their successors  $(a_1, \dots, a_{n-1})$  and  $(b_1, \dots, b_{n-1})$  are still distinct. Thus, the condition that the cycles in the state diagram have no branch points if and only if  $(a_0, a_1, \dots, a_{n-1})$  and  $(a_0 + 1, a_1, \dots, a_{n-1})$  have distinct successors. This simply says that

$$f(a_0 + 1, a_1, \dots, a_{n-1}) = f(a_0, a_1, \dots, a_{n-1}) + 1.$$

Defining  $g(a_1, \dots, a_{n-1}) = f(0, a_1, \dots, a_{n-1})$ , the above expression can be written as

$$f(a_0, a_1, \dots, a_{n-1}) = g(a_1, \dots, a_{n-1}) + a_0.$$

### Question 3

**Solution.**

The LFSR over  $(GF(2))$  for implementation of the linear recurrence relation  $a_{5+k} = a_{3+k} + a_k, k = 0, 1, \dots$  is shown in Figure 2. The characteristic polynomial of the sequence is  $f(x) = x^5 + x^3 + 1$ . There are  $2^5 = 32$  sequences in  $G(f)$ .

If we set the initial state as  $(a_0, a_1, a_2, a_3, a_4) = (0, 0, 0, 0, 1)$ , the first 50 bits is

$$a = 10000101011101100011111001101001000010101110110001 \dots$$

The period of the sequence is 31, so it begins to repeat after 31 bits.

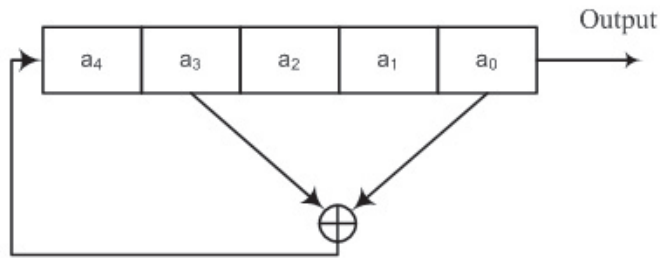


Figure 2: The LFSR (Question 3)

### Question 4

**Solution.**

The LFSR over  $GF(2)$  for implementation of the linear recurrence relation  $a_{6+k} = a_{1+k} + a_k, k = 0, 1, \dots$  is shown in Figure 3.

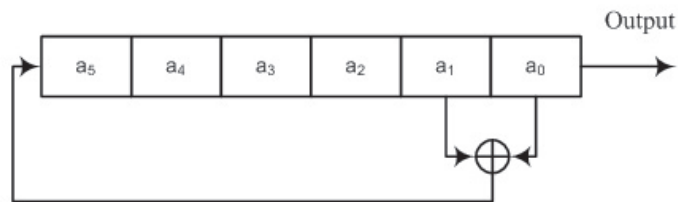


Figure 3: The LFSR (Question 4)

The characteristic polynomial of the sequence is  $f(x) = x^6 + x + 1$ . There are  $2^6 = 64$  sequences in  $G(f)$ .

### Question 5

**Solution.**

The LFSR over  $(GF(2))$  for implementation of the linear recurrence relation  $a_{7+k} = a_{1+k} + a_k, k = 0, 1, \dots$  is shown in Figure 4

The characteristic polynomial of the sequence is  $f(x) = x^7 + x + 1$ . There are  $2^7 = 128$  sequences in  $G(f)$ .

### Question 6

**Solution.**

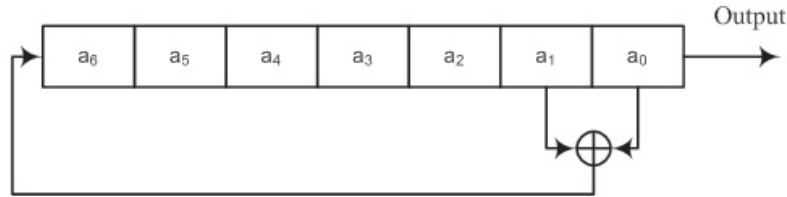


Figure 4: The LFSR (Question 5)

In general, we can construct a de Bruijn sequences with period  $2^n$  by inserting one zero into zero run of length  $n - 1$  of an  $m$ -sequence with period  $2^n - 1$ . There are  $T_n = \phi(2^n - 1)/n$  shift-distinct  $m$ -sequences with period  $2^n - 1$ . Thus, this construction gives  $T_n$  shift-distinct de Bruijn sequences with period  $2^n$ .

From this general construction, for  $n = 4$ , there are two shift-distinct  $m$  sequences with period 15. Thus we can two different (shift-distinct) de Bruijn sequences with period 16 by inserting one zero into zero run of length 3 of two respective shift-distinct  $m$ -sequences with period 15. This is shown below.

(1)  $\mathbf{a} = (111101011001000)$  generated by the minimal polynomial  $x^4 + x^3 + 1$ . Then  $\mathbf{a}' = (0111101011001000)$  is a de Bruijn sequence of period 16, generated by the feedback function

$$f(x_0, x_1, x_2, x_3) = x_1x_2x_3 + x_1 + x_0 + 1.$$

(2)  $\mathbf{b} = (000100110101111)$ , generated by the minimal polynomial  $f(x) = x^4 + x + 1$ . Then  $\mathbf{b}' = (0000100110101111)$  is a de Bruijn sequence of period 16 which is shift-distinct from  $\mathbf{a}'$ .

## Question 7

**Solution.**

(a) The first 50 bits of the output sequence with the initial state 00101 is

$$0010111001011100101110010111001011100101110010111001011100101110$$

which has a period of 7. The minimal polynomial of the sequence is  $x^3 + x + 1$ .

(b) The first 50 bits of the output sequence with the initial state 01000 is

$$01000011111010100110001000011111010100110001000011$$

which has a period of 21. The minimal polynomial of the sequence is  $f(x) = x^5 + x^4 + 1$ .

(c) There are  $2^5 = 32$  sequences in  $G(f)$ . The state diagram is depicted in Figure 5.

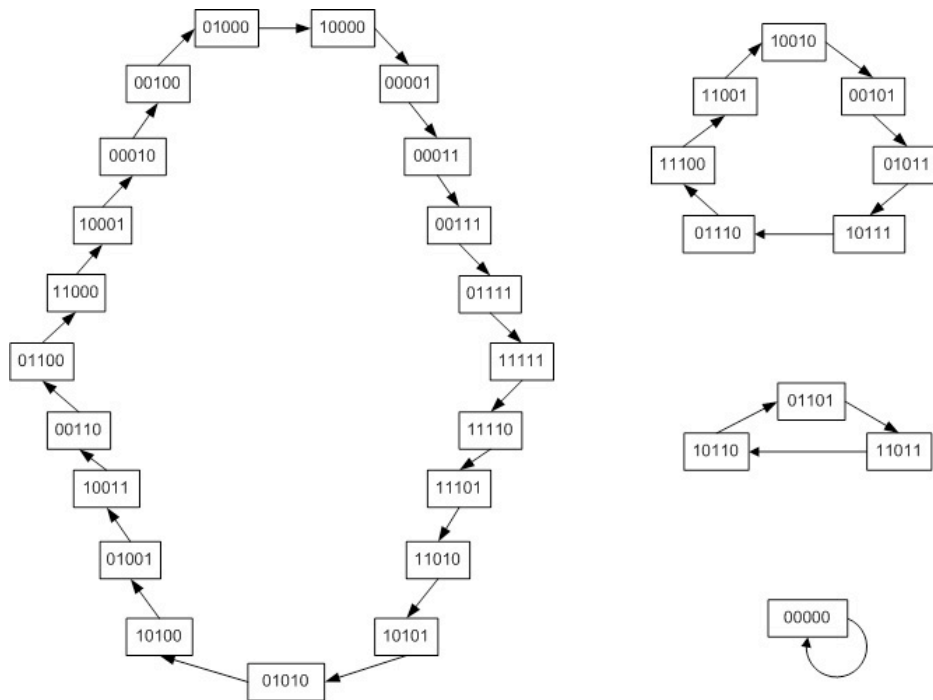


Figure 5: The state diagram (Question 7)

### Question 8

**Solution.**

Let  $n = 10$ . The output sequences of a primitive polynomial  $f(x) = x^{10} + x^3 + 1$  are binary  $m$ -sequences of period 1023.

### Question 9

**Solution.**

The number of LFSRs over  $GF(2)$  which generate a binary  $m$ -sequence with period  $2^8 - 1 = 255$  equal to the number of primitive polynomials in degree 8. The number of primitive polynomials in degree 8 can be calculated as:

$$\frac{\phi(255)}{8} = \frac{255}{8} \times \left(1 - \frac{1}{5}\right) \times \left(1 - \frac{1}{3}\right) \times \left(1 - \frac{1}{17}\right) = 16.$$

Thus, there are 16 various primitive polynomials in degree 8 over  $GF(2)$ . So the number of LFSRs over  $GF(2)$  which generate binary  $m$ -sequences with period  $2^8 - 1 = 255$  are given by 16.

In general, let  $m = p_1^{e_1} \cdots p_s^{e_s}$  where  $p_i$ 's are distinct prime numbers and  $e_i > 0$  are positive

integers. Then  $\phi(m)$  can be computed by

$$\phi(m) = p_1^{e_1-1}(p_1 - 1) \cdots p_s^{e_s-1}(p_s - 1) = m \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$