

## Assignment 1 (Topic 2. Feedback shift register (FSR) sequences)

1. Given a 3-stage shift register with the boolean feedback function  $f(x_0, x_1, x_2) = x_0 + x_1x_2$ :
  - (a) draw the state diagram of the FSR;
  - (b) if the initial state is set as  $(a_0, a_1, a_2) = (011)$ , determine the output sequence and the period of the sequence.
2. Let  $f(x_0, x_1, \dots, x_{n-1})$  be a boolean function in  $n$  variables which is employed as the feedback function of a shift register. Prove that the cycles in the state diagram have no branch points if and only if the feedback function can be decomposed into

$$f(x_0, x_1, \dots, x_{n-1}) = x_0 + g(x_1, \dots, x_{n-1})$$

where  $g(x_1, \dots, x_{n-1})$  is a boolean function in  $n - 1$  variables. (Hint: 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  $(a_1, \dots, a_n)$  and  $(b_1, \dots, b_n)$  are still distinct. So, one only needs to consider whether  $(a_0, a_1, \dots, a_{n-1})$  and  $(a_0 + 1, b_1, \dots, b_{n-1})$  have distinct successors. )

3. Design an LFSR over  $GF(2)$  for implementation of the linear recurrence relation

$$a_{5+k} = a_{3+k} + a_k, k = 0, 1, \dots, .$$

Determine the characteristic polynomial  $f(x)$  of the sequence and the number of sequences in  $G(f)$ . Write the first 50 bits of the output sequence with a nonzero initial state.

4. Design an LFSR over  $GF(2)$  for implementation of the linear recurrence relation

$$a_{6+k} = a_{1+k} + a_k, k = 0, 1, \dots.$$

Determine the characteristic polynomial  $f(x)$  of the sequence and the number of sequences in  $G(f)$ .

5. Design an LFSR over  $GF(2)$  for implementation of the linear recurrence relation

$$a_{7+k} = a_{1+k} + a_k, k = 0, 1, \dots.$$

Determine the characteristic polynomial  $f(x)$  of the sequence and the number of sequences in  $G(f)$ .

6. Construct two different (shift-distinct) de Bruijn sequences with period 16.

7. Let  $f(x) = x^5 + x^4 + 1$  over  $\mathbb{F}_2$  be the characteristic polynomial of a 5-stage LFSR.

- (a) Write the first 50 bits of the output sequence with the initial state 00101 and determine the period and the minimal polynomial of the sequence. (Hint:  $f(x) = (x^3 + x + 1)(x^2 + x + 1)$ .)

- (b) Write the first 50 bits of the output sequence with the initial state 01000 and determine the period and the minimal polynomial of the sequence.
  - (c) Determine the number of sequences in  $G(f)$  and draw the state diagram.
8. Design an LFSR over  $GF(2)$  which generates a binary  $m$ -sequence with period 1023.
  9. Determine the number of LFSRs over  $GF(2)$  which generate a binary  $m$ -sequence with period  $2^8 - 1 = 255$ .
  10. Let  $\alpha$  be a primitive element of  $\mathbb{F}_{2^n}$ . Let  $\mathbf{a} = \{a_i\}$  be a binary  $m$ -sequence of degree  $n$  of period  $2^n - 1$  whose elements are given by  $a_i = Tr(\beta\alpha^i), \forall i \geq 0$  where  $Tr(x) = x + x^2 + \dots + x^{2^{n-1}}$ , the trace function from  $\mathbb{F}_{2^n}$  to  $\mathbb{F}_2, \beta \in \mathbb{F}_{2^n}, \forall i$ . Prove that  $\mathbf{a}$  has the following property:  $a_{2i} = a_i, \forall i \geq 0$ , if and only if  $\beta = 1$ . (This property is also referred to as *constant-on-cosets*).
  11. Find the initial state of an  $m$ -sequence which is generated by the primitive polynomial  $f(x) = x^7 + x + 1$  which satisfies the property of being constant-on-cosets.
  12. An  $m$ -sequence of period 31 with the minimal polynomial  $f(x) = x^5 + x^3 + 1$  is given by:

$$\mathbf{a} = (1000010101110110001111100110100).$$

Determine its 7-decimation sequence  $\mathbf{a}^{(7)}$  and compute the minimal polynomial of this sequence.

13. Let  $\mathbf{a}$  be an  $m$ -sequence over  $GF(2)$  of period 511. Determine the periods and linear spans of the following decimation sequences.

$$\mathbf{a}^{(r)}, \text{ where } r = 2, 3, 5, 14, 146.$$

(It is not necessary to generate the  $m$ -sequences.)

14. An  $m$ -sequence  $\mathbf{a}$  of period 127 with the minimal polynomial  $f(x) = x^7 + x + 1$  is given by:

```

1 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0 0 0 0 1 0 1 0 0 0 1 1 1 1 0
0 1 0 0 0 1 0 1 1 0 0 1 1 1 0 1 0 1 0 0 1 1 1 1 1 0 1 0 0 0
0 1 1 1 0 0 0 1 0 0 1 0 0 1 1 0 1 1 0 1 0 1 1 0 1 1 1 1 0 1
1 0 0 0 1 1 0 1 0 0 1 0 1 1 1 0 1 1 1 0 0 1 1 0 0 1 0 1 0 1
0 1 1 1 1 1 1 1
    
```

- (a) The set  $\Gamma$  consisting all the coset leaders modulo 127 is given by

$$\Gamma = \{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 27, 29, 31, 43, 47, 55, 63\}.$$

Find the individual terms  $a_i, \forall i \in \Gamma$ .

- (b) Verify that the sequence  $\mathbf{a}$  is constant-on-cosets.

The following three unsolved problems and conjectures related to shift register sequences are proposed by S.W. Golomb.

15. (**Golomb's Conjecture**) There exist infinitely many  $n$  such that  $f(x) = x^n + x^k + 1$  is a primitive polynomial over  $GF(2)$ , where  $1 \leq k < n$  and  $k$  may differ for different  $n$ .

*Notes Regarding Golomb's Conjecture:*

- 1) It is easy to show that there are infinitely many irreducible trinomials over  $GF(2)$ . For example,  $x^{2 \cdot 3^k} + x^{3^k} + 1$  is irreducible for every  $k = 0, 1, 2, \dots$ , with period  $3^{k+1}$ , but it is primitive only for  $k = 0$ .
  - 2) Can you prove that there are infinitely many primitive polynomials over  $GF(2)$  which have no more than  $t$  terms, for any fixed integer  $t$ ? This would be a new result.
  - 3) It seems to be true for every degree  $n \geq 5$  that there are primitive 5-term polynomials (pentanomials) of degree  $n$  over  $GF(2)$ . This would be a far stranger result than 2) above.
16. It is known that an  $n$ -stage shift register with the boolean feedback function  $f(x_0, x_1, \dots, x_{n-1})$  produce "pure cycles" (without "branches") if and only if we can write  $f(x_0, x_1, \dots, x_{n-1}) = x_0 + g(x_1, \dots, x_{n-1})$  (see Problem 2). It is also known that for  $n > 2$ , the *number* of (pure) cycles, for this case, is *even (odd)* if and only if the number of *ones* in the truth table for  $g(x_1, \dots, x_{n-1})$  is *even (odd)*. Are there other general, qualitative results about the cycles of a nonlinear shift register that can be similarly and simply stated in terms of the boolean functions  $f(x_0, x_1, \dots, x_{n-1})$  or  $g(x_1, \dots, x_{n-1})$  ?
17. If  $f(x_0, x_1, \dots, x_{n-1}) = x_0 + g(x_1, \dots, x_{n-1})$ , and  $g(0, \dots, 0) = 0$ , then the "all zero state" forms a pure cycle by itself. What further conditions on  $g$  will guarantee that the remaining  $2^n - 1$  states lie on a single cycle of the shift register? (It is not necessary to find conditions for all  $2^{2^{n-1}-n}$  such sequences. It would be very interesting to find conditions for even a small family of *nonlinear* sequences of period  $2^n - 1$ .)