

Solutions to Assignment 2

Question 1

Solution.

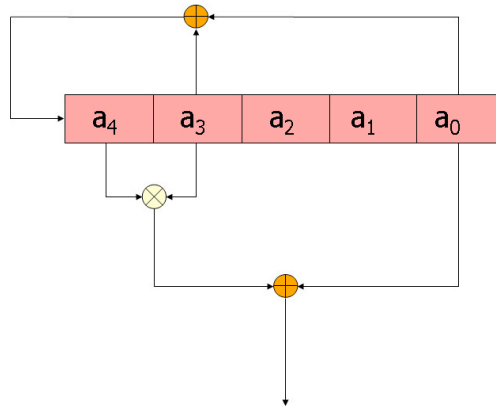


Figure 1: Question 1

Please see Figure 1. The characteristic polynomial for the LFSR is $x^5 + x^3 + 1 = 0$. We choose $d_0 = 0, d_1 = 3, d_2 = 4$, and $f(x_0, x_1, x_2) = x_0 + x_1x_2$. (Because the linear span of the output sequence is 15, $f(x_0, x_1, x_2)$ can be selected as quadratic function. The term x_0 is used to make the output sequence balance.) If the initial state is $(a_4, a_3, a_2, a_1, a_0) = (0, 0, 0, 0, 1)$, then the output sequence is 1000011001010111110111000110100. It is balanced with linear span 15.

Question 2

Solution.

Since 2, 3, and 5 are relatively prime, the periods of the sequences generated by these three LFSRs are also relatively prime. For the period and linear span distribution, please see Table 1.

Let \mathbf{a} be the m -sequence generated by the LFSR with degree 2, and \mathbf{b} be the m -sequence generated by the LFSR with degree 3. The period of $\mathbf{a} + \mathbf{b}$ is 21. The number of 1's in $\mathbf{a} + \mathbf{b}$ is $2 \times 3 + 1 \times 4 = 10$, and the number of 0's in $\mathbf{a} + \mathbf{b}$ is $21 - 10 = 11$. Hence $\mathbf{a} + \mathbf{b}$ is balanced. Therefore, if the initial state of the LFSR with degree 5 is loaded to zero, the number of balanced output sequences is $2^2 \times 2^3 - 1 = 31$ (The all 0 sequence should be excluded.).

Question 3

Corrected version: Let $\mathbf{a} = \{a_i\}$ and $\mathbf{b} = \{b_i\}$ be two sequences generated by LFSRs with two different primitive polynomials of degree n , say $f(x)$ and $g(x)$, as their respective characteristic polynomials, and $\mathbf{c} = \{c_i\}$ where $c_i = a_i b_i, i = 0, 1, \dots$. Show that the linear span of \mathbf{c} is n^2 . (Hint. Let α, θ be two primitive elements in $GF(2^n)$ satisfies that $f(\alpha) = 0$ and $g(\theta) = 0$. Then the trace representations of \mathbf{a} and \mathbf{b} are given by $a_i = Tr(\beta\alpha^i)$ and $b_i = Tr(\gamma\theta^i)$, β and $\gamma \in GF(2^n)$. Then

$$c_i = a_i b_i = (\beta\alpha^i + \beta^2\alpha^{2i} + \dots + \beta^{2^{n-1}}\alpha^{2^{n-1}i})(\gamma\theta^i + \gamma^2\theta^{2i} + \dots + \gamma^{2^{n-1}}\theta^{2^{n-1}i}).$$

⁰Copyright ©2009 Guang Gong. All rights reserved. May be freely reproduced for educational or personal use.

Table 1: Period and Linear Span Distribution

	Period	Linear Span	Number of Sequences
Case 1	1	0	1
Case 2	3	2	3
Case 3	7	3	7
Case 4	31	5	31
Case 5	21	5	21
Case 6	93	7	93
Case 7	217	8	217
Case 8	651	10	651

The linear span of \mathbf{c} is equal to the number of non-zero coefficients of $\alpha^{2^t i} \theta^{2^k i}$, since we can group these terms into several trace terms and each trace term represents an LFSR.)

Solution omitted.

Question 4

Solution.

(a) Please see Figure 2. We choose $d_0 = 0, d_1 = 2, d_2 = 3$, and $f(x_0, x_1, x_2) = x_0 x_1 x_2$. If the initial state is $(a_3, a_2, a_1, a_0) = (0, 0, 0, 1)$, then the output sequence is 000000000010100. Its linear span is 14 which is verified by the Berlekamp-Massey algorithm.

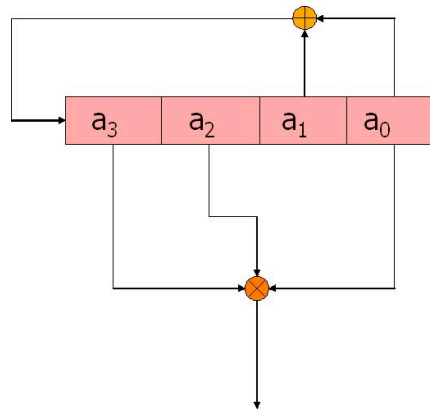


Figure 2: Question 4 (a)

(b)

Solution 1: We choose $d_0 = 0, d_1 = 1, d_2 = 2, d_3 = 3$, and the filtering function $f(x_0, x_1, x_2, x_3)$ in Figure 3 is

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

If the initial state is $(a_3, a_2, a_1, a_0) = (0, 0, 0, 1)$, then the output sequence is 100010111100110. Its linear span is 14.

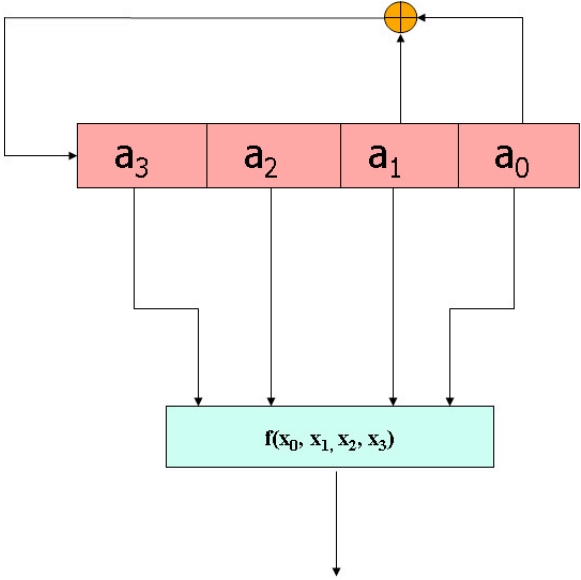


Figure 3: Question 4 (b)-Solution 1

Solution 2: There is one simple solution by choosing $f(x_0) = x_0 + 1$. If the initial state is $(a_3, a_2, a_1, a_0) = (0, 0, 0, 1)$, then the output sequence is 011101100101000. Its linear span is 5. Please see Figure 4.

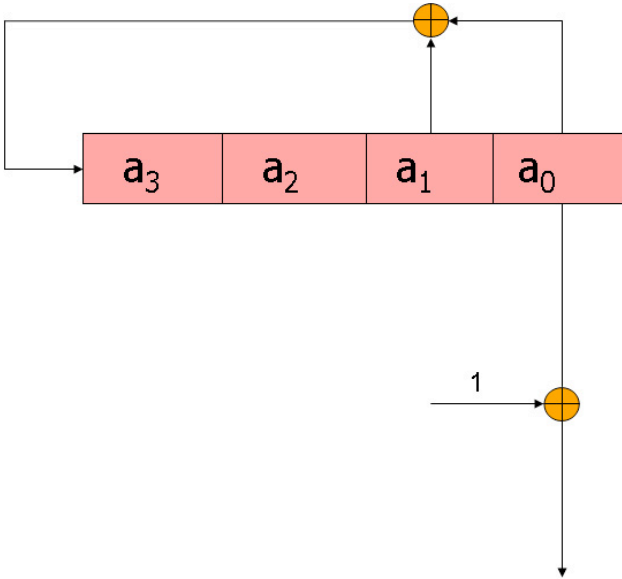


Figure 4: Question 4 (b)-Solution 2