

Solutions to Some Questions in Assignments 2 and 3

Assignment 2

Question 4

Solution. The cyclotomic cosets mod 15 with respect to 2 are given by

$$\begin{aligned} C_0 &= \{0\}, \\ C_1 &= \{1, 2, 4, 8\}, \\ C_3 &= \{3, 6, 12, 9\}, \\ C_5 &= \{5, 10\}, \\ C_7 &= \{7, 14, 13, 11\}. \end{aligned}$$

In order to find a sequence S of period 15 which is constant-on-cosets, we can assign $s_i = 1$ for i belongs to some cosets. For example, define the sequence S by

$$s_i = \begin{cases} 1, & \text{if } i \in C_5; \\ 0, & \text{if } i \in C_0 \cup C_1 \cup C_3 \cup C_7. \end{cases}$$

Then S is 000001000010000. It is constant-on-cosets. Because S is not balance, it does not have the two-level correlation property R -3.

Question 8

Solution. The designs which can be used here are listed as follows:

1. Gold-pair construction: $(2^n - 1, 2^n + 1, 2^{(n+1)/2} + 1)$, where n is odd. If $n = 11$, then we obtain a signal set with parameter $(2047, 2049, 65)$. If $n = 13$, then the bound for the crosscorrelation becomes 129 which is bigger than 80.

The decimation number d can be selected as one of the following values:

- 1) Gold exponent: $d = 2^k + 1$, $(k, n) = 1, k < (n + 1)/2$. Hence $d = 3, 5, 9, 17, 33$.
- 2) Kasami (large set) exponent: $d = 2^{2k} - 2^k + 1$, $(k, n) = 1, k < (n + 1)/2$. Hence $d = 3, 13, 57, 241, 993$.
- 3) Welch conjecture exponent: $d = 2^{(n-1)/2} + 3$. Hence $d = 35$.

Because the number of primitive polynomials with degree 11 is $(23 - 1)(89 - 1)/11 = 176$, the number of the designs from Gold-pair construction is $176 * 10 = 1760$.

2. Kasami (small) signal set: $(2^n - 1, 2^{n/2}, 2^{n/2} + 1)$, where n is even. If $n = 12$, then we obtain a signal set with parameter $(4095, 64, 65)$. If $n = 14$, then the bound for the crosscorrelation becomes 129 which is bigger than 80.

The decimation number d is $2^6 + 1 = 65$. Because the number of primitive polynomials with degree 12 is $3(3 - 1)(5 - 1)(7 - 1)(13 - 1)/12 = 144$, the number of the designs from Kasami (small) signal set is 144.

Assignment 3

Question 1

Solution.

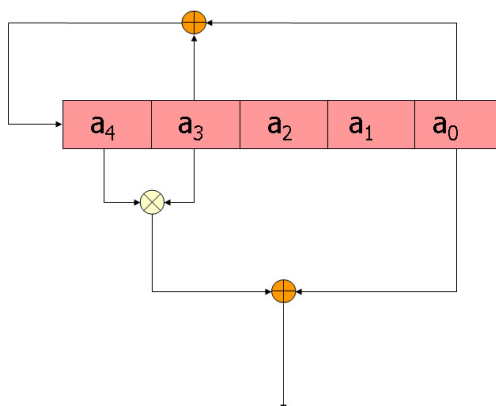


Figure 1: Question 1

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 balanced.) 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 100001100101011110111000110100. It is balanced with linear span 15.

Question 4

Solution.

(a) Please see Figure 2. We choose $d_0 = 0, d_1 = 2, d_2 = 3$, and $f(x_0, x_1, x_2) = x_0x_1x_2$. 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.

(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

$$f(x_0, x_1, x_2, x_3) = x_0x_2x_3 + x_0x_1 + x_1x_2 + x_1x_3 + x_0.$$

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.

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.

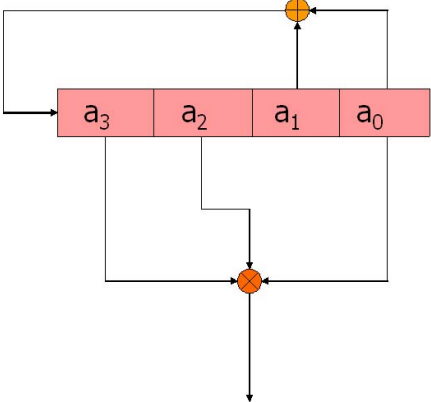


Figure 2: Question 4 (a)

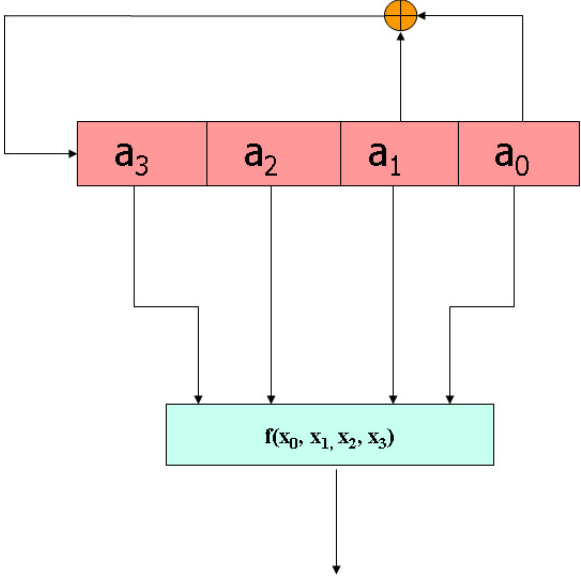


Figure 3: Question 4 (b)-Solution 1

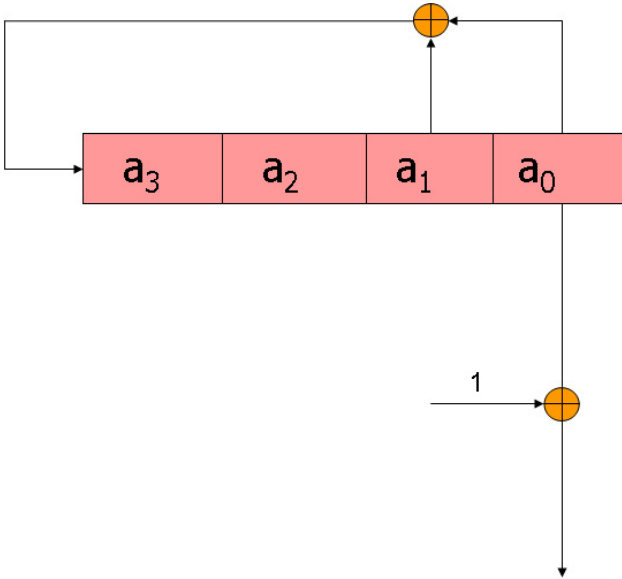


Figure 4: Question 4 (b)-Solution 2