Problems in cryptology, week 4

Exercise 4.11. *Determine the cycle set for each of the following connection polynomials*

a) $1 + D^2 + D^4$ *in GF(2)*

b) $1 + D^4$ *in GF(2)*

c) $1 - D - 2D^2$ *in GF(3)*

d) $1 - 2D - D^2$ *in GF(3)*

e) $1 - D - D^2$ *in GF(3)*

Exercise 4.12. *Determine the cycle set for* $C(D) = 1 - 8D + 2D^2$ *in GF(13).*

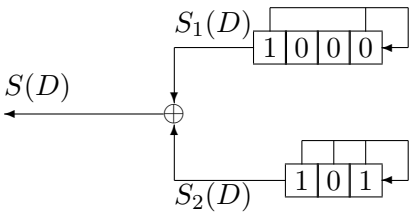
Exercise 4.13.

a) *Find the shortest LFSR in GF(2) that generates the sequence* `[101100001]`.

b) *Find the shortest LFSR in GF(2) that generates the sequence* $[101100001]^\infty$.

Exercise 4.14. *Find the shortest linear feedback shift register over the field GF(*2^4*) that generates the following sequence of 4-tuples:* `A,6,0,B,0,1,4,1,9,B,E`. *Hexadecimal notation has been used. The polynomial* $a_3x^3 + a_2x^2 + a_1x + a_0$ *corresponds to the 4-tuple* (a_3, a_2, a_1, a_0). *The field GF(*2^4*) should be generated by the irreducible polynomial* $\pi(x) = x^4 + x^3 + x^2 + x + 1$.

Exercise 4.15. *A cipher manufacturer has a large collection of short shift registers,* $L \leq 4$. *As a part in one of his ciphers we find the following construction, generating a sequence* $S(D)$.



a) *Find the expressions* $S_i(D) = \frac{P_i(D)}{C_i(D)}$ *for* $S_1(D)$ *and* $S_2(D)$.

b) *If the price for the construction is proportional to the sum of the D-elements, did the designer find the best construction?*

Exercise 4.16 *Find the shortest LFSR that generates the sequence*

$$s = [10000010101000]^\infty + [1010011]^\infty$$

in the field GF(2).