INF 240 - Exercise problems - Sequences

Nikolay Kaleyski

1 Generation of sequences. Finding periods and preperiods

Sequences over finite fields can be given in several different representations, including linear feedback shift registers (LFSR's), characteristic polynomials, and recurrence relations. Converting between them is useful and quite easy. Note that the characteristic polynomial is only defined in the case of a homogeneous sequence, i.e. one with a zero constant term.

Regardless of the concrete representation, one of the most basic tasks involving sequences is, given the first few values of the sequence, to generate further values, typically until it loops, and to find the least period and preperiod of the sequence.

Exercise 1. *Consider the linear recurrence relation*

$$s_{n+4} = s_{n+3} + s_{n+1} + s_n$$

for $n \geq 0$ *over the finite field* $\mathbb{F}_2$.

1. *Draw the corresponding LFSR.*
2. *Find its characteristic polynomial.*
3. *Given the initial state* $(s_0, s_1, s_2, s_3) = (0, 1, 1, 1)$, *determine the least period and the preperiod of the sequence.*

Exercise 2. *Consider the linear recurrence relation*

$$s_{n+4} = s_{n+2} - s_{n+1} + s_n$$

for $n \geq 0$ *over the finite field* $\mathbb{F}_3$.

1. *Draw the corresponding LFSR.*
2. *Find its characteristic polynomial.*
3. *Given the initial state* $(s_0, s_1, s_2, s_3) = (0, 1, 2, 0)$, *determine the least period and the preperiod of the sequence.*

Exercise 3. *Consider the LFSR over* $\mathbb{F}_5$ *given in the following diagram.*

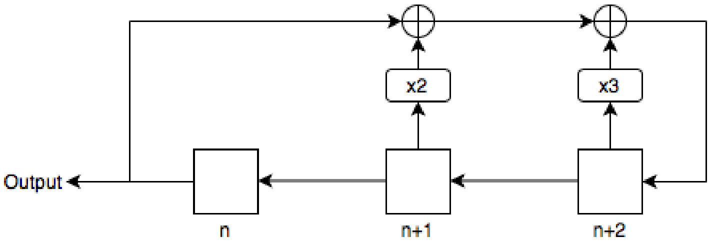

Figure 1: LFSR for Exercise 3

1. *Find the corresponding recurrence relation.*
2. *Find its characteristic polynomial.*
3. *Given the initial state* $(s_0, s_1, s_2) = (0, 1, 2)$, *determine the least period and the preperiod of the sequence.*

Exercise 4. *Consider a sequence over* $\mathbb{F}_3$ *with characteristic polynomial*

$$f(x) = x^5 - x^4 + x^3 - x.$$

1. *Draw a diagram of the LFSR implementing this sequence.*
2. *Write down the corresponding linear recurrence.*
3. *Given the initial state* $(s_0, s_1, s_2, s_3, s_4) = (0, 1, 2, 1, 2)$, *determine the least period and the preperiod of the sequence.*

2 Properties of sequences

Certain properties of a sequence can be derived without explicitly computing the elements that follow from some given initial state. For instance, we know that if the characteristic polynomial of a sequence is primitive, then the corresponding sequence has the largest possible period. Another useful property is that every period of a sequence must be a multiple of its least period.

Exercise 5. *Consider the linear recurrence*

$$s_{n+2} = s_{n+1} + s_n$$

over the finite field $\mathbb{F}_3$. *Find its characteristic polynomial* $f(x)$, *and show that it is primitive. Use this to determine the least period of the sequence corresponding to* $f(x)$ *without computing any elements of the sequence.*

Exercise 6. *Suppose that* $\{s_n\}_n$ *is a periodic sequence over* $\mathbb{F}_2$ *with* $(s_0, s_1) = (0, 1)$ *satisfying*

$$s_{n+21} = s_n$$

and

$$s_{n+70} = s_n$$

for any $n \geq 0$.

1. *Can* 5 *be a period of this sequence?*
2. *What are all possible periods of this sequence?*