B Linear Feedback Shift Registers

Note that the notation used here can differ from the lecture notes. Be careful with indexing (starting from 0 or 1, going from left to right or from right to left etc.).

B.1 Fibonacci and Galois LFSRs

We define two variations of linear feedback shift registers (LFSRs), and prove that they are essentially equivalent. LFSRs are defined over a finite field. Most often this will be the field $\mathbb{F}_2 = \{0, 1\}$, in which case the LFSRs are called binary. We will start with mathematical definitions, followed by a more concrete description.

A Fibonacci LFSR with feedback structure $(a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, $a_{n-1} \neq 0$, can be defined as a function

$$R : \mathbb{F}_q^n \to \mathbb{F}_q, \quad R(b_0, \ldots, b_{n-1}) = (a_0 b_0 + \cdots + a_{n-1} b_{n-1}, b_0, \ldots, b_{n-2}).$$

(1)

A Galois LFSR with feedback structure $(a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, $a_0 \neq 0$, can be defined as a function

$$R : \mathbb{F}_q^n \to \mathbb{F}_q, \quad R(b_0, \ldots, b_{n-1}) = (a_0 b_{n-1}, b_0 + a_1 b_{n-1}, \ldots, b_{n-2} + a_{n-1} b_{n-1})$$

$$= (0, b_0, \ldots, b_{n-2}) + b_{n-1}(a_0, \ldots, a_{n-1}).$$

(2)

Let $R$ be an LFSR (Fibonacci or Galois). If we fix an initial state $s \in \mathbb{F}_q^n$, $s \neq (0, \ldots, 0)$, we can define the state sequence to be

$$R^0(s), R^1(s), R^2(s), \ldots,$$

where $R^0(s) = s$ and $R^{t+1}(s) = R(R^t(s))$, and the output sequence to be

$$r(0), r(1), r(2), \ldots,$$

where $r(t)$ is the last element of $R^t(s)$. Then $R^t(s)$ and $r(t)$ are called the state and output at time moment $t \in \mathbb{Z}_{\geq 0}$, respectively. All of these definitions depend on the initial state. We excluded the zero state $(0, \ldots, 0)$ because it is always mapped to itself, and no other state is mapped to it.

The above LFSRs can also be described as follows: They consist of $n$ cells, indexed from 0 to $n-1$ (starting from the left), each containing an element of $\mathbb{F}_q$. If, at some time moment, the cells contain the values $b_0, \ldots, b_{n-1}$, then, when moving to the next time moment, we first compute the feedback element (it is $a_0 b_0 + \cdots + a_{n-1} b_{n-1}$ for a Fibonacci LFSR and $b_{n-1}$ for a Galois LFSR), then we shift the elements one cell to the right (the rightmost one is thrown out and the leftmost cell filled with 0), and finally we add the feedback element, either to the leftmost cell (Fibonacci), or to every cell multiplied by the corresponding element of the feedback structure (Galois).

The following theorems prove that for every Fibonacci LFSR there exists a Galois LFSR that generates the same output sequences (with different initial states), and vice versa.
Figure 1: The Fibonacci LFSR over $\mathbb{F}_3$ with feedback structure $(2, 1, 0, 2)$. If the initial state is $(1, 0, 1, 2)$, then the next state is $(0, 1, 0, 1)$.

Figure 2: The Galois LFSR over $\mathbb{F}_3$ with feedback structure $(2, 1, 0, 2)$. If the initial state is $(1, 0, 1, 2)$, then the next state is $(1, 0, 2, 0)$.

**Theorem B.1.** The output sequence $r(0), r(1), r(2), \ldots$ of a Fibonacci LFSR with feedback structure $(a_0, \ldots, a_{n-1})$ satisfies the recursion formula

$$r(t + n) = a_0 r(t + n - 1) + \cdots + a_{n-1} r(t).$$

**Proof.** It is easy to see that the state at time moment $t$ must be $(r(t + n - 1), \ldots, r(t))$. At the next time moment, the leftmost element will be $a_0 r(t + n - 1) + \cdots + a_{n-1} r(t)$ by (1). On the other hand, it must be $r(t + n)$.

**Theorem B.2.** The output sequence $r(0), r(1), r(2), \ldots$ of a Galois LFSR with feedback structure $(a_0, \ldots, a_{n-1})$ satisfies the recursion formula

$$r(t + n) = a_{n-1} r(t + n - 1) + \cdots + a_0 r(t).$$

**Proof.** It can be proved inductively using (2) that, for $i = 0, \ldots, n-1$, the $i$th element of the state at time moment $t + i + 1$ contains $a_0 r(t) + \cdots + a_i r(t+i)$. The case $i = n-1$ proves the theorem.

Figure 3: The binary Fibonacci LFSR with feedback structure $(0, 1, 0, 0, 1)$ and the binary Galois LFSR with feedback structure $(1, 0, 0, 1, 0)$. If their initial states are $(1, 0, 1, 0, 1)$ and $(0, 0, 0, 0, 1)$, respectively, then they both generate the same output sequence, beginning with $1, 0, 1, 0, 1$.
B.2 Polynomials

The characteristic polynomial of a Galois LFSR with feedback structure \((a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n\) is
\[
f(x) = x^n - a_{n-1}x^{n-1} - \cdots - a_0x^0 \in \mathbb{F}_q[x].
\]

If the state of a Galois LFSR is \((b_0, \ldots, b_{n-1}) \in \mathbb{F}_q^n\), then the state element is
\[
b_0x^0 + \cdots + b_{n-1}x^{n-1} \pmod{f(x)}.
\]

If \(f(x)\) is irreducible, then the state elements are in the field \(\mathbb{F}_{q^n}\) defined by \(f(x)\).

**Theorem B.3.** Let \(f(x)\) be the characteristic polynomial of a Galois LFSR, and let \(\gamma(t)\) be the state element at time moment \(t\). Then \(\gamma(t+k) = x^k\gamma(t)\) for all \(k \geq 0\).

**Proof.** It is enough to prove the claim for \(k = 1\). If the feedback structure is \((a_0, \ldots, a_{n-1})\) and \(\gamma(t) = b_0x^0 + \cdots + b_{n-1}x^{n-1}\), then
\[
x\gamma(t) = b_0x^1 + \cdots + b_{n-1}x^n
\]
\[
= b_0x^1 + \cdots + b_{n-2}x^{n-1} + b_{n-1}(a_0x^0 + \cdots + a_{n-1}x^{n-1}) = \gamma(t+1)
\]
by \(x^n = a_{n-1}x^{n-1} + \cdots + a_0x^0\) and (2).

**Example B.4.** Consider the Galois LFSR of Figure 2. Its characteristic polynomial is \(f(x) = x^4 - 2x^3 - x - 2 \in \mathbb{F}_3[x]\). Using the notation of Theorem B.3, we have \(\gamma(0) = 1 + x^3 + 2x^4 \pmod{f(x)}\) and
\[
\gamma(1) = x\gamma(0) = x + x^3 + 2x^4 = x + x^3 + 2(2 + x + 2x^3) = 1 + 2x^3 \pmod{f(x)}.
\]

B.3 Periods

A sequence \(u_0, u_1, u_2, \ldots\) is ultimately periodic if there exists integers \(n \geq 0\) and \(p \geq 1\) such that \(u_{i+p} = u_i\) for all \(i \geq n\). Then we can use the notation
\[
u_0, u_1, u_2, \ldots = u_0, \ldots, u_{n-1}, u_n, \ldots, u_{n+p-1}.
\]

If we can take \(n = 0\), then the sequence is periodic. The number \(p\) is a period of the sequence. The smallest period is the period. A sequence that is not ultimately periodic is aperiodic.

**Lemma B.5.** The state and output sequences of an LFSR are periodic and they have the same periods (the period might depend on the initial state).

**Proof.** We give here the basic idea of the proof; details are left as an exercise.

The number of states is finite, so the state sequence must be ultimately periodic. There does not exist two different states leading to the same state, so the state sequence is periodic. A period of the state sequence is clearly a period of the output sequence. Different initial states lead to different output sequences, so a period of the output sequence is a period of the state sequence.
Theorem B.6. Let \( f(x) \) be the characteristic polynomial of an \( n \)-cell Galois LFSR over \( \mathbb{F}_q \). If \( f(x) \) is irreducible, then the period of the output sequence is \( \text{ord}(x) \) in the field \( \mathbb{F}_{q^n} \) defined by \( f(x) \). In particular, the period does not depend on the initial state. If \( f(x) \) is primitive, then the period is \( q^n - 1 \).

Proof. A number \( k \) is a period of the output sequence iff \( \gamma(t + k) = \gamma(t) \) for all \( t \), where \( \gamma(t) \) is the state element at time moment \( t \). By Theorem B.3, this is equivalent to \( x^k \gamma(t) = \gamma(t) \). If \( f(x) \) is irreducible, the elements are in a field, and \( \gamma(t) \neq 0 \) because the zero state was forbidden, so we can divide by \( \gamma(t) \) to get \( x^k = 1 \). This is equivalent to \( \text{ord}(x)|k \), so \( \text{ord}(x) \) is the period. If \( f(x) \) is primitive, then \( \text{ord}(x) = q^n - 1 \). \( \square \)

Example B.7. The polynomial \( 1 + x^3 + x^5 \in \mathbb{F}_2[x] \) is primitive, so the period of the output sequence of the LFSRs of Figure 3 is \( 2^5 - 1 = 31 \).

The following theorem shows that LFSRs with primitive characteristic polynomials have not only long periods but also good statistical properties.

Theorem B.8. Let \( r(0), r(1), r(2), \ldots \) be the output sequence of an \( n \)-cell Galois LFSR over \( \mathbb{F}_q \) with a primitive characteristic polynomial. Let \( k \in \{1, \ldots, n\} \) and

\[
s(t) = (r(t), \ldots, r(t + k - 1)) \in \mathbb{F}_q^k
\]

for all \( t \). Every element of \( \mathbb{F}_q^k \) appears in the sequence \( s(0), \ldots, s(q^n - 2) \) exactly \( q^{n-k} \) times, except \((0, \ldots, 0)\), which appears \( q^{n-k} - 1 \) times.

Proof. First, let \( k = n \). If we reverse \( s(t) \), we get the state at time moment \( t \) of the Fibonacci LFSR with the output sequence \( r(0), r(1), r(2), \ldots \). Because the characteristic polynomial is primitive, the period of the state sequence is \( q^n - 1 \). This is also the number of different nonzero states, so every nonzero element of \( \mathbb{F}_q^n \) appears exactly once in the sequence \( s(0), \ldots, s(q^n - 2) \).

The cases \( k < n \) can be proved with the help of the above case; this is left as an exercise. \( \square \)