3.1 The Linear Complexity of a Bit Sequence

We consider bit sequences $u = (u_i)_{i \in \mathbb{N}} \in \mathbb{F}_2^{\mathbb{N}}$—for the moment infinite ones. We search an LFSR of smallest length that produces the sequence.

If the sequence is generated by an LFSR, it must be periodic. On the other hand every periodic sequence is generated by an LFSR whose length is the sum of the lengths of preperiod and period—namely by the **circular LFSR** that feeds back the bit where the period begins: If $u_{l+i} = u_{k+i}$ for $i \geq 0$, then the taps are $a_{l-k} = 1$, $a_i = 0$ else, as in Figure 3.1. This consideration shows:

Lemma 11 *A bit sequence $u \in \mathbb{F}_2^{\mathbb{N}}$ is generated by an LFSR if and only if it is (eventually) periodic.*

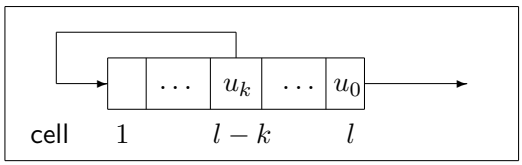


Figure 3.1: A circular LFSR

Definition The **linear complexity** $\lambda(u)$ of a bit sequence $u \in \mathbb{F}_2^{\mathbb{N}}$ is the minimal length of an LFSR that generates u.

For u constant 0 let $\lambda(u) = 0$, for a non-periodic u set $\lambda(u) = \infty$.

This concept of complexity uses the quite special machine model of an LFSR.

Remarks and examples

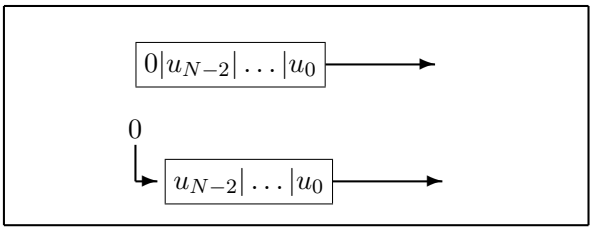
1. Let $\tau(u)$ be the sum of the lengths of the preperiod and the period of u. Assume that u is generated by an LFSR of length l. Then
$$\lambda(u) \leq \tau(u) \leq 2^l - 1 \quad \text{and} \quad \lambda(u) \leq l.$$
2. The periodically repeated sequence $0, \ldots, 0, 1$ ($l-1$ zeroes) has period l and linear complexity l. An LFSR of length $< l$ would start with the null vector as initial value and thus force the complete output sequence to zero.

For a finite bit sequence $u = (u_0, \ldots, u_{N-1}) \in \mathbb{F}_2^N$ the linear complexity is analogously defined. In particular $\lambda(u)$ is the minimum integer l for which there exist $a_1, \ldots, a_l \in \mathbb{F}_2$ with
$$u_i = a_1 u_{i-1} + \cdots + a_l u_{i-l} \quad \text{for } i = l, \ldots, N-1.$$

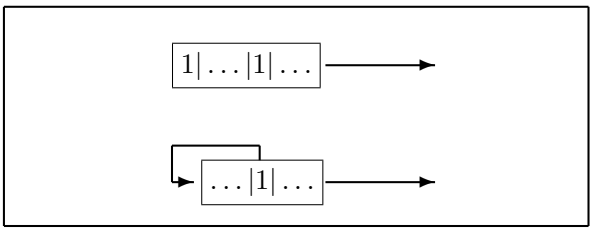
3. For $u \in \mathbb{F}_2^N$ we have $0 \leq \lambda(u) \leq N$.

4. $\lambda(u) = 0 \iff u_0 = \cdots = u_{N-1} = 0$.

5. $\lambda(u) = N \iff u = (0, \ldots, 0, 1)$. The implication "$\Longleftarrow$" follows as in remark 2. For the reverse direction assume $u_{N-1} = 0$. Then we can take the LFSR of length $N - 1$ with feedback constant 0—the two LFSRs



both generate the same output of length N. This contradiction shows that $u_{N-1} = 1$. Assume there is a 1 at an earlier position. Then we can take the LFSR of length $N - 1$ that feeds back exactly this position—the two LFSRs



both generate the same output up to length N.

6. From the first $2\lambda(u)$ bits of the sequence u all the following bits are predictable. (Note that the cryptanalyst who knows that many bits of the sequence, but no further bits, also doesn't know $\lambda(u)$. Therefore she doesn't know that her predictions will be correct from now on. This ignorance doesn't prevent her from correctly predicting bit for bit!)