LFSR sequences

September 2013

Outline of presentation:

1. History and motivation
2. Basic definitions
3. Connection with polynomials
4. Randomness properties

Linear recurring sequences

Around 1200:
$F_n = F_{n-1} + F_{n-2}$
0, 1, 1, 2, 3, 5, 8, 13 ...

Leonardo Pisano
(Fibonacci)

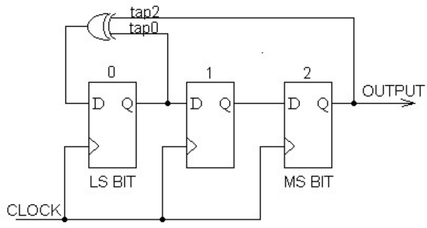
Linear recurring sequences

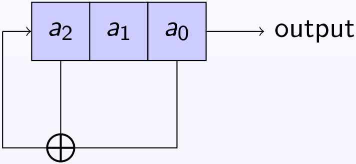
Throughout the years:

- integers
- reals
- complex
- integers mod p
- finite fields (1900)


The Fifties
If your husband ever finds out
you're not "store-testing" for fresher coffee . . .
. . . if he discovers you're still taking chances on getting flat, stale coffee . . . woe be unto you! For today there's a sure and certain way to test for freshness before you buy
Chase & Sanborn COFFEE
Why we have the youngest customers in the business
Nothing does it like Seven-Up!

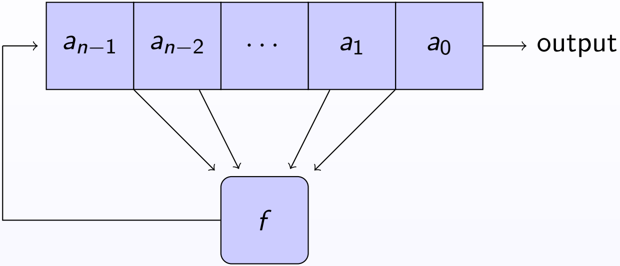
Binary linear recurring sequences are implemented in circuits using feedback shift registers





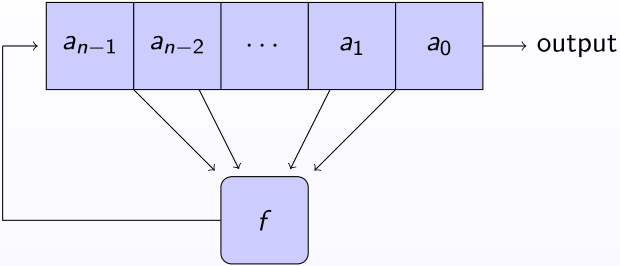
$$a_n = a_{n-1} + a_{n-3}$$

$$a_0 = 1, a_1 = 0, a_2 = 0$$



Definition (q-ary FSR sequence)

A sequence $\mathbf{a} = (a_0, a_1, \dots)$ is called a q-ary FSR sequence generated by a n-stage FSR with feedback function $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ and initial state $(a_0, \dots, a_{n-1})$ if it satisfies the recursion $a_{k+n} = f(a_k, \dots, a_{k+n-1}),\ k = 0, 1, 2, \dots$



Definition (LFSR sequence)

A FSR sequence with feedback function f is called a LFSR sequence if f is linear. That is, f is of the form

$$f(a_0, \ldots, a_{n-1}) = c_{n-1}a_{n-1} + c_{n-2}a_{n-2} + \cdots + c_1 a_1 + c_0$$

with $c_i \in \mathbb{F}_q$

Definition

Let $\{a\}_{i\in\mathbb{N}}$ be a q-ary sequence. If there exists an $r > 0$ such that $a_{i+r} = a_i$ for all $i \geq 0$ then the sequence is said to be periodic with period r.

Theorem

The period of a sequence generated by a n-stage LFSR over $\mathbb{F}_q$ divides $q^n - 1$.

Connection with polynomials

Definition (Left shift operator)

For any sequence $\{a_i\}_{i\geq 0} = (a_0, a_1, \dots) \in V(\mathbb{F}_q)$ the left shift operator L is defined as $L(a_0, a_1, \dots) = (a_1, a_2, \dots)$.

L is a linear transformation of the v.s. of sequences over $\mathbb{F}_q$

Suppose $\mathbf{a} = (a_0, a_1, \dots)$ satisfies

$$a_{k+n} = \sum_{i=0}^{n-1} c_i a_{k+i}, k \in \mathbb{Z}_{\geq 0}, c_i \in \mathbb{F}_q$$

Then we also have

$$L^n(a_0, a_1, \dots) = \sum_{i=0}^{n-1} c_i L^i(a_0, a_1, \dots).$$

Equivalently,

$$\left(L^n - \sum_{i=0}^{n-1} c_i L^i\right)(a_0, a_1, \dots) = (0, 0, \dots)$$

Denote

$$f(x) = x^n - \sum_{i=0}^{n-1} c_i x^i$$

We have

$$f(L) = L^n - c_{n-1}L^{n-1} - \cdots - c_1 L - c_0 I$$

and $f(L)(a_0, a_1, \dots) = \mathbf{0}$

Definition

For any infinite sequence $(a_0, a_1, \dots)$ if there exists a nonzero polynomial $f \in \mathbb{F}_q[x]$ such that $f(L)(a_0, a_1, \dots) = 0$, then the sequence $(a_0, a_1, \dots)$ is called an LFSR sequence. The polynomial f is called a characteristic polynomial of $(a_0, a_1, \dots)$ over $\mathbb{F}_q$. The reciprocal polynomial of f is called the feedback polynomial of $(a_0, a_1, \dots)$.

Definition

Let **a** be a q-ary LFSR sequence and P be the set of all characteristic polynomials of **a**. The lowest degree polynomial in P is called the minimal polynomial of **a** over $\mathbb{F}_q$.

Theorem

Let **a** *be an LFSR sequence over* $\mathbb{F}_q$ *and* $m \in \mathbb{F}_q[x]$ *be a minimal polynomial for the sequence* **a**. *This minimal polynomial of* **a** *is unique and satisfies*

- $m(L)(\mathbf{a}) = 0$
- *for* $f \in \mathbb{F}_q[x]$, *we have* $f(L)(\mathbf{a}) = 0$ *if and only if* $m|f$

Theorem

Let **a** *be an LFSR sequence with minimal polynomial* m. *Assume that* m *is irreducible over* $\mathbb{F}_q$ *of degree* n. *Let* α *be a root of* m *in* $\mathbb{F}_{q^n}$. *We have* $period(\mathbf{a}) = period(m) = \mathrm{ord}(\alpha)$.

maximal sequences

Theorem

The period of a sequence generated by a n-stage LFSR over $\mathbb{F}_q$ divides $q^n - 1$.

Definition (m-sequence)

A sequence over $\mathbb{F}_q$ generated by a n-stage LFSR is called a *maximal length sequence*, or in short a *m-sequence*, if it has period $q^n - 1$.

We have the following important fact for such sequences.

Theorem

A LFSR sequence is a m-sequence if and only if its characteristic polynomial is primitive.

Definition

The linear complexity of a LFSR sequence is the degree of its minimal polynomial. Equivalently, it is the number of registers of the smallest LFSR that produces the sequence

Definition

1. We define k consecutive zeros (ones) preceded by a one (zero) and followed by a one (zero) of a binary sequence of period N as a run of k zeros (ones).
2. For a binary sequence $\mathbf{a}$ of period N, the autocorrelation function of $\mathbf{a}$, denoted by $c_{\mathbf{a}}(\tau)$ is defined as

$$c_{\mathbf{a}}(\tau) = \sum_{i=0}^{N-1} (-1)^{a_i + a_{i+\tau}}$$

where the indices are taken modulo N.

Definition (Golomb's randomness postulates)

- **Balance property.** In every period, the number of zeros is nearly equal to the number of ones (the disparity does not exceed 1, or $|\sum_{i=0}^{N-1}(-1)^{a_i}| \leq 1$).
- **The run property.** In every period, half of the run have length 1, one fourth have length 2, one eighth have length 3, and so on. For each of these lengths there are the same number of runs of 0's and runs of 1's.
- **Two level autocorrelation.** The autocorrelation function $c(\tau)$ is two-valued given by

$$c(\tau) = \begin{cases} N & \text{if } \tau = 0 \mod N \\ k & \text{if } \tau \neq 0 \mod N, \end{cases}$$

where k is a constant. If $k = -1$ for N odd, or $k = 0$ for N even, we say that the sequence has the *ideal two level autocorrelation function*.

Definition (Golomb's randomness postulates)

- **The ideal k-tuple distribution.** In every period of $\mathbf{a}$, if each nonzero k-tuple $(l_1, l_2, \ldots, l_k) \in \mathbb{F}_q^k$ occurs q^{n-k} times and the zero k-tuple occurs $q^{n-k} - 1$ times, then we say that the sequence satisfies the ideal k-tuple distribution

Theorem

m-sequences satisfy all of the above properties