1.7 Multistep generators

Multistep (linear recursive) generators are a common generalization of linear congruential generators and LFSRs. A convenient framework for their treatment is a finite ring R (commutative with 1); this comprises not only the residue class rings $\mathbb{Z}/m\mathbb{Z}$ but also the finite fields including the prime fields $\mathbb{F}_p$.

An r-step linear recursive generator outputs a sequence (x_n) in R by the rule

$$x_n = a_1 x_{n-1} + \cdots + a_r x_{n-r} + b.$$

The parameters of this procedure are

- the **recursion depth** r (assume $a_r \neq 0$),
- the **coefficient tuple** $a = (a_1, \ldots, a_r) \in R^r$,
- the **increment** $b \in R$,
- a **start vector** $(x_0, \ldots, x_{r-1}) \in R^r$.

The linear recursive generator is called **homogeneous** if the increment $b = 0$, **inhomogeneous** otherwise.

Figure 1.9 visualizes the operation of a linear recursive generator in analogy with an LFSR.

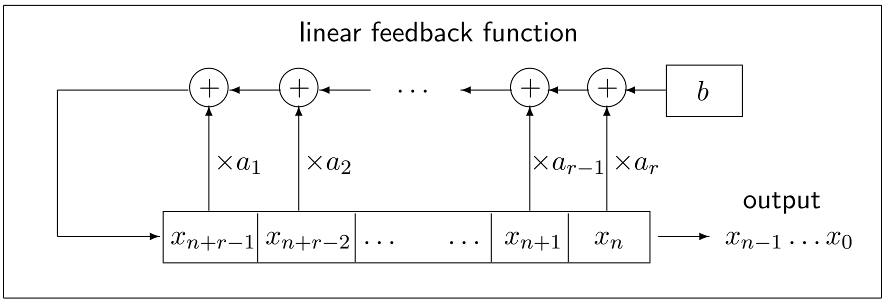

Figure 1.9: A linear recursive generator

Inhomogeneous linear recursive generators easily reduce to homogeneous ones, but only with an additional recursion step: Subtracting the two equations

$$\begin{aligned} x_{n+1} &= a_1 x_n + \cdots + a_r x_{n-r+1} + b, \\ x_n &= a_1 x_{n-1} + \cdots + a_r x_{n-r} + b, \end{aligned}$$

we get

$$x_{n+1} = (a_1 + 1)x_n + (a_2 - a_1)x_{n-1} \cdots + (-a_r)x_{n-r}.$$

Example In the case $r = 1$, $x_n = ax_{n-1} + b$, this formula becomes

$$x_n = (a+1)x_{n-1} - ax_{n-2}.$$

In the following we often neglect the inhomogeneous case.

In the homogeneous case we introduce the **state vectors** $x_{(n)} = (x_n, \ldots, x_{n+r-1})^t$ and write

$$x_{(n)} = Ax_{(n-1)} \quad \text{for } n \geq 1,$$

using the **companion matrix**

$$A = \begin{pmatrix} 0 & 1 & \ldots & 0 \\ & \ddots & \ddots & \\ & & & 1 \\ a_r & a_{r-1} & \ldots & a_1 \end{pmatrix}.$$

This suggests the next step of generalization: the **matrix generator** with parameters:

- an $r \times r$-matrix $A \in M_r(R)$,
- a start vector $x_0 \in R^r$.

The output sequence is generated by the formula

$$x_n = Ax_{n-1} \in R^r.$$