1.8 General linear generators

Even more general (and conceptually simpler) is the abstract algebraic version, the **general linear generator**. This is the setting:

- a ring R (commutative with 1),
- an R-module M,
- an R-linear map $A : M \longrightarrow M$,
- a start value $x_0 \in M$.

From this we generate a sequence $(x_n)_{n\in\mathbb{N}}$ by the formula

$$x_n = Ax_{n-1} \quad \text{for } n \geq 1. \tag{6}$$

Examples

1. For a homogeneous linear congruential generator we have
$$R = \mathbb{Z}/m\mathbb{Z}, \quad M = R \quad (r = 1), \quad A = (a).$$
2. For an inhomogeneous linear congruential generator we have
$$R = \mathbb{Z}/m\mathbb{Z}, \quad M = R^2 \quad (r = 2), \quad A = \begin{pmatrix} 0 & 1 \\ -a & a+1 \end{pmatrix}.$$
3. For an LFSR we have
$$R = \mathbb{F}_2, \quad M = \mathbb{F}_2^l \quad (r = l), \quad A = \text{the companion matrix},$$
that contains only 0's and 1's.

In the case of a finite M the recursion (6) can assume only finitely many different values, therefore (after a potential preperiod) must become periodic.

Proposition 3 *Let M be a finite R-module and $A : M \longrightarrow M$ be linear. Then the following statements are equivalent:*

(i) *All sequences generated by the corresponding general linear generator (6) are purely periodic.*

(ii) *A is bijective.*

Proof. "(i) $\Longrightarrow$ (ii)": Assume that A is not bijective. Since M is finite A is not surjective. Hence there is an $x_0 \in M - A(M)$. Then $x_0 = Ax_t$ can never occur, hence the sequence is not purely periodic.

"(ii) $\Longrightarrow$ (i)": Let A be bijective and x_0, an arbitrary start vector. Let t be the first index such that x_t assumes a value that occured before, and let s be the smallest index with $x_t = x_s$. Since $x_s = Ax_{s-1}$ and $x_t = Ax_{t-1}$ the assumption $s \geq 1$ leads to

$$x_{t-1} = A^{-1}x_t = A^{-1}x_s = x_{s-1},$$

contradicting the minimality of t. $\diamond$

Looking at the companion matrix we immediately apply this result to homogeneous multistep congruential generators, and in particular to LFSRs:

Corollary 1 *A homogeneous linear congruential generator of recursion depth r always generates purely periodic sequences if the coefficient a_r is invertible in $\mathbb{Z}/m\mathbb{Z}$.*

This is true also in the inhomogeneous case since the formula

$$x_{n-r} = a_r^{-1}(x_n - a_1x_{n-1} - \cdots - a_{r-1}x_{n-r+1} - b)$$

reproduces the sequence in the reverse direction.

Corollary 2 *An LFSR of length l generates only purely periodic sequences if the rightmost tap is set (that is, $a_l \neq 0$).*