2.2 Linear Generators over Fields

In this section we consider the special case where $R = K$ is a field and M a finite dimensional vector space over K (hence a Noetherian K-module).

Then we have to find the minimal k with

$$\dim(Kx_0 + \cdots + Kx_k) = \dim(Kx_0 + \cdots + Kx_{k-1})$$

and then to find the linear combination

$$x_k = c_1 x_{k-1} + \cdots + c_k x_0.$$

This is a standard exercise in linear algebra.

For a concrete calculation we chose a fixed basis $(e_1, \ldots, e_m)$ of M. Let

$$x_n = \sum_{i=1}^{m} x_{in} e_i$$

denote the corresponding basis representation. Since $\operatorname{rank}(x_0, \ldots, x_{k-1}) = k$, there is a set $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, m\}$ of indices with $\#I = k$ such that the matrix

$$X = (x_{ij})_{i\in I, 0\leq j<k} = \begin{pmatrix} x_{i_1 0} & \ldots & x_{i_1 k-1} \\ \vdots & & \vdots \\ x_{i_k 0} & \ldots & x_{i_k k-1} \end{pmatrix}$$

is invertible. The coefficients c_j in the relation

$$x_k = \sum_{j=0}^{k-1} c_j x_j,$$

are not yet known, we get them by substituting

$$\sum_{i=1}^{m} x_{ik} e_i = \sum_{j=0}^{k-1} \sum_{i=1}^{m} c_j x_{ij} e_i,$$

hence by the uniqueness of basis coefficients

$$x_{ik} = \sum_{j=0}^{k-1} x_{ij} c_j \quad \text{for all } i \in I,$$

or, in matrix notation,

$$\bar{x} = (x_{ik})_{i\in I} = X \cdot c.$$

The solution for the coefficients c_j is

$$c = X^{-1} \cdot \bar{x}.$$

This proves the first two statements of the following proposition that extends Proposition 4:

Proposition 6 *Under the assumptions of Proposition 4 let $R = K$ be a field and M be finite dimensional of dimension m. Then:*

(i) *The minimal k that fulfils the statements on r in Proposition 4 is the smallest index with $\dim(Kx_0 + \cdots + Kx_k) = k$, and $k \leq m$.*

(ii) *The coefficients $c_1, \ldots, c_k$ are determined by a system of linear equations with an invertible square coefficient matrix whose entries consist of basis coefficients of $x_0, \ldots, x_{k-1}$.*

(iii) *If $k = m$, then A is uniquely determined by the basis coefficients of $x_0, \ldots, x_k$.*

Proof. (iii) Let

$$X_1 = (x_m, \ldots, x_1),\ X_0 = (x_{m-1}, \ldots, x_0) \in M_m(K).$$

Then $X_1 = AX_0$ in matrix representation for the basis $(e_1, \ldots, e_m)$ of M. Since $\operatorname{rank} X_0 = m$ the matrix X_0 is invertible, and

$$A = X_1 X_0^{-1},$$

as claimed. ◇

If A is invertible, then we can determine the sequence (x_n) also in backwards direction as soon as we have a subsequence $x_t, \ldots, x_{t+m}$ of length $m+1$ with $\operatorname{rank}(x_t, \ldots, x_{t+m-1}) = m$ at our disposition.

Example

For the special case of an r-step homogeneous linear congruential generator $x_n = a_1 x_{n-1} + \cdots + a_r x_{n-r}$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ where p is prime we use the companion matrix

$$A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ a_r & \ldots & a_2 & a_1 \end{pmatrix}, \quad \operatorname{Det} A = (-1)^r a_r.$$

In this case A is invertible if and only if $a_r \neq 0$, a condition we may assume without loss of generality—otherwise the recursion depth would be $< r$.

For predicting the sequence we need at most $r+1$ state vectors, or $2r$ elements of the sequence:

Corollary 1 *An r-step homogeneous linear congruential generator with known prime module is predictable given the $2r$ elements $x_0, \ldots, x_{2r-1}$ of the output sequence.*

Corollary 2 *An LFSR of length l is predictable from the first $2l$ output bits.*

Corollary 3 *A homogeneous linear congruential generator with known prime module is predictable from x_0, x_1, an inhomogeneous one, from x_0, x_1, x_2, x_3.*

In the Section 2.4 we'll see that even x_0, x_1, x_2 suffice.

These results knock off LFSRs as sources of key bits for cryptological applications. Keeping the length secret is useless since the attacker may easily determine it by trial and error, putting up with a slight complication of the attack.

For linear congruential generators we might hope that keeping the module m secret (and maybe not choosing a prime) might erect a serious obstacle. However we'll also put this hope at rest in Section 2.5.