1.9 Matrix generators over finite fields

A matrix generator over a field K is completely specified by an $r \times r$ matrix

$$A \in M_r(K)$$

(except for the choice of the start vector $x_0 \in K^r$). The objective of the present section is the characterization of the sequences with maximum period length.

In the polynomial ring $K[T]$ in one indeterminate T the set

$$\{\rho \in K[T] \mid \rho(A) = 0\}$$

is an ideal. Since $K[T]$ is a principal ring (even Euclidean) this ideal is generated by a unique monic polynomial μ. This polynomial is called the **minimal polynomial** of A. Since the matrix A is a zero of its own characteristic polynomial χ we have $\mu|\chi$. If A is invertible, then the absolute term of μ is $\neq 0$; otherwise μ would have the root 0, and A, the eigenvalue 0.

Lemma 4 *Let K be a field, $A \in GL_r(K)$, a matrix of finite order t, μ, the minimal polynomial of A, $s = \deg \mu$, $R := K[T]/\mu K[T]$, and $a \in R$, the residue class of T. Then:*

$$a^k = 1 \Longleftrightarrow \mu | T^k - 1 \Longleftrightarrow A^k = \mathbf{1}.$$

In particular $a \in R^\times$, t is also the order of a, and $\mu | T^t - 1$.

Proof. R is a K-algebra of dimension s. If $\mu = b_s T^s + \cdots + b_0$ (where $b_s = 1$), then

$$\mu - b_0 = T \cdot (b_s T^{s-1} + \cdots + b_1).$$

Since $b_0 \neq 0$, the residue class $T \bmod \mu$ is invertible, hence $a \in R^\times$. Since a^k is the residue class of T^k all the equivalences follow. $\diamond$

Corollary 1 *If K is a finite field with q elements, then*

$$t \leq \#R^\times \leq q^s - 1 \leq q^r - 1.$$

From now on let K be a finite field with q elements. Then also the group $GL_r(K)$ of invertible $r \times r$-matrices is finite. The vector space K^r consists of q^r vectors. We know already that every sequence from the matrix generator corresponding to $A \in GL_r(K)$ is purely periodic. One full cycle consists of the null vector $0 \in K^r$ alone. The remaining vectors in general distribute over several cycles. If s is the length of such a cycle, and x_0, the corresponding start vector, then $x_0 = x_s = A^s x_0$. Hence A^s has the eigenvalue 1, and consequently, A has as eigenvalue an s-th root of unity.

Maybe all vectors $\neq 0$ are in a single cycle of the maximum possible period length $q^r - 1$. In this case $A^s x = x$ for all vectors $x \in K^r$ if $s = q^r - 1$, but not for a smaller exponent > 0. Hence $t = q^r - 1$ is the order of A. This shows:

Corollary 2 *Let K be finite with q elements. Then:*

(i) *If the matrix generator for A and a start vector $\neq 0$ outputs a sequence of period s, then A has as eigenvalue an s-th root of unity.*

(ii) *If there is an output sequence of period length $q^r - 1$, then $t = q^r - 1$ is the order of A.*

Lemma 5 *Let K be a finite field with q elements, and $\varphi \in K[T]$ be an irreducible polynomial of degree d. Then $\varphi | T^{q^d - 1} - 1$.*

Proof. The residue class ring $R = k[T]/\varphi K[T]$ is an extension field of degree $d = \dim_K R$, hence has $h := q^d$ elements, and R contains at least one zero a of φ, namely the residue class of T. Since each $x \in R^\times$ satisfies the equation $x^{h-1} = 1$ we conclude that a is also a zero of $T^{h-1} - 1$. Hence $\mathrm{ggT}(\varphi, T^{h-1} - 1)$ is not a constant. Since φ is irreducible $\varphi | T^{h-1} - 1$. $\diamond$

Definition Let K be a finite field with q elements. A polynomial $\varphi \in K[T]$ of degree d is called **primitive** if φ is irreducible and is not a divisor of $T^k - 1$ for $1 \leq k < q^d - 1$.

Theorem 1 *Let K be a finite field with q elements and $A \in GL_r(K)$. Then the following statements are equivalent:*

(i) *The matrix generator for A generates a sequence of period $q^r - 1$.*

(ii) *The order of A is $q^r - 1$.*

(iii) *The characteristic polynomial χ of A is primitive.*

Proof. "(i) $\Longrightarrow$ (ii)": See Corollary 2 (ii).

"(ii) $\Longrightarrow$ (iii)": In Corollary 1 we now have $t = q^r - 1$. Hence $\#R^\times = q^s - 1$, hence R is a field, and thus μ is irreducible. Moreover $s = r$, hence $\mu = \chi$, and μ is not a divisor of $T^k - 1$ for $1 \leq k < q^r - 1$ by Lemma 4. Therefore μ is primitive.

"(iii) $\Longrightarrow$ (i)": Since χ is irreducible, $\chi = \mu$. The residue class a of T is a zero of μ and has multiplicative order $q^r - 1$ by the definition of "primitive". Since taking the q-th power is an automorphism of the field R that fixes K elementwise all the r powers a^{q^k} for $0 \leq k < r$ are zeroes of μ, and they are all different. Therefore they must represent all the zeroes, and they all have multiplicative order $q^r - 1$. Hence A has no eigenvalue of lower order. By Corollary 2 (i) there is no shorter period. $\diamond$

For an LFSR take A as the companion matrix as in Section 1.7. Hence the characteric polynomial is $T^l - a_1 T^{l-1} - \cdots - a_l$.

Corollary 1 *An LFSR of length l generates a sequence of the maximum possible period length $2^l - 1$ if and only if its characteristic polynomial is primitive, and the start vector is $\neq 0$.*

This result reduces the construction of LFSRs that generate maximum period sequences to the construction of primitive polynomials over the field $\mathbb{F}_2$.

The special case of dimension $r = 1$ describes a multiplicative generator $x_n = a x_{n-1}$ over the finite field K with q elements. The corresponding 1×1 matrix $A = (a)$ is the multiplication by a. Thus a is the only eigenvalue, and $\chi = T - a \in K[T]$ is the characteristic polynomial. It is linear, hence irreducible. Since

$$\chi | T^k - 1 \Longleftrightarrow a \text{ is a zero of } T^k - 1 \Longleftrightarrow a^k = 1,$$

χ is primitive if and only if a is a generating element of the multiplicative group $K^\times$, hence a primitive element. This proves the following slight generalization of the corollary of Proposition 2.

Corollary 2 *The multiplicative generator over K with multiplier a generates a sequence of period $q - 1$ if and only if a is primitive and the start value is $x_0 \neq 0$.*