Linear Recurrences with a Single Minimal Period

Robert Israel

March 27, 2024

Consider an m-step linear recurrence over a finite field $\mathbb{F}$:

$$x(k) = \sum_{i=1}^{m} c_i x(k-i)$$

where $c_m \neq 0$. Each m-tuple $(a(0), \ldots, a(m-1)) \in \mathbb{F}^m$ determines a sequence $x(k)$ with the initial condition $x(i) = a(i)$ for $0 \leq i \leq m-1$, which is periodic because $\mathbb{F}^m$ is finite [1]. We wish to determine whether the minimal period of the sequence is the same for all initial conditions except $(0, \ldots, 0)$ (which has period 1).

Let M be the $m \times m$ matrix with last row $(c_m, c_{m-1}, \ldots, c_1$, first super-diagonal all 1's, and all other entries 0. The recurrence can be written in matrix-vector form as $X(k) = MX(k-1)$ where $X(k) = (x(k+1-m), x(k+2-m), \ldots, x(k))^T$. Thus for the case $m = 3$ we have

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{pmatrix} \text{ and } \begin{pmatrix} x(k-2) \\ x(k-1) \\ x(k) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ c_3 & c_2 & c_1 \end{pmatrix} \begin{pmatrix} x(k-3) \\ x(k-2) \\ x(k-1) \end{pmatrix}$$

' The characteristic polynomial of M is $C(z) = z^m - c_1 z^{m-1} - \ldots - c_m$. This is also the minimal polynomial of M.

Now the sequence with initial condition $v \in \mathbb{F}^m$ has period k if $M^k v = v$. The minimal period for initial condition v is the least positive integer k such that $M^k v = v$. All periods for v will be multiples of this minimal period by positive integers.

Let $G(z) = \gcd(z^k - 1, C(z))$. Then $z^k - 1 = G(z)Q(z)$ and $C(z) = G(z)R(z)$ for some $Q(z), R(z) \in \mathbb{F}[z]$, so $G(M)v = 0$ for $v \in \mathrm{Ran}(R(z))$. If $G(z)$ has positive degree, this is not just $\{0\}$ because $C(z)$ is the minimal polynomial of M), and then $M^k v - v = Q(M)G(M)v = 0$, i.e. such v will have period k. On the other hand, by Bezout's identity $G(z) = A(z)(z^k - 1) + B(z)C(z)$ for some $A(z), B(z) \in \mathbb{F}[z]$, so $G(M) = A(M)(M^k - 1)$.

[1] Note that since $c_m \neq 0$ and we are working over a field, the sequence can be run backwards as well. So if $(x(k), \ldots, x(k+m-1)) = (x(j), \ldots, x(j+m-1))$ with $k > j$, then $(x(k-j), \ldots, x(k-j+m-1)) = (x(0), \ldots, x(m-1))$. Thus the sequence is periodic, not just everntually periodic.

If $x^k - 1$ is not divisible by $C(z)$, so G has degree $< m$, then $G(M) \neq 0$ so $M^k - 1 \neq 0$, and thus not all nonzero initial conditions v have period k. Thus a necessary and sufficient condition for the minimal period to be the same for all initial conditions except $(0, \ldots, 0)$ is that the least k for which $z^k - 1$ is divisible by $C(z)$ is also the least k for which $z^k - 1$ and $C(z)$ are not coprime.

For a polynomial $q(z)$ over $\mathbb{F}$ with $q(0) \neq 0$, I will denote the least k such that $x^k - 1$ is divisible by $q(z)$ as $K(q(z))$.

If $z^k - 1$ is divisible by $q(z)^e$ for some $e > 1$, say $z^k - 1 = q(z)^e A(z)$, then taking the derivative with respect to z we have $kz^{k-1} = eq(z)^{e-1}q'(z)A(z) + q(z)^e A'(z)$, Of course $q(0) \neq 0$, so this can only be true if k is a multiple of the characteristic of $\mathbb{F}$. On the other hand, if p is the characteristic, $z^{jp} - 1 = (z^j - 1)^p$, so if $q(z)$ is a factor of $z^j - 1$, $q(z)^p$ is a factor of $z^{kj} - 1$. And if $z^{jp} - 1$ is divisible by an irreducible polynomial $q(z)$, then $z^j - 1$ must be divisible by $q(z)$, and $z^{jp} - 1$ is divisible by $q(z)^p$. In particular, if the minimal period is the same for all initial conditions except $(0, \ldots, 0)$, $C(z)$ must be squarefree.

In the case of a linear factor $z - r$, $z^k - 1$ is divisible by $z - r$ if and only if $r^k - 1 = 0$, Thus $K(z - r)$ is the order of r in the multiplicative group $F^\times$ of F. This can be efficiently computed in Maple using `MultiplicativeOrder` in the `NumberTheory` package.

For an irreducible factor $q(z)$ of higher degree, we consider the splitting field $\mathbb{K}$ of $q(z)$. If $z^k - 1$ is divisible (over $\mathbb{F}$) by $q(z)$, then $r^k - 1 = 0$ (in $\mathbb{K}$) for any root of $q(z)$. Thus $K(q(z)$ is the multiplicative order of a root of $q(z)$ in $\mathbb{K}^\times$. This can be efficiently computed in Maple using `order` in the `GF` package.