PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 34, Number 2, August 1972

SHIFT DYNAMICAL SYSTEMS OVER FINITE FIELDS

MELVYN B. NATHANSON[1]

ABSTRACT. A trajectory over the finite field F_q is a function from the integers I to F_q. The set $X(F_q)$ of all trajectories over F_q is a topological vector space in the product topology induced by the discrete topology on F_q, and coordinatewise addition and scalar multiplication of trajectories. Let ϕ be a continuous linear operator on $X(F_q)$ which commutes with the shift. If x is a trajectory over F_q, then the ϕ-orbit of x is the sequence of trajectories x, $\phi(x)$, $\phi^2(x)$, $\cdots$. Suppose that ϕ is not a scalar multiple of the identity.
THEOREM. *The trajectory x is periodic if and only if the ϕ-orbit of x is eventually periodic.*

Let S be a finite set, and let I be the set of all integers. A *trajectory over S* is a function from I to S. Let $X(S)$ be the set of all trajectories over S. The discrete topology on S induces a product topology on $X(S)$. The *shift* is the continuous map $\sigma: X(S) \to X(S)$ defined by $(\sigma(x))(i) = x(i+1)$ for all $x \in X(S)$ and $i \in I$. The pair $(X(S), \sigma)$ is called the *shift dynamical system over S*.

A shift-invariant operator on S is a continuous map $\phi: X(S) \to X(S)$ which commutes with the shift. These operators have been characterized by Curtis, Hedlund, and Lyndon [**1**]. Let S^n be the set of n-tuples of elements of S, and let f be any function from S^n to S. Let $m \in I$. Define $\phi: X(S) \to X(S)$ by

$$(\phi(x))(i) = f(x(i + m + 1), x(i + m + 2), \cdots, x(i + m + n)).$$

It is proved in [**1**] that ϕ is a shift-invariant operator on $X(S)$, and, conversely, that every shift-invariant operator on $X(S)$ has this form for some integers m and n, and some function $f: S^n \to S$.

Let ϕ be a shift-invariant operator on $X(S)$, and let $x \in X(S)$. The *ϕ-orbit of x* is the sequence of trajectories x, $\phi(x)$, $\phi^2(x)$, $\phi^3(x)$, $\cdots$. The ϕ-orbit of x is *eventually periodic* if $\phi^{k+Q}(x) = \phi^k(x)$ for some positive

---

Received by the editors August 24, 1971.
AMS 1970 *subject classifications*. Primary 58F20, 39A40; Secondary 12C10, 46A45, 54H20.
Key words and phrases. Shift dynamical systems, symbolic flows, periodic trajectories, periodic orbits, sequence spaces.
[1] Research supported in part by NSF Predoctoral Traineeship from the University of Rochester.

integer Q and for all sufficiently large k. The trajectory x is *periodic* if $x(i+p)=x(i)$ for some positive integer p and for all $i \in I$.

LEMMA 1. *Let x be a trajectory over S, and let ϕ be a shift-invariant operator on $X(S)$. If x is periodic, then the ϕ-orbit of x is eventually periodic.*

PROOF. Observe that if $x(i+p)=x(i)$ for all $i \in I$, then $(\phi(x))(i+p)=(\phi(x))(i)$ for all $i \in I$. For by the above characterization of shift-invariant operators, there exist integers m and n and a function $f: S^n \to S$ such that

$$\begin{aligned}(\phi(x))(i+p) &= f(x(i+p+m+1), \cdots, x(i+p+m+n)) \\ &= f(x(i+m+1), \cdots, x(i+m+n)) \\ &= (\phi(x))(i).\end{aligned}$$

It follows that $(\phi^k(x))(i+p)=(\phi^k(x))(i)$ for all nonnegative integers k and for all $i \in I$. Therefore, each trajectory $\phi^k(x)$ is completely determined by the p-tuple $R_k=((\phi^k(x))(1), (\phi^k(x))(2), \cdots, (\phi^k(x))(p))$. But there are only $|S|^p$ distinct p-tuples of elements of S. By the pigeon-hole principle, there must exist integers k_0 and k_1 with $0 \leqq k_0 < k_1 \leqq |S|^p$ such that $R_{k_0}=R_{k_1}$. Then $\phi^{k_0}(x)=\phi^{k_1}(x)$. Let $Q=k_1-k_0$. Then $\phi^{k+Q}(x)=\phi^k(x)$ for all $k \geqq k_0$, and so the ϕ-orbit of x is eventually periodic.

The converse of Lemma 1 is false. For example, let $S=\{0, 1, 2\}$, and define $f: S \to S$ by $f(0)=0$ and $f(1)=f(2)=1$. Let ϕ be the shift-invariant operator on $X(S)$ defined by $(\phi(x))(i)=f(x(i))$. Let $y \in X(S)$ be any nonperiodic sequence of 1's and 2's. Define $x \in X(S)$ by $x(2i+1)=0$ and $x(2i)=y(i)$ for all $i \in I$. Then $\phi^{k+1}(x)=\phi^k(x)$ for all $k \geqq 1$, and so the ϕ-orbit of x is eventually periodic. But x is not a periodic trajectory over S.

Let F_q be the finite field with q elements. Define addition and scalar multiplication of trajectories over F_q component-wise: If $x, y \in X(F_q)$ and $a, b \in F_q$, then $(ax+by)(i)=ax(i)+by(i)$. In the product topology induced by the discrete topology on F_q, the dynamical system $X(F_q)$ is a topological vector space.

LEMMA 2. *Let ϕ be a nonzero shift-invariant linear operator on $X(F_q)$. Then there is an integer $m \in I$ and constants $a_1, a_2, \cdots, a_n \in F_q$ with $a_1 \neq 0$ and $a_n \neq 0$ such that*

$$(\phi(x))(i) = a_1 x(i+m+1) + a_2 x(i+m+2) + \cdots + a_n x(i+m+n)$$

for all $i \in I$.

PROOF. For some $m \in I$ and some $f: F_q^n \to F_q$, we have

$$(\phi(x))(i) = f(x(i+m+1), x(i+m+2), \cdots, x(i+m+n)).$$

Since ϕ is linear and nonzero on $X(F_q)$, it follows that f is linear and nonzero on F_q^n, that is, f is a nonzero linear functional on the finite-dimensional

vector space F_q^n. Therefore, there exist constants $a_1, a_2, \cdots, a_n \in F_q$ not all zero such that

$$f(x(i+m+1), x(i+m+2), \cdots, x(i+m+n)) = a_1x(i+m+1) + a_2x(i+m+2) + \cdots + a_nx(i+m+n).$$

Clearly, we can choose m and n so that $a_1 \neq 0$ and $a_n \neq 0$.

LEMMA 3. *Let x be a trajectory over a finite field F_q. Then x is periodic if and only if there exist constants $a_0, a_1, \cdots, a_n \in F_q$ not all zero such that*

$$\sum_{r=0}^{n} a_r x(i+r) = 0 \tag{1}$$

for all $i \in I$.

PROOF. Suppose that (1) holds for all $i \in I$. Clearly, we can assume that $a_0 \neq 0$ and $a_n \neq 0$. If $n=0$, then $x(i)=0$ for all $i \in I$, and so x is periodic. If $n>0$, then

$$x(i) = -a_0^{-1} \sum_{r=1}^{n} a_r x(i+r) \tag{2}$$

and

$$x(i+n) = -a_n^{-1} \sum_{r=0}^{n-1} a_r x(i+r). \tag{3}$$

Let T_j be the n-tuple $(x(j+1), x(j+2), \cdots, x(j+n))$. Since there are only q^n distinct n-tuples of elements of F_q, it follows that $T_{j_0} = T_{j_1}$ for some integers j_0 and j_1 such that $0 \leqq j_0 < j_1 \leqq q^n$. Let $p = j_1 - j_0$. Then $x(i+p)=x(i)$ for $i = j_0+1, j_0+2, \cdots, j_0+n$. But then (2) and (3) imply that $x(i+p)=x(i)$ for $i=j_0$ and $i=j_0+n+1$. By induction, it follows that $x(i+p)=x(i)$ for all $i \in I$, and so the trajectory x is periodic.

Conversely, if $x(i+p)=x(i)$ for all $i \in I$, let $n=2p-1$, and set $a_r=1$ for $r=0, 1, \cdots, p-1$ and $a_r=-1$ for $r=p, p+1, \cdots, 2p-1$. Then

$$\begin{aligned} \sum_{r=0}^{2p-1} a_r x(i+r) &= \sum_{r=0}^{p-1} x(i+r) - \sum_{r=p}^{2p-1} x(i+r) \\ &= \sum_{r=0}^{p-1} x(i+r) - \sum_{r=0}^{p-1} x(i+r) \\ &= 0 \end{aligned}$$

for all $i \in I$, and so condition (1) is satisfied.

COROLLARY. *Let x be a trajectory over a finite field F_q, and let ϕ be a nonzero shift-invariant linear operator on $X(F_q)$. If $\phi(x)$ is periodic, then x is periodic.*

PROOF. By Lemma 2, there exist constants $a_1, a_2, \cdots, a_n \in F_q$ with $a_1 \neq 0$ and $a_n \neq 0$ and an integer m such that $(\phi(x))(i) = \sum_{r=1}^{n} a_r x(i+m+r)$. If $(\phi(x))(i+p) = (\phi(x))(i)$ for some positive integer p and all $i \in I$, then

$$\sum_{r=1}^{n} a_r x(i + m + r) - \sum_{r=1}^{n} a_r x(i + p + m + r) = 0$$

for all $i \in I$. By Lemma 3, the trajectory x is periodic.

THEOREM. *Let x be a trajectory over a finite field F_q, and let ϕ be a shift-invariant linear operator on $X(F_q)$. Assume that ϕ is not a scalar multiple of the identity. Then x is periodic if and only if the ϕ-orbit of x is eventually periodic.*

PROOF. Suppose that $\phi^{k+Q}(x) = \phi^k(x)$ for all $k \geqq k_0$. Let $y = \phi^{k_0}(x)$. Then $\phi^Q(y) = \phi^{k_0+Q}(x) = \phi^{k_0}(x) = y$. By Lemma 2, there exist $m \in I$ and constants $a_1, a_2, \cdots, a_n \in F_q$ not all zero such that

$$y(i) = (\phi^Q(y))(i) = \sum_{r=1}^{n} a_r y(i + m + r)$$

for all $i \in I$. Since ϕ is not a scalar multiple of the identity, then ϕ^Q is also not a scalar multiple of the identity. Therefore, if $n = 1$, then $m \neq -1$. By Lemma 3, it follows that $y = \phi^Q(x)$ is periodic. Then the Q-fold application of the corollary to Lemmas 2 and 3 proves that the trajectory x is periodic.

Conversely, if the trajectory x is periodic, then by Lemma 1 the ϕ-orbit of x is eventually periodic.

REFERENCE

1. G. A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory **3** (1969), 320–375. MR **41** #4510.

SOUTHERN ILLINOIS UNIVERSITY, CARBONDALE, ILLINOIS 62901