TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 302, Number 1, July 1987

PERIODIC POINTS AND AUTOMORPHISMS OF THE SHIFT

MIKE BOYLE AND WOLFGANG KRIEGER

ABSTRACT. The automorphism group of a topological Markov shift is studied by way of periodic points and unstable sets. A new invariant for automorphisms of dynamical systems, the gyration function, is used to characterize those automorphisms of finite subsystems of the full shift on n symbols which can be extended to a composition of involutions of the shift. It is found that for any automorphism U of a subshift of finite type S, for all large integers M the map US^M is a topological Markov shift whose unstable sets equal those of S. This fact yields, by way of canonical measures and dimension groups, information about dynamical properties of US^k such as the zeta function and entropy.

Introduction. Let (X, S) be a dynamical system. (In the most general case, S is just a bijection of the set X.) For $n \in \mathbf{N}$, we denote by $P_n(S)$ the set of points of period n under S, and by $P_n^0(S)$ the set of points of least period n under S. $\mathcal{P}_n(S)$ will be the set of S-orbits of length n. We assume that the $P_n(S)$ are finite sets. (This is satisfied, for example, if S is an expansive homeomorphism of a compact metric space X.) We then associate to (X, S) the family of finite dynamical systems that is obtained by restricting S to the sets $P_n^0(S)$, $n \in I(S)$, where

$$I(S) = \{n\colon P_n^0(S) \neq \varnothing\}.$$

Some of our results will be formulated in terms of the group

$$\mathcal{A}(S) = \prod_{n \in I(S)} \mathrm{Aut}(P_n^0(S), S|P_n^0(S))$$

equipped with the product topology of the discrete topologies. This topology reflects the idea that an automorphism is approximated by its action on finite collections of periodic points. Every automorphism U of S gives rise to an element $(U_n)_{n \in I(S)}$ of $\mathcal{A}(S)$, where U_n is the restriction of U to $P_n^0(S)$. Invariants for the conjugacy in $\mathrm{Aut}(P_n^0(S), S|P_n^0(S))$ are the number of cycles of the permutations $\pi(U_n)$ that are induced by U_n on $\mathcal{P}_n(S)$, and the lengths of these cycles. A complete system of invariants for the conjugacy in $\mathrm{Aut}(P_n(S), S|P_n(S))$ is obtained by adding what we call the return number of the cycles. Here we mean by the return number of a cycle of $\pi(U_n)$ the integer r, $0 \leq r < n$, such that, with l the length of the cycle, for every point x in any orbit that belongs to the cycle $U^l x = S^r x$. Of particular interest to us will be an invariant of the conjugacy in $\mathrm{Aut}(S)$ that we call the gyration function. The gyration function assigns to a $U \in \mathrm{Aut}(S)$ an element $(g(U)(n))_{n \in I(S)}$ of $\prod_{n \in I(S)} \mathbf{Z}/n\mathbf{Z}$.

Received by the editors March 13, 1985.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 58F20; Secondary 28D99, 54H15, 54H20.

We will call $g(U)(n)$ the nth gyration number of U. One way of defining $g(U)(n)$ is to say that it is the sum of the return numbers of the cycles of $\pi(U_n)$ taken modulo n. It turns out that the gyration function is a homomorphism. We describe some of the general properties of this homomorphism in §1, and in the later sections use it as one tool in studying the automorphism group of a topological Markov shift.

Let S now represent a topological Markov shift. In the study of any group, it is natural to consider the elements of finite order. However, we find the subgroup generated by the elements of finite order in $\mathrm{Aut}(S)$ to be of particular interest. This is because examples of automorphisms of, for instance, the two-shift, are generally obtained by composing a power of the shift with automorphisms that are constructed using the marker method, and all automorphisms that are constructed by the marker method have finite order. (For the marker method see §6 of [**6**]. We make use of this method in §3.) It is an open problem of long standing whether the automorphism group of the two-shift is generated by the shift and its elements of finite order. This problem constitutes part of the motivation for the present paper. The gyration numbers are particularly useful for the analysis of the action of automorphisms of finite order on periodic points. For example, if U has order k in $\mathrm{Aut}(S)$, then

$$kg(U)(n) = 0, \qquad n \in I(S),$$

and therefore the same constraint holds for a composition of elements of order k. More generally, if λ_S denotes the spectral radius of (a transition matrix for) S, if the inverse of the zeta function of S is a polynomial of degree $I \in \mathbf{N}$, and if p is a prime such that $p > I\lambda_S$, then the gyration function of S must vanish at p for every automorphism of S of finite order, and hence also for every composition of automorphisms of S of finite order. Furthermore, if the inverse of the zeta function of S is an irreducible polynomial and U is an automorphism of S of finite order, then US^i is shift equivalent to S^i for all $i \in \mathbf{Z}$, $i \neq 0$. (For the notion of shift equivalence see [**9**].)

We also find for an automorphism U of S, that for all sufficiently large $M \in \mathbf{N}$, US^M is a topological Markov shift whose stable and unstable sets agree with those of S. From this we obtain information about US^M. For example, the inverses of the zeta functions of S and US^M are polynomials of equal degree. Also, if S is irreducible, then the entropy of US^M is equal to

$$h(US^M) = M \log \lambda_S + \log \lambda_U$$

where λ_U is the factor by which U multiplies the natural measures on unstable sets. If $\lambda_U = 1$, and the inverse of the zeta function of S is an irreducible polynomial, then US^M is shift equivalent to S^M. Finally the action of U on periodic points is constrained. If S is irreducible and aperiodic, then U must leave orbits of arbitrarily long period fixed, and one can derive explicit restrictions on the return numbers U may assume on cycles of a given length. A cardinality argument shows that there are also restrictions on the gyration numbers of the automorphisms of S. However, we are unable to give an explicit description of an element not in the range of the gyration function of some topological Markov shift, or even in the range of the function which assigns to an automorphism the sequence $(\mathrm{sign}\,\pi(U_n))_{n \in I(S)}$.

In §3 we consider the subgroup $\mathcal{I}(S_{(N)})$ of the automorphism group of the N-shift $S_{(N)}$ that is generated by the involutions. There we ask when an automorphism

of the restriction of the shift to a finite collection of periodic points extends to an element of $I(S_{(N)})$. This question we answer completely. Suppose $n \in \mathbf{N}$, and for $1 \leq m \leq n, U^{(m)}$ is an automorphism of the restriction of $S_{(N)}$ to $P_m^0(S_{(N)})$. Then there exists an element U of $I(S_{(N)})$ with $U_m = U^{(m)}$, $1 \leq m \leq n$, if and only if the following conditions hold for all nonnegative integers k and q with q odd, $1 \leq 2^k q \leq n$:

$$g(U^{(2^k q)})(2^k q) = \begin{cases} 0 \\ 2^{K-1} q \end{cases} \quad \text{if} \prod_{0 \leq m < k} \operatorname{sign}(\pi(U^{(2^m q)})) = \begin{cases} 1, \\ -1. \end{cases}$$

We call attention to one more longstanding open problem, raised by Bob Williams: does every automorphism of the restriction of an irreducible and aperiodic Markov shift S to a finite subsystem of S extend to an automorphism of S? We relate this problem to the final result of this paper, that any automorphism of a finite dynamical system may be obtained by restricting an automorphism of some irreducible and aperiodic topological Markov shift to the points of low period.

1. Invariants for the conjugacy of automorphisms of a dynamical system. To explain the basic idea, we consider first a finite dynamical system (P, S), where for some $n \in \mathbf{N}$ all orbits of (P, S) have length n. Let $\mathcal{P}$ be the set of these orbits. For every $U \in \operatorname{Aut}(S)$ we denote by $\pi(U)$ the permutation of $\mathcal{P}$ induced by U,

$$\pi(U)(Q) = UQ, \qquad Q \in \mathcal{P}.$$

Pick out of every $Q \in \mathcal{P}$ an element x_Q. Define for a permutation π of $\mathcal{P}$ an automorphism W_π of S by

$$W_\pi S^i x_Q = S^i x_{\pi Q}, \qquad 0 \leq i < n,\ Q \in \mathcal{P}.$$

One has $\pi(W_\pi) = \pi$. Thus the mapping $U \to \pi(U)$, $U \in \operatorname{Aut}(S)$ is a homomorphism of $\operatorname{Aut}(S)$ onto the full symmetric group $\mathcal{S}(\mathcal{P})$ of $\mathcal{P}$. The kernel of this homomorphism is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}}$. An isomorphism between $(\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}}$ and this kernel is set up by assigning to an element γ of $(\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}}$ the automorphism $W(\gamma)$ of S that is given by

$$W(\gamma) S^i x_Q = S^{i+\gamma(Q)} x_Q, \qquad 0 \leq i < n,\ Q \in \mathcal{P}.$$

One has

$$W_\pi^{-1} W(\gamma) W_\pi = W(\gamma \circ \pi), \qquad \gamma \in (\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}},\ \pi \in \mathcal{S}(\mathcal{P}).$$

Denoting by ψ the homomorphism of $\mathcal{S}(\mathcal{P})$ into the automorphism group of $(\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}}$ that sends a $\pi \in \mathcal{S}(\mathcal{P})$ into the automorphism $\gamma \to \gamma \circ \pi$, $\gamma \in (\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}}$, we have therefore that $\operatorname{Aut}(S)$ is isomorphic to the semidirect product $(\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}} \otimes_\psi \mathcal{S}(\mathcal{P})$. Every $U \in \operatorname{Aut}(S)$ can be uniquely expressed as a product $U = W_{\pi(U)} W_U$ where W_U is in the kernel of $U \to \pi(U), U \in \operatorname{Aut}(S)$. We define an element γ_U of $(\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}}$ by $W_U = W(\gamma_U)$. Equivalently γ_U can be defined as the γ satisfying

$$U x_Q = S^{\gamma(Q)} x_{\pi(Q)}, \qquad Q \in \mathcal{P}.$$

We set now

$$g(U) = \sum_{Q \in \mathcal{P}} \gamma_U(Q).$$

We call $g(U)$ the gyration number of U. $g(U)$ does in fact not depend on the choice of the $x_Q \in Q \in \mathcal{P}$. For another choice $x'_Q \in Q \in \mathcal{P}$, with

$$Ux'_Q = S^{\gamma'(Q)}x'_{\pi(Q)}, \qquad Q \in \mathcal{P},$$

define $l \in (\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}}$ by

$$x'_Q = S^{l(Q)}x_Q.$$

Then or $Q \in \mathcal{P}$,

$$\begin{aligned} Ux'_Q &= US^{l(Q)}x_Q = S^{l(Q)}Ux_Q = S^{l(Q)}S^{\gamma(Q)}x_{\pi(Q)} \\ &= S^{l(Q)}S^{\gamma(Q)}S^{-(l\cdot\pi)(Q)}x'_{\pi(Q)}. \end{aligned}$$

Therefore

$$\gamma'(Q) = l(Q) - l(\pi Q) + \gamma_U(Q), \qquad Q \in \mathcal{P},$$

and

$$\sum_{Q\in\mathcal{P}} \gamma'(Q) = \sum_{Q\in\mathcal{P}} \gamma_U(Q).$$

If $U, V \in \mathrm{Aut}(S)$, then

$$\gamma_{UV} = (\gamma_U \circ \pi(V)) + \gamma_V$$

so that

$$\sum_Q \gamma_{UV} = \sum_Q \gamma_U(\pi(V)(Q)) + \gamma_V(Q)$$

and therefore

$$g(UV) = g(U) + g(V).$$

Thus the mapping $U \to g(U), U \in \mathrm{Aut}(S)$, is a homomorphism onto $\mathbf{Z}/n\mathbf{Z}$. (In fact, as was pointed out to us by Carol Wood, for any $Q \in \mathcal{P}$, this map is the transfer (see Theorem 7.3.1 of [**5**]) of $\mathrm{Aut}(S)$ into $\mathbf{Z}/n\mathbf{Z}$ induced by the homomorphism $U \to \gamma_U(Q)$ from the stabilizer of Q into $\mathbf{Z}/n\mathbf{Z}$.) The map $U \to \mathrm{sign}\,\pi(U)$ yields another abelian factor. Essentially, there are no others: if $|\mathcal{P}(S)| > 4$, then any homomorphism from $\mathrm{Aut}(S)$ onto an abelian group factors through $U \to (g(U), \mathrm{sign}\,\pi(U))$. Let $U \in \mathrm{Aut}(S)$. Let $Q \in \mathcal{P}$ belong to a cycle of length L under $\pi(U)$. We define then the return number $R_Q(U)$ of Q by

$$U^L x = S^{R_Q(U)}x, \qquad 0 \le R_Q(U) < n,\ x \in Q.$$

Sometimes we refer to this number also as the return number of an $x \in Q$ or of the $\pi(U)$ cycle of Q.

A complete invariant for the conjugacy of the automorphism of the finite dynamical system S is the number of cycles of $\pi(U)$, the lengths of these cycles, and their return numbers. Let us denote the number of cycles of $\pi(U)$ by $K(U,S)$, and let us collect the length and return numbers into a vector $(L_k(U,S), R_k(U,S))_{1\le k\le K(U,S)}$ where

$$|\mathcal{P}| = \sum_{1\le k\le K(U,S)} L_k(U,S)$$

and where we normalize such that

$$L_k(U,S) \ge L_{k+1}(U,S), \qquad 1 \le k < K(U,S),$$

and

$$R_k(U,S) \geq R_{k+1}(U,S) \quad \text{if } L_k(U,S) = L_{k+1}(U,S),\ 1 \leq k < K(U,S).$$

Choosing $x_Q \in Q \in \mathcal{P}$ such that for a $Q \in \mathcal{P}$ whose cycle has length l and return number r

$$x_{\pi_U^i(Q)} = U^i x_Q, \qquad 1 \leq i < l,$$

one sees that

$$U x_{\pi^{l-1}(U)(Q)} = S^r x_Q$$

and therefore

$$g(U) = \sum_{1 \leq k \leq K(U,S)} R_k(U,S) \pmod{n}.$$

We turn now to a dynamical system (X,S) such that $|P_n(S)| < \infty, n \in \mathbf{N}$. To every $U \in \mathrm{Aut}(S)$ we have associated the automorphisms

$$U_n = U|P_n^0(S), \qquad n \in I(S),$$

of the dynamical system $(P_n^0(S), S|P_n^0(S))$. We denote

$$g(U,S)(n) = g(U_n), \qquad n \in I(S),$$

and call the mapping $U \to (g(U,S)(n))_{n \in I(S)}$ the gyration function. We say that $g(U,S)(n)$ is the nth gyration number of U. What we have said about finite dynamical systems results in the following theorems.

(1.1) THEOREM. *The gyration function is a homomorphism of* $\mathrm{Aut}(S)$ *into* $\prod_{n \in I(S)} \mathbf{Z}/n\mathbf{Z}$.

(1.2) THEOREM. *For* $U \in \mathrm{Aut}(S)$ *and* $n \in I(S)$,

$$g(U,S)(n) = \sum_{1 \leq k \leq K(U_n)} R_k(U_n).$$

(1.3) COROLLARY. *Let* $V_i, 1 \leq i \leq I$, *be automorphisms of finite order of* S. *Let* $n \in I(S)$ *be relatively prime to the order of* $V_i, 1 \leq i \leq I$. *Then*

$$g\left(\prod_{1 \leq i \leq I} V_i, S\right)(n) = 0. \tag{1}$$

PROOF. Let k_i be the order of $V_i, 1 \leq i \leq I$. Since $U \to g(U,S)$ $(U \in \mathrm{Aut}(S))$ is a homomorphism $k_i g(V_i,S) = 0$, $1 \leq i \leq I$, and therefore

$$\left(\prod_{1 \leq i \leq I} k_i\right) g\left(\prod_{1 \leq i \leq I} V_i, S\right)(n) = 0.$$

This implies (1) since n is relatively prime to $\prod_{1 \leq i \leq I} k_i$. Q.E.D.

We note next that for any individual automorphism of finite order one has also restrictions on the individual return times.

(1.4) PROPOSITION. *Let $U \in \mathrm{Aut}(S)$ be of finite order k. Let $n \in I(S)$. Then for all return numbers r of U_n, $kr = 0 \pmod{n}$.*

PROOF. Let x be a point in an orbit in $\mathcal{P}_n(S)$ that belongs to a cycle of length l and has return number r. Then $U^l x = S^r x$. Since $U^k x = x$ one must then have that $U^{kl}x = S^{kr}x = x$. Q.E.D.

(1.5) LEMMA. *Let $i, n \in \mathbf{N}$, $J = \{j \in \mathbf{N} : j = \gcd(i, jn)\}$. Then*

$$P_n^0(S^i) = \bigcup_{j \in J} P_{jn}^0(S).$$

PROOF. Any S^i-orbit of length n is contained in some S-orbit of length jn, with $1 \le j \le i$. But an S-orbit of length k is the union of $\gcd(k,i)$ S^i-orbits of length $k/\gcd(k,i)$. If $k = jn$, then the S-orbit splits into S^i-orbits of length n if and only if $n = jn/\gcd(jn, i)$ which is equivalent to $j = \gcd(i, jn)$. Q.E.D.

(1.6) PROPOSITION. *Let $i, n \in \mathbf{N}$. If $j \in \mathbf{N}$ and $j = \gcd(i, jn)$ then let a_j be an integer such that $ia_j = j \pmod{jn}$. For other j, set $a_j = 0$. Then for all $U \in \mathrm{Aut}(S)$*

$$g(U, S^i)(n) = \sum_{j \mid i} a_j g(U, S)(jn).$$

PROOF. By Lemma (1.5), a point lies in an S^i-orbit of length n if and only if it lies in some S-orbit of length jn, where $j = \gcd(i, jn)$. Let x be such a point, $x \in Q \in \mathcal{P}_{jn}(S)$, $x \in Q' \in \mathcal{P}_n(S^i)$. With respect to S, let Q be in a $\pi(U_{jn})$-cycle of length L and return number R. With respect to S^i, let Q' be in a $\pi'(U_n)$ cycle of length L' and return number R'. The collection C of jnL points in the cycle of S-orbits contributes R to $g(U,S)(jn)$. We will compute the contribution of C to $g(U, S^i)(n)$. Under U, x first returns to Q' at $U^{Lp}x = S^{p^R}x$, where $p = j/\gcd(j, R)$ is the least positive integer such that j divides pR. Because

$$S^{pR}x = S^{iR'}x$$

and

$$pR = \frac{jR}{\gcd(j,R)} = \frac{ia_jR}{\gcd(j,R)} \pmod{jn}$$

we see that

$$R' = \frac{Ra_j}{\gcd(j,R)} \pmod{n}.$$

Because each $\pi'(U)$ cycle in C has length $L' = pL$, there are j/p such cycles. Each contributes R' to $g(U, S^i)(n)$. So the contribution of C to $g(U, S^i)(n)$ is just

$$(j/p)R' = \gcd(j,R)R' = Ra_j.$$

The result follows by summing. Q.E.D.

For example, from Proposition (1.6) it follows that if p is a prime, and n, $k \in \mathbf{N}$, then

$$g(U,S)(p^{n+k}) = g(U, S^{p^k})(p^n) \pmod{p^n}.$$

(1.7) LEMMA. $g(U, S^{-1}) = -g(U, S)$, $U \in \mathrm{Aut}(S)$.

PROOF. For all $n \in I(S)$ and $U \in \mathrm{Aut}(S)$,

$$\begin{aligned} L(U, S^{-1})(Q) &= L(U, S)(Q), \\ R(U, S^{-1})(Q) &= n - R(U, S)(Q), \end{aligned} \qquad Q \in \mathcal{P}_n(S). \quad \text{Q.E.D.}$$

We say that a bijection $V: X \to X$ (that also preserves any additional structure that might be given on X) is a time reversal for (X, S) if $VSV^{-1} = S^{-1}$. Note that for a time reversal V of S, and an automorphism U of S, $V^{-1}UV$ is also an automorphism of S.

(1.8) PROPOSITION. *For a time reversal V of S, $g(V^{-1}UV, S) = -g(U, S)$.*

PROOF. One has

$$g(V^{-1}UV, S) = g(U, VSV^{-1}) = g(U, S^{-1}),$$

and the proposition follows from Lemma (1.7). Q.E.D.

For later use we note the following lemma.

(1.9) LEMMA. *Let $U \in \mathrm{Aut}(S)$ be an automorphism of finite order. Let for some $n \in I(S)$ $Q \in \mathcal{P}_n(S)$ have return number r. Let m be the g.c.d. of r and n. Then there exists a $V \in \mathrm{Aut}(S)$ of finite order such that $VS^m x = x$, $x \in Q$.*

PROOF. Let l be the length of the cycle of Q. Then $U^l x = S^r x$, $x \in Q$. There is an $i \in \mathbf{Z}$ such that $U^{il} x = S^{-m} x$, $x \in Q$. Let $V = U^{il}$. Q.E.D.

2. Topological Markov shifts. In this section we are concerned with topological Markov shifts. However, some of the tools we use from dimension group theory will be described in greater generality. Expositions of the basic theory of topological Markov shifts are in [**1**, **4**, **8**]. Recall for a topological Markov shift (X, S) with transition matrix A that

$$|P_n(S)| = \mathrm{trace}\, A^n, \qquad n \in \mathbf{N},$$

and that the zeta function

$$\zeta_S(t) = \exp \sum_{n \in \mathbf{N}} \frac{1}{n} |P_n(S)| t^n$$

of S is given by

$$\zeta_S(t) = \prod_i (1 - \lambda_i t)^{-1}$$

where $\prod_i (t - \lambda_i)$ is the characteristic polynomial of A.

We begin by computing the gyration function in an example. For this recall that Möbius function μ on $\mathbf{N}$, defined by

$$\mu(1) = 1,$$
$$\mu(n) = \begin{cases} (-1)^l & \text{if } n \text{ is the product of } l \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

(2.1) PROPOSITION. *Let F be the automorphism of $S_{(2)}$ defined by*

$$(Fx)_i = x_i + 1 \pmod 2, \qquad i \in \mathbf{Z},\ x \in \{0, 1\}^{\mathbf{Z}}.$$

If $n \in \mathbf{N}$ is even, with $n/2$ squarefree, then

$$g(F, S_{(2)})(n) = n/2,$$

while otherwise

$$g(F, S_{(2)})(n) = 0. \tag{1}$$

PROOF. For odd n the result is in Corollary (1.3). Let $n = 2^k q$, q odd, $k \in \mathbf{N}$. Let

$$C = \{x \in P_n^0(S_{(2)}) \colon Fx = S_{(2)}^{2^{k-1}q} x\}.$$

Then

$$g(F, S_{(2)})(n) = \tfrac{1}{2}|C| \pmod{n},$$

and since $g(F, S_{(2)})(n)$ must vanish or have value $n/2$, (1) will hold precisely if $|C|$ is divisible by 2^{k+1}. For $r|q$ set

$$f^0(r) = \left|\{x \in P_{2^k r}^0(S_{(2)}) \colon Fx = S_{(2)}^{2^{k-1}r} x\}\right|,$$
$$f(r) = \left|\{x \in P_{2^k r}(S_{(2)}) \colon Fx = S_{(2)}^{2^{k-1}r} x\}\right|.$$

Then

$$f(r) = \sum_{s|r} f^0(s) = 2^{2^{k-1}r}, \qquad r|q.$$

By Möbius inversion

$$f^0(q) = \sum_{r|q} \mu\left(\frac{q}{r}\right) f(r),$$

so that

$$|C| = \sum_{r|q} \mu\left(\frac{q}{r}\right) 2^{2^{k-1}r}.$$

This integer is divisible by 2^{k+1} if and only if the integer $\sum_{r|q} \mu(q/r) 2^{2^{k-1}r-k}$ is even. All the terms in this sum are even, except possibly $\mu(q)2^{2^{k-1}-k}$ which is odd if and only if $\mu(q) \neq 0$ and k is 1 or 2. Q.E.D.

We want now to obtain some information on the gyration numbers of $S_{(N)}, N \geq 2$, considered as an automorphism of itself. Here Fermat's Little Theorem gets us started.

(2.2) PROPOSITION. *Let p be a prime that does not divide N, and let $k, m \in \mathbf{N}$ be such that*

$$N^{p-1} = 1 + kp^m \tag{1}$$

where p does not divide k. Then

$$g(S_{(N)}, S_{(N)})(p^n) = 0, \qquad 1 \leq n < m, \tag{2}$$

and (except in the case where $p = 2$ and $N = 3 \bmod 4$)

$$g(S_{(N)}, S_{(N)})(p^n) \begin{cases} = 0 \pmod{p^{m-1}}, \\ \neq 0 \pmod{p^m}, \end{cases} \qquad m \leq n. \tag{3}$$

PROOF. $g(S_{(N)}, S_{(N)})(p^n)$ is modulo p^n equal to

$$p^{-n}[N^{p^n} - N^{p^{n-1}}] = p^{-n}N^{p^{n-1}}[N^{(p-1)p^{n-1}} - 1].$$

Therefore, since p does not divide N, (2) is equivalent to

$$N^{(p-1)p^{n-1}} = 1 \pmod{p^{2n}}, \qquad 1 \leq n < m, \tag{4}$$

and (3) is equivalent to

$$N^{(p-1)p^{n-1}} \begin{cases} = 1 \pmod{p^{n+m-1}}, \\ \neq 1 \pmod{p^{n+m}}, \end{cases} \qquad n \geq m. \tag{5}$$

It is

$$\begin{aligned} (N^{p-1})^{p^{n-1}} &= (1 + kp^m)^{p^{n-1}} \\ &= 1 + kp^{m+n-1} + \sum_{1<l\leq p^{n-1}} \binom{p^{n-1}}{l} (kp^m)^l. \end{aligned} \tag{6}$$

This proves (4). Also, (5) follows from (6) whenever

$$\binom{p^{n-1}}{l}(kp^m)^l = 0 \pmod{p^{n+m}}, \qquad l > 1. \tag{7}$$

Given $l \in \mathbf{N}$, $1 < l \leq p^{n-1}$, let p^j be the largest power of p dividing l. If $1 \leq i < p^{n-1}$, $i \in \mathbf{N}$, then i and $(p^{n-1} - i)$ are divisible by the same powers of p. Because

$$\binom{p^{n-1}}{l} = \left(\frac{p^{n-1}}{l}\right) \prod_{1\leq i<l} \left(\frac{p^{n-1} - i}{i}\right)$$

it follows that p^{n-1-j} is the largest power of p which divides $\binom{p^{n-1}}{l}$. Therefore $p^{n+m+(l-1)m-j-1}$ divides $\binom{p^{n-1}}{l}(kp^m)^l$, $1 < l \leq p^{n-1}$, and this implies (7) whenever $(l-1)m - j - 1$ is nonnegative. However,

$$(l-1)m - j - 1 \geq (p^j - 1)m - j - 1 \geq p^j - j - 2,$$

and this last quantity is nonnegative, except in the single case where $p = 2$ and $j = 1$. Thus, $(l-1)m-j-1$ is nonnegative except in the single case where $p = l = 2$ and $m = j = 1$, in which case

$$N = N^{p-1} = 1 + kp^m = 1 + 2k = 3 \pmod 4$$

since k is odd. Thus (7) holds unless $p = 2$ and $N = 3 \pmod 4$. Q.E.D.

(2.3) COROLLARY. *$g(S_{(N)}, S_{(N)})$ is of infinite order in $\prod_{n\in\mathbf{N}} \mathbf{Z}/n\mathbf{Z}$.*

PROOF. Assume for some $k \in \mathbf{N}$, $kg(S_{(N)}, S_{(N)}) = 0$. We know from the proposition that there is a prime $p > k$ and $m \in \mathbf{N}$ such that $g(S_{(N)}, S_{(N)})(p^m) \neq 0$, but $kg(S_{(N)}, S_{(N)})(p^m) = 0$. Therefore p must divide k which is impossible. Q.E.D.

Also $g(S_{(L)} \times 1, S_{(L)} \times S_{(M)})$ is of infinite order in $\prod_{n\in\mathbf{N}} \mathbf{Z}/n\mathbf{Z}$, as can be seen by the same method from the following proposition.

(2.4) PROPOSITION. *Let p be a prime. Then*

$$g(S_{(L)} \times 1, S_{(L)} \times S_{(M)})(p^n) = p^{-n} M^{p^{n-1}} [L^{p^n} - L^{p^{n-1}}] \pmod{p^n}, \qquad n \in \mathbf{N}.$$

PROOF. We choose suitable points in the orbits of length p^n of $S_{(L)} \times S_{(M)}$. For this we first pick $x_Q \in Q \in \mathcal{P}_{p^n}(S_{(L)})$ and $y_R \in R \in \mathcal{P}_{p^n}(S_{(M)})$. If now an orbit in $\mathcal{P}_{p^n}(S_{(L)} \times S_{(M)})$ contains a point (x_Q, y), where $Q \in \mathcal{P}_{p^n}(S_{(L)})$ and $y \in P_{p^n}(S_{(M)})$, then choose this point as its representative. These orbits each contribute one unit to the gyration number, since

$$(S_{(L)} \times 1)(x_Q, y) = (S_{(L)} \times S_{(M)})(x_Q, S_{(M)}^{-1} y).$$

If an orbit in $\mathcal{P}_{p^n}(S_{(L)} \times S_{(M)})$ contains a point (x, y_R), where $x \in P_{p^n}(S_{(L)})$ and $R \in \mathcal{P}_{p^n}(S_M)$, then choose this point as its representative. These points do not contribute, since $(S_L \times 1)(x, y_R) = (S_{(L)} x, y_R)$. Q.E.D.

We introduce at this point some terminology for automorphisms U of a subshift (X, S). Let us say that U has coding bound $N \in \mathbf{N}$ if for all $x \in X$, $(Ux)_0$ is determined by $(x_i)_{-N \le i \le N}$.

The next theorem shows that there is one case where the invariants completely determine the automorphism.

(2.5) THEOREM. *Let (X, S) be an irreducible and aperiodic topological Markov shift. Let $U \in \mathrm{Aut}(S)$ be such that for all sufficiently large $n \in \mathbf{N}$, $L_{n,k}(U, S) = 1$, $1 \le k \le K_n(U, S)$. Then U is a power of S.*

PROOF. Let S be given by a 0-1 transition matrix A. Let $M \in \mathbf{N}$ be such that A^M has all entries positive, and let $N \in \mathbf{N}$ be a coding bound for both U and U^{-1}. Let x and x' be periodic points from distinct orbits of S with least periods n and n' greater than $4N + 2M$ and also large enough for the hypothesis to apply. Let

$$Ux = S^r x, \qquad -\tfrac{1}{2}n < r \le \tfrac{1}{2}n,$$
$$Ux' = S^{r'} x', \qquad -\tfrac{1}{2}n' < r' \le \tfrac{1}{2}n'.$$

Let x and x' be given by blocks a and a', and let Ux and Ux' be given by blocks $\bar{a}$ and $\bar{a}'$, that is, let

$$\bar{a}_i = a_{i+r} \pmod{n}, \quad 1 \le i \le n, \qquad \bar{a}'_i = a'_{i+r' (\mathrm{mod}\ n')}, \quad 1 \le i \le n'.$$

Choose now A-admissible blocks b and b' of length $2N + 3M$ such that a periodic point y of S, with period $m = 2nn' + 4N + 6M$, is given by the block

$$c = \underbrace{a \cdots a}_{n'} b \underbrace{a' \cdots a'}_{n} b'$$

and also

(i) $b_1 \cdots b_N = a_1 \cdots a_N = b'_{3M+N+1} \cdots b'_{3M+2N}$,
$b'_1 \cdots b'_N = a'_1 \cdots a'_N = b_{3M+N+1} \cdots b_{3M+2N}$,
(ii) $b_{N+M} \ne a_{N+M}, b'_{N+2M} \ne a_{n-N-M}$,
(iii) $b'_{N+M} \ne a'_{N+M}, b_{N+2M} \ne a'_{n-N-M}$.

We choose q such that

$$Uy = S^q y, \quad \text{and} \quad -m/2 < q \le m/2$$

and let Uy be given by a block $\bar{c}$. Condition (i) ensures that $\bar{c}$ has the form

$$\bar{c} = \underbrace{\bar{a}\cdots\bar{a}}_{n'}\bar{b}\underbrace{\bar{a}'\cdots\bar{a}'}_{n}\bar{b}'.$$

Condition (ii) ensures that the periodic pattern of $\bar{a}\cdots\bar{a}$ extends less than $2N+M$ symbols into $\bar{b}$ and $\bar{b}'$ (because U^{-1} has coding bound N), and therefore (because x and x' are in distinct orbits) $|q| < 2N + M < n/2$ which forces $q = r$. In the same way, by (iii), one has $q = r'$. The theorem follows now from the density of the periodic points of large periods. Q.E.D.

REMARK. When the numbers $L_{n,K}(U,S)$ are uniformly bounded, Theorem (2.5) implies that U is a root of a power of S. In some cases this result can be sharpened.

Let (X,d) be a compact metric space, and let $T\colon X \to X$ be a homeomorphism. We denote

$$\begin{aligned} W_\delta^+(x,T,I) &= \{y \in X\colon d(T^i x, T^i y) \le \delta, i \ge I\},\\ W_\delta^-(x,T,I) &= \{y \in X\colon d(T^{-i} x, T^{-i} y) \le \delta, i \ge I\}, \end{aligned} \qquad \delta > 0,\ x \in X,\ I \in \mathbf{Z}.$$

One says that a $\delta > 0$ is an expansive constant for (X,d,T) if for all $x, y \in X$, $x \ne y$, there exists an $i \in \mathbf{Z}$ such that $d(T^i x, T^i y) > \delta$. If T has an expansive constant, then T is said to be expansive. This definition does not depend on the choice of the metric (compatible with the topology). One says that an expansive homeomorphism T has canonical coordinates if for every $\delta > 0$ there exists an $\varepsilon > 0$ such that $d(x,y) < \varepsilon$, $x, y \in X$, implies that

$$W_\delta^+(x,T,0) \cap W_\delta^-(y,T,0) \ne \varnothing.$$

Again this definition does not depend on the choice of the metric. Topological Markov shifts are intrinsically characterized as the expansive homeomorphisms of zero-dimensional compacta with canonical coordinates [**2**, Proposition 6.2]. Since it is immaterial which metric is used, we make a convenient choice; from now on, given a subshift (X,S), we use only the metric d on X that is given by

$$I(x,y) = \min_{\{i \in \mathbf{Z}\colon x_i \ne y_i\}} |i|, \qquad x, y \in X,\ x \ne y,$$

$$d(x,y) = \begin{cases} 2^{-I(x,y)} & \text{if } x \ne y,\\ 0 & \text{if } x = y. \end{cases}$$

$\frac{1}{2}$ is an expansive constant for (X,d,S).

(2.6) LEMMA. *The root of a topological Markov shift is a topological Markov shift.*

PROOF. Let T be the topological Markov shift on X, and let $R^k = T$, $k \in \mathbf{N}$. Then R is also expansive. Let T have canonical coordinates. We show that R also has canonical coordinates. For this, let $\delta > 0$. Then let $\eta > 0$ be such that for all $x, y \in X$, $d(x,y) \le \eta$ implies that

$$d(R^l x, R^l y) \le \delta, \qquad -k < l < k.$$

Then

$$W_\delta^+(x,R,0) \supset W_\eta^+(x,T,0), \qquad x \in X. \tag{1}$$

Indeed, if $z \in W_\eta^+(x,T,0)$, then

$$d(T^n x, T^n z) \le \eta, \qquad n \in \mathbf{N},$$

and by the choice of η, then

$$d(R^{nk+l}x, R^{nk+l}z) \le \delta, \qquad k \in \mathbf{Z}_+,\ 0 < l < k,\ n \in \mathbf{N}.$$

Similarly

$$W_\delta^-(x,R,0) \supset W_\eta^-(x,T,0), \qquad x \in X. \tag{2}$$

Since T has canonical coordinates, there is an $\varepsilon > 0$ such that for all $x, y \in X$, $d(x,y) < \varepsilon$ implies that

$$W_\eta^+(x,T,0) \cap W_\eta^-(y,T,0) \neq \varnothing.$$

From (1) and (2) also

$$W_\delta^+(x,R,0) \cap W_\delta^-(y,R,0) \neq \varnothing. \quad \text{Q.E.D.}$$

We use Lemma (2.6) to give a further restriction on the gyration numbers of an automorphism of finite order of a topological Markov shift.

(2.7) PROPOSITION. *Let (X,S) be a topological Markov shift. Let I be the degree of ζ_S^{-1}, let p be a prime, and let $m, n \in \mathbf{N}$, $m \le n$, be such that*

$$p^n > I\lambda_S^{p^{m-1}}. \tag{1}$$

Then for every automorphism U of finite order of S

$$g(U,S)(p^n) = 0 \pmod{p^m}. \tag{2}$$

PROOF. Assume that (2) does not hold. Then there exits an S-orbit of length p^n with return number r under U such that the g.c.d. of r and p^n is equal to p^k, $0 \le k < m$. By Lemma (1.9) there is an automorphism V of S of finite order such that VS^{p^k} has at least p^n fixpoints. By Lemma (2.6) VS^{p^k}, as a root of a power of S, is a topological Markov shift, and $\lambda_{VS^{p^k}} = \lambda_S^{p^k}$. It follows that the number of fixpoints of VS^{p^k} can be at most $I\lambda_S^{p^k}$ and we have a contradiction with (1). Q.E.D.

If in Proposition (2.7) S is taken to be aperiodic, and if also ζ_S^{-1} is an irreducible polynomial, then, writing

$$\zeta_S(t)^{-1} = \prod_{1 \le i \le I} (1 - \lambda_i t)$$

one can replace (1) by

$$p^n > \sum_{1 \le i \le I} \lambda_i^{p^{m-1}}. \tag{3}$$

More generally, one can replace (1) by (3) whenever S has the property that for all $k \in \mathbf{N}$ every kth root of S^k has zeta function identical to the zeta function of S. This is the case, for instance, if S has transition matrix

$$\begin{pmatrix} 0 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix}$$

as one sees from its characteristic polynomial $(t^3 - t^2 - 7t - 6)(t - 2)$. In general, however, the zeta function of S does not determine whether S has this property.

Our next result is formulated in terms of the group $\mathcal{A}(S)$. Note that an automorphism U of an irreducible topological Markov shift (X, S) can be identified with the element $(U|P_n^0(S))_{n\in I(S)}$ of $\mathcal{A}(S)$ since the periodic points of S are dense. We denote by $\mathcal{T}(S)$ the group that is generated by the automorphisms of finite order of S.

(2.8) THEOREM. $S_{(N)} \notin \overline{\mathcal{T}(S_{(N)})}$.

PROOF. Let p be an odd prime that does not divide N. On the one hand we know from Proposition (2.2) that there is an $m \in \mathbf{N}$ such that for all $n \geq m$

$$g(S_{(N)}, S_{(N)})(p^n) \neq 0 \pmod{p^m}.$$

On the other hand, we know from Proposition (2.7) that, if here $p^n > N^{p^{m-1}}$, then for every automorphism U of $S_{(N)}$ of finite order

$$g(U, S_{(N)})(p^n) = 0 \pmod{p^m}.$$

Assuming that $S_{(N)}$ is a limit of compositions of automorphisms of finite order of $S_{(N)}$ leads therefore to a contradiction. Q.E.D.

Also $S_{(L)} \times 1 \notin \overline{\mathcal{T}(S_{(L)} \times S_{(M)})}$ as can be seen by the same method from Proposition (2.4).

We describe now the construction of a dimension group. For this we consider a subshift (X, S) and for any point x in X let

$$W^-(x, S) = \left\{ y \in X : \lim_{i\to\infty} d(S^{-i}x, S^{-i}y) = 0 \right\},$$
$$W^+(x, S) = W^-(x, S^{-1}),$$

define the unstable and stable sets of x. For any expansive constant δ of (X, S),

$$W^-(x, S) = \bigcup_{I\in\mathbf{Z}_+} W_\delta^-(x, S, I), \qquad x \in X.$$

Let for a set $D \subset X$,

$$W(D, S) = \bigcup_{x\in D} W^-(x, S),$$

and write

$$W(D, S) = \bigcup_{x\in D} \bigcup_{i\in\mathbf{Z}} W_\delta^-(x, S, I).$$

On the sets $W_\delta^-(x, S, I)$, $x \in D$, $I \in \mathbf{Z}$, there are the compact topologies that these sets inherit as subsets of X, and we put on $W(D, S)$ the resulting inductive limit topology. On $W(D, S)$ we have the group $\mathcal{F}_D(S)$ of uniformly finite dimensional homeomorphisms. A homeomorphism v of $W(D, S)$ belongs to $\mathcal{F}_D(S)$ if there is an $I \in \mathbf{Z}_+$ such that $vy \in W_\delta^+(y, S, I)$, $y \in W(D, S)$. $(W(D, S), \mathcal{F}_D(S))$ does not depend on the choice of the metric d, nor on the choice of the expansive constant δ. This is a consequence of the fact that for any two expansive constants δ, η of (X, d, S), $\delta < \eta$, there is a $K \in \mathbf{N}$ such that

$$W_\eta^+(x, S, I) \subset W_\delta^+(x, S, I + K),$$
$$W_\eta^-(x, S, I) \subset W_\delta^-(x, S, I + K), \qquad x \in X,\ I \in \mathbf{Z}.$$

Note that

$$W^-_{1/2}(x,S,I) = \{y \in X\colon y_i = x_i, i \le -I\},$$
$$W^+_{1/2}(x,S,I) = \{y \in X\colon y_i = x_i, i \ge I\}, \qquad x \in X,\ I \in \mathbf{Z}.$$

Observe at this point that a homeomorphism v of $W(D,S)$ is in $\mathcal{F}_D(S)$ precisely if for some $I \in \mathbf{Z}_+$

$$(vy)_i = y_i, \qquad i \ge I,\ y \in W(D,S).$$

One considers next the Boolean ring $\mathcal{C}_D(S)$ of compact open subsets of $W(D,S)$. The group $\mathcal{F}_D(S)$ acts on $\mathcal{C}_D(S)$ and one obtains the (future) dimension function $\delta_{D,S}$ as the quotient map of $\mathcal{C}_D(S)$ onto the orbit space of this action. The range of the dimension function carries an algebraic structure, where for $\gamma, \gamma' \in \delta_{D,S}(\mathcal{C}_D(S))$

$$\gamma + \gamma' = \delta_{D,S}(C \cup C'), \qquad C \in \gamma,\ C' \in \gamma',\ C \cap C' = \emptyset,$$

and generates the positive cone $K_0^+(D,S)$ of $(K_0(D,S), K_0^+(D,S))$, an ordered abelian group. Let now D be such that

$$W(D,S) \cap W^-(x,S) \neq \emptyset, \qquad x \in X.$$

Then $(K_0(D,S), K_0^+(D,S))$ does not depend anymore on the choice of D. We suppress it from the notation, and call $(K_0(S), K_0^+(S))$ the (future) dimension group of S. One can set D equal to X. Note that $W(X,S)$ and X are equal as sets and differ only by the topology they carry. S induces an automorphism ϕ_S of $(K_0(S), K_0^+(S))$. More generally, every $U \in \mathrm{Aut}(S)$ induces an automorphism ϕ_U of $(K_0(S), K_0^+(S))$ that commutes with ϕ_S.

For a topological Markov shift (X,S) the characteristic polynomial of $\phi_S \otimes 1\colon K_0(S) \otimes \mathbf{C} \to K_0(S) \otimes \mathbf{C}$ is $t^d \zeta_S^{-1}(t^{-1})$, where d is the degree of the polynomial ζ_S^{-1}. In fact, $(K_0(S), K_0^+(S), \phi_S)$ determines the shift equivalence class of S (see §4 of [7]). Also recall that for an irreducible topological Markov shift (X,S) there exists an (up to a factor) unique $\mathcal{F}_D(S)$-invariant Borel measure $\tau_D(S)$ on $W(D,S)$ such that

$$0 < \tau_D(S)(SC) = \lambda_S \tau_D(C), \qquad C \in \mathcal{C}_D(S).$$

$\tau_D(S)$ gives rise to an (up to a factor) unique state τ on $(K_0(S), K_0^+(S))$ by

$$\tau(\gamma) = \tau_D(C), \qquad C \in \gamma \in K_0^+(S),$$

such that

$$\tau(\phi_S \gamma) = \lambda_S(\tau(\gamma)), \qquad \gamma \in K_0(S).$$

For every $U \in \mathrm{Aut}(S)$ there is a $\lambda_U > 0$ such that

$$\tau(\phi_U \gamma) = \lambda_U \tau(\gamma), \qquad \gamma \in K_0(S).$$

We say that a $U \in \mathrm{Aut}(S)$ is *shiftless*, if $\lambda_U = 1$.

As is seen from Theorem (2.5), if for a $U \in \mathrm{Aut}(S)$ for sufficiently large $n \in \mathbf{N}$

$$L_{n,k}(U,S) = 1, \qquad 1 \le k \le K_n(U,S),$$

then λ_U uniquely determines U. Also note at this point, that in the situation where $\mathrm{Aut}(S)$ is generated by the shiftless automorphisms together with S—for example, if S is a full shift on a prime number of symbols—we have from Theorem (2.5) that every $U \in \mathrm{Aut}(S)$, such that

$$\sup_{n \in \mathbf{N}} \sup_{1 \le k \le K_n(U,S)} L_{n,k}(U,S) < \infty,$$

is a composition of a power of S with an automorphism of finite order.

(2.9) THEOREM. *Let (X, S) be a topological Markov shift of positive entropy. Then no composition of automorphisms of finite order of S is equal to S.*

PROOF. Suppose that S is the composition of U_i, $1 \le i \le k$, U_i an element of finite order in $\mathrm{Aut}(S)$. Pick $n \in \mathbf{N}$ such that for any irreducible component (Y, T) of (X, S) of positive entropy $U_i^n Y = Y$, $1 \le i \le k$. Then each $U_i^n | Y$ is shiftless. Therefore each $S^n | Y$ is shiftless. This contradicts $\log \lambda_S^n = nh(S) > 0$. Q.E.D.

(2.10) PROPOSITION. *Let (X, S) be a topological Markov shift. Suppose ζ_S^{-1} is an irreducible polynomial and $U \in \mathrm{Aut}(X, S)$ is of finite order. Then US^i is a topological Markov shift that is shift equivalent to S^i, $i \in \mathbf{Z}$, $i \neq 0$.*

PROOF. The hypothesis on the zeta function implies that the kernel of $\tau\colon K_0(S) \to \mathbf{R}$ is trivial. From $\lambda_U = 1$ we conclude that ϕ_U is the identity. Also, if m is the order of U, then $(US^i)^m = S^{im}$, and by Lemma (2.7) it follows that US^i is a topological Markov shift. Also for an S- and U-invariant subset D of X

$$(W(D, S), \mathcal{F}_D(S)) = (W(D, S^i), \mathcal{F}_D(S^i)) = (W(D, US^i), \mathcal{F}_D(US^i))$$

and therefore,

$$\begin{aligned}(K_0, (US^i), K_0^+(US^i), \phi_{US^i}) &= (K_0(S), K_0^+(S), \phi_U \phi_S^i) \\ &= (K_0(S), K_0^+(S), \phi_S^i), \qquad i \in \mathbf{Z}. \quad \text{Q.E.D.}\end{aligned}$$

(2.11) LEMMA. *Let N, M be integers with $M > N \ge 0$. Let (X, S) be a subshift, and let U be an automorphism of S such that U and U^{-1} have coding bound N. Let $0 < \eta \le 2^{-(M+N)}$. Then US^M is expansive with expansive constant η, and*

$$W_\eta^+(x, US^M, I) \subset W_{1/2}^+(x, S, I(M+N)), \tag{1}$$

$$W_\eta^+(x, US^M, -I) \subset W_{1/2}^+(x, S, -I), \qquad I \in \mathbf{Z}_+,\ x \in X. \tag{2}$$

Both (1) *and* (2) *also hold with the unstable sets replacing the stable sets.*

PROOF. We first remark that for $x, y \in X$ and $i \in \mathbf{Z}$ with

$$x_i \neq y_i \tag{3}$$

there exist $j_-, j_+ \in \mathbf{Z}$, $i - M - N < j_- < i < j_+ < i + M + N$ such that

$$(US^M x)_{j-} \neq (US^M y)_{j-}, \qquad (U^{-1} S^{-M} x)_{j+} \neq (U^{-1} S^M y)_{j+}.$$

To see this, observe that for $i - N \le k \le i + N$ neither $(Ux)_k = (Uy)_k$, nor $(U^{-1}x)_k = (U^{-1}y)_k$ is possible, since this would contradict (3). Therefore we have a doubly infinite sequence of integers k_l, with $k_0 = i$, such that

$$k_{l-1} - M - N < k_l < k_{l-1}, \qquad l \in \mathbf{Z}, \tag{4}$$

and

$$(U^l S^{Ml} x)_{k_l} \neq (U^l S^{Ml} y)_{k_l}, \qquad l \in \mathbf{Z}. \tag{5}$$

In particular, for some integer L, $d(U^L S^{ML} x, U^L S^{ML} y) > 2^{-M-N}$ so η is an expansive constant for SU^M. Now suppose $x, y \in X$, $I \ge 0$ and

$$y \notin W_{1/2}^+(S, x, I(M+N)),$$

that is, we have some $k_0 \geq I(M+N)$ such that $x_{k_0} \neq y_{k_0}$. To prove (1), it is enough to show

$$y \notin W_\eta(US^M, x, I). \tag{6}$$

But it follows from (4) and (5) that there is an $L \geq I$ such that for some $k \in \mathbf{Z}$, $|k| < M+N$, $k = k_L$ and $(U^L S^{ML} x)_k \neq (U^L S^{ML} y)_k$, which shows (6). A similar argument establishes (2). The replacement of U and S by their inverses in (1) and (2) gives the final claim. Q.E.D.

(2.12) LEMMA. *Let N, M be integers with $M > N \geq 0$. Let (X, S) be a subshift, and let U be an automorphism of S such that U and U^{-1} have coding bound N. Let $\eta = 2^{-(M+N)}$. Then for I in $\mathbf{Z}_+$,*

$$W^+_{1/2}(x, S, I-(M+N)) \subset W^+_\eta(x, US^M, I), \tag{1}$$

$$W^+_{1/2}(x, S, (I-1)(M+N)) \supset W^+_\eta(x, US^M, I), \tag{2}$$

and

$$W^+_{1/2}(x, S, -(I+M+N)) \supset W^+_\eta(x, US^M, -I), \tag{3}$$

$$W^+_{1/2}(x, S, -(I+1)(M+N)) \subset W^+_\eta(x, US^M, -I). \tag{4}$$

Also, (1)–(4) *hold with the unstable sets replacing the stable sets.*

PROOF. For any $x \in X$, $i \in \mathbf{Z}$, $(x_j)_{i \leq j < \infty}$ determines $(US^M x)_j, i-1 \leq j < \infty$. From this, (1) follows by an induction. Also, $(x_j)_{-i \leq j < \infty}$ determines $(U^{-1}S^{-M}x)_j, i+(M+N) \leq j < \infty$. From this, (4) follows by an induction. Also, $W^+_\eta(x, US^M, i)$ determines $((US^M)^i x)_j, -(M+N) \leq j < \infty$. This with the previous facts gives (2) and (3). The replacement of U and S by their inverses in (1)–(4) gives the final claim. Q.E.D.

(2.13) LEMMA. *Let N, M be integers with $M > N \geq 0$. Let (X, S) be a subshift, and let U be an automorphism of S such that U and U^{-1} both have coding bound N. Then*

$$(W(D, US^M), \mathcal{F}_D(US^M)) = (W(D, S), \mathcal{F}_D(S)), \qquad D \subset X.$$

PROOF. $\frac{1}{2}$ is an expansive constant for S and $\eta = 2^{-(M+N)}$ is an expansive constant for $S^M U$. Then

$$W(D, S) = \bigcup_{x \in D} \bigcup_{I \in \mathbf{Z}} W^-_{1/2}(S, x, I)$$

while

$$W(D, US^M) = \bigcup_{x \in D} \bigcup_{I \in \mathbf{Z}} W^-_\eta(S^M U, x, I).$$

Therefore, by Lemmas (2.11) and (2.12), $W(D, US^M)$ and $W(D, S)$ are identical as sets. Now suppose $x \in W(D, S)$. In the topology of $W(D, S)$, the collection $\{W^-_{1/2}(S, x, I) \colon I \in \mathbf{Z}\}$ is a local basis of open sets for x, while in the topology of $W(D, S^M U)$ the collection $\{W^-_\eta(S^M U, x, I) \colon I \in \mathbf{Z}\}$ is a local basis. By Lemmas (2.11) and (2.12), these local bases refine each other. Therefore, $W(D, US^M)$ and $W(D, S)$ are identical as topological spaces.

By the same means, one has that the groups $\mathcal{F}_D(US^M)$ and $\mathcal{F}_D(S)$ are identical, recalling that a homeomorphism v is in $\mathcal{F}_D(US^M)$ if and only if there is an $I \in \mathbf{Z}_+$ such that $vy \in W_\eta^+(y, US^M, I)$, $y \in W(D,S)$, and is in $\mathcal{F}_D(D,S)$ if and only if there is an I in $\mathbf{Z}^+$ such that $vy \in W_{1/2}^+(y,S,I)$, $y \in W(D,S)$. Q.E.D.

(2.14) LEMMA. *Let (X,S) and (X,T) be commuting topological Markov shifts, S irreducible with period $p \in \mathbf{N}$. Then for some k dividing p, T is the union of p/k disjoint conjugate irreducible topological Markov shifts of period k.*

PROOF. X is the union of pairwise disjoint closed open sets $X_i, 1 \le i \le p$, where $S(X_i) = X_{i+1 \,(\mathrm{mod}\, p)}$. Since T is an automorphism of S, there is an integer L such that $T(X_i) = X_{i+L \,(\mathrm{mod}\, p)}$, $1 \le i \le p$. Then $S^p|X_i$ is an irreducible and aperiodic topological Markov shift, and therefore $T^p|X_i$ is also, $1 \le i \le p$.

Let $d = \gcd(p, L)$, let $p = dk$. Then for each i, the sets $T^j X_i$ are disjoint, $0 \le j < k$, and $T^k X_i = X_i$. Since $(T^k|X_i)^d$ is an irreducible and aperiodic topological Markov shift, so is $T^k|X_i$. Let T_i denote the restriction of T to $X_i \cup \cdots \cup T^{k-1}X_i$, $1 \le i \le p$. Then T_i is an irreducible topological Markov shift of period k, $1 \le i \le p/k$, and T_i and T_j are conjugate by way of $S^{j-i}T_i = T_j S^{j-i}$, $1 \le i, j \le p/k$. Q.E.D.

(2.15) LEMMA. *Let (X,S) be an irreducible topological Markov shift, and let $D \subset X$ be an S-invariant set. Let $\lambda' > 0$, and let τ' be an $\mathcal{F}_D(S)$-invariant Borel measure on $W(D,S)$ such that $0 < \tau'(SC) = \lambda'\tau'(C)$, $C \in \mathcal{C}_D(S)$. Then τ' is equal to $\tau_D(S)$ (up to a factor), and $\lambda' = \lambda_S$.*

PROOF. This follows from the fact that λ_S is the unique eigenvalue for a transition matrix of S that has a strictly positive eigenvector. Q.E.D.

(2.16) PROPOSITION. *Let N, M be integers with $M > N \ge 0$. Let (X,S) be a topological Markov shift, and let U be an automorphism of S such that U and U^{-1} have coding bound N. Then US^M is a topological Markov shift.*

PROOF. We know from Lemma (2.11) that US^M is expansive. We prove now that US^M has canonical coordinates. For all $I \in \mathbf{Z}_+$ and all $x \in X$, $(x_i)_{-I \le i < \infty}$ determines $(US^M x)_i, -I \le i < \infty$, and $(x_i)_{-\infty < i \le I}$ determines $(U^{-1}S^{-M}x)_i, -\infty < i \le I$. Therefore for all $\delta > 0$

$$W_\delta^+(x,S,0) \subset W_\delta^+(x, US^M, 0), \qquad x \in X,$$

and

$$W_\delta^-(y,S,0) \subset W_\delta^-(y, US^M, 0), \qquad y \in X.$$

Let $\varepsilon > 0$ be such that $d(x,y) < \varepsilon$ implies

$$W_\delta^+(x,S,0) \cap W_\delta^-(y,S,0) \neq \varnothing.$$

Then also

$$W_\delta^+(x, US^M, 0) \cap W_\delta^-(y, US^M, 0) \neq \varnothing. \quad \text{Q.E.D.}$$

(2.17) THEOREM. *Let M, N be integers with $M > N \ge 0$. Let (X,S) be a topological Markov shift, and let $U \in \mathrm{Aut}(S)$ be such that N is a coding bound for U and U^{-1}. Then US^M is a topological Markov shift with*

$$(1) \qquad (K_0(S^M U), K_0^+(S^M U), \phi_{S^M U}) = (K_0(S), K_0^+(S), \phi_S^M \phi_U).$$

The degree of ζ_S^{-1} *equals the degree of* $\zeta_{S^M U}^{-1}$. *If* S *is irreducible, then*

$$h(S^M U) = \log \lambda_U + M \log \lambda_S$$

and US^M *is irreducible and aperiodic if and only if* S *is aperiodic. If* ζ_S^{-1} *is an irreducible polynomial and* U *is shiftless, then* $S^M U$ *is shift equivalent to* S^M.

PROOF. Lemma (2.13) implies (1). The claim on degrees follows (1) because for any topological Markov shift T, the degree of ζ_T^{-1} equals the rank of $K_0(T)$.

Now suppose S is irreducible. By Lemma (2.14) and Proposition (2.16), US^M is the union of finitely many disjoint conjugate irreducible topological Markov shifts. Let (Y, T) be one of these, so $h(US^M) = h(T)$. By Lemma (2.13),

$$(W(Y, US^M), \mathcal{F}_Y(US^M)) = (W(Y, S), \mathcal{F}_Y(S)).$$

Because $\tau_Y(S)(C) = \tau_X(S)(C)$, $C \in \mathcal{C}_Y(S)$, it follows that

$$\tau_Y(S)(TC) = \tau_Y(S)(US^M C) = \lambda_U \lambda_S^M \tau_Y(S)(C), \qquad C \in \mathcal{C}_Y(T).$$

So by Lemma (2.15), $\tau_Y(T)$ equals $\tau_Y(S)$ (up to factor) and $h(T) = \log \lambda_U \lambda_S^M$. For aperiodicity, apply Lemma (2.14) to S and US^M. Finally, if ζ_S^{-1} is an irreducible polynomial and U is shiftless, then from (1)

$$(K_0(S^M), K_0^+(S^M), \phi_S^M) = (K_0(US^M), K_0^+(US^M), \phi_{US^M}). \quad \text{Q.E.D.}$$

(2.18) THEOREM. *Let* (X, S) *be an irreducible and aperiodic topological Markov shift, and let* $U \in \mathrm{Aut}(S)$. *Then*

$$\lim_{i \to \infty} |P_1(US^i)| \lambda_U^{-1} \lambda_S^{-i} = 1. \tag{1}$$

In particular, U *fixes arbitrarily long periodic* S*-orbits.*

PROOF. Let I be the rank of $K_0(S)$ and let μ be the maximal modulus of the eigenvalues of $\phi_S \otimes 1 \colon K_0(S) \otimes \mathbf{C} \to K_0(S) \otimes \mathbf{C}$ that are different from λ_S. By Theorem (2.17) we have an $i_0 \in \mathbf{N}$ such that, for $i \geq i_0$, US^i is an irreducible and aperiodic topological Markov shift, and

$$\phi_{US^i} = \phi_U \circ \phi_S^i, \tag{2}$$

$$\lambda_{US^i} = \lambda_U \lambda_S^i, \tag{3}$$

$$|P_1(US^i)| = \operatorname{trace} \phi_{US^i}, \qquad i \geq i_0. \tag{4}$$

Since $\phi_U \otimes 1$ and $\phi_S \otimes 1$ are commuting linear transformations of $K_0(S) \otimes \mathbf{C}$, it follows from (2) and (3), using $\mu < \lambda_S$, that the eigenvector of $\phi_S \otimes 1$ for the eigenvalue λ_S is also an eigenvector of $\phi_U \otimes 1$, and for $\phi_U \otimes 1$ has eigenvalue λ_U. It further follows that, with α the maximal modulus of the eigenvalues of $\phi_U \otimes 1$,

$$|\operatorname{trace} \phi_{US^i} - \lambda_U \lambda_S^i| < \alpha(I-1)\mu^i, \qquad i \in \mathbf{N},$$

and this together with (4) gives(1).

Now given $M \in \mathbf{N}$, choose $i \geq i_0$ such that

$$\operatorname{trace} \phi_{US^i} > \sum_{1 \leq m \leq M} |P_m^0(S)|.$$

Then for some $x \in X$ we have

$$US^i x = x \tag{5}$$

but

$$S^m x \neq x, \qquad 1 \leq m \leq M. \tag{6}$$

Here $Ux = S^{-i}x$, so U fixes the S-orbit of x, which must be finite, since by (5) all its points are fixpoints of the topological Markov shift US^i, and which by (6) contains more than M points. Q.E.D.

There are restrictions on the values that the return numbers of an automorphism can assume. In the next proposition, we explicitly formulate such a restriction.

(2.19) PROPOSITION. *Let (X, S) be an irreducible and aperiodic topological Markov shift, and let $U \in \mathrm{Aut}(X)$. Then there are $M, c > 0$ such that the length n and return number r under U of any S-orbit left fixed by U cannot satisfy $M < r < (\log n)/(\log \lambda_S) - c$.*

PROOF. Let M be a coding bound for U and U^{-1}. By Theorems (2.17) and (2.18) there is a $d > 0$ such that $|P_1(US^{-i})| < d\lambda_S^i$, $i > M$. Suppose $r > M, Q \in \mathcal{P}_n(S)$, $UQ = Q$, and the return number of Q under U is r. Then US^{-r} has at least n fixpoints. Therefore

$$n \leq d\lambda_S^r \quad \text{and} \quad r \geq \frac{\log n}{\log \lambda_S} - \frac{\log d}{\log \lambda_S}.$$

Set $c = (\log d)/(\log \lambda_S)$. Q.E.D.

3. Involutions. Extensions of automorphisms of finite subsystems. Consider again a dynamical system (X, S) such that $|P_n(S)| < \infty$, $n \in \mathbf{N}$. Let U be an involution in $\mathrm{Aut}(S)$, and let q be an odd integer. We partition $\mathcal{P}_q(S)$ into sets $\mathcal{D}_q(U, S)$ and $\mathcal{E}_q(U, S)$, setting

$$\mathcal{D}_q(U, S) = \{Q \in \mathcal{P}_q(S) \colon Ux \notin Q, x \in Q\},$$
$$\mathcal{E}_q(U, S) = \{Q \in \mathcal{P}_q(S) \colon Ux = x, x \in Q\},$$

and for $k \in \mathbf{N}$ we partition $\mathcal{P}_{2^k q}(S)$ into sets $\mathcal{C}_{2^k q}(U, S)$, $\mathcal{D}_{2^k q}(U, S)$ and $\mathcal{E}_{2^k q}(U, S)$, setting

$$\mathcal{C}_{2^k q}(U, S) = \{Q \in \mathcal{P}_{2^k q}(S) \colon Ux = S^{2^{k-1}q}x, x \in Q\},$$
$$\mathcal{D}_{2^k q}(U, S) = \{Q \in \mathcal{P}_{2^k q}(S) \colon Ux \notin Q, x \in Q\},$$
$$\mathcal{E}_{2^k q}(U, S) = \{Q \in \mathcal{P}_{2^k q}(S) \colon Ux = x, x \in Q\}.$$

(3.1) LEMMA. *Let S be such that every square-root of S^2 has zeta function equal to the zeta function of S. Let U be an involution in $\mathrm{Aut}(S)$. Then for all odd integers q,*

$$|\mathcal{C}_{2q}(U, S)| = \tfrac{1}{2}|\mathcal{D}_q(U, S)|. \tag{1}$$

PROOF. Since U is an involution

$$P_q^0(US) \subset P_{2q}(S). \tag{2}$$

If now for a divisor l of q, $x \in P_l^0(S) \cup P_{2l}^0(S)$, then $x \in P_{2l}(US)$, and if also $x \in P_q^0(US)$, then necessarily l is equal to q. Hence (2) implies that $P_q^0(US) \subset P_q^0(S) \cup P_{2q}^0(S)$. Since q is odd, a point in $P_q^0(S)$ will have period q under US only if its orbit belongs to $\mathcal{E}_q(U, S)$. A point in $P_{2q}^0(S)$ will have period $2q$ under US if its orbit is not in $\mathcal{C}_{2q}(U, S)$. If the orbit of an x in $\mathcal{P}_{2q}^0(S)$ is in $\mathcal{C}_{2q}(U, S)$ then

$USx = S^{q+1}x$, and we see that then the US-period of x is the least positive integer m such that $2q$ divides $m(q+1)$. Since q is odd, $2q$ divides $q(q+1)$, and since q and $q+1$ are relatively prime, no m smaller than q will do. The zeta functions of S and US being the same, (1) must hold. Q.E.D.

(3.2) LEMMA. *Let S be such that every square-root of S^{2^k} has zeta function identical to the zeta function of $S^{2^{k-1}}$, $k \in \mathbf{N}$. Let U be an involution in* $\mathrm{Aut}(S)$. *Then for all positive integers q,*

$$|D_q(U, S^{2^k})| = 2^k \left(\sum_{0 \le m \le k} |\mathcal{D}_{2^m q}(U, S)| \right), \qquad k \in \mathbf{N}.$$

PROOF. By Lemma (1.5)

$$P_q^0(S^2) = P_q^0(S) \cup P_{2q}^0(S).$$

Observe that an S^2-orbit that is contained in $P_q^0(S)$ is in $\mathcal{D}_q(U, S^2)$ if and only if it is in $\mathcal{D}_q(U, S)$. Also an S-orbit contained in $P_{2q}^0(S)$ splits into two S^2-orbits in $\mathcal{D}_q(U, S^2)$ precisely if it is in $\mathcal{C}_{2q}(U, S) \cup \mathcal{D}_{2q}(U, S)$. Therefore by Lemma (3.1)

$$\begin{aligned} |\mathcal{D}_q(U, S^2)| &= |\mathcal{D}_q(U, S)| + 2|\mathcal{D}_{2q}(U, S)| + 2|\mathcal{C}_{2q}(U, S)| \\ &= 2(|\mathcal{D}_q(U, S)| + |\mathcal{D}_{2q}(U, S)|). \end{aligned} \tag{1}$$

To prove the lemma by induction recall from Lemma (1.5) that

$$P_{2q}^0(S^{2^{k-1}}) = P_{2^k q}^0(S), \qquad k \in \mathbf{N},$$

and observe that an S-orbit in $P_{2^k q}^0(S)$ splits into $2^{k-1} S^{2^{k-1}}$-orbits in $D_{2q}(S^{2^{k-1}})$ if and only if it is in $D_{2^k q}(U, S)$. The induction step taken from (1) is then

$$\begin{aligned} |\mathcal{D}_q(U, (S^{2^{k-1}})^2)| &= 2(|\mathcal{D}_q(U, S^{2^{k-1}})| + |\mathcal{D}_{2q}(U, S^{2^{k-1}})|) \\ &= 2 \left(2^{k-1} \sum_{0 \le m < k} |\mathcal{D}_{2^m q}(U, S)| + 2^{k-1} |\mathcal{D}_{2^k q}(U, S)| \right) \\ &= 2^k \left(\sum_{0 \le m \le k} |\mathcal{D}_{2^m q}(U, S)| \right). \quad \text{Q.E.D.} \end{aligned}$$

(3.3) LEMMA. *Let S be such that for all $k \in \mathbf{N}$ every square-root of S^{2^k} has zeta function identical to the zeta function of $S^{2^{k-1}}$, $k \in \mathbf{N}$. Let U be an involution in* $\mathrm{Aut}(S)$. *Then for all odd positive integers q and all $k \in \mathbf{N}$,*

$$g(U, S)(2^k q) = \begin{cases} 0 & \text{if } \prod_{0 \le m < k} \operatorname{sign} \pi_{2^m q}(U, S) = 1, \\ 2^{k-1} q & \text{if } \prod_{0 \le m < k} \operatorname{sign} \pi_{2^m q}(U, S) = -1. \end{cases}$$

PROOF. Since U is an involution the return number of a point in $P_{2^k q}^0(S)$ whose orbit is not in $\mathcal{C}_{2^k q}(U, S)$ is zero. Therefore by Lemma (1.1)

$$g(U, S)(2^k q) = 2^{k-1} q |\mathcal{C}_{2^k q}(U, S)| \pmod{2^k q}.$$

Since the permutations $\pi_{2^m q}(U,S)$, $1 \le m < k$, are products of disjoint transpositions the lemma will be proved by showing that

$$|\mathcal{C}_{2^k q}(U,S)| = \frac{1}{2} \sum_{0 \le m < k} |\mathcal{D}_{2^m q}(U,S)|. \tag{1}$$

For this recall again from Lemma (1.5) that $P^0_{2^k q}(S) = P^0_{2q}(S^{2^{k-1}})$. Also, observe that an orbit Q in $P_{2^k q}(S)$ splits into 2^{k-1} orbits in $\mathcal{C}_{2q}(U, S^{2^{k-1}})$ if and only if Q is in $\mathcal{C}_{2^k q}(U,S)$. Therefore

$$2^{k-1}|\mathcal{C}_{2^k q}(U,S)| = |\mathcal{C}_{2q}(U, S^{2^{k-1}})|,$$

and an application of Lemmas (3.1) and (3.2) proves (1). Q.E.D.

All irreducible topological Markov shifts S with odd period and such that ζ_S^{-1} is an irreducible polynomial satisfy the hypothesis of Lemma (3.3).

We turn now to the automorphisms of the full shifts $(X_{(N)}, S_{(N)})$, $X_{(N)} = [0,N)^{\mathbf{Z}}$, $N > 1$. Here we use $[0,N)$ to represent $[0,N) \cap \mathbf{N}$; similar notation is used below. Our aim is to construct involutions of $S_{(N)}$ that interchange periodic orbits. We say that a periodic orbit of $S_{(N)}$ is given by a block $a \in [0,N)^{[0,L)}$, $L \in \mathbf{N}$, if it contains the periodic point that is given by the block a.

(3.4) LEMMA. *Let $L \in \mathbf{N}$, and let $a, b \in [0, N-1]^{[0,L)}$, $a \ne b$. Let the periodic orbit that is given by the block ab have length smaller than or equal to $2L/9$. Then there exists an l, $0 \le l < L$, such that with $\tilde{a} = a_l a_{l+1} \cdots a_{L-1} a_0 \cdots a_{l-1}$, $\tilde{b} = b_l b_{l+1} \cdots b_{L-1} b_0 \cdots b_{l-1}$ the periodic orbit that is given by the block $\tilde{a}\tilde{b}$ has length $2L$.*

PROOF. Since a is different from b, the length of the periodic orbit that is given by the block ab is even, say equal to $2k$. One has for some $q \ge 4$, $L = (2q+1)k$. Let

$$c^{(1)} = a_0 \cdots a_{k-1}, \quad c^{(2)} = a_k \cdots a_{2k-1}, \quad c = a_0 \cdots a_{2k-1}.$$

Then

$$a = \underbrace{c \cdots c}_{q} c^{(1)}, \qquad b = c^{(2)} \underbrace{c \cdots c}_{q}.$$

Let $l = 2qk - 1$. We assume that the periodic orbit that is given by the block

$$c^{(1)} \underbrace{c \cdots c}_{q} c^{(2)} c^{(2)} \underbrace{c \cdots c}_{q-1} c^{(1)}$$

has length $M < 2L$ and we derive a contradiction. Observe that the block cc admits c as a subblock only as its first or second half. Otherwise $2k$ would not be the length of the periodic orbit given by the block ab. In particular, $c^{(1)} \ne c^{(2)}$, and

$$c^{(1)} \underbrace{c \cdots c}_{q} \ne c^{(2)} c^{(2)} \underbrace{c \cdots c}_{q-1} c^{(1)},$$

and therefore $M < L$. It follows that M can only be a multiple of $2k$ smaller than or equal to $\frac{2}{3}L$. But this contradicts $c^{(1)} \ne c^{(2)}$. Q.E.D.

(3.5) LEMMA. *Let $L \in \mathbf{N}$, and let $a, b \in [0,N)^{[0,L)}$ be blocks such that the periodic orbits given by a and b have length L and are distinct. Then there exists an l, $0 \le l < L$, such that with $\tilde{a} = a_l a_{l+1} \cdots a_{L-1} a_0 \cdots a_{l-1}$, $\tilde{b} = b_l b_{l+1} \cdots b_{L-1} b_0 \cdots b_{l-1}$ the periodic orbit that is given by the block $\tilde{a}\tilde{b}$ has length $2L$.*

PROOF. By Lemma (3.4) we are left with a small number of cases. We indicate the proof for one of these. We consider the case that L is divisible by 105. Write $L = 105L_0$. There is then an $l', 0 \le l' < L$ such that $a_{L-l'} \ne b_{L-l'+35L_0 \,(\mathrm{mod}\ L)}$. Consider the case that

$$a_{L-l'} \cdots a_{L-l'+85L_0 \,(\mathrm{mod}\ L)} = b_{L-l'+21L_0 \,(\mathrm{mod}\ L)} \cdots b_{2L-l' \,(\mathrm{mod}\ L)}.$$

There is then an $l'', 0 \le l'' < 21L_0$ such that

$$a_{L-l'-l''} \ne b_{L-l'-l''+21L_0 \,(\mathrm{mod}\ L)}.$$

We consider the case that

$$a_{L-l'-l''} \cdots a_{L-l'-l''+90L_0 \,(\mathrm{mod}\ L)} = b_{L-l'-l''+15L_0} \cdots b_{2L-l'-l'' \,(\mathrm{mod}\ L)}.$$

There exists then finally an $l''', 0 < l''' < 15L_0$ such that

$$a_{L-l'-l''-l'''} \ne b_{L-l'-l''-l'''+15L_0 \,(\mathrm{mod}\ L)}.$$

Let then $l = L - l' - l'' - l'''$. Q.E.D.

(3.6) THEOREM. *Let $L \in \mathbf{N}$, and let x, y be periodic points of $(X_{(N)}, S_{(N)})$ of least period L whose orbits are distinct. Then there exists an involution $U(x,y)$ in $\mathrm{Aut}(S_{(N)})$ that maps x into y and leaves fixed all periodic points with a period less than or equal to L that are not in the orbits of x and y.*

PROOF. By Lemma (3.7) there exists an $i \in \mathbf{Z}$ such that the blocks $a = x_{i+1} \cdots x_{i+L}$, $b = y_{i+1} \cdots y_{i+L}$ have the following properties: the block aa admits the block a as a subblock only as its first or second half and does not admit the block b as a subblock, and also the block bb admits the block b as a subblock only as its first or second half, and does not admit the block a as a subblock. Let

$$\begin{aligned} E_l(a) = \{x \in X_{(N)} :\ & x_{-l} \cdots x_{-l+L-1} = a, \\ & x_{-l+kL} \cdots x_{-l+(k+1)L-1} \in \{a,b\}, k = -2,-1,1,2\}, \\ E_l(b) = \{x \in X_{(N)} :\ & x_{-l} \cdots x_{-l+L-1} = b, \\ & x_{-l+kL} \cdots x_{-l+(k+1)L-1} \in \{a,b\}, k = -2,-1,1,2\}, \\ & 0 \le l < L. \end{aligned}$$

The sets $E_i(a), E_i(b)$, $0 \le l < L$ are disjoint. One defines $U(x,y)$ by specifying the zero-coordinate mapping

$$(U(x,y)z)_0 = \begin{cases} b_l, & \text{if } z \in E_l(a),\ 0 \le l < L, \\ a_l, & \text{if } z \in E_l(b),\ 0 \le l < L, \\ z_0, & \text{if } z \in X_{(N)} - \bigcup_{0 \le l < L}(E_l(a) \cup E_l(b)). \end{cases}$$ Q.E.D.

We denote the group generated by the involutions in $\mathrm{Aut}(S_{(N)})$ by $J(S_{(N)})$.

(3.7) LEMMA. *Let $n \in \mathbf{N}$ and let V be an automorphism of $(\mathcal{P}_n(S_{(N)}), S_{(N)}|\mathcal{P}_n(S_{(N)}))$ with vanishing gyration number. Then there exists a $U \in J(S_{(N)})$ that leaves all periodic points of period less than n fixed, and such that $U_n = V$.*

PROOF. We fix $x_Q \in Q \in \mathcal{P}_n(S_{(N)})$, and adopt notation as at the beginning of §1. First, note that for all permutations π of $\mathcal{P}_n(S_{(N)})$ there exists a $U \in J(S_{(N)})$ that leaves all periodic points of period less than n fixed, and such that $U_n = W(\pi)$. If here π is a transposition, say of Q' and Q'', then $U(x_{Q'}, x_{Q''})$ will do. In general, write π as a product of transpositions.

The group $\{(\gamma_Q)_{Q\in\mathcal{P}_n(S_{(N)})} \in (\mathbf{Z}/n\mathbf{Z})^{\mathcal{P}_n(S_{(N)})}: \sum_{Q\in\mathcal{P}_n(S_{(N)})} \gamma_Q = 0\}$ is generated by the vectors $\gamma(Q', Q'')$, $Q', Q'' \in \mathcal{P}_n(S_{(N)})$, $Q' \neq Q''$, where

$$\gamma_Q(Q', Q'') = \begin{cases} 1 \pmod n & \text{if } Q = Q', \\ -1 \pmod n & \text{if } Q = Q'', \\ 0 \pmod n & \text{if } Q \neq Q', Q''. \end{cases}$$

The proof is completed by observing that the restriction of $U(x_{Q'}, x_{Q''})U(Sx_{Q''}, x_{Q'})$ to $\mathcal{P}_n(S_{(N)})$ is equal to $W(\gamma(Q', Q''))$. Q.E.D.

(3.8) THEOREM. *Let $n \in \mathbf{N}$, and let $U^{(l)}$, $1 \leq l \leq n$, be automorphisms of $(\mathcal{P}_l(S_{(N)}), S_{(N)}|\mathcal{P}_l(S_{(N)}))$, $1 \leq l \leq n$, such that for all odd q and all $k \in \mathbf{N}$, $1 \leq 2^k q \leq n$,*

$$g(U^{(2^k q)}) = \begin{cases} 0 & \text{if } \prod_{0\leq m<k} \operatorname{sign} \pi(U^{(2^m q)}) = 1, \\ 2^{k-1}q & \text{if } \prod_{0\leq m<k} \operatorname{sign} \pi(U^{(2^m q)}) = -1. \end{cases}$$

Then there exists a $V \in J(S_{(N)})$ such that $U^{(l)} = V_l$, $1 \leq l \leq n$.

PROOF. The argument is by induction. Assume a $V^0 \in J(S_{(N)})$ has been constructed such that $U^{(l)} = V_l^0$, $1 \leq l < n$. By Lemma (3.3) $g(U^{(n)}V_n^{0-1}) = 0$, so by Lemma (3.7) there is a $V' \in J(S_{(N)})$ such that $V_n' = U^{(n)}V_n^{0-1}$ and such that V_l' is the identity for $1 \leq l < n$. Let $V = V'V^0$. Q.E.D.

(3.9) COROLLARY. *Let $L \in \mathbf{N}$, and let π_l be a permutation of $\mathcal{P}_l(S_{(N)})$, $1 \leq l \leq L$. Then there exists a $U \in J(S_{(N)})$ such that $\pi(U_l) = \pi_l$, $1 \leq l \leq L$.*

PROOF. Use automorphisms $U^{(l)}$ of $(\mathcal{P}_l(S_{(N)}), S_{(N)}|\mathcal{P}_l(S_{(N)}))$ such that $\pi(U^{(l)}) = \pi_l$ and such that

$$g(U^{(2^k q)}) = \begin{cases} 0 & \text{if } \prod_{0\leq m<k} \operatorname{sign} \pi_{2^m q} = 1, \\ 2^{k-1}q & \text{if } \prod_{0\leq m<k} \operatorname{sign} \pi_{2^m q} = -1, \end{cases}$$

and apply Theorem (3.8). Q.E.D.

(3.10) COROLLARY. $\overline{(U^{(n)})}_{n\in\mathbf{N}} \in \overline{J(S_{(N)})}$ *if and only if for all odd q and all k*

$$g(U^{(2^k q)}) = \begin{cases} 0 & \text{if } \prod_{0\leq m<k} \operatorname{sign} \pi(U^{(2^m q)}) = 1, \\ 2^{k-1}q & \text{if } \prod_{0\leq m<k} \operatorname{sign} \pi(U^{(2^m q)}) = -1. \end{cases}$$

PROOF. The condition is necessary by Lemma (3.3) and sufficient by Theorem (3.8). Q.E.D.

We have obtained a necessary and sufficient condition for an automorphism of a finite subsystem of a full shift $S_{(N)}$ to possess an extension to an element of $J(S_{(N)})$. We must leave it open for the time being if every automorphism of a finite subsystem of an irreducible and aperiodic topological Markov shift can be extended to an automorphism of the shift. We prove now that every finite dynamical system can be embedded into an irreducible and aperiodic topological Markov shift in such a way that every automorphism of the finite system extends to an automorphism of the shift.

(3.12) THEOERM. *Let (X^0, S^0) be a finite dynamical system. Then there exists an irreducible and aperiodic topological Markov shift (X, S) that has (X^0, S^0) as a subsystem such that every automorphism of (X^0, S^0) extends to an automorphism of (X, S). The entropy of S can be made arbitrarily small. Given $L \in \mathbf{N}$, $|P_i(S)|$ can be made any number greater than or equal to $|P_i(S^0)|$, $1 \leq i \leq L$.*

PROOF. Let $n_1, \ldots, n_L$ be nonnegataive integers, with n_L nonzero. We produce a suitable (X, S) with the desired properties such that (X, S) has exactly n_l orbits of length l, $1 \leq l \leq L$. We will use two types of symbols for S. Symbols $a(j, k, l)$ will define the prescribed periodic orbits. A symbol $a(j, k, l)$ will be the jth symbol in the kth orbit of length l. So altogether we use $\{a(j, k, l) \colon 1 \leq l \leq L, 1 \leq k \leq n_l, 1 \leq j \leq l\}$. There is a transition allowed from $a(j, k, l)$ to $a(j', k', l')$ if and only if $l = l'$, $k = k'$ and $j' = j + 1 \pmod{l}$.

The other symbols will be $\{b_i \colon 1 \leq i \leq p - 1\}$, where p is a prime strictly larger than L. We allow a transition from b_i to b_j if and only if $1 < j = i + 1 \leq p - 1$. Finally, we allow any $a(j, k, l)$ to precede b_1 and to follow b_{p-1}. So, the graph we have is a collection of disjoint cycles on the $a(j, k, l)$ joined by a long ring formed from the b_i. There is a path from any symbol to any other, and there exist cycles whose lengths are relatively prime, since the cycle $b_1 \cdots b_{p-1} a(1, 1, L)$ has length $p > L$. So, the graph defines an aperiodic and irreducible topological Markov shift (X, S). By choosing p large enough, we can make the entropy of (X, S) as small as we like.

All orbits of length at most L come from the disjoint cycles defined on the $a(j, k, l)$. Any automorphism of the restriction of the shift to these orbits is given by an appropriate permutation of the symbols $a(j, k, l)$. Because all the $a(j, k, l)$ have the same followers and predecessors outside their l-cycles, such a permutation gives a well-defined 1-block map (fixing the symbols b_i) which is an automorphism of S. Q.E.D.

In particular, from the proposition one can obtain for any prime p an irreducible and aperiodic topological Markov shift (X, S) and an element U of finite order in $\mathrm{Aut}(X, S)$ such that $g(U, S)(p) \neq 0$. This U cannot be the composition of elements of finite order strictly less than p. In contrast, for $S_{(N)}$ we are unable to rule out the possibility that all elements of finite order are products of involutions, or even that all shiftless automorphisms are products of involutions.

ACKNOWLEDGMENT. We thank Doug Lind for stimulating discussions and the generation by computer of various gyration numbers. We thank the Mathematical Sciences Research Institute in Berkeley for the hospitality and support which made our collaboration possible. The work of the first author was supported in part by the IBM Watson Research Center. The work of the second author was done in part at

the Sonderforschungsbereich Stochastiche Mathematische Modelle of the University of Heidelberg under the auspices of the Deutsche Forschungsgemeinschaft.

REFERENCES

1. V. M. Alekseev, *Symbolic dynamics*, Eleventh Mathematical School (Summer School, Kolomyva, 1973), Izdanie Inst. Mat. Akad. Nauk Ukrain. SSR, Kiev, 1976, pp. 5–120. (Russian)
2. R. Bowen, *Topological entropy and Axiom* A, Proc. Sympos. Pure Math., vol. 14, Amer. Math. Soc., Providence, R.I., 1970, pp. 23–42.
3. R. Bowen and O. E. Lanford, *Zeta functions of restrictions of the shift transformation*, Proc. Sympos. Pure Math., vol. 14, Amer. Math. Soc., Providence, R.I., 1970, pp. 43–50.
4. M. Denker, C. Grillenberger and K. Sigmund, *Ergodic theory on compact spaces*, Lecture Notes in Math., vol. 527, Springer-Verlag, Berlin, 1976.
5. D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
6. G. A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory **3** (1969), 320–375.
7. W. Krieger, *On dimension functions and topological Markov chains*, Invent. Math. **56** (1980), 239–250.
8. W. Parry and S. Tuncel, *Classification problems in ergodic theory*, London Math. Soc. Lecture Notes Series 67, Cambridge Univ. Press, 1982.
9. R. F. Williams, *Classification of subshifts of finite type*, Ann. of Math. (2) **98** (1973), 120–153; *Errata* **99** (1974), 380–381.

MATHEMATICAL SCIENCES DEPARTMENT, IBM T. J. WATSON RESEARCH CENTER, YORKTOWN HEIGHTS, NEW YORK 10541

INSTITUT FUR ANGEWANDTE MATHEMATIK DER UNIVERSITAT, IM NEUENHEIMER FELD 294, 69 HEIDELBERG, FEDERAL REPUBLIC OF GERMANY (Current address of Wolfgang Krieger)

Current address (Mike Boyle): Department of Mathematics, University of Maryland, College Park, Maryland 20742