I.

SOME PROPERTIES AND EXAMPLES OF AUTOMORPHISMS ON THE BISEQUENCE SPACE.

by

SUSAN EVE GORDON

A DISSERTATION SUBMITTED TO THE FACULTY OF SCIENCE, UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG FOR THE DEGREE OF MASTER OF SCIENCE.

Johannesburg, 1976.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisor Dr. Michael Sears for his guidance, patient assistance and encouragement. I would also like to thank Mrs. Lilian Berger for her fine job of typing this dissertation.

TABLE OF CONTENTS

1. INTRODUCTION

Let $X(S)$ be the bisequence space over a finite symbol set S, where S has more than one element. Let σ be the shift transformation on $X(S)$. The topological properties of the shift dynamical system $(X(S),\sigma)$ have been analysed in [1], [2] and [3], and a study of the continuous transformations on $X(S)$ which commute with the shift was initiated in [3].

In this discussion, some of the known properties of the shift are summarised. The work done in [3] and [5] on the set $\Phi(S)$ of continuous, shift-commuting mappings on $X(S)$ is surveyed and further properties of $\Phi(S)$ are developed.

The basic structure theorem which characterises members of $\Phi(S)$ was first proved by Curtis, Hedlund and Lyndon, [3]. A proof of this result, due to Ryan [5] is given in section three, while the theorems, proved in [3], establishing conditions under which members of $\Phi(S)$ are onto or one-to-one, appear in sections four and five. In particular, the structure of the group of shift-commuting automorphisms, $A(S)$, was developed in [3], and Theorem 7.05, first proved by Curtis, Hedlund and Lyndon, shows that every finite group is isomorphic to some subgroup of $A(S)$.

The properties of members of $A(S)$ are of particular interest in an investigation of symbolic flows. A study of periodicity is undertaken in section six and results are developed which establish when a member of $A(S)$ is periodic. The concepts of permutivity and dependence, due to Hedlund [3] are used. It follows from Theorem 7.05 that for each integer k, there is a member of $A(S)$

which has period k. Based on an example by Hedlund [3], it is shown in 6.19 that a member of $A(S)$ also exists which has infinite order.

A question which arises from previous studies is that of determining which automorphisms on $X(S)$ have the same properties as the shift. A proof is given in section two of the statement that any property of the shift which is preserved by isomorphism of flows, will hold on the flow $(X(S),\sigma^n)$, where n is any non-zero integer. Furthermore, it is shown in this dissertation that a continuous mapping of $X(S)$ onto $X(S)$ behaves like the shift with respect to the topological properties of expansiveness, transitivity and mixing if the map is a root of some power of the shift. It can also be seen from section seven that not all mappings which satisfy the hypothesis of this theorem commute with the shift. It has, however, been proved by Ryan [5] that if a mapping commutes with every member of $A(S)$, then it is a power of the shift. Finally, it is deduced that every finite group is isomorphic to some subgroup of the inner automorphisms on $A(S)$.

2. THE BISEQUENCE SPACE AND THE SHIFT DYNAMICAL SYSTEM.

2.01. NOTATION. Let I denote the set of all integers. For i a member of I, let $I_i = \{j : j \in I , j \geq i\}$.

2.02. DEFINITIONS.

(i) Let S be a finite set which contains more than one element. The set S is called the *symbol set* and any element of S is a *symbol*. A convenient choice of S is the set $\{0, 1, \ldots , s - 1\}$, with s in I_2. The cardinal of S will be denoted *card* S.

(ii) A *bisequence over* S is a function on I to S. Let $X(S)$ denote the set of all bisequences over S, that is, $X(S)$ is S^I. The set $X(S)$ is the *bisequence set over* S.

2.03. NOTATION. If $x \in X(S)$ and $i \in I$, then $x(i)$ will often be denoted by x_i.

2.04. DEFINITION. *The bisequence space* $X(S)$ over S is the set $X(S)$ together with the metric d defined as follows: let x,y be members of $X(S)$. If $x = y$, then let $d(x,y) = 0$. If $x \neq y$ let k be the least non-negative integer such that either $x_k \neq y_k$ or $x_{-k} \neq y_{-k}$, and define $d(x,y) = (1 + k)^{-1}$.

2.05. REMARK. The metric topology induced by d coincides with the product topology induced by the discrete topology of S. The space $X(S)$ is a compact, totally disconnected, perfect,

2. THE BISEQUENCE SPACE AND THE SHIFT DYNAMICAL SYSTEM.

2.01. NOTATION. Let I denote the set of all integers. For i a member of I, let $I_i = \{j : j \in I , j \geq i\}$.

2.02. DEFINITIONS.

(i) Let S be a finite set which contains more than one element. The set S is called the *symbol set* and any element of S is a *symbol*. A convenient choice of S is the set $\{0, 1, \ldots , s - 1\}$, with s in I_2. The cardinal of S will be denoted *card* S.

(ii) A *bisequence over* S is a function on I to S. Let $X(S)$ denote the set of all bisequences over S, that is, $X(S)$ is S^I. The set $X(S)$ is the *bisequence set over* S.

2.03. NOTATION. If $x \in X(S)$ and $i \in I$, then $x(i)$ will often be denoted by x_i.

2.04. DEFINITION. *The bisequence space* $X(S)$ over S is the set $X(S)$ together with the metric d defined as follows: let x,y be members of $X(S)$. If $x = y$, then let $d(x,y) = 0$. If $x \neq y$ let k be the least non-negative integer such that either $x_k \neq y_k$ or $x_{-k} \neq y_{-k}$, and define $d(x,y) = (1 + k)^{-1}$.

2.05. REMARK. The metric topology induced by d coincides with the product topology induced by the discrete topology of S. The space $X(S)$ is a compact, totally disconnected, perfect, metric space and hence is homeomorphic to the Cantor discontinuum.

2.06. DEFINITIONS.

(i) The shift or shift transformation is the homeomorphism

$$\sigma : X(S) \xrightarrow{\text{onto}} X(S)$$

defined by $[\sigma(x)]_i = x_{i+1}$, x in $X(S)$, i in I.

(ii) The flow $(X(S),\sigma)$ is called the *discrete flow over* S or the *symbolic flow over* S or the *shift dynamical system over* S.

The following properties of the shift are well known.

2.07. DEFINITION. A homeomorphism θ on $X(S)$ is said to be *expansive* provided there exists a positive number δ such that if $x,y \in X(S)$ with $x \neq y$, then there exists an integer n such that $d(\theta^n(x), \theta^n(y)) \geq \delta$.

2.08. REMARK. The shift is expansive on $X(S)$, since if x and y are members of $X(S)$ with $x \neq y$, then there exists i in I such that $x_i \neq y_i$, and so $d(\sigma^i(x), \sigma^i(y)) = 1$.

2.09. DEFINITION. The homeomorphism θ is *point transitive* on $X(S)$ if there exists some x in $X(S)$ such that $\{\theta^i(x), i \in I\}$ is dense in $X(S)$.

2.10. NOTATION. An ordered set $x_1 x_2 \ldots x_n$, where $x_i \in S$, $(i = 1, 2, \ldots, n)$ is called a *block* of length n over S. If $x \in X(S)$ and A is an n-block over S, then A

appears in x if and only if there exists i in I such that $x_{i+1}x_{i+2}\ldots x_{i+n} = A$.

2.11. REMARK. If x is a member of $X(S)$ such that every block appears in x then the set $\bigcup_{i=-\infty}^{\infty}\{\sigma^i(x)\}$ is dense in $X(S)$, hence σ is point transitive on $X(S)$.

2.12. DEFINITION. The homeomorphism θ is said to be *strongly mixing* provided that if U and V are any two non-empty open subsets of $X(S)$, then there exists N such that $|n| \geq N$ implies that $\theta^n(U) \cap V \neq \phi$.

2.13. REMARK. To show that σ is strongly mixing on $X(S)$ we need only consider open sets of the form $S_{\frac{1}{n}}(x) = \{y : d(x,y) < \frac{1}{n}\}$, $x \in X(S)$, $n \in I$. Let $U = S_{\frac{1}{p}}(x)$ and $V = S_{\frac{1}{m}}(y)$, x and y in $X(S)$, m,p in I_1. Take $N = \max\{2p, 2m\}$. For each n with $|n| \geq N$, define $z^{(n)}$ by

$$z_i^{(n)} = y_i, \quad \text{if } |i| < m,$$

$$z_{i-n}^{(n)} = x_i, \quad \text{if } |i| < p,$$

$$z_j^{(n)} = 0 \quad \text{elsewhere.}$$

Then $z^{(n)}$ is a member of $V \cap \sigma^n(U)$.

2.14. DEFINITION. A homeomorphism θ on $X(S)$ is *transitive* or *ergodic* if for any two non-empty open sets U and V of $X(S)$ there exists some n in I such that $\theta^n(U) \cap V \neq \phi$.

2.15. REMARK. It is clear that if θ is point transitive or *strongly mixing on* $X(S)$ then θ is transitive, hence the shift is transitive on $X(S)$.

It is obvious that the *properties of the shift discussed* above hold also for the inverse of the shift. A problem which is suggested by this is that of determining to what extent powers of the shift behave like the shift on the bisequence space. Theorem 2.17 is concerned with this question.

2.16. DEFINITION. A flow (X,ϕ) is *isomorphic* to a flow (Y,θ) if there exists a homeomorphism ψ from X onto Y such that $\theta(\psi(x)) = \psi(\phi(x))$ for all x in X.

2.17. THEOREM. *Given any symbol set* S *of cardinality* $s > 1$ *and* n *in* I_1, *there exists a symbol set* S' *of cardinality* s^n *such that* $(X(S),\sigma^n)$ *is isomorphic to* $(X(S'),\sigma)$.

Proof. Let n be in I, and let $B_n(S)$ be the set of all n-blocks over S. Define S' to be the symbol set obtained by regarding each member of $B_n(S)$ as being written to the base S and converting it to the base s^n. Then the cardinal of S' is s^n.

Now suppose that x is [illegible] of $X(S)$, say x is the bisequence

$$\ldots x_{-2}x_{-1}\overset{\downarrow}{x_0}x_1x_2 \ldots,$$

then x may be represented as follows:

$$\ldots B_{-2}B_{-1}\overset{\downarrow}{B_0}B_1B_2 \ldots$$

where B_i is the n-block $x(n_i)x(n_{i+1}) \ldots x(n_i + n-1)$ and the "arrow" indicates tha... ...s indexed at the first position of B_0. Define $\psi : X(S) \to X(S')$ by $\psi(x) = y$, where $y(i)$ is the symbol of S' obtained by converting the n-block B_i from base S to base S^n.

It is easily verified that ψ is well-defined, one-to-one and onto.

The following argument shows that $\psi(\sigma^n(x)) = \sigma(\psi(x))$ for all x in $X(S)$. Let x be any bisequence over S represented in the form

$$\ldots B_{-2} B_{-1} \overset{\downarrow}{B_0} B_1 B_2 \ldots \qquad \text{as above.}$$

Then $\sigma^n(x)$ is

$$\ldots B_{-1} B_0 \overset{\downarrow}{B_1} B_2 B_3 \ldots$$

and $\psi(\sigma^n(x)) = y$, where $y(i)$ is obtained by regarding the block B_{i+1} as a number written to base S and converting it to base S^n. Now $\sigma(\psi(x)) = \sigma(z)$, where $z(i)$ is the conversion of B_i to base S^n. Thus $[\sigma(z)]_i = z_{i+1}$ which is the conversion of B_{i+1}.

To show that ψ is a homeomorphism of $X(S)$ onto $X(S')$, it is sufficient to show that ψ is continuous. Let $\varepsilon > 0$ and choose k in I_1 such that $(k+1)^{-1} < \varepsilon$. Let $\delta = (nk+1)^{-1} > 0$. Now if $x^{(1)}$ and $x^{(2)}$ are members of $X(S)$ with $d(x^{(1)}, x^{(2)}) < \delta$, then $x^{(1)}(ni)x^{(1)}(ni+1) \ldots x^{(1)}(ni+n-1) = x^{(2)}(ni)x^{(2)}(ni+1)\ldots x^{(2)}(ni+n-1)$, for all i with $|i| < k$. Hence, if $B_i^{(j)} = x^{(j)}(ni)\ldots x^{(j)}(ni+n-1), (j=1,2)$, then $B_i^{(1)} = B_i^{(2)}$ for all i with $|i| < k$. Suppose that $\psi(x^{(1)}) = y^{(1)}$ and $\psi(x^{(2)}) = y^{(2)}$. It follows from the above that

$y_i^{(1)} = y_i^{(2)}$ whenever $|i| < k$, whence $d(y^{(1)}, y^{(2)}) \leq \frac{1}{k+1} < \varepsilon$.

This completes the proof.

2.18. COROLLARY. *If property* P *holds on the flow* $(X(S'),\sigma)$ *for every symbol set* S', *and* P *is an isomorphism invariant, then given any symbol set* S *and* n *in* I_1, P *holds on the flow* $(X(S),\sigma^n)$.

Proof. Let n be an element of I_1 and $S = \{0, 1, \ldots, s-1\}$. Then there exists a symbol set S' of cardinality s^n such that $(X(S),\sigma^n)$ is isomorphic to $(X(S'),\sigma)$. Now P holds on $(X(S'),\sigma)$, hence on $(X(S),\sigma^n)$.

2.19. REMARK. The shift may be replaced by its inverse in the above Theorem and Corollary.

2.20. REMARK. It is well known that the properties of being point transitive and strongly mixing are isomorphism invariants and expansiveness is preserved under an isomorphism in the case of a compact space. It therefore follows that if n is any non-zero integer and S is a symbol set then σ^n is expansive, point transitive and strongly mixing on $X(S)$.

2.21. DEFINITION. Let x be in $X(S)$. The point x is said to be *periodic* if there exists some w in I_1 such that $x_i = x_{i+w}$ for all i in I. Hence x is periodic if and only if there exists w in I_1 such that $\sigma^w(x) = x$.

2.22 REMARK. Clearly the set of periodic points in dense in $X(S)$.

2.23. DEFINITION. Furstenburg, [1], defines a flow (X,T) to be an *F-flow* if is satisfies the following two conditions:

(i) Each of the flows (X,T^m) , $m = 1 , 2 , 3 , \ldots$ is ergodic.

(ii) The set of all fixed points of all the powers T^m (i.e. , $\{w : \text{for some } m , T^m(w) = w\}$) is dense in X.

2.24. REMARK. Since the flows $(X(S),\sigma^n)$ $n = 1 , 2 , 3 , \ldots$ are strongly mixing, hence ergodic, and the periodic points are dense in $X(S)$, the flow $(X(S),\sigma)$ is an F-flow.

3. CONTINUOUS MAPPINGS WHICH COMMUTE WITH THE SHIFT.

3.01. NOTATION. Let n be an element of I_1 and $B_n(S)$ denote the set of all n-blocks over S. Let f be a mapping of $B_n(S)$ into $B_1(S) = S$. The set of all such mappings for a given n in I_1 and a given symbol set S is denoted by $F(S,n)$. Each member f of $F(S,n)$ induces a function $f_\infty : X(S) \to X(S)$ in the following way: for x in $X(S)$ and any integer i define $[f_\infty(x)]_i = f(x_i \dots x_{i+n-1})$.

3.02. PROPOSITION. *Let* f *be a member of* $F(S,n)$. *Then* $f_\infty : X(S) \to X(S)$ *is continuous and commutes with the shift* σ.

Proof. Let f be in $F(S,n)$, let x be a member of $X(S)$ and let $f_\infty(x) = y$. Suppose that $\varepsilon > 0$ and let k be in I_1 with $(1+k)^{-1} < \varepsilon$. Choose $\delta > 0$ such that $\delta < (1 + k + n)^{-1}$ and let u be an element of $X(S)$ with $d(x,u) < \delta$. Then if $|i| \leqslant k + n$, $x_i = u_i$. Let $f_\infty(u) = v$. Then for all i with $|i| \leqslant k$, $y_i = v_i$, whence $d(y,v) = d(f_\infty(x), f_\infty(u)) < \varepsilon$. It follows that f_∞ is continuous.

Now suppose that $x \in X(S)$ and $y = f_\infty(x)$. Then for each integer i, $[\sigma f_\infty(x)]_i = [\sigma(y)]_i = y_{i+1} = f(x_{i+1} \dots x_{i+n})$; $[f_\infty \sigma(x)]_i = f([\sigma(x)]_i \dots [\sigma(x)]_{i+n-1}) = f(x_{i+1} \dots x_{i+n})$. Thus $\sigma f_\infty(x) = f_\infty \sigma(x)$ so f_∞ commutes with the shift.

3.03. NOTATION. Let $F_\infty(S,n) = \{f_\infty : f \in F(S,n)\}$.

3.04. REMARK. If $1 \leqslant m < n$ then $F_\infty(S,m) \subset F_\infty(S,n)$. For if

$f \in F(S,m)$, we may define $g : B_n(S) \to B_1(S)$ by

$g(x_1 \ldots x_n) = f(x_1 \ldots x_m)$. Then $f_\infty = g_\infty \in F_\infty(S,n)$.

3.05. PROPOSITION. *Let* n *be in* I_1 *and* S *be a symbol set. Then* $\sigma^k \in F_\infty(S,n)$ *if and only if* $0 \leq k \leq n-1$.

Proof. Let n be an element of I_1 and let k be an integer, $0 \leq k \leq n-1$. Define $f : B_n(S) \to B_1(S)$ by $f(x_i x_{i+1} \ldots x_{i+n-1}) = x_{k+i}$, $(i \in I)$. Then $\sigma^k = f_\infty \in F_\infty(S,n)$.

Conversely, suppose that $\sigma^k \in F_\infty(S,n)$ for k an integer. Then there exists f in $F(S,n)$ such that $\sigma^k = f_\infty$, whence $f_\infty \sigma^{-k} = \sigma^{-k} f_\infty$ is the identity map on $X(S)$ and $[\sigma^{-k} f_\infty(x)]_i = [f_\infty(x)]_{i-k} = f(x_{i-k} \ldots x_{i-k+n-1}) = x_i$ for all x in $X(S)$ and all integers i. In particular, $f(x_1 \ldots x_n) = x_{k+1}$ for all x. Suppose that $k < 0$ or $k > n-1$. Define x by choosing $x_i = 0$ if $i \neq k+1$ and $x_{k+1} \neq f(x_1 \ldots x_n)$. It follows that $\sigma^k \notin F_\infty(S,n)$.

3.06. NOTATION. (i) Let $F_\infty(S)$ denote the set $\bigcup_{n=1}^{\infty} F_\infty(S,n)$. Note that if $k \geq 0$, then $\sigma^k \in F_\infty(S)$, but as the cardinal of S is > 1 , $\sigma^k \notin F_\infty(S)$ if $k < 0$.

(ii) Let $F^*_\infty(S)$ denote the set $\{\sigma^m \phi : m \in I , \phi \in F_\infty(S)\}$.

(iii) Let $\Phi(S)$ be the set of all continuous mappings of $X(S)$ into $X(S)$ which commute with σ.

3.07. REMARK. It is clear that $F_\infty(S) \subset F^*_\infty(S) \subset \Phi(S)$ and as $k < 0$ implies that $\sigma^k \notin F_\infty(S)$, $F_\infty(S)$ is a proper subset of $F^*_\infty(S)$. The next theorem shows that the last two sets are identical. The proof is due to J.P. Ryan [5].

3.08. THEOREM. $F_{\infty}^{*}(S) = \Phi(S)$.

Proof. It is sufficient to show that $\Phi(S) \subset F_{\infty}^{*}(S)$. Let ϕ be in $\Phi(S)$. Since ϕ is uniformly continuous, there exists a positive integer m such that if x and y are in $X(S)$ and $d(x,y) < (1+m)^{-1}$, then $d(\phi(x), \phi(y)) < 1$ or equivalently, $[\phi(x)]_0 = [\phi(y)]_0$. Let $n = 2m+1$ and define $f : B_n(S) \to S$ as follows : if A is any n-block such that $A = x_{-m} \ldots x_0 \ldots x_m$ for some x in $X(S)$, then $f(A) = [\phi(x)]_0$. The function f is a well-defined member of $F(S,n)$. Now let x be any element of $X(S)$. Then

$[\sigma^{-m} f_{\infty}(x)]_i = [f_{\infty}(x)]_{i-m} = [\sigma^{i} f_{\infty}(x)]_{-m} = [f_{\infty}\sigma^{i}(x)]_{-m}$

$= f([\sigma^{i}(x)]_{-m}[\sigma^{i}(x)]_{-m+1} \ldots [\sigma^{i}(x)]_{m}) = [\phi\sigma^{i}(x)]_0$

$= [\sigma^{i}\phi(x)]_0 = [\phi(x)]_i$, for any integer i.

Hence $\phi = \sigma^{-m} f_{\infty}$ and the proof is complete.

4. ONTO MEMBERS OF $F_{\infty}(S)$

4.01 DEFINITION. Let n be an element of I_1. For every f in $F(S,n)$ and m in I_1 define a mapping $f_m : B_{m+n-1}(S) \to B_m(S)$ as follows : if $B = b_1 b_2 \ldots b_{m+n-1}$ is any $(m+n-1)$-block over S then

$f_m(b_1 \ldots b_{m+n-1}) = f(b_1 \ldots b_n) f(b_2 \ldots b_{n+1}) \quad . \; f(b_m \ldots b_{m+n-1})$.

Clearly $f_1 = f$.

4.02. THEOREM. *Let n be in I_1 and let f be a member of $F(S,n)$. Then f_{∞} is onto if and only if each $f_m : B_{m+n-1}(S) \to B_m(S)$ is onto for all m in I_1.*

Proof. Assume that f_{∞} is onto. Let m be in I_1 and let $B = b_1 b_2 \ldots b_m$ be a member of $B_m(S)$. Let x in $X(S)$ be defined by $x_i = 0$ if $i > m$ or $i \leq 0$ and $x_1 x_2 \ldots x_m = B$.

There exists y in $X(S)$ such that $f_\infty(y) = x$. Let $A = y_1 y_2 \dots y_{m+n-1}$. Then $f_m(A) = B$, hence f_m is onto.

Conversely, assume that $f_m : \mathcal{B}_{m+n-1}(S) \to \mathcal{B}_m(S)$ is onto for each m in I_1. Let x be in $X(S)$ and let k be in I_1. Let $m = 2k + 1$. Then $B = x_{-k} \dots x_k \in \mathcal{B}_m(S)$ and there exists an $(m+n-1)$-block A such that $A = y_{-k} \dots y_{k+n-1}$ and $f_m(A) = B$. Define y in $X(S)$ by $y_{-k} \dots y_{k+n-1} = A$, $y_i = 0$ if $i < -k$ or $i > k+n-1$, and let $f_\infty(y) = u$. Then $u_{-k} \dots u_k = x_{-k} \dots x_k$ and $d(x,u) < (1+k)^{-1}$. Since k is arbitrary in I_1, it follows that the set $f_\infty(X(S))$ is dense in $X(S)$. But since f_∞ is continuous and $X(S)$ is compact, $f_\infty(X(S))$ is compact, hence closed, and so $f_\infty(X(S)) = \overline{f_\infty(X(S))} = X(S)$. Thus f_∞ is onto.

4.03. REMARK. If card $S = s$ and n is in I_1, and if card $f_m^{-1}\{B\} = s^{n-1}$ for all B in $\mathcal{B}_m(S)$ and all m in I_1, then it follows from Theorem 4.02 that f_∞ is onto. Theorem 4.07 shows that the converse of this statement is also true. The result is due to W.A. Blankenship and O.S. Rothaus [3].

4.04. NOTATION. Let n, m be in I_1. If $A = a_1 \dots a_m \in \mathcal{B}_m(S)$ and $B = b_1 \dots b_n \in \mathcal{B}_n(S)$, then AB will denote the $(m+n)$-block $a_1 \dots a_m b_1 \dots b_n$. If $\mathcal{A}$ and $\mathcal{B}$ are collections of blocks over S, then $\mathcal{A}\mathcal{B}$ will denote $\{AB : A \in \mathcal{A}, B \in \mathcal{B}\}$. The notation may be generalised in the obvious way.

4.05. LEMMA. *Let* n *be in* I_1 *and let* f *be in* $F(S,n)$. *Suppose there exists an* m*-block* B *over* S *such that* *card* $f_m^{-1}\{B\} = k > 0$ *and card* $f_{m+1}^{-1}(Bb) \geqslant k$ *for each* b *in* S. *Then card* $f_{m+1}^{-1}(Bb) = k$ *for each* b *in* S.

Proof. Let B be a member of $\mathcal{B}_m(S)$ such that card $f_m^{-1}\{B\} = k > 0$. Suppose that $f_m^{-1}\{B\} = \{C_1, C_2, \ldots, C_k\} = \mathcal{C}$. Then $f_{m+1}^{-1}(BS) = \mathcal{C}S$. For if $c \in S$, $f_{m+1}(C\,c) \in BS$ if and only if C is an $(m+n-1)$-block such that $f_m(C) = B$, that is *if and only if* $C \in \mathcal{C}$.

Thus card $f_{m+1}^{-1}(BS) = kS = \sum\limits_{b \text{ in } S} \text{card } f_{m+1}^{-1}\{Bb\}$. Now suppose that card $f_{m+1}^{-1}\{Bb\} \geqslant k$ for each b in S. If, for some b in S, card $f_{m+1}^{-1}\{Bb\} > k$, then card $f_{m+1}^{-1}(BS) > kS$. Hence card $f_{m+1}^{-1}\{Bb\} = k$ for each b in S, which concludes the proof of the Lemma.

4.06. LEMMA. *Let* n *be in* I_2 *and let* f *be a member of* $F(S,n)$. *Let there exist an* n*-block* B *over* S *such that card* $f_m^{-1}\{B\} = k > 0$ *and card* $f_{2m+n-1}^{-1}\{BDB\} = k$ *for every* $(n-1)$*-block* D. *Then* $k = s^{n-1}$.

Proof. Let $f_m^{-1}\{B\} = \{C_1, \ldots, C_k\} = \mathcal{C}$. Let $\mathcal{D} = \mathcal{B}_{n-1}(S)$. The following argument shows that

$$f_{2m+n-1}^{-1}(B\mathcal{D}B) = \mathcal{C}\mathcal{C} \qquad (1)$$

Let A be a member of $\mathcal{C}\mathcal{C}$. Then $A = C_iC_j$ where C_i, C_j are in $\mathcal{C}$. Since C_i and C_j are of length $m+n-1$ each, A is of length $2m + 2n - 2$ and $f_{2m+n-1}(A) = E$ is of length $2m + n - 1$. Since $f_m(C_i) = B = f_m(C_j)$, E *is of the form* BDB, *where* D *is* of length $n-1$, so that $A \in f_{2m+n-1}^{-1}(B\mathcal{D}B)$.

Now suppose that $f_{2m+n-1}(A) = BDB$, where $D \in \mathcal{D}$. Then

A is of length $2m + 2n - 2$, $A = A_1 A_2$, where A_1 and A_2 are of length $m + n - 1$, $f_m(A_1) = B = f_m(A_2)$, so that $A_1, A_2 \in \mathcal{C}$ and $A_1 A_2 \in \mathcal{CC}$.

It follows that $f^{-1}_{2m+n-1}(B\mathcal{D}B) = \mathcal{CC}$.

Clearly card $\mathcal{CC} = k^2$. If card $f^{-1}_{2m+n-1}\{BDB\} = k$ for each D in $\mathcal{D}$, then since card $\mathcal{D} = S^{n-1}$, card $f^{-1}_{2m+n-1}(B\mathcal{D}B) = k\, S^{n-1}$. From (1) it follows that $k^2 = k\, S^{n-1}$; thus $k = S^{n-1}$.

4.07. THEOREM. *Let* n *be in* I_1 *and let* f *be in* $F(S,n)$. *Then the following statements are equivalent.*

(1) f_∞ *is onto*

(2) *card* $f_m^{-1}\{B\} = S^{n-1}$ *for all* B *in* $\mathcal{B}_m(S)$ *and for all* m *in* I_1.

Proof. It is sufficient to prove that (1) implies (2). Suppose $n = 1$. For any a in S, define x in $X(S)$ by $x_0 = a$, $x_i = 0$, $i \neq 0$. Then there exists y in $X(S)$ such that $f_\infty(y) = x$; thus $f(y_0) = a$ and f is onto, hence f is a permutation on S. Now it follows from Theorem 4.02 that for any m in I_1 and B in $\mathcal{B}_m(S)$, card $f_m^{-1}\{B\} \geq 1$. Suppose for some m-block B there exist blocks $A = a_1 \ldots a_m$ and $A' = a'_1 \ldots a'_m$ in $\mathcal{B}_m(S)$ such that $f_m(A) = f_m(A') = B$. Then $f(a_i) = f(a'_i) = b_i$, $1 \leq i \leq m$; thus $a_i = a'_i$, $1 \leq i \leq m$, and so $A = A'$. It follows that card $f_m^{-1}\{B\} = S^0$, for all B in $\mathcal{B}_m(S)$ and for all m in I_1.

Now suppose that $n \geq 2$. Let

$$k = \inf\{\text{card } f_m^{-1}\{B_m\} : B_m \in \mathcal{B}_m(S),\ m \in I_1\}.$$

It follows from Theorem 4.02 that $k \geq 1$. There exist an integer m and an m-block B over S such that card $f_m^{-1}(B) = k$. Then card $f_{m+1}^{-1}(Bb) \geq k$ for each b in S, so it follows from Lemma 4.05 that card $f_{m+1}^{-1}(Bb) = k$ for each b in S. It can be inferred by induction that card $f_{m+i}(BA) = k$ for every i-block A and hence, in particular, card $f_{2m+n-1}^{-1}(BDB) = k$ for every D in $\mathcal{B}_{n-1}(S)$ It follows from Lemma 4.06 that $k = s^{n-1}$ and thus card $f_p^{-1}(B_p) \geq s^{n-1}$ for each B_p in $\mathcal{B}_p(S)$ and each p in I_1.

Suppose there exist p in I_1 and B in $\mathcal{B}_p(S)$ such that card $f_p^{-1}(B) > s^{n-1}$. Then

$$\sum_{B_p \text{ in } \mathcal{B}_p(S)} \text{card } f_p^{-1}(B_p) > s^{p+n-1}, \tag{2}$$

since card $f_p^{-1}(B) > s^{n-1}$ and card $f_p^{-1}(B_p) \geq s^{n-1}$ for each B_p in $\mathcal{B}_p(S)$. It follows, however, from Theorem 4.02 that $f_p^{-1}(\mathcal{B}_p(S)) = \mathcal{B}_{p+n-1}(S)$, so that

$$\sum_{B_p \text{ in } \mathcal{B}_p(S)} \text{card } f_p^{-1}(B_p) = \text{card } f_p^{-1}(\mathcal{B}_p(S))$$

$$= \text{card } \mathcal{B}_{p+n-1}(S) = s^{p+n-1}$$ which

contradicts (2). Hence card $f_m^{-1}(B) = s^{n-1}$ for B in $\mathcal{B}_m(S)$ and all m in I_1. This completes the proof.

5. CHARACTERISATION OF SHIFT-COMMUTING AUTOMORPHISMS ON $X(S)$.

5.01. NOTATION. The set of shift-commuting automorphisms on $X(S)$ will be denoted $A(S)$. Thus $A(S)$ is the set of homeomorphisms of $X(S)$ onto $X(S)$ which commute with the shift.

5.02. PROPOSITION. *Let* f *be a member of* $F(S,1)$. *Then* $f_\infty \in A(S)$ *if and only if* f *is a permutation of* S.

Proof. Suppose that f is a permutation of S. Let x be in $X(S)$. Then for each integer i, there is an element y_i in S such that $f(y_i) = x_i$. Hence there exists y in $X(S)$ such that $f_\infty(y) = x$ and f_∞ is onto. Suppose that f_∞ is not one-to-one. Then there are elements x,y in $X(S)$ such that $x \neq y$ and $f_\infty(x) = f_\infty(y)$. By definition of f_∞, $[f(x)]_i = [f(y)]_i$ for all integers i. But since $x \neq y$, there exists an integer i such that $x_i \neq y_i$, which implies that $f(x_i) \neq f(y_i)$, as f is a permutation of S. Hence f_∞ must be one-to-one and so is a member of $A(S)$.

Conversely, suppose that $f_\infty \in A(S)$. As f_∞ is onto, it follows from Theorem 4.02 that $f : S \to S$ is onto, hence f is a permutation of S.

5.03. REMARK. *The following theorems proved in* [3] *show that* $A(S)$ consists precisely of those members of $\Phi(S)$ which are one-to-one.

5.04. LEMMA. *Let* m *be in* I_1 *and let* B *be an m-block over* S. *For* q *in* I_1, $q \geqslant m$, *Let* $\mathcal{D}(B,q)$ *be the set of all q-blocks over* S *in which* B *appears and let* $N(B,q) = \operatorname{card} \mathcal{D}(B,q)$ *Then*

$$\lim_{q\to\infty} \frac{N(B,q)}{S^q} = 1$$

Proof. Let $\phi(q) = S^{-q}N(B,q)$. Let c be in $\mathcal{D}(B,q)$. Then $Cc \in \mathcal{D}(B,q+1)$ for each c in S, so that $N(B,q+1) \geqslant S.N(B,q)$ and hence $\phi(q+1) = S^{-(q+1)}N(B,q+1) \geqslant S^{-q}N(B,=) = \phi(q)$. Since card $B_q(S) = S^q$, it follows that $N(B,q) \leqslant S^q$, whence $\phi(q) \leqslant 1$. Thus $\lim_q \phi(q) = \alpha$, where $0 \leqslant \alpha \leqslant 1$.

Let k be in I_1 and let A be a block of length km. Then $A = B_1B_2 \dots B_k$, where each B_i is an m-block, $1 \leqslant i \leqslant k$. Let $\mathcal{A}_i$ be the collection of all such blocks A for which $B_i = B$, $B_j \neq B$ if $j < i$ and B_j is arbitrary for $j > i$. If $i \neq j$, then $\mathcal{A}_i \cap \mathcal{A}_j = \phi$. Let $\mathcal{A}(k) = \bigcup_{i=1}^{k} \mathcal{A}_i$. Then B appears in every member of $\mathcal{A}(k)$; hence $N(B,km) \geqslant$ card $\mathcal{A}(k)$, and so

$$\phi(km) = S^{-km}N(B,km) \geqslant S^{-km} \text{ card } \mathcal{A}(k). \qquad (1)$$

Let $a = S^m - 1$, $b = S^m$. Then

$$\text{card } \mathcal{A}(k) = \sum_{i=1}^{k} \text{card } \mathcal{A}_i = \sum_{i=1}^{k} a^{i-1}b^{k-i} = \sum_{i=1}^{k} \frac{b^k}{a}\left(\frac{a}{b}\right)^i$$

$$= (a^k - b^k)/(a - b) = S^{km} - (S^m - 1)^k.$$

It follows from (1) that

$$1 \geqslant \lim_{q\to\infty} \phi(q) = \lim_{h\to\infty} \phi(km) \geqslant \lim_{k\to\infty} S^{-km}[S^{km} - (S^m-1)^k]$$

$$= \lim_{k\to\infty} \{1 - [1 - \frac{1}{S^m}]^k\} = 1.$$

Hence $\lim_{q\to\infty} N(B,q)S^{-q} = 1$.

5.05 LEMMA. *Let* m *be in* I_1 , *let* f *be in* $F(S,n)$ *and suppose that* f_∞ *is not onto. Let* k,t *be in* I_1. *Then there exists an m-block* A *with* $m \geqslant t$ *such that card* $f_m^{-1}\{A\} > k$.

Proof. Assume the hypothesis of the lemma and suppose that card $f_m^{-1}\{A\} \leqslant k$ for all m-blocks A , $m \geqslant t$. Since f_∞ is not onto, it follows from Theorem 4.02 that there exists an integer $q \geqslant 1$ and B in $\mathcal{B}_q(S)$ such that $fq^{-1}\{B\} = \phi$, whence card $fq^{-1}\{B\} = 0$. This plies that card $f_m^{-1}\{D\} = 0$, where D is any m-block in which B appears.

Let $\mathcal{D}(B,m)$ be the set of all m-blocks over S in which B appears and let $\mathcal{D}'(B,m)$ be the set of all m-blocks over S in which B does not appear. Let $N(B,m) = \text{card } \mathcal{D}(B,m)$. Since $\mathcal{B}_m(S) = \mathcal{D}(B,m) \cup \mathcal{D}'(B,m)$ and card $\mathcal{B}_m(S) = s^m$,
card $\mathcal{D}'(B,m) = s^m - N(B,m)$. Now $\mathcal{B}_{m+n-1}(S) = f_m^{-1}(\mathcal{B}_m(S))$
$= f_m^{-1}(\mathcal{D}(B,m) \cup f_m^{-1}(\mathcal{D}'(B,m))$ and the sets $\mathcal{D}(B,m)$ and $\mathcal{D}'(B,m)$ are disjoint, so that
$s^{m+n-1} = \text{card } \mathcal{B}_{m+n-1}(S) = \text{card } f_m^{-1}(\mathcal{D}(B,m) + \text{card } f_m^{-1}(\mathcal{D}'(B,m))$.
If $m \geqslant q$, card $f_m^{-1}(\mathcal{D}(B,m)) = 0$, so that $s^{m+n-1} = \text{card } f_m^{-1}(\mathcal{D}'(B,m))$.
By assumption, card $f_m^{-1}\{A\} \leqslant k$ for all m-blocks A , $m \geqslant t$.
Thus if $m \geqslant t + q$

$$s^{m+n-1} \leqslant k \text{ card } \mathcal{D}'(B,m) = k\,[\,s^m - N(B,m)]$$

Hence

$$N(B,m) \leqslant s^m - s^{m+n-1}/k$$

that is ,

$$N(B,m)/S^m \leq 1 - S^{n-1}/k$$

This implies that

$$\limsup_{m\to\infty} N(B,m)/_{S^m} \leq 1 - S^{n-1}/k < 1 \text{ , contrary to}$$

Lemma 5.04.

This completes the proof.

5.06. LEMMA. *Let* n *be in* I_2 , m *in* I_1 *and let* E *be a collection of* $(m + 2n - 2)$-blocks *over* S *such that* card $E > S^{2n-2}$. *Then there exist distinct blocks* E *and* E^* *in* E *such that* $E = ADB$ *and* $E^* = AD^*B$, *where* A *and* B *are* $(n-1)$-blocks.

Proof. Let $B_n(S) = \{A_i : i = 1 , 2 , \ldots , S^{n-1}\}$. For $1 \leq i \leq S^{n-1}$, Let E_i be the collection of all members of E with initial $(n-1)$-block A_i. Suppose that for all i , card $E_i \leq S^{n-1}$. Then card $E = \sum_{i=1}^{S^{n-1}}$ card $E_i \leq S^{n-1}S^{n-1} = S^{2n-2}$, contrary to hypothesis.

Thus there exists an integer j such that card $E_j > S^{n-1}$. But then at least two distinct members of E_j must have the same terminal $(n-1)$-block B. Let these be A_jDB and A_jD^*B. The proof of the Lemma is concluded by taking $A = A_j$, $E = ADB$ and $E^* = AD^*B$.

5.07. LEMMA. *Let* n *be in* I_2 , *let* f *be a member of* $F(S,n)$ *and let* m *be in* I_1. *Let there exist an* $(m+n-1)$-block C *over* S *such that* card $f^{-1}_{m+n-1}(C) > S^{2n-2}$. *Then there exist distinct* $(m+n-1)$-blocks P *and* P^* *and an* $(n-1)$-block A *such that*

$$f_{m+2(n-1)}(APA) = f_{m+2(n-1)}(AP^*A).$$

Proof. Let $\mathcal{E} = f^{-1}_{m+n-1}\{C\}$. Then $\mathcal{E}$ is a collection of $(m+2n-2)$-blocks and, by hypothesis, card $\mathcal{E} > s^{2n-2}$. It follows from Lemma 5.06 that there exist distinct blocks E and E^* in $\mathcal{E}$ such that $E = ADB$ and $E^* = AD^*B$, where A and B are $(n-1)$-blocks. Then D and D^* are m-blocks and $D \neq D^*$. Since E and E^* are members of $\mathcal{E}$, $f_{m+n-1}(E) = C = f_{m+n-1}(E^*)$.

Let $P = DB$, $P^* = D^*B$. Then P and P^* are distinct $(m+n-1)$-*blocks*. Let $f_{n-1}(BA) = Q$. Then

$$f_{m+2(n-1)}(APA) = f_{m+2(n-1)}ADBA = CQ\text{ , and}$$

$$f_{m+2(n-1)}(AP^*A) = f_{m+2(n-1)}AD^*BA) = CQ.$$

5.08. THEOREM. *Let* n *be in* I_1, *let* f *be in* $F(S,n)$ *and suppose that* f_∞ *is not onto. Then there exists a periodic point* x *in* $X(S)$ *such that the set* $f_\infty^{-1}\{x\}$ *is uncountable.*

Proof. Suppose $n = 1$. Since f_∞ is not onto, f is not a permutation of S, so there exist elements a,b in S with $a \neq b$ such that $f(a) = c = f(b)$. Let x be the bisequence defined by $x_i = c$, all i in I. Then x is periodic and the set $f_\infty^{-1}\{x\}$ includes all bisequences y defined by $y_i = a$ or b, i in I. This set is uncountable.

Now assume that $n \geq 2$. From Lemma 5.05 there exists an $(m+n-1)$-block C such that card $f^{-1}_{m+n-1}\{C\} > s^{2n-2}$. It follows from Lemma 5.07 that there exist distinct $(m+n-1)$-blocks P and P^* and an $(n-1)$-block A such that

$$f_{m+2(n-1)}(APA) = D = f_{m+2(n-1)}(AP^*A).$$

Let Y be the subset of $X(S)$ defined by

$$\ldots\ A\,Q_{-1}\ \overset{\downarrow}{A}\,Q_0\ A\,Q_1\ A\,Q_2\ \ldots$$

where, for i in I, Q_i is either P or P^*. Let x in $X(S)$ be defined by $x = \ldots DDDD \ldots$. Then x is periodic, and if $y \in Y$, then $f_\infty(y) = x$. The set Y is uncountable, and since $Y \subset f_\infty^{-1}\{x\}$, the set $f_\infty^{-1}\{x\}$ is uncountable.

5.09. THEOREM. *Let ϕ be a member of $\Phi(S)$ and suppose that ϕ is not onto. Then there exists a periodic point x of $X(S)$ and an uncountable subset Y of $X(S)$ such that $\phi(Y) = x$.*

Proof. Let ϕ be in $\Phi(S)$. By Theorem 3.08, there exist m in I and n in I_1 such that $\phi = \sigma^m f_\infty$, where $f \in F(S,n)$. Since ϕ is not onto, f_∞ is not onto, hence, according to Theorem 5.08, there exist an uncountable subset Y of $X(S)$ and z in $X(S)$, z periodic, such that $f_\infty(Y) = z$. But then $\phi(Y) = \sigma^m f_\infty(Y) = \sigma^m(z)$. Let $x = \sigma^m(z)$. Then x is periodic.

5.10. THEOREM. $A(S) = \{\phi : \phi \in \Phi(S)$ *and* ϕ *is one-to-one*$\}$.

Proof. Clearly $A(S) \subset \{\phi : \phi \in \Phi(S)$ and ϕ is one-to-one$\}$. Now suppose that ϕ in $\Phi(S)$ is one-to-one, then by Theorem 5.09, ϕ is onto, whence $\phi \in A(S)$.

6. PERIODICITY OF MEMBERS OF $A(S)$.

6.01. DEFINITION. A function θ is *periodic* on $X(S)$, if there exists a positive integer n such that $\theta^n(x) = x$, all x in $X(S)$.

6.02. REMARK. If $f \in F(S,n)$ for n in I_1 and f_∞ is periodic, then $f_\infty \in A(S)$. For, suppose the period of f_∞ is p, p in I_1. Then $f_\infty(x) = f_\infty(y)$ implies that $f_\infty^{p-1}[f_\infty(x)] = f_\infty^{p-1}[f_\infty(y)]$, whence $f_\infty^{p}(x) = f_\infty^{p}(y)$, that is, $x = y$.

6.03. NOTATION. Let m,n be in I_1, and let f be a member of $F(S,m)$ and g an element of $F(S,n)$. Then g_m maps $B_{m+n-1}(S)$ into $B_m(S)$ and f maps $B_m(S)$ into $B_1(S) = S$, so that fg_m is a well defined mapping of $B_{m+n-1}(S)$ into S. The mapping fg_m will also be denoted by fg.

6.04. LEMMA. *Let f be a member of $F(S,m)$, g an element of $F(S,n)$. Then* $(fg)_\infty = f_\infty g_\infty$.

Proof. Let x be a bisequence in $X(S)$ and let $(fg)_\infty(x) = y$. Let i be in I. Then $y_i = fg_m[x_i\, x_{i+1} \ldots x_{i+m+n-2}]$ $= f[g(x_i \ldots x_{i+n-1}) \ldots g(x_{i+n-1} \ldots x_{i+m+n-2})]$. Let $g_\infty(x) = u$; thus $u_i = g(x_i \ldots x_{i+n-1})$. Let $f_\infty(u) = v$. Then $v_i = f(u_i \ldots u_{i+m-1})$ $= f[g(x_i \ldots x_{i+n-1}) \ldots g(x_{i+m-1} \ldots x_{i+m+n-2})]$. Thus for all integers i, $y_i = v_i$. Hence $y = v$ and so $(fg)_\infty(x) = (f_\infty g_\infty)(x)$. Since this is true for all x in $X(S)$, $(fg)_\infty = f_\infty g_\infty$.

6.05. PROPOSITION. *If $f \in F(S,1)$ then f_∞ is periodic if and only if f is a permutation of S.*

Proof. Let $S = \{0, 1, 2, \ldots, s-1\}$ and let f be a permutation of S. Then there is a positive integer p, $p \leqslant s^s$ such that f^p is the identity on S. Then $(f^p)_\infty$ is the identity on $X(S)$. It follows from Lemma 6.04 that $(f^p)_\infty = (f_\infty)^p$. Hence $(f_\infty)^p(x) = x$, for all x in $X(S)$, so f_∞ is periodic.

Now suppose that f_∞ is periodic. Then f_∞ is one-to-one, thus $f_\infty \in A(S)$. By Proposition 5.02, f is a permutation of S.

6.06. DEFINITION. Let n be in I_1. A function f in $F(S,n)$ *depends on* x_i, $1 \leqslant i \leqslant n$, if and only if there exist elements $x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ in S, and x_i, x_i' in S with $x_i \neq x_i'$, such that $f(x_1 x_2 \ldots x_i \ldots x_n) \neq f(x_1 x_2 \ldots x_i' \ldots x_n)$.

6.07. PROPOSITION. *Let* n *be in* I_2 *and* f *be an element of* $F(S,n)$ *with* f_∞ *one-to-one. If* f *does not depend on* $x_2, x_3, \ldots, x_n$, *then* f_∞ *is periodic.*

Proof. Define g in $F(S,1)$ by $g(a) = f(a\, x_2 \ldots x_n)$ for each a in S and any members $x_2, \ldots, x_n$ in S. Then since f does not depend on $x_2, \ldots, x_n$, g is well defined and $g_\infty = f_\infty$. Since $f_\infty \in A(S)$, $g_\infty \in A(S)$, whence, by Proposition 5.02, g is a permutation on S. Thus, by Proposition 6.05, $f_\infty = g_\infty$ is periodic.

6.08. REMARK. The converse of the above Proposition does not hold as example 6.09 shows.

6.09. EXAMPLE. Let $S = \{0, 1, 2\}$ and define f in $F(S,2)$ by

$f(00) = 0$	$f(01) = 2$	$f(02) = 0$
$f(10) = 1$	$f(11) = 1$	$f(12) = 1$
$f(20) = 2$	$f(21) = 0$	$f(22) = 2.$

The following argument shows that f_∞ has period two, that is, $f(f(x_i\ x_{i+1})f(x_{i+1}\ ,\ x_{i+2})) = x_i$, for any $x_i\ ,\ x_{i+1}\ ,\ x_{i+2}$ in S.

Suppose that $x_i = 1$. Then since $f(1a) = 1$, for any a in S , $f[f(1\ ,\ x_{i+1})f(x_{i+1}\ ,\ x_{i+2})] = 1$.

If $x_i = 2$ and $x_{i+1} = 1$ then $f(x_i\ x_{i+1}) = 0$ and $f(x_{i+1}\ ,\ x_{i+2}) = 1$. Since $f(01) = 2 = x_i$, this case is done.

If $x_i = 2$ and $x_{i+1} \neq 1$, then $f[f(x_i\ x_{i+1})f(x_{i+1}\ x_{i+2})]$ is $f(20)$ or $f(22)$ both of which equal 2. Similarly if $x_i=0$, $f[f(x_i\ x_{i+1})f(x_{i+1}\ x_{i+2})] = 0$. This shows that f_∞^2 is the identity on $X(S)$ and so $f_\infty \in A(S)$, but f *depends on* x_2.

6.10 DEFINITION. Let n be in I_2. A function f in $F(S,n)$ is said to be *permutive in* x_1 *, if for every choice of* fixed elements $\bar{x}_2\ ,\ \ldots\ ,\ \bar{x}_n$, and x_1 any element of S , $f(x_1\ \bar{x}_2\ \ldots\ \bar{x}_n) = g(x_1)$ where g is some permutation of S. Hence f is permutive in x_1 if and only if for any given elements $\bar{x}_2\ ,\ \ldots\ ,\ \bar{x}_n$ in S , $f(x_1\ \bar{x}_2\ \ldots\ \bar{x}_n) = f(x_1'\ \bar{x}_2\ \ldots\ \bar{x}_n)$ implies that $x_1 = x_1'$.

6.11 REMARK. Let n be in I_2 and f in $F(S,n)$. Then the following example shows that f_∞ a member of $A(S)$ does not imply that f is permutive in x_1. However, it will be shown in Proposition 6.13 that if f_∞ is periodic, then f is permutive in x_1.

6.12. EXAMPLE. Let n be in I_2. Define f in $F(S,n)$ by $f(a_1 \ldots a_n) = a_n$ for all n-blocks $a_1 \ldots a_n$ over S. Then $f_\infty = \sigma^{-(n+1)} \in A(S)$, but f is not permutative in x_1.

6.13. PROPOSITION. *Let n be in I_2 and suppose that $f \in F(S,n)$ Then if f_∞ is periodic, f is permutive in x_1.*

Proof. *Assume that f_ω is periodic on $X(S)$* but that f is not permutive in x_1. Then there exist n-blocks $A = x_1 \tilde{x}_2 \ldots \tilde{x}_n$ and $A' = x'_1 \tilde{x}_2 \ldots \tilde{x}_n$, with $x_1 \neq x'_1$ such that $f(A) = f(A')$. Let x be the member of $X(S)$ defined by $x_i = 0$ if $i \leq 0$ or $i > n$, and $x_1 \ldots x_n = A$ and let y in $X(S)$ be defined by $y_i = 0$ if $i \leq 0$ or $i > n$ and $y_1 \ldots y_n = A'$. Now there is some integer $p \geq 1$ such that $(f_\infty)^p$ is the identity on $X(S)$. Hence $(f_\infty)^p(x) = x$ and $(f_\infty)^p(y) = y$. Since for any integer $i \geq 1$, $[f_\infty(x)]_i = [f_\infty(y)]_i$, it follows that

$$x_1 = [f_\infty{}^p(x)]_1 = [f_\infty{}^p(y)]_1 = x'_1.$$

This contradiction completes the proof.

6.14. *REMARK. The converse of Proposition 6.13* is not true in general. For suppose $S = \{0, 1, 2\}$ and consider f defined by

$f(00) = 1$	$f(01) = 0$	$f(02) = 0$
$f(10) = 0$	$f(11) = 1$	$f(12) = 1$
$f(20) = 2$	$f(21) = 2$	$f(22) = 2.$

Then f is permutive in x_1, but if x in $X(S)$ is defined by $x_i = 0$, all i in I, then for all positive integers p, $f_\infty^p(x) = y$, where $y_i = 1$, all i in I.

If the cardinal of S is two, however, then Theorem 6.16 due to Hedlund, [3], shows that f_∞ is periodic if and only if f is permutive in x_1.

6.15. NOTATION. Let $S = \{0, 1\}$. Let $\bar{a} = 0$, if $a = 1$ and $\bar{a} = 1$, if $a = 0$.

6.16. THEOREM. *Let* $S = \{0, 1\}$ *and* n *be in* I_2. *Let* f *be a member of* $F(S,n)$ *such that* f *is permutive in* x_1 *and* $f_\infty \in A(S)$. *Then there exists* g *in* $F(S,1)$ *such that* $f_\infty = g_\infty$.

Proof. Suppose there does not exist g in $F(S,1)$ such that $f_\infty = g_\infty$. Let k be the least integer such that $f_\infty \in F_\infty(S,k)$. Then $k > 1$ and there exists g in $F(S,k)$ such that $f_\infty = g_\infty$. Since f_∞ is one-to-one so is g_∞. There must exist a k-block $a_1 \ldots a_{k-1}a_k$ such that $g(a_1 \ldots a_{k-1}\, a_k) \neq g(a_1 \ldots a_{k-1}\, \bar{a}_k)$. For if not, define $h : B_{k-1}(S) \to S$ by $h(x_1 \ldots x_{k-1}) = g(a_1 \ldots a_{k-1}a_k)$. Then h is a well defined member of $F(S,k-1)$ and $h_\infty = g_\infty = f_\infty$, contradicting the minimality of k. Hence g depends on x_k. Since f is permutive in x_1, so is g and thus $g(0\, a_2 \ldots a_k) = g(1\, a_2 \ldots a_{k-1}\, \bar{a}_k)$. Let $A = a_2 \ldots a_{k-1}\, a_k$, $B = a_2 \ldots a_{k-1}\, \bar{a}_k$. Then $g(0A) = g(1B)$.

Let P be the set of all integers $p \geq k$ with the property that there exist p-blocks $Ap = 0a_2 \ldots ap$ and $Bp = 1b_2 \ldots bp$ such that $g_{p-k+1}(Ap) = g_{p-k+1}(Bp)$. Then $k \in P$. The following argument shows that $P = \{m \mid m \in I, m \geq k\}$. If $p > q > k$ and

$p \in P$, then $q \in P$. Thus it is sufficient to show that P is not bounded.

Suppose that P is bounded and that m is the least upper bound of P. Then there are m-blocks $Am = 0\, c_2 \ldots cm$, $Bm = 1\, d_2 \ldots dm$ such that $g_{m-k+1}(Am) = g_{m-k+1}(Bm)$. Now since m is maximal,

$$g_{m-k+2}(0\ Am) \neq g_{m-k+2}(1\ Bm) \quad , \quad \text{and} .$$

$$g_{m-k+2}(1\ Am) \neq g_{m-k+2}(0\ Bm) .$$

Hence, as g is permutive in x_1 , $g_{m-k+2}(0\ Am) = g_{m-k+2}(0\ Bm)$ and $g_{m-k+2}(1\ Am) = g_{m-k+2}(1\ Bm)$.

Thus $g_{m-k+2}(e\ Am) = g_{m-k+2}(e\ Bm)$, $e = 0$ or 1. This process can be continued to obtain

$$g_m(D\ Am) = g_m(D\ Bm) \quad , \quad \text{all } (k-1)\text{-blocks } D.$$

But then $g(D0) = g(D1)$ for all D in $\mathcal{B}_{k-1}(S)$, which contradicts the fact that g depends on x_k. Thus $P = \{m : m \in I \ , m \geq k\}$.

Let p be in P. There exist $(p-1)$-blocks $A^{(p)} = y_1^{(p)} \ldots y_{p-1}^{(p)}$ and $B^{(p)} = z_1^{(p)} \ldots z_{p-1}^{(p)}$ over S such that $g_{p-k+1}(0\ A^{(p)}) = g_{p-k+1}(1\ B^{(p)})$. Define $y^{(p)}$ in $X(S)$ by

$$y_i^{(p)} = 0 \quad \text{if} \quad i \leq 0 \quad \text{or} \quad i \geq p$$

$$y_1^{(p)} \ldots y_{p-1}^{(p)} = A^{(p)} .$$

Define

$$z_0^{(p)} = 1 \ ,$$

$$z_i^{(p)} = 0 \quad \text{if} \quad i \geq p$$

$$\text{and} \quad z_1^{(p)} \ldots z_{p-1}^{(p)} = B^{(p)} .$$

Since g is permutive in x_1, for each $i \leqslant -1$ there exists $z_i^{(p)}$ in S such that $g(z_i^{(p)} \ldots z_{i+k-1}^{(p)}) = g(y_i^{(p)} \ldots y_{i+k-1}^{(p)})$ $(i \leqslant -1)$. This defines $z^{(p)}$ in $X(S)$.

Let $g_\infty(y^{(p)}) = u^{(p)}$, $g_\infty(z^{(p)}) = v^{(p)}$. Then $u_i^{(p)} = v_i^{(p)} (i \leqslant p - k)$. This implies that $d(u^{(p)}, v^{(p)}) \leqslant (p - k + 2)^{-1}$. Thus $\lim\limits_{p\to\infty} d(u^{(p)} , v^{(p)}) = 0$.

Since $X(S)$ is a compact metric space, any infinite sequence of points contains a convergent subsequence, so assume that $\lim\limits_{p\to\infty} y^{(p)} = y$, $\lim\limits_{p\to\infty} z^{(p)} = z$, $\lim\limits_{p\to\infty} u^{(p)} = u$, $\lim\limits_{p\to\infty} v^{(p)} = v$. Since $\lim\limits_{p\to\infty} d(u^{(p)},v^{(p)}) = 0$, it follows that $u = v$. Since $y_0^{(p)} = 0$, $y_0 = 0$, and since $z_0^{(p)} = 1$, $z_0 = 1$. Thus $y \neq z$. Now $g_\infty(y) = g_\infty(\lim\limits_{p\to\infty} y^{(p)}) = \lim\limits_{p\to\infty} g_\infty(y^{(p)}) = \lim\limits_{p\to\infty} u^{(p)} = u$ and $g_\infty(z) = g_\infty(\lim\limits_{p\to\infty} z^{(p)}) = \lim\limits_{p\to\infty} g_\infty(z^{(p)}) = \lim\limits_{p\to\infty} v^{(p)} = v = u$, so that $g_\infty(y) = g_\infty(z)$. This contradicts the hypothesis that f_∞ , and hence g_∞ , is one-to-one.

The proof of the theorem is completed.

6.17. COROLLARY. *Let* $S = \{0 , 1\}$ *and* n *be in* I_2. *Then if* $f \in F(S,n)$ *and* $f_\infty \in A(S)$, f_∞ *is periodic, if and only if* f *is permutive in* x_1.

Proof. If f_∞ is periodic, then the result follows from Proposition 6.13. Suppose f is permutive in x_1 and $f_\infty \in A(S)$. Then by Theorem 6.16 there exists g in $F(S,1)$ such that $g_\infty = f_\infty$. Since $f_\infty \in A(S)$, $g_\infty \in A(S)$, whence by Proposition 5.02 g is a permutation of S. It follows from Proposition 6.05 that $f_\infty = g_\infty$ is periodic.

6.18. NOTATION. Denote the set of all powers of the shift by $P(\sigma)$. That is, $P(\sigma) = \{\sigma^n : n \in I\}$. Clearly $P(\sigma) \subset A(S)$.

6.19. REMARK. The following example due to Hedlund, [3], shows that $A(S)$ contains two elements α and β, each of period two, such that the product of these elements, ϕ, is not a member of $P(\sigma)$, yet has infinite order.

6.20. EXAMPLE. Let S be any symbol set and define f in $F(S,4)$ by $f(x_i\, x_{i+1}\, x_{i+2}\, x_{i+3}) = x_{i+1}$ for all 4-blocks except 1001 and 1101. Let $f(1001) = 1$ and $f(1101) = 0$.

Define $\alpha : X(S) \to X(S)$ by $[\alpha(x)]_i = x_i$ unless $x_i = 0$ or 1, if $x_i = 0$ or 1, let $[\alpha(x)]_i = \bar{x}_i$. Clearly $\alpha \in A(S)$ and α has period two. Let $\beta = \sigma^{-1} f_\infty$. Then it can be seen that $\beta \in A(S)$ and β^2 is the identity on $X(S)$.

Now let $\phi = \alpha\beta$. Then, as $A(S)$ is a group, $\phi \in A(S)$. Let z be the member of $X(S)$ having $z_i = 0$, all i in I. Then, clearly, for all integers p, $\phi^{2p}(z) = z$, and $\phi^{2p+1}(z) = y$, where $y_i = 1$, all i in I. From this it can be deduced that $\phi \notin P(\sigma)$, and, if there is some positive integer n such that $\phi^n(x) = x$, for all x in $X(S)$, then n is even and $n \geqslant 2$. Hence $n = 2p$, for some p in I_1.

Now let x in $X(S)$ be defined by

$$x_i = 0 \;,\quad i \geqslant 0 \;,$$

$$x_{-7}x_{-6} \ldots x_{-1} = 1001001 ,$$

$$\text{and} \quad x_{-2i-1}x_{-2i} = 10 , \ i \geq 4.$$

That is, x is the bisequence

$$L\ 1001001\ \overset{\downarrow}{R}$$

where L is the left infinite sequence ... 1010 ,

R is the right infinite sequence ... 00 ... ,

and x is indexed at the first element of R. It will be shown by induc ion that $\phi^{2p}(x) = L\ 1001001\ (01)^p\ \overset{\downarrow}{R}$, for all p in I_1.

Now x is $L\ 1001001\ \overset{\downarrow}{R}$

Thus $\beta(x)$ is $L\ 1101101\ \overset{\downarrow}{R}$

and $\phi(x)$ is $L\ 10010010\ \overset{\downarrow}{\bar{R}}$

where $\bar{R}$ is the right infinite sequence 111 ... .

Then $\beta\phi(x) = L\ 11011010\ \overset{\downarrow}{\bar{R}}$,

whence $\phi^2(x) = L\ 100100101\ \overset{\downarrow}{R}$,

that is, $\phi^2(x)$ is $L\ 1001001(01)\ \overset{\downarrow}{R}$.

Assume that $\phi^{2p}(x) = L\ 1001001(01)^p\ \overset{\downarrow}{R}$.

Then $\phi^{2p+1}(x)$ is $L\ 1001001\ 0(10)^p\ \overset{\downarrow}{\bar{R}}$ and so

$\phi^{2(p+1)}(x)$ is $L\ 1001001\ 01(01)^p\ \overset{\downarrow}{R}$.

We have $\phi^{2(p+1)}(x) = L\ 1001001(01)^{p+1}\ \overset{\downarrow}{R}$ which completes the inductive argument.

Since the block 100101 does not appear in x but appears in $\phi^{2p}(x)$, all p in I_1 it follows that ϕ is not periodic.

7. SOME FURTHER PROPERTIES OF AUTOMORPHISMS ON $X(S)$.

7.01. REMARK. It is clear that $A(S)$ is a group. It has been shown by Curtis, Hedlund and Lyndon [3] that every finite group is isomorphic to some subgroup of $A(S)$.

7.02. NOTATION. Let n be an element of I_1 and let $B = b_1 b_2 \ldots b_n$ be an n-block over S. Let m be in I_1, $m \leq n$. The initial m-block of B is the block $b_1 \ldots b_m$. The terminal m-block of B is the block $b_{n-m+1} \ldots b_n$.

7.03. DEFINITION. Let m,n be in I_1. Let B be an m-block over S and let C be an n-block over S. Then B and C *overlap* provided there exists k in I_1 such that either the terminal k-block of B coincides with the initial k-block of C or the initial k-block of B coincides with the terminal k-block of C.

Let n be in I_1 and A be an n-block over S. Then A^m is the (mn)-block $A_1 A_2 \ldots A_m$, where $A_i = A$ $(i = 1, 2, \ldots, m)$.

7.04. LEMMA. Let n be in I_1, $A = 1^{n+1}$ and let $B = (10)^m$ where $m = n/2$ if n is even and $m = (n+1)/2$ if n is odd. Let

$$\mathcal{C} = A \circ \mathcal{B}_n(S) \circ B.$$

Then no two members of $\mathcal{C}$ overlap.

Proof. Let C,D be unequal elements of $\mathcal{C}$, say

$$C = A \circ c_1 \ldots c_n \circ B,$$

$$D = A \circ d_1 \ldots d_n \circ B.$$

Suppose there exists k in I_1 such that the terminal k-block of C coincides with the initial k-block of D. Since $C \neq D$, and $C, D \in B_{2n+2m+3}$, it follows that $1 \leqslant k < 2n + 2m + 3$.

Suppose $k \geqslant n + 1$. Then the initial k-block of D contains 1^{n+1} as a sub-block. But no terminal k-block of C contains 1^{n+1} as a sub-block for $k < 2n + 2m + 3$. Thus $1 \leqslant k \leqslant n$. Since the initial 1-block of D is 1 and the terminal 1-block of C is O, $k \neq 1$, whence $2 \leqslant k \leqslant n$.

If $2 \leqslant k \leqslant n$, the initial k-block of D contains 11 as a sub-block. Since the length of $OB \geqslant n$, the terminal k-block of C is a sub-block of OB. But 11 is not a sub-block of OB.

Hence there cannot exist k in I_1 such that the terminal k-block of C coincides with the initial k-block of D. The proof is completed by interchanging the roles of C and D.

7.05. THEOREM. *Every finite group is isomorphic to some subgroup of the group* $X(S)$ *of automorphisms of* $\langle X(S), \sigma \rangle$.

Proof. For n in I_1, let $H(S,n)$ be the symmetric group on $B_n(S)$. If G is an arbitrary finite group, then G can be represented isomorphically as a subgroup of some symmetric group. Hence there exists an integer $n \geqslant 2$ such that G is isomorphic to a subgroup of $H(S,n)$. It is thus sufficient to prove that $A(S)$ contains a subgroup isomorphic to $H(S,n)$, n in I_2.

Let n be an element of I_2. Corresponding to each π in $H(S,n)$ define a map $\gamma_\pi : X(S) \to X(S)$ as follows. Let $\mathcal{C}$ be as in the above lemma and let x be a member of $X(S)$. If $C = A\,O\,c_1 \ldots c_n\,O\,B$ is a member of $\mathcal{C}$ which appears in x, then γ_π changes C into the block $A \; O \; \pi(c_1 \; \ldots \; c_n) \; O \; B$, while any other block in x not overlapping a member of C is left unchanged. Since no two members of C overlap, γ_π is well defined, and it is clear that γ_π is uniquely defined by π.

Since any member of $\Pi(S,n)$ has period $(S^n)!$, the map γ_π is periodic of period $(S^n)!$ and so is one-to-one. To show that $\gamma_\pi \in \rangle(S)$, it is sufficient to show that γ_π is continuous and commutes with the shift.

Let $\varepsilon > 0$ and choose m in I_+ such that $(1+m)^{-1} < \varepsilon$. Let j be the length of each member of C and let $\delta = (m+j)^{-1}$. Suppose that x and z are elements in $X(S)$ with $d(x,z) < \delta$. Then $x_i = z_i$ if $|i| < m + j$. Let $\gamma_\pi(x) = y$, $\gamma_\pi(z) = u$. For each integer i, y_i is uniquely determined by the block $x_{i-(j-1)} \ldots x_{i+(j-1)}$ while u_i is uniquely determined by $z_{i-(j-1)} \ldots z_{i+(j-1)}$. Thus $y_i = u_i$ if $|i| \leqslant m$, whence $d(\gamma_\pi(x), \gamma_\pi(z)) = d(u,v) \leqslant (1+m)^{-1} < \varepsilon$. Thus γ_π is continuous.

The following argument shows that γ_π commutes with σ. Let x be in $X(S)$, $\gamma_\pi(x) = y$ and $\sigma(x) = u$. Then $[\sigma\, \gamma_\pi(x)]_i = y_{i+1}$, and $u_i = x_{i+1}$, i in I. Let $\gamma_\pi(u) = v$. It must be shown that for i any integer, $y_{i+1} = v_i$, or, equivalently, $y_i = v_{i-1}$. *Suppose there exists an integer* k such that $k \leqslant i \leqslant k + j - 1$ and $x_k \ldots x_{k+j-1} \in C$, where j is the length of an element of C. Then $x_k \ldots x_{k+j-1} = A \; O \; c_1 \ldots c_n \; OB$, say, and this equals $u_{k-1} \ldots u_{k+j-2}$. But then $v_{k-1} \ldots v_{k+j-2} = A \; O \; d_1 \ldots d_n \; O \; B = y_k \ldots y_{k+j-1}$, where $d_1 \ldots d_n = \pi(c_1 \ldots c_n)$. Since $k - 1 \leqslant i - 1 \leqslant k + j - 2$, it follows that $v_{i-1} = y_i$.

If there does not exist an integer k such that $k \leq i \leq k+j-1$ and $x_k \ldots x_{k+j-1} \in C$, then $y_i = x_i$. But $x_k \ldots x_{k+j-1} = u_{k-1} \ldots u_{k+j-2}$, so that there does not exist an integer p such that $p \leq i-1 < p+j-1$ and $u_p \ldots u_{p+j-1} \in C$. This implies that $v_{i-1} = u_{i-1} = x_i = y_i$. Thus $\sigma\gamma_\pi = \gamma_\pi\sigma$. It follows that $\gamma_\pi \in A(S)$.

If α, β are elements of $H(S,n)$, then $\gamma_\beta\gamma_\alpha = \gamma_{\beta\alpha}$. For if $A\,0\,a_1 \ldots a_n\,0\,B$ is a block of C appearing in x, x in $X(S)$, then the block $A\,0\,b_1 \ldots b_n\,0\,B$, where $b_1 \ldots b_n = \alpha(a_1 \ldots a_n)$ will appear in the same position in $y = \gamma_\alpha(x)$ as the block $A\,0\,a_1 \ldots a_n\,0\,B$ is in x. Similarly, γ_β transforms the block $A\,0\,b_1 \ldots b_n\,0\,B$ in y into the block $A\,0\,c_1 \ldots c_n\,0\,B$, where $c_1 \ldots c_n = \beta(b_1 \ldots b_n)$, in the same position in $z = \gamma_\beta(y)$.

Now $\gamma_{\beta\alpha}$ transforms $A\,0\,a_1 \ldots a_n\,0\,B$ appearing in x into the block $A\,0\,(\beta\alpha)(a_1 \ldots a_n)\,0\,B = A\,0\,\beta(b_1 \ldots b_n)\,0\,B$ $= A\,0\,c_1 \ldots c_n\,0\,B$ in $\gamma_{\beta\alpha}(x)$ and the transformation does not change the position of the block.

If $i \in I$ and there is no $k \in I$ such that $k \leq i \leq k+j-1$ and $x_k \ldots x_{k+j-1} \in C$, then $y_i = x_i$, $z_i = y_i$, and $u_i = x_i$, so that $z_i = u_i$. Thus $\gamma_{\beta\alpha} = \gamma_\beta\gamma_\alpha$.

It has been shown that the mapping $\Lambda : H(S,n) \to A(S)$ defined by $\Lambda_\pi = \gamma_\pi$ is an isomorphism of $H(S,n)$ into $A(S)$. Hence the set $\Lambda(H(S,n))$ is a subgroup of $A(S)$ isomorphic to $H(S,n)$. This completes the proof of the theorem.

7.06. COROLLARY. *The set* $A(S) - P(\sigma)$ *is infinite.*

Proof. It follows from Theorem 7.05 that given any k in I_1, there exists an element of $A(S)$ of order k. Since σ^k is not the identity for any k in I_1, the element is not a power of the shift.

7.07. COROLLARY. *Every finite group is isomorphic to some subgroup of* $A(S)/P(\sigma)$.

Proof. Since the elements of $A(S)$ commute with σ, $P(S)$ is a normal subgroup of $A(S)$ and the quotient group $A(S)/P(\sigma)$ is well defined. It has been shown that $H(S,n)$ is isomorphic to the subgroup $G = \Lambda(H(S,n))$ of $A(S)$. Let $G' = G/P(\sigma)$. Then since $G \cap P(\sigma) = \{I\}$ where I is the identity element of $X(S)$, G' is isomorphic to G and so to $H(S,n)$.

It follows that every finite subgroup is isomorphic to some subgroup of $A(S)/P(\sigma)$.

7.08. REMARK. Since $A(S)$ is a subgroup of the group of all automorphisms on $X(S)$, it follows from Theorem 7.05 that the group of automorphisms on $X(S)$ contains elements of every finite order.

If θ is a map from $X(S)$ onto $X(S)$ such that some power *of* θ *is a member of* $P(\sigma)$ *, then* θ *has infinite order.* Such maps are *roots of powers of the shift.* In the following theorem we describe some of the properties of continuous roots of powers of the shift.

7.09. THEOREM. *If* θ *is a continuous map from* $X(S)$ *onto* $X(S)$ *such that* $\theta^p = \sigma^k$ *for some positive integers* p *and* k*, then*

(1) θ *is an automorphism of* $X(S)$,

(2) θ *is expansive,*

(3) θ *is point transitive,*

(4) θ *is strongly mixing,*

(5) θ *is not periodic.*

Proof. (1) It is sufficient to show that θ is one-to-one. Suppose that $\theta(x) = \theta(y)$, for x,y in $X(S)$. Then $\sigma^{p-1}(\theta(x)) = \theta^{p-1}(\theta(y))$, whence $\theta^p(x) = \theta^p(y)$ and so $\sigma^k(x) = \sigma^k(y)$. Since the shift is one-to-one , $x = y$.

(2) It has been shown in Section two that σ^k is expansive, for any integer k. Hence there exists $\delta \geqslant 0$ such that if $x \neq y$, there exists an integer n such that $d(\sigma^{kn}(x) , \sigma^{kn}(y)) \geqslant \delta$. Hence $d(\theta^{pn}(x) , \theta^{pn}(y)) \geqslant \delta$ so θ is expansive.

(3) Since σ^k is point transitive, any k in I_1 , there is some x in $X(S)$ such that $\{(\sigma^k)^n(x) : n \in I\}$ is dense in $X(S)$. Hence $\{\theta^{pn}(x) : n \in I\}$ is dense in $X(S)$, so clearly θ is point transitive.

(4) Let U and V be any two non-empty open sets in $X(S)$. Since θ is a homeomorphism, if j is an integer, $0 \leqslant j < p$, $\theta^{-j}(U)$ is open and non-empty. Now as σ^k is strongly mixing, there exists N_j such that

$$\theta^{-j}(U) \cap \sigma^{ki}(V) \neq \phi \text{ , for all } i \text{ with } |i| > N_j .$$

Thus $\theta^{-j}(U) \cap \theta^{pi}(V) \neq \phi$, for all i with $|i| > N_j$

and so $U \cap \theta^{pi+j}(V) \neq \phi$, if $|i| > N_j$.

Thus for $|i| > \max\limits_{0 \leqslant j < p} N_j$, $U \cap \theta^{pi+j}(V) \neq \phi$ for any j.

This is sufficient to prove that θ is strongly mixing and it follows that θ *is also ergodic.*

(5) Suppose that θ is periodic. Then there is a positive integer n such that $\theta^n = I$, where I is the identity on $X(S)$. Hence $(\theta^n)^p = \sigma^{kn} = I$. But σ is not periodic. This contradiction concludes the proof.

7.10. EXAMPLE. If θ is any member of $A(S)$ which is periodic, then for n in I_1, $\sigma^n\theta$ satisfies the five properties of Theorem 7.09. *For, if θ has period p,* $p \geq 1$, then as $\theta \in A(S)$ and so commutes with the shift,
$(\sigma^n\theta)^p = \sigma^{np}\theta^p = \sigma^{np}$.

7.11. EXAMPLE. We construct a class of functions in $F_\infty(S)$ such that each function, h_∞, is a member of $A(S) \setminus P(\sigma)$ and $h_\infty^p = \sigma^p$, for $p \geq 2$.

Let p be in I_2 and S be a symbol set such that the cardinal of S is at least p, say
$S = \{0, 1, \ldots, p-1, \ldots, s-1\}$. Define $B \subset S$ to be $\{0, 1, \ldots, p-1\}$ and let π be the cyclic permutation on B. *For any n in* I_4, *define* h in $F(S,n)$ as follows. If $x_i\, x_{i+1} \ldots x_{i+n-1}$ is any n-block, let $h(x_i x_{i+1} \ldots x_{i+n-1}) = x_{i+1}$, except in the following p cases. Let A be the set of p *distinct n-blocks* $A_i = a_1\, i\, a_3 a_4 \ldots a_n$, such that $a_1 = a_n = 1$, $a_3 = a_4 = \ldots = a_{n-1} = 0$ and i is a member of B, and let $h(A_i) = \pi^{i+1}(i)$, each i in B.

Hence $h(100 \ \ldots\ 01) = \pi(0) = 1$,

$h(110 \ \ldots\ 01) = \pi^2(0) = 2$,

$\vdots$

$h(1\ p{-}1\ 0 \ldots 01) = \pi^p(0) = 0$.

Since no two members of Λ overlap, h is a well defined member of $F(S,n)$.

Now let x be any member of $X(S)$. If a block B appearing in x is not a member of Λ, then h_∞ acts on the block in the same way as σ does, whence $\sigma^{-1}h_\infty$ leaves B unchanged. It follows that $(\sigma^{-1}h_\infty)^p$ acts as the identity on B. If B is a member of Λ, that is, $B = A_i$ some i, $0 \leq i \leq p-1$, then the map $\sigma^{-1}h_\infty$ changes A_i to A_{i+1} if $0 \leq i < p-1$ and $\sigma^{-1}h_\infty$ changes A_{p-1} to A_0. Thus $(\sigma^{-1}h_\infty)^p$ also leaves any member of Λ unchanged. It follows that $\sigma^{-p}h_\infty^p = (\sigma^{-1}h_\infty)^p$ acts as the identity on x. Thus $h_\infty^p = \sigma^p$. Thus h_∞ is one-to-one and so is a member of $A(S)$.

To show that $h_\infty \notin P(\sigma)$, let x be the element of $X(S)$ defined by $x = L\,A_0\,R$ where R is the right infinite sequence $00\ldots$ and L is the left infinite sequence $\ldots 00$ and x is indexed at the first element of A_0.

That is, x is $\quad \ldots 0100\ldots 010 \ldots$.

Then $h_\infty(x)$ is $\quad L\,A_1\,R = \ldots 0110 \ldots 010 \ldots$,

and clearly $h_\infty(x) \neq \sigma^p(x)$ for any integer p. Since $h_\infty^p = \sigma^p$, h_∞ has the five properties of Theorem 7.09.

7.12. REMARKS. (i) If j is an integer such that $1 \leq j < n-1$, where $n \in I_5$, then a member h of $F(S,n)$ may be obtained with $(h_\infty)^p = \sigma^{jp}$, by defining $h(x_i x_{i+1} \ldots x_{i+n-1}) = x_{i+j}$ for all n-blocks $x_i x_{i+1} \ldots x_{i+n-1}$ except the n-blocks $A_i = a_1 a_2 \ldots a_j\ i\ a_{j+2} \ldots a_n$ where $a_1 = a_n = 1$, $a_2 = a_3 = \ldots = a_j = a_{j+2} = \ldots = a_{n-1} = 0$ and i is in B.

Define $h(A_i) = \pi^{i+1}(i)$, each i in $\mathcal{B}$.

(ii) It is not known whether all roots of powers of the shift which are members of $F_\infty(S)$ have this form. However, in the case where the cardinal of S is a prime, C.R. Welch [3] has proved the following theorem, which is stated below without proof.

7.13. THEOREM. *Let s = card S be a prime. Let n be in I_1, let f be a member of $F(S,n)$ and let there exist q in I_1, p in I, such that $f_\infty^q = \sigma^p$ then q divides p.*

7.14. EXAMPLE. If ϕ is the member of $A(S)$ constructed in Example 6.20 , then there do not exist *non-zero integers* p and k such that $\phi^p = \sigma^k$.

It is sufficient to show that ϕ is not expansive. Suppose ϕ is expansive. *Then there exists* $\delta \geq 0$, such that if x and y are members of $X(S)$ and $x \neq y$, then there is some integer i such that $d(\phi^i(x) , \phi^i(y)) \geq \delta$. Choose k in I_1 with $\frac{1}{k+1} < \delta$. Let x in $X(S)$ be defined by $x_k x_{k+1} x_{k+2} x_{k+3} = 1001$ and $x_i = 1$ elsewhere. Then x may be represented as

$\overset{L}{1}\overset{X}{1}001\overset{R}{1}$ where $\overset{L}{1}$ denotes the left infinite sequence ... 11 , $\overset{R}{1}$ *is the right infinite sequence* 11 ... and "X" indicates the position of x_k.

$$\text{Now } \phi(x) = \overset{L}{0}\overset{X}{0}010\overset{R}{0} ,$$
$$\text{and } \phi^2(x) = \overset{L}{1}\overset{X}{1}101\overset{R}{1} ,$$
$$\phi^3(x) = \overset{L}{0}\overset{X}{0}110\overset{R}{0} ,$$
$$\text{and } \phi^4(x) = \overset{L}{1}\overset{X}{1}001\overset{R}{1} = x.$$

Now let y be the bisequence defined by $y_i = 1$, all i in I. Clearly $y \neq x$, and for any integer n, $\phi^{2n}(y) = y$, while $\phi^{2n+1}(y) = \bar{y}$, where $[\bar{y}]_i = 0$, all i in I.

$$\text{Then} \quad d(x,y) = \frac{1}{k+2} \, ,$$

$$d(\phi(x)\phi(y) = \frac{1}{k+3} \, ,$$

$$d(\phi^2(x) \, , \, \phi^2(y)) = \frac{1}{k+3} \, ,$$

$$\text{and} \quad d(\phi^3(x) \, , \, \phi^3(y)) = \frac{1}{k+2} \, .$$

Hence for all integers i, $d(\phi^i(x) \, , \, \phi^i(y)) < \frac{1}{k+1} < \delta$. This contradiction proves that ϕ is not expansive, and *so for all non-zero integers* p, $\phi^p \in A(S) \setminus P(\sigma)$.

The following example show that the map θ of Theorem 7.09 need not commute with the shift.

7.15. EXAMPLE. Let $S = \{0,1\}$. Let $\bar{0} = 1$ and $\bar{1} = 0$. Define $\theta : X(S) \to X(S)$ as follows:

$$[\theta(x)]_{2i} = x_{2i+1} \, ,$$

$$[\theta(x)]_{2i+1} = \overline{x_{2i+2}} \, , \text{ all } i \text{ in } I.$$

Hence if x *is the bisequence*

$$\cdots x_{-3}x_{-2}x_{-1}\overset{\downarrow}{x_0}x_1x_2x_3 \cdots$$

then $\theta(x)$ is

$$\cdots \bar{x}_{-2}x_{-1}\overset{\downarrow}{\bar{x}_0}x_1\bar{x}_2x_3\bar{x}_4 \cdots .$$

It is clear that θ is a well defined map from $X(S)$ onto $X(S)$. The following argument shows that θ is continuous. Let $\varepsilon > 0$. Choose k in I_1 such that $\frac{1}{k+1} < \varepsilon$. Let $\delta = \frac{1}{2k+1}$.

$$
\begin{aligned}
\text{Now } d(x,y) < \delta &\Rightarrow x_i = y_i \quad , \quad (-2k \leq i \leq 2k) \; , \\
&\Rightarrow \begin{cases} x_{2i} = y_{2i} \quad , \quad (-k \leq i \leq k) \text{ and} \\ x_{2i+2} = y_{2i+2} \quad , \quad (-k < i < k) \quad , \end{cases} \\
&\Rightarrow [\theta(x)]_i = [\theta(y)]_i \quad , \quad (-k < i < k) \quad , \\
&\Rightarrow d(\theta(x) \; , \theta(y)) \leq \frac{1}{k+1} < \varepsilon \; .
\end{aligned}
$$

Also, if $x \in X(S)$, $\sigma\theta(x)$ is

$$\ldots x_{-1}\bar{x}_0 x_1 \overset{\downarrow}{\bar{x}_2} x_3 \bar{x}_4 x_5 \ldots \quad ,$$

while $\theta\sigma(x)$ is

$$\ldots \bar{x}_{-1} x_0 \bar{x}_1 \overset{\downarrow}{x_2} \bar{x}_3 x_1 \bar{x}_5 \quad , \qquad \text{and it can be}$$

seen that $\theta\sigma \neq \sigma\theta$. Hence $\theta \notin \Phi(S)$. Now if $x \in X(S)$, $[\sigma^4(x)]_i = x_{i+4}$, all i in I , and it may easily be verified that

$$[\theta^4(x)]_{2i} = x_{2i+4} \quad , \quad [\theta^4(x)]_{2i+1} = x_{(2i+1)+4} \; .$$

7.16. REMARK. The preceding example shows that there exist continuous, onto transformations of $X(S)$ which behave like the shift with respect to the properties of expansiveness, transitivity, mixing and periodicity, but do note commute with every member of $A(S)$. It has, however, been proved by J.P. Ryan , [5] that any continuous, onto transformation of $X(S)$ which commutes with elements of $A(S)$ is a power of the shift.

7.17. NOTATION. Let n be in I_1. Let $\mathcal{C} = A\ 0\ B_n(S)\ 0\ B$ where $A = 1^{n+1}$ and $B = (10)^m$ where $m = n/2$ if n is even and $m = (n+1)/2$ if n is odd, as in Lemma 7.04. If $C = A\ 0\ c_1 \ldots c_n\ 0\ B$ is a member of $\mathcal{C}$ the block $c_1 \ldots c_n$ will be called the *central block* of C. Let $H(S,n)$ be the symmetric group on $B_n(S)$. For each π in $H(S,n)$ define γ_π as in Theorem 7.05. Then $\gamma_\pi \in A(S)$. Let $\Gamma(n) = \{\gamma_\pi : \pi \in H(S,n)\}$.

7.18. THEOREM. *Let f be in $F(S,n)$ such that f_∞ is onto. Then if f_∞ commutes with all elements of $\Gamma(n)$, f_∞ is a power of the shift.*

Proof. Let $I = \{0, 1, \ldots, s-1\}$. If $s = 2$, then the only elements of $F(S,1)$ such that f_∞ is onto are the identity map and the map g_∞ where $[g_\infty(x)]_i = \overline{x_i}$. The identity map is σ^0, and it may easily be verified that g_∞ does not commute with γ_π if π is the permutation on S defined by $\pi(0) = 1$, $\pi(1) = 0$. Hence, it may be assumed that $n \in I_2$, or $s > 2$, or both.

Let $c_1 c_2 \ldots c_n$ be a fixed n-block and let $C = A\ 0\ c_1 \ldots c_n\ 0\ B$. Let x be a member of $X(S)$ such that C appears in x with $x_0\ x_1 \ldots x_{n-1}$ equal to the central block of C. That is, x is the bisequence

$$\ldots A\ 0\ \overset{\downarrow}{c_1} \ldots c_n\ 0\ B \ldots .$$

Suppose there is no member of $\mathcal{C}$ which appears in $f_\infty(x)$ and has $[f_\infty(x)]_0$ as a member of its central block. Then for every π in $H(S,n)$, $[f_\infty \gamma_\pi(x)]_0 = [\gamma_\pi f_\infty(x)]_0 = [f_\infty(x)]_0$. But then for any π ; $f(\pi(c_1 \ldots c_n) = [f_\infty \gamma_\pi(x)]_0 = [f_\infty(x)]_0 = f(c_1 \ldots c_n)$, which is impossible since f_∞ is onto. Thus there is some member of C which appears in $f_\infty(x)$ and has $[f_\infty(x)]_0$ as a member of its central block , that is , $f_\infty(x)$ is

$$\ldots A\ 0\ d_1 d_2 \ldots \overset{\downarrow}{d_j} \ldots d_n\ 0\ B \ldots$$

where $d_1 \ldots d_n$ is some member of $B_n(S)$ and $1 \leq j \leq n$. Then if $\pi(d_1 \ldots d_n) = e_1 e_2 \ldots e_n$, since f_∞ and γ_π commute, $e_j = [\gamma_\pi f_\infty(x)]_0 = [f_\infty \gamma_\pi(x)]_0 = f\,\pi(c_1 \ldots c_n)$. The following argument proves that $c_1 \ldots c_n = d_1 \ldots d_n$. For, suppose this is not true and let $e'_1 e'_2 \ldots e'_n$ be any n-block. Define $\pi'(d_1 \ldots\ )$ to be $e'_1 \ldots e'_n$. Since the map f_∞ is onto, by Theorem 4.07 , card $f^{-1}\{a\} = s^{n-1}$ for any a in S. Also, either $s > 2$ or $n > 1$, so that

$$\text{card}(f^{-1}(S - \{e'_j\}) \geq s^{n-1} > 1 \ , \quad \text{if } n > 1 \ ,$$
$$\text{and} \quad \text{card}(f^{-1}(S - \{e'_j\}) > s^{n-1} \geq 1 \ , \quad \text{if } s > 2.$$

In either case an n-block A can be found such that $A \neq e'_1 \ldots e'_n$ and $f(A) \neq e'_j$. Let $\pi'(c_1 c_2 \ldots c_n) = A$. Then π' can be extended as a permutation on $B_n(S)$ but $f(\pi'(c_1 \ldots c_n) = f(A) \neq e'_j$, which contradicts the commutativity of γ'_π. Hence $c_1 \ldots c_n = d_1 \ldots d_n$.

Now for any n-block $e_1 \ldots e_n$, there is some π in $H(S,n)$ such that $\pi(c_1 \ldots c_n) = e_1 \ldots e_n$ and $f(e_1 \ldots e_n) = f(\pi(c_1 \ldots c_n)) = e_j$. It follows that f_∞ is equal to σ^{j-1}.

7.19. COROLLARY. *The centre of* $A(S)$ *is* $P(\delta)$.

Proof. Clearly every power of the shift is in the centre of $A(S)$. Let ϕ be any continuous onto transformation of $X(S)$ which commutes with all members of $A(S)$. Since ϕ commutes with the shift, it follows from Theorem 3.08 that there exist integers $m, n \geq 1$ such that $\phi = \sigma^m f_\infty$, where $f \in F(S,n)$ and f_∞ is onto. If ϕ commutes with every element of $\Gamma(n)$, then f_∞ commutes with all elements of $\Gamma(n)$, whence f_∞ is a power of the shift. It follows that ϕ is a power of the shift.

7.20. NOTATION. Let $Z(A(S))$ denote the centre of $A(S)$. For each ϕ in $A(S)$ define $T_\phi : A(S) \to A(S)$ by $T_\phi(\theta) = \phi^{-1}\theta\phi$, for all θ in $A(S)$. Then the set $I(A(S)) = \{T_\phi : \phi \in A(S)\}$ is the group of inner automorphisms of $A(S)$.

7.21. COROLLARY. Every finite group is isomorphic to some subgroup of $I(A(S))$.

Proof. Since $I(A(S))$ is isomorphic to $A(S)/Z(A(S))$, the result follows from Corollary 7.07.

BIBLIOGRAPHY

[1] FURSTENBERG, H. : Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation, *Math. Systems Theory* , (1967), 1-49.

[2] GOTTSCHALK, W.H., and HEDLUND, G.A. : *Topological Dynamics*, Amer. Math. Soc. Colloq, Publ. Vol. 36, American Mathematical Society, Providence, 1955.

[3] HEDLUND, G.A. : Endomorphisms and automorphisms of the shift dynamical system, *Math. Systems Theory*, 3(1969), 320-375.

[4] KEYNES, H.B. : *Lectures on Ergodic Theory*, University of Minnesota Lecture Notes, 1972.

[5] RYAN, J.P., : The shift and comutativity, *Math. Systems Theory*, Vol. 6 , No. 1 (1971), 82-85.