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 WATERSRAND, JOHANNESBURG FOR THE
DEGREE OF MASTER OF SCIENCE.

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 1.

2. THE BISEQUENCE SPACE AND THE SHIFT DYNAMICAL SYSTEM 3.

3. CONTINUOUS MAPPINGS WHICH COMMUTE WITH THE SHIFT 10.

4. ONTO MEMBERS OF \( F_{\infty}(S) \) 12.

5. CHARACTERISATION ON SHIFT COMPUTING AUTOMORPHISMS ON \( X(S) \) 17.

6. PERIODICITY OF MEMBERS OF \( A(S) \) 23.

7. SOME FURTHER PROPERTIES OF AUTOMORPHISMS ON \( X(S) \) 32.

8. BIBLIOGRAPHY 46.
1. INTRODUCTION

Let $X(S)$ be the biscquenco space over a finite symbol set $S$, where $S$ has more than one element. Let $\sigma$ 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 \((X(S), \omega^n)\), 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 \( A(S) \).
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 $I_i = \{j : j \in I, j > i\}$.

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 $I$. The cardinal of $S$ will be denoted $\text{card} S$.

(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 $I^S$. 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 \( I_i = \{ j : j \in I, j > i \} \).

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 \( s \in I \). The cardinal of \( S \) will be denoted \( \text{card} \ S \).

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

(ii) The flow \((\mathcal{X}(S), \sigma)\) 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 \( \theta \) on \( \mathcal{X}(S) \) is said to be expansive provided there exists a positive number \( \delta \) such that if \( x, y \Subset \mathcal{X}(S) \) 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 \( \mathcal{X}(S) \), since if \( x \) and \( y \) are members of \( \mathcal{X}(S) \) with \( x \neq y \), then there exists \( i \in I \) such that \( x_i \neq y_i \), and so \( d(\theta^i(x), \theta^i(y)) = 1. \)

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

2.10. NOTATION. An ordered set \( x_1x_2 \ldots x_n \), where \( x_i \Subset S \), \((i = 1, 2, \ldots, n)\) is called a block of length \( n \) over \( S \). If \( x \in \mathcal{X}(S) \) and \( A \) is an \( n \)-block over \( S \), then \( A \)
appears in $x$ if and only if there exists $i$ in $I$ such that $x_{i+1}x_{i+2} \ldots x_{i+m} = \lambda$.

2.11. REMARK. If $x$ is a member of $X(S)$ such that every block appears in $x$ then the set $\bigcup_{i=1}^{\infty} \{x_1(x)\}$ is dense in $X(S)$, hence $\sigma$ is point transitive on $X(S)$.

2.12. DEFINITION. The homeomorphism $\sigma$ 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 $|n| > N$ implies that $\sigma^n(U) \cap V \neq \emptyset$.

2.13. REMARK. To show that $\sigma$ 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 $U = S_{\frac{1}{m}}(x)$ and $V = S_{\frac{1}{p}}(y)$, where $x$ and $y$ in $X(S)$, $m, p \in I$. Take $N = \max\{2p, 2m\}$.

For each $n$ with $|n| > N$, define $z^{(n)}$ by

$z^{(n)}_i = y_i$, if $|i| < m$,
$z^{(n)}_i = x_i$, if $|i| < p$,
$z^{(n)}_i = 0$ elsewhere.

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

2.14. DEFINITION. A homeomorphism $\sigma$ 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 $\sigma^n(U) \cap V \neq \emptyset$.

2.15. REMARK. It is clear that if $\sigma$ is point transitive or
strongly mixing on \( X(S) \) then \( \theta \) 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 \((X, \tau)\) is isomorphic to a flow \((Y, \sigma)\) if there exists a homeomorphism \( \psi \) from \( X \) onto \( Y \) such that \( \sigma(\psi(x)) = \psi(\tau(x)) \) for all \( x \) in \( X \).

2.17. THEOREM. Given any symbol set \( S \) of cardinality \( s > 1 \) and \( n \) in \( \mathbb{N} \), 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 \( \mathbb{N} \), 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 a bisequence of \( X(S) \), say \( x \) is

\[
\ldots x \times x \times x \ldots ,
\]

then \( x \) may be represented as follows:

\[
\ldots B \times B \times B \ldots
\]

where \( B \) is the \( n \)-block \( x(n_1) x(n_1+1) \ldots x(n_1+n-1) \) and the
"arrow" indicates that \( a \) is indexed at the first position of \( B_o \). Define \( \psi : x(S) \rightarrow x(S') \) by \( \psi(x) = y \), where \( y(i) \) is the symbol of \( S' \) obtained by converting the \( n \)-block \( B_1 \) from base \( S \) to base \( S' \).

It is easily verified that \( \psi \) 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 bisquence over \( S \) represented in the form

\[
\ldots B B B B \ldots
\]

Then \( \sigma^n(x) \) is

\[
\ldots B B B B \ldots
\]

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 \( S' \). Now \( \sigma(\psi(x)) = \sigma(z) \), where \( z(i) \) is the conversion of \( B_i \) to base \( S' \). Thus \( [\sigma(z)]_i = z_{i+1} \) which is the conversion of \( B_{i+1} \).

To show that \( \psi \) is a homeomorphism of \( x(S) \) onto \( x(S') \), it is sufficient to show that \( \psi \) is continuous. Let \( \epsilon > 0 \) and choose \( k \) in \( \mathbb{N} \) such that \( (k+1)^{-1} < \epsilon \). 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 \( B_1^{(1)} = x^{(1)}(ni) \ldots x^{(1)}(ni+n-1), (j=1,2), \) then \( B_1^{(1)} = B_1^{(2)} \) 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
This completes the proof.

2.18. COROLLARY. If property $\mathbf{D}$ holds on the flow $(X(S'),\sigma)$ for every symbol set $S'$, and $\mathbf{D}$ is an isomorphism invariant, then given any symbol set $S$ and $n$ in $\mathbb{I}$, $\mathbf{D}$ holds on the flow $(X(S),\sigma^n)$.

Proof. Let $n$ be an element of $\mathbb{I}$ 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 $\mathbf{D}$ 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 $\sigma^n$ 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 $\mathbb{I}$ such that $x_i = x_{i+w}$ for all $i$ in $\mathbb{I}$. Hence $x$ is periodic if and only if there exists $w$ in $\mathbb{I}$ such that $\sigma^w(x) = x$.

2.22 REMARK. Clearly the set of periodic points is dense in $X(S)$.
2.23. **DEFINITION.** Furstenburg, [1], defines a flow \((X,T)\)

to be an *F-flow* if it 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 \( f^\circ : x(S) \rightarrow x(S) \) in the following way: for \( x \) in \( x(S) \) and any integer \( i \) define
\[
[f^\circ(x)]_i = f(x_i \ldots x_{i+n-1}).
\]

3.02. PROPOSITION. Let \( f \) be a member of \( F(S,n) \). Then \( f^\circ : x(S) \rightarrow x(S) \) is continuous and commutes with the shift \( \sigma \).

Proof. Let \( f \) be in \( F(S,n) \), let \( x \) be a member of \( x(S) \) and let \( f^\circ(x) = y \). 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 \( |i| < k+n \), \( x_i = u_i \). Let \( f^\circ(u) = v \). Then for all \( i \) with \( |i| < k \), \( y_i = v_i \), whence \( d(y,v) = d(f^\circ(x) , f^\circ(u)) < \varepsilon \). It follows that \( f^\circ \) is continuous.

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

3.03. NOTATION. Let \( F_\circ(S,n) = \{ f^\circ : f \in F(S,n) \} \).

3.04. REMARK. If \( 1 < m < n \) then \( F_\circ(S,m) \subset F_\circ(S,n) \). For if
3.05. \textbf{PROOF.} Let \( n \) be in \( \mathbb{N} \) and \( S \) be a symbol set. Then \( \sigma^k \in \mathcal{F}_n(S,n) \) if and only if \( 0 \leq k \leq n-1 \).

Proof. Let \( n \) be an element of \( \mathbb{N} \) and let \( k \) be an integer, \( 0 \leq k \leq n-1 \). Define \( f : \mathcal{B}_n(S) \to \mathcal{B}_1(S) \) by
\[
f(x_1 x_2 \ldots x_{k+n-1}) = x_{k+1}, \quad (i \in \mathbb{N})
\]
Then \( \sigma^k = \varphi \circ g \in \mathcal{F}_n(S,n) \).

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

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

(ii) Let \( \mathcal{F}_n^*(S) \) denote the set \( \{ \sigma^m \varphi : m \in \mathbb{N}, \varphi \in \mathcal{F}_n(S) \} \).

(iii) Let \( \mathcal{F}_n(S) \) be the set of all continuous mappings of \( X(S) \) into \( X(S) \) which commute with \( \sigma \).

3.07. \textbf{REMARK.} It is clear that \( \mathcal{F}_n(S) \subset \mathcal{F}_n^*(S) \subset \mathcal{F}_n(S) \) and as \( k < 0 \) implies that \( \sigma^k \notin \mathcal{F}_n(S) \), \( \mathcal{F}_n(S) \) is a proper subset of \( \mathcal{F}_n(S) \). The next theorem shows that the last two sets are identical. The proof is due to J.P. Ryan [5].
3.08. **Theorem.** $F^*\{S\} = \phi\{S\}$.

**Proof.** It is sufficient to show that $\phi\{S\} \subseteq F^*\{S\}$. Let $\phi$ be in $\phi\{S\}$. Since $\phi$ 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, $[\phi(x)]_0 = [\phi(y)]_0$, in $n = 2m+1$ and define $f : B(S) \rightarrow S$ as follows: if $A$ is any $n$-block such that $A = x_{-m} \ldots x_0 \ldots x_n$ 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 $[\phi^{-m} x_0 (x)]_1 = [f_0 (x)]_1 = [f_0^2 (x)]_1 = \ldots = [f_0^{m} (x)]_1 = f_0 (x)$ where $i = 1, 2, \ldots, n$.

Define $f(m) : B_{n} \rightarrow S$ as follows: if $B = b_{m-1} \ldots b_0 b_1 \ldots b_{m-1}$ is any $(m+1)$-block over $S$ then $f_m (b_0 \ldots b_{m-1}) = f(b_0 \ldots b_{m-1}) f(b_1 \ldots b_{m-1}) \ldots f(b_{m-1} \ldots b_{m-1})$. Clearly $f_1 = f$.

4. **Onto Members of $F^*\{S\}$

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

4.02 **Theorem.** Let $n$ be in $I$ and let $\phi$ be a member of $F(S,n)$. Then $f_m$ is onto if and only if each $f_m : B_{m+1}(S) \rightarrow B_m(S)$ is onto for all $m$ in $I$.

**Proof.** Assume that $f_m$ is onto. Let $m$ be in $I$ 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 $i < 0$ and $x_1 x_2 \ldots x_m = B$. Then $f(S)$ is a well-defined member of $F(S, n)$.

Hence $\phi = \phi^{m+1}$ and the proof is complete.
There exists \( y \) in \( X(S) \) such that \( f_\omega(y) = x \). Let

\[ A = y_{1} \cdots y_{m+n-1} \]

Then \( f_m(A) = B \), hence \( f_m \) is onto.

Conversely, assume that \( f_m : S_{m+n-1}(S) \to \mathcal{F}_m(S) \) is onto for each \( m \) in \( I \). Let \( x \) be in \( X(S) \) and let \( k \) be in \( I \). Let

\[ m = 2k + 1 \]

Then \( x = x_{-k} \cdots x_k \in \mathcal{F}_m(S) \) and there exists an \((m+n-1)\)-block \( A \) such that \( A = y_{-k} \cdots y_{k+n-1} \) and \( f_m(A) = B \).

Define \( y \) in \( X(S) \) by \( y_{-k} \cdots y_{k+n-1} = A \), \( y_i = 0 \) if \( i < -k \) or \( i > k+n-1 \), and let \( f_\omega(y) = u \). Then \( u_{-k} \cdots u_k = x_{-k} \cdots x_k \) and \( d(x,u) < (1+k)^{-1} \). Since \( k \) is arbitrary in \( I \), it follows that the set \( f_\omega(X(S)) \) is dense in \( X(S) \). But since \( f_\omega \) is continuous and \( X(S) \) is compact, \( f_\omega(X(S)) \) is compact, hence closed, and so \( f_\omega(X(S)) = \overline{f_\omega(X(S))} = X(S) \). Thus \( f_\omega \) is onto.

4.03. REMARK. If \( \text{card } S = S \) and \( - \) is in \( I \), and if

\[ \text{card } f_m^{-1}(S) = S^{m-1} \]

for all \( S \) in \( \mathcal{F}_m(S) \) and all \( m \) in \( I \), then it follows from Theorem 4.02 that \( f_\omega \) 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 \( I \). If \( A = a_1 \cdots a_m \in \mathcal{F}_n(S) \) and \( B = b_1 \cdots b_n \in \mathcal{F}_m(S) \), then \( AB \) will denote the \( (m+n)\)-block \( a_1 \cdots a_m b_1 \cdots b_n \). If \( A \) and \( B \) are collections of blocks over \( S \), then \( AB \) will denote \( \{AB : A \in A, B \in B\} \). The notation may be generalised in the obvious way.

4.05. LEMMA. Let \( n \) be in \( I \) and let \( \ell \) be in \( \mathcal{F}(S,n) \).

Suppose there exists an \( m\)-block \( B \) over \( S \) such that
card $f_{m+1}^{-1}(a) = k > 0$ and card $f_{m+1}^{-1}(mb) \geq k$ for each $b$ in $S$. Then card $f_{m+1}^{-1}(mb) = k$ for each $b$ in $S$.

Proof. Let $D$ be a member of $E(S)$ such that card $f_{m+1}^{-1}(D) = k > 0$. Suppose that $f_{m+1}^{-1}(D) = \{C_1, C_2, \ldots, C_k\} = C$. Then $f_{m+1}^{-1}(S) = CS$.

For if $c \in S$, $f_{m+1}^{-1}(c) \subseteq S$ if and only if $c$ is an $(m+n-1)$-block such that $f_m(c) = B$, that is if and only if $C \subseteq C$.

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

4.06. Lemma. Let $n$ be in $I$ and let $\ell$ be a member of $F(S,n)$. Let there exist an $n$-block $B$ over $S$ such that Card $f_{\ell}^{-1}(b) = k > 0$ and card $f_{2m+n-1}^{-1}(BDB) = k$ for every $(n-1)$-block $D$. Then $k = s_n^{-1}$.

Proof. Let $f_{\ell}^{-1}(B) = \{C_1, \ldots, C_k\} = C$. Let $D = s_n^{-1}(S)$.

The following argument shows that

$$f_{2m+n-1}^{-1}(BDB) = CC$$

Let $A$ be a member of $CC$. Then $A = C_1C_j$ where $C_1$ and $C_j$ are in $C$. Since $C_1$ 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 $f_m(C_1) = E = f_m(C_j)$, $E$ is of the form $BDB$, where $D$ is of length $n-1$, so that $D \in f_{2m+n-1}^{-1}(BDB)$.

Now suppose that $f_{2m+n-1}(A) = BDB$, where $D \in D$. Then
A is of length \(2m + 2n - 2\), \(A = A_1 A_2\), where \(A_1\) and \(A_2\) are of length \(m + n - 1\), \(\ell_{m}(A_1) = B = \ell_{m}(A_2)\), so that \(A_1, A_2 \in C\) and \(A_1 A_2 \in C\).

It follows that \(\ell_{2m+n-1}^{1}(B) = C\).

Clearly \(\text{card } C = k^2\). If \(\text{card } \ell_{2m+n-1}^{1}(B) = k\) for each \(D\) in \(D\), then since \(\text{card } D = s^{n-1}\), \(\text{card } \ell_{2m+n-1}^{1}(B) = k s^{n-1}\).

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) \(\text{card } \ell_{m}^{1}(B) = s^{n-1}\) for all \(B\) in \(B_{m}(S)\) 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

\[x_0 = a, \quad x_i = O, \quad i \neq 0.\]

Then there exists \(y\) in \(X(S)\) such that \(f_{\infty}(y) = x\); thus \(\ell_{y_0} = a\) 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 \(B_{m}(S)\), \(\text{card } \ell_{m}^{1}(B) > 1\). Suppose for some \(m\)-block \(B\) there exist blocks \(A = a_1 \ldots a_m\) and \(A' = a_1' \ldots a_m'\) in \(B_{m}(S)\) 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 \(\text{card } \ell_{m}^{1}(B) = s^0\), for all \(B\) in \(B_{m}(S)\) and for all \(m\) in \(I_1\).

Now suppose that \(n \geq 2\). Let

\[k = \inf \{\text{card } \ell_{m}^{1}(B) : B \in B_{m}(S), m \in I_1\},\]
It follows from Theorem 4.02 that \( k > 1 \). There exist an integer \( m \) and an \( m \)-block \( B \) over \( S \) such that \( \text{card} \ f_m^{-1}(B) = k \). Then \( \text{card} \ f_{m+1}^{-1}(\{b\}) > k \) for each \( b \) in \( S \), so it follows from Lemma 4.05 that \( \text{card} \ f_{m+1}^{-1}(\{b\}) = k \) for each \( b \) in \( S \). It can be inferred by induction that \( \text{card} \ f_{m+1}^{-1}(\{a\}) = k \) for every \( i \)-block \( A \) and hence, in particular, \( \text{card} \ f_{2m+n-1}^{-1}(\{b\}) = k \) for every \( B \) in \( S_{2m+n-1} \).

It follows from Lemma 4.06 that \( k = s^{n-1} \) and thus \( \text{card} \ f_p^{-1}(B_p) \geq s^{n-1} \) for each \( B_p \) in \( S_p[S] \) and each \( p \) in \( I \).

Suppose there exist \( p \) in \( I \) and \( B \) in \( S_p[S] \) such that \( \text{card} \ f_p^{-1}(B) > s^{n-1} \). Then

\[
\sum_{B_p \in S_p[S]} \text{card} \ f_p^{-1}(B_p) > s^{n-1} \tag{2}
\]

since \( \text{card} \ f_p^{-1}(B) > s^{n-1} \) and \( \text{card} \ f_p^{-1}(B_p) \geq s^{n-1} \) for each \( B_p \) in \( S_p[S] \). It follows, however, from Theorem 4.02 that \( f_p^{-1}(S_p[S]) = S_{p+n-1}[S] \), so that

\[
\sum_{B_p \in S_p[S]} \text{card} \ f_p^{-1}(B_p) = \text{card} f_p^{-1}(S_p[S])
\]

\[
= \text{card} S_{p+n-1}[S] = s^{n-1} \text{ which contradicts (2). Hence } \text{card} f_p^{-1}(B) = s^{n-1} \text{ for } B \text{ in } S_m[S] \text{ and all } m \text{ in } I. \text{ 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 $f \in A(S)$ if and only if $f$ is a permutation of $S$.

Proof. Suppose $f$ 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 $f(y) = x$ 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 $f(x) = f(y)$. By definition of $f$, $|f(x)| = |f(y)|$ 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 $f \in A(S)$. 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 $I_1$, $q > m$, let $D(B,q)$ be the set of all $q$-blocks over $S$ in which $B$ appears and let $N(B,q) = \text{card } D(B,q)$.

Then
Proof. Let \( \phi(q) = S^{-q}N(B,q) \). Let \( c \) be in \( D(B,q) \). Then \( c_0 \in D(B,q+1) \) for each \( c \) in \( S \), so that \( N(B,q+1) \supseteq S \cdot N(B,q) \) and hence \( \phi(q+1) = S^{-q}N(B,q+1) \supseteq S^{-q}N(B,q) = \phi(q) \). Since \( \text{card } B \cdot n = s^q \), it follows that \( N(B,q) \leq s^q \), whence \( \phi(q) \leq 1 \). Thus \( \lim_{q \to \infty} \phi(q) = a \), where \( 0 < a < 1 \).

Let \( k \) be in \( I \) and let \( A \) be a block of length \( km \). Then \( A = B_1 B_2 \ldots B_k \), where each \( B_i \) is an \( m \)-block, \( 1 \leq i \leq k \).

Let \( A_1 \) 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 \( A_1 \cap A_j = \emptyset \). Let \( A(k) = \bigcup_{i=1}^{k} A_i \). Then \( B \) appears in every member of \( A(k) \); hence \( N(B,km) \geq \text{card } A(k) \), and so

\[
\phi(km) = S^{-km}N(B,km) \geq S^{-km} \text{card } A(k).
\]

Let \( a = s^{m-1} \), \( b = s^m \). Then

\[
\text{card } A(k) = \sum_{i=1}^{k} \frac{a^{i-1}b^{k-i}}{a_i} = \sum_{i=1}^{k} \frac{b^k}{\prod_{j=1}^{k}} \frac{a^i}{b^j} = \frac{(a^k - b^k)/(a - b)}{s^k - (s^m - 1)^k}.
\]

It follows from (1) that

\[
\lim_{q \to \infty} \phi(q) = \lim_{k \to \infty} \phi(km) \geq \lim_{k \to \infty} s^{-km} \left[ s^{km} - (s^m - 1)^k \right]
\]

\[
= \lim_{k \to \infty} \left[ 1 - \left( 1 - \frac{1}{s^m} \right)^k \right] = 1.
\]

Hence \( \lim_{q \to \infty} N(B,q) s^{-q} = 1 \).
5.05 **Lemma.** Let \( m \) be in \( I \), let \( f \) be in \( F(S,m) \) and suppose that \( f_m \) is not onto. Let \( k, t \) be in \( I \).
Then there exists an \( m \)-block \( A \) with \( m > t \) such that \( \text{card } f^{-1}_m(A) > k \).

**Proof.** Assume the hypothesis of the lemma and suppose that 
\( \text{card } f^{-1}_m(A) < k \) for all \( m \)-blocks \( A \), \( m > t \). Since \( f_m \) is not onto, it follows from Theorem 4.02 that there exists an integer \( q > 1 \) and \( B \) in \( B_q \) such that \( f_q^{-1}(B) = \emptyset \), whence \( \text{card } f_q^{-1}(B) = 0 \). This implies that \( \text{card } f_m^{-1}(B) = 0 \), where \( D \) is any \( m \)-block in which \( B \) appears.

Let \( D(B,m) \) be the set of all \( m \)-blocks over \( S \) in which \( B \) appears and let \( D'(B,m) \) be the set of all \( m \)-blocks over \( S \) in which \( B \) does not appear. Let \( N(B,m) = \text{card } D(B,m) \). Since 
\[ B_m(S) = D(B,m) \cup D'(B,m) \quad \text{and} \quad \text{card } B_m(S) = S^m, \]
\( \text{card } D'(B,m) = S^m - N(B,m) \). Now \( B_{m+n-1}^{-1}(S) = f_m^{-1}(B_m(S)) \)
\[ = f_m^{-1}(D(B,m) \cup f_m^{-1}(D'(B,m))) \]
and the sets \( D(B,m) \) and \( D'(B,m) \) are disjoint, so that 
\[ S_{m+n-1} = \text{card } B_{m+n-1}^{-1}(S) = \text{card } f_m^{-1}(D(B,m)) + \text{card } f_m^{-1}(D'(B,m)). \]
If \( m > q \), \( \text{card } f_m^{-1}(D(B,m)) = 0 \), so that \( S_{m+n-1} = \text{card } f_m^{-1}(D'(B,m)). \)
By assumption, \( \text{card } f_m^{-1}(A) < k \) for all \( m \)-blocks \( A \), \( m > t \).
Thus if \( m > t + q \)
\[ S_{m+n-1} < k \quad \text{card } D'(B,m) = k \left[ S^m - N(B,m) \right] \]
Hence
\[ D(B,m) \leq S^m - S_{m+n-1}/k \]
that is,
This implies that

\[ \limsup \frac{N(B,m)}{S^n} < 1 - \frac{S^{n-1}}{k} \]

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 \( B \) and \( B^* \) in \( E \) such that \( B = AB \) and \( B^* = AB^* \), where \( A \) and \( B \) are \((n-1)\)-blocks.

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

Thus there exists an integer \( j \) such that card \( \mathcal{E}_j > s^{n-1} \). But then at least two distinct members of \( \mathcal{E}_j \) must have the same terminal \((n-1)\)-block \( B \). Let these be \( \lambda_jDB \) and \( \lambda_jD^*B \). The proof of the Lemma is concluded by taking \( A = \lambda_j \), \( B = AB \) and \( B^* = AB^* \).

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

\[ f_{m+2(n-1)}(APA) = f_{m+2(n-1)}(AD^*A) \]
Proof. Let $E = f^{-1}_{m+2n-1}(C)$. Then $E$ is a collection of $(m+2n-2)$-blocks and, by hypothesis, $\text{card } E > S^{2n-2}$. It follows from Lemma 5.06 that there exist distinct blocks $E$ and $E^*$ in $E$ such that $E = ADR$ 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 $E$, $f_{m+n-1}(E) = C = f_{m+n-1}(E^*)$.

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

$$f_{m+2(n-1)}(APA) = f_{m+2(n-1)}ADPA = CQ,$$

and

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

5.08. Theorem. Let $n$ be in $I$, let $f$ be in $F(S,n)$ and suppose that $f_n$ is not onto. Then there exists a periodic point $x$ in $x(S)$ such that the set $f^{-1}_\infty(x)$ is uncountable.

Proof. Suppose $n = 1$. Since $f_1$ 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 sequence defined by $x_i = c$, all $i$ in $I$. Then $x$ is periodic and the set $f^{-1}_\infty(x)$ includes all sequences $y$ defined by $y_i = a$ or $b$, all $i$ in $I$. This set is uncountable.

Now assume that $n > 2$. From Lemma 5.05 there exists an $(m+n-1)$-block $C$ such that $\text{card } f^{-1}_{m+n-1}(C) > S^{2n-2}$. 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

\[
\cdots A Q_1 A Q_0 A Q_1 A Q_0 \cdots
\]

where, for \( i \) in \( I \), \( Q_i \) is either \( P \) or \( P^* \). Let \( x \) in \( x(S) \) be defined by \( x = \cdots D D D D \cdots \). 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 \( \phi \) be a member of \( \Phi(S) \) and suppose that \( \phi \) 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 \( \phi \) be in \( \Phi(S) \). By Theorem 3.08, there exist \( m \) in \( I \) and \( n \) in \( I \) such that \( \phi = \sigma^m f_{\omega} \), where \( f \in F(S, n) \). Since \( \phi \) is not onto, \( f_{\omega} \) 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 \( f_{\omega}(Y) = z \). But then \( \phi(Y) = \sigma^m f_{\omega}(Y) = \sigma^m(z) \).

Let \( x = \sigma^m(z) \). Then \( x \) is periodic.

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

Proof. Clearly \( A(S) \subset \{ \phi : \phi \in \Phi(S) \text{ and } \phi \text{ is one-to-one} \} \).

Now suppose that \( \phi \) in \( \Phi(S) \) is one-to-one, then by Theorem 5.09, \( \phi \) is onto, whence \( \phi \in A(S) \).
6. PERIODICITY OF MEMBERS OF $A(S)$.

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

6.02. REMARK. If $f \in F(S,n)$ for $n$ in $I$ and $f_\infty$ is periodic, then $f_\infty \in A(S)$. For, suppose the period of $f_\infty$ is $p$, $p$ in $I$. 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 $I$, and let $f$ be a member of $F(S,m)$ and $g$ an element of $F(S,n)$. Then $g_m$ maps $E_{m+n-1}(S)$ into $E_m(S)$ and $f$ maps $E_n(S)$ into $E_1(S) = S$, so that $f g_m$ is a well defined mapping of $E_{m+n-1}(S)$ into $S$. The mapping $f g_m$ will also be denoted by $f g$.

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

Proof. Let $x$ be a bisequence in $X(S)$ and let $(f g)_\infty(x) = y$.

Let $i$ be in $I$. Then $y_i = f g_m[x_1 x_{i+1} \ldots x_i m+n-2] = f[g(x_1 \ldots x_{i+n-1}) \ldots g(x_{i+m+n-1} \ldots x_{i+2n-2})]$. Let $g_m(x) = u$; thus $y_i = f(u_1 \ldots u_{i+n-1}) = f[g(x_1 \ldots x_{i+n-1}) \ldots g(x_{i+m+n-1} \ldots x_{i+2n-2})]$. Thus for all integers $i$, $y_i = v_i$. Hence $y = v$ and so $(f g)_\infty(x) = (f_\infty g_\infty)(x)$.

Since this is true for all $x$ in $X(S)$, $(f g)_\infty = f_\infty g_\infty$.

6.05. PROPOSITION. If $f \in F(S,1)$, then $f_\infty$ is periodic if and only if $f$ is a permutation of $S$. 
Proof. Let $S = \{0, 1, 2, \ldots, n-1\}$ and let $f$ be a permutation of $S$. Then there is a positive integer $p$, $p < s^2$ such that $f^p$ is the identity on $S$. Then $(f^p)^m$ is the identity on $x(S)$.

It follows from Lemma 6.04 that $(f^p)^m = (f^m)^p$. Hence $(f^m)^p(x) = x$, for all $x$ in $x(S)$, so $f^m$ is periodic.

Now suppose that $f^m$ is periodic. Then $f^m$ is one-to-one, thus $f^m \in A(S)$. By Proposition 6.02, $f$ is a permutation of $S$.

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

6.07. PROPOSITION. Let $n$ be in $I$ and $f$ be an element of $F(S, n)$ with $f^m$ one-to-one. If $f$ does not depend on $x_1, x_2, \ldots, x_n$, then $f^m$ is periodic.

Proof. Define $g$ in $F(S, 2)$ by $g(a) = f(a x_1 x_2 \ldots x_n)$ for each $a$ in $S$ and any members $x_1, x_2, \ldots, x_n$ in $S$. Then since $f$ does not depend on $x_1, \ldots, x_n$, $g$ is well defined and $g^m = f^m$.

Since $f^m \in A(S)$, $g^m \in A(S)$, whence, by Proposition 5.02, $g$ is a permutation on $S$. Thus, by Proposition 6.05, $f^m = g^m$ 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
The following argument shows that \( f_w \) has period two, that is, \( f(f(x_i, x_{i+1})) = x_i \), for any \( x_i, x_{i+1}, x_{i+2} \) in \( S \).

Suppose that \( x_i = 1 \). Then since \( f(1) = 1 \), 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 \( f_w^2 \) is the identity on \( X[S] \) and so \( f_w \in \lambda[S] \), but \( f \) depends on \( x_i \).

6.10 DEFINITION. Let \( n \) be in \( I_2 \). A function \( f \) in \( F(S, n) \) is said to be **permutive in** \( x_i \), if for every choice of fixed elements \( \bar{x}_1, \ldots, \bar{x}_n \), and \( x_i \) any element of \( S \), \( f(x_i, \bar{x}_1, \ldots, \bar{x}_n) = g(x_i) \) where \( g \) is some permutation of \( S \). Hence \( f \) is permutive in \( x_i \) if and only if for any given elements \( \bar{x}_1, \ldots, \bar{x}_n \) in \( S \),

\[
f(x_i, \bar{x}_1, \ldots, \bar{x}_n) = f(x_1', \bar{x}_1, \ldots, \bar{x}_n) \quad \text{implies that} \quad x_i = x_1'.
\]

6.11 REMARK. Let \( n \) be in \( I_2 \) and \( f \) in \( F(S, n) \). Then the following example shows that \( f_w \) a member of \( \lambda[S] \) does not
imply that \( f \) is permutive in \( x \). However, it will be shown in Proposition 6.13 that if \( f_n \) is periodic, then \( f \) is permutive in \( x \).

6.12. **EXAMPLE.** Let \( n \) be in \( \mathcal{I} \). Define \( f \) in \( \mathcal{F}(S,n) \) by
\[
f(a_1 \ldots a_n) = a_n
\]
for all \( n \)-blocks \( a_1 \ldots a_n \) over \( S \). Then \( f_n = \sigma^{-n}(\theta) \in \mathcal{A}(\mathcal{I}) \), but \( f \) is not permutive in \( x \).

6.13. **PROPOSITION.** Let \( n \) be in \( \mathcal{I} \) and suppose that \( f \in \mathcal{F}(S,n) \). Then if \( f_n \) is periodic, \( f \) is permutive in \( x \).

**Proof.** Assume that \( f_n \) is periodic on \( x(S) \) but that \( f \) is not permutive in \( x \). Then there exist \( n \)-blocks \( A = x_1 \ldots x_n \) and \( A' = x'_1 \ldots x'_n \), with \( x_i \neq x'_i \) such that \( f(A) = f(A') \).

Let \( x \) be the member of \( x(S) \) defined by \( x_i = 0 \) if \( i \not\in 0 \) or \( i > n \), and let \( y \) in \( x(S) \) be defined by \( y_i = 0 \) if \( i \not\in 0 \) or \( i > n \) and \( y_1 \ldots y_n = A' \). Now there is some integer \( p \geq 1 \) such that \( (f_n)^p \) is the identity on \( x(S) \). Hence \( (f_n)^p(x) = x \) and \( (f_n)^p(y) = y \). Since for any integer \( i \geq 1 \), \( \{ f_n(x) \}_i = [ f_n(y) ]_i \), it follows that
\[
x_1 = [ f_n^p(x) ]_1 = [ f_n^p(y) ]_1 = x'_1.
\]
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
\[
\begin{align*}
f(00) &= 1 & f(01) &= 0 & f(02) &= 0 \\
f(10) &= 0 & f(11) &= 1 & f(12) &= 1 \\
f(20) &= 2 & f(21) &= 2 & f(22) &= 2.
\end{align*}
\]
Then \( f \) is permutive in \( x_1 \), but if \( x \) in \( X(S) \) is defined by \( x_1 = 0 \), all \( i \) in \( I \), then for all positive integers \( p \), \( f^p(x) = y \), where \( y_1 = 1 \), all \( i \) in \( I \).

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

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

6.16. Theorem. Let \( S = \{0, 1\} \) and \( n \) be in \( I \). 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 \( f_\infty \in F^k(S, k) \). Then \( k > 1 \) and there exists \( g \) in \( F(S, k) \) such that \( f_\infty = g_\infty \). Since \( f_\infty \) is one-to-one so is \( g_\infty \). There must exist a \( k \)-block \( \bar{a}_1 \ldots \bar{a}_{k-1} \bar{a}_k \) 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 \( h : \bar{F}_{k-1}(S) \to S \) 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 \( g(0a_1 \ldots a_k) = g(1a_1 \ldots a_{k-1} \bar{a}_k) \). Let \( a = a_1 \ldots a_{k-1} a_k \), \( b = a_1 \ldots a_{k-1} \bar{a}_k \). Then \( g(0a) = g(1b) \).

Let \( P \) be the set of all integers \( p > k \) with the property that there exist \( p \)-blocks \( A_p = a_0 \ldots a_p \) and \( B_p = b_0 \ldots b_p \) such that \( g_{p-k+1}(A_p) = g_p(A_p) \). Then \( k \in P \). The following argument shows that \( P = \{m|m \in I, m > k \} \). If \( p > q > k \) and
Suppose that $P$ is bounded and that $m$ is the least upper bound of $P$. Then there are $m$-blocks $A_m = 0 \leq \ldots \leq c_m$, $B_m = 1 \leq \ldots \leq d_m$ such that $\gamma_{m+k+1}(A_m) = \gamma_{m-k+1}(B_m)$. Now since $m$ is maximal,

$$\gamma_{m+k+2}(0 A_m) \neq \gamma_{m-k+2}(1 B_m),$$

and

$$\gamma_{m+k+2}(1 A_m) \neq \gamma_{m-k+2}(0 B_m).$$

Hence, as $g$ is permutative in $x_k$, $\gamma_{m+k+2}(0 A_m) = \gamma_{m-k+2}(0 B_m)$ and $\gamma_{m+k+2}(1 A_m) = \gamma_{m-k+2}(1 B_m)$.

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

$$\gamma_m(0 A_m) = \gamma_m(0 B_m), \text{ all } (k-1)-blocks D.$$ But then $g(D) = g(D)$ for all $D$ in $\mathbb{E}_{k-1} [S]$, 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 $\gamma_{p-k+1}(0 A(p)) = \gamma_{p-k+1}(1 B(p))$. Define $y(p)$ in $x[S]$ by

$$y_1^{(p)} = 0 \text{ if } i < 0 \text{ or } i > p,$$

$$y_i^{(p)} = 1 \text{ if } 0 \leq i \leq p - 1.$$

Define

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

$$z_1^{(p)} = 0 \text{ if } i \geq p,$$

and

$$z_i^{(p)} = b_i^{(p)} \text{ for } 0 \leq i \leq p - 1.$$
Since \( g \) is permutive in \( x \), for each \( i < -1 \) there exists 
\( z_{i}^{(p)} \) in \( S \) such that 
\[ g(x_{1}^{(p)} \ldots x_{i+1-k}^{(p)}) = g(y_{1}^{(p)} \ldots y_{i+k+1}^{(p)}) \] 
(\( i < -1 \)). This defines \( z^{(p)} \) in \( X[S] \).

Let \( g_{o}(y_{o}^{(p)}) = u_{o}^{(p)} \), \( g_{o}(z_{o}^{(p)}) = v_{o}^{(p)} \). Then 
\[ u_{o}^{(p)} = v_{o}^{(p)} (i < p - k) \] 
This implies that \( d(u_{o}^{(p)}, v_{o}^{(p)}) < (p - k + 2)^{-1} \).
Thus \( \lim_{p \to \infty} d(u_{o}^{(p)}, v_{o}^{(p)}) = 0 \).

Since \( X[S] \) is a compact metric space, any infinite sequence of points contains a convergent subsequence, so assume that 
\[ \lim_{p \to \infty} y_{o}^{(p)} = y, \lim_{p \to \infty} z_{o}^{(p)} = z, \lim_{p \to \infty} u_{o}^{(p)} = u, \lim_{p \to \infty} v_{o}^{(p)} = v. \] Since \( y_{o}^{(p)} = y \), \( z_{o}^{(p)} = z \), \( u_{o}^{(p)} = u \), \( v_{o}^{(p)} = v \).

Now \( g_{o}(y) = g_{o}(\lim_{p \to \infty} y_{o}^{(p)}) = \lim_{p \to \infty} g_{o}(y_{o}^{(p)}) = \lim_{p \to \infty} u_{o}^{(p)} = u \) and 
\[ g_{o}(z) = g_{o}(\lim_{p \to \infty} z_{o}^{(p)}) = \lim_{p \to \infty} g_{o}(z_{o}^{(p)}) = \lim_{p \to \infty} v_{o}^{(p)} = v = u, \] so that 
\[ g_{o}(y) = g_{o}(z). \] This contradicts the hypothesis that \( f_{n} \), and hence 
\( g_{o} \), is one-to-one.

The proof of the theorem is completed.

6.17. Corollary. Let \( S = \{0, 1\} \) and \( n \) be in \( I \). Then if 
\( f \in F(S,n) \) and \( f_{o} \in A[S] \), \( f_{o} \) is periodic, if and only if 
\( f \) is permutive in \( x_{i} \).

Proof. If \( f_{o} \) is periodic, then the result follows from Proposition 6.13. Suppose \( f \) is permutive in \( x_{i} \) and \( f_{o} \in A[S] \). Then by Theorem 6.16 there exists \( g \) in \( F(S,1) \) such that \( g_{o} = f_{o} \). Since 
\( f_{o} \in A[S] \), \( g_{o} \in A[S] \), whence by Proposition 5.02 \( g \) is a permutation
of $S$. It follows from Proposition 6.05 that $f_0 = g_0$ is periodic.

6.18. NOTATION. Denote the set of all powers of the shift by $P(0)$. That is, $P(0) = \{0^n : n \in \mathbb{N}\}$. Clearly $P(0) \subseteq A(S)$.

6.19. REMARK. The following example due to Hedlund, [3], shows that $A(S)$ contains two elements $a$ and $b$, each of period two, such that the product of these elements, $\phi$, is not a member of $P(0)$, yet has infinite order.

6.20. EXAMPLE. Let $S$ be any symbol set and define $f$ in $F(S,4)$ by $f(x_{i+1} x_{i+2} x_{i+3}) = x_{i+1}$ for all 4-blocks except 1010 and 1101. Let $f(1010) = 1$ 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 $[\alpha(x)]_i = x_i$. Clearly $\alpha \in A(S)$ and $\alpha$ has period two. Let $\beta = \sigma^{-1}f_0$. Then it can be seen that $\beta \in A(S)$ and $\beta^2$ is the identity on $X(S)$.

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

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

$X_i = 0, \quad i > 0.$
31.

\[ x_7 x_6 \ldots x_1 = 1001001 , \]

and \[ x_{-2i-1} x_{-2i} = 10 , \ i > 0. \]

That is, \( x \) is the bisquence

\[ L \ 1001001 \ R \]

where \( L \) is the left infinite sequence \( \ldots 1010 \),
\( R \) is the right infinite sequence \( \ldots 00 \),
and \( x \) is indexed at the first element of \( R \). It will
be shown by induction that \( \phi_{2p}(x) = L \ 1001001 \ 01 \ R \),
for all \( p \) in \( I \).

Now \( x \) is \( L \ 1001001 \ R \)

Thus \( \beta(x) \) is \( L \ 1101101 \ R \)

and \( \hat{\beta}(x) \) is \( L \ 10010010 \ R \)

where \( R \) is the right infinite sequence \( \ldots 111 \).

Then \( \beta \hat{\beta}(x) = L \ 1101101 \ R \),
whence \( \phi_{2}(x) = L \ 100100101 \ R \),
that is, \( \phi_{2}(x) \) is \( L \ 1001001 \ 01 \ R \).

Assume that \( \phi_{2p}(x) = L \ 1001001 \ 01 \ R \).
Then \( \phi_{2p+1}(x) = L \ 1001001 \ 01 \ 01 \ R \) and so,
\( \phi_{2}(p+1)(x) = L \ 1001001 \ 01 \ 01 \ R \).

We have \( \phi_{2}(p+1)(x) = L \ 1001001 \ 01 \ 01 \ R \) which completes
the inductive argument.

Since the block 100101 does not appear in \( x \) but appears
in \( \phi_{2p}(x) \), all \( p \) in \( I \), it follows that \( \phi \) is not periodic.
7. SOME FURTHER PROPERTIES OF AUTOMORPHISMS ON $x(S)$.

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

7.02. NOTATION. Let $n$ be an element of $I$, and let

$$B = b_1 b_2 \cdots b_n$$

be an $n$-block over $S$. Let $m$ be in $I$, $m < n$. The initial $m$-block of $B$ is the block $b_1 \cdots b_m$. The terminal $m$-block of $B$ is the block $b_{n-m+1} \cdots b_n$.

7.03. DEFINITION. Let $m,n$ be in $I$. Let $B$ be an $n$-block over $S$ and let $C$ be an $n$-block over $S$. Then $B$ and $C$ overlap provided there exists $k$ in $I$ 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 $I$, and $A$ be an $n$-block over $S$. Then $A^n$ is the $(mn)$-block $A_1 A_2 \cdots A_m$, where $A_i = A$ ($i = 1, 2, \ldots, m$).

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

$$C = A \circ S_n^{(S)} \circ B,$$

then no two members of $C$ overlap.

Proof. Let $C, D$ be unequal elements of $C$, say

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

$$D = A \circ d_1 \cdots d_n \circ B.$$
Suppose there exists $k$ in $\mathbb{I}$, such that the terminal $k$-block of $C$ coincides with the initial $k$-block of $D$. Since $C \neq D$, and $C,D \in S_{2n+2m+3}$, it follows that $1 \leq k \leq 2n + 2m + 3$.

Suppose $k > n + 1$. 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 $1 \leq k \leq n$.

Since the initial $1$-block of $D$ is $1$ and the terminal $1$-block of $C$ is $0$, $k \neq 1$, whence $2 \leq k \leq n$.

If $2 \leq k \leq n$, the initial $k$-block of $D$ contains $11$ as a sub-block. Since the length of $OB \geq n$, 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 $\mathbb{I}$ 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 $(x(S),\sigma)$.

Proof. For $n$ in $\mathbb{I}$, let $N(S,n)$ be the symmetric group on $S$. 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 $n \geq 2$ such that $G$ is isomorphic to a subgroup of $N(S,n)$. It is thus sufficient to prove that $N(S)$ contains a subgroup isomorphic to $N(S,n)$, $n$ in $\mathbb{I}$.

Let $n$ be an element of $\mathbb{I}$. Corresponding to each $\psi$ in $N(S,n)$ define a map $\nu_{\psi} : x(S) \to x(S)$ as follows. Let $C$ be as in the above lemma and let $x$ be a member of $x(S)$. If $C = a_0 a_1 \ldots a_n$ is a member of $C$ which appears in $x$, 

33.
then \( Y_{\pi} \) changes \( C \) into the block \( A \circ \tau(c_1 \ldots c_n) \circ \beta \),
while any other block in \( x \) not overlapping a member of \( C \) is
left unchanged. Since no two members of \( C \) overlap, \( Y_{\pi} \) is
well defined, and it is clear that \( Y_{\pi} \) is uniquely defined by \( \pi \).

Since any member of \( H(S, n) \) has period \( (s^n)^1 \), the map
\( Y_{\pi} \) is periodic of period \( (s^n)^1 \) and so is one-to-one. To show
that \( Y_{\pi} \in (S) \), it is sufficient to show that \( Y_{\pi} \) 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 \( \delta = (n + j)^{-1} \).
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 \( Y_{\pi}(x) = y \), \( Y_{\pi}(z) = u \).
For each integer \( i \), \( y_i \) is uniquely determined by the block
\( x_i-1(j-1) \ldots x_{i+(j-1)} \) while \( u_i \) is uniquely determined by
\( z_i-1(j-1) \ldots z_{i+(j-1)} \). Thus \( y_i = u_i \) if \( |i| < m \), whence
\( d(Y_{\pi}(x), Y_{\pi}(z)) = d(u, v) < (1 + m)^{-1} < \varepsilon \). Thus \( Y_{\pi} \) is continuous.

The following argument shows that \( Y_{\pi} \) commutes with \( \sigma \).
Let \( \sigma \) be in \( x(S) \), \( Y_{\pi}(x) = y \) and \( \sigma(x) = u \). Then
\( \sigma Y_{\pi}(x) = Y_{\pi+1} \) and \( u_i = x_{i+1} \), \( i \) in \( I \). Let \( Y_{\pi}(u) = v \).

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 \( k < i < k + j - 1 \) and \( x_k \ldots x_{k+j-1} \in C \), where \( j \) is
the length of an element of \( C \). Then \( x_k \ldots x_{k+j-1} = A \circ \tau(c_1 \ldots c_n) \circ \beta \),
say, and this equals \( u_k \ldots u_{k+j-2} \). But then
\( v_k \ldots v_{k+j-2} = A \circ \tau(d_1 \ldots d_n) \circ \beta = y_k \ldots y_{k+j-1} \), where
\( d_1 \ldots d_n = \pi(c_1 \ldots c_n) \). Since \( k - 1 < k - 1 < k + j - 2 \),
it follows that \( v_i+1 = y_i \).
If there does not exist an integer \( k \) such that
\[ k \leq i < k + j - 1 \] 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 \( p < i - 1 < p + j - 1 \) and \( u_p \ldots u_{p+j-1} \in C \).
This implies that \( v_i = u_{i-1} = x_i = y_i \). Thus \( \alpha \gamma_x = \gamma_y \). It
follows that \( \gamma_x \in A(S) \).

If \( \alpha, \beta \) are elements of \( A(S, n) \), then \( \gamma_\beta \gamma_\alpha = \gamma_\beta \alpha \). For
if \( A B_1 \ldots B_n \) is a block of \( A \) appearing in \( x \), \( \gamma_x = y \) will appear in the same position in \( y = \gamma_x (x) \) as the block
\( A B_1 \ldots B_n \) is in \( x \). Similarly, \( \gamma_x \) transforms the block
\( A B_1 \ldots B_n \) into the block \( A C_1 \ldots C_n D \), where
\( C_1 \ldots C_n = \beta (B_1 \ldots B_n) \), in the same position in \( z = \gamma_x (y) \).

Now \( \gamma_\beta \alpha \) transforms \( A B_1 \ldots B_n \) appearing in \( x \)
into the block \( A (\beta A (A \ldots A a_1 \ldots a_n) B_1 \ldots B_n) \)
= \( A C_1 \ldots C_n D \) in \( \gamma_x \alpha \) (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
\[ k < i < k \ldots i + j - 1 \] and \( x_k \ldots x_{i+j-1} \in C \), then
\( y_i = x_i \), \( z_i = y_i \),
and \( u_i = x_i \), so that \( z_i = u_i \). Thus \( \gamma_\beta = \gamma_\beta \alpha \).

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

7.06. COROLLARY. The set \( A(S) \) is infinite.
Proof. It follows from Theorem 7.05 that given any \( k \) in \( I \), there exists an element of \( A(S) \) of order \( k \). Since \( \sigma^k \) is not the identity for any \( k \) in \( I \), the element is not a power of the shift.

7.07. COROLLARY. Every finite group is isomorphic to some subgroup of \( A(S) \).

Proof. Since the elements of \( A(S) \) commute with \( \sigma \), \( P[S] \) is a normal subgroup of \( A(S) \) and the quotient group \( A(S)/P(G) \) is well defined. It has been shown that \( H(S,n) \) is isomorphic to the subgroup \( \sigma = A(H(S,n)) \) of \( A(S) \). Let \( G' = G/P(G) \). Then since \( G \cap P(G) = \{1\} \) 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 \( A(S) \).

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 \( \theta \) is a map from \( X(S) \) onto \( X(S) \) such that some power of \( \theta \) is a member of \( P(G) \), then \( \theta \) 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 \( \theta \) 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) \( \theta \) is an automorphism of \( X(S) \).

(2) \( \theta \) is expansive.

(3) \( \theta \) is point transitive.

(4) \( \theta \) is strongly mixing.

(5) \( \theta \) is not periodic.

Proof. (1) It is sufficient to show that \( \theta \) is one-to-one.

Suppose that \( \theta(x) = \theta(y) \), for \( x, y \) in \( X(S) \). Then \( \theta_{-1}(\theta(x)) = \theta_{-1}(\theta(y)) \), whence \( \theta^0(x) = \theta^0(y) \) and so \( \theta^k(x) = \theta^k(y) \).

Since the shift is one-to-one, \( x = y \).

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

Hence \( d(\theta^{pn}(x), \theta^{pn}(y)) > \delta \) so \( \theta \) is expansive.

(3) Since \( \theta^k \) is point transitive, any \( k \) in \( \mathbb{Z} \), there is some \( x \) in \( X(S) \) such that \( \{\theta^k(x) : k \in \mathbb{Z}\} \) is dense in \( X(S) \). Hence \( \{\theta^{pn}(x) : n \in \mathbb{Z}\} \) is dense in \( X(S) \), so clearly \( \theta \) is point transitive.

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

\[
\theta^{-j}(U) \cap \theta^{kN_j}(V) \neq \emptyset, \text{ for all } k \text{ with } |k| > N_j.
\]

Thus \( \theta^{-j}(U) \cap \theta^{pN_j}(V) \neq \emptyset, \text{ for all } k \text{ with } |k| > N_j \)

and so \( U \cap \theta^{pN_j}(V) \neq \emptyset, \text{ if } |k| > N_j \).

Thus for \( |k| > \max(N_j, N_k) \), \( U \cap \theta^{pN_j}(V) \neq \emptyset \) for any \( j \).
This is sufficient to prove that 0 is strongly mixing and it
follows that 0 is also ergodic.

(5) Suppose that 0 is periodic. Then there is a positive
integer n such that \(0^n = I\), where I is the identity on \(X[S]\).
Hence \((0^n)^p = 0^{kn} = I\). But 0 is not periodic. This contradiction
concludes the proof.

7.10. EXAMPLE. If \(0\) is any member of \(A(S)\) which is periodic,
then for \(n\) in \(I\), \(0^n0\) satisfies the five properties of
Theorem 7.09. For, if \(0\) has period \(p\), \(p > 1\), then as
\(0 \in A(S)\) and so commutes with the shift,
\((0^n)^p = 0^{np} = 0^p\).

7.11. EXAMPLE. We construct a class of functions in \(F_p(S)\) such
that each function, \(h_0\), is a member of \(A(S) \setminus \{0\}\) and
\(h_0^p = 0^p\), for \(p > 2\).

Let \(p\) be in \(I\), 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 \(B \subseteq S\) to
be \(\{0, 1, \ldots, p-1\}\) and let \(\pi\) be the cyclic permutation
on \(S\). For any \(n\) in \(I\), define \(h\) in \(F(S,n)\) as follows.
If \(x_1 x_2 \ldots x_{i+n-1}\) is any n-block, let \(h(x_1 x_2 \ldots x_{i+n-1}) = x_{i+1}\), except in the following \(p\) cases. Let \(A\) be the
set of \(p\) distinct n-blocks \(A_1 = a_1 a_2 \ldots a_n\), such
that \(a_1 = a_n = 1, a_1 = a_n = \ldots = a_{n-1} = 0\) and \(i\) is a
member of \(B\), and let \(h(A_i) = \pi^{i+1}(i)\), each \(i\) in \(B\).
Hence \(h(100 \ldots 01) = \pi(0) = 1\),
\(h(110 \ldots 01) = \pi^2(0) = 2\),
\(h(1 p-1 0 \ldots 01) = h^p(0) = 0\).
Since no two members of \( A \) 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 \( A \), then \( h_m \) acts on the block in the same way as \( \sigma \) does, whence \( \sigma^{-1} h_m \) leaves \( B \) unchanged. It follows that \((\sigma^{-1} h_m)^p \) acts as the identity on \( B \). If \( B \) is a member of \( A \), that is, \( B = A_i \) some \( 0 < i < p - 1 \), then the map \( \sigma^{-1} h_m \) changes \( A_i \) to \( A_{i+1} \) if \( 0 < i < p - 1 \) and \( \sigma^{-1} h_m \) changes \( A_{p-1} \) to \( A_0 \). Thus \((\sigma^{-1} h_m)^p \) also leaves any member of \( A \) unchanged. It follows that \( \sigma^{-1} h_m^p = (\sigma^{-1} h_m)^p \) acts as the identity on \( x \). Thus \( h_m^p = \sigma^p \). Thus \( h_m \) is one-to-one and so is a member of \( A(S) \).

To show that \( h_m \notin P(S) \), let \( x \) be the element of \( X(S) \) defined by \( x = L A_o R \) where \( R \) is the right infinite sequence \( \cdots 00 \cdots \) and \( L \) is the left infinite sequence \( \cdots 00 \cdots \) and \( x \) is indexed at the first element of \( A_o \).
That is, \( x = \cdots 0100 \cdots 010 \cdots \).
Then \( h_m(x) = \cdots L A_i R = \cdots 010 \cdots 010 \cdots \),
and clearly \( h_m(x) \neq \sigma^p(x) \) for any integer \( p \). Since \( h_m^p = \sigma^p \), \( h_m \) has the five properties of Theorem 7.09.

7.12. REMARKS. (1) If \( j \) is an integer such that \( 1 < j < n - 1 \),
where \( n \in N \), then a member \( h \) of \( F(S,n) \) may be obtained with \((h_o)^p = \sigma^p \), by defining \( h(x_1 x_{i+1} \ldots x_{i+p-1}) = x_{i+j} \)
for all \( n \)-blocks \( x_1 x_{i+1} \ldots x_{i+p-1} \) except the \( p \)-blocks
\( A = a_1 a_2 \ldots a_j 1 a_{j+2} \ldots a_n \) 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 \( S \).
Define \( h(x) = (x^{i+1}(l)) \), each \( l \) in \( B \).

(iii) It is not known whether all roots of powers of the shift which are members of \( \mathbb{F}_\infty[S] \) 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 \( S = \text{card} S \) be a prime. Let \( n \) be in \( I_1 \), let \( l \) be a member of \( F(S,n) \) and let there exist \( q \) in \( I_1 \), \( p \) in \( I_1 \), such that \( r_q = o^p \) then \( q \) divides \( p \).

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

It is sufficient to show that \( \phi \) is not expansive. Suppose \( \phi \) is expansive. Then there exists \( \delta > 0 \), such that if \( x \) and \( y \) are members of \( X(S) \) and \( x \neq y \), then there is some integer \( i \) such that \( d(\phi^i(x), \phi^i(y)) > \delta \).

Choose \( k \) in \( I_1 \) with \( i \in \mathbb{R}^+ \). Let \( x \) in \( X(S) \) be defined by \( x_k x_{k+1} x_{k+2} x_{k+3} = 1001 \) and \( x_1 = 1 \) elsewhere. Then \( x \) may be represented as

\[
\begin{array}{llllll}
\text{LX} & \text{R} & L & 11001 & 1 & \text{where} \ 1 \ \text{denotes} \ \text{the} \ \text{left} \\
\text{R} & \text{infinite} \ \text{sequence} \ ... \ L & 1 \ \text{in} \ \text{the} \ \text{right} \ \text{infinite} \ \text{sequence} \\
11 & ... & \text{and} \ \text{"X"} \ \text{indicates} \ \text{the} \ \text{position} \ \text{of} \ x_k.
\end{array}
\]

Now \( \phi(x) = 001100 \),

\[
\begin{array}{llllll}
\text{LX} & \text{R} & L & 110011 & 1 & \text{in the right infinite sequence} \\
\text{R} & \text{infinite} \ \text{sequence} \ ... \ L & 11 & ... & \text{and} \ \text{"X"} \ \text{indicates} \ \text{the} \ \text{position} \ \text{of} \ x_k\text{.}
\end{array}
\]

and \( \phi^3(x) = 110011 \),

\[
\begin{array}{llllll}
\text{LX} & \text{R} & L & 001100 & 1 & \text{in the right infinite sequence} \\
\text{R} & \text{infinite} \ \text{sequence} \ ... \ L & 11 & ... & \text{and} \ \text{"X"} \ \text{indicates} \ \text{the} \ \text{position} \ \text{of} \ x_k\text{.}
\end{array}
\]

and \( \phi^6(x) = 110011 = x \).
Now let \( y \) be the bisquence defined by \( y_i = 1 \), all \( i \) in \( I \). Clearly \( y \neq x \), and for any integer \( n \),
\[
\phi^{2n}(y) = y, \quad \text{while} \quad \phi^{2n+1}(y) = \tilde{y}, \quad \text{where} \quad [\tilde{y}]_i = 0, \quad \text{all} \quad i \quad \text{in} \quad I.
\]

Then \( d(x,y) = \frac{1}{k+2} \),
\[
d(\phi(x),\phi(y)) = \frac{1}{k+3},
\]
\[
d(\phi^2(x),\phi^2(y)) = \frac{1}{k+3},
\]
and \( d(\phi^3(x),\phi^3(y)) = \frac{1}{k+2} \).

Hence for all integers \( i \), \( d(\phi^i(x),\phi^i(y)) < \frac{1}{k+1} \) < \( \delta \).

This contradiction proves that \( \phi \) is not expansive, and so for all non-zero integers \( p \), \( \phi^p \in \mathcal{A}(S) \setminus p(0) \).

The following example show that the map \( \theta \) of Theorem 7.09 need not commute with the shift.

7.15. EXAMPLE. Let \( S = \{0,1\} \). Let \( \delta = 1 \) and \( I = 0 \).

Define \( \theta : x(S) \to x(S) \) as follows:
\[
[\theta(x)]_{2i} = x_{2i+1},
\]
\[
[\theta(x)]_{2i+1} = x_{2i+2}, \quad \text{all} \quad i \quad \text{in} \quad I.
\]

Hence if \( x \) is the bisquence
\[
\cdots x_3 x_2 x_1 x_0 x_1 x_2 x_3 \cdots
\]

then \( \theta(x) \) is
\[
\cdots \tilde{x}_3 \tilde{x}_2 \tilde{x}_1 \tilde{x}_0 \tilde{x}_1 \tilde{x}_2 \tilde{x}_3 \cdots
\]
It is clear that 0 is a well defined map from $X(S)$ onto $X(S)$. The following argument shows that 0 is continuous.

Let $\epsilon > 0$. Choose $k$ in $X$ such that $\frac{1}{k+1} < \epsilon$. Let $\delta = \frac{1}{2k+1}$.

Now $d(x,y) < \delta \Rightarrow x_i = y_i, \quad (-2k < i < 2k), \quad x_{2i+1} = y_{2i+1}, \quad (-k < i < k)$, and

$$\begin{align*}
\| \theta(x) - \theta(y) \| &< k\delta < \epsilon, \\
d(\theta(x), \theta(y)) &< \frac{1}{k+1} < \epsilon.
\end{align*}$$

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

\[ x_1x_2x_3x_4x_5 \ldots \]

while $\phi(x)$ is

\[ \ldots \bar{x}_1 \bar{x}_2 \bar{x}_3 \bar{x}_4 \bar{x}_5 \ldots \]

and it can be seen that $\theta \phi \neq \phi \theta$. Hence $\theta \notin \Phi(S)$. Now if $x \in X(S)$,

$\{ \phi^k(x) \} = x_{1+i}$, all $i$ in $I$, and it may easily be verified that

$$\begin{align*}
[\phi^k(x)]_{2i} &= x_{2i+4}, \\
[\phi^k(x)]_{2i+1} &= x_{(2i+1)+4}.
\end{align*}$$

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 not commute with every member of $\Lambda(S)$. It has, however, been proved by J.P. Ryan, [5] that any continuous, onto transformation of $X(S)$ which commutes with elements of $\Lambda(S)$ is a power
7.17. NOTATION. Let \( n \) be in \( I \). Let \( C = A \circ B \circ \cdots \circ B \) where \( A = A^{(n+1)} \) 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 \( C = A \circ c_{1} \circ \cdots \circ c_{n} \circ B \) is a member of \( C \) the block \( c_{1} \circ \cdots \circ c_{n} \) will be called the control block of \( C \). Let \( H(S,n) \) be the symmetric group on \( S \). For each \( \pi \) in \( H(S,n) \) define \( \gamma_{\pi} \) as in Theorem 7.05. Then \( \gamma_{\pi} \in H(S,n) \). Let \( \Gamma(n) = \{ \gamma_{\pi} : \pi \in H(S,n) \} \).

7.18. THEOREM. Let \( f \) be in \( F(S,n) \) such that \( f_{\infty} \) is onto. Then if \( f_{\infty} \) commutes with all elements of \( \Gamma(n) \), \( f_{\infty} \) 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 \( f_{\infty} \) is onto are the identity map and the map \( g_{x_{0}} \) where \( [g_{x_{0}}(x)]_{i} = x_{i} \). The identity map is \( 0^{0} \), and it may easily be verified that \( g_{x_{0}} \) does not commute with \( \gamma_{\pi} \) if \( \pi \) is the permutation on \( S \) defined by \( \pi(0) = 1, \pi(1) = 0 \). Hence, it may be assumed that \( n \in I \), or \( s > 2 \), or both.

Let \( c_{1} \circ c_{2} \circ \cdots \circ c_{n} \) be a fixed \( n \)-block and let \( C = A \circ c_{1} \circ \cdots \circ c_{n} \circ B \). Let \( x \) be a member of \( X(S) \) such that \( C \) appears in \( x \) with \( x_{0} \circ c_{1} \circ \cdots \circ c_{n-1} \) equal to the central block of \( C \). That is, \( x \) is the bisequence

\[ \vdots \quad \vdots \quad \vdots \quad \vdots \]

Suppose there is no member of \( C \) which appears in \( f_{\infty}(x) \) and has \( [f_{\infty}(x)]_{0} \) as a member of its central block. Then for
every \( \pi \) in \( H(S, n) \), \([ f_\infty \gamma_r(x) ]_0 = [ f_\infty f_\infty(x) ]_0 = [ f_\infty(x) ]_0 \). But then for any \( \pi \), \( f(\pi(c_1 \ldots c_n)) = [ f_\infty \gamma_\infty(x) ]_0 = [ f_\infty(x) ]_0 = \varepsilon(c_1 \ldots c_n) \), which is impossible since \( f_\infty \) 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

\[
\ldots a_0 \, d_1 \, d_2 \ldots a_j \ldots d_n \, \sigma \ldots \n
\]

where \( d_1 \ldots d_n \) is some member of \( R_n(S) \) and \( 1 < j < n \). Then

\[
\text{if } \pi(d_1 \ldots d_n) = e_1 \ldots e_n \text{, since } f_\infty \text{ and } \gamma_r \text{ commute,}
\]

\[
a_j = [ f_\infty f_\infty(x) ]_0 = [ f_\infty \gamma_\infty(x) ]_0 = f(\pi(c_1 \ldots c_n)) \].

The following argument proves that \( c_1 \ldots c_n = d_1 \ldots d_n \). For, suppose this is not true and let \( a_1 \, a_2 \ldots a_n \) be any \( n \)-block. Define \( \pi'(d_1 \ldots d_n) := a_1 \ldots a_n \). Since the map \( f_\infty \) is onto, by Theorem 4.07, \( \text{card } f^{-1}(a) = s^{n-1} \) for any \( a \) in \( S \). Also, either \( s > 2 \) or \( n > 1 \), so that

\[
\text{either } s > 2 \text{ or } n > 1, \text{ if } n > 1 \text{, and } \text{card}(f^{-1}(S - \{ e_j \})) > s^{n-1} > 1, \text{ if } s > 2.
\]

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 \( \pi'(c_1 \ldots c_n) := A \). Then \( \pi' \) can be extended as a permutation on \( R_n(S) \) but \( f(\pi'(c_1 \ldots c_n)) = f(A) \neq e_j \), which contradicts the commutativity of \( \gamma_j \). Hence \( c_1 \ldots c_n = d_1 \ldots d_n \).

Now for any \( n \)-block \( e_1 \ldots e_n \), there is some \( \pi \) 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 \( f_\infty \) is equal to \( \sigma^{j-1} \).
7.19. COROLLARY. The centre of $A(S)$ is $P(S)$.

Proof. Clearly every power of the shift is in the centre of $A(S)$. Let $\phi$ be any continuous onto transformation of $x(S)$ which commutes with all members of $A(S)$. Since $\phi$ commutes with the shift, it follows from Theorem 3.08 that there exist integers $m, n \geq 1$ such that $\phi = \sigma^m \phi_0$, where $f \in \Gamma(S,n)$ and $\phi_0$ is onto. If $\phi$ commutes with every element of $\Gamma(n)$, then $\phi_0$ commutes with all elements of $\Gamma(n)$, whence $\phi_0$ is a power of the shift. It follows that $\phi$ is a power of the shift.

7.20. NOTATION. Let $Z(A(S))$ denote the centre of $A(S)$. For each $\phi$ in $A(S)$ define $T_\phi : A(S) \to A(S)$ by $T_\phi(\theta) = \phi^{-1} \theta \phi$, for all $\theta$ 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


Author: Gordon Susan Eve
Name of thesis: Some Properties And Examples Of Automorphisms On The Bisequence Space. 1976

PUBLISHER:
University of the Witwatersrand, Johannesburg
©2013

LEGAL NOTICES:

Copyright Notice: All materials on the University of the Witwatersrand, Johannesburg Library website are protected by South African copyright law and may not be distributed, transmitted, displayed, or otherwise published in any format, without the prior written permission of the copyright owner.

Disclaimer and Terms of Use: Provided that you maintain all copyright and other notices contained therein, you may download material (one machine readable copy and one print copy per page) for your personal and/or educational non-commercial use only.

The University of the Witwatersrand, Johannesburg, is not responsible for any errors or omissions and excludes any and all liability for any errors in or omissions from the information on the Library website.