Shifts on the Hyperfinite $II_1$ Factor

Geoffrey L. Price*

Department of Mathematics, United States Naval Academy, Annapolis, Maryland 21402

Received June 3, 1997; accepted September 24, 1997

R. T. Powers has constructed a family of unital endomorphisms of the hyperfinite $II_1$ factor $R$. The range of each Powers shift $\sigma$ is a subfactor of index 2 in $R$. A cocycle conjugacy invariant for a Powers shift is its commutant index, i.e., the first index $k$ for which the range of $\sigma^k$ has a nontrivial relative commutant in $R$. Previously we have shown that all Powers shifts of commutant index 2 are cocycle conjugate. In this paper results are obtained on the classification of the cocycle conjugacy classes of Powers shifts of higher commutant index.

0. INTRODUCTION

In [Po] Robert Powers initiated a study into the structure of shift endomorphisms on von Neumann algebras. This study was in part motivated by the work of Vaughan Jones [J] on the index theory for subfactors of the hyperfinite $II_1$ factor. Over the past decade many authors have been attracted to this subject and have achieved remarkable progress on the problem of classifying subfactors of finite index in the hyperfinite $II_1$ factor $R$ (see, for example, the references in [GHJ, Pa]). The study of shifts on $R$ may also be viewed as an approach to the study of the subfactors of $R$. In this approach one uses a *-endomorphism $\sigma$ of $R$ to construct a sequence $R_i$ of subfactors of $R$ with the properties that $R_i$ contains $R_{i+1} = \sigma(R_i)$ for each non-negative integer $i$, and the Jones index $[R_i; R_{i+1}]$ is independent of $i$. Appropriating the notion of outer conjugacy from the study of automorphisms of factors, [Co], we say that a pair $\sigma$, $\tau$ of *-endomorphisms of $R$ are cocycle conjugate (see Section 1) if there exists a unitary element $U$ of $R$ such that $\sigma = \text{Ad}(U)$ and $\tau$ are conjugate. Then one sees that cocycle conjugacy is akin to the conjugacy of the subfactors in the sequences $\{\sigma(R)\}$ and $\{\tau(R)\}$ being implemented in a compatible way. This notion is employed in [L], where a canonical *-endomorphism is constructed via modular maps related to Jones tunnels of subfactors.

* Supported in part by a grant from the National Security Agency and a United States Naval Academy Recognition Grant.
In [1], however, the minimal Jones index \([ R : \sigma(R) ]\) of a canonical \(+\)-endomorphism is 4. Here we continue our study of a class of \(+\)-endomorphisms whose index is 2, which we call binary shifts. The construction of these shifts may be viewed as a generalization of a construction used by Jones [J] to generate subfactors of a prescribed index. These shifts are also intimately related to the structure and theory of linear recurring sequences, a major branch of study in the field of cryptology. Recently, binary shifts have been used to construct interesting examples of automorphisms of Connes–Stormer entropy 0. In particular, examples of this sort have provided counterexamples to the longstanding conjecture that the Connes–Stormer entropy is additive under the operation of tensor product, [NST].

In this paper we assemble most of the results which have been obtained on the theory of binary shifts (with the exception of entropy, see [C1, C2, NST, NT, Pr2, and Y]). This paper may therefore be read without referring to earlier papers on the subject. We also present a new result on the cocycle conjugacy classes of binary shifts, which is a significant generalization of a recent result which classified the cocycle conjugacy classes of binary shifts of minimal commutant index [Pr].

1. PRELIMINARY RESULTS AND CONJUGACY OF BINARY SHIFTS

We say that a \(+\)-endomorphism \(\sigma\) of the hyperfinite \(II_1\) factor \(R\) is a shift if \(\sigma\) satisfies the range property \(\cap_n \sigma^n(R) = C.I.\). Obviously the range of \(\sigma\) must be a proper subfactor (which is isomorphic to \(R\)). Perhaps the most straightforward way to construct examples of shifts is to view \(R\) as the completion, in the GNS representation associated with the normalized trace, of the UHF algebra \(\otimes M_n(\mathbb{C})\) of type \(n^n, n \geq 2\). Then the mapping \(\sigma(A) = I_n \otimes A\) is a shift on \(R\). The Jones index of the subfactor is \(n^2\), and it is not difficult to show that the range \(\sigma(R)\) has relative commutant in \(R\) isomorphic to the algebra \(M_n(\mathbb{C})\) of \(n\) by \(n\) matrices. In this paper we study shifts \(\sigma\) on \(R\) for which \(\sigma(R)\) has Jones index 2, i.e., \([ R : \sigma(R) ] = 2\) (see [J]). By an abuse of terminology we shall say that the \(+\)-endomorphism itself has index 2. Unlike the class of examples just described, \(\sigma(R)\) must have trivial relative commutant, and as we shall see below, Theorem 5.8, there exist examples of shifts of index 2 for which the range of \(\sigma^k\) has trivial relative commutant for any \(k\) in \(\mathbb{N}\). This behavior is in marked contrast to the situation where \(\sigma\) is a shift on a Type I factor \(M\), in which \(\sigma(M)\) and its relative commutant generate \(M\).

The notions of conjugacy and outer conjugacy are central to the classification theory of automorphisms of the hyperfinite \(II_1\) factor (see [Co]), and motivate the following definitions which pertain to unital \(+\)-endomorphisms of \(R\).
**Definition 1.1.** A pair $\sigma$ and $\beta$ of unital $*$-endomorphisms of $R$ are conjugate if there exists an automorphism $\gamma$ of $R$ such that $\gamma \cdot \sigma = \beta \cdot \gamma$.

**Definition 1.2.** A pair $\sigma$ and $\beta$ of unital $*$-endomorphisms on $R$ are cocycle conjugate if there exists a unitary element $W$ in $R$ such that $\sigma = \text{Ad}(W)$ and $\beta$ are conjugate.

Some care must be exercised in the use of the second definition. In some instances for example, there may exist unitary elements $W$ and $U$ and a shift $\lambda$ such that the elements $\sigma^k(U)$, $k \in \mathbb{Z}^+$, generate $R$, whereas if $\rho$ is the $*$-endomorphism $\sigma \cdot \text{Ad}(W)$, $\{\rho^k(U): k \in \mathbb{Z}^+\}$ may be finite dimensional.

**Proposition 1.1.** The Jones subfactor index $[R: \sigma(R)]$ is a conjugacy invariant.

Proof. Suppose $\zeta$ and $\eta$ are conjugate shifts. Then the subfactors $\sigma(R)$ and $\beta(R)$ of $R$ are conjugate. But then [1, Prop. 2.1.7] $\zeta(R)$ and $\eta(R)$ have the same subfactor index in $R$.

The proof of the following is similar.

**Proposition 1.2.** The Jones subfactor index $[R: \sigma(R)]$ is a cocycle conjugacy invariant.

There is another numerical index for shifts which is both a conjugacy and a cocycle conjugacy invariant. This is the least positive integer $k$ such that $\sigma^k(R) \cap R$ is nontrivial, which we shall call the commutant index of $\sigma$. We shall return to this notion in Section 5 where we give a detailed account of the relationship between the commutant index and a periodicity condition for our main object of study, the binary shifts on $R$ (Theorem 5.8).

Next we describe some of the notions which occur in the theory of index for subfactors and which are relevant to our study of shifts of index 2. The reader is referred to [J] (cf. also [Gd]). If $N \subset R$ is a subfactor of index 2 in $R$, then there is a hermitian unitary element $S$ in $R$ such that $R = \{ A + BS: A, B \in N \}$. In particular, $\text{Ad}(S)$ restricts to a period 2 (outer) automorphism of $N$. Note that $S$ is not unique: if $U$ is unitary and $S = USU^*$, for example, then $S'$ and $N$ also generate $R$. Let $\Phi$ be the conditional expectation from $R$ to $N$. Then the linear mapping $\theta = 2\Phi - I$ is an automorphism of $R$. Note that $\theta(S) = -S$ and that $\theta$ fixes $N$. Hence $\theta$ is itself a period 2 automorphism, which satisfies $\theta(A) = A$ if and only if $A \in N$. If $P \subset N \subset M$ are factors, $[M:N][N:P] = [M:P]$. Either $[M:N] = 1$, in which case $N = M$, or $[M:N] \geq 2$. It then follows, for shifts of index 2, that for $k, n \in \mathbb{Z}^+$, $[\sigma^k(R) : \sigma^{k+n}(R)] = 2^n$. If $R$ is the hyperfinite $I_1$ factor and if $[R:N] < 4$, the relative commutant $N' \cap R$ is trivial. If $[R:N] = 4$, either $N' \cap R$ is trivial or is generated by a hermitian unitary element, hence has dimension 2.
In particular, if \([ R: N] = 4\) and \(E \in N' \cap R\) is a projection, then the trace \(\text{tr}\) on \(R\) satisfies \(\text{tr}(E) = 0, 1/2, \) or \(1\).

**Definition 1.3.** A shift \(\alpha\) on \(R\) is called a binary shift (or Powers shift) if there is a unitary \(U \in R\) satisfying the following requirements.

(i) \(U^\alpha = I\),

(ii) \(U^\alpha(U^{-1}) = \pm \alpha^k(U)\),

(iii) \(R = \{ U, \alpha(U), \alpha^2(U), ... \}^\star\).

The unitary \(U\) is called an \(\alpha\)-generator of \(R\). We will show that if \(\alpha\) is a binary shift of \(R\) and \(U, V\) are both generators, then \(U = V\), Theorem 1.7.

Theorem 1.8 shows that the anticommutation set \(S = \{ k \in \mathbb{Z}^+ : U^\alpha_k \neq U^\alpha_l \} \) is a complete conjugacy invariant.

**Example 1.** An example of a binary shift may be constructed using the sequence of Jones projections \(\{ e_i : i \in \mathbb{Z}^+ \}\) which satisfy the identities [J, Theorem 4.1.1]

\[ e_i e_{i+1} e_i = 1/2 e_i, \quad (1.1.1) \]

Let \(u_i, i \in \mathbb{Z}^+\), be the hermitian unitaries \(2 e_i - I\). From the equation above it is straightforward to show that

\[ u_i u_j = \begin{cases} -u_j u_i, & \text{if } |i - j| = 1, \\ u_i u_j, & \text{otherwise}. \end{cases} \quad (1.1.2) \]

Since the \(e_i\)'s generate \(R\), so of course do the \(u_i\)'s. Let \(\tau\) be the \(\ast\)-endomorphism on \(R\) which is induced from the mapping \(\tau(u_i) = u_{i+1}, i \in \mathbb{Z}^+\). This is done by extending to linear combinations of (finite) words in the \(u_i\)'s in the obvious way. It is not difficult to show that \(\tau\) is a shift on \(R\) of index 2, with \(\tau\)-generator \(U = u_0\) and with \(u_i = \tau^i(U)\). From (1.1.2) it follows that the relative commutant of \(\tau^2(R)\) is nontrivial and is generated by \(u_0\), so \(\tau\) is a shift of commutant index 2. Corollary 7.13 shows that all binary shifts of commutant index 2 are cocycle conjugate to this shift.

**Definition 1.4.** The normalizer \(N(\alpha)\) of a unital \(\ast\)-endomorphism \(\alpha\) of \(R\) is the subgroup of the unitary group \(\mathbb{V}(R)\) consisting of those elements \(W\) for which \(\text{Ad}(W)\) preserves \(\alpha^k(R)\) for all \(k\).

The following results (which appear in [Po]) give a characterization of \(N(\alpha)\). Before stating these results it will be helpful to set down the following notation. If \(\alpha\) is a binary shift with generator \(U\) then for \(j \in \mathbb{Z}^+\) set \(u_j = \alpha^k(U)\). Then the anticommutation set as above is the set \(S = S_\alpha = \{ k \in \mathbb{Z}^+ : u_0 u_k = -u_k u_0 \}\). For finite subsets \(Q = \{ q_0, ..., q_n \}\) of \(\mathbb{Z}^+\), with \(q_0 < \cdots < q_n\),
define $U(Q) = U(q_0, ..., q_n) = u_{q_0}u_{q_1} \cdots u_{q_n}$. Set $U(\emptyset) = I$. Observe that for a pair of finite subsets $Q, Q'$ of $\mathbb{Z}^+$,

$$U(Q) \cap U(Q') = \pm U(QAQ'),$$

where $QAQ'$ is the symmetric difference.

**Lemma 1.3.** If $Q \subset \mathbb{Z}^+$ is nonempty and finite, then $\text{tr}(U(Q)) = 0$.

**Proof.** We shall show that there is a $u_i$ which anticommutes with $U(Q)$. If this were false then $U(Q)$ would lie in the center of $R$, and therefore we would have $U(Q) = u_0u_1 \cdots u_n = \pm I$. Multiplying both sides of this equation on the right by $u_{a_i}$ shows that $u_{a_i}$ may be expressed in terms of $u_0, ..., u_{a_i-1}$. It then follows that for all $m \geq q_0, u_m$ may be expressed in terms of the first $q_0$ generators. But this leads to the conclusion that $R$ is finite-dimensional. Hence by contradiction we have $u_i U(Q) u_i = - U(Q)$ for some $i$. Taking the trace gives $\text{tr}(U(Q)) = \text{tr}(u_i U(Q) u_i) = - \text{tr}(U(Q))$, giving the result. 

**Lemma 1.4.** Suppose $Q$ is a nonempty subset of $\{0, 1, ..., n\}$ for some $n \in \mathbb{Z}^+$. Then $\text{tr}(U(Q) x^n u_i(A)) = 0$ for all $A \in R$.

**Proof.** Any element in $x^n u_i(R)$ may be realized as the strong limit of linear combinations of words of the form $U(Q')$, where $Q' = \emptyset$ or is a finite subset of $\{n+1, n+2, \ldots\}$. Since $QAQ' = Q \cup Q'$, $U(Q) U(Q') = \pm U(Q \cup Q')$. By the preceding lemma, $\text{tr}(U(Q) U(Q')) = 0$, so $\text{tr}(U(Q) x^n u_i(A)) = 0$ for all $A \in R$.

**Lemma 1.5.** Let $\theta$ be the period 2 automorphism of $R$ given by $\theta = 2\Phi - I$, where $\Phi$ is the conditional expectation from $R$ to $\pi(R)$. Then for finite subsets $Q \subset \mathbb{Z}^+$, $\theta(U(Q)) = -\pm U(Q)$ if $0 \in Q$, and $\theta$ fixes $U(Q)$ otherwise.

**Proof.** If $0 \notin Q$ then $\pi(Q) \in \pi(R)$ and so is fixed by $\theta$. Suppose $0 \in Q$, then $\pi(U(Q)) = 0$, so $\theta(U(Q)) = -\pm U(Q)$.

**Theorem 1.6.** A unitary element $W$ lies in the normalizer $N(x)$ of $\pi$ if and only if it is a scalar multiple of $U(Q)$ for some finite subset $Q$ of $\mathbb{Z}^+$.

**Proof.** It is clear from the anticommutation relations in the definition of a binary shift above that any element $W = U(Q)$ either commutes or anticommutes with the shifts $x^k(U)$ of the generator $U$, and so must lie in $N(x)$.

Suppose $W \in N(x)$, then $\text{Ad}(W)$ restricts to an automorphism of $\pi(R)$ i.e., there exists $\gamma \in \text{Aut}(R)$ such that for all $A$ in $R$, $W\pi(A) W^{-1} = \pi(\gamma(A))$. Applying $\theta$ to this equation yields $\theta(W) \pi(\gamma(A)) \theta(W^{-1}) = \theta(\pi(\gamma(A))) = \pi(\gamma(A))$, so that $W^{-1}\theta(W) \in \pi(R) \cap R$. Since this algebra is trivial we have
$W^{-1}(W) = \lambda I$, for some $\lambda \in \mathbb{C}$, so that $\theta(W) = \lambda W$. Since $\theta \cdot \theta = \text{Id}$, either $\lambda = 1$ or $\lambda = -1$.

For convenience set $u_k = \alpha^k(U), k \in \mathbb{Z}^+$. We claim there is a unique element $W_1 \in N(\alpha)$ such that either $W = u_k \alpha(W_1)$ or $\alpha(W_1)$. If $\theta(W) = W$ then $W \in \alpha(R)$; Setting $W = \alpha(W_1)$, it is straightforward to show that $W_1 \in N(\alpha)$. Otherwise, $\theta(W) = -W$ so $\theta(u_k W) = u_k W$ and therefore $u_k W = \alpha(W_1)$ for some $W_1 \in R$. Hence $W = u_k \alpha(W_1)$, and since $u_k$ and $W$ are in $N(\alpha), W_1 \in N(\alpha)$ also. In either case we have $W = u_k \alpha(W_1)$. Arguing for $W_1$ as for $W$, one has $W_1 = u_k \alpha(W_2)$, so that $W = u_k \alpha(W_3)$. Continuing in this fashion leads, for any $n \in \mathbb{N}$, to the expression $W = u_0 \alpha^k \cdots \alpha_{n-1}^k(W_n)$. We prove that for sufficiently large $n$, $W_n$ must be a scalar multiple of the identity. For if not, let $U(Q)$ be any word in $R$, and choose $n$ greater than $\max\{q; q \in Q\}$. Since $W_n \in N(\alpha)$ and since it is nontrivial, we argue as above to conclude that there is a $j \in \mathbb{Z}^+$ such that $W_n = u_j \alpha_{j+1}(Y)$, for some $Y \in R$, so that $W = u_0 \alpha^{k_1} \cdots \alpha^{k_{n-1}}(Y)$. Since $n + j \notin Q$, applying Lemma 1.4 shows that $\text{tr}(U(Q) W) = 0$. But since linear combinations of words are dense in $R$, we have $\text{tr}(AW) = 0$ for all $A \in R$, a contradiction. Hence $W_n$ is trivial for some $n$, and we are done.

**Remark 1.1.** We refer the reader to [PP2, Theorem 3.7] where Powers and the author have given a characterization of the elements which lie in the normalizer of $N(\alpha)$ (see also Theorem 7.8), i.e., of those unitary elements $V$ which satisfy $VN(\alpha)V^{-1} \subseteq N(\alpha)$. In that paper we conjectured that a pair of binary shifts are cocycle conjugate if and only if one can find a unitary $V$ which normalizes the group $N(\alpha)$ such that $\alpha \cdot \text{Ad}(V)$ and $\beta$ are conjugate. The conjecture holds for those pairs of binary shifts having commutant index 2, (cf. Corollary 7.13).

**Theorem 1.7.** Suppose $\alpha$ is a binary shift with $\alpha$-generators $U$ and $V$. Then either $U = V$ or $U = -V$.

**Proof.** Since $U$ and $V$ are $\alpha$-generators they lie in $N(\alpha)$. From the previous theorem $V$ may be expressed in the form $\lambda_1 U^{a_1} \alpha(U)^{b_1} \cdots \alpha(U)^{b_k}$ and $U$ may be written as $\lambda_2 V^{a_2} \alpha(V)^{b_2} \cdots \alpha(V)^{b_n}$. Combining these expressions gives a representation of $U$ in terms of itself and its shifts $\alpha(U)$. By an application of Lemma 1.3 this representation could hold only if $U = \lambda V$. Since $U$ and $V$ are hermitian, $\lambda = \pm 1$.

In Theorem 4.2 we shall determine which subsets of $\mathbb{Z}^+$ arise as anticommutation sets $S(\alpha)$ for binary shifts. The following result uses the $S(\alpha)$'s to determine the conjugacy classes of these shifts.

**Theorem 1.8.** A pair of binary shifts are conjugate if and only if they have the same anticommutation sets.
Proof. If \( U \) is an \( \alpha \)-generator and \( \beta = \gamma \circ \alpha \circ \gamma^{-1} \) then \( \gamma(U) \) is a \( \beta \)-generator. It follows easily that \( S(\alpha) = S(\beta) \). Conversely, suppose \( S(\alpha) = S(\beta) \). Let \( U \) be an \( \alpha \)-generator and let \( V \) be a \( \beta \)-generator. Then the mapping \( (\beta^k(U)) = \gamma(\alpha^k(U)), k \in \mathbb{Z}^+ \), can be extended to an automorphism on \( R \) and \( \beta = \gamma \circ \alpha \circ \gamma^{-1} \).

2. TOEPLITZ MATRICES OVER FINITE FIELDS OF CHARACTERISTIC 2

This section is devoted to establishing some results about the structure of Toeplitz matrices over finite fields of characteristic 2. Of particular importance is the unimodality property governing the ranks of sequences of related Toeplitz matrices, Corollary 2.10. We shall use this result, as well as some results on congruence of sequences of Toeplitz matrices over the field \( F = \mathbb{Z}/2\mathbb{Z} \), as a means of establishing our main results on the cocycle conjugacy of binary shifts, viz., Theorem 7.12 and Corollary 7.13.

By a Toeplitz matrix \( T_n \) over a finite field \( K \) we shall mean a matrix of the form

\[
\begin{bmatrix}
a_0 & a_1 & a_2 & \cdots & a_{n-2} & a_{n-1} \\
a_1 & a_0 & a_2 & \cdots & a_{n-3} & a_{n-2} \\
a_2 & a_1 & a_0 & \cdots & a_{n-4} & a_{n-3} \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_1 & a_0
\end{bmatrix}
\]

with entries \( a_0, a_1, \ldots, a_{n-1} \) in \( K \), and with \( a_0 = 0 \). (The reader should be aware that this terminology is not used consistently in the literature. The term Toeplitz matrix is usually used to refer to semi-infinite matrices which correspond to a Toeplitz operator on a separable Hilbert space, [BH, GS]. In this case, of course \( K = \mathbb{C} \).) Although we specialize in this section to the situation in which \( K \) has characteristic 2, our motivation is drawn from the situation in which \( K = F \), the field of 2 elements, and the entries of the matrix \( T_n \) correspond to the anticommutation set of a binary shift \( \pi \), where \( a_i = 1 \) if \( i \in S(\pi) \) and \( a_i = 0 \) otherwise. In this setting it is quite straightforward (see Lemma 3.3 and Theorem 3.4) to make a connection between the nullity of the matrices \( T_n \) and the dimension the centers \( Z_n \) of the algebras \( B_n(\pi) \). In fact, we shall see that if null(\( T_n \)) = \( v_n \), then \( \dim Z_n = 2^v_n \), and so a computation of the sequence \( \{v_n : n \in \mathbb{Z}^+\} \) is a key step towards the determination of the Bratteli diagram corresponding to the \( AF \)-algebras \( \mathcal{H}(\pi) \), Theorem 3.5. In this way we also obtain detailed information about the words (in the generators \( u_i \)) which lie in the centers \( Z_n \) of \( \mathcal{H}(\pi) \). The nullity sequence
{v_n; n ∈ ℤ^+} exhibits a rather remarkable unimodality property, shown in Corollary 2.10. We believe this result to be new, although related to earlier work of Iohvidov and others [I] on the structure of Toeplitz matrices over fields of characteristic 0.

The results on the ranks of Toeplitz matrices presented in this section generalize those which appear in Section 5 of [PP2], (see also [CP]).

A pair $A$ and $B$ of $n \times n$ matrices over a field $K$ are said to be congruent if there exists an invertible matrix $U$ such that $A = U'BU$ ($U'$ is the transpose of $U$). The notion of congruence is easily seen to be an equivalence relation, and has numerous applications in number theory and classical matrix theory, [N]. In particular, let $(\cdot, \cdot)_A$ be the quadratic form on $K^n$ satisfying $(x, y)_A = x'Ay$ for vectors $x, y \in K^n$. Congruent matrices yield equivalent quadratic forms [N, Section IV.2]. In this section we present some well-known results on the congruence of matrices over the field $F$. In Section 7 we shall use these results as a key to determining some cocycle conjugacy classes of binary shifts on the hyperfinite $II_1$ factor. Unfortunately, the usual proofs used in establishing results on congruence of matrices do not provide information about the implementing matrices $U$ which is quite as detailed as we require for our purposes, so we shall be giving a largely self-contained presentation of these results, tailored to our applications.

Unless otherwise noted, we will make the standing assumption in this section that the diagonal entries $a_0$ of the Toeplitz matrices are 0.

We begin by establishing some preliminary results on the rank of the $T_n$’s. Before doing so, we introduce the following notation and terminology. We number the rows and columns of an $n$ by $n$ matrix so the initial row is the zeroeth row, the last row is the $(n-1)$th row, and similarly for the columns. Then for any $i \neq j$ between 0 and $n-1$, and $\zeta \in K$, let $E_{ij}(\zeta)$ be the matrix, usually referred to as an elementary transformation matrix, having 1’s along the main diagonal, $\zeta$ in the $(i, j)$ position, and 0’s elsewhere. Note that $AE_{ij}(\zeta)$ is the matrix obtained from $A$ by adding $\zeta$ times column $j$ of $A$ to column $i$ of $A$, and $E_{ij}(\zeta)A$ is obtained from $A$ by adding $\zeta$ times row $j$ to row $i$ of $A$. If $\zeta$ is 1 then we shall write $E_{ij}(\zeta) = E_{ij}$. The following result is obvious.

**Lemma 2.1.** Let $K$ be a field of characteristic 2. Then

(i) the transpose $E_{ij}(\zeta)'$ of $E_{ij}(\zeta)$ is $E_{ji}(\zeta),$

(ii) $E_{ij}(\zeta)^{-1} = E_{ji}(\zeta).

**Lemma 2.2.** If $A$ and $B$ are congruent matrices then they have the same rank.

**Proof.** This is obvious since the implementing matrix $U$ is required to be invertible. ■

Codes: 3293 Signs: 2607 . Length: 45 pic 0 pts, 190 mm

128 GEOFFREY L. PRICE
Lemma 2.3. If \( A \) is a symmetric matrix then so is any matrix which is congruent to \( A \).

Proof. \((U^tAU)^t = U^tA^tU = U^tAU\).

Proposition 2.4 ([N, Theorem IV.11]). A symmetric matrix \( A \in M_n(K) \) with 0 diagonal has even rank.

Proof. The result is trivial if \( a_0 = a_1 = \cdots = a_{n-1} = 0 \). Otherwise, let \( a_j = \zeta \) be the first nonzero entry element. If \( j > 1 \) the matrix \( B = E_{ij}(\zeta^{-1})^tAE_{ij}(\zeta^{-1}) \) is easily seen to have \([1 \ 0] \) as its upper left corner. If \( \zeta \) is the entry in the \((0,k)\) position of \( B \), for \( k > 1 \), let \( \delta_1 \) be the product of elementary transformations \( \delta_1 = \prod_{k=2}^n E_{ik}(\zeta) \). Then \( B \) is congruent via the product \( \delta_1 \) to a (necessarily symmetric and 0 diagonal) matrix with initial row \([0 \ 1 \ 0 \cdots 0] \). Similarly, there is a product \( \delta_0 \) of elementary transformations of the form \( E_{0k}(\zeta^{-1}), k > 1 \), such that \( \delta_1^tB\delta_1 \) is congruent via \( \delta_0 \) to a matrix with row 1 equal to \([1 \ 0 \cdots 0] \). Then \( A \) has rank equal to 2 (the rank of its upper 2 by 2 corner) plus the rank of the \((n-2) \times (n-2) \) matrix in the lower-right corner of \( \delta_0^tB\delta_1 \). The result follows by induction.

It will be useful to have the following terminology and notation. For any \( n \in \mathbb{N} \), let \( K^n \) denote the vector space of column vectors of length \( n \) over \( K \). Given a matrix \( A \) with entries in \( K \), the word kernel shall be used to refer to the right kernel of \( A \). If \( k \in K^n \), let \( \tilde{k} \) be the column vector obtained by reversing the order of the entries of \( k \). The new vector is called the flip of \( k \). Let \( \delta k \in K^{n+1} \) be the vector obtained by adjoining a final entry of 0 to \( k \). If \( k = [k_0, \ldots, k_n]^t \) is a vector with \( k_n = 0 \), then \( \delta k \), the shift of \( k \), is the vector \([0, k_0, \ldots, k_n] \) (of the same length as \( k \)). Finally, if \( T_n \) is the Toeplitz matrix above, we use the notation \( \rho_n \) and \( \nu_n \) to denote its rank and nullity, respectively.

Corollary 2.5. Let \{\( a_i : i \in \mathbb{Z} \)\} be a sequence in a field of characteristic 2, with \( a_0 = 0 \). Let \{\( T_n \)\} be the corresponding sequence of Toeplitz matrices. Either \( \rho_{n+1} = \rho_n \) or \( \rho_{n+1} = \rho_n + 2 \).

Proof. Obvious, since \( \rho_{n+1} \) must be even.

Lemma 2.6. A vector \( k \) lies in the kernel of \( T_n \) if and only its flip does.

Proof. This follows from the fact that for any \( j = 0, 1, \ldots, n-1 \), the \( j \)th row from the top of \( T_n \) is the flip of the \( j \)th row from the bottom.

Lemma 2.7. Suppose the Toeplitz matrix \( T_n \) has full rank. Then \( \nu_{n+1} = 1 \), and \( \ker(T_{n+1}) \) is spanned by a single vector \( k = [k_0, \ldots, k_n] \) such that \( k_0 \neq 0 \), \( k_n \neq 0 \), and such that \( k = ek \) for some nonzero scalar \( e \) in \( K \).
Proof. Since $T_n$ has full rank, $\rho_n = n$. Since $\rho_{n+1} \leq n+1$, and since $T_{n+1}$ must have even rank, $\rho_{n+1} = n$. Hence $v_{r+1} = 1$ so that there is a nonzero vector $k$ spanning $\ker(T_{n+1})$. By the previous lemma, $k \in \ker(T_{n+1})$, so $k$ must be a scalar multiple of $k$. Hence $k_0 = 0$ if and only if $k_{n} = 0$. But if $k_0 = 0 = k_n$, it is obvious that the vector obtained by deleting the first entry of $k$ is in $\ker(T_n)$, which contradicts the assumption that $T_n$ has full rank.

Lemma 2.8. If $\rho_n = \rho_{n+1}$ for some $n \in \mathbb{Z}^+$, then $\theta(\ker(T_n)) \subset \ker(T_{n+1})$.

Proof. If the hypotheses hold, the last row of $T_{n+1}$ is in the linear span of the first $n$ rows of the matrix. If $k \in \ker(T_n)$ then $\theta k$ annihilates the first $n$ rows of $T_{n+1}$. But since the last row of $T_{n+1}$ is in the span of the first $n$ rows, $\theta k$ also annihilates the last row.

Theorem 2.9. If $\rho_n < \rho_{n+1} < n+1$, then $\rho_{n+1} < \rho_{n+2}$.

Proof. Since $\rho_{n+1} < n+1$, $\ker(T_{n+1})$ is nontrivial. We show that any $k = [k_0, ..., k_{n+1}]$ in $\ker(T_{n+1})$ has first and last entries 0. For suppose $k_{n+1} \neq 0$, then from $T_{n+1}k = 0$ it follows that $k' = k_{n+1} = 0$. Hence the first $n$ entries $[a_{n+1}, ..., a_1]$ of the last row of $T_{n+1}$ is a vector in the span of the rows of $T_n$. But from this it would follow that $\theta \ker(T_n)$ is a subspace of $\ker(T_{n+1})$, so that $v_{n+1} \neq v_n$. This is false, however, since $\rho_n + v_n + 1 = n + 1 = n_{n+1} + v_{n+1} = (\rho_n + 2) + v_{n+1}$, using the hypotheses and the corollary above. Hence $k_{n+1} = 0$ for all $k \in \ker(T_{n+1})$. Since $\ker(T_{n+1})$ is invariant under the flip, $k_0 = 0$ also.

Now choose a vector $k \in \ker(T_{n+1})$ such that the position of its first nonzero entry occurs at or before the position of the first nonzero entry of any other nontrivial vector in $\ker(T_{n+1})$. Suppose $\rho_{n+2} = \rho_{n+1}$. Then by the previous lemma, $\theta \ker(T_{n+1}) \subset \ker(T_{n+2})$. Let $(\theta k)'$ be the vector in $K^{n+2}$ obtained by deleting the first entry of $\theta k$. Since $\theta k \in \ker(T_{n+2})$ it is clear that $(\theta k)'$ lies in $\ker(T_{n+1})$, which contradicts the assumption made about the position of the first nonzero entry of $k$. From this contradiction it follows that $\rho_{n+2} > \rho_n$.

Corollary 2.10. (Unimodality) The nullity sequence $\{v_n = \text{null}(T_n) : n \in \mathbb{Z}^+\}$ is unimodal in the sense that it satisfies one of the following properties: Either

(i) there exists a sequence of positive integers $\{m_i\}$ such that $\{v_n\}$ is the concatenation of strings of the form 1, 2, ..., $m_i - 1$, $m_i$, $m_i - 1$, ..., 1, 0, or,

(ii) $\{v_n\}$ consists of finitely many strings of the form above, followed by the sequence 1, 2, 3, ...
Condition (ii) holds if and only if the doubly-infinite sequence \( \{ \ldots, a_2, a_1, a_0, a_1, a_2, \ldots \} \) is periodic.

**Proof.** That either condition (i) or (ii) holds is clear from the theorem. Suppose the doubly-infinite sequence above is periodic. By use of a straightforward generalization of the proof of Theorem 4.1, in which the field \( F \) is replaced with any field \( K \) of characteristic 2, there is a \( q \in \mathbb{N} \) and a vector \( k = [k_0, k_1, \ldots, k_{q-1}]^t \) such that the sequence of Toeplitz matrices \( \{ T_k \} \) has scalar product 0 with any \( q \) consecutive entries of the sequence. From this it follows that for any \( j \in \mathbb{Z}^+ \) the vector \( \theta^j k \) is a scalar multiple of \( k \). But then by Corollary 2.10, the doubly-infinite sequence is obviously periodic. If \( q > 0 \), \( \rho_q \) is a sequence of non-negative integers satisfying either of the unimodality conditions in the statement of the corollary. From this it follows that for any \( j \) the corresponding \( \rho_{q+j} \) satisfies \( \rho_{q+j} = \rho_q \) (cf. \([PP2, Corollary 6.7]\)), and therefore \( \rho_q \) must have scalar product 0 with any \( q + 1 \) consecutive elements of the flipped sequence \( a_q, a_{q+1}, a_1, a_0, a_1, a_2 \). Then by repeated applications of Lemma 2.8, the vector \( \theta^j k \in \ker(T_{q+j}) \), for all \( j \geq 1 \). Hence \( k \) has scalar product 0 over \( K \) with any \( q + 1 \) consecutive elements of the sequence \( a_q, a_{q+1}, a_1, a_0, a_1, a_2 \). On the other hand the flip of \( k \) is a scalar multiple of \( k \), and therefore \( k \) must have scalar product 0 with any \( q + 1 \) consecutive elements of the flipped sequence \( a_q, a_{q+1}, a_1, a_0, a_1, a_2 \). But then \( k \) has scalar product 0 with any \( q + 1 \) consecutive entries of the doubly-infinite sequence in the statement of the corollary. From this observation it follows easily (see, e.g., \([LN, Section 6.1]\)) that the doubly-infinite sequence is periodic. \( \square \)
Suppose then that \( n \in \mathbb{N} \) is such that \( v_n = 0, v_{n+1} = 1, \) and \( v_k = \mu_k \) for \( 1 \leq k \leq n+1. \) There are two cases to consider in order to complete the argument.

**Case (i).** There is a \( q \in \mathbb{N} \) such that \( \mu_{n+j} = j \) for \( 1 \leq j \leq q, \) and \( \mu_{n+q+j} = q - j \) for \( 1 \leq j \leq q. \)

By Lemma 2.7 a single vector \( \mathbf{k}, \) whose first and last entries \( k_0 \) and \( k_n \) are nonzero, spans \( \ker(T_{n+1}). \) Then for \( j = 1, 2, ..., q^{-1} \) we may choose, successively, terms \( a_{n+j}, \) such that \( \mathbf{k} \) has scalar product 0 over \( K \) with the vectors \([a_j, ..., a_{n+j}].\) Using the fact from the same lemma that \( \mathbf{k} \) and its flip are scalar multiples of each other, it is not difficult to show that for fixed \( j, \theta^{-1} \mathbf{k} \) and its shifts, \( \theta^j \mathbf{k}, \overrightarrow{\theta^j} \mathbf{k}, ..., \theta^j \mathbf{k}, \overrightarrow{\theta^j} \mathbf{k}, \) all lie in \( \ker(T_{n+j}). \)

Hence the nullities \( v_{n+j} \) satisfy the inequalities \( v_{n+j} \geq j. \) But since \( v_{n+1} = 1, v_{n+j} \leq j, \) so \( v_{n+j} = j, \) \( \rho_{n+j} = n. \) Now choose \( a_{n+q+1} \) such that \( \mathbf{k} \) has nonzero scalar product with \([a_{q+1}, ..., a_{n+q+1}].\) This is always possible to arrange since \( k_n \neq 0. \) But then the vector \([0, 0, k_0, ..., k_n] = \mathcal{T}^q \mathbf{k} \) is not in \( \ker(T_{n+q+1}) \), hence neither is its flip, \([k_n, ..., k_0, 0, ..., 0]^\top \) and since \( \mathbf{k} \) and its flip are scalar multiples of one another, neither is \([k_0, ..., k_n, 0, ..., 0]^\top \) in \( \ker(T_{n+q+1}). \) Hence \( \theta(\ker(T_{n+q})) \) is not contained in \( \ker(T_{n+q+1}). \) and therefore, by Lemma 2.8, \( \rho_{n+q} \neq \rho_{n+q+1}. \)

If \( \mu_n = 0 \) for infinitely many \( n \in \mathbb{N} \) then we may continue to fill out the sequence \( \{a_j\} \) so that \( v = \mu. \) Otherwise, there is a last \( n \in \mathbb{N} \) such that \( \mu_n = 0, \) so that we turn to the following case.

**Case (ii).** \( \mu_{n+j} = j \) for all \( j \in \mathbb{N}. \)

As above there is a single vector \( \mathbf{k} \) spanning the \( \ker(T_{n+1}) \) and which has nonzero first and last entries. This time we choose terms \( a_{n+j} \) successively such that \( \mathbf{k} \) has 0 scalar product with \([a_j, ..., a_{n+j}].\) Then for all \( j \) we may argue as above to show \( v_{n+j} = j = \mu_{n+j}, \) so that \( v = \mu. \) Hence we have established the following.

**Theorem 2.11.** Given any unimodal sequence \( \mu \) of non-negative integers (as in the corollary above) there is a sequence \( \{a_j\} \) in \( K, \) with \( a_0 = 0, \) such that the corresponding sequence \( \{T_n\} \) of Toeplitz matrices has nullity sequence \( v = \{v_n\} \) coinciding with \( \mu. \)

In [CP] it was shown that for each \( n \in \mathbb{N} \) the number of Toeplitz matrices \( T_n \) with 0 diagonal and with rank \( s < n \) is \( (q - 1)[q^{-s-1} + q^{s+1} - 2], \) where \( K \) is any finite field of characteristic 2. If \( n \) is even the number of invertible
Toeplitz matrices is \((q - 1)q^{n-2}\). This latter result is rather straightforward to prove in the case where \(q = 2\), and we do so below.

**Theorem 2.12** (cf. [CP, Corollary 2.10]). Let \(F\) be the field of characteristic 2 consisting of 2 elements. If \(n\) is even then the number of invertible \(n \times n\) Toeplitz matrices with 0 diagonal is \(2^{n-2}\).

**Proof.** Suppose \(m\) is an even integer and \(A_m\) is an invertible Toeplitz matrix with 0 diagonal. For any integer \(p = 2k\) we count the number of invertible Toeplitz matrices \(A_{m+p}\) which (i) have \(A_m\) in the upper left corner, and (ii) satisfy \(v(A_{m+p}) = f\) for \(0 \leq f \leq k\). Since \(v(A_m) = 0\) is assumed to be 0, it follows from Corollary 2.10 above that \(v(A_{m+k}) = k - f\) for \(0 \leq f \leq k\). Therefore, once \(A_m, A_{m+1}, \ldots, A_{m+k}\) have been chosen, the nullities of the successive matrices \(A_{m+k+1}, \ldots, A_{m+2k}\) decrease regardless of the choices for \(A_{m+k+1}, \ldots, A_{m+2k-1}\) so that these entries may be chosen arbitrarily. Note also from the corollary that since \(v(A_m) = 0\), \(v(A_{m+1}) = 1\) regardless of the choice of \(a_m\), so that \(a_m\) is also arbitrary. It follows from the previous paragraph that \(A_{m+k}\) has cardinality \(2^k - 1\).

Write \(n = 2r\). Divide the invertible \(n \times n\) Toeplitz matrices (with 0 diagonal) into disjoint sets \(S_m\) for \(m = 0, 2, 4, \ldots, 2(r-1)\), where for \(m\) positive, \(S_m\) consists of those matrices \(A_m\) whose \(m \times m\) upper left corner submatrix is invertible but for which no larger upper left corner matrix is invertible, except for \(A_n\) itself. \(S_0\) is the set of those matrices \(A_m\) none of whose upper left corners is invertible except for \(A_n\) itself. From the previous paragraph, \(S_m\) has cardinality \(2^m - 2\). Then the total number of invertible matrices is \(2^{r-1} + \sum_{j=1}^{r} 2^{r+j-2} = 2^{2r-2} = 2^{n-2}\).

As an application of this result we show that there are countably many nonconjugate binary shifts of commutant index 2. In Corollary 7.13 we shall show, however, that they are all cocycle conjugate.

**Corollary 2.13.** There are infinitely conjugacy classes of binary shifts of commutant index 2.

**Proof.** Since, by Theorem 1.8, binary shifts are conjugate if and only if their bitstreams agree, we seek infinitely many distinct bitstreams \((a)\) whose corresponding binary shift \(\sigma\) has commutant index 2. Let \(n\) be a
positive even integer. By the preceding result there is an invertible Toeplitz matrix $A$ with 0's along its diagonal, and by the proof of the preceding result we may even assume $A$ to have been chosen such that no proper Toeplitz matrix lying in the upper left corner of $A$ is invertible. Let $a_0, a_1, \ldots, a_{n-1}$ be the entries of the first row of $A$. Since $A$ is invertible there exists a vector $c = [ c_1, \ldots, c_n]^t$ such that $A c = [a_1 + a_n + 1, a_2 + a_{n-1}, a_3 + a_{n-2}, \ldots, a_n + a_1]^t$. Then we may choose $a_{n+1}, a_{n+2}, \ldots$ inductively so that $c$ satisfies the system $A c = b$, where $A$ is the semi-infinite matrix

\[
\begin{pmatrix}
  a_0 & a_1 & a_2 & \cdots & a_{n-1} \\
  a_1 & a_0 & a_1 & & a_{n-2} \\
  a_2 & a_1 & a_0 & & a_{n-3} \\
  \vdots & & & & \vdots \\
  a_{n-1} & a_{n-2} & a_{n-3} & & a_0 \\
  a_n & a_{n-1} & a_{n-2} & & a_1 \\
  a_{n+1} & a_n & a_{n-1} & & a_2 \\
  \vdots & & & & \vdots 
\end{pmatrix}
\]

and $b = [ a_1 + a_n + 1, a_2 + a_{n-1}, a_3 + a_{n-2}, \ldots, a_n + a_1, a_{n+1} + a_0, a_{n+2} + a_1, \ldots ]^t$. Let $(a)$ be the bitstream constructed in this way. If $\sigma$ is the corresponding shift with generators $u_i, i \in \mathbb{Z}^+$, let $w$ be the word $u_0^{c_0} u_1^{c_1} \cdots u_n^{c_n} u_{n+1}^{c_{n+1}}$, where $c_0 = 1 = c_{n+1}$. Then one may check that the linear system represented by the matrix equation $A c = b$ is equivalent to the word $w$ possessing the following properties: (i) $w$ anticommutes with $u_i$, and (ii) $w$ commutes with $u_j$ for $j \geq 2$. Hence $w$ commutes with $\sigma^j(R)$ so that $\sigma$ has commutant index 2.

Given the invertibility conditions imposed on $A$, if $m$ is an even positive integer distinct from $n$, and $A'$ is an $m \times m$ Toeplitz matrix satisfying similar invertibility conditions as $A$, then the bitstreams $(a)$ and $(a')$ resulting from the construction of the previous paragraph are distinct.

3. BINARY SHIFT ALGEBRAS

In the next section we give an explicit characterization of which subsets of $\mathbb{N}$ are anticommutator sets for binary shifts on $R$. As a step in this direction, we construct below, for any subset $S$ of $\mathbb{N}$, a binary shift algebra $\mathcal{B}(S)$ generated (as a group algebra) by a sequence of hermitian unitaries satisfying commutation relations determined by $S$. A more precise definition is given below. We shall indicate how to construct the Bratteli diagram for the AF-algebra $\mathcal{A}(S)$ associated with $\mathcal{B}(S)$. As we shall see, if $S$ is the anticommutator set for a binary shift on $R$, then $\mathcal{A}(S)$ is the UHF algebra of type $2^\infty$. Some of the results of this section are drawn from [Po, Section 3].
Definition 3.1. Suppose $S$ is a (possibly infinite) subset of $\mathbb{N}$. The binary shift algebra $B(S)$ over $S$ is the group algebra generated by elements $u_i, i \in \mathbb{Z}^+$ satisfying the relations

(i) $u_i^* = u_i$,
(ii) $u_i^2 = I$,
(iii) $u_i u_j = a(i, j) u_j u_i$,

where $a(i, j) = -1$ if $|i - j| \in S$ and $a(i, j) = 1$ if $|i - j| \notin S$. If $Q = \{i_0, i_1, ..., i_n\}$, $i_0 < i_1 < \cdots < i_n$ is a finite subset of $\mathbb{Z}^+$ then $u(Q)$ is defined to be

$u_{i_0} u_{i_1} \cdots u_{i_n}$.

Note that Example 1.1 arises as the completion of a binary shift algebra $B(S)$ with $S = \{1\}$.

Remark 3.1. Given the translation invariance of the coefficients $a(i, j)$, i.e., $a(i + k, j + k) = a(i, j)$, for $i, j, k \in \mathbb{Z}^+$, it is possible to define a unital homomorphism $\sigma = \sigma_S$ on $B(S)$ by setting $\sigma(u(Q)) = u(Q + 1) = u_{i_0 + 1} u_{i_1 + 1} \cdots u_{i_n + 1}$. Our goal is to describe for which sets $S$ the algebra $B(S)$ may be completed to yield the hyperfinite $II_1$ factor $R$, in which case $\sigma$ will extend to form a binary shift as in Section 1.

The following notation and terminology will be used quite often in this paper. In particular, the term bitstream is appropriated from the theory of Linear Recurring Sequences, which has applications to cryptography. Although these sequences are easily generated and widely used in the transmission of encoded messages, some of their properties are quite subtle and not well understood. We shall show that some of the elementary number theoretical results pertaining to Linear Recurring Sequences may be applied in the present setting towards the analysis of binary shifts. For more about the theory of these sequences, the reader is referred to [FM, G1, LN, Z]. We shall have occasion to draw from some of these references below.

Definition 3.2. Let $S$ be a subset of $\mathbb{N}$. The bitstream, $a(S)$, corresponding to $S$, is a sequence $a_0, a_1, ...$ of 0's and 1's where $a_j = 1$ if $j \in S$ and $a_j = 0$ otherwise, (i.e., $a_j = a(j, 0)$ in the notation of the preceding definition). The corresponding Toeplitz sequence $\{O^n_S\}$ is the sequence of Toeplitz matrices defined as in the previous section, where $O^n_S$ is the $n$ by $n$ matrix whose initial row has the entries $a_0, a_1, ..., a_{n-1}$.

For $n \in \mathbb{Z}^+$, the words $u(Q)$ with $Q \subset \{0, ..., n-1\}$ generate a subalgebra $B_n(S)$ of $B(S)$ of dimension $2^n$. Since we have the unital inclusions $B_n(S) \subset B_{n+1}(S)$ of finite-dimensional algebras, it follows that the $C^*$-algebra completion $\mathfrak{A}(S)$ of any binary shift algebra is an $AF$-algebra [Br]. The rank results obtained in the previous section for sequences of Toeplitz matrices will enable us to construct the Bratteli diagrams for the binary shift.
algebras. We shall use these diagrams to show that $\mathcal{A}(S)$ is either the UHF algebra of type $2^\infty$ or is isomorphic to the tensor product of a matrix algebra with the algebra of continuous functions on the Cantor set, Theorem 3.4.

Lemma 3.1. Suppose $A$ is an element of the center of $\mathcal{B}_d(S)$. Then $A$ may be written as a linear combination of words, each of which lies in the center of $\mathcal{B}_d(S)$.

Proof. We may assume $A \neq 0$. Writing $A = \sum b_Q U(Q)$, where the sum is taken over those subsets $Q$ of $\{0, 1, \ldots, n-1\}$ for which $b_Q \neq 0$, then for any word $w$ in $\mathcal{B}_d(S)$ we have $A = w^* A w = \sum b_Q w^* U(Q) w$. Since $w^* U(Q) w = + U(Q)$, each $U(Q)$ in the expression for $A$ must commute with $w$.

Lemma 3.2. For $n \in \mathbb{N}$, a word $z = u_0^{k_0} \cdots u_{n-1}^{k_{n-1}}$ lies in the center of $\mathcal{B}_d(S)$ if and only if $k = [k_0, \ldots, k_{n-1}]^t \in \ker(\mathcal{A}_n)$, where $\mathcal{A}_n$ is the $n \times n$ Toeplitz matrix associated with $a(S)$.

Proof. It is clear that $z$ commutes with $u_j$, $j \in \{0, 1, \ldots, n-1\}$, if and only if the product of the $j$th row of $\mathcal{A}_n$ with $k$ is 0.

Lemma 3.3. If the Toeplitz matrix $\mathcal{A}_n$ has nullity $\nu_n = q$ then the center of $\mathcal{B}_d(S)$ is a $2^q$-dimensional algebra.

Proof. Combine the two preceding lemmas.

Remark 3.2. In light of the preceding result we shall also refer to the nullity sequence $\{
u_n: n \in \mathbb{N}\}$ as the center sequence corresponding to the binary shift algebra $\mathcal{B}(S)$, or corresponding to a binary shift $\sigma$ whose anti-commutator set is $S$. By the lemma we have, for $3_n$ the center of $\mathcal{B}_d(S)$, that $\nu_n = \log_2 \dim(3_n)$.

We may obtain the following useful result by combining the preceding lemmas with the unimodality results of Section 2.

Theorem 3.4. Suppose there is a positive integer $n$ such that the Toeplitz matrix $\mathcal{A}_n$ has full rank. Suppose moreover that there is a positive integer $m$ such that, for $1 \leq j \leq 2m$, the nullities $\nu_n = \dim \ker(\mathcal{A}_n^{m+j})$ are $1, \ldots, m-1, m, m-1, \ldots, 1, 0$. Then there is a word $z = u_0^{k_0} u_1^{k_1} \cdots u_n^{k_n}$ in $\mathcal{B}_{n+1}(S)$ such that

1. $k = [k_0, \ldots, k_n]^t$ is flip-symmetric,
2. $k_0 = 1 = k_n$,
3. if $1 \leq j \leq m$, the center of $\mathcal{B}_{n+j}(S)$ is the $2^j$-dimensional algebra generated by $z, \sigma(z), \ldots, \sigma^{j-1}(z)$, and
4. if $1 \leq r \leq m-1$, the center of $\mathcal{B}_{n+m+r}(S)$ is the $2^{m-r}$-dimensional algebra generated by $\sigma(z), \ldots, \sigma^{m-1}(z)$.
Proof. By the unimodality property of the nullities of the Toeplitz matrices (Corollary 2.10), either \( v_{n+1} = j \) for all \( j \in \mathbb{Z}^+ \), or there is an \( m \) such that the nullities of the Toeplitz sequence behave as above. By Lemma 2.7 there is a vector \( \mathbf{k} \) which spans the kernel of \( \mathcal{A}_{n+1} \) and which satisfies (o) and (i). By Lemma 3.3 the corresponding word \( z \) must generate the center of \( \mathcal{A}_{n+1}(S) \). The rest of (ii) follows by applying the results of Lemma 2.8, Corollary 2.10, and Lemma 3.3. Turning to (iii), the dimension of the center follows from Corollary 2.10, and Lemmas 3.1–3.3. Applying (ii) with \( j = m \), we get that \( \sigma(z), \ldots, \sigma^{m-1}(z) \) all commute with \( u_0, \ldots, u_{n+m-1} \). On the other hand, since \( z \) commutes with \( u_0, \ldots, u_{n+m-1} \), so we see that \( \sigma'(z), \ldots, \sigma^{m-1}(z) \) all commute with \( u_{n+m}, \ldots, u_{n+m+r-1} \), and (iii) follows from the fact that \( \sigma'(z), \ldots, \sigma^{m-1}(z) \) generate a \( 2^{m'-r} \) dimensional algebra.

We may use the theorem to analyze the structure of the binary shift algebras \( \mathcal{A}(S) \). First note that an argument nearly identical to the proof of Lemma 3.1 shows that the center \( Z \) of \( \mathcal{A}(S) \) is generated by the words it contains. Now suppose the nullity sequence \( v_n = \text{null} \mathcal{A}_n, n \in \mathbb{Z}^+ \) includes infinitely many 0's. Suppose \( z = u(Q) \) is a nontrivial word in the center. Choose \( n \in \mathbb{N} \) such that \( n > \max Q \). Then \( z \) lies in the center of \( \mathcal{A}_n(S) \). But if \( n \) is also chosen so that \( v_n = 0 \), then \( \mathcal{A}_n \) has trivial kernel, so that \( \mathcal{A}(S) \) has trivial center, a contradiction. Hence if \( Z \) is nontrivial then \( v_n = 0 \) at most finitely often.

If \( v_n \) is never 0 then by Corollary 2.10, \( v_n = n \) for all \( n \). Hence \( \mathcal{A}_n \) is the 0 matrix for all \( n \), so that \( S = \emptyset \). Hence \( Z = \mathcal{B}(S) = \mathcal{B}(\emptyset) \). For \( i \in \mathbb{Z}^+ \), let \( p_i^+ \) be the projection \( 1/2(I + u_i) \) and let \( p_i^- = 1/2(I - u_i) \). For \( m \in \mathbb{N} \) there are 2\(^m\)-mutually orthogonal projections \( q \) in \( \mathcal{B}_m(\emptyset) \) of the form \( q_0 q_1 \cdots q_{m-1} \), where each \( q_i \) is either \( p_i^+ \) or \( p_i^- \). Clearly \( \mathcal{B}_m(\emptyset) \) is the direct sum of the one-dimensional algebras \( \mathbb{C} q_i \). Note that \( q = q_p^+ + q_p^- \), so that \( \mathbb{C} q \) splits as the direct sum of two one-dimensional algebras in \( \mathcal{B}_{m+1}(\emptyset) \). The Bratteli diagram for \( \mathcal{B}(\emptyset) \) has the following form.

The AF algebra formed as the completion of this diagram (in the topology of uniform convergence) is therefore isomorphic to the algebra of continuous functions on the Cantor set, \([E]\).
Next suppose that $S \subseteq \mathbb{N}$ is such that the nullity sequence takes the value 0 at least once but still only finitely often. We may assume that $n$ has been chosen so that $r_n = 0$ and $r_{n+j} > 0$ for $j > 0$. Then in fact, by Corollary 2.10, $r_{n+j} = j$ for all $j > 0$ and therefore by Theorem 3.4(ii), there is a word $z$ such that $z, \sigma(z), \ldots, \sigma^{j-1}(z)$ generates the center of $\mathcal{B}_{n+j}(S)$. But then it is clear that $z, \sigma(z), \ldots$ generate the center $\mathcal{B}(S)$. Also by the theorem, $\mathcal{B}(S)$ is isomorphic to a matrix algebra $M$ (in fact $M = M_{2^n}(\mathbb{C})$), since $\mathcal{B}(S)$ is an algebra of dimension $2^n$. Since $\mathcal{B}_{n+j}(S)$ is generated by $\mathcal{B}(S), z, \ldots, \sigma^{j-1}(z)$, one can reason as above that, starting with $\mathcal{B}(S)$, the Bratteli diagram for $\mathcal{B}(S)$ is as follows.

Hence the AF-algebra associated with $\mathcal{B}(S)$ is isomorphic to the tensor product of $M$ with the algebra of the continuous functions on the Cantor set.

Next suppose that $\exists$ is trivial. Then $r_n = 0$ infinitely often. Hence by Theorem 3.4, $\mathcal{B}(S)$ has trivial center for infinitely many $n$. Hence $\mathcal{B}(S)$ is isomorphic to a matrix algebra, which, as above, must be $M_{2^n}(\mathbb{C})$. Hence the AF-algebra associated with $\mathcal{B}(S)$ is the UHF of type $2^\omega$, $[E]$. Hence we have obtained the following.

**Theorem 3.5.** Let $S$ be a subset of $\mathbb{N}$. Let $\mathcal{B}(S)$ be the corresponding binary shift algebra. If $\mathcal{B}(S)$ has a nontrivial center, then there is a word $z$ such that $z$ and all of its shifts generate the center of $\mathcal{B}(S)$. In this case, the AF-algebra $\mathfrak{A}(S)$ associated with $\mathcal{B}(S)$ is isomorphic to the tensor product of a finite-dimensional matrix algebra with the algebra of continuous functions on the Cantor set, $C(\mathbf{T})$. If $\mathcal{B}(S)$ has trivial center then $\mathfrak{A}(S)$ is the UHF algebra of type $2^\omega$.

**Definition 3.3.** A subset $S$ of $\mathbb{N}$ is said to be primary if it is the anticommutator set for a binary shift.

**Theorem 3.6.** (cf. [Po, Theorem 3.9]). Let $S$ be a subset of the positive integers. Then the following statements are equivalent.
(i) $S$ is primary.
(ii) $\mathfrak{B}(S)$ is simple.
(iii) $\mathfrak{A}(S)$ is isomorphic to the UHF algebra of type $2^\infty$.
(iv) The center of $\mathfrak{B}(S)$ consists of multiples of the identity.
(v) The center of $\mathfrak{A}(S)$ consists of multiples of the identity.
(vi) $\mathfrak{B}(S)$ has a unique trace.
(vii) $\mathfrak{A}(S)$ has a unique trace.
(viii) For each nonempty finite subset $Q$ of $N$ there is an integer $k$ so that $u_k u(Q) = -u(Q) u_k$.

Proof. Suppose statement (viii) is false. Then there is a word $u(Q) \neq I$ in the center of $\mathfrak{B}(S)$. Hence statements (ii) through (vii) are false. Hence any of the statements (ii) through (vii) imply (viii).

We prove the reverse implications. Suppose (viii) is true. Then by Theorem 3.5, $\mathfrak{B}(S)$ has trivial center. Hence (viii) implies (iv) and (v). By Theorem 3.5, either $\mathfrak{A}(S)$ is UHF or has a nontrivial center, so that (viii) implies (iii). Since $\mathfrak{A}(S)$ is simple then so is $\mathfrak{B}(S)$, [Br]. Hence (viii) implies (ii). Also if (viii) holds, let $\text{tr}$ be any trace on $\mathfrak{B}(S)$. Then for $Q$ a nonempty finite subset of $Z^+$ and $k$ as in (viii), $\text{tr}(u(Q)) = \text{tr}(u^2 u(Q)) = \text{tr}(u u(Q) u) = \text{tr}(-u(Q))$, so $\text{tr}$ is trivial on all nontrivial words of $\mathfrak{B}(S)$. Hence $\text{tr}$ is unique, so (viii) implies (i) and similarly (viii) implies (vii).

Thus conditions (ii) through (vii) are all equivalent. Note that (iii) and (vii) imply (i). Suppose (i) holds. If (viii) is false then for some nonempty $Q, u(Q)$ lies in the center of $R$, a contradiction. Hence (i) implies (viii).

Remark 3.3. For completeness we give a description of the embeddings $B_j(S) \subset B_{n+m+1}(S)$, $q \in Z^+$ (see also [EN, Section 2] for some explicit examples of Bratteli diagrams of binary shift algebras). To begin, suppose $n \in N$ is such that $v_n = 0$. Then for some $m \in N$, $v_{n+j} = j$ for $0 \leq j \leq m$ and $v_{n+m+j} = m-j$ (also for $0 \leq j \leq m$). By Theorem 3.4 there is a word $z$ generating the center of $B_{n+m+1}(S)$, and, moreover, $z, \sigma z, \ldots, \sigma^{m-1} z$ generate the center of $B_{n+m+1}(S)$, for $1 \leq j \leq m$. For $1 \leq i \leq m$, set $z_i = \sigma^{-i}(w)$. Let $p^*_j$, $p^-_j$ be the corresponding projections $p^*_j = 1/2(z_j z_j)$, $p^-_j = 1/2(1-z_j)$. Then it is straightforward to see that for $1 \leq j \leq m$, $B_{n+m+1}(S)$ consists of $2^j$ summands of matrix algebras of the form $B_j(S) q$, where $q$ is a projection of the form $q_1 \cdots q_j$, and each $q_i$ is either $p^*_i$ or $p^-_i$. But if $1 \leq j \leq m-1$, $q = q^*_j q^*_j + q^-_j q^-_j + q^*_j q^-_j q^-_j q^*_j$ so that the summand $B_j(S) q$ splits into the pair of summands $B_j(S) q^*_j q^*_j + B_j(S) q^-_j q^-_j$ in the embedding $B_j(S) \subset B_{n+m+1}(S)$. From this one sees that the part of the Bratteli diagram running from the $n$th floor to the $n+m$th floor looks like the diagram above, but with $M$ replaced by $B_j(S)$.

Next consider the algebras $B_{n+m+1}(S)$, for $1 \leq j \leq m$. By Theorem 3.4, $\sigma^j(w), \ldots, \sigma^{m-1} w$ generate the center of this algebra.
chosen \( q_{j+2} \) to be either \( p_{j+2} \) or \( p_{j+2}^* \), \( q_{j+3} \) to be \( p_{j+3} \) or \( p_{j+3}^* \), ..., \( q_{j+m} \) to be either \( p_{j+m} \) or \( p_{j+m}^* \); then both \( q^+ = p_{j+1} q_{j+2} \cdots q_{j+m} \) and \( q^- = p_{j+1}^* q_{j+2} \cdots q_{j+m}^* \) are minimal central projections in \( B_{n+m+j}(S) \). It then follows, again from Theorem 3.4, that \( q^+ + q^- = q_{j+2} q_{j+3} \cdots q_{j+m} \) is a minimal central projection in \( B_{n+m+j+1}(S) \).

4. PERIODICITY AND FACTOR CONDITION

In the preceding section Theorem 3.6 shows that a subset \( S \) of \( \mathbb{N} \) is an anticommutator set for a binary shift on \( R \) if and only if the binary shift algebra \( \mathcal{A}(S) \) has trivial center. Using this characterization and the theorem below we prove that \( S \) gives rise to a binary shift on \( R \) if and only if its bitstream satisfies a certain symmetry condition, which we call mirror-periodicity.

**Definition 4.1.** Let \( S \) be a subset of \( \mathbb{N} \), and let \( a(S) = \{a_0, a_1, \ldots \} \) be the corresponding bitstream. Then the reflected bitstream \( \mathcal{R}(S) \) is the doubly-infinite sequence \( \{\ldots, a_{-2}, a_{-1}, a_0, a_1, a_2, \ldots \} \).

**Theorem 4.1.** \( \mathcal{A}(S) \) has nontrivial center if and only if its reflected bitstream \( \mathcal{R}(S) \) is periodic.

**Proof.** Suppose \( \mathcal{A}(S) \) has a nontrivial center \( \mathcal{Z} \). Then by Theorem 3.5 there is a word \( z = u_0 u_1^t \cdots u_n^t \) satisfying the conditions (o) and (i) of Theorem 3.4, and such that \( z \) and all of its shifts generate \( \mathcal{Z} \). If \( z = u_0 \) then by the proof of Theorem 3.5, \( S = \emptyset \), so \( \mathcal{R}(S) \) is the constant sequence (of 0's) and we are done. So we assume that \( n > 0 \). Since \( z \) commutes with \( u_0, u_1, \ldots \), the vector \( k = [k_0, k_1, \ldots, k_n]^t \) lies in the right kernel of the following infinite matrix.

\[
\begin{pmatrix}
a_0 & a_1 & a_2 & a_3 & \cdots & a_n \\
a_1 & a_0 & a_1 & a_2 & \cdots & a_{n-1} \\
a_2 & a_1 & a_0 & a_1 & \cdots & a_{n-2} \\
\vdots \\
a_n & a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \\
a_{n+1} & a_n & a_{n-1} & a_{n-2} & \cdots & a_1 \\
\vdots \\
a_{n+2} & a_{n+1} & a_n & a_{n-1} & \cdots & a_2 \\
\vdots 
\end{pmatrix}
\]

Alternatively stated, \( k \) has scalar product 0 with any \( n + 1 \) consecutive terms of the sequence \( \{a_0, a_1, a_2, a_3, a_4, \ldots\} \). On the other hand, since \( k \) coincides with its flip \( k^t \), it follows that \( k \) has scalar product 0 with any
$n+1$ consecutive terms of the sequence $R(S)$. Hence $R(S)$ is periodic [LN, Section 6.1].

Now suppose $R(S)$ is periodic, with period $p$. Consider the vector $v = [1, 0, 0, \ldots, 0, 0, 1]'$ of length $p+1$. Then the scalar product of $v$ with any $p+1$ consecutive entries of $R(S)$ is 0. From this observation it is not difficult to show that the word $u_0 u_p$ lies in the center of $R(S)$. □

Combining the preceding result with Theorem 3.6 we obtain the following characterization of anticommutator sets $S$.

**Corollary 4.2.** A subset $S \subset \mathbb{N}$ is an anticommutator set for a binary shift on $R$ if and only if $R(S)$ is not mirror-periodic.

5. PERIODICITY AND THE COMMUTANT INDEX

From this point on we shall assume that $\alpha(S)$ is a bitstream which lacks the mirror-symmetry condition discussed in the previous section, so that the corresponding endomorphism $\sigma$ induces a binary shift on $R$. In this section we investigate the connections between eventually periodic bitstreams and binary shifts with finite commutant index. To make these notions precise we require the following definitions.

**Definition 5.1.** A binary shift $\sigma$ on $R$ is said to have commutant index $k$ if $k$ is the first positive integer such that the algebra $\sigma^k(R)$ has a nontrivial relative commutant $\sigma^k(R)^\cap R$ in $R$.

It follows from the Jones theory for subfactors [J, Corollary 2.2.4] that 2 is the minimal possible commutant index. On the other hand, it is easy to show that every finite commutant index $k \geq 2$ is attained: To see this, let $S = \{k-1\}$, i.e., $\alpha(S)$ is the sequence which consists of 0's except for $a_{k-1} = 1$. Then for $j \leq k - 1$, $\sigma^j(R)$ has trivial relative commutant, whereas $\sigma^k(R)^\cap R = \{u_0\}$. We shall show in Theorem 5.8 that the commutant index may be infinite. In fact there are uncountably many binary shifts with infinite commutant index which are pairwise nonconjugate (see Remark 5.1).

**Definition 5.2.** A bitstream $\alpha(S) = \{a_j\}_{j=0}^\infty$ is said to be eventually periodic if there is an $n \in \mathbb{Z}^+$ and a $p \in \mathbb{N}$ such that $\{a_n, a_{n+1}, \ldots\}$ is periodic.

The following definition occurs in the subfield of cryptology known as Linear Feedback Register Systems, or LFSR's, [G1, LN].
5.3. A bitstream \(a(S) = \{a_n\}_{n=0}^\infty\) in \(F\) is said to be (an \(s\)th order) linear recurring sequence if there is an \(s \in \mathbb{Z}^+\) and a vector \(k = [k_0, k_1, ..., k_s] \in F^{s+1}\) such that \(k_0 = 1\) and
\[
\sum_{i=0}^{s} a_{n+s-i} k_i = 0 \quad (5.1)
\]
for all \(n \in \mathbb{Z}^+\).

We shall show below that a linear recurring sequence must be eventually periodic, although it may not be periodic. To see that the latter may hold, consider the vector \(k = [1, 1, 0]\). If \(a(S) = \{0, 1, 0, 0, ...\}\) then (5.1) holds but \(a(S)\) is not periodic.

**Proposition 5.1** (cf. [LN, Theorem 6.7]). A linear recurring sequence is eventually periodic.

**Proof.** Let \(k_q\) be the last nonzero entry of \(k\), then from (5.1) we have
\[
\sum_{i=0}^{q} a_{n+s-i} k_i = 0.
\]
Consider the \(q \times q\) (companion) matrix \(K\) given by
\[
K = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
k_q & k_{q-1} & \cdots & \cdots & \cdots & \cdots & k_1
\end{bmatrix}
\]
From the equation above it follows that for any \(n \in \mathbb{Z}^+\), \(KS_n = S_{n+1}\), where \(S_n = [a_{n+s-q}, ..., a_{n+s-1}]^T\). Since \(K\) is an invertible matrix over the finite field \(F\), there is a \(p\) such that \(K^p = I\). But then from the equation \(K^p S_n = S_{n+p}\) we conclude that \(a_{n+s-q} = a_{n+s-q+p}\), for all \(n \in \mathbb{Z}^+\), so that the sequence \(\{a_{s-q}, a_{s-q+1}, ...\}\) is periodic. \(\blacksquare\)

The next result follows immediately from the proof of the proposition.

**Corollary 5.2.** If \(k_s = 1\) then \(a(S)\) is periodic.
We now show that the converse of the proposition is valid (cf. the proof of Theorem 4.1).

**Proposition 5.3.** An eventually periodic sequence \( a(S) \) is a linear recurring sequence.

**Proof.** By hypothesis there is an \( r \in \mathbb{Z}^+ \) and a positive integer \( p \) such that \( a_{m+p} = a_m \) for all \( m \geq r \). Let \( k = [k_0, \ldots, k_s]^t \) be the vector with entries \( k_0 = k_p = 1 \) and all other entries 0. Then \( k \) clearly satisfies (5.1).

The smallest \( p \) such that an eventually periodic sequence \( a(S) \) satisfies \( a_{m+p} = a_m \) for all sufficiently large \( m \), is called the least period.

**Proposition 5.4.** (cf. [LN, Theorem 6.7]) The least period of an \( s \)th order recurring sequence does not exceed \( 2^s - 1 \).

**Proof.** For \( n \in \mathbb{Z}^+ \) let \( S_n = [a_n, a_{n+1}, \ldots, a_{n+s-1}]^t \) be the \( n \)th state vector of \( a(S) \). Then \( S_{n+1} = CS_n \) where \( C \) is the \( s \times s \) companion matrix constructed as \( K \) is above, but with last row \( [k_s, \ldots, k_1]^t \). If \( S_n = 0 \) for some \( n \) then clearly \( S_{n+j} = 0 \) for all \( j \) so that the period is 1. Now suppose \( S_n \neq 0 \) for all \( n \). Since there are \( 2^s - 1 \) possible nonzero state vectors \( S_n \), there must be an \( n \in \mathbb{Z}^+ \) and an \( m \leq 2^s - 1 \) such that \( S_n = S_{n+m} \). But then for all \( k \in \mathbb{N}, S_{n+m+k} = C^kS_{n+m} = C^kS_n = S_{n+k} \), so that \( a(S) \) is eventually periodic with period no greater than \( m \).

Below we shall relate the results above to binary shifts by showing that a binary shift has a finite commutant index if and only if its corresponding bitstream is eventually periodic. First we establish the following important but straightforward result.

**Theorem 5.5.** The commutant index is a cocycle conjugacy invariant for binary shifts.

**Proof.** Suppose \( \sigma \) and \( \tau \) are cocycle conjugate. Let \( U \in \mathcal{B}(R) \) be a unitary operator and let \( \gamma \) be an automorphism of \( R \) such that \( \sigma \cdot \text{Ad}(U) = \gamma \cdot \tau \cdot \gamma^{-1} \). Then for \( k \in \mathbb{Z}^+ \), \( \text{Ad}(U_k) : \sigma^k = \gamma \cdot \sigma^k \cdot \gamma^{-1} \), where \( U_k = \sigma(U) \cdots \sigma^k(U) \), and therefore if \( w \in \sigma^k(R)^C \cap R \), then \( \gamma^{-1} \cdot \text{Ad}(U_k)(w) \in \sigma^k(R)^C \cap R \).

**Theorem 5.6.** Suppose \( \sigma \) is a binary shift with finite commutant index \( k \). Then the algebra \( \sigma^k(R)^C \cap R \) is a two-dimensional subalgebra of \( R \) which is generated by a word \( w = U(I) \) in the generators of \( \sigma \). The word \( w \) satisfies the property \( \sigma^0 \in I \).

**Proof.** We may identify \( R \) with the von Neumann algebra \( \mathcal{L}_G \) of left convolution operators on the algebra \( B(l^2(G)) \), where \( G \) is the group
generated by the words in the $u_i$'s (i.e., the generators of $\sigma$). Hence we may view $w$ as an element of $I_d(G)$ see [KR, Theorem 6.7.2]. Hence $w = \sum x_Q U(Q)$, where $Q$ runs over the set of all finite (ordered) subsets of $Z^+$ and the coefficients $x_Q$ are $I_2$-summable. Since $w \in \sigma^n(\{0\}) \cap R$, $u_j w u_j = w$ for all $r \geq k$, so that $U(Q)$ commutes with $u_j$ for all $Q$ for which $x_Q \neq 0$. We conclude that the commutant algebra $\sigma^n(\{0\}) \cap R$ is generated by all of the words which it contains. Observe that $0 \in Q$ for any nontrivial word in this algebra, for otherwise $\sigma^{-(n)}(U(Q)) = U(Q - 1)$ would commute with $\sigma^{k-1}(R)$, contradicting the minimality of $k$. Suppose $U(J), u(J)$ are nontrivial words in the $\sigma^n(\{0\}) \cap R$. Then $0 \in J, 0 \notin J \cup J'$, and $U(J \cup J')$ is a word in the $\sigma^n(\{0\}) \cap R$, so $J = J'$.

Corollary 5.7. Let $\sigma$ be a binary shift with finite commutant index $k$. Let $w$ be the word which generates $\sigma^n(\{0\}) \cap R$. Then for $j \in \mathbb{Z}^+$, $\sigma^{n+j}(\{0\}) \cap R = \{w, \sigma(w), \ldots, \sigma^n(w)\}$, an algebra of dimension $2^{j+1}$.

Proof. The theorem establishes the conclusion when $j = 0$. Suppose the statement holds for all $j \leq n$. For $j = n+1$ the right side is clearly contained in the left. To show the reverse inclusion we remark, as in the proof of the theorem, that the algebra $\sigma^{n+j+1}(\{0\}) \cap R$ can easily be shown to be generated by the words it contains. Suppose $v$ is a word in this algebra which is not in $\sigma^{n+j+1}(\{0\}) \cap R$. Multiplying $v$ by a subset of the words $w, \sigma(w), \ldots, \sigma^n(w)$, if necessary, we may assume that $v$ has the form $U(Q)$ where $Q \cap \{0, \ldots, n\} = \emptyset$. But then $\sigma^{-(n+1)}(v)$ is a word which lies in the first nontrivial commutant algebra $\sigma^n(\{0\}) \cap R$, so it must be either $I$ or $w$ by the theorem. But then $v = I$ or $\sigma^{n+1}(w)$, and we are done.

Theorem 5.8 (cf. [BY, Theorem 2.1]). A binary shift has finite commutant index if and only if its bitstream $a(S)$ is eventually periodic.

Proof. Suppose $a(S)$ is eventually periodic. Let $k \in \mathbb{Z}^+$ and $n \in \mathbb{N}$ be such that $a_{m+p} = a_m$ for all $m \geq n$. Let $w = U((0, 1)^n) = u_0 u_n$. Then for any $m \geq n$ and $r = m + p$, $u_r w = u_r u_0 u_n = (-1)^{m+1} u_0 u_r u_n = u_0 u_n u_r = w u_r$, so $\sigma^{n+k}(R)$ has a nontrivial relative commutant. For the converse, suppose $\sigma$ has finite commutant index $k$. Let $w = U(Q)$ be the word generating the relative commutant of $\sigma^n(R)$. Write $w = u_0 u_1 \cdots u_n$ and recall from Theorem 5.6 that $c_0 = 1$. For $s = \max \{q, k\}$, set $c = [c_0, \ldots, c_s] \in F^{s+1}$, where $c_{s+1} = \cdots = c_s = 0$. Since $u_{s+j}$ commutes with $w$ for all nonnegative integers $j$ we have

$$0 = c_0 q_{s+j} + c_1 a_{s+j-1} + \cdots + c_q a_{s+j-q} = \sum_{i=0}^q a_{s+j-i} c_i.$$ 

Hence $c$ generates $a(S)$ as a linear recurring sequence, as in (5.1). But then by Proposition 5.1, $a(S)$ must be eventually periodic.
Remark 5.1. From the statement of the theorem it follows that there exist binary shifts with infinite commutant index, and furthermore, these shifts correspond to bitstreams which are not eventually periodic. By applying Theorem 1.8 there are, in fact, uncountably many binary shifts with infinite commutant index, which are pairwise nonconjugate. Very little is known about the cocycle conjugacy classes of shifts of infinite commutant index. One remarkable result pertaining to these shifts is due to Narnhorfer, Stormer, and Thirring, who have shown the existence of a binary shift which has Connes–Stormer entropy 0, [NST, Theorem 2.1, Theorem 4.1]. As a consequence of their proof it follows that there exist binary shifts whose only invariant state is the (unique) trace on \( \mathbb{R} \) [NST, Remark 2.6].

Following [BY] we use the notation \( \sigma_w \) to denote the restriction of \( \sigma \) to the algebra generated by \( w \) and its shifts. The endomorphism \( \sigma_w \) is called the derived shift. It is easy to see that the derived shift is a binary shift in its own right. This follows from the observations: (i) \( w \) and \( \sigma^j(w) \) either commute or anticommute, (ii) \( w \) and \( \sigma^{k-1}(w) \) anticommute (since \( w \) anticommutes with \( u_{k-1} \) and commutes with \( \sigma^k(R) \)), and (iii) \( w \) and \( \sigma^j(w) \) commute for \( j \geq k \). From observations (ii) and (iii) it follows that \( \sigma \) has the same commutant index as \( \sigma_w \). Note also that \( (\sigma_w)_w = \sigma_w \).

**Theorem 5.9 ([BY, Theorem 1.2]).** If \( \sigma \) and \( \pi \) are cocycle conjugate binary shifts then their derived shifts \( \sigma_w \) and \( \pi_w \) are conjugate.

**Proof.** Suppose \( w \) generates \( \mathcal{A}(R') \cap R \), then \( w, \pi(w), ... \) are the generators of the binary shift \( \sigma_w \). If \( \text{Ad}(\pi(U)) \circ \pi = \gamma^{-1} \circ \pi \circ \gamma \), then using the notation of Theorem 5.5, \( w', \sigma(w'), ... \) are the \( \sigma_w \)-generators, where \( w' = \gamma^{-1} \circ \text{Ad}(U_j)(w) \). It is not difficult to show that \( w' \) commutes with \( \sigma^j(w') \) if and only if \( w \) commutes with \( \pi^j(w) \), for all \( j \in \mathbb{Z}^+ \), so that \( \sigma_w \) and \( \sigma_w \) have the same anticommutation set. Hence they are conjugate, by Theorem 1.8.

6. CONGRUENCE OF TOEPLITZ MATRICES

In this section we continue the study of binary shifts with finite commutant index. In the next section we present a proof of the main result of this paper. This is to show that if a binary shift \( \sigma \) has finite commutant index, and if the center sequences of \( \sigma \) and of \( \sigma_w \) are cofinal, then \( \sigma \) and \( \sigma_w \) are cocycle conjugate. It is not always true, however, that the center sequences of \( \sigma \) and \( \sigma_w \) are cofinal, see Remark 7.2. In this section we establish, under the above hypotheses, some congruence results for sequences of Toeplitz matrices associated with \( \sigma \) and with \( \sigma_w \). Theorem 6.12 and its corollary. These results comprise the major steps needed to prove our main result.
Most of the results of this section are generalizations of those which appear in Section 3 of [Pr].

**Remark 6.1.** We remind the reader that if $A_n$ is an $n$ by $n$ Toeplitz matrix, our convention is to number the rows and columns of $A_n$ from 0 to $n-1$. This is because the entries of the top row of $A$ are usually written as $a_0, a_1, \ldots, a_{n-1}$. For a fixed binary shift $\sigma$ with $\sigma$-generators $u_j$, $j \in \mathbb{Z}_+$, we shall use the notation $\mathfrak{U}_n$ to denote the algebra of dimension $2^n$ generated by $u_0, \ldots, u_{n-1}$, and we shall write $\mathfrak{Z}_n$ to denote the center of $\mathfrak{U}_n$.

**Lemma 6.1.** Suppose $\sigma$ is a binary shift with commutant index $k$. Then for $m$ sufficiently large, the center sequence values $v_n$ are bounded by $k-1$.

**Proof.** Suppose the conclusion of the lemma is false: Then by Corollary 2.10 there exist arbitrarily large $n \in \mathbb{N}$ such that $v_{n+j} = j$ for $0 \leq j \leq k$. Fix one of these $n$. Then there exists, by Theorem 3.4, a word $z = u(Q)$ such that $0 \in Q$ and $z, \sigma(z), \ldots, \sigma^{k-1}(z)$ generate the center $\mathfrak{Z}_{n+k}$ of $\mathfrak{U}_{n+k}$. Since $0 \in Q$, the shifted word $\sigma^{k-1}(z)$ begins with $u_{k-1}$. By Theorem 5.6, there is a word $w$ which generates $\sigma^k(R) \cap R$. Then $w$ anticommutes with $u_{k-1}$, since otherwise $w$ would be an element of $\sigma^{k-1}(R) \cap R$, which is trivial. Hence $w$ anticommutes with $\sigma^{k-1}(z)$. But $w \in \mathfrak{Z}_n$, for $n$ sufficiently large, and $w$ does not commute with $\sigma^{k-1}(z)$, so that $\sigma^{k-1}(z)$ does not lie in the center of $\mathfrak{U}_{n+k}$, a contradiction. Hence by contradiction, $v_n$ is bounded by $k-1$ for $n$ sufficiently large.

**Theorem 6.2.** Let $\sigma$ be a binary shift of commutant index $k$ with finitely nonzero bitstream $d_0d_1 \cdots d_k100 \cdots$. Then there are infinitely many indices $n \in \mathbb{N}$ such that $v_n = k$ if and only if $n = js - k$ for some positive integer $j$.

**Proof.** Since $\sigma$ has commutant index $k$, $d_{k-1} = 1$. By Corollary 2.10, the existence of infinitely many $n$ with $v_n = k - 1$ is equivalent to the existence of infinitely many positive integers $q$ such that $v_{q+k} = k - 1$. Hence by contradiction, $v_n = k - 1$ if and only if $n = js - k$ for some positive integer $j$. 

\[ \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{k-1} & d_{k-2} & d_{k-3} & d_1 & d_0 & d_1 & \cdots & d_{k-3} & d_k & d_{k-2} \end{bmatrix} \]

then $v_n = k - 1$ if and only if $n = js - k$ for some positive integer $j$. 

Theorem 6.2. Let $\sigma$ be a binary shift of commutant index $k$ with finitely nonzero bitstream $d_0d_1 \cdots d_{k-2}d_{k-1}100 \cdots$. Then there are infinitely many indices $n \in \mathbb{N}$ such that $v_n$, the $n$th entry of the center sequence for $\sigma$, is $k - 1$. More precisely, if $s$ is the order of the (invertible) matrix $C$ below,
values $1, 2, \ldots, k - 1$. By Theorem 3.4 it suffices to find infinitely many $q$ with the property that there is a nontrivial word $z = u_0^q u_1^q \cdots u_k^q$ which commutes with the $\sigma$-generators $u_0, \ldots, u_a + k - a$. Then by Lemma 3.2, it suffices to find infinitely many $q \in \mathbb{N}$ such that there is a nontrivial vector $x$ of the form $[x_0, \ldots, x_q, 0, \ldots, 0]'$ in the kernel of the $q + k - 1$ by $q + k - 1$ matrix $A_{q + k - 1}$.

Since $A_{k - 1} = 1$, the $2k - 2$ by $2k - 2$ matrix $C$ is invertible over the field $F$. Define state vectors $S_n, n \in \mathbb{Z}^+$ of length $2k - 2$ by setting $S_0 = [0, 0, \ldots, 1]'$ and $S_n = CS_{n-1}$, for $n \in \mathbb{N}$. Since $C$ is invertible and $F$ is a finite field, there exist infinitely many $m \in \mathbb{N}$ such that $C_m = I$. Fix one of these $m$ (we shall show below that $m$ must be even). Since $C_m = I$, $S_m = S_0$. Note that this implies that $S_{m-1} = [a, 0, \ldots, 0]'$, for some $a \in F$. Note that $S_{m-1} \neq 0$, however, since otherwise we would have $S_m = CS_{m-1} = 0$, a contradiction. Hence $S_{m-1} = [1, 0, \ldots, 0]'$.

Write $S_0 = [0, \ldots, 0, y_0]'$ (with $y_0 = 1$), $S_1 = [0, \ldots, 0, y_0, y_1]'$, $S_2 = [0, \ldots, y_0, y_1, y_2]'$, etc., and let $0, \ldots, 0, y_0, y_1, y_2, y_3, \ldots$ be the corresponding sequence one obtains. Note that by construction, any vector consisting of $2k - 1$ consecutive terms of this sequence has inner product $0 \mod 2$ with the vector $d = [d_{k-1}, \ldots, d_1, d_0, d_1, \ldots, d_{k-1}]$. Note also that since $S_{m-1} = [1, 0, \ldots, 0]'$ and $S_m = [0, \ldots, 0, 1]'$, that $y_1 = 1$, $y_{m-2k+2} = 1$ and $y_2 = 0$ for $m - 2k + 2 = j < m$. Hence the $m + 2k - 3$ initial terms of the sequence are $y = [0, \ldots, 0, y_0, \ldots, y_{m-1}]' = [0, \ldots, 0, y_0, y_1, \ldots, y_{m-2k+1}, y_{m-2k+2}, 0, \ldots, 0]'$, with $y_0 = y_{m-2k+2} = 1$. Using the flip symmetry of $d$, combined with the remark about inner products, one sees that $y$ is itself flip symmetric. This is seen as follows. The inner product of $[y_{m-2k+1}, y_{m-2k+2}, 0, \ldots, 0]'$ with $d$ is 0, as is the inner product of $[0, \ldots, 0, y_0, y_1]'$ with $d$. Since $y_0 = 1 = y_{m-2k+2} = 1$, since $d$ is flip symmetric, and since $d_{k-1} = 1$, we must have $y_1 = y_{m-2k+1}$. Continuing we get $y_2 = y_{m-2k}$, and so on. Hence we may rewrite $[y_0, y_1, \ldots, y_{m-2k+2}]' = [r_0, r_1, r_0, r_1, \ldots, r_p]'$, if $m$ is even or as $[r_0, r_1, r_1, \ldots, r_p]'$ if $m$ is odd.

We include a number-theoretic proof of the fact that $m$ is even. Recall [LN, Definition 3.2] that a polynomial $f \in F[x]$ is said to have order $e$ if $e$ is the smallest positive integer such that $f(x)$ divides $x^e - 1$. If $f(x)$ is a monic polynomial $c_0 + c_1 x + \cdots + c_m x^m + x^e$ and $f(0) \neq 0$, then the order of $f$ coincides with the order of the companion matrix $C$ above in the group $GL_n(F)$, [LN, Lemma 6.26]. Consider the polynomial $g(x) = d_{k-1} + d_{k-2} x + \cdots + d_k x^{k-2} + d_0 x^{k-1} + d_1 x^k + d_2 x + \cdots + d_{k-1} x^{k-2}$. The companion matrix of $g$ is the matrix $C$ in the theorem. Since $d_0 = 0$ it is clear that $g(1) = 0$, so that $x - 1$ is a factor of $g(x)$. But it is also not difficult to show that $g'(1) = 0$, so that $(x - 1)^2 = x^2 - 1$ is a factor of $g(x)$. Since $g(x)$ has a factor of multiplicity greater than 1, its order is even [LN, Theorem 3.8, Theorem 3.9]. Hence $C$ has even order $m$. 
Since \( m \) is even, \( y = [0, \ldots, 0, r_p, \ldots, r_1, r_0, r_1, \ldots, r_p, 0, \ldots, 0]' \). Let \( q = 2p = m - 2k + 2 \). The results about inner products above show that the vector \( x = [r_p, \ldots, r_1, r_0, r_1, \ldots, r_p, 0, \ldots, 0]' \), of length \( q + k - 1 \), lies in the right kernel of \( \mathcal{A}_{q+k-1} \). As pointed out above, the existence of \( x \) implies that \( k - 1 = v_{q+k-2} = v_{m-2k+2+k-2} = v_{m-k} = v_{p-k} \).

Next we note that the positive integers \( j \) are the only indices \( n \) for which \( v_n = k - 1 \). To see this, suppose \( v_n = k - 1 \). Since the proof of the lemma, combined with the fact that \( u_0 \) generates \( \sigma^+(R) \cap R \), show that \( \max \{ v_1 \} \) is \( k - 1 \); Corollary 2.10 implies that \( v_{n-k+2}, \ldots, v_n \) take the values \( 1, \ldots, k - 1 \), so by Theorem 3.4 there is a flip-symmetric vector \( s = [s_0, \ldots, s_{n-k+2}]' \in \ker \mathcal{A}_{n-k+3} \), with \( s_0 = 1 \), such that \( [s_0, \ldots, s_{n-k+2}, 0, \ldots, 0]' \in \ker \mathcal{A}_t \). Since \( s \in \ker \mathcal{A}_{n-k+3} \) it follows that the vector \( [0, \ldots, 0, s_0, \ldots, s_{n-k+2}, 0, \ldots, 0]' \), with \( k - 2 \) 0's to the left of \( s_0 \) and \( 2k - 3 \) 0's to the right of \( s_{n-k+2} \), has the property that the dot product of any \( 2k - 1 \) consecutive entries of this vector with \( d \) is 0 \( \mod 2 \). Using the flip-symmetry of both \( d \) and \( s \) it follows that the vector \( [0, \ldots, 0, s_0, \ldots, s_{n-k+2}, 0, \ldots, 0]' \), with \( 2k - 3 \) 0's to the left of \( s_0 \) and \( 2k - 3 \) 0's to the right of \( s_{n-k+2} \), has the property that the dot product of any \( 2k - 1 \) consecutive entries of this vector with \( d \) is 0. It follows that this vector must be one of the vectors \( y \) constructed in the preceding paragraphs. Therefore \( n - k + 2 \) must be of the form \( m - 2k + 2 \), i.e. \( n = m - k = js - k \).

**Remark 6.2.** Note that the sequence \( 0, \ldots, 0, v_0, y_1, \ldots \), with \( v_0 = 1 \) and with \( 2k - 3 \) 0's preceding \( v_0 \), is a linear recurring sequence corresponding to the vector \( [d_{n-1}, \ldots, d_1, d_0, d_1, \ldots, d_{n-2}] \) (see Definition 5.3). Given a vector \( c = [c_0, \ldots, c_{n-1}] \) with \( c_0 \neq 0 \) the linear recurring sequence generated by \( c \), with \( n \) initial entries \( 0, \ldots, 0, 1 \), is called an impulse response sequence. It is not difficult to show that the least period of the impulse response sequence is a multiple of the least period of any other linear recurring sequence generated by \( c \) as in Definition 5.3, [LN, Theorem 6.17]. One can also show, as is done in a specific case in the next corollary, that the least period of the impulse response sequence coincides with the order of the companion matrix below (cf. [LN, Theorem 6.17]).

\[
C' = \begin{bmatrix}
0 & 1 & 0 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & 0 & & 0 \\
0 & 0 & 0 & 1 & 0 & & 0 \\
& & & & & & \\
0 & 0 & 0 & 0 & 0 & \cdots & 0 \\
0 & c_0' & c_1' & \cdots & \cdots & \cdots & c_{n-1}'
\end{bmatrix}
\]
Corollary 6.3. For all positive integers $n$ such that $n \geq 2k - 2$, $\nu_{n+1} = \nu_n$. Hence the nullity sequence $\{\nu_n : n \in \mathbb{N}\}$ is eventually periodic, with period $s$.

Proof. For $n \geq 2k - 2$, the last $k - 1$ rows of the matrix $A_{n+1}$ are

$$
\begin{bmatrix}
0 & 0 & \cdots & 0 & d_{k-1} & d_{k-2} & \cdots & d_0 & \cdots & d_{k-2} \\
0 & 0 & \cdots & 0 & d_{k-1} & d_{k-2} & \cdots & d_1 & \cdots & d_{k-3} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & d_{k-1} & d_{k-2} & \cdots & d_0 & \cdots & d_0
\end{bmatrix}
$$

Call this matrix $Z_{n+1}$.

The remaining $n - k + 2 = n + 1 - (k - 1)$ rows of $A_{n+1}$ are

$$
\begin{bmatrix}
d_0 & d_1 & \cdots & d_{k-1} & 0 & \cdots & 0 \\
d_1 & d_0 & \cdots & d_{k-2} & d_{k-1} & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
d_{k-1} & d_{k-2} & \cdots & d_0 & d_1 & \cdots & d_{k-1} \\
0 & d_{k-1} & \cdots & d_0 & d_1 & \cdots & d_{k-1} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & d_{k-1} & d_{k-2} & \cdots & d_1 & d_0 & d_1 & \cdots & d_{k-1}
\end{bmatrix}
$$

Call this matrix $B_{n+1}$. Since $d_{k-1} \neq 0$, the matrix $B_{n+1}$ has maximal rank, so that its nullity is $k - 1$. Using the results on the impulse response sequence from the proof of the preceding theorem it is straightforward to see that the following vectors lie in the kernel of $B_{n+1}$: $[y_0, y_1, \cdots, y_n]^T$, $[0, y_0, y_1, \cdots, y_{n-1}]^T$, $[0, 0, y_0, \cdots, y_{n-2}]^T$, $[0, 0, \cdots, 0, y_0, \cdots, y_{n-k+2}]^T$. Call these vectors $y_0, \ldots, y_{k-2}$. Since $y_0 \neq 0$ these $k - 1$ vectors are linearly independent and therefore span the kernel of $B_{n+1}$. Hence if a vector $v$ lies in the kernel of $A_{n+1}$ it must be a linear combination of the vectors $y_0$ through $y_{k-2}$, and it also must lie in the kernel of $Z_{n+1}$. Suppose $v = \sum a_i y_i$ is any linear combination of these vectors. Let $z_i$ be the vector of length $2k - 2$ obtained by deleting all but the last $2k - 2$ entries of $y_i$. Clearly $v$ lies in the kernel of $Z_{n+1}$ if and only if $w = \sum a_i z_i$ lies in the kernel of the matrix $D$

$$
D = \begin{bmatrix}
d_{k-1} & d_{k-2} & \cdots & d_0 & \cdots & d_{k-2} \\
d_{k-1} & \cdots & d_0 & \cdots & d_{k-3} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \ddots \\
0 & \cdots & 0 & d_{k-1} & d_{k-2} & \cdots & d_0
\end{bmatrix}
$$
Hence the nullity \( r_n \) of \( A_{n+1} \) is the maximum number of linearly independent linear combinations \( v = \sum a_j y_j \) that can be formed such that \( w = \sum a_j z_j \) lies in the kernel of \( D \). Now consider the matrices \( A_{n+1+s} \), \( B_{n+1+s} \), \( Z_{n+1+s} \), and \( D \). It follows that the kernel of \( B_{n+1+s} \) is generated by the following vectors: \( [y_0, y_1, \ldots, y_{n+s}]^T \), \( [0, y_0, y_1, \ldots, y_{n+s-1}]^T \), \( [0, 0, y_0, \ldots, y_{n+s-2}]^T \), \ldots \( [0, 0, 0, \ldots, y_0]^T \). Call these vectors \( y_0, \ldots, y_{k-2} \).

Since the entries of the impulse response sequence are determined using the matrix \( C \) as in the preceding theorem, it follows that the last 2\( k-2 \) entries of the vectors \( y_j \), \( j = 0, \ldots, k-2 \), coincide with the last 2\( k-2 \) entries of \( y_j \). Hence the vector \( z_j \) obtained from \( y_j \) by deleting all but the last 2\( k-2 \) entries of \( y_j \) is equal to \( z_k \). Since \( v_{n+s} \) is the maximum number of linearly independent linear combinations \( w = \sum a_j z_j \) that lie in the kernel of \( D \), and since \( w' = w = \sum a_j z_j \), it follows that \( v_{n+s} = v_n \).

The paragraph above shows that \( \{v_n : n \in \mathbb{N}\} \) is eventually periodic and that \( s \) is a multiple of the period. By the preceding theorem, however, \( v_n = k-1 \) if and only if \( n = js - k \) for some \( j \in \mathbb{N} \), so the period cannot be less than \( s \). Hence \( \{v_n : n \in \mathbb{N}\} \) is eventually periodic with period \( s \).

**Remark 6.3.** One can show that the sequence \( \{v_n : n \in \mathbb{N}\} \) in Corollary 6.3 is actually periodic. Since the proof of the improved result is considerably longer than Corollary 6.3 we shall present its proof elsewhere.

**Example 6.1.** Suppose \( d_{k-1} = 1 \) and \( d_j = 0 \) for all other \( j \). Then \( C \) is the 2\( k-2 \) by 2\( k-2 \) permutation matrix

\[
\begin{pmatrix}
0 & 1 & 0 & 0 & \cdots & 0 \\
0 & 0 & 1 & 0 & \cdots & 0 \\
\vdots \\
0 & 0 & 0 & 0 & \cdots & 1 \\
1 & 0 & 0 & 0 & \cdots & 0 
\end{pmatrix}
\]

where period \( s \) is 2\( k-2 \). According to the theorem, then, \( v_n = k-1 \) for \( n \) of the form \( js - k \), for any positive integer \( j \), i.e., \( n \in \{k-2, 3k-4, 5k-6, \ldots\} \). By Corollary 2.10 the center sequence for the corresponding binary shift is 1, 2, \ldots, \( k-2 \), \( k-1 \), \( k-2 \), \ldots, 2, 1, 0 repeated infinitely often.

**Example 6.2.** Consider the bitstream 010100 \ldots, i.e., \( d_1 = d_3 = 1 \) and \( d_j = 0 \) for all other \( j \in \mathbb{Z}^+ \). Then \( k = 4 \), and the companion matrix of the theorem is the 6 by 6 matrix
which has order 8. According to the theorem \( v_n = 3 \) for \( n = 4, 12, 20, 28, ... \).

As an application of Corollary 2.10, the center sequence must have the form 10123210 repeated infinitely often.

**Theorem 6.4.** Let \( \sigma \) be a binary shift with commutant index \( k \), and let \( w = u^n_0 \cdots u^n_m \) be the word which generates \( \sigma^k(\mathbb{R}) \cap \mathbb{R} \), with \( r_m = 1 \). Then \( m = 0 \) if and only if the bitstream associated with \( \sigma \) is finitely nonzero. Otherwise, if \( m > 1 \), then for \( j > m \), set \( \delta_j = E^m_{j-m} \cdots E^1_{j-1-j} \). Let \( d_0 d_1 \cdots d_{k-2} 1000 \cdots \) be the bitstream for the derived shift \( \sigma_{\delta} \) (note \( d_{k-1} = 1 \)). Then for any \( n > m + k - 1 \) and for any \( j \) such that \( m < j \leq n - k + 1 \) the last column of the symmetric matrix \( E^i_{m-j+1} \cdots E^i_{n-1} \) has the form \([0, 0, 0, ..., 0, 1, d_{k-2} \cdots d_0]\). If \( m = 0 \) the last column of \( \sigma_{\delta} \) is already in this form.

**Proof.** The first claim of theorem is obvious. So we assume \( m > 0 \). We then have \( wu = (-1)^n u w \) where \( e_q \in F \) satisfies
\[
e_0 = r_0 a_0 + r_1 a_1 + r_2 a_2 + \cdots + r_m a_m,
\]
\[
e_1 = r_0 a_1 + r_1 a_0 + r_2 a_1 + \cdots + r_m a_{m-1},
\]
\[
e_2 = r_0 a_2 + r_1 a_1 + r_2 a_0 + \cdots + r_m a_{m-2},
\]
and so on. For \( q \geq k \), \( e_q = 0 \) modulo 2. Hence the last column of \( c_{n-1}^{i} \) is \([c_{n-1}, c_{n-2}, ..., e_1, 0]^t = [0, 0, ..., 0, 1, e_{k-2}, ..., e_1, 0]^t \) (note that left multiplication by \( c_{n-1}^{i} \) on \( \sigma_{\delta} \) has no effect on the last column except to make the last entry 0).

Now note that right multiplication by \( c_{n-2}^{i} \cdots c_{j+1}^{i} \) has no effect on the last column of \( c_{n-1}^{i} \). The last column of \( c_{n-2}^{i} \cdots c_{j+1}^{i} \) is the same as the last column of \( c_{n-1}^{i} \), except for the next-to-last entry, which is \( r_m e_{m+1} + r_{m-1} e_m + \cdots + r_1 e_1 \). Observe that (since \( r_0 = 1 \)) this is the exponent \( d_1 \) in the expression \( \sigma(w) = (-1)^{d_1} \sigma(w) \).

The last column of \( c_{n-2}^{i} \cdots c_{j+1}^{i} \) is the same as that for \( c_{n-1}^{i} \), with the exception of the second-to-last entry, which is \( r_m e_{m+1} + r_{m-1} e_{m+1} + \cdots + r_1 e_1 + e_1. \) This is the exponent \( d_2 \). Continuing in this fashion, we see that the following is the evolution of the last column, as one progresses from \( \sigma_{\delta} \) to \( c_{n-1}^{i} \) to \( c_{n-1}^{i} \) to \( c_{n-2}^{i} \cdots c_{j+1}^{i} \), and so forth. Note that the process stabilizes at the stage \( c_{n-k+1}^{i} \cdots c_{n-1}^{i} \cdots c_{n-k+1}^{i} \).
As a congruence of the proof of this theorem we obtain a matrix congruent to \( A_n \) with the form below.

**Corollary 6.5.** Same notation as above. Choose \( p \) such that \( p + 2k < n \). Then \( A_n \) is congruent to the following matrix \( B_n \). This congruence is implemented by \( \delta_{n-1} \cdots \delta_{p+k} \).

**Lemma 6.6.** Let \( \sigma \) be a binary shift of commutant index \( k \) whose derived shift has bitstream of the form \( d_0 d_1 \cdots d_{k-2} d_{k-1} \overline{0} \cdots \), where \( d_{k-1} = 1 \). Let \( p \) be a positive integer such that the following hold:

(i) \( m < p \),

(ii) the center sequence values, \( v_j \), coincide with those of \( \pi \) for \( j \geq p \),

(iii) \( A_p \) has full rank, i.e., \( v_p = 0 \), and the subsequent values of the center sequence are \( 1, \ldots, k-2, k-1, k-2, \ldots, 2, 1 \).
Then for \( n > p + 2k \) the matrix \( \mathcal{B}_n \) of the corollary is congruent to the matrix \( \mathcal{C}_n \) which has the same entries as \( \mathcal{B}_n \) except for its \( (p + 2k - 1) \) by \( (p + 2k - 1) \) upper corner, shown below.

\[
\begin{array}{cccc|c}
\mathcal{A}_p & a_0 & a_{p+1} & Z & E_O E_O E_O \\
\hline
a_0 & a_{p+1} & 0 & 0 & 1 \\
Z & E_O & E_O & 1 & 1 \\
E_O & E_O & 1 & 1 & 1 \\
\end{array}
\]

This congruence is implemented via a product of elementary transformations \( E_i \) with \( 1 \leq i \leq p + k - 2 \), and \( p \leq j \leq p + k - 2 \).

**Proof.** Consider the upper \( p + 2k - 1 \) by \( p + 2k - 1 \) submatrix of \( \mathcal{B}_n \) (where \( \mathcal{B}_n \) is the matrix of the lemma above) given below.

\[
\begin{bmatrix}
a_0 & a_1 & \cdots & a_{p+1}\n0 & a_0 & a_1 & \cdots & a_k\n0 & 0 & a_0 & a_1 & \cdots & a_k\n\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & a_0 & e_k-1\n0 & 0 & 0 & \cdots & e_k-1 & e_k-1\n0 & 0 & 0 & \cdots & e_k-1 & e_k-1\n0 & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & e_k-1 & e_k-1 \\
\end{bmatrix}
\]
Recall that since the center sequence of the corresponding shift has values
0, 1, 2, 3, ..., k \text{ as } v_q \text{ runs from } v_p \text{ to } v_{p+k-1}, \text{ there is a word } z = u_p^0 u_p^1 \cdots u_p^k \text{ which generates the center of the algebra } \mathfrak{U}_p+1 \text{ and which satisfies the following additional properties: (i) } [b_0, \ldots, b_p] \text{ is flip-symmetric, and (ii) } b_0 = b_p = 1. \text{ By Theorem 3.4, } z \text{ must commute with } u_0, \ldots, u_p, u_{p+1}, \ldots, u_{p+k-2} \text{ and anticommutes with } u_{p+k-1}. \text{ Consider the column vector } b = \{0, \ldots, 0, b_p, \ldots, b_0\} \text{ of length } p+k-1. \text{ It is easy to see that } b \text{ has dot product } 0 \text{ with all of the rows of } \mathfrak{U}_p+1. \text{ This is because } z \text{ commutes with } u_{p+k-2}, \ldots, u_0, \text{ and the exponent } q_j \text{ in the expression } u_j z = (-1)^q u_j \text{ is the dot product of row } p+k-2-j \text{ with } b.

In fact, } b \text{ has dot product } 0 \text{ with the subsequent } k-2 \text{ rows under } \mathfrak{U}_p+k-1 \text{ in the matrix above. First note that } b \text{ has dot product } 0 \text{ with the row vectors of length } p+k-1 \text{ obtained from the initial } p+k-1 \text{ entries of each of the } k-2 \text{ rows of } \mathfrak{U}_p+2k-1 \text{ above the last row of } \mathfrak{U}_p+2k-1. \text{ This follows from the fact that } z \text{ commutes with } u_{p+1}, \ldots, u_{p+k-2}. \text{ In the matrix above, however, the } k-2 \text{ rows under } \mathfrak{U}_p+k-1 \text{ were obtained from the original rows of } \mathfrak{U}_p+2k-1 \text{ by adding linear combinations of preceding rows. Since } b \text{ annihilates the first } p+k-1 \text{ entries of each of these rows, it annihilates the } k-2 \text{ rows under } \mathfrak{U}_p+k-1.

Hence if we consider the product } D_{p+k-2} = E_{p+k-2}^{b_p} E_{p+k-2}^{b_{p-1}} \cdots E_{p+k-3}^{b_{p-2}}, \text{ then the upper corner of } D_{p+k-2} \mathfrak{U}_p+k-2 \text{ will be

Continuing in this way, and defining } D_{p+j} = E_{p+j}^{b_p} \cdots E_{p+j}^{b_{j+1}} \text{ for } 1 < j < k-2, \text{ and } D_p = E_{p}^{b_p} \cdots E_{p-1}^{b_{p-1}}, \text{ similar calculations to the ones
above yield \( \mathcal{C}_n \) via \( \mathcal{C}_n = \mathcal{D}_p^1 \mathcal{D}_p^{p+1} \cdots \mathcal{D}_p^{p+k-2} \mathcal{E}_n \mathcal{D}_p^{p+k-2} \cdots \mathcal{D}_p^1 \mathcal{D}_p \) (note that the \( p \)th row (with the initial row counting as the 0th row) is replaced by \( [a_0, a_1, \ldots, a_p, 0, 0, \ldots] \) rather than all 0's since \( \mathcal{E}_n^{P} \mathcal{E}_0 \mathcal{D}_p \) is omitted from the expression for \( \mathcal{D}_p \)). Note also that any term \( \mathcal{E}_n^{P} \) in the expression for \( \mathcal{D}_p^{p+k-2} \cdots \mathcal{D}_p^1 \mathcal{D}_p \) has \( i \) and \( j \) as claimed in the statement above.

\[ \text{Notation.} \quad \text{We use } J_n \text{ to denote the } n \times n \text{ Toeplitz matrix which corresponds to the bitstream of the derived shift } \sigma_n, \text{ so that for } n \text{ sufficiently large, the initial row of } J_n \text{ has entries } 0, d_1, d_2, \ldots, d_k, 0, \ldots, 0. \]

\[ \text{Definition 6.1.} \quad \text{For } n \in \mathbb{N} \text{ let } J_n \text{ be the } n \times n \text{ triple diagonal matrix with 1's along the secondary diagonals and 0's on the main diagonal. Let } c_2 \text{ be the } 2 \times 2 \text{ matrix } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = J_2. \]

\[ \text{Lemma 6.7.} \quad J_n \text{ has rank } n \text{ if } n \text{ is even and rank } n - 1 \text{ if } n \text{ is odd.} \]

\[ \text{Proof.} \quad \text{Clear.} \]

\[ \text{Lemma 6.8.} \quad \text{Let } A \text{ be a symmetric matrix over } F \text{ with 0's along the main diagonal. Then } A \text{ has even rank. If } \text{rank}(A) = 2q \text{ then } A \text{ is congruent, via a product of elementary transformations, to the matrix consisting of } q \text{ copies of } J_2 \text{ along the main diagonal and 0's elsewhere. If } A \text{ is also symmetric with 0 diagonal, } A \text{ and } B \text{ are congruent if and only if they have the same rank.} \]

\[ \text{Proof.} \quad \text{From the proof of } [N, \text{Theorem IV.6}], A \text{ is congruent via a product of elementary matrices to a matrix with the desired form. It is obvious that rank is preserved under congruence, so } \text{rank}(A) = 2q \text{. The remaining claim is a restatement of } [N, \text{Theorem IV.11}]. \]

\[ \text{Lemma 6.9.} \quad \text{The } p \times p \text{ matrix } A_p \text{ is congruent to } J_p. \text{ This congruence is implemented via a product of elementary transformations } E_q \text{ satisfying } i, j \in \{1, 2, \ldots, p-1\}. \text{ In particular, } i \neq 0 \text{ and } j \neq 0. \]

\[ \text{Proof.} \quad \text{By the previous two lemmas, } A_p \text{ and } J_p \text{ are congruent. Since } A_p \text{ has full rank, one of the entries } a_{ij}, 1 \leq i, j \leq p-1, \text{ must be nonzero. If } a_{ij} = 0 \text{ then replace } A_p \text{ with the congruent matrix } E_{ij} A_p E_{ij} = E_{ij} A_p E_{ij}, \text{ to obtain a congruent matrix with 1's in the } (0,1) \text{ and } (1,0) \text{ positions. In order to eliminate any nonzero entries in the } (0, j) \text{ and } (j, 0) \text{ positions } (j > 1) \text{ multiply this matrix on the right by elementary matrices of the form } E_{ij} \text{ and on the left by their transposes. We obtain a matrix } A_{p1} \text{ congruent to } A_p \text{ with initial (0th) row and column all 0's except in the } (1,0) \text{ and } (0,1) \text{ positions. If } A_{p1} \text{ has no 1's in row 1 other than the } (1,0) \text{ entry then relabel } A_{p1} \text{ as } A_{p2}.} \]
and move on to row 2 and column 2. Otherwise use elementary transformations of the form $E_{22}$ or $E_{2j}$ with $3 \leq j \leq p - 1$ to obtain a matrix $A_{p2}$ congruent to $A_p$ and of the form

$$
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 \\
0 & 1 & & & * \\
0 & 0 & & & \\
\end{bmatrix}
$$

Hence $A_{p2}$ either has the form above or

$$
\begin{bmatrix}
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 \\
0 & 0 & & * \\
0 & 0 & & \\
\end{bmatrix}
$$

Continuing in this fashion, and using the fact that $A_p$ has full rank, it is clear that we can use products of elementary matrices of the required form to obtain a matrix $A_{pp}$ congruent to $A_p$ and having the form

$$
\begin{bmatrix}
\mathcal{J}_{k_1} & & 0 \\
& \mathcal{J}_{k_2} & \cdots \\
0 & & \mathcal{J}_{k_m} \\
\end{bmatrix}
$$

Since $p = \text{rank}(A_p) = \sum_{i=1}^{m} \text{rank}(\mathcal{J}_{k_i})$, each of the matrices $\mathcal{J}_{k_i}$ must have maximal rank. In particular, $\mathcal{J}_{k_i}$ has an even number of rows and columns. Since, by the previous lemmas, such an $\mathcal{J}_{k_i}$ is congruent to a matrix with 3’s along the main diagonal and 0’s elsewhere we may alter $A_{pp}$ using elementary transformations of the prescribed form to obtain a matrix $A’_{pp}$ congruent to $A_{pp}$ (and hence, to $A_p$) and of the form

$$
\begin{bmatrix}
\mathcal{J}_{k_1} & 3 & & 0 \\
& \mathcal{J} & & \cdots \\
0 & & \mathcal{J} & \\
\end{bmatrix}
$$
Let $R = E_{k_1+2,k_2}E_{k_1+4,k_2+2} \cdots E_{n,n-2}$. It is easy to check that $R' \varphi_{p \mu} R = \mathcal{Z}_p$. Hence we have shown that $\varphi_{p \mu}$ is congruent to $\mathcal{Z}_p$ using products of elementary column transformations of the prescribed form.

**Corollary 6.10.** The matrix $\varphi_{p \mu}$ of Lemma 6.6 is congruent, via a product of elementary transformations $E_{i,j}$, with $i,j \in \{1, \ldots, p-1\}$, to the matrix $M_p$ with the same entries as $\varphi_{p \mu}$ except for the upper left $p+1$ by $p+1$ corner, which is $\mathcal{Z}_{p+1}$.

**Proof.** Let $\varphi$ be the product of elementary transformations implementing the congruence between $\varphi_{p \mu}$ and $\mathcal{Z}_p$ in the lemma above. Then since the last row (respectively, column) of the matrix below agrees with the initial row (respectively, column), the matrix is

$$
\begin{bmatrix}
\varphi_{p \mu} & a_0 \\
 a_0 & a_{p-1} \\
 a_{p-1} & 0
\end{bmatrix}
$$

which is congruent via $\varphi$ to the following matrix:

$$
\begin{bmatrix}
\mathcal{Z}_p & 0 \\
0 & 1 \\
1 & 0 \\
0 & 0
\end{bmatrix}
$$

The latter matrix is then congruent, via $E_{2p}E_{4p} \cdots E_{p-2}$, to $\mathcal{Z}_{p+1}$.

**Theorem 6.11.** Let $\sigma$ be a binary shift with commutant index $k$. Suppose the center sequences of $\sigma$ and $\sigma_{\_t}$ are cofinal. Then for $n$ sufficiently large, the corresponding Toeplitz matrices $\varphi_{p \mu}$ for $\sigma$ and $\mathcal{J}_n$ for $\sigma_{\t}$ are congruent. With $p$ as in Lemma 6.6, and with $\varphi_\t$ as in Theorem 6.4, we have $\mathcal{T}_1 \varphi_{p+k-1} \varphi_{p+k-2} \cdots \varphi_{n-1} \mathcal{J}_n = \mathcal{J}_n$, where $\mathcal{T}_1$ is a product of elementary transformations of the form $E_{i,j}$, with $i,j \in \{1, \ldots, p+k-2\}$.

**Proof.** We may assume that $\sigma \neq \sigma_{\t}$. Then by Corollaries 6.5 and 6.10, there is a product $\mathcal{T}_1$ of elementary transformations of the form $E_{i,j}$ with $i,j \in \{1, \ldots, p+k-2\}$ such that $\mathcal{T}_1 \varphi_{p+k-1} \varphi_{p+k-2} \cdots \varphi_{n-1} \mathcal{J}_n = \mathcal{J}_n$. The form

$$
\begin{bmatrix}
\mathcal{Z}_p & 0 \\
0 & 1 \\
1 & 0 \\
0 & 0
\end{bmatrix}
$$

is congruent to $\mathcal{Z}_{p+1}$ via $E_{2p}E_{4p} \cdots E_{p-2}$. Therefore, $\mathcal{T}_1$ has the form

$$
\begin{bmatrix}
f_{p+k-1} & f_{p+k-2} \cdots f_{n-1} \\
f_p & f_{p+k-2} \cdots f_{n-1} \\
f_{p+k-2} & f_{p+k-3} \cdots f_{n-2} \\
& f_{p+k-3} \cdots f_{n-2} \\
& & f_{p+k-4} \cdots f_{n-3} \\
& & & & f_{n-3} \\
& & & & & f_{n-2} \\
& & & & & & f_{n-1}
\end{bmatrix}
$$

where $f_i$ is the $i$-th row of $\varphi_{p \mu}$.
Similarly, there is a product $\mathcal{F}$ of elementary transformations $E_{ij}$ with $i \neq j \in \{1, \ldots, p + k - 2\}$ such that $\mathcal{F}^t \mathcal{F}^{-1}$ is equal to the same matrix. Letting $\mathcal{F} = \mathcal{F}^t \mathcal{F}^{-1}$ establishes the result.

Definition 6.2. With $F$ the finite field of two elements, let $F^\infty$ denote the infinite-dimensional vector space consisting of finite linear combinations of the standard basis elements $e_i, i \in \mathbb{Z}^+$, which have 1 in the $i$th entry and 0's elsewhere. Let $F_0^\infty$ be the vector space spanned by $e_i, i \in \mathbb{N}$.

In the obvious way we shall view the finite-dimensional vector spaces $F_n^\infty, n \in \mathbb{Z}^+$, as embedded in $F^\infty$. Below we show that the congruences exhibited between the $A_n$'s and $J_n$'s above are compatible in the sense that one can define an invertible linear transformation $W$ on $F^\infty$ such that $W^t A_n W = J_n$ for all $n$ sufficiently large. Using this mapping (and a related map $\varphi$, see Definition 6.3 below) we shall be able to establish the cocycle conjugacy results of the next section.

Theorem 6.12. Let $\sigma$ be a binary shift with commutant index $k$ and derived shift $\sigma_{\sigma}$, and $\alpha = u_0 \alpha_1 \cdots u_m$ be a word generating $\sigma^\infty(R) \cap R$. Let $p$ be a fixed positive integer such that

(a) $\alpha$ has full rank;
(b) $m < p$;
(c) $2k < p$; and
Then for each \( n > p + 2k \) there is a product \( W_n \) of elementary transformations such that the following hold.

\[
\begin{align*}
W_n^{-1} e_j &= W_{n+1} e_j \quad \text{(i)} \\
W_n e_0 &= W_{n+1}^{-1} e_0 \quad \text{(ii)} \\
\text{if } 1 \leq j \leq n-1, \text{ then both } W_n e_0 \text{ and } W_n^{-1} e_0 \text{ lie in the linear span of the vectors } \{e_1, \ldots, e_{n-1}\} & \quad \text{(iii)} \\
\text{if } 1 \leq j \leq p+k-2, \text{ both } W_n e_j \text{ and } W_n^{-1} e_j \text{ lie in the linear span of the vectors } \{e_1, \ldots, e_{p+k-2}\} & \quad \text{(iv)} \\
\text{if } j \geq p+k \text{ then both } W_n e_j \text{ and } W_n^{-1} e_j \text{ lie in the linear span of the vectors } \{e_1, \ldots, e_k\} & \quad \text{(v)} \\
\text{if } S \text{ is the shift satisfying } S e_j = e_{j+1} \text{ for } j \in \mathbb{Z}^+, \text{ then for any } j \geq p+k, W_n S e_j = S W^j e_j, \text{ where } W = \lim W_n. & \quad \text{(vi)}
\end{align*}
\]

**Proof.** If \( \sigma = \sigma_\infty \) we simply choose \( W = I \). So we shall assume that \( \sigma \neq \sigma_\infty \), so that by Theorem 6.4, \( m > 0 \). For \( i, j \in \mathbb{Z}^+ \) we shall identify \( E_{ij} \) with the linear transformation on \( F^m \) which satisfies \( E_{ij} e_q = \delta_{ij} e_i + e_q \) on the elements \( e_i, e_q \in \mathbb{Z}^+, \) of the standard basis of \( F^m \). (Note that \( E_{ii}^{-1} = E_{ii} \).

We may represented \( E_{ij} \) as the infinite elementary transformation matrix with 1’s along the main diagonal, 1 in the \((i, j)\) position, and 0’s elsewhere. We shall also identify the matrices \( \alpha_n \) above with the infinite matrix which has \( \alpha_n \) in its upper left \( n \times n \) corner and 0’s elsewhere. Using the notation of the previous result, set \( W_n = \delta_{p-1} \cdots \delta_{p+k-1} F \). Then (o) is a restatement of Theorem 6.11. Since \( W_n \) consists of a product of transformations \( E_{ij} \) with \( i \neq 0 \) and \( j \neq 0 \), then \( W_n e_0 = W_{n+1}^{-1} e_0 \), giving (ii). Set \( \delta = \delta_{p-1} \cdots \delta_{p+k-1} \).

Then \( \delta^{-1} \) fixes \( e_1, \ldots, e_{p+k-2} \). Then \( \delta^{-1} e_j = e_{j+p} \) for \( 1 \leq j \leq p+k-2 \), so \( W_n^{-1} e_j = \delta^{-1} e_j = \delta e_j \) and \( \delta \) is in the vector subspace spanned by \( \{e_1, \ldots, e_{p+k-2}\} \). Since the same holds for \( F \alpha_n \) we have \( \delta \alpha_n = \delta \alpha_n = W_n \), and so (iv) holds. If \( p+k \leq j \leq n-1 \), \( W_n e_j = \delta_1 \cdots e_{p+k-1} = \delta_1 \cdots e_{p+k-1} = \delta_1 \cdots e_{p+k} \), which lies in the space spanned by the vectors \( \{e_1, \ldots, e_{p+k}\} \). Also \( W_n^{-1} e_j = \delta^{-1} e_j \) is a product of transformations \( E_{ij} \) with \( r, s \in \{1, 2, \ldots, f\} \), we have demonstrated both (ii) and (iv). Since \( \delta \) consists of a product of elementary transformations of the form \( E_{ij} \), with \( 1 \leq i \leq n-1 \), (i) follows from (iii).

Next suppose \( j \geq p+k \), then for \( n > j \), \( W_n e_{j+1} = \delta_{n-1} \cdots \delta_{p+k} F e_{j+1} = \delta_{n-1} \cdots \delta_{p+k} e_{j+1} = \delta_{j+1} e_{j+1} = S(\delta e_j) = S(\delta e_j) = S W_n e_j \), giving (vi).
We shall use the notation $F_0^\infty$ to denote the subspace of $F^\infty$ spanned by the vectors $e_j$, where $j \in \mathbb{N}^+$, and the notation $\varphi$ to be the mapping $W^{-1}SW^{-1}$ on $F_0^\infty$.

**Corollary 6.13.** $\varphi$ is an invertible linear transformation on $F_0^\infty$ which satisfies $\varphi(e_j) = e_{j}$ for $j \geq p + k$.

**Proof.** First we verify that $\varphi$ maps $F_0$ into itself. To see this note that by (ii) of the theorem, $\varphi(e_1) = W^{-1}SWe_1 = W^{-1}e_1$, and by (iv), $W^{-1}e_i \in F_0^\infty$. For $j \geq 1$, $\varphi(e_{j+1}) = W^{-1}SWe_j \in W^{-1}SF_0^\infty \subset W^{-1}F_0^\infty \subset F_0^\infty$. $\varphi$ is obviously injective. Surjectivity follows from combining injectivity with parts (iv) and (v) of the theorem. The last claim is simply a restatement of part (vi) of the theorem.

**7. COCYCLE CONJUGACY RESULTS**

As above, let $k \in \mathbb{N}$ be a fixed positive integer, $\sigma$ a binary shift of commutant index $k$, and $\sigma^\infty$, its derived shift (see Section 5). Corresponding to the derived shift are the bitstream $d_0d_1 \cdots d_{k-2}d_{k-1}0 \cdots$ ($d_{k-1} = 1$, $d_k = d_{k+1} = \cdots = 0$), the $\sigma^\infty$-generators $u_j$, $j \in \mathbb{Z}^+$, and the $n$ by $n$ Toeplitz matrices $f_n$, $n \in \mathbb{Z}^+$. Corresponding to $\sigma$ we fix the bitstream $a_0a_1 \cdots$, $\sigma$-generators $v_j$, $j \in \mathbb{Z}^+$, and Toeplitz matrices $A_n$, $n \in \mathbb{Z}^+$. In this section we make the standing assumption that the center sequences corresponding to $\sigma$ and $\sigma^\infty$ are cofinal. Therefore we may apply the results of the previous section, particularly Theorem 6.12, to show that any shift $\sigma$ satisfying these is cocycle conjugate to its derived shift, Theorem 7.12. The cocycle conjugacy is obtained by applying the congruence of the pair of quadratic forms associated with the pair of Toeplitz matrices $A_n$ and $J_n$. We use this congruence to construct an inner automorphism of $R$ which implements the cocycle conjugacy, Corollary 7.11. As a preliminary result, we prove the following lemma, for which we need the following notation.

**Definition 7.1.** Given a vector $s = s_0e_0 + s_1e_1 + \cdots + s_mE_m \in F^\infty$, let $\chi(s)$ be the word $u_0^s \cdots u_m^s$ in $R$.

**Lemma 7.1.** Let $f$ be the infinite matrix whose upper $n$ by $n$ corner is $f_n$, for all $n \in \mathbb{N}$. Then for any $s, t \in F^\infty$, $s^t f \neq t$ if and only if $\chi(s)$ and $\chi(t)$ commute.

**Proof.** It is immediate that $e_i^t f e_j = d_{|i-j|}$ for $i, j \in \mathbb{Z}^+$ (where $d_q = 0$ for $q \geq k$), whereas $\chi(e_i) \chi(e_j) = u_iu_j = (-1)^{|i-j|}u_iu_j$ (see Section 1). The
conclusion holds for general words $\chi(s)$ and $\chi(t)$ by using the linearity of the quadratic form induced by $\mathcal{A}$ on $F^\omega$. □

The following lemma uses the mapping $\chi$ to translate the linear algebra results in Theorem 6.12 to information about the generators for $\sigma_\omega$ and for $\sigma$.

**Lemma 7.2.** Notation as in Theorem 6.12. For $i \in \mathbb{Z}^+$, let $w_i$ be the word in the generators $\{u_j\}$ of $\sigma_\omega$ given by $w_i = \chi(W^{-1}e_i)$. Then the words $w_i$ satisfy the following:

(i) for $i, j \in \mathbb{Z}^+$, $w_i$ and $w_j$ commute if and only if $v_i$ and $v_j$ do;

(ii) $w_0 = u_0$;

(iii) $R$ is generated as a von Neumann algebra by the $w_j$'s; and

(iv) for $j \geq 1$, $w_j \in \sigma,(R)$.

**Proof.** One calculates as in the preceding lemma that $e_i^t \mathcal{A} e_j = a_{i-j}$. Setting $s = \chi(W^{-1}e_i)$ and $s' = \chi(W^{-1}e_j)$ and using Theorem 6.12(a) we compute $(W^{-1}e_i)^t \mathcal{A} (W^{-1}e_j) = e_i^t (W^{-1})^t \mathcal{A} W^{-1}e_j = e_i^t \mathcal{A} e_j = a_{i-j}$. Hence we have obtained (i). (ii) follows from Theorem 6.12(ii). (iii) follows from the invertibility of $W^{-1}$, and (iv) follows from part (iii) of Theorem 6.12. □

**Lemma 7.3.** Let $\varphi$ be as in Definition 6.3. Then for $i, j \in \mathbb{N}$, $\varphi(e_i)^t \mathcal{A} \varphi(e_j) = d_{i-j}$.

**Proof.** It is clear from the symmetry of the Toeplitz matrix $\mathcal{A}$ that $(Sx)^t \mathcal{A} Sy = x^t \mathcal{A} y$ for any $x, y \in F^\omega$. Then

$$\varphi(e_i)^t \mathcal{A} \varphi(e_j) = (W^{-1}SWS^{-1}e_i)^t \mathcal{A} (W^{-1}SWS^{-1}e_j)$$

$$= (SWS^{-1}e_i)^t (W^{-1})^t \mathcal{A} W^{-1}(SWS^{-1}e_j)$$

$$= (SWS^{-1}e_i)^t \mathcal{A} (SWS^{-1}e_j)$$

$$= (WS^{-1}e_i)^t \mathcal{A} (WS^{-1}e_j)$$

$$= (W e_{i-1})^t \mathcal{A} (W e_{j-1})$$

$$= e_{i-1}^t \mathcal{A} e_{j-1}$$

$$= e_{i-1}^t \mathcal{A} e_j$$

But by the calculation in the proof of Lemma 7.1, $e_i^t \mathcal{A} e_j = d_{i-j}$. □
Using the mapping \( \varphi \) one can define an automorphism on \( \sigma_n(R) \). This is done as follows. Setting \( y_j = \varphi(e_j), j \in \mathbb{N} \), it follows from Theorem 6.12 that \( y \), lies in \( \sigma_n(R) \). Multiplying \( y \), by \( \sqrt{-1} \), if necessary, we may assume that \( y \), is hermitian. By the lemma above, the words \( u_i \in \sigma_n(R) \) satisfy the same pairwise anticommutation relations as do the words \( y_j, j \in \mathbb{N} \). Define a mapping \( \pi \) takes ordered words \( u = u_1^n \cdots q_n^a \) in \( \sigma_n(R) \) to \( y = y_1^n \cdots y_a^n \) (also in \( \sigma_n(R) \)). Since the anticommutation relations are preserved by the mapping \( \pi \) it is not difficult to show that \( \pi \) extends by linearity to a \( * \)-isomorphism of \( \sigma_n(R) \) into itself. Since \( \varphi \) is invertible on \( F^a_n \), it follows that \( \pi \) is actually a \( * \)-automorphism of \( \sigma_n(R) \). The following results (7.4 through 7.11) are dedicated to showing that, up to a period 2 automorphism which takes any word \( w \) in \( \sigma_n(R) \) to \( \pm w \), the automorphism \( \pi \) is inner on \( \sigma_n(R) \), see Corollary 7.11 below.

**Lemma 7.4.** Let \( n \in \mathbb{N} \) be such that \( \mathcal{A}_n = \{u_0, \ldots, u_{n-1}\}^n \) is a factor. Then for any \( i \) such that \( 0 \leq i < n - 1 \), there exists a word \( w \) in the generators \( u_0, \ldots, u_{n-1} \) such that \( w \) anticommutes with \( u_i \) and commutes with \( u_{i+1}, \ldots, u_{n-1} \).

**Proof.** There are \( 2^n \) distinct words in \( \mathcal{A}_n \). Since \( \mathcal{A}_n \) is a factor, at least one word anticommutes with \( u_{n-1} \), hence exactly \( 2^{n-1} \) do. At least half of those which commute with \( u_{n-1} \) also commute with \( u_{n-2} \). Continuing, one sees that at least \( 2^{n-i-1} \) words commute with \( u_{i+1}, \ldots, u_{n-1} \). Suppose all of these commute with \( u_i \), then at least \( 2^{n-i-1} \) words commute with \( u_i, \ldots, u_{n-1} \). At last half of these commute with \( u_{n-1} \). Continuing this way, we see that at least \( 2 \) words commute with \( u_0, \ldots, u_{n-1} \). Hence there is a nontrivial word in the center of \( \mathcal{A}_n \), contradicting the property that \( \mathcal{A}_n \) is a factor. This contradiction yields the results.

**Proposition 7.5.** Let \( \sigma, \sigma_n \) be as above. Let \( n \in \mathbb{N} \) be such that both \( \mathcal{A}_n \) and \( \mathcal{A}_{n+2k-2} \) are factors with center sequence values \( 0, 1, \ldots, k-2, k-1, k-2, \ldots, 1, 0 \) starting at \( v_n \) and ending at \( v_{n+2k-2} \) (possible by Theorem 6.2). Let \( z \in \mathcal{A}_{n+1} \) be the word which generates the center of \( \mathcal{A}_{n+1} \). Then there are \( k-1 \) words \( U_j \in \{u_{n+k-1}, \ldots, u_{n+2k-3}\}^n \) and \( k-1 \) words \( z_j \in \{z, \sigma(z), \ldots, \sigma^{k-2}(z)\}^n \) such that (i) if \( A \) is a product of any subset of the words \( Z_j U_j \), then either \( A \) is trivial or does not lie in \( \{z, \sigma(z), \ldots, \sigma^{k-2}(z)\}^n \), (ii) the words \( Z_j U_j \) generate the relative commutant algebra \( \mathcal{A} = \mathcal{A}_n \cap \mathcal{A}_{n+2k-2} \cap \{u_{n+k-1}, \ldots, u_{n+2k-3}\}^n \).

**Proof.** One can argue as in the proof above to see that there are precisely \( 2^{2k-2} \) distinct words in \( \mathcal{A}_n \cap \mathcal{A}_{n+2k-2} \). It is not difficult to see that the words \( z, \sigma(z), \ldots, \sigma^{k-2}(z), u_{n+k-1}, \ldots, u_{n+2k-3} \) all lie in this algebra, so a dimension argument shows that they generate the algebra. Since \( \mathcal{A} \) is a subalgebra of this algebra, it is generated by words which can be formed in this algebra.
Observe from Theorem 3.4 that \( z \) commutes with \( u_0, \ldots, u_{n+k-1} \), and since \( z \in \mathfrak{A}_{n+1} \) (and since \( \sigma_n \)'s bitstream is 0 past \( d_{k-1} = 1 \), it commutes with the successive \( \sigma_n \)-generators \( u_{n+k}, u_{n+k-1}, \ldots \)). It follows from this observation that each of the generators \( u_{n+k-1}, \ldots, u_{n+2k-3} \) anticommutes with one and only one among the list \( z, \sigma(z), \ldots, \sigma^{k-2}(z) \), so that no nontrivial word in \( \{ z, \sigma(z), \ldots, \sigma^{k-2}(z) \} \) lies in \( \mathfrak{A} \). This gives (i). Also as in the proof above, there are \( 2^k-1 \) distinct words in \( \mathfrak{A} \). This gives (ii).

**Corollary 7.6.** Let \( n \) be as above, but sufficiently large so that \( \pi(u_q) = u_q \) for \( q \geq n \). Let \( \pi' \) be the automorphism on \( R \) obtained by setting \( \pi' = \sigma_n^{-1} \pi \sigma_n \). Suppose \( y_n \in \mathfrak{A}_n \) (respectively, \( y_{n+2k-2} \in \mathfrak{A}_{n+2k-2} \)) satisfies \( \text{Ad}(y_n) \mathfrak{A}_n = \mathfrak{A}_n \) (respectively \( \text{Ad}(y_{n+2k-2}) = \mathfrak{A}_{n+2k-2} \)). Then the unitary element \( y_n^* y_{n+2k-2} \) lies in the algebra \( \mathfrak{A} \).

**Proof.** The initial hypothesis implies that \( y_{n+2k-2} \) commutes with \( u_{n+k-1}, \ldots, u_{n+2k-2} \). The bitstream for \( \sigma_n \) is 0 past the entry \( d_{k-1} = 1 \) so that \( y_n \) also commutes with these elements. Hence \( y_n^* y_{n+2k-2} \) does, too. Since \( \text{Ad}(y_{n}) \) and \( \text{Ad}(y_{n+2k-2}) \) agree on \( \mathfrak{A}_n \), \( y_n^* y_{n+2k-2} \) commutes with the elements of \( \mathfrak{A}_n \), and so must be in \( \mathfrak{A} \).

**Definition 7.2.** For any word \( w \) in the \( u_i \)'s let \( \Gamma_{\pm}(w) \) be the unitary operators in \( R \) given by \( \Gamma_{\pm}(w) = (1/\sqrt{2})(I \pm iw) \), if \( w = w^* \); and \( \Gamma_{\pm}(w) = (I \pm iw)/\sqrt{2} \), if \( w^* = -w \).

**Lemma 7.7.** Same notation as in the definition. Then for \( i \geq 0 \),

\[
\Gamma_{\pm}(w) u_i \Gamma_{\pm}(w) = u_i, \quad \text{if } w, u_i \text{ commute,}
\]

\[
= cu_iw, \quad \text{if } w, u_i \text{ anticommute,}
\]

where \( c \) is one of the scalars \( \pm 1, \pm \sqrt{-1} \).

**Proof.** It is clear that both \( \Gamma_{\pm}(w) \) and \( \Gamma_{\pm}(w) \) are unitary elements of \( R \). If \( u_i \) commutes with \( w \) then \( u_i = \Gamma_{\pm}(w) u_i \Gamma_{\pm}(w) \). Now suppose \( u_i \) anticommutes with \( w \). Assuming that \( w^* = -w \), then

\[
\Gamma_{\pm}(w) u_i \Gamma_{\pm}(w) = ([I+w]/\sqrt{2}] u_i ([I-w]/\sqrt{2}) = u_i ([I-w]/\sqrt{2}) [([I-w]/\sqrt{2}) = -u_i w.
\]

Similarly, \( \Gamma_{\pm}(w) u_i \Gamma_{\pm}(w) = u_i w, \) and similar calculations hold for the case \( w^* = w \), when \( \Gamma_{\pm}(w) = (I \pm iw)/\sqrt{2} \).

**Theorem 7.8 (cf. [PP2, Theorem 3.7]).** Let \( \sigma, \sigma_n \) be as above and let \( n \in \mathbb{N} \) be chosen so that \( \mathfrak{A}_n \) is a factor. Suppose \( x \in \mathfrak{A}_n \) is a unitary element
with the property that $x^*wx$ is a scalar multiple of a word in $\mathfrak{A}_n$, for all words $w$ in $\mathfrak{A}_n$. Then $x$ is a finite product of terms of the following form:

(i) $I_w$, where $w$ is a word in $\mathfrak{A}_n$;

(ii) $cI$, for some $c \in \mathbb{T}$; or

(iii) $w$, a word in $\mathfrak{A}_n$.

Remark 7.1. Following the terminology of Section 3 of [PP2] we say that $x$ normalizes the words of $\mathfrak{A}_n$, and write $x \in NN(\mathfrak{A}_n)$ (cf. Definition 1.4 and Theorem 1.6).

Proof. First observe, by the preceding lemma, that conjugation by any element of the form (i) carries a word into a scalar multiple of a word. The same is obvious for any elements of the form (ii) or (iii).

Suppose $r$ is the largest integer for which $x \in \sigma_r^n(R) \cap \mathfrak{A}_n$. If $r = n$, $x$ is a scalar multiple of the identity, and we are done. Otherwise, $x$ may be written as $x = u + vu_r$, where $u, v \in \sigma_r^n(R) \cap \mathfrak{A}_n$, and $v \neq 0$. If $u = 0$, then since conjugation by $vu_r$ carries words of $\mathfrak{A}_n$ into scalar multiples of words, we may assume by replacing $x$ with $vu_r$, that $x$ lies in $\sigma_r^n(R)$. Hence we assume $x = u + vu_r$ with $u \neq 0$ and $v \neq 0$. Since $x$ is unitary,

$$I = xx^* = uu^* + vv^* + uu_r v^* + vu_r u^*.$$  

Let $\Phi$ denote the conditional expectation of $R$ onto $\sigma_r^n(R)$: Then $\Phi(uu_r v^* + vu_r u^*) = u\Phi(u_r) v^* + v\Phi(u_r) u^* = 0$, so we derive the two equations

$$I = uu^* + vv^*, \quad \text{and} \quad (7.1)$$

$$0 = uu_r v^* + vu_r u^*. \quad (7.2)$$

From Lemma 7.4 we may choose a word $w$ of $\mathfrak{A}_n$ which commutes with $u_{r+1}, \ldots, u_n$ and which anticommutes with $u_r$. Then

$$xw^* w = (u + vu_r) (w^* + u_r v^*) w^* = (u + vu_r) ww^*(u_r v^* - u v^*)$$

$$= (uu^* - vv^*) + (vu_r u^* - uu_r v^*). \quad (7.3)$$

Taking the conditional expectation $\Phi$ of this expression we see, since $xw^* w$ is a word in $\sigma_r^n(R)$, that either $uu^* - vv^* = 0$, or $vu_r u^* - uu_r v^* = 0$. Using (7.2), the latter equation is equivalent to $vu_r u^* = 0$. We divide our argument into these two cases.

Case (i). $uu^* - vv^* = 0$. This equation, along with (7.1), yields $uu^* = vv^* = 1/2I$. It follows that $vu_r u^* - uu_r v^*$ is a word, and so we conclude from (7.2) that the element $z = 2vu_r u^*$ of $\mathfrak{A}_n$ is a scalar multiple of a word.
(Note that (7.2) also implies that $z^* = -z$.) Hence $zu = 2vu, u^*u = vu$.
(since $2u^*u$ and $2uu^* = I$ are equivalent projections in the hyperfinite $II_1$
factor $R$, and therefore $2u^*u = I$). Hence

$$x = u + vu = u + zu = [(I + z)/\sqrt{2}] \sqrt{2}u.$$ 

Note that $\sqrt{2}u$ is a unitary element of $\mathfrak{H} \cap \sigma^\infty_1(R)$, and also that conju-
gation by this element normalizes words of $\mathfrak{H}$. Hence we have replaced $x$
with an element $u \in \sigma^\infty_1(R)$ which also normalizes words of $\mathfrak{H}$ under conju-
gation.

*Case (ii).* $uu^* \neq vv^* \neq 0$. Arguing as in the first case we see that
since $xwx^*w^*$ is a scalar multiple of a word, either $uu^* - vv^* = 0$, or $vu^*, vu^* = 0$. Hence $vu, vu^* = uu, vv^*$.
and combining this equation with (7.2) we obtain $uu^* - vv^* = I$.
and consequently $uu^* - vv^* = I$ is a scalar multiple of a word in $\mathfrak{H}$. Since $uu^* - vv^*$ is also hermitian, $uu^* - vv^* = 2E - I$, for some
hermitian projection $E$. Since $uu^* + vv^* = I$, we have obtained the following
three equations:

$$uu^* = E$$
$$vv^* = I - E$$
$$vu^*, vu^* = 0.$$

Let $y$ be a word in $\sigma_\infty^r(R) \cap \mathfrak{H}$, but not in $\sigma^\infty_1(R)$, i.e., $y$ has the generator
$u$, in its decomposition as a product of scalars and generators. Without loss
of generality we may assume $y^* = -y$. Since $x$ normalizes $\mathfrak{H}$, so does
$\Gamma_+(y)x$, and we have

$$\Gamma_+(y)x = [(I + y)/\sqrt{2}](u + vu)$$
$$= (1/\sqrt{2})(u + yvu) + (1/\sqrt{2})(yu + vu).$$

Observe that $u + yvu$ lies in $\sigma^\infty_1(R)$, and that $yu$ has the form $Tu_u$, for
some $T \in \sigma^\infty_1(R)$, so the above expression takes the form $\Gamma_+(y)x = u' + v'u_u$, where
$u' = (1/\sqrt{2})(u + yvu), v' = (I/\sqrt{2})(yu + v), and u', v' \in \sigma^\infty_1(R)$.

We have

$$uu^* = 1/2[(u + yvu)(u^* + u,v^*y*)]$$
$$= 1/2[(uu^* + yvv^*y*) + (yvu,u^* + uu,v*y*)]$$
$$= 1/2(uu^* + yvv^*y*),$$

since $vu_u = 0$. If $y$ commutes with $vv^* = I - E$, then $u'v' = 1/2[uu^* + vv^*]$

$$= 1/2[E + (I - E)] = 1/2I.$$

Similarly $v'v^* = 1/2I$. Therefore the element $\Gamma_+(y)x = u' + v'u_u$ satisfies the conditions of Case (i), to which we may replace $\Gamma_+(y)x$
with the element $u'$ which lies in $\sigma_{n-k}^{-1}(R)$ and which normalizes the words of $\mathfrak{U}_n$. On the other hand, if no such $y$ commutes with $E$, then every element of the form $u_y v$ commutes with $E$, so $E$ lies in the center of the subalgebra $\{u_{k+1}, \ldots, u_{n+1}\}$.

Since $u$ is also in this algebra, $u u_t = E = u^* u$. Similarly, $v^* v = I - E = E v^* v$.

Since $2E - I$ anticommutes with $u$, we obtain $u u^* u u_t = v^* v$. But since $v u = u^* = 0$ we get $0 = v^* u u_t u u_t = v^* v v^* = v^*$. Similarly, $u u_t = 0$. Then $0 = u u^* u + v^* v = u u^* + v v^* = I$, which is absurd, and we are done.

**Corollary 7.9.** The element $y^*_n y^*_{n+2k-2}$ in Corollary 7.6 lies in $NN(\mathfrak{U}_{n+2k-2}) \cap \mathfrak{U}_n$.

**Proof.** Both $\text{Ad}(Y_n)$ and $\text{Ad}(Y^*_{n+2k-2})$ normalize the words in their respective factors $\mathfrak{U}_n$ and $\mathfrak{U}_{n+2k-2}$. Since $\mathfrak{U}_n = \mathfrak{U}_{n+2k-2}$ we are done.

**Theorem 7.10.** Let $n$ be as in Theorem 6.12 (in particular, such that $\pi(u_q) = u_q$ for $q \geq n$). For all words $w$ in the generators $u_j$, $j \in \mathbb{Z}^+$, $\text{Ad}(Y^*)^n(w) = \pm \pi(w)$, where $Y = Y_n$, and where $\pi$ is as in Corollary 7.4.

**Proof.** By definition of $Y^*$, $\text{Ad}(Y^*)^n | \mathfrak{U}_n = \pi^n | \mathfrak{U}_n$ and by the assumption on the bitstream of $\sigma_{\infty}$, $\text{Ad}(Y^*)$ is trivial on $\sigma_{n-k}^{n+k-1}(R)$. Hence we need only show that $\text{Ad}(Y^*)(u_j) = \pm u_j = \pm \pi(u_j)$ for $n \leq j \leq n + k - 2$. Note that $\text{Ad}(Y^*_{n+2k-2})$ acts trivially on these generators, so that $\text{Ad}(Y^*_{n+2k-2})$ agrees with $\text{Ad}(Y^*)$ on these $u_j$'s. Hence $w = \text{Ad}(Y^*)(u_j) = \text{Ad}(Y^*_{n+2k-2})(u_j)$ is simultaneously (i) a word, by the preceding corollary, (ii) in the algebra generated by $\mathfrak{U}_n$ and $u_j$ (and must include $u_j$, since it is of the form $w = \text{Ad}(Y^*)(u_j)$ with $Y^* = \mathfrak{U}_n$), and (iii) in the algebra generated by $\mathfrak{U}_n$ and $u_j$. Hence one sees that $w$ is a word of the form $\pm (Z_1 U_1)^1 \cdots (Z_k U_k)^{k-1} u_j$, where the $Z_i$'s and $U_i$'s are as in Proposition 7.5. The product $(Z_1 U_1)^1 \cdots (Z_k U_k)^{k-1}$ cannot lie in $\mathfrak{U}_n$ by (i) of the proposition, however, unless $r_1 = \cdots = r_{k-1} = 0$.

**Corollary 7.11.** Let $Y^*$ be as above, and let $Y = \sigma_{\infty}(Y^*)$. Then $\text{Ad}(Y)(w) = \pm \pi(w)$ for all words $w$ in the $\sigma_{\infty}$-generators $u_1, u_2, \ldots$.

**Proof.** Write $w' = \sigma_{\infty}^{-1}(w)$, then by the theorem, $\text{Ad}(Y^*)^n(w') = \pm \pi(w') = \pm \sigma_{\infty}^{-1} \circ \sigma_{\infty}(w') = \pm \sigma_{\infty}^{-1} \circ \pi(w)$. Taking $\sigma_{\infty}$ of both sides gives the result.

**Theorem 7.12.** The endomorphism $\text{Ad}(Y) : \sigma$ is a binary shift on $R$ which is conjugate to $\sigma_{\infty}$. Hence $\sigma$ and $\sigma_{\infty}$ are cocycle conjugate.

**Proof.** By Theorem 6.12 and Definition 7.1, $w_i = u_0 = \chi(W^{-1} v_0)$, and for $j \in \mathbb{N}$, $w_j$ is a scalar multiple of the word $\chi(W^{-1} v_j)$ in the generators $u_i$, $i \in \mathbb{N}$. The $w_i$'s satisfy the same commutation relations $w_i w_k = (-1)^{n-k-i} w_k w_i$, as do the $v_i$'s.
We prove by induction that $\operatorname{Ad}(Y) \cdot \sigma_{w_j}(w_j) = \pm w_{j+1}$. First, 

\[
\operatorname{Ad}(Y) \cdot \sigma_{w_0}(w_0) = Y^*u_1 Y = \pm \pi(u_1) = \pm \chi(\sigma(e_1)) = \pm \chi(W^{-1}SWS^{-1}e_1) \\
= \pm \chi(W^{-1}Se_0) = \pm \chi(W^{-1}e_1) = \pm w_1.
\]

Suppose $\operatorname{Ad}(Y) \cdot \sigma_{w_j}(w_j) = \pm w_{j+1}$ for $0 \leq j \leq k - 1$. Since $\sigma \cdot Y = Y \cdot S$ on $F_0^\infty$, 

\[
\operatorname{Ad}(Y) \cdot \sigma_{w_k}(w_k) = \pm \operatorname{Ad}(Y)(\sigma_{w_k}(\chi(W^{-1}e_k))) = \pm \operatorname{Ad}(Y)(\chi(SW^{-1}e_k)) \\
= \pm \pi(\chi(SW^{-1}e_k)).
\]

Since 

\[
\pi \cdot Y \big| F_0^\infty = \pm \chi \cdot \phi \big| F_0^\infty,
\]

\[
\operatorname{Ad}(Y) \cdot \sigma_{w_k}(w_k) = \pm \chi(\phi(SW^{-1}e_k)) = \pm \chi(W^{-1}SWS^{-1}(SW^{-1}e_k)) \\
= \pm \chi(W^{-1}w_{k+1}) = \pm w_{k+1}.
\]

Hence the induction holds. By Lemma 7.2, $R = \{w_0, w_1, ..., w_n\}$, so $\operatorname{Ad}(Y) \cdot \sigma_{w_j}$ is a binary shift. Since the generators $\pm w_j$ of $\operatorname{Ad}(Y) \cdot \sigma_{w_j}$ satisfy the same commutation relations as the $\sigma$-generators $e_j$ do, $\operatorname{Ad}(Y) \cdot \sigma_{w_j}$ is conjugate to $\sigma$ by [Po, Theorem 3.6].

Corollary 7.13 (cf. [Pr, Corollary 4.10]). All binary shifts of commutant index 2 are cocycle conjugate.

Proof. Let $\sigma$ be a binary shift of commutant index 2. Then $\sigma_{w_j}$ has bitstream 0100 $\ldots$. By Lemma 6.2 and Corollary 2.10, the center sequence $[v_{n\sigma}]$ for $\sigma$ must eventually be of the form 101010 $\ldots$. Similarly for $\sigma_{w_j}$. By Proposition 2.4, Toeplitz matrices over $F$ with 0 diagonal have even rank, so by Theorem 3.4, $v_n$ is 0 for even $n$ and $v_n$ is 1 for odd $n$. Similarly for $\sigma_{w_j}$. Hence the center sequences for $\sigma$ and its derived shift are cofinal. But then by the theorem, $\sigma$ and $\sigma_{w_j}$ are cocycle conjugate. If $\tau$ is any other binary shift of commutant index 2, note that $\tau_{w_j}$ and $\sigma_{w_j}$ have the same bitstreams, so they are conjugate [Po, Theorem 3.6]. Since $\tau$ and $\tau_{w_j}$ are cocycle conjugate, and since $\tau_{w_j}$ and $\sigma_{w_j}$ are conjugate, it follows that $\sigma$ and $\tau$ are cocycle conjugate.

Corollary 7.14 (cf. [BY, Theorem 1.2]). There are at least $2^{k-2}$ distinct cocycle conjugacy classes of binary shifts of commutant index $k$.

Proof. There are $2^{k-2}$ distinct bitstreams which are finitely nonzero and which correspond to binary shifts $\sigma$ of commutant index $k$. These are the bitstreams of the form $0d_1 \cdot \cdot \cdot d_{k-2}d_{k-1}00 \cdot \cdot \cdot$. This is verified by noting
that if \( u_j \) are the \( \sigma \)-generators, then \( u_0 \in \sigma^k(R) \cap R \), but \( \sigma^{k-1}(R) \cap R = CI \). By Theorem 5.9, a necessary condition for a pair of shifts to be cocycle conjugate is that their derived shifts are conjugate. But since \( \sigma = \sigma_w \), and since distinct bitstreams give rise to nonconjugate binary shifts (Theorem 1.8), each of these binary shifts lies in a distinct cocycle conjugacy class.

Remark 7.2. We remark that not every binary shift of finite commutant index has a center sequence which is cofinal with the center sequence of the corresponding derived shift. For example, the center sequence corresponding to the shift whose bitstream is 00100\( \cdots \) is 12101210\( \cdots \) (see Example 6.1), and the center sequence corresponding to the shift with bitstream 01100\( \cdots \) is 101210101210\( \cdots \). Using an approach related to the congruence proofs of the previous section, R. T. Powers and the author (unpublished) have shown the following.

1. Suppose \( \sigma \) is a binary shift of commutant index 3 whose derived shift \( \sigma_\omega \) has bitstream 0010\( \cdots \). Then the center sequence corresponding to \( \sigma \) is cofinal with either 12101210\( \cdots \) or with 21012101210\( \cdots \). Examples of the latter type do exist!

2. Suppose \( \sigma \) is a binary shift of commutant index 3 whose derived shift \( \sigma_\omega \) has bitstream 0110\( \cdots \). Then the center sequence corresponding to \( \sigma \) is cofinal with one of the following: 101210\( \cdots \), 121010\( \cdots \), or 101012\( \cdots \). Examples of each type occur.

We conjecture that a pair of binary shifts of the same finite commutant index are cocycle conjugate if and only if their derived shifts are conjugate and their center sequences are cofinal.

ACKNOWLEDGMENTS

The author is grateful to Sigmund Vik for a careful reading of the manuscript, to Alexis Alevras for pointing out an error in the original manuscript, and to Robert T. Powers for many helpful conversations.

REFERENCES

SHIFTS ON THE HYPERFINITE $II_1$ FACTOR


