ON SOME ASPECTS OF COCYCLIC SUBSHIFTS, LANGUAGES, AND AUTOMATA

by

David Bryant Buhanan

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Mathematics

MONTANA STATE UNIVERSITY
Bozeman, Montana

June, 2012
APPROVAL

of a dissertation submitted by

David Bryant Buhanan

This dissertation has been read by each member of the dissertation committee and has been found to be satisfactory regarding content, English usage, format, citations, bibliographic style, and consistency, and is ready for submission to The Graduate School.

Dr. Jaroslaw Kwapisz

Approved for the Department of Mathematical Sciences

Dr. Kenneth L. Bowers

Approved for The Graduate School

Dr. Carl Fox
STATEMENT OF PERMISSION TO USE

In presenting this dissertation in partial fulfillment of the requirements for a doctoral degree at Montana State University, I agree that the Library shall make it available to borrowers under rules of the Library. I further agree that copying of this dissertation is allowable only for scholarly purposes, consistent with “fair use” as prescribed in the U.S. Copyright Law. Requests for extensive copying or reproduction of this dissertation should be referred to ProQuest Information and Learning, 300 North Zeeb Road, Ann Arbor, Michigan 48106, to whom I have granted “the exclusive right to reproduce and distribute my dissertation in and from microform along with the non-exclusive right to reproduce and distribute my abstract in any format in whole or in part.”

David Bryant Buhanan

June, 2012
DEDICATION

To Charlie, Willie, and Caixia.
ACKNOWLEDGEMENTS

I am grateful to all of the people I have worked with at Montana State University. Special thanks are due to my committee members Lukas Geyer, Marcy Barge, Tomas Gedeon, and Mark Pernarowski for their questions and suggestions. Most importantly, I am thankful to my thesis advisor Jarek Kwapisz for his help, support, and encouragement.

Also thanks to my wife and children for their patience and support.
# TABLE OF CONTENTS

1. INTRODUCTION ........................................................................................................ 1

2. DIOPHANTINE EQUATIONS AND COCYCLIC SUBSHIFTS ........................... 11
   Preliminaries ........................................................................................................... 11
   Diophantine Equations .......................................................................................... 13
   Correspondence Theorem ..................................................................................... 15
   Undecidability ......................................................................................................... 24
   Incompleteness ....................................................................................................... 28
   Strictly Cocyclic Subshifts and Diophantine Equations ........................................ 29
   Post Correspondence Problem and the Mortal Matrix Theorem ............................ 33

3. ALGEBRAIC PRELIMINARIES ........................................................................... 37
   Decompositions of Finite Dimensional Algebras .................................................. 37
   The Radical and Semisimplicity ............................................................................ 44
   Semisimple Part of an Algebra .............................................................................. 48
   More on Principal Modules and Module Decomposition ..................................... 51
   Miscellaneous Algebraic Results .......................................................................... 53

4. MORSE DECOMPOSITION OF COCYCLIC SUBSHIFTS ................................. 56
   Wedderburn Decomposition of Cocyclic Subshifts ............................................... 56
   Connections ........................................................................................................... 66
   The Connecting Graph ............................................................................................ 71
   Minimal Algebras and Transitivity of Connecting Diagrams .................................. 75
   Non-Unital Algebras ............................................................................................... 79
   SFT and Edge Shifts ............................................................................................... 84
   Composition Series and Connecting Diagrams ..................................................... 86
   Dynamical Disjointness ......................................................................................... 87
   Aperiodic Decomposition and Connecting Diagrams ............................................ 90
   Computation and Examples .................................................................................. 95

5. LANGUAGES AND COCYCLIC SUBSHIFTS .................................................... 99
   Background ............................................................................................................. 99
   Languages of Deterministic and Nondeterministic Cocycles .............................. 102
   Cocyclic Automata and Languages ...................................................................... 106
   Cocyclic Languages and Subshifts ....................................................................... 118

REFERENCES CITED ............................................................................................ 123
# LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Simple Connecting Diagram</td>
<td>7</td>
</tr>
<tr>
<td>4.1 Connecting Diagram</td>
<td>74</td>
</tr>
<tr>
<td>4.2 Gabriel’s Quiver</td>
<td>75</td>
</tr>
<tr>
<td>4.3 Non-transitive Connecting Diagram</td>
<td>75</td>
</tr>
<tr>
<td>4.4 Sofic System with Corresponding Non-Unital Algebra</td>
<td>83</td>
</tr>
<tr>
<td>4.5 Graph for $X_\psi$</td>
<td>84</td>
</tr>
<tr>
<td>4.6 Sofic system</td>
<td>89</td>
</tr>
<tr>
<td>4.7 Example</td>
<td>94</td>
</tr>
<tr>
<td>4.8 Connecting Graph - Simple Loop</td>
<td>96</td>
</tr>
<tr>
<td>4.9 Non-transitive Connecting Diagram</td>
<td>97</td>
</tr>
</tbody>
</table>
ABSTRACT

In this thesis we examine the class of cocyclic subshifts. First, we give a method of modeling the zeros of Diophantine equations in the multiplication of matrices. This yields many examples, and a proof that there is no algorithm than can decide if two cocyclic subshifts are equal. Next, we use the theory of finite dimensional algebras to give an algebraic technique for finding connecting orbits between topologically transitive components of a given cocyclic subshift. This gives a very complete picture of the structure of the dynamical system associated to the cocyclic subshift. Last, we characterize the languages of cocyclic subshifts via cocyclic automata, in an analogous manner to the characterization of the languages of sofic subshifts which have languages accepted by finite automata. Our automaton definition is closely related to definitions in the field of quantum computation.
INTRODUCTION

The long-term behavior of many dynamical systems can be well described by coding the system by a symbolic system, a procedure that goes back to at least Morse and Hedlund [30]. See [27, p.201] for an expositional introduction to coding. Coding involves partitioning the space into pieces and associating to each orbit the sequence of pieces visited by it. The collection of all of the possible sequences together with the shift map is a dynamical system. If the coding is done well, the symbolic system retains many properties of the original system, while being easier to manage. This technique was perhaps most famously employed in the proof that entropy is a complete metric invariant for toral automorphisms, see [1].

Symbolic systems were first introduced for coding, and after coding had proven useful, symbolic dynamics as an area in itself became interesting. Since symbolic systems could be used to give information about other systems, it became important to understand the behavior of symbolic systems. Symbolic systems also arise naturally in the study of formal languages, an area in theoretical computer science. Although the theory of formal languages deals primarily with finite sequences of symbols (instead of infinite sequences), there are many parallels in the two theories and they benefit from each other. In this thesis we seek to understand the structure of symbolic systems that belong to the class of cocyclic subshifts.

We start with the definition of the shift space. Let \( \mathcal{A} \) be a finite alphabet, that is a finite set of symbols. Then the space \( \mathcal{A}^\mathbb{Z} \) of infinite sequences with values in \( \mathcal{A} \) and indexed by the integers \( \mathbb{Z} \) is a compact metric space with

\[
d(x, y) = \begin{cases} 
2^{-k} : & \text{if } x \neq y \text{ and } k \text{ maximal so that } x_{[-k,k]} = y_{[-k,k]} \\
0 : & \text{if } x = y
\end{cases}
\]
(Here $x[i,j] := x_ix_{i+1} \ldots x_j$ for $i \leq j$.) The full (two-sided) shift is the collection $A^\mathbb{Z}$ together with the shift map $f$ given on $x = \ldots x_2x_{-1}.x_0x_1x_2\ldots \in A^\mathbb{Z}$ by $f(x) = (y_i)_i$ with $y_i = x_{i+1}$. We also look at $A^\mathbb{N}$, where $\mathbb{N}$ are the natural numbers, with the shift map and refer to this system as the full (one-sided) shift. The one-sided shift space is also a metric space with the metric above modified to only check equality on $x[1,k]$ and $y[1,k]$.

A subset of the full shift which is closed and invariant under the shift map is known as a subshift. Before continuing with the discussion of specific classes of subshifts we provide the basic definitions needed for understanding the languages of subshifts. For the alphabet $A$ a word or block over $A$ is a finite sequence of the form $w = w_1 \ldots w_k$ for $k \in \mathbb{N}$. We also allow for a word with no letters, $\epsilon$, which we call the empty word.

For words $w$ and $v$ we write $w \sqsubseteq v$ if $w$ is a subword of $v$, i.e. $v = uwz$ for some words $u, z$. Define

$$
A^+ := \{w_1w_2\ldots w_k | k \in \mathbb{N}, w_i \in A\}, \quad A^* = A^+ \cup \{\epsilon\}.
$$

A language $\mathcal{L}$ over $A$ is a subset of $A^*$. A language $\mathcal{L}$ is said to be extendable if for any word $w \in \mathcal{L}$ there is some non-empty word $v \in A^*$ such that $wv \in \mathcal{L}$. $\mathcal{L}$ is said to be factorial if for any word $w \in \mathcal{L}$, if $v \sqsubseteq w$ then $v \in \mathcal{L}$. Let $X$ be a subshift over $A$, a word $w \in A^*$ occurs if there exists $x \in X$ with $w \sqsubseteq x$, i.e. $w$ is a subword of $x$. Now the language of $X$ is defined by

$$
\mathcal{L}(X) := \{w \in A^* | \exists x \in X \text{ with } w \sqsubseteq x\}.
$$

One of the most important classes of subshifts is the class of sofic systems. Let $G$ be a graph consisting of vertices and directed edges where each edge has an element of the alphabet as a label. Then the one-sided subshift of the graph $G$ consists of the elements $x = x_1x_2x_3\ldots$ that correspond to an infinite walk over the directed edges.
Sofic systems are exactly the subshifts that can be produced in terms of these labeled, directed graphs. The original definition of sofic subshifts in terms of semigroups can be found in [36]. They were introduced as the smallest class of subshifts containing subshifts of finite type that is closed under factoring.

The definition of sofic shifts in terms of graphs is very closely related to the definition of finite automata. Finite automata can also be thought of as labeled, directed graphs with a distinguished subset of so called accepting vertices and a distinguished initial vertex. An automaton recognizes a given word over the alphabet $\mathcal{A}$ if and only if it is the label of a walk on the graph which terminates at an accepting vertex. The *language of the automaton* is the set of all words that the automaton recognizes or accepts. A language is known as *regular* if and only it is recognized by a finite automaton. Thus the definition of sofic shifts as subshifts with regular languages is equivalent to the definition in terms of graphs. For more on finite automata, regular languages and sofic subshifts see [24]. In what follows, all of these definitions will provide a guiding analogy for our work.

The concept of the cocyclic subshift, originally defined in [26], is a natural extension of the idea of sofic shifts where linear algebra takes the place of graph theory. More precisely, let $V$ be a finite dimensional vector space and, for each $a \in \mathcal{A}$, let $\Phi_a \in \text{End}(V)$ where $\text{End}(V)$ is the set of all linear maps from $V$ to itself. We refer to the tuple $\Phi = (\Phi_a)_{a \in \mathcal{A}}$ as a *cocycle*. The (one-sided) *subshift of the cocycle* $\Phi$ is given by

$$X_\Phi := \{x \in \mathcal{A}^\mathbb{N} | \Phi_{x_1} \cdots \Phi_{x_n} \neq 0, \forall n \in \mathbb{N}\}.$$ 

The class of cocyclic subshifts can be seen in a natural way as an extension of the class of sofic subshifts. However, generalization from graph theory is non-trivial. In the case of sofic subshifts the Fischer graphs allow for the identifying of different
shifts and seeing if two shifts are the same in an algorithmic way, see [27, p.90]. In Chapter Diophantine Equations and Cocyclic Subshifts, we will see that there is no general algorithm that can determine if two cocyclic subshifts are equal. We will show there is no such algorithm by applying the celebrated DPRM Theorem. An account of the history and mathematics behind the DPRM Theorem can be found in [28].

We also give another proof that there is no algorithm that can decide if two cocyclic subshifts are the same by using the mortal matrix theorem due to M.S. Paterson [31].

A Diophantine equation is an equation of the form $D(x_1, \ldots, x_m) = 0$ where $D(x_1, \ldots, x_m)$ is a polynomial with integer coefficients. Diophantine equations have been studied since antiquity, and many methods have been found for solving specific types of equations. The DPRM Theorem states that there is no general algorithm that can decide, given a Diophantine equation, if the equation has a solution in non-negative integers.

We give a method of writing matrices corresponding to a Diophantine equation $D = 0$ so that some product of the matrices is zero if and only if the equation $D = 0$ has a solution. Our method is inspired by [2] and its gist can be grasped by the following very simple example.

Example: Let $D(x, y) = x - y = 0$. $x - y$ can be thought of as a linear combination of basis vectors $1, x,$ and $y$ and we take $V$ to be linear space of all such combinations. Let $A = \{0, 1, 2\}$ and let $\Phi_1$ be the map that sends $1 \mapsto 1$, $x \mapsto x + 1$, and $y \mapsto y$. So, in the chosen basis, we write $\Phi_1 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Note that, throughout this thesis, matrices multiply on the right of row vectors. In an analogous way we take $\Phi_2$ to be the linear map which sends $1 \mapsto 1$, $x \mapsto x$, and $y \mapsto y + 1$. In our basis, we get
\[
\Phi_2 = \begin{bmatrix}
1 & 0 & 0 \\
0 & 1 & 0 \\
1 & 0 & 1
\end{bmatrix}.
\]
We also define \(\Phi_0\) as the map which takes \(1 \mapsto x - y, x \mapsto 0\) and \(y \mapsto 0\) so that \(\Phi_0 = \begin{bmatrix}
0 & 1 & -1 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix}\). Note that the left hand side of the Diophantine equation itself appears as the image of 1 under \(\Phi_0\). The key idea of this construction is that for products of the form \(\Phi_0 \Phi_1 \Phi_2 \Phi_0\) we get 0 if and only if \(D(a, b) = 0\) (for \(a, b \in \mathbb{N}_0\)). Below we will see that \(X_\Phi\) is an example of a strictly cocyclic subshift, i.e. a subshift which is cocyclic but not sofic. There is essentially one such example in the literature, but via the method of associating a cocyclic subshift to a Diophantine equation and applying Theorem 2.23 we can easily manufacture concrete examples.

The method of associating a cocyclic subshift to a Diophantine equation is formalized in Theorem 2.7. We then apply the DPRM Theorem to get a proof of the following theorem,

**Theorem.** There is no algorithm that, given a cocycle \(\Phi\) of matrices with integer entries, can decide if the subshift \(X_\Phi\) is the full shift.

In chapter Morse Decomposition of Cocyclic Subshifts we extend results in [26], where spectral decompositions of the recurrent set of the cocyclic subshift is computed based on the decomposition of a semisimple algebra into a direct sum of simple algebras. We give an analogue of the classical Morse decomposition of the subshift itself including non-recurrent dynamics. (For background on Morse Decomposition see [9], [8], and [15].) The idea is to create a graph with vertices representing irreducible components and directed edges representing dynamical connections between the components. A dynamical connection is given by an orbit under the shift map.
that backward accumulates on the component represented by the initial vertex and forward accumulates on the component represented by the target vertex of the directed edge. This work is also inspired by the method of communicating classes for sofic subshifts, see [27].

Our main tool for finding these dynamical connections comes from the representation theory of finite dimensional algebras. The details of this theory may be found in [13] and [10] and we survey the results we need in Chapter Algebraic Preliminaries. For a given cocycle $\Phi$ we define the algebra of the cocycle to be the sub-algebra $A$ of $\text{End}(V)$, the algebra of all endomorphisms of $V$, generated by the elements $\Phi_a$ where $a \in A$. An element $e$ of a finite dimensional algebra $A$ is said to be idempotent if $e^2 = e$. Idempotents $e$ and $f$ are said to be orthogonal if $ef = fe = 0$. An idempotent $e$ is said to be primitive if $e = f + g$ where $f$ and $g$ are both idempotents implies that either $f$ or $g$ is equal to zero.

If $1 \in A$ then there is a decomposition $1 = e_1 + e_2 + \ldots + e_p$, where for each $i$, $e_i$ is a primitive idempotent; and $e_i$ and $e_j$ are orthogonal for $i \neq j$. This decomposition of $1$ corresponds to a decomposition of $A$ as a module over itself. As an $A$-module we have $A = e_1A \oplus \ldots \oplus e_pA$ and $A = Ae_1 \oplus \ldots \oplus Ae_p$. The simple modules of $A$ are given by the modules $e_iA/e_i\text{rad}(A)$. After possible renumbering, we may assume that $\{e_1A/e_1\text{rad}(A), \ldots, e_nA/e_n\text{rad}(A)\}$ for some $n \leq p$ is a complete collection of simple modules, i.e. it represents all isomorphism classes of such modules. In Chapter Morse Decomposition of Cocyclic Subshifts, we show that these modules correspond to irreducible components $X_1, \ldots, X_n$, which are topologically transitive subshifts of $X_\Phi$, the union of which constitutes the recurrent set denoted by $X_+$. A connecting orbit from $X_i$ to $X_j$ is one for which the $\alpha$-limit set is a subset of $X_i$ and the $\omega$-limit set is a subset of $X_j$. We define the relation $\to$ on
the set \{1, \ldots, n\} by \(i \to j\) if and only if \(e_iAe_j \neq 0\). Then the main theorem of Chapter Morse Decomposition of Cocyclic Subshifts, Theorem 4.16, is as follows.

**Theorem.** For any \(i \neq j\) with \(i, j \in \{1, \ldots, n\}\), we have \(i \to j\) if and only if there is a connecting orbit from \(X_i\) to \(X_j\).

The following simple example illustrates the basic idea. We examine a cocyclic subshift presented by matrices

\[
\Phi_0 = \begin{bmatrix}
-2 & 0 \\
0 & 0
\end{bmatrix}, \quad \Phi_1 = \begin{bmatrix}
0 & 3 \\
0 & 0
\end{bmatrix}, \quad \Phi_2 = \begin{bmatrix}
0 & 0 \\
0 & -9
\end{bmatrix}.
\]

The algebra \(A\) that is generated by \(\Phi = (\Phi_0, \Phi_1, \Phi_2)\) is given by matrices of the form

\[
\begin{bmatrix}
a & b \\
0 & c
\end{bmatrix}
\]

where \(a, b, c \in \mathbb{C}\). We take idempotents \(e_i\) to be the matrix with 1 in the \(i, i\) entry and zero elsewhere, for \(i = 1, 2\). We have \(1 = e_1 + e_2\), with \(e_1A = \begin{bmatrix}
a & b \\
0 & 0
\end{bmatrix}\) and \(e_2A = \begin{bmatrix}
0 & 0 \\
0 & c
\end{bmatrix}\). So there are two irreducible components and since \(e_1Ae_2 = \begin{bmatrix}
0 & b \\
0 & 0
\end{bmatrix}\) \(\neq 0\) and \(e_2Ae_1 = 0\) we get the connecting diagram:

![Diagram](https://via.placeholder.com/150)

Figure 1.1: Simple Connecting Diagram

For the above example the decomposition is very natural and the computations are predictable. In general, the connecting graph is not easily divined by inspection of the given cocycle. Thus, Theorem 4.16 gives a computational tool to find connections that would otherwise be very difficult to find. We indicate at the end of Chapter 4 how one can determine the connecting diagram using computational algebra software. We
also refine the method to give a connecting diagram that shows connections between aperiodic components, see Theorem 4.44.

In Chapter 5 we seek to characterize the languages of cocyclic subshifts. Our inspiration for the theory of cocyclic languages comes from both regular languages, see [22, 25], and quantum languages [29]. Historically, regular languages have been of great interest in theoretical computer science and the practice of computer programming where they enter through the formalism of regular expressions. They also have tremendous importance in symbolic dynamics since a language is regular and the language of a subshift if and only if it is the language of a sofic system. In this thesis, we are able to give a characterization of cocyclic languages in terms of what we call cocyclic automata, of which finite automata are a subclass.

A cocyclic automaton consists of a finite dimensional vector space $V$, a cocycle $\Phi = (\Phi)_{a \in A}$ with values in $\text{End}(V)$, an initial vector $v$, and a projection $P \in \text{End}(V)$. We write the automaton as a 4-tuple, $Q = (V, \Phi, v, P)$. A word $w \in A^*$ is accepted by $Q$ if $v\Phi_wP \neq 0$, where $\Phi_w = \Phi_{w_1} \cdots \Phi_{w_n}$ if $w = w_1 \cdots w_n$ and $w_i \in A$. The language $L(Q)$ is the collection of all words that are accepted by $Q$. For an example of a cocyclic automaton we again consider Diophantine equations.

Example: Let $V$ be the vector space of linear combinations of the basis $(1, x, y)$. Let $v = [0, 1, -1]$ and $\Phi = (\Phi_1, \Phi_2)$ where these matrices are the same as defined in the first example. Let $P$ be the projection that takes $1 \mapsto 1$, $x \mapsto 0$, and $y \mapsto 0$. We get $v\Phi_1^a\Phi_2^bP = 0$ if and only if $\Phi_0\Phi_1^a\Phi_2^b\Phi_0 = 0$. Therefore the automaton $Q = (V, \Phi, v, P)$ accepts the language $\{w \in A^* | n_1(w) \neq n_2(w)\}$, where $n_1(w)$ is the number of 1’s that occur in $w$ and $n_2(w)$ is the number of 2’s that occur in $w$.

We get the following proposition inspired by the analogous theorem for sofic systems (see Theorem 5.29 and DD Hypothesis on page 66):
Theorem. If $L$ is the language of a cocyclic subshift satisfying (DD) then $L$ is a cocyclic language.

Because of the definition of cocyclic languages in terms of linear maps, there is a close connection to quantum computing. Our definition of automata that recognize cocyclic languages is very close to that of generalized quantum automata found in [29]. The viewpoint is different because the quantum automata lead to cocycles where words are accepted if the cocycle vanishes with the probability above a certain threshold, called the cutpoint. Our theory corresponds to a cutpoint of 0, see [4]. The cutpoint is the minimal certainty with which the quantum computation, which is inherently nondeterministic, has to succeed.

For a language $L$ the Kleene Star of $L$ is the set

$$L^* := \{ w \in A^* | \exists w_1, \ldots, w_n \in L, \text{ with } w = w_1 \ldots w_n \}.$$ 

The class of all regular languages forms a Kleene Algebra, see Definition 5.23 and [23]. That is, regular languages are closed under union, concatenation, and Kleene star. We define non-deterministic cocyclic automata by allowing more than one possible map for each $a \in A$. This is done formally by taking cocycles with values in the semigroup of linear subspaces in $\text{End}(V)$. Non-deterministic languages are languages recognized by non-deterministic cocyclic automata. We show that the class of non-deterministic cocyclic languages also satisfies all the closure properties in the definition of Kleene algebra. Thus we get Theorem 5.24 stated below.

Theorem. Let $K$ be the collection of all non-deterministic cocyclic languages. For any $\alpha, \beta \in K$ let $\alpha + \beta = \alpha \cup \beta$. Take $\alpha \cdot \beta$ to be the concatenation $\alpha \beta$ and $\alpha^*$ to be the Kleene star. Let $0 = \emptyset$ and $1 = \{ \epsilon \}$. With these definitions $(K, +, \cdot, 0, 1, *)$ is a Kleene algebra.
Kleene algebras are an important part of dynamic algebra which algebraically models program behavior. See [20, p. 418] for the history of Kleene algebras, regular languages, and the importance of Kleene algebras in logic as applied to computer science.
Diophantine Equations and Cocyclic Subshifts

Preliminaries

Subshifts of finite type and sofic systems have been widely studied and have found application in many areas of mathematics, see [27]. In this thesis we explore the class of cocyclic subshifts, which includes all sofic systems and subshifts of finite type. In this chapter we review the basic definitions and theory. We then give a new way of generating cocyclic subshifts, which we use to prove some undecidability results.

Let \( A \) be a finite alphabet of symbols often taken as \( A = \{1, \ldots, m\} \). A word \( w \) of letters from \( A \) is a concatenation of letters of the form \( w = w_1w_2 \ldots w_k \) where \( w_i \in A \) for each \( i \). We refer to \( k \) as the length of the word \( w \). We also allow for the case of a word with no letters, the \textit{empty word} denoted by \( \epsilon \). The set of all words with letters in \( A \) together with the empty word is denoted by \( A^* \).

The \textit{one-sided shift} over \( A \) is the product space \( A^\mathbb{N} \) with the shift map \( f : A^\mathbb{N} \to A^\mathbb{N} \) given by \( f : (x_i)_{i \in \mathbb{N}} \mapsto (x_{i+1})_{i \in \mathbb{N}} \). Likewise, the \textit{two-sided shift} over \( A \) is the product space \( A^\mathbb{Z} \) together with the shift map \( f : (x_i)_{i \in \mathbb{Z}} \mapsto (x_{i+1})_{i \in \mathbb{Z}} \). For an element \( x \) of the shift space and for \( i \leq j \) (\( i, j \in \mathbb{Z} \)), we write \( x[i,j] := x_i x_{i+1} \ldots x_j \).

A subshift \( X \) of the full shift is a closed subset (in the product topology) of the full shift which is invariant under the shift map, i.e. \( f(X) = X \). One way to generate subshifts is by considering the collection of all elements of the full shift which miss some collection of words. Formally, for any \( F \subset A^* \) the subset of the full shift \( X_F = \{ x \in A^\mathbb{Z} | \text{ no subword of } x \text{ is in } F \} \), assuming \( X_F \) is non-empty, is also shift invariant and is a subshift. \( F \) is referred to as a \textit{forbidden set} for the subshift \( X_F \). Note that different forbidden sets may generate the same subshift. A subshift \( X \) is called a \textit{subshift of finite type} if \( X = X_F \) for a forbidden set \( F \) of finite cardinality.
For any subshift $X$ the *language of $X$*, denoted by $\mathcal{L}(X)$, is the collection of all words that occur in some element of the subshift $X$.

Let $V$ be a finite dimensional vector space over a field $\mathbb{C}$, and let $\text{End}(V) = \{T : V \to V \mid T \text{ is linear}\}$. That is, $\text{End}(V)$ is the collection of linear endomorphisms from $V$ to itself. We will compose linear maps in $\text{End}(V)$ on the right. Thus for $v \in V$ and $\Phi, \Psi \in \text{End}(V)$ we have $\Phi(\Psi(v)) = v \Psi \Phi$. The following definition is fundamental to this thesis and was first formulated in [26].

**Definition 2.1.** Let $A$ be an alphabet and $m := \#A$. Then the *(one-sided) cocyclic subshift of $\Phi = (\Phi_i)_{i \in A} \in \text{End}(V)^m$ is the subshift $X_\Phi \subset A^\mathbb{N}$ given by

$$X_\Phi := \{x \in A^\mathbb{N} \mid \Phi_{x_1} \cdots \Phi_{x_n} \neq 0, \forall n \in \mathbb{N}\}.$$ 

A subshift $X \subset A^\mathbb{N}$ is a *(one-sided) cocyclic subshift iff $X = X_\Phi$ for some $\Phi$.

The *(two-sided) cocyclic subshift of $\Phi$ is the subshift $X'_{\Phi}$ given by

$$X'_{\Phi} := \{x \in A^\mathbb{Z} \mid \Phi_{x_{-n}} \cdots \Phi_{x_n} \neq 0, \forall n \in \mathbb{N}\}.$$ 

A subshift $X' \subset A^\mathbb{Z}$ is a *(two-sided) cocyclic subshift iff $X' = X'_{\Phi}$ for some $\Phi$.

For each $w \in A^*$ we use the notation $\Phi_w := \Phi_{w_1} \Phi_{w_2} \cdots \Phi_{w_k}$ where $w = w_1 \ldots w_k$ with $w_i \in A$ for each $i$. For the special case of the empty word $\epsilon$, we take $\Phi_\epsilon = \text{Id} \in \text{End}(V)$.

We can also view cocyclic subshifts from the more general viewpoint of cocycles. Let $\Phi : \mathbb{N} \times A^\mathbb{N} \to \text{End}(V)$ be a *locally constant cocycle* with values in the semigroup $\text{End}(V)$. In other words, there is a $q \in \mathbb{N}$ and $\Phi_{i_1 \ldots i_q} \in \text{End}(V), i_j \in A, j = 1, \ldots, q$, such that

$$\Phi(n, x) = \Phi_{x_1 \ldots x_q} \Phi_{x_2 \ldots x_{q+1}} \cdots \Phi_{x_n \ldots x_{n+q-1}}, \quad x \in A^\mathbb{N}, n \in \mathbb{N}.$$
The minimal such $q$ is called the *anticipation of $\Phi$*. The set

$$\{ x \in A^\mathbb{N} | \Phi(n, x) \neq 0, \forall n \in \mathbb{N} \}$$

is called the *support of $\Phi$*. Note that for $q = 1$ the support of $\Phi$ is the cocyclic subshift of $\Phi$. We quote the following proposition found in [26], and refer the reader to the proof found there.

**Proposition 2.2.** [26] The class of cocyclic subshifts of $A^\mathbb{N}$ coincides with that of the supports of locally constant cocycles on $A^\mathbb{N}$.

In what follows we refer to an $m$-tuple $\Phi = (\Phi_a)_{a \in A}$ as a *cocycle*. Given $\Phi = (\Phi_a)_{a \in A}$, a natural set of forbidden words is $F_\Phi = \{ w \in A^* | \Phi_w = 0 \}$. Then $X_\Phi = X_{F_\Phi}$.

### Diophantine Equations

We use a method inspired by the work of David Anick [2] to encode a Diophantine Equation into a collection of matrices that then can be used to generate a cocyclic subshift. This method is quite fruitful as it yields examples of non-sofic cocyclic subshifts which can be easily understood. Also this method allows for the application of the DPRM Theorem to multiplication of matrices, which yields several results about the non-existence of algorithms to determine basic properties of cocyclic subshifts.

We begin with a discussion of Diophantine equations. A *Diophantine equation (D.E.)* is an equation of the form $D(x_1, ..., x_m) = 0$ where $D(x_1, ..., x_m)$ is a polynomial in $m$ variables with integer coefficients. We are concerned only with solutions of such an equation which are $m$-tuples of nonnegative integers. Thus a D.E. is said to have no solutions if it has no solution which consists of an $m$-tuple of nonnegative integers. We will refer to the nonnegative integers as natural numbers and denote them by $\mathbb{N}_0$. 
There are many well known examples of Diophantine equations. For example each of the equations of the form, $x^n + y^n = z^n$ for $n \geq 3$, is a Diophantine equation. In 1900 Hilbert famously gave a list of problems that he saw as the most important problems for the next century. Number ten on the list was to find an algorithm for determining if a Diophantine equation has a solution. In the following we refer to problems in a more technical way. A decision problem consists of at most countably many subproblems, each of which should be answered “Yes” or “No” where each subproblem is given by a finite amount of information. Hilbert’s tenth problem can thus be rephrased in terms of the following decision problem.

**Problem 2.3.** Given a Diophantine equation $D(x_1, x_2, \ldots, x_m) = 0$, does it have a solution?

Any individual Diophantine equation yields a subproblem of this problem. In this context an algorithm is a mechanical procedure that has finite input and yields “Yes” or “No”. Mechanical procedure is a loose term which via Church’s Thesis is generally accepted to mean a procedure that can be done by a Turing Machine or any other equivalent model of computation. Church’s Thesis interpreted in this way gives a technical understanding of Hilbert’s problem. We can rephrase Hilbert’s question as the following: Is there a Turing Machine, that given any Diophantine equation can decide if it has a solution? The following celebrated result, of which several nice accounts can be found in the references [28, 11], gives a negative answer to this question.

**Theorem 2.4.** (DPRM) There is no algorithm that can decide if a Diophantine equation has a solution.
Correspondence Theorem

To apply the DPRM Theorem to cocyclic subshifts, the following definitions will be needed. Suppose $p$ and $q$ are monomials in $m$ unknowns, then $p$ divides $q$ if there is a third monomial $r$ so that $pr = q$. For a given polynomial $D$ we define a set $C(D)$ which is the ordered collection of all monomials with coefficient 1 which divide a term of $D$. The order is lexicographical, taking 1 as the smallest element and $x_i < x_j$ for $i < j$. The complexity of $D$, $\text{comp}(D)$, is the cardinality of $C(D)$.

Furthermore, we denote by $V_D$ the real linear space of dimension $\text{comp}(D)$ consisting of linear combinations of the monomials in $C(D)$, with $C(D)$ as an ordered basis. $V_D$ is a linear subspace but not a subring of the ring $\mathbb{R}[x_1, \ldots, x_m]$ of polynomials in $x_1, \ldots, x_m$.

**Example 1:** Let $D(x_1, x_2) = x_1^2 + x_2 - x_1 x_2 + 1$. First $C(D) = (1, x_1, x_1^2, x_1 x_2, x_2)$, so $\text{comp}(D) = 5$. We consider the elements of $C(D)$ as the basis of the vector space, $V_D$, of dimension 5.

**Example 2:** (Fermat) Consider the Diophantine equation $D(x_1, x_2, x_3) = (x_1 + 1)^3 + (x_2 + 1)^3 - (x_3 + 1)^3 = 0$. This Diophantine equation is known to have no solutions in non-negative integers. We have $C(D) = (1, x_1, x_1^2, x_1 x_2, x_2^2, x_2 x_3, x_3, x_3^2, x_3^3)$. Here, $\text{comp}(D) = 10$.

We now continue with the general case. For $u \in V_D$ we represent it by a row vector $[u_0, u_1, \ldots, u_{n-1}] \in \mathbb{R}^n$ where $u = u_0 + u_1 x_1 + \ldots$. We define $\phi_0 \in \text{End}(V_D)$ by $u \phi_0 = u_0 D(x_1, \ldots, x_m)$. The image of any polynomial under $\phi_0$ is the polynomial evaluated at $(0, \ldots, 0)$ multiplied by $D$. We write $\Phi_0$ for the matrix representation of $\phi_0$ acting on the right on row vectors in $\mathbb{R}^n$. As a matrix acting on the right of
vectors of $V_D$, $\Phi_0$ consists of the coefficients of $D$ in the first row and zeros elsewhere. Note that if $D$ is the zero polynomial then $\Phi_0 = 0$.

We are particularly interested in the image $D(x_1 + a_1, \ldots, x_m + a_m)\Phi_0 = D(a_1, \ldots, a_m)D(x_1, \ldots, x_m)$. Thus $\phi_0$ gives a linear algebraic way to check that $(0, \ldots, 0)$ is a solution to $D = 0$. We also define linear maps, $\phi_i : V_D \to V_D$, that take a polynomial $p(x_1, \ldots, x_i, \ldots, x_m)$ to $p(x_1, \ldots, x_i+1, x_{i+1}, \ldots, x_m)$ for any $i = 1, \ldots, m$ and any polynomial $p$. The composition of these types of maps will allow for a linear algebraic method of checking if $(a_1, \ldots, a_m)$ is a solution to $D = 0$ for any choice of $a_i$. Let us first carefully check that the substitutions $x_i \mapsto x_i + 1$ indeed induce linear maps of $V_D$.

Lemma 2.5. The map $\phi_i$ of $\mathbb{R}[x_1, \ldots, x_m]$ given by $p(x_1, \ldots, x_i, \ldots, x_m) \mapsto p(x_1, \ldots, x_i+1, \ldots, x_m)$ is a ring homomorphism, $\phi_i$ maps $V_D$ to itself, and therefore $\phi_i$ is a linear map from $V_D$ to itself. Moreover, $\phi_i$ is invertible for each $i = 1, \ldots, m$.

We need the following universal property which can be found in [21].

Theorem 2.6. (Universal Property) Let $R$ and $S$ be commutative rings with identity and $\phi : R \to S$ a ring homomorphism such that $\phi(1_R) = 1_S$. Then for any $s_1, \ldots, s_n \in S$, there is a unique ring homomorphism $\hat{\phi} : R[x_1, \ldots, x_n] \to S$ such that $\hat{\phi}|_R = \phi$ and $\hat{\phi}(x_i) = s_i$ for $i = 1, \ldots, n$. This property completely determines the polynomial ring up to isomorphism.

We now continue with the proof of Lemma 2.5.

Proof. Let $R = \mathbb{R}$ and $S = \mathbb{R}[x_1, \ldots, x_m]$ with $\phi$ the inclusion map. $\phi$ is a ring homomorphism with $\phi(1_R) = 1_s$. Furthermore, let $s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_m$ be $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m$ and $s_i = x_i + 1$. By the universal property we have a unique ring homomorphism $\phi_i$ which is the inclusion when the domain is restricted to $\mathbb{R}$.
We actually want a linear map from $V_D$ to itself. It only remains to show that $\phi_i(V_D) \subset V_D$. We verify this using the binomial theorem and the definition of $V_D$. To fix our notation let $p \in V_D$ consist of monomials of the form $x_1^{k_1} \cdots x_m^{k_m}$. Let us fix such a monomial $r = x_1^{k_1} \cdots x_m^{k_m}$ that occurs in $p$. The image of $r$ under $\phi_i$ is $x_1^{k_1} \cdots (x_i + 1)^{k_i} \cdots x_m^{k_m}$. After multiplying out $(x_i + 1)^{k_i} = \sum_{t=0}^{k_i} \binom{k_i}{t} x_i^t$ we have $\phi_i(r)$ is the sum of monomials of form $x_1^{k_1} \cdots x_i^t \cdots x_m^{k_m}$ with $t \leq k_i$. But for each $t = 0, \ldots, k_i$, the monomial $x_1^{k_1} \cdots x_i^t \cdots x_m^{k_m}$ divides $r$. By definition of $C(D)$, $x_1^{k_1} \cdots x_i^t \cdots x_m^{k_m}$ is contained in $C(D)$ as well. Thus the image of any term of $p$ is a linear combination of elements of $C(D)$ and therefore $\phi_i(p) \in V_D$.

For each $i$, the map $\phi_i^{-1}$ that sends $x_i \mapsto x_i - 1$ and $x_j \mapsto x_j$ for $j \neq i$ is the inverse of $\phi_i$. Note that $\phi_i^{-1}$ restricts to a linear map from $V_D$ to itself by completely analogous computations as for $\phi_i$. It is clear that

$$p(x_1, \ldots, x_m)\phi_i\phi_i^{-1} = p(x_1, \ldots, x_m)\phi_i^{-1}\phi_i = p(x_1, \ldots, x_m)$$

where $p(x_1, \ldots, x_m)$ is any polynomial in $V_D$. So $\phi_i$ is invertible.

Now for $i = 1, 2, \ldots, m$ we define $\phi_i$ to be the linear transformation that maps each element of $V_D$ to the polynomial obtained by substituting $x_i \mapsto x_i + 1$. Observe that for $i \neq j$, $\phi_i$ and $\phi_j$ commute since it does not matter in which order we substitute $x_i + 1$ for $x_i$ and $x_j + 1$ for $x_j$. Moreover, since $\phi_i$ and $\phi_j$ commute for $i, j > 0$, below we consider blocks of the form $01^{a_1} \cdots m^{a_m}0$. Now for any Diophantine equation $D(x_1, \ldots, x_m) = 0$ we assign the corresponding cocycle $\phi_D = (\phi_0, \phi_1, \ldots, \phi_m)$ and we take $\mathcal{A} := \{0, \ldots, m\}$. Let $\omega \in \mathcal{A}^*$ with $\omega = \omega_1 \cdots \omega_l$, then $\phi_{\omega} = \phi_{\omega_1} \cdots \phi_{\omega_l}$.

**Theorem 2.7.** *(Correspondence)* For any Diophantine equation $D(x_1, \ldots, x_m) = 0$ with $D(x_1, \ldots, x_m)$ not equal to the zero polynomial, and $\omega \in \mathcal{A}^*$, $\phi_{\omega} = 0$ if and only
if $\omega$ has a subword in the set

$$F_D := \{0\nu| \nu \text{ is a permutation of } 1^{a_1}2^{a_2}\cdots m^{a_m} \text{ with } D(a_1,\ldots,a_m) = 0\}.$$ 

Proof. ($\Leftarrow$) If $\phi$ vanishes on a subword of $\omega$ it vanishes on $\omega$, so we may assume that $\omega \in F_D$. Suppose that $D(x_1,\ldots,x_m) = 0$ has a solution $(a_1,\ldots,a_m)$ and $\nu = 1^{a_1}\cdots m^{a_m}$. We examine the product $\phi_0\phi_1^{a_1}\cdots\phi_m^{a_m}\phi_0$ on an arbitrary vector $u = u_0 + u_1 x_1 + \ldots \in V_D$. By definition of $\phi_0$ we have $u\phi_0 = u_0 D(x_1,\ldots,x_m)$. Multiplying on the right by $\phi_1^{a_1}\cdots\phi_m^{a_m}$ we get $u_0 D(x_1 + a_1,\ldots,x_m + a_m)$. Note that by substituting 0 for each $x_i$ we get the constant coefficient $D(a_1,\ldots,a_m)$ which is zero by assumption. So multiplying on the right by $\phi_0$ yields $0 D(x_1,\ldots,x_m) = 0$.

($\Rightarrow$) We argue the contrapositive. Suppose that $\omega$ has no subword in $F_D$. We want to show that $\phi_0 \omega \neq 0$.

First note that for any word $\omega$, if $\phi_0 \neq 0$ then $\phi_0 \omega j \neq 0$ by the observation above that $\phi_i, \phi_j$ are invertible for $i = 1,\ldots,m$. We can consider only those words $\omega$ that begin and end with 0. For the moment, we also assume that the constant coefficient $u_0$ of $D(x_1,\ldots,x_m)$ is non-zero.

We factor $\omega$ into blocks of the form $0^t$ and $\nu$ where $\nu$ is a permutation of a word of the form $1^{a_1}\cdots m^{a_m}$ where $D(a_1,\ldots,a_m) \neq 0$ by our assumption that $\omega$ has no subword in $F_D$. That is, $\omega = 0^{t_1} \nu_1 0^{t_2} \nu_2 \cdots \nu_k 0^{t_{k+1}}$. We proceed by induction on $k$.

If $k = 1$, then $\omega = 0^t \nu 0^s$. By the definition of $\phi_0$ we get

$$1\phi_0^t \phi_0^s = D(x_1,\ldots,x_m)\phi_0^{t-1} \phi_0^s.$$ 

But then we have

$$D(x_1,\ldots,x_m)\phi_0^{t-1} \phi_0^s = u_0^{t-1} D(x_1,\ldots,x_m)\phi_0^s.$$ 

By definition of $\phi_i$ for $i = 1,\ldots,m$, we have

$$u_0^{t-1} D(x_1,\ldots,x_m)\phi_0^s = u_0^{t-1} D(x_1 + a_1,\ldots,x_m + a_m)\phi_0^s.$$
Finally,
\[ u_0^{-1}D(x_1 + a_1, \ldots, x_m + a_m)\phi_0^s = u_0^{-1}D(a_1, \ldots, a_m)u_0^{s-1}D(x_1, \ldots, x_m) \neq 0. \]

Note that \( D(a_1, \ldots, a_m) \neq 0 \) by the assumption that no subword of \( \omega \) is in \( F_D \). So, \( \phi_\omega \neq 0 \).

Now suppose that \( \omega = 0^{t_1}\nu_1 \ldots \nu_k0^{t_{k+1}}\nu_{k+1}0^{t_{k+2}} \) has no subword in \( F_D \), and thus, by the induction hypothesis, that \( \phi_0^{t_1\nu_1 \ldots \nu_k0^{t_{k+1}}} \neq 0 \). Also we know that \( 1\phi_0^{t_1\nu_1 \ldots \nu_k0^{t_{k+1}}} \) is a non-zero constant multiple of the polynomial \( D(x_1, \ldots, x_m) \). Now,
\[ D(x_1, \ldots, x_m)\phi_{t_{k+1}}\phi_0^s = D(x_1 + b_1, \ldots, x_m + b_m)\phi_0^s \]

and \( D(b_1, \ldots, b_m) \neq 0 \). We have
\[ D(x_1 + b_1, \ldots, x_m + b_m)\phi_0^s = D(b_1, \ldots, b_m)u_0^{s-1}D(x_1, \ldots, x_m), \]
hence \( \phi_\omega \neq 0 \).

For the special case where \( u_0 = 0 \) the same proof works with the observation that for all the blocks of the form \( 0^t \) in the factorization of \( \omega \) we must have \( t = 1 \) since \( 00 \) is an element of \( F_D \).

We now continue the examples from above.

**Example 1:** (Continued) Let \( D(x_1, x_2) = x_1^2 + x_2 - x_1x_2 + 1 \). First \( C(D) = (1, x_1, x_1^2, x_1x_2, x_2) \), so \( \text{comp}(D) = 5 \). We consider the elements of \( C(D) \) as the basis of the vector space, \( V_D \), of dimension 5. Now the operation of substitution \( x_1 \mapsto x_1 + 1 \) induces a homomorphism of the ring \( \mathbb{R}[x_1, x_2] \) that restricts to a linear map \( \phi_1 \) of \( V_D \) into itself. Below we represent \( \phi_1 \) by a matrix acting on the right on row vectors. From \( \phi_1: 1 \mapsto 1, x_1 \mapsto x_1 + 1, x_1^2 \mapsto x_1^2 + 2x_1 + 1, x_1x_2 \mapsto x_1x_2 + x_2, \) and \( x_2 \mapsto x_2 \), we get:
Likewise the substitution $x_2 \mapsto x_2 + 1$ yields 

$$
\Phi_2 := \begin{bmatrix}
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
$$

Now we define a coefficient matrix 

$$
\Phi_0 := \begin{bmatrix}
1 & 0 & 1 & -1 & 1 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
\end{bmatrix},
$$

corresponding to $\phi_0 : V_D \to V_D$ sending any polynomial with constant coefficient $b_0$ to the polynomial $b_0D(x_1, x_2)$. Now, for any $(a_1, a_2) \in \mathbb{N}_0^2, D(a_1, a_2) = 0$ iff $\Phi_0\Phi_1\Phi_2\Phi_0 = 0$. For instance, $\Phi_0\Phi_1\Phi_2\Phi_0 = \begin{bmatrix}
2 & 0 & 2 & -2 & 2 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
\end{bmatrix}$. The first row of the matrix can be seen as the polynomial $D(1,5)D(x_1, x_2)$, since $D(1,5) = 2$. Now consider the product $\Phi_0\Phi_1^2\Phi_2^5\Phi_0 = 0$ where $(2,5)$ is a zero of the Diophantine
equation. We will more fully explore the power of this construction below, but first another example.

**Example 2:** (Continued) Consider the Diophantine equation $D(x_1, x_2, x_3) = (x_1 + 1)^3 + (x_2 + 1)^3 - (x_3 + 1)^3 = 0$. This Diophantine equation is known to have no solutions in non-negative integers. We construct matrices some product of which is zero iff the equation has a solution. We have $C(D) = (1, x_1, x_1^2, x_1^3, x_2, x_2^2, x_2^3, x_3, x_3^2, x_3^3)$ as above we generate the following matrices from the substitutions $x_1 \mapsto x_1 + 1, x_2 \mapsto x_2 + 1, x_3 \mapsto x_3 + 1$. (Note that blank spots take the place of zeros in the matrices to make them easier to read.)

$$\Phi_1 := \begin{bmatrix}
1 \\
1 & 1 \\
1 & 2 & 1 \\
1 & 3 & 3 & 1
\end{bmatrix}, \quad \Phi_2 := \begin{bmatrix}
1 \\
1 \\
1 & 1 \\
1 & 2 & 1 \\
1 & 3 & 3 & 1
\end{bmatrix}.$$
and $\Phi_3 := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 3 & 1 & 1 & 1 & 1 \end{bmatrix}$.

Now we have the coefficient matrix $\Phi_0 := \begin{bmatrix} \begin{bmatrix} 1 & 3 & 3 & 1 & 3 & 3 & 1 & -3 & -3 & -1 \end{bmatrix} \\ \end{bmatrix}$.

Fermat’s Last Theorem can be applied to show that no product of these matrices is ever zero. Actually, that $x^3 + y^3 = z^3$ has no solution in positive integers was already shown by Euler, see [14].

We would like to show that this method produces irreducible subshifts. We need a simple lemma about the zeros of polynomial equations. Suppose $T$ is a subset of
N_0^m. We say T is totally unbounded if for any \( N \in \mathbb{N} \) there exists \((a_1, \ldots, a_m) \in T\) such that \( a_i > N \) for \( i = 1, \ldots, m \).

**Lemma 2.8.** Let T be the complement in \( N_0^m \) of the set of solutions to a Diophantine equation \( D(x_1, \ldots, x_m) = 0 \) which is not identically zero. Then T is totally unbounded.

**Proof.** Since D is not identically 0 we have \( T \neq \emptyset \). Let \((a_1, \ldots, a_m) \in T\). Now \( D(x_1, a_2, \ldots, a_m) \) is a non-zero polynomial in the single unknown \( x_1 \). Thus there are only finitely many solutions to the equation \( D(x_1, a_2, \ldots, a_m) = 0 \). So for some \( b_1 \in \mathbb{N} \) with \( b_1 > a_1 \) and \( D(b_1, a_2, \ldots, a_m) \neq 0 \). The same argument now applies to each coordinate taken one at a time, until we get \((b_1, \ldots, b_m)\) with \( b_i > a_i \) for each \( i = 1, \ldots, m \) and \( D(b_1, \ldots, b_m) \neq 0 \). So for any \( N \in \mathbb{N} \) there exists \((b_1, \ldots, b_m)\) with \( b_i > N \) for all \( i \) and \( D(b_1, \ldots, b_m) \neq 0 \). Thus, T is totally unbounded.

\[ \square \]

**Corollary 2.9.** For any Diophantine equation \( D = 0 \) the corresponding subshift is irreducible. That is, for any two words \( u, v \) that occur in \( X_D \), there is a word \( w \) (possibly empty) such that \( uvw \) also occurs. Moreover, for any word \( w \), \( \Phi_w \neq 0 \) if and only if \( w \) occurs in \( X \).

**Proof.** The moreover part follows from the observation in Lemma 2.5 that \( \phi_i \) are invertible. Thus, if \( \phi_w \neq 0 \) then \( \phi_w \phi_i \neq 0 \) for \( i = 1, \ldots, m \). It follows that for any \( w \) with \( \phi_w \neq 0 \), \( w \) occurs in the element \( wi^\infty \in X \). We now continue with the proof of irreducibility.

If \( D \equiv 0 \), then \( \Phi_0 = 0 \) and \( X_D \) is the full shift \( \{1, \ldots, m\}^\mathbb{Z} \).

Now if \( D \) is not identically 0, and \( u \) and \( v \) occur, we have the following cases.

First suppose that either \( u \) or \( v \) does not have 0 as a subword. We may as well suppose that \( v \) does not have 0 as a subword. Thus \( \phi_v \) is invertible and so \( \phi_u \phi_v \neq 0 \). So \( uv \) occurs.
For the second case, we suppose that both \( u \) and \( v \) have 0 as a subword. Now let \( u_0 \) be the subword of \( u \) following the last 0 in \( u \). Let \( v_0 \) be the subword that precedes the first 0 in \( v \). Note that \( u_0 \) or \( v_0 \) could be the empty word. Now let \( a_i \) be the number of i’s in the word \( u_0v_0 \). Then there exists a non-solution \((b_1, \ldots, b_m)\) with \( b_i > a_i \). Now let \( w = 1^{b_1-a_1} m^{b_m-a_m} \). Then \( uwv \) occurs. This follows since no subword of \( uwv \) is of the form \( 01^{c_1} \ldots m^{c_m}0 \) with \( D(c_1, \ldots, c_m) = 0 \). Thus \( \Phi_{uwv} \neq 0 \). But then \( 1^\infty uwv1^\infty \) is in the two-sided subshift \( X_D \), or \( uwv1^\infty \) is in the one-sided subshift \( X_D \). In either case, \( uwv \) occurs.

\[ \square \]

**Undecidability**

We now apply our Correspondence Theorem (Theorem 2.7) and the DPRM Theorem to show the undecidability of several problems. It is a common goal of many mathematical fields to develop methods to determine if two objects are the same, either outright or up to some natural equivalence relation like isomorphism. The following three problems represent different possible discriminations that might be made. To examine the existence of algorithms for determining if two cocyclic subshifts are in some way the same, we consider a subclass that can be represented by a cocycle of integer valued matrices. We refer to such as integer cocyclic subshifts.

We will show below that, if we restrict to the integer cocyclic subshifts, all three problems are algorithmically undecidable by associating a cocycle to any Diophantine equation.

**Problem 2.10.** (ECS) Given two integer cocyclic subshifts on the same alphabet determine if the subshifts are equal.
Problem 2.11. (FCS) Given an integer cocyclic subshift on $n$ symbols, determine if it is equal to the full shift on $n$ symbols.

Problem 2.12. (ICS) Given two integer cocyclic subshifts determine if they are isomorphic.

We refer to the problems by the labels ECS, FCS, and ICS respectively.

Theorem 2.13. (Undecidability) FCS is algorithmically undecidable.

Proof. Suppose there was an algorithm that could determine if a given cocyclic subshift is the full shift. In particular, for any Diophantine equation $D = 0$ the algorithm would determine if the corresponding cocyclic subshift $X_D$ were the full shift. But $X_D$ is the full shift iff $D = 0$ has no solutions. Thus the algorithm would determine if $D = 0$ has a solution, which is not possible by the DPRM theorem. \hfill \Box

Corollary 2.14. ECS is algorithmically undecidable.

Proof. This is clear since FCS is a subproblem of ECS. \hfill \Box

Corollary 2.15. ICS is algorithmically undecidable.

Proof. Suppose there were an algorithm that could decide if two cocyclic subshifts were isomorphic. Then in particular, given two cocyclic subshifts that are subshifts of the same shift, the algorithm could decide if they are isomorphic. But, if we take one of those subshifts as the full shift containing the other we would have an algorithm that could decide if the full shift is isomorphic to a cocyclic subshift of itself. But this is the same as determining equality, since the full shift is not isomorphic to any proper subshift of itself. Since an isomorphic image of the full shift has the same number of periodic points of each period as the full shift; if the image is a subset of the full shift, it must contain all of the periodic points of the full shift. However,
periodic points are dense in the shift space, hence no subshift strictly contained in the full shift is also isomorphic to the full shift.

Applying Theorem 2.13, we have that no algorithm exists which can solve ICS. □

By using a method found in [18], we can strengthen Theorem 2.13 in terms of cocyclic subshifts on two symbols.

**Theorem 2.16.** There is no general algorithm that given an integer cocyclic subshift on two symbols can decide if it is equal to the full shift.

*Proof.* To fix notation we consider cocyclic subshifts with cocycles of the form \((\Psi_1, \Psi_2)\). Now the corollary follows from the lemma below, since if there is no algorithm that can decide if some product \(\Psi_w\) is zero, then there is no algorithm that can decide if an integer cocyclic subshift on two symbols is the full shift. □

**Lemma 2.17.** There is no algorithm that, given any two integer matrices \(\Psi_1\) and \(\Psi_2\), can decide if there is a word \(w \in \{1, 2\}^*\) such that the product \(\Psi_w\) is zero.

*Proof.* The idea is to associate to a Diophantine equation a cocycle of two matrices so that the vanishing of the cocycle implies solvability of the equation. Let \(D(x_1, \ldots, x_m) = 0\) be a Diophantine equation as above. Let \(\Phi = (\Phi_0, \ldots, \Phi_m)\) be the corresponding cocycle constructed from \(D\) as before. We want to give two matrices that will keep track of any product of the original matrices \(\Phi_0, \ldots, \Phi_m\). For clarity our matrices will be called \(A\) and \(B\). The first matrix \(A\) will just be a block matrix with the \(\Phi_i\) down the diagonal. The second will be a matrix \(B\) which, upon multiplying \(A\), will cycle the diagonal. That is, taking \(\text{Id}\) to be the identity matrix of the same size as the \(\Phi_i\), say \(n \times n\), we define two block matrices
\[
A := \begin{bmatrix}
\Phi_0 & 0 & \cdots & 0 \\
0 & \Phi_1 & & 0 \\
\vdots & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & \Phi_m
\end{bmatrix}
\quad \text{and} \quad
B := \begin{bmatrix}
0 & 0 & \cdots & 0 & I \\
I & 0 & 0 & \cdots & 0 \\
0 & I & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & I & 0
\end{bmatrix}.
\]

First note that \(B^{m+1}\) is the identity \(\text{Id}\). So \(B^m = B^{-1}\) and \(B^T = B^{-1}\). Now let \(C_i = B^{m+1-i}AB^i\) for \(0 \leq i \leq m\). We claim that the \(C_i\) is a block matrix with with the diagonal cyclically permuted, that is \(C_i\) has diagonal \(\Phi_i, \ldots, \Phi_m, \Phi_0, \ldots, \Phi_{i-1}\).

If \(i = 0\) the claim follows trivially since \(B^{m+1}\) and \(B^0\) are both equal to \(\text{Id}\). Now suppose that, for some \(i\) \(0 \leq i < m\), we have that \(C_i\) is as claimed. From the equation \(B^m = B^{-1}\) it follows that \(C_{i+1} = B^{m+1-(i+1)}AB^{i+1} = B^{-1}B^{m+1-i}AB^iB = B^{-1}C_iB\).

\[
B^{-1}C_iB = B^T = \begin{bmatrix}
0 & 0 & \cdots & 0 & \Phi_i \\
\Phi_{i+1} & 0 & 0 & \cdots & 0 \\
0 & \Phi_{i+2} & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & \Phi_{i-1} & 0
\end{bmatrix}
= \begin{bmatrix}
\Phi_{i+1} & 0 & \cdots & 0 \\
0 & \Phi_{i+2} & \cdots & \vdots \\
\vdots & \ddots & \ddots & 0 \\
0 & \cdots & 0 & \Phi_i
\end{bmatrix}.
\]

Using the relation, \(B^{m+1} = \text{Id}\) it follows that any product of the matrices \(A\) and \(B\) can be written in the form \(B^lC_{i_1}C_{i_2}\cdots C_{i_l}\) for some \(l \geq 0\). \(B\) is invertible so \(B^lC_{i_1}C_{i_2}\cdots C_{i_l} = 0\) implies \(C_{i_1}C_{i_2}\cdots C_{i_l} = 0\) implies \(\Phi_{i_1}\cdots \Phi_{i_l} = 0\) because \(\Phi_{i_1}\cdots \Phi_{i_l}\) is the entry in the upper left corner of \(C_{i_1}\cdots C_{i_l}\).

On the other hand, suppose that \(\Phi_{i_1}\cdots \Phi_{i_l} = 0\). Let \(D_j\) be the matrix which has \(\Phi_{i_1}\cdots \Phi_{i_l}\) on the \(j\)th diagonal, i.e. \(D_j\) is a diagonal matrix and the \(j, j\) entry is \(\Phi_{i_1}\cdots \Phi_{i_l}\). Then \(D_1\cdots D_m = 0\). By inspection we see that each \(D_j\) can be written as some product of \(A\) and \(B\).
Above we have shown that for any product of $A$ and $B$ which is zero there is a corresponding product $\Phi_w$ which is zero. Likewise, for any product $\Phi_w$ which is zero, there is a corresponding product of $A$ and $B$ which is zero. Since there is no algorithm that can decide if $\Phi_w = 0$ for some word $w$, there is no algorithm that can decide if some product of $A$ and $B$ is zero.

Incompleteness

We briefly discuss some of the ideas of mathematical logic. A formal system of logic has axioms and inference rules. A system is complete if, for any statement $p$ in the system, either $p$ or its negation $\neg p$ is provable from the axioms (using the inference rules). A system is said to be incomplete if it is not complete, i.e. there is some statement $p$ for which neither $p$ nor $\neg p$ is provable. A system is consistent if it is free of contradictions. That is, a system is consistent if there is no statement $p$ such that $p$ and $\neg p$ are both provable from the axioms. We now paraphrase the famous Gödel’s First Incompleteness Theorem and refer the reader to [35] and the original paper [17] for a more precise formulation as well as a proof.

**Theorem 2.18.** Let $S$ be a formal system strong enough to express the theorems of arithmetic. If $S$ is consistent then $S$ is incomplete.

The following special version of Gödel’s Incompleteness Theorem is implied by the DPRM Theorem. Note that the theorem assumes the consistency of the system.

**Theorem 2.19.** [11] Corresponding to any given axiomatization, there is a Diophantine equation which has no positive integer solutions, but such that this fact cannot be proved within the given axiomatization.
By our construction above this implies the following.

**Theorem 2.20.** Corresponding to any given axiomatization there is an integer valued cocycle, the cocyclic subshift of which is the full shift, but such that this fact cannot be proved within the given axiomatization.

**Strictly Cocyclic Subshifts and Diophantine Equations**

Another application of the method developed here is to create non-trivial examples of cocyclic subshifts that are relatively easy to understand. We start by observing that if a Diophantine equation has finitely many solutions then the corresponding subshift is a subshift of finite type.

**Theorem 2.21.** Suppose that \( D(x_1, \ldots, x_m) = 0 \) has finitely many solutions, then the corresponding cocyclic subshift \( X_D \) is a subshift of finite type.

**Proof.** By its construction the subshift \( X_D \) has

\[
F_D = \{0\nu0 \mid \nu \text{ is a permutation of } 1^{a_1} \cdots n^{a_n} \text{ with } D(a_1, \ldots, a_n) = 0\}
\]

as a forbidden set that determines the shift, i.e. \( X_{F_D} = X_\Phi \). \( F_D \) is clearly finite.

We refer to a cocyclic subshift that is not sofic as **strictly cocyclic**. It is not true that given any Diophantine equation with infinitely many solutions the corresponding cocyclic subshift is strictly cocyclic (see example below), but this is true if the infinite solution set of the equation is suitably non-trivial.

To discuss whether a subshift is sofic we could rely on several equivalent characterizations of sofic systems. Here we use the concept of the follower set. Let \( X \) be a subshift and \( w \in \mathcal{L}(X) \), then the **follower set** \( F_X(w) \) of \( w \) in \( X \) is the set of all words that can follow \( w \) in \( X \), \( F_X(w) := \{v \in \mathcal{L}(X) : wv \in \mathcal{L}(X)\} \). The collection of all follower sets in \( X \) is denoted by \( \mathcal{C}_X = \{F_X(w) : w \in \mathcal{L}(X)\} \).
Theorem 2.22. A shift space is sofic if and only if it has a finite number of follower sets.

For an insightful discussion of follower sets and a proof of the theorem see [27].

Before giving a criterion for producing strictly cocyclic subshifts, we give some examples of Diophantine equations which have infinitely many solutions, but for which the respective subshifts are not strictly cocyclic.

Example: Consider $D(x_1,\ldots,x_m) = 0$ where $D$ is identically zero. Then $\Phi_0$ is the zero matrix and since the remaining matrices $\Phi_1,\ldots,\Phi_m$ are invertible, $X_D$ is the full shift on $m$ symbols. We use a similar idea to create a more elaborate example.

Example: Consider the Diophantine equation in two variables given by $x(y^2+1) = 0$. By the correspondence theorem above we have that $F_D = \{02^a0|a \in \mathbb{N}_0\}$ is a forbidden set that determines the subshift. We now show that $X_D = X_{F_D}$ has finitely many follower sets. As we have seen in the proof of the Correspondence Theorem, the letter 0 as a subword in any allowed word “resets” the matrix calculations, i.e. the image of $\Phi_{w0}$ does not depend on $w$ if it is not zero. Any words which occur in the subshift and that have the final letter 0 have the same follower sets. Observe that the follower set for any allowed word $w$ that ends with 1 is the entire collection of allowed words. This follows from the fact that $w$ has no subword in $F_D$, and that $D(x,y) = 0$ does not have any solution of the form $(a,b)$ with $a \neq 0$.

For a word $w$ that ends with 2 there are three cases.

Case 1: 0 is not a subword of $w$. Suppose $v$ is a word such that $wv$ has a subword in $F_D$. Then $v$ must have a subword in $F_D$, since $w$ contains no 0. Thus, for any allowed word $v$, $wv$ is allowed.

Case 2: There is a 1 between the last 0 and the final 2 in $w$. Let $v$ be any word such that $wv$ has a subword in $F_D$. Once more $v$ must already have a subword in $F_D$.
since no subword before the last 0 in $w$ can be contained in $F_D$ and the subword of $wv$ that begins with the last 0 in $w$ and ends with the first 0 in $v$ cannot be in $F_D$ either since it contains 1 as a subword.

Case 3: 0 is a subword of $w$ and there are no 1’s between the last 0 and the 2. Then the follower set consists of all allowed words except those beginning with $2^b0$ for some $b \in \mathbb{N}_0$.

Thus there are only three different follower sets and the subshift $X_F$ is sofic.

We return to the discussion of strictly cocyclic subshifts. We say that a Diophantine equation, $D(x_1, \ldots, x_m) = 0$ is degenerate in $x_i$, if there are $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_m \in \mathbb{N}_0$ such that $D(b_1, \ldots, b_{i-1}, x_i, b_{i+1}, \ldots, b_m)$ is identically zero. The $D$ in the last example is degenerate in $y$. A Diophantine equation is said to be non-degenerate if it is not degenerate in any $x_i$.

**Theorem 2.23.** Suppose that $D(x_1, \ldots, x_m) = 0$ is non-degenerate and has infinitely many solutions in $\mathbb{N}_0^m$. Then $X_D$ is strictly cocyclic.

**Proof.** We show that for a non-degenerate Diophantine Equation with infinitely many solutions there are infinitely many distinct follower sets.

Since $D = 0$ has infinitely many solutions, there is a subset of the solution set which takes on infinitely many values $a_k$ in the $x_i$-th component for some $i$. We may as well assume that $i = 1$ and that $a_k \nearrow \infty$. By the assumption that $D = 0$ is non-degenerate, for any fixed collection $b_2, \ldots, b_m \in \mathbb{N}_0$, there are only finitely many $k$ such that $D(a_k, b_2, \ldots, b_m) = 0$. Indeed, otherwise $D(x_1, b_2, \ldots, b_n) = 0$ would be a polynomial equation in one variable with infinitely many solutions making $D(x_1, b_2, \ldots, b_n) \equiv 0$.

Letting $A_k = \{(b_2, \ldots, b_m) \mid D(a_k, b_2, \ldots, b_m) = 0\}$, we have that any fixed $(b_2, \ldots, b_m)$ can be contained in at most finitely many $A_k$. Thus there is some (infinite)
subsequence $A_{k_i}$ such that the elements of the sequence are mutually distinct. We abuse notation and use $A_k$ for the subsequence.

Now examine the follower set of $01^{a_k}$. We observe that the follower set of $01^{a_k}$ is not equal to the follower set of $01^{a_l}$ for any $k \neq l$ since there is a solution $D(a_k, b_2, \ldots, b_m) = 0$ such that $D(a_l, b_2, \ldots, b_m) \neq 0$, since $A_k \neq A_l$. (We used that if $01^{a_k}2^{c_2} \ldots m^{c_m}0$ is allowed then it occurs, say in the element $1^\infty01^{a_k}2^{c_2} \ldots m^{c_m}01^\infty$.) But this shows that the cocyclic subshift has infinitely many follower sets, hence it is not sofic.

As a special case we look at a Diophantine equation $D(x, y) = 0$ where $D$ is irreducible. Recall that a polynomial is irreducible in $\mathbb{Z}[x, y]$ if it cannot be written as the product of two non-constant polynomials in $\mathbb{Z}[x, y]$.

**Corollary 2.24.** If $D(x, y) = 0$ is a Diophantine equation with infinitely many solutions and $D(x, y)$ is irreducible in $\mathbb{Z}[x, y]$ then $X_D$ is strictly cocyclic.

**Proof.** By Theorem 2.23 it suffices to see that $D(x, y) = 0$ is non-degenerate. Suppose that $D = 0$ is degenerate in $y$, say there is $b \in \mathbb{N}_0$ with $D(x, b) = 0$. Then $D(x, y)$ as a polynomial in $\mathbb{Z}[x][y]$ has a zero at $y = b$. Hence, $y - b$ is a factor of $D(x, y)$ making $D(x, y)$ reducible, contrary to our assumption.

**Example:** The simple equation $D(x, y) = x - y = 0$ yields a strictly cocyclic subshift with a set

$$F = \{0\nu0 \mid \nu \text{ is a permutation of } 1^n2^n, \ n \in \mathbb{N}_0\}.$$
Furthermore, for any $t \in \mathbb{N}_0$, $D_t(x, y) = x - 2^t y = 0$ is also irreducible so the associated cocyclic subshifts is strictly cocyclic. Note that for $s \neq t$ we have $X_{D_t} \neq X_{D_s}$ since $(2^t, 1)$ is a solution to $D_t = 0$ but not to $D_s = 0$.

Post Correspondence Problem and the Mortal Matrix Theorem

Another method of proving that $FCS$ is undecidable, which was discovered in the literature after we had completed the work on our correspondence theorem, is via the Post Correspondence Problem. The main idea is that there is a way to assign to each instance of the post correspondence problem a matrix semigroup. Deciding whether 0 is in the semigroup is equivalent to solving the post correspondence problem. The key results in this section are originally due to M.S. Paterson, see [31], and can also be found in [19].

Given a finite collection of $n \times n$ matrices from $\mathbb{Z}^{n \times n}$, the collection of all products of these matrices constitutes a monoid $S$, where the identity is given by any of the matrices to the 0-th power. The mortality problem is the following:

**Problem 2.25.** (Mortality) Determine if the zero matrix belongs to $S$. Equivalently, determine if there is some product of the given matrices that equals 0.

If this problem were decidable, that is, if there were a general algorithm to determine if a monoid contains 0, then the same algorithm could be applied to determine if some product of the linear maps of a given cocycle $\Phi$ is 0. Thus it would determine if a given cocyclic subshift is the full shift. Even though we have proven that this problem is undecidable via the DPRM Theorem, let us briefly discuss how to get the result via the Post Correspondence Problem. One benefit of this method is that we see that the Undecidability Theorem (Theorem 2.13) is already true for the class of integer cocycles of $3 \times 3$ matrices.
$A^*$ forms a semigroup with concatenation of two words as the product. $\epsilon$, the empty word, is the identity with respect to concatenation. Thus the semigroup $A^*$ is actually a monoid.

A mapping $h : M_1 \to M_2$ is a morphism between monoids if for any words $u$ and $v$ in $M_1$ $h(uv) = h(u)h(v)$. For two morphisms $h$ and $g$ between the word monoids, $\Sigma^*$ and $\Delta^*$ the equality set of $h$ and $g$ is the set $E(h, g) = \{w \in \Sigma^+ | h(w) = g(w)\}$.

**Problem 2.26.** (PCP) Given a pair of monoid morphisms $h$ and $g$ as above, determine whether or not $E(h, g) = \emptyset$.

Note that this is not the original form of the Post Correspondence Problem but is equivalent to the original as a decision problem, see [19]. The problem, in its original form, was first proved undecidable by Post [32]. The original form of the problem concerns whether two concatenations from different sets of basic words ever give the same result.

The elements in $E(h, g)$ are called the solutions of the instance $(h, g)$ of PCP. The size of the instance $(h, g)$ of PCP is the cardinality of the alphabet $\Sigma$. $\text{PCP}(n)$ denotes the subproblem of PCP for instances of size at most $n$.

**Theorem 2.27.** The mortality problem is undecidable for $3 \times 3$-matrices with integer entries.

This theorem follows from the following stronger theorem.

**Theorem 2.28.** The problem whether there is a matrix $M$ with the upper left corner zero in a finitely generated semigroup of $3 \times 3$ matrices is undecidable.

**Proof.** The full proof for this assertion can be found in several locations but most succinctly in [19] and we follow the exposition there to give an outline of the argument.
Let \( \Gamma = \{a_1, a_2, a_3\} \) and \( \Delta = \{a_2, a_3\} \) be fixed alphabets. Define \( \sigma : \Gamma^* \to \mathbb{N} \) by \( \sigma(\epsilon) = 0 \) and
\[
\sigma(a_{i_1}a_{i_2}\ldots a_{i_k}) = \sum_{j=1}^{j=k} i_j 3^{k-j} \quad (k \in \mathbb{N}, a_{i_j} \in \Gamma).
\]

Then \( \sigma \) satisfies \( \sigma(uv) = 3^{|v|} \sigma(u) + \sigma(v) \) for all \( u \) and \( v \) in \( \Gamma^* \). This creative construction allows for the definition of an injective morphism of semigroups \( \gamma_1 : \Gamma^* \times \Gamma^* \to \mathbb{N}^{3 \times 3} \) given by
\[
\gamma_1(u,v) = \begin{bmatrix}
3^{|u|} & 0 & 0 \\
0 & 3^{|v|} & 0 \\
\sigma(u) & \sigma(v) & 1
\end{bmatrix}.
\]
Define \( \gamma : \Gamma^* \times \Gamma^* \to \mathbb{N}^{3 \times 3} \) by \( \gamma(u,v) = A\gamma_1(u,v)A^{-1} \) where
\[
A = \begin{bmatrix}
1 & 0 & 1 \\
1 & 1 & 0 \\
0 & 0 & 1
\end{bmatrix}.
\]

This yields the formula
\[
(\gamma(u,v))_{11} = 3^{|u|} + \sigma(u) - \sigma(v).
\]

Given \( h, g : \Sigma^* \to \Delta^* \) define \( N_a = \gamma(h(a), g(a)) \) and \( N'_a = \gamma(h(a), a_1g(a)) \) for all \( a \in \Sigma \) and let \( S \) be the semigroup generated by \( \{N_a, N'_a \mid a \in \Sigma\} \). Then if \( M = M_{b_1}M_{b_2}\ldots M_{b_n} \in S \) for some \( n \in \mathbb{N} \) and \( b_i \in \Sigma \) are such that \( M_{b_i} = N_{b_i} \) or \( M_{b_i} = N'_{b_i} \), then \( M_{11} = 3^{|u|} + \sigma(u) - \sigma(v) = \sigma(a_1u) - \sigma(v) \) for \( u = h(w) \in \Delta^* \) and for a word \( v \in \Gamma^* \). Since \( \sigma \) is injective, \( M_{11} = 0 \) if and only if \( v = a_1u \). Thus \( M_{11} = 0 \) if and only if \( v = a_1g(w) = a_1h(w) \), that is, \( w \) is a solution of the instance \((h, g)\). \( \square \)

The following theorem shows that when restricting to the case of two letters with \( 2 \times 2 \) matrices with integer entries, the undecidability result does not hold.
Theorem 2.29. The mortality problem for two $2 \times 2$ matrices with integer coefficients is decidable.

For a proof and a discussion of the problem for finitely many matrices see [5]. The idea of the argument is to consider cases of different ranks and then consider the Jordan form of the matrices. The problem becomes equivalent to finding integer solutions to a very particular form of exponential equation. Note that the problem for more than two $2 \times 2$ matrices has not been proven decidable or not.

Let $FCS(n)$ denote the problem of determining if a cocyclic subshift over a vector space of dimension at most $n$ is the full shift. Let $ECS(n)$ denote the problem of determining if two cocylic subshifts over the same vector space of dimension no more than $n$ are the same cocyclic subshift.

Corollary 2.30. $FCS(3)$ is undecidable. $ECS(3)$ is also undecidable.

Corollary 2.31. There is an algorithm that, given a cocyclic subshift on two symbols with cocycle given by elements of $M_2(\mathbb{Q})$, $2 \times 2$ rational-valued matrices, will decide in finite time if the subshift is equal to the full shift on two symbols.
We collect some of the fundamental definitions and results from the theory of finite dimensional algebras to be applied later. Where proofs are not given we refer the reader to [13] and [10]. Let \( \mathbb{C} \) be an algebraically closed field. An algebra \( A \) over \( \mathbb{C} \) is a vector space over \( \mathbb{C} \) which also has a product that is compatible with the addition. The fundamental examples are the algebras of \( n \times n \) complex-valued matrices, \( M_n(\mathbb{C}) \). We refer to the dimension of \( A \) as a vector space over \( \mathbb{C} \) as the dimension of the algebra \( A \). In what follows, except where explicitly mentioned, we consider only the case in which \( A \) is finite dimensional with identity. A right ideal of an algebra is a subspace \( I \) of the vector space \( A \) such that for any \( a \in A \) we have \( Ia \subseteq I \). Note that when \( I \) is proper (\( I \neq A \)) it is not a subalgebra since it does not contain 1, but it is an example of a right \( A \)-module, see below. A left ideal is defined in the same way, i.e. for all \( a \in A \) we have \( aI \subseteq I \). A two-sided ideal \( I \) is a vector space that is simultaneously a right and left ideal of \( A \). For any (right, left, or two-sided) ideal \( I \) we have \( I^2 \subseteq I \). An ideal \( I \) is said to be nilpotent if there exists \( k \in \mathbb{N} \) such that \( I^k = 0 \).

A right \( A \)-module \( M \) is a \( \mathbb{C} \)-vector space on which \( A \) acts on the right in a way compatible with the vector addition in \( M \). Of course a left \( A \)-module is defined in a similar way. We will be concerned with right and left modules but focus more on the right modules and often use the word module for right module. In the case of a right ideal \( I \) treated as a right \( A \)-module the action of \( A \) on \( I \) is just by the algebra product. If we take \( A \) as an \( A \)-module in this way we call this the regular \( A \)-module. We will also need quotient modules. Suppose \( N \subseteq M \) are \( A \)-modules. For each \( m \in M \) let
Then the factor module or quotient module is given by $M/N := \{[m] \mid m \in M\}$. The basic theorems about quotient modules can be found in [13, p. 13]. For $A$-modules $M$ and $N$, a module homomorphism $f : M \to N$ is a linear map from $M$ to $N$ which also respects the action by $A$, i.e. for all $a \in A$ and $m \in M$ $f(ma) = f(m)a$. We will use the notation $\simeq$ for isomorphisms of algebras, vector spaces, and $A$-modules. To emphasize that a map is an $A$-module isomorphism we will use the notation $\simeq_A$. The collection of all $A$-module homomorphisms from $M$ to $N$ is a vector space and is denoted by $\text{Hom}_A(M, N)$. The collection of all $A$-module homomorphisms from $M$ to itself is denoted by $\text{End}_A(M)$.

An non-zero $A$-module $M$ is called simple if the only submodules are 0 and $M$ itself. Now, for any $A$-module $M$ we can take a chain of submodules $0 = M_0 \subset M_1 \subset \ldots \subset M_m = M$ such that the module $M_{j+1}/M_j$ is simple for $j = 0, 1, \ldots, m - 1$. Such a chain can be created inductively using the fact that $M$ is finite dimensional, and we call such a chain a composition series. The following theorem shows in what sense the composition series for a module is unique.

**Theorem 3.1.** (Jordan-Hölder Theorem) Suppose $0 = M_0 \subset M_1 \subset \ldots \subset M_m = M$ and $0 = N_0 \subset N_1 \subset \ldots \subset N_n = M$ are two composition series for $M$. Then $n = m$ and there is a bijection between the collections of the respective factor modules such that the corresponding factors are isomorphic. We call $n$ the length of the module and the factor modules $M_{j+1}/M_j$ the composition factors of $M$.

There is another standard way to decompose a module. We explain the interplay between the two decompositions in a later section. We say an $A$–module $M$ is indecomposable if $M = M_1 \oplus M_2$ for $A$–modules $M_1$ and $M_2$ implies that either $M_1 = 0$ or $M_2 = 0$. We remark that we will use the notation of the inner direct sum, i.e., we consider $M_1$ and $M_2$ to be subsets of $M$. It is straightforward to see that any
module can be written as a direct sum of indecomposable modules. It is significantly more difficult to show that up to order of the composition factors and isomorphism this decomposition is unique.

**Theorem 3.2. (Krull-Schmidt)** For any module $M$ there is a decomposition of $M$ into a direct sum of indecomposable modules. Furthermore, if $M = M_1 \oplus M_2 \oplus \cdots \oplus M_n = N_1 \oplus N_2 \oplus \cdots \oplus N_m$ are two decompositions of the module $M$ into a direct sum of indecomposable modules then $m = n$ and there is a reordering of the summands so that $M_i \simeq_A N_i$ ($i = 1, \ldots, m$).

Thus for an algebra $A$ as a module over itself there is a unique way to decompose $A$ as the direct sum of indecomposable modules. Now suppose $A = P_1 \oplus \cdots \oplus P_n \oplus \cdots \oplus P_q$ has been ordered so that $P_1, \ldots, P_n$ are mutually non-isomorphic and any $P_k$ for $1 \leq k \leq q$ in the decomposition is isomorphic to one in the collection $\{P_1, \ldots, P_n\}$. $\{P_1, \ldots, P_n\}$ is called a complete set of principal indecomposable modules of $A$. We refer to the elements of the set as the principal indecomposable modules of $A$ or just the principal modules of $A$. By the previous theorem these are unique up to isomorphism and reordering.

We get a useful characterization of the principal modules by considering $e_i \in P_i$ that come from decomposing the unit in $A$, $1 = e_1 + e_2 + \ldots + e_q$. Now for any $m \in P_i$ we have $1m = e_1m + \ldots + e_qm$ with $e_jm \in P_j$ since $e_j \in P_j$ and $P_j$ is a right $A$-module. But for $j \neq i$, we have $e_jm = 0$. So $e_im = m$. In particular, if we take $m = e_i$, we get that $e_je_i = 0$ for $i \neq j$ and $e_i^2 = e_i$. If $e^2 = e$ we say $e$ is idempotent. And if we have two idempotents $e$ and $f$ with $ef = 0 = fe$ we say they are orthogonal. Additionally note that each $e_i$ is primitive, or minimal; that is, if $e_i = e + f$ where $e$ and $f$ are orthogonal idempotents, then $e = 0$ or $f = 0$. To see this, suppose $e_i = e + f$ with $e, f$ orthogonal idempotents. Then either $eP_i = 0$ or $fP_i = 0$ (because
$P_i$ is indecomposable). Now $e \in P_i$ and $f \in P_i$, so we get $ee_i = e(e+f) = e^2 = e = e_ie$ and $fe_i = f(e+f) = f^2 = f = e_if$. If $eP_i = 0$, $e \in P_i$ implies $e = e^2 = 0$. Likewise, if $fP_i = 0$, then $f \in P_i$ implies $f = f^2 = 0$. Therefore, either $e = 0$ or $f = 0$. Thus the collection $\{e_i\}_{1 \leq i \leq q}$ is a collection of primitive mutually orthogonal idempotents, and we call $1 = e_1 + \ldots + e_q$ a decomposition of the identity. Note that the decomposition of the identity is not, in general, uniquely determined by the algebra $A$, but the Krull-Schmidt Theorem says that the modules $e_iA$ are determined up to isomorphism. So for any other decomposition of the identity $1 = f_1 + \ldots + f_p$ we can see that $p = q$ and after reordering $e_iA \simeq f_iA$ $i = 1, \ldots, p$.

If $A = P_1 \oplus \cdots \oplus P_n$, with $\{P_1, \ldots, P_n\}$ a complete set of principal indecomposable modules, then $A$ is called a basic algebra. Also, given any algebra $A$, there is a basic algebra that is associated with it. Suppose that $A \simeq_A m_1P_1 \oplus \ldots \oplus m_nP_n$ where $P_i$ are the principal indecomposable modules and $m_iP_i$ stands for $\oplus_{1}^{m_i} P_i$. Then let $A^b$ be the algebra of $A$-module endomorphisms of $P = P_1 \oplus \ldots \oplus P_n$, i.e.

$$A^b := \text{End}_A(P_1 \oplus \ldots \oplus P_n) = \text{End}_A(P).$$

Thinking of $A$ as fixed we write $B = A^b$.

If $1 = e_1 + \ldots + e_n$ is a decomposition of the identity in $B$ corresponding to the decomposition of $P$, then we say the principal $B$-module $Q_i := e_iB$ corresponds to the principal $A$-module $P_i$ and that the $B$-module $Q = k_1Q_1 \oplus \ldots \oplus k_nQ_n$ corresponds to the $A$-module $k_1P_1 \oplus \ldots \oplus k_nP_n$. In the application of this material we will be primarily interested objects of the form $\text{Hom}_A(P_1, P_2)$, the collection of all $A$-module homomorphisms from $P_i$ to $P_j$. The following lemma shows that if we confine our attention to the basic algebra we will still get the information that we need.

**Lemma 3.3.** [13, p. 59] If $B$ is the basic algebra of $A$ and $Q_1, Q_2$ are the $B$-modules corresponding to the $A$-modules $P_1, P_2$ then $\text{Hom}_B(Q_1, Q_2) \simeq \text{Hom}_A(P_1, P_2)$. 
The following lemma will be used repeatedly.

**Lemma 3.4.** (1) For any idempotent $f$ and right $A$-module $M$, $\text{Hom}_A(fA, M) \simeq Mf$ as vector spaces.

(2) For any idempotents $e, f \in A$ we have $eAf \simeq \text{Hom}_A(fA, eA)$ as vector spaces.

(3) For any idempotent $f$ and left $A$-module $\hat{M}$, $\text{AHom}(Af, \hat{M}) \simeq f\hat{M}$, where $\text{AHom}(Af, \hat{M})$ denotes the collection of left $A$-module homomorphisms from $Af$ to $\hat{M}$.

**Proof.** (1) We define a linear map $F : \text{Hom}_A(fA, M) \to Mf$ by $F(g) = g(f)$ for any $g \in \text{Hom}_A(fA, M)$. $F$ is 1-1 since, for elements $g_1, g_2 \in \text{Hom}_A(fA, M)$, if $g_1(f) = g_2(f)$ then for any $a \in A$ $g_1(fa) = g_1(f)a = g_2(f)a = g_2(fa)$.

We show that $F$ is surjective. Let $m \in M$ we want to show there is an $A$-module homomorphism $g : fA \to M$ such that $F(g) = mf$. Define $g$ by $g(fa) = mfa$ ($a \in A$).

Then $g$ is an $A$-module homomorphism and by definition of $F$, $F(g) = g(f) = mf$.

(2) follows from (1) by taking $M = eA$.

(3) is just the result of switching left to right in (1) and so is its proof.

We also use decompositions of an algebra $A$ into **indecomposable algebras**, i.e. algebras that cannot be written as the product of two non-zero algebras. Much like before for the module decompositions, any such decomposition corresponds to a decomposition of the identity into **centrally primitive orthogonal idempotents**. Here a centrally primitive idempotent is an idempotent which is in the center of the algebra (i.e. commutes with any of its elements) and cannot be written as a sum of non-zero central idempotents.

**Theorem 3.5.** [13, p. 28] Let $A \simeq A_1 \times A_2 \times \cdots \times A_s \simeq B_1 \times B_2 \times \cdots \times B_q$ be decompositions of $A$ into indecomposable algebras and $1 = e_1 + \cdots + e_s = f_1 + \cdots + f_q$ be
the respective central decompositions of the identity. Then \( s = q \) and up to reordering we have \( e_i = f_i \) and \( A_i \simeq B_i \).

We will use the same notation for the inner direct product of algebras. In this case, the algebras \( A_i \) are two-sided ideals of \( A \) and hence also left and right \( A \)-modules. Thus for \( a \in A \), we write \( a = a_1 + \ldots + a_s \) where \( a_i \in A_i \).

Let us give some examples illustrating the concepts we reviewed. The first class of examples are given by the upper triangular matrices in \( M_n(\mathbb{C}) \). If \( n = 2 \), then we have

\[
A := \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{C} \right\}.
\]

Let \( e_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \) and \( e_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \). Then clearly \( 1 = e_1 + e_2 \), and \( e_1A = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \right\} \) and \( e_2A = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix} \right\} \) are non-isomorphic indecomposable modules. (We adopt the convention that where the entries are unspecified we consider them as arbitrary elements of \( \mathbb{C} \).) Below we give some criteria to check that the modules are indecomposable. So \( A \) is basic with \( e_1A \) and \( e_2A \) being the principal modules of \( A \). On the other hand, if we take

\[
B := M_2(\mathbb{C}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right\}
\]

and take \( e_1 \) and \( e_2 \) as above, then we get

\[
e_1B = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \right\}
\]

and

\[
e_2B = \left\{ \begin{bmatrix} 0 & 0 \\ c & d \end{bmatrix} \right\}.
\]
Thus we have $B = e_1B \oplus e_2B$ but $e_1B \simeq e_2B$ and $B$ is not basic. $B$ is actually a simple algebra. For a semisimple algebra which is not simple take $B \oplus B$.

Now we look at a composition series for $A$ as an $A$-module. $M_0 = 0$ and let $M_1 = \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix}$. Then $M_1$ is invariant under multiplication by arbitrary elements of $A$ and $M_1/M_0 = M_1$ is simple since $\dim(M_1) = 1$. Let $M_2 = \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix}$. $M_2$ is invariant under multiplication on the right by elements of $A$ and $M_2/M_1$ has dimension 1, hence it is simple. We take $M_3 = A$ to complete the composition series. So in particular we see that $A$ has length 3 as an $A$-module.

We do the same for $B$, but the steps are little less obvious. Take $M_0 = 0$ and $M_1 = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$. That $M_1$ is a right module is clear. It is a little more difficult to see that it is simple. Suppose $I$ is a non-zero submodule of $M_1$ and $m = \begin{pmatrix} m_1 & m_2 \\ 0 & 0 \end{pmatrix}$ a non-zero element in $I$. Without loss of generality assume $m_1 \neq 0$. Let $a_x = \begin{pmatrix} m_1^{-1}x_1 & m_1^{-1}x_2 \\ 0 & 0 \end{pmatrix}$.

Then for any $x_1, x_2 \in \mathbb{C}$,

$$\begin{pmatrix} m_1 & m_2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} m_1^{-1}x_1 & m_1^{-1}x_2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ 0 & 0 \end{pmatrix}$$

for any choice of $x = [x_1, x_2]$. Then $a_x \in B$, and $ma_x = \begin{pmatrix} x_1 & x_2 \\ 0 & 0 \end{pmatrix}$, which we can choose to be any element of $M_1$. Therefore, $I = M_1$ and $M_1$ is simple. Now take $M_2 = B$. That $M_2/M_1$ is simple follows from the same type of argument.
Comparing the two decompositions of $B$ we see that the principal modules are actually simple modules. $B$ is the sum of simple modules and is an example of a semisimple algebra, see the definition below.

**Example:** We now give an example of using centrally primitive idempotents to decompose an algebra into a product of algebras. Let

$$A := \left\{ \begin{bmatrix} a & b - a \\ 0 & b \end{bmatrix} \right\}.$$ 

Let

$$e_1 := \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad e_2 := \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$ 

That $e_1$ and $e_2$ are idempotents is clear. $e_1$ is also central since for an element in $x \in A$

$$x = \begin{bmatrix} a & b - a \\ 0 & b \end{bmatrix} \quad \text{we have} \quad e_1 x = \begin{bmatrix} a & -a \\ 0 & 0 \end{bmatrix} = x e_1.$$ 

A similar calculation shows that $e_2$ is central. Now take $A_1 := e_1 A = e_1 Ae_1$ and $A_2 := e_2 A = e_2 Ae_2$. Then $A$ is given as the (inner) direct product of the algebras $A_1$ and $A_2$, i.e.,

$$A = A_1 \times A_2 = \left\{ \begin{bmatrix} a & -a \\ 0 & 0 \end{bmatrix} \right\} \times \left\{ \begin{bmatrix} 0 & b \\ 0 & b \end{bmatrix} \right\}.$$ 

### The Radical and Semisimplicity

The concept of the radical is crucial to any further understanding of finite dimensional algebras. In this section we collect the important definitions and theorems pertaining to the radical of a module and the radical of an algebra.
A submodule $N$ of a module $M$ is maximal if $N \neq M$ and any other proper submodule $P$ containing $N$ must equal $N$. The radical of the module $M$, denoted $\text{rad}(M)$ is the intersection of all maximal submodules of $M$. Equivalently, $\text{rad}(M)$ is the set of all elements of $m \in M$ such that $f(m) = 0$ for any homomorphism $f : M \to U$ where $U$ is a simple module.

If the module $M$ is simple then 0 is the only maximal submodule so $\text{rad}(M) = 0$. If $M$ is a module for which $\text{rad}(M) = 0$ then we say that $M$ is semisimple. Equivalently $M$ is semisimple if and only if $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$ where each $M_i$ is simple. See [13, p. 32] for a complete characterization of semisimple modules. An algebra $A$ is said to be semisimple if $A$ treated as the regular module is semisimple. Here by default the regular module is the right regular module, but taking the left regular module would have resulted in the same definition. An algebra which has no two-sided ideals other than $A$ and 0 is called simple. The radical of the algebra $A$ is the radical of the regular $A$-module. That is, $\text{rad}(A)$ is the intersection of all maximal right ideals of $A$. We have the following useful characterization of $\text{rad}(A)$.

**Lemma 3.6.** [13, p. 48] The radical of an algebra is the unique nilpotent (two-sided) ideal such that the respective quotient algebra is semisimple.

To see the relationship between simple and semisimple algebras we give the following simple result.

**Proposition 3.7.** If $A$ is a simple algebra, then $A$ is semisimple.

**Proof.** Suppose $A$ is a simple algebra. Then $\text{rad}(A)$ is a two sided ideal, so $\text{rad}(A) = A$ or $\text{rad}(A) = 0$. Since $1 \in A$, then $A$ is not nilpotent and $\text{rad}(A) \neq A$. Therefore, $\text{rad}(A) = 0$ and $A$ is semisimple. \qed

The key example is the algebra $M_n(\mathbb{C})$ of $n \times n$ matrices with entries in $\mathbb{C}$. 
Proposition 3.8. For any \( n \), the algebra \( M_n(\mathbb{C}) \) is a simple algebra.

Proof. We first show that \( M_n(\mathbb{C}) \) is a semisimple algebra. That is the regular \( M_n(\mathbb{C}) \) module is the direct sum of simple modules. The regular \( M_n(\mathbb{C}) \) module is the direct sum of \( I_i \), for \( i = 1, \ldots, n \), where \( I_i \) is the ideal of \( M_n(\mathbb{C}) \) consisting of arbitrary elements of \( \mathbb{C} \) in the \( i \)th row and zeros elsewhere. For each \( i \) we have \( I_i \cong M_n(\mathbb{C}) \mathbb{C}^n \). \( \mathbb{C}^n \) is a simple \( M_n(\mathbb{C}) \) module, thus each \( I_i \) is simple.

We now show the simplicity of \( M_n(\mathbb{C}) \). Suppose \( I \) is a non-zero two-sided ideal of \( M_n(\mathbb{C}) \). We show that \( I = M_n(\mathbb{C}) \). \( I \) contains a matrix \( M = (M_{ij}) \) with some entry \( M_{kl} \neq 0 \). For each \( i, j \in \{1, \ldots, n\} \) define \( e_{i,j} \) as the matrix with 1 in the \( i, j \) position and 0 elsewhere. Then \( e_{i,k} \in I_i \). Thus \( e_{i,k} M \neq 0 \) and it belongs to both \( I \) and \( I_i \). But \( I_i \) is simple, hence \( I \supset I_i \) for every \( i \). Thus \( I \supset \sum_{i=1}^{n} I_i = M_n(\mathbb{C}) \).

The following fundamental theorem is key to our application of the theory of finite dimensional algebras to cocyclic subshifts.

Theorem 3.9. [13, p. 38] (Wedderburn-Artin) Any simple algebra over \( \mathbb{C} \) is isomorphic to a matrix algebra over \( \mathbb{C} \). Every semisimple algebra over \( \mathbb{C} \) is isomorphic to a direct product of matrix algebras over \( \mathbb{C} \).

Proposition 3.10. For any \( A \)-module \( M \), the quotient module \( M/\text{rad}(M) \) is semisimple. In particular, \( A/\text{rad}(A) \) is a semisimple algebra for any algebra \( A \).

Proof. By the homomorphism theorem for modules, see [13, p.15], the maximal sub-modules of \( M/\text{rad}(M) \) are given by \( M'/\text{rad}(M) \) where \( M' \) is a maximal submodule of \( M \). But then taking the intersection over all such \( M' \), \( \cap (M'/\text{rad}(M)) = (\cap M')/\text{rad}(M) = \text{rad}(M)/\text{rad}(M) = 0. \) \( \square \)
Lemma 3.11. (1) For any $A$-modules $M$ and $N$, if $f : M \to N$ is a module homomorphism, then $f(\text{rad}(M)) \subset \text{rad}(N)$.

(2) For any $A$-module $M$, we have that $\text{rad}(M) = M\text{rad}(A)$.

(3) For any $a \in A$, $\text{rad}(aA) = a\text{rad}(A)$.

Proof. (1) Let $m \in \text{rad}(M)$ and $g : N \to U$ be a homomorphism from $N$ to a simple module $U$. We see that $g(f(m)) = 0$ since the composition $g \circ f$ is a homomorphism from $M \to U$. So $f(m) \in \text{rad}(N)$.

(2) For any $m \in M$, the map that sends $a \mapsto ma$ for all $a \in A$ is a homomorphism. So, by (1) $m\text{rad}(A) \subset \text{rad}(M)$. Hence, $M\text{rad}(A) \subset \text{rad}(M)$.

We have to see that the inclusion is in fact equality. We assume $m \notin M\text{rad}(A)$ and show that $m \notin \text{rad}(M)$. Since $m \notin M\text{rad}(A)$ we have $m + M\text{rad}(A) \in M/M\text{rad}(A)$ is non-zero. Since $M/M\text{rad}(A)$ is a semisimple $A/\text{rad}(A)$ module (every module over a semisimple algebra is semisimple), there is a homomorphism $f : M/M\text{rad}(A) \to U$ for some simple $A/\text{rad}(A)$-module $U$, with $f(m + M\text{rad}(A)) \neq 0$. But $U$ is also a simple $A$-module (where $ua = u(a + \text{rad}(A))$ for all $u \in U, a \in A$). Let $\pi : M \to M/M\text{rad}(A)$, then for the homomorphism $f \circ \pi : M \to U$ we have $f(m) \neq 0$. Therefore, $m \notin \text{rad}(M)$ by the definition of the radical.

(3) From (2) with $M = aA$, we have $\text{rad}(aA) = a\text{rad}(A)$. From (2) with $M = A$ we have $A\text{rad}(A) = \text{rad}(A)$. Therefore we have $aA\text{rad}(A) = a\text{rad}(A)$.

\[\square\]

We will need the following corollary,

Corollary 3.12. Every semisimple $A$-module $M$ is naturally a module over the semisimple quotient algebra $A/\text{rad}(A)$. (The action of $a + \text{rad}(A)$ on $M$ is given by $m \mapsto ma$.)
Semisimple Part of an Algebra

We start with some basic definitions.

**Definition 3.13.** By the Wedderburn-Artin Theorem, given any algebra \( A \), we can decompose \( A/\text{rad}(A) \) into algebras \( A/\text{rad}(A) = B_1 \times \cdots \times B_n \) where each \( B_i \) is isomorphic to a full matrix algebra over \( \mathbb{C} \). \( B_i = e_i(A/\text{rad}(A))e_i = e_iA/e_i\text{rad}(A) \) where \( 1 = e_1 + \cdots + e_s \) and \( e_i \) are centrally primitive orthogonal idempotents in \( A/\text{rad}(A) \). We call \( B_i \) the blocks of the semisimple algebra \( A/\text{rad}(A) \).

For an arbitrary algebra \( A \) we may gain some understanding of \( A \) by considering \( A/\text{rad}(A) \). At times it is useful to consider an algebra which is contained in \( A \) and is isomorphic to \( A/\text{rad}(A) \), see the Wedderburn-Malcev Theorem below.

An algebra homomorphism \( \epsilon : A/\text{rad}(A) \to A \) such that \( \pi \circ \epsilon = \text{Id} \), where \( \pi : A \to A/\text{rad}(A) \) is the standard projection, is called a lifting of the algebra \( A/\text{rad}(A) \). Where we have a fixed \( \epsilon \) we write \( A_0 = \text{Im}(\epsilon) \). We also refer to \( A_0 \) as a complement of the radical in \( A \). There could be many liftings, but they are all unipotently conjugate. Here, two liftings \( \epsilon \) and \( \nu \) are said to be unipotently conjugate if there is \( r \in \text{rad}(A) \) such that \( a = 1 + r \in A \) is an invertible element of \( A \) and for any \( x \in A/\text{rad}(A) \), we have \( \nu(x) = a\epsilon(x)a^{-1} \).

**Theorem 3.14.** (Wedderburn-Malcev Theorem) If \( A \) is an algebra over \( \mathbb{C} \), then a lifting of \( A/\text{rad}(A) \) exists and any two liftings are unipotently conjugate.

This is a specialization of Theorem 6.2.1 in [13, p.107] to the algebraically closed field \( \mathbb{C} \). After giving an example we do a calculation that amounts to a proof in our case.
Example: Let 

\[ A = \begin{cases} 
\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} 
\end{cases} \].

We show that there are two liftings of \( A/\text{rad}(A) \) and find the element that facilitates unipotent conjugacy. First define 

\[ A_0 := \begin{cases} 
\begin{bmatrix} x & 0 \\ 0 & z \end{bmatrix} 
\end{cases} \].

Now 

\[ \text{rad}(A) = \begin{cases} 
\begin{bmatrix} 0 & y \\ 0 & 0 \end{bmatrix} 
\end{cases} \].

For an element \( \bar{b} := \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} + \text{rad}(A) \), define \( \epsilon(\bar{b}) = \begin{bmatrix} x & 0 \\ 0 & z \end{bmatrix} \). Note that \( \epsilon \) is a well defined homomorphism from \( A/\text{rad}(A) \) to \( A \). Also \( \pi(A_0) = A/\text{rad}(A) \) and \( \pi \circ \epsilon = \text{Id}_{A/\text{rad}(A)} \).

Now consider 

\[ A_0' := \begin{cases} 
\begin{bmatrix} x & x-z \\ 0 & z \end{bmatrix} 
\end{cases} \].

For \( \bar{b} \in A/\text{rad}(A) \) as above define \( \nu(\bar{b}) = \begin{bmatrix} x & x-z \\ 0 & z \end{bmatrix} \). \( \nu \) is well defined. By inspection, we get \( \pi \circ \nu = \text{Id}_{A/\text{rad}(A)} \).

Let \( a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \), then \( a^{-1} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \); and for any \( \bar{b} \in A/\text{rad}(A) \) we have 

\[ a\epsilon(\bar{b})a^{-1} = \nu(\bar{b}) \]. Therefore, \( \nu \) and \( \epsilon \) are unipotently conjugate liftings of \( A/\text{rad}(A) \).

Suppose \( A_0 \) is a complement of the radical in \( A \). Since \( A_0 \) is semisimple it can be written as \( A_0 = A_1 \times A_2 \times \cdots \times A_n \). Thus there is a corresponding decomposition of the identity in \( A_0 \) into centrally primitive idempotents in \( A_0 \), say \( 1 = e_1 + e_2 + \ldots + e_n \).
But then this is a decomposition of the identity in $A$ as well into not necessarily central but orthogonal idempotents. Thus for any complement of the radical there is a corresponding decomposition of $1 \in A$ into (not necessarily primitive or central) orthogonal idempotents that become centrally primitive when viewed in $A_0$. We explain now how to find such a decomposition. We construct $A_0$ in terms of a central decomposition of $1$ and use Lemma 3.4 to show it is semisimple.

Let $A \simeq k_1P_1 \oplus \ldots \oplus k_nP_n$ with principal modules $P_i = e_iA$. Thinking of a decomposition of $1$ into primitive orthogonal idempotents as being fixed we have the following definitions.

**Definition 3.15.** The $i$-th total idempotent is

$$f_i = \sum_{e_iA \simeq A} e_jA.$$

**Definition 3.16.** The standard complement of the radical is given by,

$$A_0 = f_1Af_1 \oplus \cdots \oplus f_nAf_n$$

Now $1 = f_1 + \cdots + f_n$ is a central decomposition of $1 \in A_0$. We show $A_0 \simeq A/\text{rad}(A)$. To see the isomorphism we use Lemma 3.4 part (2) to see that for any idempotents $f, g \in A$ we have $fAg \simeq \text{Hom}_A(gA, fA)$, in particular if $f = g$ we write $\text{End}_A(fA) = \text{Hom}_A(fA, fA)$. So we have

$$A_0 \simeq \text{End}_A(f_1A) \oplus \cdots \oplus \text{End}_A(f_nA)$$

$$\simeq \text{End}_A(k_1P_1) \oplus \cdots \oplus \text{End}_A(k_nP_n),$$

where $P_i$ is the corresponding principal module. But then $\text{End}_A(k_iP_i) \simeq M_{k_i}(A_i)$ with $A_i = \text{End}_A(P_i)$. (See Theorem 1.7.5 in [13] and the discussion of the Peirce Decomposition.) Now $\text{End}_A(P_i)$ is local by Lemma 3.24, and $\text{rad}(\text{End}_A(P_i)) = 0,$
so \( \text{End}_A(P_1) \) is a division algebra over \( \mathbb{C} \). But \( \mathbb{C} \) is algebraically closed so that \( \mathbb{C} \) is the only division algebra over \( \mathbb{C} \) (see Corollary 1.2.6 in [13]), hence \( \text{End}_A(P_1) \simeq \mathbb{C} \). Therefore we have \( A_0 \simeq M_{k_1}(\mathbb{C}) \oplus \cdots \oplus M_{k_n}(\mathbb{C}) \simeq A/\text{rad}(A) \). Note that we have not actually shown the last isomorphism in this calculation. To do so we need to know that the principal modules are the projective covers of the simple modules (see below and [13, p.107]).

**More on Principal Modules and Module Decomposition**

For this section we still assume as in the argument we just gave at the end of the last section that, \( 1 = e_1 + \ldots + e_p \) is a decomposition of \( 1 \in A \) into primitive orthogonal idempotents. We also assume that \( \{e_1A, \ldots e_nA\} \) is a complete collection of principal modules. We take \( N := \text{rad}(A) \).

**Proposition 3.17.** Suppose \( e_iA \simeq_A e_jA \) and \( e_kA \simeq_A e_lA \) (i, j, k, l \( \in \{1, \ldots, p\} \)), then \( e_iAe_k \simeq e_jAe_l \) where the last isomorphism is of vector spaces.

**Proof.** This follows from two applications of Lemma 3.4, which gives \( e_iAe_k \simeq \text{Hom}_A(e_kA, e_iA) \simeq \text{Hom}_A(e_iA, e_jA) \simeq e_jAe_l \). \( \square \)

**Corollary 3.18.** Let \( f_i \) and \( f_j \) be total idempotents for \( i, j = 1, \ldots, n \), see Definition 3.15. Then

\[ e_iAe_j = 0 \iff f_iAf_j = 0 \quad (i, j = 1, \ldots, n). \]

**Proof.** \( f_iAf_j \) resolves into a direct sum of terms of the form \( e_kAe_l \), each of which is isomorphic to \( e_iAe_j \). Hence, \( f_iAf_j = 0 \) if and only if \( e_iAe_j = 0 \). \( \square \)

A module \( P \) is called **projective** if for any epimorphism \( g : M_1 \rightarrow M_2 \) and every homomorphism \( f : P \rightarrow M_2 \) there is a homomorphism \( \phi : P \rightarrow M_1 \) such that \( f = g\phi \).
A projective module $P$ is called a projective cover of the module $M_1$ if there is an epimorphism $P \to M_1$ which induces an isomorphism $P/\text{rad}(P) \to M_1/\text{rad}(M_1)$.

**Theorem 3.19.** [13, p. 53] Every module has a projective cover which is unique up to isomorphism.

The following Theorem and Corollary are composed of various results found in [13, p. 49-54].

**Theorem 3.20.** For any finite dimensional algebra $A$ there are finitely many isomorphism classes of simple modules. Let $S_1, \ldots, S_n$ be their representatives. The principal indecomposable modules $P_1 = e_1A, \ldots, P_n = e_nA$ are the projective covers of the these simple modules and $S_i \simeq_A e_iA/\text{rad}(e_iA)$ for $i = 1, \ldots, n$ (after relabelling).

**Corollary 3.21.** [13, p. 50] $e_iA \simeq_A e_jA$ if and only if $e_iA/e_iN \simeq_A e_jA/e_jN$.

**Corollary 3.22.** [13, p. 51] $e_iA \simeq_A e_jA$ if and only if $Ae_i \simeq_A Ae_j$.

**Proposition 3.23.** For $i, j \in \{1, \ldots, n\}$ with $i \neq j$ (which implies $e_iA \not\simeq e_jA$) we have $e_i Ae_j = e_i Ne_j$.

**Proof.** Recall that $e_iAe_j \simeq \text{Hom}_A(e_jA, e_iA)$, by Lemma 3.4. The key claim is that

$$\text{Hom}_A(e_jA, e_iA) \simeq \text{Hom}_A(e_jA, \text{rad}(e_iA)),$$

for which we need to show that if $f$ is a homomorphism from $e_jA$ to $e_iA$ then $\text{Im}(f) \subset \text{rad}(e_iA)$. Since $f(\text{rad}(e_jA)) \subset \text{rad}(e_iA)$ (by Lemma 3.11), and if $\text{Im}(f) \not\subset \text{rad}(e_iA)$, then the induced map $f' : e_jA/\text{rad}(e_jA) \to e_iA/\text{rad}(e_iA)$ is non-zero, which is impossible since these are non-isomorphic simple modules (by the hypothesis).

So we have $\text{Hom}(e_jA, \text{rad}(e_iA)) \simeq \text{rad}(e_iA)e_j$ again by Lemma 3.4 and $\text{rad}(e_iA)e_j = e_i Ne_j$ by Lemma 3.11. Hence $e_i Ne_j$ is a subspace of $e_iAe_j$ of the same dimension (since they are isomorphic). So $e_i Ne_j$ and $e_iAe_j$ must be equal.

\[\Box\]
An algebra $A$ is said to be *local* if $A/rad(A)$ is a division algebra. The following lemma will be of particular use to us below to determine if we have truly found the principal modules of $A$.

**Lemma 3.24.** [13, p. 49] (Fitting) A module is indecomposable if and only if its endomorphism algebra is local.

Before getting to examples we include a couple more lemmas that allow us to determine the principal modules in practice. Recall that an ideal $I$ (right, left, or two-sided) is *nilpotent* if $I^k = \{a_1a_2\ldots a_k|a_i \in I, i = 1, \ldots , k\} = 0$ for some $k \in \mathbb{N}$.

**Lemma 3.25.** [10, p.160] For any non-nilpotent right (left) ideal $I$, there is a non-zero idempotent contained in $I$.

**Lemma 3.26.** Suppose $I$ is an indecomposable non-nilpotent right ideal of $A$. Then $I = eA$ where $e$ is a primitive idempotent. Hence $I$ is a principal indecomposable module.

*Proof.* Since $I$ is not nilpotent there is an idempotent $e \in I$. But $I$ is a right ideal so that $eA \subset I$, in particular $eI \subset I$. But then $(1-e)I \oplus eI = I$ since $(1-e)a = ea$ implies $0 = e(1-e)a = ea$. Now $I$ is indecomposable so since $eI \neq 0$ we have $(1-e)I = 0$, and therefore $eI = I$. Now $eI \subset eA \subset I$, so $eA = I$. That $e$ is primitive follows from the indecomposability of $I$. \qed

In the previous sections we have reviewed a great deal of the theory of finite dimensional algebras. We now give an example that uses much of this theory.
Example: Let

\[ A = \begin{cases} 
    \begin{bmatrix} 
        x & a & y & b \\
        0 & x & 0 & y \\
        0 & c & z & d \\
        0 & 0 & 0 & z 
    \end{bmatrix}, & a, b, c, d, z, y, z \in \mathbb{C} \\
\end{cases} \]

We compute \( \text{rad}(A) \) using Lemma 3.6. Let

\[ I = \begin{cases} 
    \begin{bmatrix} 
        0 & a & 0 & b \\
        0 & 0 & 0 & 0 \\
        0 & c & 0 & d \\
        0 & 0 & 0 & 0 
    \end{bmatrix}, & \end{cases} \]

It is straightforward to see that \( I \) is a two sided ideal of \( A \). Also, \( I^2 = 0 \) and

\[ A/I \simeq \begin{cases} 
    \begin{bmatrix} 
        x & 0 & y & 0 \\
        0 & x & 0 & y \\
        0 & 0 & z & 0 \\
        0 & 0 & 0 & z 
    \end{bmatrix}, \end{cases} \]

which is semi-simple since the ideals

\[ I_1 = \begin{cases} 
    \begin{bmatrix} 
        x & 0 & 0 & 0 \\
        0 & x & 0 & 0 \\
        0 & 0 & 0 & 0 \\
        0 & 0 & 0 & 0 
    \end{bmatrix}, I_2 = \begin{cases} 
        \begin{bmatrix} 
            0 & 0 & y & 0 \\
            0 & 0 & 0 & y \\
            0 & 0 & 0 & 0 \\
            0 & 0 & 0 & 0 
        \end{bmatrix}, I_3 = \begin{cases} 
            \begin{bmatrix} 
                0 & 0 & 0 & 0 \\
                0 & 0 & 0 & 0 \\
                0 & 0 & z & 0 \\
                0 & 0 & 0 & z 
            \end{bmatrix} \end{cases} \end{cases} \]

are all one dimensional and \( A/I \simeq I_1 \oplus I_2 \oplus I_3 \). So by Lemma 3.6 we have \( \text{rad}(A) = I \).

Now let \( e_1 = \begin{bmatrix} 
    1 & 0 & 0 & 0 \\
    0 & 1 & 0 & 0 \\
    0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 
\end{bmatrix} \), \( e_2 = \begin{bmatrix} 
    0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 \\
    0 & 0 & 1 & 0 \\
    0 & 0 & 0 & 1 
\end{bmatrix} \) then \( 1 = e_1 + e_2 \), and \( e_1 e_2 = 0 = e_2 e_1 \).
Note that \( e_1 \) is minimal (alternatively, \( e_1A \) is indecomposable) since

\[
\text{End}_A(e_1A) \cong e_1Ae_1 = \left\{ \begin{bmatrix} x & a & 0 & 0 \\ 0 & x & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \right\}
\]

with \( e_1Ae_1/e_1\text{rad}(A)e_1 \) one dimensional, hence isomorphic to \( \mathbb{C} \). The same type of calculation shows that \( e_2A \) is indecomposable and \( e_2 \) is minimal. Note that \( e_1A \) and \( e_2A \) are not isomorphic. Thus \( A \) is basic with \( A = e_1A \oplus e_2A \).
We now apply the theory of algebras to the understanding of cocyclic subshifts. Throughout this chapter we consider two-sided cocyclic subshifts, see Definition 2.1. Let $\Phi = (\Phi_k)_{k=1}^K$ be a cocycle with $\Phi_k \in \text{End}(V)$. As before, let $A^+$ be the collection of non-empty words of the alphabet $A = \{1, \ldots, K\}$. Recall that for a word $w = w_1 \ldots w_n \in A^+$ where $w_i \in A$, $\Phi_w$ stands for the product $\Phi_{w_1} \cdots \Phi_{w_n}$. We have the following fundamental definition.

**Definition 4.1.** The algebra generated by $\Phi$ is a subalgebra of $\text{End}(V)$ given by

$$A = \{ \sum_{i=1}^t a_i \Phi_{w_i} | a_i \in \mathbb{C}, w_i \in A^+, t \in \mathbb{N} \}.$$ 

Note that since we allowed only non-empty words in the definition of $A$ it is possible that the identity is not in $A$. (Note that $\Phi_\epsilon = \text{Id}$ is the natural choice for the empty word $\epsilon$, since concatenating any word with $\epsilon$ should have no effect on the corresponding product.) To simplify the presentation we assume that $A$ contains the identity, and describe in section Non-Unital Algebras how to accommodate the case when the identity is not in $A$.

Now, let $M$ be an $A$-module. The action of $\Phi_k$ on $M$ naturally induces a linear map on $M$, which we denote by $\Phi_k|_M$. For the cocyclic subshift associated to $\Phi|_M := (\Phi_k|_M)_{k=1}^K$ we write $X_{\Phi,M}$. If there is no ambiguity we simply write $X_M$. Before proving some fundamental facts pertaining to subshifts of modules, we recall some facts about formal languages.
Recall that the language of a subshift $X$, $\mathcal{L}(X)$, is the collection of all words that occur in $X$, that is

$$\mathcal{L}(X) = \{ w \in A^* \mid \exists x \in X, \text{ with } w \sqsubseteq x \}.$$ 

For a word $w \in A^*$, we define the cylinder set

$$[w] := \{ x \in A^Z \mid x_{[-k,k]} = w \text{ for } |w| = 2k + 1 \text{ or } x_{[-k,k-1]} = w \text{ for } |w| = 2k \}.$$ 

**Proposition 4.2.** For subshifts $X$ and $Y$, $X = (\bigcup \{ [w] \mid w \notin \mathcal{L}(X) \})^c$ and $X = Y$ if and only if $\mathcal{L}(X) = \mathcal{L}(Y)$.

For further discussion and proofs see [27].

We shall repeatedly use the following simple lemma that is largely responsible for the effectiveness of the algebraic approach to cocyclic subshifts.

**Lemma 4.3.** (i) For any algebra $A$, suppose we are given finite sets $E_1, \ldots, E_m \subset A$ and $\Gamma_k \in \text{span}(E_k)$ such that $\Gamma_1 \Gamma_2 \cdots \Gamma_m \neq 0$ then there are $\Psi_i \in E_i$, for $i = 1, \ldots, m$, such that

$$\Psi_1 \Psi_2 \cdots \Psi_m \neq 0.$$

(ii) Suppose we are given finite sets $E_k \subset A$ for $k \in \mathbb{Z}$. If, for any $n \in \mathbb{N}$, there are $\Gamma_k \in \text{span}(E_k)$ for $k \in \{-n, \ldots, n\}$ such that $\Gamma_{-n} \cdots \Gamma_n \neq 0$ then there are $\Psi_k \in E_k$, for $k \in \mathbb{Z}$, such that for any $n \in \mathbb{N}$

$$\Psi_{-n} \cdots \Psi_n \neq 0.$$

**Proof.** (i) (Contrapositive) If $\Psi_1 \cdots \Psi_m = 0$ for all selections of $\Psi_k \in E_k$ ($k = 1, \ldots, n$) then multiplying out $\Gamma_1 \Gamma_2 \cdots \Gamma_m$ yields a sum each term of which is zero. Hence $\Gamma_1 \Gamma_2 \cdots \Gamma_m = 0$. 


(ii) By using (i), for any \( n \in \mathbb{N} \) we have \( \Psi_{n,k} \in E_k \) for \( k \in \{-n, \ldots, n\} \) such that 
\[ \Psi_{n,-n} \cdots \Psi_{n,n} \neq 0. \]

For any \( l \in \mathbb{N} \) there is \( (n_i(l))_j \in \mathbb{N} \) such that \( n_i(l) \to \infty \) and \( (\Psi_{n_i(l),-l}, \ldots, \Psi_{n_i(l),l}) \) are independent of \( j \) and thus equal to some \( (\Psi^{(l)}_{-l}, \ldots, \Psi^{(l)}_l) \). In fact, we can choose \( (n_{i(l)+1})_j \) which is a subsequence of \( (n_i(l))_j \) for \( l \in \mathbb{N} \). In this way \( \Psi^{(l)}_k \) does not depend on \( l \) and \( \Psi_k := \Psi^{(l)}_k \) have the desired property,
\[ \Psi_{-n} \cdots \Psi_n \neq 0 \text{ for all } n \in \mathbb{N}. \]

\[ \square \]

**Proposition 4.4.** If \( 1 \in A \), where \( A \) is the algebra generated by the cocycle \( \Phi \), then \( X_\Phi \neq \emptyset \).

**Proof.** Suppose \( 1 \in A \), then there is a finite collection of non-empty words \( w_1, \ldots, w_n \) such that \( 1 = a_1 \Phi_{w_1} + \cdots + a_n \Phi_{w_n} \) and \( a_1, \ldots, a_n \in \mathbb{C} \). Take \( E = \{ \Phi_{w_1}, \ldots, \Phi_{w_n} \} \).

Then, for any \( k \in \mathbb{N} \), the product \( (\sum_i a_i \Phi_{w_i})^{2k+1} \) is non-zero. By Lemma 4.3 (i), there are choices \( \Phi_{w_{i-k}}, \ldots, \Phi_{w_{i+k}} \) such that \( \Phi_{w_{i-k}} \cdots \Phi_{w_{i+k}} \neq 0 \). By Lemma 4.3 (ii), there is a sequence, \( \ldots w_{i-1} w_{i_0} w_{i_1} \ldots \) such that \( \cdots \Phi_{w_{i-1}} \Phi_{w_{i_0}} \Phi_{w_{i_1}} \cdots \neq 0 \). Hence, \( x = \ldots w_{i-1} w_{i_0} w_{i_1} \ldots \in X_\Phi \).

\[ \square \]

**Proposition 4.5.** Let \( A \) be the algebra (containing \( 1 \)) of \( \Phi \) and \( M \) be a right \( A \)-module.

(1) For any \( w \in A^+ \), \( w \) occurs in \( X_\Phi \) if and only if \( \Phi_w \neq 0 \).

(2) For any \( w \in A^+ \), \( w \) occurs in \( X_M \) if and only if \( M \Phi_w \neq 0 \)

**Proof.** (1) The forward implication holds by definition.
Now suppose that $\Phi \neq 0$. Then $1^\infty \Phi \neq 0$. So by Lemma 4.3, there are words $w_k \in A^+$ ($k \in \mathbb{Z}$) such that $\cdots \Phi w_{-1} \Phi w_1 \cdots \neq 0$. Thus the word $w$ occurs in the element $x = \cdots w_{-1} w_1 \cdots \in X_\Phi$.

(2) The proof follows from the analogous argument starting with $M1^\infty \Phi \neq 0$.

**Proposition 4.6.** Let $A$ be the algebra of $\Phi$ containing 1 and let $M, N, M_1, M_2$ be right $A$-modules, then

(1) $X_M \subset X_\Phi = X_A$.

(2) If $f : M \rightarrow N$ is a surjective $A$-module homomorphism, then $X_M \supset X_N$.

(3) If $M \cong_A N$, then $X_M = X_N$.

(4) If $M = M_1 \oplus M_2$, then $X_M = X_{M_1} \cup X_{M_2}$.

**Proof.** (1) That $X_A = X_\Phi$ follows from the following equivalences for any $w \in A^+$:

\[ w \in \mathcal{L}(X_A) \iff A\Phi w \neq 0 \iff 1\Phi w \neq 0 \iff \Phi w \neq 0 \iff w \in \mathcal{L}(X_\Phi). \]

$X_M \subset X_\Phi$ by the following,

\[ w \in \mathcal{L}(X_M) \implies M\Phi w \neq 0 \implies \Phi w \neq 0 \implies w \in \mathcal{L}(X_\Phi). \]

(2) We argue the contrapositive:

\[ w \notin \mathcal{L}(X_M) \implies M\Phi w = 0 \implies f(M\Phi w) = 0 \implies f(\Phi w) = 0 \implies N\Phi w = 0 \implies w \notin \mathcal{L}(X_N). \]

(3) Follows from (2), since if $M \cong_A N$ then there are clearly surjective $A$-module homomorphisms in each direction. Thus the subshifts $X_M$ and $X_N$ are contained in each other.

(4) We have $w \in \mathcal{L}(X_M) \iff M\Phi w \neq 0 \iff (M_1 \oplus M_2)\Phi w \neq 0$. But $(M_1 \oplus M_2)\Phi w = M_1\Phi w \oplus M_2\Phi w$ which is non-zero if and only if $M_1\Phi w \neq 0$ or $M_2\Phi w \neq 0$. 
But, $M_1 \Phi_w \neq 0$ or $M_2 \Phi_w \neq 0$ if and only if $w \in \mathcal{L}(X_{M_1})$ or $w \in \mathcal{L}(X_{M_2})$. Now,

$$\bigcap \{[w] \mid [w] \cap X_M \neq \emptyset\} = \bigcap \{[w] \mid [w] \cap (X_{M_1} \cup X_{M_2}) \neq \emptyset\} = X_{M_1} \cup X_{M_2}.$$ 

We can immediately see the usefulness of the above proposition in decomposing a cocyclic subshift into other cocyclic subshifts, since if $A = M_1 \oplus \ldots \oplus M_n$ then $X_\Phi = X_{M_1} \cup \ldots \cup X_{M_n}$. The theory of finite dimensional algebras now allows us to decompose a cocyclic subshift in a particularly nice way, which we refer to as the *Wedderburn decomposition*. The following discussion of Wedderburn components and basic topological dynamics of cocyclic subshifts follows [26]. Note that the results here are slightly different as we are focused on two-sided cocyclic subshifts instead of one-sided ones.

We say that a cocycle $\Phi \in \text{End}(V)^k$ is *irreducible* if $V \neq 0$ and $A \simeq \text{End}(V)$. A cocyclic subshift is *irreducible* if it can be represented as $X_\Phi$ for some irreducible $\Phi$. For $x \in \mathcal{A}^\mathbb{Z}$, the *eventual rank* of $x$ (with respect to $\Phi$) is defined as

$$q(x) := \lim_{n \to \infty} \text{rank}(\Phi_x[-n,n]).$$

The set $\{x \in \mathcal{A}^\mathbb{Z} \mid q(x) > 0\} = X_\Phi$. The *forward orbit* of $x \in X_\Phi$ is given by $\mathcal{O}^+(x) := \{f^n(x) \mid n \in \mathbb{N}_0\}$. The *backward orbit* of $x \in X_\Phi$ is the set $\mathcal{O}^-(x) := \{f^{-n}(x) \mid n \in \mathbb{N}\}$.

We say that $X$ is *forward transitive* if there is an $x \in X$ such that $\mathcal{O}^+(x)$ is dense in $X_\Phi$. Likewise, $X_\Phi$ is *backward transitive* if $\mathcal{O}^-(x)$ is dense in $X_\Phi$.

**Theorem 4.7.** If $X_\Phi$ is irreducible then it is non-empty, transitive (both forward and backward), and the set of periodic points is dense.

**Proof.** These statements all hinge on the following claim.
Claim: For non-zero elements $a$ and $b$ of the algebra $A \cong \text{End}(V)$ there is an element $c \in \text{End}(V)$ with $acb \neq 0$.

Given a non-zero vector in the image of $a$ there is a map $c$ that takes that element to a non-zero vector not in $\text{Ker}(b)$. So then $acb \neq 0$.

We now show $X_\Phi$ is non-empty. There exists an element $a \neq 0$ in $A \cong \text{End}(V)$. So there is some $b \in A$ such that $ab \neq 0$. By writing $a$ and $b$ in terms of the basis of linear maps corresponding to words we can say that for any $w$ with $\Phi_w \neq 0$, by Lemma 4.3 there exists a $v$ with $\Phi_{vw} \neq 0$. This can be continued indefinitely, so applying Lemma 4.3 (ii), we see that $X_\Phi$ is not empty.

To see that $X_\Phi$ is transitive we let $\{w_l\}_{l \in \mathbb{N}}$ be an enumeration of the elements of $\mathcal{L}(X_\Phi)$. Now by the claim above we know there is some element $b_1$ with $\Phi_{w_1}b_1\Phi_{w_2} \neq 0$. Again we can write $b_1$ in terms of a basis corresponding to words to get some $u_1 \in A^+$ with $\Phi_{w_1u_1w_2} \neq 0$. Likewise, there exists $v_1 \in \mathcal{L}(X_\Phi)$ such that $\Phi_{w_2v_1w_1u_1w_2} \neq 0$. Continuing inductively (in both directions) we get

$$x = \ldots w_3v_2w_2v_1w_1u_1w_2u_2w_3 \ldots \in X_\Phi.$$ 

By construction of $x$, given some cylinder set that has non-empty intersection with $X_\Phi$, there is a forward and a backward iterate of $x$ that is contained in the cylinder set. This shows that $X$ is both forward and backward transitive.

We have found an element $x \in X$ which has forward trajectory dense in $X$. Take $n$ large enough so that $\text{rank}(\Phi_{x_{[-n,n]}}) = q(x)$, and let $w := x_{[-n,n]}$. There is a forward iterate of $x$, $f^t(x)$, such that for some $\alpha \in A^+$, we have $f^t(x)_{[-n,n+r]} = w\alpha w$ for some $r$. From the definition of $q(x)$, $\dim \text{Im}(\Phi_{w\alpha w}) = q(x) = \dim \text{Im}(\Phi_w)$ so that $V_0 := \text{Im}(\Phi_w)$ is a non-zero subspace with $\Phi_{w\alpha w}|_{V_0}$ a surjection, $V_0\Phi_{w\alpha w} = V_0$. Hence $\Phi_{w\alpha w}$ is non-nilpotent and so is $\Phi_{w^{n}w\alpha w}$. In particular, $(\Phi_{w^{n}w\alpha w})^n \neq 0$ for all $n \in \mathbb{N}$. So by
Lemma 4.3 we have \((w\omega w)\infty \in X_\phi\). But \(w\) was an arbitrary element of \(\mathcal{L}(X_\phi)\), thus the periodic points are dense. 

The following corollary follows from the proof of Theorem 4.7.

**Corollary 4.8.** If \(X\) is an irreducible cocyclic subshift, \(\forall u, v \in \mathcal{L}(X) \exists w \in \mathcal{L}(X)\) such that \(uwv \in \mathcal{L}(X)\). Also, for any \(w \in \mathcal{L}(X)\) and any \(n \in \mathbb{N}\), there is some \(x \in X\) such that \(w\) occurs infinitely many times in \(x\).

We need some additional topological dynamics of two-sided cocyclic subshifts to proceed. For a map \(f : X \to X\) a set \(U \subset X\) is **transient** if \(\sup_{x \in X} \# \{ n \in \mathbb{Z} | f^n(x) \in U \} < \infty\). The **transient set** of \(f\) is given by \(T(f) := \bigcup \{ U | U \text{ is open and transient} \} \).

The **recurrent set** is given by \(R(f) := \text{cl} \{ x \in X | x \in \omega(x) \cap \alpha(x) \}\) where \(\omega(x)\) is the accumulation set of \(\mathcal{O}^+(x)\), \(\alpha(x)\) is the accumulation set of \(\mathcal{O}^-(x)\), and “\(\text{cl}\)” denotes closure. The notation \(R(f)\) is somewhat problematic when more than one subshift is being considered, hence we also write \(X_+\) for the recurrent set of the subshift \(X\). For reference, we record the following simple lemma and leave the proof as an exercise.

**Lemma 4.9.** A set \(U\) is transient for a homeomorphism \(f : X \to X\) if and only if any one of the three supremums is finite.

(i) \(\sup_{x \in X} \# \{ n \in \mathbb{Z} | f^n(x) \in U \}\),

(ii) \(\sup_{x \in X} \# \{ n \in \mathbb{N} | f^n(x) \in U \}\),

(iii) \(\sup_{x \in X} \# \{ n \in \mathbb{N} | f^{-n}(x) \in U \}\).

**Proposition 4.10.** \(R(f) \subset T(f)^c\)

**Proof.** We argue “\(\subset\)” via the contrapositive. Suppose \(x \in T(f)\), then there is some open transient set \(U\) containing \(x\). By the definition of a transient set, there exists \(k \in \mathbb{N}\) such that for each \(y \in U\), \(\{ f^n(y) \}_{n \geq k} \cap U = \emptyset\) and \(\{ f^{-n}(y) \}_{n \geq k} \cap U = \emptyset\). So
y \notin \omega(y) \text{ or } y \notin \alpha(y). \text{ Thus } U \cap \{ z \mid z \in \alpha(z) \text{ and } z \in \omega(z) \} = \emptyset. \text{ Thus } x \text{ is not a limit of points } z \in X \text{ with } z \in \alpha(z) \cap \omega(z). \text{ Therefore } x \notin \mathcal{R}(f).

Note that when } f \text{ is the shift map on a cocyclic subshift, then } \mathcal{R}(f) = T(f)^c \text{ by Theorem 4.11, ahead.}

Let } V_1, \ldots, V_r \text{ be non-zero vector spaces. Suppose that } R : A \to \prod_{i=1}^r \text{End}(V_i) \text{ is a homomorphism of algebras such that } \ker(R) \text{ is nilpotent and the component maps } R_i : A \to \text{End}(V_i) \text{ are surjective for } i = 1, \ldots, r. \text{ For each } x \in X_{\Phi} \text{ we define the partial eventual ranks}

\[ q_i(x) = \lim_{n \to \infty} \text{rank}(R_i(\Phi_{x[-n,n]})), \quad i = 1, \ldots, r, \]

and } q_+(x) = \sum_i q_i(x). \text{ The following fundamental theorem is a modified version of Theorem 5.1 in [26].}

**Theorem 4.11.** (Spectral Decomposition) Suppose } X_{\Phi} \text{ is a (two-sided) cocyclic subshift, and } R : A \to \prod_{i=1}^r \text{End}(V_i) \text{ is as above. Let } (X_{\Phi})_i := X_{\Phi_i}, \text{ where } \Phi_i := (R_i(\Phi_k))_{k \in A}. \text{ (Note that we do not assume that } 1 \in A.) \text{ Then the union } \bigcup_{i=1}^r (X_{\Phi})_i \text{ is a cocyclic subshift and is equal to the recurrent set } (X_{\Phi})_+. \text{ Moreover,}

\[ (X_{\Phi})_+ = \{ x \in A^\mathbb{Z} \mid q_+(x) > 0 \} = T(X_{\Phi})^c. \]

**Proof.** That each } X_{\Phi_i} \text{ is irreducible is clear because the algebra of the cocycle } \Phi_i \text{ is } \text{End}(V_i) \text{ by the surjectivity hypothesis.}

Claim: } q_+(x) = 0 \text{ if and only if } x \text{ is transient.}

If } q_+(x) = 0 \text{ then there exists } n \text{ such that the image } R_i(\Phi_{x[-n,n]}) = 0 \text{ for all } i. \text{ But then } \Phi_{x[-n,n]} \in \ker(R) \subseteq \text{rad}(A). \text{ So } x[-n,n] \text{ can appear at most } t-1 \text{ times in any } y \in X_{\Phi} (\text{where } \text{rad}(A)^t = 0). \text{ So the cylinder set } [x[-n,n]] \text{ is transient and } x \in T(f).
On the other hand, suppose \( x \) is transient. Then there exists \( n \in \mathbb{N} \), such that the cylinder set \([x_{[-n,n]}] \) is transient. Now, the word \( x_{[-n,n]} \) cannot occur in an irreducible subshift since otherwise there would be a periodic orbit that contains \( x_{[-n,n]} \) infinitely many times, by Corollary 4.8. So this means that \( R_i(\Phi_{x_{[-n,n]}}) = 0 \) for each \( i \), and therefore \( q_+(x) = 0 \).

From the claim, we have \( \bigcup_{i=1}^\infty (X_\Phi) = \{ x \in X_\Phi | q_+(x) > 0 \} = (T(f))^c \). That \( (X_\Phi) \subset \mathcal{R}(f) \) follows from the irreducibility of \( (X_\Phi) \). This completes the proof since we have already shown \( \mathcal{R}(f) \subset (T(f))^c \).

Recall that if we decompose 1 in \( A \) into primitive, orthogonal idempotents \( 1 = e_1 + \ldots + e_p \), then we have \( A = e_1 A \oplus \ldots \oplus e_p A \) and \( A/N = e_1 A/e_1 N \oplus \ldots \oplus e_p A/e_p N \). We index so that \( e_1 A/e_1 N, \ldots, e_n A/e_n N \) is a complete collection of simple \( A \) modules (Theorem 3.20). We take \( B_i \) to be the sum of all \( e_j A/e_j N \), with \( j \in \{1, \ldots, p\} \) which are isomorphic \( e_i A/e_i N \), that is

\[
B_i \simeq \bigoplus_{j: e_j A \simeq e_i A} e_j A/e_j N.
\]

Recall that \( B_i \) are called the blocks of the semisimple algebra \( A/\text{rad}(A) \), and for each \( i \), \( B_i \) is isomorphic to the algebra of all endomorphisms of some vector space. Now, the canonical epimorphism \( \pi : A \to A/\text{rad}(A) = \prod_i B_i \) given by Definition 3.13 satisfies the conditions for \( R \).

**Theorem 4.12.** (1) \( (X_\Phi)_+ = X_{A/\text{rad}(A)} \).

(2) Let \( \pi_i : A \to B_i \) be the standard algebra epimorphism onto the block \( B_i \) of \( A/\text{rad}(A) \), then \( X_{B_i} = X_{\pi_i(\Phi)} \).

(3) For a simple module \( M \), \( X_M \) is irreducible.

**Proof.** (1) \( A/\text{rad}(A) \) is naturally an \( A \)-module taking \( (a + \text{rad}(A))b = ab + \text{rad}(A) \) for all \( a, b \in A \), so we can speak of \( X_{A/\text{rad}(A)} \). Since the standard projection \( \pi : A \to \)
$A/\text{rad}(A)$ satisfies the hypotheses on the homomorphism $R$ in Theorem 4.11 it follows that $X_\pi(\Phi)$ is equal to $(X_\Phi)_+$, where $\pi(\Phi) = (\pi(\Phi_k))_{k \in A}$. Now $X_{\pi(\Phi)} = X_{A/\text{rad}(A)}$ by Proposition 4.2 and the following equivalences.

$$w \in \mathcal{L}(X_{A/\text{rad}(A)}) \iff A/\text{rad}(A)\Phi_w \neq 0 \iff \Phi_w \notin \text{rad}(A)$$

$$\iff \pi(\Phi_w) \neq 0 \iff w \in \mathcal{L}(X_{\pi(\Phi)}).$$

(2) Let $B_i$ be a block of $A/\text{rad}(A)$. It is naturally an $A$-module and $X_{B_i} = X_{\pi_i(\Phi)}$ follows from

$$w \in \mathcal{L}(X_{B_i}) \iff B_i\Phi_w \neq 0 \iff \pi_i(1)\Phi_w + \text{rad}(A) \neq 0 \iff$$

$$\pi_i(\Phi_w + \text{rad}(A)) \neq 0 \iff \pi_i(\Phi_w) \neq 0 \iff w \in \mathcal{L}(X_{\pi_i(\Phi)}).$$

(3) For any simple module $M$, there exists $e_i$ such that $M \simeq e_iA/e_i\text{rad}(A)$ due to Theorem 3.20. But

$$B_i \simeq \bigoplus_{j: e_jA \simeq e_iA} e_jA/e_j\text{rad}(A).$$

Thus, using Proposition 4.6,

$$X_{\pi_i(\Phi)} = X_{B_i} = \bigcup_{j: e_jA \simeq e_iA} X_{e_jA/e_j\text{rad}(A)} = X_{e_iA/e_i\text{rad}(A)} = X_M. \quad (4.1)$$

$X_M$ is irreducible since we have previously observed that $X_{B_i}$ is irreducible.

So for the algebra $A$, the homomorphism $R : A \to A/\text{rad}(A)\simeq \prod_i \text{End}(V_i)$ provides a decomposition of $(X_\Phi)_+$ into irreducible cocyclic subshifts determined by cocycles $(\Phi)_i := (R_i(\Phi_k))_{k \in A}$. There are potentially many $R$ that can be used to decompose the space into irreducible subshifts, but this decomposition, which is called the **Wedderburn decomposition** in [26, p. 268], is ideal for our calculations.
We now think of the cocycle $\Phi$, its algebra $A$, and the decomposition $1 = e_1 + \ldots + e_p$ as being fixed. Recall that we denote $\text{rad}(A)$ by $N$. We would like to describe the connecting orbits between the irreducible subshifts given by the Wedderburn decomposition. As before $B_i$ is the $i$-th block of $A/N$. $B_i$ is an algebra which is isomorphic to the full matrix algebra of some vector space and $A/N = B_1 \times \cdots \times B_n$. Also, in Equation 4.1 we established that $X_{B_i} = X_{e_i A/e_i N}$.

**Definition 4.13.** For $i, j \in \{1, \ldots, n\}$ we write $i \rightarrow j$ if and only if $e_i A e_j \neq 0$.

**Definition 4.14.** The connecting set from $X_i$ to $X_j$ is given by

$$C_{i,j} = \{ x \in X | \alpha(x) \subset X_i \text{ and } \omega(x) \subset X_j \}.$$  

Below we will assume that the decomposition of $X_\Phi$ into Wedderburn components is a partition, i.e., we make the following Dynamical Disjointness Hypothesis on $\Phi$.

**Dynamical Disjointness Hypothesis (DD).** We say that a cocycle $\Phi$ satisfies Dynamical Disjointness if the Wedderburn Components of $X_\Phi$ are mutually disjoint, i.e. $(X_\Phi)_i \cap (X_\Phi)_j = \emptyset$ for $i \neq j$.

We will deal with the case in which there may be some overlap in section Dynamical Disjointness. In what follows we take

$$X := X_\Phi, \text{ and } X_i := X_{B_i} \ (i = 1, \ldots, n).$$

Note that we can determine whether the Wedderburn components do overlap using the following proposition.
Proposition 4.15. \(X_i \cap X_j\) is a cocyclic subshift with the cocycle given by \(R_i(\Phi) \otimes R_j(\Phi)\). Denote by \(B\) the algebra of this cocycle. The cocyclic subshift \(X_i \cap X_j\) is empty if and only if \(B = \text{rad}(B)\).

Proof. That \(X_i \cap X_j\) is a cocyclic subshift with cocycle \(R_i(\Phi) \otimes R_j(\Phi)\) follows from Theorem 4.11 and Fact 3.1 in [26].

If \(X_i \cap X_j\) is non-empty, then it has a minimal subset, (i.e. a subset in which all orbits are dense). But all points in this minimal subset are recurrent, hence the recurrent set is non-empty. It follows then by Theorem 4.11 that \(B / \text{rad}(B) \neq 0\). Thus \(B \neq \text{rad}(B)\).

If \(B \neq \text{rad}(B)\), then \(B / \text{rad}(B) \neq 0\). Therefore, \(X_{B / \text{rad}(B)} \neq \emptyset\) by Theorem 4.11. Hence \(X_i \cap X_j \neq \emptyset\) because \(X_{B / \text{rad}(B)} \subset X_i \cap X_j\). (For the last inclusion we considered \(M := B / \text{rad}(B)\) as a module over \(B\) and invoked Proposition 4.6 to get \(X_M \subset X_B = X_{R_i(\Phi) \otimes R_j(\Phi)} = X_i \cap X_j\).)

\(\square\)

The following theorem is the main result of this chapter.

Theorem 4.16. (Connection Theorem) Suppose \(\Phi\) is such that hypothesis (DD) holds and the algebra of \(A\) contains 1. Then, for any \(i, j \in \{1, \ldots, n\}\), we have

\[C_{i,j} \neq \emptyset \iff i \rightarrow j.\]

Moreover, if \(C_{i,j} \neq \emptyset\), \(x \in X_i\), and \(y \in X_j\); then there is \(z \in C_{i,j}\) such that \(\alpha(z) = \alpha(x)\) and \(\omega(z) = \omega(y)\).

The proof of Theorem 4.16 requires some preparation and lemmas. For each \(i\) we want to find a word that occurs in \(X_i\) but not \(X_k\) for \(k \neq i\).

Lemma 4.17. Fix \(i \in \{1, \ldots, n\}\). Suppose \(u \in A^*\) is such that \([u] \cap X_i \neq \emptyset\) but \([u] \cap X_j = \emptyset\) for \(j \neq i\). Then, for any \(w \in A\), we have \(e_i Aw \neq 0 \Rightarrow \Phi_u Aw \neq 0\).
Proof. We first claim that $\Phi_u + N$ is not zero and is in $B_i$. $\Phi_u + N \neq 0$ since otherwise $\Phi_u \in N$ which would imply that the word $u$ could only occur finitely many times in any element of $X_i$, contrary to its construction.

Consider $\Phi_u + N = \nu_1 + \cdots + \nu_n \in B_1 \times \cdots \times B_n$. (Recall that we are using the notation for an inner direct product of algebras.) Suppose $j \neq i$ and $\nu_j \neq 0$. Since $\nu_j = \pi_j(\Phi_u)$ and $\pi_j(\Phi)$ is irreducible, $u$ occurs in $X_j$. (We used that if $\Psi$ is irreducible then, for a word $w$, $\Psi w \neq 0$ if and only if $w$ occurs in $X_\Psi$.) This contradicts the choice of $u$.

Suppose $e_i Aw \neq 0$. We can decompose $\Phi_u A$ into indecomposable submodules, say $\Phi_u A = M_1 \oplus \cdots \oplus M_t$. Note that $M_k$ are submodules of the regular module $A$ and hence ideals of $A$. We arrange these so that $M_1, \ldots, M_s$ are not nilpotent. Note that at least one $M_k$ is not nilpotent because $\Phi_u A/\Phi_u N \neq 0$ and the radical contains all nilpotent right ideals by Proposition 3.1.9 in [13]. Consider $k$ such that $M_k$ is not nilpotent. Then $M_k$ is a principal indecomposable module of $A$ by Lemma 3.26, and so of the form $M_k = f_k A$ for some primitive idempotent $f_k$, $k = 1, \ldots, p$. Thus

$$\Phi_u A = f_1 A \oplus f_2 A \oplus \cdots \oplus f_s A \oplus M_{s+1} \cdots \oplus M_t.$$ 

Likewise

$$\text{rad}(\Phi_u A) = \text{rad}(f_1 A) \oplus \text{rad}(f_2 A) \oplus \cdots \oplus \text{rad}(f_s A) \oplus \text{rad}(M_{s+1}) \oplus \cdots \oplus \text{rad}(M_t)$$

(for finitely many modules $L_i$, $\text{rad}(\bigoplus_i L_i) = \bigoplus_i \text{rad}(L_i)$, see Proposition 3.1.2 in [13]). Now $\text{rad}(u A) = u N$ and $\text{rad}(f_k A) = f_k N$ for each $k$ by Lemma 3.11. Also, $\text{rad}(M_k) = M_k$ for nilpotent $M_k$, $k = s + 1, \ldots, t$. Hence

$$\Phi_u N = \text{rad}(\Phi_u A) = f_1 N \oplus \cdots \oplus f_s N \oplus M_{s+1} \oplus \cdots \oplus M_t$$

and so

$$\Phi_u A/\Phi_u N = f_1 A/f_1 N \oplus \cdots \oplus f_p A/f_p N.$$
(Note that the first isomorphism theorem for modules implies that for $N_i \subset M_i$, $\bigoplus_i M_i/\bigoplus_i N_i \simeq_A \bigoplus_i (M_i/N_i)$.)

We have $\phi_u A/\phi_u N = (\phi_u + N)A/N \subset B_i(A/N) \subset B_i$ by our initial claim. So that $f_i A/f_i N \oplus \cdots \oplus f_p A/f_p N \subset B_i$. But the sum $f_i A/f_i N \oplus \cdots \oplus f_p A/f_p N$ can be completed to a decomposition of $B_i$ into indecomposable $A$-modules, by finding the complement and decomposing it into indecomposable $A$-modules. (Note that for any semisimple module, any submodule has a complement. See Proposition 2.2.1 in [13, p. 32].) At the same time $B_i$ is a direct sum of modules isomorphic to $e_i A/e_i N$, see Equation 4.1. By the Krull-Schmidt Theorem (Theorem 3.2) the decomposition is unique up to isomorphism, so we have $f_k A/f_k N \simeq e_i A/e_i N$, for $k = 1, \ldots, n$. Now $f_k A \subset \phi_u A$, so $f_k A w \neq 0$ implies that $\phi_u A w \neq 0$. To finish, we have to show that $e_i A w \neq \emptyset \Rightarrow f_k A w \neq \emptyset$.

By Lemma 3.4 part (3), taking $\tilde{M} = A w$, we have $e_i A w \simeq_A \text{Hom}(A e_i, \tilde{M})$ and $f_k A w \simeq_A \text{Hom}(A f_k, \tilde{M})$. But $f_k A \simeq_A e_i A$ implies $A f_k A \simeq A e_i$, see Corollary 3.22. And $A f_k \simeq_A A e_i$ implies $A \text{Hom}(A e_i, \tilde{M}) \simeq_A \text{Hom}(A f_k, \tilde{M})$. Finally, we get $e_i A w \neq \emptyset \Rightarrow f_k A w \neq \emptyset$.

**Lemma 4.18.** Fix $j \in \{1, \ldots, n\}$. Suppose $v \in A^*$ is such that $[v] \cap X_j \neq \emptyset$ but $[v] \cap X_i = \emptyset$ for $i \neq j$. Then, for any $w \in A$, we have $w A e_j \neq 0 \Rightarrow w A \phi_v \neq 0$.

**Proof.** The proof is essentially just changing right to left. By the same argument as before we have $\phi_v + N \neq 0$, and $\phi_v + N = \nu_j \in B_j$, and $\phi_v$ occurs in $X_{B_j}$. For the argument below it is important to recall that $B_j$ is two-sided ideal, hence also a left $A$ and $A/N$-module.

Now the left $A$-module $A \phi_v$ can be decomposed into indecomposable submodules,

$$A \phi_v = A g_1 \oplus \cdots \oplus A g_q \oplus \tilde{M}_{q+1} \oplus \cdots \oplus \tilde{M}_s.$$
So $A/N(\Phi_v + N) = A\Phi_v/N\Phi_v \subset (A/N)B_j = B_j$ and for each $k' = 1, \ldots, q$ we have $A_{k'}/N_{k'} \simeq A_{e_j}/N_{e_j}$ since $A_{k'}/N_{k'} \subset B_j$.

By Lemma 3.4 $wAe_j \neq 0$ if and only if $wAg_{k'} \neq 0$. So that $wAe_j \neq 0$ implies $wAg_{k'} \neq 0$ and $wA\Phi_v \supset wAg_{k'}$ so $wA\Phi_v \neq 0$.

The main theorem now follows from the lemmas above.

Proof of Theorem 4.16. First suppose $C_{i,j} \neq \emptyset$ for some $i \neq j$. Take $x \in C_{i,j}$. Because $\alpha(x) \subset X_i$ and $\omega(x) \subset X_j$ are non-empty (by compactness of $X_i, X_j$) there are words $u, v \in A^+$ such that 

$$\alpha(x) \cap [u] \neq \emptyset \text{ and } \omega(x) \cap [v] \neq \emptyset. \quad (4.2)$$

Because of hypothesis (DD), taking $u, v$ long enough ensures that $[u] \cap [v] = \emptyset$ and also that $[u] \cap X_k = \emptyset$ for all $k \neq i$ and $[v] \cap X_k = \emptyset$ for all $k \neq j$.

From (4.2), $u$ must occur in $x_{(-\infty, 0]}$ infinitely many times and $v$ must occur in $x_{[0, \infty)}$ infinitely many times. As a result $(\Phi_u A)^t(A\Phi_v)^t \neq 0$ for all $t \in \mathbb{N}$. Now, fix $t$ large enough so that $N^t = 0$. (We used here that the radical of $A, N$, is a nilpotent ideal.) As in the proof of Lemmas 4.17 and 4.18 we can write

$$\Phi_u A = f_1 A \oplus \ldots \oplus f_p A \oplus M_{p+1} \oplus \ldots \oplus M_s$$

and

$$A\Phi_v = Ag_1 \oplus \ldots \oplus Ag_q \oplus N_{q+1} \oplus \ldots \oplus N_{s'}$$

where $M_k, N_k$ are nilpotent and $f_k, g_k$ are primitive idempotents. Multiplying out the power $(\Phi_u A)^t$ we see that the terms containing only the nilpotent factors vanish, as they are of the form $M_{k_1} \cdots M_{k_t} \subset N^t = 0$. The situation is analogous for $(A\Phi_v)^t$.

Therefore $(\Phi_u A)^t(A\Phi_v)^t$, multiplied out, is a sum of terms each of which is a product containing $f_k A$ and $Ag_{k'}$ for some $k, k'$. Since $(\Phi_u A)^t(A\Phi_v)^t \neq 0$, there is a pair of such $k, k'$ for which $f_k Ag_{k'} \neq 0$. 

\[\square\]
Finally, recall (from the proof of Lemmas 4.17, 4.18) that \( f_kA \simeq_{A} e_iA \) and \( Ae_jA \simeq_{A} A \) and so \( f_kAg \simeq_{e_iA} \) (by Lemma 3.4). Therefore \( f_kAg \neq 0 \) implies \( e_iAe_j \neq 0 \). This ends the proof of \( C_{i,j} \neq \emptyset \Rightarrow i \rightarrow j \).

Suppose now \( i \rightarrow j \), (i.e. \( e_iAe_j \neq 0 \)), \( x = (x_k)_{-\infty}^{\infty} \in X_i \) and \( y = (y_k)_{-\infty}^{\infty} \in X_j \). For \( n \in \mathbb{N} \), set \( u_n := x_{[-n, -1]} \) and \( v_n := y_{[1, n]} \). Clearly, \( [u_n] \cap X_i \neq \emptyset \) and \( [v_n] \cap X_j \neq \emptyset \). Taking \( n_0 \in \mathbb{N} \) large enough, we also have \( [u_n] \cap X_k = \emptyset \) for \( k \neq i \) and \( [v_n] \cap X_k = \emptyset \) for \( k \neq j \) as long as we restrict to \( n \geq n_0 \). (This used (DD) hypothesis.)

By Lemma 4.17, \( e_iAe_j \neq 0 \) implies \( \Phi_{u_n}Ae_j \neq 0 \) (for \( n \geq n_0 \)). By Lemma 4.18, \( \Phi_{u_n}Ae_j \neq 0 \) implies \( \Phi_{u_n}A \Phi_{v_n} \neq 0 \) (for \( n \geq n_0 \)). Now, fix a finite set of words \( w_1, \ldots, w_d \in A^+ \) such that \( E_0 := \{ \Phi_{w_i} | i = 1, \ldots, d \} \) linearly spans \( A \). Also, set \( E_k := \{ \Phi_{x_k} \} \) for \( k = -1, -2, \ldots \) and \( E_k := \{ \Phi_{y_k} \} \) for \( k = 1, 2, \ldots \). By invoking (ii) of Lemma 4.3, whose hypothesis holds due to \( \Phi_{u_n}A \Phi_{v_n} \neq 0 \), we see that there is \( i \in \{ 1, \ldots, d \} \) such that

\[
\Phi_{x_{-n}} \Phi_{x_{-n+1}} \ldots \Phi_{x_{-1}} \Phi_{w_i} \Phi_{y_1} \ldots \Phi_{y_n} \neq 0
\]

for all \( n \in \mathbb{N} \).

Hence, the infinite word \( z := x_{(-\infty, -1]}w_iy_{[1, \infty)} \) belongs to \( X \). By construction, \( z \in C_{i,j} \) with \( \alpha(z) = \alpha(x) \) and \( \omega(z) = \omega(y) \).

\( \square \)

**Corollary 4.19.** Suppose there is a connecting orbit between disjoint irreducible components \( X_i \) and \( X_j \). Then there exists \( x \in X \) such that \( \alpha(x) = X_i \) and \( \omega(x) = X_j \).

**The Connecting Graph**

We now analyze the graph of the relation \( \rightarrow \), which we call the connecting diagram.
Definition 4.20. For a finite dimensional algebra $A$, The Connecting Diagram of $A$ is the directed graph such that:

1. Vertices are in one-to-one correspondence with the blocks of $A/N$.
2. There is a directed edge from vertex $i$ to $j$ if and only if $i \to j$.

For a cocycle $\Phi$, the connecting diagram of $\Phi$ is the connecting diagram of $A$, the algebra of $\Phi$. The connecting diagram of the cocyclic subshift $X_\Phi$ is the connecting diagram of $\Phi$.

Proposition 4.21. Suppose $X$ and $Y$ are conjugate cocyclic subshifts satisfying (DD) and $G$ and $H$ are the respective connecting diagrams. Then there is a renumbering of the vertices of $H$ such that $G = H$.

Proof. Let $F$ be a conjugacy between $X$ and $Y$. We can restrict domain and images of $F$ to get a conjugacy between $X_+$ and $Y_+$. To fix notation take $X_+ = \bigcup_i X_i$, where $X_i$ are the Wedderburn components of $X_+$ and likewise $Y_+ = \bigcup_j Y_j$. $F(X_i)$ must be a transitive subset of $Y$. Suppose $x$ has a dense orbit in $X_i$. Then $F(x)$ has a dense orbit in $F(X_i)$. If $F(x) \in Y_j$, then $F(X_i) \subset \text{cl}(\mathcal{O}(F(x))) \subset Y_j$ (by invariance and closure of $Y_j$).

An analogous computation for the conjugacy $F^{-1}$ shows that for each $Y_j$ there is a unique $X_i$ such that $F^{-1}(Y_j) \subset X_i$. But then we must actually have $F(X_i) = Y_j$. Thus by appropriate indexing we get $F(X_i) = Y_i$ for all $i$. In particular, each graph has the same number of vertices.

Now suppose there is $x \in X$ such that $x \in C_{i,j}^X$, then $F(x) \in C_{i,j}^Y$ thus the edges also coincide.

Two algebras $A_1$ and $A_2$ are said to be isotypic if their basic algebras are isomorphic.
**Proposition 4.22.** Suppose $A_1$ and $A_2$ are isotypic algebras. Then the connecting diagrams for $A$ and $B$ are the same (up to renumbering of the vertices).

**Proof.** First we show that the connecting graph depends only on the basic algebra of the algebra $A$. To see why, recall that for the principal modules, $e_1A, \ldots, e_nA$, of $A$ there is a corresponding decomposition of the identity in $A^b$, i.e. $1^b = f_1 + \ldots + f_n$, (see the discussion preceding Lemma 3.3). In this notation we rephrase Lemma 3.3 (using Lemma 3.4 (2)) to get,

$$f_iBf_j \simeq \text{Hom}_B(f_jB, f_iB) \simeq \text{Hom}_A(e_jA, e_iA) \simeq e_iAe_j.$$

Thus the relation $i \rightarrow j$ is the same using $B$ or $A$, so calculating the connecting diagram using $B$ gives the same result.

In particular, if $A_1$ and $A_2$ are isotypic then their respective connecting diagrams must be the same. \qed

Our definition of the connecting diagram resembles the definition for Gabriel’s quiver, which is also a graph that represents the structure of an algebra. Because of its importance to the general theory of finite dimensional algebras, we examine Gabriel’s quiver. See [3, p.41] for a brief history of the use of quivers of algebras.

**Definition 4.23.** Gabriel’s Quiver of the basic algebra $A$ is the directed graph such that:

1. The vertices of the graph correspond to the number of isomorphism classes of principal modules.
2. There is a directed edge from $i$ to $j$ if and only if $e_i(N/N^2)e_j \neq 0$.

Note that this definition is not standard, as the usual way to do this is by taking the number of edges from $i$ to $j$ to be $\dim(e_i(N/N^2)e_j)$. Our connecting diagram does not make use of multiplicities so we have modified the definition of Gabriel’s
quiver. The following example shows that Gabriel’s quiver does not represent all the
topological features that the connecting graph does.

Example: Take the cocycle $\Phi = (\Phi_0, \Phi_1, \Phi_2, \Phi_3)$ with

$$
\Phi_0 = \begin{bmatrix}
1 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix},
\Phi_1 = \begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0
\end{bmatrix},
\Phi_2 = \begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 0
\end{bmatrix},
\Phi_3 = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 1
\end{bmatrix}.
$$

The algebra generated by these matrices is the algebra of all upper triangular matrices.

With the standard idempotents,

$$
e_1 = \begin{bmatrix}
1 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0
\end{bmatrix},
e_2 = \begin{bmatrix}
0 & 0 & 0 \\
0 & 1 & 0 \\
0 & 0 & 0
\end{bmatrix},
e_3 = \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 1
\end{bmatrix}.
$$

Since $\dim(e_1A) \neq \dim(e_2A) \neq \dim(e_3A)$, the Wedderburn decomposition has three
components with $e_1Ae_2 \neq 0$, $e_2Ae_3 \neq 0$, $e_1Ae_3 \neq 0$, and all other products $e_iAe_j = 0$
for $i \neq j$. In particular, there is a connecting orbit from $X_1$ to $X_3$. The connecting
diagram of $A$ is given by Figure 4.1.

![Figure 4.1: Connecting Diagram](image)

Now we observe that $e_1(N/N^2)e_3 = 0$. Thus there is no edge from 1 to 3 in the
Gabriel’s quiver of $A$, see Figure 4.2.

We will show in the next section that connecting diagrams are not transitive, i.e.
$i \to j$ and $j \to k$ does not imply $i \to k$, see page 75. Thus the connecting diagram of
$A$ is not just the transitive extension of Gabriel’s Quiver.
We first give an example to show that transitivity of connections does not hold in general, i.e. \( i \to j \) and \( j \to k \) does not necessarily imply \( i \to k \). We comment that transitivity holds for topological Markov chains, but fails for sofic systems as the following example is sofic.

**Example:** Let \( I \) be the \( 2 \times 2 \) identity and \( E := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \). Then we define the cocycle \( \Phi \) by the following \( 6 \times 6 \) block matrices:

\[
\Phi_0 := \begin{bmatrix} I & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \Phi_1 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \Phi_2 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & I \\ 0 & 0 & 0 \end{bmatrix}, \quad \Phi_3 := \begin{bmatrix} 0 & E & 0 \\ 0 & 0 & E \\ 0 & 0 & 0 \end{bmatrix}.
\]

In a latter section we will address how to use a computer to aid in the computations involved, but in this case the connecting diagram is intuitively clear. Take \( X_1 = \{0^\infty\}, X_2 = \{1^\infty\}, X_3 = \{2^\infty\} \) with \( 1 \to 2 \) and \( 2 \to 3 \), but \( 1 \not\to 3 \) since \( E^2 = 0 \). Thus we have the connecting diagram in Figure 4.3.

![Figure 4.3: Non-transitive Connecting Diagram](image)

We now give an account of a class of examples for which connecting diagrams are always transitive. Suppose that \( 1 \in A \) and \( 1 = e_1 + e_2 + \cdots + e_p \) is a decomposition
of 1 into primitive idempotents. A representation of an algebra $A$ is an algebra homomorphism $T : A \to \text{End}(W)$ for some vector space $W$. The degree of the representation $T$ is $\dim(W)$ as a vector space. A matrix representation of an algebra $A$ is an algebra homomorphism $T : A \to M_k(\mathbb{C})$. If $T$ is a monomorphism into $\text{End}(W)$ (or $M_k(\mathbb{C})$) then we say that $T$ is faithful. We say that $A$ is minimal if there exist a faithful representation of $A$ of degree $p$ (or a faithful matrix representation into $M_p(\mathbb{C})$) where $p$ is the number of primitive idempotents in a decomposition of the identity. Note that $\text{End}(W)$ and $M_k(\mathbb{C})$ are equivalent via an appropriate isomorphism. We write $e_{ii}$ for the element of $M_p(\mathbb{C})$ which has 1 in the $ii$ spot and 0 elsewhere.

**Proposition 4.24.** If $A$ is a subalgebra of $M_p(\mathbb{C})$ that contains $e_{i,i}$ for all $i = 1, 2, \ldots, n$ then $A$ is a minimal algebra.

**Proof.** This is true since $1 = \sum_i e_{i,i}$ is a decomposition of $1 \in A$, and the inclusion map $\iota : A \to M_p(\mathbb{C})$ is faithful.

For the remainder of this section let $A$ be an algebra of minimal degree $p$ and let $T : A \to M_p(\mathbb{C})$ be a faithful matrix representation of $A$. Then $\mathbb{C}^p = (\text{Id})\mathbb{C}^p = (T(e_1) + T(e_2) + \ldots + T(e_p))\mathbb{C}^p = T(e_1)\mathbb{C}^p \oplus \ldots \oplus T(e_p)\mathbb{C}^p$ with $\dim(T(e_i)\mathbb{C}^p) \geq 1$, so $\dim(T(e_i)\mathbb{C}^p) = 1$ for each $i = 1, 2, \ldots, p$. $T(e_i)T(e_i) = T(e_i)$, so $T(e_i)$ is an idempotent in $M_p(\mathbb{C})$. Likewise for $i \neq j$, $T(e_i)T(e_j) = T(e_ie_j) = 0$. It follows that $\text{Id} = T(e_1) + \ldots + T(e_p)$ is decomposition of the identity matrix into orthogonal, minimal idempotents. We can then choose a basis of $\mathbb{C}^p$ such that $T(e_i)$ becomes a matrix with a single non-zero entry, which must be 1. We use the same notation for the matrix representation with $T(e_i)$ as described.
We now show that for those subshifts which have a cocycle generating a minimal algebra the relation is always transitive. In fact, the relation $\rightarrow$ is actually an order on the set $\{1, 2, \ldots, p\}$, where $\{e_1A, \ldots, e_pA\}$ are the principal modules. (We also refer to the graph as being transitive if $\rightarrow$ is a transitive relation.)

**Theorem 4.25.** If $A$ is minimal then its connecting diagram is transitive and has no loops (i.e. a path that starts and ends at the same vertex) except the loops $i \rightarrow i$.

We first need the following lemma to ensure that in working only with the basic algebra of the algebra $A$ we still have a minimal algebra. The basic algebra of $A$ can defined as

$$A^b = e_A Ae_A,$$

where $e_A = e_1 + e_2 + \ldots + e_n$ and $\{e_1A, \ldots, e_nA\}$ is a complete set of principal modules. For the equivalence of this definition with the one on page 40 see [3, p. 33-34]. Note that the proof of the lemma and the theorem amount to the solution of homework problems in [13, p. 67].

**Lemma 4.26.** If $A$ is minimal then $A^b$ is minimal.

**Proof.** Suppose that $A$ is minimal algebra of degree $p$, that is $1 = e_1 + e_2 + \ldots + e_p$ is a decomposition of the identity into primitive idempotents and $T : A \rightarrow M_p(\mathbb{C})$, is a monomorphism. As usual suppose that $\{e_1A, \ldots, e_nA\}$ is a complete set of principal modules of $A$. $A^b = e_A Ae_A$ has identity $e_A$ with $e_A = e_1 + \ldots + e_n$.

Consider $U := (T(e_1) + T(e_2) + \ldots + T(e_m))\mathbb{C}^p \subset \mathbb{C}^p$. Then $\dim(U) = m$ since $\dim(T(e_i)\mathbb{C}^p) = 1$ and $U = T(e_1)\mathbb{C}^p \oplus \ldots \oplus T(e_m)\mathbb{C}^p$. But then $T|_{A^b}$ is a monomorphism to $\text{End}(U)$, which (via composition with an isomorphism) gives a faithful representation in $M_m(\mathbb{C})$. Therefore, $A^b$ is minimal of degree $m$. 

$\square$
We now continue with the proof the theorem.

Proof of Theorem 4.25. Since the connecting graph only depends on the basic algebra (see Proposition 4.22) we assume that $A$ is basic. Let $A$ be minimal and basic, and suppose $e_i Ae_j \neq 0$ and $e_j Ae_k \neq 0$ for $i \neq j$ and $j \neq k$ with $i, j, k = 1, \ldots, n$. We show $e_i Ae_k \neq 0$.

$T$ is faithful, so we have $T(e_i)T(a)T(e_j) \neq 0$ for some $a \in A$, so $T(e_i)T(a)T(e_j)$ has a non-zero entry in the $i,j$-th spot and is zero elsewhere. Likewise, for some $b \in A$, $T(e_j)T(b)T(e_k) \neq 0$ and $T(e_j)T(b)T(e_k)$ has a single non-zero entry in the $j,k$-th spot. Therefore,

$$(T(e_i)T(a)T(e_j))T(e_j)T(b)T(e_k) \neq 0.$$ 

By using the fact that $T$ is a homomorphism, we get $e_i ae_j be_k \neq 0$. So $e_i Ae_k \neq 0$, thus transitivity is proven.

Now that we know that the connection graph is transitive, to show that it has no loops it suffices to show that it is has no loops of length two.

Now suppose that $e_i Ae_j \neq 0$ and $e_j Ae_i \neq 0$ and that $A$ is basic. (Recall $A$ is basic iff $A = P_1 \oplus \ldots \oplus P_p$ with $P_i \not\cong P_j$ for $i \neq j$ and $P_i$ principal for each $i$.) Let $0 \neq f_{ij} \in \text{Hom}_A(e_i A, e_j A)$ (which is canonically identified with $e_j Ae_i$). Then $f_{ij}$ is identified with $e_j be_i$ for some $b \in A$. Thus if $e_i a \neq 0$ we have $f_{ij}(e_i a) = e_j be_i e_i a$. Then $T(e_j be_i e_i a) = T(e_j be_i)T(e_i a) \neq 0$, thus $f_{ij}$ is a monomorphism. We do the same for any non-zero $f_{ji} \in \text{Hom}_A(e_j A, e_i A)$ to get a monomorphism. Since there are monomorphisms each way we must have $\dim(e_i A) = \dim(e_j A)$. But then the monomorphism $f_{ij}$ must be an isomorphism. Therefore $e_i A \cong e_j A$, but $A$ being basic implies $i = j$. \qed
We now address the case in which the algebra \( A \) generated by a cocycle \( \Phi \in (\text{End}(V))^m \) may not be unital and explain how to construct the connecting diagram for \( X_\Phi \) in that case. For an algebra \( A \) we define the algebra with identity adjoined by

\[
A^1 := \{ a \oplus \alpha 1 \mid \alpha \in \mathbb{C}, a \in A \}
\]

where \( 1 \) is a formal symbol, addition is coordinate-wise, and the multiplication is defined by

\[
(a + \alpha 1)(b + \beta 1) = ab + \alpha b + \beta a + \alpha \beta 1 \quad a, b \in A, \alpha, \beta \in \mathbb{C}.
\]

The element \( 1 \) is the identity in \( A^1 \) and \( A \subset A^1 \). (This is a standard construction, see [13, p. 3] for discussion.)

**Proposition 4.27.** (1) Any \( A \)-module \( M \) is an \( A^1 \)-module with \( m(a + \alpha 1) := ma + ma \alpha \) \((a \in A, \alpha \in \mathbb{C})\).

(2) Any \( A^1 \)-module \( M \) is an \( A \)-module.

(3) For any \( A \)-modules \( M, N \), \( \text{Hom}_A(M, N) \simeq \text{Hom}_{A^1}(M, N) \)

The proof of the proposition is left as an exercise.

For this section we use a little more of the theory of languages of subshifts. For reference see Chapter Languages and Cocyclic Subshifts, in particular Proposition 5.1 in this thesis, as well as the references [27] and [25].

Recall from Proposition 4.4, that for an algebra \( A \) of a cocycle \( \Phi \), \( 1 \in A \) implies that \( \Phi_w \neq 0 \) if and only if \( w \) occurs in \( X_\Phi \). In general, it may be that \( \Phi_w \neq 0 \) but there is no \( x \in X_\Phi \) such that \( w \subseteq x \). In the general case we have the following condition: \( w \in \mathcal{A}^* \) does not occur in \( X_\Phi \) if and only if, for any words \( u, v \in \mathcal{A}^* \), there is an extension \( w' \) of the word \( uuv \) such that \( \Phi_{w'} = 0 \).
Proposition 4.28. Treating $A$ and $A^1$ as $A$-modules or $A^1$-modules, we have $X_A = X_\Phi = X_A^1$.

Proof. Suppose $w \notin \mathcal{L}(X_\Phi)$, then for any extension $uwv$ of $w$ there is an extension $w'$ of it such that $\Phi_{w'} = 0$. Thus $A\Phi_{w'} = 0$, so $w \notin \mathcal{L}(X_A)$. Since $w$ cannot be extended in both directions we have $w \notin \mathcal{L}(X_A)$. Thus $X_A \subset X_\Phi$.

Suppose $w \notin \mathcal{L}(X_A)$, then for any extension $uwv$ of $w$ there is a further extension $w'$ such that $A\Phi_{w'} = 0$. Since $A$ is the algebra of $\Phi$, for any word $w_0$, we have $\Phi_{w_0}\Phi_{w'} = 0$. So $w \notin \mathcal{L}(X_\Phi)$.

The proof that $X_\Phi = X_A^1$ follows in the completely analogous way. $\Phi_{uwv} \neq 0$ implies $A^1\Phi_{uwv} = 0$. Also, if $A^1\Phi_{uwv} = 0$ we have $1\Phi_{uwv} = \Phi_{uwv} = 0.$

Decompose $A$ into indecomposable $A^1$-modules $A = A_1 \oplus A_2 \oplus \cdots \oplus A_t$, where the first $s$ are non-nilpotent. Consider $k$ such that $A_k$ is not nilpotent. $A_k$ is an indecomposable ideal of $A^1$ so there is an idempotent $e_k \in A_k$ such that $e_kA_k = A_k$ by Lemma 3.25 and Lemma 3.26. But then $e_k$ must be primitive by indecomposability of $A_k$. Now let

$$f := 1 - \sum_{k=1}^{s} e_k. \tag{4.3}$$

Note that $f$ is an idempotent and $e_kf = fe_k = 0$. We decompose $f$ into primitive idempotents $f_1, f_2, \ldots, f_p$. Then we have the decomposition of the identity

$$1 = f_1 + \ldots + f_p + e_1 + \ldots + e_s. \tag{4.4}$$

There is a corresponding decomposition of $A^1$ into indecomposable submodules from which we can generate a connecting diagram, see Definition 4.20.

Proposition 4.29. For any $j$ and $a \in \mathcal{A}$, we have $f_jA^1\Phi_a \subset f_j\text{rad}(A^1)$. Moreover, $fA^1\Phi_a \subset f\text{rad}(A^1)$. 
Proof. For $a' \in A$ we have $a'\Phi_a \in A$, so it remains to see $f_jA \subset f_j\text{rad}(A^1)$. By construction of $f_j$, $f_jA \subset f_j(A_{s+1} \oplus \ldots \oplus A_t)$ where $A_{s+1} \oplus \ldots \oplus A_t$ is the sum of nilpotent ideals in $A^1$. Thus, $f_jA \subset \text{rad}(A^1)$, and $f_jA = f_jf_jA \subset f_j\text{rad}(A^1)$. The moreover part follows by taking the direct sum over $f_j$, i.e. $\bigoplus f_jA \subset \bigoplus f_j\text{rad}(A^1)$. 

\[ \square \]

**Corollary 4.30.** For any $j$ and $a \in A$, we have $(f_jA^1/f_j\text{rad}(A^1))(\Phi_a + \text{rad}(A^1)) = 0$.

**Proof.** First the multiplication $(f_jA^1/f_j\text{rad}(A^1))(\Phi_a + \text{rad}(A^1))$ makes sense by Corollary 3.12 and it is 0 if and only for any $a' \in A^1$ and $a \in A$ we have $f_ja'\Phi_a \in \text{rad}(A^1)$ which is true by the proposition. 

\[ \square \]

We want to prove a version of the Connection Theorem (Theorem 4.16) for cocycles which have non-unital algebras. To do this we first expand the cocycle $\Phi$ to a cocycle $\Psi$ with alphabet $A \cup \{1'\}$ where we assume the extra letter $1'$ does not belong to $A$ and define 

\[
\Psi_a := \Phi_a \text{ for } a \in A, \quad \Psi_{1'} := f = 1 - \sum_{k=1}^{s} e_k.
\]

The algebra of $\Psi$ is $A^1$. (We assume for the remainder of this section that $\Phi$ and $\Psi$ both satisfy (DD).) Now we can apply Theorem 4.11 to $X_\Psi$ to get the Wedderburn decomposition associated to the decomposition of the identity (4.3)

\[
(X_\Psi)_+ = \bigcup_{j=1}^{q} Y_j.
\]

We can do the same for $X_\Phi$ to get

\[
(X_\Phi)_+ = \bigcup_{i=1}^{r} X_i.
\]
(Note that the Spectral Decomposition does not rely on 1 being in the algebra.) For each \( i \), \( X_i \subset \bigcup_{j=1}^r Y_j \), so that \( X_i \subset Y_j \) for some \( j \). (This uses (DD) for \( \Psi \) and \( \Phi \) and transitivity of \( X_i \).) Thus after relabeling we have \( X_i \subset Y_i \) for \( i = 1, \ldots, r \).

**Proposition 4.31.** \( X_i = Y_i \) for \( i = 1, \ldots, r \).

**Proof.** We have seen that \( X_i \subset Y_i \). Suppose by way of contradiction that \( x \in Y_i \setminus X_i \). Thus the letter 1' occurs in \( x \). \( Y_i \) is transitive so there exists \( y \in Y_i \) with dense orbit in \( X_i \). But then \( y \) has infinitely many occurrences of 1' as well as infinitely many occurrences of letters in \( \mathcal{A} \). So there are \( w_i \in \mathcal{A}^+ \) (\( i \in \mathbb{Z} \)) such that \( \ldots f \Phi_{w_{-1}} f \Phi_{w_0} f \Phi_{w_1} \ldots \neq 0 \). This contradicts the moreover part of Proposition 4.29, i.e. \( fA\Phi_a \subset fA^1\Phi_a\text{rad}(A^1) \).

**Corollary 4.32.** Let \( \{e_1A^1, \ldots, e_rA^1\} \) be a subset of \( \{e_1A^1, \ldots, e_sA^1\} \) representing each isomorphism class of \( e_iA^1 \). Then \( (X_{\Phi})_+ = \bigcup_{i=1}^r X_{e_iA^1/e_i\text{rad}(A^1)} \).

**Proof.** \( X_i = Y_i = X_{e_iA^1/e_i\text{rad}(A^1)} \) for \( i = 1, \ldots, r \) by Theorem 4.11 and Equation 4.1.

Recall that

\[
C_{i,j} = \{ x \in X_{\Phi} | \alpha(x) \subset X_i \text{ and } \omega(x) \subset X_j \}.
\]

**Theorem 4.33.** *(Connection Theorem for Non-Unital Algebras)* Let \( A \) be the (non-unital) algebra of \( \Phi \). \( C_{i,j} \neq \emptyset \) iff \( e_iAe_j \neq 0 \).

**Proof.** We first observe that for \( e_i, e_j \) idempotents in \( A \) as above, \( e_iAe_j \simeq e_iA^1e_j \) by Proposition 4.27. In fact, since \( e_iAe_j \subset e_iA^1e_j \) and \( \dim(e_iAe_j) = \dim(e_iA^1e_j) \), we have \( e_iAe_j = e_iA^1e_j \).

Suppose \( C_{i,j} \neq \emptyset \), that is, \( X_{\Phi} \) contains a connecting orbit between \( X_i \) and \( X_j \). Since this connecting orbit is also in \( X_{\Phi} \) we have \( e_iA^1e_j \neq 0 \) (by Theorem 4.16). By our preliminary observation, \( e_iAe_j = e_iA^1e_j \), so \( e_iAe_j \neq 0 \).
Suppose $e_i A e_j \neq 0$ then $e_i A^1 e_j \neq 0$ (since $A \subset A^1$). Theorem 4.16 applied to $X_\Phi$ yields $x \in X_\Phi$ whose orbit connects $X_i$ to $X_j$. In particular, we can take $x$ with $\alpha(x) = X_i$ and $\omega(x) = X_j$, by Theorem 4.16. If $x \in X_\Phi$ then we are done. Otherwise, since the orbit of $x$ connects irreducible subshifts of $X_\Phi$, it follows that there is a sequence of words $w_l \in A^*$ ($l \in \mathbb{Z}$) such that $\Phi_{w_l} \in A$ and $\ldots \Phi_{w_{-1}} f \Phi_{w_1} \ldots \neq 0$. But this implies the long product $\ldots \Phi_{w_{-1}} 1 \Phi_{w_1} \ldots \neq 0$ since the decomposition $1 = f + \sum_{k=1}^{s} f$ decomposes $A^1$ into a direct sum. Thus $y := \ldots w_{-1} w_1 \ldots$ is an element of $X_\Phi$ whose orbit connects $X_i$ to $X_j$.

We end this section with an example that illustrates details of the proof of the Connection Theorem for Non-Unital Algebras.

Example: Consider the sofic system presented by the graph in Figure 4.4.

![Figure 4.4: Sofic System with Corresponding Non-Unital Algebra](image)

This subshift is cocyclic with a cocycle given by

$$
\Phi_1 := \begin{bmatrix}
1 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 0 \\
\end{bmatrix}, \quad
\Phi_2 := \begin{bmatrix}
0 & 1 & 0 \\
0 & 0 & 1 \\
0 & 0 & 0 \\
\end{bmatrix}, \quad
\Phi_3 := \begin{bmatrix}
0 & 0 & 0 \\
0 & 0 & 0 \\
0 & 0 & 1 \\
\end{bmatrix}.
$$

The algebra of $\Phi$ is given by

$$
A = \left\{ \begin{bmatrix}
a & b & c \\
0 & 0 & d \\
0 & 0 & e \\
\end{bmatrix} \right\}.
$$
That $A$ does not contain an identity element is left as an exercise.

$$A^1 := \mathbb{C} \oplus A \simeq \text{Lin} \left( \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right) \oplus A = \left\{ \begin{bmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{bmatrix} \right\}.$$ 

Taking

$$e_1 := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, e_2 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

we have by definition

$$\Psi_1' = f := \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$ 

$X_\Phi$ is a sofic system with the graph in Figure 4.5, with $\Psi_1 = \Phi_1$, $\Psi_2 = \Phi_2$, and $\Psi_3 = \Phi_3$.

![Figure 4.5: Graph for $X_\Phi$](image)

The connecting diagram for $X_\Phi$ is the generated by giving the connecting diagram for $X_\Phi$ and erasing the vertex corresponding to $\{1'^\infty\}$, as well as edges going into or out of that vertex.

**SFT and Edge Shifts**

We now consider the case of the edge shift, that is the collection of bi-infinite walks over a finite graph $G$ whose edges are labeled by the letters of the alphabet $A$
so that each label occurs exactly once. We denote this shift by $X_G$. Let us associate to $G$ the vector space $C^D$ where $D$ is the number of vertices in the graph and set, for $w \in A$, $\Phi_w = (a_{I,J})$ where $a_{I,J} = 1$ if the edge labeled $w$ connects vertices $I$ and $J$ and $a_{I,J} = 0$ otherwise. Note that any subshift of finite type can be recoded to yield an edge shift so that considering only edge shifts is not really a restriction, see [7, p.57].

**Proposition 4.34.** Given a labeled graph $G$, if $\Phi$ is a cocycle associated to $G$ as above, then $X_\Phi = X_G$.

**Proof.** For $w = w_1 \ldots w_n \in A^+$ we have $\Phi_w = \Phi_{w_1} \cdots \Phi_{w_n}$ is exactly the matrix with all zero entries except when there is a path in $G$ with label $w$ from $I$ to $J$ in which case $\Phi_w$ has a single entry 1 in the $I,J$ spot. But then for any $w$ we have $\Phi_w \neq 0$ if and only if there is a path in the graph with label $w$ for the for the corresponding $I,J$. Hence, $X_\Phi = X_G$.

The communicating class diagram for an edge shift is the graph of the following equivalence relation on $A^+$:

For $w,v \in A^+$ we write $w \sim v$ if there are some paths $w_1$ and $w_2$ such that $ww_1v$ and $vw_2w$ are allowed words.

We call the equivalence classes of this relation the communicating classes, see [27].

For ease of presentation we assume the graph $G$ is essential, that is every vertex has an edge coming in and an edge going out. To each communicating class, $l$, there is an irreducible subshift of $X_G$ which we get by considering subgraph of the original graph that has only the edges of that communicating class. Call the irreducible subshift $\hat{X}_l$. 
Proposition 4.35. Let \( G \) be a graph as described above and \( \Phi \) the corresponding cocycle then the following hold.

(1) The subshifts given by the communicating class method are mutually disjoint, non-empty, and for any words \( u \) and \( v \) that occur, there exists \( w \in A^* \) such that \( uvw \) occurs.

(2) If \( \Phi \) satisfies (DD) then for any block \( B_k \) of \( A \), there is a \( \hat{X}_l \) such that \( X_{B_k} = \hat{X}_l \).

Proof. (1) That the subshifts are mutually disjoint, non-empty is clear. Now for any words \( u, v \) that occur and which are in the same communicating class, there exists \( w \) such that \( uvw \) occurs.

(2) We first observe that the components yielded by the communicating classes are transitive. (Since for any words \( u \) and \( v \) which occur in the same component, there is \( w \) such that \( uvw \) occurs.) Also, \( X_+ = \bigcup_l \hat{X}_l \). Now \( X_+ \) also coincides with \( \bigcup_k X_{B_k} \) and under (DD) hypothesis \( X_{B_k} \) are mutually disjoint. So we are done by the proof of Proposition 4.21, since the proof only used the fact that we had two partitions of \( X_+ \) into transitive subsets.

\[ \square \]

Composition Series and Connecting Diagrams

If \( \Phi \in (\text{End}(V))^m \) is a cocycle, we can also use a composition series of \( V \) as an \( A \)-module to determine irreducible subshifts.

Let \( 0 = V_r \subset V_{r-1} \subset \ldots \subset V_0 = V \) be a composition series for \( V \) as an \( A \)-module. One can find in each \( V_i \) the complement \( W_i \) of \( V_{i+1} \subset V_i \) so that \( V_i = W_i \oplus V_{i+1} \). Thus \( V = W_r \oplus W_{r-1} \oplus \ldots \oplus W_1 \) and \( V_i = W_i \oplus W_{i+1} \oplus \ldots \oplus W_r \). Then we can write \( A \) as an algebra of triangular block matrices \( a^{(ij)} \) mapping \( W_i \) to \( W_j \). (Note that \( a^{(ij)} = 0 \) for
i > j.) If \( a^{(ij)} \neq 0 \) we say \( i \sim j \). The map \( \tilde{R}_j : a \to a^{(jj)} \) is a homomorphism which is either zero or onto \( \text{End}(W_j) \). (See [26, p. 269-270] for a more complete discussion.) Thus by Theorem 4.11, one can find the irreducible components of \( X \) by looking at the image of the cocycle \( \Phi \) under the map \( \tilde{R} := \prod_{j \in \{j | \tilde{R}_j \neq 0\}} \tilde{R}_j \).

**Example:** Taking \( \Phi_1 := \begin{bmatrix} 1 & 0 \\ -1 & 0 \end{bmatrix} \) and \( \Phi_2 := \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix} \), we see that \( \Phi_1 \Phi_2 = \Phi_2 \Phi_1 = 0 \) and \( X_\Phi = \{1^\infty, 0^\infty\} \). Hence there are no connecting orbits between the irreducible components.

We now show that \( i \sim j \) is not equivalent to \( i \to j \) and thus does not guarantee a topological connection from \( X_i \) to \( X_j \). To see this we look at the algebra \( A \) of \( \Phi \) given by matrices of the form \( \begin{bmatrix} a & 0 \\ b-a & b \end{bmatrix} \), where \( a \) and \( b \) are arbitrary elements of \( \mathbb{C} \).

We have the obvious composition series \( 0 \subset V_1 := \{[v_1, 0] | v_1 \in \mathbb{C}\} \subset V := \mathbb{C}^2 \), which gives \( 2 \sim 1 \). But we have already seen that there are no topological connections.

---

**Dynamical Disjointness**

Given a cocyclic subshift \( X \) it may be the case that the Wedderburn components are not disjoint. In this case we consider an extension of \( X \) which will have the “same” connections but have disjoint components. For this purpose we apply the Wedderburn-Malcev Theorem (Theorem 3.9) to get a complement \( A_0 \) of the radical. That is \( A_0 \subset A \) is a subalgebra with \( A_0 \cong A/N = B_1 \times \cdots \times B_n \), where \( B_i \) are the blocks (see Definition 3.13). We abuse notation and take

\[
A_0 = B_1 \times \cdots \times B_n
\]

and

\[
A = B_1 \oplus \cdots \oplus B_n \oplus N.
\]
For each $a \in A$ we write

$$a = a_1 + \ldots + a_n + a_N,$$

where $a_j \in B_j$ and $a_N \in \mathbb{N}$. For each $i \in A$ we have

$$\Phi_i = \Phi_{i,1} + \ldots + \Phi_{i,n} + \Phi_{i,N},$$

where $\Phi_{i,j} \in B_j$ and $\Phi_{i,N} \in \mathbb{N}$. Suppose $(X)_+ = \bigcup_{j=1}^n X_j$ is the decomposition into Wedderburn components as given by Theorem 4.11 applied to the the map $\pi : A \to A/N$ followed by the isomorphism $A/N \to A_0$. Consider the new alphabet $\mathcal{A}' := A \times \{1, \ldots, n\}$. Define a new cocycle $\Phi'$ by $\Phi'_{(i,j)} := \Phi_{i,j} + (1/n)\Phi_{i,N}$. There is a natural factor map $\pi' : X_{\Phi'} \to X_\Phi$ given by $\pi' : \ldots (a_1,j_1)(a_2,j_2)\ldots \to \ldots a_1a_2\ldots$.

**Theorem 4.36.** (1) The algebra of $\Phi'$ is equal to $A$.

(2) $X_{\Phi'}$ satisfies (DD).

(3) The restriction of $\pi'$ to $(X_{\Phi'})_+$ is finite-to-one.

**Proof.** (1) The algebra $A'$ of $\Phi'$ is a subset of $A$ since each $\Phi'_{(i,j)} \in A$. To see the opposite inclusion it is enough to show that $\Phi_i \in A'$ for each $i$. But

$$\Phi_i = \sum_{j=1}^n (\Phi_{i,j} + (1/n)\Phi_{i,N}) = \sum_{j=1}^n \Phi'_{(i,j)}.$$

(2) follows from the fact that any subword of a non-transient $x \in X_{\Phi'}$ must consist of words whose letters have the second component that is the same. This is true since if $x = \ldots (a_1,j_1)(a_2,j_2)\ldots$ with $j_1 \neq j_2$, then the linear map $\Phi_{(a_1,j_1)(a_2,j_2)} \in \text{rad}(A)$ thus this word can only occur finitely many times in $x$, but then $x$ is transient.

(3) Since a recurrent point $x$ must be of the form $x = \ldots (a_1,j_x)(a_2,j_x)\ldots$ for $j_x \in \{1, \ldots, n\}$ it follows that $\pi'$ restricted to $(X_{\Phi'})_+$ is at most $n$-to-1.

$\square$
We now collect a couple of examples that show that the factor map need not be finite-to-one on the complement of the recurrent set.

Example: Let $\Phi_0 := \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $\Phi_1 := \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$. The corresponding subshift is manifestly the full shift on two symbols, but the algebra is given by $A := \begin{\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \}}$, $A$ has the two standard idempotents $e_1 := \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $e_2 := \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ which are the central idempotents of the complement of the radical. Thus $\Phi'_{(0,1)} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$, $\Phi'_{(0,2)} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}$.

The infinitely many points of the orbit of the point $(0,1)\infty. (0,2)\infty$ in $X_{\Phi'}$ all have image $0\infty$ under the factoring map. However, this is a problem of presentation which can be eliminated by using a better cocycle since $X_{\Phi}$ is actually the full shift.

Example: The Wedderburn components for the subshift $X$ that is the edge shift of the graph in Figure 4.6 intersect but neither one is contained in the other nor are the components equal.

![Figure 4.6: Sofic system](image)

$X$ is the cocyclic subshift of $\Phi$ obtained by taking for $\Phi_i$ the adjacency matrix of the subgraphs in which only the edges labeled $i$ are retained. That is
Take the idempotents
\[ \hat{e}_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \hat{e}_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \hat{e}_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}. \]

Then the Malcev decomposition of \( A \) is the decomposition \( A = \hat{e}_1 A \hat{e}_1 \oplus \hat{e}_2 A \hat{e}_2 \oplus \hat{e}_3 A \hat{e}_3 \oplus N \) (as vector spaces). After some straightforward matrix calculations, we get
\[ \Phi(0,1) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \Phi(0,2) = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \Phi(0,3) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}. \]

But then \( \Phi(0,3) \Phi(0,1) \neq 0 \). So the entire orbit of the point \((0,3)^\infty \cdot (0,1)^\infty\) is in \( X_{\Phi'} \) and every element of the orbit has image \( 0^\infty \) under the factor map.

**Aperiodic Decomposition and Connecting Diagrams**

Above we have used the algebra \( A \) to discover a great deal about the structure of the cocyclic subshift but we can gain even more information by looking at another algebra. We recall the following definitions and theorems from [26].

**Definition 4.37.** If \( A \) is the algebra generated by the cocycle \( \Phi \), then for any \( l \in \mathbb{N} \) define \( A^l \) to be the algebra generated by \( \Phi_\sigma \) where \( \sigma \) is a word of length divisible by \( l \).

**Definition 4.38.** The tail algebra of \( \Phi \) is the algebra, denoted by \( A^{(\infty)} \), \( A^{(\infty)} := \bigcap_{l \in \mathbb{N}} A^l \).
Definition 4.39. A cocycle is aperiodic iff $V \neq 0$ and its algebra coincides with its tail algebra. A cocycle is primitive iff it is irreducible and aperiodic. A cocyclic subshift is aperiodic iff it can be represented as $X_\Phi$ for some aperiodic $\Phi$, and its it primitive if such $\Phi$ exists that is primitive.

For a subshift $X$ with shift map $f$ we can consider the same set $X^{(d)} = X$ but with the map $f^d$ for some $d \in \mathbb{N}$. The system $(X^{(d)}, f^d)$ is the $d$-th power of $X$. The $d$-th power is naturally conjugate to a subshift with alphabet $A^d$, where $A^d$ is the set of all words of length $d$ with letters in $A$. It is straightforward to see that if $X$ is cocyclic with cocycle $\Phi$ then $(X_\Phi)^{(d)}$ is cocyclic with power cocycle $\Phi^{(d)} \in \text{End}(V)^{K^d}$ with $\Phi^{(d)}_\sigma := \Phi_\sigma$ for $\sigma \in A^d$. (See Proposition 3.1 in [26] for a proof that if the power of a subshift $X$ is cocyclic then $X$ is cocyclic.)

Theorem 4.40. If $\Phi \in \text{End}(V)^m$ is irreducible then there exists $q \in \mathbb{N}, q \leq \dim(V)$, such that $X_\Phi = X_0 \cup \ldots \cup f^{q-1}X_0$ for some $X_0 \subset X_\Phi$ that is invariant under $f^q$, and $f^q : X_0 \to X_0$ is naturally conjugate to a primitive cocyclic subshift. We call $q$ the period of $X$.

With the definitions and theorem above we are now ready to proceed. Below are a couple of useful but easy observations.

If $X$ is not irreducible we consider first the subshift $X_+$, which is a union of irreducible pieces $X_1, X_2, \ldots, X_n$. For ease of presentation we assume that $\Phi$ satisfies (DD). We use the notations $\omega_d(x), \alpha_d(x), O_d(x)$ for $\omega$-limit set, $\alpha$-limit set, and orbit under $f^d$, respectively.

Proposition 4.41. For any $d \in \mathbb{N}$ and $x \in X$ with $1 \in A^d$ we have the following:

1. $\alpha_d(x) \subset \alpha(x)$, likewise $\omega_d(x) \subset \omega(x)$. Also $\alpha_d(x)$ and $\omega_d(x)$ are both non-empty.

2. $O_d(x) \subset O(x)$ thus $\text{cl}(O_d(x)) \subset \text{cl}(O(x))$. 
(3) Let $B := A^d$, and $B = f_1B \oplus \ldots \oplus f_sB$ where after possible relabelling $f_1B, \ldots, f_sB$ are the principal modules. Each $Y_{f_jB}$ (treating $f_jB$ as a $B$-module) is an irreducible cocyclic subshift (via natural conjugation) and $(X^{(d)})_+ = \bigcup_{j=1}^s Y_{f_jB}$.

(4) Any of the Wedderburn components $Y_j$ for $(X^{(d)})$ as in (3) is contained in some $X_i$.

Proof. (1) If $y \in \omega_d(x)$ then $f^{dk}(x) \to y$ as $n_k \to \infty$ but then $y \in \omega(x)$. The other part analogous.

(2) The first observation is obvious and the second follows trivially from the first.

(3) follows from the preceding theory applied to $(X^{(d)}, f^d)$ (where this is thought of as shift space with alphabet $A^d$).

(4) Suppose $x$ has dense forward orbit under $f^d$ in some irreducible component of $X^{(d)}$. Then $\text{cl}(O_d(x)) \subset \text{cl}(O(x))$. But $x$ is recurrent under $f$ since $x \in \omega_d(x) \subset \omega(x)$ and so the closure of its orbit under $f$ is contained in one the components $X_i$ of $X$.

We will use the notation $Y_j$ for the Wedderburn components of $X^{(d)}$.

**Proposition 4.42.** If $X_+ = X_1 \cup \ldots \cup X_n$. Then $i \to j$ if and only if there are irreducible components $Y_i$ and $Y_j$ of $X^{(d)}$ with $Y_i \subset X_i$ and $Y_j \subset X_j$ and $C^{(d)}_{Y_iY_j} \neq 0$.

Proof. It is trivial to see that if $x$ has a connecting orbit under $f^d$ from $Y_i \subset X_i$ to $Y_j \subset X_j$ then the orbit of $x$ is a connecting orbit from $X_i$ to $X_j$.

We look at the sequence $\{f^{nd}(x)\}_{n \in \mathbb{N}}$ where $O(x)$ is a connecting orbit from $X_i$ to $X_j$. Then, by compactness, some subsequence converges, i.e. $y := \lim_{n \to \infty} f^{nk}(x)$ exists. Since $\omega(x)$ is contained in $X_j$ then $y \in X_j$. Likewise, the sequence $\{f^{-nd}(x)\}_{n \in \mathbb{N}}$ has a convergent subsequence to $z := \lim_{k \to \infty} f^{-nk}(x)$ with $z \in X_i$. Thus there is a connection from some $Y_i \subset X_i$ to some $Y_j \subset Y_j$. \qed
Let $G^{(d)}$ be the connecting diagram for the subshift $X^{(d)}$ (assuming (DD) for $\Phi^{(d)}$), which we call the $d$-connecting diagram. For vertices $i', j'$ in the $d$-connection diagram we write $i' \simeq j'$ if $Y_{i'}, Y_{j'} \subset X_i$ for some $i$. Clearly, $\simeq$ is an equivalence relation on \{1, \ldots, s\}. Identifying $i'$ and $j'$ if and only if $i' \simeq j'$ (where we use $i$ to represent the class of $i'$ such that $Y_{i'} \subset X_i$) including an edge from equivalence class $i$ to equivalence class $k$ if and only if there are $i' \in i$ and $k' \in k$ with and edge from $j'$ to $l'$ gives a diagram, which we denote $G^{(d)}/\simeq$.

**Corollary 4.43.** Let $G$ be the connecting diagram for $X$, then $(G^{(d)}/\simeq) = G$.

**Theorem 4.44.** Suppose that $X$ has at least two disjoint Wedderburn components, $X_1$ and $X_2$. Suppose also that the GCD$(q_1, q_2) = 1$ where $q_1, q_2$ are the respective periods. Furthermore, assume that there is a connection from $X_1$ to $X_2$. Then the refinement of the connecting graph with vertices the primitive components under the map $f^d$ has a connection from any primitive component in $X_1$ to any component in $X_2$.

**Proof.** The key observation is that if GCD$(q_1, q_2) = 1$, then $q := LCM(q_1, q_2) = q_1q_2$. Let $O(x)$ be a connecting orbit from $X_1$ to $X_2$. Observe that for each $d = 0, 1, \ldots, q - 1$, the orbit of $f^d(x)$ under $f^q$, or any multiple of $q$, gives an orbit from some aperiodic component in $X_1$ to some aperiodic component in $X_2$. If $f^h(x)$ and $f^k(x)$, with $h \neq k$ and $0 \leq h, k \leq q - 1$, have $f^q$-\(\alpha\)-limit sets that lie in the same aperiodic component, then their $\omega$-limit sets must lie in different aperiodic components. Before we see why this is true, we comment that the proposition follows easily from this statement because each vertex of the connecting graph is the source of $q_2$ edges and since none of them can have the same target if follows that each of the $q_2$ vertices corresponding to the aperiodic components of $X_2$ must be the targets. Thus the proposition holds.
We write \( X_1 = \bigcup_{h=0}^{q_1-1} X_{(1,h)} \) and \( X_2 = \bigcup_{k=0}^{q_2-1} X_{(2,k)} \) where \( q_1 \) and \( q_2 \) are the respective periods and \( X_{(i,j)} \) the aperiodic components. (We use a different notation than above to more carefully keep track of where each aperiodic subshift lives.) Suppose that \( f^{n_k}(x) \to X_{(2,k)} \) as \( n_k \to \infty \), where the notation means convergence to some element of \( X_{(2,k)} \). Likewise, suppose \( f^{n_l}(x) \to X_{(1,h)} \) as \( n_l \to -\infty \). Now for any \( t \in \{1, \ldots, q\} \) we have \( f^{t+n_k}(x) \to X_{(2,(k+t) \mod q_2)} \) and \( f^{t+n_l}(x) \to X_{(1,(h+t) \mod q_1)} \). If for some \( t \), we have that the pairs are repeated, i.e. \( h = (h+t) \mod q_1 \) and \( k = (k+t) \mod q_2 \), then \( t = 0 \mod q_1 \) and \( t = 0 \mod q_2 \), so that \( t = q_1 q_2 = q \). Thus each of the pairs \( (1, h + t), (2, k + t) \) (for \( t = 0, 1, \ldots, q - 1 \)) are distinct and the proposition follows.

**Example** Consider the sofic system associated to the graph in Figure 4.7.

![Figure 4.7: Example](image)

First note that under \( f \) the subshift \( X \) has two irreducible components, \( X_1 = \mathcal{O}(\ldots 0101.0101 \ldots) \) and \( X_2 = \mathcal{O}(\ldots 3456.3456 \ldots) \). A connecting orbit is given by the orbit of the point \( \ldots 010102.3456 \ldots \). Now examining \( f^4 \) on the subshift we get aperiodic pieces, \( X_{1,1} = \{ \ldots 101.0101 \ldots \}, X_{1,2} = \{ \ldots 1010.1010 \ldots \}, X_{2,1} = \{ \ldots 3456.3456 \ldots \}, X_{2,2} = \{ f(\ldots 3456.3456 \ldots ) \}, X_{2,3} = \{ f^2(\ldots 3456.3456 \ldots ) \}, \) and \( X_{2,4} = \{ f^3(\ldots 3456.3456 \ldots ) \} \). The orbits under \( f^4 \) of the points \( \ldots 010102.3456 \ldots, f(\ldots 010102.3456 \ldots), f^2(\ldots 010102.3456 \ldots), \) and \( f^3(\ldots 010102.3456 \ldots) \) provide the
connections between components. By elementary calculations we have the connections \( X_{1,1} \to X_{2,1} \) and \( X_{1,1} \to X_{2,3} \). Also, \( X_{1,2} \to X_{2,2} \) and \( X_{1,2} \to X_{2,4} \).

**Computation and Examples**

For ease of computation we consider a slightly different method to find connections between irreducible components. Recall that \( A = A_0 \oplus \text{rad}(A) \) as vector spaces. For a centrally primitive decomposition \( f_1 + \cdots + f_n = 1 \in A_0 \) we have corresponding principal modules \( e_1A, \ldots, e_nA \) such that \( e_iAe_j = 0 \) if and only if \( f_iAf_j = 0 \), see Theorem 3.14 and Corollary 3.18.

**Example:** Let \( I \) denote the \( 2 \times 2 \) identity and \( E := \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \). Then consider the cocyclic subshift with the following cocycle given by \( 4 \times 4 \) block matrices. Let \( \Phi_1 = \begin{bmatrix} I & 0 \\ 0 & 0 \end{bmatrix}, \Phi_2 = \begin{bmatrix} 0 & E \\ E & 0 \end{bmatrix}, \text{ and } \Phi_3 = \begin{bmatrix} 0 & 0 \\ 0 & I \end{bmatrix} \). Let \( A \) be the algebra generated by the cocycle. (The corresponding subshift is sofic since the matrices above have only non-negative entries.)

We use the computer algebra program GAP ([16]) to produce the connection graph. Below we use notation that must be used for the implementation in GAP. In particular, \( * \) is the notation for multiplication in GAP.

We first input the matrices, \( \Phi_1, \Phi_2, \Phi_3 \) as given above, and find that the algebra \( A \) over \( \mathbb{Q} \) has dimension 4. We can then find the semi-simple algebra \( A_0 \) complementing the radical using \( B := \text{LeviMalcevDecomposition}(A) \). \( B[1] \) is equal to \( A_0 \), where \( B[1] \) denotes the first component of the output of \( \text{LeviMalcevDecomposition}(A) \). To compute the central idempotents of the algebra \( B[1] \) we take \( \text{Id} := \text{CentralIdempotentsOfAlgebra}(B[1]) \). This yields two idempo-
tents

\[ \text{Id}[1] = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \text{Id}[2] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \]

To apply Theorem 4.16 via GAP we find a basis for \( A \). Let \( Bv := \text{BasisVectors}(\text{Basis}(A)) \), then

\[ Bv[1] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad Bv[2] = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \]

\[ Bv[3] = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \text{and} \quad Bv[4] = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \]

Then \( (\text{Id}[1] * Bv[2]) * \text{Id}[2] \) is not zero, so we have a connection \( 1 \to 2 \). On the other hand \( (\text{Id}[2] * Bv[1]) * \text{Id}[1] \) is non-zero so \( 2 \to 1 \). Thus the connecting diagram is given by the Figure 4.8:

\begin{center}
\begin{tikzpicture}
\node (1) at (0,0) {1};
\node (2) at (1,0) {2};
\draw[->] (1) to[bend left] (2);
\draw[->] (2) to[bend left] (1);
\end{tikzpicture}
\end{center}

\textbf{Figure 4.8: Connecting Graph - Simple Loop}

Here we can explicitly see that the irreducible components have empty intersection by examining the algebras \( \text{Id}[1] * A * \text{Id}[1] \) and \( \text{Id}[2] * A * \text{Id}[2] \) which correspond to the irreducible subshifts \( X_1 \) and \( X_2 \) respectively. We see that \( (\text{Id}[1] * \Phi_1) * \text{Id}[1] = \)
0 = (Id[1] * Φ_2) * Id[1] and (Id[1] * Φ_3) * Id[1] ≠ 0 therefore X_1 = \{3^\infty\}. Likewise we see that X_2 = \{1^\infty\}.

**Example:** We revisit the example on page 75. Recall that I is the 2 × 2 identity matrix and

\[
E = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.
\]

\[
\Phi_0 := \begin{bmatrix} I & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \Phi_1 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \Phi_2 := \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & I \end{bmatrix}, \quad \Phi_3 := \begin{bmatrix} 0 & E & 0 \\ 0 & 0 & E \\ 0 & 0 & 0 \end{bmatrix}.
\]

Above we observed that the connecting diagram had three vertices and that transitivity failed. We can use GAP to check our work. We get the output \( \text{Id}[1] = \Phi_2 \), \( \text{Id}[2] = \Phi_1 \), and \( \text{Id}[3] = \Phi_3 \). A, the algebra generated by the cocycle \( \Phi \), has dimension 5. Now \((\text{Id}[3] * Bv[4]) * \text{Id}[2] \) and \((\text{Id}[2] * Bv[4]) * \text{Id}[1] \) are non-zero. Also by examining basis elements we have \((\text{Id}[1] * A) * \text{Id}[2] = 0\), \((\text{Id}[1] * A) * \text{Id}[3] \), and \((\text{Id}[3] * A) * \text{Id}[1] \) are all zero. Thus (after renumbering) we get the connecting diagram below.

Figure 4.9: Non-transitive Connecting Diagram

We briefly survey results that guarantee the computability of many of the objects in which we are interested as well as the results’ implementation in GAP. For \( A \) presented as an input basis \( a_1, \ldots, a_n \), the radical \( \text{rad}(A) \) is computable in polynomial time by Dickson’s Theorem and Corollary 2.1 in [33]. This hinges on the fact that \( \text{rad}(A) = \{ x \in A : Tr(xa_i) = 0 \text{ for } i = 1, \ldots, n \} \). Computing the radical reduces to solving a system of linear equations.

The Wedderburn-Malcev decomposition of \( A \) (over \( \mathbb{Q} \)) can be computed in polynomial time by Theorem 3.1 in [12] and reduces to solving a system of linear equations.
Note that the system does not have a unique solution since the Wedderburn-Malcev decomposition is not unique. The same algorithms are outlined in the survey paper [6], which also includes the algorithm needed to find the central idempotents of a semisimple algebra. See the GAP manual [16] for more information on syntax and commands within GAP.
Let \( \mathcal{A} \) be an alphabet. A language with alphabet \( \mathcal{A} \) is any subset \( \mathcal{L} \) of \( \mathcal{A}^* \). Below we will explore some of the theory of formal languages. We are especially interested in languages associated to subshifts. Let \( X \) be a subshift. The language \( \mathcal{L}(X) \) of \( X \) is the collection of all words \( w \in \mathcal{A}^* \) which occur in the subshift. That is, a word \( w \) belongs to \( \mathcal{L}(X) \) if and only if there is \( x \in X \) and \( i, j \) with \( i \leq j \) such that \( x[i,j] = w \).

It is clear that if \( F = \mathcal{L}(X)^c = \mathcal{A}^* \setminus \mathcal{L}(X) \) then the subshift with the forbidden set \( F \) (as introduces at the beginning of Chapter 1) coincides with \( X, X_F = X \).

As one would expect, not every language is the language of a subshift. Let \( \mathcal{L} \) be a language, then we say \( \mathcal{L} \) is factorial if for all \( w \in \mathcal{L} \), every subword of \( w \) belongs to \( \mathcal{L} \). \( \mathcal{L} \) is said to be bi-extendable if for any \( w \in \mathcal{L} \), there are nonempty words \( u \) and \( v \) in \( \mathcal{L} \) so that \( uwv \in \mathcal{L} \). \( \mathcal{L} \) is said to be extendable if for all \( w \in \mathcal{L} \), there is a non-empty word \( u \in \mathcal{L} \) such that \( uw \in \mathcal{L} \).

**Proposition 5.1.** [27, 25]

1. A language \( \mathcal{L} \) is factorial and bi-extendable if and only if there is some two-sided subshift \( X \) such that \( \mathcal{L} = \mathcal{L}(X) \).

2. A language \( \mathcal{L} \) is factorial and extendable if and only if there is some one-sided subshift \( X \) such that \( \mathcal{L} = \mathcal{L}(X) \).

To further explore languages of subshifts we need some of the theory of formal languages and theoretical computer science. A deterministic finite automaton over an alphabet \( \mathcal{A} \) is a device which reads letters of \( \mathcal{A} \) and changes its inner state. We require the set of states, \( Q \), to be finite. There are distinguished initial states and final states. So then every finite automaton is represented by a transition function
δ : Q × A → Q. Thus if the automaton is in state q and reads letter a, δ changes the state of the finite automaton to δ(q, a). We can extend the transition function δ to the domain Q × A*, with δ(q, ε) = q and δ(q, ua) = δ(δ(q, u), a), for u ∈ A*, a ∈ A. We think of this extension of the original δ as giving the ability to read words. We also consider the more general non-deterministic finite automaton for which we only have a relation δ instead of a function.

**Definition 5.2.** A non-deterministic finite automaton M over an alphabet A is a 4-tuple (Q, I, δ, F), where,

1. Q is a finite set called the set of states,
2. I is a subset of Q called the set of initial states,
3. δ ⊂ Q × A × Q called the transition relation,
4. F is a subset of Q called the set of final states.

Note that the automaton M is deterministic if and only if I has exactly one element and for every q ∈ Q and, for every a ∈ A, there exists exactly one q′ for which (q, a, q′) ∈ δ. In such case we can think of δ as a function, δ(q, a) = q′.

Given w_i ∈ A∪{ε} for i = 1, ..., n, we say that the word w = w_1 ... w_n is accepted by M = (Q, I, δ, F) if and only if there is a sequence q_1, q_2, ..., q_{n+1} of states such that q_1 ∈ I, q_{n+1} ∈ F, and for all i ≤ n, we have (q_i, w_i, q_{i+1}) ∈ δ. The set

\[ \mathcal{L}(M) = \{ w \in A^* \mid M \text{ accepts } w \} \]

is called the language accepted by M. A language \( \mathcal{L} \) is called regular if and only if \( \mathcal{L} = \mathcal{L}(M) \) for some finite automaton M.

We state without proof the following theorem that allows use of non-deterministic and finite automatons more or less interchangeably. For a proof see [22].
Theorem 5.3. A language is accepted by a non-deterministic finite automaton if and only if it is accepted by a deterministic finite automaton.

A labeled graph, $\mathcal{G}$, is a finite directed graph each edge of which is labeled with an element of $\mathcal{A}$. The (one-sided or two-sided) subshift $X_{\mathcal{G}}$ of the graph $\mathcal{G}$ is the collection of all (infinite or bi-infinite) sequences obtained by reading off the labels over the edges of a (infinite or bi-infinite) path on $\mathcal{G}$. A subshift $X$ is sofic if it is $X_{\mathcal{G}}$ for some labeled directed graph $\mathcal{G}$. We now state a well known theorem that relates the theory of regular languages to symbolic dynamics.

Theorem 5.4. Suppose $\mathcal{L}$ is the language of a subshift $X$. Then $\mathcal{L}$ is regular if and only if $X$ is sofic.

We do not give the full proof here but the main idea is that the graph presentation of a sofic shift is a finite automaton where each vertex is accepting, see [27] for more details.

Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be two alphabets. Then a homomorphism $h : \mathcal{A}_1^* \to \mathcal{A}_2^*$ is a map between the sets such that $h(w_1w_2\ldots w_n) = h(w_1)h(w_2)\ldots h(w_n)$ for any $w_i \in \mathcal{A}_1$ and $n \in \mathbb{N}$. For any language $\mathcal{L} \subset \mathcal{A}^*$, the restriction of a homomorphism $h$ to $\mathcal{L}$ is a called a homomorphism from $\mathcal{L}$ into $\mathcal{A}_2$. If we restrict the co-domain to the image of $\mathcal{L}$ under $h$, we say that $h$ is a homomorphism from $\mathcal{L}$ to $h(\mathcal{L})$. Note a homomorphism $h$ is completely determined by its image on the individual letters $\mathcal{A}_1$, and is also referred to as a substitution for that reason. However, in computer science parlance, the concept of substitution is typically more general as it allows for assigning a whole language to any letter (see [34]).
Let $\mathcal{A}$ be an alphabet with $m := \#\mathcal{A}$ and $\Phi$ a (deterministic) cocycle over $\mathcal{A}$, that is, $\Phi = (\Phi_i)_{i \in \mathcal{A}} \in (\text{End}(V))^m$. The language of $\Phi$ is

$$L(\Phi) = \{ w \in \mathcal{A}^* | \Phi_w \neq 0 \}.$$ 

We say a language $L$ is a language of a cocycle if $L = L(\Phi)$ for some cocycle $\Phi$. Note that, unless otherwise stated, we will assume $\Phi_e = \text{Id}$. Thus the empty word $\epsilon$ belongs to $L(\Phi)$ for any $\Phi$. Observe that if $L = L(\Phi)$ for some $\Phi$ then $L$ is factorial. Thus the regular language $\{01\}$ over the alphabet $\{0, 1\}$ is not the language of a cocycle.

Now given languages $L(\Phi)$ and $L(\Psi)$ over alphabets $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively we can consider both of them as languages over the alphabet $\mathcal{A} := \mathcal{A}_1 \cup \mathcal{A}_2$. We extend $\Phi$ to a cocycle over $\mathcal{A}$ by taking $\Phi_a = 0$ for any $a \in \mathcal{A}$ with $a \notin \mathcal{A}_1$. We extend $\Psi$ in the analogous manner. Unless otherwise stated, we will assume without any further mention that given languages are over the same alphabet.

**Proposition 5.5.** (1) If $L_1$ and $L_2$ are languages of cocycles, then $L_1 \cup L_2$ and $L_1 \cap L_2$ are each languages of cocycles.

(2) Suppose $h : L_1 \to L_2$ is a surjective homomorphism and that $L_2$ is the language of a cocycle, then $L_1$ is the language of a cocycle.

**Proof.** (1) First we consider the union. Suppose $L_1 = L(\Phi)$ with $\Phi \in (\text{End}(U))^m$ and $L_2 = L(\Psi)$ with $\Psi \in (\text{End}(V))^m$. Take $\Gamma_a = \Phi_a \oplus \Psi_a$ as a map on $U \oplus V$ for each $a \in \mathcal{A}$. Then for any $w \in \mathcal{A}^*$, $\Gamma_w = \Phi_w \oplus \Psi_w$ so that $\Gamma_w \neq 0$ if and only if $\Phi_w \neq 0$ or $\Psi_w \neq 0$. Hence $L(\Gamma) = L_1 \cup L_2$.

Now we look at the intersection of two languages. For each $a \in \mathcal{A}$ take $\Gamma_a = \Phi_a \otimes \Psi_a$, where $\otimes$ denotes the tensor product, which is a linear map on $U \otimes V$. Then
for any \( w \in B^* \) we have \( \Gamma_w = \Phi_w \otimes \Psi_w \). Thus \( \Gamma_w \neq 0 \) if and only if both \( \Phi_w \neq 0 \) and \( \Psi_w \neq 0 \). Therefore, \( L_1 \cap L_2 = L(\Gamma) \).

(2) Suppose that \( h : L_1 \to L_2 \) is a homomorphism and \( L_2 = L(\Phi) \). To create a cocycle \( \Psi \) such that \( L(\Psi) = L_1 \) take \( \Psi_a = \Phi_h(a) \) for all \( a \in A \).

**Proposition 5.6.** If \( X_\Phi \) is the cocyclic subshift of an irreducible cocycle \( \Phi \), then \( L(\Phi) = L(X_\Phi) \).

**Proof.** The proof follows immediately from the fact that, for an irreducible cocycle, a word \( w \) occurs in the subshift \( X_\Phi \) in if and only if \( \Phi_w \neq 0 \); see the proof of Theorem 4.7.

We have seen above that not every regular language is a language of a cocycle. The following corollary says that not every language of a cocycle is regular.

**Corollary 5.7.** There is a language of a cocycle which is not regular.

**Proof.** By Theorem 5.4, if \( X_\Phi \) is not sofic then \( L(\Phi) \) is not regular. We have shown in Theorem 2.23 that there are irreducible cocyclic subshifts which are are not sofic.

**Proposition 5.8.** If \( \mathcal{L} \) is a factorial regular language, then \( \mathcal{L} \) is the language of a cocycle.

**Proof.** For a factorial regular language \( \mathcal{L} \) we can assume that every state in the set \( Q \) is a final state. That is \( \mathcal{L} \) consists labels of paths on a labeled graph \( \mathcal{G} \) as the allowed words. Set \( m := \#Q \), the cardinality of \( Q \). Then, for each \( a \in A \), let \( \Phi_a \) be the \( m \times m \) matrix with \( i, j \) entry equal to one if \( a \) is the label of an edge going from \( i \) to \( j \) and 0 otherwise. With this construction \( \Phi_w \neq 0 \) if only if there is a walk over the graph with label \( w \). And there is a walk over the graph with label \( w \) if and only if \( w \in \mathcal{L} \). Thus \( L(\Phi) = \mathcal{L} \).
Suppose that instead of having a single linear map for each letter $a \in A$ we allow a set of possible choices $\{\Phi(a,1), \ldots, \Phi(a,n_a)\}$. This is formalized by considering the semigroup $\text{End}(V)$ of all subspaces of $\text{End}(V)$ where for two subspaces $W, V$ the product is $WV = \text{Lin}(\Psi_1\Psi_2)\forall \Psi_1 \in W, \Psi_2 \in V$. The $\text{End}(V)$ valued cocycle is given by $\Phi_a = \text{Lin}(\Phi(a,1), \ldots, \Phi(a,n_a)) \in \text{End}(V), a \in A$. We assume that $\Phi_\epsilon = \text{Lin}(\text{Id})$. Such $\Phi = (\Phi_a)_{a \in A}$ is called a non-deterministic cocycle. As before, its language is

$$L(\Phi) = \{w \in A^* \mid \Phi_w \neq 0\}.$$ 

A language $L$ is a language of a non-deterministic cocycle if and only if there is a non-deterministic cocycle $\Phi$ with $L = L(\Phi)$. Note that every language of a cocycle is a language of a non-deterministic cocycle. Most of the development generalizes from the deterministic to the non-deterministic context. In particular, Proposition 5.5 has a non-deterministic analogue. However, its part (2) holds in the following stronger form for non-deterministic languages.

**Proposition 5.9.** If $h : L_1 \rightarrow L_2$ is an onto homomorphism then $L_1$ is a language of a non-deterministic cocycle if and only if $L_2$ is the language of a non-deterministic cocycle.

**Proof.** If $L_2$ is the language of the non-deterministic cocycle $\Psi$, for each $a \in A$, take $\Phi_a = \Psi_{h(a)}$. Now $L_1 = L(\Phi)$. We saw this above for deterministic cocycles.

Now suppose that $L_1 = L(\Phi)$ with $\Phi$ a non-deterministic cocycle. Recall that we take $L_2$ to be a language over the same alphabet $A$. For each element $a \in A$ which occurs in $L_2$ it also belongs to $L_2$ since $L_2$ is factorial. Therefore $h^{-1}(a)$ is non-empty and we define the non-deterministic cocycle $\Gamma_a$ to be the linear combination of the subspaces in $\{\Phi_b \mid b \in h^{-1}(a)\}$, where $h^{-1}(a) \neq \emptyset$ since we assumed that $h$ is onto and languages of cocycles are factorial.
We claim that $L(\Gamma) = L_2$.

First we show $L(\Gamma) \subset L_2$. Suppose that $w \notin L_2$ and $w = w_1 \ldots w_n$ with $w_i \in A$ for each $i$. Then for any $v_1, \ldots, v_n \in A$ with $h(v_1) = w_1, \ldots, h(v_n) = w_n$ we have that $\Phi_{v_1} \cdots \Phi_{v_n} = 0$. But since $\Gamma_a = \text{Lin}(\Phi_b)_{h(b)=a}$ we must have that $\Gamma_{w_1} \cdots \Gamma_{w_n} = 0$. Hence, $w \notin L(\Gamma)$.

Now if $w \in L_2$ then $w = h(a_1) \ldots h(a_n)$ and the product $\Phi_{a_1} \cdots \Phi_{a_n} \neq 0$, we get $\Phi_{a_1} \cdots \Phi_{a_n} \subset \Gamma_{h(a_1) \ldots h(a_n)} \neq 0$. Therefore, $L(\Gamma) \supset L_2$ and thus $L(\Gamma) = L_2$.

For languages $L_1$ and $L_2$ over the alphabet $A$ the concatenation of the languages is denoted $L_1 L_2 := \{w_1 w_2 | w_1 \in L_1, w_2 \in L_2\}$. In case $L_1 = \emptyset$ or $L_2 = \emptyset$ we take $L_1 L_2 = \emptyset$.

**Theorem 5.10.** Let $L_1$ and $L_2$ be languages of non-deterministic cocycles. Then the concatenation $L_1 L_2$ is also the language of a non-deterministic cocycle.

**Proof.** We create a non-deterministic cocycle $\Gamma$ so that $L_1 L_2 = L(\Gamma)$. Suppose $L_1 = L(\Phi)$ and $L_2 = L(\Psi)$. Take $C = \text{Lin} \left( \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \right)$ and $D = \text{Lin} \left( \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right)$. Note that, for $i, j \in \mathbb{N}$, we have $C^i D^j = CD$ and that $DC = 0$. Then we define $\Gamma_a := \Phi_a \otimes \text{Lin}(\text{Id}) \otimes C$. Likewise take $\Omega_a := \text{Lin}(\text{Id}) \otimes \Psi_a \otimes D$. Now take $\Delta_a := \text{Lin}(\Gamma_a, \Omega_a)$.

We now claim that $L(\Delta) \subset L_1 L_2$.

Suppose that $w = w_1 \ldots w_n \in L(\Delta)$, so $\Delta_w \neq 0$. By definition of $\Delta$ as the linear combination of $\Gamma$ and $\Omega$ it follows that there are $\alpha_i, \beta_i \in \mathbb{C}$, $i, \ldots, n$, such that $(\alpha_1 \Gamma_{w_1} + \beta_1 \Omega_{w_1}) \ldots (\alpha_n \Gamma_{w_n} + \beta_n \Omega_{w_n}) \neq 0$. Now for all $a, b \in A$, we have $\Omega_a \Gamma_b = 0$. This is due to $DC = 0$, to multiplication of tensors being coordinate-wise, and the fact that the tensor product is zero if just one component is zero. Now there is a $k$, $0 \leq k \leq n$, such that $\Gamma_{w_1} \cdots \Gamma_{w_k} \Omega_{w_{k+1}} \cdots \Omega_{w_n} \neq 0$; where $k = 0$ covers the possibility...
that $\mathbf{\Omega}_w \cdots \mathbf{\Omega}_w \neq 0$. This implies that $\mathbf{\Gamma}_w \cdots \mathbf{\Gamma}_w \neq 0$, which gives $\Phi_w \cdots \Phi_w \neq 0$. Likewise, $\mathbf{\Omega}_{w_{k+1}} \cdots \mathbf{\Omega}_w \neq 0$, which gives that $\Psi_{w_{k+1}} \cdots \Psi_w \neq 0$. Thus $w_1 \ldots w_k \in \mathcal{L}_1$ and $w_{k+1} \ldots w_n \in \mathcal{L}_2$. Note that in case $k = 0$ we take $w_1 \ldots w_k$ to mean the empty word. Hence $w \in \mathcal{L}_1 \mathcal{L}_2$.

That $\mathcal{L}_1 \mathcal{L}_2 \subset \mathcal{L}(\Delta)$ is easier to see.

Let $w = w_1 w_2$ with $w_1 \in \mathcal{L}_1$ and $w_2 \in \mathcal{L}_2$ so $\Phi_{w_1} \neq 0$ and $\Psi_{w_2} \neq 0$. This means that $\mathbf{\Gamma}_{w_1} \mathbf{\Omega}_{w_2} \neq 0$ and so by definition of $\Delta$ we have that $\Delta_w \neq 0$. Therefore $w \in \mathcal{L}(\Delta)$, so $\mathcal{L}_1 \mathcal{L}_2 \subset \mathcal{L}(\Delta)$.

If $\mathcal{L}$ is a language, define $\mathcal{L}^0 = \{\epsilon\}$, $\mathcal{L}^1 = \mathcal{L}$, and $\mathcal{L}^n$ for $n \geq 2$ as the concatenation of $\mathcal{L}$ with itself $n$ times. The language $\mathcal{L}^* = \bigcup_{n=0}^{\infty} \mathcal{L}^n$ is called the Kleene closure or star closure of the language $\mathcal{L}$. We are interested in language families which form a Kleene Algebra, see Definition 5.23. Kleene closure is one of several operations of a Kleene algebra. Note that for factorial $\mathcal{L}$, with $\mathcal{A} \subset \mathcal{L}$, we have $\mathcal{L}^* = \mathcal{A}^*$.

To get a more interesting theory incorporating Kleene star we have to step outside the universe of languages of cocycles. In the next section we define (non-deterministic) cocyclic languages so that they form a Kleene algebra, generalize regular languages, and are related to cocyclic subshifts in a way analogous to the relation of regular languages to sofic shifts.

Cocyclic Automata and Languages

We now look at a type of automaton that is closely related to cocyclic subshifts. Our setting is an extreme case of the generalized real-time quantum automaton found in [29], although we initially developed our ideas oblivious to [29] and our viewpoint is somewhat different. More precisely, our automata correspond to the generalized
real-time quantum automata with cut point 0. For more on cut points see [4]. We now proceed with our definition.

**Definition 5.11.** A (deterministic) cocyclic automaton \( Q \) is a 4-tuple \((V, \Phi, v, P)\) where \( V \) is a finite dimensional vector space, and \( \Phi = (\Phi_a)_{a \in A} \) is a cocycle with \( \Phi_a \in \text{End}(V) \), \( v \in V \), and \( P \in \text{End}(V) \) is a projection, i.e. \( P^2 = P \).

We refer to \( P \) as the accepting projection and \( V_A = \text{Im}(P) \) as the accepting subspace. We refer to \( v \) as the initial vector. For a word \( w \in A^* \), we say that \( w \) is accepted by \( Q \) if \( v \Phi w P \neq 0 \). We take \( \Phi_\epsilon = \text{Id} \) on \( V \).

The language accepted by \( Q \), denoted by \( L(Q) \), is the set of all words accepted by \( Q \). A language that is accepted by some cocyclic automaton is called a cocyclic language. Observe that, for \( Q = (V, \Phi, v, P) \), the cocyclic language of \( Q \) is contained in the language of the cocycle, \( L(Q) \subset L(\Phi) \).

**Proposition 5.12.** If \( L \) is the language of a cocycle then it is a cocyclic language.

**Proof.** Let \( \Phi = (\Phi_a)_{a \in A} \) be a cocycle with \( \Phi_a \in \text{End}(V) \) and \( \Phi_\epsilon = \text{Id} \). We construct a cocyclic automaton \( Q \) such that \( L(\Phi) = L(Q) \). Let \( \{v_1, \ldots, v_n\} \) be a basis of the vector space \( V \). Take \( U := V^{\oplus n} \), \( u := v_1 \oplus \ldots \oplus v_n \in U \) as the initial vector, and \( P := \text{Id} \) as the accepting projection. Finally, take \( \Psi_a := \Phi_a^{\oplus n} \) and \( Q := (U, \Psi, u, P) \).

We claim that \( L(Q) = L(\Phi) \).

Suppose first that \( w \in L(Q) \), so that \( u \Psi w P = u \Psi w \neq 0 \). Then, for some \( i \), we have that \( v_i \Phi w \neq 0 \) so that \( w \in L(\Phi) \).

On the other hand, if \( w \in L(\Phi) \) then there exists a basis element \( v_i \) such that \( v_i \Phi w \neq 0 \). This gives \( v_1 \Phi w \oplus \ldots \oplus v_i \Phi w \oplus \ldots \oplus v_n \Phi w \neq 0 \) and therefore \( w \in L(Q) \).

**Theorem 5.13.** Every regular language is cocyclic.
Proof. Let $\mathcal{L}$ be a regular language that is accepted by an automaton $\mathcal{M}$ (which we can assume is deterministic by Theorem 5.3). Then represent $\mathcal{M}$ as a graph with $t$ vertices for some $t \in \mathbb{N}$. This can be done by taking vertices corresponding to states and edges corresponding to transitions (see Proposition 3.54 and Proposition 3.55 in [25]). To build a cocyclic automaton we use the idea of adjacency matrices of graphs.

Let $V = C^t$, and take $v \in C^t$ with 1 in the $i$th spot if and only if the $i$th vertex is an initial vertex and 0 otherwise. For the projection $P$, we take the matrix which has a 1 in the $(i, i)$th spot if and only if the $i$th vertex is a final vertex, i.e. represents a final state. We take all other entries to be 0. Now, for each $a \in \mathcal{A}$, let $\Phi_a$ be the matrix which has 1 in the $(i, j)$th entry if and only if there is an edge labelled $a$ which goes from the $i$th vertex to the $j$th vertex. As before, (see page 12), for any $w \in \mathcal{A}^*$ with $w = w_1 \ldots w_n$ and such that $w_k \in \mathcal{A}$ for $k \in \{1, \ldots, n\}$, we have $\Phi_w = \Phi_{w_1} \ldots \Phi_{w_n}$. Also take $\Phi_\epsilon = \text{Id}$.

Claim: $\mathcal{L} = \mathcal{L}(V, \Phi, v, P)$.

First consider the empty word $\epsilon$. $\epsilon \in \mathcal{L}$ if and only if some state $i$ is both initial and final. By the construction of $v$ and $P$, $v$ has 1 for its $i$th component and $P$ has 1 in its $i, i$-th entry. But this is true if and only if $\epsilon P \neq 0$ which is true if and only if $\epsilon \in \mathcal{L}(V, \Phi, v, P)$.

Observe that $(\Phi_w)_{i,j} = 1$ if and only if $w$ is the label of a path from vertex $i$ to vertex $j$ and $(\Phi_w)_{i,j} = 0$ otherwise. This gives $w \in \mathcal{L}(V, \Phi, v, P)$ if and only if $v \Phi_w P \neq 0$ if and only if there is an initial vertex $i$ and a final vertex $j$ so that $(\Phi_w)_{i,j} \neq 0$, which is true if and only if $w \in \mathcal{L}$ by construction of $G$.

Proposition 5.14. If $\mathcal{L}_1$ and $\mathcal{L}_2$ are languages accepted respectively by $\mathcal{Q}_1$ and $\mathcal{Q}_2$ then there are cocyclic automata that accept both $\mathcal{L}_1 \cap \mathcal{L}_2$ and $\mathcal{L}_1 \cup \mathcal{L}_2$. \qed
Proof. The proof is essentially the same as the proof of Proposition 5.5 for languages of cocycles. Given the two accepting cocyclic automata $Q_1 = (U, \Phi, u, P_1)$ and $Q_2 = (V, \Psi, v, P_2)$ we take the automaton $Q_1 \oplus Q_2$ to be $(U \oplus V, \Phi \oplus \Psi, u \oplus v, P_1 \oplus P_2)$ where $(\Phi \oplus \Psi)_a = \Phi_a \oplus \Psi_a$ for each $a \in A$. For $w \in \mathcal{A}^*$, $w \in L(Q_1 \oplus Q_2)$ if and only if $(u \oplus v)(\Phi_w \oplus \Psi_w)(P_1 \oplus P_2) \neq 0$. But $(u \oplus v)(\Phi_w \oplus \Psi_w)(P_1 \oplus P_2) = u\Phi_w P_1 \oplus v\Psi_w P_2$ and hence is non-zero if and only if $u\Phi_w P_1 \neq 0$ or $v\Psi_w P_2 \neq 0$. The last statement is equivalent to $w \in L_1 \cup L_2$.

For the intersection of the two languages use $Q_1 \otimes Q_2$ defined in the analogous manner.

Just as before, we also want to consider non-deterministic cocyclic automata.

Definition 5.15. A non-deterministic cocyclic automaton is a 4-tuple $(V, \Phi, v, P)$ where $V$ is a finite dimensional vector space. $\Phi$ is a non-deterministic cocycle, $P$ is a projection, $\Phi_\epsilon = \text{Lin}(\text{Id})$, and $v \in V$.

We say a word $w \in \mathcal{A}^*$ is accepted by $Q = (V, \Phi, v, P)$ if $v\Phi_w P \neq 0$. The language of the cocyclic automaton $Q$ is the set

$$L(V, \Phi, v, P) = L(Q) = \{w \in \mathcal{A}^* | Q \text{ accepts } w\}.$$ 

A language accepted by a non-deterministic cocyclic automaton is referred to as a non-deterministic cocyclic language. The following proposition summarizes some basic properties of non-deterministic cocyclic languages where the proof follows in the same way as in the deterministic case.

Proposition 5.16. If $L_1$ and $L_2$ are recognized by non-deterministic cocyclic automata $Q_1$ and $Q_2$ respectively, then $L_1 \cap L_2$ and $L_1 \cup L_2$ are recognized by automatons $Q_1 \otimes Q_2$ and $Q_1 \oplus Q_2$ respectively.
We note here that there are alternate but equivalent definitions for non-deterministic cocyclic automata. In the definition above we have allowed for a space of linear maps to be associated to each letter of the alphabet but we have kept the initial vector. Proposition 5.17 shows that allowing for an initial subspace does not change the class of languages which are recognized. Likewise, if we take a space generated by projections instead of a single projection the class of languages is the same.

**Proposition 5.17.** (1) A language is accepted by the automaton $(V, \Phi, V_0, P)$ where $V_0$ is a subspace of $V$ if and only if it is accepted by some deterministic cocyclic automaton.

(2) A language is accepted by the automaton $(V, \Phi, v, P)$ where $P$ is a subspace of $\text{End}(V)$ with a basis consisting of projections iff it is accepted by a deterministic cocyclic automaton.

(3) A language is accepted by the automaton $(V, \Phi, v, P)$ where $P$ is an arbitrary element of $\text{End}(V)$ if and only if it is accepted by a deterministic cocyclic automaton.

**Proof.** For (1), (2), and (3) it is clear that the implications $\Leftarrow$ hold. We prove $\Rightarrow$ for each below.

(1) Assume that $L = L(V, \Phi, V_0, P)$ with $V_0$ a subspace of $V$ and $P$ a projection. Let $v_1, \ldots, v_t$ be a basis for $V_0$. Now take the automaton given by

$$Q^{\oplus t} = (V^{\oplus t}, \Phi^{\oplus t}, v_1 \oplus \cdots \oplus v_t, P^{\oplus t}).$$

Then $V_0 \Phi_w = 0$ if and only if for all $i$, we have $v_i \Phi_w = 0$. But $v_i \Phi_w = 0$ for all $i$ if and only if $(v_1 \oplus \cdots \oplus v_t) \Phi^{\oplus t}_w = 0$.

(2) Now let $P_1, \ldots, P_s$ be a basis of projections for the subspace $P$. $L$ is accepted by the deterministic cocyclic automaton $(V^{\oplus s}, \Phi^{\oplus s}, v^{\oplus s}, P_1 \oplus \cdots \oplus P_s)$. 
(3) Assume \( L \) is a language accepted by \((V, \Phi, v, P)\) where \( P \in \text{End}(V) \). Then let \( v_1, \ldots, v_t \) be a basis for a subspace complementing \( \ker P \) (i.e. \( W \oplus \ker P = V \)). Extend this to a basis of \( V \), say \( v_1, \ldots, v_t, \ldots, v_n \). Define \( P' \) by \( v_i P' = v_i \) for \( i \in \{1, \ldots, t\} \) and \( v_i P' = 0 \) for \( t + 1 \leq i \leq n \). Observe that \( \ker(P) = \ker(P') \). Hence for any \( w \in A^* \), \( v\Phi_w P = 0 \) if and only if \( v\Phi_w P' = 0 \).

Below there will be some occasions for using these equivalent formulations of automata. We now continue with the theory of our class of languages.

When we prove that the concatenation of two non-deterministic cocyclic languages is a non-deterministic cocyclic language it will be useful to assume that the languages have alphabets which do not intersect.

Lemma 5.18. Let \( A \) and \( B \) be alphabets. Suppose \( L_2 \) is an image of \( L_1 \) under a homomorphism that sends letters to letters, i.e. \( \exists h : A^* \to B^* \) with \( h(A) \subset B \) and \( L_2 = h(L_1) \).

(1) If \( L_2 \) is (non-deterministic) cocyclic then \( L_1 \) is (non-deterministic) cocyclic.

(2) \( L_1 \) is non-deterministic cocyclic if and only if \( L_2 \) is non-deterministic cocyclic.

Proof. (1) Let \( L_2 \) be cocyclic or non-deterministic cocyclic, thus \( L_2 = \mathcal{L}(V, \Phi, v, P) \). Suppose that \( h : A^* \to B^* \) is a homomorphism that sends letters to letters and \( L_2 = h(L_1) \). Define \( \Phi_a := \Psi_{h(a)} \), for each \( a \in A \). (The definition of the cocycle is same in the non-deterministic and deterministic cases.) We claim that \( L_1 = \mathcal{L}(V, \Phi, v, P) \).

Suppose \( w = w_1 \ldots w_n \in L_1 \) with \( w_i \in A \). \( h(w) = h(w_1) \ldots h(w_n) \in L_2 \) hence \( v\Psi_{h(w_1)} \cdots \Psi_{h(w_n)} P \neq 0 \), but this is the same as \( v\Phi_{w_1} \cdots \Phi_{w_n} P \neq 0 \) so \( w \in L_1 \).

Now suppose that \( w = w_1 \ldots w_n \notin \mathcal{L}_1 \), \( h(w_i) \) are still defined so the product \( v\Phi_{w_1} \cdots \Phi_{w_n} P = v\Psi_{h(w_1)} \cdots \Psi_{h(w_n)} P \) makes sense and equals zero because \( h(w) \notin L_2 \). But this means that \( w \notin \mathcal{L}_1(V, \Phi, v, P) \).
(2) By (1) we only need to show that if \( L_1 \) is non-deterministic cocyclic then so is \( L_2 \). We have \( L_1 = \mathcal{L}(V, \Phi, v, P) \). For any \( b \in B \), define \( \Psi_b = \text{Lin}(\Phi_a)_{a \in A, h(a) = b} \).

The following calculation completes the proof. For \( w = w_1 \ldots w_n \) with \( w_i \in B \) for each \( i \), we have

\[
   w \notin \mathcal{L}(V, \Psi, v, P) \iff v \psi_{w_1} \cdots \psi_{w_n} P = 0 \iff \forall a_i \in h^{-1}(w_i) v \Phi_{a_i} \cdots \Phi_{a_n} P = 0
\]

\[
   \iff h^{-1}(w) \cap L_1 = \emptyset \iff w \notin L_2.
\]

\( \square \)

**Proposition 5.19.** Suppose \( L_1 \) and \( L_2 \) are non-deterministic cocyclic languages, then so is the concatenation \( L_1L_2 \).

**Proof.** First note that it is enough to consider languages over disjoint alphabets. Since if we have \( L_1, L_2 \) over the same alphabet \( A \) we can consider the language \( L'_2 \) in which every letter is replaced by its “primed” version. We now have languages \( L_1 \) over \( A \) and \( L'_2 \) over \( A' \), and we will show below that under these circumstances \( L_1L'_2 \) is non-deterministic cocyclic. The homomorphism \( h \) that sends each letter of \( a' \in A' \) to \( a \in A \) satisfies the hypotheses of Lemma 5.18, so \( L_1L_2 \) is also non-deterministic cocyclic.

Let \( L_1 = \mathcal{L}(V_1, \Psi, u_1, P_1) \) and \( L_2 = \mathcal{L}(V_2, \Gamma, u_2, P_2) \) be non-deterministic cocyclic over alphabets \( A \) and \( B \) respectively with \( A \) and \( B \) disjoint. We look at several cases.

Case 1: \( \epsilon \notin L_1 \) and \( \epsilon \notin L_2 \):

In the rest of the proof we write a matrix for the linear space with the matrix as the single basis element and we also write \( \text{Id} \) as the identity on the linear space that should be clear from the context. Let \( V = V_1 \otimes V_2 \otimes \mathbb{C}^2 \), and for each \( a \in A \) let \( \Phi_a := \Psi_a \otimes \text{Id} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \). For \( b \in B \) we take \( \Phi_b := \text{Id} \otimes \Gamma_b \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \). Let
\( v := u_1 \otimes u_2 \otimes [1, 0] \) and \( P := P_1 \otimes P_2 \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \). Note that we generate the matrices by using the cocyclic automaton for the language \( \mathcal{A}^+ \mathcal{B}^+ \), i.e.

\[
\mathcal{L} \left( \mathbb{C}^2, \left( \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, [1, 0], \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right) \right) = \mathcal{A}^+ \mathcal{B}^+.
\]

So for \( b \in \mathcal{B} \) and \( a \in \mathcal{A} \) we have \( \Phi_b \Phi_a = 0 \). Thus all words in \( \mathcal{L}(V, \Phi, v, P) \) are contained in \( \mathcal{A}^+ \mathcal{B}^+ \). Also, \( vP = 0 \) so \( \epsilon \notin \mathcal{L}(V, \Phi, v, P) \). Also, if \( \Phi_w \neq 0 \) we have that \( w = w_1 w_2 \) with \( w_1 \in \mathcal{A}^+ \) and \( w_2 \in \mathcal{B}^+ \) since for \( w_1 \in \mathcal{A}^+ \), \( v \Phi_{w_1} P = 0 \) and for \( w_2 \in \mathcal{B}^+ \) we get \( v \Phi_{w_2} P = 0 \). (We used the fact that the third components recognize when a word is in \( \mathcal{A}^+ \mathcal{B}^+ \) and that a tensor product is zero if any component is zero.)

Thus we have that \( \Phi_w = \Phi_{w_1} \Phi_{w_2} \) with \( w_1 \in \mathcal{A}^+ \) and \( w_2 \in \mathcal{B}^+ \). But \( \Phi_{w_1} \neq 0 \) if and only if \( \Psi_{w_1} \neq 0 \) if and only if \( w_1 \in \mathcal{L} \). Likewise, \( \Phi_{w_2} \neq 0 \) if and only if \( w_2 \in \mathcal{L}_2 \). So \( \mathcal{L}(V, \Phi, v, P) \subset \mathcal{L}_1 \mathcal{L}_2 \).

On the other hand, if \( w = w_1 w_2 \) with \( w_1 \in \mathcal{L}_1 \) and \( w_2 \in \mathcal{L}_2 \) it is clear that \( \Phi_{w_1} \Phi_{w_2} \neq 0 \), hence \( w \in \mathcal{L}(V, \Phi, v, P) \).

Case 2: \( \epsilon \in \mathcal{L}_1 \) but \( \epsilon \notin \mathcal{L}_2 \).

In this case we use the matrices generated by the automaton that recognizes \( \mathcal{A}^* \mathcal{B}^+ \). Take \( v = v_1 \otimes v_2 \otimes [1, 0] \) and \( P = P_1 \otimes P_2 \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \). For \( a \in \mathcal{A} \), we take \( \Phi_a = \Psi_a \otimes \text{Id} \otimes \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \) and for \( b \in \mathcal{B} \) let \( \Phi_b = \text{Id} \otimes \Gamma_b \otimes \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \).

Case 3: \( \epsilon \notin \mathcal{L}_1 \) but \( \epsilon \in \mathcal{L}_2 \).

Take \( v = v_1 \otimes v_2 \otimes [1, 0] \) and \( P = P_1 \otimes P_2 \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \). For \( a \in \mathcal{A} \) let \( \Phi_a = \Psi_a \otimes \text{Id} \otimes \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \) and for \( b \in \mathcal{B} \) let \( \Phi_b = \text{Id} \otimes \Gamma_b \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \).
Case 4: \( \epsilon \in \mathcal{L}_1 \) and \( \epsilon \in \mathcal{L}_2 \)

Let \( v = v_1 \otimes v_2 \otimes [1, 1] \) and \( P = P_1 \otimes P_2 \otimes \text{Id} \). For each \( a \in \mathcal{A} \) take \( \Phi_a = \Psi_a \otimes \text{Id} \otimes \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \) and for \( b \in \mathcal{B} \) let \( \Phi_b = \text{Id} \otimes \Gamma_b \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \).

For ease of presentation we also want to allow for some zero moves which could correspond to restarting of the algorithm, feeding results into the parallel algorithm, or doing nothing at all.

**Definition 5.20.** A non-deterministic cocyclic automaton with zero moves is a 4-tuple \((V, \Phi, v, P)\) where \( V \) is a finite dimensional vector space. \( \Phi = (\Phi_w)_{w \in \mathcal{A} \cup \{\epsilon\}} \) such that \( \Phi_w \in \text{End}(V) \) for \( w \in \mathcal{A} \). \( \Phi_\epsilon \in \text{End}(V) \) such that \( \Phi_\epsilon^2 = \Phi_\epsilon \) and \( \text{Lin}(\text{Id}) \subset \Phi_\epsilon \). \( P \) is a projection, and \( v \in V \).

For any word \( w \in \mathcal{A}^* \) we say that \( w \) is accepted by the automaton \((V, \Phi, v, P)\) if there is some factorization \( w = w_1 \ldots w_t \), with each \( w_i \) is either an element of \( \mathcal{A} \) or the empty word \( \epsilon \), such that \( v \Phi_{w_1} \Phi_{w_2} \cdots \Phi_{w_t} P \neq 0 \). In particular, \( \epsilon \) is accepted if \( v \Phi_\epsilon P \neq 0 \).

Allowing for zero moves makes construction of automata more intuitive. Before applying this flexibility let us first see that these two types of non-deterministic automata recognize the same class of languages.

**Theorem 5.21.** A language \( \mathcal{L} \) is recognized by a non-deterministic cocyclic automaton if and only if it is recognized by a non-deterministic cocyclic automaton with zero moves.

**Proof.** First we note that any language recognized by a non-deterministic cocyclic automaton is recognized by non-deterministic cocyclic automaton with zero moves since the definitions coincide for \( \Phi_\epsilon = \text{Lin}(\text{Id}) \).
Now suppose that \( L \) is recognized by a non-deterministic cocyclic automaton with zero moves, \((V, \Phi, v, P)\). We will construct a non-deterministic cocyclic automaton that also recognizes \( L \). For \( a \in \mathcal{A} \), take \( \Psi_a := \text{Lin}(\Phi_a, \Phi_a \Phi_\epsilon, \Phi_\epsilon \Phi_a) \). Also take \( \Psi_\epsilon := (\text{Id}) \). Let \( V_0 := v \Phi_\epsilon \) be the initial subspace.

We now claim that \( L \) is recognized by \((V, \Psi, V_0, P)\) where \( \Psi \) is a cocycle. First, since \( V_0 P = 0 \) if and only if \( V_0 \text{Id} P = 0 \), it follows that \( \epsilon \) is recognized by \((V, \Psi, V_0, P)\) if and only if \( \epsilon \in L \). Now suppose that \( w \in L \) with \( w \neq \epsilon \). Then there is a factorization \( w = w_1 \ldots w_t \) such that \( V_0 \Phi_{w_1} \cdots \Phi_{w_t} P \neq 0 \) with \( w_i \in \mathcal{A} \cup \{\epsilon\} \). By grouping terms of the product together, we get a product of the form \( V_0 \Psi_{z_2} \cdots \Psi_{z_s} \), with \( w = z_1 \ldots z_s \) and \( z_i \in \mathcal{A} \) for each \( i \). Now \( V_0 \Phi_{w_1} \cdots \Phi_{w_t} P \subset V_0 \Psi_{z_1} \cdots \Psi_{z_s} P \) so \( w \) is accepted by \((V, \Psi, V_0, P)\), which is enough by Proposition 5.17.

On the other hand, let \( w \) be a non-empty word accepted by \((V, \Psi, V_0, P)\), then \( V_0 \Psi_w P \neq 0 \). But \( \Psi_w \) can be resolved into spaces \( \Phi_a \) multiplied by spaces corresponding to zero moves, thus there is some factorization \( w = w_1 \ldots w_t \) with \( w_i \in \mathcal{A} \cup \{\epsilon\} \) such that \( (v \Phi_\epsilon) \Phi_{w_1} \cdots \Phi_{w_t} P \neq 0 \), where \( V_0 = v \Phi_\epsilon \). Therefore \( w \in L \). We are now done since we have previously shown that a language is accepted by an automaton with initial subspace if and only if it is accepted by an automaton with an initial vector, see Proposition 5.17.

\[ \textbf{Theorem 5.22.} \] Suppose the language \( L \) is accepted by a non-deterministic cocyclic automaton, then \( L^* \) is accepted by a non-deterministic cocyclic automaton.

\[ \textbf{Proof.} \] Suppose \( L \) is accepted by automaton \((V, \Phi, v, P)\). We construct an automaton with zero moves that accepts \( L^* \). Since \( L^* \) contains \( \epsilon \) and \( (L \cup \{\epsilon\})^* = L^* \), we may assume without loss of generality that \( \epsilon \in L \). Thus we can assume that \( vP \neq 0 \). By assumption there are is a basis \( v_1, \ldots, v_n \) of \( V \) and \( t \in \{1, \ldots, n\} \) such that \( a_1 v_1 \oplus \cdots \oplus a_nv_n P = a_1 v_1 \oplus \cdots \oplus a_tv_t \) for some \( a_i \in \mathbb{C} \). For each \( i \in \{1, \ldots, n\} \), let
$T_i$ be the linear map which takes $v_i$ to the initial vector $v$ and every other element of the basis to 0. Now take $Φ = \text{Lin}(\text{Id}, PT_i)_{i \in \{1, \ldots, n\}}$.

We now show that $Φ^2 = Φ$. The only thing we really need to show here is that a product of the form $PT_iPT_j$ may be written as an element of $Φ$. We claim that $PT_iPT_j$ is just a constant multiple of the map $PT_j$. To see this first write the initial vector as $v = b_1v_1 \oplus \ldots \oplus b_nv_n$. Let $u = a_1v_1 \oplus \ldots \oplus a_nv_n$ be arbitrary, we have $uPT_j = (a_1v_1 \oplus \ldots \oplus a_tv_t)T_j = a_jv$. On the other hand, $uPT_iPT_j = a_i(b_1v_1 \oplus \ldots \oplus b_tv_t)T_j$ which gives $a_ib_jv$. So we have for arbitrary $u$, $uPT_iPT_j = b_j(a_iv) = b_j(uPT_i) = u(b_jPT_i)$. Where $b_j$ does not depend on $u$. Thus $PT_iPT_j ∈ Φ$. We have now shown that $(V, Φ, v, P)$ is a well defined non-deterministic cocyclic automaton with zero moves, call it $Q$.

We proceed to show that $L(Q) = L^*$. For $w ∈ A^*$ which is recognized by $(V, Ψ, v, P)$, we have a factorization $w = w_1 \ldots w_t$ and choice of $Γ_i ∈ Φ_{w_i}$ such that $vΓ_1Γ_2 \ldots Γ_tP \neq 0$ and for $w_i = ϕ$ we may choose $Γ_i ∈ \{ \text{Id}, PT_j \}_{j = 1, \ldots, n}$. Group the product $Γ_1 \ldots Γ_t$ into blocks separated by occurrences of $PT_j$ for some $j$. A word $w_{kk+1} \ldots w_{k+l}$ which corresponds to a block $Γ_kΓ_{k+1} \ldots Γ_{k+l}$ between successive occurrences of maps of the form $PT_j$ must be in $L$. Thus $w$ is a concatenation of words from $L$, hence $w ∈ L^*$.

On the other hand, if $w ∈ L^*$ then $w = w_1 \ldots w_t$ for some $w_i ∈ L$. It follows that $vΦ_{w_i}P \neq 0$ for each $i = 1, \ldots, t$. Furthermore there are maps $T_{w_i}$ such that $vΨ_{w_1}PT_{w_1}Ψ_{w_2}PT_{w_2} \ldots Ψ_{w_t}P \neq 0$ (by construction we choose $T_{w_i}$ to send a non-zero vector in the image of $Ψ_{w_i}P$ to the initial vector $v$, effectively restarting the automaton). Thus $w$ is recognized by the automaton $(V, Ψ, v, P)$.
The results in this section are interesting on their own, but they are also steps to showing that the class of generalized non-deterministic cocyclic languages makes up a Kleene algebra. (See [23] for more on Kleene Algebras.)

**Definition 5.23.** A Kleene Algebra is a set $K$ equipped with binary operations $+$ and $\cdot$, unary operation $\ast$, and constants 0 and 1 in $K$, such that

$$(K, +, \cdot, 0, 1)$$

is an idempotent semiring, i.e.,

(i) $+$ is associative, commutative, and idempotent ($a + a = a$) with identity 0;
(ii) $\cdot$ is associative with two-sided identity 1;
(iii) $\cdot$ distributes over $+$ on both sides;
(iv) 0 is a two-sided annihilator for $\cdot$;

and the operation $\ast$ satisfies the following properties:

(v) $1 + aa^* \leq a^*$,
(vi) $1 + a^*a \leq a^*$,
(vii) $ax \leq x \Rightarrow a^*x \leq x$,
(viii) $xa \leq x \Rightarrow xa^* \leq x$,

where $a \leq b \iff a + b = b$.

**Theorem 5.24.** Let $K$ be the collection of all non-deterministic cocyclic languages. For any $\alpha, \beta \in K$ let $\alpha + \beta := \alpha \cup \beta$. Take $\alpha \cdot \beta$ to be the concatenation $\alpha \beta$ and $\alpha^*$ to be the Kleene star. Let 0 := $\emptyset$ and 1 := \{\epsilon\}. With these definitions $(K, +, \cdot, 0, 1, \ast)$ is a Kleene algebra.

**Proof.** We have shown in Propositions 5.19, 5.16, and Theorem 5.22 that the operations $+$, $\cdot$, and $\ast$ do not lead out of the class of non-deterministic cocyclic languages. Now (i), (ii), and (iv) are true directly from the definitions. To see (iii)
write $\alpha \cdot (\beta + \gamma) = \{ w_1w_2 \in A^* \mid w_1 \in \alpha, w_2 \in \beta \cup \gamma \} = \{ w_1w_2 \in A^* \mid w_1 \in \alpha, w_2 \in \beta \} \cup \{ w_1w_2 \mid w_1 \in \alpha, w_2 \in \gamma \} = \alpha \beta + \alpha \gamma$. The distribution on the other side is similar. For (v) and (vi) we only observe that $aa^* = a^*a$ so that $1 + aa^* = a^* = 1 + a^*a$, so we are done by the definition of $\leq$.  

Cocyclic Languages and Subshifts

Suppose that $L = L(\Phi)$ is a language of a cocycle $\Phi$. We want to study the relationship between this language and the cocyclic subshift $X_\Phi$. In this section we consider one-sided subshifts. We make this change for ease of presentation.

**Proposition 5.25.** If the language of a cocycle $\Phi$, $L = L(\Phi)$, is factorial and extendable then $L$ is the language of the cocyclic subshift $X_\Phi$.

**Proof.** We know that $L = L(\Phi)$ being factorial and extendable imply that $L$ is the language of some subshift $X$. But this implies that the complement of $L$, $L^c = \{ w \in A^* \mid \Phi_w = 0 \}$ is a forbidden set for $X$, which means that $X_\Phi = X$.

**Proposition 5.26.** If $L = L(\Phi)$ with $\Phi$ a non-deterministic cocycle and $L$ is both factorial and extendable, then $L$ is the language of a factor of cocyclic subshift.

**Proof.** $L$ is extendable and factorial implies that there is a subshift $X$ such that $L(X) = L$. But this implies the complement of $L$, $L^c = \{ w \in A^* \mid \Phi_w = 0 \}$ is a forbidden set for $X$. This is equivalent to $X$ being a factor of a cocyclic subshift by Proposition 11.1 in [26].

For a cocyclic subshift $X$ we say that $X$ is well represented by a cocycle $\Phi$ if $L(X) = L(\Phi)$. Note that this is stronger than requiring $X = X_\Phi$. 


Example: Consider a cocyclic subshift with

\[
\Phi_1 := \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \Phi_2 := \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.
\]

\(X_\Phi = \{1^\infty\}\) so \(L(X_\Phi) = \{\epsilon, 1, 11, \ldots\}\). \(L(\Phi) = \{2, \epsilon, 1, 11, \ldots\}\).

Proposition 5.27. Let \(A\) be the algebra generated by a cocycle \(\Phi\), excluding \(\Phi_\epsilon\). If \(\text{Id} \in A\) then \(X_\Phi\) is well represented by \(\Phi\).

Proof. We always have \(L(X_\Phi) \subseteq L(\Phi)\) because \(w \in L(X_\Phi)\) implies \(\Phi_w \neq 0\) by the definition of \(X_\Phi\).

On the other hand, suppose \(w \in L(\Phi)\). Since \(\Phi_w \text{Id} \cdots \neq 0\), \(w\) occurs in \(X_\Phi\) by Lemma 4.3 (one-sided version). \(\square\)

Corollary 5.28. If \(\Phi\) is a cocycle whose algebra \(A\) contains the identity then the language of \(\Phi\), \(L(X_\Phi)\), is cocyclic.

Theorem 5.29. If \(L\) is the language of a cocyclic subshift satisfying (DD) then \(L\) is a cocyclic language.

Proof. Suppose \(L = L(X_\Phi)\) and that \(A\) is the algebra generated by the \(\Phi_a\) with \(a \in A\). (Note that \(\Phi_\epsilon\) is not included.) We have already dealt with the case when \(\text{Id} \in A\).

Suppose that \(\text{Id} \notin A\). Then let \(A^1\) be the smallest sub-algebra of \(\text{End}(V)\) containing both \(A\) and \(\text{Id}\). In \(A^1\) there is a decomposition of the identity \(\text{Id} = f_1 + \ldots f_q + f_{q+1} + \ldots + f_s\) into primitive idempotents (see Equation 4.4) with \(f_1, \ldots, f_q \in A\). Also \(X_{f_j A/f_j N} \neq \emptyset\) for \(1 \leq j \leq q\) and \(X_{f_j A/f_j N} = \emptyset\) for \(q + 1 \leq j \leq s\) (by Proposition 4.29).

Claim: A word \(w\) occurs in \(X_\Phi\) if and only if \(\Phi_w A f_i \neq 0\) for some \(1 \leq i \leq q\).

Suppose that \(\Phi_w A f_i \neq 0\), for some \(1 \leq i \leq q\). Then \(\Phi_w A f_i f_i \cdots \neq 0\). By Lemma 4.3, \(w\) occurs in \(X_\Phi\).
To prove \( \implies \) in the claim, suppose that \( w \) occurs in \( x = w \ldots \in X_\Phi \). Because \( \text{rad}(A) \) is nilpotent there exists \( k > |w| \) such that \( x_{[k,\infty]} \) contains no subwords \( v \) such that \( \Phi_v \in \text{rad}(A) \). Thus for \( l > k \), the cylinder set \([x_{[k,l]}] \) has non-empty intersection with \((X_\Phi)_+ \). Since there is positive distance between components, there exists \( l \) such that \([x_{[k,l]}] \) has non-empty intersection with exactly one Wedderburn component \( X_i = X_{f_iA/f_iN} \) for some \( 1 \leq i \leq q \). By Lemma 4.18, \( \Phi_wA f_i = 0 \) if and only if \( \Phi_wA \Phi_{x_{[k,l]}} \neq 0 \). \( \Phi_wA \Phi_{x_{[k,l]}} \neq 0 \) since \( x = w \ldots x_{[k,l]} \ldots \), hence \( \Phi_wA f_i \neq 0 \).

Now that the claim is established, we proceed to create the automaton recognizing the given language. Let \( \Phi_{w_1}, \Phi_{w_2}, \ldots, \Phi_{w_t} \) be a basis for the algebra \( A \) as a linear space. For each \( i \) and \( j \), we have the automaton \( Q_{i,j} = (V, \Phi, V_0, \Phi_{w_j f_i}) \) where \( V_0 := V \). By Proposition 5.17, there are cocyclic automata that recognize the same language as each \( L(Q_{i,j}) \). By the claim, a word \( w \) is in \( L \) if and only if it is in \( L(Q_{i,j}) \) for some \( i, j \). Thus \( L \) is the union of the languages \( L(Q_{i,j}) \) and is therefore cocyclic by Proposition 5.14. \( L \) is recognized by the automaton \( \bigoplus_{i,j} Q_{i,j} \)

**Theorem 5.30.** If \( L \) is a cocyclic language which is extendable and factorial, then it is the language of a cocyclic subshift.

**Proof.** Suppose that \( L = L(V, \Phi, v, P) \). We first find cocycle \( \Psi \) on vector space \( V' \) with \( L = L(V', \Psi, V', P') \). Define \( V' := \text{Lin}(\{v\Phi_\omega | \omega \in A^*\}) \). Now \( V' \subset V \) is a vector space which is invariant under \( \Phi \), so for any \( a \in A \) take \( \Psi_a := \Phi_a|_{V'} \).

Now consider \( w \in A^* \). If \( V'\Psi_wP = 0 \) then \( v\Phi_wP = 0 \). On the other hand, suppose \( v\Phi_wP = 0 \). We claim that \( V'\Phi_wP = 0 \). Otherwise, there would be some \( w_1 \) such that \( v\Phi_{w_1} \Phi_wP \neq 0 \). Which would imply that \( w_1 w \in L \). But \( L \) is factorial, thus \( w \in L \) and so \( v\Phi_wP \neq 0 \) contrary to the assumption.
Now that we know that $L = L(V', \Psi, V', P')$, the next step is to create a vector space $\hat{V}$, and cocycle $\Gamma$ such that $L = L(\hat{V}, \Gamma, \hat{V}, \text{Id})$, and then the theorem will follow from Proposition 5.17. Let $A$ be the algebra generated by the cocycle $\Psi$. Define $B := \{ x \in V' \mid xAP = 0 \}$, which is a subspace of $V'$. Also, for any $a \in A$ and $x \in B$, we have that $x\Psi_a \in B$ since $X\Psi_a AP \subset xAP = 0$ (by $x \in B$), so $x\Psi_a \in B$.

Claim: For any $w \in A^*$, $\Psi_w P \neq 0$ if and only if $\Psi_w AP \neq 0$.

We use the fact that the language is both extendable and factorial. If $\Psi_w P \neq 0$ then, by extendabilitility, there is some $a \in A$ so that $\Psi_w \Psi_a P \neq 0$. So $\Psi_w AP \neq 0$.

If $\Psi_w AP \neq 0$ then there is some $a \in A$ such that $\Psi_w \Psi_a P \neq 0$. But then $wa$ is in the language $L$ and by factoriality $w$ is also. Hence, $\Psi_w P \neq 0$. The claim follows.

Now define $\hat{V} := V'/B = \{ [x] \mid x \in V' \}$ where $x \sim y$ if and only if $(x - y)AP = 0$. Note $\hat{V}\Psi_w = 0$ if and only if $x\Psi_w \in B$ for all $x \in V'$. This holds if and only if $x\Psi_w AP = 0$ for all $x \in V'$, which is equivalent to the statement $\Psi_w AP = 0$. By the claim, this last statement is equivalent to $\Psi_w P = 0$. We have shown $\hat{V}\Psi_w = 0 \iff \Psi_w P = 0$.

For any $a \in A$ define $\Gamma_a = \Psi_a|_{\hat{V}}$. Now $w \in L$ if and only if $\Gamma_w \neq 0$ by the following,

$L = L(V, \Phi, v, P) = L(V', \Psi, V', P') = L(\hat{V}, \Gamma, \hat{V}, \text{Id})$

thus

$w \in L \iff \hat{V}\Gamma_w \text{Id} \neq 0 \iff \Gamma \neq 0,$

so $L = L(\Gamma)$ and by Proposition 5.25 we have $L(X_\Gamma) = L$.

Therefore, $L$ is the language of a cocycle and is extendable and factorial. By Proposition 5.25 $L$ is the language of a cocyclic subshift. 

We have already seen that every regular language is cocyclic. The proof of this statement provides a method of creating for any regular language a cocyclic automa-
ton recognizing the language. We now revisit our set of examples that relate to any Diophantine equation a cocyclic subshift. We alter portions of the proof of the Correspondence Theorem (Theorem 2.7) to prove the following result.

**Proposition 5.31.** Let \( D(x_1, \ldots, x_m) = 0 \) be a Diophantine equation. Let \( A = \{1, \ldots, m\} \) and for any word \( w \in A^* \) and \( a \in A \) define \( n_a(w) \) to be the number of times \( a \) occurs in \( w \). Then the language

\[
L = \{ w \in A^* | (n_1(w), \ldots, n_m(w)) \text{ is not a solution to } D = 0 \}
\]

is cocyclic.

**Proof.** Let \( v = D(x_1, \ldots, x_m) \) be the initial vector and define \( \Phi_i \) for \( i \in \{1, \ldots, m\} \) in the same way as in the proof of the Correspondence Theorem. Now, let \( P \) be the projection that is the identity on any constant polynomial and zero on non-constant monomials. Written as a matrix in our chosen basis \( C(D) \), \( P \) has a single 1 in the upper left corner and zeros elsewhere.

Now we claim that \( L = L(V, \Phi, v, P) \). This follows by observing that in our proof of the Correspondence Theorem, we proved that \( D(x_1, \ldots, x_m)\Phi_1^{n_1} \cdots \Phi_m^{n_m}\Phi_0 = 0 \) if and only if \((n_1, \ldots, n_m)\) is a solution to \( D = 0 \). In particular, we saw that the constant term of the product \( D(x_1, \ldots, x_m)\Phi_1^{n_1} \cdots \Phi_m^{n_m} \) is equal to \( D(n_1, \ldots, n_m) \), so that we get \( D(x_1, \ldots, x_m)\Phi_1^{n_1} \cdots \Phi_m^{n_m}P = 0 \) if and only if \( D(x_1, \ldots, x_m)\Phi_1^{n_1} \cdots \Phi_m^{n_m}\Phi_0 = 0 \). Recalling that the \( \Phi_a \) for \( a \in A \) are mutually commutative, this implies the result. \( \square \)
REFERENCES CITED


