Cocyclic Subshifts from Diophantine Equations

David Buhanan[1] and Jaroslaw Kwapisz[2]

[1]Department of Mathematics and Natural Sciences
Centenary College of New Jersey
Hackettstown NJ 07840
buhanand@centenarycollege.edu
[2]Department of Mathematical Sciences
Montana State University
Bozeman MT 59717-2400
jarek@math.montana.edu

October 23, 2013

Abstract

We give a method of constructing cocyclic subshifts from Diophantine equations. As an application, we produce examples of such subshifts that are not sofic and prove that the problem of equality of two cocyclic subshifts is algorithmically undecidable. This last result also follows from 1970 work by Paterson on mortality of matrices.

1 Introduction

Motivated by the Conley index for discrete dynamical systems, cocyclic subshifts are a very natural generalization of sofic systems, which include subshifts of finite type. The goal of this note is to make a connection between cocyclic subshifts and Diophanine equations and use it to prove undecidability of cocyclic subshifts and to generate non-trivial examples.

Taking $\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$ to be the non-negative integers, the *full shift* over a finite set $\mathcal{A}$ is the space $\mathcal{A}^{\mathbb{N}_0} = \{(x_i)_{i=0}^{\infty} : \ x_i \in \mathcal{A}\}$ of all infinite sequences indexed by $\mathbb{N}_0$ and drawn from $\mathcal{A}$. $\mathcal{A}^{\mathbb{N}_0}$ is acted upon by the *shift map* $f : \mathcal{A}^{\mathbb{N}_0} \to \mathcal{A}^{\mathbb{N}_0}$ sending (x_i) to (x_{i+1}). It is customary to refer to $\mathcal{A}$ as an *alphabet* and write the sequences $(x_i)_{i=0}^{\infty} \in \mathcal{A}^{\mathbb{N}_0}$ as infinite words $x_0x_1x_2\ldots$.

The full shift is the simplest model[1] of a *stochastic memoryless source* in information theory and of *deterministic chaos* in dynamical systems theory. (See e.g. [9] and [12].) In the study of chaotic iterated maps, the full shift also serves as a universal model since many such maps can be effectively coded by a *subshift* $Y \subset \mathcal{A}^{\mathbb{N}_0}$, i.e., a closed subset $Y \subset \mathcal{A}^{\mathbb{N}_0}$ that is left invariant by the shift, $f(Y) \subset Y$. (The hope here is that Y is easier to describe than the original system.) A class of subshifts prevalent in applications (at least for systems of positive entropy) is that of *subshifts of finite type*. These arise in the context of stochastic sources with finite memory or dynamical systems with *Markov partitions* and are characterized by existence of a finite subset F of the set $\mathcal{A}^*$ of all finite *words* (i.e. finite sequences) over the alphabet $\mathcal{A}$ such that the subshift is defined by forbidding the words in F,

$$X_F = \{x \in \mathcal{A}^{\mathbb{N}_0} : \ \ \omega \text{ does not occur in } x \text{ for all } \omega \in F\}. \tag{1}$$

Often used is a bit larger class of *sofic shifts*; these are the subshifts of finite type and their images under *coding*, i.e., a shift commuting map onto another subshift. Given a subshift $X \subset \mathcal{A}^{\mathbb{N}_0}$, one can tell if it is sofic based on its language

$$\mathcal{L}(X) = \{\omega \in \mathcal{A}^* : \ \ \omega \text{ is a word that occurs in } x \text{ for some } x \in X\}. \tag{2}$$

Specifically, there has to be only finitely many *follower sets*, i.e., as ν varies over $\mathcal{L}(X)$, there are only finitely many possibilities for the sets

$$\mathcal{F}_X(\nu) := \{\omega \in \mathcal{A}^* : \ \nu\omega \in \mathcal{L}(X)\}. \tag{3}$$

We note that any subshift of finite type or sofic system can be recoded as an *edge shift* $X_{\mathcal{G}}$ associated to a finite directed graph $\mathcal{G}$ with edges labeled by the letters from $\mathcal{A}$,

$$X_{\mathcal{G}} = \{x \in \mathcal{A}^{\mathbb{N}_0} : \ x \text{ is the sequence of labels along an infinite path in } \mathcal{G}\}. \tag{4}$$

(For a proof and a more complete introduction to subshifts see [15].)

[1] Once equipped with a Bernoulli probability measure, but we skirt probabilistic aspects here.

Cocyclic subshifts [13] are motivated by a less well known but very powerful coding technique (see [23], but also [22] and the references therein) based on the *cohomological Conley index* [17, 8]. They generalize sofic subshifts and are of the form

$$X_\Phi := \{(x_k)_{k\in\mathbb{N}_0} : \ \forall_{n\in\mathbb{N}_0}\ \Phi_{x_0}\Phi_{x_1}\cdots\Phi_{x_n} \neq 0\}$$

where Φ stands for a family of $m := \#\mathcal{A}$ square matrices indexed by $\mathcal{A}$, $\Phi = (\Phi_a)_{a\in\mathcal{A}}$, the product is taken using the matrix multiplication, and 0 is the zero matrix. As a shorthand, we refer to Φ as a *cocycle* — this is motivated in [13]. (Note that if all Φ_a are non-singular X_Φ is the full shift.) For the purpose of this note, we restrict to Φ_a with integer entries, the simplest setting in which interesting cocyclic subshifts appear and what is needed for the Conley index applications.

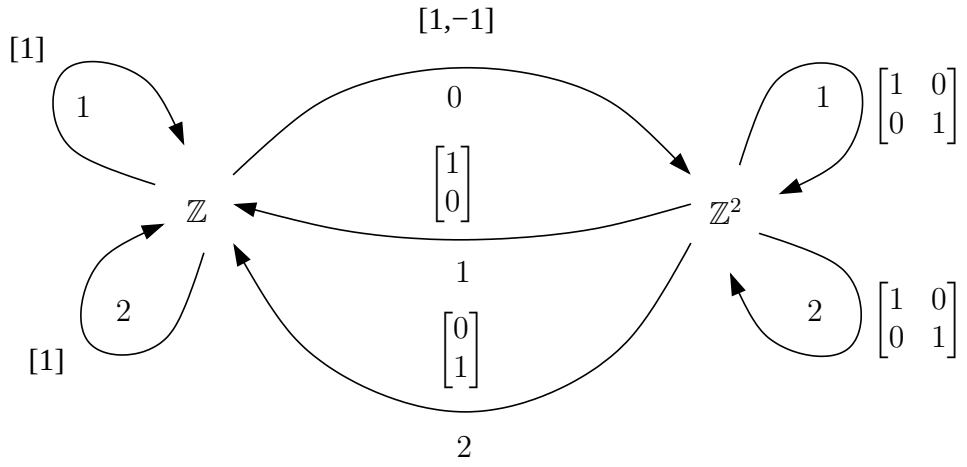

Figure 1.1: Graph with propagation corresponding to the cocycle given by equation (6). Each edge is labeled by a symbol from the alphabet $\{0, 1, 2\}$ and a matrix (in the square brackets). The associated cocyclic subshift consists of the infinite sequences of symbols that are read off those infinite paths in the graph for which the corresponding infinite product of matrices is non-vanishing, i.e., no finite partial product is zero.

Example: Take $\mathcal{A} = \{0, 1, 2\}$. The subshift X_F with the forbidden word set

$$F := \{0\omega 0 : \ \omega \text{ equals } 1^n 2^n \text{ up to permutation of letters for some } n \in \mathbb{N}_0\} \tag{5}$$

is a cocyclic subshift because $X_F = X_\Phi$ where

$$\Phi_0 := \left[\begin{array}{c|cc} 0 & 1 & -1 \\ \hline 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right], \quad \Phi_1 := \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 1 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right], \quad \Phi_2 := \left[\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 1 & 0 \\ 1 & 0 & 1 \end{array}\right]. \tag{6}$$

To show the equality $X_F = X_\Phi$, one has to check that the products

$$\Phi_\omega := \Phi_{\omega_1}\ldots\Phi_{\omega_n} \quad (\omega_1, \ldots, \omega_n \in \mathcal{A}) \tag{7}$$

vanish iff the word ω contains a subword in the set F. An instructive way of verifying this is by thinking of matrices Φ_a as acting on the row vectors in $\mathbb{Z}^3 = \mathbb{Z} \oplus \mathbb{Z}^2$ by multiplication on the right and considering diagram in Figure 1.1, an example of a *labeled graph with propagation* [13, 14].
For instance, to see that $\Phi_{01^m2^n0} = 0$ iff $m = n$, let us compute $(1 \oplus v_2)\Phi_{01^m2^n0}$ for an arbitrary $v_2 \in \mathbb{Z}^2$. Think of 1 placed in the vertex $\mathbb{Z}$ and v_2 in the vertex $\mathbb{Z}^2$. To get $(1 \oplus v_2)\Phi_0$, move 1 and v_2 along each edge labeled 0 (if any) while multiplying (on the right) by the matrix over that edge. This yields 0 in $\mathbb{Z}$ and $(1, -1)$ in $\mathbb{Z}^2$, i.e. $0 \oplus (1, -1)$. Now, m-applications of Φ_1 yield $(1 \oplus v_2)\Phi_{01^m} = m \oplus (1, -1)$. (The vectors arriving at a vertex are added.) The subsequent n-applications of Φ_2 yield $(1 \oplus v_2)\Phi_{01^m2^n} = m - n \oplus (1, -1)$. Applying the final Φ_0 yields $(1 \oplus v_2)\Phi_{01^m2^n0} = 0 \oplus (m - n)(1, -1)$, which vanishes iff $m = n$.

Looking back at the example, we have two points to make. One is that X_Φ is a subset of the edge shift $X_\mathcal{G}$ where the graph $\mathcal{G}$ is obtained by forgetting the matrices over the edges. The second is that X_Φ would have coincided with $X_\mathcal{G}$ (and thus equal $\{x \in \{0, 1, 2\}^{\mathbb{N}_0} : \ 00 \text{ does not occur in } x\}$) if not for the minus sign in Φ_0. Not only are the two subshifts not equal but, by inspecting the follower sets, one can see that the example is *strictly cocyclic*, i.e., it is not sofic (as it also follows from Theorem 3.1 ahead).

Generally, X_Φ is sofic (and thus trivial from our standpoint) if the matrix entries in Φ are all non-negative or in a finite ring [13]. It takes the infinite cardinality of $\mathbb{Z}$ and cancellations in the products Φ_ω to produce strict cocyclicity.

Our main objective is to give a systematic method of constructing strictly cocyclic subshifts and increase the scope of such known examples from one [13] to infinitely many; see the examples in Section 3. The construction associates a cocycle to a *Diophantine equation*, by which we understand an equation $D = 0$ where $D = D(z_1, \ldots, z_m)$ is a non-zero polynomial in variables $z_1, \ldots, z_m$ with integer coefficients. The *solution set* of $D = 0$ is $\{(a_1, \ldots, a_m) \in {\mathbb{N}_0}^m : \ D(a_1, \ldots, a_m) = 0\}$.

Theorem 1.1 (Correspondence)**.** *Suppose $D = 0$ is a Diophantine equation.*
(i) The subshift over the alphabet $\mathcal{A} = \{0, \ldots, m\}$ with the forbidden set

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

is a cocyclic subshift. We denote it by X_D.
(ii) X_D is irreducible, i.e., $\forall_{\nu,\,\mu \in \mathcal{L}(X_D)}\ \exists_{\gamma \in \mathcal{L}(X_D)}\ \nu\gamma\mu \in \mathcal{L}(X_D)$.
(iii) Diophantine equations with distinct solution sets yield distinct subshifts.

Recall that irreducibility of a subshift X is equivalent to topological transitivity of the shift map restricted to X (see [15]).

The proof (in Section 2) is inspired by [1] and starts with a simple idea that the substitution $z_i \mapsto z_i+1$ induces a linear transformation on the space of all Diophantine equations. In Section 3 we show (by identifying infinitely many distinct follower sets) that the subshift is strictly cocyclic if the Diophantine equation is non-trivial in a

suitable sense (see Theorem 3.1). This is already so in the case of our initial example obtained from a rather unimpressive equation $z_1 - z_2 = 0$.

As an important corollary we obtain that cocyclic subshifts are undecidable:

Theorem 1.2 (Undecidability)**.** *The question of equality of two cocyclic subshifts is algorithmically undecidable. In fact, there is no algorithm, taking a cocycle Φ as its input, that can decide if the associated cocyclic subshift X_Φ is equal to the full shift $\mathcal{A}^{\mathbb{N}_0}$. Moreover, this undecidability property holds even when one restricts to Φ over the alphabet $\mathcal{A}$ with just two symbols.*

Above, saying that a question is *algorithmically undecidable* or there is no *algorithm that can decide it* means that there is no Turing machine which can resolve the question in finite time. (See [16] for a general discussion of those concepts.) Of course, one can list all the possible words over $\mathcal{A}$ as a sequence $\omega^{(1)}, \omega^{(2)}, \ldots$ and design a simple Turing machine taking Φ as the input and computing $\Phi_{\omega^{(i)}}$ for $i = 1, 2, 3, \ldots$ with an instruction to stop and output the message "$X_\Phi \neq \mathcal{A}^{\mathbb{N}_0}$" when $\Phi_{\omega^{(i)}} = 0$. The machine will halt if and only if $X_\Phi \neq \mathcal{A}^{\mathbb{N}_0}$ but it will run forever if $X_\Phi = \mathcal{A}^{\mathbb{N}_0}$. The theorem asserts that there is no clever way of tweaking the machine so that it will always stop and output the accurate verdict, "$X_\Phi \neq \mathcal{A}^{\mathbb{N}_0}$" or "$X_\Phi = \mathcal{A}^{\mathbb{N}_0}$".

This situation puts cocyclic subshift in stark contrast with irreducible sofic systems, which are decidable via the formalism of *right Fisher covers* [15]. Because the full shift is not isomorphic to any of its (proper) subshifts[2], the theorem also implies that the question of isomorphism of two cocyclic subshifts is undecidable as well. (This is conjectured to be already so for subshifts of finite type, see e.g. [7].)

From the applied point of view, undecidability of cocyclic subshifts places a limit on what can be expected from Conley index based algorithms for analysis of smooth dynamical systems, see e.g. [18]. (One should not despair, for many important questions that require only "approximate knowledge" of X_Φ are algorithmically decidable.)

Our proof of Theorem 1.2 (in Section 4) amounts to observing that the cocyclic subshift associated to the Diophantine equation as in Theorem 1.1 is a proper subset of the full shift iff the equation has a solution in non-negative integers. By the celebrated solution to Hilbert's Tenth Problem (by the cumulative effort of Davis, Putnam, Robinson, and Matijasevich) existence of such a solution is algorithmically undecidable (see [16, 6]). A little more work is required to convert the cocycle to one over two symbols, as needed for the "moreover part" of the theorem.

For more perspective, we note that a version of Gödel's Incompleteness Theorem says that given an axiomatization of number theory there are Diophantine equations for which the existence of a solution is also *logically undecidable*: whether it is true or false cannot be proven (see [6]). Therefore, there are Φ with the same logical undecidability of the equality $X_\Phi = \mathcal{A}^{\mathbb{N}_0}$.

We do not take credit for Theorem 1.2 as we discovered that it is also a corollary of much earlier work of Paterson on undecidability of the mortality problem for products

[2] "Isomorphic" refers to a conjugacy by an invertible sliding block code. Proper subshifts have fewer periodic orbits so cannot be conjugated to the full shift.

of 3×3 matrices [20]. Paterson's approach rests on encoding by matrix products the instances of *Post Correspondence Problem* [21]. (For more dicussion see [3] and also [10].) The advantage of our approach may be only cultural: we connect cocyclic subshifts with a more extensively studied subject of Diophantine equations.

2 Proof of Correspondence Theorem

We now give a proof of Theorem 1.1. Fix a non-zero polynomial D in m variables $z_1, \ldots, z_m$ with integer coefficients. D is a linear combination of *monomials*, i.e., terms of the form $z_1^{d_1} \cdots z_m^{d_m}$ where $d_j \in \mathbb{N}_0$; and we set

$$C(D) := \{p : \ p \text{ is a monomial that divides a monomial of } D\}.$$

Note that $C(D)$ contains at least the zero degree monomial 1. We order $C(D)$, say, lexicographically by declaring that $1 \prec z_i \prec z_j$ for $i < j$. Take V_D to be the free $\mathbb{Z}$-module generated by $C(D)$, that is

$$V_D := \{\text{a linear combination with integer coefficients of monomials in } C(D)\}\,.$$

To give an example, for $D(z_1, z_2) = {z_1}^2 + z_2 - z_1 z_2 + 1$ we would have $C(D) = (1, z_1, {z_1}^2, z_1 z_2, z_2)$ and $V_D = \{u_0 + u_1 z_1 + u_2 {z_1}^2 + u_3 z_1 z_2 + u_4 z_2 : \ u_i \in \mathbb{Z}\}$.

Now, for each $i = 1, 2, ..., m$, the substitutution $z_i \mapsto z_i + 1$ induces a homomorphism of the polynomial ring $\mathbb{Z}[z_1, \ldots, z_m]$ that transforms a monomial into a linear combination of monomials that are its divisors. Thus the homomorphism maps V_D to itself and we denote by $\phi_i : V_D \to V_D$ its restriction to V_D. Furthermore, let $\phi_0 : V_D \to V_D$ send any $u \in V_D$ to the multiple of its zero degree coefficient by D, i.e.,

$$\phi_0 : u_0 + u_1 z_1 + \ldots \ \mapsto \ u_0 D(z_1, \ldots, z_m).$$

By using the ordered basis $C(D)$ of V_D, each ϕ_i is represented by an integer valued matrix denoted Φ_i. Recall that we consider matrices acting on the right on the row vectors and thus also compose maps on the right, e.g., ϕ_1 followed by ϕ_2 applied to u would be $u\phi_1\phi_2$.

In our example, the ϕ_i and Φ_i are as follows

$$\begin{aligned}
&\phi_0 : 1 \mapsto 1 + z_1^2 - z_1 z_2 + z_2, \text{ and } \phi_0 \text{ is 0 on other basis elements,}\\
&\phi_1 : 1 \mapsto 1, \ z_1 \mapsto z_1 + 1, \ {z_1}^2 \mapsto {z_1}^2 + 2z_1 + 1, \ z_1 z_2 \mapsto z_1 z_2 + z_2, \ z_2 \mapsto z_2,\\
&\phi_2 : 1 \mapsto 1, \ z_1 \mapsto z_1, \ {z_1}^2 \mapsto {z_1}^2, \ z_1 z_2 \mapsto z_1 + z_1 z_2, \ z_2 \mapsto z_2 + 1,
\end{aligned}$$

$$\Phi_0 = \begin{bmatrix} 1 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \qquad \Phi_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \qquad \Phi_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Let $F := F_D$ be the subset of the set $\mathcal{A}^*$ of all words over $\mathcal{A}$ as given by the formulation of Theorem 1.1. The main assertion (i) of the theorem is established once we prove the following claim.

Claim 2.1. *For $\sigma \in \mathcal{A}^*$, we have $\Phi_\sigma = 0$ iff σ has a subword in F.*

Proof of Claim 2.1: ($\Leftarrow$) Suppose that $\sigma \in \mathcal{A}^*$ has a subword $0\omega 0$ where ω is a permutation of $1^{a_1}2^{a_2}\dots m^{a_m}$ and $(a_1, ..., a_m)$ is a solution to $D(z_1, ..., z_m) = 0$. We have to show that $\phi_{0\omega 0} = 0$, as then of course $\Phi_{0\omega 0} = 0$ and thus also $\Phi_\sigma = 0$. Because ϕ_i commute with each other for $i = 1, \dots, m$, $\phi_{0\omega 0}$ coincides with the composition $\phi_0\phi_1^{a_1}...\phi_m^{a_m}\phi_0$, which we presently examine applied to an arbitrary $u = u_0 + u_1 z_1 + \dots \in V_D$. (As usual, ϕ_i^0 is taken to be the identity homomorphism.)

We have $u\phi_0 = u_0 D(z_1, ..., z_m)$, and subsequent appliction of the substitutions $\phi_1^{a_1}...\phi_m^{a_m}$ yields $u_0 D(z_1 + a_1, ..., z_m + a_m)$. The final projection ϕ_0 returns $u_0 D(a_1, ..., a_m)D(z_1, ..., z_m)$, which is 0 by the asumption on the a_i. By the arbitrariness of $u \in V_D$, $\phi_0\phi_1^{a_1}...\phi_m^{a_m}\phi_0 = 0$.

($\Rightarrow$) Suppose that $\sigma \in \mathcal{A}^*$ has no subword in F. We have to show $\phi_\sigma \neq 0$. First note that, for any $\omega \in \mathcal{A}^*$, if $\phi_\omega \neq 0$ then $\phi_{i\omega j} \neq 0$ for any $i, j = 1, \dots, m$ because ϕ_i, ϕ_j are invertible. We can consider then only σ that begins and ends with 0.

We factor σ as follows

$$\omega = 0^{t_1}\nu_1 0^{t_2}\nu_2 0^{t_3}\dots 0^{t_k}\nu_k 0^{t_{k+1}}$$

where $t_i \geq 1$ and each ν_i is a permutation of a word of the form $1^{a_1^{(i)}}\dots m^{a_m^{(i)}}$ with $a_k^{(i)} \in \mathbb{N}_0$. By our hypothesis on σ, we have $D(a_1^{(i)}, \dots, a_m^{(i)}) \neq 0$.

Let us examine the image of V_D under $\phi_\sigma = \phi_{0^{t_1}}\phi_{\nu_1 0^{t_2}}\dots\phi_{\nu_k 0^{t_{k+1}}}$. Application of $\phi_{0^{t_1}}$ to V_D collapses it into a subgroup generated by a multiple of $D(z_1, ..., z_m)$,

$$V_D\phi_{0^{t_1}} = \mathbb{Z}D(z_1, ..., z_m)\phi_{0^{t_1-1}} = \mathbb{Z}u_0^{t_1-1}D(z_1, ..., z_m)$$

where $u_0 := D(0, \dots, 0)$. Application of $\phi_{\nu_1 0^{t_2}}$ to $D(z_1, ..., z_m)$ yields

$$\begin{aligned} D(z_1, \dots, z_m)\phi_{\nu_1}\phi_0^{t_2} &= D(z_1 + a_1^{(1)}, \dots, z_m + a_m^{(1)})\phi_0^{t_2} \\ &= D(a_1^{(1)}, \dots, a_m^{(1)})D(z_1, ..., z_m)\phi_0^{t_2-1} \\ &= D(a_1^{(1)}, \dots, a_m^{(1)})u_0^{t_2-1}D(z_1, ..., z_m). \end{aligned}$$

Subsequent application of $\phi_{\nu_2 0^{t_3}}, \dots \phi_{\nu_k 0^{t_{k+1}}}$ has an analogous effect and we get

$$\begin{aligned} V_D\phi_\sigma &= \mathbb{Z}u_0^{t_1-1}D(a_1^{(1)}, \dots, a_m^{(1)})u_0^{t_2-1}\cdots D(a_1^{(k)}, \dots, a_m^{(k)})u_0^{t_{k+1}-1}D(z_1, ..., z_m) \\ &= \mathbb{Z}D(a_1^{(1)}, \dots, a_m^{(1)})\cdots D(a_1^{(k)}, \dots, a_m^{(k)})u_0^{t_1-1+\dots+t_{k+1}-1}D(z_1, ..., z_m). \end{aligned} \tag{8}$$

We see that if $u_0 \neq 0$ then $V_D\phi_\sigma \neq 0$ because each factor $D(a_1^{(i)}, \dots, a_m^{(i)}) \neq 0$. If $u_0 = 0$ then the word 00 is in F and thus never occurs in σ so that $t_i = 1$ for all i and we still get a non-zero image

$$V_D\phi_\sigma = \mathbb{Z}D(a_1^{(1)}, \dots, a_m^{(1)})\cdots D(a_1^{(k)}, \dots, a_m^{(k)})D(z_1, ..., z_m) \neq 0.$$

We have shown that $\phi_\sigma \neq 0$. $\square$

Now that (i) is established we turn to (ii).

Claim 2.2. *For any $\nu, \mu \in \mathcal{A}^*$ with $\Phi_\nu, \Phi_\mu \neq 0$, there is $\gamma \in \mathcal{A}^*$ such that $\Phi_{\nu\gamma\mu} \neq 0$.*

Observe that repeated application of the claim allows one to extend any word ν with $\Phi_\nu \neq 0$ to an infinite word $x \in X_\Phi$. As a result,

$$\mathcal{L}(X_D) = \{\nu \in \mathcal{A}^* : \ \Phi_\nu \neq 0\}.$$

In particular, (ii) coincides with the claim.

Proof of Claim 2.2: Write $\nu = \nu_1 0^k \nu_2$ and $\mu = \mu_1 0^l \mu_2$ where $k, l \geq 0$ and ν_1 does not end with 0, ν_2 and μ_1 do not contain 0, and μ_2 does not begin with 0. (Here k, l may be zero and some of the words ν_i and μ_i may be empty.) Absence of 0 in ν_2 and μ_1 means that $\phi_{\nu_2} = \phi_1^{a_1} \cdots \phi_m^{a_m}$ and $\phi_{\mu_1} = \phi_1^{b_1} \cdots \phi_m^{b_m}$ for some $a_i, b_i \in \mathbb{N}_0$.

Because D is not constant equal to zero, there is $(c_1, \ldots, c_m) \in {\mathbb{N}_0}^m$ such that $D(c_1, \ldots, c_m) \neq 0$ and $c_i > a_i + b_i$ for $i = 1, \ldots, m$. We claim that $\phi_{\nu\gamma\mu} \neq 0$ for $\gamma = 1^{c_1-(a_1+b_1)} \ldots m^{c_m-(a_m+b_m)}$.

Indeed, should $\phi_{\nu\gamma\mu} = 0$, $\nu\gamma\mu$ would have a subword of the form $0\omega 0$ where $\omega = 1^{d_1} \cdots m^{d_m}$ with $D(d_1, \ldots, d_m) = 0$ (see Claim 2.1). By constuction of γ, $0\omega 0$ would have to be a subword of ν or μ, contrary to $\phi_\nu, \phi_\mu \neq 0$. $\square$

It remains to attend to (iii) of Theorem 1.1. If $D = 0$ and $D' = 0$ have different solution sets, say $D'(a_1, \ldots, a_m) = 0$ and $D(a_1, \ldots, a_m) \neq 0$ for some $(a_1, \ldots, a_m) \in \mathbb{N}_0$, then $01^{a_1} \ldots m^{a_m} 0^\infty$ belongs X_D but not to $X_{D'}$, so $X_D \neq X_{D'}$.

3 Strictly Cocyclic Subshifts

The goal of this section is to produce subshifts that are strictly cocyclic (i.e. cocyclic but not sofic). For $i \in \{1, \ldots, m\}$, we say that a Diophantine equation $D(z_1, \ldots, z_m) = 0$ is *degenerate* in the variable z_i iff there are $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_m \in \mathbb{N}_0$ such that $D(b_1, \ldots, b_{i-1}, z_i, b_{i+1}, \ldots, b_n)$ is identically zero as a function of z_i. A Diophantine equation is said to be *non-degenerate* if it is not degenerate in z_i for any i.

Theorem 3.1. *Suppose that a Diophantine equation $D(z_1, \ldots, z_m) = 0$ is non-degenerate and has infinitely many solutions in ${\mathbb{N}_0}^m$, then the cocyclic subshift X_D associated to D (as in Theorem 1.1) is strictly cocyclic.*

Verifying if $D(z_1, \ldots, z_m) = 0$ is degenerate, say in z_m, amounts to writing D as an element of $\mathbb{Z}[z_1, \ldots, z_{m-1}][z_m]$, i.e., as $D = a_d z_m^d + \ldots + a_0$ where a_k are polynomials in $z_1, \ldots, z_{m-1}$, and checking if the system of $d+1$ Diophantine equations $a_k = 0$, $k = 0, \ldots, d$, has a solution in ${\mathbb{N}_0}^{m-1}$. This is generally as hard as solving any single Diophantine equation in $z_1, \ldots, z_{m-1}$. The situation gets easier when $m = 2$, as then the system consists of polynomials in one variable and can be solved algorithmically

by applying the rational root theorem [11]. Also, $D(z_1, z_2) = 0$ is non-degenerate if $D(z_1, z_2)$ is *irreducible* in $\mathbb{Z}[z_1, z_2]$, i.e., it cannot be written as the product of two non-trivial polynomials in $\mathbb{Z}[z_1, z_2]$. (Indeed, if $z_1 = b$ solves the system $a_k = 0$, then D is dvisible by $z_1 - b$.) For instance, $z_1(z_2^2 + 1) = 0$ is degenerate in z_2 and $z_1 - z_2 = 0$ is non-degenerate.

We can combine Theorems 3.1 and 1.1 to give perhaps the simplest infinite family of distinct strictly cocyclic subshifts.

Example: For a pair of coprime natural numbers (p, q), set $D_{p/q} := pz_2 - qz_1$. The subshifts $X_{D_{p/q}}$ are strictly cocyclic and pairwise distinct.

There is a multitude of other non-degenerate Diophantine equations with infinitely many solutions, including more complicated linear equations and families of quadratic and higher degree equations; see Chapter 6 of [5] or [19]. Two classical examples are the Pythagorean equation $z_1^2 + z_2^2 = z_3^2$ and Pell's equation $z_1^2 - nz_2^2 = \pm 1$ where n is a non-square integer.

Proof of Theorem 3.1: By our discussion in the introduction, it sufices to show that if $D = 0$ is non-degenerate and with infinitely many solutions then $X := X_D$ has infinitely many distinct follower sets.

Since $D = 0$ has infinitely many solutions there is an index i such that the coordinate z_i takes infinitely many values on the solution set $\{(z_1, \ldots, z_m) \in {\mathbb{N}_0}^m : D(z_1, \ldots, z_m) = 0\}$. We may well assume that $i = 1$ and that the values of z_1 are $a_k \nearrow \infty$ (as $k \to \infty$). Consider the non-empty sets

$$A_k := \{(b_2, \ldots, b_m) \in {\mathbb{N}_0}^{m-1} : \ D(a_k, b_2, \ldots, b_m) = 0\}.$$

By the assumption that $D = 0$ is non-degenerate, any $(b_2, \ldots, b_m) \in {\mathbb{N}_0}^{m-1}$ belongs to finitely many A_k (as otherwise $D(z_1, b_2, \ldots, b_n) = 0$ would be a polynomial equation in the variable z_1 with infinitely many solutions, making $D(z_1, b_2, \ldots, b_n) \equiv 0$). Thus there is some infinite sequence $(k_l)_{l=1}^{\infty}$ such that the sets in the sequence $(A_{k_l})_{l=1}^{\infty}$ are pairwise distinct.

To identify infinitely many follower sets, we claim that

$$\mathcal{F}_X(01^{a_{k_l}}) \neq \mathcal{F}_X(01^{a_{k_{l'}}}) \quad \text{for } l \neq l'.$$

Indeed, $l \neq l'$ gives $A_{k_l} \neq A_{k_{l'}}$ guaranteeing $(b_2, \ldots, b_m) \in {\mathbb{N}_0}^{m-1}$ such that $D(a_{k_l}, b_2, \ldots, b_m) = 0$ and $D(a_{k_{l'}}, b_2, \ldots, b_m) \neq 0$. By the definition of the forbidden set F_D, $01^{a_{k_l}} 2^{b_2} \ldots m^{b_m} 0$ does not belong to the language $\mathcal{L}(X)$. However, $01^{a_{k_{l'}}} 2^{b_2} \ldots m^{b_m} 0$ belongs to $\mathcal{L}(X)$ by virtue of $01^{a_{k'_l}} 2^{b_2} \ldots m^{b_m} 01^{\infty} \in X$. Hence, $2^{b_2} \ldots m^{b_m} 0 \notin \mathcal{F}_X(01^{a_{k_l}})$ and $2^{b_2} \ldots m^{b_m} 0 \in \mathcal{F}_X(01^{a_{k_{l'}}})$, showing that the two follower sets are distinct. $\square$

4 Proof of Undecidability Theorem

We now prove Theorem 1.2 by showing that, given a cocycle Φ, one cannot algorithmically decide if $X_\Phi = \mathcal{A}^{\mathbb{N}_0}$. Because existence of a solution to a Diophantine

equation is algorithmically undecidable, it suffices to associate to a Diophantine equation $D(x_1, \ldots, x_m) = 0$ a cocycle Φ so that the equation has a solution iff $X_\Phi \neq \mathcal{A}^{\mathbb{N}_0}$. This is exactly so for the cocycle $\Phi = (\Phi_i)_{i=0}^m$ provided by Theorem 1.1. However, the number of symbols in the alphabet $\mathcal{A}$ is $m+1$ and thus depends on D. To prove the "moreover" part of the theorem it remains to show how one can pass from Φ to another cocycle $\Phi' = (\Phi'_i)_{i=1}^2$ so that $X_\Phi \neq \mathcal{A}^{\mathbb{N}_0}$ iff $X_{\Phi'} \neq \{1,2\}^{\mathbb{N}_0}$.

We use a rather natural construction combining the direct sum of the Φ_i with cyclic permutation of the components, as found in [4, 2]. To simplify notations Φ'_1 and Φ'_2 will be denoted by A and B, respectively, where A and B are the following block matrices

$$A := \begin{bmatrix} \Phi_0 & 0 & \ldots & 0 \\ 0 & \Phi_1 & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \Phi_m \end{bmatrix} \quad \text{and} \quad B := \begin{bmatrix} 0 & 0 & \cdots & 0 & I \\ I & 0 & 0 & \cdots & 0 \\ 0 & I & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & I & 0 \end{bmatrix}.$$

(Above I is the $n \times n$ identity matrix where n is the common size of the matrices Φ_i.) It is convenient to introduce, for $0 \leq i \leq m$, the matrices

$$C_i := B^{m+1-i} A B^i.$$

Since B^{m+1} is the identity, denoted by $\mathbf{I}$, we have that C_i is the result of conjugating C_{i-1} via B, $C_i = B^{-i} A B^i = B^{-1} C_{i-1} B$. Conjugating by B cyclicly permutes the diagonal blocks, and the C_i is readily seen to be block-diagonal with the blocks as follows,

$$C_i = \operatorname{diag}(\Phi_i, \ldots, \Phi_m, \Phi_0, \ldots, \Phi_{i-1}).$$

Now, suppose that $X_{\Phi'} \neq \{1,2\}^{\mathbb{N}_0}$, i.e., some matrix product made of finitely many copies of A and B is zero. By using again the relation $B^{m+1} = \mathbf{I}$, this product can be written in the form

$$B^t C_{i_1} C_{i_2} \cdots C_{i_l} = 0$$

for some $l \geq 0$ and $i_j \in \{0, \ldots, m\}$. (This is done by a simple induction on the number of A in the product: If the product contains A then its tail end starting at the last A is AB^i for some $i \in \{0, \ldots, m\}$, and we can rewrite the product as $\ldots C_i$ where the "dots" are hiding a product with fewer A.) B being invertible, we have $C_{i_1} C_{i_2} \cdots C_{i_l} = 0$ and thus also $\Phi_{i_1} \cdots \Phi_{i_l} = 0$, as this is the block in the upper left corner of $C_{i_1} \cdots C_{i_l}$. Hence $X_\Phi \neq \mathcal{A}^{\mathbb{N}_0}$.

On the other hand, suppose that $X_\Phi \neq \mathcal{A}^{\mathbb{N}_0}$, i.e., $\Phi_{i_1} \cdots \Phi_{i_l} = 0$ for some $i_j \in \{0, \ldots, m\}$. Observe that, for $k = 0, \ldots, m-1$, doing the subtraction in the indices modulo $m+1$, we have that $C_{i_1-k} \cdots C_{i_l-k}$ is a block-diagonal matrix with the k-th diagonal block equal to $\Phi_{i_1} \cdots \Phi_{i_l} = 0$. (We do not care what other diagonal blocks are.) We have then

$$(C_{i_1} \cdots C_{i_l})(C_{i_1-1} \cdots C_{i_l-1}) \ldots (C_{i_1-m+1} \cdots C_{i_l-m+1}) = 0$$

since the product is block-diagonal with the zero factor in every block. It remains to express each C_i above back in terms of A and B to get a vanishing product of finitely many copies of A and B. As $\Phi' = (A, B)$, we have $X_{\Phi'} \neq \{1, 2\}^{\mathbb{N}_0}$.

5 Appendix : exponential polynomial Diophantine equations

We chose to present ideas in the simplest context of Diophantine equations that are polynomial. It may be useful to include a generalization to *exponential-polynomial Diophantine equations* [1]. Such are the equations $D(z_1, \ldots, z_m) = 0$ where $D(z_1, \ldots, z_m)$ is a linear combination of terms of the form $b_1^{z_1} \cdots b_m^{z_m} z_1^{d_1} \cdots z_m^{d_m}$ where $d_i \in \mathbb{N}_0$ and the bases b_i are complex numbers. To avoid triviality, we again assume that $m \geq 1$ and D is not constant equal to zero.

Theorem 5.1. *Theorem 1.1 holds for any exponential-polynomial Diophantine equation $D = 0$.*

The proof amounts to retracing the argument for Theorem 1.1 while using the natural generalization of the cocycle $(\Phi_i)_{i=0}^m$, which we record below (cf. [1]).

We refer to terms of the form $b_1^{z_1} \cdots b_m^{z_m} z_1^{d_1} \cdots z_m^{d_m}$ as *monomials* and say that $b_1^{z_1} \cdots b_m^{z_m} z_1^{d_1} \cdots z_m^{d_m}$ *divides* $c_1^{z_1} \cdots c_m^{z_m} z_1^{e_1} \cdots z_m^{e_m}$ if and only if $b_i = c_i$ and $d_i \leq e_i$ for $i = 1, \ldots, m$. (Thus the exponential parts of the two monomials must be equal to each other. In particular, 2^{z_1} does not *divide* $2^{z_1} 3^{z_2}$ in our sense.) Again, V_D is the free $\mathbb{Z}$-module generated by the set $C(D)$ of all monomials which *divide* a term of D. $C(D)$ has to be ordered into a sequence. How this is done is not important. For specificity, one can proceed lexicographically by declaring

$$1 \prec b_1^{z_1} \prec \cdots \prec b_m^{z_m} \prec z_1 \prec \cdots \prec z_m.$$

Additionally, in comparing powers $b_i^{z_i}$ and $c_i^{z_i}$ with the same exponent z_i, one has to use some consistent scheme. (In examples with non-negative bases, we use $b_i^{z_i} \prec c_i^{z_i}$ iff $b_i < c_i$.)

Let $(\Phi_i)_{i=0}^m$ be the matrices representing homomorphism $\phi_i : V_D \to V_D$ in the basis $C(D)$ where, for $i = 1, \ldots, m$, the ϕ_i is induced by the substitution $z_i \mapsto z_i + 1$ and ϕ_0 is sending any exponential-polynomial $\xi \in V_D$ to $\xi\phi_0 := \xi(0, \ldots, 0)D(z_1, \ldots, z_m)$. (Here, one checks that the ϕ_i map V_D to itself.)

For instance, $D(x, y, z) = 1 + 2^x + y - z = 0$ yields $C(D) = (1, 2^x, y, z)$ and $V_D = \{a_0 + a_1 2^x + a_2 y + a_3 z \,|\, a_j \in \mathbb{Z}\}$ with

$$\Phi_0 = \begin{bmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \Phi_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \Phi_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \Phi_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

At this point, one can repeat verbatim the argument for Theorem 1.1. In particular, the key formula (8) holds in this generalized context (while still taking $u_0 := D(0, \ldots, 0)$).

References

[1] David J. Anick. Diophantine equations, Hilbert series, and undecidable spaces. *Ann. of Math. (2)*, 122(1):87–112, 1985.

[2] Vincent D. Blondel and John N. Tsitsiklis. When is a pair of matrices mortal? *Information Processing Letters*, 63:283–286, 1996.

[3] David Buhanan. *On Some Aspects Of Cocyclic Subshifts, Languages, and Automata*. PhD thesis, Montana State University, 2012.

[4] Julien Cassaigne and Juhani Karhumäki. Examples of undecidable problems for 2-generator matrix semigroups. *Theoretical Computer Science*, 204(12):29 – 34, 1998.

[5] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[6] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):233, March.

[7] Søren Eilers and Ian Kiming. On some new invariants for shift equivalence for shifts of finite type. *J. Number Theory*, 132(4):502–510, 2012.

[8] John Franks and David Richeson. Shift equivalence and the Conley index. *Trans. Amer. Math. Soc.*, 352(7):3305–3322, 2000.

[9] Robert M. Gray. *Entropy and information theory*. Springer-Verlag, New York, 1990.

[10] Vesa Halava and Tero Harju. Mortality in matrix semigroups. *The American Mathematical Monthly*, 108(7):pp. 649–653, 2001.

[11] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer, New York, 1974.

[12] Anatole Katok and Boris Hasselblatt. *Introduction to the modern theory of dynamical systems*, volume 54 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 1995.

[13] Jaroslaw Kwapisz. Cocyclic subshifts. *Math. Z.*, 234(2):255–290, 2000.

[14] Jaroslaw Kwapisz. Transfer operator, topological entropy and maximal measure for cocyclic subshifts. *Ergodic Theory Dynam. Systems*, 24(4):1173–1197, 2004.

[15] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, Cambridge, 1995.

[16] Yuri V. Matiyasevich. *Hilbert's Tenth Problem*. Massachusetts Institute of Technology Press, Cambridge, Massachusetts, 1993.

[17] Konstantin Mischaikow. The Conley index theory: a brief introduction. In *Conley index theory (Warsaw, 1997)*, volume 47 of *Banach Center Publ.*, pages 9–19. Polish Acad. Sci., Warsaw, 1999.

[18] Konstantin Mischaikow. Topological techniques for efficient rigorous computation in dynamics. *Acta Numer.*, 11:435–477, 2002.

[19] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[20] M.S. Paterson. Unsolvability in 3×3 matrices. *Studies in Appl. Math.*, 49:105–107, 1970.

[21] Emil Post. A variant of a recursively unsolvable problem. *Bull. Amer. Math. Soc*, 52:264–268, 1946.

[22] David Richeson and Jim Wiseman. Symbolic dynamics for nonhyperbolic systems. *Proc. Amer. Math. Soc.*, 138(12):4373–4385, 2010.

[23] Andrzej Szymczak. The Conley index for decompositions of isolated invariant sets. *Fund. Math.*, 148(1):71–90, 1995.