TUCS

Ville Salo

Subshifts with Simple Cellular Automata

Turku Centre *for* Computer Science

TUCS Dissertations

No ????, June 2014

Subshifts with Simple Cellular Automata

Ville Salo

To be presented, with the permission of the Faculty of Mathematics and Natural Sciences of the University of Turku, for public criticism in Auditorium Cal 1 on July 28, 2014, at 12 noon.

University of Turku
Department of Mathematics and Statistics
FI-20014 Turku
Finland

2014

Supervisor

Professor Jarkko Kari
Department of Mathematics and Statistics
University of Turku
FI-20014 Turku
Finland

Reviewers

Pierre Guillon
Institut de Mathématiques de Marseille
IML Bureau 221, Campus de Luminy, Case 907
F-13288 Marseille cedex 9
France

Alejandro Maass
Center of Mathematical Modeling
University of Chile
Blanco 2120, 7th floor, Santiago
Chile

Opponent

Enrico Formenti
Département d'Informatique
Université de Nice-Sophia Antipolis
Parc Valrose, 06108 Nice Cedex 2
France

ISBN 978-952-12-3089-9
ISSN 1239-1883

Abstract

A subshift is a set of infinite one- or two-way sequences over a fixed finite set, defined by a set of forbidden patterns. In this thesis, we study subshifts in the topological setting, where the natural morphisms between them are ones defined by a (spatially uniform) local rule. Endomorphisms of subshifts are called cellular automata, and we call the set of cellular automata on a subshift its endomorphism monoid. It is known that the set of all sequences (the full shift) allows cellular automata with complex dynamical and computational properties. We are interested in subshifts that do not support such cellular automata. In particular, we study countable subshifts, minimal subshifts and subshifts with additional universal algebraic structure that cellular automata need to respect, and investigate certain criteria of 'simplicity' of the endomorphism monoid, for each of them.

In the case of countable subshifts, we concentrate on countable sofic shifts, that is, countable subshifts defined by a finite state automaton. We develop some general tools for studying cellular automata on such subshifts, and show that nilpotency and periodicity of cellular automata are decidable properties, and positive expansivity is impossible. Nevertheless, we also prove various undecidability results, by simulating counter machines with cellular automata. We prove that minimal subshifts generated by primitive Pisot substitutions only support virtually cyclic automorphism groups, and give an example of a Toeplitz subshift whose automorphism group is not finitely generated. In the algebraic setting, we study the centralizers of CA, and group and lattice homomorphic CA. In particular, we obtain results about centralizers of symbol permutations and bipermutive CA, and their connections with group structures.

Tiivistelmä

Siirtoavaruus on äärettömien yksi- tai kaksisuuntaisten kirjainjonojen joukko, jonka määrää jokin joukko kiellettyjä (äärellisiä) alisanoja. Tässä väitöskirjassa tutkitaan siirtoavaruuksia topologisina dynaamisina systeemeinä, jolloin luonnolliset morfismit niiden välillä määritellään paikallisilla säännöillä. Siirtoavaruuksien endomorfismeja kutsutaan soluautomaateiksi ja kaikkien soluautomaattien joukkoa sen endomorfismimonoidiksi. On tunnettua, että kaikkien kirjainjonojen joukko (täysi siirtoavaruus) mahdollistaa erittäin monimutkaisten soluautomaattien konstruoimisen sekä dynaamisessa että laskennallisessa mielessä. Tässä väitöskirjassa tutkitaan pääasiallisesti siirtoavaruuksien toista ääripäätä: avaruuksia, joilla soluautomaatit ovat jossain mielessä yksinkertaisia. Erityisesti tutkitaan numeroituvia siirtoavaruuksia, minimaalisia siirtoavaruuksia sekä siirtoavaruuksia, joilla on jokin algebrallinen rakenne, jota soluautomaattien tulee kunnioittaa. Näiden siirtoavaruusluokkien endomorfismimonoidien ja soluautomaattien rakennetta selvitetään erilaisten yksinkertaisuuden kriteerien suhteen.

Numeroituvien siirtoavaruuksien tapauksessa keskitytään numeroituviin sofisiin systeemeihin eli numeroituviin siirtoavaruuksiin, jotka määrää jokin äärellinen tilakone. Tällaisten siirtoavaruuksien soluautomaattien tutkimiseen kehitetään yleisiä työkaluja, joilla esimerkiksi soluautomaattien nilpotenttisuus sekä jaksollisuus näytetään ratkeaviksi ominaisuuksiksi ja positiviinen ekspansiivisuus näytetään mahdottomaksi. Toisaalta näille siirtoavaruuksille saavutetaan myös ratkeamattomuustuloksia simuloimalla laskurikoneita soluautomaateilla. Minimaalisille siirtoavaruuksille osoitetaan, että primitiivinen korvaussääntö, jolla on niin sanottu Pisot-ominaisuus, määrää siirtoavaruuden, jonka automorfismiryhmä on virtuaalisesti syklinen, ja annetaan esimerkki minimaalisesta siirtoavaruudesta, jolla on niin sanottu Toeplitz-ominaisuus mutta jonka automorfismiryhmä ei ole äärellisesti generoitu. Algebrallisten siirtoavaruuksien endomorfismimonoideja tutkitaan lähinnä unaarisen rakenteen, ryhmärakenteen sekä hilarakenteen tapauksessa. Erityisesti etsitään yhteyksiä erityyppisten soluautomaattien sentralisoijien ja ryhmärakenteisten siirtoavaruuksien välillä.

Acknowledgements

First, I of course owe thanks to the people who had a direct impact on the content of my thesis, in particular my supervisor and occasional coauthor Jarkko Kari and my costudent and frequent coauthor Ilkka Törmä. As Ilkka is the coauthor of virtually every article included in this thesis, it is needless to say that it would look very different without him. Jarkko has of course hugely improved the presentation of the thesis and suggested better versions for many proofs. Even more importantly, he is one of the reasons I even got into mathematics; without him, this thesis might be about approximation algorithms or programming language design. Jarkko is certainly the reason I got into tilings, cellular automata, computability and dynamical systems.

Of course, there are many others who had a direct influence on the scientific content of the thesis. I would like to thank Luca Zamboni for introducing me to minimality – the world of Chapter 3. In particular, he directly suggested the study of endomorphisms of subshifts generated by Toeplitz substitutions. Tero Harju, on the other hand, taught me the love of algebra, which led to the study of lattice subshifts, and eventually to the three articles Chapter 4 is based on. Kari Ylinen is to thank for my complete lack of fear of topology, and for a reasonable fear of measure theory. Juhani Karhumäki's course on combinatorics of words is why I know fancy words such as Lyndon ones, which were particularly helpful in Chapter 2. I would also like to thank the whole CA team, in particular Charalampos Zinoviadis, and Pierre Guillon and various other French people, for teaching me many things about cellular automata (and mathematics in general) in seminars and discussions. I am grateful also to the referees, Pierre Guillon and Alejandro Maass, whose comments improved the dissertation considerably, and naturally to Enrico Formenti for agreeing to act as the opponent.

Besides the scientific content, I would like to thank the administrative staff for helping me deal with (my morbid fear of) bureaucracy throughout the years. In general, I would like to thank all the people at the Department of Mathematics and Statistics for providing a great place to work at. I could hardly imagine a nicer atmosphere, or a more colorful collection of personalities.

Naturally, I also thank my other friends and friend-like beings for providing me with things to do other than mathematics. In particular, I thank

Tanja for making my time at home – if possible – even more fun than work, and for tolerating the somewhat taxing last months of writing. Last but not least, special thanks go to my parents, for life and such. In particular, my father is probably to thank for my love of science and my mother for my love of English.

Turku, June 2014
Ville Salo

Contents

Chapter 1

Dynamical Systems, Subshifts and Cellular Automata

1.1 Introduction

In this thesis, we discuss cellular automata (CA) on subshifts. *Subshifts* are (choose your favorite definition; they are equivalent)

- closed[1], shift-invariant[2] subsets of $S^{\mathbb{Z}}$ for finite S, or
- sets of two-way infinite sequences over a finite set S, which are defined by forbidding a (possibly infinite) set of words from occurring[3] anywhere in the sequences.

We give some examples of subshifts below. *Cellular automata* on a subshift $X \subset S^{\mathbb{Z}}$ are (again, choose your favorite)

- the continuous, shift-commuting[4] maps $f : X \to X$, or
- maps $f : X \to X$ defined by a local rule $f_{\text{loc}} : S^{2r+1} \to S$ for some radius $r \in \mathbb{N}$ by

$$f(x)_i = f_{\text{loc}}(x_{i-r}, x_{i-r+1}, \ldots, x_{i+r}).$$

[1] The finite set S has the discrete topology, and $S^{\mathbb{Z}}$ the product topology.

[2] The shift map is the continuous map $\sigma : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ defined by $\sigma(x)_i = x_{i+1}$ for all $i \in \mathbb{Z}$, and shift-invariance of X means $\sigma(X) = X$.

[3] A word is a finite sequence of letters from S, and to forbid a word u from occurring in a sequence x means to forbid that some contiguous subsequence of x is u.

[4] A function is shift-commuting if it commutes with the shift map σ with respect to function composition: $f(\sigma(x)) = \sigma(f(x))$ for all $x \in X$.

The name 'cellular automaton' comes from a third point of view, or rather, the intuitive description of the second definition, where we have an infinite assortment of identical finite state machines M_i (their set of states being S), one for each integer – or 'cell' – $i \in \mathbb{Z}$ and applying f means that the machines simultaneously update their states in parallel based on the states of finitely many neighbors. Usually, the idea is that f is applied to the configuration, say, once a second, and describes the evolution of the system as a function of time.

Our approach does not quite fit the machine ideology (or the once-a-second ideology), as we usually do not fix a single cellular automaton – instead, for each subshift X, we are interested in the whole set of cellular automata on X, and not only the iteration of a single CA. Since cellular automata on a subshift X are closed under (function) composition, we usually call the set of cellular automata on X the *endomorphism monoid* of X. Note that the definition we gave is that of a one-dimensional CA – for example, Game of Life, the canonical example of a CA in pop culture, is two-dimensional. Most of our study takes place in this one-dimensional setting.

1.1.1 Outline of the Thesis

Our goal in this thesis is to find subshifts whose endomorphism monoids are simple in the sense that, for example, very few cellular automata exist, or we can quickly predict how each sequence evolves when the cellular automaton is applied repeatedly.

The simplest example of a subshift is $S^{\mathbb{Z}}$ itself, called the *full shift*. This is the set of all two-way sequences of symbols in S, such as

$$\ldots 0000.0000 \ldots \text{ and } \ldots 9853562951413.14159265358979323 \ldots,$$

if $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, where by convention, the coordinate just to the right of the symbol '.' is the 0th coordinate. (Of course, we had to omit some of the infinitely many symbols.) Such subshifts are where most research on one-dimensional cellular automata takes place. The subshift $S^{\mathbb{Z}}$ is known to have a huge endomorphism monoid; it is not huge in terms of cardinality (it is easily seen to be countable), but it is huge in terms of the mathematics and computer science it contains. Apart from some examples in Section 1.5, we rarely touch this monster in the rest of this thesis.[5]

While the endomorphism monoid of $S^{\mathbb{Z}}$ is very interesting, $S^{\mathbb{Z}}$ is not a particularly interesting example of a subshift. A slightly more interesting one is the golden mean shift X_{gold} where $S = \{0, 1\}$, and the single subword

[5] Although Chapter 4 is about its domesticated cousins with algebraic structure.

11 is forbidden. Examples of sequences in X_{gold} are[6]

$$\ldots 1001000010.0100010100\ldots \text{ and } \ldots 010101.010101\ldots,$$

but the sequence

$$\ldots 0000\color{red}{11}00.00100010\ldots$$

contains a forbidden word, and is thus not in X_{gold}. The name of this subshift comes from its connection to the Fibonacci sequence

$$(0, 1, 1,)\, 2, 3, 5, 8, 13, 21, 34, \ldots.$$

Namely, if, for each n, we count the number of subwords of length n that can occur in sequences in the golden mean shift, then we obtain precisely this sequence, slightly shifted:

$$|\{0, 1\}| = 2,\ |\{00, 01, 10\}| = 3,\ |\{000, 001, 010, 100, 101\}| = 5,$$

$$|\{0000, 0001, 0010, 0100, 0101, 1000, 1001, 1010\}| = 8, \ldots$$

Thus, the number of words grows roughly according to powers of the golden mean (more often called the golden ratio) $\phi = \frac{1+\sqrt{5}}{2} = 1.618...$. This is an example of a transitive SFT. An SFT (subshift of finite type) is a subshift where only finitely many words are forbidden, and transitivity means that two words that occur in sequences in the subshift can also occur in the same sequence, in either order.

As SFTs are one of the best-studied classes of subshifts in the literature, our first question is whether we can find SFTs with simple endomorphism monoids. Unfortunately, we see directly that at least cellular automata on X_{gold} can be just as complicated to study as those on full shifts. For example, by restricting to sequences concatenated together from 00001 and 00101, such as

$$\ldots 00001\ 00001\ 00101\ 00001\ .\ 00101\ 00101\ 00101\ 00001\ldots,$$

we can simulate any cellular automaton on a binary full shift, by thinking of 00001 as 0 and of 00101 as 1 (note that the CA does not see the spaces, but it is not hard to check that one can uniquely parse each such sequence into a concatenation of the two words, so a simulation can be easily performed).

In fact, one can perform such simulations, and construct many other complex CA, on any infinite transitive SFT, so the endomorphism monoid of such a subshift is never very simple.[7] Every SFT contains at least one

[6] More precisely, based on what we see here, they *might* be in X_{gold} – of course, there might be a forbidden word somewhere further away.

[7] See Section 1.5 for such general results, although usually the slightly stronger assumption of 'mixing' is made instead.

transitive SFT when a suitable additional set of words is forbidden, and the only SFTs where we could possibly expect to find a simple endomorphism monoid are then those where all the transitive subSFTs are finite. These turn out to be precisely the SFTs containing countably many sequences, and they (and the natural generalizations, countable sofic shifts and bounded subshifts) are the main object of study in Chapter 2. A rather canonical example of a countable SFT is obtained by choosing $S = \{1, 2, \ldots, n\}$, and forbidding the words ab where $b < a$. The sequences in this subshift generally look like

$$\ldots 1111111111111222222223333333333344444444444444 \cdots nnnnnnn \ldots$$

(although some symbols may be omitted). It turns out that even countable SFTs can have rather complex endomorphism monoids, and in particular for all large enough n, cellular automata on the subshift above are computationally universal, in the sense of unpredictability, defined in Section 1.5. Yet, they are simpler than those of full shifts: For example, there cannot exist an algorithm – say, a Haskell[8] program – such that given a cellular automaton $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$, the algorithm tells whether f is nilpotent, that is, whether every configuration is eventually turned into the sequence

$$\ldots 000000000000000000000.00000000000000000000 \ldots$$

of all zeroes [Kar92]. However, we give a very simple algorithm for checking this on countable SFTs and sofics in Theorem 2.2.5.

Intuitively, the reason the endomorphism monoids of SFTs are complex is that the rules for checking whether a sequence is in the subshift are local (as there are finitely many forbidden words). This means that a CA can make local changes to the sequences rather freely, and thus, cleverly constructed cellular automata are capable of organized computation. In the example X_{gold} above, the precise way to do this was to simulate a CA of the full shift on a subshift of X_{gold} which looks roughly like the full shift. In Chapter 3, we study subshifts where such simulations are explicitly forbidden. Namely, we study cellular automata on subshifts X which are minimal, that is, do not contain any proper subshifts. More concretely, this means that every word that appears in a sequence in X actually appears in every sequence in X, with bounded gaps (that is, it even appears in all long enough subwords). Subshifts like this, when infinite, are never SFTs.

To obtain an example of such a subshift, we again take inspiration from the Fibonacci sequence. Recall that this is the sequence of the Fibonacci numbers $a_0, a_1, a_2, a_3, a_4, a_5, a_6, \ldots$, where

$$a_0 = 0, a_1 = 1, \text{and in general } a_{k+2} = a_{k+1} + a_k \text{ for } k \geq 2.$$

[8] Or C, even if arbitrary storage is somehow added to the language.

We define the Fibonacci words over the alphabet $\{0,1\}$ by the analogous recurrence relation for words, by

$$w_0 = 0, w_1 = 01, w_2 = 010, w_3 = 01001, w_4 = 01001010,$$

and in general

$$w_{k+2} = w_{k+1}w_k \text{ for } k \geq 2$$

(so that $|w_i| = a_{i+2}$). Let $S = \{0,1\}$ and forbid those finite words that do not occur in any of the words w_i to obtain a subshift X_{fib}, usually called the Fibonacci subshift. This is a particular example of a so-called substitutive subshift, since it is the subshift generated by the fixed point of the Fibonacci substitution τ defined by $0 \mapsto 01, 1 \mapsto 0$.[9] Every sequence in X_{fib} looks pretty much the same (since it is minimal), and a typical example is

$$\ldots 10010100100101001010010010.10010100100101001010010010 \ldots.$$

It turns out that the global structure of this subshift indeed results in a very simple endomorphism monoid: it is shown in [Oll13] that the only cellular automata on X_{fib} are the shift maps, that is, the only CA are the maps that shift the points left or right by some fixed amount. We prove a similar result for a large class of subshifts generated by substitutions. Namely, for all primitive substitutions with the so-called balance property (which is implied both by the well-known Pisot property, and the property that images of all letters have the same length), we prove that all CA on the subshift generated by the fixed point are kth roots[10] of shift maps for some fixed k. This result applies, for example, to X_{fib} and the Thue-Morse subshift generated by the substitution $0 \mapsto 01, 1 \mapsto 10$ (although for both of these examples, stronger results are known). We also give an example of a minimal subshift where such a result does not hold, by exhibiting a Toeplitz subshift whose endomorphism monoid is isomorphic to the non-finitely generated additive subgroup $\left\langle \left(\frac{5}{2}\right)^i \mid i \in \mathbb{N} \right\rangle$ of $\mathbb{Q}$.

In Chapter 4, our approach is a bit different. Here, our subshifts of interest will usually be the full shifts. Instead of removing sequences from them by forbidding subwords, we will directly forbid some of the cellular automata: we give $S^{\mathbb{Z}}$ a (universal) algebraic structure, and keep only the submonoid of cellular automata that respect this structure. A good way to construct examples of subshifts with algebraic structure is to choose a finite algebra S, say, a group, and give $S^{\mathbb{Z}}$ the algebraic structure where operations

[9] The fixed point of a substitution τ is a one-way infinite sequence $x \in S^{\mathbb{N}}$ such that $\tau(x) = x$. For example, the fixed point of the Fibonacci substitution is 0100101001001010010100100 1....

[10] An nth root of a CA $f : X \to X$ is another CA $g : X \to X$ such that $g^n = f$, that is, for a sequence $x \in X$, g repeated n times on x gives $f(x)$.

are applied cellwise (so that $S^{\mathbb{Z}}$ is the direct product of $\mathbb{Z}$ copies of S). By a cellular automaton f respecting the algebraic structure, we mean that it is an algebra homomorphisms from $S^{\mathbb{Z}}$ to itself. That is, if $g : (S^{\mathbb{Z}})^n \to S^{\mathbb{Z}}$ is an algebra operation, then we require $g(f(x_1), \ldots, f(x_n)) = f(g(x_1, \ldots, x_n))$ for all $x_1, \ldots, x_n \in S^{\mathbb{Z}}$. For example, the subshift $\mathbb{Z}_2^{\mathbb{Z}}$ is the binary full shift with an abelian group structure given by cellwise addition modulo 2. The cellular automata on this subshift (which respect the algebra structure) are very simple: they are cellwise sums of powers of the shift map σ.

We also study unary algebraic structures obtained by simply choosing a cellular automaton $g : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ (or sometimes, a finite set of CA), and considering it to be a unary algebra operation on the subshift. Cellular automata $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ that respect the structure given by g are exactly the ones that commute with g in the sense that $f(g(x)) = g(f(x))$ for all $x \in S^{\mathbb{Z}}$. Our main results are about cellular automata on subshifts with such unary structure, and the interplay of a group structure and a unary structure. For example, we introduce the so-called color blind cellular automata – cellular automata that commute with symbol permutations – and show how to simulate general cellular automata with them. In contrast, we then show that cellular automata other than shift maps cannot commute with all symbol maps unless the alphabet is binary, and precisely the groups $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_2^2$ allow group-endomorphic CA which are color blind.

1.1.2 Which Parts are Worth Reading?

The topic of this thesis is quite shallow, even within the theory of cellular automata, and we do not answer any big open questions. Thus, it seems possible that not everyone feels a strong need to peruse every page. This section is meant as a small guide (or advertisement) for those people, and contains what I[11] feel are some of the highlights of the thesis.

For readers not interested in cellular automata or subshifts at all, we of course have little to offer. However, when studying the borders of the concept of color blind cellular automata, we discuss the so-called typhloticness of cellular automata as well. This notion turns out to be, in a sense, an alternative definition of an ultrafilter. Some readers may find this – Lemma 4.2.29 – interesting, and this part should be readable with little preliminary knowledge.

Another somewhat exotic argument that may be of general interest[12] is our formalization of the idea of letting periodic subpatterns in points become

[11] Here, and throughout the thesis, 'we' refers to a fuzzy subset of me, the possible co-author(s) of my articles, and the reader(s). I try to use 'I' when stating my own opinions or stating that I do not know something – the reader(s) or my possible co-author(s) certainly might know the answer. The reader is of course allowed to disagree also with the sentences containing 'we'.

[12] Although it is presumably not a quick read.

infinite, in the proof of Lemma 2.2.3. This allows for the use of compactness arguments quite different from those generally used in the study of subshifts or cellular automata.

If the reader is only interested in cellular automata on full shifts (and other mixing SFTs)[13] they may find at least Chapter 4 interesting – and even the further subset of readers not particularly interested in algebra might want to look at the discussion on intersections of centralizers of CA in the end of Section 4.2.3 and solve the questions I leave open. We also prove some general results about cellular automata on mixing SFTs, such as Lemma 1.3.22. This is a variation of the well-known Ryan's theorem which states that the centralizer of the automorphism group of a full shift is the set of all shift maps. Our constructions of CA on mixing SFTs are based on the ubiquity of unbordered words, that is, Lemma 1.3.5 (from [Lot02]). Unbordered words make life much easier, at least for researchers who prefer words to matrices (such as me), and I am very happy to have bumped into this lemma, since I have spent quite a bit of time finding unbordered words manually, or finding ways around them – if this rings a bell, the reader, like me, may have missed this lemma.

For readers interested in all things cellular automata, we of course suggest reading the whole thesis. In particular, we suggest at least taking a look at the main results and open questions of each section. Indeed, our main goal has been to find new aspects of cellular automata to study. I have heard many say that the study of cellular automata is finished, or that at least, all that is left is too hard. I disagree even in the case of the full shift, but hopefully this thesis shows that there is at least a lot to study about cellular automata on subshifts.

1.1.3 Possible Future Work

As I mentioned, I believe there is still much to study in all of these areas. In particular, I believe that the study of cellular automata on countable subshifts is not at all finished. I feel we have a pretty good grip on the case of CA on one-dimensional sofic shifts already, but there are many questions of general nature one can still ask (and we list some questions in Section 2.4). As far as I know, almost nothing is known about cellular automata on countable two-dimensional SFTs, and in fact I am not aware of that many articles on countable dynamical systems in general. Often, such systems are not even mentioned in books on dynamical systems, although I feel Chapter 2 alone (and the literature listed in Section 2.1) is proof that they are worth studying. It would also be interesting to investigate the connection between CA

[13] In fact, cellular automata on other subshifts are rarely even called 'cellular automata', so I imagine there are such readers.

on countable sofic shifts and conserved quantities, hinted at in the caption of Figure 2.1.

On minimal subshifts, my general feeling[14] is that interesting cellular automata do not exist. However, I am not aware of any articles that show such general results. We make some general remarks in the beginning of Chapter 3, but leave very basic questions open. Even for minimal subshifts generated by symbol-to-word substitutions or those generated by Toeplitz sequences, little is known in general. Even the small case of primitive Pisot substitutions which we (partially) solve in Section 3.2 is new, as far as we know, and such subshifts are subsumed in the larger class generated by primitive substitutions, which are further subsumed in the study of linearly recurrent subshifts – I do not know how to take these extra steps. The most interesting examples of endomorphism monoids for minimal subshifts we have been able to build are those of Section 3.3, which – while still very simple – are at least not finitely generated.

The study of Chapter 4 where subshifts in different (universal algebraic) varieties are considered, is even less finished. The only natural varieties for which we obtain general results are the ones with only reversible unary operators whose combinations generate only finitely many different operations even in the free algebra in this variety (for example, in the case of a single operation f, we could have the identity $f^n(x) \sim x$ for some n). This corresponds to the study of the centralizer of an equicontinuous family of reversible unary cellular automata; for these, we prove the existence of an intrinsically universal CA in the endomorphism monoid, which could be considered to partially solve the endomorphism monoid of such subshifts, as it implies that some kind of copy of the endomorphism monoid of the full shift can be found in it.

About general centralizers, we can say very little, and not for the usual reason that we can prove that only little can be said: for all I know, the centralizer of a CA on a full shift might have a very simple description in general (although I certainly doubt this). I cannot even say anything about the centralizer of a single almost equicontinuous CA, or positively expansive CA, in general, although these are not that far away from the classes of equicontinuous and bipermutive CA which we study in Section 4.2 and Section 4.3, respectively.

Of course, unary operators give rather trivial examples of algebras. As far as I know, nothing general can be said about, say, the endomorphism monoid of a subshift with a single binary operator. There is a lot of study about cellular automata respecting a group structure, but for example, a lot is open even about cellular automata respecting a lattice structure. In

[14] At least, I'm not aware of much evidence to the contrary. I don't even know any convoluted tailor-made examples that have interesting endomorphisms, let alone natural ones.

Theorem 4.4.5, we prove that surjective CA on a full shift with cellwise lattice structure are very simple. In order to generalize this for all mixing SFTs with a cellwise lattice structure (and even for non-surjective CA on full shifts), one probably needs a deeper understanding of lattices than I currently have.

At least one chapter is completely missing from this thesis, and that is Chapter 5: Random Subshifts. I believe that the typical subshift has a very simple endomorphism monoid containing shift maps only. Of course, it is not clear what a 'random' or 'typical' subshift is. For example, if we forbid a random *finite* set of words (in any sense), then we have some probability to obtain the empty SFT, some probability to obtain one with positive entropy, and some probability to obtain a countable SFT. The endomorphism monoid of the empty SFT is trivial, and that of a positive entropy SFT is never even close to simple. Furthermore, as we hint in Section 2.4, we believe 'most' countable SFTs have at least somewhat complicated endomorphism monoids as well. In [Mil12], it is shown that if for each i, a word of length n_i is forbidden, for a sparse enough sequence of n_i, then the subshift obtained is necessarily nonempty. This means that we can forbid a random subset of words of such lengths, and surely obtain a nonempty subshift. I would be very interested in knowing what happens, even for particular distributions – is the endomorphism monoid typically small, typically big, and how sensitively do the answers depend on the choice of the distribution?

1.2 The General Setting – Dynamical Systems

We begin with a brief exposition of dynamical systems, as this general framework is the main motivation for the study of subshifts.

We assume a basic knowledge of set theory, topology, groups, monoids, category theory, and automata theory. In set theory, the reader should be familiar with concepts such as surjectivity, injectivity and countability. In topology, the reader should be familiar with concepts such as metrics, open and closed sets and compactness. For groups and monoids, the reader should be familiar with concepts such as subgroups and submonoids, should know what the identity element is, and should have an intuitive understanding of group and monoid actions. In category theory, the reader should know the concepts of objects and morphisms. In automata theory, the reader should know what regular languages are, and should be able to describe what kind of set a regular expression such as $0^*(1^* + 0^*)$ means. Readers with a background in mathematics should be able to quickly pick up missing preliminaries as needed in any standard reference, or Wikipedia.

We will only talk about monoid actions in this section – they are the main motivation for the definitions, but are of little use in the more restricted

setting in later sections. Our monoids always act from the left, and if M is a monoid acting on a space X (and the action is clear from the context), then $Y \subset X$ is an M-subset of X if $MY \subset Y$.

When no topology is given, a finite set is considered to have the discrete topology, and a subset of $\mathbb{R}$ has the subspace topology. Our natural numbers include 0: $\mathbb{N} = \{0, 1, 2, \ldots\} \subset \mathbb{Z}$. The metric of a metric space is usually called $d : X \times X \to \mathbb{R}$, and we write $U \Subset X$ if U is an open set in X. As a general convention, for products $X \times Y$, π_1 and π_2 denote the projections to the X- and Y-component, respectively. We use the Kleene star operation on sets of functions by

$$F^* = \{\mathrm{id}_X\} \cup \{f_1 \circ \cdots \circ f_k \mid k \in \mathbb{N} \wedge \forall i \in [1, k] : f_i \in F\},$$

when $F \subset X^X$, where id_X is the identity function on X.

Definition 1.2.1 *Let M be a (discrete) monoid. An M-dynamical system is a pair (X, T) where X is a compact metric space and T (the* dynamics *or the* action*) is a continuous action of M on X. For $m \in M$, we write $T^m : X \to X$ for the action of m on X.*

Usually, the monoid acting through T is either $(\mathbb{N}, +)$ or $(\mathbb{Z}, +)$ in this thesis. We usually use additive notation for the monoid M, as we do not discuss non-commutative actions. For both actions of $\mathbb{N}$ and $\mathbb{Z}$, the map $T = T^1$ defines the action completely, and we often just give this function, and call it the dynamics[15]. Dynamical systems are studied in many levels of generality in the literature. Often, the monoid acting on X is replaced by a topological group such as $\mathbb{R}$, and sometimes only actions of $\mathbb{Z}$ or $\mathbb{N}$ are included. Furthermore, the assumptions of compactness and metrizability can be relaxed.

Often, we say just that X or T is a dynamical system, when the action or the space, respectively, is obvious.

Definition 1.2.2 *For any monoid M, the M-dynamical systems form a category, and the morphisms between two M-dynamical systems (X, T) and (Y, T') are the continuous functions $f : X \to Y$ such that $f \circ T^m = T'^m \circ f$ for all $m \in M$. A surjective morphism is called a* factor map*, an injective morphism is called an* embedding*, and a bijective morphism is called a* conjugacy*. A subset $Z \subset X$ is said to be* invariant *if $T^m(Z) \subset Z$ for all $m \in M$, and the dynamical system $(Z, (T^m|_Z)_{m \in M})$ is called a* subsystem*.*

We now define our main object of study, the endomorphism monoid, and its better-known cousin, the automorphism group.

[15] However, in a sense, the $\mathbb{N}$-action given by a homeomorphism $f : X \to X$ differs from the $\mathbb{Z}$-action it gives, as for example the subsystems it gives are subtly different. This is why we give our definitions in terms of monoid actions.

Definition 1.2.3 *Let (X, T) be a M-dynamical system. Then we write* $\mathrm{End}(X)$ *for the* endomorphism monoid *of X, that is, the set of* endomorphisms *(morphisms $f : X \to X$) with monoid structure given by function composition, and identity element $id_X : X \to X$ (the identity function). We write* $\mathrm{Aut}(X)$ *for the* automorphism group *of X, that is, the restriction of* $\mathrm{End}(X)$ *to* automorphisms *(endomorphisms that have a left and right inverse).*

As we only consider compact dynamical systems, every bijective morphism $f : X \to Y$ is invertible in the sense that there exists a left and right inverse $f^{-1} : Y \to X$ such that $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$.

In Chapter 4, when subshifts in a (universal algebraic) variety $\mathcal{F}$ are considered, if $f_1, \ldots, f_k$ are the algebra operations on X, $\mathrm{End}(X, f_1, \ldots, f_k)$ will refer to the endomorphism monoid, and $\mathrm{Aut}(X, f_1, \ldots, f_k)$ to the automorphism group of X, in the category of dynamical systems with algebraic structure in this variety. More concretely, $\mathrm{End}(X, f_1, \ldots, f_k)$ is the restriction of $\mathrm{End}(X)$ to morphisms $f : X \to X$ such that if $f_j : X^n \to X$, then $f_j(f(x_1), \ldots, f(x_n)) = f(f_j(x_1, \ldots, x_n))$ for all $x_i \in X$ and $1 \leq j \leq k$.

Whenever the monoid M is abelian, the action of any element of M is itself an endomorphism of an M-dynamical system. Conversely, each endomorphism f of a dynamical system X gives a new action of $\mathbb{N}$ (or $\mathbb{Z}$) on X, that is, (X, f) is an $\mathbb{N}$-dynamical system in its own right (or a $\mathbb{Z}$-system if f is bijective).

We note that embeddings and subsystems are essentially the same thing: a subsystem is the image of an embedding, the image of an embedding is a subsystem, and the embedding induces a conjugacy between its domain and image. Thus, often, subsystems are *defined* as embeddings. Note that if $f : X \to Y$ is a conjugacy, then the inverse $f^{-1} : Y \to X$ is a conjugacy as well (by compactness).

1.2.1 Dynamical Notions

We now define several properties of $\mathbb{N}$- and $\mathbb{Z}$-dynamical systems. We only list brief definitions, and do not discuss them in much detail here. We discuss many of them in more detail when they are used, and give more concrete alternative definitions. The properties are often referred to as 'dynamical properties', because they are invariant under conjugacy (because they are defined in terms of the topology and the action). The following are convenient shorthands for accessing limit points.

Definition 1.2.4 *Let X be a topological space, let $f : X \to X$. Then*

- *the set of* f-limit points of Y *is* $\Omega_f(Y) = \bigcap_{m \geq 0} \overline{\bigcup_{n \geq m} f^n(Y)}$,
- *the* limit set of f *is* $\Omega_f(X) = \bigcap_{n \geq 0} f^n(X)$,

- *for* $Y \subset X$*, we define* $\omega_f(Y) = \bigcup_{y \in Y} \Omega_f(\{y\})$*,*
- *and the* asymptotic set of f *is* $\omega_f = \omega_f(X)$*.*

The limit set (resp. asymptotic set) of an $\mathbb{N}$-dynamical system (X, T) is Ω_T (resp. ω_T). In the case of compact spaces (in particular if f is the action of a dynamical system), the limit set is just the set of points x with an infinite chain of preimages $\ldots, x_{-2}, x_{-1}, x_0 = x$ such that $f(x_i) = x_{i+1}$.

Definition 1.2.5 *Let* $M = \mathbb{N}$ *or* $M = \mathbb{Z}$*. An* M*-dynamical system* (X, T) *is*

- nonwandering*, if*

$$\forall U \Subset X : \exists m > 0 : T^m(U) \cap U \neq \emptyset$$

- transitive*, if*

$$\forall U, V \Subset X : \exists m \geq 0 : T^m(U) \cap V \neq \emptyset$$

- mixing*, if*

$$\forall U, V \Subset X : \exists m \geq 0 : \forall n \geq m : T^n(U) \cap V \neq \emptyset$$

- sensitive*, if*

$$\exists \epsilon > 0 : \forall x \in X, \delta > 0 : \exists y \in X, n \geq 0 : d(x, y) < \delta \wedge d(T^n(y), T^n(x)) > \epsilon$$

- equicontinuous*, if*

$$\forall \epsilon > 0 : \exists \delta > 0 : \forall x, y : d(x, y) < \delta \implies \forall n \geq 0 : d(T^n(x), T^n(y)) < \epsilon.$$

- expansive*, if* $M = \mathbb{Z}$ *and*

$$\exists \epsilon > 0 : \forall x, y \in X : x \neq y \implies \exists n \in \mathbb{Z} : d(T^n(y), T^n(x)) > \epsilon$$

- positively expansive*, if*

$$\exists \epsilon > 0 : \forall x, y \in X : x \neq y \implies \exists n \geq 0 : d(T^n(y), T^n(x)) > \epsilon$$

- nilpotent*, if*

$$\exists x_0 \in X : T(x_0) = x_0 \wedge \forall x \in X : \exists n \geq 0 : T^n(x) = x_0$$

- uniformly recurrent*, if*

$$\forall U \Subset X : \exists n > 0 : \forall x \in X : \{x, \ldots, T^{n-1}(x)\} \cap U \neq \emptyset$$

Many of the properties we listed make sense also for, say, $M = \mathbb{Z}^d$, but we have little need for them.

It is clear that a sensitive system is not equicontinuous. There is also a natural intermediate notion. We say that $x \in X$ is an *equicontinuity point* if

$$\forall \epsilon > 0 : \exists \delta > 0 : \forall y : d(x, y) < \delta \implies \forall n \geq 0 : d(T^n(x), T^n(y)) < \epsilon.$$

It follows from compactness that (X, T) is equicontinuous if and only if every point $x \in X$ is an equicontinuity point. Sensitivity implies that there are no equicontinuity points. We say that (X, T) is *almost equicontinuous* if equicontinuity points form a residual set. For this and related observations see the discussion after Definition 5 in [Kůr97].

We say that a dynamical system X is *minimal* if it has no subsystems apart from the trivial ones, $\emptyset$ and X. It is easy to see that minimality is equivalent to uniform recurrence when $M = \mathbb{N}$ or $M = \mathbb{Z}$, and we will use the two terms rather interchangeably.

1.3 The Specific Setting – Subshifts

1.3.1 Words and Subshifts

Let S be a finite set, referred to as the *alphabet*. A *word over* S (or *pattern*) is a function $w : [0, \ell - 1] \to S$, where $\ell = |w|$ is the *length* of w. When an interval $[a, b]$ with $a \neq 0$ is used in place of $[0, \ell - 1]$, the word is implicitly shifted back to the origin. For indexing particular coordinates or intervals of words, we always use the notation $w_i = w(i)$ or $w_{[a,b]} = w|_{[a,b]}$, where $w|_{[a,b]} = u$ such that $u_i = w_{i+a}$ (and intervals with $b < a$ give the empty word $\epsilon : \emptyset \to S$). If $u = w_{[a,b]}$ for some $a, b \in \mathbb{N}$, we write $u \sqsubset w$ and say u *occurs in* w. We write

$$|w|_u = |\{i \mid w_{[i,i+|u|-1]} = u\}|,$$

that is, $|w|_u$ is the number of occurrences of u in w (used mainly when u is a letter). We write S^* for the set of all words over S. For $u, v \in S^*$, we write uv for the *concatenation* of u and v, defined by

$$(uv)_i = \begin{cases} u_i & \text{if } i < |u|, \\ v_{i-|u|} & \text{otherwise.} \end{cases}$$

This gives S^* the structure of a monoid, with the empty word as the identity element.

Remark 1.3.1 *We use* 0*-indexed words.*

The dynamical systems we are most interested in are the so-called one-dimensional subshifts, that is, spaces of one- or two-way infinite sequences, with the left shift as the natural dynamics. In general, for any monoid M, subshifts give natural examples of M-dynamical systems.

Definition 1.3.2 *Let M be a commutative monoid, and let S be a finite set (with the discrete topology). The set S^M (with the product topology) is called the* full (M-)shift on S. *It becomes an M-dynamical system (S^M, σ) with the action $\sigma^m(x)_i = x_{i+m}$ for $x \in S^M$ and $i, m \in M$. The action σ is called* the shift map. *We also refer to the functions σ^m as shift maps. Subsystems of S^M are called (M-)*subshifts.

The elements of S^M are usually called *points*, and in the case $M = \mathbb{N}$ or $M = \mathbb{Z}$, they are indexed just like words. In particular, for $x \in S^{\mathbb{Z}}$, $x_{[a,b]}$ is the word $x_a x_{a+1} \cdots x_b$ if $b \geq a$, and otherwise, the empty word. For a subshift $X \subset S^{\mathbb{Z}}$, as we did with words, we write $w \sqsubset x$ if $x_{[a,b]} = w$ for some $a, b \in Z$, and $w \sqsubset X$ if $w \sqsubset x$ for some $x \in X$. Informally, we refer to both i and the symbol x_i as the *ith cell* of x.

In the case $M = \mathbb{Z}$, the topology of S^M is given by the metric

$$d(x, y) = \inf\{2^{-n} \mid x_{[-n,n]} = y_{[-n,n]}\}.$$

There is a lot of leeway in this definition, and for example, replacing 2^{-n} by $\frac{1}{n+1}$ gives the same topology.

If we set $M = \mathbb{Z}$ in Definition 1.3.2, we obtain the *(one-dimensional) two-way subshifts*, which are our main object of interest, and which the word 'subshift' usually refers to. They can be given a nice combinatorial definition[16]: if X is a two-way subshift, then there exists a set of *forbidden words* $F \subset S^*$ such that X is the set of sequences $x \in S^{\mathbb{Z}}$ for which $x_{[i,j]} \notin F$ for all $i, j \in \mathbb{Z}$. If $M = \mathbb{N}$, we obtain the *(one-dimensional) one-way subshifts*. The combinatorial description of one-way subshifts is equivalent to that of two-way subshifts (but the shift map σ then need not be surjective, and it is almost never injective). Given a one-way subshift $X \subset S^{\mathbb{N}}$, its *two-way extension* is the two-way subshift $X^{\leftrightarrow} = \{x \in S^{\mathbb{Z}} \mid \forall i : x_{[i,\infty)} \in X\}$.

Remark 1.3.3 *The term 'shift' refers to both the map σ and the space S^M. The reason for this is that in the theory of dynamical systems, the action and the space are often considered the same object. This can be confusing. To avoid confusion while conforming to the standard terminology, we try to*

[16] We refer to definitions as 'combinatorial', when the definition is given in terms of concrete combinatorial objects such as words. Such definitions can usually be found for concepts defined for subshifts and cellular automata.

always also use the term 'map' when talking about σ, and when talking about the space S^M or its subsets, we explicitly use the term 'space', unless this is implied, as in 'full *shift'*, 'sub*shift' or* 'sofic *shift'. However, we do use this type of identification of the space and the action for cellular automata (defined below), and for example say that a cellular automaton $f : X \to X$ is transitive if the corresponding $\mathbb{N}$-system (X, f) is transitive.*

We write $\mathcal{B}_n(X) = \{w \in S^n \mid w \sqsubset X\}$, and $\mathcal{B}(X) = \cup_n \mathcal{B}_n(X)$. The set $\mathcal{B}(X)$ is called the *language* of X. It is known that two subshifts are equal if and only if their languages are equal [LM95]. If $X \subset S^{\mathbb{Z}}$ is a subshift, then the *(topological) entropy* of X is

$$h_{\text{top}}(X) = \lim_{n\to\infty} \frac{1}{n} \log |\mathcal{B}_n(X)|.$$

The entropy of a one-way subshift is defined with the same formula. Topological entropy can be defined for dynamical systems in general, but for this particular notion, the combinatorial definition is simpler to state than the topological one, so we omit the general definition (unfortunately, this means that we have to define entropy separately for cellular automata below, although both correspond to the same dynamical notion).

The language of a subshift X is always *extendable*, that is, $w \in L$ implies $awb \in L$ for some $a, b \in S^+$, and *factor-closed*, that is, $uv \in L$ implies $u \in L$ and $v \in L$. The converse holds as well, in the following sense. Given an extendable language $L \subset S^*$, we write

$$\mathcal{B}^{-1}(L) = \{x \in S^{\mathbb{Z}} \mid \forall r : \exists w \in L : x_{[-r,r]} \sqsubset w\}.$$

This is the smallest subshift whose language contains L. We always have $\mathcal{B}^{-1}(\mathcal{B}(X)) = X$, and we have $\mathcal{B}(\mathcal{B}^{-1}(L)) = L$ if and only if L is factor-closed.

The points $x, y \in S^{\mathbb{Z}}$ are *left-asymptotic* if $x_i = y_i$ for all small enough $i \in \mathbb{Z}$, and *right-asymptotic* if $x_i = y_i$ for all large enough $i \in \mathbb{Z}$. If the points are both left- and right-asymptotic, we say that they are simply *asymptotic*. For $a \in S$, we say x is *a-finite* if x is asymptotic to the point y with $y_i = a$ for all $i \in \mathbb{Z}$ (that is, only finitely many cells of x contain a symbol other than a). The sequences $x_{(-\infty,n]} \in S^{-\mathbb{N}}$ for $n \in \mathbb{Z}$ (defined in the obvious way) are called *left tails* of x, and $x_{[n,\infty)} \in S^{\mathbb{N}}$ the *right tails*. In general, we manipulate left tails and right tails as if they were words, but take care to only write uv if u is a left tail or a word, and v is a right tail or a word. The meanings of such expressions should be clear.

A point $x \in S^{\mathbb{Z}}$ (resp. $x \in S^{\mathbb{N}}$ or $S^{-\mathbb{N}}$) is *(σ-)periodic*, or *spatially periodic* with period p if $x_i = x_{i+p}$ for all $i \in \mathbb{Z}$ (resp. $i \in \mathbb{N}$ or $i \in (-\infty, -p+1]$), and the words $x_{[i,i+p-1]}$ are called *repeating patterns*. We say

that $x \in S^{\mathbb{Z}}$ is *periodic to the left* if it is left-asymptotic to a periodic point, and define *periodicity to the right* symmetrically. For $x \in S^{\mathbb{N}}$, if $x_{[i,\infty)}$ is periodic, we say x is *eventually periodic*.

For describing points in subshifts, our conventions are as follows: The notation $w^{\mathbb{Z}}$ (resp. $w^{\mathbb{N}}$ or $w^{-\mathbb{N}}$) for w a word (or symbol) means the periodic point x with period $|w|$ with $x_{[0,|w|-1]} = w$ (resp. $x_{[0,|w|-1]} = w$ or $x_{[-|w|+1,0]} = w$). We call points $a^{\mathbb{Z}}$ for $a \in S$ *unary*. The notation ${}^{\infty}uv.v'w^{\infty}$ means the point x with $x_{[0,|v'|-1]} = v'$, $x_{[-|v|,-1]} = v$, $x_{[|u|,\infty)} = w^{\mathbb{N}}$, and $x_{(-\infty,-|v|]} = u^{-\mathbb{N}}$, so that the symbol . means that the cell to the right of it is coordinate 0, and $^{\infty}$ means that the symbol or word next to it is repeated infinitely.

We say two words u and v *agree from the left* if $u = vv'$ or $v = uu'$ for some u', v'. We define *agreeing from the right* symmetrically. Given a total ordering $<$ for an alphabet S, the lexicographical order of S^n is defined by $u < v \iff u = wau', v = wbv', a < b$. A *rotation* of a word u is a word wv such that $vw = u$. A word is *primitive* if it is not the proper power of another word, that is, u is primitive if $u = v^n \implies v = u, n = 1$. If $uv = vu$, then u and v are powers of a third word w. More generally, it is known that if two words u, v satisfy a nontrivial equation, such as $u^k = v^\ell$ for some $k, \ell > 0$, then they are powers of the same word. It is also easy to see that if a word is non-primitive, then all its rotations are non-primitive, and thus a word is primitive if and only if all of its rotations are primitive. A word $u \in S^*$ is *Lyndon* if it is primitive and strictly lexicographically smaller than any of its rotations. A set of words U is *mutually unbordered* if $uv = wu' \implies v = w = \epsilon \vee |w| \geq |u|$ for all $u, u' \in U$, that is, no two words in U can overlap in a nontrivial way. A word u is *unbordered* if $\{u\}$ is mutually unbordered.

The main property of Lyndon words we need is that a periodic sequence has a unique repeating pattern which is a Lyndon word (in particular, we will not need Lyndon decompositions):

Lemma 1.3.4 *Given a finite set U of Lyndon words, there exists $M > 0$ such that if $u, v \in U$ and w is an arbitrary word such that $|w| \geq M$, $w \sqsubset u^M$ and $w \sqsubset v^M$, then $u = v$.*

Proof. It is enough to, for a single pair $u, v \in U$ with $u \neq v$, find M such that u^M and v^M cannot overlap by M. If such M does not exist, then for some rotation v' of v we even have that arbitrarily large M, u^M and $(v')^M$ even agree from the left by at least M. If M is large enough, then this means u and v' satisfy a nontrivial equation of the form $u^k = (v')^\ell$, and are thus powers of the same word. Since v is primitive, so is v', and it follows that $u = v'$. Since u and v are Lyndon, we must have $u = v$, since u

and v have the same rotations, and both v and $u = v'$ are lexicographically minimal among them. ■

A Lyndon word is in particular unbordered, but not every unbordered word is Lyndon. Unbordered words are very useful in the study of cellular automata because they allow us to, for example, talk about replacing words by other words without having to worry about possible overlaps (in which case replacement might be nondeterministic, and not doable by a CA). Luckily for us, unbordered words are unavoidable:

Lemma 1.3.5 (Theorem 8.3.9 in [Lot02]) *Let $x \in S^{\mathbb{N}}$. If x is not periodic, then for any m, there exists an unbordered word $w \sqsubset x$ with $|w| \geq m$.*

Periodicity of points can be replaced by periodicity (that is, finiteness) of subshifts using the following lemma.

Lemma 1.3.6 *If a subshift $X \subset S^{\mathbb{Z}^d}$ or $X \subset S^{\mathbb{N}}$ contains only periodic points, then it is finite.*

Proof. The case $X \subset S^{\mathbb{Z}^d}$ is proved in Theorem 3.8 in [BDJ08]. The case $X \subset S^{\mathbb{N}}$ follows by considering the two-way extension of X. ■

Lemma 1.3.7 *Let $X \subset S^{\mathbb{Z}}$ be an infinite subshift. Then for any m, there exists an unbordered word $w \sqsubset X$ with $|w| \geq m$.*

Proof. Lemma 1.3.6 and Lemma 1.3.5. ■

Of particular interest to us are the SFTs and sofic shifts, which form an important family of subshifts studied in symbolic dynamics.

Definition 1.3.8 *If the subshift $X \subset S^{\mathbb{Z}}$ can be defined by a finite set of forbidden words, it is called an* SFT *(subshift of finite type). If the set of forbidden words can be taken to be a regular language, then X is said to be* sofic.

The theory of sofic shifts, SFTs and one-dimensional subshifts in general is discussed in depth for example in [LM95] and [Kit98]. These classes appear throughout this thesis. Note that an SFT is sofic, since any finite set is regular. It is well-known that a subshift is sofic if and only if it is the image of an SFT in a block map. Another characterization of sofic shifts is that their languages are regular, and sofic subshifts of $S^{\mathbb{Z}}$ can thus be identified with regular languages $L \subset S^*$ which are extendable and factor-closed. It can be shown that when L is regular, $\mathcal{B}^{-1}(L)$ is a sofic shift, and we usually use this notation for defining sofic shifts (and even SFTs).

In addition to using languages and the $\mathcal{B}^{-1}$ operator, we can sometimes describe a subshift as the orbit closure of a point – this is particularly useful

in Chapter 3. If $x \in S^{\mathbb{Z}}$, we write $\mathcal{O}(x)$ for the *orbit* $\{\sigma^n(x) \mid n \in \mathbb{Z}\}$ of a point x, and it is easy to see that the closure $\overline{\mathcal{O}(x)} \subset S^{\mathbb{Z}}$ is always a subshift. We say $\overline{\mathcal{O}(x)}$ is the subshift *generated* by the point x. We also use this terminology in the case of one-way points, and then the subshift generated is one-way as well. It is not hard to show that $\overline{\mathcal{O}(x)}$ is always a transitive subshift, and it is minimal if and only if $\forall y \in \overline{\mathcal{O}(x)} : \overline{\mathcal{O}(y)} = \overline{\mathcal{O}(y)}$.

Essentially just by rephrasing the definitions, one can obtain combinatorial characterizations of the dynamical properties listed in Definition 1.2.5 for a one-dimensional subshift. We mainly need the characterizations of mixing, transitivity and minimality. A subshift X is transitive (resp. mixing) if for any words $u, v \sqsubset X$, for some (resp. any large enough) $n \in \mathbb{N}$, we have $uwv \sqsubset X$ for some word w with $|w| = n$. In fact, if X is a transitive (resp. mixing) sofic shift, then there exists $N \in \mathbb{N}$ such that w can be taken to have length in $\{N, \dots, 2N-1\}$ (resp. N) for any $u, v \sqsubset X$. In the case of mixing SFT, such N is called a *mixing distance*.

Minimal subshifts are another very important class of subshifts. A subshift is minimal if and only if, for each $u \sqsubset X$, there exists N_u such that if $w \sqsubset X$ and $|w| \geq N_u$, then $u \sqsubset w$. They are at the other end of the spectrum of subshifts than SFTs and sofic shifts, in the sense that nontrivial mixing SFTs allow the most freedom in the construction of points (in that they are considered the natural generalization of a full shift), while minimal subshifts allow the least.

1.3.2 Cellular Automata

We now define cellular automata as the endomorphisms of subshifts.

Definition 1.3.9 *A* cellular automaton *on an (M-)subshift X is an endomorphism $f : X \to X$ in the category of (M-)dynamical systems. A morphism between subshifts X and Y is called a* block map

By our definition of 'morphism', a cellular automaton is then a (not necessarily surjective) continuous map from X to itself which commutes with the shift map σ. Again, a combinatorial definition can be given when $M = \mathbb{Z}$: if X is a subshift, then a function $f : X \to X$ is a cellular automaton if and only if there exists $r \in \mathbb{N}$ and a function $f_{\text{loc}} : S^{2r+1} \to S$ such that $f(x)_i = f_{\text{loc}}(x_{[i-r,i+r]})$ for all $x \in X, i \in \mathbb{Z}$. Here, r is called the *radius* of f, and f_{loc} the *local rule* of f. Of course, there are infinitely many possibilities for the radius and the local rule, as one can increase the radius freely. To simplify discussion, we implicitly choose one such pair (r, f_{loc}) for each cellular automaton f. The shift map is of course a cellular automaton, with radius 1 and local rule $\sigma_{\text{loc}} : S^3 \to S$ defined by $\sigma_{\text{loc}}(a, b, c) = c$. Sometimes, it is convenient to have more general local rules $f_{\text{loc}} : S^N \to S$, where $N \subset \mathbb{Z}$ is not necessarily an interval of the form $[-r, r]$. Such N is

called a *neighborhood* for f, and we again implicitly choose a neighborhood for each CA.[17]

In the case $M = \mathbb{N}$, we can find a similar characterization, but the local rule $f_{\text{loc}} : S^{r+1} \to S$ only looks to the right of the current cell, and $f(x)_i = f_{\text{loc}}(x_{[i,i+r]})$. Namely, a morphism clearly cannot look to the left when deciding the new state of the origin in the case $M = \mathbb{N}$. Because it commutes with the shift, this means it can never look to the left. More generally, in both the cases $M = \mathbb{N}$ and $M = \mathbb{Z}$, block maps from $X \subset S^M$ to $Y \subset (S')^M$ can be given local rules $f_{\text{loc}} : S^{2r+1} \to S'$ or $f_{\text{loc}} : S^{r+1} \to S'$. In the case $M = \mathbb{Z}^d$ the combinatorial definitions generalize in the obvious way.

Similarly as for subshifts, dynamical properties of cellular automata can usually be given definitions in terms of words. For example, a cellular automaton $f : X \to X$ on a subshift $X \subset S^{\mathbb{Z}}$ is transitive if and only if for every $u, v \in \mathcal{B}_{2k+1}(X)$ there exist n and $x \in X$ such that $x_{[-k,k]} = u$ and $f^n(x)_{[-k,k]} = v$.

We say a CA is eventually periodic if there exist n, p such that $f^{n+p}(x) = f^n(x)$ for all $x \in X$. If $f^n(x) = x$ for some x, x is said to be *f-periodic*, or sometimes *temporally periodic* when the CA f is fixed. A CA $f : X \to X$ is equicontinuous if and only if it is eventually periodic[18]. The most basic examples of equicontinuous maps are the *symbol maps* $\pi : S \to S$ which (by abuse of notation) are also applied to points $x \in X$ by $\pi(x)_i = \pi(x_i)$. A *symbol permutation* is a bijective symbol map. Cellular automata corresponding to symbol maps are often called *autarkic* in the literature.

There are also properties of interest for cellular automata which do not directly come from dynamical notions. In particular, we say a CA $f : X \to X$ where $X \subset S^{\mathbb{Z}}$ is *captive* if there exists a local rule $f_{\text{loc}} : S^{2r+1} \to S$ such that $f_{\text{loc}}(w) \sqsubset w$ for all $w \in S^{2r+1}$. We say $s \in S$ is a *spreading state* for f if $f_{\text{loc}}(w) = s$ whenever $s \sqsubset w$, and the radius of f is at least 1.[19] A *quiescent state* is a state $s \in S$ such that $f(s^{\mathbb{Z}}) = s^{\mathbb{Z}}$.

We say a CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ with neighborhood $N \subset \mathbb{Z}$ is *permutive* [sic] in the coordinate $j \in N$ if for any $x \in S^{\mathbb{Z}}$, the map

$$a \mapsto f(x_{(-\infty,j-1]} a x_{[j+1,\infty)})_0,$$

[17] A CA on a full shift has a unique minimal neighborhood, but this is not the case in general.

[18] I do not know a reference for this that applies to all subshifts, so we include the proof: Equicontinuity implies eventual periodicity since there are finitely many width-1 traces, which are then eventually periodic (see below). The other direction is clear from the definitions.

[19] Note that, unlike captivity, our definition of a spreading state depends on the choice of f_{loc}. What is actually important is that this state spreads at least as fast as any other computation might happen – at the 'speed of light' – and that it fills the whole point.

where a is put in the jth coordinate on the right, is bijective from S to S. We say f is *left-permutive* if it is permutive in the coordinate j where $j = \min N$. *Right-permutivity* is defined symmetrically, and a CA is called *bipermutive* if it is both left- and right permutive, and has neighborhood size at least 2. We define permutivity similarly in the multidimensional case, and say $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ with neighborhood N is permutive in a coordinate $\vec{v} \in N$ if, when cells of the neighborhood other than $\vec{v}$ are fixed, permuting coordinate $\vec{v}$ permutes the image of f_{loc}. A CA (of any dimension) is said to be *totally extremally permutive* if it is permutive in the cells in the corners of the convex hull of its neighborhood.

If $f : X \to X$ is a CA, then a *spaceship* for f is a point $x \in X$ which is left-asymptotic to a periodic point y, right-asymptotic to a periodic point z, and $f^n(x) \in \mathcal{O}(x)$ for some $n \in \mathbb{N}$. This is slightly more general than the usual definition of spaceships, but it is the correct one for the application in Section 2.2. We say that a spaceship is *nontrivial* when x is not spatially periodic.

The abuse of notation we use with symbol maps – $\pi(x)_i = \pi(x_i)$ – is also used with cellular automata on a few occasions, when we feel it simplifies the discussion.

Definition 1.3.10 *Let X be a subshift, and let $f : X \to X$ be a CA with radius r. If $w \sqsubset X$, we define*

$$f(w) = (f_{\text{loc}}(w_{[0,2r]}), \dots, f_{\text{loc}}(w_{[|w|-2r-1,|w|-1]})) \in \mathcal{B}_{|w|-2r}(X)$$

when $|w| \geq 2r + 1$, and $f(w)$ is the empty word if $|w| \leq 2r$.

When discussing CA on product subshifts $X \times Y \subset S^{\mathbb{Z}} \times (S')^{\mathbb{Z}}$ where $X \subset S^{\mathbb{Z}}, Y \subset (S')^{\mathbb{Z}}$ are subshifts, it is more convenient to think of the products as subshifts of $(S \times S')^{\mathbb{Z}}$, in the obvious way. We sometimes refer to $\pi_i(x)$ as the ith *track* of x. More generally, we use the terminology of tracks for subshifts $Z \subset (S \times S')^{\mathbb{Z}}$. When $f : X \to X$ and $g : Y \to Y$ are cellular automata, their *Cartesian product* is the CA $f \times g : X \times Y \to X \times Y$ where f is applied in the X-component, and g in the Y-component. We use the term 'Cartesian product' instead of just 'product' to distinguish this from the composition operator $\circ$. These notions of course generalize to any finite collection of subshifts.

The study of subshifts encompasses the study of cellular automata in the following sense. Let X be an M-subshift, and let $f : X \to X$ be a cellular automaton on X. The *spacetime subshift* of f is the dynamical $(M \times \mathbb{Z})$-system (Y, T') where $Y = \{y \in X^{\mathbb{Z}} \mid \forall i \in \mathbb{Z} : y_{i+1} = f(y_i)\}$ with the action $((T^{m,n}(y))_i)_j = (y_{i+n})_{j+m}$. The elements of Y are called the *spacetime diagrams* of f. Usually, we have $M = \mathbb{Z}$, and we then call the y_i *rows* of y and $\dots (y_{-2})_i (y_{-1})_i . (y_0)_i (y_1)_i (y_2)_i \dots$ *columns* of y. The rows of

spacetime diagrams of f are exactly the limit set of f. If f is surjective, then the spacetime subshifts contain complete information about f. Similarly, we define the *one-way spacetime subshift* and *diagrams* of f, as the $(M \times \mathbb{N})$-system containing the positive orbits. Given a CA $f : X \to X$ for $X \subset S^{\mathbb{Z}}$, the *width-n trace subshift* of f of a cellular automaton is the subshift

$$\{(x_{[0,n-1]}, f(x)_{[0,n-1]}, f^2(x)_{[0,n-1]}, \ldots) \mid x \in X\} \subset (S^n)^{\mathbb{N}}.$$

Again, there is a natural two-way variant where the trace is two-way infinite.

We define the entropy of a CA using its trace subshift: the *entropy* of a CA $f : X \to X$ is

$$\lim_{n\to\infty} h_{\text{top}}(X_n),$$

where X_n is the width-n trace subshift of f.

We discuss a general concept that is useful for studying CA on multidimensional subshifts $X \subset S^{\mathbb{Z}^d}$. Namely, we define actions of matrices on points. We denote by $SL_d(\mathbb{Z})$ the set of $d \times d$ matrices over $\mathbb{Z}$ that, as functions acting on column vectors from the left, map $\mathbb{Z}^d$ bijectively to itself. It is well-known that these are exactly the matrices whose determinant is invertible in $\mathbb{Z}$, that is, ± 1. For a point $x \in S^{\mathbb{Z}^d}$ and $A \in SL_d(\mathbb{Z})$, we define $A(x) \in S^{\mathbb{Z}^d}$ by $A(x)_{\vec{n}} = x_{A(\vec{n})}$ for all $\vec{n} \in \mathbb{Z}^d$. (Here, the choice of A over A^{-1} in $x_{A(\vec{n})}$ is by analogy with how shift maps are defined: we always transform the view, not the point.) For a subshift $X \subset S^{\mathbb{Z}^d}$, we define $A(X) = \{A(x) \mid x \in X\}$. From the linearity and bijectivity of A it follows that $A(X)$ is also a subshift. For a cellular automaton $f : X \to X$, we define $A(f) : A(X) \to A(X)$ by $A(f)(x) = A(f(A^{-1}(x)))$ for all $x \in X$. It is easy to see that $A(f)$ is a cellular automaton, and if $N \subset \mathbb{Z}^d$ is the neighborhood of f, then $A^{-1}(N)$ is that of $A(f)$. Moreover, $A(f)$ usually shares all dynamical and computational properties of f. Also, if f and g are CA on $S^{\mathbb{Z}^d}$, then $A(f \circ g) = A(f) \circ A(g)$.

1.3.3 Nilpotency and Periodicity

As nilpotency is important in Chapter 2, we discuss nilpotency of (multidimensional) cellular automata and its several equivalent definitions in some detail. First, this is equivalent to having a singleton limit set [CPY89]. Of course, since the limit set is a subshift, it is then $\{0^{\mathbb{Z}^d}\}$ for some symbol $0 \in S$. We give two more equivalent definitions. The first is weak nilpotency, which is proved equivalent in the case of a transitive subshift in [GR10a], and in more generality in [Sal12] (we give the proof below). The second one, asymptotic nilpotency, is equivalent to nilpotency in the case of a full shift in all dimensions. This is proved in [GR08] in one dimension, and in more generality in [Sal12]. In one dimension, the result is in fact true for

all SFTs. The transitive case is proved in [GR10a], and the general case is noted in [Sal12].

Definition 1.3.11 *Let $X \subset S^{\mathbb{Z}^d}$ be a subshift. A CA $f : X \to X$ is* weakly nilpotent *if*

$$\exists a \in S : \forall x \in X : \exists n \in \mathbb{N} : f^n(x) = a^{\mathbb{Z}^d}.$$

It is asymptotically nilpotent *if*

$$\exists a \in S : \forall x \in X : \exists n \in \mathbb{N} : \forall m \geq n : f^m(x)_{\vec{0}} = a$$

We sometimes prefix the symbol a (usually $a = 0$) in these terms, and talk about, for example, 0-asymptotic nilpotency. A CA is weakly nilpotent if every point maps to the point $0^{\mathbb{Z}^d}$ after finitely many steps, but the number of steps needed may change depending on the point. Asymptotic nilpotency means that every individual cell eventually becomes zero (and stays that way forever) no matter what the initial point is. In other words, the width-1 trace subshift contains only points of the form $w0^\infty$.

Asymptotic nilpotency can also be defined in terms of the limit point operator ω: a cellular automaton is asymptotically nilpotent if and only if

$$\exists x^0 \in X : \forall x \in X : \omega_f(\{x\}) = \{x^0\},$$

that is, $|\omega_f| = 1$. The 'if' is because if there exists such x^0, then it must be unary:

$$\omega_f(\{x\}) = \{x^0\} \implies \omega_f(\{\sigma(x)\}) = \{\sigma(x^0)\} = \{x^0\},$$

so $x^0 = \sigma(x^0)$.

Proposition 1.3.12 (Proposition 1 in [Sal12]) *Let $X \subset S^{\mathbb{Z}^d}$ be a subshift. Then a cellular automaton f on X is nilpotent if and only if it is weakly nilpotent.*

Proof. Suppose on the contrary that the CA $f : X \to X$ is weakly nilpotent but not nilpotent for some subshift $X \subset S^{\mathbb{Z}^d}$. Since nilpotency is equivalent to the limit set being a singleton, there exists a point x in the limit set of f with $x_{\vec{0}} \neq 0$, for the symbol 0 such that all points reach the all-0 point in finitely many steps. Since x is in the limit set, it has an infinite chain $(x^i)_{i\in\mathbb{N}}$ of preimages. If r is the radius of f, then since 0 is a quiescent state, there must exist a sequence of vectors $(v^i)_{i\in\mathbb{N}}$ such that $|v^i - v^{i+1}| \leq r$ and $\sigma^{v^i}(x^i)_{\vec{0}} \neq 0$ for all $i \in \mathbb{N}$.

Let y be a limit of a converging subsequence of $(\sigma^{v^i}(x^i))_{i\in\mathbb{N}}$. Since f is weakly nilpotent, there exists $n \in \mathbb{N}$ such that $f^n(y) = 0^{\mathbb{Z}^d}$. Let $i \in \mathbb{N}$ be such that

$$y_{B_{2rn}(\vec{0})} = \sigma^{v^{i+n}}(x^{i+n})_{B_{2rn}(\vec{0})}. \tag{1.1}$$

By definition of the x^i and v^i, we have that $f^n(x^{i+n}) = x^i$ and thus

$$f^n(y)_{B_{rn}(\vec{0})} = \sigma^{v^{i+n}}(x^i)_{B_{rn}(\vec{0})}$$

contains a nonzero symbol, a contradiction, since we assumed $f^n(y) = 0^{\mathbb{Z}^d}$. ■

As in the one-dimensional case, we say $x, y \in S^{\mathbb{Z}^d}$ are asymptotic if they differ in only finitely many cells. We also define a-finiteness for points of $S^{\mathbb{Z}^d}$ in the obvious way.

Theorem 1.3.13 (Theorem 4 in [Sal12]) *Let $X \subset S^{\mathbb{Z}^d}$ be an SFT where 0-finite points are dense. Then a cellular automaton f on X is 0-nilpotent if and only if it is asymptotically 0-nilpotent.*

The denseness of finite points is not a property that is often assumed from multidimensional SFTs. A more commonly used gluing property is so-called strong irreducibility. Many other gluing properties have been defined, and some are listed for example in [BPS10].

Definition 1.3.14 *Let $X \subset S^{\mathbb{Z}^d}$ be a subshift. We say X is* strongly irreducible *if there exists $m \in \mathbb{N}$ such that for any $y, z \in X$ and any finite sets $N, N' \subset \mathbb{Z}^d$ with $\min\{|v - v'| \mid v \in N, v' \in N'\} \geq m$, there exists a point $x \in X$ with $x_N = y_N$ and $x_{N'} = z_{N'}$.*

By compactness, the sets N and N' can then be taken infinite as well, and we easily obtain the following lemma.

Lemma 1.3.15 *Let $X \subset S^{\mathbb{Z}^d}$ be a strongly irreducible SFT and let $x \in X$. Then the points asymptotic to x are dense in X.*

Since a subshift has to have the point $0^{\mathbb{Z}^d}$ in order to support asymptotically nilpotent cellular automata, we see that in our case of interest, strong irreducibility is a stronger requirement than the density of 0-finite points:

Corollary 1.3.16 *Let $X \subset S^{\mathbb{Z}^d}$ be a strongly irreducible SFT. Then a cellular automaton f on X is nilpotent if and only if it is asymptotically nilpotent.*

Proof. We only need to show that if f is asymptotically nilpotent, then it is nilpotent. Of course, if f is 0-asymptotically nilpotent, then $0^{\mathbb{Z}^d} \in X$. But then by the previous lemma, 0-finite points are dense in X, and thus f is nilpotent by Theorem 1.3.13. ■

Theorem 1.3.17 (Corollary 1 in [Sal12]) *Let $X \subset S^{\mathbb{Z}}$ be an SFT. Then a cellular automaton f on X is nilpotent if and only if it is asymptotically nilpotent.*

The equivalence of nilpotency and asymptotic nilpotency can be seen as stating that the trace of a CA is weakly nilpotent (as a subshift) if and only if the CA itself is. While it is not in general true that if the trace is eventually periodic, then the CA is as well (the Spreading State CA $f_{\text{loc}} : \{0,1\}^3 \to \{0,1\}, f_{\text{loc}}(a,b,c) = \min\{a,b,c\}$ is a counterexample), at least if all traces are periodic, then the CA is as well. This is a direct corollary of Lemma 1.3.6.

Lemma 1.3.18 *Let X be an arbitrary subshift. If the width-1 trace of $f : X \to X$ is periodic, then f is periodic.*

1.3.4 Some Standard Tools

Combining Theorem 8.1.16 and Corollary 4.4.9 of [LM95], and Corollary 2.21 of [Fio00], we get the following version of the well-known Garden of Eden Theorem.

Definition 1.3.19 *Let $X \subset S^M$ be a subshift. A CA $f : X \to X$ is said to be* preinjective *if whenever $\{i \in M \mid x_i \neq y_i\}$ is finite and nonempty for $x, y \in X$, we have $f(x) \neq f(y)$.*

Injectivity of course implies preinjectivity. In the case $M = \mathbb{Z}$, the condition that $\{i \in \mathbb{Z} \mid x_i \neq y_i\}$ is finite means precisely that x and y are asymptotic.

Lemma 1.3.20 (Garden of Eden Theorem) *Let X be a mixing sofic shift. If the CA $f : X \to X$ is preinjective, then it is surjective. If f is surjective and X is an SFT, then f is preinjective.*

In particular, it follows that an injective cellular automaton is surjective. This is no more true if X is not mixing, as shown by [Fio00], and we give some examples in Section 2.2 as well. Interestingly, the fact that injective cellular automata are surjective is true on full shifts in very high (perhaps full) generality: A huge class of groups is known where injectivity implies surjectivity [CSC10]. Groups where this implication is true are called surjunctive. They were introduced in [Got73] in 1973, and it is still not know whether there exists a group which is not surjunctive.

An important tool from symbolic dynamics is the Extension Lemma, which is useful for constructing cellular automata with desired properties:

Lemma 1.3.21 (Extension Lemma [Boy83]) *Let T, T' and U be subshifts and let $f : T' \to U$ be a block map, so that the following conditions are satisfied:*

- *U is a mixing SFT.*

- *T' is a subshift of T.*
- *the period of any periodic point of T is divisible by the period of some periodic point of U.*

Then, f can be extended to a block map $g : T \to U$ so that $g|_{T'} = f$.

By definition, all cellular automata commute with shift maps. Conversely, if a cellular automaton on a mixing SFT X commutes with all other cellular automata, then it is a shift map, with a single caveat. This is a variant of a result of Ryan from [Rya72], although the endomorphism case is a bit easier. We define the *center* of a monoid M to be the set of elements $a \in M$ such that $ba = ab$ for all $b \in M$.

Lemma 1.3.22 *If X is a mixing SFT, then f is in the center of* $\mathrm{End}(X)$ *if and only if*

- *f is a shift map, or*
- *X has a single unary point $a^{\mathbb{Z}}$ and $f(x) = a^{\mathbb{Z}}$ for all $x \in X$.*

Proof. First, suppose $f(X)$ is a single unary point. If X has another unary point $b^{\mathbb{Z}}$, then $g(x) = b^{\mathbb{Z}}$ clearly does not commute with f. If there is no other unary point in X, then for all $g \in \mathrm{End}(X)$ we have $g(a^{\mathbb{Z}}) = a^{\mathbb{Z}}$, so that f is indeed in the center.

Next, suppose that $f(X)$ is not a single unary point, and for all i there exists $x \in X$ such that $f(x)_0 \neq x_i$. We may assume f has one-sided radius. We first show that there exists a spatially periodic point x with $f(x) \notin \mathcal{O}(x)$ such that $f(x)$ is not unary. For this, let $u \sqsubset X$ be an unbordered word longer than the one-sided radius of f, and the window size and mixing distance of X. Let also v, v' be two words such that $f(v)$ contains two distinct symbols, $|v| = |v'| < |u|$ and $uvu, uv'u \sqsubset X$. Let $z = (uvu)^{\mathbb{Z}}$. If $f(z) \notin \mathcal{O}(z)$, we are done. Otherwise, let $f(z) = \sigma^j(z)$ where $0 \leq j < |uvu|$ and let $y = (uv'u(uvu)^k)^{\mathbb{Z}}$ where $k \geq 2$ is arbitrary. We necessarily have $f(y)_i = f(z)_i$ for $i \in [|uv'|, |uv'u(uvu)^k| - 1]$, which – due to the fact u is unbordered – already determines that if $f(y) \in \mathcal{O}(y)$, then $f(y) = \sigma^j(y)$. If $f(y) \notin \mathcal{O}(y)$, then we are again finished. Otherwise, let w be such that $uwu \sqsubset X$, and for all x, $x_{[0,|w|-1]} = w \implies f(x)_0 \neq x_j$. Now, choose

$$x = (uv'u(uvu)^{|w|}w)^{\mathbb{Z}}.$$

Since $v \neq v'$ and $|v| = |v'| < |u|$, it is easy to see that $f(x) \in \mathcal{O}(x) \implies f(x) = \sigma^j(x)$. But this is impossible due to the occurrence of w.

Now, we have a periodic point x such that $f(x)$ is not in its orbit and $f(x)$ is not unary. The subshifts $X' = \mathcal{O}(x)$ and $X'' = \mathcal{O}(f(x))$ are then disjoint closed sets, so the map

$$g'(x) = \begin{cases} x & \text{if } x \in X' \\ \sigma(x) & \text{if } x \in X'' \end{cases}$$

is a cellular automaton on the subshift $X' \cup X''$. Since $X' \cup X'' \subset X$, we can think of g' as a block map from $X' \cup X''$ into X, and by the Extension Lemma 1.3.21, g' extends to a cellular automaton $g : X \to X$, and then

$$g(f(x)) = \sigma(f(x)) \neq f(x) = f(g(x)),$$

so that f is not in the center. ■

Ryan's precise result in [Rya72] is that if a surjective map on the full shift commutes with all automorphisms, then it is a shift map. Ryan's theorem can be recovered by constructing the CA g more carefully to make it reversible. We skip the proof as Lemma 1.3.22 is more than enough for us.

1.4 Computation and Counter Machines

1.4.1 Counter Machines

Counter machines are one of the many equivalent ways to formalize the idea of computation. This is also one of the simplest models. A counter machine is a finite state machine equipped with a finite number of counters, each of which can contain any natural number. We pay most attention to this model since, unlike the more commonly used (and computationally equivalent) model of Turing machines, simulating counter machines can be done on countable SFTs.[20] As we will, on occasion, make quite detailed constructions with such machines, we give a precise definition.

Definition 1.4.1 *Let $k \in \mathbb{N}$. A k-*counter machine *is defined as a triplet $M = (\Sigma, k, \delta)$, where Σ is a finite* state set *and*

$$\delta \subset (\Sigma \times [1, k] \times \{Z, P\} \times \Sigma) \cup (\Sigma \times [1, k] \times \{-1, 0, 1\} \times \Sigma)$$

the transition relation. *A* configuration of M *is an element of $\Sigma \times \mathbb{N}^k$. The machine M operates in possibly nondeterministic steps as directed by δ, in the sense that M induces a relation*

$$(\Rightarrow_M) \subset (\Sigma \times \mathbb{N}^k) \times (\Sigma \times \mathbb{N}^k)$$

by $(p, n_1, \ldots, n_k) \Rightarrow_M (q, m_1, \ldots, m_k)$ if

[20] On *two*-dimensional countable SFTs, Turing machines can be used as well. For example [JV11] constructs two-dimensional countable SFTs with interesting computational and dynamical properties based on Turing machines.

- $(p, j, Z, q) \in \delta \wedge n_j = 0 \wedge \forall i : m_i = n_i$,
- $(p, j, P, q) \in \delta \wedge n_j > 0 \wedge \forall i : m_i = n_i$,
- $(p, j, 1, q) \in \delta \wedge m_j = n_j + 1 \wedge \forall i \neq j : m_i = n_i$,
- $(p, j, 0, q) \in \delta \wedge \forall i : m_i = n_i$, *or*
- $(p, j, -1, q) \in \delta \wedge m_j = n_j - 1 \wedge \forall i \neq j : m_i = n_i$.

The interpretation of $(q, n_1, \ldots, n_k)$ is of course that the machine is in state q with counter values $n_1, \ldots, n_k$. We denote the transitive and reflexive closure of $\Rightarrow_M$ by $\Rightarrow_M^*$, and if $a \Rightarrow_M b$, we call a a *predecessor* of b and b a *successor* of a. We usually do not have explicit initial and final states, as this does not affect the semantics of the machine. Instead, we say that a configuration is *initial* if it has no predecessor, and *final* if it has no successor, and dedicate states for particular purposes as needed.

We say the machine M is *(structurally) deterministic* if for any pair of distinct tuples (p_1, i_1, j_1, q_1), $(p_2, i_2, j_2, q_2) \in \delta$, if $p_1 = p_2$ then $i_1 = i_2$ and $\{j_1, j_2\} = \{Z, P\}$. That is, from any state, either there is at most one way to continue, or there are exactly two ways, depending on whether a particular counter is 0. Dually, we call the machine *(structurally) reversible* if for any $(p_1, i_1, j_1, q_1), (p_2, i_2, j_2, q_2) \in \delta$, if $q_1 = q_2$ then $i_1 = i_2$ and $\{j_1, j_2\} = \{Z, P\}$. That is, every state can either be entered in at most one way, or there are exactly two ways, and the previous state is determined by whether a particular counter is 0.

For a deterministic machine M, a configuration $(p, n_1, \ldots, n_k)$ is halting in exactly four cases. Namely, this happens if δ contains

- no tuple of the form (p, i, j, q) for $j \in \{-1, 0, 1, Z\}$ and $n_i = 0$,
- no tuple of the form (p, i, j, q) for $j \in \{-1, 0, 1, P\}$ and $n_i > 0$, or
- a tuple $(p, i, -1, q)$ and $n_i = 0$.

The first two cases mean that the counter machine has no rule that determines the new state, and the third means that the machine attempts to decrement a counter below 0. If none of these cases occurs, then $(p, n_1, \ldots, n_k)$ has a unique successor configuration.

We state some direct corollaries of the definitions as a lemma.

Lemma 1.4.2 *If M is deterministic, then $\Rightarrow_M$ is a partial function, that is,*

$$a, b, c \in \Sigma \times \mathbb{N}^k \wedge (a \Rightarrow_M b) \wedge (a \Rightarrow_M c) \implies b = c.$$

If M is reversible, then it is an 'injective relation', in the sense that

$$a, b, c \in \Sigma \times \mathbb{N}^k \wedge (a \Rightarrow_M c) \wedge (b \Rightarrow_M c) \implies a = b.$$

If M is deterministic and reversible, there exists a deterministic and reversible counter machine M^{-1} such that

$$(a \Rightarrow_M b) \iff (b \Rightarrow_{M^{-1}} a).$$

Note that (the transition relation of) a reversible counter machine need not be bijective, only injective. Furthermore, there exist injective counter machines which are not reversible with this definition (although the difference is minor). Similarly, a machine where there is a unique transition from each state is not necessarily deterministic with our definition. The classical reference for counter machines is [Min67], although our definitions are essentially from [Mor96].

Given a counter machine M, we write G_M for the directed graph (V_M, E_M) where $V_M = \Sigma \times \mathbb{N}^k$ and $E_M = \{(a, b) \in V_M^2 \mid a \Rightarrow_M b\}$, called the *configuration graph* of M. Note that if M is deterministic and reversible, then G_M is a disjoint union of paths.

There is a convenient way of converting an arbitrary deterministic counter machine into a deterministic and reversible machine. The following result can be extracted from the proof of Theorem 3.1 in [Mor96]. Namely, in Lemma 1.4.3, we state the specific way in which the reversible counter machine constructed in [Mor96] simulates the original one, since the theorem, as stated in [Mor96], is hard to use as a black box.

Lemma 1.4.3 (Proved as Theorem 3.1 of [Mor96]) *For any deterministic k-counter machine $M = (\Sigma, k, \delta)$ there exists a deterministic and reversible $(k+2)$-counter machine $M' = (\Sigma \cup \Delta, k+2, \delta')$ such that for all $m_i, n_i, h \in \mathbb{N}$ and $q, p \in \Sigma$,*

$$(q, m_1, \ldots, m_k) \Rightarrow_M (p, n_1, \ldots, n_k)$$

holds if and only if there exists $\ell \in \mathbb{N}$ with

$$(q, m_1, \ldots, m_k, h, 0) \Rightarrow_{M'}^* (p, n_1, \ldots, n_k, \ell, 0)$$

where the intermediate states of the computation are in Δ. Furthermore, if there are no $\Rightarrow_M$-transitions to (resp. from) state q in δ, then there are no $\Rightarrow_{M'}$-transitions to (resp. from) q in δ'.

This gives us a rather direct simulation of a deterministic counter machine by a reversible one. Note that we do not have much control over the $(k+1)$th counter – this is where the information needed for running the machine backwards is stored. The precise transformation from h to ℓ is that when a bit of information is forgotten by M (that is, a configuration with two distinct preimages is entered) this bit is stored in the $(k+1)$th counter

by $\ell = 2h + b$, where b is the bit that was forgotten (that is, b is 0 or 1 depending on what the previous configuration was). The transition along the states in Δ performs the computation $h \mapsto 2h + b$ in a deterministic and reversible fashion, and then returns control to the states Σ.

1.4.2 The Arithmetical Hierarchy

Let ϕ be a first-order arithmetical predicate. That is, ϕ is a predicate that contains some number of free variables, some existentially and universally quantified variables, addition, multiplication, constants in $\mathbb{N}$, the relation $\leq$ and Boolean operations, and when the free variables are given values in $\mathbb{N}$, it is either true or false. If ϕ contains only bounded quantifiers (variables are only quantified up to a function of other variables), then we say ϕ is Σ_0^0 and Π_0^0. For all $n > 0$, we say ϕ is Σ_n^0 if it is equivalent to a formula of the form $\exists k : \psi$ where ψ is Π_{n-1}^0 (and contains k as a free variable), and ϕ is Π_n^0, if it is equivalent to a formula of the form $\forall k : \psi$ where ψ is Σ_{n-1}^0. This classification of arithmetical formulas is called the *arithmetical hierarchy* (see e.g. [Odi89, Chapter IV.1] for an introduction to the topic). We write Φ_k for the set of formulas with k free variables, and other variables quantified with bounded quantifiers. The nonstandard quantifier $\exists^\infty n : \phi(n)$ has the meaning 'there exist infinitely many n such that $\phi(n)$.' This quantifier is useful due to the following lemma.

Lemma 1.4.4 (Dual of Lemma 2 in [KSW60]) *Let $k \in \mathbb{N}$ and $\phi \in \Phi_{2k+1}$. Then there exists $\psi \in \Phi_{k+1}$, uniformly computable from ϕ and k, such that*

$$\exists n_1 : \forall n_2 : \cdots \exists n_{2k-1} : \forall n_{2k} : \exists n_{2k+1} : \phi(n_1, \ldots, n_{2k+1})$$

is equivalent to

$$\exists n_1 : \exists^\infty n_2 : \exists^\infty n_3 : \cdots \exists^\infty n_k \exists^\infty n_{k+1} : \psi(n_1, \ldots, n_{k+1}).$$

A subset A of $\mathbb{N}$ is Σ_n^0 or Π_n^0, if $A = \{x \in \mathbb{N} \mid \phi(x) \text{ holds}\}$ for some ϕ with the corresponding classification. It is known that the Σ_1^0 sets are exactly the recursively enumerable sets, and the Π_1^0 sets their complements. The recursive sets form precisely the intersection $\Sigma_1^0 \cap \Pi_1^0$. When classifying sets of objects other than natural numbers (e.g. words), we assume that the objects are in some natural and computable bijection with $\mathbb{N}$. Also, a subshift is given the same classification as its language, so that, for example, sofic shifts are Π_1^0 subshifts, and in general a subshift is Π_1^0 if and only if there exists a Turing machine (or counter machine) that outputs a list of forbidden patterns that defines it. Similarly, a subshift X is recursive if there is a Turing machine that, given a word w, eventually outputs $w \sqsubset X$

or $w \not\sqsubset X$, depending on which is the case. See [CR98] for a general survey on Π_1^0 sets.

A subset $A \subset \mathbb{N}$ is *many-one reducible* (or simply *reducible*) to another set $B \subset \mathbb{N}$, if there exists a computable function $f : \mathbb{N} \to \mathbb{N}$ such that $x \in A$ iff $f(x) \in B$. If every set in a class $\mathcal{C}$ is reducible to B, then B is said to be *$\mathcal{C}$-hard*. If, in addition, B is in $\mathcal{C}$, then B is *$\mathcal{C}$-complete*.

It is well-known that the computational power for the formulas does not change if general recursive languages are allowed in place of the formulas with only bounded quantifiers, in the sense that Σ_1^0 consists of precisely the recursively enumerable languages, and in general Σ_k^0 contains the kth Turing jump of the empty language.

1.5 What is 'Simple'?

We now make the idea of simplicity precise, by defining three properties that an endomorphism monoid may or may not have. The three properties we define are predictability, sparseness, and being finitely generated. These will be our canonical measuring sticks of simplicity, and we try to investigate them for the subshifts of each of the chapters. Endomorphism monoids of mixing SFT are not simple in the sense of any of these definitions.

The first definition, being finitely generated, is rather self-explanatory.

Definition 1.5.1 *The endomorphism monoid is* finitely generated *if there exists a finite set of endomorphisms F such that all endomorphisms are composed of those in F.*

It is well known that the endomorphism monoid of a mixing SFT is not simple in this sense:

Proposition 1.5.2 *The endomorphism monoid of an infinite mixing SFT is not finitely generated.*

Proof. By Theorem 7.8 in [BLR88], the automorphism group is not finitely generated. On mixing SFTs, the product of two endomorphisms f, g is an automorphism if and only both f and g are automorphisms. This can be seen as follows: By Lemma 1.3.20, all injective cellular automata are surjective. If $g \circ f$ is an automorphism, then f is injective, and it follows that f is surjective. Since g has to be injective on the image of f, it is injective, and thus surjective as well. This means that if the endomorphism monoid were finitely generated, then the finitely many automorphisms in the set of generators would generate the automorphism group. Thus, the endomorphism monoid is not finitely generated. ■

We choose the following as our canonical notion of computational simplicity:

Definition 1.5.3 *The endomorphism monoid of $X \subset S^{\mathbb{Z}}$ is* predictable *if, given a local rule $f_{\text{loc}} : S^{2r+1} \to S$ corresponding to a CA $f : X \to X$ and a pair of words $u, v \sqsubset X$, it is decidable whether there exists $n \in \mathbb{N}$ and a point $x \in X$ with $x_{[0,|u|-1]} = u$ such that $f^n(x)_{[0,|v|-1]} = v$. If this problem is decidable for a single f, we say f is predictable.*

Of course, if there is an unpredictable endomorphism, then the endomorphism monoid is not predictable either.

This notion captures, into a yes/no question, whether the subshift X can support dynamics for which the reachability problem for pairs of words is undecidable. There are many other ways to state this basic idea, such as considering, instead, whether a given point eventually evolves into another one. However, such a definition often either hides computation in the description of the points, or requires periodic points, which we do not have in Chapter 3. The reachability problem is (up to a subtle technical difference[21]) referred to as the *halting problem* in [DKVB06].

Proposition 1.5.4 *The endomorphism monoid of an infinite mixing SFT is not predictable.*

Proof. First, the problem is very easy on a full shift if we can choose the alphabet, and we begin with this case. We choose the alphabet $S = ((\Sigma \cup \{\leftarrow, \rightarrow\}) \times A) \cup \{\#\}$, where Σ is the set of states of a Turing machine M and A is the alphabet of M. The state $\#$ will be spreading for the CA we construct. For $x \in S^{\mathbb{Z}}$, we write $\pi_1(x)$ for the point y with $y_i = a$ if $x_i = (a, b)$, and $y_i = \#$ otherwise. If $\pi_1(x)$ is locally not in the countable SFT $Y = \mathcal{B}^{-1}(\rightarrow^* \Sigma \leftarrow^*)$, the CA outputs the spreading state $\#$. On points where $\pi_1(x) \in Y$, the Turing machine M is simulated in the obvious way.

Now, it is easy to choose the machine M so that the prediction problem is undecidable – all we need to do is to make sure the fact that the tape is infinite in both directions is not a problem. For this, we can take the alphabet A to contain left and right border symbols $\#_\ell$ and $\#_r$, such that the head cannot escape from between them, the left border symbol never moves and the right border symbol is moved to the right as space is needed, and can also be moved back to the left by the Turing machine. Nothing is read from the other side of the borders. Now, even restricting to pairs of words of the form $((\#_\ell w \#_r, \rightarrow s \leftarrow^{|w|}), (\#_\ell w' \#_r, \rightarrow t \leftarrow^{|w'|}))$, where $s, t \in \Sigma$ are states of the Turing machine (on top of some symbol) and $w, w' \in A^*$, the prediction problem for the CA is clearly undecidable if we choose the Turing machine properly. By blocking r symbols together, where r is the

[21] Unlike [DKVB06], we do not require that the system $f : X \to X$ be *effective*. However, the symbolic dynamical system $f : X \to X$ is effective whenever X has a recursive language, and this is usually the case in this thesis.

radius of this CA, we obtain a CA on the full shift $(S^r)^{\mathbb{Z}}$ which has radius 1, and an undecidable prediction problem.

As for the case of a general mixing SFT $X \subset S^{\mathbb{Z}}$, let m be a window size and a mixing distance for X, and let k be the minimal alphabet size needed for the construction in the previous paragraph, with a CA with radius 1. Use Lemma 1.3.7 to obtain an unbordered word v of sufficient length that we can find $k+1$ words $u_0, \dots, u_k \sqsubset X$, all of the same length $|u_i| < |v|$, such that $X' = \mathcal{B}^{-1}((vu_1 + \cdots + vu_k)^*)$ is an SFT and a subset of X. For this, we can first choose the $k+1$ words u_i' of the same length, then choose v such that $|v| > |u_i'| + 2m$, and finally extend the words u_i' by words of length m on both sides to obtain words u_i such that $vu_iv \sqsubset X$. Let $J = |v|$, $N = |u_i|$ and $U = \{u_0, \dots, u_k\}$.

Now, there is a unique way to parse each point of X' into a concatenation of the vu_i, since v is unbordered and $N < J$. Given any radius 1 cellular automaton g on a full shift $[1,k]^{\mathbb{Z}}$, we construct a corresponding CA on X. First, extend g to the full shift $[0,k]^{\mathbb{Z}}$ by making 0 a spreading state.

Now, we define an auxiliary block map $h : X \to (S \dot\cup \{\#, \$\})^{\mathbb{Z}}$ as follows:

$$h(x)_k = \begin{cases} \#, & \text{if } \exists j, j' : k \in [j, j'] \wedge x_{[j,j']} = v, \\ x_k, & \text{if } \exists j, j' : k \in [j+J, j'-J] \wedge x_{[j,j']} \in vUv, \text{ and} \\ \$, & \text{otherwise.} \end{cases}$$

We define $f(x)$ as a function of $(x, h(x))$ as follows:

- If $h(x)_i \in \{\#, \$\}$, then $f(x)_i = x_i$.
- If $h(x)_{[j,j']} = u_i \#^J u_{i'} \#^J u_{i''}$, then

$$f(x)_{[j+J+N, j'-J-N]} = u_{g(i,i',i'')}.$$

- If $h(x)_{[j+J+N, j'-J-N]} \in U$ but $h(x)_{[j,j']} \notin U\#^J U\#^J U$, then

$$f(x)_{[j+J+N, j'-J-N]} = u_0.$$

The three cases do not overlap, and the new value of each coordinate is determined by exactly one of them. Furthermore, the locations of vs never change, and $f(x)_{[j,j']} \in vUv \iff x_{[j,j']} \in vUv$, so the image of each point in X is in X. Now, f simulates g on X', and if $j_i, j_i' \in [1,k]$ for all $i \in [1,n]$, then the word $\#^J u_{j_1} \#^J \dots \#^J u_{j_n} \#^J$ is reachable from $\#^J u_{j_1'} \#^J \dots \#^J u_{j_n'} \#^J$ in the action of f if and only if $j_1 \cdots j_n$ is reachable from $j_1' \cdots j_n'$ in the action of g. This of course means that f is not predictable for suitable g. ■

Roots of predictable CA are also predictable, in the following sense.

Lemma 1.5.5 *Let $X \subset S^{\mathbb{Z}}$ be a recursive subshift. Suppose there exist $m \in \mathbb{N}$ and $p > 0$ such that given a local rule $f_{\mathrm{loc}} : S^{2r+1} \to S$ corresponding to a CA $f : X \to X$ and a pair of words $u, v \sqsubset X$, it is decidable whether there exists $j \in \mathbb{N}$ and a point $x \in X$ with $x_{[0,|u|-1]} = u$ such that $f^{m+jp}(x)_{[0,|v|-1]} = v$. Then the endomorphism monoid of X is predictable.*

Proof. Given $f_{\mathrm{loc}} : S^{2r+1} \to S$, u and v, we need to decide whether there exists $n \in \mathbb{N}$ and a point $x \in X$ with $x_{[0,|u|-1]} = u$ such that $f^n(x)_{[0,|v|-1]} = v$. First, it is clear that it is decidable whether this is true for some $0 \leq n \leq m$. Since X is recursive, we can easily enumerate the preimages $W = \bigcup_{i=0}^{p-1} f^{-1}(\{v\})$. It is then enough to check whether there exist $w \in W$, $j \in \mathbb{N}$ and $x \in X$ with $x_{[0,|u|-1]} = u$ such that $f^{m+jp}(x)_{[-(|w|-|v|)/2,(|w|+|v|)/2-1]} = w$, which is decidable by the assumption, and the fact that W is finite. ■

In [BLR88], $\mathrm{Aut}(X)$ for a mixing SFT $X \subset S^{\mathbb{Z}}$ is discussed in detail. The *symmetry of* X is defined as the relative asymptotic density of $\mathrm{Aut}(X)$ in the set of all cellular automata on X:

$$s(X) = \limsup_{n\to\infty} \frac{1}{n} \log\log |\mathrm{Aut}(X)_n|,$$

where $\mathrm{Aut}(X)_n$ denotes the set of bijective cellular automata on X that can be defined on the neighborhood $[-\lfloor n/2 \rfloor, \lceil n/2 \rceil]$. Inspired by this, we define the following.

Definition 1.5.6 *Let $\mathcal{C}$ be a family of cellular automata on $S^{\mathbb{Z}}$. The* density *of $\mathcal{C}$ is defined as*

$$d(\mathcal{C}) = \limsup_{n\to\infty} \frac{1}{n} \log_{|S|} \log_{|S|} |\mathcal{C}_n|, \tag{1.2}$$

where $\mathcal{C}_n$ denotes the set of cellular automata in $\mathcal{C}$ that can be defined on the neighborhood $[-\lfloor n/2 \rfloor, \lceil n/2 \rceil]$ (or when d-dimensional subshifts are considered, $[-\lfloor n/2 \rfloor, \lceil n/2 \rceil]^d$).

Definition 1.5.7 *A set of cellular automata (usually the endomorphism monoid) is* sparse *if it has density* 0.

We usually discuss the density of a subset of cellular automata on a fixed full shift with alphabet S, and then base $|S|$ makes the most sense for the logarithm, since then the set $\mathcal{CA}$ of all cellular automata on $S^{\mathbb{Z}}$ has density 1, as

$$\frac{1}{n} \log\log |\mathcal{CA}_n| = \frac{1}{n} \log\log |S|^{|S|^n} = \log |S| + \frac{1}{n} \log\log |S| \to \log |S|.$$

Of course, if one is studying general mixing SFTs, it makes more sense to fix the base, and in particular, one should use the same base as in the

definition of entropy. With this convention, in [BLR88], it is shown that the density of the endomorphism monoid of a mixing SFT is equal to its entropy, and Kim and Roush have proved that this is the case also for the automorphism group. Of course, the choice of base only affects the density by a multiplicative constant, so whether or not the endomorphism monoid is sparse is independent of the base.

Proposition 1.5.8 *The endomorphism monoid of an infinite mixing SFT is not sparse.*

Since density is easily seen to be smaller than or equal to the entropy in general, this is not a very good notion of simplicity for Chapter 2, as all countable subshifts have zero-entropy. However, the notion is relevant in Chapter 3 and Chapter 4.

Our definition of density measures the asymptotic growth rate of a set of cellular automata on a given alphabet, when the radius increases. An alternative perspective is taken in [The05] (developed further in [BT09]), where the radius $r \in \mathbb{N}$ is fixed, and the density of a set $\mathcal{C}$ of cellular automata is defined as the limit of $|\mathcal{C}^n|/|\mathcal{CA}^n|$, when it exists, where $\mathcal{C}^n$ is the set of CA in $\mathcal{C}$ with radius r on an alphabet of size n. For example, the density of captive cellular automata is 0 with this definition, while we will show in Proposition 4.2.21 that it is 1 with Definition 1.5.6.

Many of the main results and open questions of the thesis can be expressed in terms of these concepts:

- In Section 2.4, we show that endomorphisms of countable sofic shifts have high computational power. The endomorphism monoid is (rather trivially) sparse, but not always finitely generated or predictable.

- In Section 3.1, we give a minimal subshift whose endomorphism monoid is not predictable. The example is not very satisfying, and we leave open the existence of more natural ones. We also leave open the existence of minimal subshifts whose endomorphism monoids are not sparse.

- In Section 3.2, we show that subshifts associated with primitive Pisot substitutions have a simple endomorphism monoid: it is sparse, finitely generated and predictable. This follows from the much stronger result that it is in fact virtually the group generated by the shift map.

- In Section 3.3, we show by example that Toeplitz subshifts can support non-finitely generated endomorphism monoids.

- In Section 4.2, we show that mixing SFTs with equicontinuous reversible unary operators always have a complex endomorphism monoid,

in the sense that it contains an intrinsically universal CA. We show that the endomorphism monoid of a full shift with symbol permutations as unary operations is not sparse or predictable. However, when the operations are not reversible, or there is additional algebraic structure, the endomorphism monoid may contain only shift maps.

- In Section 4.3, we show that full shifts with algebraic structure given by bipermutive unary maps have sparse endomorphism monoids. We do not know whether the endomorphism monoid is finitely generated or predictable in general, but in the case when the map is a group homomorphism for a cellwise group operation, both questions reduce to the corresponding questions for group shifts.

- In Section 4.4, we prove that the set of surjective endomorphisms of full shifts with cellwise lattice structure is sparse, finitely generated and predictable.

We mention that according to [Hoc10], it is shown in [KR90] that the automorphism group of the full shift embeds into $\mathrm{Aut}(X)$ for any mixing SFT X. More generally, it is not hard to show that the endomorphism monoid of a full shift embeds into $\mathrm{End}(X)$ for any mixing SFT X.

Chapter 2

Countable Subshifts

2.1 Cellular Automata on Countable Subshifts

In this chapter, we study subshifts with countably many points. Our emphasis is on the one-dimensional case. This chapter is an extended version of [ST12a].

General countable dynamical systems have been studied in for example [Bob02], and some interesting countable dynamical systems are constructed for example in [HY01]. Despite countability being a rather strong assumption, such systems can be quite intricate. Countable subshifts are in particular countable, compact and Hausdorff spaces, so they are homeomorphic to successor ordinals [MS20, Mil11] (although we do not take this approach when studying countable subshifts). Computational properties of general countable one-dimensional subshifts are discussed for example in [CDTW12]. The case of countable multidimensional SFTs is discussed for example in [BDJ08, JV11, BJ13, ST12b, ST13d], from the structural and computational points of view.

Entropy is the standard tool for detecting information flow in a dynamical system. A countable dynamical system necessarily has zero entropy as we show in Proposition 2.1.3, and as a consequence, also a cellular automaton on a countable subshift has zero entropy. This means that in terms of information, not much is going on. Some dynamical behaviors are also impossible in high generality, for example, transitivity is impossible in general in countable systems. See Proposition 2.1.8 for more such properties.

In the one-dimensional case, the most accessible countable subshifts are probably the bounded ones (including countable SFTs and sofic shifts). Points in such subshifts are concatenations of finitely many subwords taken from a finite set of periodic points. Cellular automata on bounded subshifts are in many ways simpler than general cellular automata in terms of dynamics. Namely, certain types of (usually common) behavior are impos-

sible, and certain (usually undecidable) properties become easily decidable. In particular, nilpotency turns out to be decidable on countable sofic shifts, while it is undecidable on the full shift. These results follow from what we like to call the Starfleet Lemma (Lemma 2.2.3), which states that, starting from any point, a fleet of spaceships eventually appears.

In terms of computational power, on the other hand, cellular automata on countable SFTs and sofic shifts can be very complicated. We show that their limit sets can be just as complicated as those of general cellular automata, and their nonwandering sets and asymptotic sets are also beyond computability. These results are proved by using the lengths of the periodic parts of points as counters of a counter machine.

Before getting to the theory, we show some examples of what cellular automata on countable sofic shifts can look like, in Figure 2.1 and Figure 2.2.

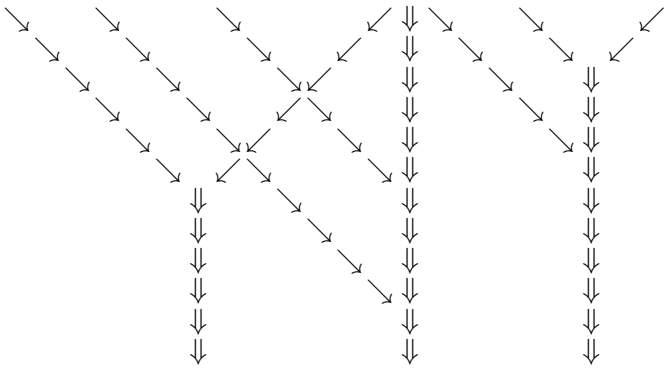


Figure 2.1: A radius 1 CA on a countable sofic shift. We have empty cells, and particles $\swarrow$, $\searrow$ and $\Downarrow$. The rule is that particles move in the direction they point to, and if two particles enter the same cell, they join into a $\Downarrow$-particle. The countable sofic shift is set of points containing at most n particles, where $n \geq 8$. In general, any CA that cannot increase the total number of particles – or some local function computed from them – gives rise to an infinite family of such systems. This includes all number-preserving CA.

2.1.1 The Cantor-Bendixson Derivative

Especially when studying countable topological dynamical systems, the Cantor-Bendixson derivative is a very important tool. While combinatorial techniques suffice in the proofs of this chapter, the Cantor-Bendixson rank gives a nice way to state general conjectures about countable sofic shifts, and we thus briefly outline this concept.

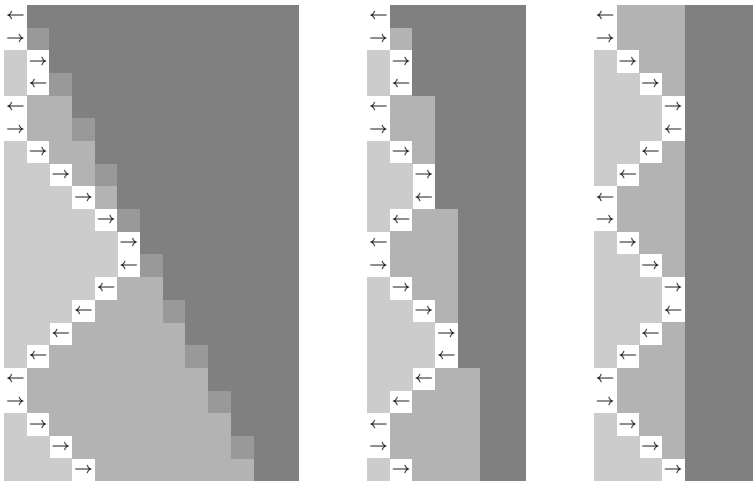


Figure 2.2: Three radius 1 CA on the countable SFT $\mathcal{B}^{-1}(0^*1^*(\leftarrow + \rightarrow)2^*(3+4)4^*)$ with bouncing arrows, and numbers indicated by 5 shades of gray. In the CA on the left, the bouncing area $1^*(\leftarrow + \rightarrow)2^*$ expands steadily. In the CA in the middle, its width expands as needed. In the CA on the right, the width of the area is preserved.

If X is a topological space, we say $x \in X$ is *isolated* if $\{x\}$ is an open set. For every ordinal λ, we define the *Cantor-Bendixson derivative of order* λ of X, denoted by $X^{(\lambda)}$ (or X' when $\lambda = 1$), by transfinite induction:

- $X^{(0)} = X$,
- $X^{(\alpha+1)} = \{x \in X^{(\alpha)} \mid x \text{ is not isolated in } X^{(\alpha)}\}$, and
- $X^{(\alpha)} = \bigcap_{\beta<\alpha} X^{(\beta)}$, if α is a limit ordinal.

There must exist an ordinal λ such that $X^{(\lambda)} = X^{(\lambda+1)}$, as X is a set. The lowest such λ is called the *Cantor-Bendixson rank* of X, and is denoted $\mathrm{rank}(X)$. We say that a space is *perfect* if it contains no isolated points. From the definition of the derivative operator, it is clear that then $X^{(\mathrm{rank}(X))}$ is a perfect space. We note that in a subshift $X \subset S^{\mathbb{Z}}$, a point x is isolated if and only if there exist $i \in \mathbb{Z}$ and $w \in S^*$ such that for $y \in X$, $y_{[i,i+|w|-1]} = w \iff y = x$. We use this fact without any explicit mention in many of our proofs. We say that a topological space X is *ranked* if and only if $X^{(\mathrm{rank}(X))} = \emptyset$. The *rank* of a point x, $\mathrm{rank}_X(x)$, in a ranked topological space X is the smallest ordinal λ such that $x \notin X^{(\lambda)}$.

Example 2.1.1 *For $n \geq 1$, let $X_n = \mathcal{B}^{-1}(1^*2^* \cdots n^*)$. The Cantor-Bendixson derivative of X_n is*

$$X_n' = \bigcup_{i=1}^{n} \mathcal{B}^{-1}(1^* \cdots (i-1)^*(i+1)^* n^*)$$

It is easy to check for subshifts X and Y that $(X \cup Y)' = X' \cup Y'$, and the subshift $\mathcal{B}^{-1}(1^* \cdots (i-1)^*(i+1)^* n^*)$ is conjugate to X_{n-1} for all i. Thus, by induction, we see X_n is ranked, and its Cantor-Bendixson rank is $n+1$.

2.1.2 Entropy and Endomorphisms in General

We begin with a few observations about countable subshifts and their endomorphisms which follow directly from topological and measure theoretical considerations. For example, the topological entropy of a countable subshift is always 0. I am not aware of a simple combinatorial proof for this fact, but it is a straightforward corollary of the following version of the Variational Principle.

A (probability) measure μ on a subshift X is called *ergodic* if for all subshifts $Y \subset X$, either $\mu(Y) = 0$ or $\mu(Y) = 1$. A measure is *extremal* is a set M of measures if $\mu = t\mu' + (1-t)\mu''$ for $t \in (0,1)$ implies $\mu' = \mu''$. It is well-known that the ergodic measures are extremal among invariant measures. The following follows easily from Theorem 8.7 in [Wal00].

Lemma 2.1.2 *Let $X \subset S^{\mathbb{Z}}$ be a subshift. Let*

$$M_{\max}(X) = \{\mu \mid \mu \text{ is shift-invariant}, h_\mu(X) = h_{\text{top}}(X)\}.$$

Then $M_{\max}(X)$ is nonempty, convex and compact, and its (nonempty set of) extremal points are exactly the ergodic measures of X in $M_{\max}(X)$.

Here, $h_\mu(X)$ is the measure-theoretic entropy of X with respect to the measure μ. For the definition of this, see [Wal00] or any other standard reference; for understanding the corollary, we only need that a measure with finite support has entropy 0.

Proposition 2.1.3 *Let $X \subset S^{\mathbb{Z}}$ be a countable subshift. Then we have $h_{\text{top}}(X) = 0$.*

Proof. By the previous lemma, $h_\mu(X) = h_{\text{top}}(X)$ for some ergodic measure μ on X. By countable additivity and shift-invariance of μ, μ is supported by periodic points. Since μ is extremal among shift-invariant measures, there can be only one such orbit, that is, μ is of the form

$$\frac{\delta_x + \cdots + \delta_{\sigma^{k-1}(x)}}{k},$$

for some $x \in X$, $k = |\mathcal{O}(x)|$, and δ_x is the Dirac measure centered on x defined by $\delta_x(A) = |\{y \in A \mid x = y\}|$. As we mentioned, the entropy of such μ is 0, so $h_{\text{top}}(X) = h_\mu(X) = 0$. ■

The converse of Proposition 2.1.3 is not true. For example, many minimal subshifts have zero entropy and contain uncountably many points (for example, the substitution subshifts in Section 3.2).

Corollary 2.1.4 *The entropy of a cellular automaton on a countable subshift $X \subset S^{\mathbb{Z}}$ is 0.*

Proof. The entropy of a cellular automaton is, by definition, the limit of the entropies of its width n traces when n tends to infinity. If the CA $f : X \to X$ has radius r, then the length-k words in the width-n trace of f are determined by words of length $n + 2kr$ of X. It is then easy to see that the width-n trace has entropy at most $2r$ times that of X. Thus, if X has entropy 0, so does f. ■

As we mentioned in Section 1.5, the density of the endomorphism monoid is smaller than or equal to the topological entropy in general, and thus we have the following corollary.

Corollary 2.1.5 *The endomorphism monoid of a countable subshift is sparse.*

We now proceed to Proposition 2.1.8. For this, we need a few lemmas.

Lemma 2.1.6 *A nonempty perfect subset of $S^{\mathbb{Z}}$ is uncountable.*

Proof. This is well-known (in more generality), but we give a simple combinatorial proof for completeness. Let $w \sqsubset X$ be an arbitrary central pattern of a point of X. Since X is perfect, there exist two incomparable patterns w_0, w_1, both extending w, which are each the central pattern of some point of X. We continue inductively on w_0 and w_1, always splitting w_u into incomparable patterns w_{u0} and w_{u1}, which both extend w_a and are the central pattern of a point of X. The function

$$(a_0, a_1, a_2, \ldots) \mapsto \lim_n {}^\infty 0 w_{a_0 a_1 a_2 \cdots a_n} 0^\infty$$

(where $w_{a_0 a_1 a_2 \cdots a_n}$ is centered around the origin) is an embedding of $2^{\mathbb{N}}$ into X, and thus X is uncountable. ■

Lemma 2.1.7 *Let $X \subset S^{\mathbb{Z}}$ be a subshift. If X is countable, then the isolated points are dense in X.*

Proof. Suppose X is countable. Let Y be the set of all points y such that for some open neighborhood $U \ni y$, there are no isolated points in U. If Y is empty, then the isolated points are dense. Otherwise, Y is a nonempty perfect open set, so Y is perfect also with the relative topology, and thus uncountable. This is a contradiction. ■

Proposition 2.1.8 *Let f be a cellular automaton on a countably infinite subshift. Then f is not sensitive, transitive or mixing, and f is almost equicontinuous.*

Proof. Since every isolated point is trivially an equicontinuity point and the set of isolated points is countable and dense (by Lemma 2.1.7), equicontinuity points form an open dense set (in particular a residual set), so f is almost equicontinuous. Thus, f is not sensitive.

Now, suppose that f is transitive. We show that X has finitely many isolated points: If $x \in X$ is any isolated point, then since f is in particular nonwandering, we have $f^n(x) = x$ for some $n > 0$. By transitivity, each isolated point of X is in the f-orbit $\{x, f(x), \dots, f^{n-1}(x)\}$ of x. From this and another application of Lemma 2.1.7, it follows that the isolated points are a finite dense set in X. Thus X is finite as well. ■

2.1.3 Countable Sofic Shifts

One-dimensional countable sofic shifts are particularly accessible examples of countable subshifts. Points of countable sofic shifts consist of long periodic patterns and a bounded number of disturbances between them. We mention the main robustness result for this class:

Proposition 2.1.9 *Let $X \subset S^{\mathbb{Z}}$ be a sofic shift. Then X is countable if and only if $h_{\mathrm{top}}(X) = 0$.*

Proof. By Proposition 2.1.3, if X is countable, then it has entropy 0. Now, suppose X is uncountable, and let (Y, g) be a finite-to-one SFT cover for it such that the forbidden words of $Y \subset T^{\mathbb{Z}}$ have length 2 (for example, the minimal right-resolving cover, [LM95]), and g has radius 0. Since g is finite-to-one, Y has positive entropy if and only if X does, as the entropies are equal by Theorem 8.1.16 in [LM95].

Suppose that Y has zero entropy. We note that if $y \in Y$ is such that $y_{[i,i']} = awa$ and $y_{[j,j']} = aua$ and $w, u \in (T \setminus \{a\})^*$, then $w = u$. Namely, otherwise

$$(auaw + awau)^{\mathbb{Z}} \subset Y,$$

and it is then easy to see that Y has positive entropy. For such a, it follows that if $y_i = a$, $y_j = a$ and $i \leq j$, then $y_{[i,j]} \in (au)^* a$. From this it follows that Y is countable, since each point $y \in Y$ is uniquely determined by recording, for each $a \in T$, the leftmost and rightmost coordinate where a occurs, if such coordinates exist. If a occurs infinitely many times to the left (right), then the left tail (right tail) has repeating pattern au, and we record the repeating pattern and its phase. ■

From Proposition 3.8 in [ST13d], it follows that countability is further equivalent to X being ranked. The Cantor-Bendixson rank of every sofic

shift is finite, so this means $X^{(n)} = \emptyset$ for some $n \in \mathbb{N}$. From Lemma 2.1.13 below, and the easily shown fact that a positive entropy sofic shift contains an infinite transitive subshift, we obtain one more equivalent condition: every transitive subshift of X is finite.

In the next section, we need some mathematical way to express the structure of a countable sofic shift. For this, we give the following version of Lemma 1 from [ST12a], which gives a way to parse points of SFTs into unique finite representations. From this, we extract a weaker parsing result for sofic shifts.[1] In fact, for SFTs, we prove a slightly stronger result than the one given in the statement of the lemma; see the discussion after the proof. Lemma 4.8 from [PS10] is similar in spirit.

Lemma 2.1.10 *Let X be a countable SFT. Then there exists a finite set T of tuples of words in $\mathcal{B}(X)$ such that every point $x \in X$ is uniquely representable as*

$$x = {}^{\infty}u_0 v_1 u_1^{n_1} v_2 \cdots v_{m-1} u_{m-1}^{n_{m-1}} v_m u_m^{\infty} \tag{2.1}$$

for some $n_1, \ldots, n_{m-1} \in \mathbb{N} \setminus \{0\}$ and $(u_0, \ldots, u_m, v_1, \ldots, v_m) \in T$. Conversely, every point representable as such a concatenation is a point of X.

Proof. Let

$$U = \{u \in \mathcal{B}(X) \mid {}^{\infty}u^{\infty} \in X, u \text{ is a Lyndon word}\},$$

and let M be greater than the window size of X. It is easy to see that U is finite, directly using the fact that X is countable, the pigeonhole principle, and the fact that X is an SFT.

We explain a procedure that, given $x \in X$, constructs a tuple $T(x) \in T$ that can be used to represent x as in (2.1).

Let $I = \{\ldots, [j_0, k_0 - 1], [j_1, k_1 - 1], [j_2, k_2 - 1], \ldots\}$ be the list (ordered, say, by j first and k second) of all intervals $[j, k-1]$ such that, writing $N = k - j$, $x_{[j-MN, k+MN-1]} = u^{2M+1}$ for some $u \in U$. By Lemma 1.3.4, we may choose $M \geq 1$ large enough that if $u, v \in U$, and $w \sqsubset u^M$, $w \sqsubset v^M$ and $|w| \geq M$, then $u = v$. Then, intervals of I can not overlap and $x_{[j_i, k_i - 1]} = x_{[j_{i+1}, k_{i+1} - 1]}$ whenever $k_i = j_{i+1}$. It is easy to see that any long enough subword of x contains a subsequence from which a periodic point can be extracted, by the pigeonhole principle. Since periodic points are of the form $u^{\mathbb{Z}}$ for $u \in U$, this implies a bound (independent of x) on the length of intervals J such that $J \cap \bigcup I = \emptyset$. On the other hand, if $x_{[j_i, k_i - 1]} = x_{[j_{i'}, k_{i'} - 1]}$, then $[k_i, j_{i'} - 1] \subset \bigcup I$ ($x_{[k_i, j_{i'} - 1]}$ must be a power of

[1] I am sure Lemma 2.1.10 is true as such also for sofic shifts, but I do not know a nice proof for this; in particular, our proof sketch given in [ST12a] omits the details of dealing with 'nonlocal' periods of periodic parts of points, and as such, the algorithm given only works in the case of SFTs.

$x_{[j_i,k_i-1]}$, or X is uncountable). We thus obtain a bound (independent of x) on the total length of $\mathbb{Z} \setminus \bigcup I$.

The left tail of x is periodic with a unique repeating pattern $u \in U$, and we let $u_0 = u$. If x is in the orbit of $u^{\mathbb{Z}}$, we take the tuple (u) as the representation of x. Otherwise, we let $[j_{J_0}, k_{J_0} - 1] \in I$ be the coordinates of the $(M+1)$th rightmost occurrence of u_0 in the left tail of x, so that $|u_0| + [j_{J_0}, k_{J_0} - 1] \notin I$. Let $u_1, \ldots, u_m$ be the ordered list of words of U such that $u_i = x_{[j_{J_i}, k_{J_i}-1]}$ for some $[j_{J_i}, k_{J_i} - 1] = [j_{J_i}, j_{J_i} + N - 1] \in I$ and $[j_{J_i} - N, j_{J_i} - 1] \notin U$, with $\forall i : J_{i+1} > J_i$. The list is finite by the observations in the previous paragraph. The intuition is that these words u are Lyndon representatives of long enough periodic patterns of x. We choose v_i to be 'the rest' of x: $v_i = x_{[k_{(J_i-1)}, j_{J_i}-1]}$. Note that v_i is *not* taken to be $x_{[k_{J_{(i-1)}}, j_{J_i}-1]}$.

Denote by $T(x)$ the tuple $(u_0, \ldots, u_m, v_1, \ldots, v_m)$ constructed above for x. Since we choose a tuple for each point of x, it is clear that each x has a representation of the form (2.1), by the tuple $T(x)$. On the other hand, since in each tuple $T(x)$, v_i ends and v_{i+1} begins with at least M repetitions of u_i, we have that all points that have a representation of the form (2.1) are in X.

Now, we only need to show that the representation is unique. For this, we note the following properties for the tuples $T(x)$:

- v_i begins with u_{i-1}^M but does not agree from the left with u_{i-1}^{M+1}.
- v_i ends with u_i^M but does not agree from the right with u_i^{M+1}.
- v_i does not begin with v^M if $u \neq v$.
- v_i does not end with v^M if $u \neq v$.
- v_i does not contain v^{2M+1} for any $v \in U$.

We only prove the first property, the rest being similar. If there are less repetitions in the beginning of v_i, then this can only mean that v_i is a proper prefix of u_{i-1}^M, as otherwise the occurrence of u_{i-1} to the left of v would not have been in I when adding the tuple for x. In general, however, it is impossible for v_i to be a prefix of a word in u_{i-1}^*, as clearly this would imply that there is an overlap of u_{i-1}^M and u_i^M of length at least M in x. If there are more than M repetitions in the beginning of v_i, then the first $|u_{i-1}|$ coordinates of v_i would have been an interval in I when choosing this tuple for x, and the impossibility of v_i being a proper prefix of u_{i-1}^{M+1} was shown above. This concludes the proof of the first property.

Now, suppose $T(x) \neq T(y)$, but $z \in X$ has two representations

$$^{\infty}u_0 v_1 u_1^{n_1} \cdots u_{m-1}^{n_{m-1}} v_m u_m{}^{\infty} = z = {}^{\infty}s_0 t_1 s_1^{N_1} \cdots s_{M-1}^{N_{M-1}} t_M s_M{}^{\infty},$$

where the s_i and t_i are taken from $T(y)$. First, it is easy to see that we have $u_0 = s_0$ and $u_m = s_M$, by Lemma 1.3.4. Also, the two tails must exactly coincide, so that $v_1 u_1^{n_1} \cdots u_{m-1}^{n_{m-1}} v_m = t_1 s_1^{N_1} \cdots s_{M-1}^{N_{M-1}} t_M$, by the first two properties of the tuples listed above. Using the five properties, it can be proved by induction (from either direction) that $v_i = t_i, u_i = s_i, n_i = N_i$ for all i. ■

We remark that not only is there a unique decomposition for each point $x \in X$, but a block map can output the decomposition, in the sense that there exists a block map $f : X \to A^{\mathbb{Z}}$ for a suitable alphabet A such that, writing $\#[w] = a_w \#^{|w|-1}$ (where a_w is a distinct symbol for each word w), we have that

$$x = {}^{\infty}u_0.v_1 u_1^{n_1} \cdots u_{m-1}^{n_{m-1}} v_m u_m^{\infty}$$

maps to

$$f(x) = {}^{\infty}\#[u_0].\#[v_1]\#[u_1]^{n_1} \cdots \#[u_{m-1}]^{n_{m-1}}\#[v_m]\#[u_m]^{\infty}$$

for all tuples $(u_0, \ldots, u_m, v_1, \ldots, v_m) \in T$ and $n_1, \ldots, n_{m-1} \in \mathbb{N} \setminus \{0\}$. The map is realized by outputting a_u if the current cell is the leftmost symbol of $u \in U$ such that u repeats at least M times in both directions, $\#$ for other cells that occur in such $u \in U$, and finally compressing the remaining cells (whose lengths are bounded) into words $\#[w]$.

Of course, such a map does not in general exist in the sofic case. For example $\mathcal{B}^{-1}(0^*(11)^*0^*)$ does not allow such a map: necessarily, any symbol 1 sufficiently deep in a repetition of 1s is mapped to $\#[1] = a_1$. It follows that there are representations of ${}^{\infty}01^n0^{\infty}$ for all large enough n, not only even n.

Next, we define bounded subshifts, and show their connection with sofic shifts.

Definition 2.1.11 *A language $L \subset S^*$ is said to be* bounded *if there exists a finite sequence of words $(w_1, w_2, \ldots, w_n)$ such that $L \subset w_1^* \cdots w_n^*$. A subshift is said to be bounded if its language is bounded.*

Bounded languages are a very common topic of study in the theory of formal languages. The notion of a bounded subshift, however, is not standard.

Lemma 2.1.12 *A union of finitely many bounded languages is bounded, and if L is bounded, then also the factor closure*

$$\{u \mid \exists w \in L : u \sqsubset w\}$$

of L is bounded.

Proof. If L and L' are bounded by $(w_1, \dots, w_n)$ and $(w'_1, \dots, w'_{n'})$, then $L \cup L'$ is bounded by $(w_1, \dots, w_n, w'_1, \dots, w'_{n'})$.

For the second claim, suppose L is bounded. Let $u \sqsubset w$ where $w \in L$. Then $u \in vw_j^* \dots w_k^* v'$ where v is a suffix of w_j and v' a prefix of w_k. For each choice of v, v', j, k, we let $w_{(v,v',j,k)} = (v, w_j, \dots, w_k, v')$, and choose the bounding language to be the concatenation of the tuples $w_{(v,v',j,k)}$ over tuples (v, v', j, k). Clearly, the obtained tuple bounds the factor closure of L. ■

Lemma 2.1.13 *A subshift is bounded if and only if it is contained in a countable sofic shift.*

Proof. First, the subshift $\mathcal{B}^{-1}(w_1^* w_2^* \cdots w_n^*)$ is sofic by definition, and obviously countable as well. Thus, bounded subshifts are contained in countable sofic shifts.

Next, we show that a countable sofic shift is bounded, which of course implies that all subshifts contained in a countable sofic shift are bounded. For this, suppose X is countable and sofic. Let (Y, g) be a countable finite-to-one edge shift cover of X, with g a symbol map. Let T' be the set of tuples obtained for Y according to Lemma 2.1.10. We let $T = g(T')$, in the sense that for $(u_0, \dots, v_m) \in T'$, we put $(g(u_0), \dots, g(v_m)) \in T$. It is easy to see that the tuples T give representations of all points $x \in X$ (in the sense of the statement of the lemma), and only such points.

Now, for each tuple $T(x) = (u_0, \dots, u_m, v_1, \dots, v_m) \in T$, the language of finite subwords of points $y \in X$ with $T(y) = T(x)$ is bounded by the factor closure of $w_1^* \cdots w_n^*$ where $(w_1, \dots, w_n) = (u_0, v_1, u_1, \dots, v_m, u_m)$. Thus, $\mathcal{B}(X)$ is bounded as the finite union of these factor closures by Lemma 2.1.12. ■

Lemma 2.1.14 *For each $(v_0, \dots, v_{k'})$ there exists $(w_0, \dots, w_k)$ such that*

$$\mathcal{B}^{-1}(v_0^* \cdots v_{k'}^*) \subset \mathcal{B}^{-1}(w_0^* \cdots w_k^*),$$

and the w_i are Lyndon words.

Proof. We may assume the words v_i are primitive by replacing them with their primitive roots, as this can only increase the size of $\mathcal{B}^{-1}(v_0^* \cdots v_{k'}^*)$. Next, let $v_i = u_i u_{i'}$ where $u_{i'} u_i$ is Lyndon. Let $u_i = a_1 \cdots a_{|u_i|}$ and $u_{i'} = b_1 \cdots b_{|u_{i'}|}$ where $a_i, b_i \in S$. Now, replace each v_i in the tuple by the words $a_1, \dots, a_{|u_i|}, u_{i'} u_i, b_1, \dots, b_{|u_{i'}|}$, which are all trivially Lyndon. ■

We choose such a bounding tuple $(w_0, \dots, w_k)$ for each bounded subshift X, called a *Lyndon bound* for X.

In Section 2.2, to prove Lemma 2.2.3, we will need a way to associate tuples of numbers to points of a bounded shift. For this, it is useful to observe that a bounded subshift does not contain arbitrarily large powers of words other than those in the Lyndon bound, in the following sense.

Lemma 2.1.15 *Let $\{w_i \mid i \in [1,n]\}$ be Lyndon words. Then for large enough m, if $w^m \sqsubset \mathcal{B}^{-1}(w_1^* \cdots w_n^*)$, then $\mathcal{O}(w^{\mathbb{Z}}) = \mathcal{O}(w_i^{\mathbb{Z}})$ for some $i \in [1,n]$.*

Proof. Let $k = \max\{|w_i| \mid i \in [1,n]\}$. Suppose $w \sqsubset \mathcal{B}^{-1}(w_1^* \cdots w_n^*)$. If $m > 2n$ and $|w| > k$, then $w^2 \sqsubset w_i^{\mathbb{Z}}$ for some i. Since w_i is Lyndon, it is in particular unbordered, and it is easy to see that $|w_i|$ divides $|w|$, from which the claim follows.

There are finitely many words $|w| \leq k$, and it is enough to prove the claim for such Lyndon words (since every word is the power of a rotation of a Lyndon word). Let M be given by Lemma 1.3.4 for $U = \{u \mid u \text{ Lyndon}, |u| \leq k\}$. Now, $w^{Mn} \sqsubset \mathcal{B}^{-1}(w_1^* \cdots w_n^*)$ implies $w^M \sqsubset \mathcal{B}^{-1}(w_i^*)$ for some i, and since $w, w_i \in U$, we have $w = w_i$. ■

We can now parse general bounded subshifts with the same ideas as in Lemma 2.1.10.

Definition 2.1.16 *Let X be a bounded subshift, let $w_1^* \cdots w_n^*$ be its Lyndon bound, and let m be minimal such that*

- *Lemma 1.3.4 holds for $M = m$ and $U = \{w_i \mid i \in [1,n]\}$, and*
- *if $w^m \sqsubset \mathcal{B}^{-1}(w_1^* \cdots w_n^*)$, then $\mathcal{O}(w^{\mathbb{Z}}) = \mathcal{O}(w_i^{\mathbb{Z}})$ for some $i \in [1,n]$.*

Now, let $x \in X$. If $x_{[j,j']} = w_i^{k+2m}$ but $x_{[j-|w_i|,j']}, x_{[j,j'+|w_i|]} \notin w_i^*$, then the interval $[j + m|w_i|, j' - m|w_i|]$ is said to be a w_i-sea of x. *There can also be infinite seas, which are also referred to as* oceans*:*

- *If $x \in \mathcal{O}(w_i^{\mathbb{Z}})$, then $(-\infty, \infty)$ is a w_i-sea of x.*
- *If $x_{(-\infty,j']} \in w_i^{-\mathbb{N}}$ but $x_{(-\infty,j'+|w_i|]} \notin w_i^{-\mathbb{N}}$, then $(-\infty, j' - m|w_i|)$ is a w_i-sea of x.*
- *If $x_{[j,\infty)} \in w_i^{\mathbb{N}}$ but $x_{[j-|w_i|,\infty)} \notin w_i^{\mathbb{N}}$, then $[j + m|w_i|, \infty)$ is a w_i-sea of x.*

The maximal intervals $[j, j']$ not intersecting any of the seas are called islands of x.

We make some easy observations, which are proved using the properties of m, similarly as in Lemma 2.1.10. First, no two seas can overlap, and in fact there must be a nonempty island between any two seas (by the assumption on m). A periodic point contains a single two-way infinite ocean (and thus no islands), but every other point contains precisely two oceans. Also, the number of seas in $x \in X$ is exactly one more than the number of islands.

An important property to ensure is that whenever we see something periodic, it is actually part of a sea. This follows directly from our choice of m.

Lemma 2.1.17 *Let X be a bounded subshift and let m be as in Definition 2.1.16. If $x \in X$ and $x_{[j-(m+2)|w|,j'+(m+2)|w|]} \sqsubset w^{\mathbb{Z}}$, then $[j, j']$ (if nonempty) is completely contained in a u-sea of x, where u is the unique Lyndon word satisfying $\mathcal{O}(u^{\mathbb{Z}}) = \mathcal{O}(w^{\mathbb{Z}})$.*

Note that in particular this means $u = w_i$ for some w_i in the Lyndon bound of X (by the definition of a sea).

Proof. By decreasing j and increasing j' if necessary, we may assume

$$x_{[j-(m+1)|w|,j'+(m+1)|w|]} \in w^*.$$

By the second assumption on m, we have $\mathcal{O}(w^{\mathbb{Z}}) = \mathcal{O}(w_i^{\mathbb{Z}})$ for some w_i in the Lyndon bound of X. In particular, by again decreasing j and increasing j' if necessary, we may assume $w = w_i$ and $x_{[j-m|w_i|,j'+m|w_i|]} = w_i^k$ where $k \geq 2m + 1$. Then, by the definition of a w_i-sea, $[j, j']$ is contained in one. The uniqueness is just a property of Lyndon words: $\mathcal{O}(u^{\mathbb{Z}}) = \mathcal{O}(v^{\mathbb{Z}})$ implies $u = v$ if both are Lyndon. ■

Another important observation is that there is a global upper bound on the total length of the islands, although we only need the following corollary of this:

Lemma 2.1.18 *Let X be a bounded subshift. Then there exists ℓ such that if $x \in X$, then $[j, j']$ intersects a sea in x of length at least $\frac{j'-j-\ell}{\ell}$.*

Proof. Let $w_1^* \cdots w_n^*$ be the Lyndon bound of X. Let $k = \max\{|w_i| \mid i \in [1, n]\}$. If $x \in X$, then $x_{[j,j']}$ is a subword of a word in $w_1^* \cdots w_n^*$. Writing $t = j' - j$, $x_{[j,j']}$ contains a subword $w \in w_1^* \cdots w_n^*$ of length at least $t - 2k$ (by dropping a suffix of one of the words w_i from the beginning of $x_{[j,j']}$, and such a prefix from the end of $x_{[j,j']}$). The word w further contains a subword w_i^h where $|w_i^h| \geq (t-2k)/n$ by the (generalized) pigeonhole principle, so that $[j, j']$ intersects a w_i-sea of x of length at least $(t - 2k)/n - 2mk$. The claim follows because

$$(t - 2k)/n - 2mk \geq (t - 2k(1 + mn))/n \geq (t - \ell)/\ell,$$

if $\ell = 2k(1 + mn)$. ■

We now show some basic results about how this definition interacts with cellular automata. First, we show that islands cannot appear from thin air. Indeed they should not: islands represent the aperiodic parts of the point, and cellular automata cannot make a periodic sequence aperiodic.

Lemma 2.1.19 *Let X be a bounded subshift with canonical Lyndon bound $w_1^* \cdots w_n^*$, and let $f : X \to X$ be a CA. Then there exists k such that if i is in an island of $f(x)$, then $[i - k, i + k]$ intersects an island of x.*

Proof. Let r be the radius of f, and let $q = \max\{|w_i| \mid i \in [1,n]\}$. Let m be as in Definition 2.1.16. Let $k = q(m+2)+r$. Suppose $[i-k, i+k]$ does not intersect an island of x. Then, $x_{[i-k,i+k]}$ has period p for some $p = |w_i|$, so that in particular $f(x)_{[i-k+r,i+k-r]} = f(x)_{[i-q(m+2),i+q(m+2)]}$, and thus $f(x)_{[i-p(m+2),i+p(m+2)]}$ also, has period p. It then follows that i is in a sea of $f(x)$ by the Lemma 2.1.17, which is a contradiction. ■

Using the previous lemmas, we see that long seas must have 'corresponding' long seas in the preimage, although their length can, in theory, decrease quite a bit. The asymmetry is due to the fact that seas *can* appear from thin air: a cellular automaton can of course make an aperiodic sequence periodic.

Lemma 2.1.20 *Let k and ℓ be as in the previous lemmas. Then if $f(x)$ has h seas of length at least $2k+\ell+j$, then x has at least h seas of length at least j/ℓ.*

Proof. Enumerate the islands of $f(x)$ as $[j_i, j_i']$ in increasing order of j_i, and for each i, choose a coordinate $\alpha_i \in [j_i - k, j_i' + k]$ which is part of an island of x (guaranteed by Lemma 2.1.19), so that α_i is an increasing sequence (reordering if needed). Now, for every sea $[j_i'+1, j_{i+1}-1]$ of length at least $2k+\ell+j$, $[\alpha_i+1, \alpha_{i+1}-1]$ is of length at least $\ell+j$, and thus contains a sea of length at least j/ℓ by Lemma 2.1.18. ■

Remark 2.1.21 *Just like countable sofic shifts are a common generalization of (the incomparable classes of) countable SFTs and subshifts of the form $\mathcal{B}^{-1}(w_1^* \cdots w_n^*)$, transitive sofic shifts are a common generalization of (the incomparable classes of) transitive SFTs and subshifts of the form $\mathcal{B}^{-1}((w_1 + \cdots + w_n)^*)$. Subshifts of the form $\mathcal{B}^{-1}((w_1 + \cdots + w_n)^*)$ are usually called* renewal systems*, and they are a well-studied class of subshifts.*

2.2 CA on Countable Sofics – the Simple

In this section, we show that endomorphisms of countable sofic shifts are a bit easier to analyze than those of the full shift. We introduce two tools for studying countable sofic shifts. One is the Starfleet Lemma, so named because in the terminology of cellular automata, it states that a collection of spaceships appears infinitely many times in the orbit of any point. This lemma is used to show that nilpotency and periodicity are decidable properties, and positive expansivity is impossible on countable sofic shifts, and also 2-dimensional countable SFTs. The other tool is what we use to prove the Starfleet Lemma: While countable sofic shifts are compact as subshifts, they become discrete when we project them into tuples of numbers denoting the lengths of their periodic subwords. We recompactify them by letting these

lengths become infinite, and show that cellular automata have well-defined extensions in this new space. Interestingly, this lets us conclude things about the original subshift.

2.2.1 The Starfleet Lemma

We first introduce some notation for accessing the seas and islands, and give a simple continuity lemma.

Definition 2.2.1 *Let X be a bounded subshift, and $w_1^* \cdots w_n^*$ its Lyndon bound. For an aperiodic $x \in X$,[2] let*

$$S(x) = ((-\infty, j_0'], [j_1, j_1'], \dots, [j_\beta, \infty)),$$

where $\beta = \beta(x)$ is the number of islands, be the sequence of seas of x, in increasing order of j_i. We also write

$$U(x) = (j_1' - j_1, \dots, j_{\beta-1}' - j_{\beta-1}),$$

and

$$T(x) = (r_0, \dots, r_\beta, s_1, \dots, s_\beta) \in \mathcal{B}(X)^{2\beta+1},$$

if $[j_i, j_i']$ is an r_i-sea, and $s_i = x_{[j_{i-1}'+1, j_i-1]}$. For periodic $x \in X$, we write $T(x) = (w_i)$ if $x \in \mathcal{O}(w_i^{\mathbb{Z}})$, and $U(x) = ()$.

Note that if x has precisely one infinite sea, then $U(x) = ()$. Also note that for aperiodic $x \in X$, $T(x)$ and $S(x)$ uniquely determine x. For both periodic and aperiodic $x \in X$, $T(x)$ and $U(x)$ uniquely determine $\mathcal{O}(x)$, and conversely $(T(\sigma(x)), U(\sigma(x))) = (T(x), U(x))$ since the locations of seas and islands are defined by local properties of x. Furthermore, there are finitely many different tuples $T(x)$.

We show that if points have the same structure apart from the length of the seas, then their images share this property. This is important, because it implies that extensions of cellular automata to the topological space defined in the proof of Lemma 2.2.3 are well-defined and continuous.

Lemma 2.2.2 *Let $f : X \to X$ be a CA. There exists ℓ such that if $T(x) = T(y)$ and for all i either $U(x)_i = U(y)_i$ or $U(x)_i, U(y)_i > h$ for some $h \geq \ell$, then $T(f(x)) = T(f(y))$ and for all i either $U(f(x))_i = U(f(y))_i$ holds, or $U(f(x))_i, U(f(y))_i > h - \ell$ holds.*

Proof. Although we generally try to avoid this practice, in this proof, to avoid naming all the coordinates we need, variables denoting words remember their position in the point where they occur. For example, if

[2] For periodic x, one could say $S(x) = ((-\infty, \infty))$.

$x = {}^{\infty}u.vw^{\infty}$, we may talk about v containing a sea. By this, we mean that a sea occurs in x in the subsequence the variable v took its contents from.

Let r be the radius of f and m as in Definition 2.1.16 and let α be the length of the longest word in the Lyndon bound of X. Let $\ell = 2m\alpha + 2r + 1$, and suppose

$$x = {}^{\infty}r_0.r_0^r s_1 r_1^{n_1} s_2 r_2^{n_2} \cdots s_k r_k^{\infty}$$

is the decomposition of x according to Definition 2.2.1 (so that the subwords $r_i^{n_i}$ for $i \in [1, k-1]$ are precisely the finite seas of x). Consider another point

$$y = {}^{\infty}r_0.r_0^r s_1 r_1^{n_1'} s_2 r_2^{n_2'} \cdots s_k r_k^{\infty},$$

with $n_i = n_i'$ or $n_i, n_i' > h \geq \ell$ for $i \in [1, k]$. Since seas are defined by a local property and $\ell > m$, it is clear that this is in fact the decomposition of y into seas and islands according to Definition 2.2.1. Next, we group together maximal subwords of (the presentation of) x of the form $s_j r_j^{n_j} \cdots r_{j'}^{n_{j'}} s_{j'+1}$ where $n_i \leq h$ for $i \in [j, j']$. These subwords are shared by x and y by the assumption that $n_i = n_i'$ if $n_i \leq h$. Thus, we obtain a subsequence $j_0, j_1, j_2 \ldots, j_c, j_{c+1}$ of $[0, k]$ where $j_0 = 0$ and $j_{c+1} = k$, words $u_1, \ldots, u_{c+1}$, and new presentations

$$x = {}^{\infty}r_{j_0}.r_{j_0}^r u_1 r_{j_1}^{n_{j_1}} u_2 \cdots r_{j_c}^{n_{j_c}} u_{c+1} r_{j_{c+1}}^{\infty}$$

and

$$y = {}^{\infty}r_{j_0}.r_{j_0}^r u_1 r_{j_1}^{n_{j_1}'} u_2 \cdots r_{j_c}^{n_{j_c}'} u_{c+1} r_{j_{c+1}}^{\infty},$$

where $n_{j_i}, n_{j_i}' > h$ for all $i \in [1, c]$.

Now, decompose $f(x)$ as

$$f(x) = {}^{\infty}w_0.v_1 w_1^{n_{j_1}-2r} v_2 w_2^{n_{j_2}-2r} \cdots w_c^{n_{j_c}-2r} v_{c+1} w_{c+1}^{\infty},$$

where $|w_i| = |r_{j_i}|$ for $i \in [0, c+1]$, and $|v_i| = |u_i| + |r_{j_{i-1}}^r| + |r_{j_i}^r|$. That is, we let w_i be the periodic image of the periodic subword $r_{j_i}^{n_{j_i}}$ of x, except for subsuming the images of the r left- and rightmost repetitions in the words v_i, since these need not be periodic. Of course $n_{j_i} - 2r \geq 2m + 1$ since $h \geq \ell = 2m\alpha + 2r + 1$. Note that this decomposition of $f(x)$ is generally not the decomposition according to Definition 2.1.16. Still, since r is the radius of f, it is easy to see that

$$f(y) = {}^{\infty}w_0.v_1 w_1^{n_{j_1}'-2r} v_2 w_2^{n_{j_2}'-2r} \cdots w_c^{n_{j_c}'-2r} v_{c+1} w_{c+1}^{\infty},$$

where again $n_{j_c}' - 2r \geq 2m + 1$

First, we need to show $T(f(x)) = T(f(y))$. Because the subwords $w_i^{n_{j_i}-2r}$ and $w_i^{n_{j_i}'-2r}$ (in the decompositions we gave) both have length at

least $2m+1$, it follows that both of these subwords contain a w_i-sea spanning all but possibly the $2m$ bordermost repetitions. Two things can happen with the words v_i. For some i, it could be that $\mathcal{O}(w_i) = \mathcal{O}(w_{i+1})$, and in fact $w_{i-1}^{n_{j_{i-1}}-2r} v_i w_i^{n_{j_i}-2r}$ has period $|w_i|$. Then, the 'w_{i-1}-sea' and the 'w_i-sea' are actually a single longer u-sea for the unique Lyndon word u such that $\mathcal{O}(u^{\mathbb{Z}}) = \mathcal{O}(w_{i-1}^{\mathbb{Z}}) = \mathcal{O}(w_i^{\mathbb{Z}})$. The same then happens in $f(y)$ for the subword $w_{i-1}^{n'_{j_{i-1}}-2r} v_i w_i^{n'_{j_i}-2r}$. Other v_i intersect an island. Then, identical seas and islands appear in $f(x)$ and $f(y)$ near the occurrence of v_i because the local rule for determining the islands – looking at $(2m+1)$-repetitions of the words in the Lyndon bound of X – does not look further than αm cells into the periodic subword with repeating pattern w_i, and thus $f(x)$ and $f(y)$ look identical in terms of seas, and thus also islands. All in all, precisely the same seas and islands are formed, so $T(f(x)) = T(f(y))$.[3]

Now that $T(f(x)) = T(f(y))$, all that is left is to show that if the ith seas of $f(x)$ and $f(y)$ have a different length, then this sea contains more than $h-\ell$ repetitions of the repeating pattern. But clearly the only seas that could have different lengths are the ones intersecting the middle $|w_i^{n_{j_i}-2r-2m}|$ cells of the subwords $w_i^{n_{j_i}-2r}$ in $f(x)$. Such seas contain at least $n_{j_i} - 2r - 2m$ (resp. $n'_{j_i} - 2r - 2m$) repetitions of some u in the Lyndon bound of X in $f(x)$ (resp. $f(y)$), and since $n_{j_i}, n'_{j_i} > h$ and $2r + 2m \leq \ell$, this is more than $h - \ell$. ■

Lemma 2.2.3 (Starfleet Lemma) *If f is a CA on a bounded subshift X, then for all $x \in X$, there exist $\ell \in \mathbb{N}$ and a tuple*

$$t = (r_0, \dots, r_\ell, s_1, \dots, s_\ell) \in \mathcal{B}(X)^{2\ell+1}$$

such that

- *for all $h \in \mathbb{N}$, there exist $n \in \mathbb{N}$ and $n_1, \dots, n_{\ell-1} \geq h$ such that*

$$f^n(x) \in \mathcal{O}({}^{\infty}r_0 s_1 r_1^{n_1} s_2 \cdots s_{\ell-1} r_{\ell-1}^{n_{\ell-1}} s_\ell r_\ell^{\infty}),$$

- *and for all $i \in [1, \ell]$, the point ${}^{\infty}r_{i-1}s_i r_i^{\infty}$ is a nontrivial spaceship for f.*

[3]The reason we included α in the argument is that the local rule for determining whether to put a v-sea in a repetition of w_i, for a word v in the Lyndon bound with $|v| >> |w_i|$, can see way past the repetition of w_i in both directions, if we do not have the factor α. Of course, our choice of m ensures that a v-sea will not actually be there, since it would intersect the sea induced by the repetition of the primitive root of w_i, but we feel the argument is clearer when the local rule determining the seas truly sees the same things when decomposing $f(x)$ and $f(y)$.

We call a tuple t as above a *starfleet for* x.

Proof. The main idea in the proof is to extend the space X by allowing infinite periodic patterns in the points. In terms of our nautical metaphor, we allow more than two oceans in a point. We take a limit point of $f^n(x)$ in this new space containing a maximal number of oceans. We follow the preimages of the finite words (the 'archipelagos' of seas and islands) between oceans. As the number of oceans was taken to be maximal, these do not grow infinitely, and thus repeat. This of course means that the same point of spaceships occurs infinitely many times in the orbit of x.

We now formalize this in terms of the Alexandroff extension of $\mathbb{N}$, that is, the one-point compactification $\mathbb{N} \cup \{\infty\}$ of $\mathbb{N}$ with base

$$\{\{n\}, [n, \infty] \mid n \in \mathbb{N}\}.$$

Let $\mathcal{T}(X) = \{T(x) \mid x \in X\}$, and define $\mathcal{X} = \{(T(x), U(x)) \mid x \in X\}$. We topologize $(\mathbb{N} \cup \{\infty\})^{\beta-1}$ by the product topology for each $\beta - 1$. The space is compact by Tychonoff's theorem, and it is clearly metrizable (so we may use sequential reasoning when working with it). Now, $\mathcal{X}$ can be considered (by some abuse of notation, depending on the definition of the disjoint union) a subspace of the topological space

$$\mathcal{Z} = \dot{\bigcup}_{T \in \mathcal{T}(X)} (\mathbb{N} \cup \{\infty\})^{\beta(T)-1}$$

(where $\beta(T) = \beta(x)$ for any $x \in X$ with $T(x) = T$).

We define a function $\hat{f} : \mathcal{X} \to \mathcal{X}$ by

$$\hat{f}((T(x), U(x))) = (T(f(x)), U(f(x))).$$

This map is well-defined since $T(x)$ and $U(x)$ uniquely determine the orbit of x, f preserves orbits, and $(T(\sigma(x)), U(\sigma(x))) = (T(x), U(x))$. It is trivially continuous, since $\mathcal{X}$ is a discrete subspace of $\mathcal{Z}$.

Next, we extend $\hat{f}$ to the compact space $\mathcal{Y} = \overline{\mathcal{X}} \subset \mathcal{Z}$ by the obvious formula:

$$\hat{f}((T, U)) = \lim \hat{f}((T(x_i), U(x_i))),$$

when $(T(x_i), U(x_i)) \to (T, U)$. To show this is well-defined, suppose that $(T(x_i), U(x_i)) \to (T, U)$ and $(T(y_i), U(y_i)) \to (T, U)$ as $i \to \infty$. We may assume that for all $U_j < \infty$ we have $U(x_i)_j = U(y_i)_j = U_j$, since $\{U_j\}$ is an open set in $\mathbb{N} \cup \{\infty\}$. Now, what we have are points x_i and y_i with $T(x_i) = T(y_i)$ and either $U(x_i)_j = U(y_i)_j$ or both $U(x_i)_j$ and $U(y_i)_j$ tend to infinity as $i \to \infty$. The claim then easily follows from Lemma 2.2.2.

Now, consider the sequence $(T^n, U^n) = (T(f^n(x)), U(f^n(x)))$, and let (T, U) be its limit point such that $h = |U|_\infty$ is maximal, that is, there are a maximal amount of coordinates in U containing the value ∞. First, suppose

there are no limit points with $|U|_\infty > 0$. It is then easy to see that the set $\{U^n_j \mid n \in \mathbb{N}, j \in [1, |U^n|]\}$ must be finite, so that $(T^n, U^n) = (T^{n'}, U^{n'})$ for some $n < n'$. Then $f^n(x)$ is a spaceship, and the claim easily follows.

Now, suppose $|U|_\infty > 0$, and let $p_1, p_2, \ldots$ be a sequence such that $(T^{p_i}, U^{p_i}) \to (T, U)$. By restricting to a subsequence, and by an easy compactness argument, we may assume

$$T^{p_1} = T^{p_2} = T^{p_3} = \cdots,$$

$$T^{p_2-1} = T^{p_3-1} = T^{p_4-1} = \cdots,$$

and in general for all i

$$T^{p_{i+1}-i} = T^{p_{i+2}-i} = T^{p_{i+3}-i} = \cdots.$$

Now, consider the sequence of tuples

$$((U^{p_1}), (U^{p_2}, U^{p_2-1}), (U^{p_3}, U^{p_3-1}, U^{p_3-2}), \ldots),$$

and let

$$N = (N^0, N^1, N^2, N^3, \ldots)$$

be a limit point of a subsequence of it, in the sense that for all j, N^j is a limit point of $(U^{p'_i-j})_i$ for a subsequence $(p'_i)_i$ of $(p_i)_i$.

Now, observe that by continuity, $\hat{f}((T^{p_{i+2}-i-1}, N^{i+1})) = (T^{p_{i+1}-i}, N^i)$ for all i. Since $N^0 = U$ has a maximal amount of islands h, there are h coordinates j such that $U^{p'_i}_j \to \infty$ as $i \to \infty$. By Lemma 2.1.20, we must have $U^{p'_i-1}_{j'} \to \infty$ for at least h coordinates j', so that N^1 has at least h infinite coordinates as well. Inductively, we see that N^i has at least h infinite coordinates for all i. Of course, if some N^i has more than h infinite coordinates, then h was not maximal. Let H_i be the set of infinite coordinates of N^i. If for all n there were i, j such that $N^i_j > n$ but $j \notin H_i$, then some limit of a subsequence of N^i would have at least $h + 1$ infinite coordinates. Thus, there must be a uniform bound on the finite coordinates of N^i. This implies $N^n = N^{n'}$ for some $n < n'$, and we can further take $T^n = T^{n'}$. The result then follows by opening up the definitions. ■

Note that we only used Tychonoff's theorem for a finite product of compact metric spaces – a case which is particularly easy to prove. Of course, this means that the proof readily turns into one omitting the explicit use of compactness.

2.2.2 Dynamical Properties of CA on Countable Sofic Shifts

In this section, we study the dynamics of CA on sofic bounded subshifts. For this, we do not need the specifics of parsing of points in bounded subshifts, and only use the Starfleet Lemma.

As we saw in Lemma 1.3.20, on mixing sofic shifts, injectivity implies surjectivity, and on mixing SFTs, preinjectivity is equal to surjectivity. We now give two very simple examples of a CA on a countable subshift, showing that neither result holds on countable SFTs (although the examples given in [Fio00] are just as simple).

Example 2.2.4 *Let $X = \mathcal{B}^{-1}(0^*1^*2^*)$ and let $f = f_{\text{increment}}$ be the cellular automaton defined by*

$$f({}^{\infty}0.1^n2^{\infty}) = {}^{\infty}0.1^{n+1}2^{\infty}.$$

Clearly, such a CA is injective on X, but it is not surjective. Similarly, the CA $g = f_{\text{decrement}}$ defined by

$$g({}^{\infty}0.1^n2^{\infty}) = {}^{\infty}0.1^{\max\{0,n-1\}}2^{\infty}.$$

is surjective but not even preinjective.

Not everything is different of course. For example, a CA on a countable sofic subshift that is surjective and injective is a homeomorphism (and thus reversible), since this is in general true on compact spaces, for continuous functions.

Next, we discuss decidability results for countable sofic subshifts. Many such results hold on general sofic shifts, and thus also on countable ones. This includes the decidability of surjectivity, injectivity, reversibility and periodicity with a fixed period p. In general, any property which is expressible as a first-order statement where variables range over points of sofic shifts is decidable by the results of [Büc60].

One of the most important undecidable properties of cellular automata on full shifts is nilpotency [Kar92]. Its importance lies in the many further undecidability results that follow from it. We show that this property is in fact decidable on countable sofic shifts due to the Starfleet Lemma. This is interesting, since nilpotency is undecidable also for counter machines [BBK$^+$01], and CA on countable sofic shifts are in some sense a hybrid between counter machines and cellular automata (see for example Section 2.3), so that one might expect this problem to be undecidable as well.

Theorem 2.2.5 *If X is a countable sofic shift, then given a CA $f : X \to X$ it is decidable whether f is nilpotent.*

Proof. We will prove that one of the following cases holds for a CA f on a countable sofic shift X: either f is nilpotent, it is not nilpotent on periodic points, or X contains a nontrivial spaceship for f. Since the latter cases imply non-nilpotency and all three are semi-decidable, this proves the proposition.

Assume that f is not nilpotent, but is nilpotent on the finitely many periodic points of X, and let $0^{\mathbb{Z}}$ be their limit. We will show that X contains a nontrivial spaceship for f. By Proposition 1.3.12, f is not even weakly nilpotent, so there exists a point $x \in X$ with $f^n(x) \neq 0^{\mathbb{Z}}$ for all n. Let $(r_0, \dots, r_\ell, s_1, \dots, s_\ell) \in \mathcal{B}(X)^{2\ell+1}$ be a starfleet for x. Since f is nilpotent on periodic points, we have $r_i \in 0^*$ for all i. Since $f^n(x) \neq 0^{\mathbb{Z}}$, ${}^\infty r_{i-1} s_i r_i{}^\infty$ is a nontrivial spaceship for f. ■

For countable SFTs, this question is not very interesting, and there is no need to apply the Starfleet Lemma. Namely, if all periodic points map to 0 in f^n, then the CA is already nilpotent. This is because $f^n(X)$ must be a singleton, since every point in it is left- and right-asymptotic to $0^{\mathbb{Z}}$, and if such a point is not $0^{\mathbb{Z}}$, then X is uncountable (since it is an SFT).

By Theorem 1.3.17, nilpotency is equivalent to asymptotic nilpotency on all SFTs, including countable ones. Thus, we have the following.

Corollary 2.2.6 *It is decidable whether a given CA on a countable SFTs is asymptotically nilpotent.*

However, we will see in Section 2.4 that asymptotic nilpotency is undecidable on countable sofic shifts.

Rice's theorem, Theorem 8 in [Ric53], states that for any nontrivial class of languages $\mathcal{C}$, it is undecidable whether the language of a given Turing machine is in $\mathcal{C}$. There is an analogous result for the limit sets of CA on the full shift [Kar94] which states that for any nontrivial class of limit sets, it is undecidable whether the limit set of a given CA is in this class. By the previous proposition, whether the limit set is $\{0^{\mathbb{Z}}\}$ is decidable for cellular automata on countable sofic shifts. An interesting question is whether some weaker form of Rice's theorem holds on countable sofic shifts, since Theorem 2.4.6 proved in Section 2.4 implies that individual limit sets can have very complicated structure. In fact, the result of [Kar94] only holds if the full shift on which the cellular automaton is run is not fixed: for cellular automata on a fixed full shift $S^{\mathbb{Z}}$, it is certainly decidable whether the limit set is $S^{\mathbb{Z}}$, as this is easily seen to be equivalent to surjectivity. However, all other questions about the contents of the limit set are undecidable [GR10b]. Similarly, it could be that the singleton limit sets are special in the countable case, but a natural partial Rice's theorem still exists. We can at least show that some properties of the limit set *are* undecidable: for an example of an undecidable property about the limit sets of CA on countable SFTs, see Corollary 2.4.11.

Also the decidability of periodicity follows from the Starfleet Lemma. By the results of [KO08], the problem is again undecidable for both counter machines and cellular automata, even when restricting to reversible machines.

Proposition 2.2.7 *For CA on countable sofic shifts, periodicity is a decidable property.*

Proof. We will prove that one of the following cases holds for a CA f on a countable sofic shift X: either f is periodic, f is non-injective, or X contains a spaceship for f which is not temporally periodic. Since the latter cases imply non-periodicity and all three are semi-decidable, this proves the proposition.

Suppose on the contrary that f is non-periodic (and hence not weakly periodic by Lemma 1.3.18) and injective, and all spaceships are temporally periodic. Now let $x \in X$ be arbitrary, and let $(r_0, \dots, r_\ell, s_1, \dots, s_\ell)$ be a starfleet for it. Since the points ${}^\infty r_{i-1} s_i r_i^\infty$ are spaceships, they must be temporally periodic, so we can choose $\ell = 1$. Now $f^n(x)$ is a spaceship for large enough n, and by injectivity of f, x is a spaceship itself, hence temporally periodic. This is a contradiction, since f was not weakly periodic. ■

Question 2.2.8 *Is eventual periodicity of CA decidable on countable sofic shifts?*

It is easy to see that nilpotency and periodicity are nontrivial properties of cellular automata on countable sofic shifts. An interesting dynamical property of cellular automata on the full shift is positive expansivity. Positively expansive CA have the nice dynamical property that they are conjugate to their one-directional trace, which makes them easy to study. It is not known whether the property is itself decidable for cellular automata, but many decidability results can be proved for CA that have this property. In the case of countable sofic shifts, we can show that positive expansivity is not possible at all.

Proposition 2.2.9 *Let f be a cellular automaton on an infinite countable sofic shift $X \subset S^{\mathbb{Z}}$. Then f is not positively expansive.*

Proof. If f has a nontrivial spaceship, then it is clearly not positively expansive. If f has no non-trivial spaceships, then $f^n(x)$ is spatially periodic for some n and any $x \in X$ by the Starfleet Lemma. Clearly, there exists C such that $d(f(y), f(z)) < Cd(y, z)$ (a Lipschitz constant for f). Now, for any $\epsilon > 0$, one can take a non-periodic x such that $0 < d(x, \sigma^p(x)) < \frac{\epsilon}{C^n}$, so that $d(f^i(x), f^i(\sigma^p(x)) < \epsilon$ for all $i < [0, n-1]$, and $f^i(x) = f^i(\sigma^p(x))$ for $i \geq n$. f is not positively expansive. ■

Note that expansivity is of course possible, as the shift map is itself expansive. I do not know whether positive expansivity is possible on countable subshifts in general. As a corollary of our result and a result of [BDJ08], we see that it is at least not possible for cellular automata on countable two-dimensional SFTs.

Lemma 2.2.10 (Theorem 3.11 in [BDJ08]) *Let $X \subset S^{\mathbb{Z}^2}$ be an infinite countable SFT. Then there exists $x \in X$ which has exactly one direction of periodicity.*

Proposition 2.2.11 *Let $X \subset S^{\mathbb{Z}^2}$ be an infinite countable SFT, and let $f : X \to X$ be a CA. Then f is not positively expansive.*

Proof. Take a singly but not doubly periodic point $x \in X$. Let x have period vector $\vec{v}$. Now, let Y be the set of points of X with period $\vec{v}$. Of course, $f(Y) \subset Y$. By a matrix translation argument, we may assume $\vec{v} = (0, 1)$. Namely, let $\vec{w} \in \mathbb{Z}^2$ be such that

$$A = \begin{pmatrix} \vec{w} \\ \vec{v} \end{pmatrix} \in SL_2(\mathbb{Z})$$

(using, say Bézout's identity). Then $A(x)$ has period $(0, 1)$. Now, f induces a natural action on the one-dimensional subshift $Y' = Y_{(\mathbb{Z},0)}$. Of course, Y' is countable, and since Y was singly but not doubly periodic, Y' is infinite. By Proposition 2.2.9, f is not positively expansive on Y', and thus not on Y either. ■

2.3 From Counter Machines to Cellular Automata

Let $M = (\Sigma, k, \delta)$ be a deterministic counter machine. We construct a countable SFT X_M and a CA f_M on X_M simulating M in a concrete fashion. The idea is that the tape contains a symbol # marking an 'origin', and there are k tracks corresponding to the k counters of M, each of which contain a single symbol which is m cells to the right of # if the corresponding counter contains the value m. A symbol called the 'zig-zag head' bounces between # and the rightmost counter, performing the computation.

As we want to do the simulation in a countable SFT, we have to locally remember which counters (or # or the zig-zag head) are to the left and right of the current cell. Thus, the content of each track will be of the form ${}^{\infty}asb^{\infty}$ for some symbol s. The construction works equally well if we set $a = b = 0$, but the forbidden patterns have to be adjusted, and the subshift obtained will be proper sofic.

Definition 2.3.1 *Let $\Sigma_1 \subset \Sigma$ be the set of those states q for which we have $(q, i, Z, q') \in \delta$ or $(q, i, P, q') \in \delta$, where $i \in [1, k]$, $q' \in \Sigma$. Let $\Sigma_2 = \Sigma \setminus \Sigma_1$. We define a subshift $X_M \subset S^{\mathbb{Z}}$ where*

$$S = (\Sigma' \cup \{a, b\}) \times \{\#, a, b\} \times \prod_{i \in [1,k]} \{i, a, b\},$$

and $\Sigma' = (\Sigma_1 \times \{\leftarrow, \rightarrow\}) \cup (\Sigma_2 \times \{\leftarrow, \leftarrow', \rightarrow\})$. *The subshift* X_M *is a subset of*

$$\mathcal{B}^{-1}(a^*\Sigma' b^*) \times \mathcal{B}^{-1}(a^*\#b^*) \times \prod_{i\in[1,k]} \mathcal{B}^{-1}(a^* i b^*),$$

and we also forbid some extra patterns of length at most 2*: First, we forbid the symbols* (s, m, w) *where*

- $s \in \Sigma'$ *and* $m = a$,
- $s \in \Sigma'$ *and* $w_i = b$ *for* $i \in [1, k]$, *or*
- $m = a$ *and* $w_i \neq a$ *for some* $i \in [1, k]$

are forbidden. Furthermore, if $(q, i, j, q') \in \delta$ *for* $j \in [-1, 1]$,

- *we forbid the symbol* $((q, \leftarrow), m, w)$ *if* $w_i = a$.
- *and if* $j = -1$, *we forbid the symbol* $((q, \leftarrow'), m, w)$ *if* $w_i = b$.
- *and if* $j \in \{0, 1\}$, *we forbid the symbol* $((q, \leftarrow'), m, w)$ *if* $w_i \neq a$.
- *and if* $j = 1$, *we forbid the length-*2 *patterns*

$$((q_1, \leftarrow'), m^1, w^1)(b, m^2, w^2)$$

where $w_i^2 \neq a$.

Write $X = X_M$ for short. The first list of forbidden patterns (letters) specifies that none of the symbols $[1, k]$ can occur to the left of $\#$, and not all symbols $[1, k] \cup \{\#\}$ can occur on the same side of $s \in \Sigma'$. The second specify when the left arrow should be $\leftarrow$ and when $\leftarrow'$. It is clear that X is a countable SFT. A point of X_M is *good* if it contains some $s' \in \Sigma'$, the symbol $\#$ and all symbols $i \in [1, k]$.

We refer to the (at most one) symbol Σ' in a point as the *zig-zag head*. The idea of the CA f_M is that the zig-zag head sweeps back and forth between the symbol $\#$ and the rightmost counter, updating the counters based on the tuples in δ. (Note that the rightmost counter can be detected locally, by waiting until none of the symbols on the tracks containing counters are a.) The state of the simulated counter machine is kept in the component Σ, and it is updated at the origin, when a new sweep begins. The component $\{\rightarrow, \leftarrow, \leftarrow'\}$ is used to remember which direction the head is going, and we have two versions of the left arrow to remember whether a counter value has been changed yet, $\leftarrow$ meaning that a counter has not been updated, and $\leftarrow'$ that one has. The counter values are changed when going to the left toward the origin, on the step where the zig-zag head is on top of the counter we want to change. Cells of the point more than one cell away from the zig-zag

head are unchanged by the CA, so that at most 3 cells can be changed in a single step.

We now define f_M in detail. The important properties of f_M will be summarized in Lemma 2.3.2.

The coordinate i of a good point $x \in X_M$ such that x_i contains the symbol # in the second component is called the *root* of x. To define f_M, we define an auxiliary function $\phi : \Sigma' \times \mathbb{N}^{k+1} \to S^{\mathbb{Z}}$ by

$$\phi(p, m, n_1, \ldots, n_k) = ({}^{\infty}a.a^m pb^{\infty}) \times ({}^{\infty}a.\#b^{\infty}) \times \prod_{i \in [1,k]} {}^{\infty}a.a^{n_i} ib^{\infty}.$$

Let $D \subset \Sigma' \times \mathbb{N}^{k+1}$ be the set of those configurations c for which $\phi(c) \in X_M$. Then ϕ is a bijection between D and the good points of X_M rooted at the origin. In particular, the orbit closure of $\phi(D)$ is X_M.

We now define the image of f_M on the points $\phi(D)$. The set of points in $\phi(D)$ will be closed under the CA, so that

$$f_M(\phi((q, d), m, n_1, \ldots, n_k)) = \phi((q', d'), m', n'_1, \ldots, n'_k)$$

for some $((q', d'), m', n'_1, \ldots, n'_k) \in D$. We now give global rules for determining each of the components in $((q', d'), m', n'_1, \ldots, n'_k)$, and the rules amount to a specification of a CA with radius 1. The rules do not cover every case, and we say that *updating is successful* if for *all* of the components, one of the rules for determining a new state for it applies. If updating is not successful, then *none* of the components is updated as described, and the CA behaves as the identity map instead, that is,

$$((q', d'), m', n'_1, \ldots, n'_k)) = (q, d), m, n_1, \ldots, n_k).$$

First, we define the movement of the zig-zag head, that is, the new value of m':

- If $d \in \{\leftarrow, \leftarrow'\}$, and $m > 0$, then $m' = m - 1$.
- If $d \in \{\leftarrow, \leftarrow'\}$, and $m = 0$, then $m' = 0$.
- If $d = \rightarrow$ and $m < \max\{n_i \mid i \in [1, k]\}$, then $m' = m + 1$.
- If $d = \rightarrow$ and $m = \max\{n_i \mid i \in [1, k]\}$, then $m' = m$.

For determining the new values of other components, we need to name a particular situation: we say that we *see the CoI* (counter of interest) if $m = n_i$ and $(q, i, j, r) \in \delta$ for $j \in \{-1, 0, 1\}$. In this situation, we will update the value of the counter n_i, if we are going to the left, and $d = \leftarrow$. There are some things worth noting here. First, since we are updating while moving to the left, the zig-zag head cannot exit the area spanned by the #-symbol and

the rightmost counter. Second, when we update a counter, we change the direction component to $\leftarrow'$, so that at most a single counter can be updated during a sweep. Third, by the definition of a deterministic counter machine, if $(q, i, j, r) \in \delta$ for $j \in \{-1, 0, 1\}$, then this is the only tuple in δ with q as the leftmost component. Thus, it is indeed enough to update the state of one counter.

Next, we determine the new value of the direction component d':

- If $d = \leftarrow'$ and $m > 0$, then $d = \leftarrow'$.
- If $d = \leftarrow'$ and $m = 0$, then $d = \rightarrow$.
- If $d = \leftarrow$, $m > 0$, and we do not see the CoI, then $d' = \leftarrow$.
- If $d = \leftarrow$, $m > 0$, and we see the CoI, then $d' = \leftarrow'$.
- If $d = \leftarrow$ and $m = 0$, then $d = \rightarrow$.
- If $d = \rightarrow$ and $m < \max\{n_i \mid i \in [1, k]\}$, then $d' = \rightarrow$.
- If $d = \rightarrow$ and $m = \max\{n_i \mid i \in [1, k]\}$, then $d' = \leftarrow$.

Next, we determine the new value of the state component q':

- If $m > 0$, then $q' = q$.
- If $d = \rightarrow$ and $m = 0$, then $q' = q$.
- If $d \in \{\leftarrow, \leftarrow'\}$, $m = 0$, $(q, i, Z, r) \in \delta$ and $n_i = 0$, then $q' = r$.
- If $d \in \{\leftarrow, \leftarrow'\}$, $m = 0$, $(q, i, P, r) \in \delta$ and $n_i > 0$, then $q' = r$.
- If $d \in \{\leftarrow, \leftarrow'\}$, $m = 0$, $(q, i, j, r) \in \delta$ and $j \in [-1, 1]$, then $q' = r$.

Finally, we determine the new values of counters:

- If $d \in \{\leftarrow', \rightarrow\}$, then $\forall i : n'_i = n_i$.
- If $d = \leftarrow$ and we do not see the CoI, then $\forall i : n'_i = n_i$.
- If $d = \leftarrow$ and we see the CoI (so that $m = n_i$ and $(q, i, j, r) \in \delta$ for $j \in [-1, 1]$), then if $n_i + j \geq 0$, we put $n'_i = n_i + j$ and $n'_h = n_h$ for $h \neq i$.

By inspecting the cases determining the new state for each component, we find that the only points where updating is not successful are ones where the zig-zag head is at the origin, $d \in \{\leftarrow, \leftarrow'\}$, and the counter machine halts on the configuration $(q, n_1, \ldots, n_k)$. That is, exactly mirroring the situation for counter machines, we are in one of the cases below:

- $d \in \{\leftarrow, \leftarrow'\}$, $m = 0$ and there is no tuple of the form (q, i, j, r) in δ for $j \in \{-1, 0, 1, Z\}$ and $n_i = 0$.
- $d \in \{\leftarrow, \leftarrow'\}$, $m = 0$ and there is no tuple of the form (q, i, j, r) in δ for $j \in \{-1, 0, 1, P\}$ and $n_i > 0$.
- $d = \leftarrow$, $m = 0 = n_i$ and $(q, i, -1, r) \in \delta$.

Note that the new value of each component in each cell is determined by a local rule of radius 1 on $\phi(D)$. Thus, f_M extends to a cellular automaton on X_M, with a radius 1 local rule $(f_M)_{\text{loc}} : S^3 \to S$.

We list some properties of the construction without proofs. Namely, we formalize the idea that points where the zig-zag head is at the origin and going to the right correspond to configurations of the counter machine. Let

$$E = \{((q, d), m, n_1, \ldots, n_k) \in D \mid m = 0, d = \rightarrow\},$$

the set of tuples corresponding to such points. We show that if we restrict our attention to rows of spacetime diagrams containing elements of $\phi(E)$, then we will see encoded computations of M, in the following sense:

Lemma 2.3.2 *We have the following correspondence between M and f_M:*

- *The point $f_M(x)$ is good if and only if x is.*
- *If $(q, n_1, \ldots, n_k) \Rightarrow_M (q', n'_1, \ldots, n'_k)$, then there exists a smallest number $n > 0$ such that $f^n(\phi((q, \rightarrow), 0, n_1, \ldots, n_k)) \in \phi(E)$, and we have*

$$f^n(\phi((q, \rightarrow), 0, n_1, \ldots, n_k)) = \phi((q', \rightarrow), 0, n'_1, \ldots, n'_k).$$

- *If $(q', n'_1, \ldots, n'_k)$ is not initial for M, then there exists $m > 0$ such that if $\ldots, x_{-2}, x_{-1}$ is a preimage chain for $x_0 = \phi((q', \rightarrow), 0, n'_1, \ldots, n'_k)$, that is, $f_M(x_{i-1}) = x_i$ for all $i \leq 0$, then there exists a largest n with $-m < n < 0$ such that $x_n \in \phi(E)$, and if $x_n = \phi((q, \rightarrow), 0, n_1, \ldots, n_k)$, then*

$$(q, n_1, \ldots, n_k) \Rightarrow_M (q', n'_1, \ldots, n'_k).$$

- *If $(q', n'_1, \ldots, n'_k)$ is initial, then $\phi((q', \rightarrow), 0, n'_1, \ldots, n'_k)$ has no infinite preimage chain.*

The CA f_M constructed above simulates a counter machine M on a countable subshift X_M. When the counter machine M is also reversible, we can make a further modification and add a *direction of time*, simulating the machine in both directions. More precisely, we define a countable SFT

$$Y_M \subset \mathcal{B}^{-1}(a^*\Sigma''b^*) \times \mathcal{B}^{-1}(a^*\#b^*) \times \prod_{i \in [1,k]} \mathcal{B}^{-1}(a^*ib^*)$$

with additional forbidden symbols determined as for X_M, but we add an extra component in the zig-zag head:

$$\Sigma'' = \Sigma' \times \{\downarrow, \uparrow\}.$$

The idea of this component is that M is simulated forward if the component is $\downarrow$, and backward if the component is $\uparrow$.

More precisely, for $x \in Y_M$, write $\pi(x) \in X_M$ for the point in X_M where the $\{\downarrow, \uparrow\}$-component is removed from the zig-zag head (so that $\pi : Y_M \to X_M$ is a symbol map), and $\pi_\downarrow^{-1} : X_M \to Y_M$ and $\pi_\uparrow^{-1} : X_M \to Y_M$ for the symbol maps that add the $\{\downarrow, \uparrow\}$-component determined by the subscript.

On good points (defined as before), we define a CA $g_M : Y_M \to Y_M$ by

$$g_M(x) = \pi_\downarrow^{-1}(f_M(\pi(x))),$$

if the direction of time is forward ($\downarrow$) and updating of f_M is successful on x. If the direction of time is backward, and there exists a unique point y with a backward direction of time such that $x = \pi_\downarrow^{-1}(f_M(\pi(y)))$, then $g_M(x) = y$ (uniqueness can clearly be checked by a local rule). If neither of the previous cases occurs, then the direction of time is flipped.

Note that while a deterministic and reversible counter machine M has an inverse counter machine M^{-1} and $X_M = X_{M^{-1}}$, we cannot simply run one of the CA f_M or $f_{M^{-1}}$ on X_M depending on the direction of time: $f_{M^{-1}}$ is not the inverse of f_M. In fact, g_M has radius 2.

We need to show that g_M is bijective. For this, we prove a general lemma about this type of direction-of-time constructions.

Lemma 2.3.3 *Let $f : X \to X \dot\cup \{\textvisiblespace\}$ be a function satisfying $f(x) = f(y) \in X \implies x = y$.[4] We add a time component, to obtain a new space $Y = X \times \{\downarrow, \uparrow\}$, and define $g : Y \to Y$ by*

- $g(x, \downarrow) = (y, \downarrow)$, *if* $f(x) = y \in X$,
- $g(x, \downarrow) = (x, \uparrow)$, *if* $f(x) = \textvisiblespace$,
- $g(y, \uparrow) = (x, \uparrow)$, *if* $f(x) = y$, $x \in X$, *and*
- $g(y, \uparrow) = (y, \downarrow)$, *if* $y \notin f(X)$.

Then g is a well-defined bijective function.

Proof. It is easy to verify that precisely one of the four cases always occurs, so g is a well-defined function.

[4] If we think of $f(x) = \textvisiblespace$ as meaning that x does not have an image in f, then the assumption is that f is an injective partial function from X to itself.

First, let us show g is injective. Suppose on the contrary that $g(x,d) = g(x',d') = (y,e)$ and $(x,d) \neq (x',d')$. If $d \neq d'$, then without loss of generality, we may assume $e = d$. Then $x' = y$, since the arrow component cannot change if the point changes. If $d = \downarrow$, then $f(x) = y$, so $g(x',d') = (x,\uparrow) \neq (y,e)$, a contradiction. If $d = \uparrow$, then $f(y) = x$, so $g(x',d') = (x,\downarrow) \neq (y,e)$, a contradiction. We thus have that $d = d'$. If $e \neq d$, then $x = y = x'$, so necessarily also $e = d$. Finally, the case $d = \downarrow$ is impossible by the injectivity of f and the case $d = \uparrow$ is impossible because f is a function. Thus, g is indeed injective.

To show that g is surjective, let (y,d) be arbitrary. Then

- if $d = \downarrow$ and $f(x) = y$ for some x, then $g(x,d) = (y,d)$,
- if $d = \downarrow$ and $y \notin f(X)$, then $g(y,\uparrow) = (y,d)$,
- if $d = \uparrow$ and $f(y) = x \in X$ for some x, then $g(x,\uparrow) = (y,d)$, and
- if $d = \uparrow$ and $f(y) = \_$, then $g(y,\downarrow) = (y,d)$.

■

Lemma 2.3.4 *If M is deterministic and reversible, then the CA $g_M : Y_M \to Y_M$ is bijective.*

Proof. It is enough to show that $f_M : X_M \to X_M$ is injective on points where updating is successful, as the claim then follows from Lemma 2.3.3 and the fact that because changes to the current point only happen near the zig-zag head, it is enough to carry the direction of time in the zig-zag head. The injectivity of f_M on points where updating is successful is a simple case analysis. ■

2.4 CA on Countable Sofics – the Complex

In this section, we focus on the computational properties of cellular automata, mainly considering the computational complexity of their limit sets and asymptotic sets. This section slightly differs in spirit from the rest of this thesis, as it turns out that both limit sets and asymptotic sets are computationally rather complicated.

Before moving on to such results, let us briefly consider the finitely generatedness of the endomorphism monoid.

Example 2.4.1 *There exists a countable sofic shift whose endomorphism monoid is not finitely generated. For example, $X = \mathcal{B}^{-1}(0^*10^*10^*)$ does not have a finitely generated endomorphism monoid, since if $f_1, \dots, f_n$ is any finite set of CA on X, and r is the maximal radius among the f_i, then the f_i do not generate any CA on X mapping ${}^\infty 0.10^r 10^\infty \mapsto {}^\infty 0.10^{r-1}10^\infty$.*

It is slightly harder to construct a countable SFT without a finitely generated endomorphism monoid, because the global structure of the point must be visible to the local rules of the CA, so that one might in theory be able to move the interesting patterns close to each other, perform the logic of the CA locally, and then send them to their final locations. We show by a very simple example that this is at least not possible in general.

Proposition 2.4.2 *There exists a countable SFT whose endomorphism monoid is not finitely generated.*

Proof. We claim that the countable SFT $X = \mathcal{B}^{-1}(0^*1^*2^*)$ does not have a finitely generated endomorphism monoid. Suppose on the contrary that $f_1, \dots, f_n$ generate the endomorphism monoid, and let r be the maximal radius among their local rules. Let f be defined by

$$f(^\infty 0.1^k 2^\infty) = {}^\infty 0.1^{k'} 2^\infty,$$

where $k' = 4r + 1 - k$ if $k \in [2r, 2r + 1]$, and $k' = k$ otherwise.

Suppose $f = f_{j_n} \cdots f_{j_1}$. First, it is clear that also the f_{j_i} map $0^\mathbb{Z} \mapsto 0^\mathbb{Z}$ and $2^\mathbb{Z} \mapsto 2^\mathbb{Z}$, or f would not behave as the identity for large enough lengths of the run of 1s. Similarly, we see that on the points $^\infty 0.1^k 2^\infty$ with $k \geq 2r$, all of the f_{j_i} simply increment of decrement k by some $r' \in [-2r, 2r]$ (and possibly shift the whole point).

Now, there must exist a prefix $g = f_{j_h} \cdots f_{j_1}$ of $f_{j_n} \cdots f_{j_1}$ such that $g(^\infty 0.1^{2r} 2^\infty) \in \mathcal{O}(^\infty 0.1^{2r-\ell} 2^\infty)$ where $\ell > 0$, since otherwise we have

$$\exists m : \forall k \geq 2r : f(^\infty 0.1^{k+m} 2^\infty),$$

which contradicts the choice of f. But then

$$g(^\infty 0.1^m 2^\infty) \in \mathcal{O}(^\infty 0.1^{m-\ell} 2^\infty)$$

for all $m \geq 2r$, which clearly means that g is not injective, which is a contradiction since f is injective. ■

Next, we discuss predictability. In fact, using the construction in the previous section, there is little work in showing that the endomorphism monoid of a countable SFT need not be predictable:[5]

Proposition 2.4.3 *There exists a countable SFT X whose endomorphism monoid is not predictable.*

[5] In fact, this is even easier than on the full shift, because unlike on the full shift, isolated points are dense in a countable sofic shift, so the finite pattern can completely determine the orbit of the point.

Proof. Let M be a counter machine for which it is undecidable whether, given two configurations c_1 and c_2, $c_1 \Rightarrow_M^* c_2$. Then, X_M has an unpredictable endomorphism monoid, as f_M is clearly unpredictable. ■

A more interesting question than whether such examples exist is how common they are. I believe they are common – even ubiquitous.

Conjecture 2.4.4 *There exists k such that every countable SFT of Cantor-Bendixson rank at least k has a non-finitely generated endomorphism monoid.*

If this is the case, the next question is what the minimal such k is. As we saw in Proposition 2.4.2, there exists a rank 3 countable SFT with this property. On the other hand, it is easy to see that a rank 2 countable SFT always has a finitely generated endomorphism monoid. Thus, $k = 3$ is a plausible candidate.

Conjecture 2.4.5 *There exists m such that every countable SFT of Cantor-Bendixson rank at least m has a non-predictable endomorphism monoid.*

Again, if this is the case, it would be interesting to know the minimal value of m. It is well-known that for counter machines, two counters suffice for general computation (see for example [Min67]). This means that there exists such a countable SFT with an unpredictable endomorphism monoid for $m = 4$ by the proof of Proposition 2.4.3. It seems clear that a CA on a countable SFT with Cantor-Bendixson rank 3 or less cannot perform any kind of computation,[6] so $m = 4$ is the smallest possible candidate.

We recall the hierarchy $X_n = \mathcal{B}^{-1}(1^*2^* \cdots n^*)$ of countable SFTs from Example 2.1.1. The subshifts X_n seem like good canonical examples of countable SFTs. In Proposition 2.4.2, we showed that X_3 does not have a finitely generated endomorphism monoid. We can also easily perform the construction of Section 2.3 on a subSFT of X_n for large enough n, and find X_n with an unpredictable endomorphism monoid: If k colors are needed for the subshift X in Proposition 2.4.3, and n is larger than $2k \cdot k!$, we can dedicate a contiguous subset of length at most k of the *even* colors of X_n, for each order in which the colors may occur in X. To make sure the points where extra patterns occur are not a problem, we leave all odd colors unused, and use them as spreading states. It is easily seen that X_n then has an unpredictable endomorphism monoid for large n.

In the rest of this section, we refine the message of Proposition 2.4.3 that cellular automata on countable SFTs and sofic shifts are capable of general computation, by proving a sequence of undecidability results for them.

[6] The points of such an SFT can contain at most 2 islands. Cellular automata can only increase the lengths to infinity, or decrease them until it reaches a finite set of points, depending on its radius.

2.4.1 Limit Sets and Transient Behavior

Recall that the limit set of a CA $f : X \to X$ is the set of points $x \in X$ with arbitrarily long chains of preimages (and by compactness, also an infinite one) in the action of f.

If f is a cellular automaton on a Π^0_1 subshift X, then the (language of the) limit set of f is also Π^0_1, since if a word w is not in the language of the limit set of f, then a Turing machine enumerating forbidden patterns of X will eventually find an n such that there is no preimage chain of length n along legal patterns of X. It is folklore that this is tight, in the sense that there exists a CA with a Π^0_1-complete limit set on a full shift, although I am not aware of a published proof of this. In Corollary 2 of [Hur87], the existence of a cellular automaton with a non-recursive limit set on a full shift is claimed, but the article only proves that it is undecidable to compute whether, *given a cellular automaton*, its limit set contains a particular letter, which on the face of it has no implications on the complexity of the limit set. We show the existence of a cellular automaton on a countable SFT with such a complicated limit set, from which the result follows also on a full shift.

Theorem 2.4.6 *There exists a CA $f : X \to X$ on a countable SFT X such that the limit set of f is Π^0_1-complete.*

Proof. Let $M = (\Sigma, k, \delta)$ be a deterministic and reversible counter machine such that

$$L(M) = \{n \mid \text{The computation starting from } (q_0, n, 0, \dots, 0) \text{ is infinite.}\}$$

is Π^0_1-complete for some $q_0 \in \Sigma$, and there are no transitions (q, i, j, q_0) in δ. Such a machine is obtained by first finding such deterministic counter machine M' (for example, $L(M)$ could contain the indices of non-halting machines in some effective enumeration of Turing machines), and making it reversible with Lemma 1.4.3.

Let N be the inverse counter machine of M, and construct the countable SFT X_N and the cellular automaton f_N as in Section 1.4. Note that we use the one-directional version of the simulation, but for the inverse counter machine.

Now, we claim that the point

$$x_n = \phi((q_0, \to), 0, n, 0, \dots, 0)$$

is in the limit set of g if and only if $n \in L(M)$. First, if $n \in L(M)$, then an infinite chain of preimages is obtained by simply running M: if

$$c \Rightarrow_M (q_1, n_{1,1}, \dots, n_{1,k}) \Rightarrow_M (q_2, n_{2,1}, \dots, n_{2,k}) \Rightarrow_M \cdots,$$

for $c = (q_0, n, 0, \ldots, 0)$, then the same configurations form an infinite N-preimage chain. An infinite preimage chain for x_n is then found by stitching together f_N-computations between points

$$\phi((q_i, \rightarrow), 0, n_{i,1}, \ldots, n_{i,k}))$$

(see Lemma 2.3.2).

Consider then the case $n \notin L(M)$. Suppose the full computation of M starting from $c = (q_0, n, 0, \ldots, 0)$ is

$$c \Rightarrow_M (q_1, n_{1,1}, \ldots, n_{1,k}) \Rightarrow_M \cdots \Rightarrow_M (q_m, n_{m,1}, \ldots, n_{m,k}).$$

Then, by Lemma 2.3.2, any f_N-preimage chain of x_n will, in a bounded number of steps, reach the point

$$\phi((q_m, \rightarrow), 0, n_{m,1}, \ldots, n_{m,k}),$$

which has no infinite preimage chain. Thus, x_n does not have one either.

Now, to show that the language of the limit set of f is Π^0_1-complete, simply note that the points x_n are isolated, and the isolating pattern is easily computed from n. ■

The corresponding result follows also on the full shift, proving Corollary 2 in [Hur87].

Corollary 2.4.7 *There exists a CA f on a full shift such that the limit set of f is Π^0_1-complete.*

Proof. Let X and f be given by Theorem 2.4.6. We embed X in the full shift $(\mathcal{B}_1(X) \cup \{\#\})^{\mathbb{Z}}$ and make $\#$ a new spreading state for f which appears whenever a neighborhood is forbidden in X. The complexity of the limit set can only increase, since words not containing $\#$ have only preimages not containing $\#$. ■

In addition to what the limit set looks like, it is also interesting how the limit set is approached, often called the transient behavior. One precise property qualifying the transient behavior is whether the CA is stable or unstable, that is, whether, for a CA $f : X \to X$, $f^n(X)$ is equal to the limit set of f for large enough n. As usual, the first thing we should ask is of course whether this concept even makes sense in the countable case, that is, whether it is trivial.

Example 2.4.8 *Cellular automata on countable SFTs can be stable or unstable: The identity automaton always has a stable limit set. For an example of an unstable limit set, see the automaton $f_{\text{increment}}$ in Example 2.2.4.*

An example is known of a subshift which is the limit set of both stable and unstable cellular automata on the full shift [BGK11]. We show that this can also happen on a countable sofic shift.

Example 2.4.9 *Let X be the union of the countable sofics $\mathcal{B}^{-1}(0^*10^*20^*)$ and $Y = \mathcal{B}^{-1}(0^*(1^* + 2^*)0^*)$. Then X is also a countable sofic shift. Let $f : X \to X$ be the radius-1 CA for which 0 is a spreading state, and let $g : X \to X$ be the CA that moves every lone 1 to the left, and otherwise acts as the identity map.*

Consider the set $f(X)$. It clearly contains the set Y, but points of the form $^\infty 010^n 20^\infty$ have no preimage under f. Also, $f^2(X) = f(X)$, so Y is the limit set of f reached in one step.

Consider then the limit set of g, which also clearly contains Y. For all n, the point $^\infty 010^n 20^\infty$ has a preimage under g^n, but not g^{n+1}. Thus the limit set of g is also Y, and g is unstable.

For cellular automata on countable SFTs, on the other hand, an example like this is impossible:

Theorem 2.4.10 *Let X be a countable SFT and $f : X \to X$ a cellular automaton. Then f is stable if and only if its limit set is an SFT.*

Proof. It is true on every SFT that if the limit set is an SFT, then f is stable: the finitely many forbidden patterns defining the limit set must already be forbidden in some $f^n(X)$.

For the other direction, assume the contrary, so that f is stable but the limit set is not an SFT. Let k be such that f reaches its (necessarily sofic) limit set Y in k steps. Without loss of generality, we may assume $k = 1$, since f^m has the same limit set as f for all m, and f is stable if and only if f^m is. Also, since all (finitely many) spatially periodic points are temporally eventually periodic for f, we may assume without loss of generality that all spatially periodic points of X are mapped in one step into a spatially periodic fixed point of f. Let p be a common spatial period for all the spatially periodic points.

First, we show that, within Y, the only preimage of a periodic point is itself. That is,

$$x, y \in Y \wedge f(x) = y \wedge y \text{ periodic } \implies x = y.$$

It is clear that at least a periodic point cannot have another periodic point as a preimage, since by the assumption every periodic point in Y is mapped to itself by f. But in general, x will have periodic left and right tails. This means that x is actually left and right asymptotic to y. It follows that if $x \neq y$, then X is uncountable, a contradiction.

Now, let n be a window size for X. Clearly, if there exists m such that for all w with $|w| > m$ forbidden in Y, either $w_{[1,|w|-1]}$ or $w_{[2,|w|]}$ is forbidden, then Y is an SFT, so suppose this is not the case. For all $i > n$ we may then take a word $w_i \sqsubset X$ of length at least i such that for $u_i = (w_i)_{[1,|w_i|-1]}$

and $v_i = (w_i)_{[2,|w_i|]}$, we have $u_i, v_i \sqsubset Y$, but w_i is forbidden in Y. Since Y is sofic, there exists m such that any p-periodic prefix or suffix of any w_i has length at most m.

Since $u_i \sqsubset Y$, there is a preimage $u_i' \sqsubset Y$ for it, and similarly there is a preimage $v_i' \sqsubset Y$ for v_i. Since X is countable, w_i must contain a long periodic sequence, which then occurs in both u_i and v_i as well, in the sense that we find arbitrarily large $j_2 - j_1$ such that $(u_i)_{[j_1,j_2]} = (v_i)_{[j_1-1,j_2-1]}$ is periodic. The only preimage for this sequence is itself, and thus, if the sequence is long enough, u_i' and v_i' can be glued along this sequence to obtain a preimage for w_i in X (even in Y). ■

Theorem 2.4.11 *It is undecidable whether a CA on a countable SFT is stable.*

Proof. From Lemma 1.4.3, it easily follows that given a deterministic and reversible counter machine M, it is undecidable whether M halts on $c = (q_0, 0, \dots, 0)$, even when restricted to machines where this configuration has no preimage.

Now, given M, construct the countable SFT Y_M and the CA g_M running M in both directions. Recall that g_M is bijective, so that the limit set is Y_M. Now, we modify g_M so that the points in the orbit of $\phi((q_0, \rightarrow, \uparrow), 0, \dots, 0)$ (modifying the ϕ-map in the obvious way) become fixed points, but no other point is affected, and call the automaton obtained g. We now claim that g is stable if and only if M halts from c.

Suppose first that M does not halt from c. Then $g^n(\phi((q_0, \rightarrow, \downarrow)))$ has a preimage chain of length at least n, but this preimage chain cannot be extended. Thus, g is unstable.

Suppose then that M halts from x. Then in the computation starting from $x = \phi((q_0, \rightarrow, \downarrow), 0, \dots, 0)$ the simulation of f_M is eventually reversed, and thus for some n, we have

$$g^n(x) = \phi((q_0, \rightarrow, \uparrow), 0, \dots, 0),$$

which is a fixed point. The finitely many points on this path do not have infinite preimage chains (except for $\phi((q_0, \rightarrow, \uparrow), 0, \dots, 0)$), but the orbit of no other point in Y_M is affected by our modification of g_M, since the bijectivity of g_M guarantees that orbits are disjoint. Thus, $g^n(Y_M)$ is the limit set of g, so g is stable. ■

From the previous theorems, we also obtain an undecidable property of the limit set:

Corollary 2.4.12 *It is undecidable whether the limit set of a CA on a countable SFT is an SFT.*

Of course, a fortiori, both problems are undecidable on countable sofic shifts, even though Theorem 2.4.10 does not hold on countable sofics in general.

2.4.2 Asymptotic Sets

The limit set is not the only notion corresponding to 'where points eventually go'. Another such concept, studied at least in [GR10a], is the asymptotic set. We show that such sets can be interesting in the countable sofic case as well. Recall that the asymptotic set of a CA $f : X \to X$ is

$$\bigcup_{x \in X} \bigcap_{J \in \mathbb{N}} \overline{\{f^n(x) \mid n \geq J\}}$$

A point $y \in X$ lies in the asymptotic set if and only if there exists another point $x \in X$ and a subsequence of the orbit $(f^n(x))_{n \in \mathbb{N}}$ which converges to y. Note that the asymptotic set contains all temporally periodic points of f, but not necessarily all the spaceships, unlike the limit set. Asymptotic sets have much stronger computational capabilities than limit sets, and turn out to live in Σ^0_3, a few steps north of Π^0_1, the home of limit sets.

Lemma 2.4.13 *The asymptotic set Y of a CA f on a countable sofic shift X is Σ^0_3.*

Proof. Given a word w, it is clearly in Σ^0_3 to check that

$$\exists x \in X : \forall n : \exists m > n : f^m(x)_{[1,|w|]} = w,$$

which is equivalent to $w \in \mathcal{B}(Y)$. Note that the values x of the first quantifier can easily be enumerated by a Turing machine. ■

Theorem 2.4.14 *There exists a countable SFT X and a CA $f : X \to X$ such that the language of the asymptotic set of f is Σ^0_3-complete.*

Proof. By Lemma 1.4.4, there exists a recursive set L such that solving

$$\exists r : \exists^\infty \ell : (r, \ell, w) \in L$$

for given $w \in \mathbb{N}$ is Σ^0_3-complete. We say that such a w is a *solution to* L. We will many-one reduce any such set to the language of the asymptotic set of a CA.

Let M be a deterministic counter machine that always halts and accepts the language L. That is,

$$(q_0, r, \ell, w, 0, \ldots, 0) \Rightarrow^*_M (q_{\text{acc}}, 0, 0, 0, 0, \ldots, 0)$$

if $(r, \ell, w) \in L$ and

$$(q_0, r, \ell, w, 0, \ldots, 0) \Rightarrow_M^* (q_{\text{rej}}, 0, 0, 0, 0, \ldots, 0)$$

if $(r, \ell, w) \notin L$, and there are no transitions from q_{acc} or q_{rej}.

We construct a counter machine M' with state set $\{s_1, s_2, \ldots, s_p\}$, counters C_w, C_r, C_ℓ, and a suitable set of auxiliary counters, having the property that when started from the configuration $(s_1, w, 2^r \cdot n, \ell, i_1, \ldots, i_h)$ for odd n (w, $2^r \cdot n$ and ℓ being the values of counters C_w, C_r and C_ℓ, respectively), M' enters the state s_1 infinitely many times if and only if w is a solution to L for that choice of r, no matter what the values of i_j are. The counter C_w will always contain the value w and is never modified. The counters C_r and C_ℓ play the role of quantifiers, and C_r contains the value $2^r \cdot n$ instead of r since we want to have its value tend to infinity while preserving the choice of r. The counter C_ℓ contains the value ℓ, and it also tends to infinity, one step at a time.

The states s_1 and s_2 are identical in the sense that $(s_1, i, j, q) \in \delta \iff (s_2, i, j, q) \in \delta$ where δ is the transition function of M, that is, computation proceeds exactly the same way from either state. When started from the state $(s_1, w, 2^r \cdot n, \ell, i_1, \ldots, i_h)$ (or $(s_2, w, 2^r \cdot n, \ell, i_1, \ldots, i_h)$) for odd n, the machine M' multiplies the value in C_r by 3, increments C_ℓ, and then checks if $(r, \ell, w) \in L$ by computing r and simulating a computation of M without using the states s_1 or s_2. Once the check is finished, all counters except C_w, C_r and C_ℓ are set to 0, and M' re-enters the state s_1 if $(r, \ell, w) \in L$, and s_2 otherwise. It follows that the state s_1 is visited infinitely many times if and only if r was a correct guess for w.

Now, construct the countable SFT $X_{M'}$ and the CA $f_{M'} : X_{M'} \to X_{M'}$ as usual. We claim that the point

$$x_w = \lim_{n \longrightarrow \infty} \phi((s_1, \rightarrow), 0, w, n, n, 0, \ldots, 0)$$

is in the asymptotic set of the CA if w is a solution to L, and otherwise no central pattern of this point containing the zig-zag head and the value of the counter C_w occurs in a point in the asymptotic set. First, suppose w is indeed a solution. Then, letting r be such that $\exists^\infty \ell : (r, \ell, w) \in L$, the point x_w is in the asymptotic set because it is a limit point of $\phi((s_1, \rightarrow), 0, w, 2^r, 0, 0, \ldots, 0)$ (for this, note that the values in the counters C_r and C_ℓ tend to infinity).

Now, suppose w is not a solution to L. Suppose that the asymptotic set contains a point $y \in X$ containing a central pattern u of x_w showing the counter C_w and the zig-zag head. Suppose y occurs as a limit point of $x \in X$, and consider the computation that follows after u has occurred in $f^n(x)$. Clearly, $f^n(x)$ must be a good point, or the zig-zag head will never return from its next sweep (so that y is not a limit point of f). But then, a

computation of M' is simulated by $f_{M'}$, and the state s_1 will not be entered infinitely many times. ■

As in the case of limit sets, the corresponding result follows also on the full shift: by adding a spreading state, we obtain a CA f on the full shift such that the asymptotic set of f is Σ_3^0-complete. However, this is not very interesting, since in [Sal13] we show that asymptotic sets can be Σ_1^1-complete in the case of the full shift (with essentially the same proof). The complexity of the asymptotic set has also been investigated from another point of view in the literature: in [DP09], a cellular automaton with a maximally high Kolmogorov complexity in the asymptotic set was constructed. We cannot hope for a result mirroring this, as the Kolmogorov complexity of any point in a countable SFT is 0: By Lemma 2.1.10, all configurations are even computable.[7]

By Theorem 2.4.14, not every asymptotic set is the limit set of a cellular automaton. Besides the computational, there is a topological reason for this: the limit set must necessarily be a subshift, but asymptotic sets need not be closed in general. We show that this can happen in the countable case as well.

Example 2.4.15 *Let $X = \mathcal{B}^{-1}(0^*1^*(\ell + r)2^*3^*)$. Let $f : X \to X$ be the bouncing ball CA defined by*

$$f({}^\infty 0.1^k \ell 2^{k'} 3^\infty) = {}^\infty 0.1^{k-1} \ell 2^{k'+1} 3^\infty$$

if $k > 0$, and

$$f({}^\infty 0.\ell 2^{k'} 3^\infty) = {}^\infty 0.r 2^{k'} 3^\infty,$$

and symmetrically

$$f({}^\infty 0.1^k r 2^{k'} 3^\infty) = {}^\infty 0.1^{k+1} r 2^{k'-1} 3^\infty$$

if $k' > 0$ and

$$f({}^\infty 0.1^k r 3^\infty) = {}^\infty 0.1^k \ell 3^\infty$$

if $k' = 0$. The asymptotic set of f is

$$Y = \mathcal{O}({}^\infty 01^*(\ell + r)2^*3^\infty\}) \cup \overline{\mathcal{O}({}^\infty 01^\infty) \cup \mathcal{O}({}^\infty 23^\infty)},$$

which is not topologically closed, since ${}^\infty 1\ell 2^\infty \notin Y$ is a limit point of Y.

Conversely, we show that starting from a fixed sofic shift, asymptotic sets do not necessarily form a larger class than limit sets. We note that such an example does not exist for mixing SFTs (see Corollary 33 in [GR10a] for the case of full shifts).

[7] More generally, countable subshifts have topological entropy 0, and Lemma 5.1 in [Sim11] shows that this is an upper bound on the Kolmogorov complexity of the points.

Proposition 2.4.16 *There exists a countable sofic shift X and a CA $f : X \to X$ such that the limit set of f is not the asymptotic set of any CA on X.*

Proof. Let

$$X = \mathcal{B}^{-1}(0^*\ell 0^*\#0^*r0^* + 0^*\ell' 0^*\#0^*r'0^*)$$

and g the CA on X which moves ℓ and r towards $\#$, and moves ℓ' and r' away from $\#$, changing $\ell\#r$ to $\ell'\#r'$, but $\ell\#0$ and $0\#r$ to $0\#0$. It is clear that the limit set of g is

$$Y = \mathcal{B}^{-1}(0^*\ell 0^*\#0^*r0^* + \bigcup_{n\in\mathbb{N}} (0^*\ell' 0^n\#0^n r'0^*)).$$

We claim that no CA f on X has Y as its asymptotic set. Assume on the contrary that this is the case, and let f have radius R. In general, it is clearly true for asymptotic sets that for all N and $x \in X$, the word $f^n(x)_{[-N,N]}$ must occur in Y for sufficiently large n. In particular, words of Y must map to words of Y and points in Y have preimages in Y.

Since points of the form $y(M, M') = {}^\infty 0\ell 0^M\#0^{M'}r0^\infty$ appear in the asymptotic set with no restriction on M and M', but the point $z(M, M') = {}^\infty 0\ell' 0^M\#0^{M'}r'0^\infty$ only appears for $M = M'$, a simple case analysis shows that for large M and M', such points map to points of the same form.

Since $z(M, M)$ is isolated in X, and in the asymptotic set, it must be f-periodic. It must also map to a point of the form $z(N, N)$. If for some M, no point of the form $z(N, N)$ with $N \leq 2R - 1$ were to appear in the orbit, then $z(M, M + 1)$ would also be periodic. Therefore, there exists a point $z(N, N)$ with $N \leq 2R - 1$ such that $z(M, M)$ appears in its orbit for arbitrarily large M. But this is a contradiction, since $z(N, N)$ must be f-periodic as well. ■

We sketch in [ST12a] the proof of the following result, showing that any bounded Σ^0_3 subshift can be implemented as an asymptotic set. In particular, according to the result, in contrast to Proposition 2.4.16, every limit set on a countable sofic shift is also an asymptotic set of some CA, if we are allowed to change the countable sofic shift on which the CA is running.

Theorem 2.4.17 *Let Y be any bounded Σ^0_3 subshift. Then there exists a countable sofic shift $Z \supset Y$ and a CA $f : Z \to Z$ such that the asymptotic set of f from Z is exactly Y.*

Theorem 2.4.10 is an example of a property that is specific to countable SFTs, and not true for general countable sofic shifts. We end this section with another such result, by proving that asymptotic nilpotency is undecidable on countable sofic shifts. In fact, we show that – in stark contrast with the decidability result Corollary 2.2.6 for countable SFTs – it is Π^0_3-complete.

Theorem 2.4.18 *Given a countable sofic shift X and a cellular automaton $f : X \to X$ on it, it is Π^0_3-complete to decide whether f is asymptotically nilpotent.*

Proof. First, it is easy to see that asymptotic nilpotency is in Π^0_3, by form:

$$\forall x \in X : \exists m : \forall n \geq m : f^n(x)_0 = 0.$$

Let L be a recursive set such that

$$\{w \in \mathbb{N} \mid \exists r \in \mathbb{N} : \exists^\infty \ell : (w, r, \ell) \in L\}.$$

is Σ^0_3-hard, let M be an always halting deterministic counter machine accepting L. Similarly as in the proof of Theorem 2.4.14, we construct a counter machine M' with counters C_w, C_r and C_ℓ. The counters C_w, C_r and C_ℓ again correspond to the variables w, r and ℓ, but this time we do not need a fancy encoding for r. As in the proof of Theorem 2.4.14, the machine repeatedly checks $(w, r, \ell) \in L$, and increments ℓ between checks, keeping r and w fixed. If $(w, r, \ell) \in L$, M' visits the state s_1.

Let

$$X \subset \mathcal{B}^{-1}(0^*\#_\ell 0^*(0 + \leftarrow + \rightarrow)0^*\#_r 0^*) \times X'_{M'},$$

where the component $X'_{M'}$ is a copy of $X_{M'}$ with a small modification: we remove the symbols a and b that tell in which direction the counters, root and zig-zag head are, in the sense of setting $a = b = 0$. We make the corresponding change to the ϕ-map of $X_{M'}$ to obtain the map ϕ'. We restrict the points of X so that roots of points in $X'_{M'}$ must occur on top of the $\#_r$ symbol (but make no other restrictions). Now, given w, we construct a CA $f : X \to X$ which is not asymptotically nilpotent if and only if $w \in L$.

The CA f on X behaves as follows. The symbol $\#_\ell$ moves to the left by two cells each step, and $\#_r$ and the $X'_{M'}$-point are similarly shifted two steps to the right on every step. The symbols $\leftarrow$ and $\rightarrow$ are called the *potent arrows*. They move three cells each step. The symbol $\leftarrow$ moves to the left, and turns into $\rightarrow$ when it reaches $\#_\ell$. Symmetrically, $\rightarrow$ is moved to the right. However, when it hits $\#_r$, it does not turn into $\leftarrow$, but simply starts following $\#_r$. On the component $X'_{M'}$, f simulates $f_{M'}$ if the counter C_w has value w, and otherwise halts the computation, staying in some state $q \neq s_1$. The potent arrow reacts to the zig-zag head, so that if the state s_1 is entered, and the potent arrow is next to $\#_r$ in state $\rightarrow$, it turns into $\leftarrow$.

Now, we claim that f is not asymptotically nilpotent if and only if w is a solution to L. If it is a solution, we can guess the correct r and start f on the point

$$^\infty 0\#_\ell \rightarrow .\#_r 0^\infty \times \phi((s_1, \rightarrow), 0, w, r, 0, \ldots, 0).$$

The zig-zag head will enter the state s_1 infinitely many times so that $\rightarrow$ is next to $\#_r$, and thus the trace at the origin contains the potent arrow infinitely many times. Thus, f is not asymptotically nilpotent.

If w is not a solution, then we first note that it is clear that the only possible reason for non-asymptotic nilpotency is the potent arrow: every other symbol is moving steadily in one direction, so that, apart from the potent arrow, only 0 will be visible on all tracks given enough time. On the other hand, as in the proof of Theorem 2.4.14, the state s_1 is entered infinitely many times only if the point on the $X'_{M'}$-track is good, C_w contains the value w, and C_r contains a correct guess of r for the word w. Thus, the potent arrow can only make infinitely many sweeps if w is a solution to L. ■

Chapter 3

Minimal Subshifts

3.1 Cellular Automata on Minimal Subshifts

In this section, we study minimal subshifts. These are just the dynamical systems with no proper subshifts. More concretely, X is a minimal subshift if and only if it is uniformly recurrent: for every word w that appears in a point of X, w in fact appears with *bounded gaps* in *every* point of X.

It is hard to say much about endomorphisms of general minimal subshifts, but we mention some easy observations and constructions. The following is folklore, although we do not know a reference.[1]

Lemma 3.1.1 *If the language of a minimal subshift X is Π_1^0, then it is also Σ_1^0, and hence recursive.*

Of course, the shift map σ is predictable on all minimal subshifts by the definition of predictability: given any pair of words $u, v \in \mathcal{B}(X)$, the algorithm says 'yes'. By Lemma 3.1.1, if X is Π_1^0, we have a stronger decidability result, as we can check whether u, v are in the language *and* whether v is reachable from u. We can also show, in general, that shift maps are predictable on minimal Π_1^0 subshifts.[2] This also follows easily from Theorem 4.40 in [GH55], and more explicitly from Proposition 8 in [DKVB06], but we give a direct proof.

Lemma 3.1.2 *If the X is minimal and Π_1^0, then the class of shift maps $\{\sigma^m \mid m \in \mathbb{Z}\}$ is predictable (uniformly in m).*

Proof. Again, we may assume X is nonempty. Suppose we are given $m \in \mathbb{Z}$ and $u, v \in \mathcal{B}(X)$. Of course, if there exists $x \in X$ such that

[1] The SFT case is proved in [Hoc09] with the same proof.

[2] Thanks to Pierre Guillon for telling me this.

$x_{[j,j+|u|-1]} = u$, $x_{[j',j'+|v|-1]} = v$, $j \leq j'$ and $j' - j \equiv 0 \mod m$, then we will find such x, and this is equivalent to reachability.

First, suppose that $x_{[0,|u|-1]} = u$ for some $x \in X$. We show that $x_{[km,km+|u|-1]} = u$ for some $k > 0$. For this, let $j_1 = |u| - 1$, and continue by induction as follows: if j_i is defined, we let $j_{i+1} > j_i$ be such that $x_{[j_{i+1}-j_i,j_{i+1}]} = x_{[0,j_i]}$ (using minimality). Define $J_i \subset \mathbb{Z}_m$ to be the set of $h \in \mathbb{Z}_m$ such that $x_{[km+h,km+h+|u|-1]} = u$ for some $k \in \mathbb{N}$, $km + h > 0$ and $km + h + |u| - 1 \leq j_i$. We clearly have $J_i \subset J_{i+1}$. Let i be minimal such that $J_i = J_{i+1}$. Clearly, $h \in J_{i+1}$ always holds for $h \equiv j_{i+1} - j_i \mod m$, and $J_i + h \subset J_{i+1}$. We now have

$$\{h\} \cup (J_i + h) \subset J_{i+1} = J_i,$$

and it follows that $\ell h \mod m \in J_i$ for all $\ell > 0$. In particular, $mh \equiv 0 \in J_i$, and the claim again follows.

Since recurrence is uniform, it is easy to extend the argument of the previous paragraph to find a uniform bound n such that if $x_{[0,|u|-1]} = u$, then $x_{[km,km+|u|-1]} = u$ for some $0 < km \leq n$. Now, suppose $x_{[j,j+|u|-1]} = u$, $x_{[j',j'+|v|-1]} = v$, $j \leq j'$, $j' - j \equiv 0 \mod m$, and $j' - j$ is minimal. Then $j' - j \leq n$, as otherwise $x_{[j+km,j+km+|u|-1]} = u$, $x_{[j',j'+|v|-1]} = v$ for some $j + km < j'$. It follows that v is reachable from u by σ^m if and only if it is reachable in the first n/m steps. Since n can be easily computed from X and u, reachability is decidable. ■

Of course, if there are no computability restrictions, the endomorphism monoids of minimal subshifts can be unpredictable for rather boring reasons (even if we restrict to shift maps):

Proposition 3.1.3 *There exists a minimal subshift X whose endomorphism monoid is unpredictable.*

Proof. To each sequence $s = (s_1, s_2, \ldots) \in 2^{\mathbb{N}}$ we associate a minimal subshift, such that for two distinct sequences, the prediction problems of the associated subshifts are distinct. Let $W_0^s = \{a, b\}$. Given $W_i^s = \{w_1, w_2\}$ where $|w_1| = |w_2| = k_i$, and w_1 and w_2 mutually unbordered, we define two sets of words U_{i+1}^0 and U_{i+1}^1:

$$U_{i+1}^0 = \{w_1^5 w_2 w_1 w_1 w_2 w_2, w_1^5 w_2 w_1 w_2 w_2 w_2\},$$

and

$$U_{i+1}^1 = \{w_1^5 w_2 w_2 w_1 w_2 w_2, w_1^5 w_2 w_2 w_2 w_2 w_2\}.$$

We set $W_{i+1}^s = U_{i+1}^{s_{i+1}}$. Note that W_{i+1}^s contains two mutually unbordered words of the same length, so that we may continue constructing such sets by induction.

We define X_s as the subshift generated by the words in the sets $(W_i^s)_i$. Now, suppose $(s_1, s_2, \ldots) \neq (t_1, t_2 \ldots)$, and let j be the minimal coordinate such that $s_{j+1} \neq t_{j+1}$; suppose $s_{j+1} = 0$ and $t_{j+1} = 1$. Then $W_j^s = W_j^t = \{w_1, w_2\}$ with $|w_1| = |w_2| = k_j$, but

$$W_{j+1}^s = \{w_1^5 w_2 w_1 w_1 w_2 w_2, w_1^5 w_2 w_1 w_2 w_2 w_2\},$$

and

$$W_{i+1}^t = \{w_1^5 w_2 w_2 w_1 w_2 w_2, w_1^5 w_2 w_2 w_2 w_2 w_2\}.$$

It follows that (no matter how the inductive word building process continues), the words w_1^5 and w_2^2 occur in both X_s and X_t, and w_2^2 is reachable from w_1^5 by σ^{5k_j} in X_t, but not in X_s. However, the local rule of σ^{5k_j} can be specified the same way for both subshifts, so their prediction problems are distinct.

The subshift X_s is minimal for any sequence $s \in 2^{\mathbb{N}}$: By definition, a word v that occurs in X_s is a subword of one of the two words in W_i^s. Then, v is a subword of both words in W_{i+1}^s, and every point in X_s is an infinite concatenation of words in W_{i+1}^s. Thus, the map $s \mapsto X_s$ is an injection from the uncountable set $2^{\mathbb{N}}$ to the set of prediction problems for minimal subshifts. Since there are only countably many Turing machines, uncountable many of these prediction problems are undecidable. ■

Note that Proposition 3.1.3 does not give an example of a minimal subshift with a single unpredictable CA, although I do not believe finding such an example would be very hard.

A more interesting question is what can happen for Π_1^0 subshifts in general. I'm not aware of minimal subshifts supporting CA which are not very closely related to shift maps (for example, I do not know minimal subshifts supporting automorphisms which are not roots of shift maps). The examples in Section 3.2, and the examples I know of in the literature, have endomorphism monoids that 'virtually' consist of shift maps only, in the sense that the endomorphism monoid is a group, and the subgroup of shift maps has finite index in it. The example given in Section 3.3 has a self-similar structure, and the endomorphism monoid consists of the shift maps on each level of the self-similar structure. In such cases, Lemma 3.1.2 or a modification thereof shows the predictability of the endomorphism monoid. However, for all I know, there could be minimal subshifts supporting much more complicated endomorphisms.

Question 3.1.4 *Does there exist a minimal Π_1^0 subshift whose endomorphism monoid is unpredictable?*

It is well-known that a minimal subshift need not have zero entropy in general. Some constructions can be found in [Gri73, Bru01, HK67, Kůr03, Wil84].

Proposition 3.1.5 *There exists a minimal subshift with positive entropy.*

This raises the natural question of whether the endomorphism monoid needs to be sparse. We conjecture that it need not.

Conjecture 3.1.6 *There exists a minimal subshift whose endomorphism monoid is not sparse.*

In Section 3.2 and Section 3.3, we concentrate on accessible and natural classes of minimal subshifts: those defined by letter-to-word substitutions, and those defined by Toeplitz substitutions.

For letter-to-word substitutions with the additional properties of primitivity and balance (in particular uniformness or the Pisot property), we obtain that all cellular automata on the associated subshift are rather trivial, and in particular we show that the endomorphism monoid is finitely generated and predictable. Special cases of our results have been proved at least in [Cov71, HP89, Oll13, dJRS80, Son14] (with stronger assumptions and stronger conclusions). For Toeplitz substitutions, we do not aim at a characterization, but simply show by (natural) example that the automorphism group need not be finitely generated.

3.2 CA on Subshifts Generated by Substitutions

In this section, we show that subshifts X associated with primitive balanced substitutions – in particular Pisot substitutions – have a very simple endomorphism monoid. It satisfies our three criteria of simplicity, and more: it is a group, and virtually $\mathbb{Z}$, in the sense that the shift maps form a subgroup which has finite index in $\mathrm{Aut}(X)$.

This section is mostly based on [ST13a].

Definition 3.2.1 *A* substitution *is a function* $\tau : S \to S^+$.

While we take this as the definition, the term "substitution" implies a more robust domain for the function, in the following sense: A substitution $\tau : S \to S^+$ can also be applied to words $w \in S^*$, by (uniquely) extending it to a monoid homomorphism (in the monoid of words with respect to concatenation) by $\tau(uv) = \tau(u)\tau(v)$. We can also apply τ to points $x \in S^{\mathbb{N}}$ by $\tau(x) = \tau(x_0)\tau(x_1)\tau(x_2)\cdots$.

The *associated matrix* of a substitution τ is the $|S| \times |S|$ matrix M^τ defined by $M^\tau_{a,b} = |\tau(b)|_a$. If $\vec{v}$ is a column vector containing the number of occurrences of each letter in a word w, then $M^\tau \cdot \vec{v}$ is the corresponding column vector for $\tau(w)$.

A substitution τ is called

- *uniform* if $|\tau(a)| = |\tau(b)|$ for all $a, b \in S$,
- *injective* if $\tau(a) \neq \tau(b)$ for all $a \neq b \in S$,
- *primitive* if $a \sqsubset \tau^n(b)$ for all $a, b \in S$ and large enough $n \in \mathbb{N}$,
- *Pisot*, if the eigenvalues of its associated matrix are $\lambda_1, \ldots, \lambda_k$, where $|\lambda_1| > 1$ and $|\lambda_i| < 1$ for all $i > 1$.

To a primitive substitution $\tau : S \to S^+$ such that $\tau^n(a)_1 = a$ for some $a \in S$, $n \in \mathbb{N}$, we assign the subshift

$$X_\tau = \overline{\mathcal{O}(\lim_{k\to\infty} \tau^{kn}(a))} \subset S^{\mathbb{N}},$$

and its two-way extension $X_\tau^{\leftrightarrow} \subset S^{\mathbb{Z}}$. We say that τ *generates* the subshifts X_τ and $X_\tau^{\leftrightarrow}$. It is well-known that X_τ is independent of the choices of n and a, and it is minimal. In this section, we study the endomorphism monoids of such subshifts, when τ satisfies some technical conditions. A substitution τ is called *aperiodic* if X_τ does not contain a periodic point.

A primitive substitution has good recurrence properties. It is easy to see that if τ is a primitive substitutions, then X_τ is indeed minimal, that is, uniformly recurrent. Namely, if $w \sqsubset X_\tau$, then $w \sqsubset \tau^n(a)$ for some $a \in S$ and $n \in \mathbb{N}$. Since τ is primitive, $\tau^{n+k}(b)$ then contains w for all $b \in S$. Every point in X_τ is a concatenation of these words. By a more quantitative analysis, one can show that the recurrence is even linear:

Definition 3.2.2 *A subshift $X \subset S^{\mathbb{Z}}$ is* linearly recurrent *if there exists C such that for all $w \sqsubset X$ we have $w \sqsubset u$ whenever $u \sqsubset X$ and $|u| \geq C|w|$.*

Lemma 3.2.3 ([DHS99]) *Let τ be a primitive substitution on S. Then X_τ is linearly recurrent.*

In fact, [DHS99] exactly characterizes linearly recurrent subshifts in terms of substitutions. An important result for primitive substitutions is Theorem 2.4 of [Mos92], which we give as a lemma below. This follows as a corollary from Lemma 3.2.3, although the direct proof in [Mos92] is also clear.

Lemma 3.2.4 ([Mos92]) *Let τ be a primitive aperiodic substitution on S. Then there exists $N \in \mathbb{N}$ such that $w^N \not\sqsubset X_\tau$ for all $w \in S^+$.*

In the case of the previous lemma, we say *X_τ has bounded powers*.

A disjoint, but equally interesting notion is *unique ergodicity*, which states that in every point, every word appears with the same asymptotic frequency.

Lemma 3.2.5 ([Mic76], [Que87]) *Let τ be a primitive substitution on S. Then X_τ is uniquely ergodic.*

For linearly recurrent subshifts, we have a useful result from [Dur00].

Lemma 3.2.6 *Every endomorphism of a linearly recurrent subshift is an automorphism.*

Proof. This is Corollary 18 in [Dur00] – the corollary only talks about surjective maps, but since a linearly recurrent subshift is minimal, every endomorphism is of course surjective. ■

In particular, all endomorphisms of subshifts generated by primitive substitutions are automorphisms. Subshifts whose endomorphisms are injective are called *coalescent* in the literature. Examples of minimal subshifts supporting surjective and non-injective cellular automata are known [Dow97].

Our main results, Theorem 3.2.50 and Theorem 3.2.51 state that if τ is primitive and has the balance property (see Definition 3.2.31) – in particular if it is Pisot or uniform – then the endomorphism monoid is roughly as simple as one could hope (although it need not consist of the shift maps only): it is sparse, finitely generated and predictable.

Endomorphism monoids (rather, automorphism groups) of minimal subshifts have been studied to some extent in the literature, although most references have concentrated more on structural aspects of the subshifts.[3] Perhaps the first result explicitly about this problem was proved in [Cov71], where it was shown that all primitive uniform binary (having alphabet $S = \{0, 1\}$) substitutions generated a subshift with only shift maps as endomorphisms, unless 0 and 1 are in symmetric roles in the substitution, in which case also the bit flip $b \mapsto 1 - b$ is an endomorphism. In [HP89], this was generalized to all uniform primitive substitutions, and a result analogous to ours was obtained about the larger class of all measurable, almost everywhere shift-commuting maps. In [Oll13], it was proved for a general class of Sturmian systems (including for example the subshift generated by the Fibonacci substitution), that the endomorphism monoid consists of the shift maps only.

Further such examples follow from the fact that a system with minimal self-joinings cannot have automorphisms other than shift maps;[4] minimal self-joinings have been proved for many substitutions in the literature, although the automorphism group is usually not mentioned. We skip the formal definition of minimal self-joinings, and details of the proof, to avoid a detour in measure theory. We only give the following description [Son14]:

[3] Moreover, in the study of substitutions, it is not uncommon for authors to restrict to particular examples instead of considering large classes of substitutions.

[4] Thanks to Tom Meyerovitch for telling me this.

By a *(two-fold) self-joining* of a $\mathbb{Z}$-dynamical system (X, T) with a fixed ergodic measure μ, we mean a measure on $X \times X$ invariant under $T \times T$ whose left and right marginals are both μ. We say X has minimal self-joinings if the only self-joinings are images of μ in the maps $x \mapsto (x, T^n(x))$ where $n \in \mathbb{Z}$.

Lemma 3.2.7 *If (X, T) is uniquely ergodic, and has minimal self-joinings, then X has no automorphisms other than the shift maps.*

Proof sketch. Suppose $f : X \to X$ is an automorphism. Since X is uniquely ergodic, there is a unique shift-invariant measure μ, which is ergodic. Define $f\mu$ by $f\mu(S) = \mu(f^{-1}(S))$. A direct computation shows that this is an shift-invariant measure on X, and thus $f\mu = \mu$. It follows that f is a measure-theoretic isomorphism (because the previous argument also applies to f^{-1}). Now, the image of μ in the map $x \mapsto (x, f(x))$ is clearly a self-joining, hence it is the image of μ by a map $x \mapsto (x, \sigma^m(x))$ for some $m \in \mathbb{Z}$. This is a contradiction, as these measures are separated by the set $\{(x, \sigma^m(x)) \mid x \in X\}$. ■

Combining this with Lemma 3.2.3, Lemma 3.2.6 and Lemma 3.2.5, we see that if the subshift generated by a primitive substitution has minimal self-joinings, then its endomorphism monoid consists of the shift maps. In [Son14], it is shown that the substitution $0 \mapsto 001, 1 \mapsto 11001$ and the substitution $0 \mapsto 001, 1 \mapsto 11100$ have minimal self-joinings, and thus only shift maps in the endomorphism monoid. Note that these substitutions, although primitive, are not uniform or Pisot (and thus not even balanced by Lemma 3.2.35). It is also known that the famous Chacon substitution $0 \mapsto 0010, 1 \mapsto 1$ has minimal self-joinings [dJRS80], and thus its automorphism group consists of only the shift maps.

The proof of our main theorem is based on the following simple analytical lemma.

Lemma 3.2.8 *There exists a function $\alpha : [0, 1) \times \mathbb{R} \to \mathbb{R}$ such that for any sequence of real numbers $(x_i)_{i \in \mathbb{N}}$ such that $x_{i+1} \leq ax_i + b$ for all i, we have $x_i \leq \alpha(a, b)$ for large enough i. Furthermore, $x \leq \alpha(a, b) \implies ax + b \leq \alpha(a, b)$.*

Proof. It is enough to prove the claim for a fixed pair $a \in [0, 1)$ and $b \in \mathbb{R}$, and it is enough to consider the sequences where $x_0 = c$ and $x_{i+1} = ax_i + b$ for $i > 0$, for arbitrarily large $c \in \mathbb{R}$. Let $(x_i)_i$ be such a sequence. Since the map $x \mapsto ax + b$ is contracting, it has a unique fixed point $\beta(a, b)$, and $x_i \longrightarrow \beta(a, b)$ (see for example Theorem 2.2 in [KS01]). We can now take $\alpha(a, b) = \beta(a, b) + \epsilon$ for any $\epsilon > 0$. ■

3.2.1 Recognizability

We discuss the important notions of unilateral and bilateral recognizability. Recognizability refers to the ability to deduce the structure of the fixed point of a substitution and to 'desubstitute' it with a local rule. Slightly more precisely (we give a formal definition later), if $\tau(x) = x$, then x has the natural decomposition

$$x = \tau(x_0)\tau(x_1)\tau(x_2)\dots$$

Now, given the word $x_{[i,j+R]}$ or $x_{[i-R,j+R]}$, we obviously cannot determine the values of i and j, since x is recurrent. Thus, we ask the next best thing, namely how $x_{[i,j]}$ splits into τ-images of symbols of Σ in the decomposition above. If we can do this given $x_{[i,j+R]}$ (but without knowing i and j), then we say the substitution is unilaterally recognizable. If we can do this given $x_{[i-R,j+R]}$, then it is called bilaterally recognizable. We make the idea of desubstitution concrete in Section 3.2.4, where desubstitution rules are used as actual inverse maps to substitutions, making them bijective on orbits.

The present notion of unilateral recognizability was first defined in [Hos86], and bilateral recognizability was defined in [Mos92]. In [Hos86], this was used as a simplifying assumption, and results about the eigenvalues of the matrix associated with such a substitution were proved. The fact that all primitive substitutions are bilaterally recognizable was first proved in [Mos92]. In [Mar73], a predecessor of these notions was considered. Namely, a stronger decoding property was shown to hold for primitive substitutions on two letters, and claimed to hold with a similar proof for a larger alphabet. Unfortunately, no one seems to be convinced of the proof even in the binary case; at least [Hos86, Mos92, DHS99] state that the proof is not convincing, although I am not aware of counterexamples.

The following definitions of recognizability are direct generalizations of the ones from [Mos92] and [Mos96] (although the term 'strictly recognizable' is nonstandard), where the accepted version of the result and proof is given.

Let τ be a substitution on S with aperiodic fixed point $x \in S^{\mathbb{N}}$ in which all elements of S occur. We denote $E(0) = 0$ and $E(p) = |\tau(x_{[0,p-1]})|$ for $p > 0$, and $E_1 = \{E(p) \mid p \geq 0\}$. If

$$w = x_{[i,i+|w|-1]} = x_{[j,j+|w|-1]},$$

then we say w *has the same* 1*-cutting* at i and j if

$$E_1 \cap [i, i + |w| - 1] + (j - i) = E_1 \cap [j, j + |w| - 1].$$

We say that w *comes from* the word v at i if $v = x_{[p,q-1]}$ for the unique p and q such that $i \in [E(p), E(p+1) - 1]$ and $i + |w| - 1 \in [E(q-1), E(q) - 1]$. We say that τ is *bilaterally recognizable* (or simply *recognizable*) if there exists

$L \in \mathbb{N}$ such that if $x_{[i-L,j+L]} = x_{[i'-L,j'+L]}$, then $x_{[i,j]} (= x_{[i',j']})$ has the same 1-cutting at i and i'. If in addition $x_{[i,j]}$ comes from the same word at i and i', we say τ is *strictly recognizable*.

One of the main results of [Mos96] is that strict recognizability is in fact implied by primitivity.

Lemma 3.2.9 (Theorem 2 of [Mos96]) *Every primitive aperiodic substitution is strictly recognizable.*

Lemma 3.2.10 *Let τ have a one-sided fixed point $x \in X_\tau$, and let $x' \in X_\tau^{\leftrightarrow}$ be such that $x'_i = x_i$ for all $i \geq 0$. Then τ is recognizable if and only if there exists a block map $R^\circ = R^\circ_\tau : X_\tau^{\leftrightarrow} \to \{0,1\}^{\mathbb{Z}}$ such that for large enough $i \in \mathbb{N}$, $R^\circ(x')_i = 1$ if and only if $i \in E_1$. It is strictly recognizable if and only if there exists a block map $R = R_\tau : X_\tau^{\leftrightarrow} \to (\{\#\} \cup S)^{\mathbb{Z}}$ such that for large enough $i \in \mathbb{N}$, $R(x')_i \neq \#$ if and only if $i \in E_1$, and then x_i comes from the letter $R(x')_i$ at i.*

Proof. Suppose τ is recognizable, let $L \in \mathbb{N}$ be as in the definition of recognizability, and set L as the radius of R°. Then for all $w \sqsubset x$ with $|w| = 2L+1$, either $i \in E_1$ whenever $w = x_{[i-L,i+L]}$, or $i \notin E_1$ for all such i. In the first case, the local rule of R° outputs 1 on input w, and in the second, 0. If τ is also strictly recognizable with the same L, then x_i always comes from the same letter $a \in S$ at i when $w = x_{[i-L,i+L]}$. If the local rule of R° outputs 0 on input w, then R outputs $\#$; otherwise, it outputs the above a.

Conversely, if r is the radius of R° (R, respectively), then one can take $r + \max\{|\tau(a)| \mid a \in S\}$ as L in the definition of recognizability (strict recognizability, respectively). ■

If the map R° (R, respectively) in the previous lemma can be taken to have one-sided radius, then τ is said to be (strictly) *unilaterally recognizable*.

3.2.2 The Special Case of Uniform Primitive Substitutions

As the special case of endomorphisms of the subshift generated by an injective uniform primitive substitution is easy to establish, we begin with a relatively self-contained treatment of it. As the proof of Lemma 3.2.9 is quite complicated, we give a simpler proof of this in the injective uniform case in Lemma 3.2.12. This section is mainly pedagogical, and its aim is to explain our proof technique: the main result of this section, Proposition 3.2.14, follows both from the results of [HP89], and those of Section 3.2.5, which generalize it in different directions.

For the rest of this section, fix an alphabet S, an injective primitive uniform aperiodic substitution τ on S, so that $|\tau(a)| = m$ and $\tau(a) \neq \tau(b)$ for all $a, b \in S$, and suppose τ has a fixed point $x \in X_\tau$. Only primitivity and

uniformness are essential for our proof technique, and injectivity simplifies our proof. Ensuring the existence of a fixed point on the other hand is a matter of taking a power of τ.

For example, the *Thue-Morse substitution* $\tau(a) = ab, \tau(b) = ba$ satisfies the assumptions.

In the following, an h mod m-factor of a word u is another word v such that $v = u_{[i,i+|v|-1]}$ for some i with $i \equiv h \bmod m$.

Lemma 3.2.11 *Suppose that for all $h \in [1, m-1]$, there exists $w_h \in S^+$ which is a 0 mod m-factor, but not an h mod m-factor, of the fixed point x of τ. Then τ is recognizable.*

Proof. Let w be a prefix of the fixed-point x such that each w_h appears in w as a 0 mod m-factor. Then w can only appear as a 0 mod m-factor in x: if $x_{[j,j+|w|-1]} = w$ and $j \equiv h \bmod m$, then w_h would be an h mod m-factor in x. Since w appears with bounded gaps, recognizability follows easily. ■

We restate, and prove, Lemma 3.2.9 for the injective uniform case, as this is substantially easier than the general primitive case. See [Mos96] for a proof in the case where τ is not necessarily uniform.

Lemma 3.2.12 *The substitution τ is recognizable.*

Proof. Suppose on the contrary that τ is not recognizable, so that Lemma 3.2.11 gives an $h \in [1, m-1]$ such that every 0 mod m-factor of x is also an h mod m-factor. Let $w^{(0)} \in \mathcal{F}(x)$ with $|w^{(0)}| = 2$ be arbitrary. For all $i \geq 1$, define $w^{(i)} = \tau(w^{(i-1)})$. Denote by $N_i \subset [0, m^i - 1]$ the set of coordinates n such that $w^{(i)}_{[n,n+m^i-1]} = \tau^i(a)$ for some $a \in S$.

We now claim that $|N_i| \geq i + 1$. For $i = 0$, this is clear, so suppose that $i \geq 1$, so that by the induction hypothesis we have $|N_{i-1}| \geq i$. By the definition of τ, for each $n \in N_{i-1}$, we have $(w^{(i)})_{[mn,mn+m^i-1]} = \tau^i(a)$ for some $a \in S$, hence $mn \in N_i$. Since $w^{(i)}$ is the τ-image of a factor of x, it is a 0 mod m-factor of x. But then it is also an h mod m-factor, and since $|w^{(i)}| = 2m^i$, some $\tau^i(a)$ is a $(-h)$ mod m-factor of $w^{(i)}$. Namely, $w^{(i)}$ occurs in an h mod m coordinate of x, and some $\tau^i(a)$ in the natural decomposition of x overlaps this occurrence in a 0 mod m coordinate of x, which is then a $(-h)$ mod m-coordinate of $w^{(i)}$. Thus $km - h \in N_i$ for some $k \geq 1$, and since it is not divisible by m, it is not one of the factors introduced previously, so $|N_i| \geq i + 1$.

Let now $K \geq 2$ be arbitrary. We will show that $u^K \sqsubset x$ for some $u \in S^+$, contradicting Lemma 3.2.4 and finishing the proof. Let $i = (K+1)|S| - 1$, and consider the word $w^{(i)}$. Denote

$$I_a = \{n \in [0, m^i - 1] \mid w^{(i)}_{[n,n+m^i-1]} = \tau^i(a)\}$$

for each $a \in S$, so that $N_i = \bigcup_{a \in S} I_a$. By the above, we have $|\bigcup_a I_a| \geq (K+1)|S|$, implying that $|I_a| \geq K+1$ for some $a \in S$. Then there exist $n_1, n_2 \in I_a$ with $0 < k = |n_1 - n_2| \leq \frac{m^i}{K}$. But then $\tau^i(a)_{[0,m^i-k-1]} = \tau^i(a)_{[k,m^i-1]}$, from which it easily follows that $\tau^i(a)$ is periodic with period k, and then $\tau^i(a)^K_{[0,k-1]} \sqsubset x$, which is the desired contradiction. ■

In fact, combining the previous result with our proof of Lemma 3.2.11 shows something slightly stronger: that τ is 'recognizable from the right', in the sense that we only need to look at $w_{[i,i+M]}$, and not $w_{[i-M,i+M]}$, to determine whether the coordinate i is in E_1. This property is not shared by primitive substitutions in general.

Since τ is injective, recognizability of course means that it is also strictly recognizable[5]. Let $R : X_\tau^\leftrightarrow \to \mathcal{O}(^\infty(S\#^{m-1}))^\infty)$ be as in Lemma 3.2.10. To access the image of R, we define the map $\pi_m : (S \cup \{\#\})^\mathbb{Z} \to (S \cup \{\#\})^\mathbb{Z}$ by $\pi_m(x)_j = x_{jm}$. Using recognizability, it is easy to see that $X_\tau^\leftrightarrow$ is a disjoint union $\bigcup_{0 \leq p < m} X^p$ where $X^0 = \tau(X_\tau^\leftrightarrow)$ and $X^p = \sigma^p(X^0)$ for all $p \neq 0$. The $p \in [0, m-1]$ such that $y \in X^p$ is called the *period class* of y.

In the following proof, it is convenient to apply cellular automata to words, according to Definition 1.3.10.

Lemma 3.2.13 *Let $f : X_\tau^\leftrightarrow \to X_\tau^\leftrightarrow$ be a block map. Then $f(X^0) \subset X^p$ for some $p \in [0, m-1]$.*

Proof. By composing f with a shift, we may assume it has neighborhood $[0, r]$ for some $r \in \mathbb{N}$. Let $y, y' \in X^0$, and let $w \sqsubset X_\tau^\leftrightarrow$ be long enough that $|R(f(w))| \geq m$ (and thus also $|R(w)| \geq m$). We have $y_{[i,i+|w|-1]} = w = y'_{[j,j+|w|-1]}$ for some $i, j \in \mathbb{Z}$ by uniform recurrence of $X_\tau^\leftrightarrow$. By the structure of x, it is easy to see that $R(X_\tau^\leftrightarrow) \subset \mathcal{B}^{-1}((S\#^{m-1})^*)$. Thus, since $|R(w)| \geq m$, the word $R(w)$ must contain a letter different from $\#$, and we then have $j - i \equiv 0 \mod m$. Because the neighborhood of f is $[0, r]$, we have $f(y)_{[i,i+|f(w)|-1]} = f(w) = f(y')_{[j,j+|f(w)|-1]}$, and since $|R(f(w))| \geq m$, $R(f(w))$ again contains a letter other than $\#$, so $f(y)$ and $f(y')$ must have the same period class. ■

We can now prove the main result of this section, the following special case of Theorem 3.2.45.

Proposition 3.2.14 *There exists a finite set P of block maps on $X_\tau^\leftrightarrow$ such that if $f : X_\tau^\leftrightarrow \to X_\tau^\leftrightarrow$ is a block map, then $f = \sigma^k \circ f'$ for some $k \in \mathbb{Z}$ and $f' \in P$.*

Proof. Let $p \in [0, m-1]$ be such that $\sigma^p(f(X^0)) \subset X^0$, and define $f_0 = \sigma^p \circ f$. Now, suppose the block map $f_i : X_\tau^\leftrightarrow \to X_\tau^\leftrightarrow$ is defined and

[5] A simple proof of this implication in the non-injective case is given in [Mos96].

$f_i(X^0) \subset X^0$. We will 'conjugate' f_i by τ to obtain f_{i+1} with a (hopefully) smaller radius: For $y \in X^0$, let

$$f'_{i+1} = C_\tau(f_i) = \pi_m \circ R \circ f_i \circ \tau.$$

By the assumptions on R and f_i, the function f'_{i+1} is shift-commuting and continuous, hence a block map on $X_\tau^\leftrightarrow$. We again let $f_{i+1} = \sigma^q \circ f'_{i+1}$ for some q such that $f_{i+1}(X^0) \subset X^0$.

We show that there exists some number $N \in \mathbb{N}$ depending on τ such that if $g : X_\tau^\leftrightarrow \to X_\tau^\leftrightarrow$ satisfies $g(X^0) \subset X^0$ and has radius $r > N$, then $C_\tau(g)$ has radius $r' < r$: Let r_R be the radius of R. Then, to determine $C_\tau(g)(x)_i$, by the definition of π_m it is enough to determine the word $R(g(\tau(x)))_{[im,im+m-1]}$. To determine this, by the definition of R and g, it is enough to determine $\tau(x)_{[im-r-r_R,im+m-1+r+r_R]}$. To determine this, by the definition of τ, it is enough to know the word $x_{[i-s,i+s]}$ where $s = \left\lceil \frac{r+r_R}{m} \right\rceil$. The claim then follows by Lemma 3.2.8.

We may assume without loss of generality that if $r \leq N$, then $r' \leq N-m$, by increasing N if needed. We let P be the set of radius-N block maps on $X_\tau^\leftrightarrow$. In the process of repeated conjugation, the radii of f_i will decrease until they reach the size N, and thus $f_i \in P$ for some $i > 0$.

We define the equivalence relation $\sim$ on block maps on $X_\tau^\leftrightarrow$ by $g \sim g' \iff g = \sigma^n \circ g'$ for some $n \in \mathbb{Z}$, and note that $f_{i+1} \sim C_\tau(f_i)$ holds for all $i \in \mathbb{N}$. Now, for all block maps $g : X_\tau^\leftrightarrow \to X_\tau^\leftrightarrow$, define the map $C_\tau^{-1}(g) = \tau \circ g \circ \pi_m \circ R$ from X^0 to itself, and extend it to all of $X_\tau^\leftrightarrow$ in the natural way to obtain a shift-commuting map.

We extend C_τ to the whole class of endomorphisms by $C_\tau(g) = C_\tau(\sigma^p \circ g)$ where $0 \leq p$ is minimal such that $\sigma^p(g(X^0)) \subset X^0$. It is then easy to see that both C_τ and C_τ^{-1} are well-defined on σ-classes of endomorphisms. Clearly, if $g(X^0) \subset X^0$, we have

$$C_\tau^{-1}(C_\tau(g)) = \tau \circ \pi_m \circ R \circ g \circ \tau \circ \pi_m \circ R = g$$

on X^0, since $\tau \circ \pi_m \circ R = \mathrm{id}_{X^0}$, and otherwise at least $C_\tau^{-1}(C_\tau(g)) \sim g$. Similarly, we always have have

$$C_\tau(C_\tau^{-1}(g)) = \pi_m \circ R \circ \tau \circ g \circ \pi_m \circ R \circ \tau = g,$$

since $\pi_m \circ R \circ \tau = \mathrm{id}_{X_\tau^\leftrightarrow}$.

Thus, up to $\sim$-equivalence, conjugation by τ is actually an action of the group $\mathbb{Z}$ on the set of block maps on X. If $f : X_\tau^\leftrightarrow \to X_\tau^\leftrightarrow$ is a block map, then $f_i = f_{i+n} \in P$ for some $i, n > 0$ in the process of repeated conjugation, and then $f \sim f_{i+\ell} \in P$ where $i + \ell \equiv 0 \bmod n$. ■

We show that this result is optimal in the sense that one can construct arbitrarily many nonequivalent block maps with arbitrarily large radii on the

subshift of a primitive uniform substitution. Contrast this with the result of [Cov71], stating that the endomorphisms of subshifts of binary uniform substitutions are symbol maps.[6]

Example 3.2.15 *Let $m \in \mathbb{N}$ and $n \geq 4$, and consider the substitution τ on the alphabet $S = \{a_i, b_i \mid 0 \leq i < m\}$ defined by $\tau(a_i) = b_{i+1}a_i^{n-1}$ and $\tau(b_i) = b_i a_i^{n-1}$, where the indices are taken modulo m. This is a uniform primitive substitution whose subshift has the symbol map $f(a_i) = a_{i+1}$, $f(b_i) = b_{i+1}$ and its powers as endomorphisms. We perform a state-splitting on the letter a_0, obtaining the substitution $\hat{\tau}$ on the alphabet $\hat{S} = S \cup \{c\}$ defined as*

$$\begin{aligned}
\hat{\tau}(a_i) &= \tau(a_i) \text{ for } 0 \leq i < m, \\
\hat{\tau}(c) &= \tau(a_0), \\
\hat{\tau}(b_0) &= b_0 c^{n-1}, \\
\hat{\tau}(b_i) &= \tau(b_i) \text{ for } 0 < i < m.
\end{aligned}$$

The letters c and a_0 of $\hat{\tau}$ together represent the letter a_0 of τ, with the extra information of whether its preimage is a_0 or b_0. The subshift $X_\tau^\leftrightarrow$ is isomorphic to the two-sided subshift $X_{\hat{\tau}}^\leftrightarrow$ via an obvious isomorphism $\phi : X_\tau^\leftrightarrow \to X_{\hat{\tau}}^\leftrightarrow$ (induced by the state-splitting) with neighborhood $[-n+1, 0]$, such that ϕ^{-1} has neighborhood $\{0\}$. In particular, f induces an endomorphism $\hat{f} = \phi \circ f \circ \phi^{-1}$ on $X_{\hat{\tau}}^\leftrightarrow$.

We claim that the endomorphism $\hat{f}$ cannot be defined by a contiguous neighborhood $[d, d+n-2] \subset \mathbb{Z}$. First, if $d \geq n$ or $d + n - 2 < 0$, then $f = \phi^{-1} \circ \hat{f} \circ \phi$ (and thus the identity morphism) can be defined by a contiguous neighborhood not containing 0. Since $X_\tau^\leftrightarrow$ is not a periodic subshift, this is a contradiction. Thus we may assume $d < n$ and $d > -n + 1$.

Let then $x \in \phi(X_{\hat{\tau}}^\leftrightarrow)$ be such that $x_{[0,3]} = b_{m-1}a_{m-1}a_{m-1}a_{m-1}$, and denote $y = \sigma(x)$. Then

$$\begin{aligned}
\hat{\tau}(x)_{[0,3n-1]} &= b_{m-1}a_{m-1}^{n-1}b_0a_{m-1}^{n-1}b_0a_{m-1}^{n-1}, \\
\hat{\tau}(y)_{[0,3n-1]} &= b_0 \quad a_{m-1}^{n-1}b_0a_{m-1}^{n-1}b_0a_{m-1}^{n-1}.
\end{aligned}$$

Due to $d > -n + 1$, the local rule of $\hat{f}$, applied at coordinate $n-1$, cannot see the coordinate 0. Thus, $\hat{f}(\hat{\tau}(x))_{n-1} = \hat{f}(\hat{\tau}(y))_{n-1}$. However, we should have $\hat{f}(\hat{\tau}(x))_{n-1} = a_0$ and $\hat{f}(\hat{\tau}(y))_{n-1} = c$, a contradiction.

An analogous argument can be applied to all powers of $\hat{f}$, except the identity map. All in all, the subshift $\phi(X_\tau^\leftrightarrow)$ has at least $m-1$ endomorphisms that are pairwise distinct even modulo powers of the shift, and cannot be defined by contiguous neighborhoods of size less than $n-1$.

[6] Thanks to Timo Jolivet for the idea of using state-splitting to find such an example.

3.2.3 Orbit-preserving Maps and Dill Maps

The proofs of our main results are based on the study of a larger class of maps than just cellular automata: the orbit-preserving maps, that is, continuous functions that map orbits to orbits. There is extensive literature on orbit-equivalence of Cantor dynamical systems, that is, the existence of orbit-preserving homeomorphisms; see for example [GPS95, BT98, GPS09]. Our perspective is a bit different, as we do not compare different subshifts, but instead try to understand the endomorphism monoids of individual subshifts.

Unlike in Section 3.2.2, it is now more convenient to consider one-way subshifts $X \subset S^{\mathbb{N}}$, as this makes indexing slightly less taxing. We note that when studying block maps from one-way subshifts to one-way subshifts, we are simultaneously studying the block maps between the corresponding two-way subshifts, as if $f : X \to Y$ is a block map between two-way subshifts, then for large enough r, we have

$$x_{[0,\infty)} = x'_{[0,\infty)} \implies f(x)_{[r,\infty)} = f(x')_{[r,\infty)},$$

so that $\sigma^r \circ f$ is well-defined between right tails of points.

Definition 3.2.16 *Let $X, Y \subset S^{\mathbb{N}}$ be subshifts, and let $f : X \to Y$ be a function. If $s : X \to \mathbb{N}$ satisfies*

$$f(\sigma(x)) = \sigma^{s(x)}(f(x))$$

for all $x \in X$, then we call s a cocycle *for f.*

Definition 3.2.17 *Let $X, Y \subset S^{\mathbb{N}}$ be subshifts. A continuous function $f : X \to Y$ is said to be* orbit-preserving *if $f(\mathcal{O}(x)) \subset \mathcal{O}(f(x))$. If f is continuous and has a continuous cocycle $s : X \to \mathbb{N}$ with the property*

$$\forall x \in X : \exists n \in \mathbb{N} : s(\sigma^n(x)) > 0, \tag{3.1}$$

then we say f is a dill[1] map*, and s is a* nice cocycle *for it.*

Clearly, a continuous map is orbit-preserving if and only if it has a cocycle, so that in particular a dill map is orbit-preserving. Note that a continuous cocycle has a finite image: since X is compact, its image in a continuous map is compact as well. Note also that if $f : X \to Y$ is a dill map, and Y contains no periodic points, then the cocycle of f is unique.

[1]The word 'dill' comes from the theory of L systems: a dill map corresponds to a DIL system, that is, a Deterministic Lindenmayer system with Interactions. We add an extra 'l' since we are interested in the action of these maps on Long (infinite) words.

Lemma 3.2.18 *Let $X, Y \subset S^{\mathbb{N}}$ be subshifts, and let $f : X \to Y$ be a block map. Then f is a dill map.*

Proof. Since $f \circ \sigma = \sigma \circ f$, $s(x) = 1$ is a nice cocycle for f. ■

Define a *substitutive map* to be a function $\tau : S \to T^+$. Just like substitutions, we also apply substitutive maps to general points, by applying the map cellwise and concatenating the results.

Lemma 3.2.19 *Let $\tau : S \to T^*$ be a substitutive map such that $|\tau(a)| > 0$ for some $a \in S$, and let $X \subset S^{\mathbb{N}}$ be a uniformly recurrent subshift with $\mathcal{B}_1(X) = S$. Then the extension $\tau : X \to \tau(X)$ is a dill map.*

Proof. Clearly, $s(x) = |\tau(x_0)|$ is a nice cocycle for f. ■

Lemma 3.2.20 *Suppose $f : X \to Y$ and $g : Y \to Z$ are dill maps. Then $g \circ f : X \to Z$ is a dill map.*

Proof. Let s_1 be a nice cocycle for f, and s_2 for g. Of course, $g \circ f$ is continuous. Now, it is easy to see that

$$g(f(\sigma(x))) = g(\sigma^{s_1(x)}(f(x))) = \sigma^{\sum_{j=0}^{s_1(x)-1} s_2(\sigma^j(f(x)))}(g(f(x))).$$

Thus, $s(x) = \sum_{j=0}^{s_1(x)-1} s_2(\sigma^j(f(x)))$ is a cocycle for $g \circ f$. It is easy to check the continuity of s, and that (3.1) holds. ■

By the three previous lemmas, the composition of a block map and a substitutive map is a dill map. Next, we show a kind of converse to this: every dill map is obtained as a composition of a block map and a substitution (although we have little control over their codomain and domain).

Lemma 3.2.21 *Let $X, Z \subset S^{\mathbb{N}}$ be subshifts, and $\Phi : X \to Z$ a dill map with nice cocycle s. Then there exists a subshift Y, a block map $f : X \to Y$ and a substitutive map $\tau : Y \to Z$ such that $\Phi = \tau \circ f$.*

Proof. Since s is nice, there exist $r, m \in \mathbb{N}$ and a function $s' : S^{r+1} \to [0, m]$ such that $s(x) = s'(x_{[0,r]})$ for all x, that is, $x_{[0,r]}$ uniquely determines the image of s on x. Similarly, since Φ is continuous, there exists r' such that $x_{[0,r']}$ determines $\Phi(x)_{[0,m]}$. Let $R = \max(r, r')$, and define $Y = (S^{R+1})^{\mathbb{N}}$, that is, Y is the full shift over the alphabet S^{R+1}. Define the block map $f : X \to Y$ by $f(x)_0 = x_{[0,R]}$, and the substitutive map $\tau : S^{R+1} \to S^*$ (where S^{R+1} is considered an alphabet) by $\tau(w) = \Phi(x)_{[0,s(x)-1]}$, when x is a point with $x_{[0,R]} = w$ (and $\tau(w)$ is arbitrary when $w \not\sqsubset \mathcal{B}(X)$). It is easy

to see that τ is well-defined and the choice of x does not matter. It is then easy to see that

$$\begin{aligned}\tau(f(x)) &= \tau(x_{[0,R]})\tau(x_{[1,R+1]})\tau(x_{[2,R+2]})\cdots \\ &= \Phi(x)_{[0,s(x)-1]}\Phi(\sigma(x))_{[0,s(\sigma(x))-1]}\Phi(\sigma^2(x))_{[0,s(\sigma^2(x))-1]}\cdots \\ &= \Phi(x).\end{aligned}$$

■

Thus, dill maps are, in some sense, the closure of substitutive maps and block maps under composition. This was also the original motivation for them, as for the proof of Proposition 3.2.14 to generalize to non-uniform substitutions, we need a class of maps which is closed under conjugation by substitutions, and contains all cellular automata. However, for the direction that all dill maps are indeed the composition of a block map and a substitutive map (as shown in Lemma 3.2.21), note that even if $\Phi : X \to X$ is a dill map, f usually can not be taken to be a CA on X, or τ a substitution on X, and we really need the extra subshift Y.

The maps f and τ given by the previous lemma are important in later sections: In Section 3.2.2, we showed that the radius of the local rule of a block map becomes small as it is conjugated by a substitution. Similarly, to prove the main theorem, we will show that when a dill map is conjugated by substitution, both components f and τ in the representation given by Lemma 3.2.21 become 'small'. To formalize this, we define an analogue of radius for dill maps. Namely, the radius pair.

Definition 3.2.22 *Let $\Phi : X \to Z$ be a dill map, and let $f : X \to Y$ and $\tau : Y \to Z$ a decomposition of Φ into a block map and a substitution. If the radius of f is r and $m = \max_{a\in S}(|\tau(a)|)$, then we say Φ has* radius pair (r, m).

Of course, a dill map can have multiple radius pairs.

Another way to state the previous lemma is that if $\Phi : X \to Y$ is a dill map between subshifts $X, Y \subset S^{\mathbb{N}}$, then there exists a continuous function called an *implementation* $\phi : X \to S^*$ such that

$$\Phi(x) = \phi(x)\phi(\sigma(x))\phi(\sigma^2(x))\cdots, \tag{3.2}$$

We usually write ${}^n\phi(x) = \phi(x)\phi(\sigma(x))\cdots\phi(\sigma^{n-1}(x))$, and (abusing notation), we then have

$$\Phi(x) = \lim_{n\to\infty} {}^n\phi(x) = {}^\infty\phi(x).$$

Such a map ϕ is of course obtained from the maps f and τ given by Lemma 3.2.21, by $\phi(x) = \tau(f(x)_0)$.

Definition 3.2.23 *A continuous function ϕ satisfying* (3.2) *is called an* implementation *of* Φ.

The radius pair of an implementation ϕ is, correspondingly, (r, m), where r is the number of coordinates (minus one) ϕ needs to look at before determining its image, and m is the maximal image size of ϕ. We write $I(\phi) = r$ and $O(\phi) = m$, and say r and m are the *in-radius* and *out-radius* of ϕ, respectively.

Finally, we can also compose two dill maps by composing their implementations:

Lemma 3.2.24 *Suppose $\Phi_1 : X \to Y$ and $\Phi_2 : Y \to Z$ are dill maps with implementations ϕ_1 and ϕ_2. Then*

$$\phi(x) = {}^{|\phi_1(x)|}\phi_2({}^{\infty}\phi_1(x)) \tag{3.3}$$

is an implementation for $\Phi_2 \circ \Phi_1$. Also,

$$({}^{n}\phi)(x) = {}^{|({}^{n}\phi_1)(x)|}\phi_2({}^{\infty}\phi_1(x)) \tag{3.4}$$

holds for all $x \in X$ and $n \in \mathbb{N}$.

Now, what we are interested in is how $I(\Phi)$ and $O(\Phi)$ behave as dill maps are composed. It turns out that little can be said about this directly, since $O(\Phi)$ does not capture enough information about the dill map. Namely, the information $O(\Phi)$ gives us is only the rough upper bound $|({}^{n}\phi)(x)| \leq O(\Phi)n$; we need much more.

Our solution is to turn $O(\Phi)$ into a pair of invariants λ and D, which together give strong analytical information about the growth of words in the dill map. For $\phi : X \to S^*$, the invariant λ is the limit of $\frac{|({}^{n}\phi)(x)|}{n}$ when this exists and is independent of $x \in X$, and thus measures the average[7] size of $\phi(x)$. The invariant D measures the maximum of the absolute differences between $|({}^{n}\phi)(x)|$ and $n \cdot \lambda(\phi)$ for $x \in X$, so that D and λ together tell us the length $|({}^{n}\phi)(x)|$ up to a constant error. The invariants λ and D of course also give an upper bound for the out-radius $O(\phi)$ when we take $n = 1$.

We now define these invariants more formally, and discuss their behavior in the composition of dill maps. These inequalities – in particular Lemma 3.2.30 – are the main technical tool in the proof of the main theorem.

While λ exists for all dill maps on uniquely ergodic subshifts, the existence of D is quite a strong assumption. However, both exist for both block maps (on any subshift) and primitive Pisot substitutions (on their associated subshifts). The claim is trivial for block maps, and it is proved for substitutions in Section 3.2.4.

[7]Rather, it measures the time average. Of course, our interest is in uniquely ergodic subshifts, so that the time average is equal to the space average by Birkhoff's Ergodic Theorem, see Lemma 3.2.26.

Definition 3.2.25 *Let $\phi : X \to S^*$. We define $\lambda(\phi) = \lambda \in \mathbb{R}$, if for all $x \in X$, we have $\lim_n \frac{|({}^n\phi)(x)|}{n} = \lambda$.*

Lemma 3.2.26 *If X is uniquely ergodic and $\phi : X \to S^*$ is a dill map, then $\lambda(\phi)$ exists.*

Proof. We have

$$\lim_n \frac{|({}^n\phi)(x)|}{n} = \lim_n \frac{\sum_{i=0}^{n-1} |\phi(\sigma^i(x))|}{n} = \int |\phi(x)| dx,$$

by unique ergodicity, since $x \mapsto |\phi(x)|$ is continuous. ■

In what follows, the notation $\lambda(\Phi)$ implies that the quantity is well-defined, unless otherwise noted. The invariant $D(\phi)$ is defined in terms of $\lambda(\phi)$ as follows:

Definition 3.2.27 *Let $\lambda(\phi) = \lambda$. We define $D(\phi)$ as the smallest $D \in \mathbb{N}$ such that for all $x \in X$ and for all $n \in \mathbb{N}$, we have $|({}^n\phi)(x)| \in [\lambda n - D, \lambda n + D]$ (when such a D exists).*

Lemma 3.2.28 *Suppose X and Y are subshifts, Y contains no periodic points, and $\Phi : X \to Y$ is a dill map such that $\lambda(\Phi)$ and $D(\Phi)$ exist. Then the first $\lambda(\Phi)^{-1}(m + D(\Phi)) + I(\Phi)$ coordinates of x determine the first m coordinates of $\Phi(x)$.*

Proof. We prove that the first n coordinates of x determine (at least) the first $\lambda(\Phi)(n - I(\Phi)) - D(\Phi)$ coordinates of $\Phi(x)$: The in-radius of ϕ can be taken to be $I(\Phi)$, so the first n coordinates determine that $\Phi(x)$ begins with ${}^{n-I(\Phi)}\phi(x)$. By the definition of $\lambda(\Phi)$ and $D(\Phi)$, the length of this word is at least $\lambda(\Phi)(n - I(\Phi)) - D(\Phi)$. The claim follows by setting $n = \lambda(\Phi)^{-1}(m + D(\Phi)) + I(\Phi)$. ■

We now do some computations about how the invariants behave in composition. To avoid clutter in the statements of the lemmas, we make the standing assumptions that X, Y and Z have no periodic points, $\Phi_1 : X \to Y$ and $\Phi_2 : Y \to Z$ are global dill maps for which the invariants in question are defined, ϕ_1 and ϕ_2 are their implementations, Φ their composition, and ϕ the implementation of Φ given by (3.3). We also denote $H_i = H(\Phi_i)$ for each invariant H.

Lemma 3.2.29 *With the standing assumptions, we have*

$$\begin{aligned}
\lambda(\Phi_2 \circ \Phi_1) &= \lambda_1 \lambda_2 \\
D(\Phi_2 \circ \Phi_1) &\leq \lambda_2 D_1 + D_2 \\
I(\Phi_2 \circ \Phi_1) &\leq \lambda_1^{-1}(2D_1 + I_2) + I_1 + 1
\end{aligned}$$

Proof. Let $x \in X$. Using (3.4), we have

$$\begin{aligned} |({}^n\phi)(x)| &= |({}^{|({}^n\phi_1)(x)|}\phi_2)(({}^\infty\phi_1)(x))| \\ &= |({}^{\lambda_1 n+k_1}\phi_2)(({}^\infty\phi_1)(x))| && k_1 \in [-D_1, D_1] \\ &= \lambda_2(\lambda_1 n + k_1) + k_2 && k_2 \in [-D_2, D_2] \end{aligned}$$

where the k_i are taken among reals. Dividing by n and taking the limit $n \longrightarrow \infty$, we see $\lambda(\Phi) = \lambda_2\lambda_1$. The claim for $D(\Phi)$ is then obvious.

As for $I(\Phi)$, we need to bound the in-radius of

$$x \mapsto \phi(x) = {}^{|\phi_1(x)|}\phi_2({}^\infty\phi_1(x)),$$

that is, we need to bound the number of coordinates of x we need to know in order to determine the word $\phi(x)$. To compute $\phi(x)$, it is enough to know the value of $|\phi_1(x)|$ and to know the first $|\phi_1(x)| + I(\Phi_2)$ coordinates of ${}^\infty\phi_1(x)$. The value $|\phi_1(x)|$ is determined by the first $I(\Phi_1)+1$ coordinates. By Lemma 3.2.28, the first $\lambda(\Phi_1)^{-1}(m + D(\Phi_1)) + I(\Phi_1)$ coordinates of x uniquely determine the first m coordinates of ${}^\infty\phi_1(x)$. Setting $m = O(\Phi_1) + I(\Phi_2)$, we thus have that the first

$$A = \lambda(\Phi_1)^{-1}(O(\Phi_1) + I(\Phi_2) + D(\Phi_1)) + I(\Phi_1)$$

coordinates of x determine at least the first $O(\Phi_1)+I(\Phi_2) \geq |\phi_1(x)|+I(\Phi_2)$ coordinates of ${}^\infty\phi_1(x)$. Since A is greater than $I(\Phi_1)$, $|\phi_1(x)|$ is also determined. Finally, $O(\Phi_1) \leq \lambda(\Phi_1) + D(\Phi_1)$ by taking $n = 1$ in the definition of $D(\Phi_1)$. Substituting this into the expression for A gives the formula in the claim. ■

In fact, we need such formulas for compositions of three dill maps. Proving these inequalities is of course a matter of applying the previous lemmas twice.

Lemma 3.2.30 *Let $X = Y = Z$, so that Φ_1 and Φ_2 are dill maps on X. Then for some function $C : \mathcal{D} \times \mathbb{R} \times \mathcal{D} \to \mathbb{R}$, where $\mathcal{D}$ is the set of dill maps on X, we have*

$$\begin{aligned} D(\Phi_3 \circ \Phi_2 \circ \Phi_1) &\leq \lambda_3\lambda_2 D_1 + \lambda_3 D_2 + D_3 \\ &\leq \lambda_3 D_2 + C(\Phi_1, \lambda_2, \Phi_3) \\ I(\Phi_3 \circ \Phi_2 \circ \Phi_1) &\leq \lambda_1^{-1}(2D_1 + \lambda_2^{-1}(2D_2 + I_3) + I_2 + 1) + I_1 + 1 \\ &\leq \lambda_1^{-1} I_2 + 2\lambda_1^{-1}\lambda_2^{-1} D_2 + C(\Phi_1, \lambda_2, \Phi_3) \end{aligned}$$

In particular, if $\lambda_1 > 1$, $\lambda_2 = 1$ and $\lambda_3 < 1$ (which will be the case in our application), the invariants D_2 and I_2 contribute to the corresponding invariant of $\Phi_3 \circ \Phi_2 \circ \Phi_1$ with a coefficient less than 1.

3.2.4 Back to Block Maps and Substitutions

We define notions of balance, almost equivalence and almost invertibility for global dill maps. A dill map is balanced if all words 'blow up' by roughly the same amount in the application of its local rule. Almost equivalence of two dill maps Φ_1 and Φ_2 means that the Φ_1-image and the Φ_2-image of each point differ only by a shift. By almost invertibility, we mean invertibility up to almost equivalence. For substitutions, we show that almost invertibility follows from primitivity, and balance from both uniformity and the Pisot property. Using these ideas, we then generalize the arguments of Section 3.2.2.

Definition 3.2.31 *A global dill map is* balanced *if the invariants λ and D are well-defined for it. We say that a substitution $\tau : S \to S^+$ is balanced if the corresponding dill map $\tau : X_\tau \to X_\tau$ is balanced.*

This notion of balance has nothing to do with the notion of balanced cellular automata on the full shift.

We note that λ exists for all primitive substitutions, and corresponds to a well-known property of the substitution.

Lemma 3.2.32 *For every primitive substitution $\tau : X_\tau \to X_\tau$, $\lambda(\tau)$ is well-defined and equal to the dominant eigenvalue of τ.*

Proof. By Lemma 3.2.5, X_τ is uniquely ergodic, so that Lemma 3.2.26 applies, and thus $\lambda(\tau)$ exists. Therefore, we only need to show that it is indeed equal to the dominant eigenvalue λ. Let M be the associated matrix of τ, where $M_{a,b} = |\tau(b)|_a$ for $a, b \in S$. For $a \in S$, define

$$\mu(a) = \lim_n \frac{|x_{[0,n-1]}|_a}{n}$$

where $x \in X_\tau$. By the proof of Proposition 5.8 in [Que87], this is well-defined for all $a \in S$, and independent of the choice of x, $\sum_a \mu(a) = 1$, and $\mu = (\mu(a))_{a \in S}$ is a right eigenvector of λ for M. Writing $|v| = \sum_a v_a$ for $v \in \mathbb{R}^S$, for any $x \in X_\tau$ and some $\lim_n \epsilon_{x,n} = 0$, we have

$$\begin{aligned} \frac{|({}^n\tau)(x)|}{n} = \frac{|\tau(x_{[0,n-1]})|}{n} &= \sum_{a \in S} |\tau(a)|(\mu(a) + \epsilon_{x,n}) \\ &\longrightarrow \sum_{a \in S} |\tau(a)|\mu(a) = |M\mu| = \lambda|\mu| = \lambda. \end{aligned}$$

■

Note that while Lemma 3.2.29 shows that Z behaves nicely in the composition of dill maps, we cannot conclude from the previous lemma that

the dominant eigenvalue behaves nicely in the composition of two primitive substitutions. This is because the well-definedness of λ for primitive substitutions comes from the subshift X_τ more than from the action of τ: We do not iterate τ in the definition of $\lambda(\tau)$, but only in the definition of X_τ, and this iteration is what connects $\lambda(\tau)$ to the dominant eigenvalue.

It is obvious that uniform substitutions are balanced as dill maps, and we next show that Pisot substitutions are also balanced.

Lemma 3.2.33 (Part of Corollary 2 in [Ada04]) *Let $x \in S^{\mathbb{N}}$ be a fixed point of a primitive Pisot substitution, and let $\mu(a) = \lim_N \frac{|x_{[0,N-1]}|_a}{N}$ for all letters $a \in S$. Then there exists $C > 0$ such that for all $a \in S$ and $N \in \mathbb{N}$, we have $||x_{[0,N-1]}|_a - N\mu(a)| < C$.*

Actually, Corollary 2 of [Ada04] completely characterizes the substitutions for which the conclusion holds, and in particular shows that they form a larger class than Pisot substitutions. However, the condition is quite involved, so we do not state it here. The balancedness of primitive Pisot substitutions is an easy corollary of this lemma.

Lemma 3.2.34 *Every primitive Pisot substitution $\tau : X_\tau \to X_\tau$ is balanced.*

Proof. By Lemma 3.2.32, $\lambda(\tau)$ is well-defined. By Lemma 3.2.33, apart from a uniformly bounded error, $x_{[0,n-1]}$ and $y_{[0,n-1]}$ contain the same number of each letter for all $x, y \in X_\tau$. It is then easy to see that for some $C \in \mathbb{R}$, we have

$$||({}^n\tau)(x)| - |({}^n\tau)(y)|| = ||\tau(x_{[0,n-1]})| - |\tau(y_{[0,n-1]})|| < C$$

for all $n \in \mathbb{N}$ and $x, y \in X_\tau$. Since the limit of $\frac{|({}^n\tau)(x)|}{n}$ is $\lambda(\tau)$, it is easy to see that for each n, there exist points x, y such that $|({}^n\tau)(x)| \leq \lambda(\tau)n \leq |({}^n\tau)(y)|$. From this, the claim follows. ■

It is well-known that no substitution is both uniform and Pisot, so that balanced dill maps are a common generalization of the two. In the binary case, the balanced substitutions are precisely the disjoint union of uniform or Pisot substitutions.

Lemma 3.2.35 *A binary substitution is balanced if and only if it is uniform or Pisot.*

Proof. We have already seen that both uniform and Pisot substitutions are balanced. Now suppose $\tau : \{0,1\} \to \{0,1\}^+$ is not uniform and not Pisot. Since τ is not Pisot, by Theorem 1 of [Ada04], there exist arbitrarily large n such that for some pair $u, v \sqsubset X_\tau$ we have $|u| = |v|$ and $||u|_0 - |v|_0| > n$. Then of course $||\tau(u)| - |\tau(v)|| > n$, since $|\tau(0)| \neq |\tau(1)|$. ■

Definition 3.2.36 *Let $\Phi, \Psi : X \to Y$ be dill maps with X uniformly recurrent. If*

$$\forall x \in X : \exists i, j \in \mathbb{N} : \sigma^i(\Phi(x)) = \sigma^j(\Psi(x)),$$

then we write $\Phi \sim \Psi$, and say Φ and Ψ are almost equivalent. *If $\Phi_1 : X \to Y$, $\Phi_2 : Y \to X$ and $\Phi_2 \circ \Phi_1 \sim id_X$, then we say Φ_2 is an* almost left inverse *of Φ_1, and it is an* almost right inverse *if $\Phi_1 \circ \Phi_2 \sim id_Y$. An almost right and almost left inverse is called an* almost inverse. *A dill map is* almost invertible *if it has an almost inverse.*

To make sure that it is safe to talk about dill maps 'up to almost equivalence', we need to check that almost equivalence is an equivalence relation, and behaves well under composition of dill maps.

Lemma 3.2.37 *Almost equivalence is an equivalence relation, that is,*

$$\Phi_1 \sim \Phi_2 \wedge \Phi_2 \sim \Phi_3 \implies \Phi_1 \sim \Phi_3.$$

Almost equivalence is a congruence with respect to composition, that is,

$$\Phi_1 \sim \Psi_1 \wedge \Phi_2 \sim \Psi_2 \implies \Phi_2 \circ \Phi_1 \sim \Psi_2 \circ \Psi_1.$$

Proof. If $\sigma^{i_1}(\Phi_1(x)) = \sigma^{j_1}(\Phi_2(x))$ and $\sigma^{i_2}(\Phi_2(x)) = \sigma^{j_2}(\Phi_3(x))$, then

$$\sigma^{i_1+i_2}(\Phi_1(x)) = \sigma^{j_1+i_2}(\Phi_2(x)) = \sigma^{j_1+j_2}(\Phi_3(x)),$$

so $(\sim)$ is an equivalence relation.

We also need to show that if $\Phi_1 \sim \Psi_1$ and $\Phi_2 \sim \Psi_2$, then $\Phi_2 \circ \Phi_1 \sim \Psi_2 \circ \Psi_1$. We have $\sigma^{j_1}(\Phi_1(x)) = \sigma^{k_1}(\Psi_1(x))$ for some j_1, k_1, and thus

$$\sigma^{j_2}(\Phi_2(\sigma^{j_1}(\Phi_1(x)))) = \sigma^{k_2}(\Psi_2(\sigma^{k_1}(\Psi_1(x))),$$

for some j_2, k_2. The claim follows by applying the cocycles of Φ_2 and Ψ_2 appropriately. ■

In fact, the reason we call these maps 'almost invertible' and not 'invertible' is only an artifact of considering one-way subshifts.[8] The two-way extensions are, in a sense, actually invertible.

Remark 3.2.38 *Let $\Phi_1 : X \to Y$ be a dill map (or a general orbit-preserving map), and let $\Phi_2 : X^{\leftrightarrow} \to Y^{\leftrightarrow}$ be its two-way extension. Then Φ_2 induces a well-defined map $\Phi_3 : X^{\leftrightarrow}/(\sim) \to Y^{\leftrightarrow}/(\sim)$, where $\sim$ is the orbit relation $x \sim y \iff y \in \mathcal{O}(x)$, by $\Phi_3([x]) = [\Phi_2(x)]$. If Φ_1 is almost invertible, then Φ_3 is* bijective.

[8] On the other hand, considering two-way subshifts leads to worse artifacts, as defining the invariants I, O, λ and D is very messy.

Next, we use the recognizability of primitive substitutions to obtain almost inverse dill maps for them.

Lemma 3.2.39 *A primitive aperiodic substitution τ on S is almost invertible as a dill map on X_τ. If τ is balanced, it has a balanced almost inverse.*

Proof. First, τ is strictly recognizable by Lemma 3.2.9, so let R be the block map given by Lemma 3.2.10, and let $r \in \mathbb{N}$ be its radius. Then the neighborhood of $\sigma^r \circ R$ contains only nonnegative elements, so $f_R = \sigma^r \circ R$ can be thought of as a block map from X_τ to $(\{\#\} \cup S)^{\mathbb{N}}$. Define $\phi : X_\tau \to S^*$ by

$$\phi(x) = \begin{cases} a, & \text{if } f_R(x)_0 = a \in S, \text{ and} \\ \epsilon, & \text{if } f_R(x)_0 = \#, \end{cases}$$

(where ϵ denotes the empty word). It is easy to see that $\tau^{-1} = {}^\infty\phi$ is a dill map, and an almost inverse of τ.

By the way we defined τ^{-1}, the composition $\tau \circ \tau^{-1}$ has an implementation $\psi : X_\tau \to S^*$ such that there exists $C \geq 0$ with $|({}^n\psi)(x)| \in [n-C, n+C]$ for all $x \in X_\tau$ and $n \in \mathbb{N}$. It is then easy to see that τ^{-1} is balanced if τ is. ■

As an example, we give an almost inverse of the Thue-Morse substitution.

Example 3.2.40 *Let τ be the Thue-Morse substitution, and let $\tau^{-1} : X_\tau \to \{0,1\}^*$ be defined by*

$$\begin{array}{ll} \tau^{-1}(00101) = \epsilon, & \tau^{-1}(00110) = \epsilon \\ \tau^{-1}(01001) = \epsilon, & \tau^{-1}(01011) = 0 \\ \tau^{-1}(01100) = 0, & \tau^{-1}(01101) = 0 \\ \tau^{-1}(10010) = 1, & \tau^{-1}(10011) = 1 \\ \tau^{-1}(10100) = 1, & \tau^{-1}(10110) = \epsilon \\ \tau^{-1}(11001) = \epsilon, & \tau^{-1}(11010) = \epsilon \end{array}$$

One can check that $({}^\infty\tau) \circ ({}^\infty\tau^{-1}) \sim id_{X_\tau} = ({}^\infty\tau^{-1}) \circ ({}^\infty\tau)$.

Next, we characterize the almost equivalence of block maps on our subshifts of interest.

Lemma 3.2.41 *If $f, g : X \to Y$ are almost equivalent block maps, where X is uniformly recurrent, then $g \circ \sigma^k = f$ or $g = f \circ \sigma^k$ for some $k \in \mathbb{N}$.*

Proof. Suppose f and g both have neighborhood $[0, r]$ for some $r \in \mathbb{N}$. If $x \in X$, then $\sigma^\ell(f(x)) = \sigma^{\ell'}(g(x))$ for some $\ell, \ell' \in \mathbb{N}$. Suppose $\ell \leq \ell'$ (the other case being symmetric). Then, using shift-commutation, we have $f(\sigma^\ell(x)) = \sigma^{\ell'-\ell}(g(\sigma^\ell(x)))$. Set $y = \sigma^\ell(x)$ and $k = \ell' - \ell$, so that $f(y) = \sigma^k(g(y))$. We show that $f = \sigma^k \circ g$. Namely, if this is not the case, then

there exists a point $z \in X$ such that $f(z)_i \neq g(z)_{i+k}$ for some $i \in \mathbb{N}$. Since X is uniformly recurrent, $w = z_{[i,i+k+r]}$ appears with bounded gaps in y, so $f(y) = \sigma^k(g(y))$ does not hold. ■

Lemma 3.2.41 does not apply in the case that $f \sim \Phi$, f is a block map and Φ a dill map: for example on the Thue-Morse shift, Φ could behave differently depending on whether the input point is of the form $\tau(x)$ or $\sigma(\tau(x))$ for some $x \in X_\tau$.

We can now generalize the conjugation argument of Proposition 3.2.14 to balanced primitive substitutions.

Example 3.2.42 *We continue Example 3.2.40. The endomorphisms of the Thue-Morse subshift are characterized in [Cov71], and they are the shift maps, possibly composed with a bit flip. We show that the process of repeated conjugation eventually sends each such map into a finite set of maps. First, we consider the shift maps and show that*

$$\tau^{-1} \circ \sigma^n \circ \tau = \sigma^{\lceil n/2 \rceil}$$

on X_τ, for all $n \in \mathbb{N}$. Then, for all $n \in \mathbb{N}$, $\tau^{-j} \circ \sigma^n \circ \tau^j \in \{id, \sigma\}$ for large enough j. The odd case $n = 2k+1$ is the more interesting one, and writing $\overline{0} = 1$ and $\overline{1} = 0$, we have

$$\begin{aligned} x = x_0x_1x_2x_3\cdots &\overset{\tau}{\mapsto} x_0\overline{x_0}x_1\overline{x_1}x_2\overline{x_2}x_3\overline{x_3}\cdots \\ &\overset{\sigma_n}{\mapsto} \overline{x_k}x_{k+1}\overline{x_{k+1}}x_{k+2}\overline{x_{k+2}}x_{k+3}\overline{x_{k+3}}\cdots \\ &\overset{\tau^{-1}}{\mapsto} \epsilon \cdot x_{k+1} \cdot \epsilon \cdot x_{k+2} \cdot \epsilon \cdot x_{k+3} \cdot \epsilon \cdots \\ &= \sigma^{k+1}(x). \end{aligned}$$

As for the bit flip g, a similar computation shows that

$$\tau^{-1} \circ \sigma^n \circ g \circ \tau = \sigma^{\lceil n/2 \rceil} \circ g,$$

so that for any endomorphism f of the Thue-Morse subshift, we have

$$\tau^{-j} \circ f \circ \tau^j \in \{id, g, \sigma, \sigma \circ g\}$$

for large enough j.

We will again make some standing assumptions. Suppose τ is a balanced almost invertible substitution on the alphabets S, and $\lambda = \lambda(\tau) > 1$.

By Lemma 3.2.39, there exists a balanced almost inverse τ^{-1} for τ. We will repeatedly conjugate (in the group theoretical sense, up to almost invertibility) a cellular automaton $f : X_\tau \to X_\tau$ with τ, that is, apply the transformation $f \mapsto \tau^{-1} \circ f \circ \tau$, and observe the invariants λ, D, and I. Thinking of τ as fixed, we show the following evolution for the invariants:

- λ stays at 1,
- D stays bounded by a constant,
- I decreases until it is bounded by a constant.

Lemma 3.2.43 *With the standing assumptions, there exist $D = D_\tau$ and $I = I_\tau$ such that for any CA $f : X_\tau \to X_\tau$, for all $i \in \mathbb{N}$, for $\Phi_i = \tau^{-i} \circ f \circ \tau^i$ we have $\lambda(\Phi_i) = 1$, $D(\Phi_i) \leq D$. For large enough $i \in \mathbb{N}$, we have $I(\Phi_i) \leq I$.*

Proof. The claim for $\lambda(\Phi_i)$ follows directly from Lemma 3.2.29. As for $D(\Phi_i)$, we have $D(\Phi_0) = 0$ since f is a block map, and from Lemma 3.2.30, we obtain

$$D(\Phi_{i+1}) \leq \lambda^{-1} D(\Phi_i) + \lambda^{-1} D(\tau) + D(\tau^{-1}),$$

where $\lambda = \lambda(\tau)$, so the claim for $D(\Phi_i)$ follows from Lemma 3.2.8. For $I(\Phi_i)$, we similarly obtain from Lemma 3.2.30 that

$$I(\Phi_{i+1}) \leq \lambda^{-1} I(\Phi_i) + 2\lambda^{-1} D(\Phi_i) + C.$$

Since $D(\Phi_i)$ stays bounded by the constant D, the claim for $I(\Phi_i)$ also follows from Lemma 3.2.8. ■

When all the invariants are bounded, there are only finitely many choices for the corresponding dill map.

Lemma 3.2.44 *For any λ, D and I, there are finitely many dill maps $\Phi : X \to Y$ with*

$$\lambda(\Phi) \leq \lambda, D(\Phi) \leq D, I(\Phi) \leq I. \tag{3.5}$$

Proof. The in-radius of the implementation is at most I, and out-radius at most $\lambda + D$. The claim follows because there are at most $(\sum_{k=0}^{\lambda+D} |S|^k)^M$ such functions, where $M = S^{I+1}$. ■

3.2.5 Description of the Cellular Automata

We are now ready to prove our main results.

Proposition 3.2.45 *Let τ be a primitive aperiodic balanced substitution. Then there exists a finite set P of CA on X_τ such that if $f : X_\tau \to X_\tau$ is a CA, then $f = \sigma^k \circ g$ or $g = \sigma^k \circ f$ for some $g \in P$ and $k \in \mathbb{N}$.*

Proof. Let Q be the set of dill maps on X_τ satisfying (3.5) for $\lambda = 1$, $D = D_\tau$ and $I = I_\tau$. The set Q is finite by Lemma 3.2.44.

Let $f : X_\tau \to X_\tau$ be a CA, in particular a dill map. Since τ is balanced, and almost invertible by Lemma 3.2.39, we can apply Lemma 3.2.43 to see

that for some $n \in \mathbb{N}$, the invariants D and I of $\Phi_i = \tau^{-i} \circ f \circ \tau^i$ are smaller than the constants D_τ and I_τ for all $i \geq n$. Then $\Phi_i \in Q$ for all $i \geq n$.

Since Q is finite, we must in fact have $\Phi_{i+j} = \Phi_i$ for some $i \geq n$ and $j > 0$. Because the operation $\Phi \mapsto \tau^{-1} \circ \Phi \circ \tau$ is reversible up to almost equivalence (its almost inverse being $\Phi \mapsto \tau \circ \Phi \circ \tau^{-1}$), we must (by Lemma 3.2.37) then have $f \sim \Phi_{i+\ell} \in Q$ for some $\ell \in [0, j-1]$.

If two block maps are almost equivalent to the same dill map $\Phi \in Q$, they are almost equivalent to each other, and thus one is a shift of the other by Lemma 3.2.41. We choose P as a set of representatives of these finitely many almost equivalence classes. ■

We mention the small subtlety that we do *not* choose a subset P of Q, but instead, for each dill map in Q, we take in P some CA that happens to be almost equivalent to it, if one exists. Thus, more work is needed to obtain a computable bound on the *radii* of the CA in P, although we obtain the concrete upper bound $|P| \leq |Q|$ for the size of this set.

Corollary 3.2.46 *Let τ be a primitive aperiodic balanced substitution. Then there exists m such that if $f : X_\tau \to X_\tau$ is a CA, then f^m is a shift map.*

Proof. We have $f^{n+k} \sim f^n$ for some $n \in [0, |P|], k \in [1, |P|]$ by the pigeonhole principle. Thus, either $f^{n+k} = \sigma^i \circ f^n$ or $f^n = \sigma^i \circ f^{n+k}$. Since f^n is necessarily surjective, in the first case we have $f^k = \sigma^i$. In the second, we have $\sigma^i \circ f^k = \mathrm{id}$, which is impossible since σ^i is not injective. Thus, we can take $m = |P|!$. ■

Corollary 3.2.47 *Let τ be a primitive aperiodic balanced substitution. Then there exists a finite set P of CA on X_τ such that if $f : X_\tau \to X_\tau$ is a CA, then $f = \sigma^k \circ g$ for some $g \in P$ and $k \in \mathbb{N}$.*

Proof. If we have chosen a set of CA P with the property stated in Proposition 3.2.45, and $g = \sigma^k \circ f$ occurs, then this means g can be defined by a neighborhood not containing 0. If it can be defined with neighborhood $[i, i+r]$, then $\sigma^i \circ g \sim g$, and we replace g in P by $\sigma^i \circ g$. If this process of replacing the CA in P with their shifted versions never ends, then some $g \in P$ can be defined by a neighborhood $[i, i+r_i]$ for all $i \in \mathbb{N}$, and some $r_i \in \mathbb{N}$.

However, if g is such a CA, then $g^m = \sigma^i$ is a shift map for some m, i by Corollary 3.2.46. Clearly, any neighborhood of g^m – and thus also g – must then contain a coordinate at most i. Namely, otherwise, the identity map can be defined by a neighborhood not containing 0, and thus factors through a shift map. This is impossible, since a shift map is not injective. ■

While Proposition 3.2.45 and the corollaries are interesting in themselves, our main interest is in two-way subshifts. Since each block map between two-sided subshifts becomes a block map between the corresponding one-sided subshifts when composed with a large enough power of the shift, and almost equivalence is preserved by this operation (with the obvious definition in the two-sided case), we can apply Proposition 3.2.45 also to morphisms between two-sided subshifts.

Theorem 3.2.48 *Let τ be a primitive aperiodic balanced substitution. Then there exists a finite set of CA P on $X_\tau^{\leftrightarrow}$ such that if $f : X_\tau^{\leftrightarrow} \to X_\tau^{\leftrightarrow}$ is a CA, then $f = \sigma^k \circ g$ for some $g \in P$ and $k \in \mathbb{Z}$.*

We also obtain a new proof of Lemma 3.2.6 in our restricted case.

Corollary 3.2.49 *Let τ be a primitive aperiodic balanced substitution. Then all endomorphisms of $X_\tau^{\leftrightarrow}$ are automorphisms.*

Proof. Let $f \in \mathrm{End}(X_\tau^{\leftrightarrow})$. Then, $\sigma^i \circ f$ gives a CA on X_τ for large enough i. Since $(\sigma^i \circ f)^k = \sigma^{ik} \circ f^k$ is a shift map on X_τ for some k by Corollary 3.2.46, f^k must be a shift map on $X_\tau^{\leftrightarrow}$. Thus, f is bijective. ■

In the following, if a group G has a subgroup of finite index isomorphic to another group H, then we say that G is *virtually* H. Using the observations and terminology above, we obtain the following restatement of Theorem 3.2.48:

Theorem 3.2.50 *The endomorphism monoid of the two-sided subshift of a primitive aperiodic balanced substitution is a group, and is virtually $\mathbb{Z}$ (the subgroup isomorphic to $\mathbb{Z}$ being the subgroup of shifts).*

Now, we can easily prove our simplicity properties of interest for these substitutions.

Theorem 3.2.51 *The endomorphism monoid of the two-sided subshift X of a primitive aperiodic balanced substitution is finitely generated, sparse and predictable.*

Proof. The endomorphism monoid is finitely generated since it is generated by the shift map and representatives of each of the finitely many cosets.

To see that the endomorphism monoid is sparse, simply note that the entropy of a substitutive subshift X is 0; see for example [Kůr03].

To see that the endomorphism monoid is predictable, we observe that because the endomorphism monoid is virtually $\mathbb{Z} \cong \langle\sigma\rangle$, (or by extending Corollary 3.2.46 directly), there exists n such that for any CA $f : X \to X$

we have $f^n \in \langle\sigma\rangle$. The claim then follows from Lemma 3.1.1, Lemma 3.1.2 and Lemma 1.5.5. ■

Note that even though X is minimal, (X, σ^m) need not be uniformly recurrent. For example, by recognizability, (X, σ^2) is not uniformly recurrent if X is the subshift of the Thue-Morse substitution. Thus, $f^n = \sigma^m$ does not immediately tell us everything about reachability unless $m = 1$ (in which case the answer is always yes by minimality).

Note that it is not true for all substitutions that all endomorphisms are surjective, as the subshift generated by the substitution

$$0 \mapsto 010, 1 \mapsto 11$$

has the non-surjective endomorphism $x \mapsto {}^{\infty}1^{\infty}$. In particular, the assumption of primitivity is needed in Theorem 3.2.50.

Recall Example 3.2.15 from the uniform case, where we constructed an arbitrary number of not almost equivalent endomorphisms with arbitrarily large radii on the subshift of a primitive uniform substitution. One might ask whether the finitely many maps must in fact be symbol maps in the non-uniform case. However, there are examples where the maps have a larger radius, and in fact, we can construct arbitrarily large radii also in the non-uniform case.

Example 3.2.52 *Recall the notation of Example 3.2.15 from the uniform case. Let again $m \in \mathbb{N}$ and $n \geq 4$, and define $\tau(a_i) = b_{i+1}a_i^{n-1}$ and $\tau(b_i) = b_i a_i^n$. Now τ is not uniform, but the original argument can be directly applied, providing a non-uniform primitive substitution and $m - 1$ pairwise $\sim$-nonequivalent endomorphisms with large neighborhoods.*

The substitution in the previous example is not Pisot, and we do not know examples of Pisot substitutions with large numbers of nonequivalent endomorphisms. For example, Sturmian subshifts are a subcase of Pisot substitutions, and all their endomorphisms are shift maps by the result of [Oll13].

While the Pisot property (or rather, balance) is strongly depended on in our argument, we believe it is not needed for the result that the automorphism group is virtually $\mathbb{Z}$. One can also ask if, more generally, the automorphism group of a linearly recurrent subshift is virtually $\mathbb{Z}$. We would not be particularly surprised if this were the case, but it does not seem likely to us that our method can tackle this problem.

Conjecture 3.2.53 *The automorphism group of the subshift of a primitive aperiodic substitution is virtually $\mathbb{Z}$.*

Question 3.2.54 *Is the automorphism group of every linearly recurrent subshift virtually $\mathbb{Z}$?*

Our result could also be generalized in another direction, namely, for measure-preserving[9] maps between subshifts generated by primitive substitutions. The uniform case has been partially solved in [HP89], where it was shown that there are only finitely many (up to shifting and almost everywhere equivalence) measure-preserving, almost everywhere shift-commuting maps between two subshifts generated by uniform primitive substitutions satisfying certain injectivity conditions.

Question 3.2.55 *Does the result of [HP89] hold in the Pisot case? The general primitive case?*

3.3 Cellular Automata on Toeplitz Subshifts

Given that a minimal subshift necessarily has a restricting global structure, one could ask whether in fact there even *exists* a minimal subshift with interesting self-maps. We can at least show that there exists a minimal subshift whose endomorphism monoid is not finitely generated, so that in particular the analogue of Theorem 3.2.45 does not hold in general on minimal subshifts. Finding such an example is the purpose of this section. We will develop basic tools for computing endomorphism monoids of Toeplitz subshifts, and compute them for some examples where the endomorphism monoid is not finitely generated. As in Section 3.2, we prove our results for one-sided subshifts, and extract two-sided corollaries in the end of this section.

A *Toeplitz point* is a point $x \in S^{\mathbb{N}}$ such that for all coordinates i there exists a *period* $p > 0$ such that $x_{i+kp} = x_i$ for all $k \in \mathbb{N}$. Then, for all intervals $[j, j']$, we also find $p > 0$ such that have $x_{[j,j']+kp} = x_{[j,j']}$ for all $k \in \mathbb{N}$, and we similarly say p is the period of $[j, j']$ in x. A Toeplitz point is clearly uniformly recurrent, so the subshift $X \subset S^{\mathbb{N}}$ it generates is minimal. A *Toeplitz subshift* is any subshift generated by a Toeplitz point. Not every point in a Toeplitz subshift need be Toeplitz, but the Toeplitz points are necessarily dense, since the orbit of the point generating the subshift is dense, and contains only Toeplitz points. Note that periodic points are Toeplitz with our definition, and they generate Toeplitz subshifts conjugate to finite systems $(\mathbb{Z}_n, (x \mapsto x + 1))$. In fact, these finite systems are important in what follows. Thus, in this section, we will consider $\mathbb{Z}_n$ a dynamical system with dynamics $x \mapsto x + 1$, and it is often considered synonymous with the subshift $(10^{n-1})^{\mathbb{Z}}$. However, when used as an invariant, its dynamics will be $\mathrm{id}_{\mathbb{Z}_n}$.

One way to generate Toeplitz sequences is the following type of substitution process. Let $w \in (S \dot{\cup} \{\_\})^*$. We say w is a *partial word* over the

[9] Measure-preserving with respect to the unique measure that is preserved by the shift-map.

alphabet S, and $\llcorner$ represents 'missing' coordinates. Let ϕ be the map that, given y and z in $(S\dot\cup\{\llcorner\})^{\mathbb{N}}$, writes z in the 'unknown coordinates' of y. More precisely,

$$\phi(y,z)_j = \begin{cases} z_{k-1} & \text{if } k = |y_{[0,j]}|_{\llcorner} \wedge y_j = \llcorner \text{ and} \\ y_j & \text{if } y_j \neq \llcorner. \end{cases}$$

If $w_0 \in S$, then writing $\psi_w(x) = \phi(w^\infty, x)$, we define

$$x(w) = \lim_{n\to\infty} \psi_w^n(\llcorner^\infty).$$

It is easy to see that $x(w) \in S^{\mathbb{N}}$ is a Toeplitz point. We write $X_w \subset S^{\mathbb{N}}$ for the subshift $\overline{\mathcal{O}(x(w))}$ it generates.

We will, in particular, compute the endomorphism monoid of the two-way extension $X^{\leftrightarrow}_{10\llcorner 0\llcorner}$ of $X_{10\llcorner 0\llcorner}$: as in the previous section, this again consists of automorphisms only, and it is isomorphic to the additive subgroup $\left\langle \left(\frac{5}{2}\right)^i \mid i \in \mathbb{N} \right\rangle$ of $\mathbb{Q}$, which is not finitely generated.

3.3.1 Preliminary Results

We begin with a general discussion of Toeplitz subshifts. Our methods are very elementary, and we do not need much of the theory of Toeplitz subshifts – in particular, while the discussion below is strongly based on the maximal equicontinuous factor of a Toeplitz subshift (which is an odometer), we will not discuss this factor explicitly, but only its finite factors.[10] The lemmas 3.3.2 and 3.3.3 can be extracted from any reference that discusses the maximal equicontinuous factor of a Toeplitz subshift [Kůr03, Wil84, Dow05], but we prove them directly.

Definition 3.3.1 *Let x be a Toeplitz point which is not periodic. For each k, define the* k-skeleton of x *as the point*

$$\mathrm{Sk}(k,x)_i = \begin{cases} x_i, & \text{if } \forall m \in \mathbb{N} : x_{i+mk} = x_i, \text{ and} \\ \llcorner, & \text{otherwise.} \end{cases}$$

The number k is an essential period *of x if $\sigma^\ell(\mathrm{Sk}(k,x)) \neq \mathrm{Sk}(k,x)$ for all $0 < \ell < k$.*

Lemma 3.3.2 *Let x be a Toeplitz point, and X the subshift it generates. Then $\mathbb{Z}_n$ is a factor of X is and only if $n|k$ for some essential period k of x.*

Proof. We first show that if k is an essential period, then $\mathbb{Z}_k$ is a factor of X. Clearly every coordinate of $\mathrm{Sk}(k,x)$ containing a symbol other than

[10] The maximal equicontinuous factor of a Toeplitz subshift is just an inverse limit of the finite factors, so the difference is small.

␣ has period k. On the other hand, it is not hard to show that there exists m such that if $x_j = x_{j+1} = \cdots = x_{j+mk}$, then $\mathrm{Sk}(k,x)_j = x_j$. This, and the fact that $\sigma^\ell(\mathrm{Sk}(k,x)) \neq \mathrm{Sk}(k,x)$ for all $0 < \ell < k$, imply that $x_{[i,i+(m+1)k]}$ 'matches' $\mathrm{Sk}(x,k)_{[0,(m+1)k]}$ (in the sense of being equal to it in the non-␣ coordinates) if and only if $i \equiv 0 \bmod k$, and from this, we obtain a block map from X to $\mathbb{Z}_k$, so that also $\mathbb{Z}_n$ for $n|k$ are factors of X.

Next, suppose $f : X \to \mathbb{Z}_n$ is a factor map. By continuity, $y_{[0,r]}$ determines the image $f(y)$ for $y \in X$. Let w be such that $f(y) = 0$ whenever $y_{[0,|w|-1]} = w$. Then w occurs at $x_{[i,i+|w|-1]}$ only if $i \equiv 0 \bmod k$. Let k be minimal such that w occurs in $\mathrm{Sk}(x,k)$. Then it is easy to see that k is an essential period, and $n|k$. ■

Lemma 3.3.3 *If X is a Toeplitz subshift, $x \in X$ is Toeplitz, and the least period of $[i,j]$ in x is k, then $\mathbb{Z}_k$ is a factor of X.*

Proof. Clearly, $\mathrm{Sk}(x,k)_{[i,j]} = x_{[i,j]}$. If $\sigma^\ell(\mathrm{Sk}(k,x)) \neq \mathrm{Sk}(k,x)$ for some $0 < \ell < k$, then ℓ is a smaller period of $[i,j]$ in x. Thus, k is an essential period, and the result follows from the previous lemma. ■

We now define the notions of disjointness and independence. Disjointness is a relatively well-known concept in the theory of dynamical systems, and it was introduced in [Fur67]. We do not know if independence has been studied previously, but it is very useful for studying the endomorphism monoid, see Section 3.3.2. While distinct for minimal subshifts in general, we show in Theorem 3.3.15 that the two notions, disjointness and independence, are equivalent for Toeplitz subshifts. We give the definition of disjointness given in [HY05], in the case of subshifts.

Definition 3.3.4 *If X, Y are two subshifts, we say that a subshift $J \subset X \times Y$ is a joining of X and Y if the restrictions of the projection maps $\pi_1 : J \to X$ and $\pi_2 : J \to Y$ are surjective. If each joining is equal to $X \times Y$, we then say that X and Y are* disjoint*, and denote this by $X \perp Y$.*

Lemma 3.3.5 *Suppose X and Y are minimal. Then $X \perp Y$ if and only if $X \times Y$ is minimal.*

Proof. If $X \times Y$ is minimal and J is a joining of X and Y, then J is a nonempty subshift of $X \times Y$, and thus $J = X \times Y$ by minimality, so that $X \perp Y$.

Suppose then that $X \perp Y$ and J is a nonempty subshift of $X \times Y$. Then $(x,y) \in J$ for some $x \in X$ and $y \in Y$. Since both X and Y are minimal, x generates X and y generates Y, so that the orbit closure K of (x,y) projects onto X through π_1 and onto Y through π_2. By $X \perp Y$, we have $K = X \times Y$. Of course, we then have $J = X \times Y$, so that $X \times Y$ is minimal. ■

In the case that one of the systems is finite, we have the following alternative characterization.

Lemma 3.3.6 *Let X be minimal. Then $X \perp \mathbb{Z}_m$ if and only if (X, σ^m) is minimal.*

Proof. We have $X \perp \mathbb{Z}_m$ if and only if $X \times \mathbb{Z}_m$ is minimal.

If (X, σ^m) is minimal, then for all $\epsilon > 0$ and $x, y \in X$, if $(x, n_1), (y, n_2) \in X \times \mathbb{Z}_n$ and $n_1 \leq n_2$ (the other case being symmetric), by the minimality of σ^m, there exists k such that $d(\sigma^{km}(\sigma^{n_2-n_1}(x)), y) < \epsilon$, and then

$$d(\sigma^{km+n_2-n_1}((x, n_1)), (y, n_2)) = d((\sigma^{km+n_2-n_1}(x), n_2), (y, n_2)) < \epsilon.$$

If $X \times \mathbb{Z}_m$ is minimal then for any $\epsilon > 0$ and $x, y \in X$, for some $n \in \mathbb{N}$ we have $\sigma^n(x, 0) = (z, 0)$ where $d(z, y) < \epsilon$. Clearly $n = km$ for some k, so (X, σ^m) is minimal. ■

Definition 3.3.7 *A block map $\phi : X \times Y \to Z$ is* right-independent *if ϕ factors through the projection map $\pi_1 : X \times Y \to X$. We define* right-dependence *as the complement of right-independence, and* left-independence *and* left-dependence *symmetrically. If all block maps $\phi : X \times Y \to X$ are right-independent then we say X is independent from Y. If X is independent from Y and Y from X, then we say the two are* mutually independent. *Again, in the converse case, we say X is dependent of Y.*

In general, we can define these notions in categories with products, and in concrete categories where products correspond to set theoretic products, X is independent from Y if there are no maps $\phi : X \times Y \to X$ which actually depend on the Y-coordinate.

The two notions have nontrivial interplay within the class of minimal systems. We can at least construct two minimal systems X and Y such that $X \times Y$ is minimal, but X depends on Y:

Example 3.3.8 *For all $u \in \{0,1\}^*$, let $O(u)$ be the word where odd coordinates of u have been flipped (counting from the left, starting with 0), and $E(u)$ the word where even coordinates have been flipped. Let $B(u) = E(O(u))$. If $|u|$ is odd, then $O(uv) = O(u)E(v)$ and $E(uv) = E(u)O(v)$.*

Let $w_0 = 000$, and inductively define $w_{i+1} = w_i w_i O(w_i) O(w_i) B(w_i)$, all of which are of odd length. For all i, w_i occurs in all of w_{i+1}, $O(w_{i+1})$, $E(w_{i+1})$ and $B(w_{i+1})$:

- $O(w_{i+1}) = O(w_i)E(w_i)w_i B(w_i)E(w_i)$,
- $E(w_{i+1}) = E(w_i)O(w_i)B(w_i)w_i O(w_i)$, *and*
- $B(w_{i+1}) = B(w_i)B(w_i)E(w_i)E(w_i)w_i$.

For any i, the point $x = \lim_j w_j$ is an infinite product of the words w_{i+1}, $O(w_{i+1})$, $E(w_{i+1})$ and $B(w_{i+1})$. By the previous observation, it is then uniformly recurrent. Thus, the system $X = \overline{\mathcal{O}(x)}$ with the shift dynamics σ is minimal. Since $w_i w_i \sqsubset X$ for all i and $|w_i|$ is odd, also σ^2 is minimal.

Now, let $Y = \mathcal{O}(^\infty(01)^\infty)$. It follows from the minimality of σ^2, Lemma 3.3.6 and Lemma 3.3.5 that also $X \times Y$ is minimal. By the inductive definition of X, the map

$$\phi(x, y) = x + y,$$

where $+$ is the binary XOR-operation, is well-defined from $X \times Y$ to X. It clearly depends on the Y-coordinate.

In the case of Toeplitz subshifts, the two notions are simply state that the systems have no common finite factor. These, and some other equivalent notions, are listed in Theorem 3.3.15.

Definition 3.3.9 *A* (nontrivial) invariant *of a system X is a factor map from X to a system $(\mathbb{Z}_m, id)$.*

Lemma 3.3.10 *If X is transitive, then it has no nontrivial invariant.*

Proof. The image of a transitive system in a factor map is transitive. ■

We give an obvious composition result. Of the two claims we prove, we only need the first one.[11]

Definition 3.3.11 *A map $\xi : X \times Y \to Z$ is* right-surjective *if for all x, the function $\xi|_{\{x\}\times Y} : \{x\} \times Y \to Z$ is surjective. We define* left-surjectivity, right-injectivity *and* left-injectivity *in the obvious way, and* bi-surjectivity *and* bi-injectivity *as the conjunction of the respective left- and right notions.*

Lemma 3.3.12 *Let $\xi : X \times Y \to Z$ and $\xi' : X \times Z \to X$ be block maps. If*

- *ξ is right-surjective and ξ' right-dependent, then X is dependent of Y.*
- *ξ is right-dependent and ξ' right-injective, then X is dependent of Y.*

Proof. Define $\phi(x, y) = \xi'(x, \xi(x, y))$. If either assumption holds for ξ and ξ', this map shows that X is dependent of Y. ■

Lemma 3.3.13 *A nontrivial subshift X is dependent of every system $(\mathbb{Z}_m, id)$ with $m > 1$.*

[11] There are many more symmetric versions of this lemma. We can of course replace right by left, but we can also define a dual notion of 'coindependence' by considering maps from X to the coproduct (disjoint union) $X \cup Y$ instead of maps from the product $X \times Y$ to X.

Proof. Let X be any such subshift. There exist two distinct endomorphisms ϕ_1 and ϕ_2 of X, for example, id_X and the shift map. Let $\emptyset \subsetneq C \subsetneq \mathbb{Z}_m$ be any subset. Let

$$\phi(x, y) = \begin{cases} \phi_1(x), & \text{if } y \in C, \\ \phi_2(x), & \text{otherwise.} \end{cases}$$

Then ϕ is a right-dependent map, so X is not independent of $(\mathbb{Z}_m, \mathrm{id})$. ■

Lemma 3.3.14 *If X is nontrivial and $X \times Y$ has a nontrivial right-surjective invariant, then X is dependent of Y.*

Proof. Let $\xi : X \times Y \to (\mathbb{Z}_m, \mathrm{id})$ be a nontrivial right-surjective invariant. By Lemma 3.3.13, X depends on $(\mathbb{Z}_m, \mathrm{id})$, so that some map $\xi' : X \times (\mathbb{Z}_m, \mathrm{id}) \to X$ is right-dependent. The result then follows from Lemma 3.3.12. ■

Theorem 3.3.15 *Let X, Y be nontrivial Toeplitz subshifts. Then the following are equivalent:*

1. *$X \perp Y$*
2. *$X \times Y$ is minimal*
3. *$X \times Y$ is transitive*
4. *X and Y are mutually independent*
5. *X is independent from Y*
6. *X and Y have no common nontrivial finite factors.*

Proof. The equivalence of (1) and (2) was proved in Lemma 3.3.5. It is clear that (3) follows from (2) and (5) follows from (4). If (6) does not hold, then X and Y have a common finite factor $\mathbb{Z}_m$ through factor maps $\phi_1 : X \to \mathbb{Z}_m$ and $\phi_2 : Y \to \mathbb{Z}_m$ (since the systems systems $\mathbb{Z}_m$ are the only minimal finite systems). This means $\xi(x, y) \mapsto \phi_1(x) - \phi_2(y)$ is a bi-surjective invariant, so that (3) does not hold by Lemma 3.3.10, and (5) does not hold by Lemma 3.3.14.

We now tackle the hard part, the implications (6) $\implies$ (2) and (6) $\implies$ (4), which conclude the proof.

So, suppose (6). We first show that (4) follows. Let $\xi : X \times Y \to X$ be a block map with (one-directional) radius R. Choose $w \in \mathcal{B}_{R+1}(X)$ and $u, u' \in \mathcal{B}_{R+1}(Y)$ arbitrarily. Fix Toeplitz points $x \in X$ and $y \in Y$ such that $x_{[0,R]} = w$ and $y_{[0,R]} = u$ (using the fact that Toeplitz points are dense) and choose $j \in \mathbb{N}$ such that $y_{[j,j+R]} = u'$. Of course, $z = \xi(x, y) \in X$ is Toeplitz,

since x and y are. Let $[0, R]$ have least period k_x in x, let 0 have least period k_z in z, and let $[0, j + R]$ have least period k_y in y.

By Lemma 3.3.3, there exists a factor map from X to both $\mathbb{Z}_{k_x}$ and $\mathbb{Z}_{k_z}$, and from Y to $\mathbb{Z}_{k_y}$. This means that $\gcd(k_x k_z, k_y) = 1$ by the assumption that X and Y have no common finite factors.

If $\gcd(k_x k_z, k_y) = 1$, then there exists m such that $mk_x k_z \equiv j \bmod k_y$, so that

$$\xi_{\text{loc}}(w, u) = \xi(x, y)_0 = \sigma^{mk_x k_z}(\xi(x, y))_0 = \xi(x, \sigma^{mk_x k_z}(y))_0 = \xi_{\text{loc}}(w, u').$$

Because w, u and u' were chosen arbitrarily, ξ is right-independent. Left-independence is proved symmetrically, and thus (6) $\implies$ (4).

Next, we prove (2) assuming (6), along similar lines: Fix Toeplitz points $x \in X$ and $y \in Y$. Let $R \in \mathbb{N}$ be arbitrary and let $w \in \mathcal{B}_{R+1}(X)$ and $u \in \mathcal{B}_{R+1}(Y)$ be arbitrary words. Let j_1, j_2 be such that $x_{[j_1, j_1+R]} = w$ and $y_{[j_2, j_2+R]} = u$. As previously, the least period k_x of $[0, j_1 + R]$ in x is coprime with the least period k_y of $[0, j_2 + R]$ in y. Thus, there exists m such that $mk_x \equiv j_2 - j_1 \bmod k_y$. We have

$$\sigma^{nk_x k_y + mk_x + j_1}(x, y)_{[0,R]} = (w, u)$$

for all $n \in \mathbb{N}$. Thus, the orbit of (x, y) is dense in $X \times Y$. Since (x, y) is Toeplitz, $X \times Y$ is minimal. ■

We also briefly discuss the groups we will implement as endomorphism monoids.

Definition 3.3.16 *For $m, n \in \mathbb{N}$, we define a subgroup of $(\mathbb{Q}, +)$ by*

$$A(n, m) = \left\langle \left(\frac{n}{m}\right)^i \mid i \in \mathbb{N} \right\rangle.$$

Lemma 3.3.17 *The group $A(n, m)$ is not finitely generated if $m \nmid n$.*

Definition 3.3.18 *Let G be an abelian group with generators $\{g_i \mid i \in \mathbb{N}\}$ such that $ng_i = mg_{i+1}$ for all i. Then G is said to be* (n, m)-lifting.

The group $A(n, m)$ is easily seen to be (n, m)-lifting.

Lemma 3.3.19 *Let $(n, n', m) \in \mathbb{N}^3$ satisfy*

$$n = 2n' + 1, 1 < m \leq n' \text{ and } \gcd(m, n) = 1, \tag{3.6}$$

and let $G = \langle g_i \mid i \in \mathbb{N} \rangle$ be (n, m)-lifting. Then every element $g \in G$ can be written as

$$g = k_1 g_1 + k_2 g_2 + \ldots + k_j g_j,$$

where $k_i \in [-n', n']$ for all i, and $k_j \neq 0$. In the group $A(n, m)$, there is a unique such representation for each $g \in G$. Conversely, if there is a unique such representation, then G is isomorphic to $A(n, m)$.

Proof. All elements of G can be put into such form by first adding a suitable multiple of $ng_1 - mg_2 = 0$ to reduce k_1, then $ng_2 - mg_3 = 0$ to reduce k_2, and so on. This process eventually terminates because $m \leq n'$.

If the form is not unique for some element of the group, then by subtracting two distinct but equivalent forms and putting the result in the normal form, we obtain

$$k_j g_j + k_{j+1} g_{j+1} + \cdots + k_{j'} g_{j'} = 0$$

where $k_j \neq 0$, $k_{j'} \neq 0$ and $k_i \in [-n', n']$ for all i. Letting $G = A(n, m)$, the equation above then cannot hold:

$$\begin{aligned}(k_j g_j + \cdots + k_{j'} g_{j'}) m^{j'} &= \left(k_j \left(\frac{n}{m}\right)^j + k_{j+1} \left(\frac{n}{m}\right)^{j+1} + \cdots + k_{j'} \left(\frac{n}{m}\right)^{j'} \right) m^{j'} \\ &= k_j n^j m^{j'-j} + k_{j+1} n^{j+1} m^{j'-j-1} + \cdots + k_{j'} n^{j'} \\ &\equiv k_j n^j m^{j'-j} \bmod n^{j+1} \\ &\not\equiv 0 \bmod n^{j+1}\end{aligned}$$

since $\gcd(m, n) = 1$ and $k_j \in [-n', n']$.

Let $G = A(n, m)$, and let $H = \langle h_i \mid i \in \mathbb{N} \rangle$ be another (n, m)-lifting group. We define a map ϕ from G to H by mapping $g_i \mapsto h_i$, and in general mapping

$$k_1 g_1 + k_2 g_2 + \ldots + k_j g_j \mapsto k_1 h_1 + k_2 h_2 + \ldots + k_j h_j,$$

when the left side is in the normal form. It is clear that this is a bijection between the groups, since we assumed that the representations are unique on both sides. To see that it is a homomorphism, note that if $g, h \in G$, then the unique normal form for $g + h$ is obtained by summing the components of the normal forms of g and h, and applying the algorithm described in the first paragraph of the proof. By applying the same transformations to the representation of $\phi(g) + \phi(h)$ obtained by summing the representations of $\phi(g)$ and $\phi(h)$, we obtain precisely $\phi(g+h)$, and thus $\phi(g+h) = \phi(g)+\phi(h)$. ■

3.3.2 A Non-Finitely Generated Endomorphism Monoid

We can now construct our example of a Toeplitz subshift whose endomorphism monoid is not finitely generated: for any triple (n, n', m) satisfying (3.6), we will find a Toeplitz subshift whose endomorphism monoid is isomorphic to the group $A(n, m)$.

We say $p > 0$ is a *lazy period* of a partial point $y \in (S \cup \{\_\})^{\mathbb{N}}$ if $y_i = y_{i+kp}$ whenever $y_i, y_{i+kp} \in S$ for $i, k \in \mathbb{N}$. The interpretation of having lazy period p is that there is a way to fill the $\_$-gaps so that the resulting point has period p. We note that having lazy periods j and j' does not imply the lazy period $\gcd(j, j')$. However, the following is easy to verify.

Lemma 3.3.20 *If $y \in (S \cup \{␣\})^{\mathbb{N}}$ has period j and lazy period j', the y has lazy period* $\gcd(j, j')$.

We make some standing assumptions for the rest of this section. We fix a triple (n, n', m) satisfying (3.6). We also fix a word $w \in (S \cup \{␣\})^n$, the fixed point $x = x(w)$ and the subshift $X = X_w$, with the properties

- w^∞ has least lazy period n,
- $|w|_␣ = m$,
- $␣␣ \not\sqsubset w^\infty$, and
- id_X is the only symbol map on X.

For example, it is easy to check that $w = 1(0␣)^m 0^{2(n'-m)}$ is such a word.

Example 3.3.21 *We illustrate the structure of x for $w = 10␣0␣$:*

$$\begin{aligned} x = {} & 1\ 0\, x_0\, 0\, x_1\, 1\ 0\, x_2\, 0\, x_3\, 1\ 0\, x_4\, 0\, x_5\, 1\ 0\, x_6\, 0\, x_7\, 1\ 0\, x_8 \ldots \\ = {} & 1\ 0\ 1\ 0\ 0\ 1\ 0\, x_0\, 0\ 0\ 1\ 0\, x_1\, 0\ 1\ 1\ 0\ 0\ 0\, x_2\, 1\ 0\ 0\ \ldots \\ = {} & 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\, x_0\, 1\ 0\ 0\ \ldots \\ = {} & 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ \ldots \end{aligned}$$

We write $y|_{(J)}$ for the point where all but the subsequence J is turned to $␣$:

$$(y|_{(J)})_i = \begin{cases} y_i, & \text{if } i \in J, \text{ and} \\ ␣, & \text{otherwise.} \end{cases}$$

The point $y|_K$ is the actual subsequence of y along K:

$$(y|_K)_i = y_k \text{ if } |K \cap [0, k]| = i + 1 \wedge k \in K.$$

Define $K_\ell = \{i \mid \psi_w^\ell(␣^\infty)_i = ␣\}$ and $J_\ell = \mathbb{N} \setminus K_\ell$. We now prove two lemmas about w and the point $x = x(w)$.

Lemma 3.3.22 *With the standing assumptions and notation above, for all j there exists ℓ such that*

$$i_1, i_2 \in K_\ell \implies i_1 = i_2 \vee |i_1 - i_2| > j.$$

Proof. Since $␣␣ \not\sqsubset w^\infty$, the minimal distance between two distinct elements of K_1 is at least 2. If the minimal distance between two distinct elements of K_i is k, then the minimal distance between two distinct elements of K_{i+1} is at least $2k$. Thus we can take $\ell = \lceil \log_2 j \rceil$. ■

Lemma 3.3.23 *With the standing assumptions and notation above, the finite factors of X are the systems $\mathbb{Z}_k$ where $k | n^\ell$ for some $\ell \in \mathbb{N}$.*

Proof. By assumption, the point $x|_{(J_1)} = w^\infty$ has least lazy period n. Since it also has period n, n divides all its lazy periods by Lemma 3.3.20. It follows that n also divides the least lazy period of $x|_{(J_2)}$. By the self-similar structure of x, $x|_{(J_2)}$ having least lazy period kn means that km is a lazy period of $(x|_{(J_2)})|_{K_1}$. Since $x|_{K_1} = x$, it follows that $(x|_{(J_2)})|_{K_1} = x_{(J_1)}$. From $\gcd(m, n) = 1$, we then obtain $k = n$ (or k was not minimal). Continuing by induction, we can prove that $x|_{(J_\ell)}$ has least lazy period n^ℓ.

Now, consider the point $\mathrm{Sk}(x, n^\ell)$ for some $\ell \in \mathbb{N}$. It is easy to see from the definition of ψ_w that we have $(x|_{(J_\ell)})_i \in S \implies \mathrm{Sk}(x, n^\ell)_i \in S$. Now, if we had $\sigma^j(\mathrm{Sk}(x, n^\ell)) = \mathrm{Sk}(x, n^\ell)$ for some $0 < j < n^\ell$, clearly $x|_{(J_\ell)}$ would have j as a lazy period. Thus, n^ℓ is an essential period of x, so that $\mathbb{Z}_k$ is a finite factor of X for any $k|n^\ell$. Conversely, suppose $\mathbb{Z}_k$ is finite factor of X. If k divides n^ℓ for some ℓ, we are done. Otherwise, we may remove any common divisors of k and n^ℓ (by considering a suitable factor of $\mathbb{Z}_k$), so that without loss of generality, we have $\gcd(k, n^\ell) = 1$ for all ℓ. A contradiction can then be obtained as in the proof of Lemma 3.3.2. ■

We mentioned $(x|_{(J_\ell)})_i \in S \implies \mathrm{Sk}(x, n^\ell)_i \in S$ in the proof. The converse implication is true as well: If $j \notin J_\ell$, then the sequence x_{j+in^ℓ} moves along an arithmetic progression of cells of $x|_{K_\ell} = x$ with steps of length m^ℓ. Since $\gcd(m, n) = 1$ and every cell has a period of the form n^ℓ, it is easy to see that this sequence is not constant. Thus, the n^ℓ-skeleton is what one would expect. (However, this does not automatically mean that the numbers n^ℓ are the only essential periods.)

Lemma 3.3.24 *With the standing assumptions, we have that $X \perp \mathbb{Z}_{m^j}$. In particular, (X, σ^{m^j}) is minimal for all j.*

Proof. The finite factors of $\mathbb{Z}_{m^j}$ are the systems $\mathbb{Z}_\ell$ where $\ell|m^j$. The finite factors of X, on the other hand, are the finite factors of the systems $\mathbb{Z}_{n^i}$ for $i \in \mathbb{N}$ by Lemma 3.3.2. Since $\gcd(m, n) = 1$, there are no common finite factors, and then $X \perp \mathbb{Z}_{m^j}$ by Theorem 3.3.15. The latter claim follows from Lemma 3.3.6. ■

For f an endomorphism of X, we define the *unlifted* function $\downarrow f$ which applies f in the 'holes', that is, the coordinates that do not come from the n-skeleton w^∞. More precisely, we specify the image of $\downarrow f$ on x as

$$\downarrow f(x) = \psi_w(f(\psi_w^{-1}(x))) = \psi_w(f(x)) \in S^{\mathbb{N}},$$

and extend this to a continuous and shift-commuting map from X to $S^{\mathbb{N}}$. This is possible because the periodic structure contains n, so that there exists a factor map from X to $\mathbb{Z}_n$, and this factor map identifies precisely the n-skeleton w^∞.

Lemma 3.3.25 *With the standing assumptions, for any block map $f : X \to X$, the unlifted map $\downarrow f$ is an endomorphism of X.*

Proof. Since (X, σ^m) is minimal by the previous lemma, it is easy to see that $\psi_w(y) \in X$ for any $y \in X$, which implies $\downarrow f(x) \in X$. ■

More generally, if we take any $y \in X$, take its n^j-skeleton, and replace the rest of the coordinates with a point $z \in X$, the resulting point is in X.

Lemma 3.3.26 *With the standing assumptions, there exists r such that for every endomorphism $f : X \to X$ with radius $R \geq r$, there exists a block map $h : X \to X$ with radius less than R such that*

$$\sigma^k \circ f = \downarrow h$$

for some $0 \leq k < n$.

Proof. Suppose R is the radius of f, and $R \geq n$. Since n is in the periodic structure of x, there exists a map $\pi : X \to \mathbb{Z}_n$ giving the phase of the n-skeleton w^∞. It is easy to see that there exists k with $0 \leq k < n$ such that $\pi \circ f \circ \sigma^k = \pi$, and $f_1 = f \circ \sigma^k$ has radius at most $R + n$. Let $g_1 : X \times \mathbb{Z}_m \to X$ be defined by

$$g_1(y, i) = (\sigma^i \circ \psi_w^{-1} \circ f_1 \circ \psi_w \circ \sigma^{-i})(y).$$

Note that this does not, strictly speaking, make much sense, since σ is not invertible.[12] However, we can choose a continuous section (right inverse) for σ, for example $\sigma^{-i}(x) = \#^i x$ for a new symbol $\#$, and extend ψ_w and ψ_w^{-1} so that they add and remove the n-skeleton w^∞ even in the presence of the new symbol. We extend $(f_1)_{\text{loc}} : S^{R+k+1} \to S$ to the alphabet $S \cup \{\#\}$ by having it behave as the identity map if the symbol $\#$ occurs in the neighborhood. Since f_1 preserves the n-skeleton even in the presence of new symbols, ψ_w^{-1} can indeed be applied after it.

It is now easy to see that the new symbols do not actually occur in $g_1(y, i)$ for any $(y, i) \in X \times Z$. Namely, $\#^i$ is prefixed to y by σ^{-i}, and $\psi_w(\sigma^{-i}(y))$ is then a n-skeleton with the first i symbols $\sqcup$ filled with $\#$, and the rest of the coordinates filled with the letters of y. Our extension of f_1 preserves the n-skeleton and it is easy to see that it does not remove or add $\#$-symbols. Thus, $\sigma^i \circ \psi_w^{-1}$ undoes the adding of $\#$-symbols.

Since all the maps in the composition are continuous, g_1 is continuous. To check that g_1 is a block map, we now only have to check that it is shift-commuting. If $i < m - 1$, then this is true basically by definition:

$$\begin{aligned} g_1(\sigma(ay), i + 1) &= (\sigma^{i+1} \circ \psi_w^{-1} \circ f_1 \circ \psi_w \circ \sigma^{-i-1})(y) \\ &= \sigma((\sigma^i \circ \psi_w^{-1} \circ f_1 \circ \psi_w \circ \sigma^{-i})(\#y)) \\ &= \sigma((\sigma^i \circ \psi_w^{-1} \circ f_1 \circ \psi_w \circ \sigma^{-i})(ay)) \\ &= \sigma(g_1(ay, i)), \end{aligned}$$

[12] An alternative to the use of the dummy symbol $\#$ would be to move to two-way subshifts already at this point, but we have chosen this clumsier way to avoid translating results from one-way subshifts to two-way subshifts.

where the third equality follows by tracking the leftmost symbol, and noting that it is removed by the σ at the end.

If $i = m - 1$, then

$$\begin{aligned} g_1(\sigma(y), 0) &= (\psi_w^{-1} \circ f_1 \circ \psi_w)(\sigma(y)) \\ &= (\sigma^m \circ \psi_w^{-1} \circ f_1 \circ \psi_w \circ \sigma^{-m})(\sigma(y)) \\ &= \sigma((\sigma^{m-1} \circ \psi_w^{-1} \circ f_1 \circ \psi_w \circ \sigma^{-m+1})(y)) \\ &= \sigma(g_1(y, m-1)). \end{aligned}$$

For the second equality, note that σ^{-m} simply adds $\#^m$ in the beginning of $\sigma(y)$, so that $\psi_w(\sigma^{-m}(\sigma(y))) = w'\psi_w(\sigma(y))$, where w' is w with the symbols $\textvisiblespace$ replaced with $\#$ (since w contains exactly m symbols $\textvisiblespace$). Then

$$(f_1 \circ \psi_w \circ \sigma^{-m})(\sigma(y)) = w' f_1(\psi_w(\sigma(y))),$$

from which the second equality follows easily.

Because $X \perp \mathbb{Z}_m$, it follows from Theorem 3.3.15 that X is independent of $\mathbb{Z}_m$. Thus, there exists a map $h_1 : X \to X$ such that $g_1(y, i) = h_1(y)$ for all $y \in X$ and $i \in \mathbb{Z}_m$. But then, by the definition of the unlifting operation, $f_1 = \downarrow h_1$. It is easy to see that h_1 can be taken to have the same radius as g_1 (since its local rule can use the local rule of g_1 with arbitrary data on the $\mathbb{Z}_m$-track). For a large enough constant C (independent of f), g_1 – and thus h_1 – has radius at most $\frac{m}{n}R + C$. As in Section 3.2, we see that this is smaller than R if R is large enough. ■

Let $Y = X^{\leftrightarrow}$ be the two-way extension of X. For $f : Y \to Y$, we define $\downarrow f : Y \to Y$ in the obvious way. It is easy to check the equality $\downarrow (g \circ h) = \downarrow g \circ \downarrow h$ for CA $g, h : Y \to Y$. Notions such as skeletons directly translate to the two-way case. We write $\sigma_i = \downarrow^i \sigma$, so that $\sigma_0 = \sigma$, and in general σ_i shifts the coordinates not in the n^i-skeleton one step to the left (jumping over coordinates in the n^i-skeleton).

We note that Lemma 3.3.26 is true in a slightly nicer form in the two-way case, since we can put the shift on the right hand side of the equation.

Lemma 3.3.27 *There exists r such that for every endomorphism $f : Y \to Y$ with radius $R \geq r$, there exists a block map $h : Y \to Y$ with radius less than R such that*

$$f = \sigma^k \circ \downarrow h$$

for some $k \in \mathbb{Z}$.

Proof sketch. Considering the action of $\sigma^j \circ f$ on right tails of points, where j is large enough that $\sigma^j \circ f$ has one-sided radius, we see that $\sigma^k \circ \sigma^j \circ f = \downarrow h$ for some k also in the two-way case. The proof follows by composing both sides with σ^{-k-j}. ■

Lemma 3.3.28 *With the assumptions and notation above, for any CA $h : Y \to Y$, if $p > 0$ and*

$$h = \sigma_0^{\ell_0} \circ \sigma_1^{\ell_1} \circ \cdots \circ \sigma_{p-1}^{\ell_{p-1}} \circ \downarrow^p h,$$

then $h = \sigma^i$ for some $i \in \mathbb{Z}$.

Proof. First, note that we can make p as large as we like by repeatedly substituting this expression for h on the right-hand side and using $\downarrow (g \circ h) = \downarrow g \circ \downarrow h$. Analogously to how K_i was defined in the one-directional case for the point $x \in X$, we write $K_i(y)$ for the set of coordinates in y that are not in its n^i-skeleton. Note that σ_i then shifts the coordinates in $K_i(y)$ to the left (jumping over coordinates in $J_i(y)$). Let $g = \sigma_0^{\ell_0} \circ \sigma_1^{\ell_1} \circ \cdots \circ \sigma_{p-1}^{\ell_{p-1}}$.

If r is the radius of h, we take p large enough that $\ell = p$ satisfies Lemma 3.3.22 for $j = 2r + 1$. Choose a point y with $0 \in K_p(y)$ and define a function $\phi : Y \to Y$ where

$$\phi(z)_j = \begin{cases} z_{k-1} & \text{if } j \geq 0 \wedge |K_p(y) \cap [0, j]| = k \wedge j \in K_p(y) \text{ and} \\ z_{-k+1} & \text{if } j \leq 0 \wedge |K_p(y) \cap [j, 0]| = k \wedge j \in K_p(y) \text{ and} \\ y_j & \text{if } j \in J_p(y). \end{cases}$$

that is, $\phi(z)$ is the point where the coordinates $K_p(y)$ of y are replaced by symbols of z in order, so that $\phi(z)_0 = z_0$, and other coordinates are taken from y.

Now, we note that there exists k such that $g(\phi(z))_k = z_0$ for all $z \in Y$. Namely, whatever $z \in Y$ is, it will be shifted in the exact same way, as a subsequence of $\phi(z)$, by all the maps $\sigma_i^{\ell_i}$ for $i < p$, since by definition, σ^i simply shifts the contents of the coordinates $K_i(y) \supset K_p(y)$ to the left, jumping over coordinates in $J_i(y)$.

The equation $\downarrow^p h(\phi(z)) = \phi(h(z))$ holds basically by the definition of the $\downarrow$-operation, as $\downarrow^p h$ applies h to the subsequence of y found in the coordinates $K_p(y)$. Thus,

$$h(\phi(z))_k = (g \circ \downarrow^p h)(\phi(z))_k = g(\phi(h(z)))_k = h(z)_0$$

holds for all $z \in Y$.

Now, we have $t \in K_p(y)$ for at most one $t \in [k - r, k + r]$, by the assumption on p. If there is no such t, then h is a constant map:

$$\forall z \in Y : h(z)_0 = h(\phi(z))_k = h_{\text{loc}}(y_{[k-r,k+r]}).$$

Due to the assumption that X_w supports no symbol maps other than the identity, this is impossible. If there is such t, then we note that, by the definition of ϕ, there exists i such that for all z, $\phi(z)_t = z_i$. Then,

$$\forall z \in Y : h(z)_0 = h(\phi(z))_k = h_{\text{loc}}(y'_{[k-r,t-1]}, z_i, y'_{[t+1,k+r]}),$$

so $h = \sigma^i \circ \pi$ for some symbol map π. Again, by the assumption that X_w has no symbol maps other than the identity, we have that h is a shift map. ■

Theorem 3.3.29 *For every tuple (n, n', m) satisfying (3.6), there exists a two-way Toeplitz subshift whose endomorphism monoid is isomorphic to the group $A(n, m)$.*

Proof. With the standing assumptions and the notation above, we show that the endomorphism monoid of Y is $\langle \sigma_i \mid i \in \mathbb{N} \rangle$, and it is isomorphic to the group $A(n, m)$ by the isomorphism $\sigma_i \mapsto \left(\frac{n}{m}\right)^i$. Note that the σ_i indeed generate an (n, m)-lifting group. Namely, both $\sigma_i \circ \sigma_j = \sigma_j \circ \sigma_i$ and $\sigma_i^n = \sigma_{i+1}^m$ are seen to hold on Y by considering the images of x in these functions (rather, the images of x in their one-way restrictions; note that these maps have one-directional radii).

Given any $f : Y \to Y$, we start iterating Lemma 3.3.26 on f to obtain

$$f = \sigma^{k_1} \circ \downarrow h_1 = \sigma^{k_1} \circ \downarrow (\sigma^{k_2} \circ \downarrow h_2) = \sigma^{k_1} \circ \downarrow (\sigma^{k_2} \circ \downarrow (\sigma^{k_3} \circ \downarrow h_3)) = \cdots,$$

which can be rewritten, using the equality $\downarrow (g \circ h) = \downarrow g \circ \downarrow h$, as

$$f = \sigma_0^{k_1} \circ \downarrow h_1 = \sigma_0^{k_1} \circ \sigma_1^{k_2} \circ \downarrow^2 h_2 = \sigma_0^{k_1} \circ \sigma_1^{k_2} \circ \sigma_2^{k_3} \circ \downarrow^3 h_3 = \cdots.$$

By Lemma 3.3.26, the radii of the h_i eventually decrease below some constant r, and then for some n, we have $h_n = h_{n+p}$ for some $p > 0$.

Then we have

$$h_n = \sigma_0^{k_{n+1}} \circ \sigma_1^{k_{n+2}} \cdots \sigma_{p-1}^{k_{n+p}} \circ \downarrow^p h_n.$$

It follows from Lemma 3.3.28 that h_n is a shift map, and then $f \in \langle \sigma_i \mid i \in \mathbb{N} \rangle$.

Now, we have seen that there are no endomorphisms other than the maps in $\langle \sigma_i \mid i \in \mathbb{N} \rangle$. To see that this group is isomorphic to $A(n, m)$, by Lemma 3.3.19 it is enough to show

$$\sigma_j^{k_j} \circ \sigma_{j+1}^{k_{j+1}} \circ \cdots \circ \sigma_{j'}^{k_{j'}} = 0$$

where $k_j \neq 0$, $k_{j'} \neq 0$ and $k_i \in [-n', n']$ for all i is impossible. But this is again clear from the periodic structure of Y: $\sigma_j^{k_j}$ shifts the jth level of x, and does not change other coordinates. ■

Corollary 3.3.30 *There exists a minimal subshift whose automorphism group is not finitely generated.*

Remark 3.3.31 *It was recently proved in [CK14] that a transitive subshift whose language has a subquadratic growth satisfies that the automorphism group becomes periodic when we quotient out the shift maps, where a group G is* periodic *if*

$$\forall g \in G : \exists n : g^n = 1.$$

It is not hard to check that in the case $w = 10␣0␣$ (so that $n = 5$, $m = 2$), our example X_w has subquadratic growth. Thus, the result of [CK14] should hold, and indeed it does. Namely, the automorphism group we obtained is periodic when the shift maps are quotiented out: the automorphism group of X_w is isomorphic to $A(n, m)$ where the subgroup $\mathbb{Z}$ corresponds to the shift maps. Since the group is abelian, and for the generators $\left(\frac{5}{2}\right)^i$ we have $2^i \left(\frac{5}{2}\right)^i \in \mathbb{Z}$ for all i, the group is of the required form. In particular, this shows that subshifts of the type considered in [CK14] need not have a finitely generated automorphism group.

Chapter 4

Algebraic Subshifts

4.1 Cellular Automata on Algebraic Subshifts

Giving algebraic structure to subshifts is a common topic in the literature. Usually, the structure given is that of a group (or something related). A standard reference for dynamical systems with algebraic structure is [Sch95], and a more symbolic approach can be found for example in [Kit87, BS08]. We are of course mainly interested in the endomorphisms – cellular automata that respect the algebraic structure of the subshift. Cellular automata respecting a group structure have been investigated for example in [ION83, CFMM00, MM98, Sat97, Kar00]. Since the study of group homomorphic cellular automata and group subshifts has proved fruitful, it seems natural to give other algebraic structures to subshifts, and look at their endomorphisms.[1]

Another question studied in multiple sources is the commutation of cellular automata, see for example [Voo93, MB97, CHR79]. Given a cellular automaton f (or a finite set of cellular automata), which other cellular automata commute with it? We can restate this question in algebraic terms in at least two ways. On the one hand, this can be thought of as the study of the centralizer of f in the endomorphism monoid. On the other hand, it can be considered as the study of the endomorphism monoid of the subshift with an algebraic structure given by the unary operator f.

In this chapter, we study these questions. We give subshifts general (though always shift-commuting and continuous) algebraic structures, and the natural self-maps are then the cellular automata that are algebra endomorphisms with respect to this structure. Our main emphasis is on the classical cases of group shifts, and structures given by unary maps, and especially the interplay of such structures. This is the topic of both Section 4.2

[1] Of course, there is a lot to study even in the subshifts with algebra operations themselves, but we only consider endomorphism monoids in this thesis.

and Section 4.3. We also briefly study endomorphisms of subshifts with lattice structure in Section 4.4. Since our goal is to derive simplicity from the algebraic structure, and not the subshift itself, many considerations in this chapter take place on the full shift, with an algebraic structure defined cellwise (that is, we consider the subshift $A^{\mathbb{Z}}$ for a finite algebra A).

We begin with the universal algebraic objects needed in this chapter, and then discuss the general idea of recoding a general algebraic structure to one defined cellwise.

4.1.1 Types, Identities, Varieties and Algebras

Our definitions are condensed, and some even slightly imprecise, see [BS81] for details.

Let $\mathcal{T}$ be a set of pairs (f, n), where f is a symbol and $n \in \mathbb{N}$, with the property that $(f, m), (f, n) \in \mathcal{T} \implies m = n$. Here, f is called a *function symbol*, and n is called the *arity* of f. An *algebra of type* $\mathcal{T}$ is a pair (X, F), where X is a set and for each $(f, n) \in \mathcal{T}$ we have a function $f' : X^n \to X$ in the set F. In this case, we identify f' with f, and the functions f are called *algebra operations*. We usually identify (X, F) with X, if F is clear from the context.

The *terms (of type* $\mathcal{T}$*, over variables* $(a_1, \dots, a_k)$*)* are defined inductively as follows: a_i is a term for all $i \in [1, k]$, and for all $(f, n) \in \mathcal{T}$, if $b_1, \dots, b_n$ are terms, then $f(b_1, \dots, b_n)$ is a term. In particular, if $n = 0$, then $f = f()$ is itself a term. An *identity (of type* $\mathcal{T}$*)* is a pair of terms (b, b'), usually written $b \approx b'$. An algebra X of type $\mathcal{T}$ satisfies an identity $b \approx b'$ of type $\mathcal{T}$ if, whenever elements of X are substituted for the variables in b and b' in any possible way, the equality $b = b'$ holds.

A *variety of type* $\mathcal{T}$ *defined by the set of identities* I is the class of algebras of type $\mathcal{T}$ that satisfy the identities in I. If (X, F) is an algebra and $Y \subset X$ is closed under the operations of X in the sense that $f(Y \times \cdots \times Y) \subset Y$ for all operations $f \in F$, then we call (Y, F) a *subalgebra* of X. If (X, F) is in a variety $\mathcal{F}$, and Y is a subalgebra, then Y is automatically in $\mathcal{F}$ as well. The set of subalgebras of an algebra X is denoted $\mathrm{Sub}(X)$. A function $g : X \to Y$ between two algebras in $\mathcal{F}$ is called an *($\mathcal{F}$-)homomorphism* if $g(f(x_1, \dots, x_n)) = f(g(x_1), \dots, g(x_n))$ for each n-ary operation f. If g is bijective, it is called an *isomorphism*. The *direct product* of an indexed family $(X_i)_{i \in \mathcal{I}}$ of algebras is the algebra $\prod_{i \in \mathcal{I}} X_i$, where the operations are defined cellwise $(f(x^1, \dots, x^n)_i = f(x_i^1, \dots, x_i^n))$. An algebra is *directly indecomposable*, if it is not isomorphic to a product of two nontrivial algebras. All finite algebras are isomorphic to a finite product of directly indecomposable finite algebras. All varieties are closed under subalgebras, homomorphic images and products (and in fact the converse holds).

If $\sim \subset X \times X$ is an equivalence relation that satisfies

$$x_1 \sim y_1, \ldots, x_n \sim y_n \Longrightarrow f(x_1, \ldots, x_n) \sim f(y_1, \ldots, y_n)$$

for all $x_i, y_i \in X$ and all n-ary operations f, we say that $\sim$ is a *congruence* on X. The set of congruences on an algebra X is denoted $\mathrm{Con}(X)$. A natural algebraic structure is induced by the algebra operations on the set of equivalence classes $X/\sim$. The kernel $\ker(g) = \{(x, y) \in X \times X \mid g(x) = g(y)\}$ of a homomorphism g is always a congruence, and $X/\ker(g)$ is isomorphic to $g(X)$ (the last claim is known as the *Homomorphism Theorem*).

The variety of *groups* has type $\{(\cdot, 2), (()^{-1}, 1), (1, 0)\}$, and satisfies the identities

$$x \cdot (y \cdot z) \approx (x \cdot y) \cdot z$$
$$1 \cdot x \approx x \approx 1 \cdot x$$
$$x \cdot x^{-1} \approx 1 \approx x^{-1} \cdot x$$

In the variety of abelian groups, there is an additional identity $x \cdot y \approx y \cdot x$, and the operations are usually renamed so that the type is $\{(+, 2), (-, 1), (0, 0)\}$ (referred to as *additive notation*).

For example, the variety of *lattices* has type $\{(\wedge, 2), (\vee, 2)\}$ and is defined by the identities

$$x \wedge x \approx x, \quad x \wedge y \approx y \wedge x,$$
$$(x \wedge y) \wedge z \approx x \wedge (y \wedge z), \quad x \wedge (x \vee y) \approx x,$$

and the same identities with $\wedge$ and $\vee$ interchanged (their *dual versions*). The operations $\wedge$ and $\vee$ are called *meet* and *join*, respectively. It is known that the variety of lattices coincides with the class of partially ordered sets where all pairs of elements have suprema and infima, where the correspondence is given by $x \wedge y = \inf\{x, y\}$ and $x \vee y = \sup\{x, y\}$. If S is a lattice and $a, b \in S$, then we denote $[a, b] = \{c \in S \mid a \leq c \leq b\}$, where $\leq$ is the partial order of S.

The variety of *distributive lattices* satisfies the lattice identities and the additional identity

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

and its dual version. Of particular interest is the binary lattice $\mathbb{2}$ containing the elements $\{0, 1\}$ with their usual numerical order.

The variety of *Boolean algebras* has type $\{(\wedge, 2), (\vee, 2), (\bar{\cdot}, 1), (1, 0), (0, 0)\}$. A Boolean algebra is a distributive lattice w.r.t. $\wedge$ and $\vee$, and also satisfies

$$x \wedge 0 \approx 0, \quad x \vee 1 \approx 1,$$
$$x \wedge \bar{x} \approx 0, \quad x \vee \bar{x} \approx 1.$$

It is known that every finite Boolean algebra is isomorphic to the algebra of subsets 2^T of some set T where the ordering is given by set inclusion.

4.1.2 Algebraic Subshifts and Recoding

This section is mostly based on [ST12c], and the slightly extended version [ST12d].

Let $\mathcal{F}$ be a variety of algebras of type $\mathcal{T}$. We call $X \subset S^{\mathbb{Z}}$ an *$\mathcal{F}$-subshift*, if it is a subshift and has an algebra structure in $\mathcal{F}$ whose operations are block maps (so that whenever $(f, n) \in \mathcal{T}$, we have a corresponding block map $f : (S^n)^{\mathbb{Z}} \to S^{\mathbb{Z}}$). In particular, every finite $S \in \mathcal{F}$ induces a natural cellwise algebra structure on $S^{\mathbb{Z}}$ by $f(x^1, \dots, x^n)_i = f(x_i^1, \dots, x_i^n)$ for all i, whenever $f : S^n \to S$ is an algebra operation of S (that is, $S^{\mathbb{Z}}$ is taken to be a direct product), and in this case, if $X \subset S^{\mathbb{Z}}$ is a subshift in $\mathrm{Sub}(S^{\mathbb{Z}})$, it is called a *cellwise $\mathcal{F}$-subshift*. A conjugacy that is also an $\mathcal{F}$-homomorphism is called *algebraic*. A cellular automaton with state set S that is also an $\mathcal{F}$-homomorphism is said to be *$\mathcal{F}$-homomorphic* (or simply homomorphic, when the variety is clear from context). When $\mathcal{F}$ is a variety, and X is a subshift in that variety with operations $f_1, \dots, f_m$, we write $\mathrm{End}_{\mathcal{F}}(X)$ or $\mathrm{End}_{\mathcal{F}}(X, f_1, \dots, f_m)$ for its set of $\mathcal{F}$-endomorphisms. We often use this notation without explicitly stating which variety $\mathcal{F}$ is, since it conveys no extra information when the operators are given: $\mathrm{End}_{\mathcal{F}}(X, f_1, \dots, f_m)$ is simply the set of cellular automata g on X satisfying $g(f(x_1, \dots x_n)) = f(g(x_1), \dots, g(x_n))$ whenever $f = f_i$ and f_i has arity n.

Both Section 4.2 and Section 4.3 discuss the interplay between unary operators and group operators, and in particular emphasize the unary operators. In the case where the operators are unary, we can interpret endomorphisms as centralizers in the monoid of cellular automata. Namely, if $f_1, \dots, f_m : X \to X$ are unary CA operators, then $\mathrm{End}(X, f_1, \dots, f_m)$ consists of those cellular automata that commute with f_i for all $i \in [1, m]$. Writing $C_X(f)$ for the *centralizer* of f, that is, the set of cellular automata on X that commute with f, and more generally $C_X(f_1, \dots, f_m) = \bigcap_i C_X(f_i)$, we have

$$\mathrm{End}(X, f_1, \dots, f_m) = C_X(f_1, \dots, f_m).$$

As the subshift X is determined by the types of the CA, we often just write $C(f)$ or $C(f_1, \dots, f_m)$ for centralizers. We use the notation and terminology of centralizers especially in Section 4.3, where the unary operator is an arbitrary extremally permutive cellular automaton, and not really considered an intrinsic operator.

Note that in universal algebra, it is important that the type of a variety contains all the relevant information about it. For example, it is important that the type of a group contains the identity operator as a nullary operator. Namely, the existence of an identity element is not representable as an identity (b, b') of two terms, so that groups do not form a variety unless the identity element is an explicit operator. However, to avoid clutter, we will omit both the nullary identity operator and the unary inverse operator

from the type of groups, and simply write $(X, \cdot)$ or $(X, +)$ to denote a group shift X.

Now, let $\mathcal{F}$ be a variety of algebras. We give a general way to produce subshifts in $\mathcal{F}$ whose operations are not cellwise. For this, begin with a cellwise $\mathcal{F}$-subshift Y and a conjugacy $\phi : X \to Y$, and define

$$f(x_1, \dots, x_n) = \phi^{-1}(f(\phi(x_1), \dots, \phi(x_n)))$$

for all n-ary algebra operations f of $\mathcal{F}$. Clearly, ϕ now becomes an algebraic conjugacy. Not every algebraic subshift arises this way in general, but it turns out that in many well-known varieties $\mathcal{F}$ (such as that of groups, see Corollary 4.1.5), this is the only way to produce subshifts in $\mathcal{F}$. The main theorems in this section address the issue of deciding whether a given $\mathcal{F}$-subshift is algebraically conjugate to some cellwise $\mathcal{F}$-subshift.

Definition 4.1.1 *An* affine map *of an algebra X is inductively defined as either $t(\xi) = \xi$ (the identity map), $t(\xi) = a$ for some $a \in X$ (the constant map) or $t(\xi) = f(a_1, \dots, a_n)$, where f is an n-ary operation, one of the a_i is an affine map and the rest are constants $a_j \in X$. Here, $\xi \notin X$ is used as a variable. To each affine map t we also associate a function* $\mathrm{Eval}(t) : X \to X$ *by replacing ξ with the function argument and evaluating the resulting expression. By a bit of abuse of notation, we also write $t(a) = \mathrm{Eval}(t)(a)$. The set of affine maps of X is denoted by* $\mathrm{Af}(X)$.

Note in particular that each affine map is associated with a *single* algebra. It contains (at most) a single variable, and any amount of constants from the algebra. For example, in the ring $\mathbb{Z}$, the term $t(\xi) = 2{\cdot}(3{+}(\xi{\cdot}(-4)))$ is an affine map, and $\mathrm{Eval}(t)(i) = -8i + 6$ for all $i \in \mathbb{Z}$. An affine map of an $\mathcal{F}$-subshift is a block map if the constants are unary points. In general, it is a non-uniform CA in the class $\mathbf{r}\nu\text{-}\mathcal{CA}$ of [DFP12] (different rule in each cell, but the radii are globally bounded).

The following is a dynamical characterization of $\mathcal{F}$-subshifts that are cellwise up to algebraic conjugacy. The proof uses a common recoding technique found, for example, in the Recoding Construction 4.3.1 of [Kit98].

Theorem 4.1.2 *Let $X \subset S^{\mathbb{Z}}$ be an $\mathcal{F}$-subshift. Then there exists a cellwise $\mathcal{F}$-subshift Y and an algebraic conjugacy $\psi : X \to Y$ if and only if there is an $r \in \mathbb{N}$ such that for all $t \in \mathrm{Af}(X)$, $\mathrm{Eval}(t)(x)_0$ is a function of $x_{[-r,r]}$.*

In dynamical terms, the existence of such r means that the family of affine maps is equicontinuous. In terms of non-uniform cellular automata, it means that the radii of the local rules of the non-uniform CA associated with affine maps are uniformly bounded over all affine maps.

Proof. Suppose first that such an r exists. Then, we can also meaningfully apply an affine map $t \in \mathrm{Af}(X)$ to a word $w \in B_{2r+1}(X)$ by taking an

arbitrary point $x \in X$ with $x_{[-r,r]} = w$, and taking the center cell of $t(x)$. We define the following equivalence relation on $B_{2r+1}(X)$:

$$\forall v, w \in B_{2r+1}(X) : v \sim w \iff \forall t \in \mathrm{Af}(X) : t(v)_0 = t(w)_0 \ .$$

Note that, in particular, $v \sim w \implies v_0 = w_0$, since the identity translation $t(\xi) = \xi$ separates such words. We define an injective block map $\psi : X \to (B_{2r+1}(X)/\sim)^{\mathbb{Z}}$ by $\psi(x)_i = x_{[i-r,i+r]}/\sim$, and denote $Y = \psi(X)$. Restricting the codomain of ψ, we obtain a conjugacy $\psi : X \to Y$.

In order to make the algebra operations commute with ψ, we define

$$f(y_1, \dots, y_n) = \psi(f(\psi^{-1}(y_1), \dots, \psi^{-1}(y_n)))$$

for all n-ary algebra operations f, which is obviously well-defined. Now ψ extends to a bijection between $\mathrm{Af}(X)$ and $\mathrm{Af}(Y)$ in a natural way. Let us show that every algebra operation f is then defined cellwise in Y. Consider two points $y, y' \in Y$ with $y_0 = y'_0$. We need to show that $\psi(t)(y)_0 = \psi(t)(y')_0$ for all $\psi(t) \in \mathrm{Af}(Y)$. Assume the contrary, that $\psi(t)(y)_0 \neq \psi(t)(y')_0$ for some $\psi(t) \in \mathrm{Af}(Y)$. Let $x = \psi^{-1}(y)$ and $x' = \psi^{-1}(y')$. Then also $t(x)_{[-r,r]} = v \not\sim w = t(x')_{[-r,r]}$, and thus there exists $t' \in \mathrm{Af}(X)$ such that $t'(v) \neq t'(w)$. But by the assumption on affine maps, $t'' = t' \circ t$ has radius r. Now we have $t''(x)_0 \neq t''(x')_0$, which is a contradiction, since $x_{[-r,r]} \sim x'_{[-r,r]}$.

For the converse, note that if X is algebraically conjugate to a cellwise $\mathcal{F}$-subshift Y via the conjugacy ψ, then the radius of every affine map is at most the sum of the radii of ψ and ψ^{-1}. ■

We also obtain a sufficient algebraic condition for algebraic conjugacy with a cellwise $\mathcal{F}$-subshift. In the special case of the full shift, this becomes a characterization.

Definition 4.1.3 *We define the* depth *of an affine map as the number of nested algebra operations in it. We say an algebra S is* k-shallow *if for every $t \in \mathrm{Af}(S)$ there exists $t' \in \mathrm{Af}(S)$ of depth at most k such that* $\mathrm{Eval}(t) = \mathrm{Eval}(t')$*. If every algebra in the variety $\mathcal{F}$ is k-shallow, then we say $\mathcal{F}$ is k-shallow.*

For example, the depth of $2 \cdot (3 + (\xi \cdot (-4)))$ is 3 because the depth of $3 + (\xi \cdot (-4))$ is 2 because the depth of $\xi \cdot (-4)$ is 1 because the depth of ξ is 0.

Theorem 4.1.4 *Let $X \subset S^{\mathbb{Z}}$ be an $\mathcal{F}$-subshift. If X is k-shallow, then it is cellwise up to algebraic conjugacy. Conversely, if X is algebraically conjugate to a cellwise $\mathcal{F}$-subshift Y, and either*

- *$Y = R^{\mathbb{Z}}$ where $R \in \mathcal{F}$, or*

- *$\mathcal{F}$ contains only unary operations.*

then X is k-shallow for some k.

Proof. If X is k-shallow, then clearly all affine maps have uniformly bounded radii, and Theorem 4.1.2 gives the result.

For the first item of the other claim, it suffices to show that $R^{\mathbb{Z}}$ is k-shallow for some k. Since R is finite, the set $\Gamma = \{\mathrm{Eval}(t) \mid t \in \mathrm{Af}(R)\}$ is finite. For an affine map $t \in \mathrm{Af}(R^{\mathbb{Z}})$ we denote by t_i the affine map in $\mathrm{Af}(R)$ that t computes in coordinate i, obtained by taking coordinate i from each constant. For each affine map $t \in \mathrm{Af}(R^{\mathbb{Z}})$ we define $\Delta_t = \{\mathrm{Eval}(t_i) \mid i \in \mathbb{Z}\}$. Let $n = |\Gamma|$ and note that since R^n is finite, it is k-shallow for some k.

Let $t \in \mathrm{Af}(R^{\mathbb{Z}})$ and let $j_1, \ldots, j_n$ be coordinates such that for all $h \in \Delta_t$ we have $\mathrm{Eval}(t_{j_i}) = h$ for some i. Construct an affine map $s \in \mathrm{Af}(R^n)$ by $s_i = t_{j_i}$, copying the j_ith coordinate of each constant. Since R^n is k-shallow we find some affine map $s' \in \mathrm{Af}(R^n)$ of depth at most k with $\mathrm{Eval}(s) = \mathrm{Eval}(s')$. We may now define an affine map $t' \in \mathrm{Af}(R^{\mathbb{Z}})$ by $t'_i = s'_{j'_i}$ for all i (again copying constants coordinatewise), where j'_i is such that $\mathrm{Eval}(t_i) = \mathrm{Eval}(s_{j'_i})$. Since $\mathrm{Eval}(s_j) = \mathrm{Eval}(s'_j)$ for all j, we have $\mathrm{Eval}(t) = \mathrm{Eval}(t')$.

For the second item, in the case that $\mathcal{F}$ contains only unary operations, we can repeat the previous argument: we only needed $Y = R^{\mathbb{Z}}$ so that the constants needed for the affine map t' would be in Y. If $\mathcal{F}$ has only unary operations, then no constants are needed. ■

It can be shown that there exists a mixing SFT (in the variety of groupoids) with cellwise defined operations which is not k-shallow for any k. Thus, when the operations are not unary (so that affine maps can actually contain constants), it is hard to find a generalization beyond full shifts.

In the corollary below, we list varieties where Theorem 4.1.4 applies. To add a bit of color, we include heaps (groups without identity elements) in our list. A heap has type $\{([\cdot,\cdot,\cdot], 3)\}$, and satisfies the identities

$$[a, a, b] \approx b \approx [b, a, a]$$

$$[[a, b, c], d, e] \approx [a, [d, c, b], e] \approx [a, b, [c, d, e]]$$

Corollary 4.1.5 *Up to algebraic conjugacy, every distributive lattice, Boolean algebra, ring, semigroup, monoid, group and heap subshift is defined cellwise.*

Proof. By finding suitable normal forms, one easily sees that the varieties of distributive lattices, semigroups and monoids are 2-shallow, while the varieties of Boolean algebras, groups and rings are 3-shallow. We list the deepest possible normal forms below.

- Distributive lattices: $a \vee (b \wedge \xi)$.

- Semigroups and monoids: $a \cdot (\xi \cdot b)$.
- Heaps: $[a, [b, \xi, c], d]$.
- Boolean algebras: $a \vee (b \wedge \xi^c)$.
- Groups: $a \cdot ((\xi)^{-1} \cdot b)$.
- Rings: $a + b \cdot (\xi \cdot c)$.

These normal forms are well-known in all cases, except perhaps for heaps, where the normal form easily follows from the identity

$$[a, [b, [c, \xi, d], e], f] \approx [[a, e, c], \xi, [d, b, f]].$$

■

The recodability of groups is well-known [Kit87], but to our knowledge, the others (possibly excepting rings) have not appeared in the literature. The recodability of quasigroup shifts is discussed in at least [ST12d] and [Sob07]. In [ST12d], we show that not all quasigroup shifts can be recoded to cellwise ones, and [Sob07] shows that this is doable if the quasigroup satisfies some additional identities. An example of a lattice subshift which is not recodable to be cellwise is also given in [ST12d].

Once we have recoded to a cellwise algebraic subshift, homomorphisms are easy to describe. Note that if R is an algebra and $X \subset R^{\mathbb{Z}}$ is an $\mathcal{F}$-subshift, then $\mathcal{B}_n(X)$ is a subalgebra of R^n for all n.

Lemma 4.1.6 *Let $R \in \mathcal{F}$, and let $X \subset R^{\mathbb{Z}}$ be a subshift. A CA $f : X \to X$ with radius r is an $\mathcal{F}$-homomorphic if and only if $f_{\mathrm{loc}} : \mathcal{B}_{2r+1}(X) \to R$ is an $\mathcal{F}$-homomorphism.*

Proof. Let g be an n-ary algebra operation on R, and denote the corresponding operators on R^n and $R^{\mathbb{Z}}$ by g as well.

Assume first that f is $\mathcal{F}$-homomorphic. Let $w_i \in \mathcal{B}_{2r+1}(X)$ for all $i \in [1, n]$, and let $s \in S$ be arbitrary. Let $x^i \in X$ be arbitrary points such that $x^i_{[-r,r]} = w_i$. Then

$$f(g(x^1, \ldots, x^n))_0 = g(f(x^1)_0, \ldots, f(x^n)_0),$$

so in particular

$$f_{\mathrm{loc}}(g(w_1, \ldots, w_n)) = g(f_{\mathrm{loc}}(w_1), \ldots, f_{\mathrm{loc}}(w_n)).$$

Thus, g is an $\mathcal{F}$-homomorphism.

On the other hand, if the local function f_{loc} is an $\mathcal{F}$-homomorphism, consider arbitrary points $x^1, \dots, x^n \in X$. We have

$$\begin{aligned} f(g(x^1, \dots, x^n))_i &= f_{\mathrm{loc}}(g(x^1_{[i-r,i+r]}, \dots, x^n_{[i-r,i+r]})) \\ &= g(f_{\mathrm{loc}}(x^1_{[i-r,i+r]}), \dots, f_{\mathrm{loc}}(x^n_{[i-r,i+r]})) \\ &= g(f(x^1)_i, \dots, f(x^n)_i) \end{aligned}$$

for all $i \in \mathbb{Z}$, which implies that f is $\mathcal{F}$-homomorphic. ■

As we mentioned in the beginning of this section, we mostly restrict to subshifts $A^{\mathbb{Z}}$ for finite algebras A in the rest of this chapter. This may seem harmless, and it is a common choice when studying, say, group homomorphic cellular automata. However, in fact there are good reasons to look a bit further, at the general case of mixing SFTs.

It is true in general that while results about cellular automata often have the nicest possible description in the case of the full shift, one can argue that the 'right' playground for cellular automata is actually the class of mixing SFTs. This is, for example, the content of the sermon part of the 'Introduction and sermon' section of [BK99]. For me, the primary reasons for this opinion are twofold. First, mixing SFTs have a beautiful theory, whereas full shifts are only interesting in combination with cellular automata. Second, almost every result about cellular automata generalizes, in some way, to mixing SFTs, and in general there is little dynamical difference between a full shift and a mixing SFT (especially if there is a unary point), so that once you are familiar with mixing SFTs, full shifts seem like a rather sparse subset of examples.

However, there are of course also practical reasons to study cellular automata on general mixing SFTs. Namely, recoding. The results of this section are a case in point. Suppose $\mathcal{F}$ is a variety where recoding of operations to cellwise ones is doable in general (such as those in Corollary 4.1.5). In such a case, studying mixing SFTs with cellwise algebra operations in $\mathcal{F}$ means that we are studying mixing SFTs with *arbitrary* (shift-commuting and continuous) algebra operations in $\mathcal{F}$, which is, for a mathematician, quite satisfying a class to study. This is of course because the class of mixing SFTs is closed under conjugacy. On the other hand, if we study only full shifts with cellwise algebra operations (that is, $A^{\mathbb{Z}}$ for $A \in \mathcal{F}$), then we are not even studying all questions about full shifts, as full shifts with general algebra operations are not usually recodable to another full shift with cellwise algebra operations. We obtain such general results in Section 4.2, but unfortunately, the results in both Section 4.3 and Section 4.4 seem hard to generalize beyond full shifts.

4.1.3 Cellular Automata on Group Shifts

In this section, we make a few (probably well-known) remarks about concrete representations of self-maps of group shifts. Namely, in the case of full group shifts $G^{\mathbb{Z}}$, we can say much more than Lemma 4.1.6. We use additive notation, as only the abelian case is interesting in most of the applications of the following lemmas.

Lemma 4.1.7 *Let G be a finite (not necessarily abelian) group and let $f : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ be a homomorphic CA with neighborhood $N = [-r, r]$. For all $i \in N$, there exists a group endomorphism $f_i : G \to G$ such that*

- *$f_i(g) + f_j(h) = f_j(h) + f_i(g)$ whenever $h, g \in G$ and $i \neq j \in N$, and*
- *$f_{\mathrm{loc}}(g_{-r}, \dots, g_r) = f_{-r}(g_{-r}) + \cdots + f_r(g_r)$ for $g_{-r}, \dots, g_r \in G$.*

Note that the order of summation in the above formula for f_{loc} is irrelevant by the first item.

Proof. For all $i \in N$, define the function $f_i : G \to G$ by

$$f_i(g) = f_{\mathrm{loc}}(\underbrace{0, \dots, 0}_{i+r}, g, \underbrace{0, \dots, 0}_{r-i}),$$

and note that this is an endomorphism of G. Let $i < j \in N$ and $g, h \in G$. Since f_{loc} is a homomorphism, we have

$$\begin{aligned} f_i(g) + f_j(h) &= f_{\mathrm{loc}}(0, \dots, g, \dots, 0, \dots, 0) + f_{\mathrm{loc}}(0, \dots, 0, \dots, h, \dots, 0) \\ &= f_{\mathrm{loc}}(0, \dots, g, \dots, h, \dots, 0) \\ &= f_{\mathrm{loc}}(0, \dots, 0, \dots, h, \dots, 0) + f_{\mathrm{loc}}(0, \dots, g, \dots, 0, \dots, 0) \\ &= f_j(h) + f_i(g), \end{aligned}$$

and for all $g_{-r}, \dots, g_r \in G$,

$$\begin{aligned} f_{\mathrm{loc}}(g_{-r}, \dots, g_r) &= \sum_{i=-r}^{r} f_{\mathrm{loc}}(\underbrace{0, \dots, 0}_{i+r}, g_i, \underbrace{0, \dots, 0}_{r-i}) \\ &= f_{-r}(g_{-r}) + \cdots + f_r(g_r). \end{aligned}$$

This concludes the proof. ■

We call the endomorphisms f_i the *symbol endomorphisms of f*. In the case of an abelian group G, a CA $f : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ is called a *sum of shifts* if $f = \sum_{i \in N} k_i \cdot \sigma^i$ for a finite set $N \subset \mathbb{Z}$, and $k_i \in \mathbb{N}$, where the sum is taken pointwise, and $k_i \cdot \sigma^i = \sigma^i + \cdots + \sigma^i$. In terms of symbol endomorphisms, this means $f_i(g) = k_i g$. If we can take $k_i = 1$ for all i, then f is called a *sum of distinct shifts*, and this means that the symbol endomorphisms are identity maps.

Lemma 4.1.8 *Suppose that G is a finite abelian group with decomposition $G = \prod_{i=1}^{m} \mathbb{Z}_{p_i^{m_i}}$, where the p_i are prime numbers and $m_i \geq 1$. Then every homomorphic cellular automaton on $G^{\mathbb{Z}}$ is a sum of shifts if and only if the primes p_i are distinct.*

Proof. It is easy to find a homomorphic cellular automaton which is not a sum of shifts if the primes are not distinct. Namely, if $p_i = p_j$ and $k_i \geq k_j$, then the symbol map

$$(a_1, \ldots, a_i, \ldots, a_j, \ldots, a_m) \mapsto (a_1, \ldots, a_i + a_j p^{k_i - k_j}, \ldots, a_j, \ldots, a_m)$$

provides such an example.

For the other direction, first suppose $m = 1$. Then, since $\mathbb{Z}_{p_i^{m_i}}$ is cyclic, it is clear symbol endomorphisms are maps of the form $g \mapsto g \cdot k$ for constant k, so that f is a sums of shifts.

Now, suppose $m > 1$ and the primes p_i are distinct, and let $f : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$. We will give an algebraic way to zero a single track without affecting the others. More precisely, in the terminology of [BS81], we construct a term R_i over the term algebra of groups type with one variable ξ such that the corresponding term function $R_i^G : G \to G$ maps

$$(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_m) \mapsto (0, \ldots, 0, a_i, 0, \ldots, 0).$$

Constructing such a term is a matter of noting that by the Chinese Remainder Theorem, there exists k_i such that $k_i \equiv 1 \bmod p_i^{m_i}$ and $k_i \equiv 0 \bmod p_j^{m_j}$ for $j \neq i$. Then $R_i = \xi + \cdots + \xi = k_i \cdot \xi$ has the desired property.

We extend the terms R_i to points of $G^{\mathbb{Z}}$ in the usual way, and observe that $f(R_i(x)) = R_i(f(x))$ (see, for example, Theorem 10.3. (b) in [BS81]), so that the tracks corresponding to distinct primes are independent. Combining this and the observation in the case $m = 1$, we obtain that f is a sum of *partial* shifts σ_i which map the track corresponding to the prime p_i one step to the left. Of course, $k_i \cdot \sigma = \sigma_i$, which concludes the proof. ∎

Thus, in general every group homomorphic CA on a full group shift is a *sum of shifted symbol endomorphisms*, and by Lemma 4.1.8, for certain abelian groups, the endomorphisms can be taken to be identity maps. Note that the fact that the images of distinct symbol endomorphisms commute means that, even in the non-abelian case, the local rule of a homomorphic cellular automaton first projects its inputs to subgroups of G which commute with each other, and then multiplies them together. In particular, we have the following.

Lemma 4.1.9 *Let G be a group and let the CA $f : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ be homomorphic. If at least two of the symbol endomorphisms of f are surjective, then G is abelian.*

Finally, in Section 4.3, we will need cellular automata which are homomorphic up to the addition of a constant:

Definition 4.1.10 *Let $(G,+)$ be an abelian group. Then a function $f : G \to G$ is* homomorphic plus a constant*, or* homomorphic+C *if there exist $a \in G$ and a group endomorphism g of $(G,+)$ such that $f(x) = g(x) + a$ for all $x \in G$.*

Of course, we usually apply this definition to cellular automata. It is easy to see that if G is a finite abelian group and $f : G^{\mathbb{Z}} \to G^{\mathbb{Z}}$ is homomorphic+C, then the constant $a \in G^{\mathbb{Z}}$ in the definition is a unary point, since $f(0^{\mathbb{Z}}) = a$.

In the case of abelian groups (especially $\mathbb{Z}_p$), it would make a lot of sense to call homomorphic CA 'linear' and maps that are homomorphic plus a constant 'affine'. However, we have already reserved the latter term for something more general in Definition 4.1.1, and the first term has quite many definitions in the literature; we have tried to choose our definitions to be as unambiguous as possible.

We now give an easy alternative characterization of maps that are homomorphic plus a constant.

Lemma 4.1.11 *Let G, H be abelian groups, and let $g : G \to H$ be such that $g(a+b-c) = g(a) + g(b) - d$ holds for some $c \in G$ and $d \in H$, and all $a, b \in G$. Then, $g(a) = h(a) - g(2c) + 2d$ for a homomorphism $h : G \to H$. In particular, g is homomorphic plus a constant.*

Proof. We have

$$\begin{aligned} g(a+b) &= g(a + (b+c) - c) \\ &= g(a) + g(b+c) - d \\ &= g(a) + g(b + 2c - c) - d \\ &= g(a) + g(b) + g(2c) - 2d. \end{aligned}$$

Denote $e = g(2c) - 2d$, and let $h(a) = g(a) + e$. Then

$$\begin{aligned} h(a+b) &= g(a+b) + e \\ &= g(a) + g(b) + 2e \\ &= h(a) + h(b), \end{aligned}$$

so h is a homomorphism and g is homomorphic+C. ■

4.2 Subshifts with Equicontinuous Unary Operators

This section is based on [ST13b].

In this section (and the next one) we discuss subshifts with algebraic structure given by a single cellular automaton, or a finite family of cellular automata. We think of these cellular automata as unary algebra operations, so that the natural endomorphisms have to commute with the operations. As the commutation of cellular automata is a complicated problem, we make some simplifying assumptions. Namely, in this section, we require that the family of operations buildable from the cellular automata is equicontinuous, in the following sense:

Definition 4.2.1 *Let X be a subshift and let $F = \{f_1, \dots, f_k\} \subset \mathrm{End}(X)$. A point $x \in X$ is called an* equicontinuity point for F *if for all $\epsilon > 0$, there exists $\delta > 0$ such that*

$$\forall f \in F^*, y \in X : d(x, y) < \delta \implies d(f(x), f(y)) < \epsilon. \tag{4.1}$$

If every point $x \in X$ is an equicontinuity point for F, then we say F is equicontinuous. *We say F is reversible if every cellular automaton f_i is bijective.*

The main results of this section are that mixing SFTs with equicontinuous reversible unary operators have complicated endomorphism monoids, but when the operations are not reversible, or there is additional algebraic structure, the endomorphism monoid may contain only the shift maps.

In the case of unary operations, as a corollary of Theorem 4.1.4, we obtain that equicontinuity is equivalent to recodability of the operations to symbol maps, and further equivalent to there being only finitely many distinct affine maps.

Corollary 4.2.2 (of Theorem 4.1.4) *Let X be a mixing SFT with algebraic structure given by unary operations $F = \{f_1, \dots, f_k\}$. Then the following are equivalent:*

- *F is equicontinuous.*
- *X is algebraically conjugate to a subshift Y with algebraic structure given by symbol maps $g_1, \dots, g_k$.*
- *F^* is finite.*

By Corollary 4.2.2, the study of endomorphisms of subshifts with algebraic structure given by equicontinuous families of unary operators is just

the study of cellular automata that commute with symbol maps. It is thus this class that we focus on.

We begin with the case of *bijective* equicontinuous unary operations. In Section 4.2.1, we define the combinatorial notion of color blindness. This is the notion of cellular automata that commute with all symbol permutations. We begin our study on the full shift. In Section 4.2.2, we show that color blindness, on its own, is not sufficient to guarantee that the endomorphism monoid is simple, by constructing an intrinsically universal color blind cellular automaton. We also show that the endomorphism monoid is far from sparse – it has full density. In Theorem 4.2.23, we show that this happens in general, in the sense that *no* structure given by a reversible equicontinuous family of unary maps on a mixing SFT prevents the existence of an intrinsically universal endomorphism.

In Section 4.2.3, we relax the assumption of reversibility, and the picture changes drastically. Here, our main result is that the full shift $\{0,1,2\}^{\mathbb{Z}}$ with algebraic structure given by the set of all symbol maps has *no* endomorphisms other than the shift maps. We prove this by reducing it to the obvious fact that a finite set supports no non-principal ultrafilters (and in fact obtain a general characterization of ultrafilters). We also see that the structure given by symbol maps on $\{0,1\}^{\mathbb{Z}}$ is not enough to prevent a rich endomorphism monoid.

In Section 4.2.4, we look at subshifts with group structure and a structure by unary maps simultaneously. More concretely, we consider the color blind endomorphisms of full shifts will cellwise group operations. The results are similar to those of Section 4.2.3: if the alphabet (and thus the group) is small, there exist interesting color blind endomorphisms, but if the group is large, then all endomorphisms are shift maps. The (nontrivial) small groups are precisely the groups $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_2^2$.

4.2.1 Color Blind Cellular Automata

We begin with the definition and discussion of a purely combinatorial object: the color blind cellular automaton. Color-blind cellular automata are endomorphisms of subshifts where the equicontinuous family of unary maps is given by symbol permutations. By Corollary 4.2.2, such cellular automata are representative of general reversible equicontinuous families of unary operations.

Recall that a symbol map $\pi \in S^S$ is also applied to points $x \in S^{\mathbb{Z}}$ by $\pi(x)_i = \pi(x_i)$, and we also apply them to words (with the same formula).

Definition 4.2.3 *Let $\Pi \subset S^S$ be a set of symbol maps. A cellular automaton $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ satisfying $\pi \circ f = f \circ \pi$ for all $\pi \in \Pi$ is called* Π-blind. *If Π contains precisely the symbol permutations, we say f is* color blind, *and if $\Pi = S^S$, we say f is* typhlotic.

In other words, Π-blind cellular automata are exactly the endomorphisms of $S^{\mathbb{Z}}$ with algebraic structure given by the symbol maps Π. Alternatively, the set of Π-blind cellular automata on $S^{\mathbb{Z}}$ is exactly the centralizer of Π in the monoid of all cellular automata on $S^{\mathbb{Z}}$ with respect to composition. A concrete characterization is that the set of spacetime diagrams of a Π-blind CA is closed under cellwise applications of elements of Π, and in particular, in a spacetime diagram of a color blind cellular automaton, the colors can be renamed in any way. We use the somewhat obscure term typhlotic, meaning blind, to avoid cluttering the global namespace of cellular automata: we will soon see that these automata are rather trivial (Theorem 4.2.31).

Example 4.2.4 *The radius-1 cellular automaton f on $\{0,1,2\}^{\mathbb{Z}}$ defined by*

$$f_{\text{loc}}(a,b,c) = \begin{cases} c, & \text{if } a = b \neq c, \\ a, & \text{if } a \neq b = c, \\ b, & \text{otherwise} \end{cases}$$

is clearly color blind. It always chooses the symbol in its neighborhood that is in the minority, or acts as the identity CA if such a symbol does not exist. A portion of a spacetime diagram of f is shown in Figure 4.1.

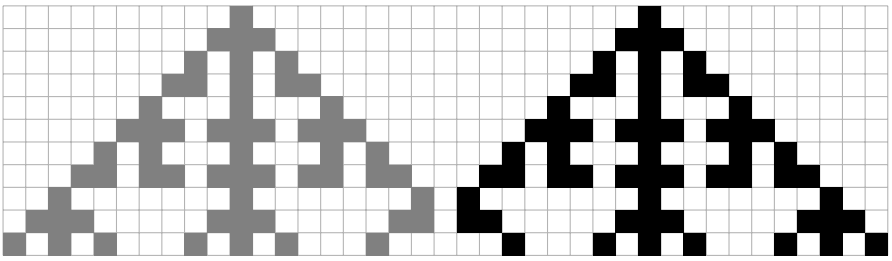


Figure 4.1: A sample spacetime diagram of the cellular automaton of Example 4.2.4, with time advancing downward. It is of course unimportant which of the symbols $\{0,1,2\}$ each color corresponds to, since any symbol permutation of a spacetime diagram of a color blind CA is also its spacetime diagram.

Recall that a cellular automaton f on $S^{\mathbb{Z}}$ is called *captive* if the local rule f_{loc} satisfies $f_{\text{loc}}(a_1,\ldots,a_n) \in \{a_1,\ldots,a_n\}$ for all $a_1,\ldots,a_n \in S$. Color blind CA are 'almost captive' in the following sense.

Lemma 4.2.5 *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a color blind CA. Then $f_{\text{loc}}(a_1,\ldots,a_n) \in \{a_1,\ldots,a_n\}$ whenever $|\{a_1,\ldots,a_n\}| < |S| - 1$.*

Proof. Suppose for a contradiction that we have $|\{a_1, \ldots, a_n\}| < |S|-1$, but $a = f_{\text{loc}}(a_1, \ldots, a_n) \notin \{a_1, \ldots, a_n\}$. Then, there exists

$$b \in S \setminus \{a, a_1, \ldots, a_n\}.$$

Now, f does not commute with the transposition $(a\ b)$. ■

The automaton of Example 4.2.4 is captive. However, not all color blind automata are captive, since the local rule may output the 'last remaining color' unambiguously when all but one color appear in the neighborhood, as the alphabet size is known. The following is an example of this phenomenon.

Example 4.2.6 *The radius-1 cellular automaton f on $\{0,1,2\}^{\mathbb{Z}}$ defined by*

$$f_{\text{loc}}(a,b,c) = \begin{cases} d, & \text{if } |\{a,b,c\}| = 2 \text{ and } d \notin \{a,b,c\}, \\ b, & \text{otherwise} \end{cases}$$

is color blind. It always chooses the unique symbol that does not appear in its neighborhood, or acts as the identity CA if such a symbol does not exist. It is clearly not captive. A portion of a spacetime diagram of f is shown in Figure 4.2.

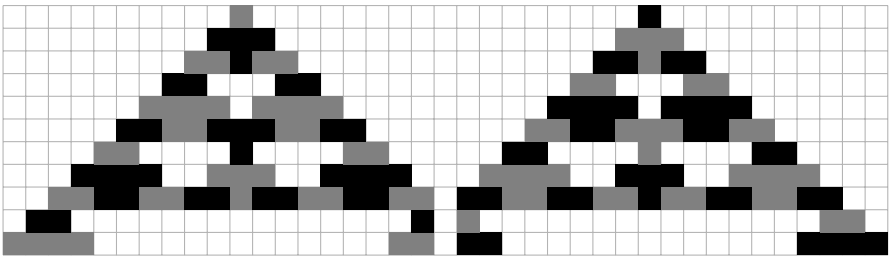


Figure 4.2: A sample spacetime diagram of the non-captive cellular automaton of Example 4.2.6.

Typhlotic CA are in fact captive, which we will obtain as a corollary of Theorem 4.2.31. We continue with a simple logical characterization of color blind cellular automata which gives yet another way to define this class.

Definition 4.2.7 *Fix a set of variables $V = \{v_1, \ldots, v_n\}$. A* color blind formula over V *is a Boolean combination of basic equations of the form $v_i = v_j$. For a color blind formula E over V, an alphabet S and a word $w \in S^n$, we denote by $E(w)$ the formula obtained by replacing each v_i by w_i in E (so that $E(w)$ is formula on the letters w_i, with no free variables). The formula E defines a set of words $E(S) \subset S^n$ by $E(S) = \{w \in S^n \mid E(w) \text{ holds}\}$. We say E is* captive on S *if the last letter of w occurs at least twice in w for all*

$w \in E(S)$, *and* captive, *if it is captive on* S *for all finite* S. *If* $n = 2r + 2$ *and* $E(S)$ *defines a function from* S^{2r+1} *to* S *(seen as a subset of* $S^{2r+1} \times S$*), we let* $f_E^S : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ *be the radius* r *cellular automaton whose local function it is. We say* f_E^S *is* defined by a color blind formula.

Lemma 4.2.8 *A set of words* $W \subset S^n$ *is defined by a color blind formula if and only if it is closed under symbol permutations.*

Proof. First, let $W = E(S)$ for a formula E, and consider an arbitrary symbol permutation $\pi : S \to S$. It is clear that if $E(w)$ holds for a word $w \in S^n$, then so does $E(\pi(w))$, and thus W is closed under symbol permutations.

Suppose then that W is closed under symbol permutations. For all $w \in W$, define the formula $E_w = \bigwedge_{i,j \in [0,n-1]} t(i,j)$, where $t(i,j)$ is $v_i = v_j$ if $w_i = w_j$, and $\neg(v_i = v_j)$ otherwise. We let $E = \bigvee_{w \in W} E_w$. Now, it is clear that $W \subset E(S)$. On the other hand, let $v \in E(S)$. This means that $v \in E_w(S)$ for some $w \in W$. It is easy to see that there then exists a symbol permutation $\pi : S \to S$ with $\pi(w) = v$, and since W is closed under symbol permutations, we have $v \in W$. ■

As a cellular automaton commutes with symbol permutations if and only if its local rule does (by Lemma 4.1.6), we obtain the following corollary.

Corollary 4.2.9 *A CA* $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ *is (captive and) color blind if and only if it is defined by a (captive and) color blind formula.*

Example 4.2.10 *The cellular automaton of Example 4.2.4 is defined by the captive and color blind equation*

$$(v_1 = v_2 \neq v_3 \wedge v_3 = v_4) \vee (v_1 \neq v_2 = v_3 \wedge v_1 = v_4) \vee$$

$$(v_1 = v_2 = v_3 = v_4) \vee (v_1 \neq v_2 \neq v_3 \neq v_1 \wedge v_2 = v_4)$$

where v_1, v_2, v_3 *and* v_4 *correspond to* a, b, c *and* $f_{\mathrm{loc}}(a,b,c)$ *in the definition, respectively.*

The characterization essentially says that a cellular automaton is color blind if and only if it can be defined without referring to any particular colors, but only their arrangements on the neighborhood.

Corollary 4.2.11 *Let* $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ *be a captive and color blind CA such that* $|S| > 2r+1$ *where* r *is the radius of* f, *and let* $S \subset T$. *Then there exists a captive and color blind CA* $g : T^{\mathbb{Z}} \to T^{\mathbb{Z}}$ *with radius* r *such that* $f = g|_{S^{\mathbb{Z}}}$, *and there is no other such extension of radius* r.

Proof. Let E be a color blind equation such that $f = f_E^S$, that is, $E(S)$ defines precisely the local function of f. Since $|S| > 2r+1$ and f is captive, it is easy to see that $E(T)$ also defines a function, since exactly the same set of equivalences between the $2r+2$ variables can occur no matter which alphabet of size at least $2r+2$ is used. We then have that $g = f_E^T$ is a color blind CA on $T^{\mathbb{Z}}$. Uniqueness is also easy to verify. ■

Remark 4.2.12 *An interesting further corollary of Corollary 4.2.11 is that since captive and color blind CA with small enough radii have natural extensions to all full shifts, we, in some sense, obtain a cellular automaton on $\mathbb{N}^{\mathbb{Z}}$ in the limit, when we consider such extensions for larger and larger alphabets $[0, k]$. More precisely, we obtain a function $\mathbb{N}^{\mathbb{Z}}$ defined by*

$$f_E^{\mathbb{N}}(x)_i = f_E^{\mathcal{B}_1(x_{[i-r,i+r]})}(x)_i,$$

where $\mathcal{B}_1(w)$ is the set of symbols that occur in w. Note that the choice of the infinite set $\mathbb{N}$ is immaterial due to color blindness (and it can even be taken to be uncountable). Let $\mathcal{C}$ be the class of such maps, and note that they are closed under composition. The class $\mathcal{C}$ is very much incomparable with class of sand automata introduced in [CF03] (even if we choose $\mathbb{Z}$ or $\mathbb{Z} \cup \{-\infty, \infty\}$ as the state set). Finding out what the dynamics of automata in $\mathcal{C}$ can look like is a possible direction for future research.

We generalize the idea of extending a color blind CA to a larger subshift in Proposition 4.2.16. To prove it, we need a few definitions and a standard topological lemma.

Lemma 4.2.13 (Pasting Lemma) *Let X and Y be topological spaces, let $A_1, \ldots, A_k \subset X$ be closed, such that $\bigcup_i A_i = X$, and let $f : X \to Y$ be a function. If $f|_{A_i}$ is continuous for all i, then so is f.*

Definition 4.2.14 *Let $X \subset S^{\mathbb{Z}}$ be a subshift, let $f : X \to X$ be a CA, and let $\Pi \subset S^S$. Suppose that whenever $\pi \in \Pi^*$ and $x \in X$ satisfy $\pi(x) \in X$, then $\pi(f(x)) = f(\pi(x))$. Then we say f is* Π-blind on X. *If there exists $r \in \mathbb{N}$ such that for all $x \in X$ there exists $k \in [-r, r]$ such that $f(x)_0 = x_k$, we say f is* captive on X.

We note a small subtlety in the definition:

Example 4.2.15 *Let $S = \{0, 1, 2\}$ and $X = \{0, 1\}^{\mathbb{Z}}$. Then the symbol permutation $f = (0\ 1)$ is not Π-blind on X where Π is the set of all symbol permutations $\pi : S \to S$ (although it is clearly color blind on X in the sense of the earlier definition). Namely, if $\pi = (1\ 2)$, then $\pi(^\infty 0^\infty) = {}^\infty 0^\infty \in X$, but $f(\pi(^\infty 0^\infty)) = {}^\infty 1^\infty \neq {}^\infty 2^\infty = \pi(f(^\infty 0^\infty))$.*

Another important observation is that if $\pi(X) \cap X = \emptyset$ for all $\pi \in \Pi^*$, then every cellular automaton on X is Π-blind. Definition 4.2.14 is the correct one if we want it to correspond to f being a restriction of a Π-blind cellular automaton on $S^{\mathbb{Z}}$. The following extension result shows this and more.

Proposition 4.2.16 *Let $X \subset S^{\mathbb{Z}}$ be a subshift, and let Π be a set of permutations on S. Then a CA $f : X \to X$ is (captive and) Π-blind on X if and only if $f = g|_X$ for a (captive and) Π-blind CA $g : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ which satisfies $g(X) \subset X$.*

Proof. First, if $f = g|_X$ for such a $g : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$, and $\pi \in \Pi^*$ is arbitrary, then $\pi(g(x)) = g(\pi(x))$ for all $x \in S^{\mathbb{Z}}$, so in particular this is the case when $x, \pi(x) \in X$, and then $\pi(f(x)) = f(\pi(x))$. In this case f is also clearly captive on X, if g is captive.

For the other direction, we first claim that X can be assumed to be closed under the action of Π^*. Namely, replace X by $\hat{X} = \bigcup_{\pi \in \Pi^*} \pi(X)$, which as a finite union of subshifts is a subshift, and for all $\pi \in \Pi^*$, define $f_\pi : \pi(X) \to \pi(X)$ by $f_\pi(\pi(x)) = \pi(f(x))$. Now, if $x \in \pi(X) \cup \rho(X)$ for $\rho \in \Pi^*$, then $x = \pi(y) = \rho(z)$ for some $y, z \in X$. Since Π^* is a subgroup of the symmetric group on S, we have $\rho^{-1} \circ \pi \in \Pi^*$, and also $\rho^{-1}(\pi(y)) = z \in X$. Since f is Π-blind, this implies $f(z) = f(\rho^{-1}(\pi(y))) = \rho^{-1}(\pi(f(y)))$, that is,

$$f_\rho(x) = f_\rho(\rho(z)) = \rho(f(z)) = \pi(f(y)) = f_\pi(\pi(y)) = f_\pi(x).$$

By the Pasting Lemma, the well-defined function $\hat{f} : \hat{X} \to \hat{X}$ such that $\hat{f}|_{\pi(X)} = f_\pi$ for all $\pi \in \Pi^*$ is continuous, and it is easily seen to be shift-commuting. It is also Π-blind by definition, and clearly captive if f is.

Suppose thus that X is closed under Π^*, and let $r \in \mathbb{N}$ be a radius for f that also witnesses its captivity, if f is captive. Define the radius-r CA $g : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ by the local rule

$$g_{\mathrm{loc}}(w) = \begin{cases} f_{\mathrm{loc}}(w), & \text{if } w \in \mathcal{B}_{2r+1}(X) \\ w_r, & \text{otherwise.} \end{cases}$$

It is clear that $g|_X = f$ (and thus $g(X) \subset X$) and that g is captive if f is. It remains to be shown that g is Π-blind, and for that, let $\pi \in \Pi^*$ and $x \in S^{\mathbb{Z}}$ be arbitrary, and let $i \in \mathbb{Z}$. We now have $x_{[i-r,i+r]} \in \mathcal{B}_{2r+1}(X)$ if and only if $\pi(x_{[i-r,i+r]}) \in \mathcal{B}_{2r+1}(X)$. If $x_{[i-r,i+r]} \in \mathcal{B}_{2r+1}(X)$, then

$$g(\pi(x))_i = f_{\mathrm{loc}}(\pi(x_{[i-r,i+r]})) = \pi(f_{\mathrm{loc}}(x_{[i-r,i+r]})) = \pi(g(x))_i.$$

If $x_{[i-r,i+r]} \notin \mathcal{B}_{2r+1}(X)$, we have $g(\pi(x))_i = \pi(x)_i = \pi(g(x))_i$. This shows that g is Π-blind. ∎

From this and Corollary 4.2.9 we deduce the following.

Corollary 4.2.17 *Let $X \subset S^{\mathbb{Z}}$ be a subshift. Then a CA $f : X \to X$ is (captive and) color blind on X if and only if $f = f_E^S|_X$ for a (captive) color blind formula E.*

The restriction to sets of symbol permutations (and not general symbol maps) is necessary, as an easy corollary of Theorem 4.2.31.

We also show by example that the radius of f may not be sufficient to define g even if it witnesses the captivity of f on X. Let X consist of the points $x = (0122)^{\mathbb{Z}}$ and $y = (0022)^{\mathbb{Z}}$ and their shifts, and define $f_{\mathrm{loc}} : \{0,1,2\}^3 \to \{0,1,2\}$ by $f_{\mathrm{loc}}(a,b,c) = b$, except for $f_{\mathrm{loc}}(0,1,2) = 0$. Now, f is captive and color blind on X (the only symbol permutation we need to check is (0 2)). However, no color blind cellular automaton on $\{0,1,2\}^{\mathbb{Z}}$ with radius 1 is an extension of f, since $f_{\mathrm{loc}}(012) = 0 = f_{\mathrm{loc}}(201)$. One can check that the neighborhood $N = [-1,2]$ suffices though.

After Proposition 4.2.16 has been established, a natural question arises: if we have a sufficiently 'well-behaved' subshift $Y \subset S^{\mathbb{Z}}$ that contains X, is it possible to extend f to a CA $g : Y \to Y$ which is Π-blind on Y? The following example shows that assuming Y to be a mixing SFT with window size 2 closed under Π is not sufficient.

Example 4.2.18 *Let $S = \{0,1,\#,a,b,c,d\}$ and $X = \{{}^{\infty}0^{\infty}, {}^{\infty}1^{\infty}\}$, and define the mixing SFT $Y \subset S^{\mathbb{Z}}$ by forbidding all words of length 2 except the set*

$$\{00, 11, \#\#, 0a, 0b, 1c, 1d, a\#, b\#, c\#, d\#, \#0, \#1\},$$

that is, $Y = \mathcal{B}^{-1}(((0^+(a+b) + 1^+(c+d))\#^+)^*)$. Define the symbol permutations $\pi = (a\ b)$ and $\rho = (c\ d)$ and let $\Pi = \{\pi, \rho\}$, so that both X and Y are closed under Π, and the automaton $f : X \to X$ that swaps ${}^{\infty}0^{\infty}$ and ${}^{\infty}1^{\infty}$ is Π-blind. We claim that f cannot be extended to a Π-blind automaton $g : Y \to Y$. Assume the contrary, and consider the point $y = {}^{\infty}0.a\#^{\infty} \in Y$. Since $g|_X = f$, the image $g(y) \in Y$ is left asymptotic to $1^{\mathbb{Z}}$. Now, if $g(y) \neq 1^{\mathbb{Z}}$, then $g(y)_i \in \{c,d\}$ for some $i \in \mathbb{Z}$, but then $\rho(g(y)) \neq g(y)$, even though $\rho(y) = y$, contradicting the Π-blindness of g. Thus $g(y) = 1^{\mathbb{Z}}$, implying $g(\#^{\mathbb{Z}}) = 1^{\mathbb{Z}}$. Similarly (using the permutation π) we see that $g({}^{\infty}1c\#^{\infty}) = 0^{\mathbb{Z}}$, implying $g(\#^{\mathbb{Z}}) = 0^{\mathbb{Z}}$, a contradiction.

We are not aware of an easy characterization for the situations where the extension succeeds, but there is at least the following sufficient condition. This is rather technical, and not particularly interesting as such, but we will need it in the proof of Theorem 4.2.23.

Lemma 4.2.19 *Let $X \subset Y \subset S^{\mathbb{Z}}$ be subshifts, of which X is an SFT and Y is a mixing SFT, and let Π be a set of permutations on S such that Y is closed under Π. Suppose further that for some r, every symbol $a \in S$ occurs*

in every word of $\mathcal{B}_r(X)$*. Then a CA* $f : X \to X$ *is* Π*-blind on* X *if and only if* $f = g|_X$ *for a CA* $g : Y \to Y$ *which is captive and* Π*-blind on* Y *and satisfies* $g(X) \subset X$*.*

Note that any automaton $f : X \to X$ is automatically captive due to the strong assumption on X.

Proof. The backward implication is proved as in Proposition 4.2.16. For the forward implication, we can again assume that X is closed under Π^*, and we may assume $\Pi = \Pi^*$.

Let $r \in \mathbb{N}$ be a radius for f, a window size for X, and a mixing distance and windows size for Y, and such that every symbol $a \in S$ occurs in every word of $\mathcal{B}_r(X)$. Note that then the only element of Π having a fixed point in $\mathcal{B}_r(X)$ is the identity. We now define the automaton g.

As in Proposition 4.2.16, what we wish to do is to update long enough patterns from X according to the local rule of f, and other cells by the identity function, except for some gluing in the borders. For this, let $h_1 : Y \to \{0,1\}^{\mathbb{Z}}$ be the auxiliary automaton mapping

$$h_1(x)_i = \begin{cases} 0, & \text{if } x_{[i-2r,i+2r]} \in \mathcal{B}(X), \\ 1, & \text{otherwise.} \end{cases}$$

Clearly we have

$$\forall \pi \in \Pi, x \in Y : h_1(x)_i = h_1(\pi(x)),$$

since X is closed under Π. In coordinates i of x where $h_1(x)_i = 0$, we could sensibly apply the local rule of f. Note that if $h_1(x)_j = h_1(x)_{j'} = 0$, $j < j'$ and $j' - j < 3r$, then $h_1(x)_{[j,j']} \in 0^*$, since X has window size r. If $x \in X$, then we have $h_1(x) = 0^{\mathbb{Z}}$.

Now, we define a second auxiliary automaton $h_2 : Y \to \{0,1\}^{\mathbb{Z}}$ mapping

$$h_2(x)_i = \begin{cases} 0, & \text{if } \exists j : i \in [j, j+r-1] \wedge h_1(x)_{[j,j+r-1]} \in 0^*, \\ 1, & \text{otherwise.} \end{cases}$$

Note that h_2 satisfies the same properties as h_1, and also has the additional property that every maximal subword of all zeroes in $h_2(x)$ has length at least r. The coordinates i of x where $h_2(x)_i = 0$ will be the ones where f_{loc} is applied, in the final CA g.

We now locate the coordinates where the identity map is applied, by defining a third auxiliary CA $h_3 : Y \to \{0,1,2\}^{\mathbb{Z}}$ by

$$h_3(x)_i = \begin{cases} 0, & \text{if } h_2(x)_i = 0 \\ 1, & \text{if } h_2(x)_{[i-r,i+r]} = 1^{2r+1} \\ 2, & \text{otherwise.} \end{cases}$$

Note that $h_3(x)_i = 0 \iff h_2(x)_i = 0$. The coordinates i where $h_3(x)_i = 1$ will be the ones where the final CA g applies the identity CA, and they

form runs of length at least $r+1$ by the property that two 0s separated by 1s in $h_2(x)$ are separated by at least $3r+1$ repetitions of 1 (which in turn was inherited from $h_1(x)$). The coordinates i where $h_3(x)_i = 2$ form runs of length precisely r.

To sum up the properties of h_3,

$$h_3(Y) \subset \mathcal{B}^{-1}(((0^r0^*)2^r(1^r1^*)2^r)^*),$$

and

$$h_3(X) = \{0^{\mathbb{Z}}\},$$

and $h_3(x) = h_3(\pi(x))$ for all $\pi \in \Pi$, $x \in Y$.

Next, we define the map $g : Y \to Y$. We already mentioned that we will at least have $g(x)_i = f_{\mathrm{loc}}(x_{[i-r,i+r]})$ if $h_3(x)_i = 0$, and $g(x)_i = x_i$ if $h_3(x)_i = 1$. We now choose the rule for filling the rest of the coordinates. Of course, we will just use the fact that Y is mixing, and the only trick is to choose only one gluing per Π-orbit, in the following sense. Consider the natural Π-action on $\mathcal{B}_r(X)$ obtained in the obvious way. Since each symbol of S occurs in every word of $\mathcal{B}_r(X)$, every orbit is of the same size, that is, $|\Pi(w)| = |\Pi|$ for all $w \in \mathcal{B}_r(X)$. Now, if

$$h_3(x)_{[0,3r-1]} = 0^r2^r1^r,$$

then

$$g(x)_{[0,3r-1]} = uvw,$$

where $u = f(x)_{[0,r-1]}$, $w = x_{[2r,3r-1]}$, and if $\pi^{-1}(x_{[0,r-1]})$ is lexicographically minimal in the Π-orbit of $x_{[0,r-1]}$ (note that there is a unique such π) and v' lexicographically minimal such that

$$\pi^{-1}(f(x)_{[0,r-1]})v'\pi^{-1}(w) \sqsubset Y,$$

then $v = \pi(v')$. When $h_3(x)_{[0,3r-1]} = 1^r2^r0^r$, we define $g(x)_{[0,3r-1]}$ symmetrically.

It is easy to see that g is a well-defined captive cellular automaton and $g(Y) \subset Y$. We show that it is color blind. Let $x \in Y$ and $\pi \in \Pi$ and recall that $h_3(x) = h_3(\pi(x))$. If $h_3(x)_i = 0$, then

$$\pi(g(x))_i = \pi(f_{\mathrm{loc}}(x_{[i-r,i+r]})) = f_{\mathrm{loc}}(\pi(x_{[i-r,i+r]})) = g(\pi(x))_i.$$

If $h_3(x)_i = 1$, then

$$\pi(g(x))_i = \pi(x)_i = g(\pi(x))_i.$$

Finally, if $h_3(x)_{[0,3r-1]} = 0^r2^r1^r$, then if $\psi \in \Pi$ and $\psi^{-1}(x_{[0,r-1]})$ is lexicographically minimal in the Π-orbit of $x_{[0,r-1]}$, then

$$(\pi \circ \psi)^{-1}(\pi(x_{[0,r-1]})) = \psi^{-1}(\pi^{-1}(\pi(x_{[0,r-1]}))) = \psi^{-1}(x)_{[0,r-1]}$$

is also minimal in the Π-orbit of $\pi(x)_{[0,r-1]}$. The same word v' is chosen for the gluing of the words $\psi^{-1}(f(x_{[0,r-1]}))$ and $\psi^{-1}(x_{[2r,3r-1]})$ when deciding the contents of $g(x)_{[r,2r-1]}$ and $g(\pi(x))_{[r,2r-1]}$, and thus $g(x)_{[r,2r-1]} = \psi(v')$ and $g(\pi(x))_{[r,2r-1]} = \pi(\psi(v'))$. Thus, g is indeed color blind. ■

We remark that to prove Lemma 4.2.19, what we actually needed was that

- no element of Π^* except the identity has a fixed point in X, and that
- we can always glue together $f(u) \sqsubset X$ and $v \sqsubset Y$ using only the symbols occurring in uv.

We note that the lemma is not a generalization of the usual Extension Lemma. One can find a generalization by elaborating on the above, but the conditions obtained are still somewhat artificial. It is an interesting question what the right conditions for the existence of color-blind extensions are.

4.2.2 Constructing Color Blind Cellular Automata

In this section, we give concrete examples of color blind cellular automata, and construct color blind automata with interesting properties.

Definition 4.2.20 *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a cellular automaton with a neighborhood of size n. We say f is a* majority CA *if, whenever $f_{\text{loc}}(s_1, \dots, s_n) = s$, we have $|\{i \in [1, n] \mid s_i = s\}| \geq |\{i \in [1, n] \mid s_i = s'\}|$ for all $s' \in S$.*

This means that the local rule of a majority CA always outputs a symbol that occurs a maximal number of times in the input. All majority CA are of course captive. In the binary case, there is a unique majority CA for each odd neighborhood size, and this CA is color blind. In other cases, the CA must have a tie-breaking rule. To make such a CA color blind we can, for example, always choose the leftmost input symbol s_m that maximizes $|\{i \in [1, n] \mid s_i = s_m\}|$.

Of the 256 elementary cellular automata, 16 rules are color blind. The even-numbered rules are summarized in Table 4.1, while the odd-numbered rules are obtained by subtracting their numbers from 255, effectively composing them with the symbol permutation (0 1). We show the even-numbered color blind rules, as they are exactly the captive ones.

Of these 8 elementary automata, the most interesting ones for us are 232 and 150. Rule 232, the Majority CA (which, as its name suggests, is a particular majority CA), has the property that it in fact commutes with *all* symbol maps on $\{0, 1\}$, not just permutations. This is something that cannot occur when the alphabet is larger, by the results of Section 4.2.3. The rule 150 has this property as well, and the additional property that if we give the binary full shift the obvious group structure $\mathbb{Z}_2^{\mathbb{Z}}$, then it is

Table 4.1: The even-numbered color blind elementary CA. The variables v_1, v_2 and v_3 denote inputs to the local rule, and v_4 is its output.

CA	Color blind formula	Description
142	$(v_4 \neq v_2) \iff (v_1 = v_2 \neq v_3)$	Flip left, then majority
150	$(v_1 = v_2) \iff (v_4 = v_3)$	XOR of neighborhood
170	$v_4 = v_3$	Left shift
178	$(v_4 = v_2) \iff (v_1 = v_2 = v_3)$	Flip unless all equal
204	$v_4 = v_2$	Identity
212	$(v_4 \neq v_2) \iff (v_1 \neq v_2 = v_3)$	Flip right, then majority
232	$(v_4 \neq v_2) \iff (v_1 \neq v_2 \neq v_3)$	Majority
240	$v_4 = v_1$	Right shift

a pointwise sum of three distinct shifts, and thus a group endomorphism. As we mentioned in the introduction, we show in Section 4.2.4 that color blind CA with this property are quite exceptional, or rather $\mathbb{Z}_2$ is rather exceptional, in that group homomorphisms cannot be color blind for groups other than $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_2^2$.

Our first result is that (on the full shift) color blind cellular automata are abundant in the sense of density (see Definition 1.5.6). In particular, the endomorphism monoid is far from sparse.

Proposition 4.2.21 *Denote by $\mathcal{CB}$ the set of captive color blind cellular automata on $S^{\mathbb{Z}}$. Then $d(\mathcal{CB}) = 1$.*

Proof. Let $S = \{s_1, \dots, s_{|S|}\}$, and let $n \in \mathbb{N}$ be arbitrary. We define an injective map $\phi : \mathcal{CA}_n \to \mathcal{CB}_{n+|S|}$, which shows that $|\mathcal{CA}_n| \leq |\mathcal{CB}_{n+|S|}|$. For that, let $f \in \mathcal{CA}_n$ have neighborhood size n. The local function $\phi(f)_{\mathrm{loc}} : S^{n+|S|} \to S$ works as follows on the inputs $a_1, \dots, a_{n+|S|} \in S$. If the symbols $a_{n+1}, \dots, a_{n+|S|}$ are pairwise distinct, we let $\pi : S \to S$ be the symbol permutation that maps each a_{n+i} to s_i. The local function then returns $\pi^{-1}(f_{\mathrm{loc}}(\pi(a_1), \dots, \pi(a_n)))$. If the symbols $a_{n+1}, \dots, a_{n+|S|}$ are not pairwise distinct, $\phi(f)_{\mathrm{loc}}$ returns a_1. Then $\phi(f)$ is captive and color blind, and ϕ is injective.

Now, we calculate

$$\begin{aligned}
&\frac{1}{n+|S|} \log_{|S|} \log_{|S|} |\mathcal{CB}_{n+|S|}| \geq \frac{1}{n+|S|} \log_{|S|} \log_{|S|} |\mathcal{CA}_n| \\
&= \frac{1}{n+|S|} \log_{|S|} \log_{|S|} |S|^{|S|^n} = \frac{n}{n+|S|} \overset{n\to\infty}{\longrightarrow} 1,
\end{aligned}$$

which proves the claim. ■

In the next result, *intrinsic universality* is understood with respect to simulation by injective bulking, in the sense of [Oll08] (this is the same

simulation that we did in Proposition 1.5.4). In this formalism, a cellular automaton $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ *simulates* another automaton $g : T^{\mathbb{Z}} \to T^{\mathbb{Z}}$ if there exists an injective function $\phi : T \to S^{m \times n}$ from T-symbols to S-rectangles such that for every one-way spacetime diagram $x \in T^{\mathbb{Z} \times \mathbb{N}}$ of g, the point $\phi(x) \in S^{\mathbb{Z} \times \mathbb{N}}$ (defined in the obvious way, by replacing each symbol s in x by the rectangle $\phi(s)$) is a one-way spacetime diagram of f. An *intrinsically universal automaton* is then one that simulates any other CA. Note that it does not, strictly speaking, follow that the endomorphism monoid is not predictable, but one could argue that intrinsic universality is a stronger kind of computational universality, since it means we can simulate *every* CA (and thus, in particular ones that are unpredictable), as long as we can restrict to a subshift.

We begin with a simple lemma. A similar, though much more quantitative, result is Proposition 2.1 in [Mil12], although our result does not directly follow from it. In the next lemma, when X is a subshift and $w \sqsubset X$, we write $[w]_i$ for the set of points $x \in X$ with $x_{[i,i+|w|-1]} = w$ (of course, strictly speaking, $[w]_i$ depends also on X).

Lemma 4.2.22 *Let X be an infinite mixing SFT and $k \in \mathbb{N}$. Then for large enough n, and for any set of words $\{w_1, \dots, w_k\} \subset \mathcal{B}(X)$ with $\forall i : |w_i| = n$, the SFT*

$$Y = X \setminus \bigcup_{i \in \mathbb{Z}, j \in [1,k]} [w_j]_i$$

contains a mixing SFT of positive entropy.

Proof. Let $w_1, \dots, w_k$ be words of length n. We will find sufficient conditions on n such that the claim holds. Let $n > 4m$, where m is the window size and mixing distance of X. Let μ be a probability measure on X [LM95] with

$$\forall w \sqsubset X, i \in \mathbb{Z} : c^{-1}\lambda^{-|w|} \leq \mu([w]_i) \leq d^{-1}\lambda^{-|w|}$$

for some $\lambda > 1$ and $0 < d \leq c \in \mathbb{R}$. Then in particular there are between $d\lambda^n$ and $c\lambda^n$ words of length n in X. Let U be the set of words of length n which overlap with one of the words w_i by at least $\frac{n}{4}$. It is easy to see that

$$|U| < k \cdot 2n \cdot c\lambda^{\frac{3}{4}n} < d\lambda^n - 1$$

for all large enough n. We thus take such n, and then $V = \mathcal{B}_n(X) \setminus U$ satisfies $|V| \geq 2$. Now, define Z as the subSFT of X where we require every cell to either be in an occurrence of a word in V, or in a gap of length at most $m + 1$ between two such occurrences. This is an SFT by definition, has positive entropy because it contains the positive entropy subshift

$$\mathcal{B}^{-1}((V\mathcal{B}_m(X)^*) \cap X,$$

and is mixing because if $u, v \sqsubset Z$, u ends in a word in V and v begins with a word of V, then u can be glued to v by a word in

$$((\mathcal{B}_m(X) + \mathcal{B}_{m+1}(X)V)^*\mathcal{B}_m(X)$$

that is long enough. Note that $Z \subset Y$ since $n > 4m$. ■

Theorem 4.2.23 *Let F be a reversible equicontinuous family of cellular automata on a mixing SFT. Then the centralizer of F contains an intrinsically universal cellular automaton.*

Proof. Let $g : [1,k]^{\mathbb{Z}} \to [1,k]^{\mathbb{Z}}$ be any CA. We show how to simulate this map on X by a CA that commutes with the operations in F (an 'F-blind' cellular automaton). This proves the claim, since there exists an intrinsically universal cellular automaton on the full shift.

Let F be a reversible and equicontinuous family of CA on a mixing SFT X'. First, we apply Corollary 4.2.2 to F, and obtain a conjugacy α from X' to a nontrivial mixing SFT $X \subset T^{\mathbb{Z}}$ with $\mathcal{B}_1(X) = T$ that sends F to a subset Π of the symbol permutations on $T^{\mathbb{Z}}$. We may suppose $\Pi = \Pi^*$. Note that X is closed under Π, and the centralizer of F corresponds to the set of Π-blind maps on X. Let $m \in \mathbb{N}$ be the window size and mixing distance of X, and suppose further that this is more than twice the radius of α^{-1}.

Take an unbordered word $v \sqsubset X$ of length $n > m$ such that $\mathcal{B}_1(X) \sqsubset v$, by applying Lemma 1.3.5 to an aperiodic point of X where every symbol is uniformly recurrent (in the sense that every symbol appears in every long enough subword). Now, let $W = \Pi(v)$, and note that $|W| = |\Pi|$ since v contains every letter of X. If n is taken large enough, then $X \setminus \bigcup_{i\in\mathbb{Z},\pi\in\Pi}[\pi(v)]_i$ contains a mixing SFT Y of positive entropy, by the previous lemma.

Let $\xi_W(x)_i = 1 \iff x_{[i,i+|v|-1]} \in W$. We have $\xi_W(x) = \xi_W(\pi(x))$ since W is closed under Π, and thus $\mathcal{B}_n(X) \setminus W$ is as well.

Now, note that for n large enough (we can find v for arbitrarily large n), since X has positive entropy, there are k pairwise distinct words $v_i \in \mathcal{B}_n(X)$ that share a prefix and suffix of length m (by the pigeonhole principle). Choose such v_i, let $u \sqsubset Y$ be an unbordered word of length $M > 10n$, and choose $a, b, c \in \mathcal{B}_n(X)$ such that $w_i = uavbv_ic \sqsubset X$ (where b and c can be taken independent of i because the v_i share a common prefix and suffix).

Define the injection $h : [1,k]^{\mathbb{Z}} \to S^{\mathbb{Z}}$ by

$$h(x) = \cdots w_{x_{-2}} w_{x_{-1}} . w_{x_0} w_{x_1} \cdots .$$

Let $Z = h([1,k]^{\mathbb{Z}})$ and $Z' = \bigcup_{i=0}^{M+5n-1} \sigma^i(Z)$. It is easy to see that $Z' \subset S^{\mathbb{Z}}$ is an SFT, since

$$Z' = \mathcal{B}^{-1}((w_1 + \cdots + w_k)^*),$$

the set of concatenations of the words w_i, and the words w_i begin precisely where the unbordered word u occurs. Define $f : Z \to Z$ by $f \circ h = h \circ g$, and extend it to a CA $f : Z' \to Z'$ in the unique way. We may assume f has radius $r > 2M$. Since v contains all symbols of X, f is trivially captive.

Next, we show that f is Π-blind. We show that it is trivially so, by showing $\pi(Z') \cap Z' = \emptyset$ if $\pi \in \Pi$ and $\pi \neq \mathrm{id}$. For this, note that in a point $z \in Z'$, the occurrences of u can be determined by looking at $\xi_W(z)$ only:

$$\xi_W(\cdots w_{x_{-2}} w_{x_{-1}} . w_{x_0} w_{x_1} \cdots) = \cdots 0^{|u|-n} t_{-2} 0^{|u|-n} t_{-1} . 0^{|u|-n} t_0 0^{|u|-n} t_1 \cdots,$$

for some words $t_i \in \{0,1\}^{6n}$ each containing at least one 1. The leftmost 1 in each t_i occurs in the same coordinate h, and $0^{|u|-n}$ is of length at least $9n > 6n$. Thus, we can locally determine the subwords $0^{|u|-n}$ in the decomposition above, in the sense that

$$y_{[i,i+|u|-1]} = u \iff \xi_W(y)_{[i,i+|ut|-n-1]} = 0^{|u|-n} t,$$

for some $t \in \{0,1\}^{6n}$ whose leftmost coordinate containing 1 is h. Thus, for $y \in Z'$, we can uniquely determine $0 \leq i < 15n - 1$ such that $y \in \sigma^i(Z)$ based on $\xi_W(y)$ only. Of course, this means that if we have $\pi(Z') \cap Z' \neq \emptyset$, then $z = \pi(z')$ for some $z, z \in Z$. But this is impossible if π is not the identity map, again since v contains every letter.

Since f is Π-blind, Lemma 4.2.19 gives us a Π-blind extension $\hat{f} : X \to X$, since v contains every letter. Then $\hat{f}' = \alpha^{-1} \circ \hat{f} \circ \alpha : X' \to X'$ is a cellular automaton that commutes with every element of F. Since we chose $|a| = |b| = n > m$ to be more than twice the radius of α^{-1}, every point in $\alpha^{-1}(Z)$ is an infinite concatenation of some words $s_1, \ldots, s_k$ of the same length as $uavbv_ic$, and $\hat{f}'$ behaves as g on such points, treating the word s_i as the symbol i. This implies that h simulates g. ■

Clearly the endomorphism monoid should not be predictable in the general case of Theorem 4.2.23, but we do not obtain this result easily from the current proof. As we mentioned, intrinsic universality is, in some sense, a stronger notion of universality than unpredictability (although neither implies the other), so we have chosen to prove a general result for intrinsic universality instead of unpredictability. However, we at least sketch the proof that color blind CA on full shifts are not predictable.

Theorem 4.2.24 *Let S be a finite alphabet of size at least 2 and let Π be the set of symbol permutations on S. Then $\mathrm{End}(S^{\mathbb{Z}}, \Pi)$ is not predictable.*

Proof sketch. Let $f \in \mathrm{End}(S^{\mathbb{Z}}, \Pi)$ simulate a CA $g : [0,k]^{\mathbb{Z}} \to [0,k]^{\mathbb{Z}}$ for which 0 is a spreading state, as in the proof of the previous theorem. The simulations of g happen on some SFT $Y = \mathcal{B}^{-1}((w_0 + \cdots w_k)^*)$ where the words w_i are all of the same length n, and $\pi(Y)$ does not intersect Y for

any $\pi \in \Pi$, and if a forbidden pattern of Y occurs around coordinate i, we apply the identity map in some neighborhood of i. We may also suppose w_i is not unary for any i.

Now, the reachability problem is already almost undecidable if g is chosen suitably: given u, v it is undecidable whether there exist extensions of u and v to points $y, z \in Y$ such that $f^n(y) = z$. The problem is that even if v is not reachable from u this way, there might still be an extension of u to a point of $S^{\mathbb{Z}} \setminus Y$ such that, somehow, eventually v appears in the origin. Let $m > n$ be a window size of Y. Suppose the radius of f is r. We make a modified CA f' which behaves as follows: If $x_{[i,i+m-1]}$ is unary, then the unary pattern tries to spread in both directions by more than r. If there is another unary pattern of length at least n in the way, the patterns merge if they are of the same color, and otherwise they grow until they touch, and then become fixed. Note that a color blind CA need not be left-right symmetric, so tie-breaking can be done rather freely when the patterns collide. Now, if $x_{[i,i+m-1]}$ is not forbidden in Y but $x_{[i-1,i+m-2]}$ is, then $f'(x)_{[i,i+m-1]} = x_i^m$ (introducing a long spreading unary pattern). Similarly, if $x_{[i,i+m-1]}$ is not forbidden in Y but $x_{[i+1,i+m]}$ is, and the previous rule did not change any of the coordinates $[i, i+m-1]$, then $f'(x)_{[i,i+m-1]} = x_i^m$.

Then f' is color blind because we did not refer to any specific colors in its definition. It is not predictable if g is chosen suitably, because the prediction problem for $u, v \sqsubset Y$ is undecidable within continuations to points of Y, and if u is continued to a point of $S^{\mathbb{Z}}$ not in Y, then a unary pattern appears in $f'(x)$ where the forbidden pattern of Y closest to the origin appears in x. The unary pattern spreads faster than the speed of light r of f, so the only way the run of f' might differ from a simulation of f is that a long unary pattern appears near the origin, and v does not contain such a pattern if it is long enough. ■

It seems obvious that with the assumptions of the previous theorem, $\mathrm{End}(S^{\mathbb{Z}}, \Pi)$ is not finitely generated. However, we do not have a proof of this fact.

4.2.3 Typhlotic Cellular Automata

We now turn our attention to typhlotic cellular automata, and start with the observation that they are not necessarily trivial. For example, from Theorem 4.2.23 we obtain an intrinsically universal color blind CA on $\{0,1\}^{\mathbb{Z}}$, and this automaton is in fact automatically typhlotic. Furthermore, every binary majority CA is typhlotic. These CA are already color blind, so we only need to check that they commute with the symbol maps that are not permutations, namely the constant maps $s \mapsto 0$ and $s \mapsto 1$. But this easily follows from the fact that both the intrinsically universal CA and majority CA are captive, and the following lemma.

Lemma 4.2.25 *A CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ commutes with the constant map $g(x) = a^{\mathbb{Z}}$ if and only if $f(a^{\mathbb{Z}}) = a^{\mathbb{Z}}$.*

Proof. If f commutes with such g, then

$$f(a^{\mathbb{Z}}) = f(g(a^{\mathbb{Z}})) = g(f(a^{\mathbb{Z}})) = a^{\mathbb{Z}}.$$

Conversely, if $f(a^{\mathbb{Z}}) = a^{\mathbb{Z}}$, then $f(g(x)) = f(a^{\mathbb{Z}}) = a^{\mathbb{Z}}$ and $g(f(x)) = a^{\mathbb{Z}}$. ■

Somewhat curiously, if the alphabet S has more than two elements, the situation changes drastically: in Theorem 4.2.31, we show that shift maps are the only typhlotic CA. The proof of Theorem 4.2.31 follows from some rather general set theory. Namely, we show that a typhlotic CA is defined by an ultrafilter on its neighborhood, and ultrafilters on finite sets are very simple. We note that we do not need any hard set theoretic results on ultrafilters: they just happen to provide convenient terminology for the proof.

Definition 4.2.26 *Let X be a nonempty set. We say that $Q \subset 2^X$ is a* filter (on X) *if*

- $\emptyset \notin Q, X \in Q$, *and if* $A, B \in Q$, *then* $A \cap B \in Q$, *and*
- *if* $A \in Q$ *and* $A \subset B$, *then* $B \in Q$.

If Q is a filter, and for all A, either $A \in Q$ or $X \setminus A \in Q$, then Q is called an ultrafilter. *An ultrafilter Q is principal if $Q = \{A \subset X \mid j \in A\}$ for some $j \in X$.*

On infinite sets, the rather dramatic term 'ultrafilter' is fitting. Ultrafilters are exactly the filters that cannot be extended to a larger filter. Having access to non-principal ultrafilters (even on $\mathbb{N}$) allows for some rather mind-blowing constructions, such as the non-standard reals of Robinson [Rob66].

We start with two characterizations of ultrafilters. The first one is just the observation that a well-known partition property of ultrafilters characterizes them, as also the filter axioms follow from it. This result has already appeared in at least [Lei12] (and is presumably well-known). The second one is rather specific to typhloticity, and is in fact just the first part of Theorem 4.2.31 in thin disguise.

Lemma 4.2.27 (Corollary 1.6 of [Lei12]) *Let X be a nonempty set, let $k \in \mathbb{N}$ with $k \geq 3$, and let $Q \subset 2^X$ have the property that for all partitions $(A_1, \ldots, A_k)$ of X, exactly one A_i is in Q. Then Q is an ultrafilter. Furthermore, every ultrafilter satisfies the property for every $k \geq 1$.*

Proof. To show that Q is an ultrafilter, we need to show that it is a filter, and that for all A, either A or $X \setminus A$ is in Q.

First, from the partition $(X, \emptyset, \ldots, \emptyset)$ we deduce that $\emptyset \notin Q$ and $X \in Q$. Thus, if $A \subset X$, then exactly one of A and $X \setminus A$ is in Q, by the partition $(A, X \setminus A, \emptyset, \ldots, \emptyset)$.

Suppose then that $A \in Q$ and $A \subset B$. The partition $(X \setminus B, A, B \setminus A, \emptyset, \ldots, \emptyset)$ proves that $X \setminus B \notin Q$, so by the above, $B \in Q$. Finally, we have to show that $A, B \in Q$ implies $A \cap B \in Q$. For this, consider the partition $(A \cap B, X \setminus A, A \setminus B, \emptyset, \ldots, \emptyset)$. Since $A \in Q$, we have $X \setminus A \notin Q$, and similarly $A \setminus B \subset X \setminus B \notin Q$. Thus, $A \cap B$.

The converse claim is a well known property of ultrafilters. ■

For the next lemma, we give a more general definition of typhloticity.

Definition 4.2.28 *Let S and T be sets with S finite, and let $f : S^T \to S$ be a function. Then we say f is* typhlotic *if for every function $g : S \to S$, we have $f \circ g = g \circ f$, where g is applied coordinatewise on the left side of the equation.*

Lemma 4.2.29 *Let T be a set, and S a finite set with $|S| \geq 3$. Then the map $f \mapsto \{\{i \in T \mid x_i = f(x)\} \mid x \in S^T\}$ is a bijection from the set of typhlotic maps $f : S^T \to S$ to the set of ultrafilters on T.*

Proof. Without loss of generality, let $S = [1, k]$. For all $x \in S^T$ and $s \in S$ we define $x|_s = \{i \in T \mid x_i = s\}$.

Let first $f : S^T \to S$ be typhlotic, and denote by $Q \subset 2^T$ the image of f under the mapping. By Lemma 4.2.27, we need to show that if $(A_1, A_2, \ldots, A_k)$ is a partition of T, then exactly one of the A_i is in Q, that is, of the form $x|_{f(x)}$ for some $x \in S^T$. Let $x \in S^T$ be such that $x|_i = A_i$ for all $i \in [1, k]$. Then of course $x|_{f(x)} \in Q$ by the definition of Q, and $x|_{f(x)} = A_{f(x)}$.

Suppose then that, for example, we have $A_1 = y|_{f(y)}$ and $A_2 = z|_{f(z)}$ for some $y, z \in S^T$, where we may assume $f(y) = 1$ and $f(z) = 2$ by applying symbol permutations. Let again $x \in S^T$ be the point with $x|_i = A_i$ for all $i \in [1, k]$. If $f(x) = 1$, define the symbol map $\pi : S \to S$ by $\pi(2) = 2$ and $\pi(s) = 1$ for all $s \in S \setminus \{2\}$. Then

$$1 = \pi(f(x)) = f(\pi(x)) = f(\pi(z)) = \pi(f(z)) = \pi(2) = 2,$$

a contradiction. A symmetric argument shows that $f(x) \neq 1$ is likewise impossible. Thus exactly one of the A_i is in Q, and Q is a ultrafilter.

Conversely, let Q be an ultrafilter on T, and define $f : S^T \to S$ by $f(x) = a$ if and only if $x|_a \in Q$. Again by Lemma 4.2.27 (the converse direction), f is then well-defined. Since ultrafilters are closed under supersets, f is easily seen to be typhlotic. As the ultrafilter corresponding to f is Q, this concludes the claim. ■

The following is also a well known property of ultrafilters (for instance, it appears as Example 1.3 in [Lei12]).

Lemma 4.2.30 *Let T be finite and let Q be an ultrafilter on T. Then Q is principal.*

Proof. Since T is finite, we can take a minimal set A in Q. If A is a singleton, we are done. If A is not a singleton, let $x \in A$. Either $\{x\} \in Q$ or $A \cap (X \setminus \{x\}) \in Q$. In either case, A was not minimal. ■

Theorem 4.2.31 *If $|S| \geq 3$, the typhlotic CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ are exactly the shift maps. If $|S| = 2$, they are exactly the captive color blind CA.*

Proof. First, suppose $|S| \geq 3$, and let $N \subset \mathbb{Z}$ be the neighborhood of f. The local rule $f_{\text{loc}} : S^N \to S$ is typhlotic since f is. Let Q be the ultrafilter on N that defines it, given by Lemma 4.2.29. Since N is finite, $Q = \{A \subset N \mid j \in A\}$ for some $j \in N$ by Lemma 4.2.30, which means

$$f(x)_0 = a \iff \{i \in N \mid x_i = a\} \in Q \iff x_j = a.$$

Thus, f is a shift map.

In the case $|S| = 2$, a CA is captive if and only if it commutes with constant maps by Lemma 4.2.25, and all symbol maps are either permutations or constant maps. This concludes the proof. ■

In terms of endomorphisms monoids:

Theorem 4.2.32 *If $|S| \geq 3$, and F is the set of all symbol maps on S, then $\text{End}(S^{\mathbb{Z}}, F)$ consists of only the shift maps (in particular, it is finitely generated, sparse and predictable).*

We end this section with some questions arising from the previous theorem. Namely, the result states in particular that there exists a set of 27 CA $\{f_1, \ldots, f_{27}\}$ on $\{0,1,2\}^{\mathbb{Z}}$ such that $\text{End}(\{0,1,2\}^{\mathbb{Z}}, f_1, \ldots, f_{27})$ consists of the shift maps only. By Lemma 1.3.22, the center of $\text{End}(\{0,1,2\}^{\mathbb{Z}})$ is precisely the set of shift maps. This suggests the following definition:

Definition 4.2.33 *Given X, let $m(X)$ be the smallest number m such that there exists a set of cellular automata $\{f_1, \ldots, f_m\}$ on X such that*

$$\text{End}(X, f_1, \ldots, f_m) = \{f : X \to X \mid \forall g : X \to X : f \circ g = g \circ f\},$$

if such m exists. Otherwise, let $m(X) = \infty$.

We mention the obvious upper bound given by the previous theorem.

Corollary 4.2.34 *If $n > 2$, then $m([1,n]^{\mathbb{Z}}) \leq n$.*

Proof. There are n^n symbol maps on $[1,n]^{\mathbb{Z}}$. These symbol maps are generated by $n-1$ transpositions (which generate the symbol permutations), and the map $\pi(1) = \pi(2) = 1$, $\pi(i) = i$ for $i \in [3,n]$ that merges two symbols together. The result then follows from Theorem 4.2.32, since the center of a full shift is precisely the set of shift maps by Lemma 1.3.22. ■

I do not know what the actual value of $m([1,n]^{\mathbb{Z}})$ is. Here's my best guess:

Conjecture 4.2.35 *If X is a mixing SFT with at least two unary points, then $m(X) = 2$.*

The inequality $m(X) > 1$ of course holds in general whenever $\mathrm{End}(X)$ is not abelian: if $f \in \mathrm{End}(X)$ commutes with all CA in $\mathrm{End}(X)$, then $C(f) = \mathrm{End}(X)$ is not the center of $\mathrm{End}(X)$, and similarly if f does not commute with all CA in $\mathrm{End}(X)$, then $f \in C(f)$ is not in the center of $\mathrm{End}(X)$. On the other hand, if $\mathrm{End}(X)$ is abelian, then $m(X) = 0$, since $\mathrm{End}(X)$ is its own center. There are many subshifts whose center contains more maps than just the shift maps. A mixing SFT has this property if and only if it contains a unique unary point, by Lemma 1.3.22. A more interesting case is when the endomorphism monoid is abelian and contains maps other than the shifts, such as those constructed in Section 3.3. I do not have an example of a subshift with $m(X) = \infty$.

The reason $m(X)$ is interesting is that it is (by definition) a property of the endomorphism monoid only.

Proposition 4.2.36 *If X and Y be subshifts with isomorphic endomorphism monoids, then $m(X) = m(Y)$.*

Invariants like this are interesting, since one of the big open problems in symbolic dynamics is to find out when two mixing SFTs have isomorphic automorphism groups. While this has been solved in some cases, it is for example still open whether $\mathrm{Aut}(\{0,1\}^{\mathbb{Z}}) \cong \mathrm{Aut}(\{0,1,2\}^{\mathbb{Z}})$. If we had $m(\{0,1\}^{\mathbb{Z}}) \neq m(\{0,1,2\}^{\mathbb{Z}})$ (and in particular, Conjecture 4.2.35 were wrong), then at least the endomorphism monoids would not be isomorphic. As far as I know, the isomorphism question is unsolved for endomorphism monoids as well, and interesting in its own right. Of course, the fact this question is open might well be only because no one asked. So let us ask:

Question 4.2.37 *For mixing SFTs X and Y, when are $\mathrm{End}(X)$ and $\mathrm{End}(Y)$ isomorphic monoids? Are $\mathrm{End}(\{0,1\}^{\mathbb{Z}})$ and $\mathrm{End}(\{0,1,2\}^{\mathbb{Z}})$ isomorphic?*

Of course, as usual in mathematics, if the automorphism groups or endomorphism monoids *are* isomorphic, then invariants do not show much.

One can naturally also define an automorphism group version of $m(X)$, say $m'(X)$, with the same formulas. I do not have an upper bound for this quantity for any mixing SFT X. Theorem 4.2.23 suggests that a set of $m'(X)$ reversible automata whose centralizers intersect to the center of $\mathrm{Aut}(X)$ at least should not form an equicontinuous family, since I do not believe there is an inherent obstacle in making the automata constructed in the proof reversible.

4.2.4 Homomorphic Color Blind Automata

In Section 4.2.2, we saw that color blind cellular automata can do almost anything a general cellular automaton can do, with any alphabet size. On the other hand, typhlotic cellular automata turned out to be almost the same objects as color blind CA in the binary case, but shift maps for larger alphabets. In this section, we show that cellular automata that are color blind *group homomorphisms* satisfy a similar property: if the group is very simple, the color blind homomorphic CA form a large subclass of all homomorphic CA, but when the group is larger, they are all shift maps.

In algebraic terms, we are giving a full shift the structure given by the set of all symbol permutations, and the structure given by a cellwise group operation, simultaneously (without assuming any axioms linking the two structures together). We show that in this case, the endomorphism monoid contains only shift maps. Of course, we do not claim that such algebras are particularly interesting as such, but they do show an interesting contrast with the elementary CA number 150.

Another motivation for this study is that it generalizes a few results of [MB04], where a section was devoted to color blindness of homomorphic CA. There, the term k-rule was used for a sum of k distinct shifts. In the article, two particular cases of our main result Theorem 4.2.45 were proved. We prove Theorem 4.2.45 in a series of simple lemmas. By the following lemma, only the abelian case is interesting.

Lemma 4.2.38 *Let S be a finite group and let the CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be color blind and homomorphic with minimal neighborhood size at least 2. Then S is abelian, and if $|S| \geq 4$, then f is a sum of distinct shifts.*

Proof. All groups of order at most 3 are abelian, so we may assume $|S| \geq 4$. Let $0 \neq g \in S$, and consider the point $z(g) = {}^{\infty}0.g0^{\infty}$. Since the local rule sees at most two distinct symbols in its neighborhood, the image $f(z(g))$ must also be a point over $\{0, g\}$ by Lemma 4.2.5. Since f commutes with the permutation $(g\ h)$, we have $I = \{i \in \mathbb{Z} \mid f(z(g))_i = g\} = \{i \in \mathbb{Z} \mid f(z(h))_i = h\}$ for all $0 \neq h \in S$. From this we deduce that the symbol endomorphisms of f (in the sense of Lemma 4.1.7) are either trivial or identity maps, and since at least two of them must be nontrivial, S is abelian by Lemma 4.1.9.

Also, we clearly have $f = \sum_{i \in N} \sigma^i$, where $N \subset \mathbb{Z}$ is the set of those i for which the symbol endomorphism f_i is nontrivial, so f is a sum of distinct shifts. ■

Lemma 4.1.8 and the fact that only the groups $\mathbb{Z}_2$ and $\mathbb{Z}_3$ (and the trivial group) do not fit in Lemma 4.2.38 together give us the following.

Corollary 4.2.39 *Let S be a finite abelian group and $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ a color blind homomorphic CA. Then f is a sum of shifts, which are distinct if $|S| \geq 4$.*

The radius-1 CA f with local rule $(a, b, c) \mapsto a + 2b + c$ is an example of a color blind homomorphic CA on $\mathbb{Z}_3^{\mathbb{Z}}$ which is not a sum of distinct shifts.

Lemma 4.2.40 *Let S be a finite abelian group and $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ a homomorphic CA. Then f commutes with the symbol permutation $\phi_g(h) = h + g$ if and only if $f(g^{\mathbb{Z}}) = g^{\mathbb{Z}}$.*

Proof. Having $f(g^{\mathbb{Z}}) = g^{\mathbb{Z}}$ is equivalent to $f(x) + g^{\mathbb{Z}} = f(x) + f(g^{\mathbb{Z}})$ for all $x \in S^{\mathbb{Z}}$, which is simply commutation with ϕ_g, since $f(x) + f(g^{\mathbb{Z}}) = f(x + g^{\mathbb{Z}})$. ■

We now proceed with a case analysis on the small groups $\mathbb{Z}_2$, $\mathbb{Z}_3$ and $\mathbb{Z}_2^2$.

Lemma 4.2.41 *Let the CA $f : \mathbb{Z}_2^{\mathbb{Z}} \to \mathbb{Z}_2^{\mathbb{Z}}$ be homomorphic with minimal neighborhood size $m \in \mathbb{N}$. Then f is color blind if and only if f fixes $1^{\mathbb{Z}}$ if and only if m is odd.*

Proof. The only nontrivial permutation of $\mathbb{Z}_2$ is $\phi_1 = (0\ 1)$, so from Lemma 4.2.40 it follows that f is color blind if and only if it fixes $1^{\mathbb{Z}}$. Since f is a sum of shifts by Corollary 4.2.39, it is clear that it is in fact a sum of exactly the m different shifts in its neighborhood. Thus, f fixes $1^{\mathbb{Z}}$ if and only if m is odd. ■

Lemma 4.2.42 *Denote $S = \mathbb{Z}_2^2$, and let the CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be homomorphic. Then f is color blind if and only if it is a sum of an odd number of distinct shifts.*

Proof. Suppose first that f is color blind. Corollary 4.2.39 applies, so that f is a sum of m distinct shifts for some $m \in \mathbb{N}$. This means that $X = \{(0,0),(0,1)\}^{\mathbb{Z}} \cong \mathbb{Z}_2^{\mathbb{Z}}$ is closed under f, and the restriction of f to X is also a sum of shifts. If $f|_X$ were not color blind then f would not be either, so m must be odd by Lemma 4.2.41.

On the other hand, let f be a sum of m distinct shifts for odd m, and consider an arbitrary transposition $\phi = (g\ h)$. Denote $S = \{a, b, g, h\}$. Let $g_1, \ldots, g_m \in S$, and for $c \in S$, let n_c be the number of $i \in \{1, \ldots, m\}$ such

that $g_i = c$. We note a few facts about the group $\mathbb{Z}_2^2$, namely that $2ng = 0$ for all $g \in S$ and $n \in \mathbb{N}$, and if $S = \{a, b, c, d\}$ then $a + b + c = d$.

Since m is odd, either exactly one of the numbers n_c is odd for $c \in \mathbb{Z}_2^2$, or exactly three of them are odd. Let $c \in \mathbb{Z}_2^2$ be the oddball with different parity than the others. Then $f_{\text{loc}}(g_1, \ldots, g_m) = c$ by the properties of $\mathbb{Z}_2^2$ noted in the previous paragraph. If $c \in \{a, b\}$, then $f_{\text{loc}}(\phi(g_1), \ldots, \phi(g_m)) = c = \phi(f_{\text{loc}}(g_1, \ldots, g_m))$ because the parities of the number of occurrences of the group elements are not changed by ϕ. On the other hand, if $c \in \{g, h\}$, then letting $\{c, d\} = \{g, h\}$ we have

$$f_{\text{loc}}(\phi(g_1), \ldots, \phi(g_m)) = d = \phi(f_{\text{loc}}(g_1, \ldots, g_m))$$

since the oddball changes from c to d on the left, when ϕ is applied, and ϕ maps the oddball c to d on the right. ■

Lemma 4.2.43 *Let the CA $f : \mathbb{Z}_3^{\mathbb{Z}} \to \mathbb{Z}_3^{\mathbb{Z}}$ be homomorphic. Then f is color blind if and only if it fixes $1^{\mathbb{Z}}$ if and only if it is a sum of $3k + 1$ shifts for some k.*

Proof. By Lemma 4.2.40, f fixes $1^{\mathbb{Z}}$ if and only if it commutes with the symbol permutation ϕ_1. We prove that all such homomorphic CA are color blind, for which it is enough to show that they also commute with the transposition (1 2). By Corollary 4.2.39, f is a sum of shifts $\sum_{i=1}^{m} \sigma^{k_i}$ for some $m \in \mathbb{N}$ and $k_i \in \mathbb{Z}$. For all $x \in \mathbb{Z}_3^{\mathbb{Z}}$, we then have

$$\begin{aligned}((1\ 2) \circ f)(x) = (1\ 2)\left(\sum_{i=1}^{m} \sigma^{k_i}(x)\right) &= \sum_{i=0}^{m} (1\ 2)(\sigma^{k_i}(x))) \\ &= \sum_{i=0}^{m} \sigma^{k_i}((1\ 2)(x)) = (f \circ (1\ 2))(x),\end{aligned}$$

where the second equality follows from the fact that (1 2) is an automorphism of $\mathbb{Z}_3$ and the third one directly from the fact that (1 2) is a cellular automaton.

Finally, it is easy to see that a sum of m shifts on $\mathbb{Z}_3^{\mathbb{Z}}$ fixes the point $1^{\mathbb{Z}}$ if and only if $m \equiv 1 \bmod 3$. ■

We handle the remaining cases in a single lemma.

Lemma 4.2.44 *Let S be a finite abelian group such that $|S| > 3$ and $S \ncong \mathbb{Z}_2^2$, and let the CA $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be homomorphic. Then f is color blind if and only if it is a shift map.*

Proof. First, a shift map is trivially a color blind homomorphic CA for any group alphabet.

As for the nontrivial direction, Corollary 4.2.39 again applies, so that f_{loc} simply adds together n of the inputs, for some n. If $n = 0$, then f does not commute with symbol permutations, as it sends everything to $0^{\mathbb{Z}}$. Assume then that $n \geq 2$.

We first suppose $|S| > 4$. In this case, we take $0 \neq g \in S$ and $h \in S$ such that $h \notin \{0, g, -g\}$. Now, $g + h \notin \{0, g, h\}$, so that $f_{\text{loc}}(g, h, 0, \ldots, 0) = g + h \notin \{0, g, h\}$, which is a contradiction by Lemma 4.2.5. Now, let $|S| = 4$, so by the assumption that $S \ncong \mathbb{Z}_2^2$, we have that $S \cong \mathbb{Z}_4$. Then $f_{\text{loc}}(1, 1, 0, \ldots, 0) = 2$, again contradicting Lemma 4.2.5.

Of course, in the remaining case that $n = 1$, f is a shift map. ■

We collect the results of this section into a single statement.

Theorem 4.2.45 *Let S be a finite (nontrivial) group, and let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a homomorphic cellular automaton. Then, f is color blind if and only if one of the following conditions holds.*

- *$S = \mathbb{Z}_2$ or $S = \mathbb{Z}_2^2$, and f is a sum of an odd number of shifts,*
- *$S = \mathbb{Z}_3$, and f is a sum of $3k + 1$ shifts for some k,*
- *$|S| > 4$ or $S = \mathbb{Z}_4$, and f is a shift map.*

Proof. If S is not abelian, then by Lemma 4.2.38 f has neighborhood size 1, and since a non-abelian group has size at least 6, such a CA can only be a shift map by Lemma 4.2.5. In the abelian case, Lemma 4.2.41, Lemma 4.2.42, Lemma 4.2.43 and Lemma 4.2.44 give the claim. ■

In each of the cases $S = \mathbb{Z}_2$, $S = \mathbb{Z}_2^2$ or $S = \mathbb{Z}_3$, the condition is equivalent to f fixing the unary points.

This gives a complete characterization of homomorphic color blind cellular automata on full shifts whose alphabet is a finite group. We also note that in our arguments we only manipulated the local functions of cellular automata, so the result holds for multidimensional CA with the same proof. Thus, Theorem 4.2.45 is a generalization of the results of [MB04], which state that for all dimensions $d \geq 1$, any sum of 4 distinct shifts on $\mathbb{Z}_3^{\mathbb{Z}^d}$ is color blind, and no sum of m distinct shifts on $\mathbb{Z}_n^{\mathbb{Z}^d}$ is color blind if $n \geq m > 1$.

Theorem 4.2.46 *If $\cdot$ is a group operation on S giving rise to any group other than $\mathbb{Z}_2$, $\mathbb{Z}_3$ or $\mathbb{Z}_2^2$, and F is the set of all symbol maps on S, then $\text{End}(S^{\mathbb{Z}}, \cdot, F)$ consists of only the shift maps (in particular, it is finitely generated, sparse and predictable).*

4.3 Subshifts with a Bipermutive Unary Operator

This section is based on [ST13c].

In this section, we study the opposite case of Section 4.2, in the sense that we study structure given by bipermutive maps, which are very far from equicontinuous. We show that bipermutive maps are transitive in a strong sense, which we call topological randomization. As a corollary, we obtain that the endomorphism monoid of a subshift with an algebraic structure given by one such map is always sparse.

Again, we also prove some interesting connections with cellular automata that respect a group structure. Namely, we give a new proof to a result of [MB97], showing that the centralizer of a bipermutive homomorphic+C automaton contains only homomorphic+C automata. One of their conjectures is whether an analogous result holds also for general d-dimensional cellular automata. We show that it indeed does: if $S^{\mathbb{Z}^d}$ has a cellwise abelian group structure $(S, +)$, then any 'extremally permutive' homomorphic+C CA $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ 'remembers' the group structure in the sense that the endomorphism monoid of the unary algebra $(S^{\mathbb{Z}^d}, f)$ consists of only homomorphic+C CA.

If we choose an extremally permutive homomorphic CA carefully, we obtain from this that for the full group shift $X = S^{\mathbb{Z}^d}$ for a finite abelian group S, there exist a unary operator $g : X \to X$ such that

$$\mathrm{End}(X, +) = \mathrm{End}(X, g).$$

In this section, we only consider full shifts, and do not look at more general mixing SFTs at all (except as tools), for the simple reason that bipermutivity does not really make much sense in this generality, as it is very deeply tied in the exact symbols that occur in the subshift. For example, the notion is not closed under conjugacy. Also, in Theorem 4.3.2, we show that many mixing SFTs in fact have the full shift as their limit in the action of a bipermutive CA; obviously, such a mixing SFT cannot support a bipermutive cellular automaton in a very interesting sense. A more sensible generalization might be to consider positively expansive CA, which could be considered a dynamical generalization of bipermutive CA. Positively expansive CA make perfect sense on mixing SFTs in general, and are a much larger natural class of CA than bipermutive ones. However, they are much harder to study. Namely, one of our main proof techniques in this section is 'sharpshooting permutations at the speed of light', where by 'speed of light' we mean the maximal speed at which information can travel, based on the radius of the CA. That is, if we permute a cell and apply a bipermutive CA, the permutation will, in a sense, travel at the edge of the light cone, and land exactly where we wish. Trying to do this directly using the combinatorial characterization of positively expansive CA is rather hard, as the

permutation bullets then usually do not travel at the speed of light, and I do not know how to control their path.

4.3.1 Orbits of Subshifts in Bipermutive CA

We begin by studying the behavior of individual points under the action of bipermutive CA. Recall that our definition of a bipermutive CA requires a neighborhood of size at least 2. A 'bipermutive' CA with neighborhood size 1 would be a symbol permutation composed with a shift map. The centralizers of such maps look very different, and were the topic of the previous section.

We give some examples, and prove Lemma 4.3.1 which states that every pattern, when surrounded by temporally and spatially periodic content, eventually self-replicates in the orbit of a bipermutive cellular automaton. All of the results of this section are, to some extent, based on this very simple observation.

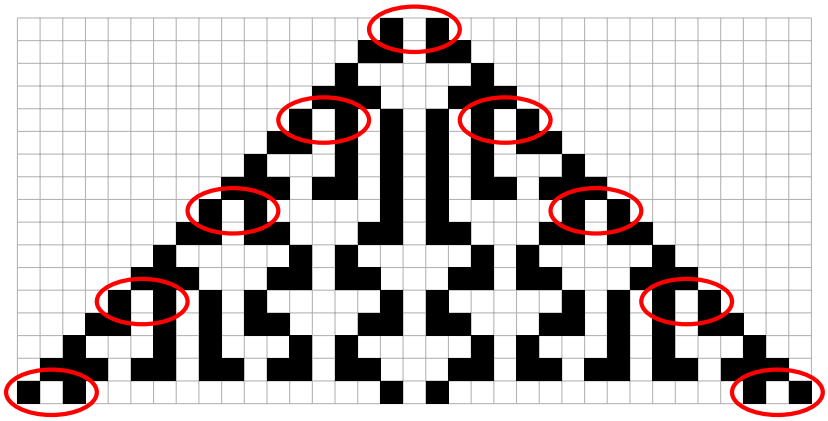


Figure 4.3: An illustration of the elementary CA 150 running from the initial pattern 101 for 16 generations. While the overall picture is rather complicated, the red ellipses show that the initial pattern repeats periodically at the borders.

We start with an illustration of this fundamental property of bipermutive CA for a particularly simple example: the binary CA with local rule $g_{\text{loc}}(a, b, c) = a + b + c \bmod 2$ and neighborhood $\{-1, 0, 1\}$. This is the elementary cellular automaton number 150, which we already discussed in Section 4.2 as an example of a homomorphic and typhlotic CA. See Figure 4.3 for a sample spacetime diagram.

Let f be bipermutive, and let $u \in S^*$ be such that $f^p(u^{\mathbb{Z}}) = u^{\mathbb{Z}}$. Then, any word $w \in S^*$, when superposed on the periodic background $u^{\mathbb{Z}}$, is a kind of self-replicating pattern: Copies of w periodically appear on both borders

of the light cone starting from w. See Figure 4.3 for a concrete illustration. The precise statement is formulated in Lemma 4.3.1.

Lemma 4.3.1 *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a left permutive CA with neighborhood $[-r, r']$, and let $y \in S^{\mathbb{Z}}$ be temporally and spatially periodic with periods t and p, respectively. Let $x \in S^{\mathbb{Z}}$ be such that $x_i = y_i$ for all $i > 0$, and let $n \in \mathbb{N}$. Then, denoting $C = pt(|S|^n)!$ and $I = [-n+1, 0]$, for all $\ell \in \mathbb{N}$, we have*

$$f^{\ell C}(x)_{I+\ell rC} = x_I.$$

Proof. We begin with an auxiliary observation. Let $\delta : Q \times \Sigma \to Q$ be such that $\delta(\cdot, a) : Q \to Q$ is bijective for all $a \in \Sigma$ (in other words, (Q, Σ, δ) is a reversible deterministic finite automaton), and let $q \in Q$ and $w \in \Sigma^*$ be arbitrary. Inductively, write $\delta(q, aw) = \delta(\delta(q, a), w)$. Clearly, $\delta(\cdot, w) : Q \to Q$ is then bijective for all $w \in \Sigma^*$. Then, $\delta(q, w^{\ell \cdot |Q|!}) = q$ for all $q \in Q$ and $\ell \in \mathbb{N}$.

Then, let $Q = S^n$ and $\Sigma = S^{r+r'}$, and let $\delta : (Q \times \Sigma) \to Q$ be defined by $\delta(q, a) = f(qa)$. We claim that $\delta(\cdot, a)$ is bijective. For this, let $q, q' \in Q$ and $a \in \Sigma$ with $q_i \neq q'_i$, where $i \in [0, n-1]$ is maximal. Since f is left permutive, we have $\delta(q, a)_i \neq \delta(q', a)_i$.

Consider the words $q^i = f^i(x)_{I+ri} \in Q$ and $a^i = f^i(x)_{[1,r+r']+ri} \in \Sigma$ for $i \in \mathbb{N}$. Since r is the right speed of light for f, we actually have $a^i = f^i(y)_{[1,r+r']+ri}$ for all $i \in \mathbb{N}$, and thus the sequence $(a^i)_{i \in \mathbb{N}}$ is periodic with period pt. Furthermore, we see that $\delta(q^i, a^i) = q^{i+1}$ holds for all i. Denoting $w = a^0 \cdot \cdots \cdot a^{pt-1} \in \Sigma^{pt}$, we have $\delta(q^0, w^{\ell \cdot |Q|!}) = q^0$ for all $\ell \in \mathbb{N}$ by the first paragraph, and expanding the definitions gives the claim. ■

The lemma states that in the left-permutive case the pattern x_I is repeated on every Cth step on the right border of the light cone. Of course, in the right-permutive (or bipermutive) case, a symmetric result holds. We refer to both results as Lemma 4.3.1. A similar result is true for all cellular automata, when started on a point with the right tail $x_{[1,\infty)}$ periodic: At the border of the light-cone, there is no time for computation, so the contents of the light-cone will be *eventually* periodic for all CA. Of course, often, this just means that from some point on, the border of the light cone is no longer carrying any information from the interesting pattern $x_{[-n+1,0]}$.

With the help of Lemma 4.3.1, we now consider the orbits of *subshifts* in bipermutive cellular automata. The focus is on their long-term (asymptotic) dynamics, in particular the set of patterns that will eventually appear during the evolution. As an example, we first illustrate how, for the elementary CA 150, one can build an initial point where 1s are spaced arbitrarily far apart, yet a given word eventually appears at the origin in the orbit of the point, using nothing but the bipermutivity of the CA. See Figure 4.4.

The first nontrivial result that follows from Lemma 4.3.1 is a generalization of the idea in the caption of Figure 4.4. Namely, the property

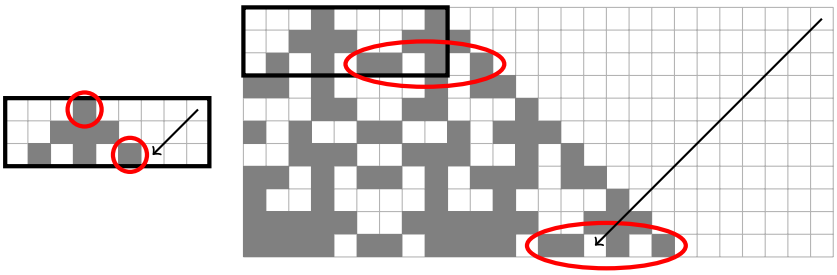


Figure 4.4: We illustrate the idea of building sparse points such that a particular word appears in the evolution, for the CA 150 and the pattern 111 (although it 'accidentally' already appears on the first step). The red circles indicate patterns that reappear on the right border of the light cone (by left-permutivity), and an arrow from cell A to cell B means that permuting the contents of cell A permutes the contents of cell B (by right-permutivity). As the cell A in the rightmost picture is permuted to 1, the cell B pointed to by the arrow changes to 1 as well, and the pattern 111101 (which begins with the desired pattern 111) appears on the right border of the light cone.

of a bipermutive cellular automaton $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ that every word is self-replicating can be used to show that every word occurs in some image $f^n(X)$ – that is, the set of limit points of X in f is the full shift – if the SFT $X \subset S^{\mathbb{Z}}$ satisfies certain mixing properties.

Theorem 4.3.2 *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a bipermutive CA and $X \subset S^{\mathbb{Z}}$ a nontrivial mixing SFT with window size m. If there exists $v_1 \in \mathcal{B}_{m-1}(X)$ such that $v_1 s \in \mathcal{B}_m(X)$ for all $s \in S$, then $\Omega_f(X) = S^{\mathbb{Z}}$.*

Proof. The idea of the proof is simple: Supposing that the claim $w \in \mathcal{B}(\Omega_f(X))$ holds for the word w, we show it holds for wa, for arbitrary $a \in S$. We show this by extending w to the right with a periodic tail so that it eventually repeats on the right border of the light cone by left permutivity and Lemma 4.3.1. Since we have carefully chosen the periodic right tail so that it contains v_1 in just the right place, we can 'shoot a permutation' from the coordinate to the right of v_1 to the coordinate to the right of the repeated occurrence of w, by right permutivity and Lemma 4.3.1. While this is straightforward to formalize, the precise indexing needed is a bit cumbersome.

So, suppose that such a v_1 exists. Without loss of generality we can assume that $v_1^{\mathbb{Z}} \in X$, and that m is also a mixing distance for X. Namely, since periodic points are dense in X, we have $(v'v_1)^{\mathbb{Z}} \in X$ for some $v' \in \mathcal{B}(X)$, and then we can simply replace v_1 by $v'v_1$. Also, it is clear that m can be replaced by a larger value. We will show, by induction on word

length, that for all $w \in S^*$, there exist arbitrarily large $n \in \mathbb{N}$ such that $w \in \mathcal{B}(f^n(X))$, from which the claim then follows. The case $|w| = 0$ is trivial.

Suppose then that the claim holds for $w \in S^*$, and let $s \in S$. We will prove the claim for the word ws. The proof is illustrated in Figure 4.5. Let r and r' be the left and right radii of f, respectively. By the induction hypothesis, for arbitrarily large $n \in \mathbb{N}$, there exists a word $u \in \mathcal{B}_{|w|+n(r+r')}(X)$ such that $f^n(u) = w$. We can take n so large that $f^n(v_1^{\mathbb{Z}}) = v_2^{\mathbb{Z}}$ has the property that $f^p(v_2^{\mathbb{Z}}) = v_2^{\mathbb{Z}}$ for some $p \in \mathbb{N}$, where $|v_2| = m - 1$.

For all $k \in [m, 2m-2]$ we choose a mixing word $z_k \in \mathcal{B}_k(X)$ and an arbitrary left extension $y_k \in S^{-\mathbb{N}}$ such that $x_k = y_k.uz_kv_1^\infty \in X$. Now, $f^n(x_k)_{[rn,\infty)} = wz_k'v_2^\infty$ for some $z_k' \in \mathcal{B}_{k+n(r+r')}(X)$. This is illustrated on line 2 in Figure 4.5.

By Lemma 4.3.1, there exists $t_k > k + n(r + r') + |v_1|$ such that

$$f^{n+\ell t_k}(x_k)_{[r(n+\ell t_k),\infty)} = wz_k'v_2^\infty$$

for all $\ell \in \mathbb{N}$. Let $h = \operatorname{lcm}\{t_k \mid k \in [m, 2m-2]\}$, so that

$$f^{n+h}(x_k)_{[r(n+h),\infty)} = wz_k'v_2^\infty,$$

for all k.

Let now k be such that

$$j = (r + r')(n + h) + |w| \equiv |u| + k \bmod (m - 1). \tag{4.2}$$

We can permute the coordinate j of x_k freely (and choose a new right tail arbitrarily), because (4.2) and the fact that $h > k+n(r+r')+|v_1|$ imply that it is preceded by the word v_1, and m is the window size of X. Permuting the coordinate j in x_k (point A in Figure 4.5) permutes the coordinate $j - r'(n + h) = r(n + h) + |w|$ in $f^{n+h}(x_k)$ (point B in Figure 4.5) without affecting any coordinate to the left of it, and thus all the words ws for $s \in S$ occur in $f^{n+h}(X)$. Since n may be chosen arbitrarily large, this concludes the induction step. ■

As we mentioned in the beginning of the proof of Theorem 4.3.2, both left and right permutivity are really used: As the CA is left-permutive, Lemma 4.3.1 guarantees that w repeats on the right border of the light cone. Right-permutivity on the other hand guarantees that the permutation applied to the coordinate a of x_k propagates along the left side of the light cone to a permutation of the $(n + h)$th image. It is easy to find examples of CA which are left- or right-permutive, but for which Theorem 4.3.2 does not hold (for example, shift maps can be considered to be such examples).

We also note that if X is a proper subshift of $S^{\mathbb{Z}}$, then $\bigcup_{n\in\mathbb{N}} f^n(X)$ is never actually equal to $S^{\mathbb{Z}}$. In fact, for all n, the subshift $f^n(X)$ has the

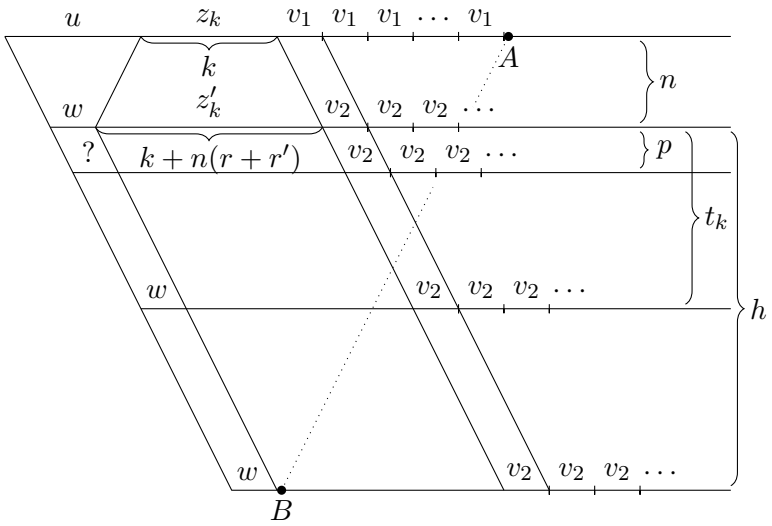


Figure 4.5: A schematic diagram of the proof of Theorem 4.3.2. The coordinate A may be changed to any symbol without changing the left part, and by permuting A, we also permute B.

same entropy as X, since a bipermutive CA is finite-to-one [LM95], and in general its entropy can only decrease. This means that the appearance of all words of S^k for larger and larger k in $f^n(X)$ is somehow compensated by having these words appear in only a small number of different contexts.

Example 4.3.3 *Let $X \subset \{0,1\}^{\mathbb{Z}}$ be the golden mean shift (the SFT with the single forbidden pattern 11), and let $f : \{0,1\}^{\mathbb{Z}} \to \{0,1\}^{\mathbb{Z}}$ be the two-neighbor XOR automaton with neighborhood $\{0,1\}$ and local rule $f_{\mathrm{loc}}(a,b) = a + b$, which is bipermutive. Then*

$$f(X) = \mathcal{B}^{-1}((0^*(11)^*)^*).$$

Thus, $f(X)$ is conjugate to the even shift $\mathcal{B}^{-1}((1^*(00)^*)^*)$ by the CA that applies the permutation (0 1) cellwise, and it is indeed well known that the golden mean shift and the even shift have equal entropy. However, $\mathcal{B}_2(X) = \{00, 01, 10\}$, while $\mathcal{B}_2(f(X)) = \{00, 01, 10, 11\}$.

We continue one more step:

$$f^2(X) = \mathcal{B}^{-1}((0^*10(00)^*1)^*),$$

the binary subshift where every second maximal contiguous segment of 0s between two 1s (counting empty segments between adjacent 1s as even seg-

ments of 0*s) is of odd length. Note that*

$$\begin{aligned}\mathcal{B}_3(X) &= \{000, 001, 010, 100, 101\},\\ \mathcal{B}_3(f(X)) &= \{000, 001, 011, 100, 101, 110, 111\},\\ \mathcal{B}_3(f^2(X)) &= \{000, 001, 010, 011, 100, 101, 110\}, \text{and}\\ \mathcal{B}_3(f^3(X)) &= \{000, 001, 010, 011, 100, 101, 110, 111\}.\end{aligned}$$

but all four subshifts X*,* $f(X)$*,* $f^2(X)$ *and* $f^3(X)$ *necessarily all have equal entropy. This example also shows that the convergence to the full language is not monotone, since*

$$010 \in (\mathcal{B}_3(X) \cap \mathcal{B}_3(f^2(X))) \setminus \mathcal{B}_3(f(X)).$$

Let $Y \subset S^{\mathbb{Z}}$ be a subshift. If these exists $m \in \mathbb{N}$ such that no word $w \in \mathcal{B}_m(Y)$ can be followed in Y by every letter of S, then the entropy of Y satisfies $h(Y) \leq \log(|S| - 1)$. If Y is also binary, then the existence of such an m implies that Y is periodic. Thus we have the following corollaries to Theorem 4.3.2.

Corollary 4.3.4 *If* $Y \subset S^{\mathbb{Z}}$ *is a mixing SFT with* $h(Y) > \log(|S| - 1)$ *and the automaton* $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ *is bipermutive, then* $\Omega_f(Y) = S^{\mathbb{Z}}$*.*

Corollary 4.3.5 *If* $Y \subset \{0, 1\}^{\mathbb{Z}}$ *is a nontrivial mixing SFT and the automaton* $f : \{0, 1\}^{\mathbb{Z}} \to \{0, 1\}^{\mathbb{Z}}$ *is bipermutive, then* $\Omega_f(Y) = \{0, 1\}^{\mathbb{Z}}$*.*

In the special case that the alphabet is a group of prime order and the cellular automaton is a homomorphism, we can relax our assumptions on the SFT X. We only sketch the proof of the following result, as it is mostly the same as that of Theorem 4.3.2.

Theorem 4.3.6 *Let* $p \in \mathbb{N}$ *be a prime, let* $S = \mathbb{Z}_p$*, let the CA* $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ *be a group endomorphism with minimal neighborhood size at least* 2*, and let* $X \subset S^{\mathbb{Z}}$ *be a nontrivial mixing SFT. Then* $\Omega_f(X) = S^{\mathbb{Z}}$*.*

Proof sketch. First, note that f is automatically bipermutive, since the symbol endomorphisms are permutations of S. Since X is nontrivial, there exists a long word $v_1 \in \mathcal{B}(X)$ such that $v_1a, v_1b \in \mathcal{B}(X)$ for some $a \neq b \in \mathbb{Z}_p$. Let $wc \in \mathcal{B}(\Omega_f(X))$ for some $c \in \mathbb{Z}_p$, and as in the proof of Theorem 4.3.2, there exist $k \in \mathbb{N}$ and $u \in \mathcal{B}(X)$ such that uv_1a is an f^{pk}-preimage of wc. Then uv_1b is an f^{pk}-preimage of wd, where $d = c+b-a$ in $\mathbb{Z}_p$ since f is homomorphic. After p such operations, we see that $we \in \mathcal{B}(\Omega_f(X))$ for all $e \in \mathbb{Z}_p$. ■

Theorem 4.3.6 can be thought of as a kind of topological analogue of Theorem 5.3 in [Piv12] (proved in [PY04]), which in particular states that

the ergodic averages of Markov measures with full support converge to the uniform Bernoulli measure in the weak-star topology, under the action of a bipermutive homomorphic CA on $\mathbb{Z}_p^{\mathbb{Z}}$. The automaton is said to *asymptotically randomize* such a measure. Using analogous terminology, we can say that a CA f *topologically randomizes* a subshift X if $\Omega_f(X) = S^{\mathbb{Z}}$, and Theorem 4.3.6 then states that a bipermutive homomorphic CA topologically randomizes every nontrivial mixing SFT $X \subset \mathbb{Z}_p^{\mathbb{Z}}$. Theorem 4.3.2 can of course also be phrased in terms of topological randomization, but the class of subshifts randomized is not quite as natural (see Question 4.3.9).

There is also a more familiar meaning to these results, as topological randomization for a left (or right) permutive cellular automaton in fact corresponds to the existence of a transitive point.

Theorem 4.3.7 *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a left permutive CA with neighborhood $[-r, r']$, where $r > 0$, and let $X \subset S^{\mathbb{Z}}$ be a mixing SFT. Then $\Omega_f(X) = S^{\mathbb{Z}}$ if and only if X contains a transitive point for f, that is, $\exists x \in X : \omega_f(x) = S^{\mathbb{Z}}$.*

Proof. If $\exists x \in X : \omega_f(x) = S^{\mathbb{Z}}$, then clearly $\Omega_f(X) = S^{\mathbb{Z}}$.

Now, suppose $\Omega_f(X) = S^{\mathbb{Z}}$. We show that given any $w \in \mathcal{B}_p(X)$ and $v \in S^p$, there exist $x \in X$ and $N \in \mathbb{N}$ such that $x_{[0,p-1]} = w$ and $f^N(x)_{[0,p-1]} = v$. We may assume without loss of generality that $w^{\mathbb{Z}} \in X$, and then there exist $m, t \in \mathbb{N}$ such that $f^m(w^{\mathbb{Z}}) = f^{t+m}(w^{\mathbb{Z}}) = u^{\mathbb{Z}}$ for some $u \in \mathcal{B}(X)$. Since $\Omega_f(X) = S^{\mathbb{Z}}$, there exists $M \geq m$ and $v_1 v_2 \in \mathcal{B}(X)$ such that $f^M(v_1 v_2) = v$ and $|v_1| = rM$. Define $y = z v_1 . v_2 w' w^{\infty}$, where $z \in S^{-\mathbb{N}}$ and $w' \in \mathcal{B}(X)$ are chosen such that $y \in X$ and p divides $|v_2 w'|$. Now, $f^M(y) = z' . v w'' u'^{\infty}$ for some $z' \in S^{-\mathbb{N}}$, $w'' \in (S^p)^*$ and $u' \in S^p$. Lemma 4.3.1 now implies that for $C = pt(|S|^{p+|w''|})!$ and all $\ell \in \mathbb{N}$, we have $f^{M+\ell C}(y)_{\ell r C + [0,p-1]} = v$. Since $y_{\ell r C + [0,p-1]} = w$ for large enough ℓ, some translate of y can be chosen as x. ■

The notion that 'the asymptotic set of f from X is $S^{\mathbb{Z}}$', that is, $\omega_f(X) = S^{\mathbb{Z}}$, fits into the picture in the obvious way: in general,

$$\exists x \in X : \omega_f(x) = S^{\mathbb{Z}} \implies \omega_f(X) = S^{\mathbb{Z}} \implies \Omega_f(X) = S^{\mathbb{Z}}.$$

The next (rather trivial) example shows that the restriction to a group of prime order is necessary in Theorem 4.3.6, that just mixing does not suffice for proving Theorem 4.3.2, and that entropy $h(Y) \geq \log(|S|/2)$ is not enough for Corollary 4.3.4.

Example 4.3.8 *Let $f : \{0,1\}^{\mathbb{Z}} \to \{0,1\}^{\mathbb{Z}}$ be the elementary CA 150, $X = (\{0,1\} \times \{0\})^{\mathbb{Z}} \subset (\{0,1\}^2)^{\mathbb{Z}} = Y$ and $g = f \times f$. Then X is a mixing SFT with $h(X) = \log 2$, g is homomorphic and bipermutive, and $h(Y) = \log 4$, but $g(X) = X$.*

Here, the CA g is a group homomorphism, and $\mathcal{B}_1(X)$ is a subgroup of the full group that g cannot expand. We do not know whether such cheating is the only way to guarantee that a mixing SFT does not expand to the full shift. In fact, we do not know whether a bipermutive CA randomizes every mixing SFT that uses the full alphabet.

Question 4.3.9 *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a bipermutive cellular automaton, and $Y \subset S^{\mathbb{Z}}$ a nontrivial mixing SFT with $\mathcal{B}_1(Y) = S$. Do we then have $\Omega_f(Y) = S^{\mathbb{Z}}$?*

A positive solution to Question 4.3.9 seems plausible, especially if f is also a group homomorphism, and would extend Theorem 4.3.2 to a much more natural class of topologically randomized subshifts.

Definition 4.3.10 *Let $0 \in S$ and $d, k \geq 1$. The* k-sparse subshift *of dimension d is the SFT $X \subset S^{\mathbb{Z}^d}$ defined by the forbidden patterns*

$$\{P \in S^{[1,k]^d} \mid |P|_0 \leq k^d - 2\}.$$

For example, the one-dimensional binary 2-sparse subshift is just the golden mean shift, since it is defined by the set of forbidden patterns

$$\{w \in \{0,1\}^2 \mid |w|_0 \leq 0\} = \{11\}.$$

We can apply Theorem 4.3.2 to such subshifts to obtain concrete examples of simple subshifts that bipermutive automata take to the full shift in the limit, as the k-sparse subshift obviously satisfies the assumption of Theorem 4.3.2. This observation (and especially its generalization Proposition 4.3.16) is useful in the study of commutation of cellular automata, as we will see in the next section.

Corollary 4.3.11 *Let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a bipermutive CA, $k \in \mathbb{N}$, and $X \subset S^{\mathbb{Z}}$ the k-sparse subshift. Then $\Omega_f(X) = S^{\mathbb{Z}}$. In fact, X contains a transitive point for f.*

Proof. Combine Theorem 4.3.2 and Theorem 4.3.7. ■

While it is hard to say much about multidimensional SFTs in general, we can at least extend Corollary 4.3.11 to higher dimensions. The proof is essentially the same as that of Theorem 4.3.2, but we use some additional tricks to make the argument cleaner. Namely, we apply a certain transformation of $SL_d(\mathbb{Z})$ to make the neighborhood shape more suitable, and then use a similar shoot-and-reperiodize technique as in [Sal12] to partially reduce the problem to the one-dimensional case.

Definition 4.3.12 *For $\vec{n} = (n_1, \ldots, n_d) \in \mathbb{Z}^d$, denote $\pi(\vec{n}) = n_1$. A set $N \subset Z^d$ is* pointy*, if*

$$|N \cap \pi^{-1}(\min \pi(N))| = |N \cap \pi^{-1}(\max \pi(N))| = 1.$$

Lemma 4.3.13 *Let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a cellular automaton. Then, there exists $A \in SL_d(\mathbb{Z})$ such that $A(f)$ has a pointy neighborhood.*

Proof. For $n = (n_2, \ldots, n_d) \in \mathbb{N}^{d-1}$, define the *shear map* A_n by

$$A_n(x_1, x_2, \ldots, x_d) = (x_1 + \sum_{i=2}^{d} n_i x_i, x_2, \ldots, x_d).$$

We have $A \in SL_d(\mathbb{Z})$ for all $n \in \mathbb{N}^{d-1}$, since A is given by an upper triangular matrix with only 1s on the diagonal, and thus has determinant 1. Now, let $N \subset \mathbb{Z}^d$ be the neighborhood of f. It is easy to see that if we choose n suitably, the image $A(N)$ is pointy, and thus $A(f)$ has a pointy neighborhood. ■

Definition 4.3.14 *Let*

$$X_p^d = \{x \in S^{\mathbb{Z}^d} \mid \forall i \in \{2, \ldots, d\} : \sigma^{pe_i}(x) = x\},$$

where $(e_i)_i$ are the natural basis of $\mathbb{Z}^d$. The natural bijection between X_p^d and $(S^{p^{d-1}})^{\mathbb{Z}}$, is called ρ_p^d.

Thus, X_p^d is the d-dimensional full shift restricted to points with period $p \in \mathbb{N}$ in all but the first dimension. The usefulness of pointy neighborhoods comes from the following observation.

Lemma 4.3.15 *Let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a totally extremally permutive CA with a pointy neighborhood. Then for all p, the automaton $f' = \rho_p^d(f) : (S^{p^{d-1}})^{\mathbb{Z}} \to (S^{p^{d-1}})^{\mathbb{Z}}$ defined by $f' = \rho_p^d \circ f \circ (\rho_p^d)^{-1}$ is bipermutive.*

Proposition 4.3.16 *If the CA $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ is totally extremally permutive with quiescent state 0, then $\Omega_f(X) = S^{\mathbb{Z}^d}$, where X is the d-dimensional k-sparse subshift.*

Proof. We prove here the case $d = 2$. The general case follows similarly, but is notationally more complex. We first ensure that the neighborhood is pointy (the first axis is the horizontal one) and is located at the west border of the east half-plane, so that on points with a vertical period, a one-dimensional bipermutive CA with right speed of light 0 is simulated. The general idea is to successively draw larger and larger patterns at the origin

as follows: As vertically periodic points are in a sense just one-dimensional (horizontal) points, we can apply Lemma 4.3.1 to any vertically periodic and horizontally 0-finite point to obtain that any finite set of columns repeats infinitely many times in the orbit. Now, as in the proof of Theorem 4.3.2, we carefully shoot a signal in the right cell at the right time, and add a huge vertical period to conclude the induction step.

Let us make this precise. We may assume without loss of generality that the lexicographically minimal element in the neighborhood of f is $(0, 0)$, and that the maximal is (m_1, m_2) with $m_1 > 0$. We may also assume that f has a pointy neighborhood by Lemma 4.3.13. Note that applying a shear map of course changes the k-sparse subshift as well. However, for any shear map A and any k, there exists $k' > k$ such that the A-image of the k'-sparse subshift is included in the k-sparse subshift. Thus, if we prove the claim for arbitrarily large k and CA with pointy neighborhoods, the claim follows for arbitrarily large k and all CA.

Let $n \geq k$, and let $P \in S^{n \times n}$ be arbitrary. We inductively construct vertically periodic points $x^i \in X$ such that the lexicographical prefix of P of size i occurs in some $f^t(x^i)$ at the origin, and $x^i_{(a,b)} = 0$ for all $b \in \mathbb{Z}$ for large enough $a \in \mathbb{Z}$. For x^1, we choose $x^1_{(0,nm)} = P_{(0,0)}$ for all $m \in \mathbb{Z}$, and $x^1_{\vec{n}} = 0$ for all other $\vec{n} \in \mathbb{Z}^2$.

Suppose then that x^i has already been constructed, and let $p \in \mathbb{N}$ be its vertical period. By Lemma 4.3.15, when restricted to the set X^2_p, f simulates a bipermutive one-dimensional CA $g : (S^p)^{\mathbb{Z}} \to (S^p)^{\mathbb{Z}}$ through the bijection ρ^2_p. Denote $H = \{(a, b) \mid a \geq 0\} \subset \mathbb{Z}^2$. Since $\rho^2_p(x^i)_\ell = 0^p$ for all large enough $\ell \in \mathbb{Z}$ and the left radius of g is 0, we can use Lemma 4.3.1 to conclude that there exist arbitrarily large $t > 0$ such that $x^i|_H = f^t(x^i)|_H$.

Now, there are arbitrarily large $t \in \mathbb{N}$ such that $f^t(x^i)$ contains the lexicographical prefix of P of size i at the origin. Let thus t be larger than the maximal $a \in \mathbb{Z}$ with $x^i_{(a-k,b)} \neq 0$ for some $b \in \mathbb{Z}$. Let (c, d) be the lexicographically $(i + 1)$th coordinate of P. We let $y(s)^i \in X$ be as x^i, but with the coordinate (tm_1+c, tm_2+d) containing $s \in S$. Now, permuting s in $y(s)^i$ permutes $f^t(y(s)^i)_{(c,d)}$, so we can choose s so that $f^t(y(s)^i)_{(c,d)} = P_{(c,d)}$, and denote $y^i = y(s)^i$.

Since (m_1, m_2) is the lexicographically maximal vector in the neighborhood of f, (c, d) is the lexicographically minimal coordinate which can change in $f^t(y(s)^i)$, when we permute s. Thus, $f^t(y^i)$ contains the lexicographical prefix of P of size $i + 1$ at the origin. We obtain x^{i+1} from y^i by adding any sufficiently large vertical period. ■

Similarly to how Theorem 4.3.2 could be generalized to Theorem 4.3.6, we can generalize Proposition 4.3.16 to Proposition 4.3.17. We omit the proof.

Proposition 4.3.17 *Let $p \in \mathbb{N}$ be a prime, let $S = \mathbb{Z}_p$, let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a group homomorphism with at least two neighbors, and let $Y \subset S^{\mathbb{Z}^d}$ be the k-sparse shift. Then $\Omega_f(\{0,1\}^{\mathbb{Z}^d} \cap Y) = S^{\mathbb{Z}}$.*

4.3.2 Counting and Describing the CA

In this section, we give mixing SFTs and d-dimensional full shifts an algebraic structure with a bipermutive, and more generally totally extremally permutive cellular automaton. This, of course, amounts to the study of the centralizer of such an automaton. First, we consider the size of the centralizer, and find that it is very small in general. As in Section 4.2.4, we then look at what happens when the totally extremally permutive CA is also a homomorphism (or more generally, homomorphic+C) on a full shift with cellwise defined group structure – that is, we again give the subshift both the structure of a group, and a structure by unary operations. We can always find such a map in the abelian case, and it turns out that such maps necessarily 'capture' the endomorphism monoid of the group structure, see Theorem 4.3.25.

We first prove a strong upper bound on the number of commuting cellular automata of any radius. This result is based on the following lemma, which relates the centralizer of a given CA f to the f-orbit closures of subshifts.

Definition 4.3.18 *Let X be a subshift, $f : X \to X$ a cellular automaton and $Y \subset X$ a subshift of X. We define the* f-orbit closure *Y^f of Y to be the set $\overline{\bigcup_{i\in\mathbb{N}} f^i(Y)}$.*

Lemma 4.3.19 *Let $X \subset S^{\mathbb{Z}^d}$ be a subshift, let $f : X \to X$ be a CA and let $Y \subset X$ with $Y^f = X$. Then the map $\phi : C(f) \to X^Y$ defined by $\phi(g) = g|_Y$ is injective.*

In other words, the restriction of a cellular automaton in the centralizer of f to the subshift Y determines it uniquely. Note also that we always have $\Omega_f(Y) \subset Y^f$, so that $Y^f = X$ is a weaker assumption than $\Omega_f(Y) = X$.

Proof. Let $g, h \in C(f)$ be such that $g|_Y = h|_Y$, and let $x \in X$ be arbitrary. Let $r \in \mathbb{N}$ be a common radius for g and h, and let $y \in Y$ and $i \in \mathbb{N}$ be such that $f^i(y)_{[-r,r]^d} = x_{[-r,r]^d}$. Then, since $g, h \in C(f)$, we have

$$g(x)_0 = g(f^i(y))_0 = f^i(g(y))_0 = f^i(h(y))_0 = h(f^i(y))_0 = h(x)_0.$$

Since x was arbitrary, we have $g = h$. ■

Proposition 4.3.20 *Let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a totally extremally permutive CA with a quiescent state $0 \in S$. For all $n \in \mathbb{N}$, define*

$$C_n(f) = \left\{ g \in C(f) \mid [0, n-1]^d \text{ is a neighborhood for } g \right\}.$$

Then $|C_n(f)| \leq |S|^{1+n^d(|S|-1)}$. *If* $S = \mathbb{Z}_p$ *for a prime* $p \in \mathbb{N}$ *and* f *is a group homomorphism, then* $|C_n(f)| \leq |S|^{1+n^d}$.

Proof. Let $X \subset S^{\mathbb{Z}^d}$ be the n-sparse shift. Proposition 4.3.16 and Lemma 4.3.19 together imply that $|C_n(f)|$ is at most the number of local maps $\mathcal{B}_{[0,n-1]^d}(X) \to S$. Since we have $|\mathcal{B}_{[0,n-1]^d}(X)| = 1 + n^d(|S| - 1)$, the number of such maps is $|S|^{1+n^d(|S|-1)}$. In the homomorphic case, apply Proposition 4.3.17 to replace X with $Y = X \cap \{0,1\}^{\mathbb{Z}^d}$, where we have $|\mathcal{B}_{[0,n-1]^d}(Y)| = 1 + n^d$. ■

Thus, the density of the centralizer of any totally extremally permutive CA is 0. In other words:

Theorem 4.3.21 *Let* $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ *be a totally extremally permutive CA. Then the endomorphism monoid* $\mathrm{End}(S^{\mathbb{Z}^d}, f)$ *is sparse.*

In [MB97], it was proved that if $f, g : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ are commuting radius-$\frac{1}{2}$ (that is, neighborhood $\{0,1\}$) cellular automata and f is bipermutive, then there exist functions $\phi, \psi : S \to S$ such that $g_{\mathrm{loc}}(a,b) = f_{\mathrm{loc}}(\phi(a), \psi(b))$ (g is an *isotope* of f). From this one can compute the weaker upper bound of $\frac{1}{2}$ for the density of the centralizer of a bipermutive CA.

Next, we turn to homomorphic+C totally extremally permutive cellular automata on $S^{\mathbb{Z}^d}$, where S is a finite group. As in the case of color blind CA (Lemma 4.2.38), there is nothing of interest to say when S is not abelian.

Lemma 4.3.22 *Let* S *be a finite group, and suppose there exists a totally extremally permutive and homomorphic+*C *cellular automaton on* $S^{\mathbb{Z}^d}$ *with minimal neighborhood of size at least* 2. *Then,* S *is abelian.*

Proof. If there exists such a homomorphic+C cellular automaton, then there must in particular exist a *homomorphism* f with minimal neighborhood N of size at least 2. It is easy to see that any symbol endomorphism corresponding to a coordinate that is in a corner of N is surjective, and thus S is abelian by Lemma 4.1.9. ■

Conversely, it is easy to find totally extremally permutive homomorphic maps in the abelian case.

Lemma 4.3.23 *Let* S *be a finite abelian group. Then there exists a totally extremally permutive and homomorphic cellular automaton* g *on* $S^{\mathbb{Z}^d}$ *with minimal neighborhood of size at least* 2. *Furthermore, we can ensure that* $C(g)$ *contains all homomorphic CA, and* g *maps all unary points to* $0^{\mathbb{Z}^d}$.

Proof. Any nontrivial sum of shifts is totally extremally permutive and homomorphic. Furthermore, if f is homomorphic, then

$$f(g(x)) = f(\sum_{i \in I} \sigma^{k_i}(x)) = \sum_{i \in I} f(\sigma^{k_i}(x)) = \sum_{i \in I} \sigma^{k_i}(f(x)) = g(f(x)).$$

If $|I| = |S|$, then g maps all unary points to $0^{\mathbb{Z}^d}$. ■

In [MB97] it was proved, using algebraic methods, that among CA with radius 1/2, bipermutive homomorphic+C CA can only commute with homomorphic+C CA. We show the small step required to generalize this result for our definition of centralizer in one dimension.[2]

Theorem 4.3.24 *Let S be a finite group, let $f : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ be a bipermutive and homomorphic+C CA (so that S is abelian), and let $g : S^{\mathbb{Z}} \to S^{\mathbb{Z}}$ commute with f. Then g is homomorphic+C.*

Proof based on the results of [MB97]. By composing with shifts, we may assume f has neighborhood $[0, m_f]$ and g has neighborhood $[0, m_g]$. Then, since g commutes with f, it also commutes with f^k. Let k be large enough that $m_f \cdot k \geq m_g$. Then, the $m_f \cdot k$ blocking of f^k (the automaton obtained from f^k by joining blocks of $m_f \cdot k$ consecutive cells into single symbols) is bipermutive and homomorphic+C with radius 1/2, and the corresponding blocking h of g has radius 1/2. Thus, the result of [MB97] applies, and h is an homomorphic+C self-map of $(S^{m_f \cdot k})^{\mathbb{Z}}$.

From this, we easily obtain that also g must be homomorphic+C for $S^{\mathbb{Z}}$. Namely, the constant associated with h must be of the form $a^{m_f \cdot k}$ for some $a \in S$, since $h((0^{m_f \cdot k})^{\mathbb{Z}})$ is a blocking of the unary point $g(0^{\mathbb{Z}})$. Because the blocking operation is a group isomorphism between $S^{\mathbb{Z}}$ and $(S^{m_f \cdot k})^{\mathbb{Z}}$, we obtain that $x \mapsto g(x) - a^{\mathbb{Z}}$ is a homomorphic cellular automaton on $S^{\mathbb{Z}}$, so that g is indeed homomorphic+C. ■

We can also prove this directly, using Lemma 4.3.1:

Proof using Lemma 4.3.1. First, we can assume that f has a unary fixed point $a^{\mathbb{Z}}$ by taking powers of f, and we denote $g(a^{\mathbb{Z}}) = b^{\mathbb{Z}}$. Now, f also fixes $b^{\mathbb{Z}}$. Without loss of generality, assume f has neighborhood $[0, m]$ and g has neighborhood $[0, n]$. Let $w \in S^{2n+1}$ and $e \in \{a, b\}$, and let $y \in S^{\mathbb{Z}}$ be the point with $y_{[-n,n]} = w$ and $y_i = e$ for $i \notin [-n, n]$. Denote $M = (|S|^{2n+1})!$ and apply Lemma 4.3.1, so that

$$f^M(y)_j = f^M(y)_{j-mM} = w_j \tag{4.3}$$

for all $j \in [-n, n]$.

Let then $w^1, w^2 \in S^{n+1}$, let $x \in S^{\mathbb{Z}}$ be the point with $x_j = w^1_j$ and $x_{j+mM} = w^2_j$ for all $j \in [0, n]$, and a everywhere else. By (4.3) and the fact f is homomorphic+C we have

$$f^M(x)_j = w^1_j + w^2_j - C$$

[2]Of course, [MB97] studies cellular automata with radius 1/2 precisely because all cellular automata can be reduced to such CA with a blocking operation, but the authors do not make the complete proof very explicit.

for all $j \in [0, n]$ and some constant $C \in S$. Thus we have $g(f^M(x))_{\vec{0}} = g_{\text{loc}}(w^1 + w^2 - \underbrace{(C, \dots, C)}_{n+1})$. On the other hand, we have $g(x)_j \neq b$ only when $j \in [-n, n]$ or $j - mM \in [-n, n]$, so using the fact f is homomorphic+C and (4.3), we see that $f^M(g(x))_{\vec{0}} = g_{\text{loc}}(w^1) + g_{\text{loc}}(w^2) - C$. Since f and g commute, these values are equal, and thus g is homomorphic+C by Lemma 4.1.11 (setting $c = (C, \dots, C)$ and $d = C$). ■

Now, let us reduce the multidimensional case to the one-dimensional case. For this, note that if $A = SL_d(\mathbb{Z})$, then $A(f)$ is totally extremally permutive, homomorphic or homomorphic+C if and only if f is.

Theorem 4.3.25 *Let S be a finite group, $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ a totally extremally permutive and homomorphic+C CA (so that S is abelian), and let $g : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ commute with f. Then g is homomorphic+C.*

Proof. We only present a proof for $d = 2$. We first modify the neighborhoods of f and g. First, we compose with a shift so that the lexicographically minimal element in the neighborhood of f is $(0, 0)$. Then, we ensure that for the lexicographically maximal element (m_1, m_2) of the neighborhood, we have $m_1 > 0$ by considering $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)(f)$ instead in the case $m_1 = 0$. We also make sure f has a pointy neighborhood by applying Lemma 4.3.13. These transformations amount to mapping $f \mapsto \sigma^{\vec{v}}(A(f))$ for some $A \in SL_2(\mathbb{Z})$ and $\vec{v} \in \mathbb{Z}^2$. Note that $f' = \sigma^{\vec{v}} \circ A(f)$ and $g' = \sigma^{\vec{v}'} \circ A(g)$ commute for all $\vec{v}' \in \mathbb{Z}^2$, and f' is homomorphic+C and totally extremally permutive.

Now, let the neighborhood of g' be contained in $[0, p-1]^2$ (by choosing $\vec{v}'$ appropriately), and consider the vertically periodic subshift $X = X_p^2$. The restrictions $f'|_X$ and $g'|_X$ simulate one-dimensional cellular automata on $(S^p)^{\mathbb{Z}}$ through the bijection ρ_p^2. By Lemma 4.3.15, the one-dimensional CA corresponding to $f'|_X$ is bipermutive, and it is clearly homomorphic+C. Then, by Theorem 4.3.24, $g'|_X$ is homomorphic+C. Since g' has neighborhood $[0, p-1]^2$, as in our first proof of Theorem 4.3.24, we then see that g' is homomorphic+C too. Finally, g is homomorphic+C since transformations of $SL_d(\mathbb{Z})$ are group isomorphisms. ■

For the special case of totally extremally permutive *homomorphic* CA on a group of prime order, there is a very nice characterization for the centralizer restricted to CA with quiescent state 0. This can be seen as a corollary of the previous results, but we present a very short direct proof based on Proposition 4.3.17 and Lemma 4.3.19.

Proposition 4.3.26 *Let $S = \mathbb{Z}_p$, let $f : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ be a totally extremally permutive homomorphism. Then $g : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ with $g(0^{\mathbb{Z}^d}) = 0^{\mathbb{Z}^d}$ commutes with f if and only if g is homomorphic.*

Proof. Let g have radius r. Then $X^f = S^{\mathbb{Z}}$, where $X = \{0,1\}^{\mathbb{Z}^d} \cap Y$ and Y is the r-sparse shift, by Proposition 4.3.17. As $S = \mathbb{Z}_p$, it follows easily from Lemma 4.1.8 that all homomorphic automata commute (we only stated it in the one-dimensional case, but the proof applies in the general case as well), so in particular $h \circ f = f \circ h$ for the unique homomorphic automaton defined by $h|_X = g|_X$. Thus, $g = h$ by Lemma 4.3.19. ■

Finally, we show how to exactly capture the endomorphism monoid:

Theorem 4.3.27 *Let $(S^{\mathbb{Z}^d}, +)$ be a cellwise abelian group shift. Then there exists a cellular automaton $g : S^{\mathbb{Z}^d} \to S^{\mathbb{Z}^d}$ such that*

$$\mathrm{End}(S^{\mathbb{Z}^d}, +) = \mathrm{End}(S^{\mathbb{Z}^d}, g).$$

Proof. Let g be given by Lemma 4.3.23. Then every homomorphic CA commutes with g, and by Theorem 4.3.25, all cellular automata that commute with g are homomorphic+C. Since g maps all unary points to $0^{\mathbb{Z}^d}$, we see as in the proof of Lemma 4.2.25 that any CA commuting with g must map $0^{\mathbb{Z}^d}$ to $0^{\mathbb{Z}^d}$, and no homomorphic+C CA with a nontrivial constant satisfies this. Thus, $\mathrm{End}(S^{\mathbb{Z}^d}, +) = \mathrm{End}(S^{\mathbb{Z}^d}, g)$. ■

As far as I know, no bipermutive CA with strong computational properties is known, but neither is a reason why there couldn't exist one. In the sense of predictability, they have no computational properties: since bipermutive CA are transitive, the whole class of bipermutive CA is predictable – any word v is reachable from any word u in the action of any bipermutive CA, so the algorithm need only say 'yes'. By Proposition 4.3.20, a CA in the centralizer of a bipermutive CA on $S^{\mathbb{Z}}$ is determined uniquely by the images of ${}^{\infty}0s0^{\infty}$ for $s \in S$, and is thus very small. However, it is hard to say what this set actually looks like.

Question 4.3.28 *Is there a bipermutive CA with an unpredictable centralizer?*

The centralizer of a homomorphic+C bipermutive CA consists of only homomorphic+C CA. Thus, the question of predictability reduces to the corresponding question for group homomorphisms. On some group shifts $S^{\mathbb{Z}}$, such as $S = \prod_{i=1}^{m} \mathbb{Z}_{p_i^{m_i}}$ for distinct primes p_i and $m_i = 1$ for all i, all homomorphic CA (and thus also homomorphic+C CA) are Cartesian products of bipermutive CA, as an easy corollary of Lemma 4.1.8, and then the prediction problem is again trivial.

4.4 Cellular Automata on Lattice Subshifts

This section is based on [ST12c].

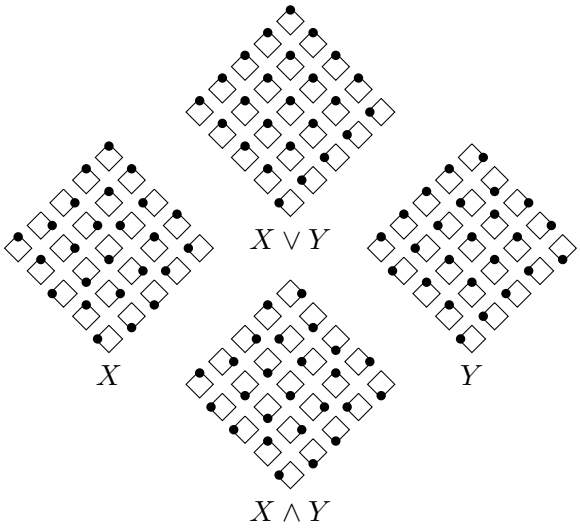
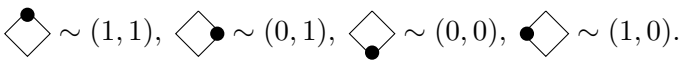


Figure 4.6: A run of the lattice homomorphic CA of Example 4.4.1.

We consider the self-maps of full shifts with a cellwise lattice structure (and other varieties that satisfy what we call the congruence-product property) whose local rule is surjective. Our main objective is correcting a mistake in [ST12c].

Example 4.4.1 *We define the* diamond lattice $S = \{$  $,$$,$$,$$\}$. *The diamond represents the Hasse diagram of S, and the dots represent the location of an element in the diagram. More precisely, $S \sim \{0,1\}^2$, the direct product of two copies of the two-element lattice $\{0,1\}$ where $0 < 1$, and*



We define a CA with radius $1/2$ *(neighborhood* $\{0,1\}$*, with the neighbors thought of as the top left and top right neighbor, and pictures drawn slanted) on* $S^{\mathbb{Z}}$ *by* $f_{\text{loc}}((a,b),(c,d)) = (a,d)$*. It can be checked that this CA is lattice homomorphic. Two pictures of its runs, and their cellwise meet and join, are show in Figure 4.6*

Of course, while the picture is arguably pretty nice, this is a rather trivial CA: it is nothing but a CA on two binary tracks that shifts one track to the left, and one track to the right. We now show that this is, in a sense, the best one can do.

Let $\mathcal{F}$ be a variety, and S a finite member of $\mathcal{F}$. We only consider cellwise defined algebraic structures of $S^{\mathbb{Z}}$ in this section.

Definition 4.4.2 *The variety $\mathcal{F}$ has the* congruence-product property*, if for all finite families $(S_i)_{i\in[1,n]}$ of algebras in $\mathcal{F}$ we have that*

$$\mathrm{Con}(\prod_{i=1}^{n} S_i) = \prod_{i=1}^{n} \mathrm{Con}(S_i) \ .$$

A proof of the following can be found, for example, in [Grä71].

Lemma 4.4.3 *The variety of lattices has the congruence-product property.*

We show that if $\mathcal{F}$ has the congruence-product property, then the $\mathcal{F}$-homomorphic cellular automata have very simple limit sets and limit dynamics. In particular, by the above lemma, our results hold for lattice-homomorphic automata.

Lemma 4.4.4 *Let $\mathcal{F}$ be a variety with the congruence-product property and $S \in \mathcal{F}$ finite. Let $f_{\mathrm{loc}} : S^{2r+1} \to S$ be surjective and $\mathcal{F}$-homomorphic. Denote by π'_i the canonical projections $S^{2r+1} \to S$. Let $\prod_{i=1}^{m} S_i$ be a decomposition of S into directly indecomposable algebras, and denote by π_i the canonical projections $S \to S_i$. Then for each $i \in [1, m]$ there exist j_i, k_i and a surjective $\mathcal{F}$-homomorphism $h_i : S_{j_i} \to S_i$ such that $\pi_i \circ f_{\mathrm{loc}} = h_i \circ \pi_{j_i} \circ \pi'_{k_i}$.*

Proof. Denote $f_i = \pi_i \circ f_{\mathrm{loc}}$ and $n = 2r + 1$, and decompose the domain $S^n = \prod_{j=1}^{n} \prod_{k=1}^{m} S_k$ into the directly indecomposable algebras S_k. Now $\ker f_i$ is a congruence, and since $f_i(S^n) = S_i$ is directly indecomposable, the homomorphism theorem states that $S^n / \ker f_i$ must be directly indecomposable. Since $\mathcal{F}$ has the congruence-product property, we have that $\ker f_i = \prod_{j=0}^{nm} (\sim_j) \ \in \prod_{j=1}^{n} \prod_{k=1}^{m} \mathrm{Con}(S_k)$, and now only one of these $\sim_j$ can be nontrivial, or $S^n / \ker f_i$ has a nontrivial decomposition. Thus f_i is of the desired form. ■

We obtain an interesting simplicity result for full lattice shifts for cellular automata with a surjective local rule. The proof is essentially that of Theorem 4 in [ST12c], but the statement is different – the without loss of generality claim in the beginning of the proof in [ST12c] is wrong, and although it seems minor, I do not know how to fix it (nor whether it is fixable). My apologies to those inflicted.

Theorem 4.4.5 *Let $\mathcal{F}$ be a variety with the congruence-product property (for example, the variety of lattices) and $S \in \mathcal{F}$ finite. Then there exists $p, n \in \mathbb{N}$ such that for any $\mathcal{F}$-homomorphic cellular automaton f on $S^{\mathbb{Z}}$ such that $f_{\mathrm{loc}} : S^{2r+1} \to S$ is surjective, the limit set of f is $f^n(S^{\mathbb{Z}})$, which is conjugate to a product of subshifts $\prod_{i\in\mathcal{I}} S_i^{\mathbb{Z}}$, and on this limit set, f^p is conjugate to a Cartesian product of shift maps on the tracks $S_i^{\mathbb{Z}}$.*

Proof. Let $\prod_{i=1}^{m} S_i$ be the decomposition of S into directly indecomposable algebras. We apply Lemma 4.4.4, and define $H = (\{S_1, \dots, S_m\}, E)$ as the directed graph where $(S_i, S_j) \in E$ if the domain of the surjective map h_j given by Lemma 4.4.4 is S_i. Since each S_i has exactly one incoming arrow, every strongly connected component of H is a cycle or a single vertex. Let S_i be in a cycle, say $S_i \to S_{i_1} \to \cdots \to S_{i_{p'-1}} \to S_i$. Since S_i is finite, the map $f_i = h_i \circ h_{i_{p'-1}} \circ \cdots \circ h_{i_1}$ is an automorphism of S_i, and there exists $p_i \in \mathbb{N}$ such that $f_i^{p_i}$ is the identity map of S_i. This in turn implies that for all $x \in S^{\mathbb{Z}}$, we have

$$\pi_i(f^{p_i}(x)) = \pi_i(\sigma^{\ell_i}(x))$$

for some $\ell_i \in \mathbb{Z}$. That is, f^{p_i} simply shifts the S_i-components of points by a constant amount. Let $\mathcal{I}$ be the set of indices i such that S_i occurs in a cycle, and let $p = \operatorname{lcm}_{i \in \mathcal{I}}(p_i)$. Clearly, f^p has a natural reversible restriction on the full shift $S_{\mathcal{I}}^{\mathbb{Z}}$, where $S_{\mathcal{I}} = \prod_{i \in \mathcal{I}} S_i$.

Consider then S_j for some $j \in \mathcal{J} = [1, m] - \mathcal{I}$. By following the incoming arrows we necessarily find an $i(j) \in \mathcal{I}$ and a path of the form

$$S_{i(j)} \to S_{i_1} \to \cdots \to S_{i_{p'-1}} \to S_{i(j)} \to S_{j_1} \to \cdots \to S_{j_{q'-1}} \to S_j \ ,$$

where $j_k \in \mathcal{J}$ for all k. Denote by $q(j)$ the length q' of the path from $S_{i(j)}$ to S_j, and let $n = p \max_{j \in \mathcal{J}} q(j)$.

Clearly, if $y = f^n(x)$ and $j \in \mathcal{J}$, then $\pi_j(y)$ is a function of $\pi_{i(j)}(x)$, which in turn is a function of some $\pi_i(y)$ with $i \in \mathcal{I}$. But this means that the $\mathcal{J}$-components of y are uniquely determined by its $\mathcal{I}$-components. This and the fact that f is reversible on $S_{\mathcal{I}}^{\mathbb{Z}}$ imply that the limit set of f is $X = f^n(S^{\mathbb{Z}})$, which is conjugate to $S_{\mathcal{I}}^{\mathbb{Z}}$. On X, f^p is conjugate to a Cartesian product of shift maps. Finally, note that n and p can be chosen independently of f. ■

Of course, a surjective CA has a surjective local rule. The local rule is automatically surjective also if f is captive, since unary point are mapped to themselves.

Question 4.4.6 *Is the assumption that f_{loc} is surjective needed? Does a similar result hold in general on mixing SFTs?*

Proposition 4.4.7 *Let $\mathcal{F}$ be a variety with the congruence-product property and $S \in \mathcal{F}$ finite. Then the set of homomorphic endomorphisms of $S^{\mathbb{Z}}$ with surjective local rules is sparse, finitely generated and predictable*

Proof. Finitely generatedness is easy to show, since if $S = \prod_{i=1}^{m} S_i$ is the decomposition of S into directly indecomposable algebras, then by Lemma 4.4.4, all endomorphisms are generated by symbol endomorphisms of S and shift maps on the tracks $S_i^{\mathbb{Z}}$. If k is the number of symbol endomorphisms, then there are at most $k \cdot m^n$ endomorphisms of $S^{\mathbb{Z}}$ with

neighborhood $[0, n-1]$. Since this is only singly exponential, the endomorphism monoid is sparse.

For the predictability, suppose we are given u, v (which we may assume to be of the same length) and $f_{\mathrm{loc}} : S^{2r+1} \to S$. First, by the previous theorem, there exists n such that $f^n(S^{\mathbb{Z}})$ is the limit set of f for all homomorphic CA f. Furthermore, we may decompose the alphabet as $S = S_1 \times S_2$, so that $S^{\mathbb{Z}} = S_1^{\mathbb{Z}} \times S_2^{\mathbb{Z}}$, and f^p is a Cartesian product of shift maps on the S_1-track, and on $f^n(S^{\mathbb{Z}})$, the component S_2 is computed by a block map $g : S_1^{\mathbb{Z}} \to S_2^{\mathbb{Z}}$ (with some radius r); letting π_1 and π_2 be the corresponding projections, we have $x \in f^n(S^{\mathbb{Z}}) \implies g(\pi_1(x)) = \pi_2(x)$. Clearly, there also exists a CA $\hat{f} : S_1^{\mathbb{Z}} \to S_1^{\mathbb{Z}}$ such that $\pi_1(f(x)) = \hat{f}(\pi_1(x))$ for all $x \in S^{\mathbb{Z}}$ (that is, the S_1-component is independent of the S_2-component in the action of f).

Now, let V be the finite set of words $v' \in S_1^{|v|+2r}$ with $g(v') = \pi_2(v)$ and $v'_{[r,|v|+r-1]} = \pi_1(v)$, and let U be the set of words $u' \in S_1^{|u|+2r}$ with $u'_{[r,|u|+r-1]} = \pi_1(u)$. We then have $f^{n+jp}(x)_{[0,|v|-1]} = v$ for some $j \in \mathbb{N}$ and $x_{[0,|u|-1]} = u$ if and only if $\hat{f}^{n+jp}(x)_{[0,|v'|-1]} = v'$ for some $j \in \mathbb{N}$, $v' \in V$ and $x_{[0,|u|+2r-1]} \in U$. The latter problem is decidable since Cartesian products of shifts are obviously decidable, and the result then follows from Lemma 1.5.5. ■

In fact, we do not know whether there are essentially different varieties with the congruence-product property than lattices, but we state our results for this class instead of the variety of lattices, since the result then encompasses all varieties in the 'lattice family' (as long as one checks the congruence-product property).

Bibliography

[Ada04] Boris Adamczewski. Symbolic discrepancy and self-similar dynamics. In *Annales de l'institut Fourier*, volume 54, pages 2201–2234. Chartres: L'Institut, 1950-, 2004.

[BBK+01] Vincent D. Blondel, Olivier Bournez, Pascal Koiran, Christos H. Papadimitriou, John N. Tsitsiklis, John N. Tsitsiklise Acesame, Université Catholique de Louvain, Av. Georges Lematre, and Communicated M. Sintzo. Deciding stability and mortality of piecewise affine dynamical systems, 2001.

[BDJ08] Alexis Ballier, Bruno Durand, and Emmanuel Jeandel. Structural aspects of tilings. In Pascal Weil Susanne Albers, editor, *Proceedings of the 25th Annual Symposium on the Theoretical Aspects of Computer Science*, pages 61–72, Bordeaux, France, February 2008. IBFI Schloss Dagstuhl. 11 pages.

[BGK11] Alexis Ballier, Pierre Guillon, and Jarkko Kari. Limit sets of stable and unstable cellular automata. *Fund. Inform.*, 110(1-4):45–57, 2011.

[BJ13] Alexis Ballier and Emmanuel Jeandel. Structuring multidimensional subshifts. *ArXiv e-prints*, September 2013.

[BK99] Mike Boyle and Bruce Kitchens. Periodic points for onto cellular automata. *Indag. Math. (N.S*, 10:483–493, 1999.

[BLR88] Mike Boyle, Douglas Lind, and Daniel Rudolph. The automorphism group of a shift of finite type. *Transactions of the American Mathematical Society*, 306(1):pp. 71–114, 1988.

[Bob02] Jozef Bobok. Chaos in countable dynamical system. *Topology and its Applications*, 126(12):207 – 216, 2002.

[Boy83] Mike Boyle. Lower entropy factors of sofic systems. *Ergodic Theory Dynam. Systems*, 3(4):541–557, 1983.

[BPS10] Mike Boyle, Ronnie Pavlov, and Michael Schraudner. Multidimensional sofic shifts without separation and their factors. *Transactions of the American Mathematical Society*, 362(9):4617–4653, 2010.

[Bru01] Henk Bruin. Dimensions of recurrence times and minimal subshifts, 2001.

[BS81] Stanley Burris and Hanamantagouda P. Sankappanavar. *A course in universal algebra*, volume 78 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1981.

[BS08] Mike Boyle and Michael Schraudner. $\mathbb{Z}^d$ group shifts and Bernoulli factors. *Ergodic Theory Dynam. Systems*, 28(2):367–387, 2008.

[BT98] Mike Boyle and Jun Tomiyama. Bounded topological orbit equivalence and C^*-algebras. *Journal of the Mathematical Society of Japan*, 50(2):317–329, 1998.

[BT09] Laurent Boyer and Guillaume Theyssier. On Local Symmetries and Universality in Cellular Automata. In Susanne Albers and Jean-Yves Marion, editors, *26th International Symposium on Theoretical Aspects of Computer Science STACS 2009*, pages 195–206, Freiburg, Germany, 2009. IBFI Schloss Dagstuhl.

[Büc60] J. Richard Büchi. Weak second-order arithmetic and finite automata. *Mathematical Logic Quarterly*, 6(1-6):66–92, 1960.

[CDTW12] Douglas Cenzer, Ali Dashti, Ferit Toska, and Sebastian Wyman. Computability of countable subshifts in one dimension. *Theory of Computing Systems*, 51(3):352–371, 2012.

[CF03] Julien Cervelle and Enrico Formenti. On sand automata. In *Proceedings of the 20th Annual Symposium on Theoretical Aspects of Computer Science*, STACS '03, pages 642–653, London, UK, UK, 2003. Springer-Verlag.

[CFMM00] Gianpiero Cattaneo, Enrico Formenti, Giovanni Manzini, and Luciano Margara. Ergodicity, transitivity, and regularity for linear cellular automata over $\mathbb{Z}_m$. *Theoret. Comput. Sci.*, 233(1-2):147–164, 2000.

[CHR79] Ethan M. Coven, Gustav A. Hedlund, and Frank Rhodes. The commuting block maps problem. *Trans. Amer. Math. Soc.*, 249(1):113–138, 1979.

[CK14] Van Cyr and Bryna Kra. The automorphism group of a shift of subquadratic growth. *ArXiv e-prints*, March 2014.

[Cov71] Ethan M. Coven. Endomorphisms of substitution minimal sets. *Probability Theory and Related Fields*, 20(2):129–133, 1971.

[CPY89] Karel Culik, II, Jan K. Pachl, and Sheng Yu. On the limit sets of cellular automata. *SIAM J. Comput.*, 18(4):831–842, August 1989.

[CR98] Douglas Cenzer and Jeffrey B. Remmel. Π^0_1 classes in mathematics. In *Handbook of recursive mathematics, Vol. 2*, volume 139 of *Stud. Logic Found. Math.*, pages 623–821. North-Holland, Amsterdam, 1998.

[CSC10] Tullio Ceccherini-Silberstein and Michel Coornaert. Surjunctive groups. In *Cellular Automata and Groups*, Springer Monographs in Mathematics, pages 57–75. Springer Berlin Heidelberg, 2010.

[DFP12] Alberto Dennunzio, Enrico Formenti, and Julien Provillard. Non-uniform cellular automata: Classes, dynamics, and decidability. *Information and Computation*, 215(0):32 – 46, 2012.

[DHS99] Fabien Durand, Bernard Host, and Christian Skau. Substitutional dynamical systems, Bratteli diagrams and dimension groups. *Ergodic Theory Dynam. Systems*, 19(4):953–993, 1999.

[dJRS80] Andrés del Junco, Maurice H. Rahe, and Laif Swanson. Chacon's automorphism has minimal self joinings. *Journal dAnalyse Mathématique*, 37(1):276–284, 1980.

[DKVB06] Jean-Charles Delvenne, Petr Kůrka, Vincent, and D. Blondel. Decidability and universality in symbolic dynamical systems. *Fund. Inform*, 2006.

[Dow97] Tomasz Downarowicz. The royal couple conceals their mutual relationship: A noncoalescent toeplitz flow. *Israel Journal of Mathematics*, 97(1):239–251, 1997.

[Dow05] Tomasz Downarowicz. Survey of odometers and toeplitz flows. *Contemporary Mathematics*, 385:7–38, 2005.

[DP09] Bruno Durand and Victor Poupet. Asymptotic cellular complexity. In Volker Diekert and Dirk Nowotka, editors, *Developments in Language Theory*, volume 5583 of *Lecture Notes in Computer Science*, pages 195–206. Springer, 2009.

[Dur00] Fabien Durand. Linearly recurrent subshifts have a finite number of non-periodic subshift factors. *Ergodic Theory and Dynamical Systems*, 20:1061–1078, 7 2000.

[Fio00] Francesca Fiorenzi. The Garden of Eden theorem for sofic shifts. *Pure Mathematics and Applications*, 11(3):471–484, 2000.

[Fur67] Harry Furstenberg. Disjointness in ergodic theory, minimal sets, and a problem in diophantine approximation. *Mathematical systems theory*, 1(1):1–49, 1967.

[GH55] Walter H. Gottschalk and Gustav A. Hedlund. *Topological Dynamics*. American Mathematical Society: Colloquium publications. American Mathematical Society, 1955.

[Got73] Walter H. Gottschalk. Some general dynamical notions. In Anatole Beck, editor, *Recent Advances in Topological Dynamics*, volume 318 of *Lecture Notes in Mathematics*, pages 120–125. Springer Berlin Heidelberg, 1973.

[GPS95] Thierry Giordano, Ian F. Putnam, and Christian F. Skau. Topological orbit equivalence and C^*-crossed products. *J. Reine Angew. Math.*, 469:51–111, 1995.

[GPS09] Thierry Giordano, Ian F. Putnam, and Christian F. Skau. Cocycles for Cantor minimal $\mathbb{Z}^d$-systems. *International Journal of Mathematics*, 20(09):1107–1135, 2009.

[GR08] Pierre Guillon and Gaétan Richard. Nilpotency and limit sets of cellular automata. In *Mathematical foundations of computer science 2008*, volume 5162 of *Lecture Notes in Comput. Sci.*, pages 375–386. Springer, Berlin, 2008.

[GR10a] Pierre Guillon and Gaétan Richard. Asymptotic behavior of dynamical systems and cellular automata. *ArXiv e-prints*, April 2010.

[GR10b] Pierre Guillon and Gaétan Richard. Revisiting the Rice Theorem of Cellular Automata. *ArXiv e-prints*, January 2010.

[Grä71] George Grätzer. *Lattice theory. First concepts and distributive lattices*. W. H. Freeman and Co., San Francisco, Calif., 1971.

[Gri73] Christian Grillenberger. Constructions of strictly ergodic systems. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 25(4):335–342, 1973.

[HK67] Frank Hahn and Yitzhak Katznelson. On the entropy of uniquely ergodic transformations. *Transactions of the American Mathematical Society*, pages 335–360, 1967.

[Hoc09] Michael Hochman. On the dynamics and recursive properties of multidimensional symbolic systems. *Invent. Math.*, 176(1):131–167, 2009.

[Hoc10] Michael Hochman. On the automorphism groups of multidimensional shifts of finite type. *Ergodic Theory Dynam. Systems*, 30(3):809–840, 2010.

[Hos86] Bernard Host. Valeurs propres des systèmes dynamiques définis par des substitutions de longueur variable. *Ergodic Theory and Dynamical Systems*, 6:529–540, 12 1986.

[HP89] Bernard Host and François Parreau. Homomorphismes entre systèmes dynamiques définis par substitutions. *Ergodic Theory and Dynamical Systems*, 9:469–477, 8 1989.

[Hur87] Lyman P. Hurd. Formal language characterizations of cellular automaton limit sets. *Complex Systems*, 1987.

[HY01] Wen Huang and Xiangdong Ye. Homeomorphisms with the whole compacta being scrambled sets. *Ergodic Theory and Dynamical Systems*, 21:77–91, 2 2001.

[HY05] Wen Huang and Xiangdong Ye. Dynamical systems disjoint from any minimal system. *Transactions of the American Mathematical Society*, 357(2):669–694, 2005.

[ION83] Masanobu Ito, Nobuyasu Osato, and Masakazu Nasu. Linear cellular automata over $\mathbb{Z}_m$. *J. Comput. System Sci.*, 27(1):125–140, 1983.

[JV11] Emmanuel Jeandel and Pascal Vanier. Π_1^0 sets and tilings. In *Theory and Applications of Models of Computation (TAMC)*, volume 6648 of *Lecture Notes in Computer Science*, pages 230–239, 2011.

[Kar92] Jarkko Kari. The nilpotency problem of one-dimensional cellular automata. *SIAM J. Comput.*, 21(3):571–586, 1992.

[Kar94] Jarkko Kari. Rice's theorem for the limit sets of cellular automata. *Theoret. Comput. Sci.*, 127(2):229–254, 1994.

[Kar00] Jarkko Kari. Linear cellular automata with multiple state variables. In *STACS 2000 (Lille)*, volume 1770 of *Lecture Notes in Comput. Sci.*, pages 110–121. Springer, Berlin, 2000.

[Kit87] Bruce P. Kitchens. Expansive dynamics on zero-dimensional groups. *Ergodic Theory Dyn. Syst.*, 7:249–261, 1987.

[Kit98] Bruce P. Kitchens. *Symbolic dynamics – One-sided, two-sided and countable state Markov shifts.* Universitext. Springer-Verlag, Berlin, 1998.

[KO08] Jarkko Kari and Nicolas Ollinger. Periodicity and immortality in reversible computing. In *Proceedings of the 33rd international symposium on Mathematical Foundations of Computer Science*, MFCS '08, pages 419–430, Berlin, Heidelberg, 2008. Springer-Verlag.

[KR90] Ki Hang Kim and Fred William Roush, Roush. On the automorphism groups of subshifts. *Pure Mathematics and Applications*, 1(4):203–230, 1990.

[KS01] William Kirk and Brailey Sims. *Handbook of Metric Fixed Point Theory.* Springer, 2001.

[KSW60] Georg Kreisel, Georg Shoenfield, and Hao Wang. Number theoretic concepts and recursive well-orderings. *Arch. Math. Logik Grundlagenforsch.*, 5:42–64, 1960.

[Kůr97] Petr Kůrka. Languages, equicontinuity and attractors in cellular automata. *Ergodic theory and dynamical systems*, 17(2):417–434, 1997.

[Kůr03] Petr Kůrka. *Topological and symbolic dynamics*, volume 11 of *Cours Spécialisés [Specialized Courses]*. Société Mathématique de France, Paris, 2003.

[Lei12] Tom Leinster. Codensity and the ultrafilter monad. *ArXiv e-prints*, September 2012.

[LM95] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding.* Cambridge University Press, Cambridge, 1995.

[Lot02] M. Lothaire. *Algebraic combinatorics on words*, volume 90 of *Encyclopedia of Mathematics and its Applications.* Cambridge University Press, Cambridge, 2002.

[Mar73] John C. Martin. Minimal flows arising from substitutions of non-constant length. *Mathematical systems theory*, 7(1):73–82, 1973.

[MB97] Cristopher Moore and Timothy Boykett. Commuting cellular automata. *Complex Systems*, 11(1):55–64, 1997.

[MB04] Nicole R. Miller and Michael J. Bardzell. The evolution homomorphism and permutation actions on group generated cellular automata. *Complex Systems*, 15(2):121–136, 2004.

[Mic76] Pierre Michel. Stricte ergodicité d'ensembles minimaux de substitution. *Théorie Ergodique*, pages 189–201, 1976.

[Mil11] Cédric Milliet. A remark on Cantor derivative. *ArXiv e-prints*, April 2011.

[Mil12] Joseph Miller. Two notes on subshifts. *Proceedings of the American Mathematical Society*, 140(5):1617–1622, 2012.

[Min67] Marvin L. Minsky. *Computation: finite and infinite machines*. Prentice-Hall Inc., Englewood Cliffs, N.J., 1967. Prentice-Hall Series in Automatic Computation.

[MM98] Giovanni Manzini and Luciano Margara. Invertible linear cellular automata over $\mathbb{Z}_m$: algorithmic and dynamical aspects. *J. Comput. System Sci.*, 56(1):60–67, 1998.

[Mor96] Kenichi Morita. Universality of a reversible two-counter machine. *Theoretical Computer Science*, 1996.

[Mos92] Brigitte Mossé. Puissances de mots et reconnaissabilité des points fixes d'une substitution. *Theoret. Comput. Sci.*, 99(2):327–334, 1992.

[Mos96] Brigitte Mossé. Reconnaissabilité des substitutions et complexité des suites automatiques. *Bulletin de la Société Mathématique de France*, 124(2):329–346, 1996.

[MS20] Stefan Mazurkiewicz and Wacaw Sierpiski. Contribution à la topologie des ensembles dénombrables. *Fundamenta Mathematicae*, 1(1):17–27, 1920.

[Odi89] Piergiorgio Odifreddi. *Classical recursion theory*, volume 125 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam, 1989. The theory of functions and sets of natural numbers, With a foreword by G. E. Sacks.

[Oll08] Nicolas Ollinger. Intrinsically universal cellular automata. In Turlough Neary, Damien Woods, Anthony Karel Seda, and Niall Murphy, editors, *CSP*, volume 1 of *EPTCS*, pages 199–204, 2008.

[Oll13] Jeanette Olli. Endomorphisms of sturmian systems and the discrete chair substitution tiling system. *Dynamical Systems*, 33(9):4173–4186, 2013.

[Piv12] Marcus Pivato. The ergodic theory of cellular automata. *Int. J. General Systems*, 41(6):583–594, 2012.

[PS10] Ronnie Pavlov and Michael Schraudner. Classification of sofic projective subdynamics of multidimensional shifts of finite type. submitted, 2010.

[PY04] Marcus Pivato and Reem Yassawi. Limit measures for affine cellular automata ii. *Ergodic Theory and Dynamical Systems*, 24:1961–1980, 11 2004.

[Que87] Martine Queffélec. *Substitution Dynamical Systems, Spectral Analysis*. Number no. 1294 in Lecture Notes in Mathematics. Springer-Verlag, 1987.

[Ric53] Henry Gordon Rice. Classes of recursively enumerable sets and their decision problems. *Transactions of the American Mathematical Society*, 74(2):358–366, 1953.

[Rob66] Abraham Robinson. *Non-standard analysis*. Studies in logic and the foundations of mathematics. North-Holland Pub. Co., 1966.

[Rya72] J. Patrick Ryan. The shift and commutativity. *Mathematical systems theory*, 6(1-2):82–85, 1972.

[Sal12] Ville Salo. On nilpotency and asymptotic nilpotency of cellular automata. *ArXiv e-prints*, May 2012.

[Sal13] Ville Salo. Hard asymptotic sets for one-dimensional cellular automata. *ArXiv e-prints*, July 2013.

[Sat97] Tadakazu Sato. Ergodicity of linear cellular automata over $\mathbb{Z}_m$. *Inform. Process. Lett.*, 61(3):169–172, 1997.

[Sch95] Klaus Schmidt. *Dynamical systems of algebraic origin*, volume 128 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1995.

[Sim11] Stephen G Simpson. Symbolic dynamics: entropy = dimension = complexity. *preprint*, 2011.

[Sob07] Marcelo Sobottka. Topological quasi-group shifts. *Discrete and Continuous Dynamical Systems*, 2007.

[Son14] Younghwan Son. Substitutions, tiling dynamical systems and minimal self-joinings. *ArXiv e-prints*, February 2014.

[ST12a] Ville Salo and Ilkka Törmä. Computational aspects of cellular automata on countable sofic shifts. *Mathematical Foundations of Computer Science 2012*, pages 777–788, 2012.

[ST12b] Ville Salo and Ilkka Törmä. On derivatives and subpattern orders of countable subshifts. *ArXiv e-prints*, August 2012.

[ST12c] Ville Salo and Ilkka Törmä. On shift spaces with algebraic structure. In S.Barry Cooper, Anuj Dawar, and Benedikt Löwe, editors, *How the World Computes*, volume 7318 of *Lecture Notes in Computer Science*, pages 636–645. Springer Berlin Heidelberg, 2012.

[ST12d] Ville Salo and Ilkka Törmä. On shift spaces with algebraic structure. *ArXiv e-prints*, March 2012.

[ST13a] Ville Salo and Ilkka Törmä. Block maps between primitive uniform and Pisot substitutions. *ArXiv e-prints*, June 2013. Accepted to Ergodic Theory and Dynamical Systems.

[ST13b] Ville Salo and Ilkka Törmä. Color blind cellular automata. In Jarkko Kari, Martin Kutrib, and Andreas Malcher, editors, *Cellular Automata and Discrete Complex Systems*, volume 8155 of *Lecture Notes in Computer Science*, pages 139–154. Springer Berlin Heidelberg, 2013.

[ST13c] Ville Salo and Ilkka Törmä. Commutators of bipermutive and affine cellular automata. In Jarkko Kari, Martin Kutrib, and Andreas Malcher, editors, *Cellular Automata and Discrete Complex Systems*, volume 8155 of *Lecture Notes in Computer Science*, pages 155–170. Springer Berlin Heidelberg, 2013.

[ST13d] Ville Salo and Ilkka Törmä. Constructions with countable subshifts of finite type. *Fundam. Inform.*, 126(2-3):263–300, 2013.

[The05] Guillaume Theyssier. How common can be universality for cellular automata? In *STACS 2005*, volume 3404 of *Lecture Notes in Comput. Sci.*, pages 121–132. Springer, Berlin, 2005.

[Voo93] Burton Voorhees. Commutation of cellular automata rules. *Complex Systems*, 7(4):309, 1993.

[Wal00] Peter Walters. *An Introduction to Ergodic Theory*. Graduate Texts in Mathematics. Springer New York, 2000.

[Wil84] Susan Williams. Toeplitz minimal flows which are not uniquely ergodic. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 67(1):95–107, 1984.

Turku
Centre *for*
Computer
Science

Joukahaisenkatu 3-5 B, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics

Åbo Akademi University
- Department of Information Technologies

Turku School of Economics
- Institute of Information Systems Sciences

ISBN 978-952-12-3089-9
ISSN 1239-1883