

# AUTOMORPHISM GROUPS OF RANDOM SUBSTITUTION SUBSHIFTS

ROBBERT FOKKINK, DAN RUST, VILLE SALO

*Dedicated to the memory of Uwe Grimm*

**ABSTRACT.** We prove that for a suitably nice class of random substitutions, their corresponding subshifts have automorphism groups that contain an infinite simple subgroup and a copy of the automorphism group of a full shift. Hence, they are countable, non-amenable and non-residually finite. To show this, we introduce the concept of shuffles and generalised shuffles for random substitutions, as well as a local version of recognisability for random substitutions that will be of independent interest. Without recognisability, we need a more refined notion of recognisable words in order to understand their automorphisms. We show that the existence of a single recognisable word is often enough to embed the automorphism group of a full shift in the automorphism group of the random substitution subshift.

## 1. INTRODUCTION

The study of automorphism groups of subshifts has a rich history [5, 17, 18]. The general philosophy is that algebraic properties of the automorphism group can reveal dynamical properties of the subshift. In particular, the larger the automorphism group, the more ‘complex’ should be the subshift. This is by no means a hard-and-fast rule, but broadly rings true; subshifts with positive entropy typically have large automorphism groups (for instance, often containing every finite group), while the automorphism groups of subshifts with low subword complexity are virtually  $\mathbb{Z}$  [6, 7, 8]. Pavlov and Schmieding give a good survey of results in the low complexity setting [23].

Random substitutions are a relatively new object of study in symbolic dynamics, generalising the notion of substitutions (here called *deterministic substitutions*). They are of particular interest in the study of mathematical quasicrystals, first studied in this context by Godrèche and Luck [11] in the 80s, as they provide a mechanism for generating quasicrystals with both positive entropy and long-range order, in the sense that they can have a non-trivial pure point component in their diffraction spectrum. Baake and Grimm’s series *Aperiodic Order* does well to explain this significance [2, Sec. 11.2.3]. For a gentle introduction to random substitutions in the context of symbolic dynamics, see the foundational paper of Rust and Spindeler [25].

Whereas deterministic substitutions such as the Fibonacci substitution  $a \mapsto ab$ ,  $b \mapsto a$  specify a single image for each letter in the alphabet, a random substitution allows for multiple independent images. So, for instance, the *random Fibonacci substitution* is given

---

*Date:* March 28, 2022.

2010 *Mathematics Subject Classification.* 37B10, 37A50, 37B40, 52C23.

*Key words and phrases.* automorphisms, random substitutions, topological conjugacy, amenability.

by  $a \mapsto \{ab, ba\}$ ,  $b \mapsto \{a\}$ , where each letter in a word can be independently mapped to one of its possible realisations under the random substitution. By considering all possible realisations under repeated applications of a random substitution, a language is produced and hence a subshift may be defined.

Under mild assumptions, the corresponding subshift is transitive and has positive entropy. The subshift retains many of the hierarchical properties of its deterministic counterpart (especially when the random substitution is *recognisable*), but positive entropy and a dense collection of minimal subsets mean that they also mirror aspects of more ‘complex’ subshifts, such as shifts of finite type. The study of random substitutions is still somewhat in its infancy, however aspects that have been studied already include their topological entropy [12], measure theoretic entropy [13], ergodic measures [15], periodic points [24], topological mixing [9, 20], diffraction [4] and connections to SFTs [14]. Here, we begin the first investigation of their automorphism groups. We focus on subgroups that can appear within the automorphism group and conditions that are necessary for such subgroups to appear.

Our main results concern the structure of certain subgroups of the automorphism group. Under some basic assumptions, we show that the automorphism group of a random substitution subshift contains an infinite simple subgroup (Theorem 3.13), as well as the automorphism group of the full 2-shift (Theorem 4.4). Section 2 introduces the necessary notation and preliminaries on random substitution subshifts and automorphism groups of subshifts. In Section 3, we introduce the concept of *shuffles* and the shuffle group, which is an important class of automorphisms on which our main methods are based. Many of our methods rely on a notion of recognisability for random substitutions, which has been previously hinted at in previous work [24], but which we fully investigate and exploit in Section 4; most notably proving an equivalence between recognisability and local recognisability for compatible random substitutions (Proposition 5.7) in Section 5. Full recognisability is less ubiquitous in the random setting than in the deterministic setting (even the random Fibonacci substitution is not recognisable). So, it is important to study random substitutions that only satisfy weaker notations of recognisability. We introduce the concept of a word being recognisable. The existence of a single recognisable word is often enough to induce a weak hierarchical structure. Hence, when the random substitution is of constant length and admits at least one recognisable word in its language, we are still able to show in Section 6 that the automorphism group of a full shift embeds in the automorphism group of the random substitution subshift (Theorem 6.12).

## 2. NOTATION AND PRELIMINARIES

Let  $\mathcal{A} = \{a_1, \dots, a_d\}$  be a finite alphabet with  $d$  letters, let  $\mathcal{A}^n$  denote the set of length- $n$  words over  $\mathcal{A}$ , and let  $|u| := n$  denote the length of the word  $u \in \mathcal{A}^n$ . Let  $\mathcal{A}^+ = \bigcup_{n=1}^{\infty} \mathcal{A}^n$  and let  $\mathcal{A}^* = \mathcal{A}^+ \cup \{\epsilon\}$ , where  $\epsilon$  is the *empty word*. Let  $\mathcal{A}^{\mathbb{Z}}$  denote the *full shift* over  $\mathcal{A}$  with the usual product topology and for  $x \in \mathcal{A}^{\mathbb{Z}}$  and  $j \geq i$ , write  $x_{[i,j]} := x_i \cdots x_j$ . Let  $\sigma: \mathcal{A}^{\mathbb{Z}} \rightarrow \mathcal{A}^{\mathbb{Z}}$  denote the usual shift action given by  $\sigma(x)_i := x_{i+1}$ . If  $u = u_0 \cdots u_n$  and  $v = v_0 \cdots v_m$  are words in  $\mathcal{A}^*$ , then their *concatenation*

$$uv = u_0 \cdots u_n v_0 \cdots v_m$$

is a word in  $\mathcal{A}^*$  and the set  $\mathcal{A}^*$  forms a monoid under concatenation with the identity given by the empty word  $\epsilon$ . If  $u \in \mathcal{A}^n$  is a finite word and  $v$  is a finite or (bi-)infinite word such that  $u_i = v_{k+i}$  for some  $k$  and all  $0 \leq i \leq n-1$ , then we say that  $u$  is a *subword* of  $v$  and write  $u \triangleleft v$ . If  $k=0$  then we call  $u$  a *prefix* of  $v$ , and if  $k=|v|-n$  then we call  $u$  a *suffix* of  $v$ .

**2.1. Random substitutions.** If  $U, V \subseteq \mathcal{A}^*$  are two non-empty sets of words, then we define their concatenation to be the set

$$UV := \{uv \mid u \in U, v \in V\} \subset \mathcal{A}^*$$

with the obvious generalisation to the concatenation of finitely many and countably many sets of words. Let  $\mathcal{S}$  denote the set of non-empty finite subsets of  $\mathcal{A}^+$ . A *random substitution* is a function  $\vartheta: \mathcal{A} \rightarrow \mathcal{S}$ . We extend  $\vartheta$  to words by defining  $\vartheta(u_0 \cdots u_n) := \vartheta(u_0) \cdots \vartheta(u_n)$  and to finite sets of words  $\vartheta: \mathcal{S} \rightarrow \mathcal{S}$  by defining  $\vartheta(U) := \{\vartheta(u) \mid u \in U\}$ . In this way, we may define iterated powers of  $\vartheta$  by  $\vartheta^0 := \text{Id}_{\mathcal{S}}$  and  $\vartheta^{p+1} := \vartheta \circ \vartheta^p$ .

As an example, on the alphabet  $\{a, b\}$ , the *random Fibonacci substitution* is given by

$$\vartheta: a \mapsto \{ab, ba\}, \quad b \mapsto \{a\}$$

with the second and third iterate of the random substitution on the letter  $a$  being

$$\vartheta^2(a) = \{aba, baa, aab\}, \quad \vartheta^3(a) = \{abaab, ababa, baaab, baaba, aabab, aabba, abbaa, babaa\}.$$

A word  $u \in \vartheta(v)$  is called a *realisation* of the random substitution  $\vartheta$  on  $v$ . Similarly, we call a bi-infinite sequence  $x \in \vartheta(y)$  a *realisation* of the random substitution  $\vartheta$  on the bi-infinite sequence  $y \in \mathcal{A}^{\mathbb{Z}}$ . If  $u \in \vartheta^p(a)$  for some letter  $a \in \mathcal{A}$ , then we call  $u$  a *level- $p$  inflation word* or *level- $p$  supertile*.

Let  $U \in \mathcal{S}$  be a set of words. If there exists a word  $v \in U$  such that  $u \triangleleft v$ , then we write  $u \blacktriangleleft U$ . We say that a word  $u \in \mathcal{A}^+$  is  $\vartheta$ -*legal* or just *legal* if there exists a letter  $a \in \mathcal{A}$  and a power  $p \geq 0$  such that  $u \blacktriangleleft \vartheta^p(a)$ . We let  $\mathcal{L}_{\vartheta} \subset \mathcal{A}^*$  denote the set of all  $\vartheta$ -legal words and call  $\mathcal{L}_{\vartheta}$  the *language* of  $\vartheta$ . We let  $\mathcal{L}_{\vartheta}^n := \mathcal{L}_{\vartheta} \cap \mathcal{A}^n$  denote the set of  $\vartheta$ -legal words of length  $n$ .

The *random substitution subshift (RS-subshift)* of  $\vartheta$ , written as  $X_{\vartheta}$ , is the set of bi-infinite words in  $\mathcal{A}^{\mathbb{Z}}$  whose subwords are all  $\vartheta$ -legal. That is,

$$X_{\vartheta} := \{x \in \mathcal{A}^{\mathbb{Z}} \mid u \triangleleft x \implies u \in \mathcal{L}_{\vartheta}\}.$$

The RS-subshift  $X_{\vartheta}$  associated to a random substitution  $\vartheta$  is a closed, shift-invariant subspace of the full shift  $\mathcal{A}^{\mathbb{Z}}$ . The random substitution  $\vartheta$  extends to a set-valued function  $\vartheta: X_{\vartheta} \rightarrow X_{\vartheta}$ .

Let  $|u|_v$  denote the number of appearances of the word  $v$  as a subword of  $u$  and let  $\psi: \mathcal{A}^* \rightarrow \mathbb{N}^d$  denote the *abelianisation function*  $\psi: u \mapsto (|u|_{a_1}, \dots, |u|_{a_d})^T$ .

**Definition 2.1.** Let  $\vartheta$  be a random substitution on the alphabet  $\mathcal{A}$ . We call  $\vartheta$  *compatible* if for all  $a \in \mathcal{A}$  and every pair of words  $u, v \in \vartheta(a)$ ,  $\psi(u) = \psi(v)$ . The *substitution matrix*  $M_{\vartheta}$  associated with a compatible random substitution is given by  $(M_{\vartheta})_{ij} = |\vartheta(a_j)|_{a_i}$ , which is well defined by compatibility.

**Definition 2.2.** Let  $\vartheta$  be a random substitution on the alphabet  $\mathcal{A}$ . We call  $\vartheta$  *primitive* if there exists a power  $p \geq 1$  such that for all  $a, b \in \mathcal{A}$ ,  $a \blacktriangleleft \vartheta^p(b)$ .

If  $\vartheta$  is compatible, then  $\vartheta$  is primitive if and only if  $M_\vartheta$  is a primitive matrix. That is, if  $M_\vartheta^p$  has positive entries for some power  $p \geq 1$ . For the majority of this article, we will only consider compatible primitive substitutions.

A random substitution  $\vartheta: \mathcal{A} \rightarrow \mathcal{S}$  is said to be *constant length* with length  $L$  if, for every  $a \in \mathcal{A}$  and  $u \in \vartheta(a)$ ,  $|u| = L$ . An example of a compatible random substitution of constant length is the *random period doubling* substitution  $\vartheta: a \mapsto \{ab, ba\}, b \mapsto \{aa\}$  with constant length  $L = 2$ , first introduced by Baake, Spindeler and Strungaru [4].

**Definition 2.3.** Let  $\vartheta$  be a compatible random substitution on the alphabet  $\mathcal{A}$ . We call  $\vartheta$  *recognisable* if for every  $x \in X_\vartheta$ , there exists a unique  $y \in X_\vartheta$  and a unique  $0 \leq k \leq |\vartheta(y_0)| - 1$  such that  $\sigma^{-k}(x) \in \vartheta(y)$ .

Rust showed that recognisability of  $\vartheta$  implies aperiodicity of  $X_\vartheta$  [24]. That is, if  $\vartheta$  is recognisable, then the RS-subshift  $X_\vartheta$  contains no periodic points. The converse is in general not true, as the random Fibonacci substitution  $a \mapsto \{ab, ba\}, b \mapsto \{a\}$  is not recognisable but, by considering letter frequencies, its RS-subshift is aperiodic.

While recognisability is a useful property, and the above global definition is theoretically useful, it is often difficult to directly verify for examples. Instead, one generally checks an equivalent local version of recognisability. This will be introduced and studied in Section 5, where the local and global definitions will be shown to be equivalent. Until then, without loss of rigour, we interpret recognisability of a compatible random substitution as meaning that for any  $x \in X_\vartheta$ , there is a unique decomposition of  $x$  into inflation words, and the type of each inflation word is also uniquely determined.

It is straightforward to check [24] that  $\vartheta$  is recognisable if and only if  $\vartheta^n$  is recognisable for all  $n \geq 1$ .

**Example 2.4.** Consider the substitution  $\vartheta$  on the alphabet  $\{a, b\}$  given by

$$a \mapsto \{abb, bab\}, \quad b \mapsto \{aa\}.$$

First, notice that we can determine how to decompose any string of consecutive  $as$  of length at least two into inflation words, as the start of any such string must begin with an inflation word of type  $\vartheta(b)$ . So, for instance, the word  $baaaaab$  must be decomposed as  $b|aa|aa|ab$ . Notice also that every word of length at least twenty four must contain the word  $aa$ , and so  $aa$  occurs with uniformly bounded gaps in any element  $x \in X_\vartheta$ . As all inflation words of type  $\vartheta(b)$  are uniquely determined, anything not yet determined must be a concatenation of inflation words of type  $\vartheta(a)$ , which then are also uniquely determined as they both have length three. It follows that  $\vartheta$  is recognisable.

So, for example, the word  $baaaabababbabbaab$  can be decomposed by first decomposing the strings of  $as$  as

$$b|aa|aa|bababbabb|aa|ab$$

and then noticing that there is exactly one choice in how the word between the strings of  $as$  can be decomposed. So the entire word has the unique decomposition

$$b|aa|aa|bab|abb|abb|aa|ab.$$

**Example 2.5** (random square Fibonacci). The following example is worth mentioning as it is related to the square of the Fibonacci substitution<sup>1</sup> but has the advantage that, unlike the usual random Fibonacci substitution, this one is recognisable. Consider the random substitution  $\vartheta$  on  $\{a, b\}$  given by

$$a \mapsto \{aab\}, b \mapsto \{ab, ba\}.$$

This example first appeared (reversed) in the work of Nilsson [22]. We check recognisability as follows. Any appearance of  $bb$  must mean that the second  $b$  comes from the start of an inflation word of type  $\vartheta(b)$  and all inflation words  $ba$  of type  $\vartheta(b)$  are found in this way. As  $bbb$  is not legal, any appearance of the word  $abaab$  can only be decomposed as  $ab|aab$ . Any appearance of the word  $baaab$  can only be decomposed as  $ba|aab$ , and all inflation words  $aab$  of type  $\vartheta(a)$  are found in either of these two ways. Anything not yet identified must then be the inflation word  $ab$  of type  $\vartheta(b)$ . Recognisability then follows.

**2.2. Automorphisms.** Let  $(X, \sigma)$  and  $(Y, \tau)$  be topological dynamical systems. A function  $f: X \rightarrow Y$  is called a *topological conjugacy* if  $f$  is a homeomorphism and  $f \circ \sigma = \tau \circ f$ . A topological conjugacy  $h: X \rightarrow X$  is called an *automorphism*. We denote the set of all automorphism of  $(X, \sigma)$  by

$$\text{Aut}(X, \sigma) := \{h: X \rightarrow X \mid h \circ \sigma = \sigma \circ h\},$$

which forms a group under composition. If the action is unambiguous, then we write  $\text{Aut}(X) := \text{Aut}(X, \sigma)$  without loss of generality.

For a subshift  $X$ , the shift map  $\sigma$  is always an automorphism of  $X$  and so, if  $X$  contains a non-periodic orbit, then  $\langle \sigma \rangle \cong \mathbb{Z}$  is an infinite subgroup of  $\text{Aut}(X)$ . Indeed,  $\text{Aut}(X)$  is the centraliser of the element  $\sigma$  in the group  $\text{Homeo}(X)$  of homeomorphisms of the subshift<sup>2</sup>. It is a consequence of the Curtis–Hedlund–Lyndon Theorem [17] that  $\text{Aut}(X)$  is countable.

Recall that a group  $G$  is residually finite if for every  $g \in G \setminus \{1\}$ , there exists a finite group  $H$  and a homomorphism  $h: G \rightarrow H$  such that  $h(g) \neq 1$ .

It was shown by various authors that for  $X$  a mixing shift of finite type,  $\text{Aut}(X)$  contains subgroups isomorphic to the following:

- every countable direct sum of finite groups [5],
- the free group  $F_2$  on two generators, hence the free group on countably many generators [5],
- a countable direct sum of the integers  $\bigoplus_{i=1}^{\infty} \mathbb{Z}$  [5],

---

<sup>1</sup>The marginal  $a \mapsto aab$ ,  $b \mapsto ab$  is conjugate to the square of the Fibonacci substitution  $a \mapsto aba$ ,  $b \mapsto ab$ . Hence, the usual Fibonacci subshift is contained in the RS-subshift of  $\vartheta$ .

<sup>2</sup>This observation recently inspired Baake, Roberts and Yassawi [3] to consider the *normaliser* of  $\sigma$  in  $\text{Homeo}(X)$ , rather than the centraliser, the so-called group of ‘reversing symmetries’ of the subshift.

- finite free products of finite groups [1],
- every residually finite countable group that is a union of finite groups [18],
- all right-angled Artin groups, including the fundamental group of any surface [18].

Boyle, Lind and Rudolph further observed that  $\text{Aut}(X)$  is residually finite, and therefore any finitely presented subgroup has a solvable word problem (in fact any finitely *generated* subgroup).  $\text{Aut}(X)$  itself is not finitely generated [5, Theorem 7.8]. Kim and Roush proved in [18] that the set of subgroups of  $\text{Aut}(X)$  is closed under virtual extensions, and Salo proved that they are also closed under cograph products (free and direct products) [26] and general countable graph products [27]. Combining these, we immediately get all the items on the above list and more.

The statement above regarding residually finite automorphism groups is a general statement about subshifts with a dense subset of periodic points. As far as we are aware, this result is part of the folklore of automorphism groups of subshifts. A proof for mixing subshifts of finite type appears in the paper of Boyle, Lind and Rudolph [5, Theorem 3.1], although their proof also readily applies to the general case. As this will play a role later, we provide here a short proof of this statement in order to remain as self-contained as possible.

**Proposition 2.6.** *Let  $X$  be a subshift such that the set of periodic points  $\text{Per}(X)$  is dense in  $X$ . The automorphism group  $\text{Aut}(X)$  is residually finite.*

*Proof.* The set of periodic points  $P := \text{Per}(X)$  is shift-invariant. An automorphism of  $X$  induces an automorphism of  $P$ . Since  $P$  is dense, the restriction  $\text{Aut}(X) \rightarrow \text{Aut}(P)$  is injective and so  $\text{Aut}(X)$  embeds as a subgroup of  $\text{Aut}(P)$ . It therefore suffices to show that  $\text{Aut}(P)$  is residually finite.

Let  $P(n)$  be the set of points of period  $n$  in  $X$ . There is an induced map  $f_n: \text{Aut}(P) \rightarrow \text{Aut}(P(n))$  given by restriction. Note that  $\text{Aut}(P(n))$  is finite, as  $P(n)$  is finite. For every automorphism  $g \in \text{Aut}(P) \setminus \{1\}$ , there is a natural number  $n$  such that  $g(x) \neq x$  for some  $x \in P(n)$ . Hence,  $f_n(g) \neq 1$ , and so  $\text{Aut}(P)$  is residually finite.  $\square$

### 3. THE SHUFFLE GROUP

In this section, we introduce an important building block and precursor to many of the automorphisms that we will construct on RS-subshifts, so-called *shuffles*. Deterministic substitutions are also random substitutions, however they are precisely the substitutions for which shuffles will turn out to always be trivial—deterministic substitutions are also extremely well-studied. We therefore restrict our attention to the study of subshifts coming from properly random substitutions, and so it makes sense to restrict to this class and to treat the deterministic case as ‘degenerate’.

**Definition 3.1.** A random substitution  $\vartheta$  is *degenerate* if  $\#\vartheta(a) = 1$  for all  $a \in \mathcal{A}$  and *non-degenerate* otherwise. A random substitution  $\vartheta$  is *k*-*branching* if there exists a letter  $a \in \mathcal{A}$  and  $p \geq 1$  with  $\#\vartheta^p(a) \geq k$  and is *branching* if  $\vartheta$  is *k*-branching for all  $k \geq 1$ .

It turns out that one requires only very weak conditions in order to have branching.

**Proposition 3.2.** *If  $\vartheta$  is a non-degenerate, primitive random substitution and  $X_\vartheta$  is non-empty, then  $\vartheta$  is branching.*

We leave the proof as an exercise to the reader, but note that when  $X_\vartheta$  is non-empty, then by results in [25], there exists a letter  $a \in \mathcal{A}$  such that  $\vartheta(a)$  contains a word of length greater than 1.

**Remark 3.3.** Primitivity is only a sufficient condition in the above proposition, as the non-primitive branching substitution  $a \mapsto \{ab, ba\}$ ,  $b \mapsto \{a\}$ ,  $c \mapsto \{aca\}$  illustrates.

**Definition 3.4.** Let  $\vartheta$  be a recognisable compatible random substitution and let  $x \in X_\vartheta$  be an element of the RS-subshift. By recognisability, for  $0 \leq k \leq |\vartheta(y_0)| - 1$ , we may unambiguously write  $x$  as a bi-infinite concatenation of level- $n$  inflation words as

$$\sigma^{-k}(\cdots u_{-1}.u_0u_1\cdots) \quad \in \quad \sigma^{-k}(\cdots \vartheta^n(y_{-1}).\vartheta^n(y_0)\vartheta^n(y_1)\cdots).$$

Let  $a \in \mathcal{A}$  and let  $\alpha \in \text{Sym}(\vartheta^n(a))$  be a permutation of the set of level- $n$  inflation words  $\vartheta^n(a)$ . We define the map  $f_\alpha: X_\vartheta \rightarrow X_\vartheta$  by applying the permutation  $\alpha$  to each  $u_i$  of type  $\vartheta^n(a)$  in the above decomposition of  $x$ .

Note that such a map is well-defined for recognisable substitutions and it is clearly a continuous, invertible function that commutes with the shift action. It follows that  $f_\alpha$  is an automorphism of  $X_\theta$ . So, the set

$$\Gamma_{n,a} := \{f_\alpha \colon X_\vartheta \rightarrow X_\vartheta \mid \alpha \in \text{Sym}(\vartheta^n(a))\}$$

forms a group of automorphisms of  $X_\vartheta$  isomorphic to the symmetric group  $S_{|\vartheta^n(a)|}$ . We similarly define

$$\Gamma_n := \langle \Gamma_{n,a} \mid a \in \mathcal{A} \rangle = \prod_{a \in \mathcal{A}} \Gamma_{n,a}, \quad \Gamma := \bigcup_{n \geq 1} \Gamma_n,$$

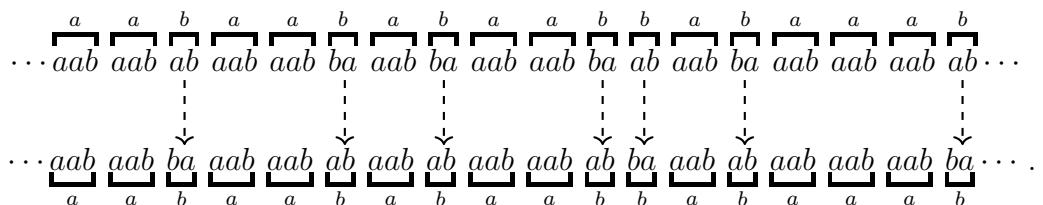
and call  $\Gamma$  the *shuffle group* of  $\vartheta$ . An element  $f_\alpha \in \Gamma_n$  is called a *level- $n$  shuffle*. Note that  $\Gamma_n$  is a subgroup of  $\Gamma_{n+1}$  and so  $\Gamma$  is an infinite union of nested subgroups of  $\text{Aut}(X_\vartheta)$ . It follows that  $\Gamma$  is also a subgroup of  $\text{Aut}(X_\vartheta)$ .

**Example 3.5.** Let  $\vartheta$  be the random square Fibonacci substitution given by

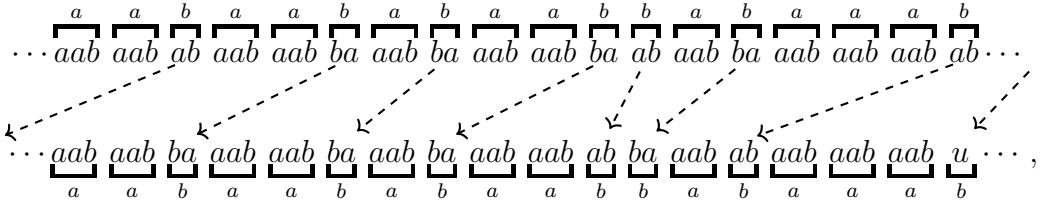
$$\vartheta: a \mapsto \{aab\}, b \mapsto \{ab, ba\}.$$

Write  $u_1 = ab$  and  $u_2 = ba$ . We already showed that  $\vartheta$  is recognisable in Example 2.5.

Let  $\alpha$  be the non-trivial element of  $\text{Sym}(\vartheta(b))$ . The shuffle  $f_\alpha \in \Gamma_{1,b}$  is the one which replaces all occurrences of  $u_1$  in an element of  $X_\vartheta$  by  $u_2$  and vice versa. So, for instance, the action of  $f_\alpha$  maps in the following way



A shuffle can be thought of as a local rule on inflation words which can only see as far as the nearest inflation word. It is therefore also natural to consider *generalised shuffles* that can see further than just the nearest inflation word, in order to give rise to more interesting automorphisms (in analogue to sliding block codes with radius larger than 0). For instance, consider the following example, where the local rule also depends on the next nearest inflation word to the right. Define an automorphism  $f$ , which replaces an occurrence of  $u_i$  with  $u_j$  where  $u_j$  is the inflation word of type  $\vartheta(b)$  that is immediately to the right of  $u_i$ . For instance, the same element as before is mapped in the following way under the action of  $f$



where  $u$  depends on unknown information to the right. The inverse is then given by replacing each  $u_i$  with the inflation word to its immediate left. Continuity of  $f$  is clear, as is the fact that  $f$  commutes with the shift. Indeed, every word of length 12 contains at least one occurrence of a type- $b$  inflation word, so  $f$  is locally defined and describes a sliding block code. In essence, this automorphism keeps all type- $a$  inflation words fixed, but ‘shifts’ the type- $b$  inflation words to the left. Notice that shuffles have finite order, whereas this generalised shuffle  $f$  has infinite order. Aperiodicity of  $X_\vartheta$  follows from recognisability of  $\vartheta$ . As  $\mathcal{A}$  has only two letters, that means the  $as$ , and hence also the inflation words of type  $\vartheta(a)$ , are aperiodically positioned and so this automorphism  $f$  is not a power of the shift  $\sigma$ . Nor is  $f$  contained in  $\langle \sigma \rangle \Gamma$ , the subgroup of  $\text{Aut}(X)$  generated by shuffles and shifts.

With the previous example in mind, it is not so surprising that automorphism groups of RS-subshifts are similar in many respects to the automorphism groups of full shifts. As we shall see later, this pseudo-embedding of the shift on  $\{0, 1\}^\mathbb{Z}$  into  $\text{Aut}(X_\vartheta)$  can be generalised to any automorphism on  $\{0, 1, \dots, n\}^\mathbb{Z}$ . For now though, we concentrate just on the shuffle group, which has its own rich structure.

Clearly, for a degenerate random substitution, the shuffle group is trivial. Conversely, the shuffle group for a  $k$ -branching substitution is always non-trivial. In fact, for a branching random substitution, as  $\#\vartheta^n(a)$  can be arbitrarily large, and  $\Gamma_{n,a}$  is a symmetric group on  $\#\vartheta^n(a)$  elements, Cayley’s theorem tells us that every finite group  $G$  embeds into  $\Gamma_{n,a}$  for some  $n \geq 1$ ,  $a \in \mathcal{A}$ .

**Proposition 3.6.** *Let  $\vartheta$  be a recognisable, branching, compatible, random substitution. Any finite group  $G$  embeds into the shuffle group  $\Gamma$ .*  $\square$

**Remark 3.7.** Given the above discussion, we now make the standing assumption that all random substitutions under consideration are branching, unless stated otherwise.

Much more can be said about the structure of the shuffle group. Before introducing general results, we begin with a particularly illuminating example which showcases some of the more varied subgroups that can be found within the shuffle group.

**Example 3.8.** Let  $\vartheta$  be a random substitution on the alphabet  $\mathcal{A} = \{0, 1, 2\}$  given by

$$\vartheta: 0 \mapsto \{012, 210\}, \quad 1 \mapsto \{120, 021\}, \quad 2 \mapsto \{201, 102\}.$$

Notice that  $\vartheta$  is invariant under cyclic permutation of letters. That is, if we define  $\bar{a} := a + 1 \pmod{3}$  and we extend this to words  $u$ , so that  $\overline{u_1 \cdots u_k} := \overline{u_1} \cdots \overline{u_k}$ , then  $u \in \vartheta(a) \iff \bar{u} \in \vartheta(\bar{a})$ . Further, this extends to powers, so  $u \in \vartheta^k(a) \iff \bar{u} \in \vartheta^k(\bar{a})$ .

This random substitution is primitive and compatible. To see that  $\vartheta$  is recognisable, let

$$\cdots c_{-2} a_{-1} b_{-1} c_{-1} a_0 b_0 c_0 a_1 b_1 c_1 a_2 b_2 \cdots$$

$\underbrace{\phantom{c_{-2} a_{-1} b_{-1} c_{-1}}}_{\vartheta(y_{-1})} \underbrace{\phantom{a_0 b_0 c_0}}_{\vartheta(y_0)} \underbrace{\phantom{a_1 b_1 c_1}}_{\vartheta(y_1)}$

be a decomposition of  $x \in X_\vartheta$ , with preimage  $y \in X_\vartheta$ . If there is another decomposition of  $x$ , then by the fact that  $\vartheta$  is constant length, the borders of inflation words are offset everywhere from the above decomposition by either 1 or 2 to the right. Without loss of generality, suppose that the offset is 1. That is, there is another decomposition of  $x$  which looks like

$$\cdots c_{-2} a_{-1} b_{-1} c_{-1} a_0 b_0 c_0 a_1 b_1 c_1 a_2 b_2 \cdots$$

$\underbrace{\phantom{c_{-2} a_{-1} b_{-1} c_{-1} a_0}}_{\vartheta(z_{-1})} \underbrace{\phantom{b_0 c_0 a_1}}_{\vartheta(z_0)} \underbrace{\phantom{b_1 c_1 a_2}}_{\vartheta(z_1)}$

for some other preimage  $z \in X_\vartheta$ .

Observe that  $\vartheta(a)$  contains exactly one copy of each letter 0, 1, 2 and so it follows by induction that  $a_i = a_j$  for all  $i, j \in \mathbb{Z}$ . However, this is impossible because if  $a_0 = 0$  for instance, then this would imply that every realisation of  $\vartheta(z_i)$  ends with 0, which cannot be the case if  $z_i = 2$  (and infinitely many of the  $z_i$  are 2). We reach similar contradictions if  $a_0 = 1$  or  $a_0 = 2$ . It follows that the second decomposition cannot exist and so  $x$  has a unique substitutive preimage. Hence,  $\vartheta$  is recognisable.

We now define a set of shuffles which respect the symmetry under adding bars. Let  $n \geq 1$  and  $\alpha \in \text{Sym}(\vartheta^n(0))$ . Given this permutation  $\alpha$ , define the associated permutations  $\bar{\alpha} \in \text{Sym}(\vartheta^n(1))$  and  $\overline{\bar{\alpha}} \in \text{Sym}(\vartheta^n(2))$  by

$$\bar{\alpha}(\overline{u}) = \overline{\alpha(u)}, \quad \overline{\bar{\alpha}}(\overline{\overline{u}}) = \overline{\overline{\alpha(u)}}.$$

Then the automorphism  $g_\alpha = f_\alpha \circ f_{\bar{\alpha}} \circ f_{\overline{\bar{\alpha}}}$  is a level- $n$  shuffle. If we define

$$G_n := \{g_\alpha \mid \alpha \in \text{Sym}(\vartheta^n(0))\} \leq \Gamma_n,$$

then it is clear that  $G_n$  is isomorphic to the symmetric group  $S_{|\vartheta^n(0)|}$  and is a subgroup of  $G_{n+1}$ .

The number of inflation words in  $\vartheta^n(0)$  is calculated to be

$$\prod_{i=0}^{n-1} 2^{3^i} = 2^{a(n)},$$

where  $a(n) = \frac{1}{2}(3^n - 1) \in \mathbb{N}$  and so is an integral power of 2. Hence,  $G_n \cong S_{2^{a(n)}}$ . The inclusion  $G_n \hookrightarrow G_{n+1}$  then commutes with the induced map  $S_{2^{a(n)}} \hookrightarrow S_{2^{a(n+1)}}$  which permutes partitions of  $\{1, \dots, 2^{a(n+1)}\}$  into blocks of length  $2^{a(n)}$  of consecutive integers

(in analogue to how  $S_n$  embeds into  $S_{2n}$  by acting on  $\{1, \dots, 2n\}$  by permuting pairs of the form  $(2i-1, 2i)$ ); a so-called *strictly diagonal embedding* in the sense of [19]. The inclusion  $G_n \hookrightarrow G_{n+1}$  is therefore defined as follows. Let  $\alpha \in \text{Sym}(\vartheta^n(0))$  and  $g_\alpha \in G_n$  and write  $\alpha_0 = \alpha$ ,  $\alpha_1 = \overline{\alpha}$  and  $\alpha_2 = \overline{\overline{\alpha}}$ . Let  $u \in \vartheta^{n+1}(0)$ . The word  $u$  is a concatenation of three words  $u = u_1 u_2 u_3$ , where  $u_i \in \vartheta^n(j(i))$  for  $j(i) \in \mathcal{A}$ . We define  $\beta(u) = \alpha_{j(1)}(u_1) \alpha_{j(2)}(u_2) \alpha_{j(3)}(u_3)$  and then the embedding is given by  $g_\alpha \mapsto g_\beta$ .

It turns out that the direct limit

$$G = \varinjlim (S_{2^{a(n)}} \hookrightarrow S_{2^{a(n+1)}})$$

is isomorphic to the intersection of the group of finite interval exchange transformations IET and Thompson's group  $V$ .

Recall that Thompson's group  $V$  is the group of piecewise-linear bijections of the interval  $[0, 1]$  whose set of discontinuities are dyadic rationals (points of the form  $\frac{i}{2^n}$ ,  $0 \leq i \leq 2^n$ ). Therefore, the intersection  $\text{IET} \cap V$  is the group of piecewise-linear bijections of  $[0, 1]$  of constant slope 1 (IETs), with finitely many discontinuities at dyadic rationals.

The isomorphism  $\iota: G \rightarrow \text{IET} \cap V$  is given as follows. Let  $\alpha \in \text{Sym}(\vartheta^n(0)) \cong S_{2^{a(n)}}$  be a permutation of level- $n$  inflation words, which we identify with a permutation of the set  $\{1, \dots, 2^{a(n)}\}$  and let  $g_\alpha \in G_n$  be the corresponding shuffle. For  $m \geq n$ , let  $f_{nm}: G_n \hookrightarrow G_m$  be the diagonal embedding described above. Define  $\iota_n: G_n \rightarrow \text{IET} \cap V$  to be the interval exchange transformation

$$\iota_n(g_\alpha): \left[ \frac{i-1}{2^{a(n)}}, \frac{i}{2^{a(n)}} \right] \mapsto \left[ \frac{\alpha(i)-1}{2^{a(n)}}, \frac{\alpha(i)}{2^{a(n)}} \right]$$

for  $1 \leq i \leq 2^{a(n)}$ . From the definition of the diagonal embedding  $f_{nm}$ , we have  $\iota_n = \iota_m \circ f_{nm}$ , and so we get an induced homomorphism  $\iota: G \rightarrow \text{IET} \cap V$ .

Every element of  $\text{IET} \cap V$  is given as the image of some  $g_\alpha$  under  $\iota_n$  for some  $n \geq 1$  and so  $\iota$  is surjective. Injectivity of  $\iota$  is clear because the only shuffle which maps to the identity exchange transformation is the identity shuffle.

Another description of  $G$  is as a direct limit of the automorphism groups of finite binary rooted trees of height  $n$ ,  $n \geq 1$ , where the connecting morphisms are the diagonal embeddings of height- $n$  automorphisms into height- $(n+1)$  automorphisms (acting the same on both height- $n$  subtrees that do not contain the root).

Notice that if  $\alpha \in S_{2^{a(n)}}$  is an even permutation, then  $f_{nm}(g_\alpha) = g_\beta$  where  $\beta \in S_{2^{a(m)}}$  is also an even permutation (this is a general property of homomorphic images of alternating groups in symmetric groups). Hence,  $f_{nm}$  restricts to a diagonal embedding of alternating groups  $A_{2^{a(n)}} \hookrightarrow A_{2^{a(m)}}$ . The direct limit  $H = \varinjlim (A_{2^{a(n)}} \hookrightarrow A_{2^{a(n+1)}})$  associated with these embeddings is a union of simple groups and is therefore itself simple. Moreover,  $H$  is clearly an infinite group, and so  $\Gamma$ , and hence  $\text{Aut}(X_\vartheta)$ , contains an infinite simple subgroup. It follows that  $\text{Aut}(X_\vartheta)$  cannot be residually finite.

We emphasise the remarkable property that  $\text{Aut}(X_\vartheta)$  contains both the automorphism group  $\text{Aut}(X_2)$  of a full shift and an infinite simple subgroup. Other such examples exist, but of a rather artificial flavour, such as the product of the Thue-Morse subshift  $X_{TM}$

and  $X_2$  with the diagonal action<sup>3</sup>. Whereas, most would agree that  $X_\vartheta$  is a more natural example. Of course, it should be noted that  $X_{TM} \times X_2$  is in fact an RS-subshift with (non-compatible, non-recognisable) random substitution given by

$$\vartheta: a_i \mapsto \{a_0b_0, a_0b_1, a_1b_0, a_1b_1\}, \quad b_i \mapsto \{b_0a_0, b_0a_1, b_1a_0, b_1a_1\}, \quad i \in \{0, 1\}.$$

There are few known classes of examples for which the automorphism group contains an infinite simple subgroup. Perhaps the simplest example is the subshift  $X_{\leq 2}$  comprising all sequences in  $\{0, 1\}$  for which the letter 1 appears at most twice. Indeed, Salo and Shraudner [29] showed that if a countable subshift  $X$  contains an infinite set of isolated points in distinct orbits with the same eventually periodic tails, then  $\mathbb{Z}^\omega \rtimes S_\infty$  is a subgroup of  $\text{Aut}(X)$  and so contains the infinite alternating group  $A_\infty$ . In  $X_{\leq 2}$ , such a set of isolated points is given by  $\{\cdots 0010^n100\cdots \mid n \geq 0\}$ . However, our subshift  $X_\vartheta$  is very different, being uncountable and containing no isolated points. In particular,  $X_\vartheta$  is even transitive.

**3.1. The alternating shuffle group.** The shuffle group in the last example was shown to contain an infinite simple subgroup, and therefore the automorphism group  $\text{Aut}(X_\vartheta)$  is not residually finite. This property applies more generally than just for this example. To show this, we need to introduce some results from basic group theory.

For the benefit of the reader, we restate Goursat's Lemma [16, Theorem 5.5.1].

**Lemma 3.9** (Goursat's Lemma). *Let  $G = G_1 \times G_2$  be a product of groups with projection maps  $\pi_i$  onto  $G_i$ . Let  $N$  be a subgroup of  $G$  with the property that  $\pi_i(N) = G_i$  and write  $N_1 = N \cap \ker \pi_2$ ,  $N_2 = N \cap \ker \pi_1$ . Then, the image of  $N$  under the quotient  $q: G \rightarrow G_1/N_1 \times G_2/N_2$  is the graph of an isomorphism  $\phi: G_1/N_1 \rightarrow G_2/N_2$ . That is,*

$$q(N) = \{(g, \phi(g)) \mid g \in G_1/N_1\}.$$

Using Goursat's Lemma, we can prove the following classification result for normal subgroups of finite products of non-abelian simple groups.

**Lemma 3.10.** *Let  $G = G_1 \times \cdots \times G_n$  be a product of non-abelian simple groups and let  $N \subset G$  be a normal subgroup. Then  $N$  is a product of  $G_i$ 's.*

*Proof.* We proceed by induction on  $n$ . The statement is trivially true if  $n = 1$ . Suppose the statement holds for  $n - 1$ . We identify the factors  $G_i$  with elements of  $G$  that have all coordinates equal to 1 except their  $i$ -th coordinate. Write  $G$  as  $G_1 \times (G_2 \times \cdots \times G_n) = G_1 \times \widehat{G}$ . By the inductive hypothesis, a normal subgroup of  $\widehat{G}$  is a product of  $G_i$ 's for  $i > 1$ . If the projection of  $N$  onto  $\widehat{G}$  is not surjective, then  $N$  is contained in a product of fewer than  $n$  simple groups and we are done by induction. By a similar argument, the projection of  $N$  on the first coordinate is also surjective. Let  $K_1$  be the kernel of the projection of  $N$  onto the second coordinate. It is a normal subgroup of  $G_1$ , hence it is either equal to  $G_1$  or to  $\{1\}$ . In the first case,  $G_1$  is a Cartesian factor of  $N$  and we are done by induction.

---

<sup>3</sup>This is a non-trivial result, the proof of which is beyond the scope of this work. Unfortunately, we are not aware of a reference.

Now, suppose that  $K_1 = \{1\}$  and let  $\widehat{K}$  be the kernel of the projection onto the *first* coordinate. By Goursat's lemma, the image of  $N$  in  $G_1 \times \widehat{G}/\widehat{K}$  is the graph of an isomorphism  $\phi: G_1 \rightarrow \widehat{G}/\widehat{K}$ . Since  $N$  is a normal subgroup of  $G_1 \times \widehat{G}$ , the graph  $\{(g, \phi(g)) \mid g \in G_1\}$  is normal in  $G_1 \times \widehat{G}/\widehat{K}$ . In particular, for all  $h \in \widehat{G}/\widehat{K}$  and  $g \in G_1$ ,  $(1, h)(g, \phi(g))(1, h)^{-1} = (g', \phi(g'))$  for some  $g' \in G_1$ . Then

$$\begin{aligned} (g', \phi(g')) &= (1, h)(g, \phi(g))(1, h)^{-1} \\ &= (1, h)(g, \phi(g))(1, h^{-1}) \\ &= (g, h\phi(g)h^{-1}). \end{aligned}$$

So,  $g' = g$ . Hence, for all  $h \in \widehat{G}/\widehat{K}$  and  $g \in G_1$ , we have  $\phi(g) = h\phi(g)h^{-1}$ . So,  $\phi(G_1)$  is in the center of  $\widehat{G}/\widehat{K}$ . Since  $\phi(G_1) = \widehat{G}/\widehat{K}$ , this group is abelian, which contradicts our assumption that  $G_1$  is non-abelian.  $\square$

In particular,  $G = G_1 \times \cdots \times G_n$  has the remarkable property that if  $N$  is a normal subgroup of  $G$  and  $M$  is a normal subgroup of  $N$ , then  $M$  is normal in  $G$ .

We now return to our shuffle groups. It is clear from the definitions that  $\Gamma_n \subset \Gamma_{n+1}$  and we have an ascending chain of finite products of symmetric groups. Let  $A_{n,a} \subset \Gamma_{n,a}$  be the alternating subgroup. That is,  $A_{n,a}$  is the subgroup  $\{f_\alpha \mid \alpha \in \text{Sym}(\vartheta^n(a)), \alpha \text{ is even}\}$ . Let  $A_n = \prod A_{n,a}$ . By construction,  $A_n$  is a product of simple groups. Finally, we define  $A = \bigcup_{n \geq 1} A_n$  and call this subgroup the *alternating shuffle group*. While the group  $H$  in Example 3.8 is not an alternating shuffle group, it is a subgroup of  $A$ . Our goal will be to generalise that construction and to find an analogue for the group  $H$  in general, which is an infinite simple subgroup of shuffles.

**Lemma 3.11.** *Let  $d$  be the cardinality of the alphabet  $\mathcal{A}$ . The groups  $A_n$  form an ascending chain and  $A \subset \Gamma$  is a normal subgroup of index bounded above by  $2^d$ .*

*Proof.* Consider the composition  $q \circ i$  of the inclusion  $i: \Gamma_n \rightarrow \Gamma_{n+1}$  and the quotient map  $q: \Gamma_{n+1} \rightarrow \Gamma_{n+1}/A_{n+1} \cong (\mathbb{Z}/2\mathbb{Z})^d$ . It maps  $\Gamma_n$  to an abelian group. Since  $A_n$  is the commutator subgroup of  $\Gamma_n$ , it is in the kernel of  $q \circ i$ . In other words,  $A_n$  is a subgroup of  $A_{n+1}$ . We have  $\Gamma/A = \bigcup \Gamma_n A/A$ , an increasing union of sets. Since  $\Gamma_n A/A \cong \Gamma_n/(\Gamma_n \cap A)$  and since  $\Gamma_n/(\Gamma_n \cap A)$  is a quotient of  $\Gamma_n/A_n$ , its order divides  $2^d$ . Therefore,  $[\Gamma : A]$  divides  $2^d$ .  $\square$

We note that in our considerations, we do not impose any restrictions on how  $\Gamma_n$  embeds into  $\Gamma_{n+1}$ . It is possible to define a chain  $G_1 \subset G_2 \subset \cdots$  of products of symmetric groups such that each  $G_n$  embeds in the alternating group of the first factor of  $G_{n+1}$ . In such a case,  $G = \bigcup G_n$  would be a union of an ascending chain of symmetric groups, which is equal to the union of the alternating subgroups  $A$ . In other words, the index of  $A$  would be equal to 1.

**Corollary 3.12.** *All non-trivial normal subgroups of the alternating shuffle group  $A$  have infinite index. Hence,  $A$  is not residually finite.*

*Proof.* Suppose  $N \subseteq A$  is a non-trivial normal subgroup. Then each  $N \cap A_n$  is normal. For large enough  $n$ ,  $N \cap A_n$  is eventually always non-trivial, as otherwise, every  $N \cap A_n$  would be trivial (because  $N \cap A_n \subseteq N \cap A_{n+1}$ ), contradicting  $N \cap A$  being non-trivial. Without loss of generality, assume that  $A_{n,a}$  is simple for all  $n \geq 1$  and  $a \in \mathcal{A}$  (if not, by branching, replace  $\vartheta$  with a large enough power  $\vartheta^p$  so that  $\#\vartheta^p(a) \geq 5$  for all  $a$ ). Then, since  $A_n$  is a product of simple groups, either  $N \cap A_n$  is equal to  $A_n$ , or it has index at least as large as the smallest cardinality of one of its factors  $A_{n,a}$  because  $N \cap A_n$  is eventually non-trivial. Since these cardinalities increase to  $\infty$  with  $n$ , either  $N$  is equal to  $A$  or it has infinite index. For a group to be residually finite, it must contain at least one non-trivial normal subgroup of finite index.  $\square$

**Theorem 3.13.** *The alternating shuffle group  $A$  contains an infinite simple subgroup.*

*Proof.* First of all observe that  $A$  inherits the remarkable property that if  $N$  is normal in  $A$  and  $M$  is normal in  $N$ , then  $M$  is normal in  $A$ . By Lemma 3.10, every descending chain of normal subgroups in  $A_n$  has length at most  $n + 1$ . This implies that every descending chain of normal subgroups in  $A$  has length at most  $n + 1$ . Let  $N$  be the last non-trivial normal subgroup in such a chain. It contains no proper normal subgroup, since every  $M$  that is normal in  $N$  is normal in  $A$ .  $N$  is a simple group.  $\square$

Hence, the shuffle group  $\Gamma$  and the full automorphism group  $\text{Aut}(X_\vartheta)$  contain an infinite simple subgroup and are not residually finite.

While the shuffle group is a large subgroup of the automorphism group, there are many more varied automorphisms for RS-subshifts. By generalising the shuffle procedure slightly; allowing shuffles to depend on local information (in analogue to finite block codes), we get a more complete picture of how the automorphism group looks. This is what we explore in the next section.

#### 4. AUTOMORPHISM GROUPS FOR RECOGNISABLE SUBSTITUTIONS

**Definition 4.1.** We say that the letter  $a \in \mathcal{A}$  appears with uniformly bounded gaps in a subshift  $X$  if the set  $\{aua \in \mathcal{L}(X) \mid u \in (\mathcal{A} \setminus \{a\})^*\}$  is finite.

Equivalently, the letter  $a \in \mathcal{A}$  appears with uniformly bounded gaps in  $X$  if and only if there exists a uniform bound  $m$  such that  $u \in \mathcal{L}^m(X)$  implies that  $|u|_a \geq 1$ .

**Lemma 4.2.** *Let  $\vartheta$  be a primitive, compatible random substitution. For every  $a$  in  $\mathcal{A}$ , the letter  $a$  appears infinitely often in every element in  $X_\vartheta$  and with uniformly bounded gaps.*

*Proof.* By primitivity, we may suppose without loss of generality that every entry of  $M_\vartheta$  is positive. Let  $m = \max_{a \in \mathcal{A}} \{|\vartheta(a)|\}$ . Let  $a \in \mathcal{A}$  be some fixed letter and let  $x \in X_\vartheta$  be an arbitrary element in the RS-subshift. By results in [25], there exists an element  $y \in X_\vartheta$  such that  $\sigma^{-i}(x) \in \vartheta(y)$  for some  $0 \leq i \leq |\vartheta(y_0)|$ . It follows that  $x$  can be decomposed into an exact concatenation of words of the form  $\vartheta(y_j)$ . As  $M_\vartheta$  is positive, every such word contains the letter  $a$ , and so  $x$  contains infinitely many appearances of the letter  $a$ .

and each appearance of  $a$  is at most a distance  $2m$  apart. As  $m$  depends only on  $M_\vartheta$ , it is a uniform bound for all  $x$ , as required.  $\square$

**Remark 4.3.** We should mention that the above Lemma is perfectly compatible with the fact that  $X_\vartheta$  is, in general, not uniformly recurrent. All that Lemma 4.2 gives us is uniformly bounded returns to single letters, rather than words. In fact, for suitably nice RS-subshifts, there must exist a word  $u$  that has arbitrarily large gaps between occurrences in some elements of the subshift. This will be proved later and used when studying the constant length case in Section 6.

**Theorem 4.4.** *Let  $\vartheta$  be a non-degenerate, compatible, primitive, recognisable random substitution. Let  $X_n$  be the full shift on  $n$  letters. The automorphism group  $\text{Aut}(X_2)$  embeds into the automorphism group  $\text{Aut}(X_\vartheta)$ .*

*Proof.* It is well-known that for every  $n, m \geq 2$  the automorphism group  $\text{Aut}(X_n)$  embeds into the automorphism group  $\text{Aut}(X_m)$  [18], and so it is enough to show that for some  $n$ ,  $\text{Aut}(X_n)$  embeds into  $X_\vartheta$ . Let  $a \in \mathcal{A}$  be any letter in the alphabet. Without loss of generality, by Proposition 3.2, suppose that  $\#\vartheta(a) \geq 2$  and let  $n = \#\vartheta(a)$  (if not, take a higher power  $\vartheta^k$ , for which all of the assumptions on  $\vartheta$  still hold). Write  $\vartheta(a) = \{u_1, \dots, u_n\}$ . For every  $x \in X_\vartheta$ , by recognisability, we may write  $x$  uniquely as a concatenation of words

$$\cdots \square \vartheta(a) \square \vartheta(a) \square \vartheta(a) \square \vartheta(a) \square \vartheta(a) \square \vartheta(a) \square \cdots,$$

where  $\square$  is used to represent some collection of inflation words not of type  $a$ , that is,  $\square$  is a word of the form  $\vartheta(w)$  with  $w \in (\mathcal{A} \setminus \{a\})^*$ . Our arguments will all be compatible with action under the shift, and so it is not necessary for us to identify the origin of  $x$ . Note that the possible realisations of the  $\square$ s are uniformly bounded in length by Lemma 4.2. That is, there exists some  $M \geq 1$  such that for all realisations of  $\square$ ,  $|\square| \leq M$ .

So, there exists a unique bi-infinite sequence  $\omega \in \{1, \dots, n\}^{\mathbb{Z}}$  (up to a shift) such that

$$x = \cdots \square u_{\omega(-2)} \square u_{\omega(-1)} \square u_{\omega(0)} \square u_{\omega(1)} \square u_{\omega(2)} \square \cdots.$$

Let  $\alpha$  be an automorphism of  $X_n$ . We define a map  $f_\alpha: X_\vartheta \rightarrow X_\vartheta$  by

$$f_\alpha(x) = \cdots \square u_{(\alpha\omega)(-2)} \square u_{(\alpha\omega)(-1)} \square u_{(\alpha\omega)(0)} \square u_{(\alpha\omega)(1)} \square u_{(\alpha\omega)(2)} \square \cdots.$$

To see that  $f_\alpha(x) \in X_\vartheta$ , note that, by recognisability, there exists a unique  $y \in X_\vartheta$  and a unique  $0 \leq k \leq |\vartheta(y_0) - 1|$  such that  $\sigma^{-k}(x) \in \vartheta(y)$ . This unique preimage  $y$  is also a preimage of  $f_\alpha(x)$ , by construction of  $f_\alpha(x)$ , as the placement of inflation words and their types has not changed, only their realisations. That is,  $\sigma^{-k}(f_\alpha(x)) \in \vartheta(y)$ . As  $\vartheta(y) \subset X_\vartheta$ , it follows that  $f_\alpha(x) \in X_\vartheta$ .

The map  $f_\alpha$  is an example of a generalised shuffle, as mentioned in the discussion of Example 3.5, whose radius is uniformly bounded in length. This follows from the fact that  $\alpha$  is a sliding block code, all realisations of  $\square$  are uniformly bounded in length, and the length  $|\vartheta(a)|$  is fixed for all realisations. As such  $f_\alpha$  is itself a sliding block code, and so is a shift-commuting continuous function on  $X_\vartheta$ .

It is not difficult to see that  $f_\alpha \circ f_{\alpha^{-1}} = f_{\alpha^{-1}} \circ f_\alpha = \text{Id}_{X_\vartheta}$ , and so  $f_\alpha \in \text{Aut}(X_\vartheta)$ . Further, it is clear that  $f_{\alpha \circ \beta} = f_\alpha \circ f_\beta$  and so the map  $\text{Aut}(X_n) \rightarrow \text{Aut}(X_\vartheta): \alpha \mapsto f_\alpha$  is a group homomorphism.

As  $f_\alpha(x)$  is derived from  $x$  by replacing inflation words with other inflation words of the same type,  $f_\alpha(x) = x$  if and only if  $u_{\alpha\omega(i)} = u_{\omega(i)}$  for every  $i$ , hence  $\alpha\omega = \omega$ . If  $\alpha$  is non-trivial, then there exists some  $\hat{\omega} \in \{1, \dots, n\}^{\mathbb{Z}}$  such that  $\alpha\hat{\omega} \neq \hat{\omega}$ , and so

$$f_\alpha(\cdots \square u_{\hat{\omega}(-1)} \square u_{\hat{\omega}(0)} \square u_{\hat{\omega}(1)} \square \cdots) \neq \cdots \square u_{\hat{\omega}(-1)} \square u_{\hat{\omega}(0)} \square u_{\hat{\omega}(1)} \square \cdots.$$

It follows that  $f_\alpha$  is not the identity, and so the map  $\text{Aut}(X_n) \rightarrow \text{Aut}(X_\vartheta): \alpha \mapsto f_\alpha$  is an embedding.  $\square$

As an immediate corollary, any subgroup of  $\text{Aut}(X_2)$  embeds into  $\text{Aut}(X_\vartheta)$ , and so by results of Boyle, Lind and Rudolph [5], we can also identify the following subgroups of  $\text{Aut}(X_\vartheta)$ .

**Corollary 4.5.** *Let  $\vartheta$  be a non-degenerate, compatible, primitive, recognisable random substitution. The following groups embed into the automorphism group  $\text{Aut}(X_\vartheta)$ :*

- $\text{Aut}(X_n)$ ,  $n \geq 2$ ,
- every countable direct sum of finite groups,
- Any finite free product  $(\mathbb{Z}/2\mathbb{Z})^{*n} = \mathbb{Z}/2\mathbb{Z} * \cdots * \mathbb{Z}/2\mathbb{Z}$ , hence the free group  $F_2$  on 2 generators, hence the free group  $F_n$  on  $n \geq 1$  generators, and the free group  $F_\omega$  on countably many generators,
- the countable direct sum  $\mathbb{Z}^\omega = \bigoplus_{i=1}^{\infty} \mathbb{Z}$ .

Moreover,  $\text{Aut}(X_\vartheta)$  contains all of the other subgroups mentioned in the discussion in Section 2.2.

Given the above, a natural question is whether there are subgroups of  $\text{Aut}(X_\vartheta)$  which do not appear as subgroups of the group  $\text{Aut}(X_2)$ . In fact, this follows from Theorem 3.13, as the alternating shuffle group  $A$  contains an infinite simple group.  $\text{Aut}(X_2)$  is residually finite (by Proposition 2.6), and so  $A$  cannot appear as a subgroup of  $\text{Aut}(X_2)$ . It follows that  $\text{Aut}(X_\vartheta)$  is in a very concrete sense ‘larger’ than  $\text{Aut}(X_2)$ .

## 5. LOCAL RECOGNISABILITY

Gohlke, Rust and Spindeler introduced the notion of an *inflation word decomposition* for random substitutions [14]. This definition is key to defining a local version of recognisability, as is done for deterministic substitutions. This is also a useful framework in which to define what it means for a single word in the language to be recognisable. This notion will be used in Section 6 to relax full recognisability.

**Definition 5.1.** Let  $\vartheta$  be a random substitution and let  $u \in \mathcal{L}_\vartheta$  be a legal word. Let  $n \geq 1$  be a natural number. For words  $u_i \in \mathcal{A}^+$ , the tuple  $[u_1, \dots, u_\ell]$  is called a  $\vartheta$ -cutting of  $u$  if  $u_1 \cdots u_\ell = u$  and there exists a  $\vartheta$ -legal word  $v = v_1 \cdots v_\ell$  such that

- For  $i = 2, \dots, \ell - 1$ ,  $u_i$  is an inflation word built from the letter  $v_i$ . That is,  $u_i \in \vartheta(v_i)$ . Note that  $u_i$  is a word, while  $v_i$  is a single letter.
- $u_1$  is the suffix of an inflation word built from  $v_1$ , and
- $u_\ell$  is the prefix of an inflation word built from  $v_\ell$ .

That is,  $u$  is contained in a realisation of  $\vartheta(v)$ , which is a concatenation of inflation words, with each of the interior  $u_i$ 's being one of those inflation words.

We call  $v$  a *root* of the  $\vartheta$ -cutting and we call  $([u_1, \dots, u_\ell], v)$  the corresponding *inflation word decomposition* of  $u$ . If  $u$  actually is a realisation of  $\vartheta(v)$  for some  $v$ , so  $u_1 \in \vartheta(v_1)$  and  $u_\ell \in \vartheta(v_\ell)$ , then we say that  $u$  is an *exact* inflation word. Finally, we let  $D_\vartheta(u)$  denote the set of all decompositions of the word  $u$ .

**Example 5.2.** Let  $\vartheta: a \mapsto \{ab, ba\}, b \mapsto \{aa\}$  be the random period doubling substitution. The word  $aab$  has two possible  $\vartheta$ -cuttings  $[a, ab]$  and  $[aa, b]$  with two and one distinct roots respectively. The set of inflation word decompositions of  $aab$  is

$$D_\vartheta(aab) = \{([a, ab], aa), ([a, ab], ba), ([aa, b], ba)\}.$$

For this random substitution,  $abba$  is an exact inflation word. However,  $bb$  is not an exact inflation word, since any concatenation of inflation words containing  $bb$  must also contain some  $as$ .

Let  $u$  be a  $\vartheta$ -legal word and let  $u_{[i,j]}$  be a subword. An inflation word decomposition of  $u$  restricts to an inflation word decomposition of  $u_{[i,j]}$ , which we call an *induced inflation word decomposition*. The idea is simple, but the precise definition is somewhat technical:

**Definition 5.3.** Let  $\vartheta$  be a random substitution and let  $d = ([u_1, \dots, u_\ell], v) \in D_\vartheta(u)$  be an inflation word decomposition of  $u$ . For  $1 \leq i \leq j \leq |u| - 1$ , we write  $d_{[i,j]}$  for the *induced inflation word decomposition on the subword  $u_{[i,j]}$* , defined by

$$d_{[i,j]} = ([u_1, \dots, u_\ell], v)_{[i,j]} = ([\hat{u}_{k(i)}, u_{k(i)+1}, \dots, u_{k(j)-1}, \hat{u}_{k(j)}], v_{[k(i), k(j)]}),$$

where  $1 \leq k(i) \leq k(j) \leq \ell$  are natural numbers such that

$$|u_1 \cdots u_{k(i)-1}| < i \leq |u_1 \cdots u_{k(i)}| \text{ and } |u_1 \cdots u_{k(j)-1}| < j \leq |u_1 \cdots u_{k(j)}|,$$

$\hat{u}_{k(i)}$  is a suffix of  $u_{k(i)}$  and  $\hat{u}_{k(j)}$  is a prefix of  $u_{k(j)}$  such that

$$\hat{u}_{k(i)}u_{k(i)+1} \cdots u_{k(j)-1}\hat{u}_{k(j)} = u_{[i,j]}.$$

**Example 5.4.** Let  $\vartheta: a \mapsto \{ab, ba\}, b \mapsto \{aa\}$  be the random period doubling substitution. The legal word  $u = ababa \in \mathcal{L}_\vartheta$  has exactly four inflation word decompositions given by

$$D_\vartheta(u) = \{([a, ba, ba], aaa), ([a, ba, ba], baa), ([ab, ab, a], aaa), ([ab, ab, a], aab)\}.$$

For the subword  $u_{[2,4]} = bab$  of  $u$ , the first two elements of  $D_\vartheta(u)$  yield the induced decomposition  $d_{[2,4]}^{(1)} = ([ba, b], aa)$ , while the next two elements yield  $d_{[2,4]}^{(2)} = ([b, ab], aa)$ . Thus,  $\#\{d_{[2,4]} \mid d \in D_\vartheta(u)\} = 2$ . In this example, both possible  $\vartheta$ -cuttings of  $bab$  are induced from cuttings of  $u$ .

By contrast, the word  $u' = bbaba$  has a unique inflation word decomposition  $d' = ([b, ba, ba], aaa)$  which yields a unique induced inflation word decomposition on the subword  $u'_{[2,4]} = bab$  given by  $d'_{[2,4]} = ([ba, b], aa)$ . That is, when  $bab$  sits inside  $u$ , the embedding tells us nothing about the  $\vartheta$ -cutting of  $bab$ , but when  $bab$  sits inside  $u'$ , the embedding uniquely defines the  $\vartheta$ -cutting of  $bab$ .

**Definition 5.5.** Let  $\vartheta$  be a random substitution and let  $u \in \mathcal{L}_\vartheta$  be a legal word. We say that  $u$  is *recognisable* if there exists a natural number  $N$  such that for each legal word of the form  $w = u^{(l)}uu^{(r)}$  with  $|u^{(l)}| = |u^{(r)}| = N$ , all inflation word decompositions of  $w$  induce the same inflation word decomposition of  $u$ . That is, knowing the  $N$  letters to the left of  $u$  and the  $N$  letters to the right of  $u$  determines a unique induced inflation word decomposition of  $u$ . We call the minimum such  $N$  the *radius of recognisability* for  $u$ .

**Definition 5.6.** We call a random substitution  $\vartheta$  *locally recognisable* if there exists a natural number  $N$  such that every  $\vartheta$ -legal word is recognisable with radius at most  $N$ . The minimum such  $N$  is called the *radius of recognisability for  $\vartheta$* .

Intuitively, this means that there is a ‘window’ of radius  $2N + 1$  such that if we place the window somewhere in a word, the induced inflation word decomposition of the central letter in the window is uniquely determined. Then, for a long enough word  $u$ , as we slide the window along the word, all but the very extremal inflation words that make up  $u$  are determined. That is, we know how to uniquely decompose  $u$  into inflation words except possibly at the very ends of the word. Without loss of rigour, we will normally work with this intuitive idea of local recognisability rather than the explicit definition, as the notation can become cumbersome.

Equivalence of (global) recognisability and local recognisability is the next result.

**Proposition 5.7.** A compatible random substitution  $\vartheta$  is recognisable if and only if it is locally recognisable.

*Proof.* ( $\implies$ ) We prove the contrapositive. Suppose that  $\vartheta$  is not locally recognisable. Then for every  $N \geq 0$ , there exists a word  $v_N = v$  of the form  $v = u^{(l)}uu^{(r)}$  such that  $|u^{(l)}| = |u^{(r)}| = N$  and such that the induced inflation word decomposition of  $u$  is not unique. Note that we can assume  $|u| = 2$  without loss of generality. Extend  $v_N$  arbitrarily to a bi-infinite element  $x_N \in X_\vartheta$ . By compactness, the sequence  $(x_N)_{N \geq 0}$  has an accumulation point  $x \in X_\vartheta$ . Let  $n \in \mathbb{N}$ . We have  $x_{[-n,n]} = (x_N)_{[-n,n]}$  for some  $N \in \mathbb{N}$  and hence there are two inflation word decompositions of  $x_{[-n,n]}$  that differ at the origin. Sending  $n \rightarrow \infty$  and using compactness for the  $\vartheta$ -preimages, we find two distinct preimages of  $x$  in  $X_\vartheta$ . It follows that  $\vartheta$  is not recognisable.

( $\impliedby$ ) Let  $x \in X_\vartheta$  be an arbitrary element. Let  $N$  be the radius of recognisability for  $\vartheta$ . Existence of a preimage  $y$  for  $x$  under  $\vartheta$  is already known from work of Rust and Spindeler [25]. That is, there exists an element  $y \in X_\vartheta$  and  $0 \leq k \leq |\vartheta(y_0)| - 1$  such that  $\sigma^{-k}(x) \in \vartheta(y)$ . It remains to show uniqueness. Let  $n \geq 0$  be an arbitrary natural number and consider the word  $u := x_{[-n,n]}$ . We note that  $u$  is a subword of the word  $u' = x_{[-n-N,n+N]}$  and by local recognisability, all inflation word decompositions of  $u'$  must

induce the same inflation word decomposition on  $u$ . So any preimage  $y$  must coincide with the root of this inflation word decomposition for  $u$  on some central subword  $v = y_{[-n', n']}$ , where  $n'$  has approximate order  $n' \sim n/|\vartheta|$ . As  $n$  was arbitrary and  $\frac{n}{|\vartheta|} \rightarrow \infty$ , it follows that arbitrarily large central subwords of  $y$  are determined by  $x$ . Hence,  $y$  is unique. As  $x$  was arbitrary,  $\vartheta$  is recognisable.  $\square$

The definition of local recognisability used here was a delicate notion to formalise, as the choice of images of letters under random substitutions means that one must be more careful than in the deterministic setting in order to capture the correct meaning (which is relatively simple as far as intuition is concerned), especially as one really wants the definition to be equivalent to global recognisability. Both the definition of local recognisability and the above proof were pieced together from those appearing in [10] in the context of deterministic substitutions and conversations with Philipp Gohlke, to whom we are extremely grateful.

## 6. AUTOMORPHISM GROUPS FOR CONSTANT LENGTH RANDOM SUBSTITUTIONS

Recognisability is used heavily in Section 4 in order to ensure that the automorphisms being constructed are well-defined. In general, we do not have recognisability and so shuffles and generalised shuffles are no longer well-defined. This includes important examples for which one is interested in studying the associated automorphism groups, such as the random Fibonacci [11, 21] and random period doubling substitutions [4]. The random period doubling substitution is especially of interest as the associated RS-subshift contains periodic points, unlike for RS-subshifts associated with recognisable substitutions. Rust and Spindeler showed that primitive random substitutions that contain a periodic point actually contain a dense set of periodic points [25], so by Proposition 2.6, the automorphism group of the random period doubling subshift is residually finite. The existence of periodic points in the RS-subshift therefore forces the automorphism group to be ‘smaller’ in this sense (compare Theorem 3.13). In general, we have the following.

**Corollary 6.1.** *Let  $\vartheta$  be a primitive random substitution. If  $X_\vartheta$  contains a single periodic element, then  $\text{Aut}(X_\vartheta)$  is residually finite.*

For a discussion of the existence/non-existence and enumeration of periodic points for compatible random substitutions, the reader is directed to the work of Rust [24].

In order to study properties such as subgroups for automorphism groups of RS-subshifts without recognisability, it is helpful to introduce other restrictions on our random substitutions. Our aim is to introduce conditions that are satisfied by the random period doubling substitution, so that consequent results apply to this example.

To motivate this direction, let us construct a non-trivial automorphism of the random period doubling substitution.

**Example 6.2.** Recall that the random period doubling substitution is given on the alphabet  $\mathcal{A} = \{a, b\}$  by  $\vartheta: a \mapsto \{ab, ba\}, b \mapsto \{aa\}$ . This is a primitive, compatible random substitution of constant length  $L = 2$  and which is not recognisable, but for

which the word  $bb$  is recognisable with radius of recognisability 0, admitting the unique inflation word decomposition  $([b, b], (aa))$  (see Example 6.6).

We can use the word  $bb$  as a marker between which local shuffles can be applied. For instance, the following is the list of all words of length 8 in the language  $\mathcal{L}_\vartheta$  that both begin and end with  $bb$ :

$$u_1 = bbaaaabb, \quad u_2 = bbaababb, \quad u_3 = bbabaabb$$

Because  $bb$  has a unique inflation word decomposition, it actually means that these three words  $u_i$ ,  $i = 1, 2, 3$  also have unique inflation word decompositions. Notice that  $u_2$  and  $u_3$  have the same root. That is  $u_2$  and  $u_3$  are uniquely decomposed as

$$u_2 = \underbrace{-b}_{a} \underbrace{ba}_{a} \underbrace{ab}_{a} \underbrace{ab}_{a} \underbrace{bb-}_{a}, \quad u_3 = \underbrace{-b}_{a} \underbrace{ba}_{a} \underbrace{ba}_{a} \underbrace{ab}_{a} \underbrace{bb-}_{a}.$$

We may therefore define an automorphism of  $X_\vartheta$  in the following way. The automorphism  $f: X_\vartheta \rightarrow X_\vartheta$  replaces any occurrence of the word  $u_2$  with the word  $u_3$  and vice versa. This is well-defined because if  $u_2$  and  $u_3$  were ever to overlap in an element of the subshift<sup>4</sup>, then the rule defining  $f$  can still act on both words, as the place where they overlap, the word  $bb$ , is fixed by the rule. In this sense,  $bb$  is a *marker*. As  $u_2$  and  $u_3$  have the same unique root,  $f$  is well-defined on  $X_\vartheta$ . By now, it is also clear that  $f$  really is an automorphism and is its own inverse. There are plenty of elements in the subshift for which  $u_2$  and  $u_3$  appear as subwords, and so it is clear that  $f$  is non-trivial. We hence see that  $f$  is a non-trivial involution in  $\text{Aut}(X_\vartheta)$ .

Notice that it was necessary to define our automorphism in such a way that a nearby word ( $bb$ ) was recognisable, in order to make the mapping well-defined. If we would try to define an automorphism that, for example, just replaced the word  $ab$  with  $ba$  and vice versa, this would not be well-defined on all  $x \in X_\vartheta$  due to the lack of recognisability for  $\vartheta$  (and several other reasons).

The longer we make our words  $u_i$  (which contain  $bb$  on the ends but not in between), the more choice we have for applying similar local shuffles, such as the automorphism that performs the cyclic replacement

$$\begin{array}{ccc} bbaabaaababb & \longrightarrow & bbabaaaababb \\ \uparrow & & \downarrow \\ bbaabaaababb & \longleftarrow & bbabaaaababb \end{array}$$

on words that share the unique root  $aaabaaa$ . One just has to ensure that no new occurrences of  $bb$  are being created between the two ‘border’  $bbs$ .

The above mentioned properties will form the basis for a general argument and so we now take the time to formalise them, in order to understand better how to apply them in a general setting.

---

<sup>4</sup>In fact, this cannot happen because  $a^9$  is not legal for  $\vartheta$ .

**6.1. Relaxing recognisability.** If there exists a recognisable word  $u \in \mathcal{L}_\vartheta$ , then we say that  $\vartheta$  *admits a recognisable word*. We say that the random substitution  $\vartheta$  *has disjoint images of letters* if, for all  $a, b \in \mathcal{A}$ ,  $\vartheta(a) \cap \vartheta(b) \neq \emptyset \implies a = b$ . We say that the random substitution  $\vartheta$  *has disjoint images* if, for all legal words  $u, v \in \mathcal{L}_\vartheta$ ,  $\vartheta(u) \cap \vartheta(v) \neq \emptyset \implies u = v$ . Although recognisability neither implies nor is implied by the disjoint images property, they are intuitively similar, as they both restrict how legal words may be ‘desubstituted’. On the other hand, the existence of a recognisable word is a direct relaxation of recognisability.

Recognisable words may always be extended to a minimal recognisable word that constitutes an exact inflation word. This is done by picking a long enough superword  $w \in \mathcal{L}_\vartheta$  of  $u$  that induces a unique inflation word decomposition  $([u_{(0)}, \dots, u_{(\ell)}], v) \in D_\vartheta(u)$  and extending  $u$  within  $w$  to  $u' = u'_{(0)}u_{(1)} \cdots u_{(\ell-1)}u'_{(\ell)} \in \vartheta(v)$ , which is also recognisable by construction. We may therefore always assume that a recognisable word is an exact inflation word when it is convenient to do so and that each of the decomposition words  $u_{(0)}, \dots, u_{(\ell)}$  for the recognisable word  $u$  are images of the random substitution on a single letter, so  $u \in \vartheta(v)$  for some  $v \in \mathcal{L}_\vartheta$ .

It has previously been shown that a constant length random substitution has disjoint images of letters if and only if it has disjoint images [24]. In particular, a constant length random substitution  $\vartheta$  has disjoint images of letters if and only if all of its powers  $\vartheta^p$  also have disjoint images of letters. In the case of non-constant length substitutions, disjoint images can be strictly stronger than disjoint images of letters, as demonstrated by the random Fibonacci substitution  $\vartheta: a \mapsto \{ab, ba\}, b \mapsto \{a\}$ , which has disjoint images of letters. Nevertheless, we see that  $\vartheta$  does not have disjoint images because  $\vartheta(ab) \cap \vartheta(ba) = \{aba\}$ .

The following result says that the existence of a recognisable word in an element  $x$  for a constant length random substitution enforces unique cutting points (boundaries of inflation words) in the whole of  $x$ . This result will be used later to ensure that an automorphism is well-defined. Notice that  $y$  is not necessarily unique in the following result.

**Lemma 6.3.** *Let  $\vartheta$  be a substitution of constant length  $L$  which admits one recognisable word  $u$ . If  $x \in X_\vartheta$  contains at least one appearance of the word  $u$  as a subword, then there exists a unique  $0 \leq i \leq L - 1$  such that  $\sigma^{-i}(x) \in \vartheta(y)$  for some  $y \in X_\vartheta$ .*

*Proof.* Without loss of generality, assume that  $u \in \vartheta(\hat{v})$  for some  $\hat{v} \in \mathcal{L}_\vartheta$ . Suppose that the radius of recognisability for  $u$  is  $N$ . Let  $i \leq j$  be such that  $x_{[i,j]} = u$ . Suppose that the unique inflation word decomposition of  $u$  induced by any inflation word decomposition of  $x_{[i-N,j+N]}$  is given by  $([u_{(0)}, \dots, u_{(\ell)}], v)$ . By shifting  $x$ , we may assume without loss of generality that  $x_{[0,|u|-1]} = u$ .

We know that  $x$  has at least one preimage  $y$  under the substitution. As  $\vartheta$  is constant length, say with length  $L$ , and the subword  $x_{[0,|u|-1]}$  has a unique decomposition into inflation words which is compatible with an inflation word decomposition of the whole of  $x$ , it means that  $x \in \vartheta(y)$ , with no allowed shifting of  $x$ . Or more succinctly,  $i = 0$ , and so is unique.  $\square$

If we further assume that  $\vartheta$  has disjoint images of letters, then not only is  $i$  unique, but so is the preimage  $y$ . So not only do we enforce the cutting point structure in  $x$ , but also the types of the inflation words.

**Proposition 6.4.** *Let  $\vartheta$  be a substitution of constant length  $L$  with disjoint images of letters and which admits one recognisable word  $u$ . If  $x \in X_\vartheta$  contains at least one appearance of the word  $u$  as a subword, then there exists a unique  $y \in X_\vartheta$  and  $0 \leq i \leq L - 1$  such that  $\sigma^{-i}(x) \in \vartheta(y)$ .*

*Proof.* That  $i$  is unique follows from Lemma 6.3, and so without loss of generality, assume that  $i = 0$ . In particular, every subword of  $x$  of the form  $x_{[iL, (i+1)L-1]}$  is an exact inflation of a single letter. That is,  $x_{[iL, (i+1)L-1]} \in \vartheta(y_i)$ , where  $y$  is some preimage of  $x$  under  $\vartheta$ . But, as  $\vartheta$  has disjoint images of letters, we can conclude that the word  $x_{[iL, (i+1)L-1]}$  uniquely determines the letter  $y_i$ . It follows that  $y$  is uniquely determined by  $x$ , and so both the element  $y$  and the integer  $i$  are unique.  $\square$

Hence, for constant length substitutions with disjoint images of letters, a suitable abundance of recognisable words actually gives full recognisability.

**Corollary 6.5.** *Let  $\vartheta$  be a substitution of constant length with disjoint images of letters and suppose that every element in the RS-subshift  $X_\vartheta$  contains at least one recognisable subword. Then  $\vartheta$  is recognisable.*

**Example 6.6.** Let  $\vartheta: a \mapsto \{ab, ba\}, b \mapsto \{aa\}$  be the random period doubling substitution. It is a constant length random substitution with length  $L = 2$ . The word  $aa$  is not recognisable for  $\vartheta$  but showing this is not so simple. Note that  $aa$  has five inflation word decompositions

$$\begin{aligned} D_\vartheta(aa) = & \{([aa], b), ([a, a], bb), \\ & ([a, a], ba), ([a, a], ab), ([a, a], aa)\} \end{aligned}$$

and for any  $n \geq 0$ , the word  $u_n = (aabaab)^n aa(baabaa)^n$  is legal for  $\vartheta$ . We then notice that  $u_n$  admits the inflation word decompositions

$$([\overbrace{aa, ba, ab, aa}^{\times 2n}, (baa)^{2n}b] \quad \text{and} \quad ([a, \overbrace{ab, aa, ba, a}^{\times 2n}], a(aba)^{2n}a),$$

which induce different inflation word decompositions on the central word  $aa$  (even different  $\vartheta$ -cuttings). In particular, they induce the inflation word decompositions  $([aa], b)$  and  $([a, a], aa)$  respectively. Hence, no radius of recognisability exists for  $aa$ .

On the other hand, the word  $bb$  is recognisable, as the only inflation word decomposition for  $bb$  (regardless of how it is induced) is

$$D_\vartheta(bb) = \{([b, b], aa)\}.$$

Although  $\vartheta$  admits a recognisable word  $bb$  (and in fact infinitely many recognisable words), it is not true that  $\vartheta$  is recognisable, as  $bb$  does not appear as a subword of every element in  $X_\vartheta$ , as demonstrated by the element  $(aab)^\infty \in X_\vartheta$ . In fact, by Corollary 6.5, not every element of  $X_\vartheta$  can contain a recognisable word as a subword, since the existence of a periodic element in the subshift rules out full recognisability by results from [24].

We will need to also control the existence of recognisable words for powers of substitutions.

**Lemma 6.7.** *Let  $\vartheta$  be a primitive, constant length random substitution with disjoint images of letters and let  $p \geq 1$  be an integer. The random substitution  $\vartheta$  admits a recognisable word if and only if  $\vartheta^p$  admits a recognisable word.*

*Proof.* ( $\implies$ ) Write  $L$  for the length of the substitution, so for all  $a \in \mathcal{A}$ ,  $|\vartheta(a)| = L$ . Let  $u$  be a recognisable word for  $\vartheta$  with radius of recognisability  $N$  and let  $\hat{u} = u^{(l)}uu^{(r)}$  be a legal extension of  $u$  with  $|u^{(l)}| = |u^{(r)}| = L$ . Suppose that all inflation word decompositions of  $\hat{u}$  induce the unique inflation word decomposition  $([u_{(0)}, \dots, u_{(\ell)}], v)$  on  $u$  and without loss of generality assume that  $u \in \vartheta(v)$ . By primitivity, there exists a legal word  $w \in \mathcal{L}_\vartheta$  that contains both  $\hat{u}$  and  $v$ . Consider now a word  $w' \in \vartheta(w)$  which is given by realising the subword  $\vartheta(v)$  to be  $u$ . As  $u \triangleleft w'$ ,  $u$  is recognisable for  $\vartheta$  and  $\vartheta$  is constant length, this forces the possible  $\vartheta$ -cuttings of  $w'$  to be fixed as soon as we know an  $N$ -neighbourhood of  $w'$ . Disjoint images of letters means that in fact  $w'$  can then only have a single inflation word decomposition induced by any inflation word decomposition of an  $N$ -neighbourhood. Hence,  $w'$  is recognisable for  $\vartheta$  with radius of recognisability  $N$ . Now, as  $w$  contains  $\hat{u}$  and  $\vartheta$  is constant length, that means that  $\hat{u}$  forces the possible sequence of cuts for  $w$  into level-1 inflation words to also be fixed. Hence, by disjoint images of letters and the fact that  $w'$  has a unique decomposition into level-1 inflation words given an  $N$ -neighbourhood, the level-2 inflation word decomposition of  $w'$  is also unique given an  $LN$ -neighbourhood. That is,  $w'$  is recognisable for  $\vartheta^2$  with radius of recognisability  $LN$ .

To extend the argument to all  $p \geq 1$ , let  $w_{(2)} := w$  and  $w'_{(2)} := w'$ , then define  $w_{(p)}$  to be a legal word containing  $v, \hat{u}, w'_{(2)}, \dots, w'_{(p-1)}$ . Then  $w'_{(p)}$  is chosen to be an appropriate realisation of  $\vartheta(w_{(p)})$ . The analogous argument to the above then shows that  $w'_{(p)}$  is recognisable for  $\vartheta^p$  with radius of recognisability  $L^{p-1}N$ .

( $\impliedby$ ) To prove the right-to-left implication, suppose that  $u$  is an  $N$ -recognisable word for  $\vartheta^p$  and let  $w = u_luu_r$  be a legal superword of  $u$  with  $|u_l| = |u_r| = N$ . Suppose that any inflation word decomposition of  $w$  for  $\vartheta^p$  induces the inflation word decomposition  $([u_{(0)}, \dots, u_{(\ell)}], v)$  on  $u$ . Without loss of generality, assume that  $u \in \vartheta^p(v)$ . Then,  $u \in \vartheta(\vartheta^{p-1}(v))$ . As  $u$  has a unique decomposition into level- $p$  inflation words induced by  $w$  and  $\vartheta$  has disjoint images of letters (and hence disjoint images by the fact that  $\vartheta$  is constant length), there is only one word  $v' \in \vartheta^{p-1}(v)$  such that  $u \in \vartheta(v')$ . It follows that  $w$  induces a unique inflation word decomposition of  $u$  for  $\vartheta$  given by

$$([\vartheta(v'_0), \dots, \vartheta(v'_{|v'| - 1})], v')$$

for appropriate unique choices of  $\vartheta(v'_i)$ .  $\square$

Note that for a constant length substitution with disjoint images of letters, if  $u$  is a recognisable word, and we consider a word  $\hat{u}$  for which  $u$  is a subword, then for some  $N$ -neighbourhood  $\hat{u}_{(N)}$  of  $\hat{u}$ , any inflation word decomposition  $d \in D_\vartheta(\hat{u}_{(N)})$  will induce the same inflation word decomposition on  $u$ . In particular, this means that all  $\vartheta$ -cuttings of both  $\hat{u}$  and  $\hat{u}_{(N)}$  must be the same due to  $\vartheta$  being constant length. Then, by the disjoint images property, this implies remarkably that  $\hat{u}$  and even  $\hat{u}_{(N)}$  have unique inflation word

decompositions. More precisely, we have shown that if  $u$  is recognisable with radius of recognisability  $N$ , then all superwords of  $u$  are also recognisable with radius of recognisability  $N$ , and all sufficiently long superwords (say  $w = u^{(l)}uu^{(r)}$  with  $|u^{(l)}|, |u^{(r)}| \geq N$ ) are recognisable with radius of recognisability 0.

**Lemma 6.8.** *Let  $\vartheta$  be a constant length random substitution with disjoint images of letters. Let  $u \in \mathcal{L}_\vartheta$  be a subword of  $w = u^{(l)}uu^{(r)} \in \mathcal{L}_\vartheta$ . If  $u$  is  $N$ -recognisable, then  $w$  is  $N$ -recognisable. Further, if  $|u^{(l)}|, |u^{(r)}| \geq N$ , then  $w$  is 0-recognisable.  $\square$*

This will be used for the main results in this section.

The following technical Lemma will also be needed, allowing us to use a general marker-based method for building automorphisms.

**Lemma 6.9.** *Let  $\vartheta$  be a non-degenerate, constant length, primitive, compatible random substitution with disjoint images of letters. If  $\vartheta$  admits a recognisable word, then for some power  $p \geq 1$ ,  $\vartheta^p$  admits a recognisable word  $u$  such that there is an increasing sequence of lengths  $(n_k)_{k \geq 1}$  whereby the sets*

$$V_k := \{v \mid |v| = n_k, |uvu|_u = 2, uvu \in \mathcal{L}_\vartheta\}$$

*contain at least  $k$  words that share a common unique root.*

*Proof.* Let  $u$  be a recognisable word. Let  $p$  be large enough so that  $\#\vartheta^p(a) \geq 2$  for all  $a \in \mathcal{A}$  and such that  $u \blacktriangleleft \vartheta^p(a)$  for some  $a \in \mathcal{A}$ . Let  $a \in \mathcal{A}$  be a fixed letter of the alphabet and choose  $u_1(a), u_2(a) \in \vartheta^p(a)$  such that  $u \triangleleft u_1(a)$ . For every other letter  $b \in \mathcal{A} \setminus \{a\}$ , choose a single word  $u(b)$ . Now define a new random substitution  $\vartheta' : \mathcal{A} \rightarrow \mathcal{S}$  by  $\vartheta'(a) = \{u_1(a), u_2(a)\}$  and  $\vartheta'(b) = \{u(b)\}$  for all  $b \neq a$ . By construction,  $X_{\vartheta'}$  is a non-empty, closed, invariant subspace of  $X_\vartheta$ . In order to see that  $X_{\vartheta'}$  is a proper subset of  $X_\vartheta$ , note that Gohlke [12] showed that the topological entropy  $h$  of a compatible random substitution with the ‘disjoint set condition’ is given by a formula just in terms of the associated substitution matrix  $M_\vartheta$  and the vector  $\mathbf{q} := (\#\vartheta(a_i))_{a_i \in \mathcal{A}}$  which is monotonically increasing in the entries of  $\mathbf{q}$ . In particular, a constant length random substitution with disjoint images of letters satisfies the disjoint set condition, and so it can easily be shown from Gohlke’s formula that  $h(X_{\vartheta'}) < h(X_\vartheta)$  and so  $X_{\vartheta'} \subsetneq X_\vartheta$ .

We may now, without loss of generality, assume that  $p = 1$ . Let  $v \in \mathcal{L}_\vartheta$  be some legal word which does not appear in the language of  $\vartheta'$ . It was shown by Rust and Spindeler [25] that  $X_\vartheta$  contains a point  $x$  with a dense orbit. Both the recognisable word  $u$  and the word  $v$  appear as subwords of  $x$  and so there exists some legal word  $\hat{u}$  which contains both  $u$  and  $v$  as subwords. In particular,  $\hat{u}$  is both recognisable by Lemma 6.8 and does not appear in the language of  $\vartheta'$ . For a given  $k$ , let  $w_k \in \mathcal{L}_{\vartheta'}$  be a word sufficiently longer than the word  $\hat{u}$  and containing many more than  $k$  appearances of the inflation word  $u_1(a)$ . By the denseness of the orbit of  $x$ , there exists a  $\vartheta$ -legal word of the form  $y_k = \hat{u} \square w_k \square \hat{u}$  such that  $|y_k|_{\hat{u}} = 2$ . Let  $n_k := |y_k| - 2|\hat{u}|$ .

As  $w_k$  has many more than  $k$  appearances of the inflation word  $u_1(a)$ , there are at least  $2^k$  possible inflation word replacements which can be performed on  $w_k$ , replacing a subset of the  $u_1(a)$ s with  $u_2(a)$ s, to produce a new word  $w'_k$ . As these replacements are also

legal replacements for  $\vartheta$ , the same replacements in  $y_k$  will still produce an element  $y'_k$  of  $\mathcal{L}_\vartheta$ . Further, because  $w_k$  is sufficiently long, such a set of inflation word replacements can be performed at least a distance  $|\hat{u}|$  away from the boundaries between the subword  $w_k$  and the unknown blocks  $\square$  in  $y_k$ . As such, sufficiently many replacements can be performed with no new appearances of  $\hat{u}$  being introduced into the new words  $y'_k$  because the modified subword  $w'_k$  is  $\vartheta'$ -legal. It follows that  $|y'_k|_{\hat{u}} = 2$  for sufficiently many new words  $y'_k$  that are obtained from  $y_k$  by an inflation word replacement of this kind. Also, for each of these words  $y'_k$ ,  $|y'_k| - 2|\hat{u}| = n_k$  by compatibility of  $\vartheta$ , as required.  $\square$

In order to make up for the fact that we do not have full recognisability of the random substitution, we will use the word  $u$  constructed in Lemma 6.9 as a ‘marker’ between which we are allowed to apply inflation word replacements. Further, as we can control the distances between these gaps, thanks to the fact that the words in the sets  $V_k$  all have the same length  $n_k$ , it means that such inflation word replacements are applied at mutually distinct locations in an element  $x \in X_\vartheta$ , and so commute with one another. This allows us to mimic the classic marker-based argument introduced by Hedlund [17] and generalised by Boyle–Lind–Rudolph [5] in order to embed an arbitrary countable direct sum of finite groups into the automorphism group  $\text{Aut}(X_\vartheta)$  when the random substitution is not necessarily recognisable but is constant length, has disjoint images and admits a recognisable word (as the random period doubling substitution does).

**Theorem 6.10.** *Let  $\vartheta$  be a non-degenerate, constant length, primitive, compatible random substitution with disjoint images of letters and which admits at least one recognisable word  $u$ . Let  $G$  be a countable direct sum of finite groups. The group  $G$  embeds into the automorphism group  $\text{Aut}(X_\vartheta)$ .*

*Proof.* Let  $p \geq 1$  and  $u \in \mathcal{L}_\vartheta$  be such that  $u$  is recognisable with respect to  $\vartheta^p$  and there is an increasing sequence of lengths  $(n_k)_{k \geq 1}$  whereby the sets

$$V_k := \{v \mid |v| = n_k, |uvu|_u = 2, uvu \in \mathcal{L}_\vartheta\}$$

contain at least  $k$  words that share a common unique root, as guaranteed to exist by Lemma 6.9. Let  $k \geq 1$  be given. Our goal is to show that the symmetric group  $S_k$  embeds into  $\text{Aut}(X_\vartheta)$ .

Let  $v_1, \dots, v_k$  be  $k$  elements in the set  $V_k$ . For a permutation  $\pi \in S_k$ , we define an automorphism  $f_\pi: X_\vartheta \rightarrow X_\vartheta$  by mapping an element  $x \in X_\vartheta$  to an inflation word replacement  $f_\pi(x)$  given by replacing any occurrence of  $uv_iu$  in  $x$  with the word  $uv_{\pi(i)}u$ . The map  $f_\pi$  is well-defined, as the recognisable word  $u$  only appears as a subword of  $uv_ku$  as a prefix and suffix, and nowhere else. Hence, no two words  $uv_ku$  and  $uv_\ell u$  can overlap in  $x$  except as a prefix-suffix pair. As  $u$  remains unchanged under the map, there is no ambiguity in where inflation words are being replaced. As  $f_\pi$  is defined locally, it is continuous, and shift-invariant. It is clear that  $f_\pi \circ f_{\pi^{-1}} = f_{\pi^{-1}} \circ f_\pi = \text{Id}_{X_\vartheta}$  and so  $f_\pi$  is an automorphism. Likewise, the map  $S_k \rightarrow \text{Aut}(X_\vartheta): \pi \mapsto f_\pi$  is a homomorphism, and as  $v_k = v_{\pi(k)}$  for all  $k$  if and only if  $\pi = e$ , this mapping is also an embedding.

Write  $H_k = \{f_\pi \mid \pi \in S_k\}$ . We note, by construction, that if  $k \neq \ell$ , then  $n_k \neq n_\ell$  and so if  $f_\pi \in H_k$  and  $f_\rho \in H_\ell$ , then  $[f_\pi, f_\rho] = \text{Id}_{X_\vartheta}$ . That is, if  $k \neq \ell$ , then automorphisms in

$H_k$  commute with automorphisms in  $H_\ell$ . So  $\bigoplus_{k=1}^\infty H_k$  is a subgroup of  $\text{Aut}(X_\vartheta)$ . Hence, by Cayley's theorem,  $G$  embeds into  $\text{Aut}(X_\vartheta)$  because  $\bigoplus_{k=1}^\infty H_k$  does.  $\square$

A similar marker-based technique, again in the style of Hedlund and Boyle–Lind–Rudolph, can be used to show that the free product  $(\mathbb{Z}/2\mathbb{Z})^{*k}$  of  $k$  involutions also embeds into  $\text{Aut}(X_\vartheta)$ , and hence any free group  $F_k$  on  $k \geq 1$  generators, and the free group  $F_\omega$  on countably many generators. We omit this proof, as the method is now well-established.

**Theorem 6.11.** *Let  $\vartheta$  be a constant length, primitive, compatible random substitution which admits at least one recognisable word  $u$ . Let  $k \geq 1$  and let  $G = (\mathbb{Z}/2\mathbb{Z})^{*k}$ . The group  $G$  embeds into the automorphism group  $\text{Aut}(X_\vartheta)$ .*

In fact, the marker method can be generalised to show that the automorphism group  $\text{Aut}(X_n)$  of any full shift embeds into  $\text{Aut}(X_\vartheta)$  when the conditions on  $\vartheta$  in Theorem 6.10 are satisfied. Theorems 6.10 and 6.11 are then simple corollaries of this stronger embedding result.

The idea is that for  $v_0, v_1 \in V_2$ , we use  $uv_iu$  as a marker to code elements of the full 2-shift over the symbols  $\{0, 1\}$ . As the words  $uv_iu$  appear with uniformly bounded gaps in some element  $x \in X_\vartheta$ , then an automorphism on the 2-shift induces a local map on the coding words  $v_i$ .

The tricky thing is what one then does for elements that do not have the words  $uv_iu$  appearing with uniformly bounded gaps. What does one do when reaching the ‘end’ of a run of  $uv_ius$  that is followed by a large gap before the next occurrence (if any)? To get around this difficulty, we use a slightly more involved encoding of a full shift which carries two bits of information, rather than one. The induced action of an automorphism on a full shift then acts on the ‘top’ bit of information as usual, but on the ‘bottom’ bit of information in reverse. At the end of a run, you then ‘wrap’ this action around. This idea is sometimes referred to as the *conveyor belt* method [28].

**Theorem 6.12.** *Let  $\vartheta$  be a constant length, primitive, compatible random substitution that admits at least one recognisable word  $u$ . Then  $\text{Aut}(X_\vartheta)$  contains the automorphism group  $\text{Aut}(X_2)$  of the full 2-shift  $X_2$ .*

*Proof.* By Lemma 6.9, and replacing  $\vartheta$  with a power if necessary, there exists a word  $u \in \mathcal{L}_\vartheta$  such that  $u$  is recognisable with respect to  $\vartheta$  and there is a length  $n_4$  whereby the set

$$V_4 = \{v \mid |v| = n_4, |uvu|_u = 2, uvu \in \mathcal{L}_\vartheta\}$$

contains at least 4 words that share a common unique root. Label four of these words  $v_0^0, v_1^0, v_0^1, v_1^1$ . In this coding, we think of the superscript as referring to the ‘top track’, and the subscript as being the ‘bottom track’ of a conveyor belt.

As  $X_\vartheta$  has uniformly bounded gaps between letters, let  $\hat{N} \geq 1$  be such that every legal word in  $\mathcal{L}_\vartheta$  contains at least two copies of the letter  $a$ . Let  $p \geq 1$  be such that  $uv_i^j u \blacktriangleleft \vartheta^p(a)$  for all  $(i, j) \in \{0, 1\}^2$ . Let  $N = L^p \hat{N}$ . Then, by taking all realisations of  $\vartheta^p(a)$  to contain  $uv_0^0 u$ , there exists an element  $x_\infty \in X_\vartheta$  such that every subword  $w \triangleleft x_\infty$  of length at least  $|w| \geq N$  contains two copies of  $uv_0^0 u$ .

For  $x \in X_\vartheta$ , write

$$x = \cdots \blacksquare uv_{i(n)}^{j(-n)} u \square \cdots \square uv_{i(1)}^{j(-1)} u \square uv_{i(0)}^{j(0)} u \square uv_{i(-1)}^{j(1)} u \square \cdots \square uv_{i(-m)}^{j(m)} u \blacksquare \cdots,$$

where  $\square$  represents a word such that  $u\square u$  contains no appearances of a word  $uv_i^j u$  with  $(i, j) \in \{0, 1\}^2$  with length  $|\square| \leq N$ , and  $\blacksquare$  represents a word such that  $u\blacksquare u$  contains no appearance of a word  $uv_i^j u$  with  $(i, j) \in \{0, 1\}^2$  with length  $|\blacksquare| > N$ . Note that  $\blacksquare$  can possibly be a left(right)-infinite word. Notice that the indices  $i$  of the bottom track are reversed. For ease of notation, we will suppress the markers  $u$  in this representation, being absorbed into a neighbouring  $\square$  or  $\blacksquare$ , and so write

$$x = \cdots \blacksquare v_{i(n)}^{j(-n)} \square \cdots \square v_{i(1)}^{j(-1)} \square v_{i(0)}^{j(0)} \square v_{i(-1)}^{j(1)} \square \cdots \square v_{i(-m)}^{j(m)} \blacksquare \cdots.$$

Let  $X_2$  be the full 2-shift. Let  $\alpha$  be an automorphism of the full 2-shift  $X_2$ . We define an automorphism  $f_\alpha: X_\vartheta \rightarrow X_\vartheta$  on  $x$  in the following way.

If  $x$  contains no  $\blacksquare$ , then

$$f_\alpha(x) := \cdots \square v_{\alpha(i)(2)}^{\alpha(j)(-2)} \square v_{\alpha(i)(1)}^{\alpha(j)(-1)} \square v_{\alpha(i)(0)}^{\alpha(j)(0)} \square v_{\alpha(i)(-1)}^{\alpha(j)(1)} \square v_{\alpha(i)(-2)}^{\alpha(j)(2)} \square \cdots,$$

where  $i$  and  $j$  are considered as elements of the full 2-shift  $X_2$ . So we have applied  $\alpha$  to the top indices of the  $v_i^j$  and also to the bottom indices of  $v_i^j$  but where the sequence  $i$  is in reverse.

If  $x$  contains a  $\blacksquare$ , then near this position, write

$$x = \cdots v_{i(2)}^{i(-3)} \square v_{i(1)}^{i(-2)} \square v_{i(0)}^{i(-1)} \blacksquare v_{j(-1)}^{j(0)} \square v_{j(-2)}^{j(1)} \square v_{j(-3)}^{j(2)} \square \cdots,$$

where  $i$  and  $j$  are considered as elements of the full 2-shift that have been ‘wrapped over’ when they get near a  $\blacksquare$ . Then we define

$$f_\alpha(x) := \cdots v_{\alpha(i)(2)}^{\alpha(i)(-3)} \square v_{\alpha(i)(1)}^{\alpha(i)(-2)} \square v_{\alpha(i)(0)}^{\alpha(i)(-1)} \blacksquare v_{\alpha(j)(-1)}^{\alpha(j)(0)} \square v_{\alpha(j)(-2)}^{\alpha(j)(1)} \square v_{\alpha(j)(-3)}^{\alpha(j)(2)} \square \cdots.$$

Between two appearances of  $\blacksquare$ , the indices of the  $v_i^j$  act like the coding of a periodic element of  $X_2$  wrapped around in a circle.

As everything is locally defined,  $f_\alpha$  is well-defined, continuous and commutes with the shift action. It is also clear that  $f_{\alpha^{-1}} = f_\alpha^{-1}$  and  $f_{\alpha \circ \beta} = f_\alpha \circ f_\beta$ , and so  $f_\alpha$  is an automorphism. It remains to check that the map  $\alpha \mapsto f_\alpha$  is faithful.

Let  $\alpha$  be non-trivial. So there exists an element  $j \in X_2$  such that  $\alpha(j) \neq j$ . Take an element  $x \in X_\vartheta$  with no appearances of a  $\blacksquare$  with the form

$$x = \cdots \square v_{\alpha(j)(2)}^{\alpha(j)(-2)} \square v_{\alpha(j)(1)}^{\alpha(j)(-1)} \square v_{\alpha(j)(0)}^{\alpha(j)(0)} \square v_{\alpha(j)(-1)}^{\alpha(j)(1)} \square v_{\alpha(j)(-2)}^{\alpha(j)(2)} \square \cdots,$$

which exists because the element  $x_\infty$  constructed above exists (just replace the appearances of  $v_0^0$  with a corresponding  $v_{-n}^n$ ). By construction,  $f_\alpha(x) \neq x$  and so  $f_\alpha$  is non-trivial. Hence the map  $\alpha \mapsto f_\alpha$  is faithful and so  $\text{Aut}(X_2)$  embeds in  $\text{Aut}(X_\vartheta)$ .  $\square$

**Corollary 6.13.** *Let  $\vartheta: a \mapsto \{ab, ba\}, b \mapsto \{aa\}$  be the random period doubling substitution and let  $X_\vartheta$  be its RS-subshift. The automorphism group  $\text{Aut}(X_\vartheta)$  contains the automorphism group  $\text{Aut}(X_2)$  of the full 2-shift  $X_2$ .*  $\square$

**6.2. Open Questions.** We have only provided here a first investigation of these intricate automorphism groups and their interplay with the particular properties of the defining random substitution. There is still much to be understood about the subgroup structure and other open questions.

While the random period doubling substitution admits periodic elements in its subshift, not all of the random substitutions satisfying the conditions of Theorem 6.12 have periodic points. Therefore, it is an open question as to whether these RS-subshifts have residually finite automorphism groups when they are aperiodic and non-recognisable.

For example, consider the random substitution  $\vartheta: a \mapsto \{abaa, aaba\}, b \mapsto \{abab, baba\}$ . It is constant length, primitive, compatible and admits the recognisable word  $aaaa$ . It is not recognisable because the two marginal substitutions  $\theta_1: a \mapsto abaa, b \mapsto abab$  and  $\theta_2: a \mapsto aaba, b \mapsto baba$  are conjugate ( $(aba)^{-1}\theta_1(aba) = \theta_2$ ), and therefore their bi-infinite fixed points are the same up to a shift, hence admit two preimages. Nevertheless,  $X_\vartheta$  is aperiodic, which can be seen by verifying the criterion given in [24, Corollary 36], as every element of  $X_\vartheta$  must contain at least one of  $aaab, baaa, abba$  or  $baab$  as a subword. We therefore do not currently know if  $\text{Aut}(X_\vartheta)$  is residually finite or not. Most likely the existence of a recognisable word is still enough for the automorphism group to contain an infinite simple subgroup. So, as well as the above, we ask the following more general question.

**Question 6.14.** Does there exist a primitive, compatible, non-recognisable random substitution  $\vartheta$  whose subshift is aperiodic but whose automorphism group **(i)** is residually finite, **(ii)** does not contain an infinite simple subgroup?

An example satisfying Question 6.14 would be interesting, as we do not yet have any examples of random substitutions whose subshifts can be differentiated up to topological conjugacy by comparing their automorphism groups, other than by using much simpler invariants such as the existence of periodic points. Perhaps, when  $\vartheta$  is recognisable, the shuffle group  $\Gamma$  is a good candidate for differentiating pairs of examples, as we have a much better understanding of the structure of  $\Gamma$ .

**Question 6.15.** Is  $\Gamma$  (or a characteristic property of  $\Gamma$  such as some notion of asymptotic growth rate) an invariant of topological conjugacy for  $X_\vartheta$ ? Is the growth rate of  $\Gamma$  related to the topological entropy  $h_{\text{top}}(X_\vartheta)$ ?

This gives rise to the more philosophical question:

**Question 6.16.** How good is  $\text{Aut}(X_\vartheta)$  at classifying RS-subshifts?

As far as more general properties of the automorphism group are concerned, natural questions that we have not yet explored include whether  $\text{Aut}(X_\vartheta)$  is finitely generated, whether Ryan's Theorem holds for  $\text{Aut}(X_\vartheta)$ , and whether the shift can admit finite roots.

**Question 6.17.** Under what conditions is  $\text{Aut}(X_\vartheta)$  finitely generated.

**Question 6.18.** Is the center  $Z(\text{Aut}(X_\vartheta))$  always generated by the shift  $\sigma$ ?

**Question 6.19.** In  $\text{Aut}(X_\vartheta)$ , can the shift map  $\sigma$  have a finite root? That is, does there exist  $f \in \text{Aut}(X_\vartheta)$  and  $n \geq 2$  such that  $f^n = \sigma$ ?

#### ACKNOWLEDGEMENT

The authors would like to thank Raf Bocklandt, Philipp Gohlke, Neil Mañibo, Eden Miro, Samuel Petite and Scott Schmieding for helpful discussions. We are especially thankful to Scott Schmieding for alerting us to other examples of subshifts with automorphism groups containing an infinite simple subgroup. Dan Rust would like to acknowledge the support of the DFG via SFB1283/1 and the support of the Dutch Science Federation (NWO) through visitor grant 040.11.700.

#### REFERENCES

- [1] R. C. Alperin, Free products as automorphisms of a shift of finite type, *unpublished note* (1988).
- [2] M. Baake and U. Grimm, *Aperiodic Order. Volume 1: A Mathematical Invitation*, Vol. 149 of *Encyclopedia Math. Appl.*, Cambridge Univ. Press, 2013.
- [3] M. Baake, J. A. G. Roberts, and R. Yassawi, Reversing and extended symmetries of shift spaces, *Discrete Contin. Dyn. Syst.* **38**(2) (2018), 835–866.
- [4] M. Baake, T. Spindeler, and N. Strungaru, Diffraction of compatible random substitutions in one dimension, *Indag. Math. (N.S.)* **29**(4) (2018), 1031–1071.
- [5] M. Boyle, D. Lind, and D. Rudolph, The automorphism group of a shift of finite type, *Trans. Amer. Math. Soc.* **306**(1) (1988), 71–114.
- [6] Van Cyr and Bryna Kra, The automorphism group of a shift of linear growth: beyond transitivity, *Forum Math. Sigma* **3** (2015), e5, 27.
- [7] Van Cyr and Bryna Kra, The automorphism group of a shift of subquadratic growth, *Proc. Amer. Math. Soc.* **144**(2) (2016), 613–621.
- [8] Sebastián Donoso, Fabien Durand, Alejandro Maass, and Samuel Petite, On automorphism groups of low complexity subshifts, *Ergodic Theory Dynam. Systems* **36**(1) (2016), 64–95.
- [9] G. B. Escolano, E. D. P. Miro, and N. Mañibo, Mixing properties and entropy bounds of a family of pisot random substitutions, *preprint*, [arxiv:2103.04866](https://arxiv.org/abs/2103.04866) (2021).
- [10] N. P. Fogg, *Substitutions in Dynamics, Arithmetics and Combinatorics*, Vol. 1794 of *Lecture Notes in Math.*, Springer-Verlag, 2002.
- [11] C. Godrèche and J. M. Luck, Quasiperiodicity and randomness in tilings of the plane, *J. Statist. Phys.* **55** (1989), 1–28.
- [12] P. Gohlke, Inflation word entropy for semi-compatible random substitutions, *Monatsh. Math.* **192**(1) (2020), 93–110.
- [13] P. Gohlke, A. Mitchell, D. Rust, and T. Samuel, Measure theoretic entropy of random substitution subshifts, *preprint*, [arxiv:2105.11224](https://arxiv.org/abs/2105.11224) (2021).
- [14] P. Gohlke, D. Rust, and T. Spindeler, Shifts of finite type and random substitutions, *Discrete Contin. Dyn. Syst.* **39** (2019), 5085–5103.
- [15] P. Gohlke and T. Spindeler, Ergodic frequency measures for random substitutions, *Studia Math.* **255**(3) (2020), 265–301.
- [16] M. Hall, *The theory of groups*, Chelsea Publishing Co., New York, 1976.
- [17] G. A. Hedlund, Endomorphisms and automorphisms of the shift dynamical system, *Math. Systems Theory* **3** (1969), 320–375.
- [18] K. H. Kim and F. W. Roush, On the automorphism groups of subshifts, *Pure Mathematics and Applications* **1**(4) (1990), 203–230.
- [19] N. V. Kroshko and V. I. Sushchansky, Direct limits of symmetric and alternating groups with strictly diagonal embeddings, *Arch. Math. (Basel)* **71**(3) (1998), 173–182.
- [20] E. D. P. Miro, D. Rust, L. Sadun, and G. Tadeo, Random substitution subshifts and topological mixing, *Israel Journal of Mathematics* (2022), in print.

- [21] J. Nilsson, On the entropy of a family of random substitutions, *Monatsh. Math.* **168**(3-4) (2012), 563–577.
- [22] J. Nilsson, On the entropy of a two step random Fibonacci substitution, *Entropy* **15** (2013), 3312–3324.
- [23] R. Pavlov and S. Schmieding, Local finiteness and automorphism groups of low complexity subshifts, *preprint*, [arxiv:2107.06062](https://arxiv.org/abs/2107.06062) (2021).
- [24] D. Rust, Periodic points in random substitution subshifts, *Monatsh. Math.* **193**(3) (2020), 683–704.
- [25] D. Rust and T. Spindeler, Dynamical systems arising from random substitutions, *Indag. Math. (N.S.)* **29**(4) (2018), 1131–1155.
- [26] V. Salo, A note on subgroups of automorphism groups of full shifts, *Ergodic Theory Dynam. Systems* **38**(4) (2018), 1588–1600.
- [27] V. Salo, Graph and wreath products of cellular automata, *preprint*, [arxiv:2012.10186](https://arxiv.org/abs/2012.10186) (2020).
- [28] V. Salo, Conjugacy of reversible cellular automata, *preprint*, [arxiv:2011.07827](https://arxiv.org/abs/2011.07827) (2021).
- [29] V. Salo and M. Schraudner, Automorphism groups of subshifts via group extensions. *preprint*.

INSTITUTE OF APPLIED MATHEMATICS, DELFT UNIVERSITY OF TECHNOLOGY,  
MOURIKBROEKMANWEG 6, 2628 XE, DELFT, THE NETHERLANDS

*Email address:* r.j.fokkink@tudelft.nl

SCHOOL OF MATHEMATICS AND STATISTICS, THE OPEN UNIVERSITY,  
WALTON HALL, MILTON KEYNES, MK7 6AA, UK

*Email address:* dan.rust@open.ac.uk

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF TURKU,  
FI-20014 TURKU, FINLAND

*Email address:* vosalo@utu.fi