

# Automorphisms of shift spaces and the Higman–Thompson groups: the one-sided case

Collin Bleak      Peter J. Cameron      Feyisayo Olukoya\*

Received 8 May 2020; Published 20 September 2021

**Abstract:** Let  $1 \leq r < n$  be integers. We give a proof that the group  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  of automorphisms of the one-sided shift on  $n$  letters embeds naturally as a subgroup  $\mathcal{H}_n$  of the outer automorphism group  $\text{Out}(G_{n,r})$  of the Higman–Thompson group  $G_{n,r}$ . From this, we can represent the elements of  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  by finite state non-initial transducers admitting a very strong synchronizing condition.

Let  $H \in \mathcal{H}_n$  and write  $|H|$  for the number of states of the minimal transducer representing  $H$ . We show that  $H$  can be written as a product of at most  $|H|$  torsion elements. This result strengthens a similar result of Boyle, Franks and Kitchens, where the decomposition involves more complex torsion elements and also does not support practical *a priori* estimates of the length of the resulting product.

We also explore the number of foldings of de Bruijn graphs and give a counting result for these for word length 2 and alphabet size  $n$ .

Finally, we offer new proofs of some known results about  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ .

**Key words and phrases:** 54H15, 28D15, 22F50, 68Q99, dynamics, group theory, generating sets, strongly synchronizing automata, counting strongly synchronizing automata, transducers, automorphisms of the one-sided shift, Higman–Thompson groups

\*The authors are all grateful for support from EPSRC research grant EP/R032866/1; the third author also gratefully acknowledges support from Leverhulme Trust Research Project Grant RPG-2017-159

## 1 Introduction

Let  $1 \leq r < n$  be integers. In this article, we prove that the group  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  of automorphisms of the one-sided full shift is isomorphic to a subgroup  $\mathcal{H}_n$  of the group of outer automorphisms of the Higman–Thompson groups  $G_{n,r}$ . Using this embedding we are able to study  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  from a new perspective.

Fix an alphabet  $X_n := \{0, 1, 2, \dots, n-1\}$  of size  $n$ . The shift map  $\sigma_n$  on the Cantor space of infinite sequences  $X_n^{\mathbb{N}}$  is the map which shifts a sequence to the left; i.e., a point that was formerly at index  $i+1$  now occupies the index  $i$ . An automorphism of the dynamical system  $(X_n^{\mathbb{N}}, \sigma_n)$ , is a homeomorphism of  $X_n^{\mathbb{N}}$  that commutes with the map  $\sigma_n$ . The collection of all such automorphisms forms a group  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ . We refer to this group as the group of automorphisms of the shift dynamical system.

The group  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  has been well studied (although many questions about it remain). For instance, the seminal paper of Hedlund [14] shows that elements of this group can be represented by *sliding block codes* requiring no future information. In the same paper, as mentioned above, it is shown that if  $n = 2$ , this group is isomorphic to the cyclic group of order 2; in the paper [8] the finite subgroups of  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  are characterized, and a full description of the numbers which arise as the order of some torsion element is also given.

The paper [5] gives a description of  $\text{Out}(G_{n,r})$  as a particular group of non-initial *transducers*. Note that here a transducer is a finite state machine where each state reads an element from an input alphabet, possibly changes state, and writes a string from an output alphabet. Let  $T$  be such a transducer. We call the number of states of  $T$  the size of  $T$  and denote this by  $|T|$ .

While realizing elements of  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  by transducers has been seen before (see [8, 13]), our realization takes advantage of extra structure arising from a small category of “folded” de Bruijn graphs. These are a special set of labeled directed graphs each admitting a synchronizing condition stronger than that appearing in the literature around the Road Colouring Problem and the Černý Conjecture. We refer to these as *strongly synchronizing automata*, below. Using this structure, we give a combinatorial proof of the following theorem (see Theorem 5.4 for the more detailed statement).

**Theorem 1.1.** *Let  $n > 1$  be an integer. An element  $T \in \mathcal{H}_n \cong \text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  can be written as a product of at most  $|T|$  elements of  $\mathcal{H}_n$  arising from automorphisms of directed graphs which are quotients of the underlying graph of  $T$ .*

This result is an improvement on a similar result in [8]. There, in order to decompose an element  $T$  of  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  as a product of torsion elements, one first needs to construct, in the best case, a graph with vertex size of the order of  $n^{|T|}$ , and it is unclear at the end how many torsion elements one ends up with in the decomposition. Our decomposition on the other hand begins with the transducer  $T$  and at each step  $i$ , produces a torsion factor  $H_i$  of  $T$  with strictly fewer states than  $T$ .

We also give new combinatorial arguments for the following two results (see Section 4).

- Any finite subgroup of  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  is isomorphic to a subgroup of automorphisms of a folded de Bruijn graph. For any such strongly synchronizing automaton the group of label ignoring automorphisms embeds as a subgroup of  $\text{Aut}(X_n^{\mathbb{Z}}, \sigma_n)$ . For the full one-sided shift, the directed graphs arising from *state splitting* as described in [8] and [3] are actually unlabeled directed graphs

of strongly synchronizing automata when the directions of the arrows are reversed. Thus, this embedding result is implicit in [8, 3].

- When  $n = 2$ , the unlabeled directed graph corresponding to a strongly synchronizing automaton over a 2 letter alphabet either has trivial automorphism group or its automorphism group is isomorphic to the cyclic group of order 2. This gives a new proof of a classic result of Hedlund [14] that  $\text{Aut}(X_2^{\mathbb{N}}, \sigma_2) \cong C_2$ . (Note that in [8] it is shown that when  $n > 2$  that  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  contains a non-abelian free group.)

Our next result is the promised embedding of  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  in  $\text{Out}(G_{n,r})$  (given in Section 3). Recall that the Higman–Thompson groups  $G_{n,r}$ , for  $1 \leq r < n$ , are among the first examples of finitely presented infinite simple groups (when  $n$  is even  $G_{n,r}$  is simple, and otherwise its derived subgroup is simple, see [15]).

**Theorem 1.2.** *Let  $1 \leq r < n$  be integers, then  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  embeds as a subgroup of  $\text{Out}(G_{n,r})$ .*

We briefly discuss the strategy of the proof.

A synchronous transducer that satisfies the strong synchronizing condition induces in a natural way a shift commuting map on  $X_n^{\mathbb{N}}$ . The subgroup of  $\text{Out}(G_{n,r})$  consisting of synchronous transducers that induce automorphisms of  $(X_n^{\mathbb{N}}, \sigma_n)$  is what is denoted in the paper [5] as  $\mathcal{H}_n$ . (A result of [5] asserts that  $\mathcal{H}_n$  does not depend on  $r$ .) The action of  $\mathcal{H}_n$  on  $X_n^{\mathbb{N}}$  yields an injective homomorphism to the group  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ . In order to show that this map is onto, we use the characterization by Hedlund of automorphisms of  $(X_n^{\mathbb{N}}, \sigma_n)$  as sliding block codes which require no past information; we show that a sliding block code with no past information can be simulated by a strongly synchronizing transducer. Thus, we show that  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  is isomorphic to the group  $\mathcal{H}_n$  of bi-synchronizing synchronous transducers. It is in the framework of this group  $\mathcal{H}_n$ , that we prove the results stated above.

As mentioned above, in the discussion of the group  $\text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ , there arises an interesting family of small categories of automata and foldings between them. The automata in any such category are what we call strongly synchronizing automata, below, and are a finite set of natural quotients of some particular de Bruijn graph ([10]). The categories are organized in a two-parameter family, and our final result (given in Section 6) is to count the number of elements in any such category when one of the parameters is less than or equal to 2, extending earlier results from [6]. The *Bell number*  $B(a)$ , the number of partitions of a set of size  $a$ , naturally occurs in the obtained formula.

**Theorem 1.3.** *The number of foldings of the de Bruijn graph with word length 2 over an alphabet of cardinality  $n$  is*

$$\sum_{\pi} \prod_{i=1}^{|\pi|} R(|\pi|, |A_i|),$$

where  $\pi$  runs over partitions of the alphabet,  $A_i$  is the  $i$ th part, and

$$R(s, t) = \sum_{\rho} (-1)^{|\rho|-1} (|\rho| - 1)! \prod_{i=1}^{|\rho|} B(|C_i|s),$$

where  $\rho$  runs over all partitions of  $\{1, \dots, t\}$ , and  $C_i$  is the  $i$ th part.

## 2 The Curtis, Hedlund, Lyndon Theorem

In this paper, unlike the paper of Hedlund [14], operators will be on the right of their arguments; but sequences will be indexed from left to right in the usual way.

We begin with some basic definitions and notation.

We denote by  $X_n$  the  $n$ -element set  $\{0, 1, \dots, n-1\}$ . Then  $X_n^*$  denotes the set of all finite strings (including the empty string  $\varepsilon$ ) consisting of elements of  $X_n$ . For an element  $w \in X_n^*$ , we let  $|w|$  denote the length of  $w$  (so that  $|\varepsilon| = 0$ ). We further define

$$X_n^+ = X_n^* \setminus \{\varepsilon\}, \quad X_n^k = \{w \in X_n^* : |w| = k\}, \quad X_n^{\leq k} = \bigcup_{0 \leq i \leq k} X_n^i.$$

We denote the concatenation of strings  $x, y \in X_n^*$  by  $xy$ ; in this notation we do not distinguish between an element of  $X_n$  and the corresponding element of  $X_n^1$ .

For  $x, x_1, x_2 \in X_n^*$ , if  $x$  is the concatenation  $x_1x_2$  of  $x_1$  and  $x_2$ , we write  $x_2 = x - x_1$ . One can think of the minus operator as “subtracting off a prefix”.

A bi-infinite sequence is a map  $x : \mathbb{Z} \rightarrow X_n$ . We sometimes write this sequence as  $\dots x_{-1}x_0x_1x_2\dots$ , where  $x_i = x(i) \in X_n$  (we use left actions for determining sequences). We denote the set of such sequences by  $X_n^{\mathbb{Z}}$ . In a similar way, we define a (positive) singly-infinite sequence as a map  $x : \mathbb{N} \rightarrow X_n$  (where, by convention,  $0 \in \mathbb{N}$ ). We write such a sequence as  $x_0x_1x_2\dots$  and denote the set of all such maps as  $X_n^{\mathbb{N}}$ . Finally, we also set  $X_n^{-\mathbb{N}}$  for the set of all maps  $x : X_n^{-\mathbb{N}} \rightarrow X_n$  (the (negative) singly infinite sequences). Such a map will be written as a sequence  $\dots x_{-2}x_{-1}x_0$ .

Normally, one thinks of a full one-sided shift as  $(X_n^{\mathbb{N}}, \sigma_n)$ , where the shift operator  $\sigma_n$  operates as  $y = x\sigma_n$ , where  $y_i = x_{i+1}$  for all  $i \in \mathbb{N}$ . However, in our context it will be much more natural to think of the one-sided shift space as  $(X_n^{-\mathbb{N}}, \sigma_n)$ , where the shift operator  $\sigma_n$  operates as  $y = x\sigma_n$ , where  $y_i = x_{i-1}$  for all  $i \in -\mathbb{N}$ . In Hedlund’s characterization, the automorphisms of  $(X_n^{-\mathbb{N}}, \sigma_n)$  are sliding block codes that rely on no future information, instead of no past information. This will ease many notational difficulties later on.

We can concatenate a string  $y \in X_n^*$  with a singly infinite string  $x \in X_n^{-\mathbb{N}}$ , by adding  $y$  as a suffix to  $x$ . We will sometimes subtract a finite string  $y$  from a singly infinite string  $x$  which has  $y$  as a suffix by deleting the suffix  $y$ .

For a string  $v \in X_n^*$  we write  $[v]$  for the set of all elements of  $X_n^{-\mathbb{N}}$  with  $v$  as a suffix. Clearly  $[\varepsilon] = X_n^{-\mathbb{N}}$ .

Let  $F(X_n, m)$  denote the set of functions from  $X_n^m$  to  $X_n$ . Then, for all  $m, r > 0$ , and all  $f \in F(X_n, m)$ , we define a map  $f_r : X_n^{m+r-1} \rightarrow X_n^r$  as follows.

Let  $x = x_{-m-r+2}\dots x_0$ . For  $-r+1 \leq i \leq 0$ , set  $y_i = (x_{i-m+1}x_{i-m+2}\dots x_i)f$ . Then  $xf_r = y$ , where  $y = y_{-r+1}\dots y_0$ .

In other words, we take a “window” of length  $m$  which slides along the sequence  $x$ , and at the  $i$ th step we apply  $f$  to the symbols visible in the window. (One may think of the map as acting on the rightmost letter in the viewing window, with  $m-1$  digits of history.) This procedure can be extended to define a map  $f_\infty : X_n^{\mathbb{Z}} \rightarrow X_n^{\mathbb{Z}}$ , by setting  $xf_\infty = y$  where  $y_i = (x_{i-m+1}\dots x_i)f$  for all  $i \in \mathbb{Z}$ ; and similarly for  $X_n^{-\mathbb{N}}$ .

A function  $f \in F(X_n, m)$  is called *right permutive* if, for distinct  $x, y \in X_n$  and any fixed block  $a \in X_n^{m-1}$ , we have  $(ax)f \neq (ay)f$ . Alternatively, the map from  $X_n$  to itself given by  $x \mapsto (ax)f$  is a

permutation for all  $a \in X_n^{m-1}$ . Analogously, a function  $f \in F(X_n, m)$  is called *left permutive* if the map from  $X_n$  to itself given by  $x \mapsto (xa)f$  is a permutation for all  $a \in X_n^{m-1}$ .

We note that, if  $f$  is not right permutive, then the induced map  $f_\infty$  from  $X_n^{-\mathbb{N}}$  to itself is not injective. The preceding sentence is false if we replace ‘right’ with ‘left’. For example, take the map  $g \in F(X_3, 2)$  defined by  $ax \mapsto x$  for all  $x \in \{0, 1, 2\}$  and all  $a \in \{0, 1\}$ ;  $20 \mapsto 1$ ,  $21 \mapsto 0$  and  $22 \mapsto 2$ . Then  $g$  is right permutive but not left permutive and  $g_\infty$  is a bijection. It is not always the case that a right permutive map  $f \in F(X_n, m)$  induces a bijective map  $f_\infty : X_n^{\mathbb{N}} \rightarrow X_n^{\mathbb{N}}$ . For example the map  $f \in F(X_3, 2)$  defined by  $a0 \mapsto 0$ ,  $a1 \mapsto 2$ ,  $a2 \mapsto 1$  for all  $a \in \{0, 1\}$ ;  $20 \mapsto 1$ ,  $21 \mapsto 0$ ,  $22 \mapsto 2$  is a right permutive map such that  $(\dots 111\dots)f_\infty = (\dots 222\dots)f_\infty$ . We note that a right permutive map always induces a surjective map from  $X_n^{-\mathbb{N}}$  to itself.

**Remark 2.1.** Observe that, if  $f \in F(X_n, m)$  and  $k \geq 1$ , then the map  $g \in F(X_n, m+k)$  given by

$$(x_{-m-k+1} \dots x_0)g = (x_{-m+1} \dots x_0)f,$$

satisfies  $g_\infty = f_\infty$ .

The sets  $X_n^{\mathbb{Z}}$ ,  $X_n^{\mathbb{N}}$  and  $X_n^{-\mathbb{N}}$  are topological spaces, equipped with the Tychonoff product topology derived from the discrete topology on  $X_n$ . Each is homeomorphic to Cantor space. The set  $\{\{v\} \mid v \in X_n^*\}$  is a basis of clopen sets for the topology on  $X_n^{-\mathbb{N}}$ .

In this paper the *shift map*  $\sigma_n$  is the map which sends a sequence  $x$  in  $X_n^{\mathbb{Z}}$  or  $X_n^{-\mathbb{N}}$  to the sequence  $y$  given by  $y(i) = x(i-1)$  for all  $i$  in  $\mathbb{Z}$  or  $-\mathbb{N}$  respectively.

The following result is due to Curtis, Hedlund and Lyndon [14, Theorem 3.1]:

**Theorem 2.2.** *Let  $f \in F(X_n, m)$ . Then  $f_\infty$  is continuous on  $X_n^{-\mathbb{N}}$  and  $X_n^{\mathbb{Z}}$  and commutes with the shift map on  $X_n^{\mathbb{Z}}$  and  $X_n^{-\mathbb{N}}$ .*

A continuous function from  $X_n^{\mathbb{Z}}$  to itself which commutes with the shift map is called an *endomorphism* of the shift dynamical system  $(X_n^{\mathbb{Z}}, \sigma_n)$ . If the function is invertible, since  $X_n^{\mathbb{Z}}$  is compact and Hausdorff, its inverse is continuous: it is an *automorphism* of the shift system. The sets of endomorphisms and of automorphisms are denoted by  $\text{End}(X_n^{\mathbb{Z}}, \sigma_n)$  and  $\text{Aut}(X_n^{\mathbb{Z}}, \sigma_n)$  respectively. Under composition, the first is a monoid, and the second a group.

Analogously, a continuous function from  $X_n^{-\mathbb{N}}$  to itself which commutes with the shift map on this space is an *endomorphism of the one-sided shift*  $(X_n^{-\mathbb{N}}, \sigma_n)$ ; if it is invertible, it is an *automorphism* of this shift system. The sets of such maps are denoted by  $\text{End}(X_n^{-\mathbb{N}}, \sigma_n)$  and  $\text{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ ; again the first is a monoid and the second a group.

Note that  $\sigma_n \in \text{Aut}(X_n^{\mathbb{Z}}, \sigma_n)$ , whereas  $\sigma_n \in \text{End}(X_n^{-\mathbb{N}}, \sigma_n) \setminus \text{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ . More generally, the inclusions

$$\text{End}(X_n^{-\mathbb{N}}, \sigma_n) \subsetneq \text{End}(X_n^{\mathbb{Z}}, \sigma_n) \text{ and } \text{Aut}(X_n^{-\mathbb{N}}, \sigma_n) \subsetneq \text{Aut}(X_n^{\mathbb{Z}}, \sigma_n)$$

are valid.

Define

$$F_\infty(X_n) := \bigcup_{m \geq 0} \{f_\infty : f \in F(X_n, m)\},$$

$$RF_\infty(X_n) := \bigcup_{m \geq 0} \{f_\infty : f \in F(X_n, m), f \text{ is right permutive}\}.$$

Theorem 2.2 shows that  $F_\infty(X_n) \subseteq \text{End}(X_n^{\mathbb{Z}}, \sigma_n)$ . In fact  $F_\infty(X_n)$  and  $RF_\infty(X_n)$  are submonoids of  $\text{End}(X_n^{\mathbb{Z}}, \sigma_n)$ . For given natural numbers  $l$  and  $m$ ,  $f \in F(X_n, l)$  and  $g \in F(X_n, m)$ , the function  $h \in F(X_n, l+m-1)$  defined by  $(a_{-l-m+2} \dots a_{-1} a_0)h = ((a_{-l-m+2} \dots a_{-1} a_0)f_{l+m-1})g$  satisfies  $h_\infty = f_\infty \circ g_\infty$ . If  $f$  and  $g$  are both right permutive, then so also is  $h$ . Note that  $\sigma_n \in F_\infty(X_n)$  since the function  $f \in X_n^2$  defined by

$$(x_{-1}x_0)f = x_{-1},$$

satisfies  $f_\infty = \sigma_n$ . However  $\sigma_n^{-1}$  is not an element of  $F_\infty(X_n)$ . Now, [14, Theorem 3.4] shows:

**Theorem 2.3.**  $\text{End}(X_n^{\mathbb{Z}}, \sigma_n) = \{\sigma_n^i \phi \mid i \in \mathbb{Z}, \phi \in F_\infty(X_n)\}$ .

The following result is a corollary:

**Theorem 2.4.**  $RF_\infty(X_n)$  is a submonoid of  $\text{End}(X_n^{\mathbb{Z}}, \sigma_n)$  and  $\text{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$  is the largest inverse closed subset of  $RF_\infty(X_n)$ .

### 3 Connections to transducers

In this section we will give a definition and very brief history of the Higman–Thompson groups  $G_{n,r}$ , and an incomplete list of references to related research on these in the literature. We then flesh out the connection between  $\text{Out}(G_{n,r})$  and  $\text{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ , explaining that one can represent all elements of these groups by a certain class of finite strongly synchronizing transducers. It follows from these characterizations that  $\text{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$  embeds in a straightforward fashion in  $\text{Out}(G_{n,r})$ .

#### 3.1 The Higman–Thompson groups $G_{n,r}$

Richard Thompson’s notes from 1965 [22] introduce three infinite finitely presented groups, now commonly known as  $F \leq T \leq V$ , and show that  $T$  and  $V$  are also simple. These are the first known examples of infinite finitely presented simple groups. See [11] for a standard survey on the Thompson groups.

The Higman–Thompson groups  $G_{n,r}$  were introduced by Higman in [15], where he generalizes Thompson’s construction of the group  $V$  from [22] ( $V \cong G_{2,1}$ ). Calculations in the Higman–Thompson groups do not play a role in the main body of this article, but for the curious reader, in Subsubsection 3.1.2 we still provide an oft-used concrete realization of the groups  $G_{n,r}$  as specific groups of homeomorphisms of Cantor spaces.

In any case, Higman in [15] shows that the groups  $G_{n,r}$  are simple when  $n$  is even, and that they have a simple commutator subgroup  $G'_{n,r}$  of index two when  $n$  is odd. Thus he obtains the first known infinite family of infinite, finitely presented simple groups (Higman also shows there are infinitely many isomorphism types amongst the groups  $G_{n,r}$ ). See [15, 9, 4, 19, 16, 12, 5, 21] for some research on these groups. The paper [5] provides the characterization of  $\text{Out}(G_{n,r})$  that is relevant to this article.

It is expressed in [7] that R. Thompson’s group  $V$  represents a “gentle” realization of the alternating groups  $A_k$  into an infinite context. In Subsubsection 3.1.2 we generate a given group  $G_{n,r}$  by transpositions of clopen subsets of Cantor space (which themselves can each be written as a product of  $n$  “smaller” transpositions). This type of generation is part of the justification for this view on the fundamental nature of the groups  $G_{n,r}$  (or at least, for the group  $V \cong G_{2,1}$ ).

### 3.1.1 The Cantor spaces $\mathfrak{C}_{n,r}$

Let  $r$  and  $n$  be given natural numbers with  $n \geq 2$ .

Given such  $r$  and  $n$ , determine two finite alphabets  $\dot{r} := \{\dot{0}, \dot{1}, \dots, \dot{r} - 1\}$  and our standard  $n$ -letter alphabet  $\{0, 1, \dots, n - 1\}$  and give each of these sets the discrete topology. A standard characterization of  $n$ -ary Cantor space  $\mathfrak{C}_n$  is as the space  $\mathfrak{C}_n := \{0, 1, \dots, n - 1\}^{\mathbb{N}}$  under the product topology, and we can then form another Cantor space  $\mathfrak{C}_{n,r}$  as the product  $\dot{r} \times \mathfrak{C}_n$ .

$$\mathfrak{C}_{n,r} := \{ca_0a_1a_2\dots \mid a_i \in \{0, 1, \dots, n - 1\}, c \in \dot{r}\}.$$

That is,  $\mathfrak{C}_{n,r}$  can be thought of as a disjoint union of  $r$  copies of the standard infinite  $n$ -ary Cantor space  $\mathfrak{C}_n$ .

The space  $\mathfrak{C}_{n,r}$  has the topology generated by using *cones* as basic open sets. A cone is any subset of the form  $\mathbf{x}\mathfrak{C}_n$ , where  $\mathbf{x}$  is a finite sequence of the form  $cx_0x_1\dots x_j$  for  $c \in \dot{r}$  and each  $x_i \in \{0, 1, \dots, n - 1\}$ . Thus, the cone at  $\mathbf{x}$  is all of the elements of  $\mathfrak{C}_{n,r}$  which have leading prefix equal to  $\mathbf{x}$ .

### 3.1.2 The Higman–Thompson groups $G_{n,r}$

The group  $G_{n,r}$  can be realized as a subgroup of  $\text{Homeo}(\mathfrak{C}_{n,r})$  as follows. It is the subgroup generated by *prefix replacement swaps*: one specifies two incomparable finite prefixes (that is, neither is a prefix of the other), say  $\mathbf{x} := c_1a_0a_1\dots a_j$  and  $\mathbf{y} := c_2b_0b_1\dots b_k$  (for some  $c_1, c_2 \in \dot{r}$  and with each  $a_i$  and  $b_i$  from the alphabet  $\{0, 1, 2, \dots, n - 1\}$ ), and then interchanges the cones in the Cantor space  $\mathfrak{C}_{n,r}$  determined by these prefixes, using an element we denote by  $(\mathbf{x} \ \mathbf{y})$ . For example, for this particular swap we have:

$$\begin{aligned} c_1a_0a_1\dots a_ja_{j+1}a_{j+2}\dots (\mathbf{x} \ \mathbf{y}) &= c_2b_0b_1\dots b_ka_{j+1}a_{j+2}\dots \\ c_2b_0b_1\dots b_kb_{k+1}b_{k+2}\dots (\mathbf{x} \ \mathbf{y}) &= c_1a_0a_1\dots a_jb_{k+1}b_{k+2}\dots \\ \vec{z}(\mathbf{x} \ \mathbf{y}) &= \vec{z} \text{ where } \vec{z} \text{ does not have prefix } \mathbf{x} \text{ or } \mathbf{y}. \end{aligned}$$

Composition of these swaps results in homeomorphisms of  $\mathfrak{C}_{n,r}$  that replace some finite decomposition  $D$  of  $\mathfrak{C}_{n,r}$  into pairwise disjoint cones by some other such decomposition  $R$ , given a bijection from the set  $D$  of cones to the set  $R$  of cones. This works as follows: one replaces the maximal common prefix of the points in a cone appearing in  $D$  by the maximal common prefix of the points in the corresponding cone from  $R$ .

## 3.2 Automata and transducers

An *automaton*, in our context, is a triple  $A = (X_A, Q_A, \pi_A)$ , where

- (a)  $X_A$  is a finite set called the *alphabet* of  $A$  (we assume that this has cardinality  $n$ , and identify it with  $X_n$ , for some  $n$ );
- (b)  $Q_A$  is a finite set called the *set of states* of  $A$ ;
- (c)  $\pi_A$  is a function  $X_A \times Q_A \rightarrow Q_A$ , called the *transition function*.

The *size* of an automaton  $A$  is the cardinality of its state set. We use the notation  $|A|$  for the size of the  $A$ .

We regard an automaton  $A$  as operating as follows. If it is in state  $q$  and reads symbol  $a$  (which we suppose to be written on an input tape), it moves into state  $\pi_A(a, q)$  before reading the next symbol. As this suggests, we can imagine that the automaton  $A$  is in the middle of an input word, reads the next letter and moves to the right, possibly changing state in the process.

We can extend the notation as follows. For  $w \in X_n^m$ , let  $\pi_A(w, q)$  be the final state of the automaton which reads the word  $w$  from initial state  $q$ . Thus, if  $w = x_0x_1 \dots x_{m-1}$ , then

$$\pi_A(w, q) = \pi_A(x_{m-1}, \pi_A(x_{m-2}, \dots, \pi_A(x_0, q) \dots)).$$

By convention, we take  $\pi_A(\varepsilon, q) = q$ .

For a given state  $q \in Q_A$ , we call the automaton  $A$  which starts in state  $q$  an *initial automaton*, denoted by  $A_q$ , and say that it is *initialized* at  $q$ .

An automaton  $A$  can be represented by a labeled directed graph, whose vertex set is  $Q_A$ ; there is a directed edge labeled by  $a \in X_A$  from  $q$  to  $r$  if  $\pi_A(a, q) = r$ .

A *transducer* is a quadruple  $T = (X_T, Q_T, \pi_T, \lambda_T)$ , where

- (a)  $(X_T, Q_T, \pi_T)$  is an automaton;
- (b)  $\lambda_T : X_T \times Q_T \rightarrow X_T^*$  is the *output function*.

Such a transducer is an automaton which can write as well as read; after reading symbol  $a$  in state  $q$ , it writes the string  $\lambda_T(a, q)$  on an output tape, and makes a transition into state  $\pi_T(a, q)$ . We call the automaton  $(X_T, Q_T, \pi_T)$  the underlying automaton of  $T$ . Thus, the size of a transducer is the size of its underlying automaton. An *initial transducer*  $T_q$  is simply a transducer which starts in state  $q$ . Transducers which are *synchronous* (i.e., which always write one letter whenever they read one letter) are also known as *Mealy machines* (see [13]), although we generally will not use that language here. Transducers which are not synchronous are described as *asynchronous* when this aspect of the transducer is being highlighted. In this paper, we will only work with synchronous transducers without an initial state, and, below, **we will simply call these transducers**.

In the same manner as for automata, we can extend the notation to allow transducers to act on finite strings: we let  $\pi_T(w, q)$  and  $\lambda_T(w, q)$  be, respectively, the final state and the concatenation of all the outputs obtained when a transducer  $T$  reads a string  $w$  from a state  $q$ .

A transducer  $T$  can also be represented as an edge-labeled directed graph. Again the vertex set is  $Q_T$ ; now, if  $\pi_T(a, q) = r$ , we put an edge with label  $a|\lambda_T(a, q)$  from  $q$  to  $r$ . In other words, the edge label describes both the input and the output associated with that edge. We call  $a$  the *input label* of the edge and  $\lambda_T(a, q)$  the *output label* of the edge.

For example, Figure 1 describes a synchronous transducer over the alphabet  $X_2$ .

We can regard an automaton, or a transducer, as acting on an infinite string from  $X_n^{\mathbb{N}}$  where  $X_n$  is the alphabet. This action is given by iterating the action on a single symbol; so the output string is given by

$$\lambda_T(xw, q) = \lambda_T(x, q)\lambda_T(w, \pi_T(x, q)).$$

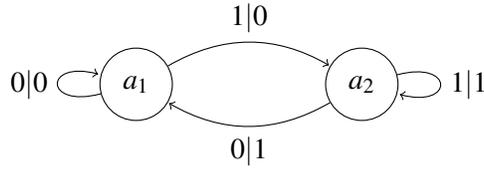


Figure 1: A transducer over  $X_2$

Thus  $T_q$  induces a map  $w \mapsto \lambda_T(w, q)$  from  $X_n^{\mathbb{N}}$  to itself; it is easy to see that this map is continuous. If it is a homeomorphism, then we call the state  $q$  a *homeomorphism state*. We write  $\text{image}(q)$  for the image of the map induced by  $T_q$ .

Two states  $q_1$  and  $q_2$  are said to be  $\omega$ -equivalent if the transducers  $T_{q_1}$  and  $T_{q_2}$  induce the same continuous map. (This can be checked in finite time, see [13].) More generally, we say that two initial transducers  $T_q$  and  $T'_q$  are  $\omega$ -equivalent if they induce the same continuous map on  $X_n^{\mathbb{N}}$ .

A transducer is said to be *weakly minimal* if no two states are  $\omega$ -equivalent. For a synchronous transducer  $T$ , two states  $q_1$  and  $q_2$  are  $\omega$ -equivalent if  $\lambda_T(a, q_1) = \lambda_T(a, q_2)$  for any finite word  $a \in X_n^*$ . Moreover, if  $q_1$  and  $q_2$  are  $\omega$ -equivalent states of a synchronous transducer, then for any finite word  $a \in X_n^+$ ,  $\pi_T(a, q_1)$  and  $\pi_T(a, q_2)$  are also  $\omega$ -equivalent states.

There is a stronger notion of minimality which appears in [13] and applies also to asynchronous transducer, hence our use of the adjective *weakly*.

Two weakly minimal non-initial transducers  $T$  and  $U$  are said to be  $\omega$ -equal if there is a bijection  $f : Q_T \rightarrow Q_U$ , such that for any  $q \in Q_T$ ,  $T_q$  is  $\omega$ -equivalent to  $U_{(q)f}$ . Two weakly minimal initial transducers  $T_p$  and  $U_q$  are said to be  $\omega$ -equal if there is a bijection  $f : Q_T \rightarrow Q_U$ , such that  $(p)f = q$  and for any  $t \in Q_T$ ,  $T_t$  is  $\omega$ -equivalent to  $U_{(t)f}$ . We shall use the symbol ‘=’ to represent  $\omega$ -equality of initial and non-initial transducers. Two non-initial transducers are said to be  $\omega$ -equivalent if they have  $\omega$ -equal minimal representatives.

In the class of synchronous transducers, the  $\omega$ -equivalence class of any transducer has a unique weakly minimal representative. In the general case, if one permits infinite outputs from finite inputs, Grigorchuk *et al.* [13] prove that the  $\omega$ -equivalence class of an initialized transducer  $T_q$  has a unique minimal representative and give an algorithm for computing this representative.

Throughout this article, as a matter of convenience, we shall not distinguish between  $\omega$ -equivalent transducers. Thus, for example, we introduce various groups as if the elements of those groups are transducers, whereas the elements of these groups are in fact  $\omega$ -equivalence classes of transducers.

Given two transducers  $T = (X_n, Q_T, \pi_T, \lambda_T)$  and  $U = (X_n, Q_U, \pi_U, \lambda_U)$  with the same alphabet  $X_n$ , we define their product  $T * U$ . The intuition is that the output for  $T$  will become the input for  $U$ . Thus we take the alphabet of  $T * U$  to be  $X_n$ , the set of states to be  $Q_{T*U} = Q_T \times Q_U$ , and define the transition and rewrite functions by the rules

$$\begin{aligned} \pi_{T*U}(x, (p, q)) &= (\pi_T(x, p), \pi_U(\lambda_T(x, p), q)), \\ \lambda_{T*U}(x, (p, q)) &= \lambda_U(\lambda_T(x, p), q), \end{aligned}$$

for  $x \in X_n$ ,  $p \in Q_T$  and  $q \in Q_U$ . Here we use the earlier convention about extending  $\lambda$  and  $\pi$  to the case

when the transducer reads a finite string. If  $T$  and  $U$  are initial with initial states  $q$  and  $p$  respectively then the state  $(q, p)$  is considered the initial state of the product transducer  $T * U$ .

In automata theory a synchronous (not necessarily initial) transducer  $T = (X_n, Q_T, \pi_T, \lambda_T)$  is *invertible* if for any state  $q$  of  $T$ , the map  $\rho_q := \lambda_T(\cdot, q) : X_n \rightarrow X_n$  is a bijection. In this case the inverse of  $T$  is the transducer  $T^{-1}$  with state set  $Q_{T^{-1}} := \{q^{-1} \mid q \in Q_T\}$ , transition function  $\pi_{T^{-1}} : X_n \times Q_{T^{-1}} \rightarrow Q_{T^{-1}}$  defined by  $(x, p^{-1}) \mapsto q^{-1}$  if and only if  $\pi_T((x)\rho_p^{-1}, p) = q$ , and output function  $\lambda_{T^{-1}} : X_n \times Q_{T^{-1}} \rightarrow X_n$  defined by  $(x, p) \mapsto (x)\rho_p^{-1}$ .

One can interpret the previous paragraph as follows: For the invertible synchronous transducer  $T$ , the inverse transducer  $T^{-1}$  is the result of switching inputs and outputs on all transitions of  $T$ . In particular, we can think of a synchronous transducer as an ordered pair of automata, each with the same structure as directed graphs. Inversion then corresponds to swapping the ordering on this ordered pair, much as we do in constructing inverses for non-zero fractions by switching the numerator and denominator in a non-zero fraction of integers. In the transducer  $T$  depicted in Figure 2 below, the input automaton corresponds to the directed graph with the input labels on the edges and the output automaton corresponds to the directed graph with the output labels on the edges. Henceforth, we will refer to the input automaton as the *domain automaton* and the output automaton as the *range automaton*.

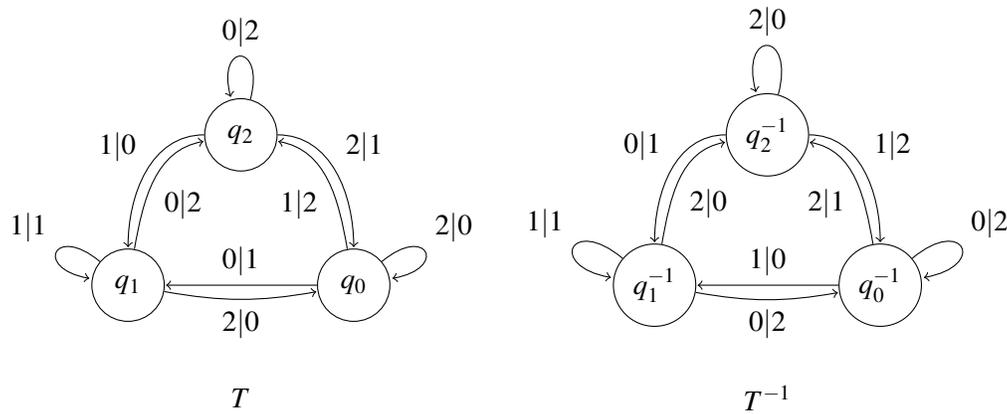


Figure 2: Inverting a synchronous transducer  $T$ .

In this article, we will come across synchronous transducers which are not invertible in the automata theoretic sense but which nevertheless induce self-homeomorphisms of the spaces  $X_n^{\mathbb{Z}}$  and  $X_n^{-\mathbb{N}}$ . Consequently it will be important to distinguish between an automaton theoretic inverse and the inverse of the induced action on the various spaces we consider.

### 3.3 Synchronizing automata and bisynchronizing transducers

Given a natural number  $k$ , we say that an automaton  $A$  with alphabet  $X_n$  is *synchronizing at level  $k$*  if there is a map  $\mathfrak{s}_k : X_n^k \mapsto Q_A$  such that, for all  $q$  and any word  $w \in X_n^k$ , we have  $\pi_A(w, q) = \mathfrak{s}_k(w)$ . In other words,  $A$  is synchronizing at level  $k$  if, after reading a word  $w$  of length  $k$  from a state  $q$ , the final state

depends only on  $w$  and not on  $q$ . (Again we use the extension of  $\pi_A$  to allow the reading of an input string rather than a single symbol.) We call  $\mathfrak{s}_k(w)$  the state of  $A$  forced by  $w$ ; the map  $\mathfrak{s}_k$  is called the *synchronizing map at level  $k$* . An automaton  $A$  is called *strongly synchronizing* if it is synchronizing at level  $k$  for some  $k$ .

We remark here that the notion of synchronization occurs in automata theory in considerations around the *Černý conjecture*, in a weaker sense. A word  $w$  is said to be a *reset word* for  $A$  if  $\pi_A(w, q)$  is independent of  $q$ ; an automaton is called *synchronizing* if it has a reset word [23, 2]. Our definition of “synchronizing at level  $k$ ”/“strongly synchronizing” requires every word of length  $k$  to be a reset word for the automaton.

If the automaton  $A$  is synchronizing at level  $k$ , we define the *core* of  $A$  to be the set of states forming the image of the map  $\mathfrak{s}$ . It is an easy observation that, if  $A$  is synchronizing at level  $k$ , then its core is an automaton in its own right, and is also synchronizing at level  $k$ . We denote this automaton by  $\text{core}(A)$ . We say that an automaton or transducer is *core* if it is equal to its core. Moreover, if  $T$  is a transducer which (regarded as an automaton) is synchronizing at level  $k$ , then the core of  $T$  (similarly denoted  $\text{core}(T)$ ) induces a continuous map  $f_T : X_n^{\mathbb{Z}} \rightarrow X_n^{\mathbb{Z}}$ .

Clearly, if  $A$  is synchronizing at level  $k$ , then it is synchronizing at level  $l$  for all  $l \geq k$ ; but the map  $f_T$  is independent of the level chosen to define it.

Let  $T_q$  be an initial transducer which is invertible with inverse  $T_q^{-1}$ . If  $T_q$  is synchronizing at level  $k$ , and  $T_q^{-1}$  is synchronizing at level  $l$ , we say that  $T_q$  is *bisynchronizing* at level  $(k, l)$ . If  $T_q$  is invertible and is synchronizing at level  $k$  but not bisynchronizing, we say that it is *one-way synchronizing* at level  $k$ .

For a non-initial invertible transducer  $T$  we also say  $T$  is *bi-synchronizing* (at level  $(k, l)$ ) if both  $T$  and its inverse  $T^{-1}$  are synchronizing at levels  $k$  and  $l$  respectively.

**Notation 3.1.** Let  $T$  be a transducer which is synchronizing at level  $k$  and let  $l \geq k$  be any natural number. Then for any word  $w \in X_n^l$ , we write  $q_w$  for the state  $\mathfrak{s}_l(w)$ , where  $\mathfrak{s}_l : X_n^l \rightarrow Q_T$  is the synchronizing map at level  $l$ .

The following result was proved in Bleak *et al.* [5].

**Proposition 3.2.** *Let  $T, U$  be transducers which (as automata) are synchronizing at levels  $j, k$  respectively, Then  $T * U$  is synchronizing at level at most  $j + k$ .*

In what follows we give a formula specifying how strongly synchronizing transducers act by continuous functions on  $X_n^{\mathbb{Z}}$ . The formula induces a natural action on  $X_n^{-\mathbb{N}}$  which immediately commutes with the shift. We recall that in our context the shift map  $\sigma_n$  is the map which sends a sequence  $x \in X_n^{-\mathbb{N}} \sqcup X_n^{\mathbb{Z}}$  to the sequence  $y \in X_n^{-\mathbb{N}} \sqcup X_n^{\mathbb{Z}}$  given by  $y_i = x_{i-1}$  for all valid  $i \in -\mathbb{N} \sqcup \mathbb{Z}$ . This represents a deviation from the way the shift map conventionally operates, however, in this point of view, as we will become clear, synchronizing transducers can locally process inputs in a manner consistent with the definition given in Subsection 3.2. The formula is as follows:

Let  $T$  be a transducer which is core, and is synchronizing at level  $k$ . The map  $f_T : X_n^{\mathbb{Z}} \rightarrow X_n^{\mathbb{Z}}$  maps an element  $x \in X_n^{\mathbb{Z}}$  to the sequence  $y$  defined by  $y_i = \lambda_T(x_i, q_{x_{i-k}x_{i-k+1}\dots x_{i-1}})$ . We also write  $f_T$  for the continuous map from  $X_n^{-\mathbb{N}}$  to itself defined by  $y_i = \lambda_T(x_i, q_{x_{i-k}x_{i-k+1}\dots x_{i-1}})$  for all  $i \in -\mathbb{N}$ . We note that the induced map on  $X_n^{-\mathbb{N}}$  is simply the restriction of the map on  $X_n^{\mathbb{Z}}$  to the subsequence indexed by the negative integers.

We note that given an element  $x \in X_n^{\mathbb{Z}}$  such that  $(x)f_T = y$ , then  $y_0y_1 \dots = (x_0x_1 \dots)T_{q_{x_{-k}x_{-k+1} \dots x_{-1}}}$ . This is what was meant by the transducer  $T$  acts locally in a manner consistent with the definitions of Subsection 3.2.

Now strongly synchronizing transducers may induce endomorphisms of the shift:

**Proposition 3.3.** *Let  $T$  be a minimal transducer which is synchronizing at level  $k$  and which is core. Then  $f_T \in \text{End}(X_n^{\mathbb{Z}}, \sigma_n)$  and  $f_T \in \text{End}(X_n^{-\mathbb{N}}, \sigma_n)$ .*

**Proof.** It is clear from the assumptions that  $f_T$  is continuous and by definition induces a map from  $X_n^{\mathbb{Z}}$  to itself and from  $X_n^{-\mathbb{N}}$  to itself. Now let  $x \in X_n^{\mathbb{Z}} \sqcup X_n^{-\mathbb{N}}$  and  $i \in \mathbb{Z}$  an appropriate index for  $x$ . Let  $y = (x)f_T$ . Observe that  $y_i = \lambda(x_i, q)$ , where  $q = s(x_{i-k} \dots x_{i-1})$  is the state forced by  $x_{i-k} \dots x_{i-1}$ .

Now let  $u = (x)\sigma_n$  and  $v = (u)f_T$ . Then

$$v_{i-1} = \lambda(u_{i-1}, q'),$$

where  $q'$  is the state of  $T$  forced by  $u_{i-k-1} \dots u_{i-2}$ . But by assumption,  $u_{i-k-1} \dots u_{i-2} = x_{i-k} \dots x_{i-1}$ , and this string forces state  $q$ ; so  $q' = q$ , and hence  $v_{i-1} = y_i$ .

It now follows that  $(x)f_T\sigma_n = (y)\sigma_n = v = (u)f_T = (x)\sigma_n f_T$ . □

The transducer in Figure 1 induces the shift map on  $X_n^{\mathbb{Z}}$ . More generally, let  $\mathfrak{S}_n = (X_n, Q_{\mathfrak{S}_n}, \pi_{\mathfrak{S}_n}, \lambda_{\mathfrak{S}_n})$  be the transducer defined as follows. Let  $Q_{\mathfrak{S}_n} := \{0, 1, 2, \dots, n-1\}$ , and let  $\pi_{\mathfrak{S}_n} : X_n \times Q_{\mathfrak{S}_n} \rightarrow Q_{\mathfrak{S}_n}$  and  $\lambda_{\mathfrak{S}_n} : X_n \times Q_{\mathfrak{S}_n} \rightarrow X_n$  be defined by  $\pi_{\mathfrak{S}_n}(x, i) = x$  and  $\lambda_{\mathfrak{S}_n}(x, i) = i$  for all  $x \in X_n, i \in Q_{\mathfrak{S}_n}$ . Then  $f_{\mathfrak{S}_n} = \sigma_n$ .

In [5], the authors show that the set  $\widetilde{\mathcal{P}}_n$  of weakly minimal finite synchronous core transducers is a monoid. (Note that core transducers are strongly synchronizing.) The monoid operation consists of taking the product of transducers and reducing it by removing non-core states and identifying  $\omega$ -equivalent states to obtain a weakly minimal and synchronous representative. Let  $\mathcal{P}_n$  be the subset of  $\widetilde{\mathcal{P}}_n$  consisting of transducers  $T$  such that  $f_T$  is an automorphism of the two-sided shift dynamical system. We observe that elements of  $\mathcal{P}_n$  may not be minimal. It is clear that  $\mathfrak{S}_n \in \mathcal{P}_n$ . For an element  $T \in \mathcal{P}_n$ , we use the language  $T$  induces an automorphism of the two-sided shift dynamical system to mean that  $f_T$  is an element of  $\text{Aut}(X_n^{\mathbb{Z}}, \sigma_n)$ .

### 3.4 De Bruijn graphs and $\text{End}(X_n^{\mathbb{Z}}, \sigma_n)$

The *de Bruijn graph*  $G(n, m)$  can be defined as follows, for integers  $m \geq 1$  and  $n \geq 2$ . The vertex set is  $X_n^m$ , where  $X_n$  is the alphabet  $\{0, \dots, n-1\}$  of cardinality  $n$ . There is a directed arc from  $a_1 \dots a_m$  to  $a_2 \dots a_m a_0$ , with label  $a_0$ .

Note that, in the literature, the directed edge is from  $a_0 a_1 \dots a_{m-1}$  to  $a_1 \dots a_{m-1} a_m$  and the label on this edge is often given as the  $(m+1)$ -tuple  $a_0 a_1 \dots a_{m-1} a_m$ . However, to fit with the notation already defined, the equivalent definition given above is more apt.

Figure 3 shows the de Bruijn graph  $G(3, 2)$ .

Observe that the de Bruijn graph  $G(n, m)$  describes an automaton over the alphabet  $X_n$ . Moreover, this automaton is synchronizing at level  $m$ : when it reads the string  $b_0 b_1 \dots b_{m-1}$  from any initial state, it moves into the state labeled  $b_0 b_1 \dots b_{m-1}$ .

The de Bruijn graph is, in a sense we now describe, the universal automaton over  $X_n$  which is synchronizing at level  $m$ .

DECOMPOSING ONE-SIDED SHIFT AUTOMORPHISMS

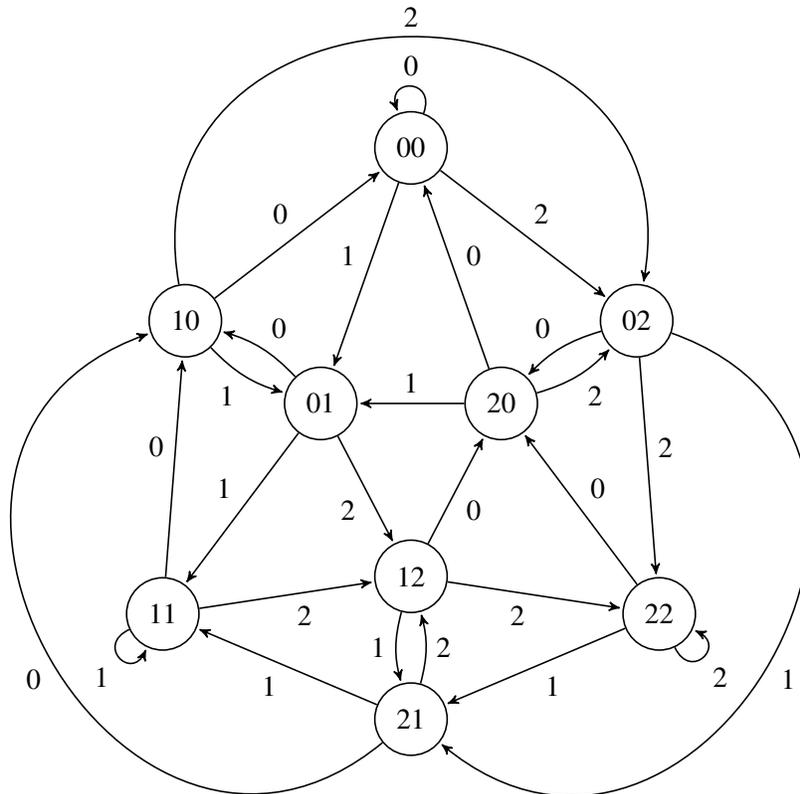


Figure 3: The de Bruijn graph  $G(3,2)$ .

We define a *folding* of an automaton  $A$  over the alphabet  $X_n$  to be an equivalence relation  $\equiv$  on the state set of  $A$  with the property that, if  $a \equiv a'$  and  $\pi_A(x, a) = b$ ,  $\pi_A(x, a') = b'$ , then  $b \equiv b'$ . That is, reading the same letter from equivalent states takes the automaton to equivalent states. If  $\equiv$  is a folding of  $A$ , then we can uniquely define the *folded automaton*  $A/\equiv$ : the state set is the set of  $\equiv$ -classes of states of  $A$ ; and, denoting the  $\equiv$ -class of  $a$  by  $[a]$ , we have  $\pi_{A/\equiv}(x, [a]) = [\pi_A(x, a)]$  (note that this is well-defined).

**Proposition 3.4.** *The following are equivalent for an automaton  $A$  on the alphabet  $X_n$ :*

- $A$  is synchronizing at level  $m$ , and is core;
- $A$  is the folded automaton from a folding of the de Bruijn graph  $G(n, m)$ .

**Proof.** The “if” statement is clear. So suppose that  $A$  is synchronizing at level  $m$ . Define a relation  $\equiv$  on the vertex set  $X_n^m$  of  $G(n, m)$  by the rule that  $a \equiv b$  if the states of  $A$  after reading  $a$  and  $b$  respectively are equal. (These states are independent of the initial state, by assumption.) It is readily seen that  $\equiv$  is a folding of  $G(n, m)$ , and the  $\equiv$ -classes are bijective with the states of  $A$ . (The fact that  $A$  is core shows that the map which takes the state  $q$  of  $A$  to the set of  $\equiv$ -classes of  $m$ -tuples which bring  $A$  to state  $q$  is well-defined and injective by definition of  $\equiv$ , and is onto since  $A$  is core.) Moreover, this bijection is clearly an isomorphism.  $\square$

**Remark 3.5.** An automaton  $A$  over an alphabet  $X_n$  can be regarded, in terms of universal algebra, as an algebra with unary operators  $v_x$  for  $x \in X_n$ , where the elements of the algebra are the states, and  $av_x = \pi(x, a)$ . A folding is precisely the kernel of an algebra homomorphism, and the folded automaton is isomorphic to the image of the homomorphism. The automata which are synchronizing at level  $m$  form a variety, defined by the identities

$$av_{x_0}v_{x_1}\cdots v_{x_{m-1}} = bv_{x_0}v_{x_1}\cdots v_{x_{m-1}}$$

for all elements  $a, b$  of the algebra and all choices of  $x_0, \dots, x_{m-1}$ .

We now describe how to make the de Bruijn automaton into a transducer by specifying outputs. Let  $f \in F(X_n, m + 1)$  be a function from  $X_n^{m+1}$  to  $X_n$ . The output function of the transducer  $T_f$  will be given by

$$\lambda_T(x, a_{m-1}a_{m-2}\cdots a_0) = (a_{m-1}a_{m-2}\cdots a_0x)f.$$

In other words, if the transducer reads  $m + 1$  symbols, then its output is obtained by applying  $f$  to the sequence of symbols read. Note that this transducer is synchronous; it writes one symbol for each symbol read. When applied to  $x \in X_n^{\mathbb{Z}}$ , it produces  $y = (x)f_\infty \in X_n^{\mathbb{Z}}$ . Recall that the function  $f \in F(X_n, 2)$  given by  $(x_{-1}x_0)f = x_{-1}$  for all  $x_{-1}, x_0 \in X_n$ , induces the shift map  $\sigma_n$  on  $X_n^{\mathbb{Z}}$  and  $X_n^{-\mathbb{N}}$ . For this map we have  $T_f = \mathfrak{S}_n$ .

**Remark 3.6.** Given any de Bruijn graph  $G(n, m)$ , and any transducer  $T$  with underlying directed graph  $G(n, m)$  there is a function  $f \in F(X_n, m + 1)$  such that  $T_f = T$ .

Clearly the transducer  $T_f$  is synchronizing at level  $m$ . This remains true if we minimise it or identify its  $\omega$ -equivalent states; so by Proposition 3.4, the resulting minimal or weakly minimal transducer is a folding of the de Bruijn graph  $G(n, m)$ . Let  $T \in \mathcal{P}_n$  be the weakly-minimal representative of  $T_f$ , then  $f_T = f_{T_f} = f_\infty$  holds since identifying  $\omega$ -equivalent states does not affect the map  $f_T$ .

**Remark 3.7.** The preceding paragraph together with Remarks 2.1 and 3.6 show that there is a bijection from  $F_\infty(X_n)$  to  $\widetilde{\mathcal{P}}_n$ . The next result demonstrates that this bijection is a monoid homomorphism.

**Proposition 3.8.** *Let  $A, B \in \widetilde{\mathcal{P}}_n$ . Then  $f_A \circ f_B = f_{A*B}$ .*

**Proof.** Let  $j, k$  be natural numbers such that  $A$  is synchronizing at level  $j$  and  $B$  is synchronizing at level  $k$ . By Proposition 3.2,  $A*B$  is synchronizing at level  $k+j$ .

Let  $x \in X_n^{\mathbb{Z}}$  and  $i \in \mathbb{Z}$  be arbitrary and  $y, z, t \in X_n^{\mathbb{Z}}$  be such that  $y = (x)f_A$ ,  $z = (y)f_B$  and  $t = (x)f_{A*B}$ . Set  $a := x_{i-j-k} \dots x_{i-1} \in X_n^{j+k}$ ,  $b := x_{i-k} \dots x_{i-1} \in X_n^k$ ,  $b' = x_{i-j} \dots x_{i-1} \in X_n^j$  and  $c := x_{i-j-k} \dots x_{i-k-1} \in X_n^j$ .

By definition of the function  $f_A$ , the block  $d := y_{i-k} y_{i-k+1} \dots y_{i-1}$  of  $y$  satisfies  $d y_i$  is precisely equal to  $\lambda_A(\overline{bx_i}, q_c)$ . Once more, by definition,  $z_i = \lambda_B(y_i, p_d)$  and since  $y_i = \lambda_A(x_i, q_{b'})$ ,  $z_i = \lambda_{A*B}(x_i, (q_{b'}, p_d))$  as well. However, the state of  $A*B$  forced by  $a$  is precisely  $(q_{b'}, p_d)$ , and so we conclude that  $t_i = \lambda_{A*B}(x_i, (q_{b'}, p_d)) = z_i$ . Since  $i$  and  $x$  were arbitrarily chosen,  $t = z$  and  $f_A \circ f_B = f_{A*B}$ .  $\square$

**Corollary 3.9.** *The monoid  $F_\infty(X_n)$  is isomorphic to  $\widetilde{\mathcal{P}}_n$ .*

Let  $\widetilde{\mathcal{H}}_n$  be the submonoid of  $\widetilde{\mathcal{P}}_n$  consisting of those elements  $P \in \widetilde{\mathcal{P}}_n$  all of whose states are homeomorphism states. Set  $\mathcal{H}_n$  to be the largest inverse closed subset of  $\widetilde{\mathcal{H}}_n$  (where we take the automata theoretic inverse in this case). Observe that  $\mathcal{H}_n$  is a group and by Proposition 3.8 the automata theoretic inverse of  $\mathcal{H}_n$  coincides with its inverse in  $\widetilde{\mathcal{P}}_n$  as a map of  $X_n^{\mathbb{Z}}$ . Thus,  $\mathcal{H}_n$ , as a set, is precisely the set of core, synchronous, invertible, minimal, bi-synchronizing transducers. It is a result in [5] that  $\mathcal{H}_n$  is isomorphic to a subgroup of  $\text{Out}(G_{n,1})$  which in turn is a subgroup of  $\text{Out}(G_{n,r})$  for all  $1 \leq r < n$ . We further remark that right permutive maps  $f \in F(X_n, m)$  give rise to transducers  $T_f$  which are elements of  $\widetilde{\mathcal{H}}_n$ . By Theorem 2.3 we therefore have the following corollary:

**Theorem 3.10.**  *$RF_\infty \cong \widetilde{\mathcal{H}}_n$  and  $\text{Aut}(X_n^{-\mathbb{N}}, \sigma_n) \cong \mathcal{H}_n$ . Thus  $\text{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$  is isomorphic to a subgroup of  $\text{Out}(G_{n,r})$ .*

## 4 Automorphisms of de Bruijn graphs and $\mathcal{H}_n$

In this section we show that a finite subgroup  $G$  of  $\mathcal{H}_n \cong \text{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$  is isomorphic to the automorphism group  $\text{Aut}(\Gamma)$  of the underlying directed graph  $\Gamma$  of an automaton  $A$  arising from a folding of a de Bruijn graph. Moreover, for any directed graph  $\Gamma$  underlying an automaton  $A$  arising from a folding of a de Bruijn graph, there is a subgroup  $G$  of  $\mathcal{H}_n$  isomorphic to  $\text{Aut}(\Gamma)$ . We make use of this result and results [8] to characterize the group  $\text{Aut}(\Gamma)$  for  $\Gamma$  the underlying directed graph of an automaton  $A$  arising from a folding of a de Bruijn graph. In particular we show that the automorphism group of a de Bruijn  $G(n, m)$  is precisely the symmetric group on a set of size  $n$ .

### 4.1 Elements of $\mathcal{H}_n$ from automorphisms of directed graphs underlying folded automata

We use the connection to de Bruijn graphs to construct elements of  $\mathcal{H}_n$ . Recall that an automaton  $A$  may be regarded as labeled directed graph with vertex set  $Q_A$ , and edge set  $E_A \subset Q_A \times X_n \times Q_A$ . In this view, for vertices or states  $p, q \in Q_A$ , and a letter  $x \in X_n$ ,  $(p, x, q) \in E_A$  is an edge from  $p$  to  $q$  with label  $x$  if and only if  $\pi_A(x, p) = q$ . Let  $G_A$  denote the unlabeled directed graph corresponding to an automaton  $A$ .

We may therefore consider the automorphisms of the directed graph  $G_A$  underlying an automaton  $A$ . We construct elements of  $\mathcal{H}_n$  from automorphisms of  $G_A$  where  $A$  is a folded automata arising from foldings of de Bruijn graphs. Though, we do not distinguish between an automaton and the labeled directed graph it generates, we shall distinguish between an automaton  $A$  and its unlabeled directed graph  $G_A$ .

It turns out that all elements of  $\mathcal{H}_n$  arising from an automorphism of the underlying graph of a folded automaton have finite order. In the paper [8] Boyle *et al.* show that  $\mathcal{H}_n$  is generated by elements of finite order, and give a generating set: the ‘vertex’ and ‘simple’ automorphisms. The elements in this generating set are in fact a subset of those elements of  $\mathcal{H}_n$  constructed from automorphisms of folded automata that are considered here.

Let  $G = (V, E, \iota, \tau)$  be a directed graph where  $V$  is the set of vertices of  $G$ ,  $E$  is its set of edges,  $\iota : E \rightarrow V$  is a map which returns the origin of an edge, and  $\tau$  is a map that returns the terminus of an edge. An automorphism of  $G$  is a map  $\phi := (\phi_V, \phi_E)$  such that:

- (a)  $\phi_V : V \rightarrow V$  is a bijection,
- (b)  $\phi_E : E \rightarrow E$  is a bijection, and,
- (c) for an edge  $e \in E$ ,  $((e)\iota)\phi_V = ((e)\phi_E)\iota$  and  $((e)\tau)\phi_V = ((e)\phi_E)\tau$ .

In general usage, we shall suppress subscripts in the maps  $\phi_E$  and  $\phi_V$ , the arguments determining which is meant in each case. Thus for an edge  $e$  we write  $(e)\phi$  for  $(e)\phi_E$  and  $((e)\iota)\phi$  for  $((e)\iota)\phi_V$ .

Let  $A$  be a folded automaton arising from a folding of a de Bruijn graph and let  $\phi$  be an automorphism of the directed graph  $G_A$  corresponding to  $A$ . Let  $H(A, \phi)$  be a transducer with state set  $Q_{H(A, \phi)} := Q_A$  transition function  $\pi_{H(A, \phi)} := \pi_A$  and output function  $\lambda_{H(A, \phi)} : X_n \times Q_{H(A, \phi)} \rightarrow X_n$  defined as follows. For  $x \in X_n$  and  $p \in Q_A$ , let  $q = \pi_A(x, p)$  so that  $(p, x, q)$  is an edge of  $G_A$ , let  $(r, y, s)$  be the image of  $(p, x, q)$  under  $\phi$ , noting that  $(p)\phi = r$  and  $(q)\phi = s$ , then set  $\lambda_{H(A, \phi)}(x, p) = y$ .

The transducer  $H(A, \phi)$  can be thought of as the result of gluing the automata  $A$  to itself along the map  $\phi : Q_A \rightarrow Q_A$ . That is, if  $p, q \in Q_A$  and  $(p, x, q)$  is an edge from  $p$  to  $q$  with label  $x$  in  $A$ , and if  $y$  is the label of the edge  $((p, x, q))\phi$  in  $A$ , then the vertex  $p$  is identified with the vertex  $(p)\phi$ , the vertex  $q$  with the vertex  $(q)\phi$ , the input label is  $x$  and the output label is the label  $y$ . Note that this fits in our view of a transducer as an ordered pair of automata where there is an isomorphism of the underlying graphs which associates to each edge of that graph a domain and range label.

We make a few observations:

- (a) For each state  $q \in Q_{H(A, \phi)}$ , the map  $\lambda_{H(A, \phi)}(\cdot, q) : X_n \rightarrow X_n$  is a bijection. This follows from the definition of  $G_A$ : for each  $x \in X_n$  there is precisely one edge of the form  $((q)\phi, x, p)$  based at the vertex  $(q)\phi$ . It follows that the transducer  $H(A, \phi)$  is invertible.
- (b) If  $A$  is synchronizing at level  $k$  (and so a folding of  $G(n, k)$  by Proposition 3.4) then both  $H(A, \phi)$  and  $H(A, \phi)^{-1}$  are synchronizing at level  $k$  hence the minimal  $H(A, \phi)$  representative of  $H(A, \phi)$  is an element of  $\mathcal{H}_n$ .
- (c) In fact, for a state  $q \in Q_A$ , if  $W_{k, q}$  is the set of words of length  $k$ , that force the state  $q$ , i.e.,

$$W_{k, q} := \{a \in X_n^k : \pi_{H(A, \phi)}(a, q) = q\},$$

then  $\{\lambda_{H(A, \phi)}(a, p) \mid a \in Q_{k, q}, p \in Q_{H(A, \phi)}\}$  is equal to  $W_{k, (q)\phi}$ .

(d) Let  $A(H(A, \phi)) = (X_n, \mathcal{Q}_{H(A, \phi)}, \pi_{H(A, \phi)})$  and

$$A(H(A, \phi)^{-1}) = (X_n, \mathcal{Q}_{H(A, \phi)^{-1}}, \pi_{H(A, \phi)^{-1}})$$

be the automata corresponding to  $H(A, \phi)$  and  $H(A, \phi)^{-1}$  when outputs are ignored. By construction  $A(H(A, \phi)) = A$ , and the previous two points indicate that  $A(H(A, \phi)^{-1})$  is also isomorphic as an automaton to  $A$  (by the map sending a state  $q^{-1}$  of  $H(A, \phi)^{-1}$  to the state  $(q)\phi$  of  $A$ ).

The third point above and results of the paper [18] show that an element of  $\mathcal{H}_n$  obtained from an automorphism of a folded automaton must have finite order. This result, which also follows from Theorem 4.2 below, means that not all elements of  $\mathcal{H}_n$  for  $n \geq 3$  arise from automorphisms of the directed graph underlying some folded automaton.

## 4.2 Automorphisms of folded automata and permutations of the alphabet.

Consider the de Bruijn graph  $G(n, m)$ . Any permutation  $\rho$  of the set  $X_n$  induces an automorphism, which we again denote by  $\rho$ , of  $G(n, m)$  as follows. A vertex  $a = a_1 a_2 \dots a_n$  of the graph  $G(n, m)$  is mapped to the vertex  $b = (a_1)\rho(a_2)\rho \dots (a_n)\rho := (a)\rho$ . An edge  $e = (a, x, b)$  is mapped to the edge  $((a)\rho, (x)\rho, (b)\rho)$ . In this case, the transducer  $H := H(G(n, m), \rho)$  arising from the pair  $(G(n, m), \rho)$  has the property that for any state  $q \in \mathcal{Q}_H$ , the bijection  $\lambda_H(\cdot, q) : X_n \rightarrow X_n$  is the permutation  $\rho$ . Therefore, the minimal transducer  $\bar{H}$  representing  $H$  has exactly one state, and this state induces the permutation  $\rho$  on the alphabet  $X_n$ . We show below that these are the only automorphisms of the automaton  $G(n, m)$ .

Let  $A$  be a folded automaton arising from a folding of  $G(n, m)$  and let  $\rho$ , as above, be a permutation of  $X_n$ . By the definition of a folding the individual states of  $A$  correspond to subsets of the vertices of  $G(n, m)$  and the set of states of  $A$  forms a partition of the vertices of  $G(n, m)$ . As vertices of  $G(n, m)$  are words of length  $m$  in  $X_n$ , we may define a map  $\phi_{V_A}$  on the vertices of  $G_A$  to the set of subsets of  $X_n^m$ , by mapping a vertex  $q$  to the set  $\{(a)\rho \mid a \in X_n^m \cap q\}$ . If the image of  $\phi_{V_A}$  in the set of subsets of  $X_n^m$  is again precisely the partition  $V_A$ , then we may define an edge map  $\phi_{E_A} : E_A \rightarrow E_A$  by mapping an edge  $(a, x, b)$  to the edge  $((a)\rho, (x)\rho, (b)\rho)$  and this will be well defined for the folding  $A$  by the definition of a folding. In this case, the map  $(\phi_{V_A}, \phi_{E_A})$  is an automorphism of  $G_A$  which we once again denote by  $\rho$ .

The example below indicates that, in general, not all automorphisms of the directed graph underlying a folded automaton arise from a permutation of the symbol set.

The automorphism group of the underlying directed graph of the automaton  $A$  in Figure 4 is the group  $S_3$  as all three vertices may be permuted and any permutation of the three vertices forces a bijection on the edges. The automaton  $A$  is a folded automaton arising from a folding of  $G(3, 2)$ ; the vertex  $q_0$  corresponds to the set  $\{00, 21, 10\}$ , the vertex  $q_1$  corresponds to the set  $\{01, 11, 20\}$  and the vertex  $q_2$  to the set  $\{02, 12, 22\}$ . The automorphism  $\phi$  which swaps the vertex  $q_0$  with  $q_2$  but fixes the vertex  $q_1$  is not induced by a permutation of the set  $X_3$ . (If  $\phi$  were induced by a permutation  $\rho$  of  $X_n$ , then  $\{(00)\rho, (21)\rho, (10)\rho\} = \{02, 12, 22\}$  and  $\{(01)\rho, (11)\rho, (20)\rho\} = \{01, 11, 20\}$ , which is not possible.)

The result below characterizes when an automorphism of the directed graph of a folded automaton is induced by a permutation of the alphabet set  $X_n$ .

**Proposition 4.1.** *Let  $A$  be a folded automaton arising from a folding of  $G(n, m)$ . An automorphism  $\phi$  of the graph  $G_A$  arises from a permutation  $\rho$  of the set  $X_n$  if and only if the minimal representative of the transducer  $H := H(A, \phi)$  has exactly one state, and this state induces the permutation  $\rho$  on  $X_n$ .*

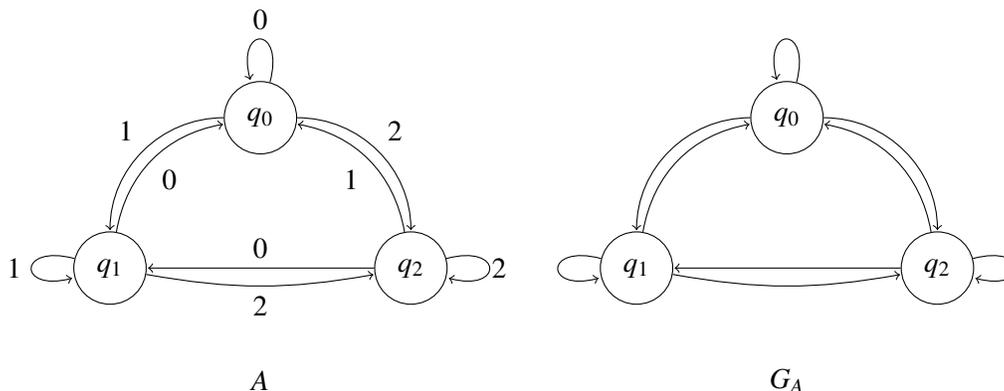


Figure 4: A folded automaton with an automorphism not induced by a permutation.

**Proof.** If the automorphism  $\phi$  arises from a permutation  $\rho$  of  $X_n$ , then as in the  $G(n, m)$  case, all state of the transducer  $H$  induce the permutation  $\rho$  on the set  $X_n$ . Therefore, the minimal representative  $\bar{H}$  of  $H$  has exactly one state, and this state induces the permutation  $\rho$  on  $X_n$ .

Therefore, suppose that the minimal representative  $\bar{H}$  of the transducer  $H = H(A, \phi)$  has exactly one state, and this state induces the permutation  $\rho$  on  $X_n$ . It must be the case that all states of  $H$  induce the permutation  $\rho$  on  $X_n$ . It follows that for an edge  $e = (p, x, q)$  of  $G_A$ ,  $(e)\phi = ((p)\phi, (x)\rho, (q)\phi)$ . Let  $q$  be state of  $H$ , then as, by definition,  $q$  is a state of  $A$   $q$  corresponds to a subset of  $X_n^m$ . In particular,  $q$  corresponds to the subset  $W_{m,q}$  of  $X_n^m$  consisting of all elements of  $X_n^m$  which force the state  $q$  when read from any state of  $A$ . Now as all states of  $H$  induce the permutation  $\rho$  on  $X_n$ , it follows that the state  $q^{-1}$  of the automaton  $H^{-1}$  corresponds to the subset  $\{(a)\rho \mid a \in W_{m,q}\}$ . Therefore as  $(q)\phi = q^{-1}$ , we see that  $\phi$  must arise from the permutation  $\rho$ .  $\square$

Returning to the automaton  $A$  in Figure 4, the automorphism  $\phi$  of  $G_A$  which swaps the vertices  $q_0$  and  $q_1$  yields the automaton  $(A)\phi$  and the transducer  $H(A, \phi)$  depicted in Figure 5. The transducer  $H(A, \phi)$  is minimal.

**Theorem 4.2.** *Let  $A$  be a folded automaton arising from a folding of  $G(n, m)$  for  $m$  minimal. The map from the group  $\text{Aut}(G_A)$  of automorphisms of the directed graph  $G_A$  to  $\mathcal{H}_n$  which maps an automorphism  $\phi$  to the minimal representative of the transducer  $H(A, \phi)$ , is a monomorphism.*

**Proof.** If  $|A| = 1$  then the result is a consequence of Proposition 4.11. Thus we may assume that  $|A| > 1$ .

Let  $\phi$  be a non-trivial automorphism of  $G_A$ . Then as  $\phi$  is not trivial, either it moves some state or fixes every state and move some edges.

Suppose firstly that  $\phi$  moves some state. Let  $p, q \in Q_A$  be distinct states that  $(p)\phi = q$ . Since,  $A$  is a folding of  $G(n, m)$ ,  $p$  and  $q$  correspond to distinct subsets of  $X_n^m$  consisting of all words  $W_{m,p}$  and  $W_{m,q}$  that force the states  $p$  and  $q$  respectively. Now, by an observation above, the state  $p$  of  $H(A, \phi)$  is such that  $\lambda_{H(A, \phi)}(\cdot, p)$  induces a bijection from  $W_{m,p}$  to  $W_{m,q}$ . Therefore, we see that  $H(A, \phi)$  is not the identity transducer.

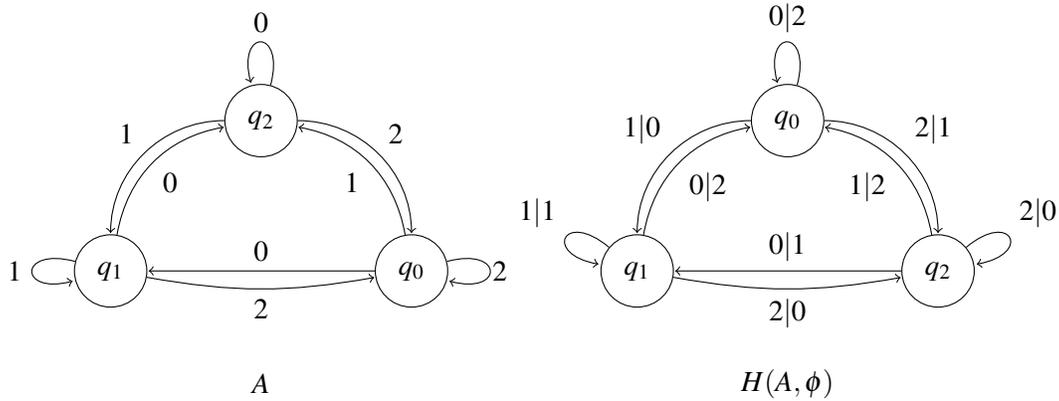


Figure 5: The transducer arising from the automorphism swapping vertices  $q_0$  and  $q_1$ .

In the case that  $\phi$  fixes every state and moves some edges, let  $e = (p, x, q)$  be an edge move by  $\phi$ . Since  $\phi$  fixes all vertices, there must be an edge  $(p, y, q)$  from  $p$  to  $q$ , for  $x \neq y$  such that  $((p, x, q))\phi = (p, y, q)$ . In this case, we have that the state  $p$  of  $H(A, \phi)$  satisfies  $\lambda_A(x, p) = y$ . We once again conclude that  $H(A, \phi)$  is not the identity transducer.

Therefore, the only element of  $\text{Aut}(G_A)$  that maps to the identity transducer, is the identity element. This means that it suffices to show that the map from  $\text{Aut}(G_A) \rightarrow \mathcal{T}_n$  which sends an automorphism  $\phi$  to the minimal representative of  $H(A, \phi)$  is a homomorphism to conclude that it is a monomorphism.

Let  $\phi, \psi$  be two automorphisms of  $G_A$  and let  $H(A, \phi)$  and  $H(A, \psi)$  be the corresponding transducers. Notice that the trio  $H(A, \phi)$ ,  $H(A, \psi)$  and  $H(A, \phi\psi)$ , all by definition, have state set  $Q_A$ . This should not cause confusion below, as whenever we write a pair  $(p, q)$   $H(A, \phi) * H(A, \psi)$ , the first coordinate corresponds to the state of  $H(A, \phi)$  and the second to the state of  $H(A, \psi)$  and for a single state  $p \in Q_A$  it will be clear below which of the three transducers  $H(A, \phi)$ ,  $H(A, \psi)$  and  $H(A, \phi\psi)$  it is being regarded as a state of. On the other hand, the set  $W_{m,q}$  for a state  $q \in Q_A$ , depends only on the automaton  $A$ . That is the set of words in  $X_n^m$  which force the state  $q$  in  $H(A, \phi)$ ,  $H(A, \psi)$  or  $H(A, \phi\psi)$  are all equal to  $W_{m,q}$ .

A state  $(p, q)$  of the product  $H(A, \phi) * H(A, \psi)$  is a state of the core if and only if  $\{a \in X_n^m \mid a = \lambda_{H(A,\phi)}(b, q) \text{ for some } b \in W_{m,p}, q \in Q_A\} = W_{m,(p)}$ . This is because, by an observation above,

$$\{a \in X_n^m \mid a = \lambda_{H(A,\phi)}(b, q) \text{ for some } b \in W_{m,p}, q \in Q_A\} = W_{m,(p)\phi}$$

and this set depends only on  $A$ . Thus a state  $(p, q)$  is a state of the core( $H(A, \phi) * H(A, \psi)$ ) if and only if it is of the form  $(p, (p)\phi)$ .

Let  $(p, x, q)$  be an edge of  $G_A$ ,  $((p)\phi, y, (q)\phi)$  be its image under  $\phi$  and  $((p)\phi\psi, z, (q)\phi\psi)$  its image under  $\phi\psi$ . This means that the state  $p$  of  $H(A, \phi)$  satisfies,  $\lambda_{H(A,\phi)}(x, p) = y$  and  $\pi_{H(A,\phi)}(x, p) = q$ . The state  $(p)\phi$  of  $H(A, \psi)$  satisfies,  $\lambda_{H(A,\psi)}(y, (p)\phi) = z$  and  $\pi_{H(A,\psi)}(y, (p)\phi) = (q)\phi$ . Thus

$$\lambda_{H(A,\phi\psi)}(x, (p, (p)\phi)) = z$$

and

$$\pi_{H(A,\phi\psi)}(x, (p, (p)\phi)) = (q, (q)\phi).$$

The above calculation demonstrates that the map from  $H(A, \phi \psi)$  to  $\text{core}(H(A, \phi) * H(A, \psi))$  which sends a state  $p$  of  $H(A, \phi \psi)$  to the state  $(p, (p)\phi)$  of  $\text{core}(H(A, \phi) * H(A, \psi))$  is an automaton isomorphism. This concludes the proof.  $\square$

### 4.3 Finite subgroups of $\mathcal{H}_n$

We observe that a converse of Theorem 4.2 is valid, namely, every finite subgroup of  $\mathcal{H}_n \cong \text{Aut}(X_n^{\mathbb{N}}, \sigma_n)$  arises from the automorphism group of a folded de Bruijn graph. This follows from work in the paper [8], however we give a proof below.

The other construction we require is the *dual automaton* (see [1, 17]).

Let  $T$  be a transducer over the alphabet  $X_n$ . Set  $T^\vee = \langle Q_T, X_n, \pi_T^\vee, \lambda_T^\vee \rangle$ , that is the state set of  $T^\vee$  is the set  $X_n$ , the alphabet of  $T^\vee$  is the state set  $Q_T$  of  $T$ , and the transition  $\pi_T^\vee$  and output functions  $\lambda_T^\vee$  are defined as follows. For  $q \in Q_T$  and  $x \in X_n$ ,  $\pi_T^\vee(q, x) = y$  and  $\lambda_T^\vee(q, x) = p$  if and only if  $\pi_T(x, q) = p$  and  $\lambda_T(x, q) = y$ .

One can easily check the following lemma.

**Lemma 4.3.** *Let  $T$  be a synchronous transducer over alphabet  $X_n$ . For positive natural  $m$ , we have  $(T^\vee)^m = T(m)^\vee$ .*

Note that to lighten our notation below, we may use the notation  $T_m^\vee$  for the transducer  $T(m)^\vee$ .

Also observe that  $T^{-1\vee}$  is obtained from  $T^\vee$  by ‘reversing the arrows’. That is if,  $x, y \in X_n$ ,  $q, p \in Q_T$  are such that  $\pi_T^\vee(q, x) = y$  and  $\lambda_T^\vee(q, x) = p$ , then  $\pi_{T^{-1}}^\vee(q^{-1}, y) = x$  and  $\lambda_{T^{-1}}^\vee(q^{-1}, y) = p^{-1}$ .

The proof we give below is more automata theoretic and is based on the following result from [18].

**Proposition 4.4.** *Let  $G \leq \mathcal{H}_n$  be a finite subgroup. Let  $k \in \mathbb{N}$  the largest minimal synchronizing level of any element of  $G$ . Then for any  $H \in G$ , and for any word  $\Gamma \in X_n^k$ , there is a word  $W(\Gamma, H) \in Q_H^+$  such that for any word  $P \in Q_H^+$ ,  $\pi_H^\vee(P, \Gamma) = W(\Gamma, H)^i \overline{W(\Gamma, H)}_r$ , where,  $i \in \mathbb{N}$ , satisfies,  $|P| = i|W(\Gamma, H)| + r$ , for  $1 \leq r < |W(\Gamma, H)|$  and  $W(\Gamma, H)_r$  is the length  $r$  prefix of  $W(\Gamma, H)$ .*

**Theorem 4.5.** *Let  $G \leq \mathcal{H}_n$  be a finite subgroup, then  $G$  is isomorphic to a subgroup of the automorphism group of the underlying digraph of a strongly synchronizing automaton  $A(G)$ . Moreover, every element of  $G$  is the minimal representative of a transducer  $H(A(G), \phi)$  for an automorphism  $\phi$  of the underlying di-graph of  $A(G)$ .*

**Proof.** Let  $k \in \mathbb{N}$  be the such that any element of  $G$  has minimal synchronizing level at most  $k$ . Define an equivalence relation  $\sim$  on  $X_n^k$  as follows:  $\Gamma \sim \Delta$  if and only if  $W(\Gamma, H) = W(\Delta, H)$  for all  $H \in G$ .

Observe that, for  $\Gamma = a\gamma$  and  $\Delta = d\delta$ , for  $a, d \in X_n$ , in the same equivalence class, then for  $x \in X_n$ ,  $\gamma x$  and  $\delta x$  are also in the same equivalence class. This is because for any  $H \in G$  and any word  $P \in Q_H^+$  we have,  $\lambda_{H^{|P|}}(a\gamma, P) = \lambda_{H^{|P|}}(a\delta, P)$ , and so  $\lambda_{H^{|P|}}(a\gamma x, P) = \lambda_{H^{|P|}}(a\delta x, P)$ . From this we deduce that  $W(\gamma x, H) = W(\delta x, H)$ .

Thus, writing  $[\gamma]$  for the equivalence class of an element  $\gamma$  of  $X_n^k$ , we may form an automaton  $A(G)$  with state set  $X_n^k / \sim$ , and transitions  $\pi_{A(G)}(x, [\gamma]) = [\bar{\gamma}x]$  where  $\bar{\gamma}$  is the length  $|\gamma| - 1$  suffix of  $\gamma$ . By the previous a paragraph the automaton  $A(G)$  is well defined; by construction the automaton  $A(G)$  is strongly synchronizing.

We now show that  $G$  acts by automorphisms on the underlying digraph of  $A(G)$ .

We begin by proving the following observation. Let  $\gamma, \delta \in X_n^k$  belong to the same equivalence class, and let  $H \in G$  be arbitrary. Then for any  $p, q \in Q_H$ , the elements of the set  $\{\lambda_H(\xi, t) \mid (\xi, t) \in \{(\gamma, p), (\delta, q)\}\}$  belong to the same equivalence class.

First observe that by Proposition 4.4, there is a word  $W_H \in Q_H^+$  such that  $W_H = W(\lambda_H(\xi, t), H)$  for all  $(\xi, t) \in \{(\gamma, p), (\delta, q)\}$ . Since  $\gamma$  and  $\delta$  are in the same equivalence class, let  $s_0$  be the state of  $H$  forced by both  $\gamma$  and  $\delta$ . Let  $I \in G, I \neq H$  be arbitrary, we show that there is a word  $W_I \in Q_I^+$  such that  $W_I = W(\lambda_H(\xi, t), I)$  for all  $\xi \in \{\gamma, \delta\}$  and all  $t \in \{p, q\}$ . We prove this inductively.

Let us establish the base case. Observe that since  $HI \in G$  and since  $\gamma$  and  $\delta$  are in the same equivalence class, there is a unique state,  $s_1$  of  $HI$  such that for any state  $s \in Q_{HI}$ , the state of  $HI$  forced by  $\lambda_{HI}(\gamma, s)$  and  $\lambda_{HI}(\delta, s)$  are equal and are equal to  $s_1$ . Notice that  $HI$  is the minimal representative of  $\text{core}(H * I)$ . There are state  $s, s' \in I$  such that  $(p, s), (q, s')$  are states of  $\text{core}(H * I)$ ; let  $t, t' \in Q_I$  be such that  $\pi_{H*I}(\gamma, (p, s)) = (s_0, t)$  and  $\pi_{H*I}(\delta, (q, s')) = (s_0, t')$ . Since the state of  $HI$  forced by  $\gamma$  and  $\delta$  is  $s_1$ , we have  $(s_0, t)$  and  $(s_0, t')$  are  $\omega$ -equivalent to the state  $s_1$ , and so  $t = t'$ . Set  $t_1 = t = t'$ . Therefore we have shown that the state of  $I$  forced by  $\lambda_H(\gamma, p)$  is equal to the state of  $I$  forced by  $\lambda_H(\delta, q)$  and that state is  $t_1$ .

Inductively assume that there is an  $m \in \mathbb{N}$  such that for any word  $u \in Q_I^+$  of length  $m$ ,  $\pi_{I^m}(\lambda_H(\gamma, p), u) = \pi_{I^m}(\lambda_H(\delta, q), u) = t_1 t_2 \dots t_m$ . We now prove the inductive step.

As before,  $HI^{m+1}$  is an element of  $G$  and, as  $\gamma$  and  $\delta$  are in the same equivalence class, they both force the same state  $s_{m+1}$  of  $HI^{m+1}$ . There are words  $s, s' \in Q_I^{m+1}$  such that  $ps$  and  $qs'$  are states of  $\text{core}(H * \underbrace{I * I \dots * I}_{m+1 \text{ times}})$ . Since  $HI^{m+1}$  is the minimal representative of  $\text{core}(H * \underbrace{I * I \dots * I}_{m+1 \text{ times}})$ , it follows that if  $T_{m+1}, T'_{m+1} \in Q_I^{m+1}$  satisfy,  $\pi_{H*I}(\gamma, ps) = s_0 T_{m+1}$  and  $\pi_{H*I}(\delta, qs') = s_0 T'_{m+1}$ , then  $s_0 T_{m+1}$  and  $s_0 T'_{m+1}$  are both  $\omega$ -equivalent to the state  $s_{m+1}$  of  $HI^{m+1}$ . By the inductive assumption, we have that that the first  $m$  letters of  $T_{m+1}$  and  $T'_{m+1}$  coincide, the preceding sentence now implies that  $T_{m+1} = T'_{m+1}$ . Set  $t_{m+1}$  to the final letter of  $T_{m+1} = T'_{m+1}$ . By Proposition 4.4 it now follows that for any word for any word  $u \in Q_I^+$  of length  $m + 1$ ,  $\pi_{I^{m+1}}(\lambda_H(\gamma, p), u) = \pi_{I^{m+1}}(\lambda_H(\delta, q), u) = t_1 t_2 \dots t_m t_{m+1}$ . We therefore conclude that there is a word  $W_I \in Q_I^+$  such that  $W_I = W(\lambda_H(\xi, t), I)$  for all  $\xi \in \{\gamma, \delta\}$  and all  $t \in \{p, q\}$ .

Since  $I \in G, I \neq H$ , was chosen arbitrarily, it follows that  $\lambda_H(\gamma, p)$  and  $\lambda_H(\delta, q)$  are in the same equivalence class.

Let  $[\gamma]$  be a vertex of  $A(G)$ , let  $\bar{\gamma}$  be the length  $k - 1$  suffix of  $\gamma$  and let  $x \in X_n$  be the label of the edge from  $[\gamma]$  to  $[\bar{\gamma}x]$ . Let  $H \in G$  be arbitrary and let  $y = \lambda_H(x, q_\gamma)$ , then by the preceding paragraph for any pair of states  $p, q \in Q_H$  and any  $I \in G, W(\lambda_H(\gamma, p)y, I) = W(\lambda_H(\gamma, q)y, I)$ . From this it follows that setting  $\mu, \nu$  to be the length  $k - 1$  suffices of  $\lambda_H(\gamma, p)$  and  $\lambda_H(\gamma, q)$  respectively,  $[\mu y] = [\nu y]$ . Now as there is a state  $s$  of  $H$  such that  $\lambda_H(\bar{\gamma}x, s) = \mu y$ , it follows, by the preceding paragraphs once more, that for any state  $t \in Q_H, [\lambda_H(\bar{\gamma}x, t)] = [\mu y]$ . Since  $\mu$  is a length  $k - 1$  suffix of an element of  $[\lambda_H(\gamma, p)]$ , there is an edge labeled  $y$  from  $[\lambda_H(\gamma, p)]$  to  $[\mu y]$ .

For  $H \in G$ , define a map  $\phi_H$  as follows. For a vertex  $[\gamma]$ , and edge labeled  $x$  from  $[\gamma]$  to  $[\bar{\gamma}x]$  of the digraph  $A(G)$  (where  $\bar{\gamma}$  is the length  $k - 1$  suffix of  $\gamma$ ) of  $A(G)$ ,  $([\gamma])\phi_H = [\lambda_H(\gamma, p)], ([\bar{\gamma}x])\phi_H = [\lambda_H(\bar{\gamma}x, p)]$ , for some state  $p \in Q_H$ , and the edge  $x$  maps to the edge labeled  $\lambda_H(x, q_\gamma)$  from the state  $[\lambda_H(\gamma, p)]$  to the state  $[\lambda_H(\bar{\gamma}x, p)]$ . By the preceding paragraphs this map is well defined. It is easily verified that for  $H, I \in G, \phi_{HI} = \phi_H \phi_I$ . Thus the map  $H \mapsto \phi_H$  is an embedding of  $G$  into the automorphism group of the underlying digraph of  $A(G)$ . Moreover, it is not hard to see that the minimal representative of the

transducer  $H(A(G), \phi_H)$  is  $H$ . □

In light of Theorem 4.2 above, Theorem 3.8 of [8] can be states as follows:

**Corollary 4.6.** *Let  $A$  be a folded automaton arising from a folding of  $G(n, m)$  for  $m$  minimal. For the group  $\text{Aut}(G_A)$  of automorphisms of the directed graph  $G_A$ , one of the following holds:*

- (i)  $\text{Aut}(G_A)$  isomorphic to a subgroup of  $\text{Sym}(X_n)$  that has a composition factor that cannot be embedded in  $\text{Sym}(X_{n-1})$ . In this case all automorphisms of  $G_A$  arise as permutations of the symbol set  $X_n$ .
- (ii) All the composition factors of  $\text{Aut}(G_A)$  are isomorphic to subgroups of  $\text{Sym}(X_{n-1})$ .

**Corollary 4.7.** *Let  $A$  be a folded automaton arising from a folding of  $G(3, m)$  for some  $m \in \mathbb{N}$ . The group  $\text{Aut}(G_A)$  is either  $\text{Sym}(X_3)$  or a 2-group.*

It is a result of Hedlund [14] that  $\text{Aut}(X_2, \sigma_2)$  is isomorphic to the cyclic group of order 2. Below we give a new proof of this result by identifying conditions on (non-minimal) strongly synchronizing transducers to have a minimal representative in  $\mathcal{H}_n$  with exactly one state. From this we also derive implications (via Proposition 4.1) for folded automata: more precisely we show that certain folded automata, including the graphs  $G(n, m)$ , admit only automorphisms arising from permutations of the symbol set  $X_n$ .

#### 4.4 Synchronizing sequences

We require an algorithm given in [5] for detecting when an automaton is strongly synchronizing. We state a version below.

Let  $A = (X_n, Q_A, \pi_A)$  be an automaton. Define an equivalence relation  $\sim_A$  on the states of  $A$  by  $p \sim_A q$  if and only if the maps  $\pi_A(\cdot, p) : Q_A \rightarrow Q_A$  and  $\pi_A(\cdot, q) : Q_A \rightarrow Q_A$  are equal. For a state  $q \in Q_A$  let  $\mathfrak{q}$  represent the equivalence class of  $q$  under  $\sim_A$ . Further set  $Q_A := \{\mathfrak{q} \mid q \in Q_A\}$  and let  $\pi_A : Q_A \rightarrow Q_A$  be defined by  $\pi_A(x, \mathfrak{q}) = \mathfrak{p}$  where  $p = \pi_A(x, q)$ . Observe that  $\pi_A$  is a well defined map. Define a new automaton  $A = (X_n, Q_A, \pi_A)$  noting that  $|Q_A| \leq |Q_A|$  and  $|Q_A| = |Q_A|$  implies that  $A$  is isomorphic to  $A$ .

Given an automaton  $A$ , let  $A_0 := A, A_1, A_2, \dots$  be the sequence of automata such that  $A_i = A_{i-1}$  for all  $i \geq 1$ . We call the sequence  $(A_i)_{i \in \mathbb{N}}$  the *synchronizing sequence* of  $A$ . We make a few observations.

By definition each term in the synchronizing sequence is a folding of the automaton which precedes it, therefore there is a  $j \in \mathbb{N}$  such that all the  $A_i$  for  $i \geq j$  are isomorphic to one another. By a simple induction argument, for each  $i$ , the states of  $A_i$  corresponds to a partition of  $Q_A$ . We identify the states of  $A_i$  with this partition. For two states  $q, p \in Q_A$  that belong to a state  $P$  of  $A_i$ ,  $\pi_A(x, q)$  and  $\pi_A(x, p)$  belong to the same state of  $Q_A$  for all  $x \in X_n$ . We will use the language ‘two states of  $A$  are identified at level  $i$ ’ if the two named states belong to the same element of  $Q_{A_i}$ .

If the automaton  $A$  is strongly synchronizing and core, then an easy induction argument shows that all the terms in its synchronizing sequence are core and strongly synchronizing as well (since they are all foldings of  $A$ ). For example if  $A = G(n, m)$ , then the first  $m$  terms of the synchronizing sequence of  $A$  are  $(G(n, m), G(n, m - 1), G(n, m - 2), \dots, G(n, 1))$ , after this all the terms in the sequence are the single state automaton on  $X_n$ .

The result below is from [5].

**Theorem 4.8.** *Let  $A$  be an automaton and  $A_0 := A, A_1, A_2, \dots$  be the sequence of automata such that  $A_i = A_{i-1}$  for all  $i > 1$ . Then*

- (a) *a pair of states  $p, q \in Q_A$ , belong to the same element  $t \in Q_{A_i}$  if and only if for all words  $a \in X_n^i$ ,  $\pi_A(a, p) = \pi_A(a, q)$ , and*
- (b)  *$A$  is strongly synchronizing if and only if there is a  $j \in \mathbb{N}$  such that  $|Q_{A_j}| = 1$ . The minimal  $j$  for which  $|A_j| = 1$  is the minimal synchronizing level of  $A$ .*

#### 4.5 Applying synchronizing sequences to understand automorphisms of de Bruijn graphs

**Lemma 4.9.** *Let  $A$  be a core strongly synchronizing automaton,  $A_0 := A, A_1, \dots$  be its synchronizing sequence and  $j \in \mathbb{N}$  be minimal such that  $A_j = 1$ . If  $A_{j-1}$  is isomorphic as an automaton to  $G(n, 1)$  then the sets  $Q_{A,x} := \{\pi_A(x, p) \mid p \in Q_A\}$  for  $x \in X_n$  form a partition of the set  $Q_A$  the states of  $A$ .*

**Proof.** This follows from the identification of the states of  $A_i$  with partitions of states of  $A$ . For if there were distinct  $x, y \in X_n$  and states  $p_1, p_2 \in Q_A$  such that  $\pi_A(x, p_1) = \pi_A(y, p_2)$ , then the states  $P_1$  and  $P_2$  of  $A_{j-1}$  containing  $p_1$  and  $p_2$  respectively satisfy,  $\pi_{A_i}(x, P_1) = \pi_{A_i}(y, P_2)$ . However, since  $A_{j-1}$  is isomorphic as an automaton to  $G(n, 1)$  this is not possible ( $A_{j-1}$  has  $n$  distinct states, is synchronizing at level 1 and core).  $\square$

A consequence of Lemma 4.9 is the following result.

**Lemma 4.10.** *There is no minimal, core, invertible transducer  $T$  which is bi-synchronizing at minimal level  $(j, k)$  and satisfies the following: if  $A$  and  $B$  are the automata obtained from  $T$  and  $T^{-1}$  respectively by forgetting outputs, then the terms  $A_{j-1}$  and  $B_{k-1}$  in the synchronizing sequences of  $A$  and  $B$  are isomorphic to  $G(n, 1)$ .*

**Proof.** Since  $T$  is minimal and strongly synchronizing, there is a pair  $p, q \in Q_T$  and  $x \in X_n$  such that  $\pi_T(x, p) = \pi_T(x, q)$  but  $y := \lambda_T(x, p) \neq \lambda_T(x, q) =: z$ . However, we therefore have that in  $T^{-1}$ , and so in  $B$ ,  $\pi_{T^{-1}}(y, p^{-1}) = \pi_{T^{-1}}(z, q^{-1})$  with  $z \neq q$ . This contradicts Lemma 4.9.  $\square$

We note the lack of the minimality hypothesis in the statement of the proposition below. We require the non-minimality hypothesis in order to deduce results about elements of  $\mathcal{H}_n$  arising from automorphisms of de Bruijn graphs  $G(n, m)$ . In particular as a consequence of the following Proposition, we show that  $\text{Aut}(G_{n,m})$  is isomorphic to the symmetric group on  $n$  symbols.

**Proposition 4.11.** *Let  $T$  be a core, invertible bi-synchronizing transducer of size at least 2 with automata theoretic inverse  $T^{-1}$ . Let  $(j, k)$  be the minimal bi-synchronizing level of  $T$ , and let  $A$  and  $B$  be the automata obtained from  $T$  and  $T^{-1}$  respectively by forgetting outputs. Suppose that the terms  $A_{j-1}$  and  $B_{k-1}$  in the synchronizing sequence  $(A_i)_{i \in \mathbb{N}}$  and  $(B_i)_{i \in \mathbb{N}}$  of  $A$  and  $B$  are both isomorphic, as automata, to  $G(n, 1)$ . Then  $j = k$  and the minimal transducer representing  $T$  has only one state.*

**Proof.** We proceed by induction on the number of states of  $T$ .

Note that as  $j, k \geq 1$ , it follows that the base case occurs when  $|T| = n$ . In this case, both  $A$  and  $B$  are isomorphic to  $G(n, 1)$  and  $j = k = 1$ . If all the states of  $T$  induce the same permutation  $\phi$  on the set  $X_n$ ,

then the minimal transducer representing  $T$  has one state, and that state also induces the permutation  $\rho$  on  $X_n$ . Therefore, suppose there are two states  $p, q \in Q_T$  and  $x \in X_n$  such that  $t := \lambda_T(x, p) \neq \lambda_T(x, q) =: z$ . Since  $\pi_T(x, p) = \pi_T(x, q)$ , it follows that in  $T^{-1}$ , the state  $p^{-1}, q^{-1}$  satisfy,  $\pi_{T^{-1}}(t, p^{-1}) = \pi_{T^{-1}}(z, q^{-1})$ . This yields the desired contradiction by Lemma 4.9, since  $B$  is isomorphic to  $G(n, 1)$ .

Now suppose the conclusion of the proposition holds for all transducers  $T$  with  $n \leq |T| < m$  and which satisfy the hypothesis of the proposition.

Let  $T$  be a transducer with size  $|T| = m$  satisfying the hypothesis. Let  $(j, k)$  be the minimal bi-synchronizing level of  $T$ . Since  $|T| > n$ , it follows that both  $j$  and  $k$  are strictly greater than 1. As, because  $T$  is core, if  $j$  or  $k$  were 1,  $T$  or  $T^{-1}$  would be a folding of  $G(n, 1)$  and so,  $T$  and  $T^{-1}$  would have size less than or equal to  $n$ .

Let  $A$  and  $B$  the automata obtained from  $T$  and  $T^{-1}$  respectively by forgetting outputs and let  $(A_i)_{i \in \mathbb{N}}$  and  $(B_i)_{i \in \mathbb{N}}$  be their respective synchronizing sequences.

Let  $p, q \in Q_T$  be any pair of states satisfying  $\pi_T(x, p) = \pi_T(x, q)$  for all  $x \in X_n$ . Then, by the argument given in the base case, we must also have  $\lambda_T(x, p) = \lambda_T(x, q)$  for all  $x \in X_n$ , otherwise we obtain the contradiction that  $T$  does not satisfy the hypothesis of the proposition. By the same argument, if  $p^{-1}, q^{-1} \in Q_{T^{-1}}$  are any pair of states satisfying  $\pi_{T^{-1}}(x, p^{-1}) = \pi_{T^{-1}}(x, q^{-1})$  for all  $x \in X_n$ , then  $\lambda_{T^{-1}}(x, p^{-1}) = \lambda_{T^{-1}}(x, q^{-1})$  for all  $x \in X_n$  as well.

Let  $\sim$  be the equivalence relation on the states of  $T$  given by  $p \sim q$  if  $\pi_T(x, p) = \pi_T(x, q)$  for all  $x \in X_n$ . By an abuse of notation we also use  $\sim$  for the same equivalence relation on the states of  $T^{-1}$ . For  $q \in Q_T$ , let  $q$  be its equivalence class and let  $Q_T := \{q \mid q \in Q_T\}$ . Notice that, by the preceding paragraph, for states  $p, q \in Q_T$ ,  $p \sim q$  if and only if  $\pi_T(\cdot, p) = \pi_T(\cdot, q)$  and  $\lambda_T(\cdot, p) = \lambda_T(\cdot, q)$  if and only if  $p^{-1} \sim q^{-1}$ . Moreover, by hypothesis,  $\sim$  is not the trivial equivalence relation i.e its equivalence classes do not all consist of singleton sets and it also does not consist of one equivalence class.

Form a new transducer  $T$  as follows. Let  $Q_T := Q_T$ . Define the transition function  $\pi_T : X_n \times Q_T \rightarrow Q_T$  by  $\pi_T(x, q) = p$  where  $p = \pi_T(x, q)$  for some  $q \in q$ . The output function  $\lambda_T : X_n \times Q_T \rightarrow X_n$  is defined by  $\lambda_T(x, q) = \lambda_T(x, q)$  for some  $q \in q$ . The preceding paragraph implies that  $T$  is well-defined.

Observe, that if  $C$  is the automaton obtained from  $T$  by forgetting outputs and  $D$  is the automaton obtained from  $T^{-1}$  by forgetting outputs, then  $C$  is isomorphic to  $A_1$  and  $D$  is isomorphic to  $B_1$ , by definition of the synchronizing sequence. This means that the minimal bi-synchronizing level of  $T$  is  $(j - 1, k - 1)$ . Moreover, as  $k - 1$  and  $j - 1$  are at least 1, in the synchronizing sequence of  $C$  and  $D$ , the terms  $C_{k-2}$  and  $D_{k-2}$  are isomorphic to  $G(n, 1)$ . This means that  $T$  satisfies the hypothesis of the proposition. Furthermore, as  $\sim$  is not the trivial relation, we have  $|T| < |T|$ . Thus, we conclude that the minimal transducer representing  $T$  has only one state and  $j - 1 = k - 1$ . However, by construction of  $T$ , the minimal transducer representing  $T$  is also the minimal transducer representing  $T$ . This concludes the proof.  $\square$

We have some corollaries of the result above.

**Corollary 4.12.** *Let  $A$  be a folded automaton arising from a folding of  $G(n, m)$ . If an element of the synchronizing sequence of  $A$  is isomorphic to  $G(n, 1)$ , then any automorphism of  $G_A$  is induced by a permutation of the symbol set  $X_n$ .*

**Proof.** Let  $\phi$  be any automorphism of  $G_A$ , and let  $H := H(A, \phi)$ . Let  $A(H)$  and  $A(H^{-1})$  be the automata obtained from  $H$  and  $H^{-1}$  by forgetting outputs. Note that since  $A(H)$  and  $A(H^{-1})$  are isomorphic as

automata to  $A$ , it follows that  $H$  satisfies the hypothesis of Proposition 4.11. This means that the minimal representative of  $H$  has exactly one state. Proposition 4.1 now implies that  $\phi$  is induced by a permutation of the symbol set  $X_n$ .  $\square$

**Corollary 4.13.** *Let  $A$  be the de Bruijn automaton  $G(n, m)$ . Then  $\text{Aut}(G_A)$  is isomorphic to the symmetric group on  $n$  points.*

**Proof.**  $G(n, m)$  is clearly a folding of itself, thus Corollary 4.12 implies that the automorphism group of its underlying directed graph is isomorphic to a subgroup of the symmetric group on  $n$  points. However, we have seen above that any permutation of  $X_n$  induces an automorphism of  $G(n, m)$ .  $\square$

The corollaries of Proposition 4.11 below require the following straight-forward lemma.

**Lemma 4.14.** *Let  $A$  be any strongly synchronizing, core automaton over the 2-letter alphabet. Let  $(A_i)_{i \in \mathbb{N}}$  be the synchronizing sequence of  $A$ . if  $|A| > 1$ , then the minimal synchronizing level  $k$  of  $A$  is at least 1 and  $A_{k-1}$  is isomorphic to  $G(2, 1)$ .*

**Proof.** If  $|A| > 1$  then it is not the single state automaton (which is the only automaton strongly synchronizing at level 0). Thus let  $k \geq 1$  be the minimal synchronizing level of  $A$ . Now, since  $A$  is core, it follows that the automaton  $A_{k-1}$  is isomorphic to  $G(2, 1)$ . This is because the only core, level 1 synchronizing automaton over the 2 letter alphabet is  $G(2, 1)$ .  $\square$

**Corollary 4.15.** *Let  $A$  be an folded automaton over the 2 letter alphabet, then  $\text{Aut}(G_A)$  is either trivial or the cyclic group of order 2. Moreover any automorphism of  $G_A$  is induced by a permutation of  $X_2$ .*

**Proof.** This is a direct consequence of Lemma 4.14 and Corollary 4.12.  $\square$

**Theorem 4.16.** *The group  $\mathcal{H}_2$  is isomorphic to the cyclic group of order 2.*

**Proof.** Let  $A$  be a minimal, core, bi-synchronizing transducer over the 2 letter alphabet. Suppose for a contradiction that  $|A| > 1$ . By Lemma 4.14,  $A$  satisfies the hypothesis of Proposition 4.11. However, this yields a contradiction as the size of  $A$  must then be 1.

Thus, every element of  $\mathcal{H}_2$  has exactly one state yielding the result.  $\square$

## 5 Decomposing elements of $\mathcal{H}_n$

In this section we give an algorithm for decomposing an arbitrary element of  $\mathcal{H}_n$  as a product of elements arising from automorphisms of the directed graphs underlying the folded automata arising from foldings of  $G(n, m)$ . Our method can be thought of as an interpretation of the approach in [8] in the language of strongly synchronizing automata. However, we are able to simplify that approach a great deal. In particular, we show that an element  $T \in \mathcal{H}_n$  of size  $l$  for some  $l \in \mathbb{N}$  can be written as a product of at most  $l$  elements of  $\mathcal{H}_n$  arising from automorphisms of directed graphs underlying foldings of the underlying automaton of  $A^{-1}$ . Note that an element  $T \in \mathcal{H}_n$  of size  $l$  is strongly synchronizing at level at most  $l - 1$ , thus  $f_T$  (by Remark 3.6) corresponds to a map  $f_\infty$  for some  $f \in F(X_n, l)$ . To decompose the element  $f_\infty$  using the approach given in [8], one would first have to construct a graph (isomorphic to the underlying graph of some folded automaton) with at least  $n^l$  vertices.

### 5.1 Collapsing chains and amalgamation

We introduce some terminology. Let  $A$  and  $B$  be automata. Then  $B$  is said to belong to a *collapse chain* of  $A$ , if there is a sequence

$$A = A_0, A_1, \dots, A_m = B$$

where, for  $i \geq 1$ ,  $A_i$  is obtained from  $A_{i-1}$  by identifying two states  $p, q \in Q_{A_{i-1}}$  such that  $\pi_{A_{i-1}}(\cdot, p) = \pi_{A_{i-1}}(\cdot, q)$ . We stress that each term in the sequence is obtained from the previous one by identifying exactly two states. Observe that if  $A$  is strongly synchronizing and  $B$  is an automaton which is in a collapse chain of  $A$ , then  $B$  is synchronizing at the minimal synchronizing level of  $A$ . More generally, let  $A$  and  $B$  be automaton with  $B$  in a collapse chain of  $A$ . Let  $(A_i)_{i \in \mathbb{N}}$  and  $(B_i)_{i \in \mathbb{N}}$  be the synchronizing sequences of  $A$  and  $B$  respectively, and suppose that  $k, l \in \mathbb{N}$  are minimal such that  $A_j = A_k$  for all  $j \geq k$  and  $B_j = B_l$  for all  $j \geq l$ , then  $A_k = B_l$ . This is a consequence of Theorem 4.8.

The following terminology, which is for the underlying graphs of an automaton, should be compared with the similarly named terminology in the paper [8] (recall the direction of edges will be reversed in our context). Let  $A$  and  $B$  be automata. Then  $G_B$  is called an *amalgamation* of  $G_A$  if there is a sequence  $G_A = G_0, G_1, \dots, G_m = G_B$  where, for  $i \geq 1$ ,  $G_i$  is obtained from  $G_{i-1}$  by identifying two vertices  $v_1$  and  $v_2$  of  $G_{i-1}$  having the property that for all vertices  $v$  of  $G_{i-1}$ , if there are precisely  $k$  outgoing edges from  $v_1$  to  $v$  (for some  $1 \leq k \leq n$ ) then there are also precisely  $k$  outgoing edges from  $v_2$  to  $v$ . That is, we replace the vertices  $v_1$  and  $v_2$  with a single vertex  $v_{1,2}$  and, for every vertex  $v$  of  $G_{i-1}$  if there are  $k$  edges from  $v_1$  to  $v$  (and hence, from  $v_2$  to  $v$ ), then there are  $k$  edges from  $v_{1,2}$  to  $v$  (and of course, we retain all other vertices and edges of  $G_{i-1}$ ). Also, if  $v$  is a vertex of  $G_{i-1}$  then there will be  $t$  edges in  $G_i$  from the vertex corresponding to  $v$  to  $v_{1,2}$  if the cardinality of the set of edges from  $v$  to  $v_1$  is  $r$  while the cardinality of the set of edges from  $v$  to  $v_2$  is  $s$ , where  $r + s = t$ . In particular, if there are  $m$  loops based at  $v_1$  and  $m'$  loops based at  $v_2$  in  $G_{i-1}$ , there are exactly  $m + m'$  loops based at  $v_{1,2}$  in  $G_i$ . In this context, the vertices  $v_1$  and  $v_2$  of  $G_{i-1}$  are called *amalgamable*.

Let  $T$  be an invertible transducer. Let  $A$  and  $B$  be the underlying automata of  $T$  and  $T^{-1}$  respectively. Let  $(B_i)_{i \in \mathbb{N}}$  be the synchronizing sequence of  $B$ . Then, by definition of the inverse transducer,  $G_{B_i}$  is an amalgamation of  $G_A$  for all  $i \in \mathbb{N}$ . The condition “for two states  $p^{-1}, q^{-1} \in Q_{T^{-1}}$ ,  $\pi_B(\cdot, p^{-1})$  and  $\pi_B(\cdot, q^{-1})$  are equal” is equivalent to the condition “the vertices  $p$  and  $q$  of  $G_A$  are amalgamable”. Further observe that for automata  $A$  and  $B$  with  $B$  in a collapse chain of  $A$ , the underlying directed graph of one is an amalgamation of the other.

### 5.2 Description of the decomposition algorithm

Here we give a short description of the algorithm for decomposing an element  $T$  of  $\mathcal{H}_n$  as a product of torsion elements as described in Theorem 1.1. The proof that our various steps can be carried out is given in full detail in Subsection 5.3. The algorithm allows the user some choices, so decomposition is not unique, but our upper bound on the decomposition length still holds.

We conclude with an example decomposition and statements of choices we made so the reader can verify by following the algorithm.

**A1** Let  $T_0 \in \mathcal{H}_n$ . Let  $A$  and  $B$  be the underlying automata of  $T_0$  and  $T_0^{-1}$  respectively.

**A2** If  $T_0$  has only one state, then it represents a permutation, and so there is a finite order single state transducer that we can multiply against  $T_0$  to produce the identity element (in this case, go to the final step of the algorithm with this finite order factor in hand). Otherwise, proceed to the next step.

**A3** Compute the synchronizing sequence  $(B_i)_{i \in \mathbb{N}}$  for  $B = B_0$ .

**A4** Compute the first step  $A_1$  of the synchronizing sequence of  $A = A_0$ .

**A5** Find a pair  $(p, q)$  of distinct states of  $A$  which belong to the same state of  $A_1$ .

**A6** Find the non-identity permutation  $\alpha$  of the output labels such that  $\lambda(\cdot, q) \circ \alpha : X_n \rightarrow X_n$  is precisely  $\lambda(\cdot, p) : X_n \rightarrow X_n$ . Determine the disjoint cycle decomposition of the permutation  $\alpha$ .

**A7** There is a smallest index  $i$  so that the state  $[q]$  of the automaton  $B_i$  has the following properties:

- The states  $[q]$  and  $[p]$  remain distinct states of  $B_i$ , and
- For all  $x, y \in X_n$  belonging to the same disjoint cycle in the cycle decomposition of  $\alpha$ , the edges labelled  $x$  and  $y$  from  $[q]$  are parallel edges.

Now determine the isomorphism  $\tau_\alpha$  of  $B_i$  which fixes all vertices and induces the permutation  $\alpha$  on the edges leaving  $[q]$ .)

**A8** Build the transducer  $H(B_i, \tau_\alpha)$ . This is a factor of finite order in a product sequence that will eventually trivialize  $T_0$ .

**A9** Compute the product  $R = \text{core}(T * H(B_i, \tau_\alpha))$ . This product has the same underlying graph as  $T$  but is not minimal. The states corresponding to  $p$  and  $q$  in this product are  $\omega$ -equivalent, and will be identified by minimizing the result  $R$  to produce a new element  $T_1$  with fewer states than  $T_0$ .

**A10** Repeat this process from the beginning, remembering the list of finite factors found so far.

**A11** The transducer  $T$  now factors as the product in reverse order of the inverses of the finite order factors found above.

We give an example. Consider the element  $T := H(A, \phi)$  from Figure 5. Working through the algorithm, with  $p = q_1$ , and  $q = q_0$  in the first instance, one obtains the following decomposition below (up to changing the final single state transducer; different choices for  $p$  and  $q$  in building the second factor result in different single-state third-factor transducers):

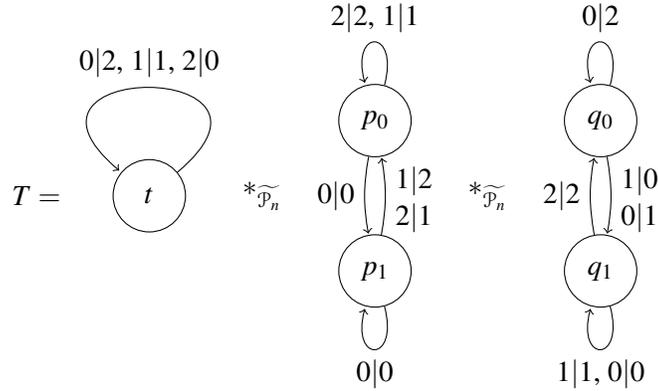


Figure 6: Decomposing an element of  $\mathcal{H}_3$  as a product of involutions.

### 5.3 Proof of Theorem 1.1

Here we prove that the algorithm above works.

Recall that  $\widetilde{\mathcal{H}}_n$  consist of those transducers which are strongly synchronizing and have an automata-theoretic inverse but which do not necessarily induce homeomorphisms of  $X_n^{\mathbb{Z}}$ . Further recall that for  $T, U \in \widetilde{\mathcal{P}}_n$  the product, in  $\mathcal{P}_n$ , of  $T$  and  $U$  is obtained by identifying the  $\omega$ -equivalent states of  $\text{core}(T * U)$ , write  $T *_{\widetilde{\mathcal{P}}_n} U$  for this transducer.

**Lemma 5.1.** *Let  $A$  be a minimal transducer in  $\mathcal{H}_n$ . Let  $B$  be the underlying automaton of  $A^{-1}$  and  $(B_i)_{i \in \mathbb{N}}$  be the synchronizing sequence of  $B$ . Let  $H \in \widetilde{\mathcal{H}}_n$  be any transducer such that the underlying automaton of  $H$  is  $B_j$  for some  $j \in \mathbb{N}$ . For a state  $p^{-1}$  of  $A^{-1}$  write  $[p^{-1}]$  for the state of  $B_j$  containing  $p^{-1}$ . Then*

- (a) *the set of states of  $\text{core}(A * H)$  is precisely the set  $\{(p, [p^{-1}]) \mid p \in Q_A\}$ . Consequently,*
- (b)  $|A *_{\widetilde{\mathcal{P}}_n} H| \leq |A|$ , *and,*
- (c) *the underlying automaton of  $A *_{\widetilde{\mathcal{P}}_n} H$  belongs to a collapse chain of the underlying automaton of  $A$ .*

**Proof.** Let  $p \in Q_A$  and  $x \in X_n$  and consider the transition  $\pi_{A * H}(x, (p, [p^{-1}]))$ . Let  $y = \lambda_A(x, p)$  and  $q = \pi_A(x, p)$ . Then, in  $A^{-1}$ , we have  $\pi_{A^{-1}}(y, p^{-1}) = q^{-1}$ , therefore, in  $B_j$ ,  $\pi_{B_j}(y, [p^{-1}]) = [q^{-1}]$ . Hence, we conclude that

$$\pi_{A * H}(x, (p, [p^{-1}])) = (q, [q^{-1}]).$$

To see that  $(p, [p^{-1}])$  is a state of  $\text{core}(A * H)$ , let  $\gamma \in X_n^+$  be a word such that  $\pi_A(\gamma, p) = p$ . The preceding paragraph now shows that  $\pi_{A * H}(\gamma, (p, [p^{-1}])) = (p, [p^{-1}])$ .

Thus we see that  $|\text{core}(A * H)| = |A|$ . In particular the underlying automaton of  $\text{core}(A * H)$  is isomorphic as an automaton to the underlying automaton of  $A$  via the map sending  $(p, [p^{-1}])$  to  $p$ .

Now,  $A *_{\widetilde{\mathcal{P}}_n} H$  is obtained by identifying  $\omega$ -equivalent states of  $\text{core}(A * H)$ . Therefore the underlying automaton of  $A *_{\widetilde{\mathcal{P}}_n} H$  belongs to a collapse chain of the underlying automaton of  $\text{core}(A * H)$  as required.  $\square$

**Lemma 5.2.** *Let  $A \in \mathcal{H}_n$  be a minimal transducer, let  $B$  be the underlying automaton of  $A^{-1}$  and  $(B_i)_{i \in \mathbb{N}}$  be the synchronizing sequence of  $B$ . Suppose there are distinct states  $q_1, q_2 \in Q_A$  such that the maps  $\pi_A(\cdot, q_1)$  and  $\pi_A(\cdot, q_2)$  are equal. Then there is a transducer  $H$  with the following properties:*

- (a) *there is a  $j \in \mathbb{N}$  such that  $H = H(B_j, \phi)$  for an automorphism  $\phi$  of  $B_j$  and,*
- (b) *writing  $[q^{-1}]$  for the state of  $B_j$  containing  $q^{-1}$ ,  $q \in Q_A$ , we have*

$$\lambda_A(\cdot, q_2) \circ \lambda_{H(B_j, \phi)}(\cdot, [q_2^{-1}]) : X_n \rightarrow X_n$$

*is precisely the map  $\lambda_A(\cdot, q_1) : X_n \rightarrow X_n$ .*

**Proof.** Since  $q_1, q_2$  are distinct states of  $A$  and since  $A$  is minimal, the states  $q_1$  and  $q_2$  are not  $\omega$ -equivalent. Therefore, there are  $x \neq y$  and  $z \in X_n$  such that  $\lambda_A(x, q_1) = \lambda_A(y, q_2) = z$ . Let  $p_1 = \pi_A(x, q_1)$  and  $p_2 = \pi_A(y, q_2)$ . In  $A^{-1}$ , we have  $\pi_{A^{-1}}(z, q_1^{-1}) = p_1^{-1}$  and  $\pi_{A^{-1}}(z, q_2^{-1}) = p_2^{-1}$ . Since  $A^{-1}$  has minimal synchronizing level  $k$ , it therefore follows that either  $k = 1$  and  $p_1 = p_2$  or  $k \geq 2$  and the maps  $\pi_{A^{-1}}(\cdot, p_1^{-1}) : X_n^{k-1} \rightarrow Q_{A^{-1}}$  and  $\pi_{A^{-1}}(\cdot, p_2^{-1}) : X_n^{k-1} \rightarrow Q_{A^{-1}}$  are equal. Therefore, by Theorem 4.8, the minimal  $j \in \mathbb{N}$  for which  $p_1^{-1}$  and  $p_2^{-1}$  belong to the same state of  $B_j$  is at most  $k - 1$ .

Define a relation  $\mathcal{R}$  on the set of states

$$Q_{q_1^{-1}, q_2^{-1}} := \{p^{-1} \in Q_{A^{-1}} \mid \exists x \in X_n, a \in \{1, 2\} : \pi_{A^{-1}}(x, q_a^{-1}) = p^{-1}\}$$

by setting  $p^{-1} \mathcal{R} q^{-1}$  if and only if there is a letter  $z \in X_n$  such that

$$\pi_{A^{-1}}(z, q_1^{-1}) = p^{-1} \text{ and } \pi_{A^{-1}}(z, q_2^{-1}) = q^{-1}.$$

Let  $\overline{\mathcal{R}}$  be the transitive closure of  $\mathcal{R}$ , so that  $\overline{\mathcal{R}}$  is an equivalence relation on  $Q_{q_1^{-1}, q_2^{-1}}$ . By the preceding paragraph, for a state  $p^{-1} \in Q_{q_1^{-1}, q_2^{-1}}$ , there is a minimal  $j \in \mathbb{N}$ ,  $j \leq k - 1$ , and all elements of  $[p^{-1}]_{\overline{\mathcal{R}}}$ , the equivalence class of  $p^{-1}$ , belong to the same state of  $B_j$ .

Let  $J \in \mathbb{N}$ ,  $J \leq k - 1$ , be minimal such that for any  $p^{-1} \in Q_{A^{-1}}$  there is a state of  $B_J$  such that all elements of  $[p^{-1}]$  belong to the same state of  $B_J$ . Observe that if  $\mathcal{R}$  is the diagonal relation, that is, if  $\mathcal{R}$  is precisely the set  $\{(p^{-1}, p^{-1}) \mid p^{-1} \in Q_{q_1^{-1}, q_2^{-1}}\}$ , then  $B_J = B_0$ . Further observe that  $\mathcal{R}$  is the diagonal relation precisely when for all  $x \in X_n$ ,  $\pi_{A^{-1}}(x, q_1^{-1}) = \pi_{A^{-1}}(x, q_2^{-1})$ . If there is  $z \in X_n$ , such that  $\pi_{A^{-1}}(z, q_1^{-1}) \neq \pi_{A^{-1}}(z, q_2^{-1})$ , then minimality of  $J$  forces that the states  $q_1^{-1}$  and  $q_2^{-1}$  do not belong to the same state of  $B_J$ . Therefore, as  $q_1$  and  $q_2$  are distinct states of  $A$ , they are contained in distinct states of  $B_J$ .

Let  $t_1$  and  $t_2$  be the distinct states of  $B_J$  containing  $q_1^{-1}$  and  $q_2^{-1}$  respectively. Observe that the maps  $\pi_{B_J}(\cdot, t_1)$  and  $\pi_{B_J}(\cdot, t_2)$  are equal by choice of  $J$  and definition of the relation  $\overline{\mathcal{R}}$ . Define a map  $\lambda_{B_J}(\cdot, t_2) : X_n \rightarrow X_n$  as follows. Let  $x, y \in X_n$  and let  $z = \lambda_A(x, q_1)$  and  $y = \lambda_A(x, q_2)$  then set  $\lambda_{B_J}(y, t_2) := z$ . Since  $\lambda_A(\cdot, q_1)$  and  $\lambda_A(\cdot, q_2)$  are permutations of  $X_n$ , then  $\lambda_A(\cdot, t_2)$  is a bijection as well. Moreover we note that

$$\lambda_A(\cdot, q_2) \circ \lambda_A(\cdot, t_2) : X_n \rightarrow X_n$$

is precisely the map  $\lambda_A(\cdot, q_1) : X_n \rightarrow X_n$ .

Let  $a, b, c \in X_n$  be arbitrary such that  $\lambda_{B_j}(a, t_2) = b$  and  $\lambda_{B_j}(b, t_2) = c$ . By definition, there are  $x, y \in X_n$  such that  $\lambda_A(x, q_1) = a$ ,  $\lambda_A(x, q_2) = b$ ,  $\lambda_A(y, q_1) = b$  and  $\lambda_A(y, q_2) = c$ . By the assumption that  $\pi_A(\cdot, q_1)$  and  $\pi_A(\cdot, q_2)$  are equal, we have  $p^{-1} := \pi_{A^{-1}}(a, q_1^{-1}) = \pi_{A^{-1}}(b, q_2^{-1})$  and  $q^{-1} := \pi_{A^{-1}}(b, q_1^{-1}) = \pi_{A^{-1}}(c, q_2^{-1})$ . Thus,  $p^{-1}$  is  $\mathcal{R}$  related to  $q^{-1}$ . Therefore, it is the case that  $\pi_{B_j}(b, t_2) = \pi_{B_j}(c, t_2)$ .

Let  $(x_1 \ x_2 \ x_3 \ \dots \ x_m)$  be a sequence of elements of  $X_n$  such that for  $1 \leq i \leq m-1$ ,  $\lambda_{B_j}(x_i, t_2) = x_{i+1}$  and  $\lambda_{B_j}(x_m, t_2) = x_1$ . By an induction argument making use of the previous paragraph we see that there is a state  $t \in Q_{B_j}$  such that  $\pi_{B_j}(x_i, t_2) = t$  for all  $1 \leq i \leq m$ . Thus, it follows that given  $a, b \in X_n$  such that  $\lambda_{B_j}(a, t_2) = b$  then,  $\pi_{B_j}(a, t_2) = \pi_{B_j}(b, t_2)$ .

Let  $t$  be any state of  $B_j$  not equal to  $t_2$ , we set  $\lambda_{B_j}(\cdot, t) : X_n \rightarrow X_n$  to be the identity permutation. Set  $H(B_j) := (X_n, Q_{B_j}, \pi_{B_j}, \lambda_{B_j})$ .

Let  $\phi$  be the automorphism of  $G_{B_j}$  which fixes all vertices of  $G_{B_j}$  and whose action on the edges of  $G_{B_j}$  is as follows. For an edge  $(t_2, x, t)$  of  $G_{B_j}$  with initial vertex  $t_2$ , set  $(t_2, x, t)\phi := (t_2, \lambda_{B_j}(x, t_2), t)$ ;  $\phi$  fixes every other edge. It is clear from the preceding paragraphs that  $H(B_j, \phi) = H(B_j)$ . Thus we may take  $H = H(B_j)$  concluding the proof.  $\square$

**Proposition 5.3.** *Let  $A \in \mathcal{H}_n$  be a minimal transducer,  $B$  be the underlying automaton of  $A^{-1}$ ,  $(B_i)_{i \in \mathbb{N}}$  be the synchronizing sequence of  $B$  and  $k \in \mathbb{N}$  be minimal such that  $|B_k| = 1$ . Suppose there are distinct states  $q_1, q_2 \in Q_A$  such that the maps  $\pi_A(\cdot, q_1)$  and  $\pi_A(\cdot, q_2)$  are equal. Then, there is an  $i \in \mathbb{N}$ , and an automorphism  $\phi$  of  $G_{B_i}$  fixing vertices and such that  $|A *_{\mathcal{P}_n} H(B_i, \phi)| < |A|$ . Thus,  $G_{H(B_i, \phi)} = G_{B_i}$  is an amalgamation of  $G_A$ . Moreover, the underlying automaton of  $A *_{\mathcal{P}_n} H(B_i, \phi)$  is belongs to a collapse chain of the underlying automaton of  $A$ . Therefore,  $(A *_{\mathcal{P}_n} H(B_i, \phi))$  has minimal synchronizing level at most the minimal synchronizing level of  $A$ .*

**Proof.** By Lemma 5.2 there is a transducer  $H$  with the following properties:

- there is a  $j \in \mathbb{N}$  such that  $H = H(B_j, \phi)$  for an automorphism  $\phi$  of  $B_j$  and,
- writing  $[q^{-1}]$  for the state of  $B_j$  containing  $q^{-1}$ ,  $q \in Q_A$ , we have

$$\lambda_A(\cdot, q_2) \circ \lambda_{H(B_j, \phi)}(\cdot, [q_2^{-1}]) : X_n \rightarrow X_n$$

is precisely the map  $\lambda_A(\cdot, q_1) : X_n \rightarrow X_n$ .

The result follows by applying Lemma 5.1 to the product  $A *_{\mathcal{P}_n} H$ .  $\square$

**Theorem 5.4.** *Let  $T \in \mathcal{H}_n$ ,  $A$  the underlying automaton of  $T$ ,  $(A_i)_{i \in \mathbb{N}}$  the synchronizing sequence of  $A$  and  $k$  be minimal such that  $A_j = A_k$  for all  $j \geq k$ . Note that since  $T$  is strongly synchronizing,  $A_k = 1$ . Then  $T$  can be written as a product of a single state transducer  $U$  and at most  $|A| - 1$  elements of  $\mathcal{H}_n$  which arise from vertex-fixing automorphisms of directed graphs which are amalgamations of  $G_A$ .*

**Proof.** The proof follows by repeatedly applying Proposition 5.3.  $\square$

We note that Theorem 1.1 is a corollary of Theorem 5.4 above.

**Lemma 5.5.** *Let  $A$  be a strongly synchronizing core automaton with more than one state. Then for any pair  $p, q \in Q_A$  there are is a least one element  $x \in X_n$  such that  $\pi_A(x, p) \neq q$ . In other words, there are at most  $n - 1$  edges in  $G_A$  from the vertex  $p$  to the vertex  $q$ .*

**Proof.** Suppose for a contradiction that there are states  $p, q \in Q_A$  such that  $\pi_A(x, p) = q$  for all  $x \in X_n$ . Let  $(A_i)_{i \in \mathbb{N}}$  be the synchronizing sequence of  $A$ , and let  $k$  be minimal such that  $A_k = 1$ . Notice that  $A_{k-1}$  is synchronizing at level 1 and core and has more than one state by assumption on  $k$ . Let  $t$  be the state of  $A_{k-1}$  which contains  $p$ , and  $t'$  be the state of  $A_{k-1}$  containing  $q$ . It follows that  $\pi_A(x_n, t) = t'$  for all  $x \in X_n$ . Since  $A_{k-1}$  is synchronizing at level 1, this forces,  $|A_{k-1}| = 1$  which yields the desired contradiction.  $\square$

**Corollary 5.6.** *Let  $A$  be a strongly synchronizing core automaton over the alphabet  $X_3$  with more than one state. Let  $\phi$  be any automorphism of  $G_A$  that fixes vertices, then  $\phi$  has order at most 2.*

**Corollary 5.7.** *Let  $T \in \mathcal{H}_3$ ,  $A$  be the underlying automaton of  $T$  and  $(A_i)_{i \in \mathbb{N}}$  be the synchronizing sequence of  $A$ . Let  $k \in \mathbb{N}$  be minimal such that  $|A_k| = 1$ . Then  $T$  can be written as a product of a single state transducer  $U$  and at most  $|A| - 1$  elements of  $\mathcal{H}_n$  of order 2 which arise from vertex-fixing automorphisms of directed graphs which are amalgamations of  $G_A$ .*

**Proof.** The proof follows by repeated applications of Proposition 5.3 and Corollary 5.6.  $\square$

We generalize Corollary 5.7 to all  $n$ . However, the number of elements of order 2 required is bigger than the number of states in general. We require first the following straight-forward observation.

**Lemma 5.8.** *Let  $G$  be a directed graph and  $\phi$  be an automorphism of  $G$  that fixes vertices. Then  $\phi$  can be written as a product of vertex-fixing automorphisms of  $G$  of order 2.*

**Corollary 5.9.** *Let  $T \in \mathcal{H}_n$ ,  $(A_i)_{i \in \mathbb{N}}$  be the synchronizing sequence of  $A$  and  $k$  be minimal such that  $A_j = A_k$  for all  $j \geq k$ . Then  $T$  can be written as a product of a single state transducer  $U$  with underlying automaton  $A_k$ , and elements of  $\mathcal{H}_n$  of order 2 arising from vertex-fixing automorphisms of directed graphs which are amalgamations of  $G_A$ .*

It is possible to bound the number of involutions appearing in Corollary 5.9 in terms of  $A$  (i.e the number of vertices and edges of  $G_A$ ) but we have not attempted to do so.

## 6 Counting foldings

Counting foldings of the de Bruijn graph  $G(n, k)$  is an important and challenging problem. We give here the solution for  $k = 1$  (which is trivial) and for  $k = 2$ .

The *Bell number*  $B(n)$  is the number of partitions of an  $n$ -set. This well-studied combinatorial sequence is given by the recurrence relation

$$B(n) = \sum_{k=1}^n \binom{n-1}{k-1} B(n-k)$$

for  $n > 0$ , with  $B(0) = 1$ .

**Proposition 6.1.** *The number of foldings of  $G(n, 1)$  is the Bell number  $B(n)$ .*

**Proof.** The vertex set is identified with  $X_n$ , so any folding is a partition of  $X_n$ ; and clearly any partition of  $X_n$  is a folding.  $\square$

**Theorem 6.2.** *The number of foldings of the de Bruijn graph with word length 2 over an alphabet of cardinality  $n$  is*

$$\sum_{\pi} \prod_{i=1}^{|\pi|} R(|\pi|, |A_i|),$$

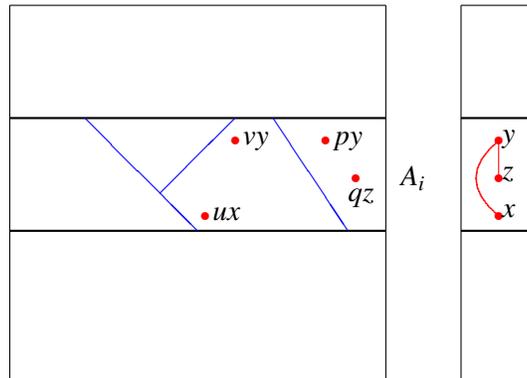
where  $\pi$  runs over partitions of the alphabet,  $A_i$  is the  $i$ th part, and

$$R(s, t) = \sum_{\rho} (-1)^{|\rho|-1} (|\rho| - 1)! \prod_{i=1}^{|\rho|} B(|C_i|s),$$

where  $\rho$  runs over all partitions of  $\{1, \dots, t\}$ , and  $C_i$  is the  $i$ th part.

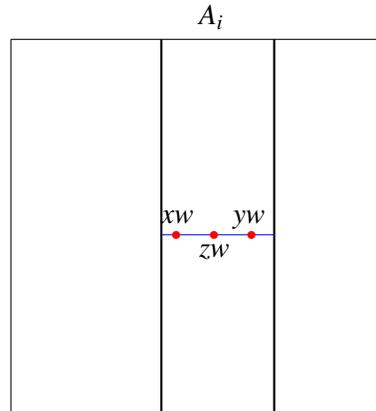
The formula is somewhat complicated, but values are easily computed (and rapidly growing): the numbers for  $n = 1, \dots, 7$  are 1, 5, 192, 78721, 519338423, 82833228599906, 429768478195109381814.

**Proof.** We define a graph  $\Gamma$  associated with a folding: the vertex set is the alphabet  $X_n$ , and two vertices  $x$  and  $y$  are joined if there exist  $u$  and  $v$  such that  $ux \equiv vy$ .



Let  $\pi$  be the partition of  $X_n$  into connected components of the graph  $\Gamma$ . If  $A_i$  is a part of  $\Gamma$ , then the set  $X_n \times A_i$  (the horizontal stripe in the figure) is a union of parts of the folding: no part can cross into a different horizontal stripe.

Moreover, by the definition of a folding, we see that if  $x, y \in A_i$ , then  $xw$  and  $yw$  lie in the same part of the folding.



The sets  $X_n \times A_i$  can be treated independently, so we have to count the number of good partitions of each and multiply them. Moreover, by the last remark, we can shrink each horizontal interval  $A_j \times \{v\}$  to a point, so we have to partition  $\pi \times A_i$ .

There are  $B(|\pi| \cdot |A_i|)$  partitions of  $\pi \times A_i$ . We have to filter out the ones which do not induce partitions of  $\pi \times B$  for any proper subset  $B$  of  $A_i$ . By Möbius inversion [20, Section 3.7] over the lattice of partitions of  $A_i$ , we find that the number of these is  $R(|\pi|, |A_i|)$ , where  $R$  is as defined earlier.

Putting all this together gives the result. □

Apart from this result, only a few values of the function counting foldings are known:  $G(2, 3)$  has 30 foldings, while  $G(2, 4)$  has 1247. (These numbers were obtained by brute-force computation.)

## Acknowledgements

The authors are grateful for partial support from EPSRC research grant EP/R032866/1. The third author is additionally grateful for support from Leverhulme Trust Research Project Grant RPG-2017-159 and for the warm hospitality of the University of Aberdeen where some of this research was conducted. We are also grateful to Mike Boyle, Matthew G. Brin, Elliot Cawtheray, Timothy Gowers, and anonymous referees for comments on drafts of this article.

## References

- [1] Ali Akhavi, Ines Klimann, Sylvain Lombardy, Jean Mairesse, and Matthieu Picantin, *On the finiteness problem for automaton (semi)groups*, Internat. J. Algebra Comput. **22** (2012), no. 6, 1250052, 26. MR 2974106 [20](#)
- [2] João Araújo, Peter J. Cameron, and Benjamin Steinberg, *Between primitive and 2-transitive: synchronization and its friends*, EMS Surv. Math. Sci. **4** (2017), no. 2, 101–184. MR 3725240 [11](#)
- [3] Jonathan Ashley, *Marker automorphisms of the one-sided  $d$ -shift*, Ergodic Theory Dynam. Systems **10** (1990), no. 2, 247–262. MR 1062757 [2, 3](#)

- [4] Jean-Camille Birget, *Circuits, the groups of Richard Thompson, and coNP-completeness*, Internat. J. Algebra Comput. **16** (2006), no. 1, 35–90. MR MR2217642 [6](#)
- [5] Collin Bleak, Peter Cameron, Yonah Maissel, Andrés Navas, and Feyishayo Olukoya, *The further chameleon groups of Richard Thompson and Graham Higman: Automorphisms via dynamics for the Higman groups  $G_{n,r}$* , 2016, submitted, pp. 1–89. [2](#), [3](#), [6](#), [11](#), [12](#), [15](#), [22](#)
- [6] Collin Bleak and Peter J. Cameron, *The number of automata over an  $n$ -letter alphabet whose states are determined by the last  $k$ -symbols*, OEIS [a248905](#) (2015). [3](#)
- [7] Collin Bleak and Martyn Quick, *The infinite simple group  $V$  of Richard J. Thompson: presentations by permutations*, Groups Geom. Dyn. **11** (2017), no. 4, 1401–1436. MR 3737287 [6](#)
- [8] Mike Boyle, John Franks, and Bruce Kitchens, *Automorphisms of one-sided subshifts of finite type*, Ergodic Theory Dynam. Systems **10** (1990), no. 3, 421–449. MR 1074312 [2](#), [3](#), [15](#), [16](#), [20](#), [22](#), [25](#), [26](#)
- [9] Kenneth S. Brown, *The geometry of finitely presented infinite simple groups*, Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989), Math. Sci. Res. Inst. Publ., vol. 23, Springer, New York, 1992, pp. 121–136. MR 1230631 [6](#)
- [10] N.G. Bruijn, de, *A combinatorial problem*, Proceedings of the Section of Sciences of the Koninklijke Nederlandse Akademie van Wetenschappen te Amsterdam **49** (1946), no. 7, 758–764 (English). [3](#)
- [11] J. W. Cannon, W. J. Floyd, and W. R. Parry, *Introductory notes on Richard Thompson’s groups*, Enseign. Math. (2) **42** (1996), no. 3-4, 215–256. [6](#)
- [12] Warren Dicks and Conchita Martínez Pérez, *Isomorphisms of Brin-Higman-Thompson groups*, Israel J. Math. **199** (2014), no. 1, 189–218. MR 3219533 [6](#)
- [13] R. I. Grigorchuk, V. V. Nekrashevich, and V. I. Sushchanskiĭ, *Automata, dynamical systems, and groups*, Proc. Steklov Inst. Math **231** (2000), 128–203. [2](#), [8](#), [9](#)
- [14] G. A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Math. Systems Theory **3** (1969), 320–375. MR 0259881 (41 #4510) [2](#), [3](#), [4](#), [5](#), [6](#), [22](#)
- [15] Graham Higman, *Finitely presented infinite simple groups*, Department of Pure Mathematics, Department of Mathematics, I.A.S. Australian National University, Canberra, 1974, Notes on Pure Mathematics, No. 8 (1974). MR 0376874 (51 #13049) [3](#), [6](#)
- [16] Conchita Martínez-Pérez, Francesco Matucci, and Brita Nucinkis, *Presentations of generalisations of Thompson’s group  $V$* , Pacific J. Math. **296** (2018), no. 2, 371–403. MR 3830841 [6](#)
- [17] Volodymyr Nekrashevych, *Self-similar groups*, Mathematical Surveys and Monographs, vol. 117, American Mathematical Society, Providence, RI, 2005. MR 2162164 [20](#)
- [18] Feyishayo Olukoya, *The growth rates of automaton groups generated by reset automata*, 2017, submitted, pp. 1–45. [17](#), [20](#)

- [19] E. Pardo, *The isomorphism problem for Higman-Thompson groups*, J. Algebra **344** (2011), 172–183. MR 2831934 (2012g:20060) [6](#)
- [20] Richard P. Stanley, *Enumerative combinatorics: Volume 1*, 2nd ed., Cambridge University Press, New York, NY, USA, 2011. [33](#)
- [21] Markus Szymik and Nathalie Wahl, *The homology of the Higman-Thompson groups*, Invent. Math. **216** (2019), no. 2, 445–518. MR 3953508 [6](#)
- [22] Richard J. Thompson, *Notes on three groups of homeomorphisms*, Unpublished but widely circulated handwritten notes (1965), 1–11. [6](#)
- [23] Mikhail V. Volkov, *Language and automata theory and applications*, Springer-Verlag, Berlin, Heidelberg, 2008, pp. 11–27. [11](#)

#### AUTHORS

Collin Bleak  
 University of St Andrews  
 Scotland, United Kingdom  
 cb211@st-andrews.ac.uk  
<https://orcid.org/0000-0001-5790-1940>

Peter J. Cameron  
 Professor  
 University of St Andrews  
 Scotland, United Kingdom  
 pjc20@st-andrews.ac.uk  
<https://orcid.org/0000-0003-3130-9505>

Feyishayo Olukoya  
 University of St Andrews  
 Scotland, United Kingdom  
 fo55@st-andrews.ac.uk  
<https://orcid.org/0000-0003-3285-9023>