Conjugacy for certain automorphisms of the one-sided shift via transducers

Collin Bleak and Feyishayo Olukoya

Abstract

We address the following open problem, implicit in the 1990 article *Automorphisms of one-sided subshifts of finite type* of Boyle, Franks and Kitchens (BFK):

> Does there exists an element ψ in the group of automorphisms of the one-sided shift $\mathrm{Aut}(\{0,1,\ldots,n-1\}^{\mathbb{N}},\sigma_n)$ so that all points of $\{0,1,\ldots,n-1\}^{\mathbb{N}}$ have orbits of length n under ψ and ψ is not conjugate to a permutation?

Here, by a *permutation* we mean an automorphism of one-sided shift dynamical system induced by a permutation of the symbol set $\{0,1,\ldots,n-1\}$.

We resolve this question by showing that any ψ with properties as above must be conjugate to a permutation.

Our techniques naturally extend those of BFK using the strongly synchronizing automata technology developed here and in several articles of the authors and collaborators (although, this article has been written to be largely self-contained).

Contents

1 Introduction

Let n be a positive integer and set $X_n := \{0, 1, \ldots, n-1\}$. We will use X_n to represent our standard alphabet of size n and we will denote by σ_n the usual shift map on $X_n^{\mathbb{N}}$. The group $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ of homeomorphisms of $X_n^{\mathbb{N}}$ which commute with the shift map is called *the group of automorphisms of the shift dynamical system.* This is a well-studied group in symbolic dynamics, with the special property (first given by Hedlund in [10]) that if $\phi \in \mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ has $(x_0x_1x_2\ldots)\phi = y_0y_1y_2\ldots$ then there is an integer k so that for all indices i, the value y_i is determined by the finite word $x_ix_{i+1}\ldots x_{i+k}$.

The paper [6] characterises all of the finite subgroups of the group $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$, shows that this group contains non-abelian free groups whenever $n \geq 3$, and investigates other algebraic structures of the group. The papers [7, 5] develop a conjugacy invariant for the group $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$, arising from the action of the group on periodic words, which for an automorphism ϕ we will denote as $\mathrm{Sp}(\phi)$ (this invariant consists of a tuple: the well-known *gyration* and *sign* functions, together with *first return* data: bundled data associated to the permutation representation on prime words of length k).

This article resolves the following open problem, implicit in [6], which Mike Boyle suggested to us for its own sake, and, as a test of our approach.

Let Σ_n represent the group of permutations of the set X_n. By a mild abuse of language, we say $\phi \in \mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ is a *permutation* if there is a fixed permutation $\alpha \in \Sigma_n$ so that if $(x_0x_1x_2\ldots)\phi = y_0y_1y_2\ldots$ then we have $y_i = (x_i)\alpha$ for all i. We say a permutation is a *rotation* if the permutation from Σ_n is an n-cycle. We can now state the problem:

> Does there exist an automorphism $\psi \in \mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ of order n so that all points of $X_n^{\mathbb{N}}$ travel on orbits of size n, where ψ is not conjugate to a rotation?

In [6] Boyle, Franks and Kitchens show that if n is prime then any such ψ is in fact conjugate to a rotation. We show that the Boyle, Franks, and Kitchens result holds for general n.

We have written this article so that it is essentially self-contained for general researchers working with automorphisms of the shift. In particular, we gather definitions and key constructions from [15] and [4] here to simplify the presentation without insisting the reader peruse those articles to follow our discussion. We use the highlighted technology to enhance the key method in the article [6]. The paper [4] shows how to represent any automorphism ϕ of the one-sided shift by a particularly nice family of transducers (finite state machines that transform inputs sequentially) while [15] investigates the order problem for that same family of transducers. A key idea of [4] is that any such transducer T representing ϕ can be thought of as a triple (D, R, ϕ_*), where D and R are *strongly synchronizing automata* (edge-labelled directed graphs with the particularly nice property of having a *synchronizing sequence*) with D representing the domain and R representing the range, and where ϕ_* is an isomorphism of the underlying digraphs $\Gamma(D)$ and $\Gamma(R)$ of D and R determined by the action of ϕ on periodic words. In the case of a finite order element, the domain and range automata can also be chosen to be identical.

In the article [6] the central method for studying finite subgroups of $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ is firstly to find an action of the group on the underlying digraph of an automaton (now understood to be a strongly synchronizing automaton). Once the first step is accomplished, the group is decomposed as a composition series where each composition factor is isomorphic to a subgroup of the symmetric group Σ_n on n-points. This is accomplished by pushing the action down along what is called an "amalgamation sequence" (see Section 4.1.2 here) of the digraph until one has an action by automorphisms on a particularly nice digraph. The construction typically requires passing through the automorphism groups of various one-sided shifts of finite type via topological conjugations induced by the amalgamations.

Our first step simplifies this process. In particular we show that we can always find an action of a finite subgroup of $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ on the underlying digraph of a strongly synchronizing automaton whose amalgamation and synchronizing sequences cohere (Section 4.1.2), thus we can push down along the synchronizing sequence of that automaton without needing to possibly change alphabet. This is already enough, when n is prime, to show that every element of order p in $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ is conjugate in $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ to a rotation.

However, to answer the open problem above, we need to go beyond this. Suppose $\phi \in \mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$ has order n and with the condition $(\star)$ that all points of $X_n^{\mathbb{N}}$ travel on orbits of size n. It turns out that $(\star)$ is equivalent to the condition that for any transducer (A, A, ϕ_*) representing ϕ, the action of ϕ_* on $\Gamma(A)$ has the property that for every (based) circuit C of $\Gamma(A)$ the orbit length of C under this action is n. (We are using based circuits here to avoid a circuit returning to itself with some non-trivial rotation as counting as completing the orbit.) When n is a prime p, it is not hard to see that the action of ϕ_* on the underlying digraph is limited in orbit lengths for edges and vertices to 1 and p. When n is not prime, orbit lengths of edges and vertices can be any divisor of n even though all circuits have orbit length n. This last issue creates problems when trying to implement the approach successfully carried out by Boyle et al for n prime.

We overcome this issue for such a ϕ with representative transducer (A, A, ϕ_*) with several technical lemmas. These aim to show that the automaton A can be "fluffed up" by adding *shadow states* (Section 4.3) to create a new strongly synchronizing automaton B with an induced and more informative action ψ_* on $\Gamma(B)$ so that (B, B, ψ_*) still represents ϕ. By 'more informative' we mean that the correct addition of shadow states results in states and edges originally on orbits of length $< n$ having resulting orbits of length n. This new action makes it possible to find a conjugate action of ϕ on a strongly synchronizing automaton of strictly smaller size than A (where the conjugacy occurs entirely with $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$).

Our approach can now be summarised as follows. First we conjugate to get a (conjugate) action of ϕ on a strongly synchronizing automaton whose synchronizing sequence coheres with the amalgamation sequence of its underlying digraph. Then we have a series of "fluffing up" moves followed by reductions via conjugation. Eventually, these processes result in a conjugate action given by a transducer over a single state automaton with n labelled loops, where each edge is on an orbit of length n; our original element ϕ must then be conjugate to a rotation.

The example in Section 5.1 might prove helpful to the reader as an illustration of our approach and of the difficulties discussed above.

The property of being a strongly synchronizing automaton is equivalent to that of being a *folded de Bruijn graph*. Crucial to the approach we have sketched out is the process: given a finite order element $\phi \in \mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$, find the minimal folded de Bruijn graph Γ so that ϕ acts faithfully on Γ by automorphisms. The following is essentially a result from [4] stated in our context (see Lemma 3.4 and Theorem 3.5, below).

Theorem 1.1. *Let $n \geq 2$ be an integer and suppose $\phi \in Aut(X_n^{\mathbb{N}}, \sigma_n)$ is a finite order element. There is an effective process for determining Γ_ϕ, the minimal folded de Bruijn graph on an n letter alphabet, so that ϕ induces a natural automorphism of Γ_ϕ.*

Finally, we can state the theorem which answers the question of Boyle.

Theorem 1.2. *Let $\phi \in Aut(X_n^{\mathbb{N}}, \sigma_n)$ be an element of finite order. The following are equivalent:*

- *ϕ is conjugate to a rotation;*
- *every element of $X_n^{\mathbb{N}}$ is on an orbit of length n under the action of A; and*
- *for any folded de Bruijn graph Γ_ϕ admitting a faithful action by ϕ via an automorphism ϕ_*, every (based) circuit of Γ_ϕ is on an orbit of length n under ϕ_*.*

It is unclear at the moment how much our approach depends on the condition that "all circuits are on orbits of length n". In work in progress we aim to extend our current ideas towards resolving the conjugacy problem for finite order elements of $\mathrm{Aut}(X_n^{\mathbb{N}}, \sigma_n)$.

Acknowledgements

The authors are grateful for partial support from EPSRC research grant EP/R032866/1. The second author is additionally grateful for support from Leverhulme Trust Research Project Grant RPG-2017-159 and LMS ECF grant ECF-1920-105. Finally, we are also grateful to Mike Boyle for conversations on the question we address here.

2 Preliminaries

2.1 The natural numbers and some of its subsets

We use the notation $\mathbb{N}$ for the set $\{0, 1, 2, \ldots\}$; for $j \in \mathbb{N}$ we write $\mathbb{N}_j$ for the set $\{i \in \mathbb{N} : 1 \geq j\}$ of all natural numbers which are bigger than or equal to j.

2.2 Words and infinite sequences

In this subsection we set up necessary notation for words and sequences.

Firstly, we employ all of the usual notation around finitary words over the alphabet X. Namely, for a base set X, and natural n, X^n is the set of ordered n-tuples with coordinates from X. We call these the *words of length n (over alphabet X)*. By convention, we set $X^0 := \{\varepsilon\}$ and we refer to ε as *the empty word* or *empty string*, proclaiming this to be the same object, independent of the (non-empty) set X used as our alphabet. We set $X^* := \cup_{n\in\mathbb{N}} X^n$, the words of finite length over X (this is the Kleene-star operator). We also set $X^+ := X^* \backslash \{\varepsilon\}$, the non-trivial/non-empty finite length words over X. If $w \in X^*$ we set $|w| = n$ where $w \in X^n$, and we call $|w|$ the *length of* w. If X has a linear order $<$, then we give X^* the induced dictionary order. If $u \in X^n$ then we implicitly set values $u_i \in X$ for $0 \leq i < n$ so that $u = (u_0, u_i, \ldots, u_{n-1})$. In this context, from here forward we will simply write $u = u_0u_1 \ldots u_{n-1}$. For $u \in X^n$ and $i \leq |u|$, we write $u_{[1,i]}$ for the prefix $u_1 \ldots u_i$ of u. Finally, if $u, v \in X^*$, so that $u = u_0u_1 \ldots u_{r-1}$ and $v = v_0v_1 \ldots v_{s-1}$ then uv will represent the concatenation of these words: $uv := u_0u_1 \ldots u_{r-1}v_0v_1 \ldots v_{s-1}$, which is a word of length $r + s$ over X.

As in the paper [4], we take $X_n^{-\mathbb{N}} := \{\ldots x_{-2}x_{-1}x_0 \mid x_i \in X_n\}$ as our shift space, with the shift operator σ_n defined by $(x_i)_{i\in-\mathbb{N}}\sigma_n = (y_i)_{i\in-\mathbb{N}}$ where we have $y_i = x_{i-1}$. We use the characterisation of elements of $\mathcal{H}_n$ as strongly synchronizing transducers corresponding to shift commuting automorphisms of $X_n^{-\mathbb{N}}$. For a finite-length word over X_n we may index this word with negative or positive indices as seems natural at the time. When we are explicitly thinking of a finite subword $w \in X_n^k$ of a point $x \in X_n^{-\mathbb{N}}$ we will ordinarily index w as $w = w_{i-k+1}w_{i-k+2} \ldots w_i$ for some $i \in -\mathbb{N}$.

Suppose k is a positive integer and $u = u_{-(k-1)}u_{-(k-2)} \ldots u_{-1}u_0 \in X_n^k$. Define $u^\omega \in X_n^{-\mathbb{N}}$, by which notation we mean the point $\ldots x_m x_{m-1} \ldots x_{-1}x_0 =: x$ where $x_i = u_{i \pmod k}$. The word $x \in X_n^{-\mathbb{N}}$ is called a *periodic word*. The *period* of x is the smallest $j \in \mathbb{N}$ such that $(x)\sigma_n^j = x$. If the length $|u|$ is the period of the word x, then u is called *prime*. Alternatively u is prime if there is no smaller word $\gamma \in X_n^+$ such that $u = \gamma^i$ for some $i \geq 2$.

Write X_n^k for the full set of prime words of length k over the alphabet X_n.

Given two words $u, v \in X_n^+$ such that $|u| = |v| = r$, we call v a *rotation* of u if there is an $i \in \mathbb{N}$ with $(u^\omega)\sigma_n^i = v^\omega$. In this case, we may refer to v as the *i^{th}-rotation of* u (even if $i > |u|$).

It is a well-known fact that an element $\phi \in \mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ preserves the period of a periodic element of $X_n^{-\mathbb{N}}$. In this way, the action of $\mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ on periodic words gives a representation from $\mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ to the group $\Pi_{k\in\mathbb{N}} \mathrm{Sym}(\mathsf{X}_n^k)$. For $\phi \in \mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$, write

$\overline{\phi}_k$ for the action of ϕ on prime words of length k and write $\overline{\phi}$ for the element $(\overline{\phi}_k)_{k\in\mathbb{N}} \in \Pi_{k\in\mathbb{N}}\,\mathrm{Sym}(\mathsf{X}_n^k)$. The map $\overline{\phi}$ is the *periodic point representation* of $\mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$, introduced in [7].

2.3 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) π_A is a function $X_A \times Q_A \to Q_A$, 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 $w = x_0x_1 \ldots x_{m-1}$, then

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

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 *initialised* at q.

An automaton A can be represented by a labeled directed graph G_A, whose vertex set V_A is Q_A. For this directed graph there is a directed edge labeled by $a \in X_A$ from p to q if $\pi_A(a, p) = q$. Representing this, we determine the set E_A of edges of G_A to be the set of triples

$$E_A := \{(p, a, q) \mid \exists p, q \in Q_A, a \in X_A, \text{ so that } \pi_A(a, p) = q\}.$$

In what follows, the labelled directed graph G_A will be referred to as the *underlying digraph for the automaton A*.

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

(a) (X_T, Q_T, π_T) is an automaton;

(b) $\lambda_T : X_T \times Q_T \to X_T^*$ is the *output function*.

Formally 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 $\pi_T(a, q)$. Thus, the size of a transducer is the size of its underlying automaton. An *initial transducer* T_q is simply a transducer which starts processing input from 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 [9]), 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, henceforth **we 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.

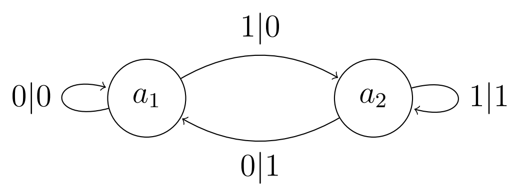

Figure 1: A transducer over X_2

In what follows, we only use the language *automaton* for those automata which are not transducers. This allows us characterise a synchronous transducer T as a pair of automata together with a directed graph isomorphism "gluing" the two automata together as a domain automaton and a range automaton (we split any edge label '$x|y$' of T as specifying the domain automaton edge with label x and the range automaton edge with label y).

We can regard any state q of 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

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

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 $\mathrm{Im}(q)$ for the image of the map induced by T_q.

Two states q_1 and q_2 are said to be *ω-equivalent* if the transducers T_{q_1} and T_{q_2} induce the same continuous map. (This can be checked in finite time, see [9].) More generally, we say that two initial transducers T_q and $T'_{q'}$ are *ω-equivalent* if they induce the same continuous map on $X_n^{\mathbb{N}}$.

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

Two minimal non-initial transducers T and U are said to be *ω-equal* if there is a bijection $f : Q_T \to Q_U$, such that for any $q \in Q_T$, T_q is ω-equivalent to $U_{(q)f}$. Two minimal initial transducers T_p and U_q are said to be ω-equal if they are ω-equal as non-initial transducers and there is a bijection $f : Q_T \to Q_U$ witnessing this which satisfies the equality $(p)f = q$. We use the symbol '=' to represent ω-equality of initial and non-initial transducers. Two non-initial transducers T and U are said to be *ω-equivalent* if they have ω-equal minimal representatives, and in this case we might instead say *T and U represent the same transformation*.

In the class of synchronous transducers, the ω-equivalence class of any transducer has a unique minimal representative.

Throughout this article, as a matter of convenience, we shall not distinguish between ω-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 ω-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 λ and π 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 $\rho_q := \lambda_T(\centerdot, q) : X_n \to X_n$ 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 $\pi_{T^{-1}} : X_n \times Q_{T^{-1}} \to Q_{T^{-1}}$ defined by $(x, p^{-1}) \mapsto q^{-1}$ if and only if $\pi_T((x)\rho_p^{-1}, p) = q$, and output function $\lambda_{T^{-1}} : X_n \times Q_{T^{-1}} \to X_n$ defined by $(x, p) \mapsto (x)\rho_p^{-1}$. Thus, in the graph of the transducer T we simply switch the input labels with the output labels and append '$^{-1}$' to the state names.

We are concerned only with **invertible, synchronous transducers** in this article.

2.4 Increasing alphabet size and the dual automaton

We require a couple of standard constructions in the theory of synchronous automata in this work.

First we consider the 'paths to letters' construction. Let T be a transducer over the alphabet X_n. Let $m \in \mathbb{N}_1$. Write $T(m)$ for the transducer over the alphabet X_n^m with state set Q_T and transition and output functions $\pi_{T(m)}$, $\lambda_{T(m)}$ satisfying the following conditions. For $x \in X_n^m$ and $q \in Q_T$ we set $\pi_{T(m)}(x, q) = p$ if and only if $\pi_T(x, q) = p$ in T; we set $\lambda_{T(m)}(x, q) := \lambda_T(x, q)$. It is clear that if T is minimal and invertible, the $T(m)$ is also minimal and invertible.

The other construction we require is the *dual automaton* (see [1, 14]).

Again 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 $\lambda_T(x, q) = y$.

There is a connection between the two constructions. The following is standard in the theory of synchronous automata and provides a key insight in the analysis of [1].

Lemma 2.1. *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 $\lambda^\vee(q, x) = p$, then $\pi_{T^{-1}}^\vee(q^{-1}, y) = x$ and $\lambda^\vee(q^{-1}, y) = p^{-1}$.

2.5 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 π_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 [16, 2]. Our definition of "synchonizing 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 maximal sub-automaton with set of states those states in 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 using the same alphabet, and is also synchronizing at level k. We denote this automaton by $\mathrm{core}(A)$. We say that an automaton or transducer is *core* if it is equal to its core.

Clearly, if A is synchronizing at level k, then it is synchronizing at level l for all $l \geq k$.

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.

Note that if T is a strongly synchronizing transducer, then for any $m \in \mathbb{N}$, $T(m)$ is also strongly synchronizing. Moreover, if k the minimal synchronizing level of T, then $T(m)$ is synchronizing at level 1 for any $m \geq k$ and, more generally, is synchronizing at level $\lceil k/m \rceil$.

Notation 2.2. 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 $\mathfrak{s}_l : X_n^l \to Q_T$ is the synchronizing map at level l.

The following result was proved in Bleak *et al.* [3].

Proposition 2.3. *Let T, U be transducers which (as automata) are synchronizing at levels j, k respectively, Then $T * U$ is synchronizing at level $j + k$.*

Note that in the statement of Proposition 2.3, the lowest synchronizing level of $T * U$ might actually be less than $j + k$.

Let T be a transducer which (regarded as an automaton) is synchronizing at level k, then the core of T (similarly denoted $\mathrm{core}(T)$) induces a continuous map

$$f_T : X_n^{-\mathbb{N}} \to X_n^{-\mathbb{N}}$$

as follows. Let $x \in X_n^{-\mathbb{N}}$ and set $y \in X_n^{-\mathbb{N}}$ to be the sequence defined by

$$y_i = \lambda_T(x_i, q_{x_{i-k}x_{i-(k-1)}\dots x_{i-1}}).$$

Note that

$$\pi_T(x_i, q_{x_{i-k}x_{i-(k-1)}\dots x_{i-1}}) = q_{x_{i-k}x_{i-(k-1)}\dots x_{i-1}}.$$

Set

$$(x)f_T = y.$$

Thus, from the point of view of the transition function of T we in fact begin processing x at $-\infty$ and move towards x_0. (This is in keeping with our interpretation of transducer as representing machines applying sliding block codes, where here, we are thinking of $\mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ as consisting of the sliding block code transformations that require past information only to determine what to do with a digit.) Note, moreover, that the map f_T is independent of the (valid) synchronizing level chosen to define it. We have the following result:

Proposition 2.4. *[4] Let T be a minimal transducer which is synchronizing at level k and which is core. Then $f_T \in \mathrm{End}(X_n^{-\mathbb{N}}, \sigma_n)$.*

The transducer in Figure 1 induces the shift map on $X_n^{-\mathbb{N}}$.

In [3], the authors show that the set $\widetilde{\mathcal{H}_n}$ of minimal finite synchronizing invertible synchronous core transducers is a monoid; the monoid operation consists of taking the product of transducers and reducing it by removing non-core states and identifying ω-equivalent states to obtain a minimal and synchronous representative.

Let $\mathcal{H}_n$ be the subset of $\widetilde{\mathcal{H}_n}$ consisting of transducers which are bi-synchronizing. A chief result of [4] is that $\mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n) \cong \mathcal{H}_n$.

2.6 De Bruijn graphs and folded automata

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 $\{0, \ldots, n-1\}$ of cardinality n. There is a directed arc from $a_0 \ldots a_{m-1}$ to $a_1 a_2 \ldots a_m$, with label a_m.

Note that, in the literature, the directed edge is also from $a_0 a_1 \ldots a_{m-1}$ to $a_1 \ldots a_{m-1} a_m$ and the label on this edge is often given as the $(m+1)$-tuple $a_0 a_1 \ldots a_{m-1} a_m$. However, the labelling given above produces an isomorphic graph and is better suited for our purposes.

Figure 2 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 $b_0 b_1 \ldots b_{m-1}$ from any initial state, it moves into the state labeled $b_0 b_1 \ldots b_{m-1}$.

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

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 2.5. *[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 $G(n, m)$.*

We may think of a de Bruijn graph $G(n, m)$ as determining a finite category, with objects the foldings of $G(n, m)$ and with arrows digraph morphisms which commute with the transition maps of the given automata. It is immediate in that point of view that all such arrows are surjective digraph morphisms (and indeed, these are folding maps).

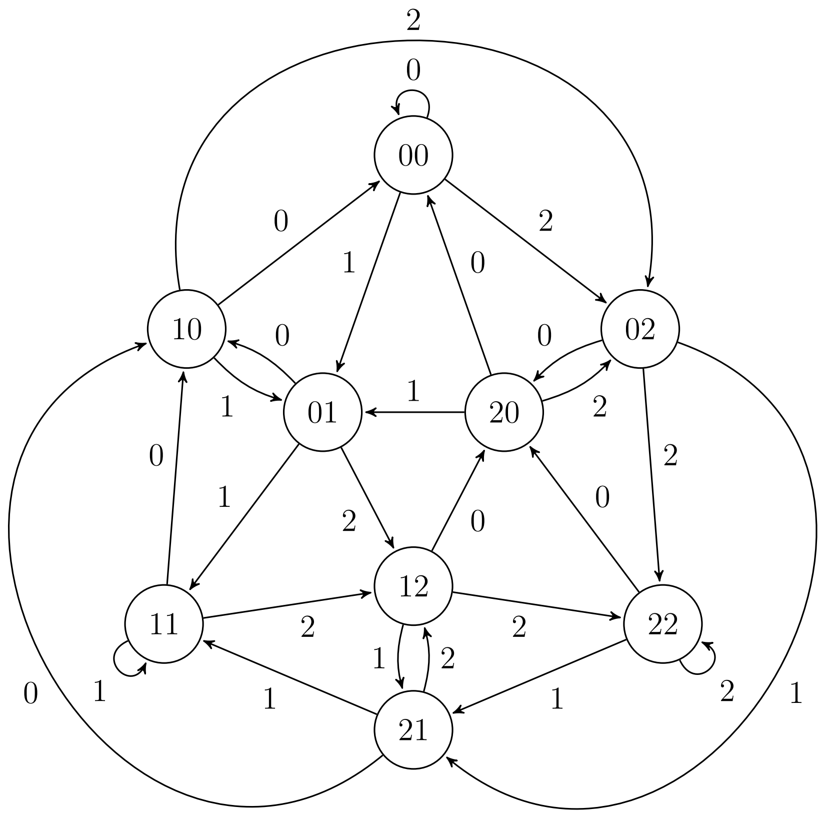

Figure 2: The de Bruijn graph $G(3,2)$.

2.7 Automorphisms of digraphs underlying de Bruijn graphs and $\mathcal{H}_n$

In this section we describe finite order elements of $\mathcal{H}_n$ as automorphisms of folded de Bruijn graphs.

Let A be a finite automaton on edge-alphabet X_n. Recall (Section 2.3) that an automaton A may be regarded as labeled directed graph with vertex set Q_A, and edge set $E_A \subset Q_A \times X_n \times Q_A$. We let G_A denote the unlabeled directed graph corresponding to an automaton A, but we retain the triple (p, x, q) to denote the edge of G_A underlying the edge (p, x, q) of A.

Let ϕ be an automorphism of the directed graph G_A. Let $H(A, \phi)$ be a transducer with

- state set $Q_{H(A,\phi)} := Q_A$,

- alphabet set X_n,
- transition function $\pi_{H(A,\phi)} := \pi_A$, and
- output function $\lambda_{H(A,\phi)} : X_n \times Q_{H(A,\phi)} \to X_n$,

where $\lambda_{H(A,\phi)}(x,p) = y$ if and only if there are edges (p,x,q) and (r,y,s) of G_A so that (p,x,q) is taken to (r,y,s) by ϕ.

The transducer $H(A,\phi)$ can be thought of as the result of gluing the automaton A to a copy of itself along the map ϕ. 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 edge (p,x,q) is identified with the edge $((p,x,q))\phi$ and has input label x and the output label y.

Remark 2.6. We make a few observations:

(a) For each state $q \in Q_{H(A,\phi)}$, the map $\lambda_{H(A,\phi)}(\cdot,q) : X_n \to X_n$ 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 2.5) then both $H(A,\phi)$ and $H(A,\phi)^{-1}$ are synchronizing at level k hence the minimal representative $\overline{H(A,\phi)}$ 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) An element of $\mathcal{H}_n$ which can be represented by a transducer $H(A,\phi)$ for some folded de Bruijn graph A and digraph automorphism ϕ of G_A must have finite order.

If $A \in \mathcal{H}_n$ and B is an automaton so that there is a digraph automorphism $\phi : G_B \to G_B$ so that A and $H(B,\phi)$ represent the same transformation then we say A *is induced from* (B,ϕ).

2.8 Synchronizing sequences and collapse chains

We require an algorithm given in [3] 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 $\pi_A(\cdot,p) : Q_A \to Q_A$ and $\pi_A(\cdot,q) : Q_A \to Q_A$ are equal. For a state $q \in Q_A$ let q represent the equivalence class of q under $\sim_A$. Further set $\mathsf{Q_A} := \{\mathsf{q} \mid q \in Q_A\}$ and let $\pi_{\mathsf{A}} : \mathsf{Q_A} \to \mathsf{Q_A}$ be defined by $\pi_{\mathsf{A}}(x,\mathsf{q}) = \mathsf{p}$ where $p = \pi_A(x,q)$.

Observe that π_{A} is a well defined map. Define a new automaton $\mathsf{A} = (X_n, \mathsf{Q}_{\mathsf{A}}, \pi_{\mathsf{A}})$ noting that $|\mathsf{Q}_{\mathsf{A}}| \leq |Q_A|$ and $|\mathsf{Q}_{\mathsf{A}}| = |Q_A|$ implies that A is isomorphic to A.

Given an automaton A, let $A_0 := A, A_1, A_2, \ldots$ be the sequence of automata such that $A_i = \mathsf{A}_{i-1}$ 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_i} 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 $(G(n, m), G(n, m-1), G(n, m-2), \ldots, G(n, 1)$, after this all the terms in the sequence are the single state automaton on X_n.

The result below is from [3].

Theorem 2.7. *Let A be an automaton and $A_0 := A, A_1, A_2, \ldots$ be the sequence of automata such that $A_i = \mathsf{A}_{i-1}$ 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.

We also require the notion of a *collapse chain* from [4]. Let A and B be strongly synchronizing automata. Let $A = A_0, A_1, \ldots, A_k = B$ be a sequence such that A_{i+1} is obtained from A_i by identifying pairs of states $p \sim_{A_i} q$. We note that as distinct from the synchronizing sequence, we do not necessarily make all possible identifications. Such a sequence is called a *collapse chain* if at each step, we make the maximal number of collapses possible relative to the final automaton B. That is, for $u, v \in Q_A$ belonging to the same state of B, in the minimal A_i such that $[u] \sim_{A_i} [v]$, we have $[u] = [v]$ in A_{i+1}. We note that this condition means that a collapse chain is unique. Therefore, for B a strongly synchronizing automaton, we say that B *belongs to a collapse chain of* A if there is a collapse chain $A = A_0, A_1, \ldots, A_k = B$. In this case, we call the collapse chain $A = A_0, A_1, \ldots, A_k = B$, the *the collapse chain from A to B*. If B is a single state automaton, the collapse chain from A to B is precisely the strongly synchronizing sequence of A. Thus a collapse chain can be thought of as a synchronizing sequence relative to its end point.

The following facts are straightforward. Let A be a strongly synchronizing automaton, and B be an automaton which is a folding of A, then there is a collapse chain from A to B. Therefore B belongs to a collapse chain of A if and only if B is a folding of A. In particular if B belongs to a collapse chain of A, then B is synchronizing at the minimal synchronizing level of A.

The following result about collapse chains is proved similarly to Theorem 2.7.

Theorem 2.8. *Let A be an automaton and B be a folding of A. Let $A_0 := A, A_1, A_2, \ldots, A_m = B$ be the collapse chain from A to B. Then a pair of states $p, q \in Q_A$ belong to the same element $t \in Q_{A_i}$ if and only if p, q belong to the same state of Q_B and for all words $a \in X_n^i$, $\pi_A(a, p) = \pi_A(a, q)$.*

3 Minimal actions of finite order elements of $\mathcal{H}_n$

For this section, we will work using facts related to dual transducers for strongly synchronizing transducers.

It has been shown in [12, 1, 14] that the dual $T^\vee$ transducer for a synchronous transducer T contains much information about the order of T, but implicit in those works also, much information about the conjugacy class of T. In [15] the dual is considered for strongly synchronizing transducers, where it is shown that for infinite order strongly synchronizing transducers the powers of the dual grow in size asymptotically exponentially while for finite order transducers the dual generates a finite semigroup with a zero. In this section we bring in some of the methods and results of those works. See [4, 15] for more details than we give below.

3.1 Duals and Splits

Recall our definition of the dual of a transducer from Subsection 2.4. We will mostly be working in a power of the dual of a transducer T, below.

We introduce the following notation. Let T be a strongly synchronizing transducer, and $q \in Q_T$ be a state. Then we write W_q for the set of words $\gamma \in X_n^+$ such that the map $\pi_T(\gamma, \cdot) : Q_T \to Q_T$ has image $\{q\}$.

Let A be an element of $\mathcal{H}_n$, with synchronizing level k. Then for $r \geq k$, $A_r^\vee$ has a *split* $((p_1, \ldots, p_l), (q_1 \ldots, q_l), \Gamma)$ if and only if the following depiction (see Figure 3) of the transitions in $A_r^\vee$ at the state Γ is valid:

More formally, we have the following.

Definition 3.1 (Splits)**.** Let A be an element of $\mathcal{H}_n$, with synchronizing level k and let $r \geq k$. Suppose there are

- $l \in \mathbb{N}_1$,
- elements $(p_1, p_2, \ldots, p_l), (q_1, q_2, \ldots, q_l), (s_1, s_2, \ldots, s_l) \in Q_A^l$,
- a word $\Gamma \in X_n^r \cap W_{s_1}$, and
- distinct states $t_1, t_2 \in Q_A$

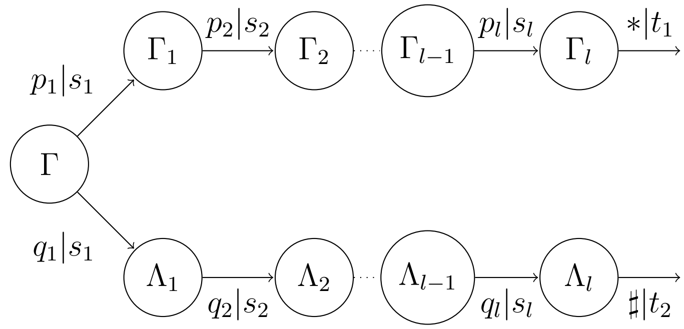

Figure 3: A split; the symbols $*$ and $\sharp$ represent arbitrary elements of Q_A.

such that when we define sequences $\Gamma_1, \Gamma_2, \ldots, \Gamma_l$ and $\Lambda_1, \Lambda_2, \ldots, \Lambda_l$ by

- $\Gamma_1 = \lambda_A(\Gamma, p_1)$ and $\Lambda_1 = \lambda_A(\Gamma, q_1)$, and
- for $1 < i \leq l$, $\Gamma_i = \lambda_A(\Gamma_{i-1}, p_i)$ and $\Lambda_i = \lambda_A(\Lambda_{i-1}, q_i)$,

then $\Gamma_i, \Lambda_i \in W_{s_{i+1}}$ for all $1 \leq i \leq l-1$, $\Gamma_l \in W_{t_1}$ and $\Lambda_l \in W_{t_2}$. In this case we say that $A_r^\vee$ *splits*.

We also say that the l-tuples $(p_1, \ldots, p_l)$ and $(q_1, \ldots, q_l)$ *split* $A_r^\vee$ *(at* Γ*)*. We call $\{p_1, q_1\}$ the *top of the split*, $\{t_1, t_2\}$ the *bottom of the split*, and the triple $((p_1, \ldots, p_l), (q_1 \ldots, q_l), \Gamma)$ a *split of* $A_r^\vee$ *(of length* l*)*.

N.B.: if we took $r < k$ in the definition of a split above, then there is no guarantee that some word Γ of length r would not even be synchronizing, and also no guarantee of the existence of any synchronizing word of length r, so the definition above breaks down.

The following concept appears implicitly in the proof of Lemma 3.8.

Definition 3.2. Let A be an element of $\mathcal{H}_n$, with synchronizing level k. Let $r \geq k$ and $((p_1, \ldots, p_l), (q_1 \ldots, q_l), \Gamma)$ be a split of $A_r^\vee$. Let $\{t_1, t_2\}$ be the bottom of this split. Then we say that *the bottom of the split* $((p_1, \ldots, p_l), (q_1 \ldots, q_l), \Gamma)$ *depends only on the top* if the following conditions hold for any other tuples $U_1, U_2 \in Q_A^{l-1}$:

- the triple $((p_1, U_1), (q_1, U_2), \Gamma)$ is also a split with bottom $\{t_1, t_2\}$ and,
- if $\lambda_{A^l}(\Gamma, (p_1, \ldots, p_l)) \in W_{t_1}$ and $\lambda_{A^l}(\Gamma, (q_1, \ldots, q_l)) \in W_{t_2}$ then $\lambda_{A^l}(\Gamma, (p_1, U_1)) \in W_{t_1}$ and $\lambda_{A^l}(\Gamma, (q_1, U_2)) \in W_{t_2}$, and vice-versa.

Observe that if, for $r \geq k$, $A_r^\vee$ has a split $((p_1, \ldots, p_l), (q_1 \ldots, q_l), \Gamma)$ whose bottom depends only on the top, then $p_1 \neq q_1$.

Splitting length as defined below is used explicitly in Lemma 3.8.

Definition 3.3. For a transducer A, we define the *r-splitting length of A* (for r greater than or equal to the minimal synchronizing length) to be minimal l such that there is a split of $A_r^\vee$ of length l. If there is no such split then we set the r-splitting length of A to be ∞.

Note that if, for $r \geq k$, $A_r^\vee$ has r-splitting length $l < \infty$, then any split of length l has the property that the bottom depends only on the top as otherwise one can find a shorter split (see [15]).

3.2 Notational inconvenience.

We are soon to run into some collisions of notation.

Firstly, if $\phi \in \mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$, then we can represent ϕ by a (minimal) transducer $A_\phi \in \mathcal{H}_n$.

Secondly, if $A \in \mathcal{H}_n$, then A represents an element $\phi_A \in \mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$.

Finally, if $\phi \in \mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ has finite order, then as we will see from Theorem 3.5 there is an automaton $\mathscr{A}(A_k^\vee)$ and an automorphism ψ of the underlying digraph $G_{\mathscr{A}(A_k^\vee)}$ so that A_ϕ and $H(\mathscr{A}(A_k^\vee), \psi)$ represent the same element. It happens that there is a way to define ψ from ϕ, and also, from A_ϕ. Similarly, we could have begun this paragraph with an element $A \in \mathcal{H}_n$, in which case ψ would be defined from both ϕ_A and from A.

In order to unify our notation here, we will simply denote ψ in the above situation as ϕ_A. This of course means that ϕ_A will represent two different things (an automorphism of the one-sided shift, or alternatively, an automorphism of a digraph underlying a folded de Bruijn graph). We hope that confounding the notation in this way will not cause confusion as it should be clear what is meant from context, noting as well that the digraph homomorphism ϕ_A is the induced digraph homomorphism that arises on $G_{\mathscr{A}(A_k^\vee)}$ by considering how ϕ maps infinite paths on $\mathscr{A}(A_k^\vee)$ to other infinite paths on $\mathscr{A}(A_k^\vee)$.

3.3 Finite order elements of $\mathcal{H}_n$

In this subsection we build, for a finite order element $A \in \mathcal{H}_n$ and corresponding $\phi_A \in \mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$, the minimal strongly synchronizing automaton $\mathscr{A}(A_k^\vee)$ which ϕ_A can act on as an automorphism of the underlying directed graph with A being the minimal representative of $H(\mathscr{A}(A_k^\vee), \phi_A)$.

Note that we will retain the notation ϕ_A for both the element of $\mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ corresponding to A as well as the digraph automorphism ϕ_A that is induced by this automorphism of the shift.

Note that the process of determining $A_\phi \in \mathcal{H}_n$ from a given element $\phi \in \mathrm{Aut}(X_n^{-\mathbb{N}}, \sigma_n)$ is not difficult: one simply relates states to different maps as determined by the fixed viewing window (it is common for differing viewing-window strings to correspond to the same map, the set of all such strings corresponding to "same" map can be used effectively as the name of that state) and then one records the local letter transformations as the edge labels. For details, see [4].

3.3.1 Building $\mathscr{A}(A_k^\vee)$ from A

Let $A \in \mathcal{H}_n$ be of finite order.

In this subsubsection, we learn a process for building a strongly synchronizing automaton $\mathscr{A}(A_k^\vee)$ so that ϕ_A acts on the underlying digraph of $\mathscr{A}(A_k^\vee)$ by automorphisms in such a way that $H(\mathscr{A}(A_k^\vee), \phi_A)$ has A as its minimal representative transducer. This process is essential in the proof that follows for finding simplified elements in the conjugacy class representing our given finite order element A. We will also given an example of the process for a specific element.

In [15, Proposition 4.15] it is shown that there is $k \in \mathbb{N}$ such that $A_k^\vee$ is the zero of the semigroup generated by $A^\vee$. Fix the minimal such $k \in \mathbb{N}$ so that $A_k^\vee$ is the zero of the semigroup generated by $A^\vee$, and let $\overline{A_k^\vee}$ be the minimal representative of $A_k^\vee$.

The following is a **very useful fact** from [15]: for every state $[\gamma]$ of the zero $\overline{A_k^\vee}$, there is a word $W([\gamma]) \in Q_A^+$ such that for any input word $s \in Q_A^+$, the output when s is processed from the state $[\gamma]$ of $\overline{A_k^\vee}$ is the word $(W([\gamma]))^l W([\gamma])_{[1,m]}$, where, $|s| = l|W([\gamma])| + m$ and $W([\gamma])_{[1,m]}$ is the length m prefix of $(W([\gamma]))$. It follows from this that $\overline{A_k^\vee}$ has the following structure: for each state $[\gamma]$ (for $\gamma \in X_n^k$) there is $q_{[\gamma]} \in Q_A$ so that for all $p \in Q_A$ we have

- $\pi_{\overline{A_k^\vee}}(p, [\gamma]) = [\gamma] \cdot A$, and
- $\lambda_{\overline{A_k^\vee}}(p, [\gamma]) = q_{[\gamma]}$.

We will call this the *$|Q_A|$-parallel cycle structure of $\overline{A_k^\vee}$*, or less formally, the *cyclical structure of $\overline{A_k^\vee}$*.

Form the automaton $\mathscr{A}(A_k^\vee)$ as follows. The states of $\mathscr{A}(A_k^\vee)$ are the states $[\gamma]$ of $\overline{A_k^\vee}$ and the transitions are given by the rule that for $x \in X_n$, and $[\gamma]$ a state of $\overline{A_k^\vee}$, we set $\pi_{\mathscr{A}(A_k^\vee)}(x, [\gamma]) = [\gamma_{[2,|\gamma|]}x]$. (For this construction it does not matter which $\gamma \in X_n^k$ one picks from the class $[\gamma]$, even though we use γ explicitly in the formula of the transition function: this follows since states of $\overline{A_k^\vee}$ are ω-equivalent classes of $A_k^\vee$.)

The following lemma is immediate from the definitions:

Lemma 3.4. *If $A \in \mathcal{H}_n$ be of finite order and let $k \in \mathbb{N}$ so that $A_k^\vee$ is the zero of the semigroup generated by $A^\vee$ then the automaton $\mathscr{A}(A_k^\vee)$ is strongly synchronizing at level k.*

We also have the following translation (into our context) of the statement of Theorem 4.5 of [4], where $A(G)$ in that theorem corresponds to $\mathscr{A}(A_k^\vee)$ here, and where the group G there is the group $\langle A \rangle$ here.

Theorem 3.5. *Let $A \in \mathcal{H}_n$ be of finite order and let $k \in \mathbb{N}$ so that $A_k^\vee$ is the zero of the semigroup generated by $A^\vee$.*

(a) A acts as an automorphism ϕ_A of the digraph underlying $\mathscr{A}(A_k^\vee)$ by mapping an edge $([\gamma], x, [\gamma_{[2,|\gamma|]}x])$ to the edge $(([\gamma])A, \lambda_A(x, q_\gamma), ([\gamma_{[2,|\gamma|]}x])A)$ where $([\gamma])A = [\lambda_A(\gamma, q)]$ for some $q \in Q_A$,

(b) The minimal representative of the transducer $H(\mathscr{A}(A_k^\vee), \phi_A^i)$ is the transducer A^i.

Example 3.6. Consider the transducer A below. The transducer A of Figure 4 is bi-synchronizing at the second level. The level 2 dual has 36 nodes and so we shall not give this below. However utilising the AutomGrp package [13] in GAP [8], together with (in AutomGrp) the

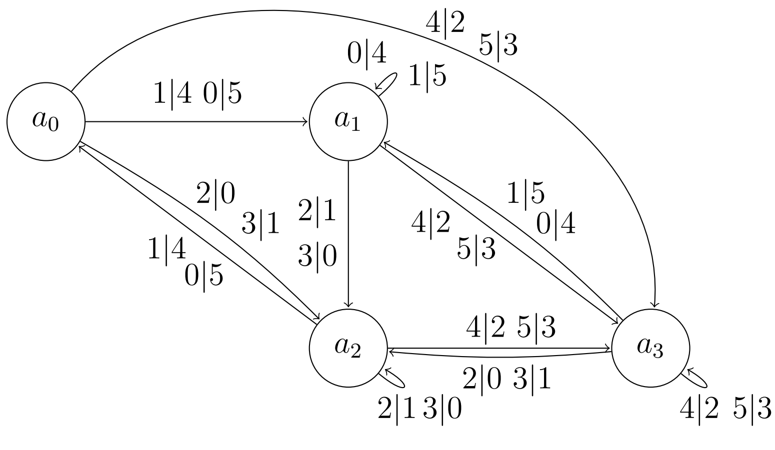

Figure 4: An element $A \in \mathcal{H}_6$ of order 6.

function "MinimizationOfAutomaton( )" which returns an ω-equivalent automaton, applied to the second power of the dual automaton, we get the result $\overline{A_2^\vee}$, depicted in Figure 5 (which is the zero of the semigroup generated by the dual):

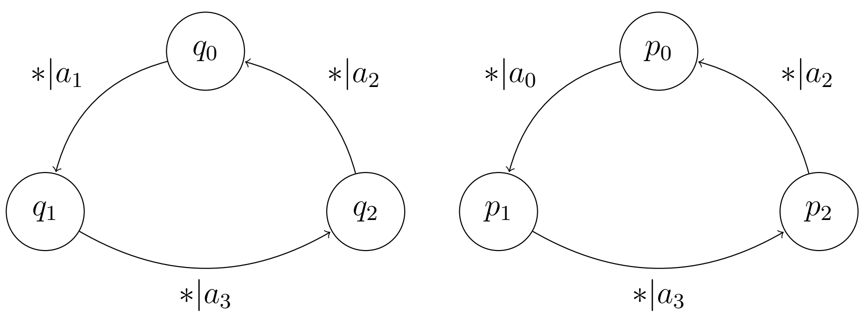

Figure 5: The level 2 dual of A.

Considering the states $\{q_0, q_1, q_2, p_0, p_1, p_2\}$ of $\overline{A_2^\vee}$ as a partition of the words of length 2 over the alphabet $\{0, 1, 2, 3, 4, 5\}$, it is easy to see that

$$\begin{aligned} q_0 &= \{00, 01, 10, 11, 40, 41, 50, 51\} & p_0 &= \{20, 21, 30, 31\} \\ q_1 &= \{24, 25, 34, 35, 44, 45, 54, 55\} & p_1 &= \{04, 05, 15, 15\} \\ q_2 &= \{02, 03, 12, 13, 22, 23, 32, 33\} & p_2 &= \{42, 43, 52, 53\} \end{aligned}$$

by verifying the 36 transitions from q_0 in A using these input words, and cross-checking state-change results against the transitions of $\overline{A_2^\vee}$. From this we can calculate the transitions of $\mathscr{A}(A_2^\vee)$, with the resulting automaton depicted in 6.

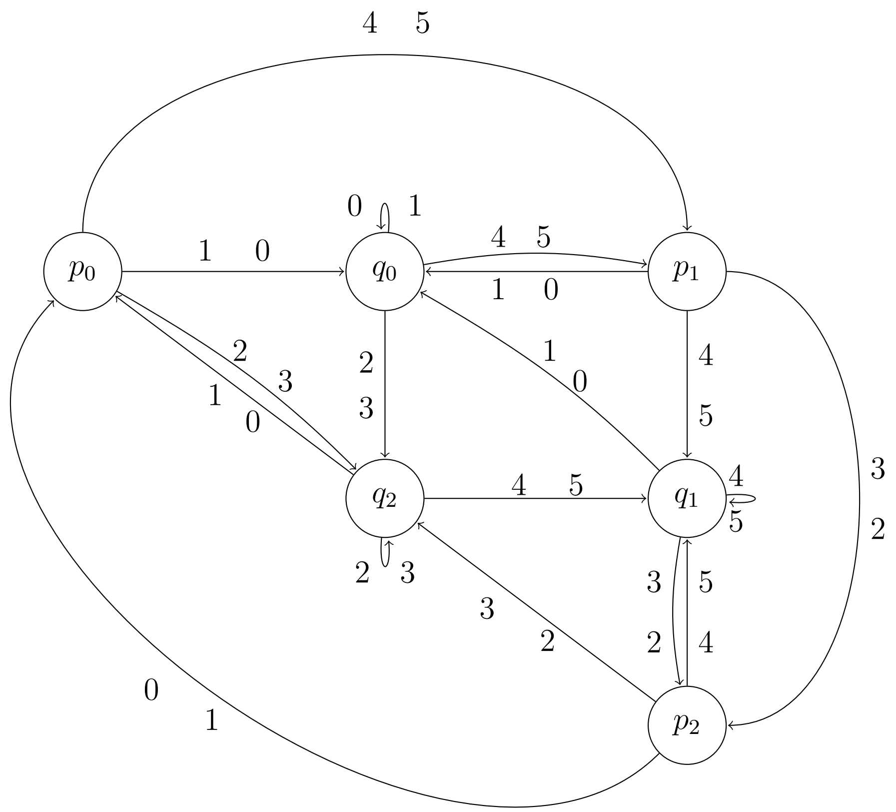

Figure 6: The automaton $\mathscr{A}(A_2^\vee)$

Notice that both the domain and range automaton of A are foldings of $\mathscr{A}(A_2^\vee)$. This phenomenon generalises, that is, for a strongly synchronizing transducer A representing an element of $\mathcal{H}_n$ of finite order, both the domain and range automata of A are foldings of $\mathscr{A}(A_k^\vee)$ (where k is appropriately chosen).

We revisit this example in Section 5.1 where we show that A is conjugate to a 6-cycle.

○

3.3.2 Duals, automata, and automorphisms

In this subsubsection, we will prove that for finite order $A \in \mathcal{H}_n$ and minimal k so that $A_k^\vee$ is the zero of the semigroup generated by $A^\vee$, that $\mathscr{A}(A_k^\vee)$ as defined above is the minimal (strongly synchronizing) automaton so that A can act on $\mathscr{A}(A_k^\vee)$ as an automorphism ϕ_A, with $(\mathscr{A}(A_k^\vee), \phi_A)$ inducing A.

We first require lemmata exploring the relationship between properties of $\mathscr{A}(A_k^\vee)$ and of

$A_k^\vee$.

Our first step is the following useful lemma about the automaton $\mathscr{A}(A_k^\vee)$ constructed as above from a finite order element $A \in \mathcal{H}_n$. In essence, it says that if two states $[\delta]$ and $[\gamma]$ are distinct in $\mathscr{A}(A_k^\vee)$ but their two transition functions are the same, then by following the cycles of the level k dual (by iteratively acting by A), we will eventually get to a pair of states which have different output letters in the level k dual, and at that pair of locations, the states of $\mathscr{A}(A_k^\vee)$ will still transition the same way, but the output functions of $H(\mathscr{A}(A_k^\vee), \phi_A)$ at these states will disagree at the first letter.

Lemma 3.7. *Let $A \in \mathcal{H}_n$ be finite order. Let $\gamma, \delta \in X_n^k$ be such that the states $[\gamma], [\delta]$ of $\mathscr{A}(A_k^\vee)$ are distinct. Suppose moreover that the maps $\pi_{\mathscr{A}(A_k^\vee)}(\cdot, [\gamma])$ and $\pi_{\mathscr{A}(A_k^\vee)}(\cdot, [\delta])$ coincide. Then there is a natural i with $0 \leq i < o(A)$ and $x, y, y' \in X_n$ such that $y \neq y'$, $\pi_{\mathscr{A}(A_k^\vee)}(\cdot, [\gamma]A^i) = \pi_{\mathscr{A}(A_k^\vee)}(\cdot, [\delta]A^i)$ but A maps the edges*

$$([\gamma]A^i, x, \pi_{\mathscr{A}(A_k^\vee)}(x, [\gamma]A^i)) \text{ and } ([\delta]A^i, x, \pi_{\mathscr{A}(A_k^\vee)}(x, [\delta]A^i))$$

respectively to the edges

$$([\gamma]A^{i+1}, y, \pi_{\mathscr{A}(A_k^\vee)}(y, [\gamma]A^{i+1})) \text{ and } ([\delta]A^{i+1}, y', \pi_{\mathscr{A}(A_k^\vee)}(y', [\delta]A^{i+1})).$$

Proof. Let $w = W([\gamma])$ and $v = W([\delta])$. Since $[\gamma] \neq [\delta]$, we may find words $u, w_2, v_2 \in Q_A^*$ and letters $t \neq t' \in Q_A$ such that $w = utw_2$ and $v = ut'v_2$. Set $i - 1 := |u|$. We note that for any $j \in \mathbb{N}$ with $j \leq i-1$, a straightforward induction argument shows, the edges $([\gamma], a, \pi_{\mathscr{A}(A_k^\vee)}(a, [\gamma])A)$ and $([\delta], a, \pi_{\mathscr{A}(A_k^\vee)}(q, [\delta]))$ map respectively under A^j to edges $([\gamma]A^j, b, \pi_{\mathscr{A}(A_k^\vee)}(a, [\gamma])A^j)$ and $([\delta]A^j, b, \pi_{\mathscr{A}(A_k^\vee)}(q, [\delta])A^j)$, where $b = \lambda_{A^j}(a, u_{[1,j]})$ (if $j = 0$, take $b = a$). In particular it follows that $\pi_A(\cdot, t) = \pi_A(\cdot, t')$ and so, since $t \neq t'$, there is an $a \in X_n$ be such that $y := \lambda_A(a, t) \neq \lambda_A(a, t') = y'$. Let $x \in X_n$ be such that $\lambda_{A^{i-1}}(x, u) = a$. Then it follows that the edges

$$([\gamma]A^i, x, \pi_{\mathscr{A}(A_k^\vee)}(x, [\gamma]A^i)) \text{ and } ([\delta]A^i, x, \pi_{\mathscr{A}(A_k^\vee)}(x, [\delta]A^i))$$

are mapped respectively under A, to the edges

$$([\gamma]A^{i+1}, y, \pi_{\mathscr{A}(A_k^\vee)}(y, [\gamma]A^{i+1})) \text{ and } ([\delta]A^{i+1}, y', \pi_{\mathscr{A}(A_k^\vee)}(y', [\delta]A^{i+1})).$$

□

Recall from Subsection 2.7 that if $A \in \mathcal{H}_n$ and B is an automaton so that there is a digraph automorphism $\phi : G_B \to G_B$ so that A and $H(B, \phi)$ represent the same transformation then we say A *is induced from* (B, ϕ).

Let $A \in \mathcal{H}_n$. We say a strongly synchronizing automaton B *is an automaton supporting* A if there is a digraph automorphism ϕ of the digraph G_B, with A induced from (B, ϕ). In this situation, if there is no proper folding B' of B and digraph automorphism $\phi' : G_{B'} \to G_{B'}$ so that A is induced from (B', ϕ'), then we say B *is a minimal automaton supporting* A (or simply, that B is minimal).

In the next lemma, we show that there is precisely one minimal automaton (up to isomorphism of automata) supporting a finite order element A of $\mathcal{H}_n$.

Lemma 3.8. *Let $A \in \mathcal{H}_n$ be an element of finite order and let $k \in \mathbb{N}$ be minimal such that $A_k^{\vee}$ is the zero of the semigroup generated by the dual. Then (up to isomorphism of automata) $\mathscr{A}(A_k^{\vee})$ is the minimal strongly synchronizing automaton admitting an automorphism ϕ of $G_{\mathscr{A}(A_k^{\vee})}$ so that A is induced by $(\mathscr{A}(A_k^{\vee}), \phi)$. Furthermore, ϕ is the automorphism ϕ_A of Theorem 3.5.*

Proof. Let $A \in \mathcal{H}_n$ be finite order of order $o(A)$. We note that by results in [15, 4] k is minimal such that all of the elements $A, A^2, \ldots, A^{o(A)-1}$ are strongly synchronizing at level k (A^i being the product in $\mathcal{H}_n$ of A with itself i times).

It follows from Theorem 3.5 that $\mathscr{A}(A_k^{\vee})$ is an automaton supporting A and indeed that $(\mathscr{A}(A_k^{\vee}), \phi_A)$ induces A. We argue below that $\mathscr{A}(A_k^{\vee})$ is a minimal such automaton, and further, that any minimal automaton supporting A is isomorphic to a folding of $\mathscr{A}(A_k^{\vee})$, and hence, must actually be $\mathscr{A}(A_k^{\vee})$ up to isomorphism.

Now suppose that there was another automaton B, such that A acts as an automorphism ψ_A of the underlying digraph of B so that $H(B, \psi_A)$ has minimal representative A. Additionally suppose that B is a minimal strongly synchronizing transducer on which A acts as an automorphism. We note that the minimal synchronizing level l of B is greater than or equal to k for, $H(B, \psi_A^i)$ is strongly synchronizing at level l and has minimal representative A^i.

Suppose for a contradiction that $B \neq \mathscr{A}(A_k^{\vee})$. There are two cases.

Firstly for any state $q \in Q_B$, there is a state $p \in Q_A$ such that the set $W(q, j)$ of words of length j which force q is contained in the set $W(p, j)$ of words of length j which force the state p of $\mathscr{A}(A_k^{\vee})$. In this case, one observes that $\mathscr{A}(A_k^{\vee})$ is a folding of B contradicting the minimality of B.

Thus we must be in the negation of the first case. That is, we assume that there is a pair of words $\gamma, \delta \in X_n^k$ such that the state of B forced by γ is the same as the state of B forced by δ but γ and δ force different states of $\mathscr{A}(A_k^{\vee})$. We may further assume that the states $[\gamma], [\delta]$ of $\mathscr{A}(A_k^{\vee})$ also satisfy $\pi_{\mathscr{A}(A_k^{\vee})}(\cdot, [\gamma]) = \pi_{\mathscr{A}(A_k^{\vee})}(\cdot, [\delta])$. This is because if $\pi_{\mathscr{A}(A_k^{\vee})}(\cdot, [\gamma]) \neq \pi_{\mathscr{A}(A_k^{\vee})}(\cdot, [\delta])$, then we may find a word $\nu \in X_n^+$ such that $[\gamma'] := \pi_{\mathscr{A}(A_k^{\vee})}(\nu, [\gamma]) \neq \pi_{\mathscr{A}(A_k^{\vee})}(\nu, [\delta]) = [\delta']$, satisfy $\pi_{\mathscr{A}(A_k^{\vee})}(\cdot, [\gamma']) = \pi_{\mathscr{A}(A_k^{\vee})}(\cdot, [\delta]')$. Thus $\gamma\nu$ and $\delta\nu$ force the same state of B but force, respectively, the states $[\gamma']$ and $[\delta']$ of $\mathscr{A}(A_k^{\vee})$. We may then replace γ, δ with γ', δ'.

Let z_1 be the state of B forced by γ and δ and let $z_1, z_2, \ldots, z_{o(A)}$ be the orbit of z_1 under the action of A. As $H(B, \psi_A) = H(\mathscr{A}(A_k^{\vee}), \phi_A)$, it must be the case that if $a, b \in X_n$ are such that the edge $([\gamma], a, [\Gamma])$ maps to $(([\gamma])A, b, ([\Gamma])A)$, then the edge $([\delta], a, [\Gamma])$ also maps to $(([\delta])A, b, ([\Gamma])A)$. Thus we conclude that $\pi_{\mathscr{A}(A_k^{\vee})}(\cdot, ([\gamma])A) = \pi_{\mathscr{A}(A_k^{\vee})}(\cdot, ([\delta])A)$. Now observe that since γ and δ are representatives of $[\gamma]$ and $[\delta]$, respectively, and since for any $q \in Q_A$, the state of B forced by $\lambda_A(\gamma, q)$ is equal to the state of B forced by $\lambda_A(\delta, q)$ is equal to z_2, it follows that there are representatives of $([\gamma])A$ and $([\delta])A$ respectively such that the states of B forced by these representative is z_2. We may thus repeat the argument in the z_1 case. By induction we therefore see that for any $1 \leq i \leq o(A)$, the points $([\gamma])A^i$ and $([\delta])A^i$ satisfy that $\pi_{\mathscr{A}(A_k^{\vee})}(\cdot, ([\gamma])A^i) = \pi_{\mathscr{A}(A_k^{\vee})}(\cdot, ([\delta])A^i)$ and whenever there are $a, b \in X_n$, such that $(([\gamma])A^i, a, \nu)$ is an edge mapping under A to the edge $(([\gamma])A^{i+1}, b(\nu)A$, then the edge $(([\delta])A^i), a, \nu)$ also maps under A to $(([\delta])A^{i+1}), b, (\nu)A)$. This contradicts Lemma 3.7. $\square$

4 Water for the witch – shrinking conjugacy class representatives

Suppose we have a finite order element $A \in \mathcal{H}_n$, induced by (B, ϕ_A) for some strongly synchronizing B with a minimal number of states. Under certain conditions we may employ a two-step process to find a new element $C \in \mathcal{H}_n$, where C is conjugate to A, and C is induced by (D, ψ) for some strongly synchronizing D with D having fewer states than B. In what follows we describe this process of finding "smaller" conjugacy class representatives of A.

The first (and main) step in this process is to employ "relabelling." This is a conjugacy which, for a pair of states that would be identified in the collapse sequence of the domain automaton, relabels inputs and outputs on edges from this pair of states, with the goal of making this pair of states represent the same local map. If this is possible, then we can collapse the carrying transducer to a smaller one than we started with.

The conditions for a successful relabelling include that the orbits of these states have the same lengths, and that for any two corresponding outgoing edges, these orbit lengths of these edges are also the same. In the case where some of these orbit lengths differ, then in certain circumstances we can employ the second step of the overall process. This step"fluffs up" the carrying automaton by executing some splittings, creating what we call *shadow states*, and where we can then employ relabelling to the result. In either case, after a relabelling, the whole resultant transducer can be minimised so as to be carried by a transducer with strictly fewer states than T_A.

In the case that A is conjugate to an n-cycle this process will eventually result in single state transducer representing an n-cycle.

4.1 Relabellings and automata sequences

Definition 4.1. Let A be a strongly synchronizing automaton and $A = A_0, A_1, \ldots, A_m$ be a collapse chain of A. Let $0 \leq k \leq m$ and ϕ_k be a vertex fixing automorphism of G_{A_k}. Define A' to be the automaton with $Q_{A'} = Q_A$ and transition function defined as follows: for $p \in Q_A$, set $\pi_{A'}(x', p) = q$ if and only if there is an $x \in X_n$ such that $\pi_A(x, p) = q$ with $\lambda_{H(A_k,\phi_k)}(x, [p]) = x'$. We call A' the *relabelling of A by (A_k, ϕ_k)* or *the relabelling of A by (the transducer) $H(A_k, \phi_k)$*.

Note that if we relabel A by (A_k, ϕ_k), then the resulting automaton A' is *strongly isomorphic* to A in the sense that there is a natural digraph isomorphism from the underlying digraph of A' to the underlying digraph of A that fixes states and which maps the relabelled edges of A' to the original edges in A. More precisely, if (p, x, q) is an edge of G_A and $\lambda_{H(A_k,\phi_k)}(x, [p]) = x'$, then the natural digraph isomorphism maps the edge (p, x', q) of

A' to the edge (p, x, q) of A. The point of view one should have in mind is that we have renamed/relabelled the edges of A by switching edge labels on edges which are parallel edges in A_k. Notice that if we relabel by (A_0, ϕ_0), then all we do is switch labels on parallel edges in A, thus the resulting underlying digraph would not change, but a "fixed" drawing of it would be relabelled.

Lemma 4.2. *Let A be a strongly synchronizing automaton and $A = A_0, A_1, \ldots, A_m$ be a collapse chain for A. Let $0 \leq k \leq m$ and ϕ be a vertex fixing automorphism of G_{A_k}. Let A' be the relabelling of A by (A_k, ϕ). Then A' has underlying digraph strongly isomorphic to the underlying digraph of A and A_m remains a folding of A'. More specifically, writing $A' = A'_0, A'_1, \ldots, A'_l$ for the collapse chain from A' to A_m, then $l \leq m$ and two states of u, v of A belong to the same state of A_i if and only if for some $i' \leq i$ we have u and v belong to the same state of $A'_{i'}$.*

Proof. We may consider A as a non-minimal synchronizing transducer where each state induces the identity transformation of the set X_n. Consider the core of the product $A * H(A_k, \phi)$. Let $p \in Q_A$, and $\gamma \in X_n^+$ be such that the state of A forced by γ is p. Then, by definition of A_k, the state of A_k forced by γ is the state $[p]$ containing p. Thus the set of states of $\text{core}(A * H(A_k, \phi))$ is the set $\{(p, [p]) \mid p \in Q_A\}$. Let $x \in X_n$ and $p, q \in Q_A$ such that $\pi_A(x, p) = q$. Then we have, $\pi_A(x, (p, [p])) = (q, [q])$ and $\lambda_A(x, (p, [p])) = \lambda_{H(A_k,\phi)}(x, [p])$. Thus setting A' to be the output automaton of $\text{core}(A * H(A_k, \phi))$ we see that A' is the relabelling of A by (A_k, ϕ). From this it follows that the underlying digraph of A' is strongly isomorphic to the underlying digraph of A.

Let u, v be two states of A which belong to the same state of A_m and which transition identically on all words of length j and suppose j is minimal for which this happens. Let $p \in Q_A$ be an arbitrary state and let $W(p) \subseteq X_n^j$ consist of those words γ such that $\pi_A(\gamma, u) = \pi_A(\gamma, v) = p$. We break into cases based on whether or not $k \geq j$ or $k < j$.

First suppose that $k \geq j$. This means that in A_k, the states $[u]$ and $[v]$ are equal. Thus, $\lambda_{H(A_k,\phi)}(\gamma, [u]) = \lambda_{H(A_k,\phi)}(\gamma, [v])$ for any $\gamma \in X_n^*$. Therefore in A' we see that the set of words $\nu \in X_n^j$ for which $\pi_{A'}(\nu, u) = \pi_{A'}(\nu, v) = p$ is precisely the set $\{\lambda_{H(A_k,\phi)}(\gamma, [u]) \mid \gamma \in W(p)\}$.

Now suppose that $k < j$. This means that the states $[u]$ and $[v]$ are distinct states of A_k such that $\pi_{A_k}(\cdot, [u])$ and $\pi_{A_k}(\cdot, [v])$ coincide on X_n^{j-k}. Let $\gamma \in W(p)$ be arbitrary. Set γ_1 to be the length $j - k$ prefix of γ and set $\gamma_2 \in X_n^k$ such that $\gamma_1\gamma_2 = \gamma$. Set $[r] = \pi_{A_k}(\gamma_1, [u]) = \pi_{A_k}(\gamma_1, [v])$ and set $\kappa \in X_n^k$ such that $\lambda_{H(A_k,\phi}(\kappa, [r]) = \gamma_2$. For $t \in \{u, v\}$, set $\delta_t \in X_n^{j-k}$ be such that $\lambda_{H(A_k,\phi)}(\delta_t, [t]) = \gamma_1$. Then since ϕ is a vertex fixing automorphism of A_k we notice that $\pi_A(\delta_u, u)$, $\pi_A(\delta_v, v)$, $\{\pi_A(\gamma_1, t) \mid t \in \{u, v\}\}$ all belong to the same state of A_k. This means that $\pi_A(\kappa, \pi_A(\delta_u, u)) = \pi_A(\kappa, \pi_A(\delta_v, v)) = s$.(Note that $[s] = [p]$ in A_k by the vertex fixing property of ϕ.) Therefore $\pi_{A*H(A_k,\phi)}(\delta_u\kappa, (u, [u])) = (s, [p]) = \pi_{A*H(A_k,\phi)}(\delta_v\kappa, (v, [v]))$. Since $\lambda_{A*H(A_k,\phi)}(\delta_u\kappa, (u, [u])) = \gamma = \lambda_{A*H(A_k,\phi)}(\delta_v\kappa, (v, [v]))$, we see that in A', $\pi_{A'}(\gamma, u) = \pi_{A'}(\gamma, v)$.

Therefore, in A', $\pi_{A'}(\cdot, u)$ and $\pi_{A'}(\cdot, v)$ coincide on the set $W(p)$. Since p was chosen arbitrarily and $\sqcup_{p \in Q_A} W(p) = X_n^j$ we conclude that $\pi_{A'}(\cdot, u)$ and $\pi_{A'}(\cdot, v)$ coincide on the set X_n^j.

The result now follows by Theorem 2.8.

Now suppose that there are states u, v of A which belong to the same state $A'_{i'}$ for some $0 \leq i' \leq l$. Then since u, v belong to the same state of A_m, there is an i between 0 and m such that u and v belong to the same state of A_i. The preceding paragraph and Theorem 2.8 show that i' must be less than or equal to i. □

Let A be a strongly synchronizing automaton and A' be the relabelling of A by (A_k, ϕ_k). Set $\iota : G_A \to G_{A'}$ to be the natural digraph isomorphism. If φ is an automorphism of the underlying digraph G_A of A, then we will mean by the *induced automorphism* φ' of $G_{A'}$ precisely the map $\iota^{-1}\varphi\iota$.

Lemma 4.3. *Let $A \in \mathcal{H}_n$ be an element of finite order and let B be a strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph of B with A the minimal representative of $H(B, \phi_A)$. Let B_k be an element of the synchronizing sequence of B and ψ a vertex fixing automorphism of B_k. Let B' be the relabelling of B according to (B_k, ψ) and φ be the induced isomorphism from the underlying digraph of B to the underlying digraph of B'. Set P to be the minimal representative of the transducer $H(B, B', \varphi)$. Then $P^{-1}AP$ is the minimal representative of $H(B', \phi_A^{\varphi})$.*

Proof. This is a straight-forward application of the definitions. □

In the situation of Lemma 4.3 we refer to the resulting transducer $P^{-1}AP$ as the *transducer induced from A by the relabelling $B \mapsto B'$*.

Lemma 4.4. *Let A be a strongly synchronizing automaton, and let s, t be distinct states of A. Let $(A_i)_{1 \leq i \leq m}$ be a collapse chain of A such that s, t belong to the same state of A_m. Let $1 \leq k < m$ be minimal such that t belongs to the state $[s]$ of the automaton A_{k+1}. Then for all $x, x' \in X_n$ such that $\pi_A(x, s) = \pi_A(x', t)$ and $[v] \in \{[s], [t]\}$, states of A_k, we have $\pi_{A_k}(x, [v]) = \pi_{A_k}(x', [v])$.*

Proof. By minimality of k, it must be the case that the states $[s]$ and $[t]$ of A_k are distinct and the equality $\pi_{A_k}(\cdot, [s]) = \pi_{A_k}(\cdot, [t])$ holds.

Let $x, x' \in X_n$ and $u \in Q_A$ be such that $\pi_A(x, s) = \pi_A(x', t) = u$. Then by definition of A_k, $\pi_{A_k}(x, [s]) = [u] = \pi_{A_k}(x', [t])$. However, the equality $\pi_{A_k}(\cdot, [s]) = \pi_{A_k}(\cdot, [t])$, now implies that $\pi_{A_k}(x', [s]) = [u] = \pi_{A_k}(x, [t])$ also. □

4.1.1 Constructing discriminant permutations $\mathrm{disc}(s, t, Q)$

Let A be an automaton and let $s, t \in Q_A$. Set the notation:

$$\mathrm{E}_A(s,t) := \{(s,x,t) \in \mathrm{E}_A\}; \textit{and}$$
$$\mathrm{Letters}_A(s,t) := \{x \in X_n \mid (s,x,t) \in \mathrm{E}_A(s,t)\}.$$

We may leave out the explicit mention of the automaton A when it is clear from context, writing simply $\mathrm{E}(s,t)$ and $\mathrm{Letters}(s,t)$ for these sets in this case.

Let $Q \subseteq Q_A$ and $s \in Q_A$. Set the notation

$$X_{s,Q} := \bigsqcup_{p \in Q} \text{Letters}(s,p).$$

Now, suppose $s, t \in Q_A$ and suppose further there is a subset $Q \subseteq Q_A$ so that

(a) $X_{s,Q} = X_{t,Q}$, and

(b) for all $p \in Q$ we have $\left|\text{Letters}(s,p)\right| = \left|\text{Letters}(t,p)\right|$.

Then to describe this situation we say *s and t distribute similarly over Q*. (Note in passing that for some choices of s and t the only possible such set Q may be empty.) For any states s and t and set $Q \subset Q_A$ so that s and t distribute similarly over Q, we denote by X_Q the set $X_{s,Q} = X_{t,Q}$. We call $X_Q \subseteq X_n$ *the agreement alphabet (of s and t on Q)* noting that if $Q = Q_A$, then $X_Q = X_n$.

Define a bijection $\text{disc}(s,t,Q) : X_Q \to X_Q$ as follows.

First, let $p_1, \ldots, p_r \in Q$ be a maximal sequence of distinct states such that for $1 \leq i \leq r$ there is an $x \in X_Q$ with $\pi_A(x,s) = p_i$. Observe that the sets

$$\{\text{Letters}(s,p_i) \mid 1 \leq i \leq r\}$$

and

$$\{\text{Letters}(t,p_i) \mid 1 \leq i \leq r\}$$

form partitions of X_Q, with equal-size corresponding parts in index i.

Now, for $1 \leq i \leq r$, set $\text{disc}(s,t,Q)$ to act as the identity on $\text{Letters}(s,p_i) \cap \text{Letters}(t,p_i)$. Set

$$\text{Letters}(s,p_i)' := \text{Letters}(s,p_i) \backslash (\text{Letters}(s,p_i) \cap \text{Letters}(t,p_i))$$

and

$$\text{Letters}(t,p_i)' := \text{Letters}(t,p_i) \backslash (\text{Letters}(s,p_i) \cap \text{Letters}(t,p_i)).$$

We note that $|\text{Letters}(s,p_i)'| = |\text{Letters}(t,p_i)'|$ and indeed that

$$Y_{s,t} := \bigcup_{1 \leq i \leq r} \text{Letters}(s,p_i)' = \bigcup_{1 \leq i \leq r} \text{Letters}(t,p_i)'.$$

Order the elements of $\text{Letters}(s,p_i)'$ and $\text{Letters}(t,p_i)'$ with the order induced from X_n. For $1 \leq i \leq r$ and $x \in \text{Letters}(s,p_i)'$ we write x' for the corresponding element of $\text{Letters}(t,p_i)'$, that is, in the ordering of $\text{Letters}(s,p_i)'$ and $\text{Letters}(t,p_i)'$ induced from X_n, x and x' have the same index.

Using the definitions and facts above we extend the definition of $\text{disc}(s,t,Q)$ over the set $Y_{s,t}$ by the rule $x \mapsto x'$. One easily checks that the resulting function

$$\text{disc}(s,t,Q) : X_Q \to X_Q$$

is a well-defined bijection. Further, observe that for $x_0 \in Y_{s,t}$ the function $\mathrm{disc}(s,t,Q)$ contains a cycle $(x_0\ x_1\ x_2\ \ldots\ x_{k-1})$ in its disjoint cycle decomposition, where for all i we have $x_{i+1} = x_i'$ (indices taken mod k). Recall as well that $\mathrm{disc}(s,t,Q)$ acts as the identity over the set $X_Q \backslash Y_{s,t}$.

For s and t satisfying points (b) and (b) for some set Q we call $\mathrm{disc}(s,t,Q)$ *the discriminant of s and t*; it is a permutation that encodes the difference in transitions between s and t amongst the set of states Q. In the case that $Q = Q_A$, we will write $\mathrm{disc}(s,t)$ for the bijection $\mathrm{disc}(s,t,Q_A)$. As with the notation $\mathrm{Letters}(p,q)$, we often run in to situations where we compute discriminant permutations in distinct automata sharing the same state set, in such cases we use the notation $\mathrm{disc}_A(s,t,Q)$ and $\mathrm{disc}(s,t)$ to emphasise the automaton in which the permutation is computed.

Lemma 4.5. *Let A be a strongly synchronizing automaton, and let s,t be distinct states of A. Let $Q \subseteq Q_A$ be such that s and t distribute similarly over Q with agreement alphabet X_Q. Let $(A_i)_{1 \le i \le m}$ be a collapse chain of A such that s,t belong to the same state of A_m. Let $1 \le k < m$ be minimal such that $\pi_{A_k}(\cdot,[t])$ and $\pi_{A_k}(\cdot,[s])$ are equal on X_Q. Then for $x,y \in X_Q$ which belong to the same disjoint cycle of* $\mathrm{disc}(s,t,Q)$,

$$\pi_{A_k}(x,[s]) = \pi_{A_k}(y,[s]) = \pi_{A_k}(y,[t]) = \pi_{A_k}(x,[t]).$$

Proof. By assumption $\pi_{A_k}(\cdot,[s]) = \pi_{A_k}(\cdot,[t])$.

An easy induction argument using the definition of $\mathrm{disc}(s,t,Q)$ now shows that for any $x,y \in X_n$ such that y belongs to the orbit of x under the action of $\mathrm{disc}(s,t,Q)$,

$$\pi_{A_k}(x,[s]) = \pi_{A_k}(y,[s]) = \pi_{A_k}(x,[t]) = \pi_{A_k}(y,[t]).$$

This follows since for any $x \in X_n$, $\pi_A(x,s) = \pi_A((x)\,\mathrm{disc}(s,t,Q),t)$.

□

4.1.2 Discriminant permutations and amalgamation sequences

Let B be an automaton and $G := G_B$ be the underlying digraph of B. Define a sequence $G := G_0, G_1, \ldots$ as follows. Assuming G_i is defined, G_{i+1} is obtained from G in the following manner. Let $\sim$ be the equivalence relation on the vertices Q_{G_i} of G_i that relates two vertices p,q precisely when for every vertex $t \in Q_{G_i}$ the number of edges from q to t is precisely the number of edges from p to t. If $p \in Q_{G_i}$ write $[p]_{i+1}$ for the equivalence class of p under the relation $\sim$. Set $Q_{G_{i+1}} = \{[p]_{i+1} \mid p \in Q_{G_i}\}$. Now suppose $p,q \in Q_{G_i}$ and enumerate those elements of $[q]_{i+1}$ which have an incoming edge from a vertex in $[p]_{i+1}$ in some order as $q_1, q_2, \ldots, q_r$. For $1 \le j \le r$, let k_j be the number of edges from p to q_j and set $ec(i+1,p,q) := \sum_{1 \le j \le r} k_j$. Set G_{i+1} to be the directed graph with vertices $Q_{G_{i+1}}$ and with $ec(i+1,p,q)$ many edges from $[p]_{i+1}$ to $[q]_{i+1}$ for each $[p]_{i+1}$, $[q]_{i+1} \in Q_{G_{i+1}}$.

We refer to the resulting sequence G_0, G_1, $\ldots$, as defined above as the *amalgamation sequence of G* (see [17]). Note that for each natural i the construction above induces an identification of the states of G_i with a partition of B. It follows that after finitely many steps, the amalgamation sequence stabilises to a fixed digraph.

The lemma below says that for a given automaton B, there is a relabelling of B such that the synchronizing sequence coincides with the amalgamation sequence.

Lemma 4.6. *Let B be an automaton with underlying digraph G and synchronizing sequence $B = B_0, B_1, \ldots$. Let $G = G_0, G_1, \ldots$ be the amalgamation sequence of G. Then there is a relabelling D of B such that if $D = D_0, D_1, \ldots$ is the synchronizing sequence of D, the underlying digraph of D_i is G_i; in particular, the partition of the state set of B induced by D_i is the same partition induced by G_i.*

Proof. Since B is strongly synchronizing there is a minimal $l \in \mathbb{N}$ for which $G_l = G_{l+1}$ and both have a single vertex with n loops. We proceed by induction on the amalgamation sequence.

We begin with the base case. Let $s, t \in Q_B$ be distinct such that s and t belong to the same state of G_1. This means that s and t distribute similarly over Q_B. Suppose that $\mathrm{disc}(s, t)$ is not trivial.

Let $k \in \mathbb{N}$ be minimal such that s and t belong to the same state of B_{k+1}. Note that since $\mathrm{disc}(s, t)$ is not trivial, then $k \geq 1$. By Lemma 4.5, for any x, y which belong to the same orbit under $\mathrm{disc}(s, t)$,

$$\pi_{B_k}(x, [s]) = \pi_{B_k}(y, [s]) = \pi_{B_k}(x, [t]) = \pi_{B_k}(x, [t]).$$

Let λ_{B_k} be defined such that $\lambda_{B_k}(\cdot, [q]) : X_n \to X_n$ is trivial whenever $[q]$ is not equal to $[t]$. We set $\lambda_{B_k}(\cdot, [t]) = \mathrm{disc}(s, t)^{-1}$. We note that the transducer B_k is induced by a vertex fixing automorphism of B_k. Furthermore, for any pair $(u, v) \neq (s, t)$ such that u, v belong to the same state of G_1 and $\mathrm{disc}(u, v)$ is trivial, $[u] = [v]$ in B_k.

Let E be the relabelling of B by the transducer B_k. Note that $Q_E = Q_B$ and G remains the underlying digraph of E. It therefore follows that for any pair u, v in B which distribute similarly over Q_B, u, v still distribute similarly over Q_B in E. If moreover, $\mathrm{disc}_B(u, v)$ is trivial, then construction of λ_{B_k}, means $\mathrm{disc}_E(u, v)$ remains trivial. Lastly we note that s, t distribute similarly over Q_B in E, and $\mathrm{disc}_E(s, t)$ is trivial.

Applying an induction argument, there is an automaton E_1 a relabelling of B such that for any pair $s, t \in Q_B$ which belong to the same state of G_1, $\mathrm{disc}_{E_1}(s, t)$ is trivial. In particular, such s, t satisfy, $\pi_{E_1}(\cdot, s) = \pi_{E_1}(\cdot, t)$.

Now assume by induction that there is a relabelling E of B with synchronizing sequence $E = E_0, E_1, \ldots$ possessing the following property: for $0 \leq i \leq k < l$ two states $s, t \in Q_B$ belonging to the same state of G_i belong to the same state of E_i.

Let $s, t \in Q_B$ and suppose s and t belong to the same state of G_{k+1} but do not belong to the same state of E_{k+1}. We note that since the underlying digraph of E_k is the same as G_k and they induce the same partition of the state set Q_B, then s and t belong to distinct states of E_k and so to distinct states of G_k. The fact that s and t belong to the same state of G_{k+1} means that $[s]$ and $[t]$ distribute similarly over Q_{E_k} but $\mathrm{disc}_{E_k}([s], [t])$ is not trivial.

Let $k < j \leq l$ be minimal such that s and t belong to the same state of E_{j+1}. By Lemma 4.5 once more, we have the equalities: for any x, y which belong to the same orbit under $\mathrm{disc}_{E_k}([s], [t])$,

$$\pi_{E_j}(x, [s]) = \pi_{E_j}(y, [s]) = \pi_{E_j}(x, [t]) = \pi_{E_j}(x, [t]).$$

Let λ_{E_j} be defined such that $\lambda_{E_j}(\cdot,[q]) : X_n \to X_n$ is trivial whenever $[q]$ is not equal to $[t]$. We set $\lambda_{E_j}(\cdot,[t]) = \mathrm{disc}_{E_k}([s],[t])^{-1}$. We note that the transducer E_j is induced by a vertex fixing automorphism of E_j. Furthermore, for any pair $(u,v) \neq (s,t)$ such that u,v belong to the same state of G_{k+1} and $\mathrm{disc}_{E_k}([u],[v])$ is trivial, $[u]=[v]$ in E_j.

Let F be the relabelling of E by the transducer E_j. Let $F_1, F_2 \ldots$ be the synchronizing sequence of F.

Let $u,v \in Q_B$ belong to the same state of G_i for some $0 \le i \le k < l$. Then by the inductive assumption and Lemma 4.2, u,v belong to the same state of F_i.

Let $u,v \in Q_B$ belong to the same state of G_{k+1} and suppose that $\mathrm{disc}_{E_k}(u,v)$ is trivial. Note that since $\mathrm{disc}_{E_k}(u,v)$ and $[u],[v]$ distribute similarly over Q_{E_k}, $[u]=[v]$ in E_{k+1}. Therefore, Lemma 4.2 implies that $[u]=[v]$ in F_{k+1} as well.

Lastly observe that $[s]=[t]$ in F_{k+1} by construction of λ_{E_k} and the fact that states which are identified in E_k remain identified in F_{k+1}.

The result now follows by induction. $\square$

4.2 Relabellings along orbits

For lemma below, we give stronger hypotheses than appear to be required as per the following observation. Let B be a strongly synchronizing automaton, ϕ an automorphism of the underlying digraph G_B of B, and, s and p states of B. Every edge from s to a state in the orbit of p (under the action of ϕ) is on an orbit of length N (when such an edge exists) if and only if every edge from any state in the orbit of s to a state in the orbit of p is on an orbit of length N (when such an edge exists). We state the lemma with the stronger hypotheses below to ease understanding.

Lemma 4.7. *Let B be a strongly synchronizing automaton and ϕ an automorphism of the underlying digraph G_B of B. Let s,p be vertices of G_B so that* $\mathrm{Letters}_B(s,p)$ *is non-empty. Suppose*

- *there is $N \in \mathbb{N}_1$ so that for every edge e from a vertex in the orbit of s to a vertex in the orbit of p, the orbit length of e is N, and secondly*

- *there is $r \in \mathbb{N}_1$ so that if $(s\phi^i, y, p\phi^j)$ is any edge from the orbit of s to the orbit of p, then we have* $\mathrm{Letters}(s\phi^i, p\phi^j) = \mathrm{Letters}(s\phi^{i+r}, p\phi^j)$.

Then there is a relabelling of B' of B such that the induced automorphism ϕ' of $G_{B'}$ satisfies the following: for any $i,j \in \mathbb{N}$,

- $\mathrm{Letters}_{B'}(s\phi^i, p\phi^j) = \mathrm{Letters}_{B'}(s\phi^{i+r}, p\phi^j)$*, and,*

- *if $x \in \mathrm{Letters}_{B'}(s\phi^i, p\phi^j)$, then the labels of the edges $(s\phi'^i, x, p\phi'^j)\phi'$ and $(s\phi'^{i+r}, x, p\phi'^j)\phi'$ are equal.*

Proof. We first set up some notational convenience. Given an edge (u,x,v) of B, with respect to this edge, we shall write $x\phi^i$ for the label of its image $(u,x,v)\phi^i$ so that we have the equality $(u,x,v)\phi^i = (u\phi^i, x\phi^i, v\phi^i)$. Note that in general we do not have an induced action of ϕ on X_n, but the notation will be well-defined in the context of a base edge (u,x,v) being understood.

Let B, ϕ, s, p, N and r be as in the hypotheses, and assume r is minimal. It follows that r divides the orbit length of s (by minimality). Write mr for the orbit length of s. Write $s_1, s_2, \ldots, s_{mr}$ for the orbit of $s = s_1$ (we note that $mr|N$ and we make this explicit below).

Let $\widetilde{P}$ be those states p' in the orbit of p which have Letters(s,p') non-empty. The set $\widetilde{P}$ can be partitioned according to the orbits under the action of ϕ^{mr}, that is, two elements of $\widetilde{P}$ belong to the same part if they belong to the same orbit. Choose $T \subset \widetilde{P}$ so that T has exactly one representative from each block of this partition. Note, by definition, for any edge $(s(\phi^r)^i, x', p\phi^j)$, $i,j \in \mathbb{N}$, there is a unique $p'' \in T$ and an element $x \in$ Letters(s,p'') so that the orbit of (s,x,p'') under ϕ^r contains $(s(\phi^r)^i, x', p\phi^j)$.

We inductively define a map λ_B (i.e., induced by a vertex fixing automorphism of B) along the orbit of an edge (s,x,q) for some $q \in T$. The map λ_B will then determine a transducer $(X_n, Q_B, \pi_B, \lambda_B)$ which can be used (as in Definition 4.1) to carry out the required relabelling. To this end fix $q \in T$ and set $k = |\{q\phi^{imr} | i \in \mathbb{N}\}|$.

For $0 \leq a \leq m-1$, partition Letters(s_{ar+1}, q) via the equivalence relation relating two edge labels whose corresponding edges are in the same orbit under ϕ^{kmr}. Recall there is an order on the elements of each equivalence class induced from the standard $\leq$ ordering on X_n. Use this ordering to determine a transversal for the equivalence classes, choosing as representative of each class the least element in that class. Write $\beta(s_{ar+1})$ for this transversal. For $b \in \beta(s_{ar+1})$ we use the phrase *the equivalence class of* b *at* s_{ar+1} to mean the edge labels in Letters(s_{ar+1}, q) which are orbit equivalent to b.

Let $0 \leq a, a' \leq m-1$. We note that since N is the orbit length of any edge from a state in the orbit of s to a state in the orbit of q we have $|\beta(s_{ar+1})| = |\beta(s_{a'r+1})|$. Let $\alpha \in \mathbb{N}$ such that for $b \in \beta(s_{ar+1})$ and $b' \in \beta(s_{a'r+1})$, the size of the equivalence class of b at s_{ar+1} is equal to the size of the equivalence class of b' at $s_{a'r+1}$ is equal to α. We fix a bijection between the sets $\beta(s_{ar+1})$ and $\beta(s_{a'r+1})$ induced by the ordering of the elements. We note that $\alpha kmr = N$.

For $1 \leq j \leq r$, and $0 \leq a \leq m-1$ we write $\beta(s_{ar+j})$ for the set $\{b\phi^{j-1} | b \in \beta(s_{ar+1})\}$. We note that the orbit equivalence class of $b\phi^{j-1}$ at s_{ar+j}, $b \in \beta(s_{ar+1})$, is precisely the image of the equivalence class of b at s_{ar+1} under the image of ϕ^{j-1}. We transport using ϕ^{j-1} the orderings of $\beta(s_{ar+1})$, and the equivalence classes of elements $b \in \beta(s_{ar+1})$ to the set $\beta(s_{ar+j})$ and the equivalence classes of its elements. That is, for instance, if $b < b' \in \beta(s_{ar+1})$, then $b\phi^{j-1} < b'\phi^{j-1}$ in $\beta(s_{ar+j})$.

Let $1 \leq l \leq m$ be minimal such that $\{q\phi^{imr} | i \in \mathbb{N}\}\phi^{rl} = \{q\phi^{imr} | i \in \mathbb{N}\}$. We note that by minimality $l|m$ since: $\{q\phi^{imr} | i \in \mathbb{N}\}\phi^{mr} = \{q\phi^{imr} | i \in \mathbb{N}\}$. Moreover $\phi^{lr} : \{q\phi^{imr} | i \in \mathbb{N}\} \to \{q\phi^{imr} | i \in \mathbb{N}\}$ is a k-cycle since $\phi^{mr} : \{q\phi^{imr} | i \in \mathbb{N}\} \to \{q\phi^{imr} | i \in \mathbb{N}\}$ is a k-cycle and ϕ^{mr} is a power of ϕ^{lr}. Let $M \in \mathbb{N}$ be such that $Ml = m$ so that $\alpha kMlr = N$.

Further observe that if $\{q\phi^{imr} | i \in \mathbb{N}\}\phi^{rd} \cap \{q\phi^{imr} | i \in \mathbb{N}\} \neq \emptyset$ for some $d \in \mathbb{N}$, then $\{q\phi^{imr} | i \in \mathbb{N}\}\phi^{rd} = \{q\phi^{imr} | i \in \mathbb{N}\}$. For suppose $q\phi^{fmr} \in \{q\phi^{imr} | i \in \mathbb{N}\}\phi^{rd}$ for some $1 \leq f \leq k$. Then there is some $1 \leq j \leq k$ such that $q\phi^{jmr}\phi^{dr} = q\phi^{fmr}$, this now means that

$q\phi^{dr}\phi^{jmr} \in \{q\phi^{imr}|i \in \mathbb{N}\}$. However since ϕ^{mr} is a k-cycle on the set $\{q\phi^{imr}|i \in \mathbb{N}\}$, then $q\phi^{dr} \in \{q\phi^{imr}|i \in \mathbb{N}\}$.

Thus we conclude that the sets $\{q\phi^{imr}|i \in \mathbb{N}\}\phi^{ar}$ for $0 \le a \le l-1$ are pairwise disjoint.

We define a relabelling map λ_B inductively as follows.

Let $b = b_0 \in \beta(s_1)$ be the smallest element such that $\lambda_B(b,s)$ is undefined and for all $1 \le i \le l-1$ $\lambda_B(b_i, s_{ir+1})$ is undefined for the element b_i of $\beta(s_{ir+1})$ corresponding to b. (Note that b_i is the least element of $\beta(s_{ir+1})$ such that $\lambda_B(b_i, s_{ir+1})$ that is undefined.) In the inductive process which follows, we will define $\lambda_B(b_i, s_{ir+1})$ for all $0 \le i \le l-1$ in order.

Define a kl-by-r matrix $\mathfrak{r}$ with entries tuples of size α as follows. Set

$$\mathfrak{r}_{0,0} = (b = b_{1,1}, b_{1,2}, \ldots, b_{1,\alpha})$$

where $(b_{1,1}, \ldots, b_{1,\alpha})$ is the ordered tuple of element $\beta(s_1)$. For $0 \le i < kl$ and $0 \le j < r$ set $\mathfrak{r}_{i,j} = (b_{1,1}, b_{1,2}, \ldots, b_{1,\alpha})\phi^{ir+j} = (b_{1,1}\phi^{ir+j}, b_{1,2}\phi^{ir+j}, \ldots, b_{1,\alpha}\phi^{ir+j})$.

Define a matrix $\mathfrak{R}$ of dimension Mkl-by-r such that $\mathfrak{R}_{i,j}$ for $0 \le i < Mkl$ and $0 \le j < r$ has entry

$$((b_{1,1}, s), \ldots, (b_{1,\alpha}, s))\phi^{ir+j} := ((b_{1,1}\phi^{ir+j}, s\phi^{ir+j}), \ldots, (b_{1,\alpha}\phi^{ir+j}, s\phi^{ir+j})).$$

For $0 \le d < M$, set $\mathfrak{R}(d)$ to be the kl-by-r matrix corresponding to rows dkl to row $(d+1)kl-1$. For $0 \le d < M$, $0 \le i < kl$ and $0 \le j < r$ we set $\lambda_B \mathfrak{R}(d)_{i,j} = \mathfrak{r}_{i,j}$, where we extend λ_B naturally to act on tuples $(X_n \times Q_B)^\alpha$ to produce tuples in X_n^α.

Let $1 \le i < l$. We note that for the element $b' \in \beta_{s_{ir+1}}$, the function $\lambda_B(b', s_{ir+1})$ remains undefined. Let the matrix $\mathfrak{r}$ be exactly as above and define the matrix $\mathfrak{R}$ as above but with b' playing the role of b and s_{ir+1} playing the role of $s_1 = s$. For $0 \le d < M$ define the component $\mathfrak{R}(d)$ as above. Then once more for $0 \le d < \alpha M$, $0 \le i < kl$ and $0 \le j < r$ we set $\lambda_B \mathfrak{R}(d)_{i,j} = \mathfrak{r}_{i,j}$.

Continuing on in this way across the set T, we define λ_B on all pairs $(x, s\phi^i)$ where $i \in \mathbb{N}$ and there is a $j \in \mathbb{N}$ such that $(s\phi^i, x, p\phi^j)$ is an edge. We set λ_B to be projection onto the first coordinate on all other pairs in $X_n \times Q_B$.

By construction λ_B is induced by a vertex fixing automorphism and induces the required relabelling of B.

□

Remark 4.8. Note that the relabelling B' of B given by Lemma 4.7 is in fact isomorphic as an automaton to B, since the relabelling is by a vertex fixing automorphism of B. This means we may instead write (B, ϕ) for the pair (B', ϕ').

Lemma 4.9. *Let B be a strongly synchronizing automaton and ϕ an automorphism of the underlying digrpah G_B of B. Let s, t, p be states of B such that there is an $x \in X_n$ with $\pi_B(x, s) = p$. Suppose*

- *for $i, j \in \mathbb{N}$, $\pi_B(x, s\phi^i) = p\phi^j$ if and only if $\pi_B(x, t\phi^i) = p\phi^j$;*
- *the orbits of s and t are distinct and have equal length l;*

- *there is an $N \in \mathbb{N}$ such that for any $j \in \mathbb{N}$, all edges $(s, x, p\phi^j)$ and $(t, x, p\phi^j)$ are on orbits of length N.*

Then there is a relabelling of B' of B such that the induced automorphism ϕ' of $G_{B'}$ satisfies: for any $i, j \in \mathbb{N}$ $\mathrm{Letters}(s\phi^i, p\phi^j) = \mathrm{Letters}(t\phi^i, p\phi^j)$, and for any $x \in \mathrm{Letters}(s\phi^i, p\phi^j)$, the labels of the edges $(s\phi^i, x, p\phi^j)\phi'$ and $(t\phi^i, x, p\phi^j)\phi'$ coincide.

Proof. This is a more straight-forward relabelling operation than the previous case. We simply match the orbits of t along p with those of s along p. We define the relabelling map λ_B inductively. As before, throughout we observe the following notation. Let $u, v \in Q_B$ and $x \in X_n$ such that (u, x, v) is an edge. For $i \in \mathbb{N}$ we write $x\phi^i$, whenever there is no ambiguity, for the label of the edge $(u, x, v)\phi^i$.

First, for any pair $(c, d) \in X_n \times Q_B$ such that $(d, c, \pi(c, d))$ is not an edge from a state in the orbit of t to a state in the orbit of p, set $\lambda_B(c, d) = c$.

Let $x \in X_n$ be smallest such that $(t, x, p\phi^i)$ is an edge for some i and $\lambda_B(x, t)$ is not defined. Let $y \in X_n$ be minimal such that $(s, y, p\phi^i)$ is an edge and y is not equal to $\lambda_B(z, t)$ for $(t, z, p\phi^i)$ an edge. For $0 \le j < N$ set $\lambda_B(x\phi^j, t\phi^j) = y\phi^j$ where $y\phi^j$ is the label of the edge $(s, y, p\phi^i)\phi^j$.

This inductively defined relabelling map λ_B is given by a vertex fixing automorphism and induces the required relabelling of B.

□

Remark 4.10. We note that, once more, B' and B are isomorphic as automata and so we may write (B, ϕ') for (B', ϕ').

4.3 Shadow states

In this second part of our process, we find new states to add to the transducer via splitting operations, to provide more room for relabelling.

Let $A \in \mathcal{H}_n$ have finite order and let B be a minimal strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph G_B of B with A the minimal representative of $H(B, \phi_A)$.

The following definition is motivated by considering paths into a vertex t that might provide an obstruction to a collapse through relabelling of B, as described in the next paragraph.

Suppose there is a state q of B so that there is a minimal length r so that all paths of length r that end on q have orbits of length n under the action of ϕ_A, and for this choice of q we have $r > 1$. Let $\mathcal{P} = e_1 e_2 \dots e_r$ be a path of length r terminating at q, where the orbit of $\mathcal{P}$ has length n but the orbit of $e_2 e_3 \dots e_r$ is of size c for some $c < n$. For indices $1 \le i \le j \le r$ set $\mathcal{P}_{i,j} := e_i e_{i+1} \dots e_j$. By construction, the least common multiple of the orbit size of the edge e_1 and of c is n, and further, the orbit length of $\mathcal{P}_{2,r-1}$ must divide $c < n$. As will become clear later, if this situation arises, it may be an obstruction to collapse of a transducer through a relabelling process.

In the definition that follows, the state t corresponds to the target of e_1 from the path mentioned above, while b is some integer multiple of the orbit length of t, but which still properly divides n.

Definition 4.11. Let $A \in \mathcal{H}_n$, B be a minimal strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph G_B of B with A the minimal representative of $H(B, \phi_A)$, and $t \in Q_B$. We say t *is heavy (for the pair* (B, ϕ_A)*)* if the following conditions hold:

- there is a proper divisor b of n, where b is divisible by the length of the orbit of t;
- there is at least one pair $(x, s) \in X_n \times Q_B$ such that (s, x, t) is an edge;
- for any $x \in X_n$ and any $s \in Q_B$ such that (s, x, t) is an edge of B, the lowest common multiple of b and the length of the orbit of (s, x, t) under ϕ_A is n.

In this case, we call the value b above a *divisibility constant for* t and observe that the set of valid divisibility constants for t might have more than one element.

In our overall process, we will apply the Lemma 4.13 (directly below) in a situation where we cannot simplify a transducer $H(B, \phi_A)$ directly by a relabelling operation. Specifically, this lemma is useful in situations where we can carry out an in-split of the domain automaton B along the orbit of a heavy state t to create a new automaton B' with automorphism ψ_A so that A is a minimal representative of both $H(B, \phi_A)$ and of $H(B', \psi_A)$, and where the new pair (B', ψ_A) has a reduced obstruction to the existence of a helpful relabelling. Note that here, we mean "in-split" in the normal sense of that operation for edge-shift equivalences, see, e.g. [11].

The following lemma characterises how to perform an *in-split along the orbit of a heavy state* t. The new automaton that is created has all of the old states, together with new states which we call *shadow states (from the orbit of* t*)*.

The following two lemmas address the same set of hypotheses, but we split the results into two statements as the lemma of primary interest is the second one.

Any such number n' which arises as in Lemma 4.12 below will be referred to as a *valid splitting length for (the heavy state)* t *with respect to divisibility constant* b.

Lemma 4.12. *Let* $A \in \mathcal{H}_n$ *and let* B *be a minimal strongly synchronizing automaton such that there is an automorphism* ϕ_A *of the underlying digraph* G_B *of* B *with* A *the minimal representative of* $H(B, \phi_A)$*. Suppose there are* $b \in \mathbb{N}$ *and* $t \in Q_B$ *so that* t *is heavy for the pair* (B, ϕ_A) *with* b *a divisibility constant for* t*, and where* $\left|\{t\phi_A^p | p \in \mathbb{Z}\}\right| = r$*.*

In these circumstances, there is $n' \in \mathbb{N}$ *a number which divides the lengths of orbits of all edges* (s, x, t) *and satisfies the following conditions:*

i) the lowest common multiple of n' *and* b *is* n*,*

ii) there is $m > 1$ *so that* $n' = mr$*.*

Proof. Let N be the greatest common divisor of the orbit lengths of all edges (s, x, t) in B. Let (s, x, t) be an edge of B with orbit length k under the action of $\langle \phi_A \rangle$. Now, by the third bullet point of the definition of the state t being heavy we see that $\mathrm{lcm}(k, b) = n$. It follows, as (s, x, t) is an arbitrary incoming edge for t, that $\mathrm{lcm}(N, b) = n$ as well. Since r is the orbit length of t we see that $r|k$ and since (s, x, t) is an arbitrary incoming edge for t we therefore have $r|N$. By assumption, $r|b$, so if $r = N$ we would have $\mathrm{lcm}(N, b) = b < n$ which is a contradiction. It then follows that $N = kr$ for some integer $k > 1$. Thus the set of numbers N which divide the orbit lengths of all edges (s, x, t) and satisfy points i) and ii) is non-empty. Now let n' be an element of this set and determine $m \in \mathbb{N}$ so that $mr = n'$ (noting that $1 < m$ by construction). ☐

Lemma 4.13. *Let $A \in \mathcal{H}_n$ and let B be a minimal strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph G_B of B with A the minimal representative of $H(B, \phi_A)$. Suppose there is $b \in \mathbb{N}$ and $t \in Q_B$ so that t is heavy for the pair (B, ϕ_A) with b a divisibility constant for t. Set $t_{0,0} = t$ and let $t_{0,0}, t_{0,1} \dots, t_{0,r-1}$ be the orbit of t under iteration by ϕ_A. Let n' be a valid splitting length of t and let $m > 1$ be determined by $n' = mr$.*

In these circumstances we may form a new strongly synchronizing automaton B' with

$$Q_{B'} = Q_B \sqcup \{t_{a,0}, \dots, t_{a,r-1} \mid 1 \leq a < m\}$$

such that we have

- *i) $\pi_{B'}(x, s) := \pi_B(x, s)$ for those pairs $(x, s) \in X_n \times Q_B$ where $\pi_B(x, s)$ is not in the orbit of t;*
- *ii) $\pi_{B'}(\cdot, t_{a,i}) := \pi_{B'}(\cdot, t_{0,i})$ for all $0 \leq a < m$, $0 \leq i < r$;*
- *iii) The incoming transitions of B' to the set of vertices $\{t_{a,i} \mid 0 \leq a < m, 0 \leq i < r\}$ are determined by the above rules, and by an automorphism ψ_A of the underlying digraph $G_{B'}$ of B' satisfying: $(t_{0,0})\psi_A^{ar+i} = t_{a,i}$ for $0 \leq a < m$, $0 \leq i < r$, $(t_{0,0})\psi_A^{n'} = t_{0,0}$, and $H(B', \psi_A) = A$.*

Proof. Let n' be a valid splitting length for the heavy state $t_{0,0}$ with divisibility constant b, and let $m > 1$ be an integer so that $n' = mr$.

Set

$$T := \{t_{0,0}, t_{0,1}, \dots, t_{0,r-1}\}$$

and build a set of new objects (the extra "shadow states" arising from the splitting along the orbit of $t_{0,0}$)

$$T' = \{t_{a,1}, t_{a,2}, \dots, t_{a,r} \mid 1 \leq a < m\}.$$

Note that $|T \cup T'| = n'$.

We will define an action ψ_A on

$$Q_{B'} := Q_B \cup T'$$

as follows.

For $s \in Q_{B'}$, set

$$s\psi_A = \begin{cases} s\phi_A & \text{if} \quad s \in Q_B \backslash T \\ t_{a,i+1} & \text{if} \quad s = t_{a,i} \text{ and } i < r-1 \\ t_{a+1,0} & \text{if} \quad s = t_{a,r-1} \text{ and } a < m-1 \\ t_{0,0} & \text{if} \quad s = t_{m-1,r-1}. \end{cases}$$

It is immediate by construction that this is an action, and also that the orbit of $t_{0,0}$ has size n'. We will specify transitions for B' by steadily expanding the definition of the underlying digraph $G_{B'}$ of B' through adding edges of the form (p, x, q) for $p, q \in Q_{B'}$ and $x \in X_n$ (thus adding the transition $(x, p)\pi_{B'} = q$ to B'), while simultaneously extending the function ψ_A on the corresponding edges of $G_{B'}$. Ultimately, B' will be a strongly synchronizing automaton and ψ_A will be an automorphism of the digraph $G_{B'}$ with $H(B', \psi_A)$ being equivalent to A.

Important in what follows will be a graph homomorphism $\iota : G_{B'} \to G_B$, which we will automatically extend to the (new) edges of $G_{B'}$ whenever they are added. On the set $Q_{B'}$, ι is defined as follows: for $s \in Q_{B'} \backslash (T \cup T')$ set $s\iota := s$, and for any $t_{a,i} \in T \cup T'$ set $t_{a,i}\iota := t_{0,i}$.

Below, whenever we extend $G_{B'}$ by adding new edges, we also extend the graph homomorphisms $\iota : G_{B'} \to G_B$ and $\psi_A : G_{B'} \to G_{B'}$ so as to maintain *rsc*, the *rule of semi-conjugacy*, which we define here.

<u>*rsc*</u>:

(a) for all $q \in Q_{B'}$ we have $q\psi_A\iota = q\iota\phi_A$, and

(b) for all edges e of $G_{B'}$ we further require $e\psi_A\iota = e\iota\phi_A$.

Of course we have part (a) of the rule because we have already defined ι and ψ_A over $Q_{B'}$ to satisfy this rule.

In the above construction of ι if $e\iota = (r, x, s)$ then we will identify e as (p, x, q) where p is the source of e and q is the target of e, so after any extension we can always think of the new $G_{B'}$ as an edge-labelled directed graph with edge labels "lifted" from G_B by the map ι.

Note that below we will sometimes add a large collection of edges at one go, but in this case, there is always a well defined triple (p, x, q) for each new edge, as we add in edges along an orbit under ψ_A which always contains a well-defined edge (r, y, s), from which we can detect the correct letter labelling of all edges along the orbit by using rsc.

It follows that if B' is a strongly synchronizing automaton then $H(B, \phi_A)$ will represent the same element of $\mathcal{H}_n$ as $H(B', \psi_A)$, since the map ι never changes edge labels, and the map ψ_A will have to change edge labels in the corresponding fashion as ϕ_A in order to uphold rsc.

We now begin to specify the edges of $G_{B'}$, and hence the transition function $\pi_{B'}$. Recall below that $Q_B \backslash T = Q_{B'} \backslash (T \cup T')$.

Partition the edges of G_B into the following four sets.

$$
\begin{aligned}
N_T :=&\{(p,x,q) \mid p,q \notin T\},\\
B_T :=&\{(p,x,q) \mid p,q \in T\},\\
D_T :=&\{(p,x,q) \mid p \in T, q \notin T\}, \text{ and}\\
R_T :=&\{(p,x,q) \mid p \notin T, q \in T\}.
\end{aligned}
$$

We observe in passing that ϕ_A acts on each of the sets N_T, B_T, D_T, and R_T.

For (p,x,q) an edge in N_T, let (p,x,q) also be an edge of $G_{B'}$ (and so $(x,p)\pi_{B'} = q$ as well) and set $(p,x,q)\psi_A := (p,x,q)\phi_A$.

Recall that for a group H acting on a set X, a traversal for the orbits is a subset $\mathscr{Y} \subset X$ so that each orbit under the group action has a unique representative in the set $\mathscr{Y}$.

Let $\mathscr{Y}_B$ be a traversal for the orbits of the edges in B_T such that each edge in $\mathscr{Y}_B$ is of the form $(t_{0,0}, x, t_{0,i})$. Similarly set $\mathscr{Y}_D$ to be a traversal for the orbits of the edges in D_T so that each edge of $\mathscr{Y}_D$ is of the form $(t_{0,0}, x, s)$ for some $s \in Q_B \backslash T$. Finally set $\mathscr{Y}_R$ to be a traversal for the orbits of the edges in R_T so that each edge of $\mathscr{Y}_R$ is of the form $(s, x, t_{0,0})$ for some $s \in Q \backslash T$.

Extend $G_{B'}$ to include $\mathscr{Y}_D \cup \mathscr{Y}_R \cup \mathscr{Y}_B$ as edges incident on $t_{0,0}$ (we will add more edges incident on $t_{0,0}$ later). Furthermore, use the action of ψ_A on the set $Q_{B'}$ together with the map ι to uniquely determine new edges (of the form (p,x,q) for $x \in X_n$) that must be added to $G_{B'}$ so that the resulting digraph is closed under the action of ψ_A, contains the transversal edges $\mathscr{Y}_D \cup \mathscr{Y}_R \cup \mathscr{Y}_B$ and satisfies rsc. Note that this process extends the definition of ι and ψ_A to these new edges as well, but these extensions are inductively well defined. Now we may use the new edges of $G_{B'}$ in the obvious way to also extend the definition of the transition function $\pi_{B'}$ so as to create a correspondingly larger automaton B'.

Observe that for any state $s \in Q_{B'} \backslash (T \cup T') = Q_B \backslash T$, the process above now has created a unique edge of the form (s,x,q) for each $x \in X_n$ (which are the "lifts" of N_T and R_T to $G_{B'}$ by ι). For edges in N_T this is simply by definition. For an edge $(s,x,t_{0,i}) \in R_T$, there is an edge $(s',x',t_{0,0}) \in \mathscr{Y}_R$ so that there is a minimal non-negative integer k with $(s',x',t_{0,0})\phi_A^k = (s,x,t_{0,i})$. It follows that $(s',x',t_{0,0})\psi_A^k = (s,x,t_{a,i})$ for the unique non-negative a so that $k = ar + i$. Now suppose there is an edge $(s,x,t_{b,j})$ of $G_{B'}$. By rsc, we see that $(s,x,t_{b,j})\iota = (s,x,t_{0,j})$ but as there is a unique outgoing edge in G_B from s with letter x we see that $t_{0,j} = t_{0,i}$ and in particular, $i = j$. We assume without meaningful loss of generality that $b \geq a$ and that $|b-a|$ is minimal amongst all such differences. Thus by rsc the orbit length of the edge $(s,x,t_{0,i})$ under ϕ_A is precisely $(b-a)r$ or else $b = a$. However, $(b-a)r < n'$ and n' divides the length of the orbit of $(s,x,t_{0,i})$ by the definition of n'. It follows that $(s,x,t_{a,i})$ is the unique pre-image of $(s,x,t_{0,i})$ under ι.

There remains a special concern that we must address. Specifically, there are now pairs $(x,t_{a,i}) \in X_n \times (T \cup T')$ so that there are no edges of the form $(t_{a,i},x,q)$ in $G_{B'}$. This happens as the orbit of $t_{0,0}$ has length r under ϕ_A but length $n' = mr > r$ under ψ_A. Also, to verify the coherence of the rsc condition for edges in $\mathscr{Y}_B$, recall that n' divides the orbit length of these edges as they are in the orbit of an edge incident to t.

Let us now deal with the "missing edges" issue. Observe that for an edge $(t_{0,0}, x, s) \in \mathscr{Y}_D \cup \mathscr{Y}_B$, its orbit under ϕ_A may contain multiple edges of the form $(t_{0,0}, y, q)$ (for various $y \in X_n$ and $q \in Q_B$). Let us organise these as the sequence of pairwise distinct edges $(e_0, e_1, \ldots, e_k)$ where $e_i = (t_{0,0}, x, s)\phi_A^{ri}$, and with $e_k\phi_A^r = e_0 = (t_{0,0}, x, s)$. In this context, the orbit of $(t_{0,0}, x, s)$ under ϕ_A has length $(k+1)r$. Let us set notation $e_i =: (t_{0,0}, x_i, q_i)$ so we can understand the letter x_i associated to e_i for each valid index i. The concern is that in our current graph $G_{B'}$ we see for any index $0 < i \leq k$ that there is no edge of the form $(t_{0,0}, x_i, q) \in G_{B'}$. For the letter x_i observe that there is an edge of the form $(t_{a,0}, x_i, q_i)$ of $G_{B'}$ for $a = ir \mod n'$ and some state q_i. The rule of modification is, add the edge $(t_{0,0}, x_i, q_i)$ to $G_{B'}$, for all indices $0 < i \leq k$. Repeat this same procedure across all of the transversal elements $(t_{0,0}, x', s') \in \mathscr{Y}_D \cup \mathscr{Y}_B$ and as a consequence, for each letter $y \in X_n$, we see that the vertex $t_{0,0}$ now has a unique outgoing edge of the form $(t_{0,0}, y, q)$. Finally, we again use the action of ψ_A on vertices and the action of ϕ_A on G_B along with the rsc condition to extend the definitions of ψ_A and ι to the necessary edges we have to add to $G_{B'}$ in order to complete the orbits of our newly-added edges based at $t_{0,0}$, and to discern what letters needed to be associated to these new edges. Now induce from $G_{B'}$ the enlarged automaton B'.

One observes that for any valid indices a and b and fixed index i, the states $t_{a,i}$ and $t_{b,i}$ of B' have all the same outgoing transitions, and indeed, that the automaton B' collapses back down to B by identifying these states for each fixed i. In particular $G_{B'}$ is strongly synchronizing as it admits a collapse sequence to the n-leafed rose. Further, the rsc condition implies that ψ_A acts as an automorphism of the directed graph $G_{B'}$ in fashion locally emulating how ϕ_A acts on G_B so that $H(G_{B'}, \psi_A)$ represents A.

$\square$

Let $A, B, t = t_{0,0}$ be as in the statement of Lemma 4.13. Assume we applied Lemma 4.13 to lengthen the orbit of t as in the lemma statement to create automaton B' with automorphism ψ_A so that $H(B', \psi_A)$ has minimal representative A and where the orbit of t in $G_{B'}$ under the action of ψ_A is the set $\{t_{a,i} \mid 0 \leq a < m, 0 \leq i < r\}$. Now for each state $t_{0,i}$ for $0 \leq i < r$ (these states are in the original orbit of t in G_B under the action of ϕ_A), we call the set of states

$$\{t_{a,i} \mid 0 < a \leq m-1\} \subsetneq Q_{B'}$$

the *shadow states for* $t_{0,i}$ *(in* $Q_{B'}$*)*. Note that these are precisely the states of $H(B', \psi_A)$ with local maps equivalent to the local map at $t_{0,i}$ for the transducer $H(B, \phi_A)$. If we apply Lemma 4.13 inductively and perhaps repeatedly on states on the now extended orbit of t, we extend the definition of the shadow states of $t_{0,i}$ to be the union of the sets of states added in each round of applying Lemma 4.13 which have local maps equivalent to the local map at $t_{0,i}$ for the transducer $H(B, \phi_A)$. Note that this process cannot go on forever as each application of Lemma 4.13 lengthens the orbit of $t_{0,0}$ with n an upper bound on the length of this orbit. Also note that each added state will be a shadow state of one of the original states $t_{0,j}$ after any number of iterated applications of Lemma 4.13.

Lemma 4.14. *Let $A \in \mathcal{H}_n$ and let B be the minimal strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph of B with A the minimal* *representative of $H(B, \phi_A)$. Suppose that all circuits in B are on orbits of length n under the action of A. Then there is a strongly synchronizing transducer $\widehat{B}$ such that A acts as an automorphism $\widehat{\psi}_A$ of $\widehat{B}$ and all edges of $\widehat{B}$ are on orbits of length n under the action of A.*

Proof. We first observe that all states of B must be on orbits of length dividing n as the underlying digraph of B is strongly synchronizing and therefore each state is visited by some circuit which is on an orbit of length n. Also, we may assume that $|B| > 1$ otherwise all loops at the state of B will be on orbits of length n and we would be done.

Let $s \in Q_B$ be such that s is on an orbit of length strictly less than n under ϕ_A. (If all states of Q_B were on orbits of length n then all edges of B would be on orbits of length n as well and we would be done.)

Inductively define states as follows.

Set $Q_B(0, s) := \{s\}$. Assume $Q_B(i, s)$ is defined for some $i \in \mathbb{N}$. We now define $Q_B(i + 1, s) \subseteq Q_B$. An element $q \in Q_B$ belongs to $Q_B(i + 1, s)$ if the following conditions hold:

(a) there are elements $x_1, x_2, \ldots, x_{i+1} \in X_n$, such that, for all $1 \leq j \leq i + 1$, we have $\pi_B(x_{i+1} \ldots x_j, q) \in Q_B(j - 1, s)$; and

(b) the path $(q, x_{i+1}x_i \ldots x_1, s)$ is on an orbit of length strictly less than n under ϕ_A.

We observe that for any state q in a set $Q_B(i+1, s)$, the orbit of q under ϕ_A has size properly dividing n. If $q \in Q_B(i + 1, s)$ and $x_{i+1}, x_i, \ldots, x_1 \in X_n$ satisfies points (a) and (b) then we call the path $(q, x_{i+1}x_i \ldots x_1, s)$ *conformant for $Q_B(i + 1, s)$*.

Let $k \in \mathbb{N}$ be minimal so that $Q_B(k + 1, s) = \emptyset$. If such k did not exist then there would a long path (as in point (b) of the definition of the sets $Q_B(i, s)$) which is long enough that it must contain a circuit in B. Any such circuit would be on an orbit of length strictly less than n under the action of ϕ_A, which is a contradiction.

From the argument directly above it also follows that whenever $j > 0$, $s \notin Q_B(j, s)$.

We now apply an induction argument using Lemma 4.13 to reduce k to 0.

Let $t \in Q_B(k, s)$ and fix $x_k, x_{k-1}, \ldots, x_1 \in X_n$, such that the path $(t, x_k x_{k-1} \cdots x_1, s)$ is conformant for $Q_B(k, s)$ and where the orbit of this path under the action of ϕ_A is of length $b < n$ (note that $b|n$ and also that the length of the orbit of t divides b). Moreover, by choice of k, for any pair $(x, p) \in X_n \times Q_B$ with $\pi_B(x, p) = t$, the lowest common multiple of the length of the orbit of the edge (p, x, t) and b is n.

Therefore t is heavy for the pair (B, ϕ_A) and b is a divisibility constant for t, so we may apply Lemma 4.13 with the state t and constant b to add states in the orbit of t and necessary edges to form a new strongly synchronizing automaton B' with ψ_A an automorphism of $G_{B'}$, and so that $H(B', \psi_A)$ still represents A (and so in particular, all circuits of $G_{B'}$ are still on orbits of length n under the action of ψ_A).

Recall that by the construction of B', the orbit of t, which includes all of its shadow states, is now of larger size n'_t under the action of the resulting digraph automorphism ψ_A. Thus, for any t' in the orbit of t (including the shadow states we have just added), if there is a path from t' to s which is conformant for $Q_{B'}(k, s)$, then t' (and therefore t) is heavy for $(Q_{B'}, \psi_A)$, so we may again inductively increase the length of the orbit of t by adding more shadow states until there are no paths from a point in the orbit of t to s which are conformant for $Q_{B'}(k,s)$ (note this happens to be a consequence of t no longer being heavy for (B',ψ_A) which must happen eventually as the orbit of t is getting longer and is bounded above by n). Note that if $p \in Q_{B'}(k,s)$ but p is not in the orbit of t, then $p \in Q_B(k,s)$. In particular, we have $|Q_{B'}(k,s)| < |Q_B(k,s)|$ as this count of states for B' no longer includes the state t nor any state in its orbit.

We can now inductively repeat this process for s until $|Q_{B'}(k,s)| = 0$.

Note that we can repeat this process for any state p with $|Q_{B'}(k,p)| \neq 0$. Thus we may now proceed inductively in this fashion until finally we have constructed an automaton B' and an automorphism ψ_A of $G_{B'}$ so that B' folds onto B and $H(B',\psi_A)$ represents A, and where if q is any state and j is minimal so that $Q_{B'}(j,q) = \emptyset$, then $j = 0$.

We set $\widehat{B} = B'$ and $\widehat{\psi}_A = \psi_A$ in this final case, noting that the orbit of every edge of $\widehat{B}$ under the action of $\widehat{\psi}_A$ is of length n.

□

Remark 4.15. Let $A \in \mathcal{H}_n$ be an element of finite order and suppose that every point in $X_n^{-\mathbb{N}}$ is on an orbit of length n under the action of A. By lemma 4.14, there is a minimal (in size) strongly synchronizing automaton B such that A acts as an automorphism ϕ_A of the underlying digraph of B and all edges of B are on orbits of length n under the action of A.

4.4 Relabelling through shadows

In this section we make use of Lemma 4.13 to deal with situations in which we are unable to directly apply Lemma 4.7 or Lemma 4.9.

The lemma below says that applying Lemma 4.13 and then suitably relabelling does not move us out of the conjugacy class of the considered finite order element $A \in \mathcal{H}_n$.

Definition 4.16. Let $A \in \mathcal{H}_n$ and let B be the minimal strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph of B with A the minimal representative of $H(B,\phi_A)$. Let D be a strongly synchronizing automaton which is obtained by repeated applications of Lemma 4.13 to the automaton B. Let ψ_A be the automorphism of the underlying digraph of D with A the minimal representative of $H(D,\psi_A)$. A relabelling D' of D is called *a relabelling through shadows* if, for the induced automorphism ψ'_A of the underlying digraph of D', for any state $q \in Q_B$ the set $S_{q,D}$ of shadow states of q are all ω-equivalent in $H(D',\psi'_A)$ to the state q.

Lemma 4.17. *Let $A \in \mathcal{H}_n$ and let B be the minimal strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph of B with A the minimal representative of $H(B,\phi_A)$. Let D be a strongly synchronizing automaton which is obtained by repeated applications of Lemma 4.13 to the automaton B. Let ψ_A be the automorphism of underlying digraph of D with A the minimal representative of $H(D,\psi_A)$. Let D' be a relabelling through shadows of D, $\psi_{A'}$ be the induced automorphism of the underlying digraph of D', and A' be the minimal representative of $H(D',\psi_{A'})$. Then A' is conjugate to A and there is a strongly synchronizing automaton B' and an automorphism $\phi_{A'}$ of the underlying* *digraph $G_{B'}$ so that A' is the minimal representative of $H(B', \phi_{A'})$, with $G_{B'}$ equal to the underlying digraph of B.*

Thus, the minimal strongly synchronizing automaton C on which A' acts is carried by a digraph G_C that is a graph quotient of G_B and we have $|G_C| \leq |G_B|$.

Proof. As the relabelling process employed is a relabelling through shadows, it preserves the equivalence of the local maps induced by the graph automorphism across all shadow states shadowing any particular original state of B. In particular the collapse of each state with all of its shadow states results in an automaton B' which still admits an automorphism $\psi_{A'}$ of its underlying graph (which graph is isomorphic to G_B) so that A' is the minimal representative of $H(B', \psi_{A'})$. The result now follows. $\square$

Lemma 4.18. *Let $A \in \mathcal{H}_n$ and let B be the minimal strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph of B with A the minimal representative of $H(B, \phi_A)$. Suppose that all circuits in B are on orbits of length n under the action of A. Let $p \in Q_B$, $i \in \mathbb{N}$ be less than or equal to the orbit length of p, and $\gamma \in X_n^*$ be such that $(p, \gamma, p\phi^i)$ is a path in B from p to $p\phi^i$, then $(p, \gamma, p\phi^i)$ is on an orbit of length n under ϕ.*

Proof. Let k be the orbit length of p and let r be the order of i in the additive group $\mathbb{Z}_k$. For $1 \leq a < r$ write γ_a for the label of the path $(p, \gamma, p\phi^i)\phi^{ia}$ and set $\gamma_0 = \gamma$. Write $\Gamma = \gamma_0\gamma_1 \ldots \gamma_{r-1}$, then the circuit (p, Γ, p) is on an orbit of length n by assumption. From this it follows that the path $(p, \gamma, p\phi^i)$ is also on an orbit of length n. $\square$

Lemma 4.19. *Let $A \in \mathcal{H}_n$ and suppose there is a minimal strongly synchronizing automaton B such that there is an automorphism ϕ_A of the underlying digraph of B with A the minimal representative of $H(B, \phi_A)$ and so that all circuits in B are on orbits of length n under ϕ_A. Let $s, t, p \in Q_B$ be such that* $\mathrm{Letters}(s, p) = \mathrm{Letters}(t, p) \neq \emptyset$. *Then by repeated application of Lemma 4.13 one may obtain from B a strongly synchronizing automaton D with automorphism ψ_A so that A is the minimal representative of $H(D, \psi_A)$ and where the pair (D, ψ_A) satisfies the following conditions:*

(a) there are no shadow states of any element in the orbit of p in D (that is, each application of Lemma 4.13 creates no shadow states for elements in the orbit of p),

(b)

$$\mathrm{Letters}_D(s, p) = \mathrm{Letters}_D(t, p) = \mathrm{Letters}_B(s, p),$$

(c) for $u \in \{s, t\}$, for any shadow state u' of u we have,

$$\mathrm{Letters}_D(u, p) = \mathrm{Letters}_D(s, p) = \mathrm{Letters}_B(s, p),$$

(d) for any $x \in \mathrm{Letters}_B(s, p)$, the length of the orbits of the edges (s, x, p), (t, x, p) under the action of ψ_A on D is n.

Proof. We proceed in a similar way to Lemma 4.14. If $|B| = 1$, then we are done. Therefore we assume that $|B| > 1$.

Inductively define subsets of Q_B as follows.

Set $Q_B(0, p) = \{p\}$. Assume that $Q_B(i, p)$ is defined for some $i \in \mathbb{N}$. Define $Q_B(i+1, p)$ as follows. A state $q \in Q_B$ belongs to $Q_B(i+1, p)$, if there are elements $x_0, x_1, \ldots, x_i \in X_n$, such that $\pi_B(x_i x_{i-1} \ldots x_j, q) \in Q_B(j, p)$ for $0 \leq j \leq i$, and the path $(q, x_i x_{i-1} \ldots x_0, p)$ is on an orbit of length strictly less than n under ϕ_A.

As in the proof of Lemma 4.14, there is a $k \in \mathbb{N}$ such that $Q_B(k+1, p) = \emptyset$. Set $k \in \mathbb{N}$ to be minimal such that $Q_B(k+1, p) = \emptyset$. If $Q_B(1, p) \cap \{s, t\} = \emptyset$, then we are done. Thus we may assume that at least one of s, t belongs to $Q_B(1, p)$ (and so $k \geq 1$).

Observe that by Lemma 4.18 for any $j \in \mathbb{N}$, $p\phi^j$ is not an element of $Q_B(i, p)$ for any $1 \leq i \leq k$.

We now repeatedly apply Lemma 4.13, as in the proof of Lemma 4.14, until we have an automaton D such that $Q_D(1, p) \cap \{s, t\} = \emptyset$. We note that since p is always the single element of $Q_D(0, p)$, then, as for any $j \in \mathbb{N}$, $p\phi^j$ is not an element of $Q_B(i, p)$ for any $1 \leq i \leq k$, we do not create a shadow state of p or elements in the orbit of p in an application of Lemma 4.13.

We prove the base case to illustrate how the proof goes. Let $q \in Q_B(k, p)$. We may find $x_0, x_1, \ldots, x_k$ such that for any $0 \leq j \leq k$, $\pi_B(q, x_k x_{k-1} \ldots x_j) \in Q_B(j, p)$. Let b be the length of the orbit of the path $(q, x_k x_{k-1} \ldots x_0, p)$. Then for any state $u \in Q_B$ for which there is an edge (u, x, q), the lowest common multiple of the length of the orbit of (u, x, q) and b is n. We may now apply Lemma 4.13 to form a new transducer B' by adding shadow states of q. We may define the sets $Q_{B'}(i, p)$ as before, noting that $Q_{B'}(k+1, p) = \emptyset$. This follows as for any edge (u, x, q) in B, the orbit of the edge (u', x, q') in B' (for u' and q' either equal to u and q or shadow states of u and q respectively) is equal to the orbit of the edge (u, x, q). Moreover, as in the proof of Lemma 4.14, the number of paths $(q', x_0 x_1 \ldots x_k, p)$, where q' is either q or one of its shadow states, witnessing that $q' \in Q_{B'}(k)$ is strictly fewer than the witness paths for q in B. Thus inductively applying Lemma 4.13, we find an automaton, which we again denote B', in which $|Q_{B'}(k, p)| < |Q_B(k, p)|$ since neither q nor any of its shadow states belong to $Q_{B'}(k, p)$. Thus, replacing B' with B we may repeat the process.

Eventually we reach an automaton D' such that $Q_D(1, p) \cap \{s, t\} = \emptyset$. Moreover, since, by Lemma 4.13, shadow states transition identically to their original counterparts on edges into states which have no shadow states added (and this transition mirrors the transition in B), the automaton D' satisfies the requirements of the lemma. $\square$

In what follows, set notation $\mathrm{ol}_\tau(\star)$ to represent the orbit length of $\star$ under the action of τ a digraph automorphism of some digraph G, where $\star$ is a vertex, edge, or path in G.

For an automaton C over alphabet Y with $a, b \in Q_C$, recall that $\mathrm{E}_C(a, b)$ represents the set of edges of G_C from a to b, while

$$\mathrm{Letters}_C(a, b) := \{y \in Y \mid \exists (a, y, b) \in \mathrm{E}_C(a, b)\}$$

represents the set of letters from Y which are the labels of these edges.

Lemma 4.20. *Let $A \in \mathcal{H}_n$ and let B be the minimal strongly synchronizing automaton such that there is an automorphism ϕ_A of the underlying digraph of B with A the minimal representative of $H(B, \phi_A)$. Suppose that all circuits in B are on orbits of length n under ϕ_A. Let $s, t, p \in Q_B$ be such that s and t belong to distinct orbits but have the same orbit length under ϕ_A, and so that* $\mathrm{Letters}(s,p) = \mathrm{Letters}(t,p)$. *Then there is $A' \in \mathcal{H}_n$ and an automorphism $\phi_{A'}$ of the underlying digraph of B so that the following hold:*

(a) the element A is conjugate to A' in $\mathcal{H}_n$, where A' is the minimal representative of $H(B, \phi_{A'})$; and,

(b) there is an $N \in \mathbb{N}$ such that for all $x \in \mathrm{Letters}(s,p)$ the edges (s,x,p) and (t,x,p) have orbit length N under $\phi_{A'}$.

Proof. The strategy is to apply Lemma 4.19 to add shadow states to B to obtain an automaton D and an automorphism ψ_A of D, such that $H(D, \psi_A)$ has minimal representative A, ψ_A preserves the orbit length of the state p, and, the orbit length of the edges from s and t into p is n. We then apply a relabelling through shadows of D by Lemma 4.17 to obtain a conjugate element A' to A represented by a transducer $H(B, \phi_{A'})$ for $\phi_{A'}$ an automorphism of the underlying digraph G_B. The key ingredient is that the relabelling of D is chosen such that the orbits of the edges of s and t into p now all have the same length under $\phi_{A'}$. In order to find a relabelling achieving this goal, we will need to track numerous integer constants.

Set $r = \mathrm{ol}_{\phi_A}(p)$ and determine m so that $mr = \mathrm{lcm}(\mathrm{ol}_{\phi_A}(s), \mathrm{ol}_{\phi_A}(p)) = \mathrm{lcm}(\mathrm{ol}_{\phi_A}(t), \mathrm{ol}_{\phi_A}(p))$. For any edge $(s,x,p) \in \mathrm{E}_B(s,p)$ we have $(s,x,p)\phi_A^k \in \mathrm{E}_B(s,p)$ if and only if k is an integer multiple of mr. For each $x \in \mathrm{Letters}_B(s,p) = \mathrm{Letters}_B(t,p)$, determine integers u_x, v_x so that $u_x mr = \mathrm{ol}_{\phi_A}((s,x,p))$ and $v_x mr = \mathrm{ol}_{\phi_A}((t,x,p))$. In particular, for any $x \in \mathrm{Letters}_B(s,p)$, the number of edges in $\mathrm{E}_B(s,p)$ which belong to the orbit of (s,x,p) under ϕ_A is precisely u_x, while v_x defines the analogous number for (t,x,p). It follows that there are permutations $\theta_s : \mathrm{Letters}_B(s,p) \to \mathrm{Letters}_B(s,p)$ and $\theta_t : \mathrm{Letters}_B(t,p) \to \mathrm{Letters}_B(t,p)$ induced from the permutations of edges from s to p (and from t to p respectively) achieved by applying ϕ_A^{mr}. In particular, for $x \in \mathrm{Letters}_B(s,p)(= \mathrm{Letters}_B(t,p))$, we have the cycle of θ_s containing x has length u_x and the cycle of θ_t containing x has length v_x.

Adding shadows:

Apply Lemma 4.19 to the quadruple (s,t,p,B) to obtain a strongly synchronizing automaton D and a corresponding automorphism ψ_A of the digraph G_D underlying D so that A is the minimal representative of $H(D, \psi_A)$, and the conclusions of Lemma 4.19 are satisfied. In particular, for any $x \in \mathrm{Letters}_B(s,p)$ we have $\mathrm{ol}_{\psi_A}((s,x,p)) = \mathrm{ol}_{\psi_A}((t,x,p)) = n$.

We now determine various constants arising from the construction so far.

By construction, r remains the length of the orbit of p in D; however, the orbit lengths of s and t have possibly been padded out with shadow states. Determine e, f so that $emr = \mathrm{lcm}(\mathrm{ol}_{\psi_A}(s), \mathrm{ol}_{\psi_A}(p))$ and $fmr = \mathrm{lcm}(\mathrm{ol}_{\psi_A}(t), \mathrm{ol}_{\psi_A}(p))$.

As $\mathrm{Letters}_B(s,p) = \mathrm{Letters}_B(t,p) = \mathrm{Letters}_D(t,p) = \mathrm{Letters}_D(s,p)$ we will often use the notation $\mathrm{Letters}\,(s\|t,p)$ for this set, although, we might use one of the other names if we specifically wish to emphasise that we are considering the action of ϕ_A or of ψ_A in that case. Set as well $\zeta := |\operatorname{Letters}(s\|t,p)|$.

Determining constants and orbit blocks from $\operatorname{Letters}_D(s,p)$ *and* $\operatorname{Letters}_D(t,p)$:

As above, consider the permutation of $\operatorname{Letters}_D(s,p)$ induced by applying ψ_A^{emr} to G_D. Note that this permutation is θ_s^e. Similarly ψ_A^{fmr} induces θ_t^f on $\operatorname{Letters}_D(t,p)$. Set q_e to be the order of θ_s^e, so that $\theta_s^{q_e e}$ is the identity permutation. Analogously define q_f to be the order of θ_t^f. Note in passing that $q_e = n/(emr)$ is the number of times the orbit of an edge of the form (s,x,p) intersects $\mathrm{E}_D(s,p)$ under the action of $\langle\psi_A\rangle$ (and that this number is independent from the choice of such edge), and similarly, $q_f = n/(fmr)$ counts the cardinality of the intersection of the orbit of an edge of the form (t,x,p) with $\mathrm{E}_D(t,p)$ under the action of $\langle\psi_A\rangle$ (again, independent of the choice of such an edge). It follows that all cycles of θ_s^e have length q_e and that all the cycles of θ_t^f have length q_f.

We note that for all $x \in \operatorname{Letters}_D(s,p)$ we have $q_e e = \operatorname{lcm}(u_x, e)$ and $q_f f = \operatorname{lcm}(v_x, f)$. Therefore, for any $x \in \operatorname{Letters}(s\|t,p)$, we have $q_e|u_x$ and $q_f|v_x$. Further, as $q_e emr = q_f fmr = n$ we have $q_e e = q_f f$.

Let $u = \gcd\{u_x : x \in \operatorname{Letters}(s\|t,p)\}$ and $v = \gcd\{v_x : x \in \operatorname{Letters}(s\|t,p)\}$. As $q_e|u_x$ and $q_f|v_x$ for all $x \in \operatorname{Letters}(s\|t,p)$, we see that $q_e|u$ and $q_f|v$. Let $\overline{u}$ and $\overline{v}$ be such that $\overline{u}q_e = u$ and $\overline{v}q_f = v$. It also follows that $\operatorname{lcm}(u,e) = q_e e = q_f f = \operatorname{lcm}(v,f)$.

Let $\tau \in \{s,t\}$ and set $\sim_{\tau,p}$ to be the equivalence relation on the set of edges from τ to p, where two edges are equivalent under $\sim_{\tau,p}$ if they are in the same orbit under ψ_B. Let $X(\tau,p)$ be a transversal for this equivalence relation. It follows that

$$\sum_{(s,x,p)\in X(s,p)} u_x = \sum_{(t,x,p)\in X(t,p)} v_x = |\operatorname{Letters}(s\|t,p)| = \zeta$$

so in particular we see that both u and v divide ζ.

Set $w := \operatorname{lcm}(u,v)$. Since u and v divide ζ we have that $w|\zeta$. Let α be such that $\alpha w = \zeta$. Further, as $u|w$ and $v|w$ there are $\mu,\nu \in \mathbb{N}$ such that $w = \mu u = \mu\overline{u}q_e$ and $w = \nu v = \nu\overline{v}q_f$. Further, $q_e e = \operatorname{lcm}(u,e)|\operatorname{lcm}(w,e)$ and $q_f f = \operatorname{lcm}(v,f)|\operatorname{lcm}(w,f)$. Since both u and v divide $q_e e = q_f f$, it follows that $w|q_e e$ and so $\operatorname{lcm}(w,e) = q_e e = q_f f = \operatorname{lcm}(w,f)$. In particular, $wmr|q_e emr = n$ and $wmr|q_f fmr = n$ and we have $\operatorname{lcm}(wmr, emr) = n = \operatorname{lcm}(wmr, fmr)$.

Building the relabelling:

Our relabelling will be a relabelling through shadows which will create a pattern of labels along an edge orbit that repeats after every wmr steps under iteration of the new automorphism $\psi_{A'}$ of G_D.

To be a relabelling through shadows we will need that for any $0 \le i < mr$ and integer k that the local map at $s\psi_{A'}^{i+kmr}$ agrees with the local map at $s\psi_{A'}^{i}$ (and similarly for the orbit of t).

We will now define a new labelling $\lambda_D : X_n \times Q_D \to X_n$. Recall that a relabelling function is always induced from a vertex fixing automorphism of the underlying digraph of an automaton in the collapse sequence of the original. In our particular construction of λ_D, the reader will see that the automorphism employed in its creation is simply a vertex fixing automorphism of the underlying digraph G_D of D.

Suppose (l, x', p') is an edge of D which does not belong to the orbit of an edge (τ, x, p) for any pair $(\tau, x) \in \{s, t\} \times \mathrm{Letters}_D(\tau, p)$. In this case we set $(x', l)\lambda_B = x'$.

For the moment we focus on edges in the orbit of some edge (s, x, p). The edges in the orbit of (t, x, p) are dealt with analogously.

As $|\,\mathrm{Letters}\,(s\|t, p)| = \zeta = w\alpha$ we may partition $\mathrm{Letters}\,(s\|t, p)$ into α blocks of size w, which partition we organise through some labelling of the set's elements as follows:

$$\mathrm{Letters}\,(s\|t, p) = \{x_i^c \mid 0 \leq i < w, 0 \leq c < \alpha\},$$

where here, the c^{th} part, denoted x^c, has w elements arranged as the ordered sequence $(x_i^c)_{0 \leq i < w}$.

For $0 \leq i < mr$ and $q = s\psi_A^i$ we define $(x, q)\lambda_D = x$. Let $0 \leq i < w$, $0 \leq c < \alpha$ and determine $u_i \in X_n$ so that $(s, x_i^c, p)\psi_A^{mr} = (s\psi_A^{mr}, u_i, p\psi_A^{mr})$. Now set $(u_i, s\psi_A^{mr})\lambda_D := x^c_{(i+1) \mod w}$.

Now, the fact that we are relabelling through shadows determines the rest of the relabelling function λ_D, as the local functions of $H(G_D, \psi_{A'})$ have to agree for each shadow state with that occurring at the state being shadowed, that is, we need the local function of the transducer $H(G_D, \psi_{A'})$ at any state $s\psi_{A'}^{a+mr}$ to agree with the local function at $s\psi_{A'}^a$ (where mr suffices as that is the orbit length of the pair (s, p) in G_B under ϕ_A, and our relabelling only impacts the labels of edges in the orbit of edges from s to p in G_D).

The following inductive definition of λ_D enforces this agreement.

In particular, suppose $mr < a < emr$ and for all $x \in X_n$ and $0 \leq i < a$ we have $(x, s\psi_A^i)\lambda_D$ defined. Suppose further that $(s\psi_A^{a-1}, u, p\psi_A^{a-1})$ is an edge of G_D, $v \in X_n$ with $(s\psi_A^{a-1}, u, p\psi_A^{a-1})\psi_A = (s\psi_A^a, v, p\psi_A^a)$, and that $u', v', x, y \in X_n$ so that:

$$\begin{aligned}
(s\psi_A^{a-1}, u)\lambda_D &= u' \\
(s\psi_A^{a-mr-1}, x)\lambda_D &= u' \\
(s\psi_A^{a-mr-1}, x, p\psi_A^{a-mr-1})\psi_A &= (s\psi_A^{a-mr}, y, p\psi_A^{a-mr}) \\
(s\psi_A^{a-mr}, y)\lambda_D &= v'
\end{aligned}$$

then set $(s\psi_A^a, v)\lambda_D := v'$.

We define λ_D analogously on all edges in the orbit of an edge from t to p.

We now determine $\psi_{A'}$ acting on G_D by the rules that $\psi_{A'}$ agrees with ψ_A on the vertices of G_D, and if $(u, x, v), (u\psi_A, y, v\psi_A)$ are edges of G_D so that $(u, x, v)\psi_A = (u\psi_A, y, v\psi_A)$ then $(u, (x, u)\lambda_D, v)\psi_{A'} = (u\psi_{A'}, (y, u\psi_{A'})\lambda_D, v\psi_{A'})$.

Note in passing that while the orbit of any edge of G_D from s to p (or, from t to p, respectively) has length n under $\psi_{A'}$, the pattern of labels taken by such an edge repeats every wmr steps, and so, as the vertex pair (s, p) (resp. (t, p)) is on an orbit of length emr (respectively fmr) and $\mathrm{lcm}(wmr, emr) = n$ (resp. $\mathrm{lcm}(wmr, fmr) = n$) we see that in the induced automorphism $\phi_{A'}$ of G_B (so that A' is represented by both $H(G_B, \phi_{A'})$ and $H(G_D, \psi_{A'})$) the orbit of any edge from s or t to p is now on an orbit of length wmr.

$\square$

5 Conjugate to an n-cycle

A circuit of length k in an automaton B is carried by k directed edges in G_B in some order $(e_0, e_1, \ldots, e_{k-1})$ where the target of e_i is the source of e_{i+1} (indices modulo k) for each index i. In the next lemma, an automorphism ϕ of G_B carries a circuit C to itself if and only if the image of each edge of C is itself under the automorphism. Specifically, a “rotation” of a circuit is not the circuit itself.

Lemma 5.1. *Let $A \in \mathcal{H}_n$ be an element of finite order. Let B be a strongly synchronizing automaton for which there is an automorphism ϕ_A of the underlying digraph G_B of B with A the minimal representative of $H(G_B, \phi_A)$. Then every point of $X_n^{-\mathbb{N}}$ is on an orbit of length n under the action of A if and only if all circuits in B are on orbits of length n under the action of ϕ_A.*

Proof. This proof follows straight-forwardly from the observation that the orbits of circuits in B under the action of ϕ_A correspond to the action of A on periodic points of $X_n^{-\mathbb{N}}$. Now as periodic points are dense in $X_n^{-\mathbb{N}}$, the following chain of equivalences is true: all points of $X_n^{-\mathbb{N}}$ are on orbits of length n under the action of A if and only if all periodic points of $X_n^{-\mathbb{N}}$ are on orbits of length n under the action of A if and only if all circuits of B are on orbits of length n under the action of A. □

Lemma 5.2. *Let $A \in \mathcal{H}_n$ be an element of finite order and let B be the minimal strongly synchronizing automaton such that A acts as an automorphism ϕ_A of G_B the underlying digraph of B. Suppose that all circuits in B are on orbits of length n, then A is conjugate to an n-cycle.*

Proof. We proceed by induction. In each iteration, we successively replace A with a conjugate C that acts as an automorphism of the underlying digraph of a smaller strongly synchronizing automaton.

By Lemma 4.6 we may assume, replacing A with a conjugate if necessary, that the amalgamation and collapse sequence of B cohere. Thus, a pair of states s, t which distribute similarly over Q_B satisfy, $\mathrm{Letters}(s, p) = \mathrm{Letters}(t, p)$ for all $p \in Q_B$.

Suppose that $|B| > 1$ (as otherwise we are done). Since B is strongly synchronising, we may find a pair of distinct states s, t which distribute similarly over Q_B.

We consider two cases.

First suppose that s and t belong to the same orbit. Fix a state p for which there is an edge from s (and so from t) into p.

We apply Lemma 4.19 to the triple (s, t, p) to obtain a transducer D'' and automorphism ψ'_A such that there are no shadow states for elements in the orbit of p, edges from s and t into p are on orbits of length n.

Now since there are no shadow states for elements in the orbit of p in D'', we may repeatedly apply Lemma 4.19 to s, t and states in the orbits of p in turn, until we obtain an automaton D' and automorphism ψ_A which has no shadow states for elements in the orbit of p, such that $\mathrm{Letters}_{D'}(s, p\psi_A^i) = \mathrm{Letters}_{D'}(t, p\psi_A^i) = \mathrm{Letters}_B(s, p\phi_A^i)$ for all $i \in \mathbb{N}$, and such that any edge from s or t into a state in the orbit of p has orbit length n.

Now we apply Lemma 4.7 to the automaton D'. This results in an automaton D and conjugate automorphism $\psi_{A'}$ with the following properties. For r minimal such that, for any $i, j \in \mathbb{N}$, $\mathrm{Letters}_D(s\psi^i_{A'}, p\psi^j_{A'}) = \mathrm{Letters}_D(s\psi^{i+r}_{A'}, p\psi^{j+r}_{A'})$, then, the labels of the edges $(s\psi^i_{A'}, x, p\psi^j_{A'})\psi_{A'}$ and $(s\psi^{i+r}_{A'}, x, p\psi^j_{A'})\psi_{A'}$ coincide. Notice that, by minimality of r, Shadow states remain ω-equivalent to the state they shadow and t is an element of the orbit of s under the action of $\psi^r_{A'}$.

We now apply Lemma 4.17 to collapse down to the automaton B with a conjugate automorphism $\phi_{A'}$. The conjugate automorphism $\phi_{A'}$ has the following properties. For edges not belonging to the orbit of an edge from s or t into a state not in the orbit of p, the action of $\phi_{A'}$ coincides with the action of A. By construction of D, the label of the edges $(s\phi^i_{A'}, x, p\phi^j_{A'})\phi_{A'}$ and $(t\phi^i_{A'}, x, t\phi^j_{A'})\phi_{A'}$ coincide for any $i, j \in \mathbb{N}$.

We now repeat this process across all states of B which have an edge from s. Thus we end up up with a conjugate automorphism ψ_C such that the label of the edges $(s\psi^i_C, x, q)\psi_C$ and $(t\phi^i_C, x, q)\psi_C$ coincide, for any state q and any incoming edge from s and t into q labelled x.

Let B' be the automaton obtained from B by identifying the pair of states $(s\psi^i_C, t\psi^i_C)$ for all $i \in \mathbb{N}$. Since ψ_C induces the same action on labels for corresponding edges from elements $s\psi^i_C$ and $t\psi^i_C$, then there is an induced action ϕ_C of ψ_C on the underlying digraph of B'. That is there is an element $C \in \mathcal{H}_n$ which is a conjugate of A such that C is the minimal representative of $H(B', \phi_C)$ an $H(B, \psi_C)$.

Now consider the case that s, t belong to distinct orbits. We may assume that the orbit lengths of s and t coincide otherwise we may find a τ' distinct from s and t which has the same orbit length and agrees with one of s or t on Q_B. Whereby we apply the previous case to the pair (s, τ) or (t, τ).

Fix a state $p \in Q_B$ with an edge from s (and so from t). We apply Lemma 4.20 to obtain a conjugate automorphism $\phi_{A''}$ of the underlying digraph of B such that all edges from s and t into p have the same orbit length.

We repeat the process along all states of B with an incoming edge from s. This yields a conjugate automorphism $\phi_{A'}$ of B, whereby, for a given state $q \in Q_B$ all edges from s and t into q have the same orbit length under $\phi_{A'}$.

We now repeatedly apply Lemma 4.9 to the triple $(s, t, B, \phi_{A'})$ to obtain a conjugate automorphism ψ_C of B which satisfies the following. For any pair of edges (s, x, q) and (t, x, q), $(s, x, q)\psi_C$ an $(t, x, q)\psi_C$ have the same labels. This means, we may once more identify the pair of states $(s\psi^i_C, t\psi^i_C)$ to obtain an action ϕ_C of C, the minimal representative of $H(B, \psi_C)$, on a smaller automaton B'.

If $|C| > 1$, then as C is conjugate to A we may now repeat the process with C instead of A.

Eventually we end up with the single state transducer.

□

We recall that by Theorem 3.5, for an element $A \in \mathcal{H}_n$ of finite order, there is a strongly synchronizing automaton B on which A acts as an automorphism ϕ_A of the underlying digraph of B so that $H(B, \phi_A)$ has minimal representative A.

Theorem 5.3. *Let $A \in \mathcal{H}_n$ be an element of finite order. Then A is conjugate to an n-cycle if and only if every element of $X_n^{-\mathbb{N}}$ is on an orbit of length n under the action of A if and only if for any strongly synchronizing automaton B on which A acts as an automorphism ϕ_A of the underlying digraph of B, every circuit of B is on an orbit of length n under the action of A.*

Proof. The equivalences follow from lemmas 5.1 and 5.2. ☐

5.1 An Example

In this section we work through an example that illustrates the key ideas of the proof.

Consider the automaton A of Figure 7 which we encountered already in Example 3.6. This

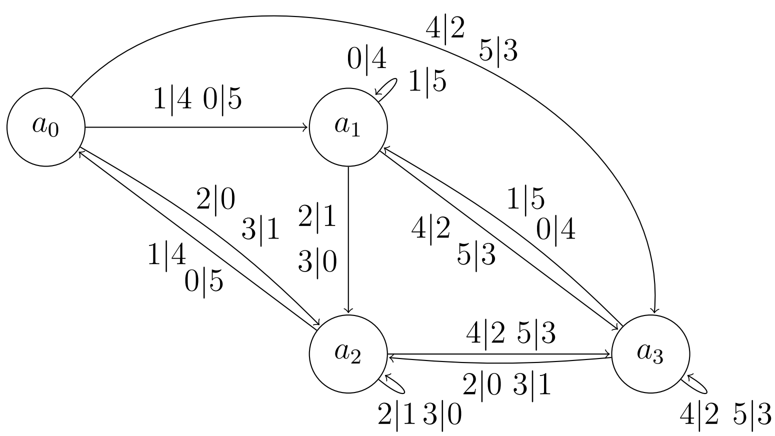

Figure 7: The element A

is an element of $\mathcal{H}_6$ of order 6, where every point in the Cantor space $X_6^{-\mathbb{N}}$ is on an orbit of length 6 under the action of A. Following the construction in Subsection 3.3.1 (see Example 3.6), the minimal strongly synchronising automaton B which admits an automorphism ϕ_A of G_B such that $H(B, \phi_A)$ has minimal representative A, is as depicted in Figure 8, where each drawn edge represents two edges with labels as listed; the map ϕ_A on the vertices on G_B is the permutation which in cycle notation is

$$(p_0\ p_1\ p_2)(q_0\ q_1\ q_2);$$

the action of ϕ_A on the vertices and edges of G_B is uniquely determined from the fact that A is the minimal representative of $H(G_B, \phi_A)$. We refer to the vertices q_0, q_1, q_2 as the vertices of the "inner triangle" and the vertices p_0, p_1, p_2 as the vertices of the "outer triangle".

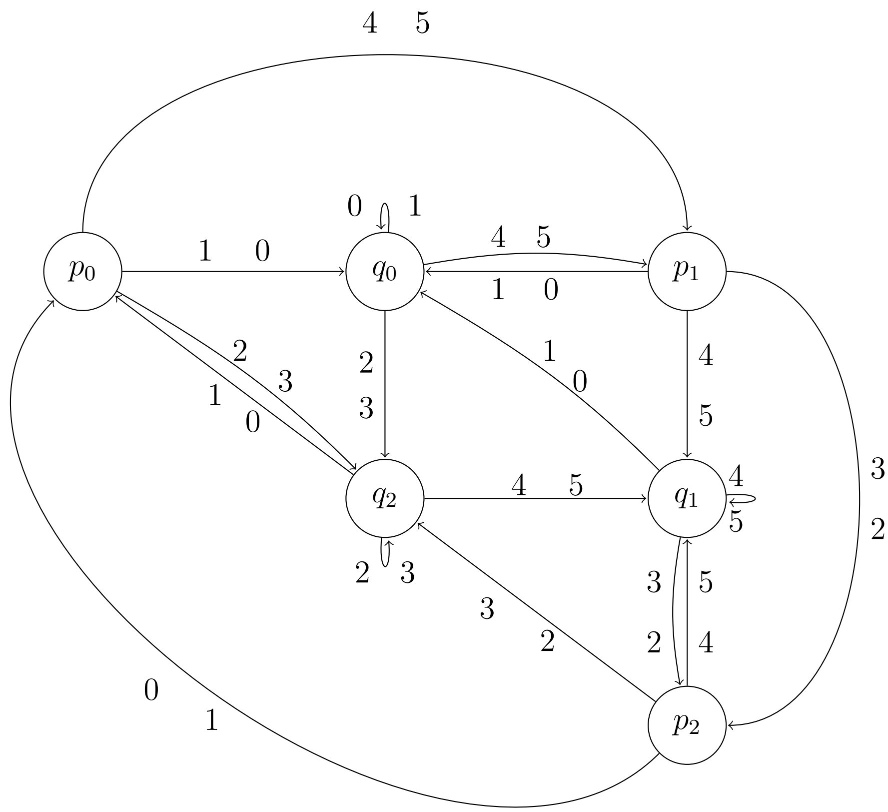

Figure 8: Minimal automaton witnessing finite order of A.

We notice that the automaton B has the property that its synchronizing and amalgamation sequences cohere. In particular both reduce to the single vertex with 6 looped edges after 2 steps.

The fact that every circuit of G_B is on orbit of length 6 can be seen as follows. A circuit of G_B which is not formed by repeating the circuit (or a cyclic rotation of it) $p_0 \to p_1 \to p_2 \to p_0$ a finite number of times, must have an edge leaving a vertex in the inner triangle — any such edge has orbit length 6.

Therefore A satisfies the hypothesis of Theorem 5.3. We work through Lemma 5.2 to find an element of $\mathcal{H}_6$ which conjugates A to a 6-cycle.

In the first step we find two states of G_B which can be collapsed i.e. which distribute similarly over Q_B. We may take the pair (p_0, q_0) (any other valid pair belongs to the orbit of this one). The orbits of p_0 and q_0 are distinct so we are in the second case of Lemma 5.2. Now all edges leaving any vertex in the orbit of q_0 have orbit length 6, whereas the edges

edges from p_0 to q_0 and p_0 to q_2 have orbit length 3 while the edges from p_0 to p_1 have orbit length 6. Thus we apply Lemma 4.20. We add shadow states using Lemma4.19. Focusing on the vertex q_0 as our vertex p (in the notation of Lemma4.19), we see that

$$\begin{aligned} Q(0, q_0) &= \{q_0\} \\ Q(1, q_0) &= \{p_0, p_1\} \\ Q(2, q_0) &= \emptyset. \end{aligned}$$

The last follows since any incoming edge to a vertex on the outer triangle is on an orbit of length 6.

We may take either p_0 or p_1 as the heavy state (since they belong to the same orbit). Our divisibility constant is 3 (the orbit lengths of the two orbits of edges from the outer triangle into the inner triangle, i.e. the edge from p_0 into q_0 represents one such orbit, and the edge from p_1 into q_0 represents the other); the number n' is precisely 6 – since every incoming edge into either p_0 or p_1 has orbit length 6. (We note as an aside that since the edge from p_1 to q_0 is in the orbit of the edge from p_0 to q_2, we only need one round of adding shadow states in order to fix the orbit lengths of both of these edges, using more words, we need not consider $p = q_2$ as a separate case).

Our new automaton B' will have shadow states p_0', p_1' and p_2' as is as depicted in Figure 9. There is a lift ψ_A of ϕ_A to $G_{B'}$. The action of $\psi_{A'}$ is uniquely determined by the facts that the orbit of p_0 under $\psi_{A'}$ is $(p_0\ p_1\ p_2\ p_0'\ p_1'\ p_2')$ and $H(B', \psi_A)$ has minimal representative A.

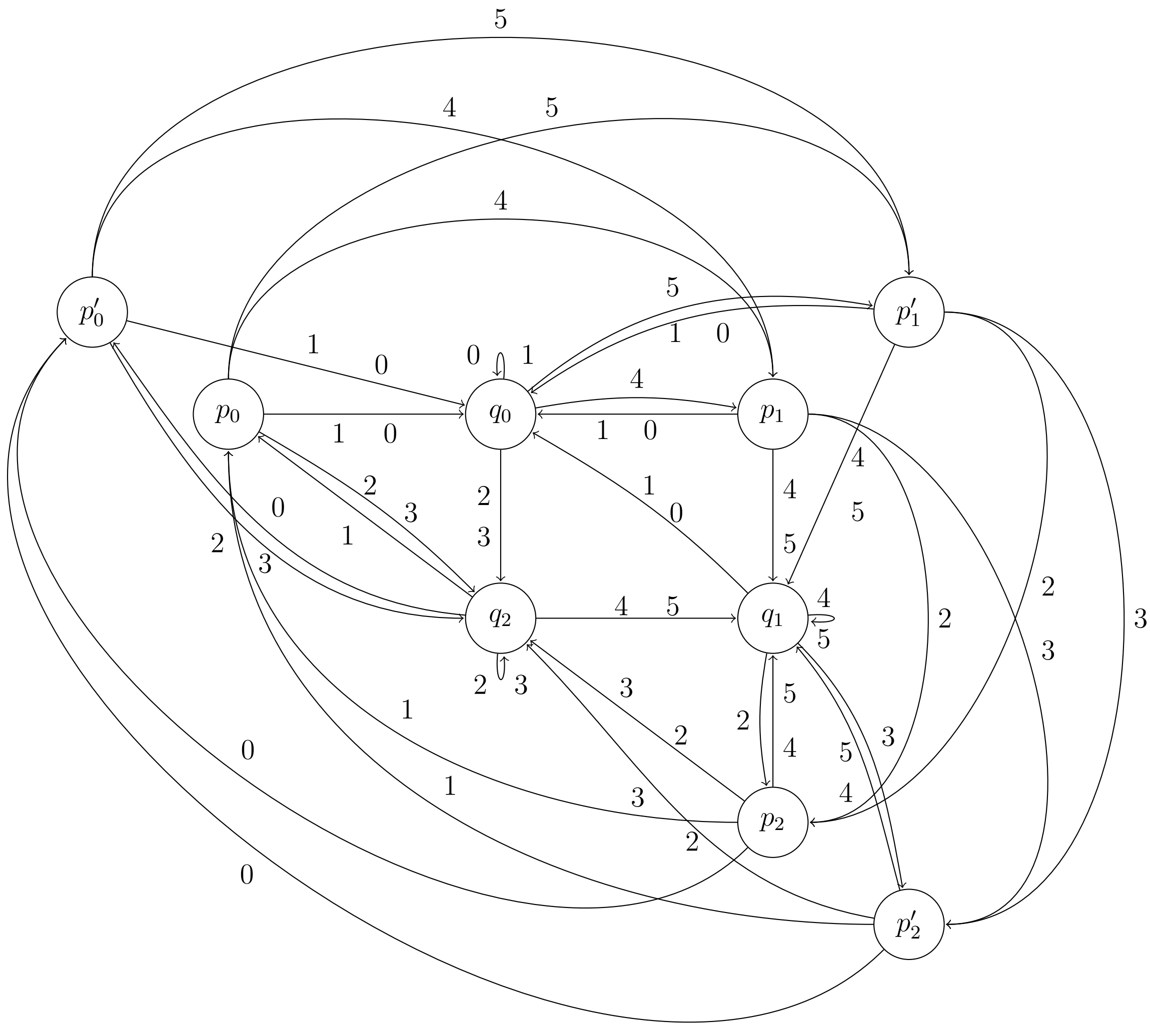

Figure 9: Adding shadows to form B'.

We can now apply Lemma 4.20 to the orbit of the edge from p_2 to q_0 and from p_1 to q_0. Notice that since the orbit lengths of edges leaving the inner triangle is 6, the relabelling map of Lemma 4.20 will simply wrap around the orbits of the relevant edges from p_2 and p_1 to increase their orbit lengths after re-identifying shadow states to 6. This can be achieved by relabelling such that the actions on letters of orbits in the edge $(p_0, \{1, 0\}, q_0)$ mirrors the action on the corresponding edge in the orbit of $(q_0, \{0, 1\}, q_0)$ (similarly for the pair $(p_1, \{1, 0\}, q_0\}$ and $(q_1, \{1, 0\}, q_0)$. One such relabelling is that induced by the vertex fixing automorphism of $G_{B'}$ that swaps the edges from p_1 to q_1, the edges from p_2 to q_2, the edges from p_0' to q_0; the edges from p_1 to q_0, from p_2 to q_1 and from p_0' to q_2. This gives rise to the element C in figure 10.

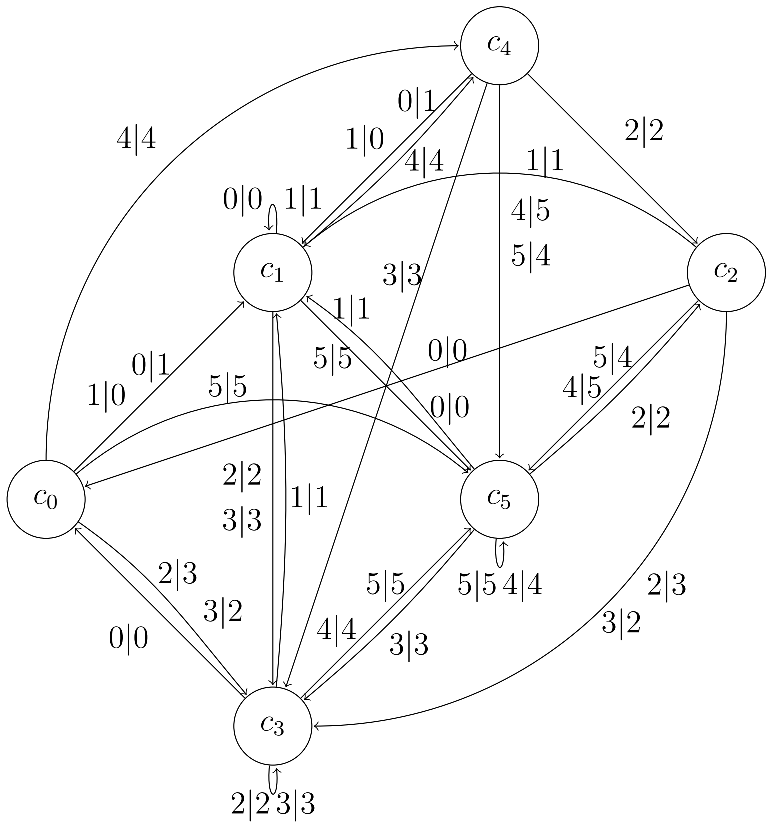

Figure 10: Conjugator C.

The reader can verify that the conjugate of A by C is the automaton D to the left of Figure 11.

The automaton E to the right of Figure 11 admits an automorphism ϕ_D of its underlying digraph such that $H(E, \phi_D)$ has minimal representative D. The map ϕ_D is uniquely determined by the fact that $H(E, \phi_D)$ has minimal representative D. Notice that all edges of G_D are on orbits of length 6 and the collapse and amalgamation sequences of G_D coincide. Following Lemma 5.2, we find a pair of vertices which distribute similarly over Q_D, any pair of distinct vertices works — we choose (a_1, a_3). Now we are in the first case of Lemma 5.2 and the relabelling protocol we apply is that given by Lemma 4.7. Essentially we want to relabel such that the action of a_1 and a_3 on X_6 coincide along their orbits. A relabelling that achieves this is obtained by swapping the edged between a_1 and a_5 and between a_5 and a_3. This relabelling gives rise to the conjugator F in figure 12

The reader can verify that conjugating D by F results in the single state transducer corresponding to the 6-cycle (0 4 2 1 5 3).

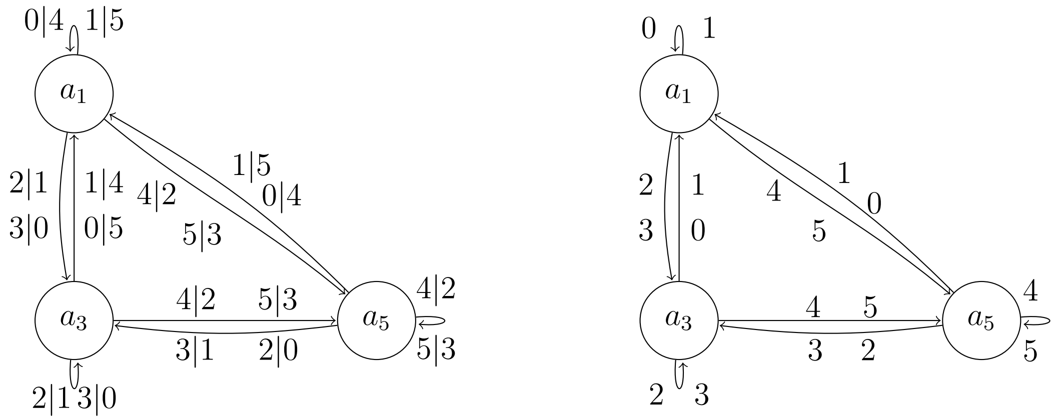

Figure 11: Conjugate of A by relabelling map C.

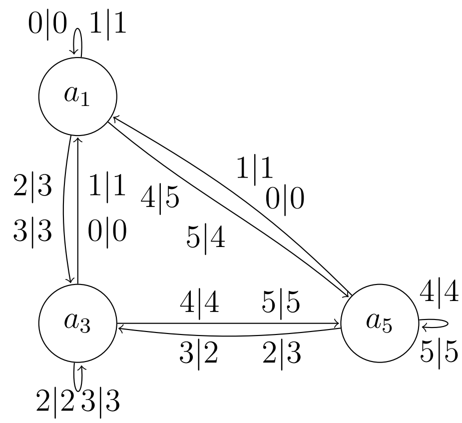

Figure 12: Conjugator F.

Therefore, the element CF of $\mathcal{H}_6$ conjugates A to the 6-cycle (0 4 2 1 5 3).

References

[1] Ali Akhavi, Ines Klimann, Sylvain Lombardy, Jean Mairesse, and Matthieu Picantin. "On the finiteness problem for automaton (semi)groups". In: *Internat. J. Algebra Comput.* 22.6 (2012), pp. 1250052, 26. ISSN: 0218-1967. DOI: `10.1142/S021819671250052X`. URL: `http://dx.doi.org/10.1142/S021819671250052X`.

[2] João Araújo, Peter J. Cameron, and Benjamin Steinberg. "Between primitive and 2-transitive: synchronization and its friends". In: *EMS Surv. Math. Sci.* 4.2 (2017), pp. 101–184. ISSN: 2308-2151. DOI: `10.4171/EMSS/4-2-1`. URL: `https://doi.org/10.4171/EMSS/4-`

[3] C. Bleak, P. Cameron, Y. Maissel, A. Navas, and F. Olukoya. "Automorphism groups for the Higman-Thompson groups $G_{n,r}$." In: *Memoirs AMS* (to appear), pp. 1–85.

[4] Collin Bleak, Peter J. Cameron, and Feyisayo Olukoya. "Automorphisms of shift spaces and the Higman-Thompson groups: the one-sided case". In: *Discrete Anal.* (2021), Paper No. 15, 35. DOI: `10.19086/da`. URL: `https://doi.org/10.19086/da`.

[5] Mike Boyle and Ulf-Rainer Fiebig. "The action of inert finite-order automorphisms on finite subsystems of the shift". In: *Ergodic Theory Dynam. Systems* 11.3 (1991), pp. 413–425. ISSN: 0143-3857. DOI: `10.1017/S0143385700006246`. URL: `https://doi.org/10.1017/S`

[6] Mike Boyle, John Franks, and Bruce Kitchens. "Automorphisms of one-sided subshifts of finite type". In: *Ergodic Theory Dynam. Systems* 10.3 (1990), pp. 421–449. ISSN: 0143-3857. DOI: `10.1017/S0143385700005678`. URL: `https://doi.org/10.1017/S014338570000567`

[7] Mike Boyle and Wolfgang Krieger. "Periodic points and automorphisms of the shift". In: *Trans. Amer. Math. Soc.* 302.1 (1987), pp. 125–149. ISSN: 0002-9947. DOI: `10.2307/2000901`. URL: `https://doi.org/10.2307/2000901`.

[8] *GAP – Groups, Algorithms, and Programming, Version 4.11.0*. The GAP Group. 2020. URL: `\url{https://www.gap-system.org}`.

[9] R. I. Grigorchuk, V. V. Nekrashevich, and V. I. Sushchanskiĭ. "Automata, dynamical systems, and groups". In: *Proc. Steklov Inst. Math* 231 (2000), pp. 128–203.

[10] G. A. Hedlund. "Endomorphisms and automorphisms of the shift dynamical system". In: *Math. Systems Theory* 3 (1969), pp. 320–375. ISSN: 0025-5661.

[11] Bruce P. Kitchens. *Symbolic dynamics*. Universitext. One-sided, two-sided and countable state Markov shifts. Springer-Verlag, Berlin, 1998, pp. x+252. ISBN: 3-540-62738-3. DOI: `10.1007/978-3-642-58822-8`. URL: `https://doi-org.ezproxy.st-andrews.ac.uk/10.1007/`

[12] Ines Klimann. "The finiteness of a group generated by a 2-letter invertible-reversible Mealy automaton is decidable". In: *preprint* (2012), pp. 1–15. URL: `http://arxiv.org/pdf/1208.632`

[13] Y. Muntyan and D. Savchuk. *AutomGrp, Automata groups, Version 1.3.2*. `https://gap-packages.gi` Refereed GAP package. 2019.

[14] Volodymyr Nekrashevych. *Self-similar groups*. Vol. 117. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 2005, pp. xii+231. ISBN: 0-8218-3831-8. DOI: `10.1090/surv/117`. URL: `https://doi.org/10.1090/surv/117`.

[15] Feyishayo Olukoya. *The growth rates of automaton groups generated by reset automata*. submitted. 2017.

[16] Mikhail V. Volkov. "Language and Automata Theory and Applications". In: ed. by Carlos Martín-Vide, Friedrich Otto, and Henning Fernau. Berlin, Heidelberg: Springer-Verlag, 2008. Chap. Synchronizing Automata and the ČErný Conjecture, pp. 11–27. ISBN: 978-3-540-88281-7. DOI: `10.1007/978-3-540-88282-4_4`. URL: `http://dx.doi.org`

[17] R. F. Williams. "Classification of subshifts of finite type". In: *Ann. of Math. (2)* 98 (1973), 120–153; errata, ibid. (2) 99 (1974), 380–381. ISSN: 0003-486X.