An algebraic analysis of Turing machines and Cook's Theorem leading to a profinite fractal differential equation and a random walk on a deterministic Turing machine*

John Rhodes

Department of Mathematics, University of California, Berkeley, California 94720, U.S.A.
e-mail: rhodes@math.berkeley.edu

Pedro V. Silva

Centro de Matemática, Faculdade de Ciências, Universidade do Porto, R. Campo Alegre 687, 4169-007 Porto, Portugal
e-mail: pvsilva@fc.up.pt

June 10, 2006

2000 Mathematics Subject Classification:
18B40 Groupoids, semigroupoids, semigroups, groups (viewed as categories)
20E08 Groups acting on trees
20E18 Limits, profinite groups
20E22 Extensions, wreath products, and other compositions
20F65 Geometric group theory
20F69 Asymptotic properties of groups
20M20 Semigroups of transformations, etc.
20M35 Semigroups in automata theory, linguistics, etc.
60Jxx Markov processes
68Q15 Complexity classes (hierarchies, relations among complexity classes, etc.)
68Q17 Computational difficulty of problems (lower bounds, completeness, difficulty of approximation, etc.)
68Q70 Algebraic theory of languages and automata
94A60 Cryptography

ABSTRACT

*This is a preliminary version of a paper to be submitted to the International Journal of Algebra and Computation. The final version may have additional results and authors.

Contents

1 Introduction **2**

2 Bimachines **7**

3 The block product–composing two bimachines **11**

4 The quest for associativity **21**

5 The trim block product **26**

6 Iterating the block product **26**

7 The matrix representation **41**

8 Turing machines and bimachines **46**

9 A profinite differential equation **51**

10 Random walks on semigroups and Turing machines **56**

1 Introduction

1.1 Existence and understanding

Existence implies feedback and is prior to understanding. That is, things exist, like cells, childern, massive computer programs using inductive loops, ecological systems with complex feedback, etc., but we may not or do not understand them.

Understanding comes later in the form of *introducing coordinates*, i. e., science, describing the system in question with time and space movements in *sequential form.* Thus, if the coordinates $(\ldots, x_n, \ldots, x_1)$ (finite or infinite) describe a system at time and space $c(t, p)$, then if the input π is a change in time or space, then coordinates

$$(\ldots, x_n, \ldots, x_1)\pi = (\ldots, y_n, \ldots, y_1).$$

Understanding implies *sequential form* which means that y_n depends only on $\pi, x_1, \ldots, x_n$ and not on $x_{n+1}, x_{n+2}, \ldots$. (See elliptic contractions above Theorem 6.4 in the text, or [12] with erratum to diagram p. 274, or [13].

Elliptic contractions which are invertible (bi-injections) form the basis of Ukranian Group Theory [6, 7].

1.2 Philosophical viewpoint towards P vs. NP

Our viewpoint toward P vs. NP is that it is obviously true that P does not equal NP, but we need to get more sophisticated relevant mathematics involved to prove there are no polynomial-time programs for NP-complete problems. This is the viewpoint of this paper. The approach may take 2 to 25 years. For an excellent reference for the standard material on P vs. NP, see [10].

1.3 Technical philosophical viewpoint towards proving that P $\neq$ NP

Let T be a deterministic Turing machine always halting and solving problem P; e. g., P is finding a Hamiltonian Cycle in a graph. Let T_n be T running for n steps. Then T_n is "some kind of finite-state machine," and the limit of $T_n \to T$ is "some kind of limit." We next describe what "sort of finite-state machine" and what "sort of limit."

1.4 Technical viewpoint

T_n is a finite-state length-preserving bimachine (see Section 2), and T_n is the iteration or composition of T_1 considered as a bimachine. (See Sections 3 and 8). The limit is the projective on profinite limit of $(T_1)^n = T_n$ (see Section 6) converging to the problem P.

Profinite limits are clearly mathematically powerful enough to prove P is not equal to NP but are difficult to use in general (e. g., Fermat's Last Theorem: see [16, 3]).

1.5 Finite-state automata and bimachines and length-preserving maps

Let A, B be nonempty finite alphabets. We consider A^+, the set of all finite strings on A (i. e., the free semigroup with generators A), and consider maps $\alpha : A^+ \to B^+$ (often with $A = B$) which preserve length (*lp-mappings*). We are interested when α can be done with a finite number of states.

We start with a finite-state automaton given by a right A-automaton (see Section 2) $\mathcal{A}_R = (I_R, Q_R, S_R)$ together with an output function $f : Q_R \times A \to B$. Then $(\mathcal{A}_R, f)$ determines the lp-mapping $\alpha(\mathcal{A}_R, f) \equiv \alpha : A^+ \to B^+$ defined by $\alpha(u, A, v) = f(I_R, u, a)$ for $u, v \in A^*$, $a \in A$ (so independent of v, i. e., (right) causal). For notation, see Section 2, page 7. So

$$\begin{array}{ccccc} a_1 & a_2 & a_3 & \cdots & a_n \\ & & \text{goes to} & & \\ b_1 & b_2 & b_3 & \cdots & b_n \\ \| & \| & \| & & \| \\ f(I_R, a_1) & f(I_R a_1, a_2) & f(I_R a_1 a_2, a_3) & \cdots & f(I_R a_1, \ldots, a_{n-1}, a_n) \end{array}$$

Notice this is linear-time, but what is the coefficient? A B-bimachine $\mathcal{B}$ (see Section 2) is given by a right A-automaton $\mathcal{A}_R = (I_R, Q_R, S_R)$, a left A-automaton $\mathcal{A}_L = (I_L, Q_L, S_L)$, and a function $f : Q_R \times A \times Q_L \to B$, and it determines $\alpha_{\mathcal{B}} : A^+ \to B^+$ by

$$\alpha_{\mathcal{B}}(u, a, v) = f(I_R u, a, v I_L) \text{ for } u, v \in A^*,\ a \in A.$$

For notation, see Section 2, page 7. Thus,

$$\begin{array}{cccc} a_1 & a_2 & \cdots & a_n \\ & \text{goes to} & & \\ b_1 & b_2 & \cdots & b_n \\ \| & \| & & \| \\ f(I_R, a_1, a_2 \cdots a_n I_L) & f(I_R a_1, a_2, a_3 \cdots a_n I_L) & \cdots & f(I_R a_1 \cdots a_{n-1}, a_n, I_L) \end{array}$$

Given $\alpha : A^+ \to B^+$, there is a unique minimal bimachine $\mathcal{B}(\alpha)$ so $\alpha_{\mathcal{B}(\alpha)} = \alpha$. See Proposition 2.3.

Thus, a finite-state bimachine computes b_i from the input string

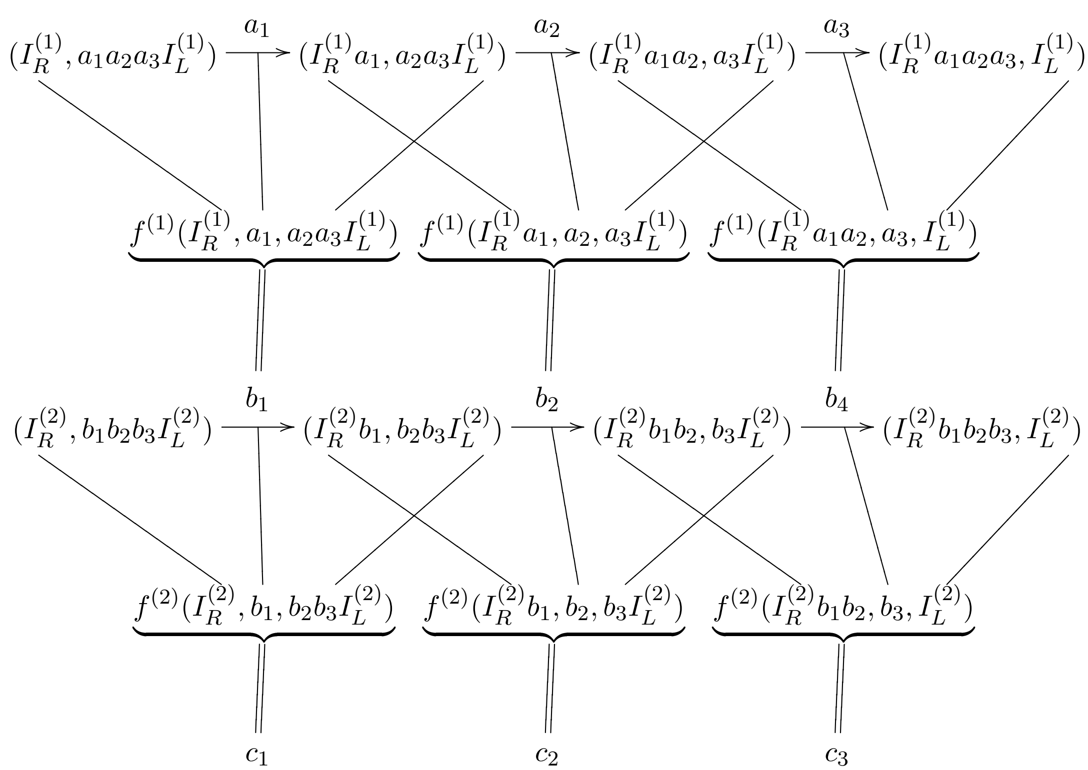
$$a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n$$

by running the right automata $\mathcal{A}_n$ starting at the left of $a_1, \ldots, a_{i-1}$ and running right, which is linear-time in $i-1$ (but what is the coefficient? See Section 6), and running the left automata $\mathcal{A}_L$ starting at the right of $a_{i+1}, \ldots, a_n$ (again, linear-time of length $n-i$) and running left and then determining b_i as $f(I_R a_1 \cdots a_{i-1}, a_i, a_{i+1} \cdots a_n I_L)$ (i. e., as (result of $\mathcal{A}_R, a_i,$ result of $\mathcal{A}_L$)).

This can be illustrated as follows:

$$\underbrace{\overset{\mathcal{A}_R}{\overrightarrow{\text{(linear time)}}}\; a_i \;\overset{\mathcal{A}_L}{\overleftarrow{\text{(linear time)}}}}_{b_i}.$$

The first course of business is to prove that the composition of two lp-maps given by finite-state bimachines is also given by a finite-state bimachine, and the semigroups of the (non-minimal) automata can be taken as double semidirect products of matrix multiplication on upper triangular matrices with coefficients in some semiring. See Section 3. The pictures are as follows:



So

$$c_2 = f^{(2)}(I_R^{(2)} f^{(1)}(I_R^{(1)}, a_1, a_2a_3I_L^{(1)}), f^{(1)}(I_R^{(1)}a_1, a_2, a_3I_L^{(1)}), f^{(1)}(I_R^{(1)}a_1a_2, a_3, I_L^{(1)})I_L^{(2)}),$$

and this corresponds to the matrix product (see Section 3, Lemma 3.1)

$$\begin{pmatrix} (a_1)_L & 0 \\ f_{a_1} & (a_1)_R \end{pmatrix} \cdot \begin{pmatrix} (a_2)_L & 0 \\ f_{a_2} & (a_2)_R \end{pmatrix} = \begin{pmatrix} (a_1)_L(a_2)_L & 0 \\ f_{a_1}(a_2)_L \dot{+} (a_1)_R f_{a_2} & (a_1)_R(a_2)_R \end{pmatrix},$$

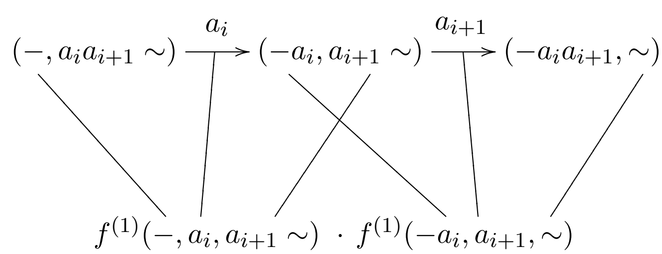
where

$$f_{a_i} : Q_R^{(1)} \times Q_L^{(1)} \to B,$$
$$f_{a_i} = f^{(1)}(-, a_i, \sim) \text{ written as } [-, a_i, \sim].$$

So

$$-(f_{a_1}(a_2)_L + (a_1)_R f_{a_2}) \sim = [-, a_1, a_2 \sim] \cdot [-a_1, a_2, \sim]$$

by considering this picture:



1.6 Associating a finite-state bimachine to a deterministing Turing machine solving a problem P which halts for all inputs

This is exposited in detail in Section 8. The following is a brief overview.

Say we are given the *instantaneous description* (ID) of the Turing machine (TM), say

$$\cdots \boxed{a_1} \cdots \boxed{a_{i-1}}\boxed{\begin{matrix} q \\ a_i \end{matrix}}\boxed{a_{i+1}} \cdots \boxed{a_n} \cdots,$$

where everything to the left of a_1 and to the right of a_n is a blank ($\boxed{B}$), q is the reading head (reading a_i), and $a_1, \ldots, a_n$ are arbitrary tape symbols (including blanks). We consider

$$\boxed{B}\boxed{a_1} \cdots \boxed{a_{i-1}}\boxed{\begin{matrix} q \\ a_i \end{matrix}}\boxed{a_{i+1}} \cdots \boxed{a_n}\boxed{B}.$$

Do one move of T, yielding

$$\begin{array}{c} \boxed{B}\boxed{a_1} \cdots \boxed{a_{i-1}}\boxed{\begin{matrix} q \\ a_i \end{matrix}}\boxed{a_{i+1}} \cdots \boxed{a_n}\boxed{B} \\ T_1 \downarrow \\ \boxed{a'_0}\boxed{a'_1} \cdots \boxed{a'_{i-1}}\boxed{a'_i}\boxed{a'_{i+1}} \cdots \boxed{a'_n}\boxed{a'_{n+1}} \end{array},$$

where $\boxed{a'_j}$ are tape symbols with one or fewer reading heads attached. Then

$$\beta_0 : \mathrm{ID} \to \mathrm{ID}$$

given by

$$\beta_0(a_1, \ldots, a_n) = a'_1, \ldots, a'_n$$

is the associated bimachine (i. e., we chop off a'_0 and a'_{n+1}).

Example 1.1

$$\beta_0\left(\begin{array}{|c|c|c|} \hline a & \overset{\leftarrow}{\boxed{\begin{array}{c} q \\ b \end{array}}} & c \\ \hline \end{array}\right) =$$

$$\begin{array}{|c|c|c|} \hline \boxed{\begin{array}{c} q' \\ a \end{array}} & b' & c \\ \hline \end{array},$$

where $\overset{\leftarrow}{\boxed{\begin{array}{c} q \\ b \end{array}}}$ means the TM will move left, print b' over b, and go into new state q':

$$\beta_0\left(\begin{array}{|c|c|c|c|} \hline \overset{\leftarrow}{\boxed{\begin{array}{c} q \\ b \end{array}}} & c & d & e \\ \hline \end{array}\right) =$$

$$\begin{array}{|c|c|c|c|} \hline b' & c & d & e \\ \hline \end{array},$$

and

$$\beta_0\left(\begin{array}{|c|c|c|c|c|} \hline B & \overset{\leftarrow}{\boxed{\begin{array}{c} q \\ b \end{array}}} & c & d & e \\ \hline \end{array}\right) =$$

$$\begin{array}{|c|c|c|c|c|} \hline \boxed{\begin{array}{c} q' \\ B \end{array}} & b' & c & d & e \\ \hline \end{array},$$

and dually for $\overset{\rightarrow}{\boxed{\begin{array}{c} q \\ b \end{array}}}$.

If S is the set of all the symbols, then $\beta_0 : S^+ \to S^+$ satisfies:

1. β_0 is a finite-state bimachine with $S_R = S^r$, with S^r being the semigroup with elements S and $s_1 s_2 = s_2$; $S_L = S^l$, with S^l being the semigroup with elements S and $s_1 s_2 = s_1$; $Q_R = S^{rI}$ add an identity; $Q_L = S^{lI}$; and $f : S \times S \times S \to S$ is essentially the data determining T.

2. With suitable stopping conventions (see Section 8 for details),

$$\lim_{n \to \infty} \beta_0^n = P,$$

   the problem. Here, $\lim \beta_0^n(w) = \beta_0^{t(w)}(w) = \beta_0(\beta_0^{t(w)}(w)) = \beta_0^{t(w)}(w)$. Time$(w)$ is the smallest $t(w)$ which works, and similarly for space. (See Section 8.)

Going from $T \to b_i \cong \beta_0$ (and we could go back: $\beta_0 \cong b_i \to T$) is essentially an (obvious!) equivalent formulation of Turing machines, so why do it? The taking of powers of β_0 under composition (i. e., running the Turing machine) leads to *algebra*, namely double semidirect products (of semigroups) as evidenced by multiplication in upper triangular matrices with coefficients in some semiring as was discussed in Section 1.5 before and continued in Sections 3 and 4. Two and three iterations of a bimachine are considered in in Sections 3 and 4 and large n iterations is considered in Section 6, and then on to the profinite infinite in Sections 9 and 10.

2 Bimachines

Let A, A' be finite nonempty alphabets. A function $\alpha : A^+ \to A'^+$ is said to be *synchronous* or *length-preserving* if $|\alpha(w)| = |w|$ for every $w \in A^+$. They shall be usually referred as *lp-mappings*.

Let $w \in A^+$ and $i \in \{1, \dots, |w|\}$. We must define a factorization of w to isolate the letter in the ith position. More precisely, we define $\lambda_i(w) \in A^{i-1}$, $\sigma_i(w) \in A$ and $\mu_i(w) \in A^{|w|-i}$ by the equality

$$w = \lambda_i(w)\, \sigma_i(w)\, \mu_i(w).$$

Let $\alpha : A^+ \to A'^+$be an lp-mapping. We extend the domain of α to $A^* \times A \times A^*$ as follows. Given $u, v \in A^*$ and $a \in A$, we write

$$\alpha(u, a, v) = \sigma_{|u|+1}\alpha(uav),$$

i.e. the value of the output string in the $|u| + 1$ position. Note that this domain extension brings no inconsistency. Since

$$\alpha(w) = \prod_{i=1}^{|w|} \sigma_i\alpha(w) = \prod_{i=1}^{|w|} \alpha(\lambda_i(w), \sigma_i(w), \mu_i(w)) \tag{1}$$

for every $w \in A^+$, it follows that an lp-mapping $A^+ \to A'^+$ is uniquely determined by the mapping $\alpha(\_,\_,\_) : A^* \times A \times A^* \to A'$ and vice-versa. More generally, given $u, w \in A^*$ and $v \in A^+$, we write

$$\alpha(u, v, w) = \prod_{i=1}^{|v|} \alpha(u\lambda_i(v), \sigma_i(v), \mu_i(v)w).$$

A semigroup S is said to be A-generated (or an A-semigroup) if there exists a surjective homomorphism $\pi : A^+ \to S$. Given $w \in A^+$, we may write $w_S = \pi(w)$. As usual, we assume that π is implicitly determined by the mention of S and we drop the subscript $_S$ whenever possible.

Given A-semigroups S and S', we say that a semigroup morphism $\varphi : S \to S'$ is an *A-semigroup morphism* if $\varphi(a_S) = a_{S'}$ for every $a \in A$. Clearly, there is at most one A-semigroup morphism from an A-semigroup into another, and it must be necessarily surjective. Thus we can define a partial order on the set of all A-semigroups (up to isomorphism) by

$$S' \leq S \quad \Leftrightarrow \quad \exists \varphi : S \to S'.$$

This is equivalent to

$$\forall u, v \in A^+ \; (u_S = v_S \Rightarrow u_{S'} = v_{S'}).$$

A *right A-automaton* is a triple $\mathcal{A}_R = (I_R, Q_R, S_R)$ where Q_R is a set, $I_R \in Q_R$ and S_R is an A-semigroup acting on Q_R on the right, so

$$(q_R s_R)s'_R = q_R(s_R s'_R)$$

for all $q_R \in Q_R$ and $s_R, s'_R \in S_R$. We recall that this action is *faithful* if

$$(\forall q_R \in Q_R \; q_R s_R = q_R s'_R) \Rightarrow s_R = s'_R$$

holds for all $s_R, s'_R \in S_R$, i.e. different elements act differently on the set of states. The action in the right A-automaton $\mathcal{A}_R$ is NOT assumed to be faithful. However, we shall assume that the action is *proper*, that is, $I_R \notin I_R S_R$. We say that $\mathcal{A}_R$ is finite if Q_R and S_R are both finite. Clearly, the action of S_R on Q_R induces an action of A^+ on Q_R defined by $q_R u = q_R u_{S_R}$.

Let $\mathcal{A}_R = (I_R, Q_R, S_R)$ and $\mathcal{A}'_R = (I'_R, Q'_R, S'_R)$ be right A-automata. A morphism $\varphi : \mathcal{A}_R \to \mathcal{A}'_R$ is defined, whenever $S'_R \leq S_R$, via a mapping $\varphi : Q_R \to Q'_R$ such that

- $\varphi(I_R) = I'_R$;
- $\varphi(q_R u) = \varphi(q_R)u$ for all $q_R \in Q_R$ and $u \in A^+$.

This corresponds exactly to the statement that there exists a mapping on the states and an A-semigroup morphism preserving initial state and the action. If φ is onto, we say that $\mathcal{A}'_R$ is a *quotient* of $\mathcal{A}_R$. We say that the morphism φ is an *embedding* (respectively *isomorphism*) of right A-automata if $S' \cong S$ and φ is an injective (respectively bijective) mapping.

Given a semigroup S, we denote by S^I the semigroup obtained by adjoining an identity to S (even if S is a monoid). If S acts on some set Q, we assume that the new identity acts on Q as the identity.

The right automaton $\mathcal{A}_R = (I_R, Q_R, S_R)$ is said to be *trim* if $Q_R = I_R S_R^I$. The trim part of $\mathcal{A}_R$ is defined by

$$\mathrm{tr}(\mathcal{A}_R) = (I_R, I_R S_R^I, S_R).$$

Clearly, the inclusion map constitutes an embedding of $\mathrm{tr}(\mathcal{A}_R)$ into $\mathcal{A}_R$.

Dually, a *left A-automaton* is a triple (S_L, Q_L, I_L) where Q_L is a set, $I_L \in Q_L$ and S_L is an A-semigroup acting on Q_L on the left. The action is also assumed to be proper and induces canonically an action of A^+ on Q_L. Morphisms are defined dually.

Let A, A' be finite alphabets. An A, A'-*bimachine* is a structure of the form

$$\mathcal{B} = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L)),$$

where

- (I_R, Q_R, S_R) is a right A-automaton;
- (S_L, Q_L, I_L) is a left A-automaton;
- $f : Q_R \times A \times Q_L \to A'$ a full map.

We refer to the function f as the *output function*. We say that $\mathcal{B}$ is finite if (I_R, Q_R, S_R) and (S_L, Q_L, I_L) are both finite. We say that $\mathcal{B}$ is faithful if both actions in (I_R, Q_R, S_R) and (S_L, Q_L, I_L) are faithful.

Let $\mathcal{B} = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L))$ and $\mathcal{B}' = ((I'_R, Q'_R, S'_R), f', (S'_L, Q'_L, I'_L))$ be A, A'-bimachines. We say that $\varphi : \mathcal{B} \to \mathcal{B}'$ is a morphism of A, A'-bimachines if $\varphi = (\varphi_R, \varphi_L)$, where

- $\varphi_R : (I_R, Q_R, S_R) \to (I'_R, Q'_R, S'_R)$ is a morphism of right A-automata;
- $\varphi_L : (S_L, Q_L, I_L) \to (S'_L, Q'_L, I'_L)$ is a morphism of left A-automata;

- $\forall u, v \in A^* \; \forall a \in A \; f'(I'_R u, a, vI'_L) = f(I_R u, a, vI_L)$.

If φ_R and φ_L are both onto, we say that φ is onto and $\mathcal{B}'$ is a quotient of $\mathcal{B}$. If φ_R and φ_L are both embeddings, we say that φ is an embedding. We shall say that φ is an isomorphism if and only if φ_R and φ_L are both isomorphisms.

It is immediate that the class of all A, A'-bimachines and their morphisms constitutes a category.

We associate an lp-mapping $\alpha_{\mathcal{B}} : A^+ \to A'^+$ to the A, A'-bimachine $\mathcal{B} = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L))$ by

$$\alpha_{\mathcal{B}}(u, a, v) = f(I_R u, a, vI_L) \quad (u, v \in A^*, a \in A).$$

Proposition 2.1 *Let $\varphi : \mathcal{B} \to \mathcal{B}'$ be a morphism of A, A'-bimachines. Then $\alpha_{\mathcal{B}} = \alpha_{\mathcal{B}'}$.*

Proof. Write $\mathcal{B} = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L))$ and $\mathcal{B}' = ((I'_R, Q'_R, S'_R), f', (S'_L, Q'_L, I'_L))$. For all $u, v \in A^*$ and $a \in A$, we have

$$\begin{aligned} \alpha_{\mathcal{B}'}(u, a, v) &= f'(I'_R u, a, vI'_L) = f(I_R u, a, vI_L) \\ &= \alpha_{\mathcal{B}}(u, a, v) \end{aligned}$$

and so $\alpha_{\mathcal{B}} = \alpha_{\mathcal{B}'}$. $\square$

A partial converse is given by:

Proposition 2.2 *Let $\mathcal{B} = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L))$ and $\mathcal{B}' = ((I'_R, Q'_R, S'_R), f', (S'_L, Q'_L, I'_L))$ be A, A'-bimachines such that $\alpha_{\mathcal{B}} = \alpha_{\mathcal{B}'}$. If $\varphi_R : (I_R, Q_R, S_R) \to (I'_R, Q'_R, S'_R)$ and $\varphi_L : (S_L, Q_L, I_L) \to (S'_L, Q'_L, I'_L)$ are morphisms of respectively right and left A-automata, then $\varphi = (\varphi_R, \varphi_L)$ is a morphism from $\mathcal{B}$ to $\mathcal{B}'$.*

Proof. For all $u, v \in A^*$ and $a \in A$, we have

$$\begin{aligned} f'(I'_R u, a, vI'_L) &= \alpha_{\mathcal{B}'}(u, a, v) = \alpha_{\mathcal{B}}(u, a, v) \\ &= f(I_R u, a, vI_L) \end{aligned}$$

and so $\varphi = (\varphi_R, \varphi_L)$ is a morphism. $\square$

An A, A'-bimachine $\mathcal{B} = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L))$ is said to be *trim* if both (I_R, Q_R, S_R) and (S_L, Q_L, I_L) are trim. The trim part of $\mathcal{B}$ is defined by

$$\mathrm{tr}(\mathcal{B}) = ((I_R, I_R S_R^I, S_R), f', (S_L, S_L^I I_L, I_L),$$

where f' is the restriction of f to $I_R S_R^I \times A \times S_L^I I_L$. Clearly, the ordered pair of inclusion maps $I_R S_R^I \to Q_R$, $S_L^I I_L \to Q_L$ constitutes an embedding of $\mathrm{tr}(\mathcal{B})$ into $\mathcal{B}$.

We show now we can associate in a canonical way a bimachine to an lp-mapping. Let $\alpha : A^+ \to A'^+$ be an lp-mapping. Given $u, v \in A^+$, we write

$$u \rho_R v \quad \text{if} \quad \forall x, y, z \in A^* \; \forall a \in A \; \alpha(xuy, a, z) = \alpha(xvy, a, z);$$

$$u \rho_L v \quad \text{if} \quad \forall x, y, z \in A^* \; \forall a \in A \; \alpha(x, a, yuz) = \alpha(x, a, yvz);$$

$$u \tau_R v \quad \text{if} \quad \forall y, z \in A^* \; \forall a \in A \; \alpha(uy, a, z) = \alpha(vy, a, z);$$

$$u\tau_L v \qquad \text{if} \qquad \forall x,y \in A^* \, \forall a \in A \; \alpha(x,a,yu) = \alpha(x,a,yv).$$

Clearly, ρ_R and ρ_L are congruences on A^+, and so $S_R = A^+/\rho_R$ and $S_L = A^+/\rho_L$ are A-semigroups. On the other hand, τ_R is a right congruence and τ_L a left congruence on A^+ satisfying

$$\rho_R \subseteq \tau_R, \quad \rho_L \subseteq \tau_L. \tag{2}$$

We can extend τ_R to a right congruence on A^* by defining $1\tau_R = \{1\}$. Let $Q_R = A^*/\tau_R$ and $I_R = 1\tau_R$. We can define a right action of S_R on Q_R by

$$(u\tau_R)(v\rho_R) = (uv)\tau_R \quad (u \in A^*, v \in A^+):$$

indeed, if $u\tau_R u'$ and $v\rho_R v'$, then $(uv)\tau_R(u'v)\rho_R(u'v')$ and so $(uv)\tau_R(u'v')$ by (2).

Similarly, we extend τ_L to A^* and let $Q_L = A^*/\tau_L$ and $I_L = 1\tau_L$. We define a left action of S_L on Q_L by

$$(u\rho_L)(v\tau_L) = (uv)\tau_L \quad (u \in A^+, v \in A^*).$$

Let $f : Q_R \times A \times Q_L \to A'$ be defined by

$$f(u\tau_R, a, v\tau_L) = \alpha(u,a,v).$$

It follows easily from the definition of τ_R and τ_L that f is well defined. Therefore

$$\mathcal{B}_\alpha = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L))$$

is a well-defined trim A, A'-bimachine.

The following result shows that we can view $\mathcal{B}_\alpha$ as the *minimum* bimachine of α.

Proposition 2.3 *Let $\alpha : A^+ \to A'^+$ be an lp-mapping. Then:*

(i) $\alpha_{\mathcal{B}_\alpha} = \alpha$.

(ii) If $\mathcal{B}'$ is a trim A, A'-bimachine such that $\alpha_{\mathcal{B}'} = \alpha$, then there exists a (surjective) morphism $\varphi : \mathcal{B}' \to \mathcal{B}_\alpha$.

(iii) Up to isomorphism, $\mathcal{B}_\alpha$ is the unique trim A, A'-bimachine satisfying (ii).

Proof. (i) Given $u, v \in A^*$ and $a \in A$, we have

$$\begin{aligned} \alpha_{\mathcal{B}_\alpha}(u,a,v) &= f(I_R u, a, vI_L) = f(u\tau_R, a, v\tau_L) \\ &= \alpha(u,a,v) \end{aligned}$$

and so $\alpha_{\mathcal{B}_\alpha} = \alpha$.

(ii) Assume that $\mathcal{B}' = ((I'_R, Q'_R, S'_R), f', (S'_L, Q'_L, I'_L))$ is a trim A, A'-bimachine such that $\alpha_{\mathcal{B}'} = \alpha$. We define mappings $\varphi_R : Q'_R \to Q_R$ and $\psi_R : S'_R \to S_R$ by

$$\varphi_R(I'_R u) = u\tau_R, \quad \psi_R(v_{S'_R}) = v\rho_R \quad (u \in A^*, v \in A^+).$$

Suppose that $v_{S'_R} = w_{S'_R}$. Let $x, y, z \in A^*$ and $a \in A$. We have $(xvy)_{S'_R} = (xwy)_{S'_R}$ and so

$$\begin{aligned} \alpha(xvy,a,z) &= \alpha_{\mathcal{B}'}(xvy,a,z) = f'(I'_R xvy, a, zI'_L) = f'(I'_R xwy, a, zI'_L) \\ &= \alpha_{\mathcal{B}'}(xwy,a,z) = \alpha(xwy,a,z) \end{aligned}$$

and so $v\rho_R = w\rho_R$ and so ψ_R is well defined. Similarly, we can show that φ_R is well defined. It is immediate that ψ_R is an A-semigroup morphism and φ_R an onto morphism of right A-automata.

Similarly, we define an A-semigroup morphism $\psi_L : S'_L \to S_L$ and an onto morphism $\varphi_L : Q'_L \to Q_L$ of left A-automata by

$$\varphi_L(uI'_L) = u\tau_L, \quad \psi_L(v_{S'_L}) = v\rho_L \quad (u \in A^*, v \in A^+).$$

Since $\alpha_{\mathcal{B}'} = \alpha$, it follows from Proposition 2.2 that $\varphi = (\varphi_R, \varphi_L)$ is an onto morphism of $\mathcal{B}'$ onto $\mathcal{B}_\alpha$.

(iii) Suppose that $\mathcal{B}'$ is another trim A, A'-bimachine satisfying (ii). Then we have onto morphisms $\varphi : \mathcal{B}' \to \mathcal{B}_\alpha$ and $\varphi' : \mathcal{B}_\alpha \to \mathcal{B}'$. Since there is at most one morphism from one trim right A-automaton into another, it follows that $\varphi_R\varphi'_R$ and $\varphi'_R\varphi_R$ are both identity mappings, and so φ_R is an isomorphism. Similarly, φ_L is an isomorphism and so is φ. $\square$

We end this section by remarking that changing the initial states in a bimachine may give a new perspective on the computation of the associated lp-mapping.

Proposition 2.4 *Let $\mathcal{B} = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L))$ be an A_1, A_2-bimachine and let $u, w \in A_1^*$, $v \in A_1^+$. If $\mathcal{B}' = ((I_R u, Q_R, S_R), f, (S_L, Q_L, wI_L))$, then*

$$\alpha_{\mathcal{B}}(u, v, w) = \alpha_{\mathcal{B}'}(1, v, 1) = \alpha_{\mathcal{B}'}(v).$$

Proof. It follows from the definitions that

$$\begin{aligned}
\alpha_{\mathcal{B}}(u, v, w) &= \textstyle\prod_{i=1}^{|v|} \alpha_{\mathcal{B}}(u\lambda_i(v), \sigma_i(v), \mu_i(v)w) \\
&= \textstyle\prod_{i=1}^{|v|} f(I_R u\lambda_i(v), \sigma_i(v), \mu_i(v)wI_L) \\
&= \textstyle\prod_{i=1}^{|v|} \alpha_{\mathcal{B}'}(\lambda_i(v), \sigma_i(v), \mu_i(v)) \\
&= \alpha_{\mathcal{B}'}(1, v, 1) = \alpha_{\mathcal{B}'}(v).
\end{aligned}$$

$\square$

An early reference on bimachines is [**?**]. Also see [5, vol. A] and [15].

3 The block product–composing two bimachines

We develop in this section a construction on bimachines appropriate do deal with composition.

Let

$$\mathcal{B}^{(i)} = ((I_R^{(i)}, Q_R^{(i)}, S_R^{(i)}), f^{(i)}, (S_L^{(i)}, Q_L^{(i)}, I_L^{(i)}))$$

be an A_i, A_{i+1}-bimachine for $i = 1, 2$. After some preparation, we shall define an A_1, A_3-bimachine

$$\mathcal{B}^{(2)}\square\mathcal{B}^{(1)} = \mathcal{B}^{(21)} = ((I_R^{(21)}, Q_R^{(21)}, S_R^{(21)}), f^{(21)}, (S_L^{(21)}, Q_L^{(21)}, I_L^{(21)}))$$

called the *block product* of $\mathcal{B}^{(2)}$ and $\mathcal{B}^{(1)}$.

The block product construction involves sets of mappings whose domain is often a direct product of the form $Q_R^{(1)} \times Q_L^{(1)}$. Following [15], we shall use the notation $q_R^{(1)} g q_L^{(1)} = g(q_R^{(1)}, q_L^{(1)})$ for $g \in U^{Q_R^{(1)} \times Q_L^{(1)}} = {}^{Q_R^{(1)}}U^{Q_L^{(1)}}$, $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$. To be consistent, we shall write maps with domains of type $Q_R^{(1)}$ on the right and type $Q_L^{(1)}$ on the left.

We define

$$\overline{S_R^{(21)}} = \begin{pmatrix} S_L^{(1)} & 0 \\ {}^{Q_R^{(1)}}S_R^{(2)Q_L^{(1)}} & S_R^{(1)} \end{pmatrix}.$$

A straightforward adaptation of [5, vol.B, p.142] shows that $\overline{S_R^{(21)}}$ is a semigroup for the product

$$\begin{pmatrix} s_L^{(1)} & 0 \\ g & s_R^{(1)} \end{pmatrix} \begin{pmatrix} s'^{(1)}_L & 0 \\ g' & s'^{(1)}_R \end{pmatrix} = \begin{pmatrix} s_L^{(1)} s'^{(1)}_L & 0 \\ g s'^{(1)}_L + s_R^{(1)} g' & s_R^{(1)} s'^{(1)}_R \end{pmatrix},$$

where

$$q_R^{(1)}(g s'^{(1)}_L + s_R^{(1)} g') q_L^{(1)} = (q_R^{(1)} g(s'^{(1)}_L q_L^{(1)})) + ((q_R^{(1)} s_R^{(1)}) g' q_L^{(1)}).$$

Following [5, vol. B], we use here $+$ to denote the semigroup operation of $S_R^{(2)}$, regardless of being commutative or not, to emphasize that we are doing the natural matrix multiplication. However, we shall revert to the more classical $\cdot$ notation in the sequel.

Let

$$Q_R^{(21)} = Q_R^{(2)Q_L^{(1)}} \times Q_R^{(1)}.$$

It will be often convenient to represent the elements of $Q_R^{(21)}$, termed *R-generalized 2 step crossing sequences*, as 1×2 matrices. The semigroup $\overline{S_R^{(21)}}$ acts on $Q_R^{(21)}$ on the right by

$$\begin{pmatrix} \gamma & q_R^{(1)} \end{pmatrix} \begin{pmatrix} s_L^{(1)} & 0 \\ g & s_R^{(1)} \end{pmatrix} = \begin{pmatrix} \gamma s_L^{(1)} \cdot q_R^{(1)} g & q_R^{(1)} s_R^{(1)} \end{pmatrix},$$

where

$$(\gamma s_L^{(1)} \cdot q_R^{(1)} g)(q_L^{(1)}) = \gamma(s_L^{(1)} q_L^{(1)}) \cdot q_R^{(1)} g q_L^{(1)}.$$

Once again, we note that this is a form of matrix multiplication (but we refrain from using $+$ for the action).

To show that this is indeed an action, we compute

$$\begin{pmatrix} \gamma & q_R^{(1)} \end{pmatrix} \left(\begin{pmatrix} s_L^{(1)} & 0 \\ g & s_R^{(1)} \end{pmatrix} \begin{pmatrix} s'^{(1)}_L & 0 \\ g' & s'^{(1)}_R \end{pmatrix} \right) = \begin{pmatrix} \gamma & q_R^{(1)} \end{pmatrix} \begin{pmatrix} s_L^{(1)} s'^{(1)}_L & 0 \\ g s'^{(1)}_L \cdot s_R^{(1)} g' & s_R^{(1)} s'^{(1)}_R \end{pmatrix}$$

$$= \begin{pmatrix} \gamma(s_L^{(1)} s'^{(1)}_L) \cdot q_R^{(1)}(g s'^{(1)}_L \cdot s_R^{(1)} g') & q_R^{(1)}(s_R^{(1)} s'^{(1)}_R) \end{pmatrix}$$

and

$$\left(\begin{pmatrix}\gamma & q_R^{(1)}\end{pmatrix}\begin{pmatrix}s_L^{(1)} & 0\\ g & s_R^{(1)}\end{pmatrix}\right)\begin{pmatrix}{s'}_L^{(1)} & 0\\ g' & {s'}_R^{(1)}\end{pmatrix} = \begin{pmatrix}\gamma s_L^{(1)}\cdot q_R^{(1)}g & q_R^{(1)}s_R^{(1)}\end{pmatrix}\begin{pmatrix}{s'}_L^{(1)} & 0\\ g' & {s'}_R^{(1)}\end{pmatrix}$$

$$= \begin{pmatrix}(\gamma s_L^{(1)}\cdot q_R^{(1)}g){s'}_L^{(1)}\cdot(q_R^{(1)}s_R^{(1)})g' & (q_R^{(1)}s_R^{(1)}){s'}_R^{(1)}\end{pmatrix}.$$

Since $S_R^{(1)}$ acts on $Q_R^{(1)}$, the second columns coincide. For the first columns, we compute

$$\begin{aligned}
[\gamma(s_L^{(1)}{s'}_L^{(1)})\cdot q_R^{(1)}(g{s'}_L^{(1)}\cdot s_R^{(1)}g')](q_L^{(1)}) &= \gamma((s_L^{(1)}{s'}_L^{(1)})q_L^{(1)})\cdot q_R^{(1)}(g{s'}_L^{(1)}\cdot s_R^{(1)}g')q_L^{(1)}\\
&= \gamma(s_L^{(1)}({s'}_L^{(1)}q_L^{(1)}))\cdot[q_R^{(1)}g({s'}_L^{(1)}q_L^{(1)})\cdot(q_R^{(1)}s_R^{(1)})g'q_L^{(1)}]\\
&= [\gamma(s_L^{(1)}({s'}_L^{(1)}q_L^{(1)}))\cdot q_R^{(1)}g({s'}_L^{(1)}q_L^{(1)})]\cdot(q_R^{(1)}s_R^{(1)})g'q_L^{(1)}\\
&= (\gamma s_L^{(1)}\cdot q_R^{(1)}g)({s'}_L^{(1)}q_L^{(1)})\cdot(q_R^{(1)}s_R^{(1)})g'q_L^{(1)}\\
&= [(\gamma s_L^{(1)}\cdot q_R^{(1)}g){s'}_L^{(1)}\cdot(q_R^{(1)}s_R^{(1)})g'](q_L^{(1)}),
\end{aligned}$$

hence we have indeed an action.

Let

$$I_R^{(21)} = (\gamma_0^{(21)}, I_R^{(1)}),$$

where $\gamma_0^{(21)} \in {Q_R^{(2)}}^{Q_L^{(1)}}$ is defined by $\gamma_0^{(21)}(q_L^{(1)}) = I_R^{(2)}$. The action is proper since $I_R^{(1)} \notin I_R^{(1)}S_R^{(1)}$ implies that $I_R^{(21)} \notin I_R^{(21)}S_R^{(21)}$.

The semigroup $\overline{S_R^{(21)}}$ is not an A_1-semigroup, so let $\eta_R : A^+ \to \overline{S_R^{(21)}}$ be the homomorphism defined by

$$\eta_R(a) = \begin{pmatrix}a_{S_L^{(1)}} & 0\\ g_a^{(1)} & a_{S_R^{(1)}}\end{pmatrix},$$

where

$$q_R^{(1)}g_a^{(1)}q_L^{(1)} = (f^{(1)}(q_R^{(1)}, a, q_L^{(1)}))_{S_R^{(2)}}$$

for all $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$. We define

$$S_R^{(21)} = \eta_R(A^+).$$

It is clear that, given $w \in A^+$, we may write

$$\eta_R(w) = \begin{pmatrix}w_{S_L^{(1)}} & 0\\ g_w^{(1)} & w_{S_R^{(1)}}\end{pmatrix}$$

for some $g_w^{(1)} \in {}^{Q_R^{(1)}}S_R^{(2)Q_L^{(1)}}$. We have now completed the definition of the right A_1-automaton $(I_R^{(21)}, Q_R^{(21)}, S_R^{(21)})$.

Dually, we define

$$Q_L^{(21)} = Q_L^{(1)} \times {}^{Q_R^{(1)}}Q_L^{(2)}.$$

It will be often convenient to represent the elements of $Q_L^{(21)}$, termed *L-generalized 2 step crossing sequences*, as 2×1 matrices. Let

$$I_L^{(21)} = (I_L^{(1)}, \delta_0^{(21)}),$$

where $q_R^{(1)}\delta_0^{(21)} = I_L^{(2)}$.

We define

$$\overline{S_L^{(21)}} = \begin{pmatrix} S_L^{(1)} & 0 \\ {}^{Q_R^{(1)}}S_L^{(2)Q_L^{(1)}} & S_R^{(1)} \end{pmatrix}.$$

Similarly, $\overline{S_L^{(21)}}$ is a semigroup for the product

$$\begin{pmatrix} s_L^{(1)} & 0 \\ h & s_R^{(1)} \end{pmatrix}\begin{pmatrix} s'^{(1)}_L & 0 \\ h' & s'^{(1)}_R \end{pmatrix} = \begin{pmatrix} s_L^{(1)}s'^{(1)}_L & 0 \\ hs'^{(1)}_L \cdot s_R^{(1)}h' & s_R^{(1)}s'^{(1)}_R \end{pmatrix},$$

where

$$q_R^{(1)}(hs'^{(1)}_L \cdot s_R^{(1)}h')q_L^{(1)} = (q_R^{(1)}h(s'^{(1)}_L q_L^{(1)}))((q_R^{(1)}s_R^{(1)})h'q_L^{(1)}).$$

The semigroup $\overline{S_L^{(21)}}$ acts on $Q_L^{(21)}$ on the left by

$$\begin{pmatrix} s_L^{(1)} & 0 \\ h & s_R^{(1)} \end{pmatrix}\begin{pmatrix} q_L^{(1)} \\ \delta \end{pmatrix} = \begin{pmatrix} s_L^{(1)}q_L^{(1)} \\ hq_L^{(1)} \cdot s_R^{(1)}\delta \end{pmatrix},$$

where

$$q_R^{(1)}(hq_L^{(1)} \cdot s_R^{(1)}\delta) = q_R^{(1)}hq_L^{(1)} \cdot (q_R^{(1)}s_R^{(1)})\delta.$$

We omit verifying that this is indeed an action.

Let $\eta_L : A^+ \to \overline{S_L^{(21)}}$ be the homomorphism defined by

$$\eta_L(a) = \begin{pmatrix} a_{S_L^{(1)}} & 0 \\ h_a^{(1)} & a_{S_R^{(1)}} \end{pmatrix},$$

where

$$q_R^{(1)}h_a^{(1)}q_L^{(1)} = (f^{(1)}(q_R^{(1)}, a, q_L^{(1)}))_{S_L^{(2)}}$$

for all $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$. We define

$$S_L^{(21)} = \eta_L(A^+).$$

It is clear that, given $w \in A^+$, we may write

$$\eta_L(w) = \begin{pmatrix} w_{S_L^{(1)}} & 0 \\ \\ h_w^{(1)} & w_{S_R^{(1)}} \end{pmatrix}$$

for some $h_w^{(1)} \in {}^{Q_R^{(1)}}S_L^{(2)Q_L^{(1)}}$. We have now completed the definition of the left A_1-automaton $(S_L^{(21)}, Q_L^{(21)}, I_L^{(21)})$.

Finally, the output function $f^{(21)} : Q_R^{(21)} \times A_1 \times Q_L^{(21)} \to A_3$ is defined by

$$f^{(21)}(\begin{pmatrix}\gamma & q_R^{(1)}\end{pmatrix}, a, \begin{pmatrix} q_L^{(1)} \\ \delta \end{pmatrix}) = f^{(2)}(\gamma(aq_L^{(1)}), f^{(1)}(q_R^{(1)}, a, q_L^{(1)}), (q_R^{(1)}a)\delta).$$

This completes the definition of the bimachine $\mathcal{B}^{(2)}\Box\mathcal{B}^{(1)}$. Note that if $\mathcal{B}^{(2)}$ and $\mathcal{B}^{(1)}$ are both finite, so is $\mathcal{B}^{(2)}\Box\mathcal{B}^{(1)}$.

We want to give an interpretation of $\begin{pmatrix}\gamma\, q_R^{(1)}\end{pmatrix}$ and why it is termed an R-generalized 2-step crossing sequence. The *interpretation* of $\begin{pmatrix}\gamma\, q_R^{(1)}\end{pmatrix}$ is first given by a picture

$$\begin{array}{l} (I_R^{(1)},\ ) \xrightarrow{\frown} (I_R^{(1)} q_R^{(1)}, q_L^{(1)}) \\ (I_R^{(2)},\ ) \longrightarrow (\gamma(q_L^{(1)}),\ ) \end{array}$$

Here, $(\ ,\ )$ represents a member of $Q_R^{(i)} \times Q_L^{(i)}$ for $i = 1, 2$.

Now in words, in considering $\mathcal{B}^{(2)}\Box\mathcal{B}^{(1)}$, if $\frown$ is an input (i. e., a member of A_1^+) which takes the R initial state of $\mathcal{B}^{(2)}\Box\mathcal{B}^{(1)}$ to $(\gamma, q_R^{(1)})$ under the action, then if $\mathcal{B}^{(2)}\Box\mathcal{B}^{(1)}$ is started in the R initial state with the first left automaton started in $q_L^{(1)}$, then the second right state will be $\gamma(q_L^{(1)})$ (which does not depend on $q_L^{(2)}$, the second state of the left machine).

For an informal proof, we must check that this interpretation persists under an application of a letter $a \in A_1$. Well,

$$\begin{aligned} \begin{pmatrix}\gamma\, q_R^{(1)}\end{pmatrix} \cdot a &= \begin{pmatrix}\gamma\, q_R^{(1)}\end{pmatrix} \begin{pmatrix} a_{S_L^{(1)}} & 0 \\ g_a^{(1)} & a_{S_R^{(1)}} \end{pmatrix} \\ &= \begin{pmatrix}\gamma a_L(\ ) \cdot q_R^{(1)} g_a^{(1)}(\ )\, q_R^{(1)} a_R\end{pmatrix} \qquad \begin{array}{r} (\text{with } a_L \equiv a_{S_L^{(1)}}, \\ a_R \equiv a_{S_R^{(1)}}) \end{array} \end{aligned}$$

with $(\ )$ standing for the variable $(q_L^{(1)})$.

But now, looking at the following pictures, we see this gives the new correct interpretation.

$$\begin{tikzcd} (I_R^{(1)},\ ) \arrow[r, "\frown"] & (I_R^{(1)} q_R^{(1)}, a_L q_L^{(1)}) \arrow[r, "a"] \arrow[dr, dash] & (I_R^{(1)} q_R^{(1)} a_R, q_L^{(1)}) \arrow[d, dash] \\ (I_R^{(2)},\ ) \arrow[r] & (\gamma(a_L q_L^{(1)}),\ ) & (x,\ ) \end{tikzcd}$$

(with $x = \gamma(a_L q_L^{(1)}) \cdot f^{(1)}(I_R^{(1)} q_R^{(1)}, a, q_L^{(1)})$.)

Note this interpretation of $(\gamma, q_R^{(1)})$ and its dual also motivates the definition of the output function $f^{(21)}$. Also, see Section 1.5 of the introduction.

Next we expose the nature of the morphisms $g_w^{(1)}$ that play an important part in the definition of η_R and $S_R^{(21)}$.

Lemma 3.1 *For all $w \in A^+$, $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$, we have*

$$q_R^{(1)} g_w^{(1)} q_L^{(1)} = [\prod_{i=1}^{|w|} f^{(1)}(q_R^{(1)} \lambda_i(w), \sigma_i(w), \mu_i(w) q_L^{(1)})]_{S_R^{(2)}}.$$

Proof. We use induction on $|w|$. The case $|w| = 1$ follows from the definition, hence we assume that $|w| > 1$ and the lemma holds for shorter words. We may write $w = va$ with $a \in A_1$. Thus

$$\begin{pmatrix} w_{S_L^{(1)}} & 0 \\ g_w^{(1)} & w_{S_R^{(1)}} \end{pmatrix} = w_{S_R^{(21)}} = v_{S_R^{(21)}} a_{S_R^{(21)}} = \begin{pmatrix} v_{S_L^{(1)}} & 0 \\ g_v^{(1)} & v_{S_R^{(1)}} \end{pmatrix} \begin{pmatrix} a_{S_L^{(1)}} & 0 \\ g_a^{(1)} & a_{S_R^{(1)}} \end{pmatrix}$$

$$= \begin{pmatrix} w_{S_L^{(1)}} & 0 \\ g_v^{(1)} a_{S_L^{(1)}} \cdot v_{S_R^{(1)}} g_a^{(1)} & w_{S_R^{(1)}} \end{pmatrix}.$$

By the induction hypothesis, we get

$$q_R^{(1)}(g_v^{(1)} a_{S_L^{(1)}} \cdot v_{S_R^{(1)}} g_a^{(1)}) q_L^{(1)} = q_R^{(1)} g_v^{(1)} (a q_L^{(1)}) \cdot (q_R^{(1)} v) g_a^{(1)} q_L^{(1)}$$

$$= [\textstyle\prod_{i=1}^{|v|} f^{(1)}(q_R^{(1)} \lambda_i(v), \sigma_i(v), \mu_i(v) a q_L^{(1)})]_{S_R^{(2)}} [f^{(1)}(q_R^{(1)} v, a, q_L^{(1)})]_{S_R^{(2)}}$$

$$= [(\textstyle\prod_{i=1}^{|w|-1} f^{(1)}(q_R^{(1)} \lambda_i(w), \sigma_i(w), \mu_i(w) q_L^{(1)})) f^{(1)}(q_R^{(1)} \lambda_{|w|}(w), \sigma_{|w|}(w), \mu_{|w|}(w) q_L^{(1)})]_{S_R^{(2)}}$$

$$= [\textstyle\prod_{i=1}^{|w|} f^{(1)}(q_R^{(1)} \lambda_i(w), \sigma_i(w), \mu_i(w) q_L^{(1)})]_{S_R^{(2)}}$$

$$= q_R^{(1)} g_w^{(1)} q_L^{(1)}$$

and the lemma holds. $\square$

Similarly, we get:

Lemma 3.2 *For all $w \in A^+$, $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$, we have*

$$q_R^{(1)} h_w^{(1)} q_L^{(1)} = [\prod_{i=1}^{|w|} f^{(1)}(q_R^{(1)} \lambda_i(w), \sigma_i(w), \mu_i(w) q_L^{(1)})]_{S_L^{(2)}}.$$

In view of Lemmas 3.1 and 3.1, we shall from now on use the notation $g_w^{(1)}$ or $h_w^{(1)}$ to denote also the mapping in ${}^{Q_R^{(1)}}A_2^{+Q_L^{(1)}}$ defined by

$$q_R^{(1)}g_w^{(1)}q_L^{(1)} = q_R^{(1)}h_w^{(1)}q_L^{(1)} = \prod_{i=1}^{|w|} f^{(1)}(q_R^{(1)}\lambda_i(w), \sigma_i(w), \mu_i(w)q_L^{(1)}).$$

We shall use the simplified notation

$$w_{S_R^{(21)}} = \begin{pmatrix} w & 0 \\ g_w^{(1)} & w \end{pmatrix}, \quad w_{S_L^{(21)}} = \begin{pmatrix} w & 0 \\ h_w^{(1)} & w \end{pmatrix}$$

when no confusion will arise.

For technical reasons, it is sometimes useful to consider the constant mapping $g_1^{(1)} = h_1^{(1)}$ defined by $q_R^{(1)}g_1^{(1)}q_L^{(1)} = 1$. Note that, under this convention, the formulae

$$(\gamma, q_R^{(1)})w = (\gamma w \cdot q_R^{(1)}g_w^{(1)}, q_R^{(1)}w) \tag{3}$$

and

$$w(q_L^{(1)}, \delta) = (wq_L^{(1)}, h_w^{(1)}q_L^{(1)} \cdot w\delta) \tag{4}$$

hold for every $w \in A^*$.

Our next result shows that the block product of bimachines is adequate to deal with the composition of lp-mappings:

Proposition 3.3 *Let $\mathcal{B}^{(1)}$ be an A_1, A_2-bimachine and let $\mathcal{B}^{(2)}$ be an A_2, A_3-bimachine. Then $\alpha_{\mathcal{B}^{(2)}\square\mathcal{B}^{(1)}} = \alpha_{\mathcal{B}^{(2)}}\alpha_{\mathcal{B}^{(1)}}$.*

Proof. Keeping the same notation used so far, we fix $u, v \in A^*$ and $a \in A$. By Lemmas 3.1 and 3.2, we have

$$\begin{aligned}
\alpha_{\mathcal{B}^{(21)}}(u,a,v) &= f^{(21)}(I_R^{(21)}u, a, vI_L^{(21)}) \\
&= f^{(21)}(\begin{pmatrix} \gamma_0^{(21)} & I_R^{(1)} \end{pmatrix} \begin{pmatrix} u & 0 \\ g_u^{(1)} & u \end{pmatrix}, a, \begin{pmatrix} v & 0 \\ h_v^{(1)} & v \end{pmatrix} \begin{pmatrix} I_L^{(1)} \\ \delta_0^{(21)} \end{pmatrix} \\
&= f^{(21)}(\begin{pmatrix} \gamma_0^{(21)}u \cdot I_R^{(1)}g_u^{(1)} & I_R^{(1)}u \end{pmatrix}, a, \begin{pmatrix} vI_L^{(1)} \\ h_v^{(1)}I_L^{(1)} \cdot v\delta_0^{(21)} \end{pmatrix} \\
&= f^{(2)}((\gamma_0^{(21)}u \cdot I_R^{(1)}g_u^{(1)})(avI_L^{(1)}), f^{(1)}(I_R^{(1)}u, a, vI_L^{(1)}), (I_R^{(1)}ua)(h_v^{(1)}I_L^{(1)} \cdot v\delta_0^{(21)})) \\
&= f^{(2)}(I_R^{(2)}(I_R^{(1)}g_u^{(1)}(avI_L^{(1)})), f^{(1)}(I_R^{(1)}u, a, vI_L^{(1)}), ((I_R^{(1)}ua)h_v^{(1)}I_L^{(1)})I_L^{(2)}).
\end{aligned}$$

On the other hand, by (1), we have

$$\begin{aligned}
\alpha_{\mathcal{B}^{(1)}}(uav) &= \textstyle\prod_{i=1}^{|uav|} \alpha_{\mathcal{B}^{(1)}}(\lambda_i(uav), \sigma_i(uav), \mu_i(uav)) \\
&= \textstyle\prod_{i=1}^{|uav|} f^{(1)}(I_R^{(1)}\lambda_i(uav), \sigma_i(uav), \mu_i(uav)\, I_L^{(1)})
\end{aligned}$$

and so

$$\alpha_{\mathcal{B}^{(2)}}\alpha_{\mathcal{B}^{(1)}}(u,a,v) = f^{(2)}(I_R^{(2)}\lambda_{|ua|}(\alpha_{\mathcal{B}^{(1)}}(uav)), \sigma_{|ua|}(\alpha_{\mathcal{B}^{(1)}}(uav)), \mu_{|ua|}(\alpha_{\mathcal{B}^{(1)}}(uav))\, I_L^{(2)}),$$

$$= f^{(2)}(I_R^{(2)} \prod_{i=1}^{|u|} f^{(1)}(I_R^{(1)}\lambda_i(uav), \sigma_i(uav), \mu_i(uav)\, I_L^{(1)}),$$

$$f^{(1)}(I_R^{(1)}u, a, vI_L^{(1)}), (\prod_{i=|ua|+1}^{|uav|} f^{(1)}(I_R^{(1)}\lambda_i(uav), \sigma_i(uav), \mu_i(uav)\, I_L^{(1)}))\, I_L^{(2)})$$

Therefore we only need to show that

$$I_R^{(1)} g_u^{(1)}(avI_L^{(1)}) = \prod_{i=1}^{|u|} f^{(1)}(I_R^{(1)}\lambda_i(uav), \sigma_i(uav), \mu_i(uav)\, I_L^{(1)} \tag{5}$$

and

$$(I_R^{(1)}ua)h_v^{(1)} I_L^{(1)} = \prod_{i=|ua|+1}^{|uav|} f^{(1)}(I_R^{(1)}\lambda_i(uav), \sigma_i(uav), \mu_i(uav)\, I_L^{(1)}). \tag{6}$$

Clearly,

$$I_R^{(1)} g_u^{(1)}(avI_L^{(1)}) = \prod_{i=1}^{|u|} f^{(1)}(I_R^{(1)}\lambda_i(u), \sigma_i(u), \mu_i(u)avI_L^{(1)})$$

$$= \prod_{i=1}^{|u|} f^{(1)}(I_R^{(1)}\lambda_i(uav), \sigma_i(uav), \mu_i(uav)\, I_L^{(1)}$$

and so (5) holds.

Similarly,

$$(I_R^{(1)}ua)h_v^{(1)} I_L^{(1)} = \prod_{i=1}^{|v|} f^{(1)}(I_R^{(1)}ua\lambda_i(v), \sigma_i(v), \mu_i(v)I_L^{(1)})$$

$$= \prod_{i=|ua|+1}^{|uav|} f^{(1)}(I_R^{(1)}\lambda_i(uav), \sigma_i(uav), \mu_i(uav)\, I_L^{(1)})$$

and so (6) holds as well. $\square$

We prove next two other results on morphisms that will become useful in later sections.

Proposition 3.4 *Let $\mathcal{B}^{(1)}$ be an A_1, A_2-bimachine and let $\mathcal{B}^{(2)}$ and $\mathcal{B'}^{(2)}$ be A_2, A_3-bimachines. Let $\varphi^{(2)} : \mathcal{B}^{(2)} \to \mathcal{B'}^{(2)}$ be a morphism. Then there exists a morphism $\varphi^{(21)} : \mathcal{B}^{(2)}\square\mathcal{B}^{(1)} \to \mathcal{B'}^{(2)}\square\mathcal{B}^{(1)}$ naturally induced by $\varphi^{(2)}$.*

Proof. Let $\mathcal{B}^{(i)} = ((I_R^{(i)}, Q_R^{(i)}, S_R^{(i)}), f^{(i)}, (S_L^{(i)}, Q_L^{(i)}, I_L^{(i)}))$ and $\mathcal{B'}^{(i)} = ((I'^{(i)}_R, Q'^{(i)}_R, S'^{(i)}_R), f'^{(i)}, (S'^{(i)}_L, Q'^{(i)}_L, I'^{(i)}_L))$. Let $\varphi^{(2)} = (\varphi_R^{(2)}, \varphi_L^{(2)})$. Write $\mathcal{B}^{(21)} = \mathcal{B}^{(2)}\square\mathcal{B}^{(1)}$ and $\mathcal{B'}^{(21)} = \mathcal{B'}^{(2)}\square\mathcal{B}^{(1)}$. We define a mapping $\varphi_R^{(21)} : Q_R^{(21)} \to Q'^{(21)}_R$ by

$$\varphi_R^{(21)}(\gamma, q_R^{(1)}) = (\gamma', q_R^{(1)}),$$

where

$$\gamma'(q_L^{(1)}) = \varphi_R^{(2)}(\gamma(q_L^{(1)})).$$

It is routine to check that

$$\varphi_R^{(21)}(I_R^{(21)}) = \varphi_R^{(21)}(\gamma_0, I_R^{(1)}) = (\gamma_0', I_R^{(1)}) = {I'}_R^{(21)}.$$

Next we show that $\varphi_R^{(21)}$ preserves the action. Let $(\gamma, q_R^{(1)}) \in Q_R^{(21)}$ and $a \in A_1$. We can write

$$\varphi_R^{(21)}((\gamma, q_R^{(1)})a) = \varphi_R^{(21)}(\gamma a \cdot q_R^{(1)} g_a^{(1)}, q_R^{(1)} a) = (\gamma_a', q_R^{(1)} a),$$

$$(\varphi_R^{(21)}(\gamma, q_R^{(1)}))a = (\gamma', q_R^{(1)})a = (\gamma' a \cdot q_R^{(1)} g_a^{(1)}, q_R^{(1)} a).$$

It remains to prove that $\gamma_a' = \gamma' a \cdot q_R^{(1)} g_a^{(1)}$. For every $q_L^{(1)} \in Q_L^{(1)}$, we have

$$\begin{aligned}\gamma_a'(q_L^{(1)}) &= \varphi_R^{(2)}((\gamma a \cdot q_R^{(1)} g_a^{(1)})(q_L^{(1)})) = \varphi_R^{(2)}(\gamma(a q_L^{(1)}) \cdot q_R^{(1)} g_a^{(1)} q_L^{(1)}) \\ &= \varphi_R^{(2)}(\gamma(a q_L^{(1)})) \cdot q_R^{(1)} g_a^{(1)} q_L^{(1)} = \gamma'(a q_L^{(1)}) \cdot q_R^{(1)} g_a^{(1)} q_L^{(1)} \\ &= (\gamma' a \cdot q_R^{(1)} g_a^{(1)})(q_L^{(1)})\end{aligned}$$

and so $\varphi_R^{(21)}$ preserves the action.

Now we prove that

$$u_{S_R^{(21)}} = v_{S_R^{(21)}} \Rightarrow u_{{S'}_R^{(21)}} = v_{{S'}_R^{(21)}} \tag{7}$$

holds for all $u, v \in A^+$. It is immediate that this is equivalent to have

$$q_R^{(1)} g_u^{(1)} q_R^{(1)} = q_R^{(1)} g_v^{(1)} q_R^{(1)} \text{ in } S_R^{(2)} \Rightarrow q_R^{(1)} g_u^{(1)} q_R^{(1)} = q_R^{(1)} g_v^{(1)} q_R^{(1)} \text{ in } {S'}_R^{(2)}$$

for all $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$. Since ${S'}_R^{(2)}$ is a quotient of $S_R^{(2)}$, (7) holds and so $\varphi_R^{(21)}$ is a morphism of right A_1-automata.

Similarly, we define a morphism of left A_1-automata $\varphi_L^{(21)} : Q_L^{(21)} \to {Q'}_L^{(21)}$ by

$$(q_L^{(1)}, \delta)\varphi_L^{(21)} = (q_L^{(1)}, \delta'),$$

where

$$q_R^{(1)} \delta' = (q_R^{(1)} \delta)\varphi_L^{(21)}.$$

Finally, let $u, v \in A_1^+$ and $a \in A_1$. Since $\varphi^{(2)}$ is a morphism, we have

$$\begin{aligned}f^{(21)}(I_R^{(21)} u, a, v I_L^{(21)}) &= f^{(21)}((\gamma_0 u \cdot I_R^{(1)} g_u^{(1)}, I_R^{(1)} u), f^{(1)}(q_R^{(1)}, a, q_L^{(1)}), (v I_L^{(1)}, h_v^{(1)} I_L^{(1)} \cdot v\delta_0)) \\ &= f^{(2)}(I_R^{(2)} \cdot I_R^{(1)} g_u^{(1)}(av I_L^{(1)}), f^{(1)}(q_R^{(1)}, a, q_L^{(1)}), (I_R^{(1)} ua) h_v^{(1)} I_L^{(1)} \cdot I_L^{(2)}) \\ &= {f'}^{(2)}({I'}_R^{(2)} \cdot I_R^{(1)} g_u^{(1)}(av I_L^{(1)}), f^{(1)}(q_R^{(1)}, a, q_L^{(1)}), (I_R^{(1)} ua) h_v^{(1)} I_L^{(1)} \cdot {I'}_L^{(2)}) \\ &= {f'}^{(21)}({I'}_R^{(21)} u, a, v {I'}_L^{(21)}),\end{aligned}$$

thus $\varphi^{(21)}$ is a morphism as claimed. □

Proposition 3.5 *Let $\mathcal{B}^{(i)}$ be an A_i, A_{i+1}-bimachine for $i = 1, 2$. Then there exist canonical surjective homomorphisms*

$$\xi_R^{(21)} : (I_R^{(21)}, Q_R^{(21)}, S_R^{(21)}) \to (I_R^{(1)}, Q_R^{(1)}, S_R^{(1)}),$$

$$\xi_L^{(21)} : (S_L^{(21)}, Q_L^{(21)}, I_L^{(21)}) \to (S_L^{(1)}, Q_L^{(1)}, I_L^{(1)}).$$

Proof. Write $\mathcal{B}^{(i)} = ((I_R^{(i)}, Q_R^{(i)}, S_R^{(i)}), f^{(i)}, (S_L^{(i)}, Q_L^{(i)}, I_L^{(i)}))$ for $i = 1, 2$. Since $S_R^{(1)}$ is a quotient of $S_R^{(21)}$, there is a canonical surjective homomorphism

$$\xi_R^{(21)} : (I_R^{(21)}, Q_R^{(21)}, S_R^{(21)}) \to (I_R^{(1)}, Q_R^{(1)}, S_R^{(1)})$$

defined by

$$\xi_R^{(21)}(\gamma, q_R^{(1)}) = q_R^{(1)}.$$

Similarly, there is a canonical surjective homomorphism

$$\xi_L^{(21)} : (S_L^{(21)}, Q_L^{(21)}, I_L^{(21)}) \to (S_L^{(1)}, Q_L^{(1)}, I_L^{(1)})$$

defined by

$$(q_L^{(1)}, \delta)\xi_L^{(21)} = q_L^{(1)}.$$

$\square$

We end this section by observing by means of an example that the block product of faithful bimachines is not necessarily faithful.

Example 3.6 *There exists a finite faithful A_1, A_2-bimachine $\mathcal{B}^{(1)}$ and a finite faithful A_2, A_3-bimachine $\mathcal{B}^{(2)}$ such that $\mathcal{B}^{(2)} \square \mathcal{B}^{(1)}$ is not faithful.*

Proof. Assume that $Q_R^{(2)} = \{I_R^{(2)}, p_R^{(2)}, q_R^{(2)}\}$, $S_R^{(2)} = \{0, 1\}$ (multiplicative) and $S_R^{(2)}$ acts on $Q_R^{(2)}$ by

$$Q_R^{(2)} 0 = q_R^{(2)} 1 = q_R^{(2)}, \quad I_R^{(2)} 1 = p_R^{(2)} 1 = p_R^{(2)}.$$

Assume furthermore that $\operatorname{Im} f = \{0\}$ and $S_R^{(1)}$ is a proper quotient of $S_L^{(1)}$. It is immediate that there exist faithful finite bimachines satisfying these conditions.

Let $u, v \in A_1^+$ be such that $u_{S_R^{(1)}} = v_{S_R^{(1)}}$ but $u_{S_L^{(1)}} \neq v_{S_L^{(1)}}$. Then

$$\begin{pmatrix} u_{s_L^{(1)}} & 0 \\ g_u^{(1)} & u_{s_R^{(1)}} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} v_{s_L^{(1)}} & 0 \\ g_v^{(1)} & v_{s_R^{(1)}} \end{pmatrix}$$

have the same action on $Q_R^{(21)}$ since $g_v^{(1)} = g_v^{(1)}$ has constant image 0. $\square$

4 The quest for associativity

We consider next the product of three bimachines and discuss associativity. Let $\mathcal{B}^{(i)} = ((I_R^{(i)}, Q_R^{(i)}, S_R^{(i)}), f^{(i)}, (S_L^{(i)}, Q_L^{(i)}, I_L^{(i)}))$ be an A_i, A_{i+1}-bimachine for $i = 1, 2, 3$. We shall use the simplified notation

$$\mathcal{B}^{(3(21))} = \mathcal{B}^{(3)} \Box (\mathcal{B}^{(2)} \Box \mathcal{B}^{(1)}), \quad \mathcal{B}^{((32)1)} = (\mathcal{B}^{(3)} \Box \mathcal{B}^{(2)}) \Box \mathcal{B}^{(1)}.$$

The following result shows that we can get associativity at the semigroup level (for three bimachines, but not necessarily for four bimachines!).

Lemma 4.1 $S_R^{(3(21))} \cong S_R^{((32)1)}$ *and* $S_L^{(3(21))} \cong S_L^{((32)1)}$.

Proof. Let $u, v \in A^+$. We show that

$$u_{S_R^{(3(21))}} = v_{S_R^{(3(21))}} \Leftrightarrow u_{S_R^{((32)1)}} = v_{S_R^{((32)1)}}. \tag{8}$$

Clearly, $u_{S_R^{(3(21))}} = v_{S_R^{(3(21))}}$ holds if and only if

(A1) $u_{S_R^{(21)}} = v_{S_R^{(21)}}$;

(A2) $u_{S_L^{(21)}} = v_{S_L^{(21)}}$;

(A3) $(\gamma, q_R^{(1)}) g_u^{(21)} (q_L^{(1)}, \delta) = (\gamma, q_R^{(1)}) g_v^{(21)} (q_L^{(1)}, \delta)$ in $S_R^{(3)}$ for all $(\gamma, q_R^{(1)}) \in Q_R^{(21)}$ and $(q_L^{(1)}, \delta) \in Q_L^{(21)}$.

Now (A1) is equivalent to

(A4) $u_{S_R^{(1)}} = v_{S_R^{(1)}}$;

(A5) $u_{S_L^{(1)}} = v_{S_L^{(1)}}$;

(A6) $q_R^{(1)} g_u^{(1)} q_L^{(1)} = q_R^{(1)} g_v^{(1)} q_L^{(1)}$ in $S_R^{(2)}$ for all $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$.

Similarly, (A2) is equivalent to (A4), (A5) and

(A7) $q_R^{(1)} h_u^{(1)} q_L^{(1)} = q_R^{(1)} h_v^{(1)} q_L^{(1)}$ in $S_L^{(2)}$ for all $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$.

On the other hand, $u_{S_R^{((32)1)}} = v_{S_R^{((32)1)}}$ holds if and only if (A4) and (A5) and

(A8) $q_R^{(1)} g_u^{(1)} q_L^{(1)} = q_R^{(1)} g_v^{(1)} q_L^{(1)}$ in $S_R^{(32)}$ for all $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$

hold. Therefore we may assume that (A4) and (A5) hold, and we must prove that

$$((A3) \wedge (A6) \wedge (A7)) \Leftrightarrow (A8). \tag{9}$$

Assume first that (A8) holds. Let $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$. Write

$$x = q_R^{(1)} g_u^{(1)} q_L^{(1)} = \prod_{i=1}^{|u|} f^{(1)}(q_R^{(1)} \lambda_i(u), \sigma_i(u), \mu_i(u)\, q_L^{(1)}),$$

$$y = q_R^{(1)} g_v^{(1)} q_L^{(1)} = \prod_{i=1}^{|v|} f^{(1)}(q_R^{(1)}\lambda_i(v), \sigma_i(v), \mu_i(v)\, q_L^{(1)}).$$

Note that

$$q_R^{(1)} g_{\lambda_i(u)}^{(1)}(\sigma_i(u)\mu_i(u)\, q_L^{(1)}) = \prod_{j=1}^{i-1} f^{(2)}(q_R^{(1)}\lambda_j(u), \sigma_j(u), \mu_j(u) q_L^{(1)}) = \lambda_i(x).$$

Similarly,

$$(q_R^{(1)}\lambda_i(u)\sigma_i(u)) h_{\mu_i(u)}^{(1)} q_L^{(1)} = \mu_i(x).$$

By (A8), $x = y$ holds in $S_R^{(32)}$. Thus $x = y$ holds in both $S_R^{(2)}$ and $S_L^{(2)}$ and so (A6) and (A7) hold.

Given $(\gamma, q_R^{(1)}) \in Q_R^{(21)}$ and $(q_L^{(1)}, \delta) \in Q_L^{(21)}$, we have by (3)

$$\begin{aligned}
(\gamma, q_R^{(1)}) g_u^{(21)}(q_L^{(1)}, \delta) &= \textstyle\prod_{i=1}^{|u|} f^{(21)}((\gamma, q_R^{(1)})\lambda_i(u), \sigma_i(u), \mu_i(u)\, (q_L^{(1)}, \delta)) \\
&= \textstyle\prod_{i=1}^{|u|} f^{(21)}((\gamma\lambda_i(u) \cdot q_R^{(1)} g_{\lambda_i(u)}^{(1)}, q_R^{(1)}\lambda_i(u)), \sigma_i(u), (\mu_i(u)\, q_L^{(1)}, h_{\mu_i(u)}^{(1)} q_L^{(1)} \cdot \mu_i(u)\delta)) \\
&= \textstyle\prod_{i=1}^{|u|} f^{(2)}(\gamma(u q_L^{(1)}) \cdot q_R^{(1)} g_{\lambda_i(u)}^{(1)}(\sigma_i(u)\mu_i(u)\, q_L^{(1)}), f^{(1)}(q_R^{(1)}\lambda_i(u), \sigma_i(u), \mu_i(u)\, q_L^{(1)}), \\
&\qquad (q_R^{(1)}\lambda_i(u)\sigma_i(u)) h_{\mu_i(u)}^{(1)} q_L^{(1)} \cdot (q_R^{(1)} u)\delta) \\
&= \textstyle\prod_{i=1}^{|x|} f^{(2)}(\gamma(u q_L^{(1)}) \cdot \lambda_i(x), \sigma_i(x), \mu_i(x) \cdot (q_R^{(1)} u)\delta) \\
&= (\gamma(u q_L^{(1)})) g_x^{(1)}((q_R^{(1)} u)\delta).
\end{aligned}$$

Similarly,

$$(\gamma, q_R^{(1)}) g_v^{(21)}(q_L^{(1)}, \delta) = (\gamma(v q_L^{(1)})) g_y^{(1)}((q_R^{(1)} v)\delta).$$

On the other hand, (A8) holds for $q_R^{(1)}$ and $q_L^{(1)}$ if and only if $x_{S_R^{(32)}} = y_{S_R^{(32)}}$ if and only if

(B1) $x_{S_R^{(2)}} = y_{S_R^{(2)}}$;

(B2) $x_{S_L^{(2)}} = y_{S_L^{(2)}}$;

(B3) $q_R^{(2)} g_x^{(2)} q_L^{(2)} = q_R^{(2)} g_y^{(2)} q_L^{(2)}$ in $S_R^{(3)}$ for all $q_R^{(2)} \in Q_R^{(2)}$ and $q_L^{(2)} \in Q_L^{(2)}$.

By (A4) and (A5), we may take

$$q_R^{(2)} = \gamma(u q_L^{(1)}) = \gamma(v q_L^{(1)}), \quad q_L^{(2)} = (q_R^{(1)} u)\delta = (q_R^{(1)} v)\delta$$

and deduce

$$(\gamma, q_R^{(1)}) g_u^{(21)}(q_L^{(1)}, \delta) = (\gamma, q_R^{(1)}) g_v^{(21)}(q_L^{(1)}, \delta)$$

from (B3). Thus (A3) holds.

Conversely, assume that (A3), (A6) and (A7) hold. Let $q_R^{(1)} \in Q_R^{(1)}$ and $q_L^{(1)} \in Q_L^{(1)}$. Since (B1) and (B2) are equivalent to (A6) and (A7), respectively, it remains to prove that (B3) holds. Let $q_R^{(2)} \in Q_R^{(2)}$ and $q_L^{(2)} \in Q_L^{(2)}$. There exist $\gamma \in Q_R^{(2)^{Q_L^{(1)}}}$ and $\delta \in {}^{Q_R^{(1)}}Q_L^{(2)}$ such that $\gamma(uq_L^{(1)}) = q_R^{(2)}$ and $(q_R^{(1)}u)\delta = q_L^{(2)}$. In view of (A4) and (A5), (B3) follows from (A3) since

$$q_R^{(2)} g_x^{(2)} q_L^{(2)} = (\gamma, q_R^{(1)}) g_u^{(21)} (q_L^{(1)}, \delta) = (\gamma, q_R^{(1)}) g_v^{(21)} (q_L^{(1)}, \delta) = q_R^{(2)} g_y^{(2)} q_L^{(2)}.$$

Thus (9) holds and so does (8). Therefore $S_R^{(3(21))} \cong S_R^{((32)1)}$. Similarly, we can show that $S_L^{(3(21))} \cong S_L^{((32)1)}$. $\square$

Unfortunately the right A_1-automata of $\mathcal{B}_R^{(3(21))}$ and $\mathcal{B}_R^{((32)1)}$ are not in general isomorphic, as one can easily show using a cardinality argument on the states, and the same goes for the left A_1-automata. However, we can define morphisms. Let $\varphi_R : Q_R^{(3(21))} \to Q_R^{((32)1)}$ be defined as follows. Given

$$(\gamma^{(3(21))}, (\gamma^{(21)}, q_R^{(1)})) \in Q_R^{(3)^{Q_L^{(21)}}} \times (Q_R^{(2)^{Q_L^{(1)}}} \times Q_R^{(1)}) = Q_R^{(3(21))},$$

we set

$$(\gamma^{(3(21))}, (\gamma^{(21)}, q_R^{(1)}))\varphi_R = (\gamma^{((32)1)}, q_R^{(1)}) \in Q_R^{(32)^{Q_L^{(1)}}} \times Q_R^{(1)} = Q_R^{((32)1)},$$

where

$$\gamma^{((32)1)}(q_L^{(1)}) = (\beta_{q_L^{(1)}}, \gamma^{(21)}(q_L^{(1)})) \in Q_R^{(3)^{Q_L^{(2)}}} \times Q_R^{(2)} = Q_R^{(32)}$$

and

$$\beta_{q_L^{(1)}}(q_L^{(2)}) = \gamma^{(3(21))}(q_L^{(1)}, \overline{q_L^{(2)}}),$$

where $\overline{q_L^{(2)}} \in {}^{Q_R^{(1)}}Q_L^{(2)}$ is the constant mapping with image $q_L^{(2)}$.

Dually, we define $\varphi_L : Q_L^{(3(21))} \to Q_L^{((32)1)}$ as follows. Given

$$((q_L^{(1)}, \delta^{(21)}), \delta^{(3(21))}) \in (Q_L^{(1)} \times {}^{Q_R^{(1)}}Q_L^{(2)}) \times {}^{Q_R^{(21)}}Q_L^{(3)} = Q_L^{(3(21))},$$

we set

$$\varphi_L((q_L^{(1)}, \delta^{(21)}), \delta^{(3(21))}) = (q_L^{(1)}, \delta^{((32)1)}) \in Q_L^{(1)} \times {}^{Q_R^{(1)}}Q_L^{(32)} = Q_L^{((32)1)},$$

where

$$q_R^{(1)}\delta^{((32)1)} = (q_R^{(1)}\delta^{(21)}, \varepsilon_{q_R^{(1)}}) \in Q_L^{(2)} \times {}^{Q_R^{(2)}}Q_L^{(3)} = Q_L^{(32)}$$

and

$$q_R^{(2)}\varepsilon_{q_R^{(1)}} = (\overline{q_R^{(2)}}, q_R^{(1)})\delta^{(3(21))}$$

where $\overline{q_R^{(2)}} \in Q_R^{(2)^{Q_L^{(1)}}}$ is the constant mapping with image $q_R^{(2)}$.

Lemma 4.2 *(i)* $\varphi_R : (I_R^{(3(21))}, Q_R^{(3(21))}, S_R^{(3(21))}) \to (I_R^{((32)1)}, Q_R^{((32)1)}, S_R^{((32)1)})$ *is a surjective morphism of right A_1-automata;*

(ii) $\varphi_L : (S_L^{(3(21))}, Q_L^{(3(21))}, I_L^{(3(21))}) \to (S_L^{((32)1)}, Q_L^{((32)1)}, I_L^{((32)1)})$ *is a surjective morphism of left A_1-automata.*

Proof. We give a proof for φ_L, the other case being dual. We have

$$\varphi_L(I_L^{(3(21))}) = \varphi_L(I_L^{(21)}, \delta_0^{(3(21))}) = \varphi_L((I_L^{(1)}, \delta_0^{(21)}), \delta_0^{(3(21))}) = (I_L^{(1)}, \delta^{((32)1)}),$$

where

$$q_R^{(1)}\delta^{((32)1)} = (q_R^{(1)}\delta_0^{(21)}, \varepsilon_{q_R^{(1)}}) = (I_L^{(2)}, \varepsilon_{q_R^{(1)}})$$

and

$$q_R^{(2)}\varepsilon_{q_R^{(1)}} = (\overline{q_R^{(2)}}, q_R^{(1)})\delta_0^{(3(21))} = I_L^{(3)}.$$

Thus

$$q_R^{(1)}\delta^{((32)1)} = (I_L^{(2)}, \delta_0^{(32)}) = I_L^{(32)}$$

and so $\delta^{((32)1)} = \delta_0^{((32)1)}$. It follows that $\varphi_L(I_L^{(3(21))}) = I_L^{((32)1)}$.

Next let $((q_L^{(1)}, \delta^{(21)}), \delta^{(3(21))}) \in Q_L^{(3(21))}$, and $a \in A_1$. We have

$$\begin{aligned} a((q_L^{(1)}, \delta^{(21)}), \delta^{(3(21))}) &= (a(q_L^{(1)}, \delta^{(21)}), h_a^{(21)}(q_L^{(1)}, \delta^{(21)}) \cdot a\delta^{(3(21))}) \\ &= ((aq_L^{(1)}, h_a^{(1)}q_L^{(1)} \cdot a\delta^{(21)}), h_a^{(21)}(q_L^{(1)}, \delta^{(21)}) \cdot a\delta^{(3(21))}), \end{aligned}$$

hence

$$\varphi_L(a((q_L^{(1)}, \delta^{(21)}), \delta^{(3(21))})) = (aq_L^{(1)}, \eta^{(3(21))})$$

for the corresponding mapping $\eta^{(3(21))}$. On the other hand,

$$a\varphi_L((q_L^{(1)}, \delta^{(21)}), \delta^{(3(21))}) = a(q_L^{(1)}, \delta^{((32)1)}) = (aq_L^{(1)}, h_a^{(1)}q_L^{(1)} \cdot a\delta^{((32)1)}).$$

Therefore, to show that φ_L preserves the action, we only need to show that

$$\eta^{(3(21))} = h_a^{(1)}q_L^{(1)} \cdot a\delta^{((32)1)}. \tag{10}$$

Let $q_R^{(1)} \in Q_R^{(1)}$. Writing $b = f^{(1)}(q_R^{(1)}, a, q_L^{(1)})$, we have

$$\begin{aligned} q_R^{(1)}(h_a^{(1)}q_L^{(1)} \cdot a\delta^{((32)1)}) &= q_R^{(1)}h_a^{(1)}q_L^{(1)} \cdot (q_R^{(1)}a)\delta^{((32)1)}) \\ &= b((q_R^{(1)}a)\delta^{(21)}, \varepsilon_{q_R^{(1)}a}) \\ &= (b \cdot (q_R^{(1)}a)\delta^{(21)}, h_b^{(2)}((q_R^{(1)}a)\delta^{(21)}) \cdot b\varepsilon_{q_R^{(1)}a}) \end{aligned}$$

and

$$q_R^{(1)}\eta^{(3(21))} = (q_R^{(1)}(h_a^{(1)}q_L^{(1)} \cdot a\delta^{(21)}), \varepsilon'_{q_R^{(1)}}),$$

where

$$q_R^{(2)}\varepsilon'_{q_R^{(1)}} = (\overline{q_R^{(2)}}, q_R^{(1)})(h_a^{(21)}(q_L^{(1)}, \delta^{(21)}) \cdot a\delta^{(3(21))}).$$

Since

$$q_R^{(1)}(h_a^{(1)}q_L^{(1)} \cdot a\delta^{(21)}) = q_R^{(1)}h_a^{(1)}q_L^{(1)} \cdot (q_R^{(1)}a)\delta^{(21)} = b \cdot (q_R^{(1)}a)\delta^{(21)},$$

(10) will follow from

$$h_b^{(2)}((q_R^{(1)}a)\delta^{(21)}) \cdot b\varepsilon_{q_R^{(1)}a} = \varepsilon'_{q_R^{(1)}}. \tag{11}$$

We have

$$q_R^{(2)}[h_b^{(2)}((q_R^{(1)}a)\delta^{(21)}) \cdot b\varepsilon_{q_R^{(1)}a}] = q_R^{(2)}h_b^{(2)}((q_R^{(1)}a)\delta^{(21)}) \cdot (q_R^{(2)}b)\varepsilon_{q_R^{(1)}a}$$

$$= f^{(2)}(q_R^{(2)}, b, (q_R^{(1)}a)\delta^{(21)}) \cdot (\overline{q_R^{(2)}b}, q_R^{(1)}a)\delta^{(3(21))},$$

$$q_R^{(2)}\varepsilon'_{q_R^{(1)}} = (\overline{q_R^{(2)}}, q_R^{(1)})(h_a^{(21)}(q_L^{(1)}, \delta^{(21)}) \cdot a\delta^{(3(21))})$$

$$= (\overline{q_R^{(2)}}, q_R^{(1)})h_a^{(21)}(q_L^{(1)}, \delta^{(21)}) \cdot ((\overline{q_R^{(2)}}, q_R^{(1)})a)\delta^{(3(21))}$$

$$= f^{(21)}((\overline{q_R^{(2)}}, q_R^{(1)}), a, (q_L^{(1)}, \delta^{(21)})) \cdot (\overline{q_R^{(2)}}a \cdot q_R^{(1)}g_a^{(1)}, q_R^{(1)}a)\delta^{(3(21))}$$

$$= f^{(2)}(q_R^{(2)}, b, (q_R^{(1)}a)\delta^{(21)}) \cdot (\overline{q_R^{(2)}}a \cdot q_R^{(1)}g_a^{(1)}, q_R^{(1)}a)\delta^{(3(21))},$$

thus we only need to show that

$$\overline{q_R^{(2)}b} = \overline{q_R^{(2)}}a \cdot q_R^{(1)}g_a^{(1)}.$$

Indeed, for every $p_L^{(1)} \in Q_L^{(1)}$,

$$(\overline{q_R^{(2)}}a \cdot q_R^{(1)}g_a^{(1)})(p_L^{(1)}) = \overline{q_R^{(2)}}(ap_L^{(1)}) \cdot q_R^{(1)}g_a^{(1)}p_L^{(1)}$$

$$= q_R^{(2)}b = \overline{q_R^{(2)}b}(p_L^{(1)}),$$

hence (11) holds and so does (10). Therefore φ_L preserves the action and so is a morphism of right A_1-automata in view of Lemma 4.1.

To show that φ_L is onto, take

$$(q_L^{(1)}, \eta) \in Q_L^{(1)} \times {}^{Q_R^{(1)}}Q_L^{(32)} = Q_L^{((32)1)}.$$

We define $\delta^{(21)} \in {}^{Q_R^{(1)}}Q_L^{(2)}$ and $\eta_{q_R^{(1)}} \in {}^{Q_R^{(2)}}Q_L^{(3)}$ for each $q_R^{(1)} \in Q_R^{(1)}$ by

$$q_R^{(1)}\eta = (q_R^{(1)}\delta^{(21)}, \eta_{q_R^{(1)}}).$$

Finally, we define $\delta^{(3(21))} \in {}^{Q_R^{(21)}}Q_L^{(3)}$ by

$$(\gamma, q_R^{(1)})\delta^{(3(21))} = (\gamma(q_L^{(1)}))\eta_{q_R^{(1)}}$$

and show that
$$(q_L^{(1)},\eta) = \varphi_L((q_L^{(1)},\delta^{(21)}),\delta^{(3(21))}).$$

We have $\varphi_L((q_L^{(1)},\delta^{(21)}),\delta^{(3(21))}) = (q_L^{(1)},\delta^{((32)1)})$ with
$$q_R^{(1)}\delta^{((32)1)} = (q_R^{(1)}\delta^{(21)},\varepsilon_{q_R^{(1)}}), \quad q_R^{(2)}\varepsilon_{q_R^{(1)}} = (\overline{q_R^{(2)}},q_R^{(1)})\delta^{(3(21))}.$$

We must show that $\delta^{((32)1)} = \eta$, which follows from $\varepsilon_{q_R^{(1)}} = \eta_{q_R^{(1)}}$. Indeed,
$$q_R^{(2)}\varepsilon_{q_R^{(1)}} = (\overline{q_R^{(2)}},q_R^{(1)})\delta^{(3(21))} = (\overline{q_R^{(2)}}(q_L^{(1)}))\eta_{q_R^{(1)}} = q_R^{(2)}\eta_{q_R^{(1)}}$$

and so φ_L is onto as claimed. $\Box$

Theorem 4.3 *$(\mathcal{B}^{(3)}\Box\mathcal{B}^{(2)})\Box\mathcal{B}^{(1)}$ is a quotient of $\mathcal{B}^{(3)}\Box(\mathcal{B}^{(2)}\Box\mathcal{B}^{(1)})$.*

Proof. By Proposition 3.3, we have
$$\alpha_{\mathcal{B}^{(3(21))}} = \alpha_{\mathcal{B}^{(3)}}\alpha_{\mathcal{B}^{(21)}} = \alpha_{\mathcal{B}^{(3)}}\alpha_{\mathcal{B}^{(2)}}\alpha_{\mathcal{B}^{(1)}} = \alpha_{\mathcal{B}^{(32)}}\alpha_{\mathcal{B}^{(1)}} = \alpha_{\mathcal{B}^{((32)1)}}.$$

By Proposition 2.2 and Lemma 4.2, $\varphi = (\varphi_R,\varphi_L)$ is an onto morphism from $\mathcal{B}$ to $\mathcal{B}'$. $\Box$

5 The trim block product

6 Iterating the block product

We intend to compose an arbitrary number of bimachines via block product. Since the block product is not associative, we must choose the bracketing to be considered. Our choice is bracketing from left to right, that is, priority is assumed to hold from left to right. In the case of three bimachines, this means that $(\mathcal{B}^{(3)}\Box\mathcal{B}^{(2)})\Box\mathcal{B}^{(1)}$ is our option.

We introduce the following recursive notation: given $n \geq 2$, let $[n,n-1] = (n,n-1)$. If $[n,k]$ is defined for $k \in \{2,\ldots,n-1\}$, let $[n,k-1] = ([n,k],k-1)$. Whenever convenient, we shall assume that $[n,n] = (n)$.

Let $\mathcal{B}^{(i)} = ((I_R^{(i)},Q_R^{(i)},S_R^{(i)}),f^{(i)},(S_L^{(i)},Q_L^{(i)},I_L^{(i)}))$ be an A_i,A_{i+1}-bimachine for $i = 1,\ldots,n$. Then
$$\mathcal{B}^{[n,k]} = ((\ldots(\mathcal{B}^{(n)}\Box\mathcal{B}^{(n-1)})\Box\mathcal{B}^{(n-2)})\Box\ldots)\Box\mathcal{B}^{(k)}.$$

It will be convenient to develop an alternative characterization of the states in the iterated block product. For all $n \geq 2$ and $k \in \{1,\ldots,n-1\}$, we define
$$P_R^{[n,k]} = Q_R^{(n)\,Q_L^{(k)}\times Q_L^{(k+1)}\times\ldots\times Q_L^{(n-1)}} \times Q_R^{(n-1)\,Q_L^{(k)}\times Q_L^{(k+1)}\times\ldots\times Q_L^{(n-2)}}$$
$$\times\ldots\times Q_R^{(k+1)\,Q_L^{(k)}} \times Q_R^{(k)}.$$

Dually, we define
$$P_L^{[n,k]} = Q_L^{(k)} \times {}^{Q_R^{(k)}}Q_L^{(k+1)} \times \ldots \times {}^{Q_R^{(n-1)}\times\ldots\times Q_R^{(k)}}Q_L^{(n)}.$$

The elements of $P_R^{[n,1]}$ and $P_L^{[n,1]}$ are termed respectively *R-generalized* and *L-generalized n step crossing sequences*.

Intuition for the following material is as follows. $\mathcal{B}^{[n,1]}$ is already defined, but to see what it is and what the action is, we first note the states are in one-to-one correspondence with

$$\begin{aligned} P_R^{[n,1]} &= {Q_R^{(n)}}^{Q_L^{(1)}\times\cdots\times Q_L^{(n-1)}} \times {Q_R^{(n-1)}}^{Q_L^{(1)}\times\cdots\times Q_L^{(n-2)}} \times\cdots\times {Q_R^{(3)}}^{Q_L^{(1)}\times Q_L^{(2)}} \times {Q_R^{(2)}}^{Q_L^{(1)}} \times Q_R^{(1)} \\ &\cong_{\text{(bijection)}} (\mathcal{B}^{[n-2]})^{Q_L^{(1)}} \times Q_R^{(1)} \end{aligned}$$

and we write a member of this as

$$(\gamma, q_R^{(1)}) \qquad \gamma : Q_L^{(1)} \to \mathcal{B}^{[n-2]}.$$

Now we use the same formula as we did for the action of $\mathcal{B}^{(2)}\Box\mathcal{B}^{(1)}$, namely for $a \in A$,

$$\begin{aligned} (\gamma, q_R^{(1)})\cdot a &\cong (\gamma, q_R^{(1)}) \begin{pmatrix} a_L = a_{S_L^{(1)}} & 0 \\ g_a^{(1)} & a_R = a_{S_R^{(1)}} \end{pmatrix} \\ &= (\gamma a_L(\ )\cdot q_R^{(1)} g_a^{(1)}, q_R^{(1)} a_R), \end{aligned}$$

where $\cdot$ is the inductively defined action on $P_R^{[n,2]}$. It is as simple as that. The details will follow.

Also, an interpretation can be given to $(\gamma_n, \dots, \gamma_1) \in P_R^{[n,1]}$ similar to the case $n = 2$ already given in Section 3, justifying why $(\gamma_n, \dots, \gamma_1)$ is called an R-generalized n-step crossing sequence, namely the following.

The *interpretation* of $(\gamma_n, \dots, \gamma_1) \in P_R^{[n,1]}$ is first given by a picture

$$\begin{aligned} (I_R^{(1)},\ ) &\overset{\sim}{\longrightarrow} (I_R^{(1)}\gamma_1, q_L^{(1)}) \\ (I_R^{(2)},\ ) &\overset{\sim}{\longrightarrow} (I_R^{(2)}\gamma_2(q_L^{(1)}), q_L^{(2)}) \\ &\vdots \\ (I_R^{(n-1)},\ ) &\overset{\sim}{\longrightarrow} (I_R^{(n-1)}\gamma_{n-1}(q_L^{(1)},\dots,q_L^{(n-2)}), q_L^{(n-1)}) \\ (I_R^{(n)},\ ) &\overset{\sim}{\longrightarrow} (I_R^{(n)}\gamma_n(q_L^{(1)},\dots,q_L^{(n-1)}), -) \end{aligned}$$

Here, $(\ ,\ )$ represents a member of $Q_R^{(i)} \times Q_L^{(i)}$, for $i = 1, \dots, n$. Now in words, in considering $\mathcal{B}^{[n,1]}$, if $\sim$ is an input (i. e., a member of A_1^+) which takes the R intitial state of $\mathcal{B}^{[n,1]}$ to $(\gamma_n, \dots, \gamma_2, \gamma_1) \in P_R^{[n,1]}$ under the action with the first, second, third, …, $(n-1)^{\text{st}}$ left automaton states being assigned arbitrarily to $q_L^{(1)}$, $q_L^{(2)}$, …, $q_L^{(n-1)}$ (*no* $q_L^{(n)}$ is given), then the final right states will be $I_R^{(1)}\gamma_1$, $I_R^{(2)}\gamma_2(q_L^{(1)})$, …, $I_R^{(n-1)}\gamma_{n-1}(q_L^{(1)}, \dots, q_L^{(n-2)})$, $I_R^{(n)}\gamma_n(q_L^{(1)}, \dots, q_L^{(n-1)})$. The proof is similar to the $n = 2$ case.

To make a little more sense of the previous pictures, perhaps the following will be helpful. See [15].

Let $\mathcal{B}$ be an A, B-bimachine. The *representing category* of $\mathcal{B}$, $\mathrm{Cat}(\mathcal{B})$, is the category with objects $Q_R \times Q_L$ and arrows $Q_R \times A^* \times Q_L$ so that the arrow (q_R, t, q_L) is written

$$(q_R,\ ) \xrightarrow{t} (\ , q_L)$$

and determines

$$(q_R, tq_L) \xrightarrow{t} (q_Rt, q_L).$$

The multiplication in the category is

$$(q_R, tq_L) \xrightarrow{t} (q_Rt, q_L = uq'_L) \xrightarrow{u} (q_Rtu, q'_L)$$

equals

$$(qr, tq_L = tuq'_L) \xrightarrow{tu} (q_Rtu, q'_L)$$

plus identity arrows. The generating arrows $Q_R \times A \times Q_L$ come equipped with an output function $(q_R, a, q_L) \to f(q_R, a, q_L)$. Later, we may identify some co-terminus (same domain and range) arrows.

Now this category can be looked at as a "generalized action" generalizing the right action $q_R \xrightarrow{t} q_Rt$ and the left action $uq_L \xleftarrow{u} q_L$: given arrow (q_R, a, q_L), consider

$$(q_R,\ ) \xrightarrow{a} (\ , q_L),$$

then fill in by the previous actions to

$$(q_R, aq_L) \xrightarrow{a} (q_Ra, q_L),$$

and similarly for $t \in A^+$ as follows: if $t = a_1, \ldots, a_n \in A^+$, then the arrow (q_R, t, q_L) decomposes as follows. (Take $n = 3$ for ease of exposition.) Starting with (q_R, t, q_L), we have

$$(q_R,\ ) \xrightarrow{t=a_1a_2a_3} (\ , q_L),$$

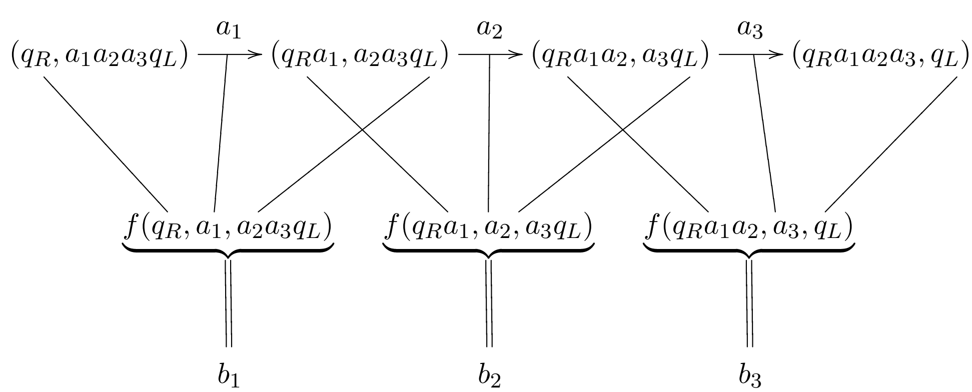
which decomposes as

$$(q_R,\ ) \xrightarrow{a_1} (q_Ra_1,\ ) \xrightarrow{a_2} (q_Ra_1a_2,\ ) \xrightarrow{a_3} (q_Ra_1a_2a_3,\ ), \text{ and}$$
$$(\ , a_1a_2a_3q_L) \xrightarrow{a_1} (\ , a_2a_3q_L) \xrightarrow{a_2} (\ , a_3q_L) \xrightarrow{a_3} (\ , q_L),$$

and combining yields the factorization in $\mathrm{Cat}(\mathcal{B})$ as

$$(q_R, a_1a_2a_3q_L) \xrightarrow{a_1} (q_Ra_1, a_2a_3q_L) \xrightarrow{a_2} (q_Ra_1a_2, a_3q_L) \xrightarrow{a_3} (q_Ra_1a_2a_3, q_L).$$

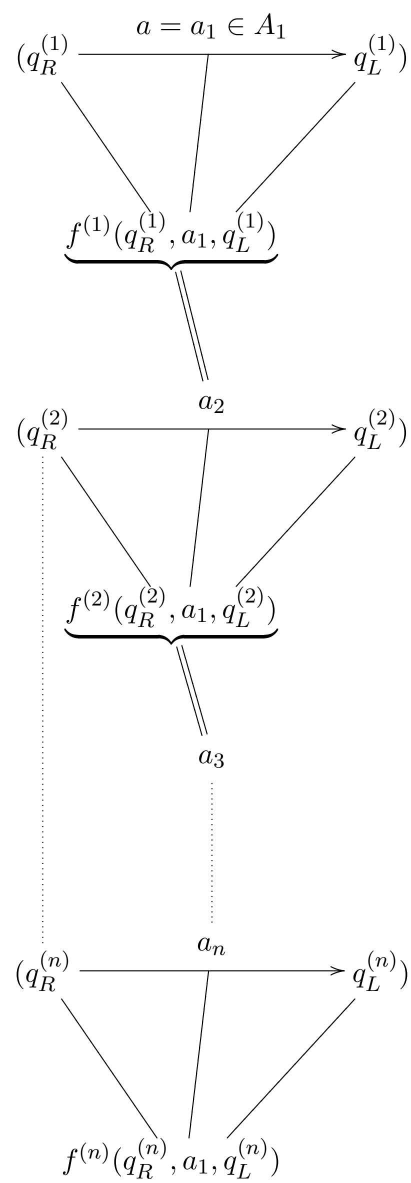
And then the output of $\mathcal{B}$ is given by



So $\mathrm{Cat}(\mathcal{B})$ equipped with the output function on the basic arrows $Q_R \times A \times Q_L$ determine $\mathcal{B}$ (and hence $\alpha_{\mathcal{B}}$) and conversely.

If we start with L and R automata (I, S^I, S, A) and (A, S, S^I, I) for some semigroup S with generators A, then the Cat of this is the 2-sided Cayley graph denoted $\mathrm{Kayley}(S)$ (notice the "K").

So looking at $\mathrm{Cat}(\mathcal{B}^{[n,1]})$, for generating arrows $a \in A_1$, we have



Now each $f^{(i)}$ can be done by one move (one Turing bit) of the Turing machine (see Section 8) if we assume $\mathcal{B}^{(i)} = \beta_0$ for all i, so in this Turing machine situation, it takes n computations to go from a_1 to a_{n+1}, so in the bimachine $\beta^{[n,1]}$ consider to be taking *all* of A_1^+ as inputs if we are computing this by

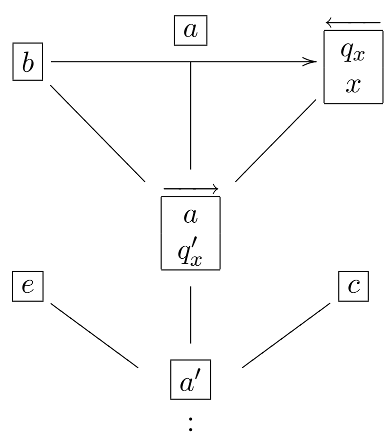
$$
\begin{array}{c}
\xrightarrow[\text{(linear time)}]{\mathcal{A}_R^{(n)}} a_i \xleftarrow[\text{(linear time)}]{\mathcal{A}_L^{(n)}} \\
\tilde{a}_1 \ldots\ldots \tilde{a}_i \ldots\ldots \tilde{a}_n \\
\beta^{[n,1]} \quad \downarrow \\
b_1 \ldots\ldots b_i \ldots\ldots b_n
\end{array}
$$

The coefficients of this linear time for $\mathcal{A}_R^{(n)}$ and $\mathcal{A}_L^{(n)}$ should be n by the above arguments, so if an input string $\tilde{a}_1 \ldots \tilde{a}_{i-1}$ is fed into $\mathcal{A}_R^{(n)}$ (the right automaton of $\beta^{[n,1]}$), then in time $(i-1) \cdot n$, the output $\tilde{b}_{i-1}$

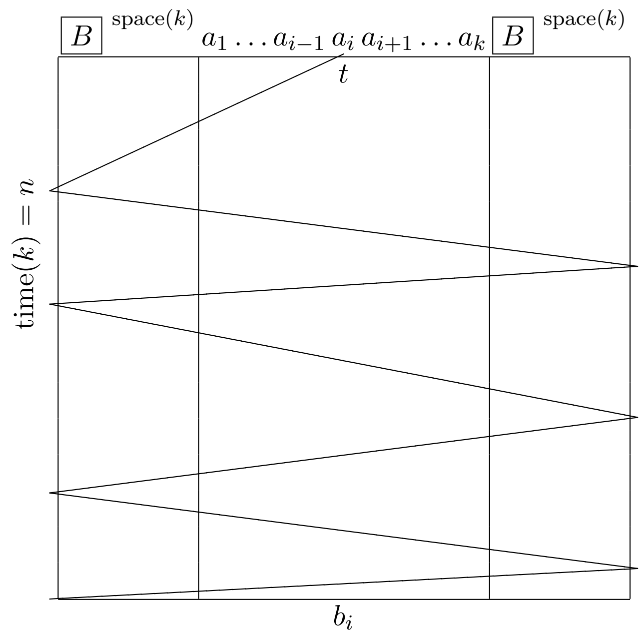
$$
\begin{array}{c}
\tilde{a}_1 \ldots\ldots\ldots \tilde{a}_{i-1} \\
\mathcal{A}_R^{(n)} \\
\tilde{b}_1 \ldots\ldots\ldots \tilde{b}_{i-1}
\end{array}
$$

can be computed.

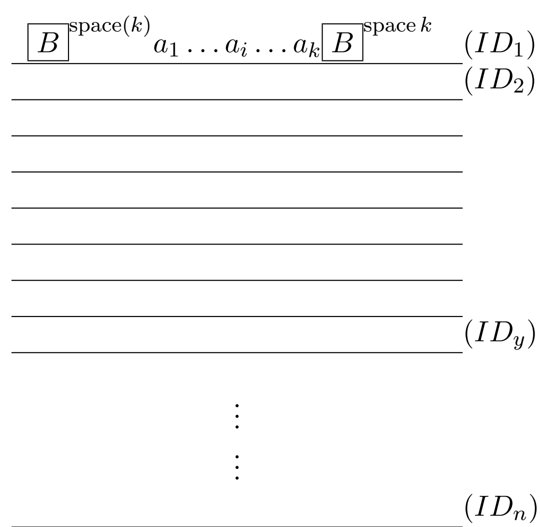
Let us look at this in more detail in the Turing machine context of $\mathcal{B}^{(i)} = \beta_0$ (see Section 8). So, for example, in the Turing machine



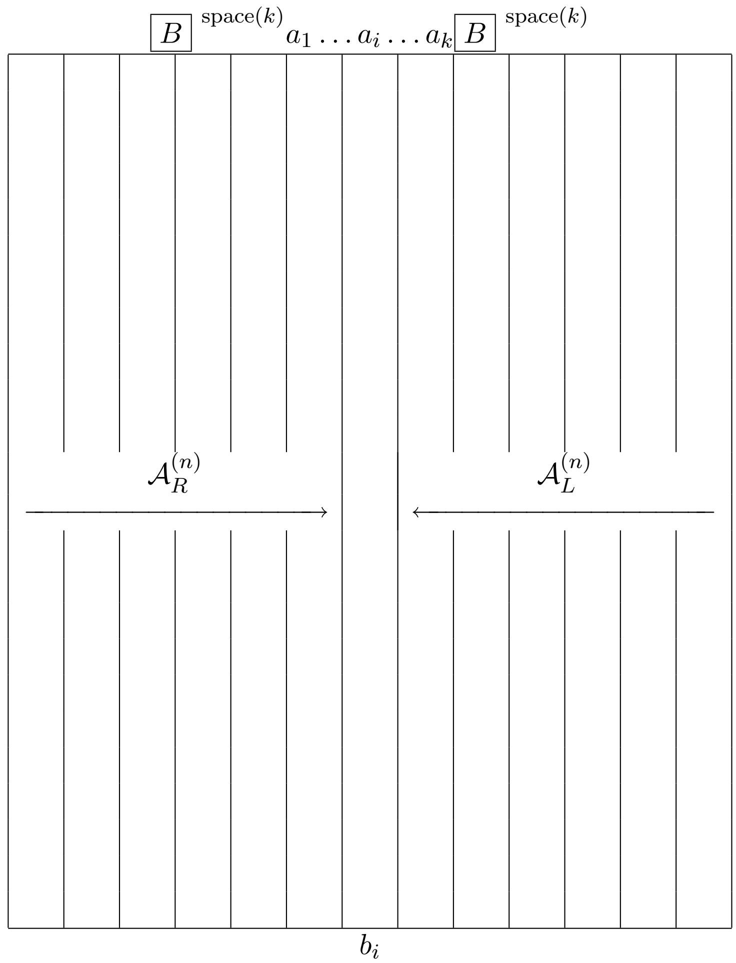
The general idea is: given a deterministic Turing machine T and input ID of length k and considering T_n (T running n times) and T_n considered as the bimachine $\mathcal{B}^{[n,1]}$ and if the time and space functions for T are time( ) and space( ), then consider:



(riding the reading head). Or better, following the IDs and not the reading head:

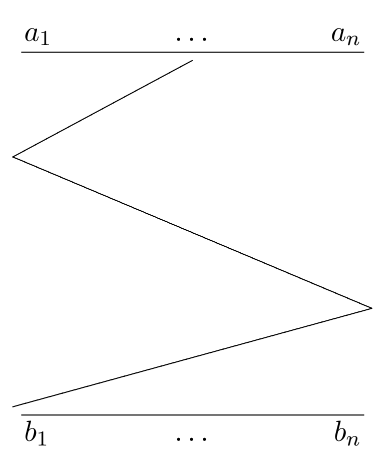


(Computation table, [10], p. 167.) Now take the adjoint (i. e., consider columns instead of rows):



This is the dual table, showing the bimachine action. Now Steve Cook's Theorem showing Circuit-Sat is NP-complete (and also that Circuit Value is P-complete) is read off from the computation table (see [10], 165-172), so the bimachines give a moving algebraic picture (with semigroups and the representation as elliptic maps, etc.) of the computational table.

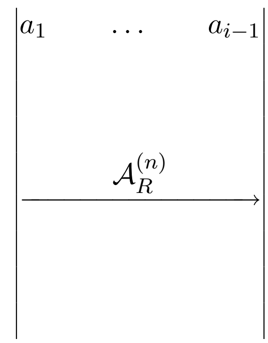
Note in all the tables that each entry represents one Turing move bit! But how can



be turned into

$$\xrightarrow[\text{(linear time)}]{\mathcal{A}_R^{(n)}} a_i \xleftarrow[\text{(linear time)}]{\mathcal{A}_L^{(n)}}?$$

How can such $\mathcal{A}_R^{(n)}$ and $\mathcal{A}_L^{(n)}$ exist?



must know the "future" (i. e., the other side L), hence

$$\left(\begin{array}{lcl} q_R^{(1)} & \xrightarrow{a_1 \dots a_{i-1}} & q_L^{(1)} \\ \vdots & & \vdots \\ q_R^{(n-1)} & & q_L^{(n-1)} \\ q_R^{(n)} & & \end{array} \right)$$

$\mathcal{A}_R^{(n)}$, for input $a_1 \dots a_n$, must "guess the future"

$$\left. \begin{array}{l} q_L^{(1)} \\ \vdots \\ q_L^{(n-1)} \end{array} \right)$$

the flow back to the left to

Papadimitriou calls this *quite subtle* ([10], p. 54). [17]

Note to the dual table, we can apply Proposition 2.4 and replace $\mathcal{B}^{[n,1]}$ by

$$\alpha_\beta(\boxed{B}^{\text{space}(k)}, a_1 \dots a_k, \boxed{B}^{\text{space}(k)}),$$

showing the power of generalized crossing sequences.

Whenever $x = (x_n, \dots, x_2, x_1)$ we shall write $\pi_j(x) = x_j$ for $j = 1, \dots, n$. Dually, for $y = (y_1, \dots, y_n)$ we shall write $y\pi_j = y_j$ for $j = 1, \dots, n$.

Clearly,

$$P_R^{[n,n-1]} = Q_R^{[n,n-1]}, \quad P_L^{[n,n-1]} = Q_L^{[n,n-1]}.$$

We define next a natural bijection $\theta_R^{[n,k]} : Q_R^{[n,k]} \to P_R^{[n,k]}$ by induction on k. We take $\theta_R^{[n,n-1]}$ to be the identity maping. Assume that $k \in \{1, \dots, n-2\}$ and $\theta_R^{[n,k+1]}$ is defined. Since the bimachines are arbitrary, $\theta_R^{[n,k]}$ is essentially the same as $\theta_R^{[n-k+1,1]}$, thus we shall assume that $k = 1$ for the sake of notation.

Let

$$(\gamma, \gamma_1) \in Q_R^{[n,2]^{Q_L^{(1)}}} \times Q_R^{(1)} = Q_R^{[n,1]}.$$

We proceed to define $\theta_R^{[n,1]}(\gamma, \gamma_1)$ in three steps.

Step 1: We use the bijection $\theta_R^{[n,2]}$ to define a bijection

$$Q_R^{[n,1]} = Q_R^{[n,2]^{Q_L^{(1)}}} \times Q_R^{(1)} \to P_R^{[n,2]^{Q_L^{(1)}}} \times Q_R^{(1)}.$$

More precisely, we consider $(\gamma, \gamma_1) \mapsto (\widehat{\gamma}, \gamma_1)$ where

$$\widehat{\gamma}(q_L^{(1)}) = \theta_R^{[n,2]}(\gamma(q_L^{(1)})).$$

Step 2: We dissociate $\widehat{\gamma}$ into its components according to the bijection

$$P_R^{[n,2]^{Q_L^{(1)}}} \to (Q_R^{(n)^{Q_L^{(2)} \times \dots \times Q_L^{(n-1)}}})^{Q_L^{(1)}} \times (Q_R^{(3)^{Q_L^{(2)}}})^{Q_L^{(1)}} \times (Q_R^{(2)})^{Q_L^{(1)}}.$$

We write $(\widehat{\gamma}, \gamma_1) \mapsto (\widehat{\gamma}_n, \dots, \widehat{\gamma}_2, \gamma_1)$.

Step 3: We use the natural bijections

$$(Q_R^{(j)^{Q_L^{(2)} \times \dots \times Q_L^{(j-1)}}})^{Q_L^{(1)}} \to Q_R^{(j)^{Q_L^{(1)} \times \dots \times Q_L^{(j-1)}}}$$

to define a mapping $(\widehat{\gamma}_n, \dots, \widehat{\gamma}_2, \gamma_1) \mapsto (\gamma_n, \dots, \gamma_2, \gamma_1)$, where

$$\gamma_j(q_L^{(1)}, \dots, q_L^{(j-1)}) = \widehat{\gamma}_j(q_L^{(1)})(q_L^{(2)}, \dots, q_L^{(j-1)}).$$

We make a liberal use of the mappings π_i in the following lemma, that provides an explicit description of the mappings γ_j from γ. Brackets have been omitted for the sake of simplicity, since there is only one possible bracketing interpretation in each case. For instance, we must have

$$\pi_1 \pi_2^2 \gamma(q_L^{(1)})(q_L^{(2)})(q_L^{(3)}) = \pi_1(\pi_2(\pi_2\gamma(q_L^{(1)}))(q_L^{(2)}))(q_L^{(3)}).$$

Lemma 6.1 *For $j = 2, \dots, n$, we have*

$$\gamma_j(q_L^{(1)}, \dots, q_L^{(j-1)}) = \begin{cases} \pi_1 \pi_2^{j-2} \gamma(q_L^{(1)}) \dots (q_L^{(j-1)}) & \text{if } j < n \\ \pi_2^{n-2} \gamma(q_L^{(1)}) \dots (q_L^{(n-1)}) & \text{if } j = n. \end{cases}$$

Proof. If $n = 2$, the lemma holds trivially since $\theta_R^{[2,1]}$ is the identity, hence we assume that $n > 2$.

By definition, we have $\gamma_j = \pi_j \theta_R^{[n,1]}(\gamma, \gamma_1)$. We must show by induction on n that

$$[\pi_j \theta_R^{[n,1]}(\gamma, \gamma_1)](q_L^{(1)}, \ldots, q_L^{(j-1)}) = \begin{cases} \pi_1 \pi_2^{j-2} \gamma(q_L^{(1)}) \ldots (q_L^{(j-1)}) & \text{if } j < n \\ \pi_2^{n-2} \gamma(q_L^{(1)}) \ldots (q_L^{(n-1)}) & \text{if } j = n \end{cases}$$

holds for $j = 2, \ldots, n$. We have

$$\begin{aligned} [\pi_j \theta_R^{[n,1]}(\gamma, \gamma_1)](q_L^{(1)}, \ldots, q_L^{(j-1)}) &= \gamma_j(q_L^{(1)}, \ldots, q_L^{(j-1)}) \\ &= \widehat{\gamma}_j(q_L^{(1)})(q_L^{(2)}, \ldots, q_L^{(j-1)}) \\ &= \pi_{j-1} \widehat{\gamma}(q_L^{(1)})(q_L^{(2)}, \ldots, q_L^{(j-1)}) \\ &= \pi_{j-1} \theta_R^{[n,2]}(\gamma(q_L^{(1)}))(q_L^{(2)}, \ldots, q_L^{(j-1)}) \\ &= \pi_{j-1} \theta_R^{[n,2]}(\pi_2 \gamma(q_L^{(1)}), \pi_1 \gamma(q_L^{(1)}))(q_L^{(2)}, \ldots, q_L^{(j-1)}) \end{aligned}$$

Ij $j = 2$, then we get

$$[\pi_2 \theta_R^{[n,1]}(\gamma, \gamma_1)](q_L^{(1)}) = \pi_1 \theta_R^{[n,2]}(\pi_2 \gamma(q_L^{(1)}), \pi_1 \gamma(q_L^{(1)})) = \pi_1 \gamma(q_L^{(1)})$$

as required since $j = 2 < n$.

Otherwise, the induction hypothesis yields

$$[\pi_j \theta_R^{[n,1]}(\gamma, \gamma_1)](q_L^{(1)}, \ldots, q_L^{(j-1)}) = \begin{cases} \pi_1 \pi_2^{j-3}(\pi_2 \gamma(q_L^{(1)}))(q_L^{(2)}) \ldots (q_L^{(j-1)}) & \text{if } j < n \\ \pi_2^{n-3}(\pi_2 \gamma(q_L^{(1)}))(q_L^{(2)}) \ldots (q_L^{(n-1)}) & \text{if } j = n \end{cases}$$

and the lemma follows. $\square$

The action of $S_R^{[n,1]}$ on $Q_R^{[n,1]}$ induces an action $P_R^{[n,1]} \times S_R^{[n,1]} \to P_R^{[n,1]}$ defined by

$$(\theta_R^{[n,1]}(q_R^{[n,1]}))s_R^{[n,1]} = \theta_R^{[n,1]}(q_R^{[n,1]} s_R^{[n,1]}).$$

The next lemma, although being of technical nature, unveils some of the properties of the action.

But first, here is some intuition and pictures for the following.

$$\begin{array}{c} (q_R^{(1)} \xrightarrow{\overrightarrow{a}_i} q_L^{(1)}) \\ \xrightarrow{\overrightarrow{a}_{i+1}} \end{array}$$

This denotes an input string $\overrightarrow{a}_i \in A_I^+$ and an output string $\overrightarrow{a}_{i+1} \in A_{i+1}^+$. If $\mathcal{B}^{(1)}$ is started in states $q_R^{(i)}$ and $q_L^{(i)}$ (see Proposition 2.4), then $\overrightarrow{a}_i$ is mapped to $\overrightarrow{a}_{i+1}$, i. e.,

$$\alpha_{\mathcal{B}}^{(i)}(u, \overrightarrow{a}_i, w) = \overrightarrow{a}_{i+1}$$

with $I_R^{(i)} u = q_R^{(i)}$ and $q_L^{(i)} = w I_L^{(i)}$. See Proposition 2.4.

Then, for some $\overrightarrow{a} \in A_1^+$,

$$\left(\begin{array}{lcl} q_R^{(1)} & \xrightarrow{\overrightarrow{a}=\overrightarrow{a}_1} & q_L^{(1)} \\ q_R^{(2)} & & q_L^{(2)} \\ \vdots & & \vdots \\ q_R^{(n-1)} & & q_L^{(n-1)} \\ q_R^{(n)} & & \end{array}\right) = \left(\begin{array}{c} q_R^{(1)} \cdot \overrightarrow{a}_1 \\ q_R^{(2)} \cdot \overrightarrow{a}_2 \\ \vdots \\ q_R^{(n-1)} \cdot \overrightarrow{a}_{n-1} \\ q_R^{n} \cdot \overrightarrow{a}_n \end{array}\right)$$

with $\overrightarrow{a}_1 = \overrightarrow{a}$ and

$$\begin{array}{c} (q_R^{(1)} \xrightarrow{\overrightarrow{a}_i} q_L^{(1)}) \\ \xrightarrow{\overrightarrow{a}_{i+1}} \end{array}$$

and $q_R^{(i)} \cdot \overrightarrow{a}_i$ denoting action in $(Q_R^{(i)}, S_R^{(i)}, A_i)$.

There is also the dual formulation

$$\begin{array}{c} \overleftarrow{a}_1 \cdot q_L^{(1)} \\ \vdots \\ \overleftarrow{a}_{n-1} \cdot q_L^{(n-1)} \\ \overleftarrow{a}_n \cdot q_L^{(n)} \end{array} = \left(\begin{array}{lcl} q_R^{(1)} & \xleftarrow{\overleftarrow{a}} & q_L^{(1)} \\ \vdots & & \vdots \\ q_R^{(n-1)} & & q_L^{(n-1)} \\ & & q_L^{(n)} \end{array}\right).$$

Now the two-sided semidirect multiplication is seen to be

$$\left(\begin{array}{lccl} q_R^{(1)} & \xrightarrow{\overrightarrow{a}_1} & \xrightarrow{\overrightarrow{b}_1} & q_L^{(1)} \\ \vdots & & & \vdots \\ \vdots & & & q_L^{(n-1)} \\ q_R^{(n)} & & & \end{array}\right) =$$

$$\left(\begin{array}{lcr} q_R^{(1)} & \xrightarrow{\overrightarrow{a}_1} & \overleftarrow{b}_1 \cdot q_L^{(1)} \\ \vdots & & \vdots \\ q_R^{(n-1)} & & \overleftarrow{b}_{n-1} \cdot q_L^{(n-1)} \\ q_R^{(n)} & & \end{array}\right) \cdot \left(\begin{array}{rcl} q_R^{(1)} \cdot \overrightarrow{a}_1 & \xrightarrow{b_1} & q_L^{(1)} \\ \vdots & & \vdots \\ q_R^{(n-1)} \cdot \overrightarrow{a}_{n-1} & & q_L^{(n-1)} \\ q_R^{(n)} \cdot \overrightarrow{a}_n & & \end{array}\right).$$

Another way to look at this is the following.

Proposition 6.2

(a) *Given $\overrightarrow{a} \in A_1^+$ and $q_L^{(1)}, \ldots, q_L^{(n-1)}$ (notice the $n-1$), this gives a member of the wreath product, see [5, vol. B], or [12].*

$$(Q_R^{(n)}, S_R^{(n)}) \circ \cdots \circ (Q_R^{(1)}, S_R^{(1)})$$

(notice the n), denoted

$$\left.\begin{matrix} \xrightarrow{\vec{a}} q_L^{(1)} \\ \vdots \\ q_L^{(n-1)} \end{matrix}\right).$$

(b)

$$\left.\begin{matrix} \xrightarrow{\vec{a}} q_L^{(1)} \\ \vdots \\ q_L^{(i)} \end{matrix}\right)$$

for $i \leq n-1$ is given by projecting

$$\left.\begin{matrix} \xrightarrow{\vec{a}} q_L^{(1)} \\ \vdots \\ q_L^{(n)} \end{matrix}\right)$$

from

$$(Q_R^{(n)}, S_R^{(n)}) \circ \cdots \circ (Q_R^{(1)}, S_R^{(1)})$$

to

$$(Q_R^{(i)}, S_R^{(i)}) \circ \cdots \circ (Q_R^{(1)}, S_R^{(1)}).$$

Proof. The proof is straighforward, but the statement is subtle. □

We note that, for all $q_R^{[n,j]} \in Q_R^{[n,j]}$ $(j < n)$ and $u \in A^+$, we have

$$\pi_1(q_R^{[n,j]} u) = \pi_1((\pi_2(q_R^{[n,j]}), \pi_1(q_R^{[n,j]}))u) = (\pi_1(q_R^{[n,j]}))u \tag{12}$$

since the action on the second component does not depend on the first.

Lemma 6.3 *Let $(\gamma_n, \ldots, \gamma_1) \in P_R^{[n,1]}$ and $u_1 \in A_1^+$. Then $(\gamma_n, \ldots, \gamma_1)u_1 = (\gamma_n', \ldots, \gamma_1')$ with*

$$\gamma_j'(q_L^{(1)}, \ldots, q_L^{(j-1)}) = (\gamma_j(u_1 q_L^{(1)}, \ldots, u_{j-1} q_L^{(j-1)}))u_j,$$

where the words $u_2, \ldots, u_n$ are defined recursively by

$$u_{j+1} = (\gamma_j(u_1 q_L^{(1)}, \ldots, u_{j-1} q_L^{(j-1)}))g_{u_j}^{(j)} q_L^{(j)} \quad (j = 1, \ldots, n-1).$$

Proof. Assume that $(\gamma_n, \ldots, \gamma_1) = \theta_R^{[n,1]}(\gamma, \gamma_1)$. Then

$$(\gamma, \gamma_1)u_1 = (\gamma u_1 \cdot \gamma_1 g_{u_1}^{(1)}, \gamma_1 u_1). \tag{13}$$

Since $\gamma_1' = \gamma_1 u_1$, the lemma holds for $j = 1$. Suppose next that $j \in \{2, \ldots, n-1\}$.

Lemma 6.1 and (13) yield

$$\begin{aligned} \gamma_j'(q_L^{(1)}, \ldots, q_L^{(j-1)}) &= \pi_1 \pi_2^{j-2}(\gamma u_1 \cdot \gamma_1 g_{u_1}^{(1)})(q_L^{(1)}) \ldots (q_L^{(j-1)}) \\ &= \pi_1 \pi_2^{j-2}[(\gamma(u_1 q_L^{(1)}))u_2](q_L^{(2)}) \ldots (q_L^{(j-1)}). \end{aligned}$$

We show that

$$\gamma_j'(q_L^{(1)},\ldots,q_L^{(j-1)}) = \pi_1\pi_2^{j-i}[(\pi_2^{i-2}\gamma(u_1q_L^{(1)})\ldots(u_{i-1}q_L^{(i-1)}))u_i](q_L^{(i)})\ldots(q_L^{(j-1)}). \tag{14}$$

for $i = 2,\ldots,j$ by induction on i.

This was already proved for $i = 2$. Assume that it holds for $i \in \{2,\ldots,j-1\}$. Then by Lemma 6.1

$$\begin{aligned}
\gamma_j'(q_L^{(1)},\ldots,q_L^{(j-1)}) &= \pi_1\pi_2^{j-i}[(\pi_2^{i-2}\gamma(u_1q_L^{(1)})\ldots(u_{i-1}q_L^{(i-1)}))u_i](q_L^{(i)})\ldots(q_L^{(j-1)})\\
&= \pi_1\pi_2^{j-i}[(\pi_2^{i-1}\gamma(u_1q_L^{(1)})\ldots(u_{i-1}q_L^{(i-1)}),\pi_1\pi_2^{i-2}\gamma(u_1q_L^{(1)})\ldots(u_{i-1}q_L^{(i-1)}))u_i]\\
&\qquad (q_L^{(i)})\ldots(q_L^{(j-1)})\\
&= \pi_1\pi_2^{j-i}[(\pi_2^{i-1}\gamma(u_1q_L^{(1)})\ldots(u_{i-1}q_L^{(i-1)}),\gamma_i(u_1q_L^{(1)},\ldots,u_{i-1}q_L^{(i-1)}))u_i]\\
&\qquad (q_L^{(i)})\ldots(q_L^{(j-1)})\\
&= \pi_1\pi_2^{j-i-1}[(\pi_2^{i-1}\gamma(u_1q_L^{(1)})\ldots(u_{i-1}q_L^{(i-1)}))u_i\cdot(\gamma_i(u_1q_L^{(1)},\ldots,u_{i-1}q_L^{(i-1)}))g_{u_i}^{(i)}]\\
&\qquad (q_L^{(i)})\ldots(q_L^{(j-1)})\\
&= \pi_1\pi_2^{j-(i+1)}[\pi_2^{i-1}\gamma(u_1q_L^{(1)})\ldots(u_iq_L^{(i)})\cdot(\gamma_i(u_1q_L^{(1)},\ldots,u_{i-1}q_L^{(i-1)}))g_{u_i}^{(i)}q_L^{(i)}]\\
&\qquad (q_L^{(i+1)})\ldots(q_L^{(j-1)})\\
&= \pi_1\pi_2^{j-(i+1)}[(\pi_2^{i-1}\gamma(u_1q_L^{(1)})\ldots(u_iq_L^{(i)}))u_{i+1}](q_L^{(i+1)})\ldots(q_L^{(j-1)}),
\end{aligned}$$

and so (14) holds. In particular, for $i = j$, we obtain

$$\gamma_j'(q_L^{(1)},\ldots,q_L^{(j-1)}) = \pi_1[(\pi_2^{j-2}\gamma(u_1q_L^{(1)})\ldots(u_{j-1}q_L^{(j-1)}))u_j]$$

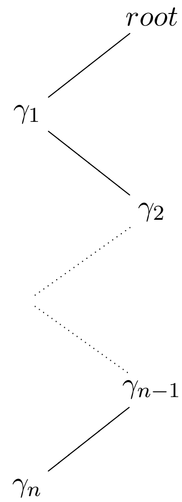
and so

$$\begin{aligned}
\gamma_j'(q_L^{(1)},\ldots,q_L^{(j-1)}) &= (\pi_1\pi_2^{j-2}\gamma(u_1q_L^{(1)})\ldots(u_{j-1}q_L^{(j-1)}))u_j\\
&= (\gamma_j(u_1q_L^{(1)},\ldots,u_{j-1}q_L^{(j-1)}))u_j
\end{aligned}$$

by (12) and Lemma 6.1.

The case $j = n$ is actually a simplification of the preceding case and can safely be omitted. □

Since $P_R^{[n,1]}$ is a direct product of n factors, we can view it as a tree of depth n having uniform degree *for each depth*. Typically, the state $(\gamma_n,\ldots,\gamma_1) \in P_R^{[n,1]}$ is represented in this tree as a path



and can be identified with the corresponding leaf. Naturally, each node of depth $j \in \{0, \ldots n-1\}$ has precisely $|Q_R^{(j)Q_L^{(1)}\times\ldots\times Q_L^{(j-1)}}|$ sons.

Following the terminology of [12], we say that an *elliptic contraction* Ψ of $P_R^{[n,1]}$ is a depth-preserving endomorphism of the associated tree. More precisely, we view Ψ of a mapping that sends vertices to vertices of same depth (fixing the root in particular) and edges to edges, preserving adjacency.

Alternatively, if $\Psi(\gamma_n, \ldots, \gamma_1) = (\gamma'_n, \ldots, \gamma'_1)$ and $\Psi(\beta_n, \ldots, \beta_1) = (\beta'_n, \ldots, \beta'_1)$, then

$$(\gamma_1 = \beta_1, \ldots, \gamma_j = \beta_j) \Rightarrow (\gamma'_1 = \beta'_1, \ldots, \gamma'_j = \beta'_j)$$

holds for $j = 1, \ldots, n$. This amounts to say that $\pi_j \Psi(\gamma_n, \ldots, \gamma_1)$ depends on $(\gamma_j, \ldots, \gamma_1)$ only.

Theorem 6.4 *For every $u \in A_1^+$, the right action of u on $P_R^{[n,1]}$ induces an elliptic contraction ν_u of $P_R^{[n,1]}$.*

Proof. By Lemma 6.3, it is clear that whenever $(\gamma_n, \ldots, \gamma_1)u = (\gamma'_n, \ldots, \gamma'_1)$ then γ'_j depends on $\gamma_j, \ldots, \gamma_1$ and u only. $\square$

We can also refer to this property by saying that the right action on $P_R^{[n,1]}$ is *sequential*.

An immediate consequence of Theorem 6.4 is the following result, which will play an important role in going into profinite limits. Note that for $m \leq n$ there exists a natural onto mapping $\pi_{[m,1]} : P_R^{[n,1]} \to P_R^{[m,1]}$ defined by

$$\pi_{[m,1]}(p_R^{[n,1]}) = (\pi_m(p_R^{[n,1]}), \ldots, \pi_1(p_R^{[n,1]})).$$

Corollary 6.5 *For all $p_R^{[n,1]} \in P_R^{[n,1]}$ and $u \in A_1^+$,*

$$\pi_{[m,1]}(p_R^{[n,1]}u) = (\pi_{[m,1]}(p_R^{[n,1]}))u.$$

We consider next then expression of the initial state in the $P_R^{[n,1]}$ description.

Proposition 6.6 *$\theta_R^{[n,1]}(I_R^{[n,1]}) = (\gamma_n, \ldots, \gamma_2, I_R^{(1)})$ with $\gamma_j(q_L^{(1)}, \ldots, q_L^{(j-1)}) = I_R^{(j)}$ for $j = 2, \ldots, n$.*

Proof. We use induction on n. The case $n = 2$ is trivial since $\theta_R^{[2,1]}$ is the identity mapping. Assume that $n > 2$ and the proposition holds for $n - 1$. We have $I_R^{[n,1]} = (\gamma, I_R^{(1)})$ with $\gamma(q_L^{(1)}) = I_R^{[n,2]}$ for every $q_L^{(1)} \in Q_L^{(1)}$. By the induction hypothesis, $(\gamma, I_R^{(1)})$ is taken by $\theta_R^{[n,1]}$ in the first step to $(\widehat{\gamma}, I_R^{(1)})$, where each $\widehat{\gamma}(q_L^{(1)})$ is an $(n-1)$-uple of constant mappings defined by

$$\widehat{\gamma}_j(q_L^{(1)})(q_L^{(2)}, \ldots, q_L^{(j-1)}) = I_R^{(j)}, \quad (j = 2, \ldots, n-1).$$

Thus $\gamma_j(q_L^{(1)}, \ldots, q_L^{(j-1)}) = I_R^{(j)}$ and the lemma holds. $\Box$

Naturally, all the results presented in this section for $P_R^{[n,1]}$ have dual versions for $P_L^{[n,1]}$ which will wisely be omitted.

We end this section by computing the output function in terms of the states $P_R^{[n,1]}$ and $P_L^{[n,1]}$. To avoid introducing extra notation, we keep the notation $f^{[n,1]}$ for the function

$$P_R^{[n,1]} \times A_1 \times P_L^{[n,1]} \to A_{n+1}$$

$$(\theta_R^{[n,1]}(q_R^{[n,1]}), a, q_L^{[n,1]}\theta_L^{[n,1]}) \mapsto f^{[n,1]}(q_R^{[n,1]}, a, q_L^{[n,1]})$$

.

Proposition 6.7 *Let $(\gamma_n, \ldots, \gamma_1) \in P_R^{[n,1]}$, $(\delta_1, \ldots, \delta_n) \in P_L^{[n,1]}$ and $a_1 \in A_1$. Let $q_R^{(1)} = \gamma_1$, $q_L^{(1)} = \delta_1$ and define $q_R^{(j)} \in Q_R^{(j)}$, $q_L^{(j)} \in Q_L^{(j)}$ and $a_j \in A_j$ $(j = 2, \ldots n)$ recursively by*

$$q_R^{(j)} = \gamma_j(a_1 q_L^{(1)}, \ldots, a_{j-1} q_L^{(j-1)}), \quad q_L^{(j)} = (q_R^{(j-1)} a_{j-1}, \ldots, q_R^{[1]} a_1)\delta_j,$$

$$a_j = f^{(j-1)}(q_R^{(j-1)}, a_{j-1}, q_L^{(j-1)}).$$

Then

$$f^{[n,1]}((\gamma_n, \ldots, \gamma_1), a_1, (\delta_1, \ldots, \delta_n)) = f^{(n)}(q_R^{(n)}, a_n, q_L^{(n)}).$$

Proof. We show that

$$\begin{aligned} &f^{[n,1]}((\gamma_n, \ldots, \gamma_1), a_1, (\delta_1, \ldots, \delta_n)) \\ &\quad = f^{[n,j]}((\pi_2^{j-1}\gamma(a_1 q_L^{(1)}) \ldots (a_{j-1} q_L^{(j-1)}), q_R^{(j)}), a_j, (q_L^{(j)}, (q_R^{(j-1)} a_{j-1}) \ldots (q_R^{(1)} a_1)\delta\pi_2^{j-1})) \end{aligned}$$

holds for $j = 1, \ldots, n$.

Since

$$f^{[n,1]}((\gamma_n, \ldots, \gamma_1), a_1, (\delta_1, \ldots, \delta_n)) = f^{[n,1]}((\gamma, q_R^{[1]}), a_1, (q_L^{(1)}, \delta)),$$

the claim holds for $j = 1$. Assume that it holds for $j < n-1$. Then

$$f^{[n,1]}((\gamma_n, \dots, \gamma_1), a_1, (\delta_1, \dots, \delta_n))$$

$$= f^{[n,j]}((\pi_2^{j-1}\gamma(a_1q_L^{(1)})\dots(a_{j-1}q_L^{(j-1)}), q_R^{(j)}), a_j, (q_L^{(j)}, (q_R^{(j-1)}a_{j-1})\dots(q_R^{(1)}a_1)\delta\pi_2^{j-1}))$$

$$= f^{[n,j+1]}(\pi_2^{j-1}\gamma(a_1q_L^{(1)})\dots(a_jq_L^{(j)}), f^{[j]}(q_R^{(j)}, a_j, q_L^{(j)}), (q_R^{(j)}a_j)\dots(q_R^{(1)}a_1)\delta\pi_2^{j-1})$$

$$= f^{[n,j+1]}((\pi_2^{j}\gamma(a_1q_L^{(1)})\dots(a_jq_L^{(j)}), \pi_1\pi_2^{j-1}\gamma(a_1q_L^{(1)})\dots(a_jq_L^{(j)})), a_{j+1},$$
$$((q_R^{(j)}a_j)\dots(q_R^{(1)}a_1)\delta\pi_2^{j-1}\pi_1, (q_R^{(j)}a_j)\dots(q_R^{(1)}a_1)\delta\pi_2^{j}))$$

$$= f^{[n,j+1]}((\pi_2^{j}\gamma(a_1q_L^{(1)})\dots(a_jq_L^{(j)}), q_R^{(j+1)}), a_{j+1}, (q_L^{(j+1)}, (q_R^{(j)}a_j)\dots(q_R^{(1)}a_1)\delta\pi_2^{j}))$$

since

$$\pi_1\pi_2^{j-1}\gamma(a_1q_L^{(1)})\dots(a_jq_L^{(j)}) = \gamma_{j+1}(a_1q_L^{(1)}, \dots, a_jq_L^{(j)}) = q_R^{(j+1)},$$
$$(q_R^{(j)}a_j)\dots(q_R^{(1)}a_1)\delta\pi_2^{j-1}\pi_1 = (q_R^{(j)}a_j, \dots, q_R^{(1)}a_1)\delta_{j+1} = q_L^{(j+1)}$$

by Lemma 6.1 and its dual. It follows that the claim holds for $j+1$ and therefore fot $n-1$. Thus

$$f^{[n,1]}((\gamma_n, \dots, \gamma_1), a_1, (\delta_1, \dots, \delta_n))$$

$$= f^{(n,n-1)}((\pi_2^{n-2}\gamma(a_1q_L^{(1)})\dots(a_{n-2}q_L^{(n-2)}), q_R^{(n-1)}), a_{n-1},$$
$$(q_L^{(n-1)}, (q_R^{(n-2)}a_{n-2})\dots(q_R^{(1)}a_1)\delta\pi_2^{n-2})$$

$$= f^{(n)}(\pi_2^{n-2}\gamma(a_1q_L^{(1)})\dots(a_{n-1}q_L^{(n-1)}), f^{(n-1)}(q_R^{(n-1)}, a_{n-1}, q_L^{(n-1)}),$$
$$(q_R^{(n-1)}a_{n-1})\dots(q_R^{(1)}a_1)\delta\pi_2^{n-2}))$$

$$= f^{(n)}(\gamma_n(a_1q_L^{(1)}, \dots, a_{n-1}q_L^{(n-1)}), a_n, (q_R^{(n-1)}a_{n-1}, \dots, q_R^{(1)}a_1)\delta_n)$$

$$= f^{(n)}(q_R^{(n)}, a_n, q_L^{(n)})$$

as required. $\square$

7 The matrix representation

We develop in this section a matrix representation for the (iterated) block product of finite bimachines. Let $\mathcal{B}^{(1)} = ((I_R^{(1)}, Q_R^{(1)}, S_R^{(1)}), f^{(1)}, (S_L^{(1)}, Q_L^{(1)}, I_L^{(1)}))$, be an A_1, A_2-bimachine. We assume that the state sets $Q_R^{(1)}$ and $Q_L^{(1)}$ are totally ordered. Let $u \in A_1^+$. We define a $Q_R^{(1)} \times Q_R^{(1)}$ boolean matrix $M_{R,u}^{(1)}$ by

$$(M_{R,u}^{(1)})_{p_R^{(1)}, q_R^{(1)}} = \begin{cases} 1 & \text{if } q_R^{(1)} = p_R^{(1)}u \\ 0 & \text{otherwise.} \end{cases}$$

Dually, we define a $Q_L^{(1)} \times Q_L^{(1)}$ boolean matrix $M_{L,u}^{(1)}$ by

$$(M_{L,u}^{(1)})_{p_L^{(1)},q_L^{(1)}} = \begin{cases} 1 & \text{if } p_L^{(1)} = uq_L^{(1)} \\ 0 & \text{otherwise.} \end{cases}$$

We write

$$M_R^{(1)} = \{M_{R,u}^{(1)} \mid u \in A^+\}, \quad M_L^{(1)} = \{M_{L,u}^{(1)} \mid u \in A^+\}.$$

We shall present the R-versions of our results, omitting the dual L-versions.

Lemma 7.1 *For all $u, v \in A_1^+$,*

$$M_{R,u}^{(1)} M_{R,v}^{(1)} = M_{R,uv}^{(1)}.$$

Moreover, $M_R^{(1)}$ is an A_1-semigroup and a quotient of $S_R^{(1)}$.

Proof. Let $p_R^{(1)}, q_R^{(1)} \in Q_R^{(1)}$. We have

$$(M_{R,u}^{(1)} M_{R,v}^{(1)})_{p_R^{(1)},q_R^{(1)}} = \sum_{t_R^{(1)} \in Q_R^{(1)}} (M_{R,u}^{(1)})_{p_R^{(1)},t_R^{(1)}} (M_{R,v}^{(1)})_{t_R^{(1)},q_R^{(1)}}.$$

We have $(M_{R,u}^{(1)})_{p_R^{(1)},t_R^{(1)}} (M_{R,v}^{(1)})_{t_R^{(1)},q_R^{(1)}} = 1$ if and only if $t_R^{(1)} = p_R^{(1)}u$ and $q_R^{(1)} = t_R^{(1)}v$, hence $(M_{R,u}^{(1)} M_{R,v}^{(1)})_{p_R^{(1)},q_R^{(1)}} \neq 0$ if and only if there exists some $t_R^{(1)} \in Q_R^{(1)}$ such that $t_R^{(1)} = p_R^{(1)}u$ and $q_R^{(1)} = t_R^{(1)}v$, that is, if and only if $q_R^{(1)} = p_R^{(1)}uv$. Since $t_R^{(1)}$ is then necessarily unique, we conclude that

$$(M_{R,u}^{(1)} M_{R,v}^{(1)})_{p_R^{(1)},q_R^{(1)}} = (M_{R,uv}^{(1)})_{p_R^{(1)},q_R^{(1)}}.$$

It follows that $M_R^{(1)}$ is an A_1-semigroup. Given $u, v \in A_1^+$, $u = v$ in $S_R^{(1)}$ implies that their action on $Q_R^{(1)}$ is the same and so $M_{R,u}^{(1)} = M_{R,v}^{(1)}$. Thus $M_R^{(1)}$ is a quotient of $S_R^{(1)}$. □

In the faithful case, these matrix semigroups turn out to be a representation of the bimachine semigroups:

Lemma 7.2 *If $\mathcal{B}^{(1)}$ is faithful, then $M_R^{(1)} \cong S_R^{(1)}$.*

Proof. By Lemma 7.1, it suffices to note that $M_{R,u}^{(1)} = M_{R,v}^{(1)}$ implies $u_{S_R^{(1)}} = v_{S_R^{(1)}}$ for all $u, v \in A_1^+$. Clearly, if $M_{R,u}^{(1)} = M_{R,v}^{(1)}$, then u and v have the same action on $Q_R^{(1)}$ and the claim follows from faithfullness. □

We consider now the states (the R-version). We associate to every $q_R^{(1)} \in Q_R^{(1)}$ the $\{1\} \times Q_R^{(1)}$ boolean row matrix $W_{R,q_R^{(1)}}^{(1)}$ defined by

$$(W_{R,q_R^{(1)}}^{(1)})_{1,p_R^{(1)}} = \begin{cases} 1 & \text{if } p_R^{(1)} = q_R^{(1)} \\ 0 & \text{otherwise.} \end{cases}$$

Together with Lemma 7.2, the following result shows that our matrices provide a matrix representation for the faithful case.

Proposition 7.3 *For all $q_R^{(1)} \in Q_R^{(1)}$ and $u \in A_1^+$, we have*

$$W^{(1)}_{R,q_R^{(1)}} M^{(1)}_{R,u} = W^{(1)}_{R,q_R^{(1)}u}.$$

Proof. Let $p_R^{(1)} \in Q_R^{(1)}$. We have $(W^{(1)}_{R,q_R^{(1)}} M^{(1)}_{R,u})_{1,p_R^{(1)}} = 1$ if and only if

$$\sum_{t_R^{(1)} \in Q_R^{(1)}} (W^{(1)}_{R,q_R^{(1)}})_{1,t_R^{(1)}} (M^{(1)}_{R,u})_{t_R^{(1)},p_R^{(1)}} = 1.$$

Since $(W^{(1)}_{R,q_R^{(1)}})_{1,t_R^{(1)}} = 1$ if and only if $t_R^{(1)} = q_R^{(1)}$, it follows that

$$\begin{aligned}(W^{(1)}_{R,q_R^{(1)}} M^{(1)}_{R,u})_{1,p_R^{(1)}} = 1 &\Leftrightarrow (M^{(1)}_{R,u})_{q_R^{(1)},p_R^{(1)}} = 1 \\ &\Leftrightarrow p_R^{(1)} = q_R^{(1)}u \\ &\Leftrightarrow (W^{(1)}_{R,q_R^{(1)}u})_{1,p_R^{(1)}} = 1.\end{aligned}$$

Thus $W^{(1)}_{R,q_R^{(1)}} M^{(1)}_{R,u} = W^{(1)}_{R,q_R^{(1)}u}$. $\Box$

Assume now that $\mathcal{B}^{(2)} = ((I_R^{(2)}, Q_R^{(2)}, S_R^{(2)}), f^{(2)}, (S_L^{(2)}, Q_L^{(2)}, I_L^{(2)}))$ is an A_2, A_3-bimachine. For every $u \in A_1^+$, we define a $Q_R^{(1)} \times Q_L^{(1)}$ matrix $M^{(1)}_{g_u}$ by

$$(M^{(1)}_{g_u})_{q_R^{(1)},q_L^{(1)}} = q_R^{(1)} g_u^{(1)} q_L^{(1)}$$

and a $(|Q_R^{(1)}| + |Q_L^{(1)}|) \times (|Q_R^{(1)}| + |Q_L^{(1)}|)$ matrix

$$\overline{M}^{(21)}_{R,u} = \begin{pmatrix} M^{(1)}_{L,u} & 0 \\ M^{(1)}_{g_u} & M^{(1)}_{R,u} \end{pmatrix}.$$

If we consider the natural matrix multiplication for the matrices $\overline{M}^{(21)}_{R,u}$ (i.e. 0 and 1 act on A_2^* by $0u = u0 = 1$, $1u = u1 = u$ and we concatenate words as usual), then we can prove:

Proposition 7.4 *For all $u, v \in A_1^+$,*

$$\overline{M}^{(21)}_{R,u} \overline{M}^{(21)}_{R,v} = \overline{M}^{(21)}_{R,uv}.$$

Proof. We must show that

$$\begin{pmatrix} M^{(1)}_{L,u} & 0 \\ M^{(1)}_{g_u} & M^{(1)}_{R,u} \end{pmatrix} \begin{pmatrix} M^{(1)}_{L,v} & 0 \\ M^{(1)}_{g_v} & M^{(1)}_{R,v} \end{pmatrix} = \begin{pmatrix} M^{(1)}_{L,uv} & 0 \\ M^{(1)}_{g_{uv}} & M^{(1)}_{R,uv} \end{pmatrix},$$

that is,

$$\begin{pmatrix} M^{(1)}_{L,u}M^{(1)}_{L,v} & 0 \\ \\ M^{(1)}_{g_u}M^{(1)}_{L,v}\cdot M^{(1)}_{R,u}M^{(1)}_{g_v} & M^{(1)}_{R,u}M^{(1)}_{R,v} \end{pmatrix} = \begin{pmatrix} M^{(1)}_{L,uv} & 0 \\ \\ M^{(1)}_{g_{uv}} & M^{(1)}_{R,uv} \end{pmatrix}.$$

Clearly, Lemma 7.1 and its dual yield $M^{(1)}_{L,u}M^{(1)}_{L,v} = M^{(1)}_{L,uv}$ and $M^{(1)}_{R,u}M^{(1)}_{R,v} = M^{(1)}_{R,uv}$. It remains to prove that

$$M^{(1)}_{g_u}M^{(1)}_{L,v}\cdot M^{(1)}_{R,u}M^{(1)}_{g_v} = M^{(1)}_{g_{uv}}. \tag{15}$$

For all $q^{(1)}_R \in Q^{(1)}_R$ and $q^{(1)}_L \in Q^{(1)}_L$, we have

$$\begin{aligned}(M^{(1)}_{g_u}M^{(1)}_{L,v}\cdot M^{(1)}_{R,u}M^{(1)}_{g_v})_{q^{(1)}_R,q^{(1)}_L} &= (M^{(1)}_{g_u}M^{(1)}_{L,v})_{q^{(1)}_R,q^{(1)}_L}\cdot(M^{(1)}_{R,u}M^{(1)}_{g_v})_{q^{(1)}_R,q^{(1)}_L} \\ &= \textstyle\prod_{p^{(1)}_L\in Q^{(1)}_L}(M^{(1)}_{g_u})_{q^{(1)}_R,p^{(1)}_L}(M^{(1)}_{L,v})_{p^{(1)}_L,q^{(1)}_L} \\ &\quad \cdot\textstyle\prod_{p^{(1)}_R\in Q^{(1)}_R}(M^{(1)}_{R,u})_{q^{(1)}_R,p^{(1)}_R}\cdot(M^{(1)}_{g_v})_{p^{(1)}_R,q^{(1)}_L}.\end{aligned}$$

Since $(M^{(1)}_{L,v})_{p^{(1)}_L,q^{(1)}_L} = 1$ if and only if $p^{(1)}_L = vq^{(1)}_L$ and $(M^{(1)}_{R,u})_{q^{(1)}_R,p^{(1)}_R} = 1$ if and only if $p^{(1)}_R = q^{(1)}_R u$, it follows that

$$\begin{aligned}(M^{(1)}_{g_u}M^{(1)}_{L,v}\cdot M^{(1)}_{R,u}M^{(1)}_{g_v})_{q^{(1)}_R,q^{(1)}_L} &= (M^{(1)}_{g_u})_{q^{(1)}_R,vq^{(1)}_L}\cdot(M^{(1)}_{g_v})_{q^{(1)}_R u,q^{(1)}_L} \\ &= q^{(1)}_R g_u(vq^{(1)}_L)\cdot(q^{(1)}_R u)g_v q^{(1)}_L \\ &= q^{(1)}_R g_{uv} q^{(1)}_L \\ &= (M^{(1)}_{g_{uv}})_{q^{(1)}_R,q^{(1)}_L}\end{aligned}$$

since

$$\begin{pmatrix} uv & 0 \\ g^{(1)}_{uv} & uv \end{pmatrix} = \begin{pmatrix} u & 0 \\ g^{(1)}_u & u \end{pmatrix}\begin{pmatrix} v & 0 \\ g^{(1)}_v & v \end{pmatrix} = \begin{pmatrix} uv & 0 \\ g^{(1)}_u v\cdot ug^{(1)}_v & uv \end{pmatrix}.$$

Thus (15) holds as required. □

Next we define, for every $q^{(21)}_R = (\gamma, q^{(1)}_R) \in Q^{(21)}_R$, a $\{1\}\times(|Q^{(1)}_L| + |Q^{(1)}_R|)$ boolean row matrix

$$\overline{W}^{(21)}_{R,q^{(21)}_R} = \begin{pmatrix} W_\gamma & W^{(1)}_{R,q^{(1)}_R} \end{pmatrix},$$

where

$$(W_\gamma)_{1,q^{(1)}_L} = \gamma(q^{(1)}_L) \in Q^{(2)}_R.$$

If we consider the natural matrix multiplication for the matrices $\overline{W}^{(21)}_{R,q^{(21)}_R}$ and $\overline{M}^{(21)}_{R,u}$ (i.e. words of A^+_2 act on $Q^{(2)}_R$ as expected), then we can prove:

Proposition 7.5 *For all $q_R^{(21)} \in Q_R^{(21)}$ and $u \in A_1^+$,*

$$\overline{W}^{(21)}_{R,q_R^{(21)}} \overline{M}^{(21)}_{R,u} = \overline{W}^{(21)}_{R,q_R^{(21)}u}.$$

Proof. Let $q_L^{(1)} \in Q_L^{(1)}$. We have

$$(\overline{W}^{(21)}_{R,q_R^{(21)}} \overline{M}^{(21)}_{R,u})_{1,q_L^{(1)}} = (W_\gamma M^{(1)}_{L,u} \cdot W^{(1)}_{R,q_R^{(1)}} M^{(1)}_{g_u})_{1,q_L^{(1)}}.$$

Since $(M^{(21)}_{L,u})_{p_L^{(1)},q_L^{(1)}} = 1$ if and only if $p_L^{(1)} = uq_L^{(1)}$, and $(W^{(1)}_{R,q_R^{(1)}})_{1,p_R^{(1)}} = 1$ if and only if $p_R^{(1)} = q_R^{(1)}$, it follows that

$$\begin{aligned}
(\overline{W}^{(21)}_{R,q_R^{(21)}} \overline{M}^{(21)}_{R,u})_{1,q_L^{(1)}} &= (W_\gamma)_{1,uq_L^{(1)}} \cdot (M^{(1)}_{g_u})_{q_R^{(1)},q_L^{(1)}} \\
&= \gamma(uq_L^{(1)}) \cdot q_R^{(1)} g_u^{(1)} q_L^{(1)} \\
&= (\gamma u \cdot q_R^{(1)} g_u^{(1)})(q_L^{(1)}) \\
&= (\overline{W}^{(21)}_{R,q_R^{(21)}u})_{1,q_L^{(1)}}.
\end{aligned}$$

Now let $q_R^{(1)} \in Q_R^{(1)}$. It follows from Proposition 7.3 that

$$\begin{aligned}
(\overline{W}^{(21)}_{R,q_R^{(21)}} \overline{M}^{(21)}_{R,u})_{1,q_R^{(1)}} &= (W^{(1)}_{R,q_R^{(1)}} M^{(1)}_{R,u})_{1,q_R^{(1)}} \\
&= (W^{(1)}_{R,q_R^{(1)}u})_{1,q_R^{(1)}} = (\overline{W}^{(21)}_{R,q_R^{(21)}u})_{1,q_R^{(1)}},
\end{aligned}$$

hence $\overline{W}^{(21)}_{R,q_R^{(21)}} \overline{M}^{(21)}_{R,u} = \overline{W}^{(21)}_{R,q_R^{(21)}u}$ and the lemma holds. $\square$

We can expand our matrices to boolean matrices as follows. Let $u \in A_1^+$. We define a $(|Q_R^{(1)}| + |Q_L^{(1)}|)(|Q_R^{(2)}| + |Q_L^{(2)}|) \times (|Q_R^{(1)}| + |Q_L^{(1)}|)(|Q_R^{(2)}| + |Q_L^{(2)}|)$ boolean matrix $M^{(21)}_{R,u}$ replacing in $\overline{M}^{(21)}_{R,u}$

- each word $w \in A_2^+$ by $M^{(2)}_{R,w}$;
- each 1 by the $Q_R^{(2)} \times Q_R^{(2)}$ identity matrix;
- each 0 by the $Q_R^{(2)} \times Q_R^{(2)}$ zero matrix.

Given $q_R^{(21)} \in Q_R^{(21)}$, we define a $\{1\} \times (|Q_R^{(1)}| + |Q_L^{(1)}|)|Q_R^{(2)}|$ boolean matrix $W^{(21)}_{R,q_R^{(21)}}$ replacing in $\overline{W}^{(21)}_{R,q_R^{(21)}}$

- each word $q_R^{(2)} \in Q_R^{(2)}$ by $W^{(2)}_{R,q_R^{(2)}}$;
- each 1 by the $\{1\} \times Q_R^{(2)}$ matrix with all entries 1;
- each 0 by the $\{1\} \times Q_R^{(2)}$ zero matrix.

It would be nice to have versions of Propositions 7.4 and 7.5 for these boolean matrices, but unfortunately the matrix operation cannot be plain multiplication of boolean matrices. Indeed, multiplication of matrices must be operated at two levels, and full exploration of this operation remains to be completed.

8 Turing machines and bimachines

We are interested in deterministic Turing machines that halt for all inputs, particularly those that can solve NP-complete problems. In comparison with the most standard model of deterministic Turing machine, the model we shall be considering in this paper presents three particular features:

- the "tape" is potentially infinite in *both* directions and has a distinguished cell named *the origin*;
- the origin contains the symbol # until the very last move of the computation, and # appears in no other cell;
- the machine always halts in one of a very restricted set of configurations.

There are of course many ways of achieving these goals, we shall just choose a particular one.

Our deterministic Turing machine is then a quadruple of the form $\mathcal{T} = (Q, q_0, A, \delta)$ where

- Q is a finite set (set of states) containing the initial state q_0;
- A is a finite set (restricted tape alphabet) containing the special symbols B (blank), B' (pseudoblank), Y (yes), N (no), G (garbage) and # (origin);
- δ is a union of full maps

$$Q \times (A \setminus \{\#\}) \to Q \times (A \setminus \{\#, B, Y, N, G\}) \times \{L, R\},$$

$$Q \times \{\#\} \to (Q \times \{\#\} \times \{L, R\}) \cup \{Y, N, G\}.$$

We write $A^o = A \setminus \{\#, B\}$.

Since the machine is not allowed to write blanks on the tape, we shall use the pseudoblank as a substitute to avoid unnecessary information in the final configurations. Since we must consider space functions, it is not convenient to allow the blanks to perform that job.

Note that, in the final move of a computation, the control head is removed from the tape and so we allow $\{Y, N, G\}$ in the image of δ. The symbols Y, N, G are used to classify the final configurations: for a TM solving a certain problem, Y will stand for *correct input, acceptance*, N for *correct input, rejection*, and G for *incorrect input*.

We intend to work exclusively with words, hence we shall soon exchange the classical model of "tape" and "control head" by a purely algebraic formalism. We introduce what we shall call henceforth the extended tape alphabet:

$$A' = A \cup \{a^q \mid a \in A, q \in Q\}.$$

The exponent q on a symbol acnowledges the present scanning of the corresponding cell by the control head, under state q.

We are now naturally led to the concept of *instantaneous description* for $\mathcal{T}$. Informally, instantaneous descriptions are meant to encode all (theoretically) possible configurations of the tape during any sequence of computations. Formally, let for : $A'^+ \to A^+$ be the "forgetting" homomorphism defined by

$$\text{for}(a) = a, \quad \text{for}(a^q) = a \quad (a \in A, q \in Q),$$

and let exp : $A'^+ \to (\mathbb{N}, +)$ be the "counting" homomorphism defined by

$$\exp(a) = 0, \quad \exp(a^q) = 1 \quad (a \in A, q \in Q).$$

Then we define

$$ID = B^*\{w \in A'^+ \mid \text{for}(w) \in (\{1\} \cup B)(A^o)^*(\{1, \#\})(A^o)^*(\{1\} \cup B),\ \exp(w)\ \leq 1\}B^*.$$

As an example, the instantaneous description $BBab\#ab^qaBBB$ indicates that $ab\#aba$ is the content of the tape, the third cell is the origin, the control head is scanning the fifth cell under state q. The presence of some blanks on the left or/and on the right can be useful in some circumstances, in others can be ignored. We should always keep in mind that the tape is potentially an infinite word $\ldots BBBBabc\#abaBBBB\ldots$ Note that we may have $\exp(w) = 0$ or 1 due to our peculiar stopping conditions. The interdiction of blanks between non-blanks follows of course from the impossibility of writing blanks.

We denote by $\overline{ID}$ the set of all nonempty factors of words in ID.

The Turing machine $\mathcal{T}$ induces a mapping $\beta : \overline{ID} \to \overline{ID}$ (the *one-move mapping*) as follows:

Let $w \in \overline{ID}$. If $|\exp(w)| = 0$, let $\beta(w) = w$. Suppose now that $w = ua^qv$ with $a \in A$ and $q \in Q$.

- if $\delta(q, a) = b \in \{Y, N, G\}$, let $\beta(w) = ubv$;
- if $\delta(q, a) = (p, b, R)$ and c is the first letter of $v = cv'$, let $\beta(w) = ubc^pv'$;
- if $\delta(q, a) = (p, b, R)$ and $v = 1$, let $\beta(w) = ubB^p$;
- if $\delta(q, a) = (p, b, L)$ and c is the last letter of $u = u'c$, let $\beta(w) = u'c^pbv$;
- if $\delta(q, a) = (p, b, R)$ and $u = 1$, let $\beta(w) = B^pbv$.

Given $w \in ID$, it should be clear that the sequence $(\beta^n(w))_n$ is eventually constant if and only if $\mathcal{T}$ stops after finitely many moves if and only if $\beta^m(w) \in A^+$ for some $m \in \mathbb{N}$. In this case, we write

$$\lim_{n\to\infty} \beta^n(w) = \beta^m(w).$$

More generally, given any eventually constant sequence $(u_n)_n$, we shall use $\lim_{n\to\infty} u_n$ with the obvious meaning.

We say that our deterministic Turing machine (TM) is *normalized* if

- $(\beta^n(w))_n$ is eventually constant for every $w \in ID$;
- $\lim_{n\to\infty} \beta^n(w) \in B^*B'^*\{Y, N, G\}B'^*B^*$ for every $w \in ID$.

In view of our stopping conventions, this implies in particular that the symbol Y, N or G must be precisely at the origin. Normalized TMs will be used as models for solving a certain problem, and we can now be more precise with respect to the possible final configurations: $\lim_{n\to\infty} \beta^n(w) \in B^*B'^*YB'^*B^*$ will correspond to *correct input, acceptance*, $\lim_{n\to\infty} \beta^n(w) \in B^*B'^*NB'^*B^*$ to *correct input, rejection*, and $\lim_{n\to\infty} \beta^n(w) \in B^*B'^*GB'^*B^*$ to *incorrect input*. It may be convenient to assume that the identification of incorrect input (garbage) can be made at low cost complexity (say polynomially).

It should be clear that any algorithm of yes/no type to solve a particular problem can be performed by a normalized TM of our type: we can keep the origin symbol constant at the cost of introducing extra states, we can always add new states so that the machine does not stop immediately following acceptance/rejection and add a terminal subroutine that will change the acceptance/rejection configuration into one of the desired form $B^*B'^*\{Y, N, G\}B'^*B^*$.

The *space* and *time* functions for the normalized TM $\mathcal{T}$ can be naturally defined by

$$\begin{aligned} s_{\mathcal{T}} : ID &\to \mathbb{N} \\ w &\mapsto |\lim_{n\to\infty} \beta^n(w)|, \end{aligned}$$

$$\begin{aligned} t_{\mathcal{T}} : ID &\to \mathbb{N} \\ w &\mapsto \min\{m \in \mathbb{N} : \beta^m(w) = \lim_{n\to\infty} \beta^n(w)\}. \end{aligned}$$

Indeed, we are assuming that our TM halts after finitely many moves, and the length of the limit gives precisely the number of cells that have been used in the computation (if we include all the cells occupied by w). On the other hand, since each iteration of β corresponds to one move of $\mathcal{T}$, the time function computes the number of moves needed to get to a terminal configuration. It follows from known results (see [2]) that any deterministic (multi-tape) Turing machine solving a problem with space and time complexities of order $s(n)$ and $t(n)$ (not less than linear) can be turned into a normalized TM with space and time functions of order $s(n)$ and $(t(n))^2$, respectively. In particular, if $s(n)$ and $t(n)$ are polynomial, we remain within the realm of polynomial complexity.

We note that, for every $w \in ID$, $\beta(w)$ either has the same length or is one letter longer than w (when $\beta(w)$ is of the form $w'B^p$ or B^pw'). The *one-move lp-mapping* $\beta_0 : ID \to ID$

is defined by

$$\beta_0(w) = \begin{cases} \beta(w) & \text{if } |\beta(w)| = |w| \\ w' & \text{if } |\beta(w)| = |w|+1 \text{ and } \beta(w) = w'B^p; \\ w' & \text{if } |\beta(w)| = |w|+1 \text{ and } \beta(w) = B^p w'. \end{cases}$$

Alternatively, we can say that $\beta_0(w)$ is obtained from $\beta(BwB)$ by removing the first and the last letter. Similarly, we can consider the extension $\beta_0 : \overline{ID} \to \overline{ID}$ which is also an lp-mapping.

We remark that, if $|\beta(w)| = |w| + 1$, then $\beta_0(w) \in A^+$ and so we cannot deduce $\beta(w)$ from $\beta_0(w)$. This loss of information is only apparent: it is a fact for a particular input, but not if we consider the *full domain of instantaneous descriptions*: indeed, we can deduce $\beta(w)$ from $\beta_0(BwB)$ and, more generally, $\beta^n(w)$ from $\beta_0(B^n wB^n)$.

Let $\iota_B : ID \to (A' \setminus \{B\})^+$ be the mapping that removes all blanks from a given $w \in ID$.

Lemma 8.1 *Let $\mathcal{T}$ be a normalized TM with one-move mapping β.Let $w \in \overline{ID}$ be such that for$(w) \in (A \setminus \{B\})^+$. Then*

(i) $\lim_{n\to\infty} \beta^n(w) = \lim_{n\to\infty} \iota_B(\beta_0^n(B^n wB^n))$;

(ii) $s_{\mathcal{T}}(w) = |\lim_{n\to\infty} \iota_B(\beta_0^n(B^n wB^n))|$;

(iii) $t_{\mathcal{T}}(w) = min\{m \in \mathbb{N} : \iota_B(\beta_0^m(B^m wB^m)) = \lim_{n\to\infty} \iota_B(\beta_0^n(B^n wB^n))\}$.

Proof. It is immediate that $\beta^n(B^n wB^n) = \beta_0^n(B^n wB^n)$ for every $n \in \mathbb{N}$, and so

$$\iota_B(\beta_0^n(B^n wB^n)) = \iota_B(\beta^n(B^n wB^n)) = \beta^n(w).$$

Thus the result follows from $\mathcal{T}$ being normalized and the definitions of space and time functions. $\square$

We prefer to extend $\beta_0 : \overline{ID} \to \overline{ID}$ to an lp-mapping $\beta_0 : A'^+ \to \overline{ID}$ for formal reasons. Since we are not really interested in non-IDs, we may consider some arbitrary lp-mapping $\Delta : A'^+ \to ID$ fixing every $w \in \overline{ID}$ and then take the composition $\beta_0\Delta$. We can take for instance

$$\Delta(w) = \begin{cases} w & \text{if } w \in \overline{ID} \\ GB'^{|w|-1} & \text{otherwise.} \end{cases}$$

So far, we have associated to the normalized TM $\mathcal{T}$ an lp-mapping β_0 encoding the full computational power of $\mathcal{T}$ with space and time functions equivalent to those of $\mathcal{T}$. We proceed now to define a canonical finite bimachine matching β_0 in $\overline{ID}$.

The A', A'-bimachine

$$\mathcal{B}_{\mathcal{T}} = ((I_R, Q_R, S_R), f, (S_L, Q_L, I_L))$$

is defined as follows:

- $Q_R = A' \cup \{I_R\}$, $Q_L = A' \cup \{I_L\}$;

- $S_R = A'$ is a right zero semigroup ($ab = b$);
- $S_L = A'$ is a left zero semigroup ($ab = a$);
- the action $Q_R \times S_R \to Q_R$ is defined by $q_R a = a$;
- the action $S_L \times Q_L \to Q_L$ is defined by $aq_L = a$

For the output function, let us write $I'_R = B$ and $q'_R = q_R$ for every $q_R \in Q_R \setminus \{I_R\}$. Similarly, we define q'_L. Given $q_R \in Q_R$, $a \in A'$ and $q_L \in Q_L$, let

$$f(q_R, a, q_L) = \beta_0(q'_R, a, q'_L).$$

If $q_R a q_L \in \overline{ID}$, then $q_R a q_L$ will encode the situation of three consecutive tape cells at a certain moment. Then $f(q_R, a, q_L)$ describes the situation of the middle cell after one move of $\mathcal{T}$. If $q_R a q_L \notin \overline{ID}$, then $f(q_R, a, q_L)$ will have some pretty arbitrary meaning, depending on the choice of Δ previously taken.

Proposition 8.2 *Let $\mathcal{T}$ be a normalized TM with one-move lp-mapping β_0. Then $\alpha_{\mathcal{B}_\mathcal{T}}(w) = \beta_0(w)$ for every $w \in \overline{ID}$.*

Proof. Write $\alpha = \alpha_{\mathcal{B}_\mathcal{T}}$. Let $w \in \overline{ID}$ and write $w = uav$ with $a \in A'$. We must show that $\alpha(u, a, v) = \beta_0(u, a, v)$. Now

$$\alpha(u, a, v) = f(I_R u, a, vI_L) = f(q_R, a, q_L)$$

where

$$q_R = \begin{cases} I_R & \text{if } u = 1 \\ \text{last letter of } u & \text{otherwise,} \end{cases}$$

$$q_L = \begin{cases} I_L & \text{if } v = 1 \\ \text{first letter of } v & \text{otherwise.} \end{cases}$$

By definition, we have

$$f(q_R, a, q_L) = \beta_0(q'_R, a, q'_L).$$

On the other hand, we certainly have

$$\beta_0(u, a, v) = \beta_0(q_R, a, q_L) = \beta_0(q'_R, a, q'_L)$$

if $u, v \neq 1$. If $u = 1$ and $v \neq 1$, then

$$f(q_R, a, q_L) = \beta_0(B, a, q_L) = \beta_0(u, a, v)$$

since both B and u are irrelevant to the computation. The other cases being of course similar, the result follows. $\square$

We consider next some sort of converse statement for our assignment of a finite bimachine to a normalized TM. We assume that A is a typical TM (restricted) tape alphabet, containing in particular the blank B.

Let $\mathcal{B}$ be a finite A, A-bimachine and write $\alpha = \alpha_\mathcal{B}$. Assume that

(1) $\alpha(u, a, v) \neq B$ if $a \neq B$;

(2) $(\alpha^n(w))_n$ is eventually constant for every $w \in A^+$;

(3) there exists a (polynomial) space function $s_{\mathcal{B}} : A^+ \to \mathbb{N}$ defined by

$$s_{\mathcal{B}}(w) = |\lim_{n\to\infty} \iota_B(\alpha^n(B^n w B^n))|;$$

(4) there exists a (polynomial) time function $s_{\mathcal{B}} : A^+ \to \mathbb{N}$ defined by

$$t_{\mathcal{B}}(w) = \min\{m \in \mathbb{N} : \iota_B(\alpha^m(B^m w B^m)) = \lim_{n\to\infty} \iota_B(\alpha^n(B^n w B^n))\},$$

where the limits are taken for eventually constant sequences. Then there exists some normalized TM $\mathcal{T}$ with (polynomial) $s_{\mathcal{T}}(w) = s_{\mathcal{B}}(w)$ and $t_{\mathcal{T}}(w) = \mathcal{O}((s_{\mathcal{B}}(w)t_{\mathcal{B}}(w))^2)$ that computes $\lim_{n\to\infty} \iota_B(\alpha^n(B^n w B^n))$.

In fact, let $w \in A^+$. Each time we perform an iteration of α on $B^m w B^m$ (for the smallest m we need to obtain the space and time limits), we perform at most $s_{\mathcal{B}}(w)$ changes of symbols. Therefore the limit can be reached within a maximum of $s_{\mathcal{B}}(w)t_{\mathcal{B}}(w)$ elementary operations, that can be assumed to have constant cost since they can be computed by the finite bimachine. In view of Church's thesis and [2], this yields a deterministic Turing machine with the claimed time bound (it is obvious for space), and the subroutines to make it normalized can be afforded at the same level of complexity.

9 A profinite differential equation

We assume from now on that $\mathcal{B}^{(1)} = \mathcal{B}^{(2)} = \mathcal{B}^{(3)} = \ldots$ are countably many copies of the A', A'-bimachine $\mathcal{B}$ defined in the preceding section for the one-move lp-mapping of a normalized TM.

Let $m, n \geq 1$ with $m < n$. We can extend the canonical surjective homomorphism

$$\xi_R^{[n,m]} : (I_R^{[n,m]}, Q_R^{[n,m]}, S_R^{[n,m]}) \to (I_R^{(m)}, Q_R^{(m)}, S_R^{(m)})$$

given by Proposition 3.5 to a morphism

$$\overline{\xi_R}^{[n,m]} : (I_R^{[n,1]}, Q_R^{[n,1]}, S_R^{[n,1]}) \to (I_R^{[m,1]}, Q_R^{[m,1]}, S_R^{[m,1]})$$

by successive application of Proposition 3.4. Similarly, we define a morphism

$$\overline{\xi_L}^{[n,m]} : (S_L^{[n,1]}, Q_L^{[n,1]}, I_L^{[n,1]}) \to (S_L^{[m,1]}, Q_L^{[m,1]}, I_L^{[m,1]}).$$

Let $\overline{\xi}_R^{[n,n]}$ and $\overline{\xi}_L^{[n,n]}$ be the obvious identity mappings.

It is straightforward that if we choose to represent the states in the $P_R^{[n,1]}$, $P_L^{[n,1]}$ versions, then

$$\overline{\xi_R}^{[n,m]}(\gamma_n, \ldots, \gamma_1) = (\gamma_m, \ldots, \gamma_1), \quad (\delta_1, \ldots, \delta_n)\overline{\xi_L}^{[n,m]} = (\delta_1, \ldots, \delta_m). \tag{16}$$

In fact, these are the mappings considered in Section 6 before Corollary 6.5.

We recall the definition of projective system and projective limit. A set $\{P_n \mid n \geq 1\}$ of algebras and morphisms $\{\pi_{ij} : P_i \to P_j \mid i \geq j\}$ is said to be a *projective system* if

- π_{nn} is the identity mapping for every $n \in \mathbb{N}$;
- $\pi_{ij}\pi_{jk} = \pi_{ik}$ whenever $i \geq j \geq k$.

Its *projective limit* is defined as

$$P = \{(a_n)_n \in \prod_{n=1}^{\infty} P_n \mid a_i\pi_{ij} = a_j \text{ whenever } i \geq j\}.$$

Lemma 9.1 $\{(I_R^{[n,1]}, Q_R^{[n,1]}, S_R^{[n,1]}) \mid n \geq 1\}$ *and the morphisms* $\overline{\xi_R}^{[n,m]}$ $(n \geq m)$ *constitute a projective system of right* A', A'*-automata.*

Proof. We must show that $\overline{\xi_R}^{[m,k]}\overline{\xi_R}^{[n,m]} = \overline{\xi_R}^{[n,k]}$ whenever $n \geq m \geq k$. This follows immediately from (16). $\square$

We denote by

$$(I_R^\omega, Q_R^\omega, S_R^\omega)$$

the projective limit of the projective system defined above. If we represent the states in the $P_R^{[n,1]}$, $P_L^{[n,1]}$ versions, it is routine to see that

$$\ldots \times {Q_R^{(n)}}^{Q_L^{(1)}\times\ldots\times Q_L^{(n-1)}} {Q_R^{(n)}}^{Q_L^{(1)}\times\ldots\times Q_L^{(n-1)}} \times {Q_R^{(n-1)}}^{Q_L^{(1)}\times\ldots\times Q_L^{(n-2)}} \times \ldots \times Q_R^{(1)}$$

provides a representation of Q_R^ω. Moreover, the initial state I_R^ω coresponds to

$$(\ldots, \overline{I_R^{(3)}}, \overline{I_R^{(2)}}, I_R^{(1)}),$$

where $\overline{I_R^{(n)}}$ is the constant mapping with image $I_R^{(n)}$.

In view of Theorem 6.4 and Corollary 6.5, it should be clear that the action of A'^+ on P_R^ω is fully determined by the action on $P_R^{[n,1]}$ in the obvious way.

We have dual L-versions of these definitions and results that lead to a projective limit

$$(S_L^\omega, Q_L^\omega, I_L^\omega)$$

and a representation

$$Q_L^\omega = Q_L^{(1)} \times \ldots \times {}^{Q_R^{(n-2)}\times\ldots\times Q_R^{(1)}}Q_L^{(n-1)} \times {}^{Q_R^{(n-1)}\times\ldots\times Q_R^{(1)}}Q_L^{(n)} \times \ldots$$

We define now an A', A'-bimachine

$$\mathcal{B}^\omega = ((I_R^\omega, Q_R^\omega, S_R^\omega), f^\omega, (S_L^\omega, Q_L^\omega, I_L^\omega))$$

as follows. Given $u, v \in A'^+$ and $a \in A'$, we define

$$f^\omega(I_R^\omega u, a, vI_L^\omega) = \lim_{n\to\infty} f^{[n,1]}(I_R^{[n,1]}B^n u, a, vB^n I_L^{[n,1]}).$$

If either q_R^ω or q_L^ω is not accessible, $f^\omega(q_R^\omega, a, q_L^\omega)$ is arbitrary (say for simplicity $f^\omega(q_R^\omega, a, q_L^\omega) = a$).

We show that $f^\omega(I_R^\omega u, a, vI_L^\omega)$ is well defined. Indeed

$$f^{[n,1]}(I_R^{[n,1]}B^n u, a, vB^n I_L^{[n,1]}) = \alpha_{\mathcal{B}^{[n,1]}}(B^n u, a, vB^n) = \beta_0^n(B^n u, a, vB^n).$$

If $uav \in \overline{ID}$, we have that

$$\lim_{n\to\infty} \beta^n(uav) = \lim_{n\to\infty} \iota_B(\beta_0^n(B^n uavB^n))$$

by Lemma 8.1 and so $(\beta_0^n(B^n u, a, vB^n))_n$ and therefore $(f^{[n,1]}(I_R^{[n,1]}B^n u, a, vB^n I_L^{[n,1]}))_n$ is eventually constant. If $uav \notin \overline{ID}$, then

$$\beta_0^n(B^n uavB^n) = B^n G B'^{|uav|-1} B^n$$

and $(f^{[n,1]}(I_R^{[n,1]}B^n u, a, vB^n I_L^{[n,1]}))_n$ is also eventually constant. Thus f^ω is well defined.

We show now that the bimachine $\mathcal{B}^\omega$ satisfies the following property, referred to as the *differential equation.*

Theorem 9.2 *$\mathcal{B}^\omega \cong \mathcal{B}^\omega \Box \mathcal{B}$.*

Proof. Write $\mathcal{B}^{(\omega,1)} = B^\omega \Box \mathcal{B}$. Since

$$Q_R^\omega = \ldots \times {Q_R}^{(Q_L)^{n-1}} \times {Q_R}^{(Q_L)^{n-2}} \times \ldots \times Q_R,$$

we define

$$\zeta_R : Q_R^\omega \to Q_R^{(\omega,1)} = {Q_R^\omega}^{Q_L} \times Q_R$$

by

$$\zeta_R(\ldots, \gamma_2, \gamma_1) = (\widehat{\gamma}, \gamma_1),$$

where

$$\widehat{\gamma} = (\ldots, \widehat{\gamma}_2, \widehat{\gamma}_1)$$

and $\widehat{\gamma}_n(q_L^{(1)}) \in {Q_R}^{(Q_L)^{n-1}}$ is defined for $n \geq 1$ by

$$\widehat{\gamma}_n(q_L^{(1)})(q_L^{(2)}, \ldots, q_L^{(n)}) = \gamma_{n+1}(q_L^{(1)}, \ldots, q_L^{(n)}).$$

Given $(\widehat{\gamma}, \gamma_1) \in Q_R^{(\omega,1)}$ with $\widehat{\gamma} = (\ldots, \widehat{\gamma}_2, \widehat{\gamma}_1)$, define $(\ldots, \gamma_2, \gamma_1) \in Q_R^\omega$ by

$$\gamma_{n+1}(q_L^{(1)}, \ldots, q_L^{(n)}) = \widehat{\gamma}_n(q_L^{(1)})(q_L^{(2)}, \ldots, q_L^{(n)}).$$

It is immediate that $(\widehat{\gamma}, \gamma_1) = \zeta_R(\ldots, \gamma_2, \gamma_1)$, hence ζ_R is surjective. It is simple routine to check that ζ_R is injective and preserves the initial state.

We show next that ζ_R preserves the action. Let $u \in A_1^+$. We may write

$$(\ldots, \gamma_2, \gamma_1)u_1 = (\ldots, \gamma_2', \gamma_1')$$

with the γ_n' defined as in Lemma 6.3. By Theorem 6.4, the action of A'^+ on $Q_R^{[n,1]}$ is sequential and so must be the action of A'^+ on Q_R^ω. Thus it suffices to remark that the mapping

$$\begin{array}{c} \zeta_R^{(n)} : P_R^{[n,1]} \to {P_R^{[n,2]}}^{Q_L} \times Q_R \\ (\gamma_n, \ldots, \gamma_1) \mapsto ((\widehat{\gamma}_{n-1}, \ldots, \widehat{\gamma}_1), \gamma_1) \end{array}$$

preserves the action. This is essentially the identity mapping on $Q_R^{[n,1]}$ with different representations of the states. Since the action is the same in

- $Q_R^{[n,2]}$ and $P_R^{[n,2]}$,
- $Q_R^{[n,1]} = {Q_R^{[n,2]}}^{Q_L} \times Q_R$ and $P_R^{[n,1]}$,

it follows that ζ_R preserves the action.

We show next that

$$S_R^{(\omega,1)} \cong S_R^{\omega}. \tag{17}$$

Let $u, v \in {A'}^+$. We have

$$\begin{aligned}
u_{S_R^\omega} = v_{S_R^\omega} &\Leftrightarrow \forall n \geq 1 \; u_{S_R^{[n,1]}} = v_{S_R^{[n,1]}} \\
&\Leftrightarrow u_{S_R} = v_{S_R} \wedge \forall n \geq 2 \; \forall q_R \in Q_R \; \forall q_L \in Q_L \; (q_R g_u q_L)_{S_R^{[n,2]}} = (q_R g_v q_L)_{S_R^{[n,2]}} \\
&\Leftrightarrow u_{S_R} = v_{S_R} \wedge \forall n \geq 1 \; \forall q_R \in Q_R \; \forall q_L \in Q_L \; (q_R g_u q_L)_{S_R^{[n,1]}} = (q_R g_v q_L)_{S_R^{[n,1]}} \\
&\Leftrightarrow u_{S_R} = v_{S_R} \wedge \forall q_R \in Q_R \; \forall q_L \in Q_L \; (q_R g_u q_L)_{S_R^\omega} = (q_R g_v q_L)_{S_R^\omega} \\
&\Leftrightarrow u_{S_R^{(\omega,1)}} = v_{S_R^{(\omega,1)}},
\end{aligned}$$

thus (17) holds and therefore ζ_R is an isomorphism of right A'-automata.

Similarly, the mapping

$$\zeta_L : Q_L^\omega \to Q_L^{(\omega,1)} = Q_L \times {}^{Q_R}Q_L^\omega$$

defined by

$$(\delta_1, \delta_2, \ldots)\zeta_L = (\delta_1, \widehat{\delta}),$$

where

$$\widehat{\delta} = (\widehat{\delta}_1, \widehat{\delta}_2, \ldots)$$

and $q_R^{(1)}\widehat{\delta}_n \in {}^{(Q_R)^{n-1}}Q_L$ is defined for $n \geq 1$ by

$$(q_R^{(n)}, \ldots, q_R^{(2)})(q_R^{(1)}\widehat{\delta}_n) = (q_R^{(n)}, \ldots, q_R^{(1)})\delta_{n+1},$$

is an isomorphism of left A'-automata.

Finally, we must show that

$$f^{(\omega,1)}(I_R^{(\omega,1)}u, a, vI_L^{(\omega,1)}) = f^\omega(I_R^\omega u, a, vI_L^\omega)$$

holds for all $u, v \in A'^+$. Indeed,

$$f^{(\omega,1)}(I_R^{(\omega,1)}u, a, vI_L^{(\omega,1)})$$

$$= f^{(\omega,1)}((\gamma_0, I_R)u, a, v(I_L, \delta_0))$$

$$= f^{(\omega,1)}((\gamma_0 u \cdot I_R g_u, I_R u), a, (vI_L, h_v I_L \cdot v\delta_0))$$

$$= f^{\omega}(I_R^{\omega} \cdot I_R g_u(vI_L), f(I_R u, a, vI_L), (I_R u)h_v I_L \cdot I_L^{\omega})$$

$$= \lim_{n\to\infty} f^{[n,1]}(I_R^{[n,1]} \cdot I_R g_u(vI_L), f(I_R u, a, vI_L), (I_R u)h_v I_L \cdot I_L^{[n,1]})$$

$$= \lim_{n\to\infty} f^{[n+1,2]}(I_R^{[n+1,2]} \cdot I_R g_u(vI_L), f(I_R u, a, vI_L), (I_R u)h_v I_L \cdot I_L^{[n+1,2]})$$

$$= \lim_{n\to\infty} f^{[n+1,1]}((\gamma_0 u \cdot I_R g_u, I_R u), a, (vI_L, h_v I_L \cdot v\delta_0))$$

$$= \lim_{n\to\infty} f^{[n+1,1]}((\gamma_0, I_R)u, a, v(I_L, \delta_0))$$

$$= f^{\omega}(I_R^{\omega}u, a, vI_L^{\omega})$$

as required. $\square$

Back to our tree model, we remark next that the elliptic contractions induced by the letters are constant at a given depth for our bimachine $\mathcal{B}$.

For every $u \in A'^+$, consider the elliptic contraction

$$\begin{aligned} \nu_u : P_R^{[n,1]} &\to P_R^{[n,1]} \\ (\gamma_n, \ldots, \gamma_1) &\mapsto (\gamma_n, \ldots, \gamma_1)u. \end{aligned}$$

Given $(\gamma_{n-1}, \ldots, \gamma_1) \in P_R^{[n-1,1]}$, let

$$\nu_{u,\gamma_{n-1},\ldots,\gamma_1} : Q_R^{(Q_L^{(1)})^{n-1}} \to Q_R^{(Q_L^{(1)})^{n-1}}$$

be the mapping defined by

$$\nu_{u,\gamma_{n-1},\ldots,\gamma_1}(\gamma_n) = \pi_n \nu_u(\gamma_n, \ldots, \gamma_1).$$

Proposition 9.3 *The mapping $\nu_{u,\gamma_{n-1},\ldots,\gamma_1}$ is constant for all $u \in A'^+$ and $(\gamma_{n-1}, \ldots, \gamma_1) \in P_R^{[n-1,1]}$.*

Proof. Write $u_1 = u \in A'^+$ and let $(\gamma_n, \ldots, \gamma_1) \in P_R^{[n,1]}$. By Lemma 6.3, we have $(\gamma_n, \ldots, \gamma_1)u_1 = (\gamma'_n, \ldots, \gamma'_1)$ with

$$\gamma'_j(q_L^{(1)}, \ldots, q_L^{(j-1)}) = (\gamma_j(u_1 q_L^{(1)}, \ldots, u_{j-1} q_L^{(j-1)}))u_j, \tag{18}$$

where the words $u_2, \ldots, u_n$ are defined recursively by

$$u_{j+1} = (\gamma_j(u_1 q_L^{(1)}, \ldots, u_{j-1} q_L^{(j-1)}))g_{u_j}^{(j)} q_L^{(j)} \quad (j = 1, \ldots, n-1). \tag{19}$$

By (18), and since the action is right zero, it is enough to show that the last letter of the word u_n is independent from γ_n. Now by (19) and Lemma 3.1, this last letter is of the form

$$f((\gamma_{n-1}(u_1 q_L^{(1)}, \ldots, u_{n-2} q_L^{(n-2)}))u'_{n-1}), u''_{n-1}, q_L^{(n-1)}),$$

where $u_{n-1} = u'_{n-1} u''_{n-1}$ and $u''_{n-1} \in A'$, therefore $\nu_{u,\gamma_{n-1},\ldots,\gamma_1}$ is constant. $\square$

10 Random walks on semigroups and Turing machines

10.1 Random walks on semigroups

Let S be a semigroup finitely generated by A and let S act to the right of the set X, not necessarily faithfully, denoted (X, S, A). In the following, a knowledge of the paper [9] is useful.

First for each $a \in A$ we can consider the $X \times X$ matrix with entry (x, xa) equal to 1 and all other entries equal to zero. The entries could be in any semiring, but we will consider them in the real or complex field. We denote this matrix by $\mathrm{op}(\cdot a)$ (operator of right action $\cdot$ of a).

We denote the transpose $\mathrm{op}(\cdot a)$, $(\mathrm{op}(\cdot a))^*$, as $\mathrm{op}(a^{-1} \cdot)$.

Now the *adjacency matrix* for (X, S, A), denoted $\mathrm{Adj}(X, S, A)$, is by definition

$$\sum_{a \in A} \mathrm{op}(\cdot a) + \mathrm{op}(a^{-1} \cdot),$$

a self-adjoint matrix or operator on the suitable Hilbert space with nonnegative integer entries. See [9].

The 2-sided simple random walk (2SRW) on (X, S, A) is

$$\begin{aligned} &\mathrm{transition}\left(\sum_{a \in A} \mathrm{op}(\cdot a) + \mathrm{op}(a^{-1} \cdot)\right) \\ \equiv\, &\mathrm{transition}(\mathrm{Adj}(X, S, A)). \end{aligned}$$

Here $\mathrm{transition}(M)$, where M is a matrix with nonnegative entries, is the matrix obtained by multiplying row x by the inverse of the sum of the entries in row $x \equiv 1/\sum_x$, so we must assume $\sum_x < \infty$ for all $x \in X$.

So the 2SRW (assuming it exists) is a self-adjoint operator on the Hilbert space $l_2(X)$ and is a stochastic matrix with nonnegative entries and with row sums 1. See [9]. So compute its spectrum, eigenvalues, spectral radius, etc. The norm of the operator is ≤ 1. The first question is what is the 2SRW of (A^+, A^+, A)? (This is well defined because A^+ is cancellative.) See [4]. Even for $|A| = 1$, the 2SRW becomes

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\ \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & \ldots \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & 0 & \ldots \\ 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Clearly, the 2SRW of (X, S, A) is well defined if X is finite. Now in our situation for Turing machines from Section 6 we have a finite number of elliptic contractions operating on a symmetric tree (see [12]), so in this case, the 2SRW is well defined by restricting the action to those vertices distance $\leq n$ from the root and then taking their 2SRW and limiting (i. e., obtaining the operator for the 2SRW as the limit of the finite operators for each n).

Notice by going to the ends ∂ with product measure μ, the adjacency matrix of the finite number of elliptic contractions $A = \{a_1, \ldots, a_k\}$ can be defined by considering $L^2(\partial, \mu)$ and then considering the operator

$$(\ )f \to (\cdot a)f$$

which corresponds to $\mathrm{op}(a^{-1}\cdot)$. So the adjoint of this operator corresponds to $\mathrm{op}(\cdot a)$, so the 2SRW is a row normalization of this Adj operator, with $\mathrm{Adj} = \sum_{a \in A}(\mathrm{op}(a^{-1}\cdot) + \mathrm{op}(\cdot a))$.

Now given $\alpha : A^+ \to B^+$ a lp-mapping, we can go to the minimal bimachine $\mathcal{B}_\alpha$ (Proposition 2.3) calculating α and obtain the right and left A-automata and take their 2SRWs, denoted R2SRW and L2SRW (assuming they are well-defined, which they will be if we apply $(\ )^L$ and $(\ )^R$ to the minimal bimachine semigroups). Thus, given an NP-complete problem P, we can obtain two 2SRWs: R2SRW(P) and L2SRW(P). We make this well defined by applying $(\ )^L$ and $(\ )^R$ to the minimal bimachine.

Also, given a deterministic Turing machine T_P solving the problem P, via Section 6, we obtain for R (for L) a finite number of elliptic contractions on a symmetric tree, so the 2SRW is defined, which we denote R2SRW(T_P) (and L2SRW(T_P)). Then we want to understand how R2SRW(T_P) and L2SRW(T_P) are related. (We need limit theorems for spectra, spectral radii, etc.)

Working Conjecture (as of 09 June, 2006). *If R2SRW(P) and L2SRW(P) are the free 2SRW of (A^+, A) for suitable finite A (or close to it), then P has no polynomial-time algorithm, by considering the spectral radius of the free vs. the spectral radius of R2SRW(T_P).*

Another approach is possible using the Brown/Steinberg method utilizing triangular complex matrices. See [18], [19].

Acknowledgement

Both authors acknowledge generous support from C.M.U.P., financed by F.C.T. (Portugal) through the programmes POCTI and POSI, with national and European Community structural funds, and the European Science Foundation program AutoMathA.

The first author thanks the University of California, Berkeley Math Department for its many kindnesses, and we thank the Math Department, the Berkeley Academic Senate, and the Rhodes Family Foundation for some financial support.

We thank Jean-Camille Birget for his help with this paper.

References

[1] J, Almeida, S. Margolis, B. Steinberg, M. Volkov, "Representation Theory of Finite Semigroups, Semigroup Radicals, and Formal Language Theory," preprint (2006)

[2] J.-C. Birget, Infinite string rewriting, *J. Symbolic Computation* 25 (1998), 759–793.

[3] Nigel Boston, “p-adic Galois Representations and pro-p Galois Groups,” in [16].

[4] M. V. Crabb, J. Duncan, C. M. McGregor, “Spectra in Some Inverse Semigroup Algebras,” Mathematical Proceedings of the Royal Irish Academy, **104A**(2), 211-218 (2004).

[5] S. Eilenberg, *Automata, Languages and Machines*, Vol. A and Vol. B, Academic Press, New York, 1974 and 1976. Christos

[6] R. I. Grigorchuk, “Just Infinite Branch Groups,” in [16], 121-180.

[7] R. I Grigorchuk and A. Zuk, “The lamplighter group as a group generated by a 2-state automaton, and its spectrum,” Geom. Dedicata 87 (2001),209-244

[8] K. Krohn., R Mateosian, J. Rhodes, “Methods of the Algebraic Theory of machines I,” J. of Computer and System Sciences, Vol 1, No. 1 April 1967, 55-85

[9] B. Mohar, W. Woess, “A Survey on Spectra of Infinite Graphs,” Bulletin of the London Mathematical Society, 21 (198), no. 3, 209-234.

[10] H. Papadimitriou, *Computational Complexity*, Reading, Mass: Addison Wesley Longman, 1995.

[11] Luis Ribes and Pavel Zalesskii, “Pro-p Trees and Applications,” in [16].

[12] J. Rhodes, Monoids acting on trees: elliptic and wreath products and the Holonomy Theorem for arbitrary monoids with applications to infinite groups, *Int. J. Alg. Comp.* 1.2 (1991), 253-279; with Erratum to diagram p. 274.

[13] J. Rhodes, *Applications of Automata Theory and Algebra via the Mathematical Thoery of Complexity to Biology, Physics, Psychology, Philosophy, Games and Codes*, ed. Chrystopher L. Nehaniv, foreword by Morris W. Hirsch, preprint 1971.

[14] J. Rhodes and B. Steinberg, *The q-theory of Finite Semigroups*, Springer-Verlag, to appear, `http://mathstat.carleton.ca/~bsteinbg/`.

[15] J. Rhodes and B. Tilson, The kernel of monoid morphisms, *J. Pure Appl. Algebra* 62 (1989), 227–268.

[16] Marcus du Sautoy, Dan Segal, Aner Shalev, eds., *New Horizons in pro-p Groups*, Boston and Basel: Birkhauser, 2000.

[17] J. C. Shepherdson, “The teduction of two-way automata to one-way automata,” IBM Journal of Research and Development, 3, pp. 195-200, 1959.

[18] B. Steinberg, “Möbius Functions and Semigroup Representations II, Character Formulas and Multiplicities,” to appear in Journal of Combinatorial Theory A.

[19] K. Brown, “Semigroups, rings, and Markov Chains,” J. of Theoret. Probab. 13 (2000), 871-938.