The "last" decision problem for rational trace languages

Jacques Sakarovitch

Institut Blaise Pascal,
4, place Jussieu
75 252 Paris Cedex 05.

To M. P. Schűtzenberger,
respectfully.

Abstract

It is established here that it is decidable whether a rational set of a free partially commutative monoid (*i.e.* trace monoid) is recognizable or not if and only if the commutation relation is transitive (*i.e.* if the trace monoid is isomorphic to a free product of free commutative monoids). The bulk of the paper consists in a characterization of recognizable sets of free products via generalized finite automata.

Introduction[1]

Since the work of Mazurkiewiecz [12], trace monoids are currently recognized as a possible model for parallel or concurrent programs. This paper deals with the recognizability of rational sets in such monoids. In order to present the result and its interpretation in terms of programs, let us first recall the "standard" teminology and notations of the domain: A is an alphabet, $\theta \subseteq A \times A$ a symmetric relation on A is the *commutation relation* . The *free partially commutative monoid*, or *trace monoid*, $\mathrm{M}(A, \theta)$ is the quotient of A^* by $[\theta]$ — where $[\theta]$ is the congruence of the free monoid A^* generated by the set of pairs $\{(ab, ba) \mid (a, b) \in \theta\}$. Elements of $\mathrm{M}(A, \theta)$ are called *traces* , subsets of $\mathrm{M}(A, \theta)$ *trace languages*. The family of rational (or regular) subsets of $\mathrm{M}(A, \theta)$ is denoted by $\mathrm{Rat}\,\mathrm{M}(A, \theta)$.

Trace monoids are a model for the behaviour of a parallel program in the sense that *one* computation of such a program is interpreted as *the set of* sequences (*i.e.* elements of A^*) of operations that can be obtained using all possible commutations between them. This set of equivalent computations is well represented by *one* element of the trace monoid. A rational subset of the trace monoid is a description of the set of computations which a parallel program performs (see [7,12]). We address here the problem of deciding whether a rational set of $\mathrm{M}(A, \theta)$ is *recognizable* and we prove:

[1] This work has been supported in part by the "'Programme de recherches coordonnées" Mathématiques et Informatique of the Ministère de la Recherche et de la Technologie, by the ESPRIT-BRA Working Group 3166 ASMICS and by the BID Program of the Universidade de Saõ Paulo

Theorem 1. *Recognizability is decidable in* Rat $\mathrm{M}(A, \theta)$ *iff* θ *is transitive.*

In the context of parallel programs, recognizability of a rational set and thus of the behaviour of a parallel program is interpreted as the property that the set of computations of the program, when expended via all possible commutations, forms a rational set of sequences of operations, that is, the parallel program can be controlled by a finite automaton (see [7]).

In the next section, we shall briefly review the other decision problems for rational trace languages. It is remarkable that the condition "θ transitive" plays such a central rôle. The fact that it is a necessary condition follows from Ibarra's undecidability result [10] (*cf.* Theorem 3 below). The fact it is sufficient — which means that these problems are decidable in *free products of free commutative monoids* — is based on two different classes of properties.

The first ones, due to Ginsburg and Spanier [8,9], say that all these problems are decidable in free commutative monoids. The second ones deal with rational sets in free products of monoids. Roughly speaking they state that the constructions that are possible on finite automata over a free monoid still hold for finite automata over a free product of monoids provided that the basic pieces of these constructions are correctly changed. In a previous work ([13]) we had established that a class of automata over a free product : the *bipartite automata*, made it possible to generalize the notion of *deterministic automaton* and thus to extend the constructions and results referring to determinization of automata and Boolean operations on rational sets.

We go on here along the same line. The deterministic automata over a free monoid that recognize a given subset naturally form a (semi-)lattice with a minimal element : *the minimal automaton* of the subset. We show here that the same holds for deterministic bipartite automata : Proposition 1 states the existence of a *minimal bipartite automaton* that recognizes a given subset of a free product and the main result (Proposition 3) states that, under the hypothesis that the factor monoids are without divisors of the identity — and this is the case for free commutative monoids —, the labels of the minimal bipartite automaton of a recognizable subset of a free product are recognizable subsets of the factors.

The paper is organized as follows. In section 1, after presenting the other decisions problems on rational trace languages we prove the necessary condition in Theorem 1 and we also show how the sufficient condition in Theorem 1 can be reduced to a closure property of the free products (Theorem 6). The rest of the paper is then devoted to that latter result. In section 2 we fix the notations for free products and we define the equivalence γ_R that will be used to define the minimal bipartite automaton of R . Before doing that, in section 3, we have to recall the definition of bipartite automata; the properties of rational subsets that are deduced from the properties of bipartite automata are recalled in section 5. In section 4 minimal bipartite automata are defined and the recognizable subsets of a free product of monoids without divisors of the identity are characterized in section 6.

1 Decision problems for rational trace languages

Theorem 1 is certainly better understood if it is compared to other decisions results in trace monoids. Given a relation θ and two trace languages K and L in $\mathrm{Rat}\,\mathrm{M}(A,\theta)$ — by means of rational expressions say — the following five decisions problems naturally arise (if we put apart membership which is obviously decidable):

Inclusion	*i.e.* can one decide if	$K \subseteq L$?
Equality	"	$K = L$?
Universality	"	$K = \mathrm{M}(A,\theta)$?
Intersection	"	$K \cap L \neq \emptyset$?
Recognizability	"	K is recognizable ?

Note that all these problems are known to be decidable in the two extreme cases of trace monoids: for free monoids (it follows from Kleene's theorem) and for the free commutative monoids (from Ginsburg and Spanier's work [8,9]).

The solution for inclusion, equality, and universality is given by two different results. We first have:

Theorem 2. [2,3,13] $\mathrm{Rat}\,\mathrm{M}(A,\theta)$ *is an (effective) Boolean algebra iff* θ *is transitive.*

And thus the three problems are decidable if θ is transitive. It follows from the next one that none of them is decidable if θ is not transitive:

Theorem 3. [10] *Universality is undecidable in* $\mathrm{Rat}\,(\{a,b\}^* \times \{c\}^*)$.

From Theorem 2 intersection is decidable when θ is transitive but this condition is not necessary:

Theorem 4. [1] *Intersection in* $\mathrm{Rat}\,\mathrm{M}(A,\theta)$ *is decidable iff the graph of* θ *is a transitive forest.*

Note that θ is transitive iff $\mathrm{M}(A,\theta)$ is isomorphic to a free product of free commutative monoids (the definition of free products is recalled in section 2). In [13] we proved Theorem 2 by means of a closure property of free products, namely:

Theorem 5. *Let* M *and* N *be two monoids such that* $\mathrm{Rat}\,M$ *and* $\mathrm{Rat}\,N$ *are effective Boolean algebras. Then* $\mathrm{Rat}\,M*N$ *is an effective Boolean algebra.*

As announced, we shall derive Theorem 1 from another closure property of free products:

Theorem 6. *Let* M *and* N *be two monoids with the following properties:*

i) *neither* M *nor* N *have divisors of the identity;*

ii) $\mathrm{Rat}\,M$ *and* $\mathrm{Rat}\,N$ *are effective Boolean algebras;*

iii) *recognizability is decidable in both* $\mathrm{Rat}\,M$ *and* $\mathrm{Rat}\,N$.

Then recognizability is decidable in $\mathrm{Rat}\,M*N$.

Proof of Theorem 1. The condition is necessary. If θ is not transitive there exist letters a, b and c in A such that $(a,c) \in \theta$, $(b,c) \in \theta$ and $(a,b) \notin \theta$, *i.e.* $S = \{a,b\}^* \times \{c\}^*$ is a submonoid of $\mathrm{M}(A,\theta)$. Note that S itself is a recognizable subset of $\mathrm{M}(A,\theta)$.

In the "classical" case of the monoid $M = \{a,b\}^* \times \{c,d\}^*$ the indecidability of the universe problem in Rat M is proved by reduction to a Post correspondence problem and the undecidability of recognizability within Rat M is then derived (*cf.* [4] for instance). We shall follow here a very similar procedure applied to S . For that purpose it is convenient to adapt the proof of Theorem 3 by Lisovik ([11]) in order to make clear the reference to a Post correspondence problem.

Let B and C be two alphabets (with at least two letters). Any Post correspondence problem $\mathcal{P}$ may be described as a pair (α,β) of morphisms from B^* into C^* . The solutions of $\mathcal{P}$ are the subset of words f in B^* such that $\alpha(f) = \beta(f)$. Let c be a symbol that do not belong to $(B \cup C)$; and define the subset W_α of $(B \cup C)^* \times \{c\}^*$ by

$$W_\alpha = \{(f\alpha(f), c^{|\alpha(f)|}) \mid f \in B^*\} .$$

Clearly the problem $\mathcal{P}$ has no solution iff $W_\alpha \cap W_\beta$ is empty that is iff

$$\overline{W_\alpha} \cup \overline{W_\beta} = (B \cup C)^* \times \{c\}^* ,$$

where $\overline{W_\alpha}$ denotes the complement of W_α . Theorem 3 (and the reason for the definition of W_α) follows then from the following.

Lemma 1. [11] *$\overline{W_\alpha}$ belongs to* Rat $((B \cup C)^* \times \{c\}^*)$ *(and is effectively computable from α).*

Let $Z = W_\alpha \cap W_\beta$. Note that (W_α and) Z is the graph of a *function* and that if Z is not empty it is *infinite*. Suppose now that $\overline{W_\alpha} \cup \overline{W_\beta}$ is recognizable; then Z is also recognizable. The classical characterization of the recognizable subsets of a direct product (finite union of products of recognizable subsets of the factors) yields that a recognizable graph of a function is *finite*. Thus Z is recognizable iff it is empty, which is undecidable. Clearly $\overline{W_\alpha} \cup \overline{W_\beta}$ can be encoded in such a way it belongs to Rat $(\{a,b\}^* \times \{c\}^*)$. If it were recognizable in $\mathrm{M}(A,\theta)$ it would be also recognizable in S and that terminates this part of the proof.

The condition is sufficient. If θ is transitive, then $\mathrm{M}(A,\theta)$ is a free product of free commutative monoids. Since free commutative monoids are without divisors of the identity, since their rational subsets form an effective Boolean algebra ([8]) in which recognizability is decidable ([9]), this part is an immediate consequence of Theorem 6. □

2 Free products

If M is a monoid, its identity element is denoted 1_M, and the complement of 1_M is denoted $M^\bullet$: $M^\bullet = M \backslash 1_M$. We say that a monoid M is *without divisors of the identity* if there is no element p and q in $M^\bullet$ such that $pq = 1_M$.

The *free product* of two monoids M and N, denoted $M*N$, can be identified with the monoid the elements of which are the finite sequences $(u_1, u_2, \cdots, u_p)$ of elements of $M^\bullet \cup N^\bullet$ alternatively taken in $M^\bullet$ and $N^\bullet$, *i.e.* $u_i \in M^\bullet \Leftrightarrow u_{i+1} \in N^\bullet$, where $M^\bullet$ and $N^\bullet$ are supposed to be disjoint. The product of two such sequences is recursively defined: $(u_1, u_2, \ldots, u_p)(v_1, v_2, \ldots, v_q)$ is equal to:

i) $(u_1, u_2, \ldots, u_p, v_1, v_2, \ldots, v_q)$ if u_p and v_1 do not belong to the same monoid;

ii) $(u_1, u_2, \ldots, u_p\, v_1, v_2, \ldots, v_q)$ if u_p and v_1 belong to the monoid and $u_p v_1$ is different from the identity element;

iii) $(u_1, u_2, \ldots, u_{p-1})(v_2, \ldots, v_q)$ otherwise.

Each of M and N is a submonoid of $M*N$ — sequences of length 1. This allows to write $u = u_1 u_2 \cdots u_p$ instead of $u = (u_1, u_2, \ldots, u_p)$; such a factorisation for an element u of $M*N$ is unique and is called its *canonical factorisation*. We call *initial monoid* of u, denoted $\mathrm{MI}(u)$, the monoid, M or N, to which u_1 belongs; the *final monoid* of u, denoted $\mathrm{MF}(u)$, is the monoid to which u_p belongs. The product uv of two elements u and v of $(M*N)^*$ is *non miscible* if $\mathrm{MF}(u) \neq \mathrm{MI}(v)$, *i.e.* if the canonical factorisation of uv is $uv = u_1 u_2 \ldots u_p\, v_1 v_2 \ldots v_r$.

In the sequel we keep the following notations : A and B are two alphabets; clearly $(A \cup B)^* = A^* * B^*$ if A and B are disjoint, which is understood from now on; M and N are two monoids, disjoint as well; $\varphi : A^* \to M$ and $\psi : B^* \to N$ are respectively two surjective morphisms that naturaly define the surjective morphism

$$\varphi * \psi : (A \cup B)^* \to M * N$$

by

$$\forall c \in A \cup B \quad \varphi*\psi(c) = \begin{cases} \varphi(c) & \text{if} \quad c \in A\,, \\ \psi(c) & \text{if} \quad c \in B\,. \end{cases}$$

By *inverse image* of an element u of $M*N$ (resp. of M, of N) we understand the inverse image of u by $\varphi*\psi$ (resp. by φ, by ψ). With these notations we have:

Lemma 2. *If M and N are without divisors of the identity, the inverse image of an element u of $M*N$ is the product of the inverse images of the factors of its canonical factorisation; i.e. if, for instance, $\mathrm{MI}(u) = M$ and $\mathrm{MF}(u) = N$, it holds:*

$$(\varphi*\psi)^{-1}(u) = \varphi^{-1}(u_1)\, \psi^{-1}(u_2)\, \varphi^{-1}(u_3) \cdots \varphi^{-1}(u_{n-1})\, \psi^{-1}(u_n)\,.$$

□

Let R be a subset of $M*N$. We denote, as usual, by ρ_R the coarsest right regular equivalence of $M*N$ that saturates R. *i.e.*

$$u \simeq v \mod \rho_R \quad \Leftrightarrow \quad u^{-1}R = v^{-1}R$$

where

$$u^{-1}R = \{w \in M*N \mid uw \in R\}$$

i.e. $u \simeq v \mod \rho_R$ if u and v have *the same right contexts* for R. And by σ_R the coarsest congruence of $M*N$ that saturates R. *i.e.*

$$u \simeq v \mod \sigma_R \quad \Leftrightarrow \quad C_R(u) = C_R(v)$$

where

$$C_R(u) = \{(x, y) \in (M*N) \times (M*N) \mid xuy \in R\}$$

i.e. $u \simeq v \mod \sigma_R$ if u and v have *the same contexts* for R. The *minimal automaton* of R is defined by means of the equivalence ρ_R. We shall define a (slightly) larger automaton

by means of another equivalence, denoted by γ_R. In order to define γ_R it is convenient to consider first the equivalence τ defined on $M*N$ by the equality of the final monoids, *i.e.*

$$\forall u, v \in (M*N)^\bullet\ , \quad u \simeq v \mod \tau \quad \Leftrightarrow \quad \mathrm{MF}(u) = \mathrm{MF}(v)\ .$$

The equivalence τ corresponds to the following partition of $M*N$:

$$M*N = \{1\} + \{(N^\bullet M^\bullet + M^\bullet)(N^\bullet M^\bullet)^*\} + \{(M^\bullet N^\bullet + N^\bullet)(M^\bullet N^\bullet)^*\}\ .$$

It is worth noting that τ is *a congruence* when M and N have no divisors of the identity.

The relation γ_R is then defined by:

$$u \simeq v \mod \gamma_R \quad \Leftrightarrow \quad \begin{cases} \text{i)} & u \simeq v \mod \tau \\ \text{ii)} & u \in R \Leftrightarrow v \in R \\ \text{iii)} & \forall w \quad \mathrm{MI}(w) \neq \mathrm{MF}(u)\ , \quad uw \in R \Leftrightarrow vw \in R \end{cases}$$

that is:

$$u \simeq v \mod \gamma_R \quad \Leftrightarrow \quad [u^{-1}R \cap \{1 \cup X(M*N)\} = v^{-1}R \cap \{1 \cup X(M*N)\}]$$

with $X = M^\bullet$ or $N^\bullet$ and $X \neq \mathrm{MF}(u)$. Which means that $u \simeq v \mod \gamma_R$ if u and v have *the same non miscible right contexts* for R. Because of i), 1_{M*N} is alone in its class mod γ_R. The following assertions are immediate.

Property 1. i) *γ_R is an equivalence relation that saturates R.*

ii) *$\rho_R \wedge \tau$ is thiner than γ_R.*

iii) *γ_R is not necessarily right regular but it holds:*

$$u \simeq v \mod \gamma_R \quad \Rightarrow \quad \forall w \quad \mathrm{MI}(w) \neq \mathrm{MF}(u)\ , \quad uw \simeq vw \mod \gamma_R\ .$$

3 Bipartite automata on a free product

Recall first the definition of an *automaton on a monoid M* . An automaton

$$\mathcal{A} = < Q, M, E, I, T >$$

is a labelled graph : Q is the set of the vertices called *states*, I and T are two distinguished subsets of Q: the *initial states* and the *terminal states*, and E is the set of the edges, labelled by elements, or — a generalization that will be of importance here — by *subsets* of M. A *computation* c of $\mathcal{A}$ is a finite sequence of labelled edges that form a path in the graph $\mathcal{A}$:

$$c = p_0 \xrightarrow{U_1} p_1 \xrightarrow{U_2} p_2 \xrightarrow{U_3} \dots \xrightarrow{U_n} p_n$$

The *label* of c is the subset $|c| = U_1 U_2 \dots U_n$ of M. The computation c is *successful* if p_0 belongs to I and p_n to T. The *result* of $\mathcal{A}$ is the subset of M, denoted $|\mathcal{A}|$, equal to the union of the labels of the successful computations. An automaton $\mathcal{A}$ is *normalised* if there is no edge arriving in an initial state; an automaton is *trimmed* if every state is both accessible from an initial state and co-accessible from a terminal state.

Recall that a graph is called *bipartite* if there exists a partition of the set of the vertices in two classes such that no edge of the graph is adjacent to two vertices of a same class. We say that $\mathcal{A}$ is *a bipartite automaton* on $M*N$ if the following conditions are met:

- i) $\mathcal{A}$ is a bipartite graph; let $S = P + Q$ be the partition of the set of vertices.
- ii) the edges from P to Q are labelled by subsets of M.
- iii) the edges from Q to P are labelled by subsets of N.

A bipartite automaton $\mathcal{A}$ can then be denoted as:

$$\mathcal{A} = < P \cup Q, M * N, E_P \cup E_Q, I_P \cup I_Q, T_P \cup T_Q >$$

with

$$E_P = \{V_{p,q} \mid (p,q) \in P \times Q\} \qquad V_{p,q} \subseteq M ,$$
$$E_Q = \{W_{q,p} \mid (q,p) \in Q \times P\} \qquad W_{q,p} \subseteq N ,$$

and these notations will be kept in the sequel.

A bipartite automaton $\mathcal{A}$ is said:

- *proper* if no label contains the identity (of M or N) *i.e.*

$$\forall p \in P \quad \forall q \in Q \quad V_{p,q} \subseteq M^\bullet \quad W_{q,p} \subseteq N^\bullet \ ;$$

- *deterministic* if
  - i) two edges going out of the same state have disjoint labels *i.e.*

$$\forall p \in P \quad \forall q', q'' \in Q \quad V_{p,q'} \cap V_{p,q''} = \emptyset \ ,$$
$$\forall q \in Q \quad \forall p', p'' \in P \quad W_{q,p'} \cap W_{q,p''} = \emptyset \ ;$$

  - ii) there is, at most, one initial state in each of the subsets P and Q *i.e.*

$$|I_P| \leq 1 \text{ and } |I_Q| \leq 1 \ ;$$

- *complete* if
  - i) the union of the labels of all edges going out of every state is $M^\bullet$, or $N^\bullet$, *i.e.*

$$\forall p \in P \quad \bigcup_{q \in Q} V_{p,q} = M^\bullet \qquad \forall q \in Q \quad \bigcup_{p \in P} W_{q,p} = N^\bullet \ ;$$

  - ii) neither I_P nor I_Q is empty.

(N.B. This does not mean that $\mathcal{A}$, as a graph, is a complete bipartite graph)

It is always possible, and easy to make complete, and normalized, and trimmed any given automaton and such transformations are effective (see [5]).

A proper bipartite automaton $\mathcal{A}$ should be understood as an automaton over a — most often non finitely generated — free monoid: every element of $M^\bullet$ or $N^\bullet$ is considered as a single letter. Since $\mathcal{A}$ is bipartite and proper, two consecutive edges on any path are labelled by elements taken in different monoids: their product is non miscible. The canonical factorization of an element of $|\mathcal{A}|$ is "read" on the computation exactly in the same way as a word recognized by a classical automaton is "spelled" on the path that recognizes it. This identification makes it necessary to consider the whole set $M^\bullet \cup N^\bullet$ as a (possibly infinite) alphabet even though M and N are finitely generated: the decidability result is still at hand but the decision procedure will be transformed (if compared to the equivalent one on classical automata).

We end this section with the verification that the classical properties of *deterministic automata* have their natural counterpart for the *deterministic proper bipartite automata*. Let thus $\mathcal{A}$ be such an automaton that is moreover chosen to be *complete*. [In the rest of the paper we write "automaton" for *bipartite automaton on* $M*N$]. By induction on the length of the canonical factorization of the elements of $(M*N)^\bullet$, it first holds:

Property 2. i) *For every p in P, and for every u in $(M*N)^\bullet$ such that* $\mathrm{MI}(u) = M$, *there exists a unique path in $\mathcal{A}$, with origin p and with label u; we note $p \cdot u = t$ the end of this path.*

ii) *For every q in Q, and for every u in $(M*N)^\bullet$ such that* $\mathrm{MI}(u) = N$, *there exists a unique path in $\mathcal{A}$, with origin q and with label u; we note $q \cdot u = t$ the end of this path.*

The automaton $\mathcal{A}$ thus determines a mapping, not everywhere defined, from $(P \cup Q) \times (M*N)^\bullet$ to $P \cup Q$: in all the cases not covered by i) or ii) above, $s \cdot u$ is undefined. This is not truly an *action* of the monoid $M*N$ on $P \cup Q$ but the following property makes the notation sound.

Property 3. $\forall u, w \in M*N \quad \forall s \in P \cup Q$

i) $s \cdot u$ *defined* $\Rightarrow \quad [(s \cdot u) \cdot w$ *defined* $\Leftrightarrow \mathrm{MF}(u) \neq \mathrm{MI}(w)]$.

ii) $(s \cdot u) \cdot w$ *defined* $\Rightarrow \quad [(s \cdot u) \cdot w = s \cdot (uw)]$.

We note $I = I_P \cup I_Q$ and — it is a slight abuse of notation — $I \cdot u$ for the end of the unique path in $\mathcal{A}$ with label u the origine of which is either I_P, or I_Q (according to $\mathrm{MI}(u) = M$ or N respectively), that is the state in which $\mathcal{A}$ stops after the "reading" of the element u. This path always exists since $\mathcal{A}$ is chosen complete. Note that one should not add a garbage state to $P \cup Q$ in order to have a true action of the monoid $M*N$ on $P \cup Q$: the path starting in I and labelled by u would not be unique anymore. It should be clear that the result of $\mathcal{A}$ is defined by

$$|\mathcal{A}| = \{u \in M*N \mid I \cdot u \in T = T_P \cup T_Q\}$$

and we have:

Lemma 3. *Let $\mathcal{A}$ be a deterministic, complete and normalised proper automaton and R the result of $\mathcal{A}$. It holds*

$$\forall u, v \in M*N \quad I \cdot u = I \cdot v \quad \Rightarrow \quad u \simeq v \mod \gamma_R \ .$$

□

4 Minimal bipartite automata

We go on in the analogies between the proper bipartite automata and the classical automata with the construction of the minimal bipartite automaton of a subset R of $M*N$. It is convenient to denote by C and D the two classes, different from 1_{M*N}, of the equivalence τ:

$$C = (M^\bullet N^\bullet + N^\bullet)(M^\bullet N^\bullet)^* \text{ and } \quad D = (N^\bullet M^\bullet + M^\bullet)(N^\bullet M^\bullet)^* \ .$$

With these conventions Property 1, iii) reads:

$$\forall m \in M \quad \forall u, v \in \{1\} + C \quad u \simeq v \mod \gamma_R \quad \Rightarrow \quad um \simeq vm \mod \gamma_R$$

$$\forall n \in N \quad \forall u, v \in \{1\} + D \quad u \simeq v \mod \gamma_R \quad \Rightarrow \quad un \simeq vn \mod \gamma_R$$

which implies:

Property 4. *Let R be any subset of $M*N$ and γ_R the equivalence associated to R. Let P be the trace of γ_R on $\{1\}+C$ and Q the trace of γ_R on $\{1\}+D$.*

Let $u \in \{1\}+C$ and $[u]$ its class modulo γ_R. For every m in M,

$$[u]\cdot m \mapsto [um]$$

defines a mapping $P \times M \to Q$. Accordingly, for u in $\{1\}+D$ and for every n in N,

$$[u]\cdot n \mapsto [un]$$

defines a mapping $Q \times N \to P$.

The sets P and Q defined in Property 4 yield a proper bipartite automaton $\mathcal{A}_R$ on $M*N$: the states of $\mathcal{A}_R$ are $P \cup Q$; for every pair $(p,q) \in P \times Q$, the edge $p \to q$ is labelled by

$$V_{p,q} = \{m \in M^* \mid p\cdot m = q\}$$

and for every pair $(q,p) \in Q \times P$, the edge (q,p) is labelled by

$$W_{q,p} = \{n \in N^* \mid q\cdot n = p\}\ .$$

For every p in P, $\{V_{p,q} \mid q \in Q\}$ is a partition of M^* and for every q in Q, $\{W_{q,p} \mid p \in P\}$ is a partition of N^*. Then $\mathcal{A}_R$ is deterministic and complete. The initial states are the classe of 1_{M*N} in P and in Q and $\mathcal{A}_R$ is normalised; the terminal states are the classes of P and Q that are contained in R. This construction implies that the result of $\mathcal{A}_R$ is the subset R itself. We call $\mathcal{A}_R$ *the minimal bipartite automaton* of R; this denomination is justified by the following property.

Proposition 1. *Every proper bipartite, deterministic, complete, normalised, and trimmed automaton the result of which is R, has $\mathcal{A}_R$ as homomorphic image.*

Proof. Let $\mathcal{B}$ be an automaton which meets the hypothesis of the proposition:

$$\mathcal{B} = < X \cup Y, M*N, E_X \cup E_Y, J_X \cup J_Y, S_X \cup S_Y > \ .$$

The mapping

$$\lambda : X \cup Y \to P \cup Q$$

is defined by

$$\forall z \in X \cup Y \quad z \mapsto \lambda(z) = [u]$$

with $u \in M*N$ and $J\cdot u = z$. For every z such a u exists since $\mathcal{B}$ is trimmed, and λ is well defined — *i.e.* its value does not depend on the choice of u — since, from Lemma 3

$$\forall u, v \in M*N \quad J\cdot u = J\cdot v \quad \Rightarrow \quad u \simeq v \mod \gamma_R \ .$$

Necessarily $\lambda(J_X) = I_P$ and $\lambda(J_Y) = I_Q$ hold. Finaly, if $(x,w,y) \in E_X$, then, with a u such that $J\cdot u = x$, it holds $(J\cdot u)\cdot w = y$ in $\mathcal{B}$ and $[u]\cdot w = [uw]$ in $\mathcal{A}_R$, that is

$$(\lambda(x))\cdot w = \lambda(x\cdot w)\ ,$$

which means that λ is a morphism of automata, as desired . □

Note that the automaton $\mathcal{A}_R$, as well as the automaton $\mathcal{B}$ in Proposition 1 do not need to be finite since there is no condition on the subset R . The next section deals precisely with an important case where this automaton $\mathcal{A}_R$ is always finite.

5 Rational subsets of a free product

The *family of rational subsets* of any monoid M is the smallest family of subsets of M that contains the finite subsets and that is closed for the operations of union, product, and star. It is denoted Rat M. It is known ([6], see also [5] for instance) that the rational subsets of M can be defined by means of automata:

Theorem 7. *A subset of M is rational iff it is the result of a finite automaton on M, the labels of which are taken in any finite subset of generators of M.*

This is part of Kleene's Theorem, true in any monoid. Any rational subset of $M*N$ is thus the result of an automaton on $M*N$ the edges of which are labelled by *elements* of M or of N. We have proved that this automaton can be chosen bipartite, under the condition that the labels may be *subsets* of $M*N$:

Proposition 2. [13] *Let M and N be two monoids with the property that, for any rational subset L (of M or of N), $L\backslash 1$ — (with $1 = 1_M$ or 1_N) — is a rational subset. Then any rational subset of $M*N$ is the result of a finite* proper *bipartite automaton on $M*N$, the edges of which are labelled by* rational *subsets of M or of N.*

From Proposition 2 the following result is then derived:

Proposition 3. [13] *Let M and N be two monoids with the property that* Rat M *and* Rat N *are two (effective) Boolean algebras. Then any rational subset R of $M*N$ is the result of a* deterministic and complete *proper bipartite automaton the edges of which are labelled by rational subsets of M or of N (and that can be effectively computed from a finite automaton or from a rational expression the result of which is R).*

The core of the proof of Proposition 3 is a generalisation of the determinization of an automaton by the subset method. As in the classical case, the complement of the result of a complete deterministic bipartite automaton is obtained by exchanging the terminal and non terminal states and this gives the proof of Theorem 5.

6 Recognizable subsets of a free product

Recall that a subset of any monoid M is *recognizable* if it is saturated by a finite index congruence of M. Kleene's Theorem asserts that *the rational subsets of a finitely generated free monoid coincide with the recognizable subsets.* From which a characterisation of the recognizable subsets is derived:

Proposition 4. *Let M be any finitely generated monoid, A a finite alphabet, and $\varphi : A^* \to M$ a surjective morphism. A subset P of M is recognizable iff $\varphi^{-1}(P)$ is a rational subset of A^*.*

The recognizable subsets of a free product can then be characterized.

Theorem 8. *Let M and N be two monoids without divisors of the identity. A subset R of $M*N$ is recognizable iff it is the result of a bipartite automaton every label of which is a recognizable subset of M or of N.*

Proof. The condition is sufficient. Let R be the result of a finite bipartite automaton $\mathcal{A}$ every label of which is recognizable subset of M or of N. Since $\mathcal{A}$ is finite its result is a rational expression f in the labels of the edges of $\mathcal{A}$:

$$R = f(\{V_{p,q}, W_{q,p} \mid p \in P, q \in Q\})$$

The inverse image of R in $(A \cup B)^*$ is equal, since the two monoids are without divisors of the identity, and from Lemma 1, to the same expression in the inverse images of these labels, *i.e.*

$$(\varphi * \psi)^{-1}(R) = f(\{\varphi^{-1}(V_{p,q}), \psi^{-1}(W_{q,p}) \mid p \in P, q \in Q\}) .$$

Since the $V_{p,q}$ and $W_{q,p}$ are recognizable, the $\varphi^{-1}(V_{p,q})$ and the $\psi^{-1}(W_{q,p})$ are rational and thus $f(\{\varphi^{-1}(V_{p,q}), \psi^{-1}(W_{q,p}) \mid p \in P, q \in Q\})$ is rational. Thus R is recognizable.

The following proposition implies that the condition is necessary and gives a more precise statement.

Proposition 5. *Let M and N be two monoids without divisors of the identity. The minimal bipartite automaton of a recognizable subset of $M*N$ is a finite automaton every label of which is a recognizable subset of M or of N.*

Proof. Let R be a recognizable subset of $M*N$. Let

$$\mathcal{A}_R = < P \cup Q, M*N, E_P \cup E_Q, I_P \cup I_Q, T_P \cup T_Q >$$

be the minimal bipartite automaton of R . The equivalence ρ_R and the congruence σ_R are of finite index thus so are also $\rho_R \wedge \tau$ and $\sigma_R \wedge \tau$. From Property 1 ii), γ_R is of finite index and $\mathcal{A}_R$ is thus a finite automaton.

For every $p \in P$ let θ_p be the coarsest right regular equivalence of M that saturates the partition $\{V_{p,q} \mid q \in Q\}$ of M^*, *i.e.*

$$\forall f, g \in M \quad f \simeq g \mod \theta_p \quad \Leftrightarrow \quad [\forall h \in M \quad \forall q \in Q \quad fh \in V_{p,q} \Leftrightarrow gh \in V_{p,q}] .$$

We show that $\sigma_R \wedge \tau$ is thiner than every θ_p. Let p be fixed and let f and g be in M such that

$$f \simeq g \mod \sigma_R \wedge \tau .$$

The element 1_M is alone in its class mod τ, and alone also in its class mod θ_p since it is the only element of M that does not belong to any $V_{p,q}$. We suppose then that f and g are in M^*. Since M and N are two monoids without divisors of the identity, τ is *a congruence* and thus $\sigma_R \wedge \tau$ as well; it holds then:

$$\forall u, w \in M*N \quad ufw \in R \Leftrightarrow ugw \in R$$

which can be written as:

$$\forall h \in M \quad \forall u, w \in M*N \quad \mathrm{MI}(w) = N , \qquad ufhw \in R \Leftrightarrow ughw \in R$$

Let $u \in M*N$ such that $J \cdot u = p$. Then it holds:

$$\forall h \in M \quad \forall w \in M*N \quad \mathrm{MI}(w) = N , \quad ufhw \in R \Leftrightarrow ughw \in R$$

that is

$$\forall h \in M \quad ufh \simeq ugh \mod \gamma_R$$

or also

$$\forall h \in M \quad [u] \cdot fh = [u] \cdot gh$$

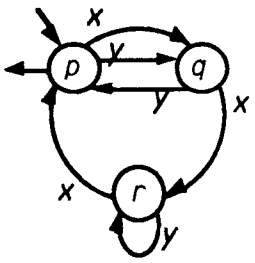
which means exactly that fh and gh belong to the same label $V_{p,q}$ with $p = [u]$ and $q = [ufh]$.

It is thus established that $\sigma_R \wedge \tau$ is thiner than θ_p which is thus of finite index and the $V_{p,q}$ are recognizable. It is shown in the same way that the $W_{q,p}$ are recognizable and this terminates the proof of Proposition 5 as well as the one of Theorem 8. □

Note that Proposition 5 does not hold any more for monoids having divisors of the identity. The following example will demonstrate this last assertion as well as it will illustrate the constructions called up in section 5.

Example 1. Let F be the free group on two generators. It holds $F = \mathbb{Z}_x * \mathbb{Z}_y$ where $\mathbb{Z}_x$ and $\mathbb{Z}_y$ are two distinct copies of $\mathbb{Z}$, the group of integers. As a monoid, $\mathbb{Z}_x$ is generated by $\{x, \bar{x}\}$ — with the defining relations $x\bar{x} = \bar{x}x = 1_{\mathbb{Z}_x}$ and $\mathbb{Z}_y$ is generated by $\{y, \bar{y}\}$.

Let α be the application that maps x on the circular permutation $(p\,q\,r)$ over a three element set $\{p, q, r\}$ and that maps y onto the transposition $(p\,q)(r)$. The application α extends into a morphism from F onto $\mathcal{S}_3$, the symmetric group over three elements. The kernel of α is a recognizable subset of F. It is also the result of an automaton $\mathcal{A}$ represented[2] below that is obtained from the very definition of α. It is convenient to give also the matrix representation of $\mathcal{A}$.



$$I = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \quad E = \begin{pmatrix} 0 & x+y+\bar{y} & \bar{x} \\ \bar{x}+y+\bar{y} & 0 & x \\ x & \bar{x} & y+\bar{y} \end{pmatrix} \quad T = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

Fig. 1. The automaton $\mathcal{A}$ and its matrix representation

Let us take the following notations:

$$\mathbb{Z}_x = 1_{\mathbb{Z}_x} + U + V + W \qquad \text{and} \qquad \mathbb{Z}_y = 1_{\mathbb{Z}_y} + X + Y$$

with

$$U = \{x^n \mid n \equiv 0 \pmod 3 \text{ and } n \neq 0\},$$

$$V = \{x^n \mid n \equiv 1 \pmod 3\} \quad \text{and} \quad W = \{x^n \mid n \equiv 2 \pmod 3\}$$

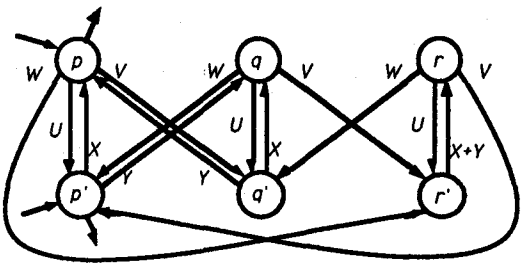
on one hand and, on the other hand,

$$X = \{y^n \mid n \equiv 0 \pmod 2 \text{ and } n \neq 0\} \quad \text{and} \quad Y = \{y^n \mid n \equiv 1 \pmod 2\}.$$

[2] with the convention that an arrow (p, x, q) represents at the same time a transition $(q, \bar{x}, p)$

for $n \in \mathbb{Z}$ and with the convention that $x^n = \bar{x}^{-n}$ for a negative n.

Having done all computations (as they are presented in [13]), it comes that a *deterministic, complete, and proper bipartite automaton* equivalent to $\mathcal{A}$ is the one represented in Figure 2.



$$I' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} \quad E' = \begin{pmatrix} & & & U & V & W \\ & 0 & & W & U & V \\ & & & V & W & U \\ X & Y & 0 & & & \\ Y & X & 0 & & 0 & \\ 0 & 0 & X+Y & & & \end{pmatrix} \quad T' = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

Fig. 2. A proper bipartite automaton equivalent to $\mathcal{A}$ and its matrix representation

It turns out that this bipartite automaton is *minimal*; its result is recognizable and nevertheless its labels are not all recognizable (U, X, and $X+Y$ are not recognizable).

We are now in a position to prove Theorem 6.

Proof of Theorem 6. Let R be a rational subset of $M*N$. From Proposition 2, R is the result of a finite proper bipartite automaton $\mathcal{A}$ that can be effectively computed from a rational expression, or from an automaton, that specifies R.

Since Rat M and Rat N are effective Boolean algebras, it is possible, from Proposition 3, to effectively compute a finite automaton $\mathcal{B}$, proper, deterministic, and complete, the result of which is again R. Since, from Proposition 1, the minimal bipartite automaton $\mathcal{A}_R$ is a homomorphic image of $\mathcal{B}$, it can be effectively computed by trying *all the possible partitions* of the set of states of $\mathcal{B}$ and by testing the equality of the result of these automata with R; this last test is effective by Theorem 5. It remains to test whether the labels of the minimal automaton are recognizable, which is decidable by hypothesis on M and N, and necessary for R being recognizable by Proposition 5. □

And this terminates the proof of Theorem 1.

Conclusion

For this decision problem on rational trace languages again the reference to properties of free products proved to be useful. (It may be noted that the original proof of Theorem 4 in [1] might also be reduced to closure properties of free products.) Let us add one remark.

The restriction of Theorem 6 to monoids without divisors of the identity is somewhat frustrating — eventhough the key result does not hold anymore without this hypothesis. The free group on two generators F of our Example 1 is the free product of two copies of $\mathbb{Z}$. And it is known that it is decidable whether a rational subset of F is recognizable ([14]). The problem of generalizing Theorem 6 to a larger class of monoids is thus open.

Acknowledgements. The final version of this paper has been terminated while the author was visiting the Instituto de Matemática e Estatística of the Universidade de Saõ Paulo. It is a pleasure to express in the proceedings of a conference held in Saõ Paulo the warmest thanks for the friendly hospitality and the excellent working conditions the author was given there. An unknown and careful referee pointed out a mistake in a step of a former version of the proof of Proposition 5 and gave several advices to improve the presentation. Jean Berstel taught me how to include figures in Latex files.

References

1. IJ. J. Aalbersberg and H. J. Hoogeboom, Characterizations of the Decidability of Some Problems for Regular Trace Languages, *Math. Systems Theory* **20**, 1989, 1–19.
2. IJ. J. Aalbersberg and E. Welz, Trace languages defined by regular string languages, *RAIRO Inform. Théor.* **22**, 1986, 103–119.
3. A. Bertoni, G. Mauri and N. Sabadini, Unambiguous regular trace languages, in *Algebra, Combinatorics, and Logic in Computer Science* (J. Demetrovics, G. Katona, and A. Salomaa, eds), Col. Math. Soc. Janos Bolyay **42**, North Holland, 1985.
4. J. Berstel, *Transductions and Context-Free Languages*, Teubner, 1979.
5. S. Eilenberg, *Automata, Languages and Machines*, vol. A, Academic Press, 1974.
6. C. C. Elgot and J. E. Mezei, On relations defined by generalized finite automata, *IBM J. Res. and Develop.* **9**, 1965, 47–68.
7. M. P. Flé et G. Roucairol, Maximal serializability of iterated transactions, *Theoret. Comput. Sci.* **38**, 1985, 1–16.
8. S. Ginsburg and E. Spanier, Bounded ALGOL-like Languages, *Trans. Amer. Math. Soc.* **113**, 1964, 333–368.
9. S. Ginsburg and E. Spanier, Semigroups, Presburger formulas and languages, *Pacif. J. Math.* **16**, 1966, 285–296.
10. O. Ibarra, Reversal-Bounded Multicounter Machines and their Decisions Problems, *J. Assoc. Comp. Machinery* **25**, 1978, 116–133.
11. L. P. Lisovik, The identity problem for regular events over the direct product of free and cyclic semigroups (in Ukrainian) *Dok. Akad. Nauk Ukraiinskoj RSR ser. A* **6**, 1979, 410–413. [translation in English by Andreas Weber, manuscript].
12. A. Mazurkiewicz, Trace theory, in *Petri Nets, Applications and Relationship to other Models of Concurrency*, L. N. C. S. **255**, 1987, 279–324.
13. J. Sakarovitch, On regular trace languages, *Theoret. Comput. Sci.* **52**, 1987, 59–75.
14. G. Sénizergues, Solution of a conjecture about rational subsets of a free group, to appear in *Acta Informatica*.

This article was processed using the LaTeX macro package with LMAMULT style