Bull. Austral. Math. Soc. 20M
Vol. 38 (1988) [421–431]

A TOPOLOGICAL APPROACH TO A CONJECTURE OF RHODES

J.E. Pin

The "type II conjecture", proposed by J. Rhodes, gives an algorithm to compute the kernel of a given finite semigroup. We show that this conjecture is a consequence of another conjecture, of a topological nature. This new conjecture gives a simple and effective characterisation of the recognisable subsets of a free monoid that are closed in the finite group topology for the free monoid.

In this paper, all semigroups (respectively monoids, groups) are finite except in the case of free monoids or free groups.

Recently, Rhodes has offered $100 for the solution of his "type II conjecture" [**15**], which gives an algorithm to compute the "kernel" of a semigroup. This conjecture implies in particular that if a (pseudo) variety of finite monoids is decidable, then the Malcev product of this variety by the variety of all groups is also decidable. This general statement contains as particular cases the important results of Ash [**1**] (every semigroup with commuting idempotents divides a finite inverse semigroup), Birget, Margolis and Rhodes [**2**, **3**] (every semigroup whose idempotents form a subsemigroup divides an orthodox semigroup) and others. We refer the reader to the survery article [**11**] or to [**2**, **3**, **15**, **16**, **18**] for a detailed discussion of this problem.

The aim of this article is to show that the Rhodes conjecture is a consequence of another conjecture, of a topological nature. Let A^* be the free monoid on a finite set A. The "finite group topology" on A^* is the coarsest topology such that all monoid morphisms from A^* into a finite discrete group are continuous. The "topological conjecture" gives a simple and effective characterisation of the recognisable subsets of A^* that are closed for this topology. This conjecture and its consequences in language theory are discussed in more detail in [**12**].

Only particular cases of both conjectures have been proved so far, but research is still very active. However, even if the Rhodes conjecture can be proved directly, the topological approach will remain interesting, in particular for extensions of the problem to Malcev products of a variety by certain varieties of groups, such as solvable groups, nilpotent groups or p-groups.

Received 17 February 1988
This work was supported by the PRC Matématiques et Informatique.

1. Terminology and notations

If S is a semigroup, S^1 denotes the monoid equal to S if S has an identity and to $S \cup \{1\}$, where 1 is a new identity, if S has no identity.

A *(pseudo) variety of semigroups* is a class of semigroups closed under taking subsemigroups, quotients (that is, homomorphic images) and finite direct products. *Varieties of monoids* are defined similarly. For instance, $\mathbf{G}$ denotes the variety of monoids consisting of all groups. A variety $\mathbf{V}$ is said to be *decidable* if there is an algorithm to decide whether or not a given semigroup (or monoid) belongs to $\mathbf{V}$. A semigroup S is "given" either by its multiplication table or as a transformation semigroup, generated by a set of transformations on a finite set. We refer the reader to [**4**, **6**, **9**] for results concerning varieties of semigroups.

Let S and T be two semigroups. A *relational morphism* $\tau: S \to T$ is a function τ from S into the subsets of T such that

(a) $(\forall s)(s\tau \neq \emptyset)$,
(b) $(\forall s, t \in S)((s\tau)(t\tau) \subseteq (st)\tau)$.

If $\tau: S \to T$ is a relational morphism, then there exist a semigroup R, a surjective morphism $\alpha: R \to S$ and a morphism $\beta: R \to T$ such that $\tau = \alpha^{-1}\beta$. Other properties of rational morphisms are discussed for instance in [**8**, **17**].

Let $\mathbf{V}$ be a variety of semigroups. The Malcev product $\mathbf{V}^{-1}\mathbf{G}$ is the variety of semigroups generated by all semigroups S such that there exists a morphism $\pi: S \to G$ into a group G satisfying $1\pi^{-1} \in \mathbf{V}$. Equivalently $\mathbf{V}^{-1}\mathbf{G}$ is the variety of all semigroups such that there is a relational morphism $\tau: S \to G$ into a group G satisfying $1\tau^{-1} \in \mathbf{V}$.

Let A be a finite set, called the alphabet. We denote by A^* the free monoid over A. The elements of A^* are *words*, and the subsets of A^* are called *languages*. The product of two words u and v is simply denoted by uv. The *length* of a word u is denoted by $|u|$. In particular, the empty word, denoted by 1, is the only word of length 0. If L is a language, L^+ (respectively L^*) denotes the subsemigroup (respectively submonoid) of A^* generated by L. In particular, if u is a word, we set $u^0 = 1$, and for every $n \geqslant 0$, $u^{n+1} = uu^n$, and

$$u^+ = \{u^n \mid n > 0\} \text{ and } u^* = \{u^n \mid n \geqslant 0\}.$$

A language L is *recognisable* (or *regular*) if there exists a monoid morphism $\pi: A^* \to M$ into a monoid M, and a subset P of M such that $L = P\pi^{-1}$. We say in this case that M *recognises* L. If a language L is recognisable, every monoid that recognises L is divided by the *syntactic monoid* of L, defined as follows. The *syntactic congruence* of L is the equivalence $\sim_L$ defined by

$$(u \sim_L v) \iff ((\forall x, y \in A^*), (xuy \in L \iff xvy \in L)).$$

https://doi.org/10.1017/S0004972700027805 Published online by Cambridge University Press

The quotient $M(L) = A^*/\sim_L$ is the syntactic monoid of L, and the natural morphism $\eta\colon A^* \to M(L)$ is called the *syntactic morphism.*. Note that $L = L\eta\eta^{-1}$, so that a recognisable language can be completely described by the pair $(\eta, L\eta)$, that is, by a finite set. Equivalent descriptions of recognisable languages can be given with the help of finite automata or rational expressions. Note that there are some well-known algorithms to pass from one description to another. See [**4**, **6**, **9**] for more details.

Let M be a monoid. A *(context-free) grammar* on M is a triple $\mathcal{G} = (\Sigma, P, \xi_0)$ where Σ is a finite alphabet, ξ_0 is an element of Σ, and P is a subset of $\Sigma \times (M \cup \Sigma)^*$. The elements of P are called the *productions* of the grammar and are usually written in the form $\xi \to u$, where $\xi \in \Sigma$ and $u \in (M \cup \Sigma)^*$. Such a production should be considered as a rewriting rule in the free monoid $(M \cup \Sigma)^*$, which allows the replacement of every occurrence of ξ by the word u. Let $v, w \in (M \cup \Sigma)^*$. We say there is a *direct derivation* from v to w, denoted $v \to w$, if there are two factorisations $v = x\xi y$ and $w = xuy$ such that $x, y \in (M \cup \Sigma)^*$ and $\xi \to u$ is a production of the grammar. We say there is a *derivation* from v to w, denoted $v \mapsto w$, if there exists a finite sequence $v = v_0, v_1, \dots, v_n = w$ such that for $0 \leqslant i \leqslant n-1$, $v_i \to v_{i+1}$. The subset of M^* generated by the grammar is the set

$$L(\mathcal{G}) = \{w \in M^* \mid \text{there is a derivation } \xi_0 \mapsto w\}.$$

Let $\pi\colon M^* \to M$ be the natural morphism defined by $m\pi = m$ for every $m \in M$. Then every word of M^* defines a unique element $m\pi$ of M. The subset of M generated by the grammar is the set

$$S(\mathcal{G}) = \{w\pi \in M \mid \text{there is a derivation } \xi_0 \mapsto w\}.$$

2. The Rhodes conjecutre

Let S be a semigroup. The *kernel* of S is the subsemigroup

$$K(S) = \cap 1\tau^{-1}$$

where the intersection is taken over all relational morphisms τ from S into a group G. The kernel (called "type II" by Rhodes) is related to the Malcev product by the following proposition (see [**16**, **11**] for a proof).

Proposition 2.1. *Let* $\mathbf{V}$ *be a variety of semigroups and let* S *be a semigroup. Then* S *belongs to* $\mathbf{V}^{-1}\mathbf{G}$ *if and only if* $K(S)$ *belongs to* $\mathbf{V}$.

Corollary 2.2. *If there is an algorithm to compute the kernel of a semigroup, then, for every decidable variety of semigroups* $\mathbf{V}$, *the Malcev product* $\mathbf{V}^{-1}G$ *is decidable.*

The main problem is that it is not clear whether or not there is an algorithm to compute the kernel of a given semigroup S. Since $K(S) = S \cap K(S^1)$, it would

https://doi.org/10.1017/S0004972700027805 Published online by Cambridge University Press

suffice to produce an algorithm when S is a monoid. Rhodes has conjectured that such an algorithm exists. More precisely, we define for each monoid M an effectively computable submonoid $D(M)$ as follows.

DEFINITION: $D(M)$ is the smallest submonoid of M closed under "weak conjugation": for every $s, t \in M$ such that either $sts = s$ or $tst = t$, the condition $u \in D(M)$ implies $sut \in D(M)$.

We can now state the "type II conjecture", for the solution of which Rhodes has offered $100 [**14**].

Rhodes conjecture.

(a) (weak form) The exists an algorithm to compute the kernel of a given monoid.

(b) (strong form) For every monoid M, $K(M)$ is equal to $D(M)$.

The following theorems summarise the known properties of $D(M)$. (See [**1**, **2**, **3**, **11**, **16**, **18**] for more details).

THEOREM 2.3. [**16**, **18**]

(a) *$D(M)$ is a submonoid of $K(M)$ containing the idempotents of M.*

(b) *A regular element $r \in M$ belongs to $K(M)$ if and only if it belongs to $D(M)$.*

THEOREM 2.4. [**2**, **3**] *The Rhodes conjecture holds true when the set $E(M)$ of idempotents of M form a submonoid of M. In this case $D(M) = K(M) = E(M)$.*

3. A TOPOLOGY OF THE FREE MONOID

In this section, we present our main conjecture, which is related to a topology of the free monoid. This topology was introduced by Hall for the free group [**5**] and by Reutenauer [**13**] for the free monoid. We refer the interested reader to [**14**] for an extensive study of this topology.

Let A^* be the free monoid on a finite set A. We say that a (finite) group G *separates* two words u and v if there exists a monoid morphism $\varphi : A^* \to G$ such that $u\varphi \neq v\varphi$. One can show that distinct words can always be separated by a group. Given two words u and v, set

$$r(u, v) = \min\{\text{Card } G \mid G \text{ is finite group that separates } u \text{ and } v\},$$

and

$$d(u, v) = 2^{-r(u,v)}.$$

https://doi.org/10.1017/S0004972700027805 Published online by Cambridge University Press

Then d is a linear, ultrametric distance; that is, d satisfies the following properties: for every $u, v, w \in A^*$:

$$\begin{aligned}
&(1) \quad d(u, v) = d(v, u),\\
&(2) \quad (d(u, v) = 0) \iff (u = v),\\
&(3) \quad d(u, w) \leqslant \max(d(u, v), d(v, w)),\\
&(4) \quad d(wu, wv) = d(u,v) = d(uw, vw).
\end{aligned}$$

One can show that the multiplication is continuous for the topology defined by d, which is also the coarsest topology on A^* such that all the monoid morphisms from A^* into a (finite) discrete group are continuous. In particular, general results of topology imply the following result, where $\overline{L}$ denotes the topological closure of a set L.

LEMMA 3.1. *Let L be a subset of A^*. Then a word u belongs to $\overline{L}$ if and only if $u\varphi \in L\varphi$ for every monoid morphism $\varphi: A^* \to G$ into a group G.*

Let L be a recognisable subset of A^*. We denote by $\eta : A^* \to M(L)$ the syntactic morphism of L and we set $P = L\eta$. The following result is proved in [**8**, **12**].

THEOREM 3.2. *If L is closed, then L satisfies the condition $(*)$ below:*

$$(*) \qquad (\forall s, t \in M(L))(\forall e \in M(L),\ e^2 = e)(set \in P \Rightarrow st \in P)$$

Whether the converse of this theorem holds is unknown. However, we make the following conjecture.

TOPOLOGICAL CONJECTURE. *Let L be a recognisable subset of A^*. If L satisfies condition (*), then L is closed.*

For any subset L of A^*, we set

$$F(L) = \{v \in A^* \mid (\exists x, y, u \in A^*)(v = xy) \text{ and } xu^+y \subseteq L\}$$

One can show that $F(L)$ is a recognisable language containing L. The operator F can be iterated by setting, for every $n > 0$, $F^{(0)}(L) = L$ and $F^{n+1}(L) = F(F^n(L))$. Finally, set $F^*(L) = \bigcup_{n \geqslant 0} F^n(L)$. The following results are proved in [**12**].

THEOREM 3.3.

(a) *For every recognisable language L, $F^*(L)$ is a recognisable language and, given L, there is an algorithm to compute $F^*(L)$.*

(b) *If the topological conjecture holds true, then, for every recognisable language L, the topological closure $\overline{L}$ of L is equal to $F^*(L)$.*

THEOREM 3.4. *The topological conjecture is true in the following two particular cases:*

(a) *if L is a submonoid of A^* or*

(b) *if the idempotents of $M(L)$ commute.*

https://doi.org/10.1017/S0004972700027805 Published online by Cambridge University Press

4.4 Main result.

The aim of this section is to analyse the relations between the Rhodes conjecture and the topological conjecture. These connections are based on the following result. Let M be a monoid. Since M is finite, one can find effectively a finite set A (for instance $A = M$) and a surjective morphism $\pi\colon A^* \to M$ (for instance the morphism defined by $a\pi = a$ for every a in M). Then we have:

Proposition 4.1. *Let $m \in M$. Then $(m \in K(M)) \iff \left(1 \in \overline{(m\pi^{-1})}\right)$.*

Proof: First assume that $m \in K(M)$ and let $\varphi\colon A^* \to G$ be a monoid morphism from A^* into a group G. Then $\tau = \pi^{-1}\varphi$ is a relational morphism from M into G, so that $m \in 1\tau^{-1}$ by definition of $K(M)$. It follows that $1 \in m\tau$ and thus $1\varphi \in (m\pi^{-1})\varphi$. But this property holds for every morphism $\varphi\colon A^* \to G$ from A^* into a group G, and hence $1 \in \overline{(m\pi^{-1})}$ by Lemma 3.1.

Conversely, assume that $1 \in \overline{(m\pi^{-1})}$ and let $\tau\colon M \to G$ be a relational morphism from M into a group G. The general properties of relational morphisms imply that there exist a monoid N, a surjective morphism $\alpha\colon N \to M$ and a morphism $\beta\colon N \to G$ such that $\tau = \alpha^{-1}\beta$. Now, by the universal property of the free monoid, there exists a morphism- $\gamma\colon A^* \to N$ such that the following diagram commutes:

$$\begin{tikzcd}
A^* \arrow[dr, "\gamma"] \arrow[dd, "\pi"'] & & \\
& N \arrow[dl, "\alpha"'] \arrow[dr, "\beta"] & \\
M \arrow[rr, "\tau"] & & G
\end{tikzcd}$$

Now, since $1 \in \overline{(m\pi^{-1})}$, we have $1 = 1\gamma\beta \in (m\pi^{-1})\gamma\beta$ by Lemma 3.1. Therefore, there exists a word $u \in A^*$ such that $u\pi = m$ and $u\gamma\beta = 1$. Set $n = u\gamma$. Then $n\alpha = m$ since $\gamma\alpha = \pi$ and $n\beta = 1$. Therefore $m \in 1\tau^{-1}$ and $m \in K(M)$. ∎

Corollary 4.2. *If the topological conjecture is true, then there is an alogorithm to compute the kernel of a given monoid.*

Proof: By Proposition 4.1, $m \in K(M)$ if and only if $1 \in \overline{(m\pi^{-1})}$. But $m\pi^{-1}$ is a recognisable language of A^* that can be effectively constructed and Theorem 3.2 gives an algorithm to compute $\overline{(m\pi^{-1})}$. Now, one can decide effectively whether a given word belongs to a given recognisable language. Thus the property $1 \in \overline{(m\pi^{-1})}$ is decidable, and so is the property $m \in K(M)$. ∎

Corollary 4.2 shows that the topological conjecture implies the weak form of the Rhodes conjecture. In fact, it also implies the strong form.

https://doi.org/10.1017/S0004972700027805 Published online by Cambridge University Press

THEOREM 4.3. *If the topological conjecture is true, then $K(M) = D(M)$ for any monoid M.*

The proof of Theorem 4.3, which is rather long, uses ideas borrowed from the theory of context-free languages. We first need a new definition of $D(M)$, which is more convenient for the proofs.

DEFINITION: $D(M)$ is the subset of M generated by the grammar $\mathcal{G} = (\{\xi\}, \xi, P)$ whose productions are:

(1) $\xi \to 1$,
(2) $\xi \to \xi\xi$,
(3) $(\forall s, t \in M)$ $(sts = s) \Rightarrow (\xi \to s\xi t)$,
(4) $(\forall s, t \in M)$ $(tst = t) \Rightarrow (\xi \to s\xi t)$.

We first prove a technical property of the grammar $\mathcal{G}$. Let ω be an integer such that, for every $m \in M$, m^ω is idempotent.

LEMMA 4.4. *Let s be a word of A^* and let $v = s^{3\omega}$. Then for every $q \geqslant 0$ and for every factorisation $v^q = v_0v_1 \dots v_p$ with $p \leqslant q$, there exists a derivation*

$$\xi \mapsto (v_0\pi)\xi(v_1\pi)\xi \dots \xi(v_p\pi).$$

PROOF: By induction on q. If $q = 0$ or $s = 1$, then $v^q = 1$ and $\xi \to 1$ by definition. Thus we may assume $s \neq 1$ and $q > 0$. If suffices to prove the result for $p = q$. Indeed, if $v = v_0 \dots v_p$, we also have $v = v_0 \dots v_pv_{p+1} \dots v_q$, where $v_{p+1} = \dots = v_q = 1$. Therefore, if the lemma is proved for $p = q$, there is a derivation

$$\xi \mapsto (v_0\pi)\xi(v_1\pi)\xi \dots \xi(v_p\pi)\xi 1 \dots 1\xi 1$$

and hence a derivation

$$\xi \mapsto (v_0\pi)\xi(v_1\pi)\xi \dots \xi(v_p\pi)$$

since $\xi \to 1$.

We claim that there exists $i \leqslant p$ such that

(a) $$|v_{i-1}v_i| \geqslant |v|$$

and

(b) $$|v_{i-1}| < |v| \text{ or } |v_i| < |v|.$$

The claim certainly holds if $|v_{i-1}| \geqslant |v|$ and $|v_i| < |v|$ for some i, or dually, if $|v_{i-1}| < |v|$ and $|v_i| \geqslant |v|$ for some i. Otherwise, two cases are possible. Either $|v_i| \geqslant |v|$

for every i or $|v_i| < |v|$ for every i. The first case leads to a contradiction since $q\,|v| = |v^q| = |v_0 \dots v_q|$. In the second case, condition (b) is clearly satisfied. If condition (a) is not satisfied, we would have

$$|v_0 v_1| < |v|,\, |v_2| \leqslant |v_1 v_2| < |v|, \dots, |v_q| \leqslant |v_{q-1} v_q| < |v|,$$

and hence $|v^q| = |v_0 \dots v_q| < q\,|v|$, a contradiction. Therefore the claim holds true and we may assume there is an index i such that $|v_{i-1}v_i| \geqslant |v|$ and $|v_{i-1}| < |v|$ (the case $|v_i| < |v|$ would be similar). Set $v_i = v_i' v_i''$ where $|v_{i-1}v_i'| = |v|$. Then we have

$$v_0 v_1 \dots v_{i-2} v_i'' v_{i+1} \dots v_q = v^{q-1}$$

and by induction, there is a derivation

$$\xi \mapsto (v_0\pi)\xi(v_1\pi)\xi \dots \xi(v_{i-2}\pi)\xi(v_i''\pi)\xi(v_{i+1}\pi)\xi \dots \xi(v_q\pi). \tag{1}$$

Furthermore, the word $v_{i-1}v_i'$ is a conjugate of $v = s^{3\omega}$ and hence $v_{i-1}v_i' = xs^{2\omega}z$ for some words x and z such that $zx = s^\omega$. It follows that either xs^ω is a left factor of v_{i-1} of $s^\omega z$ is a right factor of v_i'. Suppose for instance $v_{i-1} = xs^\omega y$, so that $yv_i'x = s^{2\omega}$. Then $(v_{i-1}v_i'v_{i-1})\pi = (xs^\omega yv_i'xs^\omega y)\pi = \left(xs^{4\omega}y\right)\pi = (xs^\omega y)\pi = v_{i-1}\pi$. Similarly, if $v_i' = ys^\omega z$ and $zv_{i-1}y = x^{2\omega}$, a similar argument shows that $(v_i'\pi)(v_{i-1}\pi)(v_i'\pi) = (v_i'\pi)$. In both cases there is a derivation $\xi \rightarrow (v_{i-1}\pi)\xi(v_i'\pi)$. Therefore, we have by (1).

$$\begin{aligned}\xi &\mapsto (v_0\pi)\xi(v_1\pi)\xi \dots \xi(v_{i-2}\pi)\xi\xi(v_i''\pi)\xi(v_{i+1}\pi)\xi \dots \xi(v_q\pi)\\ &\rightarrow (v_0\pi)\xi(v_1\pi)\xi \dots \xi(v_{i-2}\pi)\xi(v_{i-1}\pi)\xi(v_i'\pi)(v_i''\pi)\xi(v_{i+1}\pi)\xi \dots \xi(v_q\pi)\end{aligned}$$

and this proves the lemma since $v_i\pi = (v_i'\pi)(v_i''\pi)$. ∎

We come back to the proof of Theorem 4.3. Assume that the topological conjecture is true. By Proposition 2.3, $D(M)$ is contained in $K(M)$, and hence it suffices to show that $K(M)$ is contained in $D(M)$. Let $m \in K(M)$. Theorems 4.1 and 3.3 show that $1 \in F^*(L)$ where $L = m\pi^{-1}$. Therefore, there exists $n > 0$ such that $1 \in F^n(L)$. We now construct, by induction on i, a sequence $u_0 \dots, u_n$ of words such that $u_i \in F^{(n-i)}(L)$ as follows.

(a) $u_0 = 1$.

(b) Let $u_i \in F^{(n-i)}(L) = F\left(F^{(n-i-1)}(L)\right)$. By the definition of F, there exist some words r_i, s_i, $t_i \in A^*$ such that $u_i = r_i t_i$ and $r_i s_i^+ t_i \subseteq F^{(n-i-1)}(L)$. Then we put $u_{i+1} = r_i s_i^{3(n-i)\omega} t_i$, so that

$$u_{i+1} \in F^{(n-i-1)}(L).$$

Furthermore $u_n \in F^{(0)}(L) = L$ and hence $u_n\pi = m$ by the definition of L.

We shall prove that there is a derivation $\xi \mapsto u_n\pi = m$, as a consequence of the following lemma.

https://doi.org/10.1017/S0004972700027805 Published online by Cambridge University Press

Lemma 4.5. *For* $0 \leqslant i \leqslant n$, *and for every factorisation* $u_i = u_{i,0} \ldots u_{i,k}$ *with* $k \leqslant n - i + 1$, *there exists a derivation* $\xi \mapsto (u_{i,0}\pi)\xi(u_{i,1}\pi)\xi \ldots \xi(u_{i,k}\pi)$.

Proof: By induction on i. If $i = 0$, then $u_0 = 1$ and there is clearly a derivation $\xi \mapsto 1\xi 1 \ldots \xi 1$. Let $u_{i+1} = r_i s_i^{3(n-i)\omega} t_i = u_{i,0} \ldots u_{i,k}$ be a factorisation of u_{i+1} with $k \leqslant n - i$. Then there exist two indices $c \leqslant d$ such that the occurrence of $s_i^{3(n-i)\omega}$ defined by the factorisation

$$u_{i+1} = (r_i)\left(s_i^{3(n-i)\omega}\right)(t_i)$$

is a factor of $u_{i,c} \ldots u_{i,d}$. We may suppose that c (respectively d) is maximal (respectively minimal) for this property. Therefore there is a left factor x of $u_{i,c}$ and a right factor y of $u_{i,d}$ such that

$$u_{i,c} \ldots u_{i,d} = x s_i^{3(n-i)\omega} y.$$

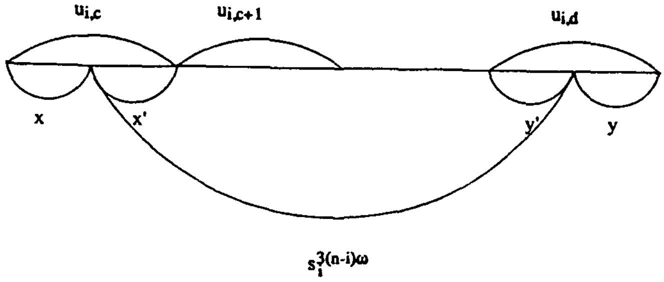
Note that we may have $c = d$.

Consider the factorisation $u_i = r_i t_i = u_{i,0} \ldots u_{i,c-1} x y u_{i,d+1} \ldots u_k$ which contains at most $k + 1 \leqslant n - i + 2$ factors. By the induction hypothesis, there is a derivation

$$\xi \mapsto (u_{i,0}\pi)\xi \ldots \xi(u_{i,c-1}\pi)\xi(x\pi)\xi(y\pi)(u_{i,d+1}\pi) \ldots \xi(u_{i,k}\pi).$$

Now, the factorisation $u_{i,c} \ldots u_{i,d}$ induces a factorisation of $s_i^{3(n-i)\omega}$ represented on one of the following diagrams.

If $c < d$, then $s_i^{3(n-i)\omega} = x' u_{i,c+1} \ldots u_{i,d-1} y'$:

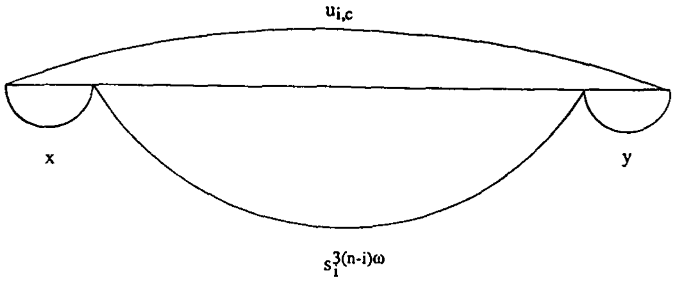


If $c = d$, then the factorisation is trivial: $s_i^{3(n-i)\omega} = s_i^{3(n-i)\omega}$.

In the first case, the factorisation contains at most $(n - i + 1)$ factors and by Lemma 4.4, there exists a derivation

$$\xi \mapsto (x'\pi)\xi \ldots \xi(u_{i,c+1}\pi)\xi \ldots \xi(u_{i,d-1}\pi)\xi(y'\pi).$$

https://doi.org/10.1017/S0004972700027805 Published online by Cambridge University Press



It follows that

$$\xi \mapsto (u_{i,0}\pi)\xi \dots (u_{i,c-1}\pi)\xi(x\pi)(x'\pi)\xi(u_{i,c+1}\pi)\dots$$
$$(u_{i,d-1}\pi)\xi(y\pi)(y'\pi)\xi(u_{i,d+1}\pi)\dots\xi(u_{i,k}\pi)$$

and this concludes the proof since $xx' = u_{i,c}$ and $y'y = u_{i,d}$.

The second case is even simpler. Indeed we have $\xi \mapsto s_i^{3(n-i)\omega}\pi$ whence

$$(x\pi)\xi(y\pi) \mapsto (x\pi)\left(s_i^{3(n-i)\omega}\pi\right)(y\pi) = u_{i,c}\pi$$

and $\xi \mapsto (u_{i,0}\pi)\xi\dots\xi(u_{i,k}\pi)$. ∎

We can now conclude the proof of Theorem 4.3. Indeed, if we apply Lemma 4.5 to the factorisation $u_n = u_n$, we have a derivation $\xi \mapsto u_n\pi = m$. ∎

References

[1] C.J. Ash, 'Finite semigroups with commuting idempotents', *J. Austral. Math. Soc. (Series A)* **43** (1987), 81–90.

[2] J.C. Birget, S.W. Margolic and J. Rhodes, 'Finite semigroups whose idempotents commute or form a subsemigroup', in *Semigroups and Their Applications*, edited by S.M. Goberstein and P.M. Higgins (Reidel, Dordrecht, 1987). pp. 25–35.

[3] J.C. Birget, S.W. Margolic and J. Rhodes, 'Finite semigroups whose idempotents form a semilattice or a band' (to appear).

[4] S. Eilenberg, *Automata, Languages and Machines* (Academic Press, New York, Vol A. 1974; Vol. B 1976).

[5] M. Hall Jr, 'A topology for free groups and related groups', *Ann. of Maths.* **52** (1950), 127–139.

[6] G. Lallement, *Semigroups and Combinatorial Applications* (Wiley, New York, 1979).

[7] S.W. Margolic and J.E. Pin, 'Varieties of finite monoids and topology for the free monoid', in *Proceedings of the Marquette Semigroup Conference*, 1984. pp. 113–130.

[8] J.E. Pin, 'Finite group topology and p-adic topology for free monoids', in *12th ICALP, Lecture Notes in Computer Science 199* (Springer, Berlin, 1985). pp. 285–299.

[9] J.E. Pin, *Varieties of formal languages* (North Oxford Academic, London and Plenum, New York, 1986).

[10] J.E. Pin, 'On the languages recognized by finite reversible automat', in *14th ICALP, Lecture Notes in Computer Science 267* (Springer, Berlin, 1987). pp. 237–249.

[11] J.E. Pin, 'On a conjecture of Rhodes', (survey paper). (toappear) .

[12] J.E. Pin, 'Topologies for the free monoid' (to appear).

[13] Ch. Reutenauer, 'Une topologie du monoïde libre', *Semigroup Forum* **18** (1979), 33–49.

[14] Ch. Reutenauer, 'Une topologie du monoïde libe', Sur mon article, *Semigroup Forum* **22** (1981), 93–95.

[15] J. Rhodes, 'New techniques in global semigroup theory', in *Semigroups and Their Applications*, edited by S.M. Goberstein and P.M. Higgins (Reidel, Dordrecht, 1987). pp. 169–181.

[16] B. Tilson and J. Rhodes, 'Improved lower bounds for the complexity of finite semigroups', *J. Pure Appl. Algebra* **2** (1972), 13–71.

[17] B. Tilson, Chapters 11 and 12 of [4].

[18] B. Tilson, 'Type II redux', in *Semigroups and Their Applications*, edited by S.M. Goberstein and P.M. Higgine (Reidel, Dordrecht, 1987). pp. 201–205.

L.I.T.P.
Tour 55-65
Université Paris VI
75252 Paris, Cedex 05
France

https://doi.org/10.1017/S0004972700027805 Published online by Cambridge University Press