BULL. AUSTRAL. MATH. SOC. 20M07
VOL. 41 (1990) [161–184]

# SEMIGROUPS WHOSE IDEMPOTENTS FORM A SUBSEMIGROUP

JEAN-CAMILLE BIRGET, STUART MARGOLIS
AND JOHN RHODES

We prove that if the "type-II-construct" subsemigroup of a finite semigroup $S$ is regular, then the "type-II" subsemigroup of $S$ is computable (actually in this case, type-II and type-II-construct are equal). This, together with certain older results about pseudo-varieties of finite semigroups, leads to further results:

(1) We get a new proof of Ash's theorem: If the idempotents in a finite semigroup $S$ commute, then $S$ divides a finite inverse semigroup. Equivalently: The pseudo-variety generated by the finite inverse semigroups consists of those finite semigroups whose idempotents commute.

(2) We prove: If the idempotents of a finite semigroup $S$ form a subsemigroup then $S$ divides a finite orthodox semigroup. Equivalently: The pseudo-variety generated by the finite orthodox semigroups consists of those finite semigroups whose idempotents form a subsemigroup.

(3) We prove: The union of all the subgroups of a semigroup $S$ forms a subsemigroup if and only if $S$ belongs to the pseudo-variety $\mathcal{UG} * G$ if and only if $S_{II}$ belongs to $\mathcal{UG}$. Here $\mathcal{UG}$ denotes the pseudo-variety of finite semigroups which are unions of groups.

For these three classes of semigroups, type-$II$ is equal to type-$II$ construct.

## 1. INTRODUCTION

In this paper we simplify the new techniques of Ash ([**1**, **2**]) and combine them with Rhodes' and Tilson's ideas ([**21**, **23**]) concerning the "type-$II$" subsemigroup of a finite semigroup. This leads to Theorem 3.1 which shows how to compute the type $II$ subsemigroup $S_{II}$ of a finite semigroup $S$, if the "type-$II$-construct" subsemigroup $S_c$ of $S$ is regular. With this assumption, $S_{II}$ is equal to $S_c$. In the general case (where $S$ is any finite semigroup) it is still unknown whether $S_{II}$ is computable from $S$ (see [**11**, **19**, **21**]). A stronger question is whether $S_{II}$ is equal to $S_c$ (the "type-$II$-construct" subsemigroup of $S$, constructed from the idempotents of $S$ via "weak conjugation" - -see Section 2 for exact definitions). Next, we combine our Theorem 3.1 with results about the variety generated by the finite inverse semigroups (Margolis and Pin [14,

Received 3 March 1989
The research of the first author was supported by National Science Foundation grant DMS 8702019 and the research of the third author was supported by National Science Foundation grant DMS 8502367.

**15, 16**], who use Simon's lemma [**22**]), and about the variety generated by the finite orthodox semigroups (Thérien [**25**]). This leads to the following results:

(1) We give a new proof of Ash's theorem [**1, 2**]: If $S$ is a finite semigroup whose idempotents commute then $S$ divides a finite inverse semigroup.

(2) We prove: If $S$ is a finite semigroup whose idempotents form a subsemigroup then $S$ divides a finite orthodox semigroup.

(The two last results, and essentially the same proof technique, were already presented in [**3**]).

(3) We prove: The union of all the subgroups of a semigroup $S$ forms a subsemigroup if and only if $S$ belongs to the pseudo variety $\mathcal{UG} * \mathbf{G}$, if and only if $S_{II} \in \mathcal{UG}$.

For these three classes of semigroups, the "type-$II$" subsemigroup $S_{II}$ is equal to the "type-$II$-construct" subsemigroup.

A LITTLE BIT OF HISTORY.

The type-$II$ subsemigroups arose from Rhodes' complexity theory of finite semigroups, in the 1960's (see [**7**] and [**10**]). Since no techniques are known for computing the complexity of a semigroup (and in fact it is not known whether the complexity is computable at all), Rhodes and Tilson developed lower bounds, involving the type-$II$ subsemigroups $S_{II}$ and the "constructible type-$II$" subsemigroups $S_c$ (see [**21**]). The "type-$II$ conjectures" or "Rhodes conjectures" were first stated in [**11**]. Margolis [**13**] discovered that, in the case of a finite semigroup $S$ whose idempotents commute we have: $S$ divides a finite inverse semigroup if and only if $S_{II} = S_c = E(S)$. So he posed the following quesiton (which is equivalent to the strong type-$II$ conjecture "$S_{II} = ?S_c$" for this special class of semigroups): *Does a finite semigroup $S$ divide a finite inverse semigroup if and only if the idempotents of $S$ commute?* The detailed proof of this equivalence follows from Margolis' and Pin's work [**14, 15, 16**]. Margolis' question was answered affirmatively by Chris Ash [**1, 2**].

In [**3**] and in this paper we combine Ash's construction (in simplified form) and the older type-$II$ results of [**21**]; we also use some results on varieties, obtained by Margolis and Pin [**14, 15, 16**] (using Simon [**22**] and by Thérien [**25**] (further clarified by Tilson's derived categories [**24**].)

## 2. Relational morphisms into groups

All semigroups used in this paper are *finite* (except for free semigroups). A *pseudo-variety* (of finite semigroups) is a class of finite semigroups closed under finite direct product and under division. From now on we will use the word "*variety*" to mean "pseudo-variety". See for example [**7, 12, 18, 10**] for standard definitions and results. Tilson first demonstrated the usefulness of the following notion:

DEFINITION: A *relational morphism* between two semigroups $S$ and $T$ is a subsemigroup $\tau$ of $S \times T$ such that the projection of $\tau$ into $S$ is surjective. We denote the set of these by $R(S, T)$. Equivalently, a relational morphism $\tau$ from $S$ to $T$ is a relation $S \to T$ satisfying:

$$(\forall s \in S)(s\tau \neq \emptyset) \,\&\, (\forall s_1, s_2 \in S)((s_1\tau)(s_2\tau) \subseteq (s_1 s_2)\tau).$$

Notation: To express that $s(\in S)$ is related to $t(\in T)$ by $\tau$ we write "$(s,t) \in \tau$" or "$t \in s\tau$" or "$s \in (t)\tau^{-1}$"

DEFINITION: Let $\mathbf{V}$ and $\mathbf{W}$ be varieties and $\mathcal{F}$ the set of finite semigroups. We define

$$\mathbf{V}_e^{-1}\mathbf{W} = \{S \mid (S \in \mathcal{F}) \& (\exists T \in \mathbf{W}, \tau \in R(S,T)) \\ (\forall f = f^2 \in T)((f)\tau^{-1} \in \mathbf{V})\}$$

One can check easily that $\mathbf{V}_e^{-1}\mathbf{W}$ is a variety of finite semigroups.

DEFINITION: The *Malcev produce* $\mathbf{V}\mathbf{m}\mathbf{W}$ of the varieties $\mathbf{V}$ and $\mathbf{W}$ is

$$\{S \mid (S \in \mathcal{F}) \& (\exists T \in \mathbf{W}, \phi \in \mathrm{Mor}(S,T)) \\ (\forall f = f^2 \in T)((f)\phi^{-1} \in \mathbf{V})\}.$$

We will consider the variety of finite semigroups $(\mathbf{V}\,\mathbf{m}\,\mathbf{W})$ generated by $\mathbf{V}\,\mathbf{m}\,\mathbf{W}$. It turns out that the above two "products" of varieties are equivalent:

FACT 2.1. *For any varieties* $\mathbf{V}$ *and* $\mathbf{W}$ *of finite semigroups* $\mathbf{V}_e^{-1}\mathbf{W} = (\mathbf{V}\,\mathbf{m}\,\mathbf{W})$.

PROOF: [$\subseteq$] If $S \in \mathbf{V}_e^{-1}\mathbf{W}$ then there exists a relational morphism $\tau: S \to T$ with $T \in \mathbf{W}$ and $(\forall f = f^2 \in T): (f)\tau^{-1} \in \mathbf{V}$. We view $\tau$ as a subsemigroup of $S \times T$. Let $\alpha: \tau \to S$ be the projection of $\tau$ onto $S$, and let $\beta: \tau \to T$ be the projection of $\tau$ into $T$. Then we have $\tau = \alpha^{-1}\beta$ (composition of the inverse of $\alpha$, and $\beta$). If $f = f^2 \in T$ then $(f)\beta^{-1} = \{(s,f) \in S \times T \mid (s,f) \in \tau\} = (f)\tau^{-1}$. Moreover, by assumption, $(f)\tau^{-1} \in \mathbf{V}$. Therefore $(f)\beta^{-1} \in \mathbf{V}$, and thus $\tau \in (\mathbf{V}\,\mathbf{m}\,\mathbf{W})$. Since $(\mathbf{V}\,\mathbf{m}\,\mathbf{W})$ is closed under homomorphic images it follows that $S(= (\tau)\alpha)$ belongs to $(\mathbf{V}\,\mathbf{m}\,\mathbf{W})$.

[$\supseteq$] This is obvious, since every functional morphism $\phi$ is also a relational morphism. □

We will be interested in varieties of the form $(\mathbf{V}\,\mathbf{m}\,\mathbf{G})$ where $\mathbf{G}$ is the variety of all finite groups. Restating Fact 2.1 in the case of $(\mathbf{V}\,\mathbf{m}\,\mathbf{G})$, we get: $S \in (\mathbf{V}\,\mathbf{m}\,\mathbf{G})$ if and only if there exists a relational morphism $\tau: S \to G$ (for some finite group $G$, with identity element 1) such that $(1)\tau^{-1} \in \mathbf{V}$.

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

This motivates the following notion, which was introduced by Rhodes and Tilson [**21**] in the study of lower bounds for semigroup complexity.

DEFINITION: For any finite semigroup $S$, the *type-II subsemigroup* $S_{II}$ is $\{s \in S \mid (\forall G \in \mathbf{G})(\forall \tau \in R(S,G))\colon s \in (1)\tau^{-1}\}$

REMARK: If in the definition of $S_{II}$ the groups are allowed to be arbitrary (infinite) then $S_{II}$ is empty. The groups must at least be torsion.

FACT 2.2. *((1)-(4) are from* [**21**]*,*

(1) *$S_{II}$ is a subsemigroup of $S$.*

(2) *Every idempotent of $S$ belongs to $S_{II}$.*

(3) *If $s \in S_{II}$ and the elements $r$ and $x$ of $S$ satisfy $rxr = r$ (so $r$ is regular, but $x$ might be non-regular), then $rsx$ and $xsr$ also belong to $S_{II}$. (We say that $S_{II}$ is closed under "weak conjugation").*

(4) *There exists some finite group $G$ and a relational morphism $\tau\colon S \to G$ such that $S_{II} = (1)\tau^{-1}$.*

(5) *$S \in (\mathbf{V}\,\mathbf{m}\,\mathbf{G})$ if and only if $S_{II} \in \mathbf{V}$. (This connects $(\ldots\,\mathbf{m}\,\mathbf{G})$ and the type-II concept).*

PROOF: For (1), (2) and (3) see [**21**] and [**23**].

(4) For everye element $n \in S - S_{II}$ we can pick a finite group $G_n$ and a morphism $\tau_n\colon S \to G_n$ such that $n \notin (1)\tau_n^{-1}$. Let us take the finite direct product $\prod\{G_n \mid n \in S - S_{II}\} = \prod G_n$ and the relational morphism $\tau\colon S \to \prod G_n$ defined by

$$\tau = \{(s, (\ldots, g_n, \ldots)) \in S \times \prod G_n \mid (\forall n \in S - S_{II})((s, g_n) \in \tau_n)\}.$$

Then we have:
$(\forall n \in S - S_{II})\big(n \notin (1)\tau^{-1}\big)$, by the choice of $\tau_n$ and $\tau$. However, $(\forall s \in S_{II})\big(s \in (1)\tau^{-1}\big)$ by definition of $S_{II}$. Thus $S_{II}$ is precisely to $(1)\tau^{-1}$.

(5) $S \in (\mathbf{V}\,\mathbf{m}\,\mathbf{G})$ if and only if $(1)\tau^{-1} \in \mathbf{V}$ for some finite group $G$ with identity 1, and some relational morphism $\tau\colon S \to G$ (Fact 2.1). Certainly $S_{II} \leqslant (1)\tau^{-1}$, thus $S_{II} \in \mathbf{V}$ if $(1)\tau^{-1} \in \mathbf{V}$. Conversely, by (4), there exists $\tau\colon S \to G$ with $(1)\tau^{-1} = S_{II}$. If $S_{II} \in \mathbf{V}$ then $(1)\tau^{-1}(= S_{II})$ belongs to $\mathbf{V}$. □

We emphasise that the definition of $S_{II}$, and also the description of the group $G$ in (4) above, is non-constructive. It is still an open question whether $S_{II}$ is computable from $S$ (assuming for example that we are given the multiplication table of $S$). The "type-$II$ conjecture" of Rhodes is that $S_{II}$ is computable ([**11**] and [**19**]). A stronger conjecture of Rhodes is that $S_{II}$ can be obtained by using (1), (2) and (3) of fact (2.2). More precisely:

DEFINITION: For a finite semigroup $S$, the *type-II construct* subsemigroup, denoted by $S_c$, is the smallest semigroup of $S$ that contains the idempotents of $S$ and that is closed under weak conjugation.

Clearly $S_c$ is a subsemigroup of $S_{II}$ (by Fact 2.2), and $S_c$ is computable. Rhodes' "strong type-$II$ conjecture" is that $S_c = S_{II}$.

A major result of Rhodes and Tilson is:

**FACT 2.3.** *Let* $\mathrm{Reg}(S)$ *denote the set of regular elements of* $S$. *Then* $S_{II} \cap \mathrm{Reg}(S) = S_c \cap \mathrm{Reg}(S)$. *Thus for the regular elements of* $S$, *membership in* $S_{II}$ *is decidable. In particular, if* $S$ *is regular then* $S_{II} = S_c$, *and so* $S_{II}$ *is computable in that case.*

PROOF: See [21], and [23] for a simplified proof. □

A consequence of Facts 2.3 and 2.2(5) is that if $S$ is regular and membership in the variety $\mathbf{V}$ is decidable, then membership in $(\mathbf{V}\,\mathbf{m}\,\mathbf{G})$ is decidable.

For completeness we close this section by showing the connection with a paper of McAlister [17]. McAlister derives structure theorems for arbitrary regular semigroups $S$ in terms of groups, fundamental regular semigroups, and $CIG(S)$, (=the conjugate closure of the idempotents). More precisely, $CIG(S)$ is defined to be the smallest subsemigroup $T$ (necessarily regular) of $S$ containing the idempotents, and such that $aTb \subseteq T$ whenever both $aba = a$ and $bab = b$. Clearly, $CIG(S) \subseteq S_c$. It is not difficult to construct examples of finite (non-regular) semigroups where this inclusion is strict. However, we have the following result for regular semigroups:

**FACT 2.4.** *Let* $S$ *be a regular semigroup. Then* $S_c = CIG(S)$.

PROOF: Define a sequence of subsemigroups $T_n$ of $S$ by:

$$T_0 = \langle E(S) \rangle,$$

and for $i > 0$:

$$T_{i+1} = \langle \cup \{ aT_ib \cup bT_ia \mid a, b \in S^1,\ aba = a \} \rangle.$$

Clearly $T_i \leqslant T_{i+1}$, for $i \geqslant 0$, and $S_c = \cup_{i \geqslant 0} T_i$. It suffices to prove by induction on $i$, that if $S$ is regular then $T_i \leqslant CIG(S)$. The statement is clear for $i = 0$. So assume $T_i \leqslant CIG(S)$. Let $a, b \in S$ be such that $aba = a$. We need only show that for all $t \in T_i$, $atb, bta \in CIG(S)$. Since $S$ is regular, there exists $b'$ such that $bb'b = b$ and $b' = b'bb'$. Then $atb = abatb = abb'batb = (ab)(b'(bat)b)$. But $ab, ba \in E(S) \leqslant T_0 \leqslant CIG(S)$, since $t \in T_i$, and $(ba)t \in T_i$ and by induction $bat \in CIG(S)$. Thus $x = b'(bat)b \in CIG(S)$ and $abx = atb \in CIG(S)$. A similar proof shows that $bta \in CIG(S)$ as well. □

## 3. THEOREMS

In this section we state our main theorem. Other theorems (for example Ash's theorem, and its analogue for orthodox and for solid semigroups) are then derived, using

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

the main theorem together with other results (about semidirect-product decompositions of the varieties generated by inverse, respectively, orthodox semigroups).

**THEOREM 3.1.** *Let $S$ be any finite semigroup. Then $S_{II}$ consists only of regular elements of $S$ if and only if $S_c$ is regular. Moreover, if $S_c$ is regular then $S_{II} = S_c$, and the regular elements of $S$ form a subsemigroup.*

PROOF: We will prove the easy parts of this theorem now, and postpone the hard part.

(a) That if $S_{II}$ consists only of regular elements of $S$ then $S_{II} = S_c$ (and hence $S_c$ is regular):
This follows immediately from Rhodes and Tilson's theorem (Fact 2.3).

(b) That if $S_c$ is regular then the regular elements of $S$ form a subsemigroup:

Let $r_1, r_2 \in S$ be two regular elements. By regularity, there exist idempotents $e_1, f_2 \in S$ such that $r_1 \equiv_L e_1$, $r_2 \equiv_R f_2$. Therefore $r_1 r_2 \equiv_L e_1 r_2 \equiv_R e_1 f_2$, thus $r_1 r_2 \equiv_D e_1 f_2$. Obviously $e_1 f_2 \in S_c$. Since we assume that $S_c$ is regular we conclude that $e_1 f_2$, and hence $r_1 r_2$ (being $D$-related to $e_1 f_2$), is regular. □

What we still have to show is the following:

If $S_c$ is regular then $S_{II}$ consists only of regular elements of $S$.

This will be done in Section 4 and 5, where we will show that if $s$ is a non-regular element of $S$ then one can construct a finite group $G$ and a relational morphism $\tau: S \to G$ such that $(s)\tau$ does not contain the identity element of $G$ - (assuming $S_c$ is regular).

In Section 7 we give an example, showing the following:

If the regular elements of $S$ form a subsemigroup, this does *not* imply that $S_c$ and $S_{II}$ are regular. We give another characterisation of "$S_c$ is regular", and show that the proof scheme used in this paper works only when $S_c$ is regular.

We now apply the main theorem.

**FACT 3.2.** *Let $S$ be a finite semigroup whose set of idempotents $E(S)$ is a subsemigroup. Then $S_{II} = E(S)$. Hence (by Fact 2.2(5)), for any variety $\mathbf{V}$, $S \in (\mathbf{V}\,\mathbf{m}\,\mathbf{G})$ if and only if $E(S) \in \mathbf{V}$.*

PROOF: By the main theorem we only have to show that $S_c = E(S)$. (Then indeed $S_c$ will be regular, hence $S_c = S_{II}$). It is enough to show that $E(S)$ is closed under weak conjugation. Let $e \in E(S)$ and $s, t \in S$ be such that $sts = s$. Then $ts \in E(S)$ and therefore $tse \in E(S)$ (since $E(S)$ is a subsemigroups, by assumption). Then $set =$ (using $s = sts$)$sts\,et = \left(\text{using } tse = (tse)^2\right) stsets\,.et =$ (using $sts = s$)$set\,set = (set)^2$, thus $set \in E(S)$. Similarly one proves that $tes \in F(S)$. □

It is known that every variety $\mathbf{V}$ of finite idempotent semigroups can be defined

by a single identity $u = v$ along with the identity $x^2 = x$. (This is due to Gerhard, Fennemore and Birjukov. See for example [8]. Although proved for Birkhoff varieties, the proof carries over to our ease.)

FACT 3.3. *Let* $\mathbf{V}$ *be a variety of idempotent semigroups*

(1) *Then* $S \in (\mathbf{V}\,\mathrm{m}\,\mathbf{G})$ *if and only if* $E(S)$ *is a subsemigroup of* $S$ *satisfying* $E(S) \in \mathbf{V}$.

(2) *If* $\mathbf{V}$ *is given by identities* $[x = x^2, u = v]$ *then membership of a semigroup in* $(\mathbf{V}\,\mathrm{m}\,\mathbf{G})$ *is decidable.*

PROOF: (1) By Fact 2.2(5), $S \in (\mathbf{V}\,\mathrm{m}\,\mathbf{G})$ if and only if $S_{II} \in \mathbf{V}$. If $S \in (\mathbf{V}\,\mathrm{m}\,\mathbf{G})$ then $S_{II} \in \mathbf{V}$, hence (by the assumption on $\mathbf{V}$) $S_{II} = E(S)$. Then $E(S)$ is also a subsemigroup of $S$, since $S_{II}$ is. If $E(S)$ is a subsemigroup and $E(S) \in \mathbf{V}$ then (by Fact 3.2) $S_{II} = E(S)$, hence $S_{II} \in \mathbf{V}$. Thus (Fact 2.2(5)): $S \in (\mathbf{V}\,\mathrm{m}\,\mathbf{G})$.

(2) Given $S$, we can decide whether $E(S)$ is a subsemigroup and whether $E(S)$ satisfies the identity $u = v$. This then decides whether $S$ belongs to $(V\,\mathrm{m}\,\mathbf{G})$, by (1). □

One can generalise Fact 3.3, using a similar proof. Let $\mathbf{V}$ be a variety of union-of-groups semigroups. Then $S \in (\mathbf{V}\,\mathrm{m}\,\mathbf{G})$ if and only if $S_c \in \mathbf{V}$.

Our main applications are the following two theorems:

THEOREM 3.4. (Ash [1, 2]). *A semigroup* $S$ *divides a finite inverse semigroup if and only if the idempotents of* $S$ *commute.*

PROOF: Let Inv denote the variety generated by finite inverse semigroups. It is easy to see that $S \in$ Inv if and only if $S$ divides a finite inverse semigroup. Let $\mathbf{SL}$ denote the variety of finite semi-lattices (that is commutative idempotent). We will use the result of Margolis and Pin [14] that Inv $= (\mathbf{SL}\,\mathrm{m}\,\mathbf{G})$. By Fact 3.2, we have $S \in (\mathbf{SL}\,\mathrm{m}\,\mathbf{G}) =$ Inv if and only if $E(S) \in SL$. This is precisely what Theorem 3.4 claims. □

**Ortho** denotes variety generated by finite orthodox semigroups, **Id** that consisting of finite idempotent semigroups, and $*$ denotes the semidirect product of pseudovarieties.

THEOREM 3.5. *A semigroup* $S$ *divides a finite orthodox semigroups, if and only if the idempotents of* $S$ *form a subsemigroup. Moreover,* $\mathbf{Ortho} = (\mathbf{Id}\,\mathrm{m}\,\mathbf{G}) = (\mathbf{Id} * \mathbf{G})$.

PROOF: Here we will prove all but one of the statements of the theorem. Obviously, if a semigroup $S$ divides an orthodox semigroup (that is a regular semigroup whose idempotents form a subsemigroup), then the idempotents of $S$ form a subsemigroup.

*Proof that if* $E(S)$ *is a subsemigroup then* $S$ *divides an orthodox semigroup, using*

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

*the fact that* $\mathbf{Ortho} = (\mathbf{Id}\ \mathbf{m}\,\mathbf{G})$:

By Fact 3.2: $S \in (\mathbf{Id}\ \mathbf{m}\,\mathbf{G})$ if and only if $E(S) \in \mathbf{Id}$. Then if $\mathbf{Ortho} = (\mathbf{Id}\ \mathbf{m}\,G)$, we get $S \in \mathbf{Ortho}$ if and only if the idempotents of $S$ form a semigroup. Moreover it is easy to see that a semigroup belongs to **Ortho** if and only if it divides an orthodox semigroup. □

Next we have to show that $\mathbf{Ortho} = (\mathbf{Id}\ \mathbf{m}\,\mathbf{G}) = (\mathbf{Id} * \mathbf{G})$.

Proof that $\mathbf{Ortho} \subseteq (\mathbf{Id}\ \mathbf{m}\,\mathbf{G})$: Applying Fact 3.3(1) to the variety **Id** we get: $S \in (\mathbf{Id}\ \mathbf{m}\,G)$ if and only if $E(S)$ is a subsemigroup of $S$. And, if $S \in \mathbf{Ortho}$ then $E(S)$ is indeed a subsemigroup of $S$. □

Proof that $(\mathbf{Id} * \mathbf{G}) \subseteq \mathbf{Ortho}$: It is sufficient to prove that if $S \in \mathbf{Id}$ and $G \in \mathbf{G}$ then $S * G$ is an orthodox semigroup. Clearly $E(S * G) = \{(s,1) \mid s \in S\}$ and therefore $E(S * G)$ is a subsemigroup of $S * G$. Furthermore $S * G$ is regular since for any $(s,g) \in S * G$ we have $(s,g)(g^{-1}s, g^{-1})(s,g) = (s,g)$. □

The proof that $(\mathbf{Id} * \mathbf{G}) = (\mathbf{Id}\ \mathbf{m}\,\mathbf{G})$ is more involved, and will be given in Section 6.

DEFINITION: A semigroup $S$ is *solid* if and only it the union of all the subgroups of $S$ forms a subsemigroup of $S$.

NOTATION: $\mathcal{UG}$ is the variety of union-of-groups finite semigroups (so, $S \in \mathcal{UG}$ if and only if $S$ is equal to the union of its subgroups).

The finite solid semigroups form a variety. That $\mathcal{UG} * \mathbf{G}$ has a decidable membership problem follows from the next theorem.

**THEOREM 3.6.** *Let $S$ be a finite semigroup. Then: $S$ is solid if and only if $S \in \mathcal{UG} * \mathbf{G}$ if and only if $S_c \in \mathcal{UG}$ if and only if $S_{II} \in UG$. For a solid semigroup $S$, we have $S_{II} = S_c$.*

The proof uses results of Thérien [25] and is given in Section 6.

## 4. Proof of the main theorem: Constructions

In this and the next section we will give the remainder of the proof of Theorem 3.1, namely, we prove the following statement:

*For any finite semigroup $S$, if $S_c$ is regular then $S_{II}$ consists only of regular elements of $S$.*

We will show (under the assumption that $S_c$ is regular) that if $n$ is a non-regular element of $S$ then $n \notin S_{II}$. Moreover "$n \notin S_{II}$" means (by definition of type-$II$) that there exists a finite group $G_n$ and a relational morphism $\tau_n : S \to G_n$ such that $n \notin (1)\tau_n^{-1}$. For every non-regular element $n$ of $S$ we will actually construct such a $G_n$ and $\tau_n$. The group $G_n$ that we will construct will be a direct product of symmetric groups.

GENERAL OVERVIEW OF THE PROOF.

Every relational morphism $S \to G$ can be constructed as follows: First pick a non-empty subset $Z_t$ in $G$, for each $t \in S$. Second, take $\tau$ to be the subsemigroup of $S \times G$ generated by the set $\{(t,g) \mid t \in S \& g \in Z_t\}$. Then, obviously, $\tau$ is a relational morphism $S \to G$.

Let $G(Q)$ (for a given set $Q$) denote the symmetric group on $Q$. For this special kind of group one can construct certain relational morphisms $S \to G(Q)$ as follows:

(1) To every element $s \in S$, associate a partial injective function $f_s: Q \to Q$. (However, we do *not* require that $f_{st} = f_s f_t$).
(2) Extend each $f_s$ to a (total) premutation $p_s \in G(Q)$, in an arbitrary way. (So $f_s$ is just the restriction of $p_s$ to some subset of $Q$).
(3) Take $\tau$ to be the subsemigroup of $S \times G(Q)$ generated by the set $\{(s,p_s) \mid s \in S\}$. Obviously, $\tau$ is then a relational morphism $S \to G(Q)$.

Important observations concerning $\tau$ as just constructed are:

For $p \in G(Q)$ and $s \in S$, we have $p \in (s)\tau$ if and only if there exists a number $k \geqslant 1$ and elements $s_1, \ldots, s_k \in S$ such that $s = s_1 \cdot \cdots \cdot s_k$ and $p = p_{s_1} \cdot \cdots \cdot p_{s_k}$. (This is equivalent to saying that $(s,p)$ can be factored as the product $(s_1,p_{s_1}) \cdot \cdots \cdot (s_k,p_{s_k})$).

More generally, we will construct relational morphisms from $S$ into direct products of symmetric groups $G(Q_1) \times \ldots \times G(Q_n)$ (where $n$ is an integer $\geqslant 1$ and $Q_1, \ldots, Q_n$ are finite sets), as follows:

(1) For every element $s \in S$ and every set $Q_i (1 \leqslant i \leqslant n)$, pick a partial injective function $f_{s,i}: Q_i \to Q_i$.
(2) Extend each $f_{s,i}$ to a total permutation $p_{s,i} \in G(Q_i)$.
(3) Take $\tau$ to be the subsemigroup of $S \times G(Q_1) \times \ldots \times G(Q_n)$ generated by $\{(s,p_{s,1}, \ldots, p_{s,n}) \mid s \in S\}$.

We observe again that for $s \in S$, $p_1 \in G(Q_1), \cdots, p_n \in G(Q_n)$ we have $(p_1, \ldots, p_n) \in (s)\tau$ if and only if there exists a number $k \geqslant 1$ and elements $s_1 \cdots s_k \in S$ such that $s = s_1 \cdot \cdots \cdot s_k$ and such that for each $i$ (with $1 \leqslant i \leqslant n$): $p_i = p_{s_1,i} \cdot \cdots \cdot p_{s_k,i}$. In particular, $s \in (1)\tau^{-1}$ (where 1 is the identity element of $G(Q_1) \times \cdots \times G(Q_n)$) if and only if there exists a factorisation of $s$ as $s_1 \cdot \cdots \cdot s_k$ (for some $k \geqslant 1$ and some $s_1, \ldots, s_k \in S$) such that for all $i$ (with $1 \leqslant i \leqslant n$), $p_{s_1,i} \cdot \cdots \cdot p_{s_k,i} = 1_i$ (= identity of $G(Q_i)$).

Contrapositively: *$s$ does not belong to $(1)\tau^{-1}$ if and only if for all factorisations of $s$ as $s_1 \cdot \cdots \cdot s_k$ (with $k \geqslant 1$, and $s_1, \ldots, s_k \in S$) there exists $i$ (with $1 \leqslant i \leqslant n$) such that $p_{s_1,i} \cdot \cdots \cdot p_{s_k,i} \neq 1_i$.*

We shall next construct a relational morphism $\tau$ according to the method just described, and such that if $s$ is a non-regular element of $s$ then $s \notin (1)\tau^{-1}$ (hence

$s \notin S_{II}$). In order to do this we have to give sets $Q_1, \ldots, Q_n$ and to each element $s$ of $S$ we must associate some partial injective functions $f_{s,i}$ (for $1 \leqslant i \leqslant n$); and this has to be done in such a way that if $s$ is non-regular then $s \notin (1)\tau^{-1}$. In the rest of this section we will describe the sets $Q_i$ and the partial functions $f_{s,i}$. In Section 5 we will show the two properties of the construction:

(1) *Each $f_{s,i}$ is an injective partial function.*

(2) *If $s$ is non-regular then for every factorisation of $s$ as $s = s_1 \cdot \cdots \cdot s_k$ (with $k \geqslant 1$, and $s_1, \ldots, s_k \in S$) there exist $i$ such that the composition $f_{s_1,i} \cdot \cdots \cdot f_{s_k,i}$ cannot be extended to the identity function $1_i : Q_i \to Q_i$.*

This then shows (under the assumption that $S_c$ is regular) that $S_{II}$ consists only of regular elements of $S$.

Before being able to describe each $Q_i$ we need a preliminary construction which we call *an expansion*. Simply, an expansion associates with every semigroup $S$ a semigroup $\underline{\mathrm{Ex}}(S)$ such that $\underline{\mathrm{Ex}}(S) \twoheadrightarrow S$ (that is $S$ is a homomorphic image of $\underline{\mathrm{Ex}}(S)$). The full definition of an expansion can be found in [**5**] but it will not be needed here. For any semigroup $S$ we define the expansion $\widetilde{S}$ to be the semigroup presented by generators and relations as follows:

*Generators:* the set $S$.

*Relations:* the set $\{w = \prod w \mid w \in S^+ \& \prod w \in \mathrm{Reg}(S)\}$.

Here we use the following notation:

$S^+$ is the set of all finite non-empty sequences of elements of $S$.

If $w = (a_1, \ldots, a_n) \in S^+$ then $\prod w = a_1 \cdot \cdots \cdot a_n$. So $\widetilde{S}$ consists of the congruence classes in $S^+$ with respect to the smallest congruence containing the relations $\{(w, \prod w) \mid w \in S^+ \& \prod w \in \mathrm{Reg}(S)\}$.

The semigroup $S$ is a homomorphic image of $\widetilde{S}$ via the map defined on representatives (in $S^+$) by $w \to \prod w$ (the product map). More rigorously, in a congruence class (with respect to the above congruence) pick some representative $w$; the image of the congruence class is defined to be $\prod w$. It is easy to check that this image $\prod w$ depends only on the congruence class, and not on its representative $w$. We denote this homomorphism $\widetilde{S} \to S$ by $\pi$.

This expansion is close to ideas contained in Ash's proof [**1, 2**] – using the philosophy of [**5**].

FACT 4.1. *(Properties of the expansion $\widetilde{S}$). Let $S$ be any semigroup.*

*(a) For every $x \in \widetilde{S}$ we have that $x$ is regular in $\widetilde{S}$ if and only if $(x)\pi$ is regular in $S$. In this case the congruence class $(x)\pi\pi^{-1}$ contains only one element. So one can say that the regular elements of $S$ and $\widetilde{S}$ are "the same". It follows that if idempotnets of $S$ commute (respectively form a band), the same is true in $\widetilde{S}$.*

*(b) If $S$ is a finite semigroup then $\widetilde{S}$ is also finite.*

PROOF: Part (a) of this fact follows immediately from the defining relations of $\widetilde{S}$, and from the fact that homomorphic images (via the map $\pi$ in this case) of regular elements are regular.

Part (b) can be proved in several ways. One could use Ramsey's theorem (as Ash does in [1, 2]). One could use Brown's theorem [6], which states that if $S$ is (locally) finite and $\theta: T \to S$ is a surmorphism such that for every idempotent $e$ of $S$, $(e)\theta^{-1}$ is (locally) finite, then $T$ is (locally) finite. Obviously (by part (a) of this theorem) the morphism $\pi$ has the required property; in fact $(e)\pi^{-1}$ is a one-element set. A third method uses the "null-regular-layers"technique of [4]; this is more complicated but gives much better bounds on the cardinality of $\widetilde{S}$. □

FACT 4.2. *(Irreducible representatives in $S^+$ of the elements of $\widetilde{S}$)*

*(a) Every regular element of $\widetilde{S}$ can be identified with a unique regular element of $S$.*

*(b) Every non-regular element of $\widetilde{S}$ can be represented by a word in $S^+$ of the form $\mathbf{w} = (\mathbf{n}_0, r_1, \mathbf{n}_1, \ldots, r_k, \mathbf{n}_k)$ where each $r_i$ is a regular element of $S$ and each $\mathbf{n}_i$ is a (possibly empty) sequence of non-regular elements of $S$ with the property that $\prod \mathbf{n}_i$ is a non-regular element of $S$. Moreover, for every subsegement $x$ of length $> 1$ of $\mathbf{w}$ we have that $\prod x$ is non-regular (that is no rule $\mathbf{u} \to \prod \mathbf{u}$, with $\prod \mathbf{u}$ regular can be applied to $\mathbf{w}$). Therefore we call $\mathbf{w}$ an "irreducible representative".*

*(c) If the regular elements of $S$ form a subsemigroup then every element of $\widetilde{S}$ has a unique representative $\mathbf{w}$ satisfying properties (a) and (b) above. In addition, here each $\mathbf{n}_i$, for $0 < i < k$ is a non-empty word. (We allow $\mathbf{n}_0$ and $\mathbf{n}_k$ to be empty.)*

REMARK: Recall that if $S_c$ is regular then the regular elements of $S$ form a subsemigroup. (This was proved in the partial proof of Theorem 3.1). Therefore we can apply Fact 4.2(c) in our situation.

PROOF OF FACT 4.2: Parts (a) and (b) are straightforward. Part (c) is a direct consequence of the following lemma which was first discovered by Ash [1, 2], in the case of semigroups whose idempotent commute. The lemma implies (assuming that the regular elements of $S$ form a subsemigroup) that the rewrite rules "$\mathbf{w} \to \prod \mathbf{w}$ if $\prod \mathbf{w}$ is regular" have the Church-Rosser diamond property. □

LEMMA 4.3. *Let $S$ be a semigroup whose regular elements form a subsemigroup. Then for all $x, y, z \in S$ we have that if both $xy$ and $yz$ are regular then $xyz$ is also regular.*

PROOF: Let $t \in S$ be such that $xytxy = xy$. It follows $xytx \equiv_R xy$, and thus $xytx$ is regular. Furthermore $xyz = xytxyz$, which is the product of the two regular elements $xytx$ and $yz$. So $xyz$ is regular, since the regular elements of $S$ form a

subsemigroup. □

From now on we will only talk about semigroups whose regular elements form a subsemigroup; so we can identify elements of $S$ with their unique representatives as described in Fact 4.2.

A few more notions and results will be needed before we can define the sets $Q_i$. For the next definitions and for Facts 4.4 – 4.8 we need not assume that $S_c$ is regular.

DEFINITION: (Type-$II$ partition $\approx$ refining the $R$-relation - -see [23]). For $s,t \in S$ define $s \approx t$ if and only if there exist $x,y \in S_c^1$ such that $sx = t$ and $ty = s$.

So $\approx$ is just $\equiv_R$ but using only multipliers from $S_c^1$. Obviously $\approx$ is an equivalence relation on $S$ refining $\equiv_R$ (Green's $R$ relation). We will denote the equivalence class of $s$ for $\approx$ by $[s]$. The equivalence $\approx$ has the following important properties (given in Facts 4.4 – 4.8, which we will use later to prove that our partial functions $f_{s,i}$ injective), taken from [23].

FACT 4.4. *If $r,b \in S$ and $rb \equiv_R r$ then there exists $a \in S$ with $rba = r$ and $aba = a$.*

PROOF: Since $rb \equiv_R r$, there exists $w \in S$ with $rbw = r$. Hence for all $k \geqslant 1$, $r(bw)^k = r$. Since $S$ is finite we can choose $n > 1$ so that $(bw)^n$ is an idempotent. Let $a = w(bw)^{2n-1}$. Then $rba = r$, and also $aba = w(bw)^{2n-1}bw(bw)^{2n-1} = w(bw)^{4n-1} = w(bw)^{2n-1} = a$. □

The next result shows that $\approx$ is a right partial congruence when restricted to an $R$-class. Note that in Fact 4.5 we need the assumption that $sx$ and $tx$ both stay in the $R$-class of $s$ and $t$.

FACT 4.5. *If $s \approx t$ and $x \in S$ and $s \equiv_R sx \equiv_R tx$, then $sx \approx tx$.*

PROOF: Let $s,t$ and $x$ be as above. Since $s \approx t$, there exists $w \in S_c$ with $t = sw$. Furthermore, since $sx \equiv_R s$, Fact 4.4 implies that there exists $a \in S$ such that $sxa = s$ and axa=a. Therefore $tx = swx = sxawx$. Since $w \in S_c$ and $S_c$ is closed under weak conjugation, we have $z = awx \in S_c$. So $tx = sxz$ for some element $z \in S_c$. In a symmetric way one finds an element $z' \in S_c$ with $sx = txz'$. This proves that $sx \approx tx$. □

FACT 4.6. *If $s,t,x \in S$ are such that $s \equiv_R t \equiv_R sx \equiv_R tx$ then we have: $s \approx t \Leftrightarrow sx \approx tx$.*

PROOF: The implication "$\Rightarrow$" follows from Fact 4.5.

For "$\Leftarrow$": Since $sx \approx tx$ there exists $w \in S_c$ such that $tx = sxw$. Choose $a \in S$ such that $axa = a$ and $t = txa$ (by Fact 4.4). Then $t = txa = sxwa$. But $xwa \in S_c$ (by closure under weak conjugation). Thus there exists $z(= xwa) \in S_c$ such that $t = sz$. In a symmetric way one proves that there exists $z' \in S_c$ such that $s = tz'$.

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

Thus $t \approx s$. □

**COROLLARY 4.7.** *Let $R$ be an $R$-class of $S$ and let $R/\approx$ denote the set of equivalence classes of $R$ with respect to $\approx$. Let $x \in S$. Then $g_x: R/\approx \to R/\approx$ defined by*

$$[r] \in R/\approx \to \begin{cases} [r' \cdot x] & \text{if there exists } r' \text{ such that } r' \approx r \text{ and } r' \cdot x \in R, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

*is a partial function which, in addition, is injective.*

PROOF: If there exist $r'$, $r''$ such that $r' \approx r \approx r''$ and $r'x, r''x \in R$ then $[r'x] = [r''x]$ by Fact 4.6. Thus $g_x$ is a partial function.

If $[r_1]$, $[r_2] \in R/\approx$ are such $([r_1])g_x = ([r_2])g_x$ then there exist $r_1'$, $r_2'$ with $r_1' \approx r_1$, $r_2' \approx r_2$, $r_1'x$ and $r_2'x \in R$, and $[r_1'x] = [r_2'x]$. But then, by Fact 4.6, $r_1' \approx r_2'$. Hence also $r_1 \approx r_2$, thus $[r_1] = [r_2]$. Therefore $g_x$ is injective. □

**FACT 4.8.** *If $e \equiv_R f$ and $e = e^2$, $f = f^2$ then $e \approx f$. In other words, all the idempotents in an $R$-class belong to a common $\approx$-class.*

PROOF: If $e \equiv_R f$ then $e = fe$ and $f = ef$. Since $e$, $f \in S_c$ the result follows. □

**FACT 4.9.** [23]. *If $a, b \in S$ and $aba = a$, then $b \in S_{II}$ implies $a \in S_{II}$ (and hence since $a$ is regular, $a \in S_c$).*

PROOF: [**23,** Proposition 1.1]. Let $\phi: S \to G$ be a relational morphism from $S$ into the finite group $G$. Let $g \in \phi(b)$ and let $h \in \phi(a)$. Hence $(b,g),(a,h) \in$ graph $\phi$. Let $(gh)^\omega = 1$. Then $(a,g)(b,g),(a,h)^{\omega-1} = \left(a, h(gh)^{\omega-1}\right)$. But $(gh)^{\omega-1} = (gh)^{-1} = h^{-1}g^{-1}$ so $\left(a, h(gh)^{\omega-1}\right) = \left(a, h\left(h^{-1}g^{-1}\right)\right) = \left(a, g^{-1}\right)$. Hence $(b,g) \in$ graph $\phi$ implies $\left(a, g^{-1}\right) \in$ graph $\phi$. Hence $b \in S_{II}$ implies $(g,1) \in$ graph $\phi$ implies $(a,1) \in$ graph $\phi$ so $a \in S_{II}$. □

**FACT 4.10.** *Let $a, b \in S$ be inverses in $S$ (that is $aba = a$ and $bab = b$ so $a$ and $b$ are both regular elements of $S$.) Then $a \in S_c$ if and only if $b \in S_c$.*

PROOF: By Fact 4.9 $aba = a$ and $b \in S_c \subseteq S_{II}$ implies $a \in S_c$, and conversely. □

**FACT 4.11.** *For $r \in S$, $i \in S_c$, $r \equiv_R ri$ implies $r \approx ri$ (that is $\exists i' \in S_c$ such that $rii' = r$).*

PROOF: By Fact 4.4 $\exists i' \in S$ such that $rii' = r$ and $i'ii' = i'$. Now since $i \in S_c \subseteq S_{II}$ and by Fact 4.9 (with $i = b$, $i' = a$), $i' \in S_c$. □

REMARKS: (a) The statement and proof of Fact 4.1) remains the same if $S_c$ is replaced throughout by $S_{II}$.

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

(b) The relation $\approx$ is the same with respect to $S_c$ or $S_{II}$ that is

$$(\forall r_i, r_2 \in S)(\exists i_1, i_2 \in S_c)(r_1 i_1 = r_2 \& r_2 i_2 = r_1) \quad \text{if and only if}$$
$$(\forall r_1, r_2 \in S_c)(\exists i_3, i_4 \in S_{II})(r_1 i_3 = r_2 \& r_2 i_4 = r_1).$$

PROOF: If $r_1 i_3 = r_2$ with $i_3 \in S_{II}$, then by Fact (4.4) there exists an $\bar{i}_3$ such that $r_2 \bar{i}_3 = r_1 i_3 \bar{i}_3 = r_1$ and $\bar{i}_3 i_3 \bar{i}_3 = \bar{i}_3$. Hence by $i_3 \in S_{II}$ and Fact 4.10, $\bar{i}_3 \in S_c$. Now repeat the argument starting with $r_2 \bar{i}_3 = r_1$ and obtain $r_1 \bar{\bar{i}}_3 = r_2$, $\bar{\bar{i}}_3 \in S_c$. □

The relation $\approx$ on $S$ induces a function on $\widetilde{S}$ as follows:

With a reduced representative $\mathbf{w} = (\mathbf{n}_1, r_1, \mathbf{n}_1, \ldots, r_k, \mathbf{n}_k) \in \widetilde{S}$ one associates $[\mathbf{w}] = (\mathbf{n}_0, [r_1], n_1, \ldots, [r_k], \mathbf{n}_k)$. We denote the image of $\widetilde{S}$ under this function by $[\widetilde{S}]$. Recall that $[r_i]$ denotes the $\approx$-class of $r_i$. Since we assume that $S_c$ is regular, and hence that $\widetilde{S}$ has unique reduced representatives (Fact 4.2c), the above function is well defined. Also (Fact 4.2c), each $\mathbf{n}_i$ (for $0 < i < k$) is a nonempty word (but $\mathbf{n}_0$ and $\mathbf{n}_k$ can be empty).

We are now ready to define the sets $Q_i$.

**Definition of the state sets $\mathbf{Q_i}$.**

For every word $[\mathbf{w}]$ of the form $(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_k], \mathbf{n}_k)$ of $[\widetilde{S}]$ we consider a set $Q_{[w]}$ defined below. So we will have as many sets as there are elements in $[\widetilde{S}]$. Recall also that we assume that $S_c$ is regular.

Let $[\mathbf{w}] = (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_k], \mathbf{n}_k)$. Then $Q_{[w]}$, consists of all *generalised prefixes* of the word $[\mathbf{w}]$. More precisely, $Q_{[w]}$ is obtained as follows:

Firstly, take all the words of the form $(\mathbf{n}_0, [r_1], \ldots, [r_{i-1}], \mathbf{n}_{i-1}, [r])$ where $r \equiv_R r_i$ and $1 \leqslant i \leqslant k$. (Here $(\mathbf{n}_0, [r_i], \ldots, \mathbf{n}_{i-1})$ is just a prefix of $[\mathbf{w}]$, and $r$ is $R$-equivalent to $r_i$; $R$-equivalence is similar to a prefix relation.)

Secondly, take all the words of the form $(\mathbf{n}_0, \ldots, [r_i], n_{i,1}, \ldots, n_{ij})$ where $0 \leqslant i \leqslant k$, $0 \leqslant j < |\mathbf{n}_i|$ (= length of $\mathbf{n}_i$), and where we denote $\mathbf{n}_i$ by $(n_{i,1}, \ldots, n_{i,|n_i|})$. So the words taken here are prefixes of $[\mathbf{w}]$ which end within some $\mathbf{n}_i$ or at the beginning of some $\mathbf{n}_i$.

Finally, if $\mathbf{n}_0$, is *not* the empty word then we also introduce the empty word, denoted by $\varepsilon$, into $Q_{[\mathbf{w}]}$.

For a given $[\mathbf{w}] = (\mathbf{n}_0, [r_1], \ldots, \mathbf{n}_k)$ with $\mathbf{n}_0 \neq \varepsilon$, we call $\varepsilon$, the *start state* of $Q_{[\mathbf{w}]}$. If $\mathbf{n}_0 = \varepsilon$ in $[\mathbf{w}]$, then $[\mathbf{w}]$ is really of the form $([r_1], \mathbf{n}_1, \ldots, \mathbf{n}_k)$. We consider the $\approx$-class containing all the idempotents of the $R$-class of $r_1$ (recall Fact 4.8); we denote that $\approx$-calss by $[e_1]$, and call $[e_1]$ the *start state* of $Q_{[\mathbf{w}]}$ in that case.

**Definition of the functions $\mathbf{f_{s,[w]}}$.**

For every $[\mathbf{w}] = (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_k], \mathbf{n}_k) \in [\widetilde{S}]$ and every element $s \in S$ we will define a partial function $f_{s,[\mathbf{w}]} : Q_{[\mathbf{w}]} \to Q_{[\mathbf{w}]}$. In the next section we will prove various

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

properties of $f_{s,[\mathbf{w}]}$.

*Intuitively*, if $q \in Q_{[w]}$ we want $(q)f_{s,[w]}$ to be the *next* generalised prefix of [w] that is reached from prefix $q$ when the input letter $s$ is processed. (But $(q)f_{s,[w]}$ is only defined if $s$ indeed leads to $q$ to a generalised prefix $\in Q_{[w]}$ – otherwise we leave $(q)f_{s,[w]}$ undefined.) The precise definition of $(q)f_{s,[w]}$ breakes down into three cases, according to the shape of $q$. We will prove in Section 5 that the listed cases are mutually exclusive or consistent.

CASE 1. If $q \in Q_{[\mathbf{w}]}$ is of the form $q = (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, \mathbf{n}_{i-1}[r])$ with $r \equiv_R r_i$ and $1 \leqslant i \leqslant k$, then

$$(q)f_{s,[\mathbf{w}]} = \begin{cases} (\mathbf{n}_0, [r_1], \ldots, \mathbf{n}_{i-1}, [r], s) & \text{if } [r] = [r_i], \text{ and } s = n_{i+1,1} \\ & \quad \text{(the first letter of } \mathbf{n}_{i+1}) \\ & \quad [\textit{Case 1.1: Exit} \text{ from a regular } R\text{-class}]; \\ (\mathbf{n}_0, [r_1], \ldots, \mathbf{n}_{i-1}, [r' \cdot s]) & \text{if there exists } r' \text{ such that} \\ & \quad r' \approx r \text{ and } r's \equiv_R r_i (\equiv_R r) \\ & \quad \text{(see Corollary 4.7);} \qquad [\textit{Case 1.2}]; \\ (\textit{undefined} \text{ otherwise}) & \qquad [\textit{Case 1.3}]. \end{cases}$$

CASE 2. If $q \in Q_{[\mathbf{w}]}$ is of the form $q = (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_i], n_{i,1}, \ldots, n_{i,j})$ where $\mathbf{n}_i = (n_{i,1}, \ldots, n_{i,|n_i|})$, $0 \leqslant j < |\mathbf{n}_i|$, and $0 \leqslant i \leqslant k$, but if we are not in *Case (3)*, then

$$(q)f_{s,[\mathbf{w}]} = \begin{cases} (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_i], n_{i,1}, \ldots, n_{ij}, s) & \text{if } s = n_{i,j+1} \text{ and } j+1 < |\mathbf{n}_i| \\ & \qquad [\textit{Case 2.1}] \\ (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_i], \mathbf{n}_i, [e_{i+1}]) & \text{if } s = n_{i,|n_i|}, j = |\mathbf{n}_i| - 1, \text{ and} \\ & \quad [e_{i+1}] \text{ is the } \approx\text{-class of all the} \\ & \quad \text{idempotents of the} \\ & \quad R\text{-class of } r_{i+1} \\ & \quad [\textit{Case 2.2}: \\ & \quad \text{Entry into a regular } R\text{-class}]; \\ (\textit{undefined} \text{ otherwise}) & \qquad [\textit{Case 2.3}]. \end{cases}$$

CASE 3. Finally, if $q = \left(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_i], n_{i,1}, \ldots, n_{i,|\mathbf{n}_i|-1}\right)$ we define

$$(q)f_{s,[\mathbf{w}]} = \begin{cases} [\mathbf{w}] & \text{if } s = n_{i,|n_i|} \qquad [\textit{Case 3.1}]; \\ (\textit{undefined} \text{ otherwise}) & \qquad [\textit{Case 3.1}]. \end{cases}$$

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

## 5. Proof of the properties of $f_{s,[w]}$

We will prove in this section that for all $s \in S$ and all $[\mathrm{w}] \in [\widetilde{S}]$:

(1) *$f_{s,[w]}$ is a well-defined partial function;*

(2) *$f_{s,[w]}$ is an injective;*

(3) *if $s$ is a non-regular element of $S$ then we have: For every factorisation $(s_1, \ldots, s_k) \in S^+$ of $s$ there exists $[\mathrm{w}] \in [\widetilde{S}]$ such that the composition $f_{s_1,[w]} \cdot \cdots \cdot f_{s_k,[w]}$ is not extendable to the identity function $1_{w]}: Q_{[w]} \to Q_{[w]}$.*

This then shows that if $s$ is a non-regular element of $S$ then $s \notin S_{II}$. (Recall the reasoning in the "general overview of the proof", at the beginning of Section 4).

The proof that $f_{s,[w]}$ is a partial function, and the proof that $f_{s,[w]}$ is injective, are dual to each other (with just a few technical differences). The main problems are the *entry problem* (for injectiveness) and the *exit problem* (for functionality).

*Proof that $\mathbf{f_{s,[w]}: Q_{[w]} \to Q_{[w]}}$ is a partial function - or the "exit problem".*

We must show that in the definition of $(q)f_{s,[w]}$ only one of the cases applies. Clearly (from the shape of $q$) Case 1 and Case 2 never apply simultaneously. Also, Cases 2 and 3 are exclusive by definition. Cases 1 and 3 are either exclusive by the shape of $q$, or Case 3 and Case 1.1 both apply and produce the same result.

Within Case 2, and Case 3, all subcases are mutually exclusive.

When Case 1.2 applies alone, $(q)f_{s,[w]}$ is uniquely defined, by Corollary 4.7. The only place where it is not obvious that the cases are exclusive concerns Cases (1.1) and (1.2).

*Proof that subcases 1.1 and 1.2 of the definition of $\mathbf{(q)f_{s,[w]}}$ are mutually exclusing:*

If $s \neq \mathrm{n}_{i+1,1}$ or $[r] \neq [r_i]$, then obviously only one of Cases 1.1 and 1.2 applies. So consider the situation where $s = n_{i+1,1}$ and $[r] = [r_i]$. Obviously Case 1.1 applies. We must rule out Case 1.2. We call this the **exit problem**, because there apparently are two ways to leave the $R$-class of $[r_i]$ either by going to $(\ldots, \mathrm{n}_{i-1}, [r_i], s)$ or by going to $(\ldots, \mathrm{n}_{i-1}, [r' \cdot s])$ (the latter possibility will be ruled out). We shall say that $S$ has the *unique-exit property* if Cases 1.1 and 1.2 are mutually exclusive. Since Case 1.1 applies, the word $([r_i], s)$ is a subword of $[\mathrm{w}]$. Since $[\mathrm{w}]$ is a reduced word of $[\widetilde{S}]$, it follows from Fact 4.2 that $r_i \cdot s$ is a *non-regular* element of $S$. If Case 1.2 also applies then there exist $r'$ with $r' \approx r_i$ and $r' \cdot s \equiv_R r_i$. This however contradicts the assumption that $S_c$ is regular, by Lemma 5.1 given below. □

**Lemma 5.1.** *Let $r, s \in S$ be such that $r$ is regular, $r \cdot s$ is non-regular, and there exists $r'$ with $r' \approx r$ and $r's \equiv_R r$. Then $S_c$ contains an element that is non-regular in $S$.*

Proof: Let $f$ be an idempotent in the $L$-class of $r'$. So there exists $y$ with

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

$yr' = f = f^2$. Also $yr' \approx yr$ (since $r \approx r'$ and $\approx$ is preserved under left multiplication). Therefore $yr \in S_c$ (since $yr' = f = f^2 \in S_c$ and $yr \approx f$). We can apply Fact 4.4 to $r's \equiv_R r'$: there exists $x \in S$ with $r'sx = r'$ and $xsx = x$. (Actually, since $r'$ is regular, we can choose $x$ so that $x \equiv_L r'$.) Then, since $yr \in S_c$ and $S_c$ is closed under weak conjugation, we get $xyrs \in S_c$.

We shall show now that $xyrs$ is not regular in $S$. We have indeed (1) $xyr \equiv_L yr$ and (2) $yr \equiv_L r$. (2) follows since $r \approx r' \equiv_L yr' \approx yr$ and $yr \leqslant_L r$. (1) holds because $yr \equiv_R yr'$ implies $xyr \equiv_R xyr' = xf = x$ (since $x \equiv_L r' = f \equiv_L r' \approx r \equiv_L yr$). So we get $xyr \equiv_L r$. Therefore $xyrs \equiv_L rs$, which is non-regular in $S$. □

*Proof that* $\mathbf{f}_{s,[w]}\colon \mathbf{Q}_{[w]} \to \mathbf{Q}_{[w]}$ *is injective – or the entry problem.*

We must show that if $q_1, q_2 \in Q_{[w]}$ are such that $(q_1)f_{s,[w]} = (q_2)f_{s,[w]}$ and both are defined, then $q_1 = q_2$. Let $[w] = (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_k], \mathbf{n}_k)$. We denote $\mathbf{n}_i = (n_{i,1}, \ldots, n_{i,j}, \ldots, n_{i,|\mathbf{n}_i|})$ for $0 \leqslant i \leqslant k$, $0 \leqslant j \leqslant |\mathbf{n}_i|$. We will distinguish two cases, depending on the form of $(q_1)f_{s,[w]}$.

CASE A. $(q_1)f_{s,[w]}$ is of the form $(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_2], n_{i,j}, \ldots, n_{i,j+1})$ where $0 \leqslant i \leqslant k$ and $1 \leqslant j+1 < |\mathbf{n}_i|$. This case is rather simple: by the definition of $(q_1)f_{s,[w]}$ we must have $s = n_{i,j+1}$, and $q_1$ must be equal to $(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_i], n_{i,1}, \ldots, n_{i,j})$ – otherwise $(q_1)f_{s,[w]}$ would have been undefined. Similarly, since $(q_1)f_{s,[w]} = (q_2)f_{s,[w]}$, we must have $q_2 = (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, [r_i], n_{i,1}, \ldots, n_{i,j})$. Hence $q_1 = q_2$.

CASE B. $(q_1)r_{2,[w]}$ is of the form $(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, \mathbf{n}_{i-1}, [r'])$ where $r'' \equiv_R r_i$, and $1 \leqslant i \leqslant k$.

If $[r''] \neq [e_i]$ (where $[e_i]$ is the $\approx$-class of the idempotents of the $R$-class of $r_i$) or if $[r''] = [e_i]$ but $s \neq n_{i-1,|\mathbf{n}_{i-1}|}$, then the definition of $(q_1)f_{s,[w]}$ uniquely determines $q_1 = q_2$ to be $(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, \mathbf{n}_{i-1}, [r])$, where $[r]$, $[r''7]$ and $s$ are related as follows: there exists $r'$ with $r' \approx r$ and $r'' = r's \equiv_R r$. By Corollary 4.7, this uniquely determines $[r]$.

However, if $[r''] = [e_i]$ and $s = n_{i-1,|\mathbf{n}_{i-1}|}$ then there seem to be two possible values for $q_1$ and $q_2$ (which would allow $q_1 \neq q_2$). This is the *entry problem*. We must rule out one of these values, otherwise $f_{s,[w]}$ will not be injective. Two apparently possible values for $q_1$, $q_2$ are:

(1) $(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, \mathbf{n}_{i-1}, [e_i])$, and

(2) $\left(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, n_{i-1}, \ldots, n_{i-1,|\mathbf{n}_{i-1}|-1}\right)$,

assuming in both cases that $s = n_{i-1,|\mathbf{n}_{i-1}|}$ and that there exists $r'$ with $r' \approx e_i$ and $r' \cdot s \approx e_i$.

(5.1)(a) Let us prove that (1) is impossible. Indeed, assume we had $(q_1)f_{s,[w]} = (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, \mathbf{n}_{i-1}, [e_i]) = \left(\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, n_{i-1}, \ldots, n_{i-1,|\mathbf{n}_{i-1}|}, [e_i]\right)$

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

with $s = \mathbf{n}_{i-1,|n_{i-1}|}$ and $(\exists r')$: $r' \equiv_R e_i$ and $r' \cdot s \approx e_i$. Then $s \cdot e_i \left(= n_{i-1,|n_{i-1}|} \cdot e_i\right)$ must be a *non-regular* element if $S$. (This is because the word expressing $(q_1)f_{s,[w]}$ above must be reduced; no rule of the form $u \to \prod u$ can be applied to it. If $s \cdot e_i$ were regular then the rule $(s, e_i) \to s \cdot e_i$ could be applied). This however, contradicts the fact that $S_c$ is regular, by the dual of Lemma 5.1 because of the following: If $r' \approx e_1 \equiv e$ and $r' \cdot s \approx e$ and $s \cdot e$ is a non-regular element of $S$, then there exists $i_1 \in S_c$ such that $r' s i_1 = e$ so $r' s i_1 e = ee = e$ so $s \cdot (i_1 e) \equiv_L e$ so $i_1 e \equiv_L e$. Then by the dual of Fact 4.11 $i_1 e \approx e$. Hence $e = e^2$, $s \cdot e$ is not regular $i_1 e \approx e$ and $s \cdot i_1 e \equiv_L e$. Then, by taking the dual of Lemma (5.1) with $s$, $e$, $r$, $r'$ here replaced by $s$, $r$, $r'$, $i$, $e$ there, respectively, we find $S_c$ is not regular, a contradiction.

Having ruled out (1), we obtain $q_1 = q_2 = (\mathbf{n}_0, [r_1], \mathbf{n}_1, \ldots, \mathbf{n}_{i-1,1}, \ldots, \mathbf{n}_{i-1}, |\mathbf{n}_{i-1}| - 1)$. □

*Proof that if* $\mathbf{s}$ *is non-regular then* $\mathbf{s} \notin (1)\tau^{-1}$.

Let $s$ be a non-regular element of $S$ and let $(s_1, \ldots, s_k) \in S^+$ be any factorisation of $s$. (That is $k \geqslant 1$, $s_1, \ldots, s_k \in S$ and $s_1 \cdot \cdots \cdot s_k = s$). Let $\mathbf{w}$ be the reduced representative of an element of $\widetilde{S}$ obtained by applying the defining relations of $\widetilde{S}$ to the word $(s_1, \ldots, s_k)$. We will show that for this particular $\mathbf{w}$, obtained from $(s_1, \ldots, s_k)$ we have (denoting the start state of $Q_{[w]}$ by $q_0$):

$$(5.2) \qquad (q_0)f_{s_1,[w]} \cdot \cdots \cdot f_{s_k,[w]} = [\mathbf{w}].$$

Notice also that $q_0 \neq [\mathbf{w}]$ because, on the one hand, $[\mathbf{w}]$ is certainly not $\varepsilon$, and on the other hand $[\mathbf{w}]$ is not of the form $[e]$ (with $e = e^2 \in S$) because $s$ is not regular (hence $\mathbf{w}$ is not regular by Fact 4.2(b)). Therefore, from equaltiy (5.2) we deduce that $(q_0)f_{s_1,[w]} \cdot \cdots \cdot f_{s_k,[w]}$ is defined and is different from $q_0$. Thus $f_{s_1,[w]} \cdot \cdots \cdot f_{s_k,[w]}$ cannot be extended to the identity function $1_{[w]}: Q_{[w]} \to Q_{[w]}$. From this we conclude that $s \notin (1)\tau_{[w]}^{-1}$ (recall the "general overview of the proof at the beginning of Section 4).

*Proof that* $(q_0)f_{s_1,[w]} \cdot \cdots \cdot f_{s_k,[w]} = [\mathbf{w}]$.

By Fact (4.2), the word $(s_1, \ldots, s_k)$ can be broken up in a unique way into subsegments $\mathbf{n}_0, \mathbf{p}_1, \mathbf{n}_1, \ldots, \mathbf{p}_h, \mathbf{n}_h$, each belonging to $S^+$, such that:

(1) the concatenation $\mathbf{n}_0 \cdot \mathbf{p}_1 \cdot \mathbf{n}_1 \cdot \cdots \cdot \mathbf{p}_h \cdot \mathbf{n}_h$ equals $(s_1, \ldots, s_k)$;

(2) each $\mathbf{p}_i$ (with $1 \leqslant i \leqslant h$) is a maximally long subsegment of $(s_1, \ldots, s_k)$ such that $\prod \mathbf{p}_i$ is a regular element of $S$;

(3) each $\mathbf{n}_i$ (with $0 \leqslant i \leqslant h$) is a subsegment of $(s_1, \ldots, s_k)$ such that every non-empty subsegment $\mathbf{v}$ of $\mathbf{n}_i$ (including $\mathbf{n}_i$ itself) satisfies: $\prod \mathbf{v}$ is a non-regular element of $S$.

Observe that in this notation: $\mathbf{w} = (\mathbf{n}_0, \prod \mathbf{p}_1, \mathbf{n}_1, \ldots, \prod \mathbf{p}_h, \mathbf{n}_h)$. Also, if $\mathbf{n}_0 \neq \varepsilon$ then the start state of $Q_{[w]}$ is $q_0 = \varepsilon$; if $\mathbf{n}_0 = \varepsilon$ then $q_0 = [e_1] =$ the $\approx$-class of

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

all the idempotents in the $R$-class of $\prod \mathbf{p}_1$. Let us write $\mathbf{n}_i = (n_{i,1}, \ldots, n_{i,|\mathbf{n}_i|})$, for $0 \leqslant i \leqslant h$, and $\mathbf{p}_i(\mathbf{p}_{i,1}, \ldots, p_{i,|p_i|})$ for $1 \leqslant i \leqslant h$. The composition of partial functions $f_{s_1,[w]} \cdot \cdots \cdot f_{s_k,[w]}$ is the successive composition of partial functions of the form $f_{n_{0,j},[w]}$ for $j = 1, \ldots, |\mathbf{n}_0|$, followed by $f_{p_{1,j},[w]}$ for $j = 1, \ldots, |\mathbf{p}_1|$, followed by $f_{n_{1,j},[w]}$ for $j = 1, \ldots, |\mathbf{n}_1|$, et cetera.

We start out with the state $q_0$. After the functions $f_{n_{0,j},[w]}$ have been applied to $q_0$, successively for $j = 1, \ldots, |\mathbf{n}_0|$ the state reached is $(\mathbf{n}_0, [e_1])$. Again, $[e_1]$ denotes the $\approx$-class of the idempotents in the $R$-class of $\prod \mathbf{p}_1$. Next we apply successively $f_{p_{1,j},[w]}$ for $j = 1, \ldots, |\mathbf{p}_1|$. By definition the states reached will be of the form:
$(\mathbf{n}_0, [r'_1 \cdot p_{1,1}])$ where $r'_1 \approx e_1$, $r'_1 \cdot_{1,1} \equiv_R \prod \mathbf{p}_1$,
$(\mathbf{n}_0, [r'_2 \cdot p_{1,2}])$ where $r'_2 \approx p_{1,1}$, $r'_2 \cdot p_{1,2} \equiv_R \prod \mathbf{p}_1$, et cetera,
$(\mathbf{n}_0, [r'_j \cdot p_{1,j}])$ where $r'_j \approx r'_{j-1} \cdot p_{1,j-1}$, $r'_j \cdot p_{1,j} \equiv_R \prod \mathbf{p}_1$, for $j = 1, \ldots, |\mathbf{p}_1|$, et cetera, finally (for $j = |\mathbf{p}_1|$) we reach the state $\left(\mathbf{n}_0, [r'_{|p_1|} \cdot p_{1,|p_1|}]\right)$ where $r'_{|p_1|} \approx r'_{|p_1|-1} \cdot p_{1,|p_1|-1}$ and $r'_{|p_1|} \cdot p_{1,|p_1|} \equiv_R \prod \mathbf{p}_1$. But, since $e_1 \equiv_R \prod \mathbf{p}_1 = p_{1,1} \cdot \cdots \cdot p_{1,|p_1|}$ we also have $e_1 \equiv_R e_1 p_{1,1} \equiv_R e_1 p_{1,1} p_{1,2} \equiv_R \cdots \equiv_R e_1 p_{1,1} \cdot \cdots \cdot p_{1,j}$ for $j = 1, \ldots, |p_1|$. Therefore we can choose $r'_1 = e_1$, $r'_2 = r_1 p_{1,1} = e_1 p_{1,1}$, and in general $r'_j = r'_{j-1} p_{1,j-1} = e_1 p_{1,1} \cdot \cdots \cdot p_{1,j-1}$ for $j = 1, \ldots, |p_1|$, and finally we get $[r'_{|p_1|} \cdot p_{1,|p_1|}] = [\prod \mathbf{p}_1]$. Thus, after applying the functions $f_{p_{1,j},[w]}$ to the state $(\mathbf{n}_0, [e_1])$ we reach the state $(\mathbf{n}_0, [\prod \mathbf{p}_1])$.

Next, we apply $f_{n_{i,j},[w]}$ for $1 \leqslant j \leqslant |\mathbf{n}_1|$. By the definition of the actions, and by the *unique-exit* property, this leads to the state $(\mathbf{n}_0, [\prod \mathbf{p}_1], \mathbf{n}_1, [e_2])$. In the same way we can apply the further functions, corresponding to the successive $\mathbf{p}_j$ and $\mathbf{n}_j$ (for $j = 1, \ldots, h$). At the very end we apply rule (3) of the definition of $f_{s,[w]}$. This then yields the state $[\mathbf{w}]$. □

REMARKS ON THE IDEA OF THE CONSTRUCTION.

A lot of the inspiration for the definition of $Q_{[w]}$ and $f_{s,[w]}$ came from Ash [1, 2]. His proof however used induction on the $J$-order of $S$ which complicates things. The main difficulty in defining $f_{s,[w]}$ was to make it an injective partial function, while at the same time keeping the state sets $Q_{[w]}$ finite and having only finitely many of them. For example, it would have been easy to make $f_s$ injective by using $S^+$ instead of $[\widetilde{S}]$, but this would have led to infinitely many state sets, and then $\tau$ would no longer be finite. When using $\widetilde{S}$ we still treat the non-regular elements as if we were in $S^+$. However the regular elements are handled as in $S$. This dual approach leads to difficulties when successive multiplications ($s_1$, $s_1 s_2$, $s_1 s_2 s_3$. et cetera) lead from non-regular into regular $R$-calsses, (or from regular into non-regular $R$-classes). This *entrance* and *exit* problem for regular $R$-classes was solved as follows:

*Entrance problem: (into a regular R-class):*

If the current state is $q = (\ldots, n_{i,1}, \ldots, n_{i,|n_i|-1})$ and $s = n_{i,|n_i|}$ then we do not define $(q)f_{s,[w]}$ to be $(\ldots, n_i)$ but we define it to be $(\ldots, n_i, [e_{i+1})$. In other words, we anticipate in the state what the next regular $R$-class will be, although this regular $R$-class has not yet "really" been reached. This additional knowledge about the future (in the current state) makes $f_{s,[w]}$ injective ("unique past"). Notice that we can know what $[e_{i+1}]$ is, since we know [w] ($f_{s,[w]}$ is only defined on $Q_{[w]}$ for a fixed [w]). If this fails to make the function well-defined $S_c$ becomes non-regular via the dual of Lemma (5.1). See (5.1)(a).

*The exit problem (from a regular R-class):*

When we are in state $q = (\ldots, [r_i])$ and $[w] = (\ldots, [r_i], n_{i,1}, \ldots)$ and $s = n_{i,1}$ then we define $(q)f_{s,[w]}$ to be $(\ldots, [r_1], n_{i,1})$. (We do not define $(q)f_{s,[w]}$ to be $(\ldots, [r'.s])$. Again, the knowledge of [w] tells us that now we should exit from the regular $R$-class. If this fails to make the function injective $S_c$ becomes non-regular via Lemma (5.1). See (5.0).

## 6. Proof that $(\mathbf{Id} * G) = (\mathbf{Id}\ \mathbf{mG})$ and results about solid semigroups

In this section we prove the last open case of Theorem 3.5, and we prove Theorem 3.6.

We note that if $\mathbf{V}$ is any variety, then $\mathbf{V} * \mathbf{G} \subseteq (\mathbf{V}\,\mathrm{m}\,\mathbf{G})$. For if $S \in \mathbf{V}$, $G \in \mathbf{G}$ then the projection $f: S * G \to G$ satisfies $(1)f^{-1} \leqslant S \in \mathbf{V}$. However, the inclusion in the opposite direction does not hold for arbitrary varieties $\mathbf{V}$. [For example, Rhodes (unpub.) has constructed a sequence of semigroups $S_n (n \geqslant 0)$, with $S_n \in ((\mathbf{A} * \mathbf{G})\mathbf{mG})$ such that $S_n$ has complexity $n$. On the other hand, $\mathbf{A} * \mathbf{G} * \mathbf{G} = \mathbf{A} * \mathbf{G}$ is contained in the variety of semigroups of complexity $\leqslant 1$.]

To prove the inclusion in the opposite direction we must quote results from the theory of the derived category of a relation as developed by Tilson [24]; see also [20] for an exposition. We will only quote the important results.

It is well-known that if $\mathbf{V}$ and $\mathbf{W}$ are varieties of *groups*, then $\mathbf{V} * \mathbf{W} = (\mathbf{V}\,\mathrm{m}\,\mathbf{W})$ consists of all groups $G$ such that there is $H \in \mathbf{W}$ and a functional morphism $\phi: G \to H$ with $\ker(\phi) \in \mathbf{V}$. The derived category was developed to extend this situation from group theory to semigroup theory. It turns out that the "kernel" of a relational morphism $\phi: S \to T$ is a category $D(\phi)$ that is only "locally" in $S$. That is, the monoid of self-morphisms $\mathrm{Mor}(v,v)$ divides $S$ for each $v \in \mathrm{Obj}(D(\phi))$. For the case of a morphism between groups, $D(\phi)$ turns out to be the category of cosets of $K = \ker(\phi)$, and it is well-known that $D(\phi)$ is equivalent to $K$ in the sense of category theory (see [24]). This is why in group theory we can reduce extension questions to the study of $K \leqslant G$.

We will say that a (finite ) category $C$ is *locally* in a variety $\mathbf{V}$ if $\mathrm{Mor}(v,v) \in \mathbf{V}$

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

for each $v \in \mathrm{Obj}(C)$. We will say that $C$ is *globally* in $\mathbf{V}$ if there is a monoid $M \in \mathbf{V}$ and a function $\tau\colon \mathrm{Mor}(C) \to M$ such that

(1) if $\alpha \in \mathrm{Mor}(v,w)$ and $\beta \in \mathrm{Mor}(w,x)$ then $(\alpha\beta)\tau \supseteq \alpha\tau \cdot \beta\tau$;

(2) for all morphisms $\alpha$ of $C$: $(\alpha)\tau \neq \emptyset$ ($\tau^{-1}$ is surjective);

(3) $\tau^{-1}$ is a partial function.

The following fundamental theorem appears in [24].

**THEOREM 6.1.** *$S \in \mathbf{V} * \mathbf{W}$ if and only if there is $T \in \mathbf{W}$ and a relational morphism $\phi\colon S \to T$ such that $D(\phi)$ is globally in $\mathbf{V}$.*

Let $\overline{D}(\phi)$ denote the derived category without identifying arrows (see [14]. Note $D(\phi) < \overline{D}(\phi)$. Then if $\mathbf{W} = \mathbf{G}$, $D(\phi)$ and $\overline{D}(\phi)$ distinguish between $\mathbf{V} * \mathbf{G}$ and $(\mathbf{V}\,\mathrm{m}\,\mathbf{G})$, since easily

**COROLLARY 6.2.** *(a) $S \in (\mathbf{V}\,\mathrm{m}\,\mathbf{G})$ if and only if there is a relational morphism $\phi\colon S \to G$ where $G \in \mathbf{G}$ such that $\overline{D}(\phi)$ is locally in $\mathbf{V}$.*

*(b) If $\mathbf{V}$ is "local" (that is for all categories $C$, $C$ is locally in $\mathbf{V}$ if and only if $C$ is globally in $\mathbf{V}$), then $\mathbf{V} * \mathbf{G} = (\mathbf{V}\,\mathrm{m}\,\mathbf{G})$.*

It is easy to show if a category $C$ is globally in $\mathbf{V}$, then it is locally in $\mathbf{V}$. The converse is usually not true. For example, if $\mathbf{J}$ the variety of $J$-trivial monoids, then there are categories that are locally in $\mathbf{J}$ but not globally in $\mathbf{J}$ ([9], see also [25]). The same holds true for the variety $\mathbf{Com}_n$ (for $n \geqslant 1$) consisting of all commutative monoids satisfying $x^n = x^{n+1}$ (Thérien [25]). On the other hand, an important lemma of Simon [22] can be shown to give the following theorem concerning the variety $\mathbf{SL}$ of semilattices.

**THEOREM 6.3.** *Let $C$ be a category. Then $C$ is locally in $\mathbf{SL}$ if and only if $C$ is globally in $\mathbf{SL}$.*

**COROLLARY 6.4.** $\mathbf{SL} * \mathbf{G} = (\mathbf{SL}\,\mathrm{m}\,\mathbf{G})$.

Thérien and Weiss [26] have shown that a similar conclusion holds for the variety $\mathbf{Id}$ of idempotent monoids:

**THEOREM 6.5.** *Let $C$ be a category. Then $C$ is locally in $\mathbf{Id}$ if and only if $C$ is globally in $\mathbf{Id}$.*

We obtain from Corollary (6.2) and Theorem (6.5):

**COROLLARY 6.6.** $\mathbf{Id} * \mathbf{G} = (\mathbf{Id}\,\mathrm{m}\,\mathbf{G})$.

Thérien proved more – which will enable us to prove our Theorem 3.6. Let $\mathcal{UG}_n$ be the variety of monoids satisfying $x^{n+1} = x$, $n \geqslant 1$. So $\mathcal{UG} = \bigcup_{n \geqslant 1} \mathcal{UG}_n$ is the variety of union-of-group semigroups.

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

**THEOREM 6.7.** *([28]). Let $C$ be a category. Then for each $n \geqslant 1$, $C$ is locally in $\mathcal{UG}_n$ if and only if $C$ is globally in $\mathcal{UG}_n$.*

**COROLLARY 6.8.** *$C$ is locally in $\mathcal{UG}$ if and only if $C$ is globally in $\mathcal{UG}$.*

**COROLLARY 6.9.** *For all $n \geqslant 1$: $(\mathcal{UG}_n\mathbf{mG}) = (\mathcal{UG}_n * G) = \{S \mid S_c \in \mathcal{UG}_n\} = \{S \mid S_{II} \in \mathcal{UG}_n\}$. And: $(\mathcal{UG}\,\mathbf{mG}) = (\mathcal{UG} * \mathbf{G}) = \{S \mid S_c \in \mathcal{UG}\} = \{S \mid S_{II} \in \mathcal{UG}\}$.*

Notice that $S_c \in \mathcal{UG}$ implies that $S_c$ is regular. Therefore (by the main Theorem 3.1), $S_c = S_{II}$ for solid semigroups. As a consequence (using Fact 2.2(5)) we have $S \in \mathcal{UG} * \mathbf{G}$ if and only if $S_c \in \mathcal{UG}$, and thus, membership in the variety $\mathcal{UG} * \mathbf{G}$ is decidable.

## 7. A COUNTER-EXAMPLE, AND A CHARACTERISATION OF "$S_c$ IS REGULAR"

**FACT 7.1.** *There exists a finite semigroup $S$ satisfying:*

(1) *the regular elements of $S$ form a subsemigroup, but*
(2) *$S_c$ and $S_{II}$ contain some non-regular elements of $S$. So, if the regular elements of $S$ are a subsemigroup, this does not imply that $S_c$ is regular.*

The type-$II$ conjectures for semigroups whose regular elements form a subsemigroup, are still open in general.

To prove the fact, consider the following semigroup $S$:

As a set $S = \{0, n\} \cup \{a_1, a_2, a_3, a_4\} \times \{b_1, b_2, b_3\}$ and the multiplication is as follows:

(0) the element 0 is a zero (that is $(\forall x \in S)(0 \cdot x = 0 \cdot x = 0)$);
(1) $n^2 = 0$;
(2) $(\forall b \in \{b_1, b_2, b_3\})$ $(n \cdot (a_1, b) = (a_4, b)$, $n \cdot (a_2, b) = (a_3, b)$ and $n \cdot (a_3, b) = n \cdot (a_4, b) = 0)$;
(3) $(\forall a \in \{a_1, a_2, a_3, a_4\})((a, b_1) \cdot n = (a, b_2) \cdot n = 0 \& (a, b_3) \cdot n = (a, b_2))$;
(4) $\{a_1, a_2, a_3, a_4\} \times \{b_1, b_2, b_3\}$ is a Rees-matrix semigroup with trivial structure group, and with the following structure matrix $C$:

| $C$ | $a_1$ | $a_2$ | $a_3$ | $a_4$ |
|---|---|---|---|---|
| $b_1$ | 1 | 1 | 0 | 0 |
| $b_2$ | 0 | 1 | 0 | 0 |
| $b_3$ | 0 | 0 | 1 | 0 |

One checks easily that this multiplication is associative. The regular elements of $S$ form a subsemigroup (consisting of $\{0\} \cup \{a_1, a_1, a_3\} \times \{b_1, b_2\}$). Also, the element $(a_1, b_2)$ is a product of idempotents $((a_1, b_2) = (a_1, b_1)(a_2, b_2))$, hence belongs to $S_c$. Moreover, we have $(a_2, b_3) \cdot n \cdot (a_2, b_3) = (a_2, b_3)$, so $n$ and $(a_2, b_3)$ are a *weak conjugate*

https://doi.org/10.1017/S0004972700017986 Published online by Cambridge University Press

*pair*. Therefore, since $(a_1, b_2) \in S_c$ and since $S_c$ is closed under weak conjugation we have $n \cdot (a_1, b_2) \cdot (a_2, b_3) = (a_4, b_3) \in S_c$. But $(a_4, b_3)$ is a non-regular element.

To conclude the paper we give the following characterisation of our running assumption "$S_c$ is regular in $S$".

**THEOREM 7.2.** *Let $S$ be a finite semigroup and let $S_c$ be its type-II-construct subsemigroup. Then the following are equivalent:*

(1) *$S_c$ is regular in $S$ (that is every element of $S_c$ has an inverse in $S$);*

(2) *$S_c$ is regular (that is every element of $S_c$ has an inverse in $S_c$ itself);*

(3) *the regualr elements of $S$ form a subsemigroup, we have for all $x$ and $s$ in $S$: if $s$ is regular but $s \cdot x$ is non-regular, then $(\forall t \in [s])(t \cdot x <_R t)$ (strict R-order) (see Lemma (5.1)) and we have for all $x$ and $s$ in $S$; if $S$ is regular but $x \cdot s$ is non-regular, then $(\forall t \in [s]')(x \cdot t <_L t)$ (strict L-order); (Recall that $[s]$ denotes the $\approx$-class of $s$, defined before Fact 4.4. Here $[s]' = \{t \in S \mid (\exists a, b \in S_c)(t = as \& s = bt)\}$. So $[s]'$ is the equivalence class of $s$ with respect to the left dual of $\approx$).*

(4) *$S_{II}$ is regular in $S$;*

(5) *$S_{II}$ is regular;*

(6) *$S_{II} = S_c$ and $S_c$ is regular.*

PROOF: (1) $\iff$ (2) follows from Fact 4.10.

(2) $\implies$ (3) by (3.1)(a) and Lemma (5.1) and its dual.

(3) $\implies$ (4) is the long proof of Theorem (3.1) given in Sections 3, 4 and 5. Note only the assumptions of (3) are used!

(4) $\iff$ (5) follows from Fact 4.9.

(5) $\implies$ (6) follows from Fact 2.3.

(6) $\implies$ (1) is trivial. □

## REFERENCES

[1] C.J. Ash, 'Finite idempotent-commuting semigroups', in *Semigroups and their applications*, Editors S. Goberstein and P. Higgins, pp. 13–25 (Reidel, Dordrecht, 1986).

[2] C.J. Ash, 'Finite semigroups with commuting idempotents', *J. Austra. Math. Soc.* **43** (1987), 81–90.

[3] J.C. Birget, S. Margolis and J. Rhodes, 'Finite semigroups whose idempotents commute or form a subsemigroup', in *Semigroups and their applications*, Editors S. Goberstein and P. Higgins, pp. 25–36 (Reidel, Dordrecht, 1986).

[4] J.C. Birget, 'Iteration of expansions, unambiguous semigroups', *J. Pure Appl. Algebra* **34** (1984), 1–55.

[5] J.C. Birget and J. Rhodes, 'Almost finite expansions of arbitrary semigroups', *J. Pure Appl. Algebra* **32** (1984), 239–287.

[6] T.C. Brown, 'An interesting combinatorial method in the theory of locally finite semigroups', *Pacific J. Math.* **36** (1971), 285–289.

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

[8] J.A. Gerhard, 'The lattice of equational classes of idempotent semigroups', *J. Algebra* **15** (1970), 195–224.

[9] R. Knast, 'A semigroup characterization of dot-depth one languages', *RAIRO Inform. Théor. Appl.* **17** (1983), 321–330.

[10] K. Krohn, J. Rhodes and B. Tilson, 'Lectures on finite semigroups', Chapters 1, 5-9, in *Algebraic Theory of Machines, Languages and Semigroups*, Editor M. Arbib (Academic Press, New York, 1968).

[11] J. Karnofsky and J. Rhodes, 'Decidability of complexity one-half for finite semigroups' **24**: *Semigroup Forum*, pp. 55–66.

[12] G. Lallement, *Semigroups and combinatorial applications* (Wiley, New York, 1979).

[13] S.W. Margolis, 'Problem 14': *Proceedings of the Nebraska conference on semigroups*, Editor Meakin, p. 14.

[14] S.W. Margolis and J.E. Pin, 'Inverse semigroups and extensions of groups by semilattices', *J. Algebra* **110** (1987), 277–297.

[15] S.W. Margolis and J.E. Pin, 'Expansions, free inverse semigroups, and Schützenberger product', *J. Algebra* **110** (1987), 298–305.

[16] S.W. Margolic and J.E. Pin, 'Inverse semigroups and varieties of finite semigroups', *J. Algebra* **110** (1987), 306–323.

[17] D.B. MacAlister, 'Regular semigroups, fundamental semigroups and groups', Ser. A, *J. Austral. Math. Soc.* **29** (1980), 475–503.

[18] J.E. Pin, *Varieties of formal languages* (Plenum Press, New York, 1986).

[19] J. Rhodes, 'New techniques in global semigroup theory', in *Semigroups and their applications*, Editors S. Goberstein and P. Higgins, pp. 169–182 (Reidel, Dordrecht, 1986).

[20] J. Rhodes, 'Global structure theorems for arbitrary semigroups': *Proc. of the 1984 Marquette Conf. on Semigroups.* Editors K. Byleen, P. Jones and F. Pastijn .

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

[22] I. Simon, (Simon's lemma in [7]).

[23] B. Tilson, 'Type II Redux', in *Semigroups and their applications*, Editors S. Goberstein and P. Higgins, pp. 201–206 (Reidel, Dordrecht, 1986).

[24] B. Tilson, 'Categories as algebra', *J. Pure Appl. Algebra* **48** (1987), 83–198.

[25] D. Thérien, 'On the equation $x^t = x^{t+g}$ in categories', *Semigroup Forum* **37** (1988), 265–272.

[26] D. Thérien and A. Weiss, 'Varieties of finite categories', *RAIRO Inform Théor. Appl.* **20** (1986).

[27] D. Thérien and A. Weiss, 'Graph congruences and wreath product', *J. Pure Appl. Algebra* **36** (1985), 205–215.

Computer Science Department
University of Nebraska
Lincoln, NE 68588 USA

Mathematics Department
University of California
Berkeley, CA 94720 USA