J. Austral. Math. Soc. (*Series A*) **43** (1987), 81–90

FINITE SEMIGROUPS WITH COMMUTING IDEMPOTENTS

C. J. ASH

(Received 15 July 1985)

Communicated by T. E. Hall

Abstract

We show that every such semigroup is a homomorphic image of a subsemigroup of some finite inverse semigroup. This shows that the pseudovariety generated by the finite inverse semigroups consists of exactly the finite semigroups with commuting idempotents.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 20 M 10; secondary 20 M 35.

Introduction

Let S be a finite semigroup in which every two idempotents commute. The main result of this paper is Theorem 2, that for every such semigroup S there exist a finite inverse semigroup I, a subsemigroup T of I and a homomorphism from T onto S.

This result may be regarded as a structure theorem for finite semigroups with commuting idempotents. It may also be viewed in the light of the notion of a pseudovariety. A pseudovariety of semigroups is a class of finite semigroups closed under the formation of subsemigroups, finite direct products and homomorphic images. By Theorem 1, the class of all finite semigroups with commuting idempotents is a pseudovariety. Thus, since this class contains all finite inverse semigroups, it includes the pseudovariety generated by the finite inverse semigroups. Theorem 2 therefore establishes the reverse inclusion, showing that the pseudovariety generated by the finite inverse semigroups is exactly the class of all finite inverse semigroups with commuting idempotents.

The question thus answered in this paper was posed by S. Margolis [4] in 1980 and is discussed further in [5], [6] and [7]. For the sake of completeness, we give again the easier half of our result in Theorem 1 and its Corollary.

For unexplained terminology and semigroups in general we refer to [1], [2] or [3].

THEOREM 1. *The class of all finite semigroups in which idempotents commute is a pseudovariety.*

PROOF. We must show that the class is closed under the formation of subsemigroups, finite direct products and homomorphic images. The first two of these are immediate. For the third, suppose that T is finite, that $\phi: T \to S$ is a surjective homomorphism and that idempotents in T commute. Let e, f be idempotents in S. Consider $\{x \in T: \phi(x) = e\}$. Then this is a finite subsemigroup of T and so contains at least one idempotent, e', say, of T. Similarly, let f' be an idempotent of T for which $\phi(f') = f$. Then $ef = \phi(e')\phi(f') = \phi(e'f') = \phi(f'e') = \phi(f')\phi(e') = fe$.

COROLLARY. *The pseudovariety generated by the finite inverse semigroups consists only of finite semigroups with commuting idempotents.*

We now proceed to the converse of this corollary. We need to establish some properties of semigroups of this kind.

LEMMA 1. *Let S be a semigroup with commuting idempotents.*

(i) *Let $u, v, e, f \in S$ where e, f are idempotents.*

(a) *If $fu = v$ and $ev = u$ then $u = v$.*

(b) *If $uf = v$ and $ve = u$ then $u = v$.*

(ii) *If u, v are regular elements of S with inverses u', v' respectively and if $uu'v = u$ and $vv'u = v$, then $u = v$.*

(iii) *If S is finite, $u, v, s \in S$, $u \mathscr{R} us$, $v \mathscr{R} vs$ and $us = vs$, then $u = v$.*

(iv) *The regular elements of S form a subsemigroup. More generally, if uv and vw are regular, then so is uvw.*

PROOF. (i) (a) $u = ev = e(fu) = (ef)u = (fe)u = (fe)(ev) = fe^2v = f(ev) = fu = v$. (b) Similarly.

(ii) Let $e = uu'$, $f = vv'$. Then e, f are idempotents and $ev = u$, $fu = v$. So $u = v$, by (i)(a).

(iii) Since S is finite, there is a positive integer N such that for all $x \in S$, x^N is idempotent. Now let $p, q \in S^1$ be such that $usp = u$ and $vsq = v$, since $us \mathscr{R} u$ and $vs \mathscr{R} v$. Then $u(sp)^N = u$ and $v(sq)^N = v$.

https://doi.org/10.1017/S1446788700028998 Published online by Cambridge University Press

Putting $e = (sp)^N$ and $f = (sq)^N$ we have $uf = u(sq)^N = v(sq)^N$ (since $us = vs$) $= v$. Similarly, $ve = v(sp)^N = u(sp)^N = u$. So, by (i)(b), we have $u = v$.

(iv) Let u, v be regular with inverses u', v' respectively. Then $u'u$ and vv' are idempotents and so $(uv)(v'u')(uv) = u(vv')(u'u)v = u(u'u)(vv')v = uv$. Thus, uv is regular.

(The subsemigroup of regular elements is thus clearly a regular semigroup in which idempotents commute and is therefore an inverse semigroup.)

Similarly, if uv and vw are regular, having inverses p and q respectively, then we may check that vwq and vpu are idempotent and so $(uvw)(qvp)(uvw) = u(vwq)(vpu)vw = u(vpu)(vwq)vw = (uvpuv)(wqvw) = (uv)(wqvw) = u(vwqvw) = uvw$. Thus, uvw is regular.

We need also to use the following property of the partial ordering of the $\mathscr{J}$-classes.

LEMMA 2. *If S is a finite semigroup, $v, x \in S$, v is regular and vx is not, then $\mathscr{J}(vx) < \mathscr{J}(v)$.*

PROOF. Certainly $\mathscr{J}(vx) \leqslant \mathscr{J}(v)$. Suppose that $\mathscr{J}(vx) = \mathscr{J}(v)$. Then we have $v = a(vx)b$ for some $a, b \in S^1$.

Let N be such that, for all $s \in S$, s^N is idempotent. Then $v = a^N v(xb)^N$ and so $v(xb)^N = v$. But now if v' is an inverse of v, we have

$(vx)[b(xb)^{N-1}v'](vx) = v(xb)^N v'vx = vv'vx = vx$, so vx is regular, contradiction.

From now on, let S be any fixed finite semigroup with commuting idempotents. Let $s_1, \ldots, s_n$ be a fixed sequence of generators for S. (We could let $S = \{s_1, \ldots, s_n\}$.) Let F denote the free semigroup on n generators. Thus the elements of F may be viewed as finite non-empty sequences or "words" from the set $\{x_1, \ldots, x_n\}$ of symbols.

There is a unique homomorphism from F to S which maps each x_i to s_i for $i = 1, \ldots, n$. We denote by $w(S)$ the image of $w \in F$ under this homomorphism. Of course this depends on the fixed choice of $s_1, \ldots, s_n$.

We find it most convenient to describe our inverse semigroups in terms of the inverse semigroups $\mathscr{I}(A)$ of all partial one-one functions on a set A. We therefore define a *system* to mean a sequence $\mathscr{A} = (A, \alpha_1, \ldots, \alpha_n)$ where A is a finite set and each α_i is a partial one-one function on A. There is a unique homomorphism from F into $\mathscr{I}(A)$ which maps each x_i to α_i for $i = 1, \ldots, n$. We denote by $w(\mathscr{A})$ the image of $w \in F$ under this homomorphism.

For each set X, $|X|$ denotes the cardinality of X. Similarly for a semigroup S, $|S|$ denotes the cardinality of S and for a system $\mathscr{A} = (A, \alpha_1, \ldots, \alpha_n)$, we also denote $|A|$ by $|\mathscr{A}|$.

We may reformulate our problem in terms of systems, as follows.

LEMMA 3. *To show that S is a homomorphic image of a subsemigroup of an inverse semigroup, it is sufficient to show that there exists an integer K such that if $w_1, w_2 \in F$ and $w_1(S) \neq w_2(S)$ then there is a system $\mathscr{A}$ for which $|\mathscr{A}| \leqslant K$ and $w_1(\mathscr{A}) \neq w_2(\mathscr{A})$.*

PROOF. Let $\mathscr{A}_j = (A_j, \alpha_1^{(j)}, \ldots, \alpha_n^{(j)})$ be all the finitely many systems $\mathscr{A}$ for which $|\mathscr{A}| \leqslant K$. We may let I be the inverse semigroup $\prod_j \mathscr{I}(A_j)$ and let T be the subsemigroup of I generated by $t_1, \ldots, t_n$ where $t_i(j) = \alpha_i^{(j)}$. For $w \in F$, let $w(T)$ denote the image of w under the homomorphism from F to T which maps each x_i to t_i. Then, by the assumed condition, we have that if $w_1, w_2 \in F$ and $w_1(S) \neq w_2(S)$ then, for some j, $w_1(\mathscr{A}_j) \neq w_2(\mathscr{A}_j)$ and so $w_1(T) \neq w_2(T)$. Thus the map $w(T) \to w(S)$ is a well defined homomorphism from T onto S.

COMMENT. In devising these arguments, we had frequent recourse to sketches of these systems, treating them as directed graphs each of whose edges is labelled with one of the symbols $s_1, \ldots, s_n$. The reader may well prefer to reinstate such sketches. The case $n = 2$ is sufficiently representative. (In fact, although we do not need to use this, T. E. Hall has show that every finite idempotent commuting semigroup embeds into a finite two-generator idempotent commuting semigroup.) In the terminology of automata, what we call a system is an injective $\{x_1, \ldots, x_n\}$-automaton except that no initial or final states are specified.

A supply of systems is provided by S itself as follows.

DEFINITION. Let R be any $\mathscr{R}$-class of S. For $i = 1, \ldots, n$, let ρ_i be the partial function on R defined, for each $a \in R$, as follows.

$$a\rho_i = \begin{cases} as_i & \text{if } a\mathscr{R}as_i, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Now let $\mathscr{A}(R)$ denote $(R, \rho_1, \ldots, \rho_n)$.

LEMMA 4. (i) *Each $\mathscr{A}(R)$ is a system.*

(ii) *For each $a \in R$, $w \in F$,*

$$aw(\mathscr{A}(R)) = \begin{cases} aw(S) & \text{if } a\mathscr{R}aw(S), \\ \text{undefined} & \text{otherwise.} \end{cases}$$

(iii) *If $w_1(S)$ and $w_2(S)$ are regular elements of S where $w_1(S) \neq w_2(S)$, then there exists a system $\mathscr{A}$ with $|\mathscr{A}| \leqslant |S|$ for which $w_1(\mathscr{A}) \neq w_2(\mathscr{A})$.*

(iv) *If* $w(S)$ *is regular and* $(wx_k)(S)$ *is not, then there exists a system* $\mathscr{A} = (A, \alpha_1, \ldots, \alpha_n)$ *and* $a \in A$ *for which* $|\mathscr{A}| \leqslant |S|$, $aw(\mathscr{A})$ *is defined and* $aw(\mathscr{A}) \notin \mathrm{dom}(\alpha_k)$.

(v) *Similarly, if* $w(S)$ *is regular and* $(x_j w)(S)$ *is not, then there exist* $\mathscr{A} = (A, \alpha_1, \ldots, \alpha_n)$ *and* $a \in A$ *for which* $|\mathscr{A}| \leqslant |S|$, $aw(\mathscr{A})$ *is defined and* $a \notin \mathrm{ran}(\alpha_j)$.

PROOF. (i) To show that each ρ_i is one-one, suppose that $u, v \in R$, that $u\rho_i$, $v\rho_i$ are defined and that $u\rho_i = v\rho_i$. Then $u\mathscr{R}us_i$, $v\mathscr{R}vs_i$ and $us_i = vs_i$. Therefore, by Lemma 1 (iii), $u = v$.

(ii) By induction on the length of w. We need only to consider $w = w_0 x_j$ and observe that, from the definitions, $w(\mathscr{A}) = w_0(\mathscr{A})\rho_j$ and from the properties of $\mathscr{R}$, that $a\mathscr{R}aw_0(S)s_j$ iff both $a\mathscr{R}aw_0(S)$ and $aw_0(S)\mathscr{R}aw_0(S)s_j$.

(iii) Let $u = w_1(S)$, $v = w_2(S)$ and let u', v' be inverses of u and v respectively. Then we claim that $\mathscr{A} = \mathscr{A}(R)$ has the desired property where R is one or other of the $\mathscr{R}$-classes of uu' of vv'. Taking R to be the $\mathscr{R}$-class of uu', we have $(uu')w_1(\mathscr{A}) = uu'u = u$ by (ii), so, if $w_1(\mathscr{A}) = w_2(\mathscr{A})$ in this case, we must also have $uu'w_2(A) = u$ and so $uu'v = u$.

Similarly, if $w_1(\mathscr{A}) = w_2(\mathscr{A})$ when R is taken to be the $\mathscr{R}$-class of vv', we must have $vv'u = v$.

But then $u = v$, by Lemma 1 (ii), contrary to the assumption that $w_1(S) \neq w_2(S)$.

(iv) Let $u = w(S)$ and let u' be an inverse of u. We may take $\mathscr{A}$ to be $\mathscr{A}(R)$ where R is the $\mathscr{R}$-class of uu', and take a to be uu'. Then $(uu')u = u$, so $aw(\mathscr{A}) = u$, by (ii). To see that $aw(\mathscr{A}) \notin \mathrm{dom}(\alpha_k)$, suppose otherwise. Then $us_k\mathscr{R}u$, so we may let $t \in S^1$ be such that $us_k t = u$. Thus $us_k(tu')us_k = (us_k t)u'us_k = uu'us_k = us_k$, so $us_k = (wx_k)(S)$ is regular, contrary to the assumption.

(v) We could show that by defining systems on the $\mathscr{L}$-classes of S similarly to the $\mathscr{A}(R)$. For the sake of brevity, let us instead consider the dual semigroup $\hat{S}$ with the same generators $s_1, s_2, \ldots, s_n$ and, for each $w_0 \in F$, let $\hat{w}_0$ denote the result of reversing the word w_0, so that $\hat{w}_0(\hat{S}) = w_0(S)$.

Then $\hat{w}(\hat{S})$ is regular in $\hat{S}$, while $\widehat{(x_j w)}(\hat{S}) = (\hat{w}x_j)(\hat{S})$ is not. So, applying (iv) above to the semigroup $\hat{S}$, there is a system $\mathscr{B} = (A, \beta_1, \ldots, \beta_n)$ such that $|\mathscr{B}| \leqslant |S|$ and such that, for some $b \in A$, $b\hat{w}(\mathscr{B})$ is defined while $b\hat{w}(\mathscr{B}) \notin \mathrm{dom}(\beta_j)$. We may now take $a = b\hat{w}(\mathscr{B})$ and $\mathscr{A} = (A, \alpha_1, \ldots, \alpha_n)$ where each α_i is the inverse of the function β_i.

Thus, Lemma 4 (iii) shows that we already have systems fulfilling the requirements of Lemma 3 for those words whose values in S are regular. For the general case, we shall "patch together" old systems to obtain new ones, at which stage we use the details of parts (iv) and (v) of Lemma 4.

A simple device allows us sometimes to combine known properties of systems.

DEFINITION. For two systems $\mathscr{A} = (A, \alpha_1, \ldots, \alpha_n)$ and $\mathscr{B} = (B, \beta_1, \ldots, \beta_n)$ we let $\mathscr{A} \times \mathscr{B}$ denote the new system $(A \times B, \gamma_1, \ldots, \gamma_n)$ where, for each i, $(a, b)\gamma_i = (a\alpha_i, b\beta_i)$.

We use the following properties of $\mathscr{A} \times \mathscr{B}$.

LEMMA 5. (i) *Suppose that* $a_1 w(\mathscr{A}) = a_2$, $a_1 \notin \operatorname{ran}(\alpha_j)$, $b_1 w(\mathscr{B}) = b_2$ *and* $b_2 \notin \operatorname{dom}(\beta_k)$. *Then in* $\mathscr{A} \times \mathscr{B}$ *there exist* c_1, c_2 *for which* $c_1 w(\mathscr{A} \times \mathscr{B}) = c_2$, $c_1 \notin \operatorname{ran}(\gamma_j)$ *and* $c_2 \notin \operatorname{dom}(\gamma_k)$.

(ii) *Suppose that* $a_1 w_1(\mathscr{A}) = a_1 w_2(\mathscr{A}) = a_2$, $a_1 \notin \operatorname{ran}(\alpha_j)$ *and* $a_2 \notin \operatorname{dom}(\alpha_k)$. *Suppose also* $b_1 w_1(\beta) = b_2$ *while* $b_1 w_2(\mathscr{B}) \neq b_2$ (*where* $b_1 w_2(\mathscr{B})$ *may or may not be defined*). *Then there exist* c_1, c_2 *such that* $c_1 w_1(\mathscr{A} \times \mathscr{B}) = c_2$, $c_1 \notin \operatorname{ran}(\gamma_j)$ *and* $c_2 \notin \operatorname{dom}(\gamma_k)$. *If* $b_1 w_2(\mathscr{B})$ *is undefined, then* $c_1 w_2(\mathscr{A} \times \mathscr{B})$ *is undefined, while if* $b_1 w_2(\mathscr{B})$ *is defined then* $c_1 w_2(\mathscr{A} \times \mathscr{B}) \notin \operatorname{dom}(\gamma_k)$.

PROOF. In each case we take $c_1 = (a_1, b_1)$ and $c_2 = (a_2, b_2)$. The statements follow immediately from the observations that $\operatorname{ran}(\gamma_j) = \operatorname{ran}(\alpha_j) \times \operatorname{ran}(\beta_j)$, $\operatorname{dom}(\gamma_k) = \operatorname{dom}(\alpha_k) \times \operatorname{dom}(\beta_k)$ and that $(a, b)w(\mathscr{A} \times \mathscr{B})$ is defined iff both $aw(\mathscr{A})$ and $bw(\mathscr{B})$ are defined, in which case $(a, b)w(\mathscr{A} \times \mathscr{B}) = (aw(\mathscr{A}), bw(\mathscr{B}))$.

The last ingredient of our proof is to show that, even if $w(S)$ is not regular, each word w may still be written in the form $w = w_1 w_2 \cdots w_m$ so that the total length of those w_i for which $w_i(S)$ is not regular is bounded.

In showing this, we use Ramsey's Theorem [3] in the form that for every finite set S there is a number M such that, for every set U of integers for which $|U| > M$ and for every function f from $\{(u, v) \in U \times U : u < v\}$ into S there exist $r, s, t \in U$ for which $r < s < t$ and $f(r, s) = f(r, t) = f(s, t)$.

PROPOSITION 6. *Let* S *be a finite semigroup, with commuting idempotents, let* F *be the free semigroup on the letters* $x_1, \ldots, x_n$ *and let* $w \mapsto w(S)$ *be a homomorphism from* F *to* S.

Then there is a number M, *depending only on* S, *such that for every word* $w \in F$, w *can be written in the form* $u_0 v_1 u_1 v_2 \cdots v_k u_k$ *satisfying the following conditions.*

(1) *Each* $v_i(S)$ *is regular in* S.

(2) *If* x_j, *is the last symbol of* u, *then* $(x_j v_i)(S)$ *is not regular in* S.

(3) *If* x_k *is the first symbol of* u_{i+1} *then* $(v_i x_k)(S)$ *is not regular in* S.

(4) *The word* $u_0 u_1 \cdots u_k$ *has length* $\leqslant M$.

https://doi.org/10.1017/S1446788700028998 Published online by Cambridge University Press

Here we allow the possibilities that u_0 or u_k is the empty word or that $k = 0$, so that no v_i occurs. However, we require that each v_i for $i = 1, \ldots, k$ and each u_i for $i = 1, \ldots, (k-1)$ is nonempty.

PROOF. Let $w = y_1 y_2 \cdots y_m$ where each y_r is one of $x_1, \ldots, x_n$. Say that a set is *good* if it is of the form $\{r, r+1, \ldots, r+s\}$ where $1 \leqslant r \leqslant r+s \leqslant m$ and if $v(S)$ is regular, where v is the word $y_r y_{r+1} \cdots y_{r+s}$. A *maximal* good set means a good set which is not a proper subset of any other good set.

Now let $\{r, r+1, \ldots, r+s\}$ and $\{r', r'+1, \ldots, r'+s'\}$ be any two distinct maximal good sets. Then we may easily see that either $r+s+2 \leqslant r'$ or $r'+s'+2 \leqslant r$. Otherwise the two sets are adjacent or overlapping, in which case the corresponding words are pq and qr where $p, r \in F$, $q \in F^1$ and $p(S)q(S)$ and $q(S)r(S)$ are regular. But then by Lemma 1 (iv), $p(S)q(S)r(S)$ is also regular, so the union of the two sets is also good, contradicting their maximality.

Thus the maximal good sets (if any) are $\{r_1, r_1+1, \ldots, r_1+s_1\}$, $\{r_2, r_2+1, \ldots, r_2+s_2\}, \ldots, \{r_k, r_k+1, \ldots, r_k+s_k\}$ where $r_i + s_i + 2 \leqslant r_{i+1}$, and we may take $v_i = y_{r_i} \cdots y_{r_i+s_i}$ for $1 \leqslant i \leqslant k$ and $u_{i+1} = y_{r_i+s_i+1} \cdots y_{r_{i+1}-1}$ for $0 \leqslant i \leqslant k$, with the conventions that $r_0 = s_0 = 0$ and $r_{k+1} = 1 = m$ Then certainly $w = u_0 v_1 \cdots v_k u_k$, and each $v_i(S)$ is regular.

Conditions (2) and (3) follow immediately from the maximality of the sets. For condition (4), let U be the set of all $r \in \{1, \ldots, m\}$ which do not appear in any of the maximal good sets. It remains to show that $|U|$ is bounded independently of w.

For $r, s \in U$ with $r < s$, let $w_{r,s} = y_r y_{r+1} \cdots y_{s-1}$, and let $f(r,s) = w_{r,s}(S)$. By Ramsey's Theorem, there exists an M, depending only on $|S|$, for which, if $|U| > M$ then there exist $r, s, t \in U$ with $r < s < t$ for which $f(r,s) = f(r,t) = f(s,t)$, that is, $w_{rs}(S) = w_{rt}(S) = w_{st}(S) = w$, say. But in this case $w_{rt} = w_{rs} w_{st}$, so $x^2 = x$. Thus $w_{rs}(S)$ is idempotent in S and is therefore regular, so that $\{r, r+1, \ldots, s-1\}$ is a good set and so is included in one of the maximal good sets, contradicting that $r \in U$. Hence for this M we always have $|U| \leqslant M$.

NOTE. It follows from (2) and (3) and from Lemma 2 and its dual that, for each i, $\mathscr{J}(v_i(S)) > \mathscr{J}(w(S))$, except for the case where $w = v_i$.

THEOREM 2. *Let S be a finite semigroup in which idempotents commute. Then S is a homomorphic image of a subsemigroup of some finite inverse semigroup.*

PROOF. For each $s \in S$, let $d(s)$ denote the number of $\mathscr{J}$-classes of S strictly above that of s. We proceed by induction on h to show that, for each h there exists a number $K(h)$ such that whenever $w, w' \in F$, $w(S) \neq w'(S)$ and $d(w(S)) + d(w'(S)) = h$ then there exists a system $\mathscr{A}$ for which $|\mathscr{A}| \leqslant K(h)$ and

https://doi.org/10.1017/S1446788700028998 Published online by Cambridge University Press

$w(\mathscr{A}) \neq w'(\mathscr{A})$. Since S is finite we may then take $K = \max\{K(h) : h = d(s) + d(t), s, t \in S\}$ and the result follows immediately by Lemma 1.

Thus, suppose that $w, w' \in F$, $w(S) \neq w'(S)$ and $d(w(S)) + d(w'(S)) = h$. If w, w' are both regular, then we may use Lemma 4 by ensuring that $K(h) \geqslant |S|$. So without loss of generality, we may suppose that w is not regular. Let $w = u_0 v_1 \cdots v_k u_k$ as in Proposition 6.

Our notation will correspond to the case where $k \neq 0$ and both u_0 and u_k are nonempty, but the other cases may be treated in just the same way except for obvious modifications. Let $u_i = u_{i0} \cdots u_{il(i)}$ where each u_{ir} is one of $x_1, \ldots, x_n$. In particular, let u_{i0} be $x_{k(i)}$ and $u_{il(i)}$ be $x_{j(i)}$. Then, from the statement of Proposition 6, each $v_i(S)$ is regular while $(x_{j(i-1)}v_i)(S)$ and $(v_i x_{k(i)})(S)$ are not. So, by Lemma 4 (iii), (iv) and Lemma 5 (i), there is, for each i, a system $\mathscr{A}_i = (A_i, \alpha_1^{(i)}, \ldots, \alpha_n^{(i)})$ having elements a_i, b_i for which $a_i v_i(\mathscr{A}_i) = b_i$, $a_i \notin \operatorname{ran}(\alpha_{j(i-1)}^{(i)})$ and $b_i \notin \operatorname{dom}(\alpha_{k(i)}^{(i)})$.

We may now form a composite system $\mathscr{A} = (A, \alpha_1, \ldots, \alpha_n)$, where A is the disjoint union of the A_i together with new elements p_{ir} for $0 \leqslant i \leqslant k$, $1 \leqslant r \leqslant l(i)$ and also $p = p_{00}$ and $q = p_{k,l(k+1)}$. We define each α_j as follows. For an element a of some A_i where $a \neq b_i$, we define $a\alpha_j = a\alpha_j^{(i)}$. We let $b_i\alpha_j = b_i\alpha_j^{(i)}$ except for $j = k(i)$ in which case $b_i\alpha_j^{(i)}$ is undefined and we instead define $b_i\alpha_{k(i)} = p_{i1}$. For each element of the form p_{ir}, we let $p_{ir}\alpha_j$ be undefined unless $u_{ir} = x_j$, in which case, for $0 \leqslant r < l(i)$ or $i = k$ and $r = l(k)$, we define $p_{ir}\alpha_j = p_{i,r+1}$. For $i < k$ and $u_{il(k)} = x_j$ (that is, $j = j(i)$), we let $P_{il(k)}\alpha_j = a_{i+1}$, and we let $q\alpha_j$ be undefined for each j. The α_j may be seen to be one-one because of the choice of the $\mathscr{A}_i$, a_i and b_i.

The effect of this definition is that $pu_0(\mathscr{A}) = a_1$, $a_1 v_1(\mathscr{A}) = b_1$, $b_1 u_1(\mathscr{A}) = a_2, \ldots, a_k v_k(\mathscr{A}) = b_k$ and $b_k u_k(\mathscr{A}) = q$. So $pw(\mathscr{A}) = q$. Now, since the total length of the u_i is at most the number M described in Lemma 6, we have $|\mathscr{A}| \leqslant k|S|^2 + M - k + 1$. For the same reason, $k \leqslant M + 1$ and so $|\mathscr{A}| \leqslant (M + 1)|S|^2$. So the result is proved in the case where $w(\mathscr{A}) \neq w'(\mathscr{A})$ by ensuring that $K(h) \geqslant (m + 1)|S|^2$.

We may thus suppose that $w(\mathscr{A}) = w'(\mathscr{A})$, and in particular, $pw'(\mathscr{A}) = q$. But in $\mathscr{A}$, the only sequences of elements which lead from p to q and in which each arises from its predecessor by applying some α_j, are of the form

$$p = p_{00}, p_{01}, \ldots, p_{0l(0)}, a_1, \ldots, b_1, p_{11}, p_{12}, \ldots, p_{1l(1)},$$

$$a_2, \ldots, b_2, \ldots, a_k, \ldots, b_k, p_{k1}, \ldots, p_{kl(k)}, q.$$

Moreover, the *only* α_j for which $p_{ir}\alpha_j = p_{ir+1}$ is that for which $u_{ir} = \alpha_j$. It follows that w' must be of the form $u_0 v_1' u_1 v_2' \cdots v_k' u_k$ where the u_i are the same as in the decomposition of w and where, for each i, $a_i v_i'(\mathscr{A}) = b_i$.

https://doi.org/10.1017/S1446788700028998 Published online by Cambridge University Press

Of course, this expression for w' need not be the decomposition of w' given by Proposition 6, but certainly, for each i, $\mathscr{J}(v_i'(S)) \geqslant \mathscr{J}(w'(S))$ while, by the note following Proposition 6, and since $w(S)$ is assumed not to be regular, $\mathscr{J}(v_i(S)) > \mathscr{J}(w(S))$. Now, since $w(S) \neq w'(S)$, there is at least one m for which $v_m(S) \neq v_m'(S)$. Let one such m be chosen. Then $h_0 = d(v_m(S)) + d(v_m'(S)) < d(w(S)) + d(w'(S))$ and so we may apply the induction hypothesis to obtain a system $\mathscr{B}$ with $|\mathscr{B}| \leqslant K(h_0)$ for which $v_m(\mathscr{B}) \neq v_m'(\mathscr{B})$.

The argument is symmetrical with respect to w and w' from this point onwards. We use only that, for each i, $a_i v_i^{(')}(\mathscr{A}) = b_i$ and that $v_m(\mathscr{B}) \neq v_m'(\mathscr{B})$. So without loss of generality we may suppose that there exist c and d for which $cv_m(\mathscr{B}) = d$ and $cv_m'(\mathscr{B}) \neq d$, whre $cv_m'(\mathscr{B})$ may or may not be defined.

Now we may form the system $\mathscr{B}' = \mathscr{A}_m \times \mathscr{B}$ and take $a' = (a_m, c)$ and $b' = (b_m, d)$, so that, by Lemma 5 and by the choice of $\mathscr{A}_m$ and $\mathscr{B}$, we have $a'v_m(\mathscr{B}') = b'$, $a'v_m'(\mathscr{B}) \neq b'$, $a' \notin \operatorname{ran}(\alpha_{j(m-1)})$ and $b' \notin \operatorname{dom}(\alpha_{k(m)})$. Let $\mathscr{A}' = (A', \alpha_1', \ldots, \alpha_n')$ be the new system defined in just the same way as $\mathscr{A}$ except that $\mathscr{A}_m$, a_m and b_m are replaced by $\mathscr{B}'$, a' and b'. Then, since $a'v_m(\mathscr{B}') = b'$, we still have $a'v_m(\mathscr{A}') = b'$.

We now show that if $a'v_m'(\mathscr{A}')$ is defined, then $a'v_m(\mathscr{A}') \in \mathscr{B}'$ and $a'v_m'(\mathscr{A}') \neq b'$. Suppose that $a'v_m'(\mathscr{A}')$ is defined. If $a'v_m'(\mathscr{A}') \notin \mathscr{B}'$ then we must have $v_m' = ux_{k(m)}v$ where $a'u(\mathscr{A}') = b'$. So $a'u(\mathscr{B}') = b'$ and therefore $a_m u(\mathscr{A}_m) = b_m$. But then $a_m u(\mathscr{A}_m)x_{k(m)}(\mathscr{A}) \notin \mathscr{A}_m$ and so $a_m v_m'(\mathscr{A}) \notin \mathscr{A}_m$, which contradicts the fact that $a_m v_m'(\mathscr{A}) = b_m$. So if $a'v_m'(\mathscr{A}')$ is defined, then $a'v_m'(\mathscr{A}') \in \mathscr{B}'$. Thus $a'v_m'(\mathscr{A}') = a'v_m'(\mathscr{B}')$. But $a'v_m'(\mathscr{B}') \neq b'$, since $cv_m'(\mathscr{B}) \neq cv_m(\mathscr{B})$.

Now let $a'v_m'(\mathscr{B}') = (b_m, d')$ where $d' \neq d$. Then $a'v_m'(\mathscr{B}')x_{k(m)}(\mathscr{B}')$ is undefined, since $b_m x_{k(m)}(\mathscr{A}_m)$ is undefined. Hence $a'(v_m'x_{k(m)})(\mathscr{A}') = a'v_m'(\mathscr{B}')x_{k(m)}(\mathscr{A}')$ is also undefined, since $(b_m, d') \neq b'$. It follows that $pw'(\mathscr{A}')$ is undefined, and so $w'(\mathscr{A}') \neq w(\mathscr{A}')$. [In the case where $m = k$ and u_k is empty, we conclude only that if $a'v_m'(\mathscr{A}')$ is defined then $pw'(\mathscr{A}') = a'v_m'(\mathscr{A}') \neq b'$, but then again $w'(\mathscr{A}) \neq w(\mathscr{A})$.]

Since $\mathscr{A}'$ is obtained from $\mathscr{A}$ by replacing $\mathscr{A}_m$ by $\mathscr{A}_m \times \mathscr{B}$, we see that $|\mathscr{A}'| \leqslant (M+1)|S|^2 + |S|^2(K(h_0) - 1) = |S|^2(M + K(h_0))$. The proof is therefore complete if we ensure that $K(h) \geqslant |S|^2(M + K(h_0))$ for all $h_0 < h$, which implies the other conditions previously mentioned provided that $K(0) \geqslant (M+1)|S|^2$.

Acknowledgement

The author would like to thank T. E. Hall for acquainting him with this problem and for providing him in the course of several conversations with many of the essential ingredients, in particular, Lemma 4 (i), (ii), (iii).

References

[1] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups*, Vols. I & II, Math. Surveys No. 7 (Amer. Math. Soc., Providence, R. I., 1961 & 1967).
[2] J. M. Howie, *An introduction to semigroup theory* (L. M. S. Monographs, Academic Press, London, 1976).
[3] G. Lallement, *Semigroups and combinatorial applications* (Wiley, 1981).
[4] S. Margolis, 'Problem M1', *Proceedings of Nebraska Conference on semigroups*, edited by J. Meakin, p. 14 (1980).
[5] S. Margolis and J. E. Pin, 'Languages and inverse semigroups', 11*th ICALP*, pp. 337–346 (Lecture Notes in Computer Science 172, 1984).
[6] S. Margolis and J. E. Pin, 'Graphs, inverse semigroups and languages', *Proceedings of* 1984 *Marquette conference on semigroups*, pp. 85–112.
[7] J. E. Pin, *Variétés de langages formels* (Masson, Paris, 1984).
[8] F. P. Ramsey, 'On a problem of formal logic', *Proc. London Math. Soc.* **30** (1930), 264–286.

Department of Mathematics
Monash University
Clayton, Victoria 3168
Australia