J. Austral. Math. Soc. **70** (2001), 293–309

REMARKS CONCERNING FINITELY GENERATED SEMIGROUPS HAVING REGULAR SETS OF UNIQUE NORMAL FORMS

ANDREW CUTTING and ANDREW SOLOMON

(Received 31 January 1999; revised 26 July 2000)

Communicated by D. Easdown

Abstract

Properties such as automaticity, growth and decidability are investigated for the class of finitely generated semigroups which have regular sets of unique normal forms. Knowledge obtained is then applied to the task of demonstrating that a class of semigroups derived from free inverse semigroups under certain closure operations is not automatic.

2000 *Mathematics subject classification*: primary 20M18; secondary 20M05, 20F10.

1. Introduction

Automatic groups are widely studied and are the subject of a major book [3]. In [2] the notion of automaticity is extended to semigroups. The motivation of the present work is to determine whether free inverse semigroups are automatic. In the process of showing that they are not, we demonstrate that for these purposes, it is the property of having a regular set of unique normal forms that is of interest, a property considered in the context of groups by Gilman [5]. Connections with growth are exploited to prove the main theorem, and we also discuss decidability and the word problem.

We proceed now to recall some relevant definitions and notation. For any set X, X^* denotes the set of all words in the elements of X including the empty word ϵ, while X^+ denotes the set of all such words of length at least 1. We refer to the words of length 1 as *letters*. When X^* (respectively X^+) is considered along with the associative binary operation of concatenation, it is referred to as the *free monoid* (respectively

The authors gratefully acknowledge the support of European Commission ESPRIT grant number 24.969, British EPSRC grant GR/L21013 and Canadian National Center of Excellence MITACS project.

free semigroup) on the set X, and has the universal properties one would expect. A *language* over X is a subset of X^*.

Let S be a semigroup and X a set of generators with natural homomorphism $\phi : X^+ \to S$. If $L \subseteq X^+$ is any language such that the restriction of ϕ to L is surjective, say that L is a *language of normal forms for S over X*. If in addition the restriction of ϕ to L is injective, say that L is a language of *unique* normal forms for S over X.

The fact that regular languages are precisely the sets accepted by finite state machines has passed into folklore and we use it freely without comment. For details see [6].

We set out some well known facts about regular languages for later reference.

PROPOSITION 1.1. *Suppose X and Y are finite sets. Then*

(i) *if $K \subseteq Y^*$ is a regular language and $\phi : Y^* \to X^*$ is a monoid homomorphism, then $\phi(K)$ is a regular language over X;*

(ii) *if $K, L \subseteq Y^*$ are regular languages, then so are $K \cup L$, $K \cap L$, $K \setminus L$, KL, K^* and K^+.*

For convenience, we shall refer to a semigroup with a regular set of unique normal forms as a *rational* semigroup. We will see that in contrast with automaticity in semigroups, the property of being rational is independent of the choice of generating set. (This dependence of automaticity on choice of generating set is peculiar to semigroups, while an automatic monoid will have an automatic structure for any finite generating set—see [4] for details.)

1.1. Rational semigroups and automaticity Although the developments in this paper do not depend on the definition of automaticity, we sketch it here by way of background and refer the interested reader to [2] for details. Let S be a semigroup with generating set A and natural homomorphism $\phi : A^+ \to S$. An *automatic structure* for S consists of a regular language $L \subseteq A^+$ of normal forms for S such that (roughly speaking) checking whether two words of L are equal or differ by a factor of a generator can be done by a finite state machine. Any semigroup with an automatic structure over some generating set is called an *automatic semigroup*.

An immediate consequence of [2, Corollary 5.6] is that

LEMMA 1.2. *Any automatic semigroup is a rational semigroup.*

While an automatic semigroup may have an automatic structure over one generating set and not another, we show that the definition of a rational semigroup is independent of the choice of generating sets.

https://doi.org/10.1017/S1446788700002354 Published online by Cambridge University Press

LEMMA 1.3. *If a semigroup has a regular language of unique normal forms over some finite generating set, then it has a regular language of unique normal forms over every finite generating set.*

PROOF. Let L be a regular language of unique normal forms for a semigroup S over some finite generating set Y. Let $\psi_Y : Y^+ \to S$ be the natural homomorphism. Let X be some other generating set for S with natural homomorphism $\psi_X : X^+ \to S$. Then there is a function $\phi : Y \to X^+$ expressing every generator $y \in Y$ as a product of generators in X such that $\psi_X\phi(y) = \psi_Y(y)$. Extend ϕ to a homomorphism. By Proposition 1.1, $\phi(L)$ is a regular language. By definition of ϕ, $\psi_X\phi = \psi_Y$, so that since ψ_Y restricted to L is a bijection, so is ψ_X restricted to $\phi(L)$, proving that $\phi(L)$ is a regular language of unique normal forms for S over X. □

On the other hand, the stronger definition of an automatic semigroup gives rise to a number of interesting properties, most significantly

PROPOSITION 1.4 ([2, Corollary 3.7]). *If S is an automatic semigroup, we can solve the word problem for S in time quadratic in the length of the words.*

1.2. Rational semigroups and decidability We show here that for rather general reasons, rational semigroups have a solvable (recursive) word problem and that the property of being rational is therefore Markov. It has been shown that for finitely presented semigroups [8, 9], groups [1, 11] and inverse semigroups [16], Markov properties are undecidable. For general background on computability, the reader is referred to [6].

Recall that a set is *recursively enumerable* if there is an algorithm to list its elements. We shall say that the word problem of a semigroup is *recursively enumerable* if there is an algorithm which lists all pairs of words in the generators which represent equal elements of the semigroup. It is a simple observation that a finitely presented semigroup has recursively enumerable word problem. For a finitely presented semigroup S and word w in the generators of S, denote by S_w the recursively enumerable set of elements of S equal to w in S.

The word problem for a semigroup is *recursive* (or *solvable*) if there is an algorithm whose input is two words in the generators and which terminates with output 'yes' if they represent the same element of the semigroup and terminates with output 'no' otherwise.

THEOREM 1.5. *Let S be a finitely presented semigroup. Then the word problem for S is solvable if and only if S has a recursively enumerable set of unique normal forms.*

PROOF. Let A be a generating set for S. The direct part is obvious. If a semigroup has solvable word problem, simply list the elements of A^+ in some order. As we arrive

at a word which represents the same element of S as another word already in the list, do not omit it but skip over it to the next word in A^+. In this way we are able to obtain a list of unique normal forms for elements of S.

Conversely, suppose there is a recursively enumerable set L of unique normal forms for S. Given words $u, v \in A^*$ we decide equality in S as follows:

- Since S_u is a recursively enumerable set and L is recursively enumerable, their intersection is also recursively enumerable. By uniqueness, this intersection is a singleton which we denote w_u;
- Compute the unique normal form w_v of v in the same way;
- u and v represent the same element of S precisely when $w_u = w_v$. □

Since a regular language is trivially a recursively enumerable set we have

COROLLARY 1.6. *Rational semigroups (and therefore their finitely generated subsemigroups) have solvable word problem.*

This result is well known for semigroups which are groups, see for instance [3, Section 2.1].

Reflecting on the rather general argument above, we consider it an interesting question to determine what properties a semigroup will enjoy when the word problem and the set of unique normal forms are in other computability classes. For example, if the word problem were solvable by a push-down automaton or the set of unique normal forms were a context-free language.

A Markov property of semigroups [groups, inverse semigroups] is a property $\mathscr{P}$ such that:

- $\mathscr{P}$ is preserved under isomorphism;
- there is a finitely presented semigroup [group, inverse semigroup] which has property $\mathscr{P}$;
- there is a finitely presented semigroup [group, inverse semigroup] which embeds in no semigroup [group, inverse semigroup] with property $\mathscr{P}$.

As mentioned at the beginning of this section, it has been shown that Markov properties of semigroups, groups and inverse semigroups are undecidable. Among Markov properties is the property of having solvable word problem. However it is known [16] that there are undecidable properties which are not Markov.

THEOREM 1.7. *The property of being rational is Markov for semigroups, groups and inverse semigroups.*

PROOF. Since the following argument is completely generic, the reader may replace 'semigroup' with 'group' or 'inverse semigroup' throughout, simply noting that there are finitely presented semigroups S in each class which are automatic and other finitely

presented semigroups T in each class which have insoluble word problem. For details the reader is referred to [16].

By Lemma 1.3 we know that the property of being rational is preserved under isomorphism. Since every automatic semigroup is rational, there are certainly examples with this property. Let T be a finitely presented semigroup with insoluble word problem. Then by Corollary 1.6 T embeds in no semigroup which is rational. □

1.3. Closure operations on the class of rational semigroups In this section we exhibit a number of operations under which the class of rational semigroups is closed. In the following discussion, if S is a semigroup, S^1 will denote the set S with an extra element 1 adjoined which is a multiplicative identity for every element of S^1, and S^0 will denote the set S with an extra element 0 adjoined which is a multiplicative zero for every element of S^0.

PROPOSITION 1.8. *A finitely presented semigroup S is rational if and only if S^1 is rational.*

PROOF. Let S be a rational semigroup with regular language L of unique normal forms over generating set A. Let $B = A \dot{\cup} \{e\}$ be a generating set for S^1 where e maps to 1 under the natural homomorphism. Then L is a regular subset of B^+ and consequently so is $L' = L \cup \{e\}$. That L' is a regular set of unique normal forms for S^1 follows from the fact that there is no element of L which maps to $1 \in S^1$ under the natural homomorphism.

Conversely, suppose S^1 is rational. Then there is a set B of generators, a homomorphism $\phi : B^+ \to S^1$ and a regular language $L \subseteq B^+$ in bijection with S^1 under ϕ.

Firstly note that there is at least one letter $e \in B$ such that $\phi(e) = 1$, for otherwise 1 would be a product of non-identity elements of S, contradicting the definition of S^1. Let $E \subseteq B$ be the set of all e such that $\phi(e) = 1$. Put $A = B \setminus E$ and define $\psi : B^* \to A^*$ by mapping all $e \in E$ to the empty word and fixing the other generators. Put w_1 equal to the preimage of 1 in L under ϕ, then the language $L \setminus \{w_1\}$ is regular and so is $\psi(L \setminus \{w_1\}) \subseteq A^*$. Since none of the elements of $L \setminus \{w_1\}$ are the empty word, nor composed entirely of letters of E, $\psi(L \setminus \{w_1\}) \subseteq A^+$. Defining $\gamma : A^+ \to S$ as the restriction of ϕ to A^+, we see that $\mathrm{Im}(\gamma) = \mathrm{Im}(\phi) \setminus \{1\} = S$, since for all $w \in B^+$, $\phi(w) = 1$ or $\phi(w) = \gamma\psi(w)$, so $\psi(L \setminus \{w_1\})$ is a set of normal forms. If $\gamma(u) = \gamma(v)$ for $u, v \in \psi(L \setminus \{w_1\})$, then $u = \psi(u')$ and $v = \psi(v')$ for some $u', v' \in L \setminus \{w_1\}$. Then

$$\phi(u') = \gamma\psi(u') = \gamma(u) = \gamma(v) = \gamma\psi(v') = \phi(v')$$

which shows that $u' = v'$ by injectivity of ϕ on $L \setminus \{w_1\}$. But then $u = v$ giving injectivity of γ on $\psi(L \setminus \{w_1\})$ as required. □

A simpler argument gives

PROPOSITION 1.9. *A finitely presented semigroup S is rational if and only if S^0 is rational.*

THEOREM 1.10. *Let S be a rational semigroup and I an ideal of S such that S/I has no zero divisors. Then S/I is rational.*

PROOF. Suppose S has a regular language L of unique normal forms over some generating set A. Let $\natural_A : A^+ \to S$ be the natural homomorphism. Let $B = A \setminus \natural_A^{-1}(I) \dot{\cup} \{z\}$. Define $\natural_B : B \to S/I$ by

$$\natural_B(b) = \begin{cases} \natural_A(b) & \text{if } b \in A \setminus \natural_A^{-1}(I) \\ 0 & \text{if } b = z \end{cases}$$

and extend homomorphically. Under this mapping, B is clearly a generating set for S/I.

Let K be the regular language $(L \cap (B \setminus \{z\})^+) \cup \{z\}$ over B. To see that K is a set of normal forms for S/I, note that if $w \in L$ and $\natural_A(w) \in S \setminus I$, the fact that I is an ideal implies each letter of w is in B, so $w \in K$, whence the restriction of $\natural_B$ to K is onto.

Suppose $w_1, w_2 \in K$ and $\natural_B(w_1) = \natural_B(w_2) \in S \setminus I$, then $w_1, w_2 \in L$ so $w_1 = w_2$, by uniqueness in L. If $\natural_B(w) = 0$ then $w \notin K \setminus \{z\}$ since S/I has no zero divisors, therefore $w = z$. □

THEOREM 1.11. *The free product of two semigroups is rational if and only if both factors are rational.*

PROOF. Let S and T be rational semigroups with regular languages of unique normal forms $K \subseteq A^+$ and $L \subseteq B^+$ respectively. The set $(LK)^+ \cup K(LK)^* \cup (LK)^*L \cup (KL)^+$ is again a regular language with a unique representative for each element of $S * T$ as required.

Conversely, suppose $S * T$ is a rational semigroup. The semigroups S^0 and T^0 are Rees quotients of $S * T$ without zero divisors, and are therefore rational by Theorem 1.10, and by Proposition 1.9, S and T are also rational. □

1.4. Growth and rational semigroups We take the following development on the growth of functions from [15]. Consider the set of non-decreasing functions from $\mathbb{N} \to \mathbb{R}^+$. We define a preorder on this set by $f \preceq g$ if and only if there are positive natural numbers m and c such that for every $n \in \mathbb{N}$, $f(n) \leq cg(mn)$. Further define an equivalence relation $\sim$ by $f \sim g$ if $f \preceq g$ and $g \preceq f$. We refer to the $\sim$ equivalence

https://doi.org/10.1017/S1446788700002354 Published online by Cambridge University Press

class of f as the *growth* of f and denote it $[f]$. Then $\leq$ defines a partial order on the growth classes of functions $\mathbb{N} \to \mathbb{R}^+$.

We make some definitions and easy observations about growth which will be used in the sequel without comment. All polynomials of degree d have the same growth, namely $[n^d]$ which we call *polynomial of degree d*. All exponential functions of the form a^n with $a > 1$ a real number have growth $[2^n]$ which we call *exponential*. Clearly, the conditions of growth being polynomial or exponential are mutually exclusive. Growth which is either polynomial or exponential is called *alternative* and growth which is neither polynomial nor exponential is called *intermediate*. Finally we have

PROPOSITION 1.12. *Suppose that for some real numbers* $a, h > 0, b, c \geq 0$ *and for all sufficiently large* $n \in N$ *we have* $g(n) = hf(an + b) + c$, *then* $[f] = [g]$.

We now recall the notion of growth of a semigroup. Let S be a semigroup, A a set of generators for S and $\natural_A : A^+ \to S$ the natural homomorphism. For each $x \in S$ define the *length* $l(x)$ of x to be the least length of a word $w \in A^+$ such that $\natural_A(w) = x$. The *growth function* of S with respect to A is defined in [12] by

$$g_{S,A}(n) = |\{x \in S \mid l(x) \leq n\}|.$$

When S and A are understood, the growth function will be referred to simply as g. It is not difficult to see that the $\sim$-class of the growth function is independent of the generating set A so we can use *growth of the semigroup* to mean the $\sim$-class of any of its growth functions.

Finally we define the notion of growth for a formal language. Let $L \subseteq A^*$ be a language. The *growth function* h_L of L is given by defining $h_L(n)$ to be the number of words of L of length at most n. Then the *growth* of L is $[h_L]$.

1.4.1. Growth of a language of unique normal forms One may also define the growth function of S with respect to A by

$$g(n) = |\natural_A(\{w \in A^+ \mid |w| \leq n\})|$$

and it is an easy exercise to see that this definition is equivalent to the previous one. Let L be a language of unique normal forms for S over A. Then $\natural_A$ is injective on the elements of L so that

$$\begin{aligned} h_L(n) &= |\natural_A(\{w \in L \mid |w| \leq n\})| \\ &\leq |\natural_A(\{w \in A^+ \mid |w| \leq n\})| \\ &= g(n). \end{aligned}$$

Therefore, noting that any semigroup has at least polynomial growth and at most exponential growth, we have

https://doi.org/10.1017/S1446788700002354 Published online by Cambridge University Press

THEOREM 1.13. *The growth of a language of unique normal forms for a semigroup S is bounded above by the growth of S. In particular, if S has polynomial growth, then any language of unique normal forms for S has polynomial growth, and if a language of unique normal forms for S has exponential growth, then so does S.*

Considering this theorem, a number of questions immediately spring to mind: When are the growth of the semigroup and the growth of its language of normal forms in the same class? The growth of the number of paths in a graph is known to be alternative [15], and therefore the growth of a regular language is alternative – is the growth of a rational semigroup necessarily alternative? In [15] it is shown that the growth of any algebra with finite Gröbner basis is alternative.

2. The monogenic free inverse semigroup is not rational

There appears to be consensus among workers in the area of automatic semigroups that it is more difficult to show that a semigroup is not automatic than to show that it is (which is usually a matter of exhibiting an automatic structure for it). In this section we use the fact that the growth of the free monogenic inverse semigroup is polynomial to show that it is not a rational semigroup (and therefore not automatic).

In [3, Chapter 8], it is shown that nilpotent groups are not automatic, and that proof also exploits the fact that nilpotent groups have polynomial growth. Nilpotent groups are, nevertheless, rational. As mentioned by Sims in [13], they have finite confluent rewriting systems under the basic wreath product ordering and it is a simple exercise in the theory of automata that this implies the existence of a regular set of unique normal forms.

2.1. Finite state machines We start with some general facts about finite state machines, a construction used in the subsequent argument. A *finite state machine* consists of a finite set Δ of states, a finite set A of *input letters* and a function $\Gamma : \Delta \times A \to \Delta$ describing the *state transitions*. We extend Γ to a (right) monoid action of A^* on Δ. Denoting by ϵ the empty word in A^*, $\Gamma(\_, \epsilon)$ is therefore the identity on Δ. There is a distinguished state $i \in \Delta$ called the *initial* state and a subset $T \subseteq \Delta$ of *terminal* states. We will usually identify the state machine with its transition function. We also consider the *state graph* of the machine, which has vertex set Δ and an edge from s to t labelled by $a \in A$ if $\Gamma(s, a) = t$.

A word $w \in A^*$ is said to be *accepted* by Γ if $\Gamma(i, w) \in T$. A state $s \in \Delta$ is said to be *accessible* if there is some $w \in A^*$ such that $\Gamma(i, w) = s$ and *coaccessible* if there is a word $w \in A^*$ such that $\Gamma(s, w) \in T$.

The state graph of a state machine influences the growth of the language accepted by the machine in the following way.

THEOREM 2.1. *Suppose the state graph of the state machine Γ has two distinct cycles on an accessible and coaccessible state. Then the language accepted by Γ has exponential growth.*

PROOF. Recall that a cycle in a graph on the vertex s is a path from s to itself passing through no other vertex twice.

Let s be the state with two distinct cycles in the state graph. Since s is accessible and coaccessible, there are words $u, v \in A^*$ such that $\Gamma(i, u) = s$ and $\Gamma(s, v) \in T$. Since the two cycles on s are distinct, there are distinct words $w_1, w_2 \in A^+$ (which are not prefixes of one another) which label the edges of the cycles, such that all words determined by the regular expression $u\{w_1, w_2\}^* v$ are accepted by Γ. Let $l = \operatorname{lcm}(|w_1|, |w_2|)$ and fix $p_1, p_2 \in \mathbb{N}$ such that $l = |w_1|p_1 = |w_2|p_2$. Then the number of words accepted by Γ of length $m = |u| + |v| + lk$ is at least 2^k. Namely, they contain the set of words given by the regular expression $u\{w_1^{p_1}, w_2^{p_2}\}^k v$, all of which are distinct.

Therefore, if the language accepted by the automaton has growth h, we have that $h(m) \geq 2^k = 2^{(m-|u|-|v|)/l}$ as required. □

Theorem 2.1 is an automaton theoretic formulation of the fact that a language not being *simply starred* (described by a regular expression in which the star operator is only applied to singletons) implies that it has exponential growth, a fact explained in [3, Section 1.3]. The next lemma dictates the form of words in a regular language with polynomial growth. In the terminology of [3] one would say that a regular language with polynomial growth is simply starred.

LEMMA 2.2. *Let L be a regular language with polynomial growth accepted by some automaton Γ. L consists of precisely the words of the form*

$$u_1 v_1^{h_1} u_2 v_2^{h_2} \cdots u_m v_m^{h_m} u_{m+1},$$

where $u_1 \cdots u_{m+1}$ labels a cycle free path from the initial state of Γ to a terminal state, $h_i \geq 0$ for all i, $u_2, \ldots, u_m$ are nonempty, and each v_i labels a cycle in the state graph on $\Gamma(i, u_1 \cdots u_i)$.

PROOF. The result follows as a corollary of Theorem 2.1. Since L has polynomial growth, the state graph of Γ has no two cycles on a single accessible and coaccessible state. □

2.2. The monogenic free inverse semigroup For the remainder of Section 2 let FI_x denote the free monogenic inverse semigroup with (semigroup) generating set $\{x, x^{-1}\}$. We pause now to recall some simple facts and standard definitions about this

https://doi.org/10.1017/S1446788700002354 Published online by Cambridge University Press

semigroup. The reader requiring elucidation of the following development is referred to [10].

Let $\bar{\cdot}$ denote the homomorphism of FI_x onto the free group F_x of rank 1 defined by taking any word in $\{x, x^{-1}\}^+$ and freely reducing it, that is to say, cancelling xx^{-1} and $x^{-1}x$. For example, $\overline{xxx^{-1}x} = x^2$.

It is a consequence of the graph representation of free inverse semigroups (see [10, VIII.3]) that FI_x may be identified with the set of triples $(i, j, k) \in \mathbb{Z}^3$ such that $i < j$ and 0 and k are contained in the contiguous interval $[i, j]$. In particular, $i \leq 0 \leq j$. The product $(i, j, k) * (i', j', k')$ is then $(\min(i, k + i'), \max(j, k + j'), k + k')$. Let $\natural : \{x, x^{-1}\}^+ \to FI_x$ be the natural homomorphism mapping words to triples. This map is completely defined by setting $\natural(x) = (0, 1, 1)$ and $\natural(x^{-1}) = (-1, 0, -1)$.

It is a useful intuitive device to regard a triple as described above as a segment $[i, j]$ of $\mathbb{Z}$ with a distinguished element k. Then reading any word from left to right defines a path, starting at 0 and moving a step to the left every time x^{-1} is read, and a step to the right every time x is read. Then a word w such that $\natural(w) = (i, j, k)$ defines a path starting at 0, whose meanderings in the number line take it at most $\text{abs}(i)$ places left of zero and at most j places right of zero, finally ending at position k. Composing with another word v with $\natural(v) = (i', j', k')$ we start at k and meander at most $\text{abs}(i')$ places to the left of k, j' places to the right of k and end up k' places to the right of k.

More formally, set $\text{lex}(w) = \min\{i \mid \overline{u} = x^i,\ u \text{ a prefix of } w\}$ and refer to it as the *left extremum* of w's path through $\mathbb{Z}$. Similarly define $\text{rex}(w) = \max\{i \mid \overline{u} = x^i,\ u \text{ a prefix of } w\}$ (the *right extremum*) and the *endpoint* given by $\overline{w} = x^{\text{end}(w)}$. With this notation we now have $\natural(w) = (\text{lex}(w), \text{rex}(w), \text{end}(w))$.

An immediate consequence of the discussion above is that

PROPOSITION 2.3. *Let w be a word in $\{x, x^{-1}\}^+$. The following conditions are equivalent*:

- $\natural(w)$ *is idempotent*;
- $\overline{w} = 1$;
- $\natural(w) = (i, j, 0)$ *for some* $i, j \in Z$.

Finally we quote a well known result mentioned in [12] which is at the core of the proof of Theorem 2.7.

THEOREM 2.4. *The free monogenic inverse semigroup has cubic growth.*

2.3. Proof of Theorem 2.7 For the remainder of this section we derive some lemmas under the assumption that FI_x is rational so that the proof proper is a proof by contradiction.

Suppose that L is a regular language of unique normal forms for FI_x over the alphabet $\{x, x^{-1}\}$, and let Γ be a finite state machine with n states accepting precisely

https://doi.org/10.1017/S1446788700002354 Published online by Cambridge University Press

the words of L.

Since FI_x has polynomial growth (by Theorem 2.4), L also has polynomial growth, so that each word of L may be written in the form described in Lemma 2.2. In particular, any word in L is of the form

$$u_1 v_1^{h_1} u_2 v_2^{h_2} \cdots u_m v_m^{h_m} u_{m+1} \tag{1}$$

where,

- $u_1 \cdots u_{m+1}$ describes a cycle free path in the state graph of Γ from the initial state to a terminal state;
- $u_2, \ldots, u_m$ are nonempty;
- $m \leq n$;
- $\natural(v_i)$ is not idempotent, for otherwise the word obtained by increasing h_i by one, which is also accepted by Γ would represent the same element of FI_x contradicting uniqueness.

Let w be any word in L. Then w may be factored not only as in (1) but also as abc where $\mathrm{end}(a)$ and $\mathrm{end}(ab)$ are the opposite extrema of w's path. That is, either $\overline{a} = x^{\mathrm{lex}(w)}$ and $\overline{ab} = x^{\mathrm{rex}(w)}$, or $\overline{a} = x^{\mathrm{rex}(w)}$ and $\overline{ab} = x^{\mathrm{lex}(w)}$.

However it may happen (inconveniently for our purposes) that a or b ends within one of the v_i. The next lemma shows that we may choose a, b and c so that their boundaries are out of the v_i but where $\mathrm{end}(a)$ and $\mathrm{end}(ab)$ are still 'not too far' from the extrema of w's path.

LEMMA 2.5. *Let $w \in L$. Then w may be factored as abc and also as in* (1) *so that*

- $a = u_1 {v_1}^{h_1} \cdots u_{j-1} {v_{j-1}}^{h_{j-1}} u_j'$;
- $b = u_j'' {v_{j+1}}^{h_{j+1}} \cdots u_{k-1} {v_{k-1}}^{h_{k-1}} u_k'$;
- $c = u_k'' {v_{k+1}}^{h_{k+1}} \cdots u_m {v_m}^{h_m} u_{m+1}$;

and so that $\mathrm{end}(a)$ *is within n of the lower extremum of w's path in $\mathbb{Z}$ and* $\mathrm{end}(ab)$ *is within n of the upper extremum, or vice versa.*

PROOF. We prove the lemma for the case that w may be factored as $a'b'c'$ with $\mathrm{end}(a')$ the lower extremum and $\mathrm{end}(a'b')$ the upper extremum. The other case is similar.

If a' ends within u_j for some j then put $a = a'$. Otherwise, $a' = u_1 {v_1}^{h_1} \cdots u_j {v_j}^{h} v_j'$ for some prefix v_j' of v_j.

Now if $\overline{v_j}$ is a negative power of x, then h must be $h_j - 1$, in which case put $a = u_1 {v_1}^{h_1} \cdots u_j {v_j}^{h_j}$. Then $\overline{a}$ cannot be more than an $(n-1)$th power of x greater than $\overline{a'}$ since no state appears more than once going from $\Gamma(i, a')$ to $\Gamma(i, a)$ since it traces the last part of a cycle in the state graph of Γ.

If, on the other hand, $\overline{v_j}$ is a positive power of x, then $h = 0$ so we can let $a = u_1 {v_1}^{h_1} \cdots u_{j-1}$. Again $\overline{a}$ can differ from $\overline{a'}$ by no more than an $(n-1)$th power of x.

Now we have $w = ab''c'$ where $ab'' = a'b'$, defines a path in $\mathbb{Z}$ with endpoint the right extremum of w's path. We now have $\mathrm{lex}(w) \leq \mathrm{end}(a) < \mathrm{lex}(w) + n$, as required. Of course, we still have $\mathrm{end}(ab'') = \mathrm{rex}(w)$.

If ab'' ends within u_k, put $b = b''$ and $c = c'$ and we are done. Otherwise, b'' is the word starting at the end of a and ending with $u_k'' v_k^h v_k'$ for some prefix v_k' of v_k and u_k'' is some (possibly empty) suffix of u_k.

If $\overline{v_k}$ is a negative power of x then, $h = 0$. Truncate b'' at the end of u_k'' to produce b. If $\overline{v_k}$ is a positive power of x then h is $h_k - 1$. Append the rest of v_k to form b

In either case, noting that $\mathrm{end}(b'') - n < \mathrm{end}(b)$, we still have $\mathrm{rex}(w) - n < \mathrm{end}(ab) \leq \mathrm{rex}(w)$. □

It is now shown that if $w \in L$ represents a 'large enough' element of FI_x, then as Γ accepts w, each of the factors a, b and c determined by Lemma 2.5 traverses a cycle in the state graph of Γ. The astute reader will recognize this as a thinly disguised Pumping Lemma [6].

LEMMA 2.6 (Pumping Lemma). *Let w be an element of L with $\natural(w) = (p, q, 0)$. If $p < -2n$ and $q > 2n$ then w factors as in* (1), *and for some $i_1 < i_2 < i_3$, the factors $\overline{v_{i_1}}$, $\overline{v_{i_2}}$ and $\overline{v_{i_3}}$, are nonzero powers of x which alternate in sign.*

PROOF. We can write $w = abc$ as in the statement of Lemma 2.5 with $\mathrm{end}(a)$ within n of the lower extremum of w's path and $\mathrm{end}(ab)$ within n of the upper extremum, or vice versa. Without loss of generality we assume the former.

To begin with, consider $a = u_1 {v_1}^{h_1} \cdots u_{j-1} {v_{j-1}}^{h_{j-1}} u_j'$. Now $u_1 u_2 \cdots u_{j-1} u_j'$ traces out a path in the state graph of Γ which does not visit the same state twice hence $\overline{u_1 \cdots u_j'}$ is a power of x which is between $-n$ and n. But $\overline{a}$ is a power of x^{-1} which is greater than n. Thus there is some $1 \leq i_1 < j$ with $\overline{v_{i_1}}$ a negative power of x and $h_{i_1} > 0$.

Similarly, $\overline{b}$ is a power of x which is greater than $2n$, which implies that there is some $j \leq i_2 < k$ with $\overline{v_{i_2}}$ a positive power of x and $h_{i_2} > 0$.

An identical argument assures us that there is some $k \leq i_3 \leq m$ with $\overline{v_{i_3}}$ a negative power of x and $h_{i_3} > 0$. □

Finally we are in a position to prove main theorem of this section.

THEOREM 2.7. *The monogenic free inverse semigroup is not rational.*

PROOF. Suppose by way of contradiction that FI_x is rational. Then by Lemma 1.3 it must have a regular language of unique normal forms over the generating set $\{x, x^{-1}\}$.

https://doi.org/10.1017/S1446788700002354 Published online by Cambridge University Press

Let L be such a supposed language and Γ a finite state machine which accepts precisely the words of L. Let n be the number of states of Γ. Since L is neither $\{x, x^{-1}\}^*$ nor $\emptyset$, n must be at least 2.

Under these assumptions we proceed to exhibit two words in L with the same image under $\natural$ contradicting uniqueness.

Let w be the unique element of L with $\natural(w) = (-2n - 1, 2n + 1, 0)$. Then w satisfies the conditions of Lemma 2.6. So without loss of generality we may write $w = u_1 v_1^{h_1} u_2 v_2^{h_2} \cdots u_m v_m^{h_m} u_{m+1}$ as in (1) and assume that there are $i_1 < i_2 < i_3$ with:

- $\overline{v_{i_1}} = x^{f_1}$ and $f_1 < 0$;
- $\overline{v_{i_2}} = x^{f_2}$ and $f_2 > 0$;
- $\overline{v_{i_3}} = x^{f_3}$ and $f_3 < 0$; and

h_{i_1}, h_{i_2} and h_{i_3} nonzero.

Let $\delta_2, \delta_3 > 0$ be the unique integers such that

$$f_2\delta_2 = -f_3\delta_3 = \operatorname{lcm}(f_2, -f_3). \tag{2}$$

Observe that $0 < \delta_2 \leq -f_3 \leq |v_{i_3}| \leq n$ and that similarly $0 < \delta_3 \leq n$.

Let $\lambda = \operatorname{lcm}(-f_1, f_2, -f_3)$ (a positive integer). Then set

$$\alpha = \frac{8n^2\lambda}{-f_1}, \quad \beta = \frac{4n^2\lambda}{f_2}, \quad \gamma = \frac{2n^2\lambda}{-f_3}.$$

By the fact that $n \geq 2$, $\beta > n \geq \delta_2$ and $\gamma > b \geq \delta_3$.

Define

$$w_1 = u_1 u_2 \cdots u_{i_1} v_{i_1}^{\alpha} u_{i_1+1} \cdots u_{i_2} v_{i_2}^{\beta} u_{i_2+1} \cdots u_{i_3} v_{i_3}^{\gamma} u_{i_3+1} \cdots u_{m+1}$$
$$w_2 = u_1 u_2 \cdots u_{i_1} v_{i_1}^{\alpha} u_{i_1+1} \cdots u_{i_2} v_{i_2}^{\beta-\delta_2} u_{i_2+1} \cdots u_{i_3} v_{i_3}^{\gamma-\delta_3} u_{i_3+1} \cdots u_{m+1}.$$

The construction by which we arrive at the factorization (1) ensures that w_1 and w_2 are both accepted by Γ and are therefore in L. It only remains to show that $\natural(w_1) = \natural(w_2)$. The equality holds if the endpoints are equal (which is equivalent to showing that $\overline{w_1} = \overline{w_2}$) and that the left and right extrema are equal.

Now by commutativity of F_x,

$$\begin{aligned}
\overline{w_1} &= \overline{w_2 v_{i_2}^{\delta_2} v_{i_3}^{\delta_3}} \\
&= \overline{w_2} x^{f_2\delta_2} x^{f_3\delta_3} \quad \text{but by (2)} \\
&= \overline{w_2} x^{-f_3\delta_3} x^{f_3\delta_3} \\
&= \overline{w_2}
\end{aligned}$$

as required.

https://doi.org/10.1017/S1446788700002354 Published online by Cambridge University Press

Now we calculate the left and right extrema of the paths of w_1 and w_2 in $\mathbb{Z}$. A helpful observation for the following calculations is that if $\overline{v}$ is a positive power of x, then for all $k > 0$, $\mathrm{lex}(v^k) = \mathrm{lex}(v)$ and similarly, if $\overline{v}$ is a negative power of x, then for all $k > 0$, $\mathrm{rex}(v^k) = \mathrm{rex}(v)$. Note also that

$$\mathrm{lex}(uv) = \min(\mathrm{lex}(u), \mathrm{end}(u) + \mathrm{lex}(v)) \tag{3}$$

and

$$\mathrm{rex}(uv) = \max(\mathrm{rex}(u), \mathrm{end}(u) + \mathrm{rex}(v)). \tag{4}$$

Let a_1 be the prefix of w_1 given by $u_1u_2\cdots u_{i_1}v_{i_1}^{\alpha}u_{i_1+1}\cdots u_{i_2}v_{i_2}^{\beta}$ and let a_2 be the prefix of w_2 given by $u_1u_2\cdots u_{i_1}v_{i_1}^{\alpha}u_{i_1+1}\cdots u_{i_2}v_{i_2}^{\beta-\delta_2}$. Choose b_1 and b_2 so that $w_1 = a_1b_1$ and $w_2 = a_2b_2$. Since $\overline{v_{i_2}}$ is a positive power of x, we can easily deduce that

$$\begin{aligned}\mathrm{lex}(a_1) &= \mathrm{lex}(a_2)\\ &= \mathrm{lex}(u_1u_2\cdots u_{i_1}v_{i_1}^{\alpha}u_{i_1+1}\cdots u_{i_2}v_{i_2})\\ &< n - 8n^2\lambda.\end{aligned}$$

To determine lower bounds on $\mathrm{end}(a_1)$, $\mathrm{end}(a_2)$, $\mathrm{lex}(b_1)$ and $\mathrm{lex}(b_2)$, we assert only that $\mathrm{end}(u_1\cdots u_{i_2}) > -n$ and $\mathrm{end}(u_{i_2+1}\cdots u_{m+1}) > -n$. Thus,

$$\begin{aligned}\mathrm{end}(a_1) &> -n + \alpha f_1 + \beta f_2\\ &= -n - 8n^2\lambda + 4n^2\lambda\\ &= -4n^2\lambda - n,\end{aligned}$$

and similarly,

$$\begin{aligned}\mathrm{end}(a_2) &> -4n^2\lambda - n - \delta_2 f_2;\\ \mathrm{lex}(b_1) &> -2n^2\lambda - n; \quad \text{and}\\ \mathrm{lex}(b_2) &> -2n^2\lambda - n - \delta_3 f_3;\\ &= -2n^2\lambda - n + \delta_2 f_2.\end{aligned}$$

We show that $\mathrm{lex}(a_1) < \mathrm{end}(a_1) + \mathrm{lex}(b_1)$ and $\mathrm{lex}(a_2) < \mathrm{end}(a_2) + \mathrm{lex}(b_2)$ which proves (by (3)) that $\mathrm{lex}(w_1) = \mathrm{lex}(a_1b_1) = \mathrm{lex}(a_1) = \mathrm{lex}(a_2) = \mathrm{lex}(a_2b_2) = \mathrm{lex}(w_2)$ as required. Now it a simple matter of arithmetic to show that if either of these two inequalities didn't hold, then we would have $2n^2\lambda - 3n \leq 0$. But this is only true for values of n between 0 and $3/(2\lambda)$. Since $\lambda \geq 1$ we have shown a contradiction since our automaton must have at least 2 states. From this we conclude that the left extrema of w_1 and w_2 are the same.

To complete the proof of the theorem, it is now shown in a similar way that the right extrema of w_1 and w_2 are the same. Let $a = u_1u_2\cdots u_{i_1}v_{i_1}^{\alpha}$ and once again choose b_1 and b_2 so that $w_1 = ab_1$ and $w_2 = ab_2$. We claim that $\mathrm{rex}(w_1) = \mathrm{rex}(w_2) = \mathrm{rex}(a)$.

https://doi.org/10.1017/S1446788700002354 Published online by Cambridge University Press

A priori, $\text{rex}(a) \geq 0$. In the same manner as the previous part of the proof, we calculate:

$$\text{end}(a) < -8n^2\lambda + n, \quad \text{and} \quad \text{rex}(b_1), \text{rex}(b_2) < 4n^2\lambda + n.$$

If $\text{rex}(w_1)$ or $\text{rex}(w_2)$ are not equal to $\text{rex}(a)$ then (4) implies that $\text{rex}(a) < \text{end}(a) + \text{rex}(b_1)$ or $\text{rex}(a) < \text{end}(a) + \text{rex}(b_2)$. In either case we would have $-4n^2\lambda + 2n \geq 0$, which only occurs for values of n between 0 and $1/(2\lambda)$, once again contradicting the fact that the automaton has at least 2 states. Thus the right extrema of w_1 and w_2 are the same.

This completes the proof that no regular language of normal forms for FI_x can have uniqueness. □

3. Application and discussion

The remarks in Section 1 together with the theorem of Section 2 allow us to draw some useful conclusions and conjecture further results.

In contrast with finitely generated free groups and free semigroups which are both easily seen to be automatic and therefore rational

THEOREM 3.1. *No free inverse semigroup is rational. Therefore no free inverse semigroup is automatic.*

PROOF. Let FI_X denote the free inverse semigroup on a finite set X and let $x \in X$. Then define a map $\phi : X \to \{x, 0\}$ by

$$\phi(y) = \begin{cases} x & \text{if } y = x \\ 0 & \text{otherwise} \end{cases}$$

and extend it to a Rees quotient map $\phi : FI_X \to FI_x^0$. If FI_X were rational then Theorem 1.10 would imply that FI_x^0, and by Proposition 1.9, that FI_x was rational – a contradiction. □

Together with Theorem 1.11 this shows that

COROLLARY 3.2. *No semigroup can be rational (nor, therefore, automatic) if it is a free product of a free inverse semigroup with another semigroup.*

The class of semigroups which we now know not to be rational is not contained within the class of semigroups with polynomial growth, since the free inverse semigroup on more than one generator has exponential growth. This fact is somewhat intriguing since the proof of Theorem 2.7 is so dependent on the growth of FI_x.

An obvious question which arises is whether a free inverse semigroup may embed in any rational semigroup, for if not, FI_X would be an interesting semigroup satisfying the third condition in the definition of a Markov property, while still having solvable word problem.

Another class of inverse semigroups closely entwined with the present thread of discourse are defined in [7].

PROPOSITION 3.3. *Suppose S is a finitely presented Rees quotient of a free inverse semigroup with polynomial growth. Then the following conditions are equivalent*:

- *S is infinite*;
- *S contains a free monogenic inverse subsemigroup*;
- *S has growth of degree at least* 3.

We conjecture that the semigroups defined by Proposition 3.3 are not rational.

As a final remark, the observations of Section 1.2 recall a lecture given by Professor Rick Thomas at the conference CGAMA at Heriot-Watt University, Edinburgh in July 1998 [14]. For a finitely presented group G the set $W(G)$ of words representing the identity of G was considered. A number of theorems relating the position of $W(G)$ in the formal language hierarchy with the algebraic structure of G were cited. We consider it a promising line of inquiry to investigate the algebraic properties of groups and semigroups which are known to have a language of unique normal forms in the various strata of the language hierarchy.

Acknowledgements

For several stimulating discussions the authors thank Mike Atkinson, and also Nik Ruškuc who posed the motivating question of whether free inverse semigroups are automatic.

References

[1] S. I. Adjan, 'On algorithmic problems in effectively complete classes of groups', *Dokl. Akad. Nauk SSSR* **123** (1958), 13–16 (in Russian).

[2] C. M. Campbell, E. F. Robertson, N. Ruškuc and R. M. Thomas, 'Automatic semigroups', *Theoret. Comput. Sci.* (to appear).

[3] J. W. Cannon, D. B. A. Epstein, D. F. Holt, S. V. F. Levy, M. S. Paterson and W. P. Thurston, *Word processing in groups* (Jones and Bartlett Publishers, Boston, Massachusetts, 1992).

[4] A. J. Duncan, E. F. Robertson and N. Ruškuc, 'Automatic monoids and change of generators', *Math. Proc. Cambridge Philos. Soc.* **127** (1999), 403–409.

[5] R. Gilman, 'Groups with a rational cross-section', in: *Combinatorial group theory and topology* (eds. S. M. Gersten and J. R. Stallings) (Princeton University Press, Princeton, New Jersey, 1987) pp. 175–183.
[6] J. E. Hopcroft and J. D. Ullman, *Introduction to automata theory, languages and computation* (Addison-Wesley, Reading, 1979).
[7] J. Lau, 'Degree of growth of some inverse semigroups', *J. Algebra* **204** (1998), 426–439.
[8] A. Markov, 'On the impossibility of certain algorithms in the theory of associative systems', *Dokl. Akad. Nauk SSSR* **55** (1947), 583–586.
[9] ———, 'Impossibility of algorithms for recognizing some properties of associative systems', *Dokl. Akad. Nauk SSSR* **77** (1951), 953–956.
[10] M. Petrich, *Inverse semigroups*, Pure and Applied Mathematics (John Wiley and Sons, New York, 1984).
[11] M. O. Rabin, 'Recursive unsolvability of group theoretic problems', *Ann. of Math.* **67** (1958), 172–194.
[12] L. M. Schneerson and D. Easdown, 'Growth and existence of identities in a class of finitely presented inverse semigroups with zero', *Internat. J. Algebra Comput.* **6** (1996), 105–121.
[13] C. C. Sims, *Computation with finitely presented groups*, Encyclopedia Math. Appl. 48 (Cambridge University Press, Cambridge, 1994).
[14] R. Thomas, 'Groups and formal languages', Lecture at CGAMA, Heriot-Watt, July 1998.
[15] V. A. Ufnarovskij, *Combinatorial and asymptotic methods in algebra*, Encyclopedia Math. Sci. 57 (Springer, Berlin, 1995).
[16] A. Yamamura, 'HNN extensions of inverse semigroups and applications', *Internat. J. Algebra Comput.* **7** (1997), 605–624.

Mathematical Institute
University of St Andrews
Fife, KY16 9SS
Scotland
e-mail: andrewc@dcs.st-and.ac.uk

Department of Mathematics and Statistics
Simon Fraser University
Burnaby, British Columbia
VA5 1S6 Canada
e-mail: andrew@illywhacker.net