

Syntactic semigroups and the finite basis problem

Marcel Jackson

*Department of Mathematics
La Trobe University
Australia*

Abstract

The finite basis problem for semigroups asks when a given finite algebra has a finite basis for its identities. This problem is one of the most investigated in variety theory. In this note we look at some easily established equivalent decision problems.

1 Introduction

We show how one may efficiently associate with each semigroup (monoid) \mathbf{S} a syntactic semigroup (monoid) $\bar{\mathbf{S}}$ such that \mathbf{S} has a finite basis of identities if and only if $\bar{\mathbf{S}}$ has a finite basis of identities. Using this and a result of Sapir [14] we obtain a language theoretic equivalent to the finite basis problem for semigroups and monoids. While our techniques are completely elementary, the results may provide a useful alternative approach to the finite basis problem for finite semigroups.

1.1 Syntactic semigroups and monoids

In this section we gather together some basic facts concerning syntactic semigroups and monoids. For a more complete treatment, the reader should consult a book such as [6]. Recall that if \mathbf{S} is a monoid, and W is a subset of S , then the *syntactic congruence* \sim_W of W in \mathbf{S} is given by $(a, b) \in \sim_W$ if for every $c, d \in S \cup \{1\}$, $cad \in W \Leftrightarrow cbd \in W$. (This congruence is the largest congruence for which W is a union of congruence classes.) In the case where \mathbf{S} is a free semigroup (monoid), the quotient by the syntactic congruence of a subset L is called the *syntactic semigroup* (*syntactic monoid*) of L , and we denote this by $\text{Syn}(L)$ (or $\text{Syn}_M(L)$, respectively). A language is *regular* (accepted by a finite state automaton) if and only if its syntactic semigroup (or monoid) is finite.

We will say that a subset $W \subseteq S$ of a semigroup \mathbf{S} is a *syntactic subset* if the syntactic congruence of W in \mathbf{S} is the diagonal relation. In this case, if $\nu : A^+ \rightarrow \mathbf{S}$ is a surjective homomorphism onto \mathbf{S} , then \mathbf{S} is isomorphic to the syntactic semigroup of the language $\nu^{-1}(W)$.

If \mathbf{S} is a semigroup, then for every $s \in S$, we may take the syntactic congruence of the singleton $\{s\}$; the semigroup $\mathbf{S}/\sim_{\{s\}}$ is syntactic, and for distinct elements $s, t \in S$ there is an $r \in S$ for which $s/\sim_{\{r\}} \neq t/\sim_{\{r\}}$ (choosing r to be either s or t suffices). Hence there is a subdirect embedding ν of \mathbf{S} into the direct product $\prod_{s \in S} \mathbf{S}/\sim_{\{s\}}$ defined by $\nu(s) : x \mapsto$

$x/\sim_{\{s\}}$. We note that one can construct $\mathbf{S}/\sim_{\{s\}}$ from \mathbf{S} in polynomial time: to decide $x \sim_{\{s\}} y$ one must calculate uxv and uyv for each $u, v \in S^1$. Using a multi-tape Turing machine, we may encode \mathbf{S} by listing the rows of its Cayley table; let n denote the number of squares this occupies (clearly $n \geq |S|^2$ and also $n \in O(|S|^2 \log_2(|S|))$ since each element can be encoded as a binary string of length at most $\log_2(|S|)$). Calculating uxv and uyv takes $O(n)$ steps, while there are $O(|S|^2)$ pairs u, v to consider. We direct the reader to [7] for details on these notions and more information on problems of computational complexity.

For a language W and a word w we define $w^{-1}W := \{u \in W : wu \in W\}$ and $Ww^{-1} := \{u \in W : uw \in W\}$. Now let \mathcal{L} be a class of regular languages. For a finite alphabet A we denote by $\mathcal{L}(A)$ the set of all members of \mathcal{L} whose alphabet is A . We say that \mathcal{L} is a *+variety* of languages if for every finite alphabet A the following properties hold: $\mathcal{L}(A)$ is closed under taking finite unions, intersections and complementation; for every letter $a \in A$ and every $W \in \mathcal{L}(A)$ we have $a^{-1}W \in \mathcal{L}$ and $Wa^{-1} \in \mathcal{L}$; and for every pair of finite alphabets A, B and every homomorphism $\nu : A^+ \rightarrow B^+$ we have $L \in \mathcal{L}(B)$ implies $\nu^{-1}(L) \in \mathcal{L}(A)$. If we replace free semigroups in this definition by free monoids, the corresponding notion is that of a **-variety*.

There is a natural correspondence between +-varieties of regular languages and pseudovarieties (classes closed under finite direct products, subalgebras and homomorphic images) of finite semigroups. With each +-variety of regular languages \mathcal{L} , we may associate the semigroup pseudovariety generated by the syntactic semigroups of the languages in \mathcal{L} . Conversely with each pseudovariety of finite semigroups \mathcal{V} we may associate the class of regular languages whose syntactic semigroups are in \mathcal{V} . This class of languages turns out to be a +-variety of languages and the two correspondences we have described are mutually inverse bijections between the lattice of semigroup pseudovarieties and the lattice of +-varieties of regular languages (this is the so-called *Eilenberg correspondence* [6]). Monoid and *-variety versions of this correspondence are given in the obvious way.

1.2 The finite basis problem

An *identity* of a semigroup is an expression $u \approx v$ where u and v are semigroup words. A semigroup satisfies the identity $u \approx v$ (in variables A , say) if for every homomorphism $\theta : A^+ \rightarrow \mathbf{S}$, the equality $\theta(u) = \theta(v)$ holds (written $\mathbf{S} \models u \approx v$). The set of identities of \mathbf{S} over some fixed countably infinite alphabet is denoted $\text{Id}(\mathbf{S})$. The class of all semigroups satisfying the identities of \mathbf{S} is called the *variety* generated by \mathbf{S} . Equivalently, the variety of \mathbf{S} is the class of all homomorphic images of subalgebras of direct powers of \mathbf{S} . (Similar notions hold for general algebras.) We will denote the variety of an algebra \mathbf{S} by $\mathbb{V}(\mathbf{S})$, and the finite members of $\mathbb{V}(\mathbf{S})$ by $\mathbb{V}_{\text{fin}}(\mathbf{S})$. When \mathbf{S} is finite, $\mathbb{V}_{\text{fin}}(\mathbf{S})$ coincides with the pseudovariety generated by \mathbf{S} . We will also write $\mathbf{S} \cong \mathbf{T}$ when $\text{Id}(\mathbf{S}) = \text{Id}(\mathbf{T})$.

If \mathbf{S} is a semigroup without an identity element, then we let \mathbf{S}^1 denote the monoid obtained by adjoining an identity element. Otherwise we let \mathbf{S}^1 simply denote \mathbf{S} . A dual definition for zero elements 0 gives \mathbf{S}^0 . The following elementary lemma is useful because we will frequently be moving between monoids and of semigroups.

1.1 Lemma *Let \mathbf{S} be a monoid and \mathbf{T} a semigroup such that \mathbf{T} is contained in the semigroup variety generated by \mathbf{S} . Then \mathbf{T}^1 is contained in the monoid variety of \mathbf{S} .*

Proof Let \mathbf{S} and \mathbf{T} be as in the statement of the lemma. Then, working within the type

(2), we have $\mathbf{T} \in \mathbb{HSP}(\mathbf{S})$. Therefore there are semigroups $\mathbf{T}_1, \mathbf{T}_2$ such that $\mathbf{T}_1 \in \mathbb{P}(\mathbf{S})$, $\mathbf{T}_2 \in \mathbb{S}(\mathbf{T}_1)$ and $\mathbf{T} \in \mathbb{H}(\mathbf{T}_2)$. Clearly, \mathbf{T}_1 is a monoid that is also contained in the monoid variety of \mathbf{S} . If \mathbf{T}_2 contains the identity element, e say, of \mathbf{T}_1 then \mathbf{T} (a quotient of \mathbf{T}_2) is a monoid that is contained in the monoid variety of \mathbf{S} and we are done.

Now assume that $e \notin T_2$ and let \mathbf{T}'_2 denote the submonoid of \mathbf{T}_1 obtained by adjoining the element e to T_2 . Note that \mathbf{T}_2 may already be a monoid, but with an element other than e acting as the identity, whence \mathbf{T}'_2 need not be isomorphic to \mathbf{T}_2^1 . Without loss of generality we may assume that there is a congruence θ such that $\mathbf{T}_2/\theta = \mathbf{T}$.

If \mathbf{T} has an identity element 1, then choose $f \in T_2$ such that $f/\theta = 1$, and extend θ to a congruence θ' on \mathbf{T}'_2 by adjoining to θ the pairs (e, e) and $(e, x), (x, e)$ whenever (f, x) and (x, f) are in θ_1 . This gives $\mathbf{T}'_2/\theta' \cong \mathbf{T}_2/\theta = \mathbf{T}$, showing $\mathbf{T} \in \mathbb{V}(\mathbf{S})$ as a monoid.

Otherwise, if \mathbf{T} has no identity element, then we may extend θ to a congruence on \mathbf{T}'_2 by adjoining the pair (e, e) . The resulting quotient is isomorphic to \mathbf{T}^1 and again lies in the monoid variety of \mathbf{S} . \square

An equational deduction of an identity $p \approx q$ from a set of identities Σ , is a sequence of identities $p \equiv p_1 \approx p_2 \approx \cdots \approx p_n \equiv q$ such that for each $i < n$ there is an identity $u_i \approx v_i \in \Sigma$ or $v_i \approx u_i \in \Sigma$ and a semigroup substitution θ_i such that p_{i+1} is obtained from p_i by replacing a subword $\theta_i(u_i)$ with $\theta_i(v_i)$. In this case we write $\Sigma \vdash p \approx q$. If $n = 1$ we will interpret the definition of an equational deduction as saying that $\Sigma \vdash p \approx p$.

A basis for the identities of a semigroup \mathbf{S} is a subset Σ of $\text{Id}(\mathbf{S})$ such that $\Sigma \vdash \text{Id}(\mathbf{S})$. In 1964, Oates and Powell [10] showed that if \mathbf{G} is a finite group, then \mathbf{G} has a finite basis of identities. However in 1966 Perkins (see [11]) showed that the semigroup \mathbf{B}_2^1 given by the following matrices under matrix multiplication has no finite identity basis:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

In the subsequent years a great many other examples have shown that the *finite basis problem*—determining which finite semigroups admit a finite basis of identities—is very complicated. For general algebras this problem has been shown to be undecidable [8], but for semigroups the complexity of the problem remains open. For further details we direct the reader to the most recent survey of this area by Volkov [15].

The following lemma gives some well known equivalents of the finite basis property. We omit the proof, but note that the equivalence of (ii) and (iii) follows from Birkhoff's completeness theorem for equational logic (which says that $\Sigma \vdash p \approx q$ if and only if whenever some algebra \mathbf{A} satisfies all of Σ , then also $\mathbf{A} \models p \approx q$), while the equivalence of (i) and (ii) is another theorem of Birkhoff.

1.2 Lemma (Birkhoff [2]; see also [3].) *Let \mathbf{S} be a finite algebra of finite signature. The following are equivalent:*

- (i) $\text{Id}(\mathbf{S})$ is finitely based;
- (ii) there is an positive integer n such that the n -variable identities in $\text{Id}(\mathbf{S})$ are a basis for $\text{Id}(\mathbf{S})$;
- (iii) there is an positive integer n such that for all algebras \mathbf{A} , we have $\mathbf{A} \in \mathbb{V}(\mathbf{S})$ if and only if all n -generated subalgebras of \mathbf{A} are in $\mathbb{V}(\mathbf{S})$.

2 Syntactic equivalants

We are going to show that the finite basis problem for finite semigroups is equivalent to its restriction to finite syntactic semigroups. The idea is easy, so we prove it in an even more general setting.

The notion of a syntactic congruence can be extended to general algebras by defining the syntactic congruence \sim_W of a subset W of an algebra \mathbf{S} is the largest congruence θ for which W is a union of θ -classes (for further details see [1] for example). A *syntactic algebra* is an algebra with a *syntactic subset*—a subset whose syntactic congruence is the diagonal relation.

2.1 Proposition *If \mathbf{S} is an algebra with a one element subalgebra then there is a syntactic algebra $\bar{\mathbf{S}}$ such that $\mathbf{S} \cong \bar{\mathbf{S}}$. If \mathbf{S} is finite, then $\bar{\mathbf{S}}$ is finite.*

Proof Let $\{e\}$ be a one element subuniverse of \mathbf{S} . For each $t \in S \setminus \{e\}$, let \mathbf{S}_t denote $\mathbf{S}/\sim_{\{t\}}$. As in Subsection 1.1, \mathbf{S} subdirectly embeds into $\prod_{t \in S \setminus \{e\}} \mathbf{S}_t$, and so we have $\mathbf{S} \cong \prod_{t \in S \setminus \{e\}} \mathbf{S}_t$. For $s, t \in S \setminus \{e\}$, let $s_t \in \prod_{t \in S \setminus \{e\}} \mathbf{S}_t$ be defined by $s_t(r) = e/\sim_{\{r\}}$ if $r \neq t$ and $s/\sim_{\{r\}}$ otherwise. Let W be $\{s_s : s \in S\}$, let \mathbf{T} be any subalgebra of $\prod_{t \in S \setminus \{e\}} \mathbf{S}_t$ containing $\{s_t : s, t \in S\}$, and let $\bar{\mathbf{S}}$ denote \mathbf{T}/\sim_W . Now $\bar{\mathbf{S}} \in \mathbb{V}(\mathbf{S})$ so to complete the proof it will suffice to show that each \mathbf{S}_t embeds into $\bar{\mathbf{S}}$. Now for each $t \in S \setminus \{e\}$, the subalgebra of \mathbf{T} on $\{s_t : s \in S\}$ is isomorphic to \mathbf{S}_t and $\{s_t : s \in S\} \cap W = \{s_s\}$, a syntactic subset of $\{s_t : s \in S\}$. Hence the restriction of \sim_W on \mathbf{T} to $\{s_t : s \in S\}$ is trivial. Therefore \mathbf{S}_t embeds into $\bar{\mathbf{S}}$, as required. \square

Algebras satisfying the conditions of this proposition are reasonably common—every monoid, ring, lattice and finite semigroup has a one-element subalgebra. We note that Proposition 2.1 would follow trivially if the class of syntactic algebras was closed under the taking of direct products (as is suggested by Proposition VII.1.5 of [6]), however a 2-element left zero semigroup is syntactic, while its square is not.

Unfortunately, the construction in Proposition 2.1 is not very efficient—it seems possible that $\bar{\mathbf{S}}$ could have size close to $|S|^{|S|}$. To gain greater efficiency, we now restrict our attention to semigroups.

2.2 Lemma *If \mathbf{S} is a semigroup with zero element then one can construct a syntactic semigroup $\bar{\mathbf{S}}$ equationally equivalent to \mathbf{S} in polynomial time.*

Proof We are going to follow the proof of Proposition 2.1. We can fix the zero element 0 of \mathbf{S} as the one element subalgebra and then the elements $\{s_t : s, t \in S\}$ in $\prod_{t \in S \setminus \{0\}} \mathbf{S}_t$ actually form a subsemigroup, which we choose as \mathbf{T} .

Now \mathbf{T} has fewer than $|S|^2$ elements and can clearly be constructed in polynomial time from the family $\{\mathbf{S}_t : t \in S \setminus \{0\}\}$; in fact \mathbf{T} is isomorphic to the so-called *0-direct join* of $\{\mathbf{S}_t : t \in S \setminus \{0\}\}$, formed by amalgamating these semigroups at 0 and then setting any undefined products to equal 0. As each of the $|S| - 1$ semigroups of the form \mathbf{S}_t can be constructed from \mathbf{S} in polynomial time (see Subsection 1.1) it follows that $\bar{\mathbf{S}}$ can be constructed in polynomial time from \mathbf{S} . \square

For each $t \in S \setminus \{0\}$, let A_t be an alphabet (with $A_t \cap A_s = \emptyset$ for $s \neq t$) and $\nu_t : A_t^+ \rightarrow \mathbf{S}_t$ be a surjective morphism so that \mathbf{S}_t is the syntactic semigroup of some (regular) subset $L_t \subseteq A_t^+$

with $\nu_t(L_t) = \{t/\sim_{\{t\}}\}$. One can see from the proof of Lemma 2.2 that $\bar{\mathbf{S}}$ is (isomorphic to) the syntactic semigroup of the *disjoint* union of the languages L_t in the free semigroup over the disjoint union of the alphabets A_t .

The proof of Lemma 2.2 does not quite hold for monoids because 0 is not a one element submonoid and because the subsemigroup on $\{s_t : s, t \in S \setminus \{0\}\}$ is not a submonoid (except when $|S| = 2$). However, the submonoid of $\prod_{t \in S \setminus \{0\}} \mathbf{S}_t$ generated by $\{s_t : s, t \in S \setminus \{0\}\}$ is simply $\{s_t : s, t \in S \setminus \{0\}\} \cup \{\underline{1}\}$ (where $\underline{1}$ is the identity element). Choosing this as \mathbf{T} and calculating $\bar{\mathbf{S}}$ as before, we find that each of the \mathbf{S}_t are monoids that embed into $\bar{\mathbf{S}}$ as semigroups and hence are in the semigroup variety of the monoid $\bar{\mathbf{S}}$. By Lemma 1.1, they are in the monoid variety of $\bar{\mathbf{S}}$ as well. This is clearly still a polynomial time construction and hence Lemma 2.2 holds for monoids as well. In fact we do not need monoids with zero to state this result. First consider the following lemma.

2.3 Lemma *If \mathbf{S} is a semigroup whose variety contains the variety of semilattices then $\mathbf{S} \cong \mathbf{S}^0$.*

Proof If $\mathbf{S} = \mathbf{S}^0$ we are done, so assume that \mathbf{S} does not contain a zero element. Certainly \mathbf{S} lies within the variety of \mathbf{S}^0 . Conversely, as the variety of \mathbf{S} contains the two element semilattice $\mathbf{2}$ (with universe $\{0, 1\}$), it also contains $\mathbf{S} \times \mathbf{2}$. The semigroup \mathbf{S}^0 is isomorphic to the Rees quotient of $\mathbf{S} \times \mathbf{2}$ by the ideal $\{(x, 0) : x \in S\}$. \square

2.4 Lemma *Every finite monoid \mathbf{S} is equationally equivalent to the syntactic monoid of some regular language that can be constructed from \mathbf{S} in polynomial time.*

Proof By considering the one-generated submonoids of \mathbf{S} it can be seen that the monoid variety of \mathbf{S} fails to contain the variety of semilattice monoids if and only if \mathbf{S} is a finite group. If \mathbf{S} is a group then the syntactic congruence of any singleton subset of S is the diagonal relation and so \mathbf{S} is the syntactic monoid of a regular language and we are done.

Now say that the monoid variety of \mathbf{S} contains the variety of semilattice monoids. Then by Lemma 2.3 it can be generated by a monoid with zero element. A syntactic monoid generating the same variety is then given by the argument following Lemma 2.2. \square

In [15], the question is asked as to whether or not the finite basis problem for syntactic semigroups is decidable (that is, algorithmically solvable). It is clear from Proposition 2.1 that this problem is equivalent to the general finite basis problem, but in fact we can use Lemma 2.2 to show that these problems are polynomially equivalent.

We first need the following result from [9].

2.5 Lemma (Mel'nik [9].) *A semigroup \mathbf{S} is finitely based if and only if \mathbf{S}^0 is finitely based.*

Proof If $\mathbb{V}(\mathbf{S})$ contains the variety of semilattices then by Lemma 2.3 we have $\mathbf{S} \cong \mathbf{S}^0$. So we may assume throughout that $\mathbb{V}(\mathbf{S})$ does not contain the variety of semilattices.

Let us say that an identity $u \approx v$ is *homotypical* if the variables in u are the same as those in v (this is also called *regular*). The identities of $\mathbf{2}$ are exactly the class of homotypical semigroup identities and so it follows that \mathbf{S} satisfies some non-homotypical identity. In this case \mathbf{S}^0 generates the smallest variety containing $\mathbb{V}(\mathbf{S})$ that is definable by homotypical identities. Following [9], it can be shown that \mathbf{S} has a basis of the form $\Sigma \cup (x^m y^m x^m)^m \approx x^m$ for some $m \in \mathbb{N}$ and where Σ is a collection of homotypical identities. It is shown in [9] that

one can find a basis for \mathbf{S}^0 by adjoining to Σ a finite set of homotypical identities. Thus if \mathbf{S} is finitely based, then Σ can be chosen to be finite, and we get a finite basis for \mathbf{S}^0 (this is also discussed in [15]). Now if \mathbf{S} is not finitely based, then Σ must be infinite and no finite subset of $\text{Id}(\mathbf{S})$ is sufficient to derive all of Σ . As Σ is also satisfied by \mathbf{S}^0 , and $\text{Id}(\mathbf{S}^0) \subseteq \text{Id}(\mathbf{S})$, it follows that \mathbf{S}^0 also has no finite basis of identities. \square

2.6 Corollary *The finite basis problem for finite semigroups (monoids) is polynomially equivalent to its restriction to the class of finite syntactic semigroups (monoids).*

Proof The monoid version of this result follows immediately from Lemma 2.4.

Now let \mathbf{S} be a finite semigroup. By Lemma 2.5, \mathbf{S} is finitely based if and only if \mathbf{S}^0 is finitely based. By Lemma 2.2, \mathbf{S}^0 generates a variety equal to one generated by a single syntactic semigroup (that can be constructed in polynomial time from \mathbf{S}^0). \square

3 A language theoretic approach

The finite basis problem for monoids has a natural analogue in terms of varieties of regular languages. Analogous statements will hold for semigroups as well.

3.1 Definition For K a class of regular languages, let $\mathcal{V}^*(K)$ denote the $*$ -variety of languages generated by K and let $\mathcal{V}_n^*(K)$ denote the subclass of $\mathcal{V}^*(K)$ consisting of those languages which are in alphabets of at most n letters. We say that a $*$ -variety of languages $\underline{\mathcal{V}}$ is *finitely $*$ -verifiable for K languages* if there exists an $n \in \mathbb{N}$ such that for all languages $W \in K$,

$$W \in \underline{\mathcal{V}} \Leftrightarrow \mathcal{V}_n^*(W) \subseteq \underline{\mathcal{V}}.$$

If K is the class of all regular languages, then we say that a $*$ -variety is finitely $*$ -verifiable instead of finitely $*$ -verifiable by K -languages.

The connection between the finite $*$ -verification property for $*$ -varieties of languages and the finite basis problem for monoids arises through the Eilenberg correspondence and the following result essentially due to M. Sapir.

3.2 Lemma (*M. Sapir [14].*) *Let \mathcal{V} be a subvariety of a finitely generated variety of semigroups (monoids). Then \mathcal{V} is non-finitely based if and only if for each $n \in \mathbb{N}$ there are finite semigroups (monoids, respectively) $\mathbf{S}_n \notin \mathcal{V}$ such that \mathbf{S}_n satisfies all n -variable identities of \mathcal{V} but not all identities of \mathcal{V} . Equivalently, $\mathbf{S}_n \notin \mathcal{V}$ but all n -generated subsemigroups (submonoids) of \mathbf{S}_n are contained in \mathcal{V} .*

Proof We first discuss the semigroup case. The statement above differs from the main result of [14] only in that it allows for the possibility that \mathcal{V} is not generated by any finite semigroup. All arguments in [14] except for Proposition 1 depend only on the local finiteness of \mathcal{V} . Proposition 1 however, is itself an extract from a more general result from [12] that concerns any locally finite variety in which all groups are finitely based. As Sapir notes in [12], this is true of any finitely generated semigroup variety (by [10]) and hence in any subvariety of such a variety. Therefore Sapir's proof in fact extends to the semigroup part of the lemma we have stated above.

Now we investigate the monoid case which again follows without significant change from Sapir's result for semigroups. As is discussed in [15], a monoid is non-finitely based (in the type $\langle 2, 0 \rangle$) if and only if it is non-finitely based as a semigroup (in the type $\langle 2 \rangle$). Let \mathcal{V}' denote the semigroup variety generated by the members of \mathcal{V} considered as semigroups, and say that \mathcal{V} (whence \mathcal{V}') is not finitely based. Using the semigroup version of the lemma, there are finite semigroups \mathbf{S}_n such that \mathbf{S}_n is not contained in \mathcal{V}' , while all n -generated subsemigroups of \mathbf{S}_n are contained in \mathcal{V}' . Now consider \mathbf{S}_n^1 , also not in \mathcal{V}' and therefore not in \mathcal{V} (as a monoid). As semigroups, the n -generated *submonoids* of \mathbf{S}_n^1 are either n -generated *subsemigroups* of \mathbf{S} (that happen to be monoids) or are of the form of an n -generated subsemigroup of \mathbf{S}_n with adjoined identity element. In either case, Lemma 1.1 shows that the n -generated submonoids lie in \mathcal{V} . Thus we have, for all $n \in \mathbb{N}$, a finite monoid not in \mathcal{V} but whose n -generated submonoids are in \mathcal{V} . \square

This result guarantees that for finite semigroups and monoids, the third condition of Lemma 1.2 can be replaced by its restriction to finite algebras. The corresponding result for general algebras appears to be an interesting open problem; see [4, 5].

3.3 Lemma *If \mathbf{S} is a finite monoid with no finite basis of identities then for each $n \in \mathbb{N}$ there is a regular language W_n such that every n -generated submonoid of $\text{Syn}_M(W_n)$ is contained in $\mathbb{V}(\mathbf{S})$ but $\text{Syn}_M(W_n) \notin \mathbb{V}(\mathbf{S})$.*

Proof By Lemma 3.2, for each $n \in \mathbb{N}$ there is a finite monoid \mathbf{S}_n such that every n -generated submonoid of \mathbf{S}_n is contained in $\mathbb{V}(\mathbf{S})$ but $\mathbf{S}_n \notin \mathbb{V}(\mathbf{S})$.

Let us fix some arbitrary $n \in \mathbb{N}$. For each element $s \in \mathbf{S}_n$, let $\mathbf{S}_{n,s}$ denote the semigroup $\mathbf{S}_n / \sim_{\{s\}}$. Now each $\mathbf{S}_{n,s}$ is a quotient of \mathbf{S}_n and therefore satisfies all identities satisfied by \mathbf{S}_n . However $\mathbb{V}(\mathbf{S})$ is generated by $\{\mathbf{S}_{n,s} : s \in S\}$ (see Subsection 1.1) and therefore there must be an identity of \mathbf{S} that fails on $\mathbf{S}_{n,s}$ for some $s \in \mathbf{S}_n$. Therefore we have a finite syntactic monoid of a regular language, W_n say, that satisfies all identities of \mathbf{S}_n (and therefore all n -variable identities of \mathbf{S}) but not all identities of \mathbf{S} . Equivalently (see Lemma 1.2), we have shown that there is a regular language W_n such that every n -generated submonoid of $\text{Syn}_M(W_n)$ lies in the monoid variety of \mathbf{S} while $\text{Syn}_M(W_n)$ does not. \square

The extension of Lemma 3.3 to semigroups is obvious and we omit the details.

3.4 Theorem *Let \mathbf{S} be a finite monoid and $\underline{\mathcal{V}}$ denote the $*$ -variety of languages whose syntactic monoids are finite and contained in $\mathbb{V}(\mathbf{S})$. Then \mathbf{S} is finitely based if and only if $\underline{\mathcal{V}}$ is finitely $*$ -verifiable.*

Proof Let \mathbf{S} be a finite monoid with a finite basis of identities Σ in n variables and let $\underline{\mathcal{V}}$ denote the $*$ -variety of regular languages whose syntactic monoids are in $\mathbb{V}_{\text{fin}}(\mathbf{S})$. Obviously if $W \in \underline{\mathcal{V}}$ then $\mathcal{V}_n^*(W) \subseteq \underline{\mathcal{V}}$, while if W is a language not in $\underline{\mathcal{V}}$ then the Eilenberg correspondence guarantees that $\text{Syn}_M(W) \not\models \Sigma$. Hence there is an n -variable identity $u \approx v$ that fails on $\text{Syn}_M(W)$. Evidently, there is an n -generated submonoid \mathbf{T} of $\text{Syn}_M(W)$ on which $u \approx v$ fails. By examining the syntactic quotients of \mathbf{T} with respect to the singleton subsets of T (as in the proof of Lemma 3.3), it follows that there is $t \in T$ such that $u \approx v$ fails on $\mathbf{T} / \sim_{\{t\}}$, also n -generated. Let $A = \{a_1, \dots, a_n\}$ be a set of free generators for a free monoid A^* and let $\phi : A^* \rightarrow \mathbf{T}$ be a surjective homomorphism. Then $\mathbf{T} / \sim_{\{t\}}$ is the syntactic monoid of the regular language $W_t := \phi^{-1}(t / \sim_{\{t\}})$ in the n -letter alphabet A , whence it follows that

$W_t \in \mathcal{V}_n^*(W) \setminus \underline{\mathcal{V}}$. This shows that there is an $n \in \mathbb{N}$ such that for regular languages W , $W \notin \underline{\mathcal{V}} \implies \mathcal{V}_n^*(W) \not\subseteq \underline{\mathcal{V}}$, that is, $\underline{\mathcal{V}}$ is finitely $*$ -verifiable.

Now assume that \mathbf{S} is non-finitely based. By Lemma 3.3, for all $n \in \mathbb{N}$ there are regular languages W_n such that $\text{Syn}_M(W_n) \notin \mathbb{V}(\mathbf{S})$ but such that every n -variable identity satisfied by \mathbf{S} is satisfied by $\text{Syn}_M(W_n)$. Now if $U \in \mathcal{V}_n^*(W_n)$ then $\text{Syn}_M(U)$ is n -generated and satisfies all identities of $\text{Syn}_M(W_n)$ and in particular, all n -letter identities of \mathbf{S} . Elementary arguments then show that $\text{Syn}_M(U) \in \mathbb{V}(\mathbf{S})$. Hence $U \in \underline{\mathcal{V}}$ so $\mathcal{V}_n^*(W_n)$ is a subclass of $\underline{\mathcal{V}}$, while W_n is not in $\underline{\mathcal{V}}$. Because $n \in \mathbb{N}$ is arbitrary, $\underline{\mathcal{V}}$ is not finitely $*$ -verifiable. \square

Again, trivial variations of this Theorem give the corresponding result for semigroup varieties and $+$ -varieties of languages.

It is interesting to note that the main proof in [14] shows that if \mathbf{S} is a finite inherently non-finitely based monoid (or semigroup), then the corresponding $*$ -variety of languages is not finitely $*$ -verifiable for singleton languages. For example, the monoid \mathbf{B}_2^1 given in the introduction is known to be (isomorphic to) the syntactic monoid of the language $\{ab\}^*$ (in the alphabet $\{a, b\}$) and is also known to be inherently non-finitely based [13]. Hence $\mathcal{V}^*(\{ab\}^*)$ is not finitely $*$ -verifiable for singleton languages. In fact from [11] and the proof of Theorem 3.4, we have $\{ba_1a_2 \dots a_nba_na_{n-1} \dots a_1\} \notin \mathcal{V}^*(\{ab\}^*)$ for any $n \in \mathbb{N}$, but $\mathcal{V}_n^*(\{ba_1a_2 \dots a_nba_na_{n-1} \dots a_1\}) \in \mathcal{V}^*(\{ab\}^*)$.

Let the *finite $*$ -verification problem for regular expressions* denote the following decision problem: given a regular expression, decide if the corresponding language generates a finitely $*$ -verifiable $*$ -variety. The finite $+$ -verification problem is defined analogously.

3.5 Corollary *The finite basis problem for finite semigroups (monoids) is decidable if and only if the finite $+$ -verification ($*$ -verification, respectively) problem for regular expressions is decidable.*

Proof We discuss the monoid case; the semigroup case is almost identical. The standard proofs of the equivalence of the class of languages recognisable by finite state automata and languages corresponding to regular expressions are constructive. That is, with each finite automata, we can effectively associate a regular expression corresponding to the language recognised by the machine and vice versa. Likewise, with a syntactic monoid $\text{Syn}_M(W)$ of a language W we may construct an automata recognising W (by representing $\text{Syn}_M(W)$ as a monoid of transformations), and conversely with each automata, we may effectively construct a minimal automata recognising the same language and then construct the syntactic monoid of this language as the transition monoid of the automata. Therefore we can effectively associate a syntactic monoid \mathbf{S} with a regular expression for a language recognised by \mathbf{S} and vice versa.

The result now follows by combining Theorem 3.4 and its semigroup variant with Corollary 2.6. \square

We note that the translation from syntactic semigroups or monoids to regular expressions is polynomial time, however the reverse may not be true. It is a well known PSPACE-complete problem to determine if a regular expression r over $\{0, 1\}$ represents the same language as $\{0, 1\}^*$; see [7]. The syntactic monoid of $\{0, 1\}^*$ (as a regular language in the alphabet $\{0, 1\}$) is trivial, however if r represents a non-empty language W distinct from $\{0, 1\}^*$, then the syntactic monoid of W is non-trivial and so $\text{Syn}_M(W)$ generates a non-trivial variety. Thus

if $P \neq PSPACE$, there can be no polynomial time method for constructing, from a regular expression r for a language W , a monoid generating the same variety as $\text{Syn}_M(W)$.

References

- [1] J. Almeida, *Finite Semigroups and Universal Algebra*, Series in Algebra, Vol. 3, World Scientific Publishing, Singapore, 1994.
- [2] G. Birkhoff, *On the structure of abstract algebras*, Proc. Camb. Philos. Soc. **31** (1935), 433–454.
- [3] S. Burris and H. Sankappanavar, *A Course in Universal Algebra*, Graduate Texts in Mathematics **78**, Springer Verlag, New York, 1980.
- [4] R. Cacioppo, *Finite bases for varieties and pseudovarieties*, Algebra Universalis **25** (1988), 263–280.
- [5] R. Cacioppo, *Nonfinitely based pseudovarieties and inherently nonfinitely based varieties*, Semigroup Forum **47** (1993), 223–226.
- [6] S. Eilenberg, *Automata, Languages and Machines Vol B*, Pure and Applied Mathematics, Academic Press, New York, 1976.
- [7] M. Garey and D. Johnson, *Computers and Intractability: A Guide to the theory of NP-Completeness*, W. H. Freeman and Company, New York, 1979.
- [8] R. McKenzie, Tarski’s finite basis problem is undecidable, *Internat. J. Algebra Comput.* **6** (1996), 49–104.
- [9] I. I. Mel’nik, On varieties and lattices of varieties of semigroups, in: *Studies in algebra. No. 2*, (V. V. Vagner, ed.), Izdat. Saratov. Univ., Saratov (1970), 47–57 [Russian].
- [10] S. Oates and M. B. Powell, *Identical relations in finite groups*, J. Algebra **1** (1964), 11–39.
- [11] P. Perkins, *Bases for equational theories of semigroups*, J. Algebra **11** (1969), 298–314.
- [12] M. V. Sapir, *Problems of Burnside type and the finite basis property in varieties of semigroups*, Math. USSR Izv., **30** No. 2 (1988), 295–314.
- [13] M. V. Sapir, *Inherently nonfinitely based finite semigroups*, Math. USSR-Sb., **61** No. 1 (1988), 155–166.
- [14] M. Sapir, *Sur la propriété de base finie pour les pseudovariétés de semigroupes finis*, C. R. Acad. Sci. Paris (Sér. I) **306** (1988), 795–797 [English and French].
- [15] M. V. Volkov, *The finite basis problem for finite semigroups*, Sci. Math. Jpn. **53** (2001), 171–199.