International Journal of Algebra and Computation
Vol. 15, No. 3 (2005) 405–422

World Scientific
www.worldscientific.com

FINITE SEMIGROUPS WITH INFINITE IRREDUNDANT IDENTITY BASES

MARCEL JACKSON
Department of Mathematics, La Trobe University
Victoria 3086, Australia
m.g.jackson@latrobe.edu.au

Received 16 February 2002
Revised 1 March 2004

Communicated by M. Sapir

We give the first examples of finite semigroups whose identities have infinite irredundant bases.

Keywords: Semigroup varieties; irredundant bases.

Mathematics Subject Classification: 20M07

A *basis* of identities Σ for a semigroup $\mathbf{S}$ is a set of identities satisfied by $\mathbf{S}$ from which all other identities of $\mathbf{S}$ can be derived. The basis Σ is said to be *irredundant* (or irreducible) if no proper subset of Σ is a basis for the identities of $\mathbf{S}$. If the basis Σ is finite, then it is always possible to extract an irredundant basis, however if Σ is infinite then it is conceivable that no irredundant basis exists. According to [20], initial optimism led to the supposition that all finite semigroups without a finite basis of identities might at least have an irredundant basis of identities. Subsequent examples of finite semigroups without irredundant identity bases (see [8], [9] or [14] for example) have shown this to be false, and moreover have provided increasing evidence that there are no finite semigroups with infinite irredundant bases of identities. The possible existence of such a semigroup was first explicitly raised as far back as [16, Question 2.51a] and then in [17, Question 8.6] and most recently in [20, Problem 2.6], where it is speculated that the answer might be negative. We show that the answer is in fact positive and, at least within a restricted class, there are numerous examples.

The main result of the paper is Theorem 2.6 of Sec. 2, with our smallest example established in Proposition 2.7. In Sec. 3 we extend the applicability of this theorem. The proofs up to this point are not constructive in any practical sense and so Sec. 4 is devoted to giving a finite semigroup with an infinite irredundant basis that is of a basic form and that is also unique within a certain finitely based variety of semigroups.

1. Preliminaries

We begin with some notational definitions. Throughout this paper the symbols u, v, w, p, q — with or without subscripts — will be used exclusively to denote *words* (elements of the free semigroup X^+ over an alphabet X) or *possibly empty words* (elements of a free monoid X^* over X). For a word w, we will let $|w|$ denote the number of not necessarily distinct letters appearing in w (the *length* of w).

The relation of equality in free monoids and semigroups will be denoted by $\equiv$, while a formal expression $u \approx v$ (where u and v are words) will be called an *identity.* The identity $u \approx v$ is *satisfied* by a semigroup $\mathbf{S}$ (written $\mathbf{S} \models u \approx v$) if for all homomorphisms θ: $X^+ \to \mathbf{S}$ we have $\theta(u) = \theta(v)$. In this context, the homomorphism θ will be called an *assignment* while a homomorphism between free semigroups (or free monoids) will be called a *semigroup substitution* (or *monoid substitution* respectively). The set of all identities (over some fixed countably infinite set of letters) satisfied by $\mathbf{S}$ will be denoted by $\mathrm{Id}(\mathbf{S})$. An *equational deduction* of an identity $p \approx q$ from a set of identities Σ will be a sequence of identities $p_i \approx p_{i+1}$ (where i ranges from 1 up to $n-1$ for some $n \in \mathbb{N}$) such that $p_1 \equiv p$, $p_n \equiv q$ and 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 substitution θ_i such that p_{i+1} is obtained from p_i by replacing the subword $\theta_i(u_i)$ with the word $\theta_i(v_i)$. In this case (or if $p \equiv q$) we write $\Sigma \vdash p \approx q$. We will assume throughout that each of the words $p_1, p_2, \ldots, p_n$ in an equational deduction is distinct from each other. A variety $\mathbf{V}$ is said to finitely based (abbreviated FB) if there is a finite set of satisfied identities from which all identities of $\mathbf{V}$ may be deduced by equational deduction. A semigroup $\mathbf{S}$ is FB if the variety it generates, denoted $\mathbb{V}(\mathbf{S})$, is FB. Varieties and semigroups that are not FB are said to be not finitely based, or NFB. For further details on finite basis problems for semigroup identities, see [20].

It will be useful to let $\mathrm{occ}(x, w)$ denote the number of occurrences of the letter x in the word w and x will be said to be $\mathrm{occ}(x, w)$-occurring in w (or *linear* in w if $\mathrm{occ}(x, w) = 1$). We use $\mathrm{c}(w)$ (the *content* of w) to denote the set of letters that are at least 1-occurring in w. A word will be *n-limited* if for all letters x, we have $\mathrm{occ}(x, w) \leq n$.

Our examples of semigroups with infinite irredundant bases of identities are going to be nilpotent monoids. A finite semigroup $\mathbf{S}$ is said to be a *nilpotent monoid* if it has an identity element 1 and there is a number k such that the product of any k elements in $S \backslash \{1\}$ coincide. The value of any product of length k is clearly a zero element for $\mathbf{S}$. The semigroup $\mathbf{S}$ is also said to be *k-nilpotent*, and the smallest choice of k is the *nilpotency length* of $\mathbf{S}$. The class of finite nilpotent monoids was studied by Straubing [18] who showed that the closure of this class under taking isomorphic copies of subalgebras, homomorphic images and finite products is the class of finite monoids with trivial subgroups (that is, *aperiodic*) and central idempotents.

2. Irredundant Bases

Throughout this paper we will use ω to denote $\{0, 1, 2, 3, \ldots\}$ (where $0 := \emptyset$ and $n + 1 := \{0, 1, \ldots, n\}$), while $\mathbb{N}$ will be $\{1, 2, \ldots\}$. Our results will be based on the following lemma. (There are obvious variants using ordinals other than ω.)

Lemma 2.1. *Let* $\mathbf{S}$ *be a semigroup and* $f\colon \omega \to \omega$ *be a function satisfying* $f(n) \geq n$. *Suppose there is a family* $\{\Sigma_i\colon i \leq \omega\}$ *of finite and pairwise disjoint sets of nontrivial identities satisfied by* $\mathbf{S}$ *and satisfying the following properties*:

(1) $\Sigma := \bigcup_{i \leq \omega} \Sigma_i$ *is a basis for the identities of* $\mathbf{S}$;

(2) *if* $k < \omega$ *and* $p \approx q \in \Sigma_k$, *and* $\mathbf{S} \models p \approx p'$ *then for any identity* $u \approx v \in \Sigma_i$ *with* $i > f(k)$, *there is no substitution* θ *for which* $\theta(u)$ *is a subword of* p'.

Then $\mathbf{S}$ *has an irredundant basis.*

Proof. In this proof it is convenient to let $\Sigma_{i \leq j \leq k}$ denote the union $\bigcup_{i \leq j \leq k} \Sigma_j$. The irredundant basis, Φ, for $\mathbf{S}$ is created inductively by a careful selection of identities from Σ. First we select an irredundant subset $\Xi_0 \subseteq \Sigma_0$ as follows. We begin with Ξ_0 empty and will add new identities to it as we progress. We also consider a set Ξ'_0 initially given the value Σ_0. Assume that we have ordered the identities in Σ_0 in some fashion (while the choice here is arbitrary, it will be convenient for later reference to assume that a lexicographic ordering has been used). If the first identity in Σ_0, say $p \approx q$ follows from $\big(\Sigma_{0<i\leq f(0)} \cup \Xi'_0\big)\backslash\{p \approx q\}$, then leave Ξ_0 unchanged but remove $p \approx q$ from Ξ'_0. If $p \approx q$ does not follow from $\big(\Sigma_{0<i\leq f(0)} \cup \Xi'_0\big)\backslash\{p \approx q\}$ then add $p \approx q$ to Ξ_0 and leave Ξ'_0 unchanged. Now move to the next identity in Σ_0 and repeat the process. Since Σ_0 is finite, eventually this process finishes with $\Xi'_0 = \Xi_0$. Note that $\Xi_0 \cup \Sigma_{0<i\leq f(0)} \vdash \Sigma_0$.

Now assume that we have constructed Ξ_i for all i less than or equal to $k < \omega$ and let Φ_k denote the set $\cup_{i \leq k} \Xi_k$. Assume further that $\Phi_k \cup \Sigma_{k<i\leq f(k)} \vdash \Sigma_{i \leq k}$. In a similar fashion to before, we will construct a new set Ξ_{k+1} which is initially set to be empty and a set Ξ'_{k+1} which is initially set to equal Σ_{k+1}. We will assume that Σ_{k+1} is ordered in some fashion. Now consider the first identity $p \approx q$ in Σ_{k+1}. If $\big(\Phi_k \cup \Xi'_{k+1} \cup \Sigma_{k+1<i\leq f(k+1)}\big)\backslash\{p \approx q\} \vdash p \approx q$, then leave Ξ_{k+1} unchanged but remove $p \approx q$ from Ξ'_{k+1}. Otherwise, add the identity $p \approx q$ to Ξ_{k+1} and leave Ξ'_{k+1} unchanged. Then repeat this process with the next identity in Σ_{k+1}, and so on until all identities in Σ_{k+1} have been considered. This is the final value of Ξ_{k+1}. With $\Phi_{k+1} := \Phi_k \cup \Xi_{k+1}$ we have $\big(\Phi_{k+1} \cup \Sigma_{k+1<i\leq f(k+1)}\big) \vdash \bigcup_{j \leq k+1} \Sigma_j$.

Next we let Φ' denote the set $\bigcup_{n<\omega} \Phi_n$. To create the set Φ, we set Ξ_ω to be empty and Ξ'_ω to equal Σ_ω. Take the first identity $p \approx q$ in Σ_ω. If $(\Phi' \cup \Sigma_\omega)\backslash\{p \approx q\} \vdash p \approx q$ then leave Ξ_ω unchanged but remove $p \approx q$ from Ξ'_ω. Otherwise, include $p \approx q$ in Ξ_ω and leave Ξ'_ω unchanged. Move to the next identity and repeat. When this process finishes, define $\Phi := \Phi' \cup \Xi_\omega$.

We claim that Φ is an irredundant basis for $\mathbf{S}$. Firstly, we show it is a basis by showing that $\Phi \vdash \Sigma$. Let $u \approx v \in \Sigma$. If $u \approx v \in \Sigma_i$ for $i < \omega$ then by the above construction, $\Phi_{f(i)} \cup \Sigma_{f(i)<j\leq f(f(i))} \vdash u \approx v$. Now if $\mathbf{S} \models u \approx u'$, then by condition (2), there is no identity in $\Sigma_{f(i)<j\leq f(f(i))}$ that can be applied to u'. Hence the deduction of $u \approx v$ from $\Phi_k \cup \Sigma_{f(i)<j\leq f(f(i))}$ only involves identities in $\Phi_{f(i)}$, a subset of Φ. Hence $\Phi \vdash u \approx v$. The case when $u \approx v \in \Sigma_\omega$ is similar but easier.

Now we show that if we remove any identity from Φ, then the remaining identities fail to form a basis for the identities of $\mathbf{S}$. We argue by contradiction. Say that there is an identity $p \approx q \in \Phi$ such that $\Phi\backslash\{p \approx q\} \vdash p \approx q$. Specifically, let $p \equiv p_0 \approx p_1 \approx p_2 \approx \cdots \approx p_n \equiv q$ be a sequence of satisfied identities such that for each $i \leq n-1$, $p_i \not\equiv p_{i+1}$ and there is $u_i \approx v_i \in \Phi\backslash\{p \approx q\}$ and substitutions θ_i such that p_{i+1} is obtained from p_i by replacing the subword $\theta(u_i)$ in p_i by $\theta(v_i)$. Now there is a $k \leq \omega$ such that $p \approx q \in \Xi_k$. If $k < \omega$ then for each $i \leq n$, $\mathbf{S} \models p \approx p_i$, and so condition (2) implies that $u_i \approx v_i \in \Phi_{f(k)}\backslash\{p \approx q\}$, but this contradicts the inclusion of $p \approx q$ in Ξ_k and therefore also in Φ. Again, the case when $k = \omega$ is similar though easier. $\square$

We note that an obvious extension of this lemma will hold for arbitrary algebras, not only semigroups. However to find some applications of Lemma 2.1 we are going to focus on the restricted class of finite nilpotent monoids as defined in Sec. 1.

If w is a word then we say that a letter $x \in \mathrm{c}(w)$ is *primitive* in w with respect to a finite nilpotent monoid $\mathbf{S}$ if under any assignment θ: $X^+ \to \mathbf{S}$ we have $\theta(x) = 1$ or $\theta(w) = 0$. A word w will be said to be primitive if it contains a primitive letter. It is obvious that if w is primitive and $\mathbf{S} \models w \approx w'$ then w' is primitive; hence we will also refer to primitive identities.

For the following lemmas we will fix some finite nilpotent monoid $\mathbf{S}$.

Lemma 2.2. *If w is primitive with respect to $\mathbf{S}$ and θ: $X^+ \to X^+$ is a substitution then $\theta(w)$ is primitive.*

Proof. Let $x \in \mathrm{c}(w)$ be primitive and $y \in \mathrm{c}(\theta(x))$. Say there is an assignment ϕ: $X^+ \to \mathbf{S}$ such that $\phi(y) \neq 1$. So $(\phi \circ \theta)(x) \neq 1$ and then $(\phi \circ \theta)(w) = 0$. $\square$

Lemma 2.3. *Let w be primitive with respect to $\mathbf{S}$. If $v \equiv w_1ww_2$ then v is primitive.*

Proof. Let x be primitive in w with respect to $\mathbf{S}$ and θ: $X^+ \to \mathbf{S}$ be such that $\theta(x) \neq 1$. Then $\theta(v) = \theta(w_1)\theta(w)\theta(w_2) = \theta(w_1)0\theta(w_2) = 0$. $\square$

This shows that the semigroup identities satisfied by $\mathbf{S}$ that are between primitive words imply no non-trivial identities between non-primitive words.

Let us say that a nilpotent monoid $\mathbf{S}$ is *n-limited*, if for every $a \in S\backslash\{1\}$, any product equals 0 if it involves more than n copies of a. Note that if a monoid is n-nilpotent, then it is $(n-1)$-limited. The following lemma follows almost immediately.

Lemma 2.4. *Let $n \in \mathbb{N}$ be such that $\mathbf{S}$ is n-limited. If $\mathrm{occ}(x, w) > n$ then x is primitive in w with respect to $\mathbf{S}$.*

Lemma 2.5. *Let* $n \in \mathbb{N}$ *be such that* $\mathbf{S}$ *is* n*-limited and let* w *be a non-primitive word for* $\mathbf{S}$*. If* $\mathbf{S} \models w \approx w'$ *then* $|w'| \leq n|w|$*.*

Proof. Let w be a word and $\mathbf{S} \models w \approx w'$ where $|w'| > n|w|$. We show that w is primitive.

Firstly, because $\mathbf{S}$ contains a non-trivial subsemilattice (on $\{0,1\}$), w' must contain the same letters as w. Now, since $|w'| > n|w|$, the pigeonhole principle implies that at least one letter occurs n times or more in w'. Hence w' is primitive by Lemma 2.4, and then w is also primitive because $\mathbf{S} \models w \approx w'$. □

We may now prove our main theorem.

Theorem 2.6. *Let* $\mathbf{S}$ *be a finite nilpotent monoid and let* $\mathrm{Id}_{\mathrm{p}}(\mathbf{S})$ *denote the set of all identities satisfied by* $\mathbf{S}$ *between non-primitive words over some fixed countable alphabet of letters. If there is a finite set* Σ_{p} *of identities of* $\mathbf{S}$ *between primitive words such that* $\mathrm{Id}_{\mathrm{p}}(\mathbf{S}) \cup \Sigma_{\mathrm{p}}$ *is a basis for the identities of* $\mathbf{S}$ *then* $\mathbf{S}$ *has an irredundant basis.*

Proof. We will apply Lemma 2.1. We begin by assuming that identities are included in $\mathrm{Id}_{\mathrm{p}}(\mathbf{S})$ only up to a change of letter names. For example, we can first insist that non-primitive identities are only included in $\mathrm{Id}_{\mathrm{p}}(\mathbf{S})$ if their letters form an initial segment of the list $x_1, x_2, \ldots$ and then remove all but the lexicographically earliest of each (finite) class of identities equivalent up to a change of letter names. Let $n \in \mathbb{N}$ be such that $\mathbf{S}$ is n-limited and let $f\colon \omega \to \omega$ be defined by $f(i) := ni$.

Now let Σ_ω denote the set Σ_{p} and for $i < \omega$, let Σ_i denote the subset of $\mathrm{Id}_{\mathrm{p}}(\mathbf{S})$ consisting of those identities $u \approx v$ where $\min\{|u|, |v|\} = i$. Since each identity is included only up to a change in letter names and since, by Lemma 2.5, the word u can be at most n times the length of v (and vice versa), Σ_i is a finite set. Also, $\Sigma_{i<\omega} \cup \Sigma_\omega$ is a basis for the identities of $\mathbf{S}$, whence condition (1) of Lemma 2.1 is satisfied.

We now check condition (2). Let $p \approx q \in \Sigma_k$ for some $k < \omega$ and p' be such that $\mathbf{S} \models p \approx p'$. Notice that the length of p' is at most nk. Now consider an identity $u \approx v \in \Sigma_i$ for some $i > f(k) = nk$ and let θ be a substitution. If $i = \omega$ then u is primitive and by Lemma 2.2 and Lemma 2.3, $\theta(u)$ is not a subword of p'. If $i < \omega$ then $|\theta(u)| \geq |u| \geq i > f(k) = nk \geq |p'|$ so $\theta(u)$ is again not a subword of p'. Hence condition (2) of Lemma 2.1 is satisfied and $\mathbf{S}$ has an irredundant basis of identities. □

Our application of Theorem 2.6 will be aided by an elegant construction due to Perkins [10]. Let W be a finite set of words over a finite alphabet X (not containing the symbol 0). The set $W_{\leq}$ of all possibly empty subwords of words in W inherits a partially defined product from the free monoid X^* — namely, if $u, v \in W_{\leq}$ and $uv \in W_{\leq}$, then we let $u \cdot v = uv$. Now adjoin a new element 0 and let any undefined products take the value 0. The multiplication on this groupoid is associative because it is isomorphic to the free monoid X^* factored by the ideal $X^* \backslash W_{\leq}$. We will denote this semigroup by $\mathrm{S}(W)$; it is clearly a nilpotent monoid because W is finite. Perkins used this construction to give the second example of a finite semigroup without a finite basis of identities (the first example also appears in [10]). It was also used (without the identity element) by M. Sapir in [13] and is the central source of examples in [5, 7, 15].

Consider $\mathrm{S}(\{abab\})$ whose 9 elements are

$$1, a, b, ab, ba, aba, bab, abab, 0.$$

In [7] it is shown that this is NFB and moreover, all monoids $\mathrm{S}(W)$ with fewer than 9 elements are FB. Specifically, it is shown that $\mathrm{S}(\{abab\})$ satisfies the identity

$$\begin{aligned} &x_1x_2\cdots x_{2n}t_1x_2x_4\cdots x_{2n}x_1x_3\cdots x_{2n-1}t_2 \\ &\quad\approx x_2x_4\cdots x_{2n}x_1x_3\cdots x_{2n-1}t_1x_1x_2\cdots x_{2n}t_2 \end{aligned}$$

for every $n \in \mathbb{N}$, but no finite subset of $\mathrm{Id}(\mathrm{S}(\{abab\}))$ is sufficient to derive all such identities (see [7, Example 4.2]).

We now use Theorem 2.6 to prove that $\mathrm{S}(\{abab\})$ has an infinite irredundant basis of identities.

Proposition 2.7. *The semigroup* $\mathrm{S}(\{abab\})$ *has an infinite irredundant identity basis.*

Proof. We first claim that an identity is primitive for $\mathrm{S}(\{abab\})$ if and only if it contains a letter occurring at least 3 times. The "if" direction follows from Lemma 2.4. For the other direction, assume that $\mathrm{occ}(x, w) \leq 2$ and consider the assignment sending x to the subword ab, and all other letters to 1. Then neither x nor w take the value 0.

Let Σ'_{p} denote the set of identities $\{x^3 \approx x^4,\ xt_1xt_2x \approx x^3t_1t_2,\ x^3y \approx yx^3\}$. These identities are all satisfied because x is a primitive letter in every participating word, and assigning 1 to x produces a tautology in each case. Let Σ_{p} denote the set of identities that can be obtained from Σ'_{p} by deleting a subset of $\{t_1, t_2\}$ (we call this the *closure under deletion of subsets of* $\{t_1, t_2\}$). Because $\mathrm{S}(\{abab\})$ is a monoid, these identities are also satisfied[a] and are primitive.

Now let $\mathrm{S}(\{abab\}) \models u \approx v$. We need to show that $\mathrm{Id}_{\mathrm{p}}(\mathbf{S}) \cup \Sigma_{\mathrm{p}} \models u \approx v$. This is trivial if $u \approx v \in \mathrm{Id}_{\mathrm{p}}(\mathbf{S})$, so we assume that $u \approx v$ is primitive. Using the laws of Σ_{p} we may move every occurrence of a primitive letter in u to the left-hand end and reduce it to a third power. Now recall that the set of primitive letters in u coincides with those in v, and so by performing the same procedure for v, we can use Σ_{p} to derive the identities $u \approx wu'$ and $v \approx wv'$, where w is the product $x_1^3x_2^3\cdots x_k^3$ of all third powers of primitive letters $x_1, \ldots, x_k$ in $u \approx v$. Also, $\mathrm{S}(\{abab\}) \models wu' \approx wv'$

---

[a] Note that substitution of 1 for a variable t in an identity $p \approx q$ is not an allowable equational deduction in the language of semigroups. However the resulting identity will hold in any semigroup that has a 1 and satisfies $p \approx q$.

and then the non-primitive identity $u' \approx v'$ must be satisfied by $\mathrm{S}(\{abab\})$, because this is the identity obtained by assigning the value 1 to each primitive letter in $wu' \approx wv'$. Hence $\mathrm{Id}_\mathrm{p} \cup \Sigma_\mathrm{p} \vdash u \approx wu' \approx wv' \approx v$, as required.

Theorem 2.6 now shows that $\mathrm{S}(\{abab\})$ has an irredundant identity basis. We have already observed that this basis is necessarily infinite. $\square$

We note that in this example we found that non-primitive identities are *balanced*, in the sense that letters occur the same number of times on either side of an identity. In this case one may observe that the function f in the proof of Theorem 2.6 can be chosen to be the identity map. While this appears to be a property of many semigroups of the form $\mathrm{S}(W)$, it does not hold universally. For example, consider the word $\sigma \equiv cabacbacabcbacabcacbc$ and let τ be the identity $ztxzxzyzxzyztzsz \approx zytzxzyzxzyztzsz$.

Example 2.8. τ is a non-balanced but non-primitive identity of $\mathrm{S}(\{\sigma\})$.

Proof. It is certainly not balanced because x occurs 3 times on the left and 2 times on the right. To see that τ is satisfied, first note that both sides have the same content, and so assignment of 0 to any letter in τ will lead to equality.

One can routinely check that σ is square free, in the sense that for all non-empty subwords u, the word uu is not a subword. It is also easily checked that if any set of letters is deleted from τ, then the result is an identity between words containing squares. Hence we need only consider assignments, θ, that assign no letter the value 1. Now $\mathrm{occ}(z, ztxzxzyzxzyztzsz) = \mathrm{occ}(z, zytzxzyzxzyztzsz) = 8$, while the only subword of σ that occurs 8 times is the single letter c. Hence, either both sides of τ take the value 0 under θ, or $\theta(z) = c$. From this one finds that the only way to avoid both sides of τ equaling 0 is if $\theta(s) = b$, $\theta(t) = a$, $\theta(x) = ba$, $\theta(y) = ab$ and $\theta(z) = c$. This assignment gives both sides of τ the value σ, showing that τ is satisfied by $\mathrm{S}(\{\sigma\})$ and also that it is non-primitive. $\square$

3. Increasing the Number of Examples

There are many other semigroups of the form $\mathrm{S}(W)$ shown to be not finitely based in [5, 7, 15]. Theorem 2.6 appears to apply to many of these, however there is a complication — to apply the theorem we require a finite choice of the set Σ_p, and this may not be possible. We do not give an example where Σ_p cannot be chosen to be finite, but instead provide an elementary adjustment to our construction that guarantees the existence of a finite choice in all the known cases. Some preliminary lemmas will be useful.

Lemma 3.1. *Let* $n \in \mathbb{N}$. *An identity* $u \approx v$ *is satisfied by* $\mathrm{S}(\{a^n\})$ *if and only if the following conditions hold*:

(1) $\mathrm{c}(u) = \mathrm{c}(v)$;
(2) *if either* $\mathrm{occ}(x, u) \leq n$ *or* $\mathrm{occ}(x, v) \leq n$ *then* $\mathrm{occ}(x, u) = \mathrm{occ}(x, v)$.

Proof. To begin, note that $\mathrm{S}(\{a^n\})$ contains a non-trivial subsemilattice (on $\{0,1\}$), and hence any satisfied identity must have property (1). So we will assume throughout the remainder of the proof that $u \approx v$ is some fixed identity satisfying (1).

Say $\mathrm{S}(\{a^n\}) \models u \approx v$. If $\mathrm{occ}(x,u) \leq n$, then the assignment, θ, taking x to a and all other letters to 1 gives $\theta(u) = a^{\mathrm{occ}(x,u)}$. Hence $\theta(v) = a^{\mathrm{occ}(x,u)}$ as well and because $a^{\mathrm{occ}(x,u)} \in \mathrm{S}(\{a^n\})$, this shows that $\mathrm{occ}(x,u) = \mathrm{occ}(x,v)$.

Now say that $u \approx v$ satisfies (2) and let θ be an assignment. Letters occurring more than n times in a word are primitive with respect to $\mathrm{S}(\{a^n\})$ and (2) implies that $\mathrm{occ}(y,u) > n$ if and only if $\mathrm{occ}(y,v) > n$. Thus if $\theta(u)$ was to differ from $\theta(v)$, we would need $\theta(y) = 1$ whenever $\mathrm{occ}(y,u) > n$. But the remaining letters satisfy $\mathrm{occ}(x,u) = \mathrm{occ}(x,v)$ and so $\theta(u) = \theta(v)$ because $\mathrm{S}(\{a^n\})$ is commutative. Hence $\mathrm{S}(\{a^n\}) \models u \approx v$. □

If $\mathbf{S}$ and $\mathbf{T}$ are finite nilpotent monoids then we let the $\{0,1\}$-*direct join* of $\mathbf{S}$ with $\mathbf{T}$ be the semigroup obtained by amalgamating $\mathbf{S}$ and $\mathbf{T}$ at $\{0,1\}$ and letting all undefined products equal 0 (this definition tacitly assumes that the non-idempotent elements of $\mathbf{S}$ and $\mathbf{T}$ have empty intersection). We denote this by $\mathbf{S} \vee \mathbf{T}$ and observe that the $\{0,1\}$-direct join of two n-limited nilpotent monoids is again an n-limited monoid. Note also that if V and W are sets of words over disjoint alphabets then the definitions give us $\mathrm{S}(V) \vee \mathrm{S}(W) = \mathrm{S}(V \cup W)$.

Lemma 3.2. *Let* $\mathbf{S}$ *and* $\mathbf{T}$ *be nilpotent monoids. Then* $\mathrm{Id}(\mathbf{S} \vee \mathbf{T}) = \mathrm{Id}(\mathbf{S}) \cap \mathrm{Id}(\mathbf{T})$.

Proof. Certainly $\mathbf{S}$ and $\mathbf{T}$ are subsemigroups of $\mathbf{S} \vee \mathbf{T}$ and so $\mathrm{Id}(\mathbf{S} \vee \mathbf{T}) \subseteq \mathrm{Id}(\mathbf{S}) \cap \mathrm{Id}(\mathbf{T})$. For the other direction, note that $\mathbf{S} \vee \mathbf{T}$ is isomorphic to the subsemigroup of the direct product $\mathbf{S} \times \mathbf{T}$ on the elements

$$\{(s,t) : s = t = 1 \text{ or both } 0 \in \{s,t\} \text{ and } 1 \notin \{s,t\}\}.$$

Hence any variety containing both $\mathbf{S}$ and $\mathbf{T}$ contains $\mathbf{S} \vee \mathbf{T}$. □

Lemma 3.3. *If* $\mathbf{S}$ *is an* n*-limited nilpotent monoid then a letter* x *is primitive in a word* w *with respect to* $\mathbf{S} \vee \mathrm{S}(\{a^n\})$ *if and only if* $\mathrm{occ}(x,w) > n$.

Proof. Say that $\mathrm{occ}(x,w) \leq n$. Let θ assign 1 to all letters except x, and assign x the value a. Then $\theta(x) \neq 1$ and $\theta(w) \neq 0$, so x is not primitive in w with respect to $\mathbf{S} \vee \mathrm{S}(\{a^n\})$.

Conversely, if $\mathrm{occ}(x,w) > n$, and θ is an assignment with $\theta(x) \neq 1$, then $\theta(w) = 0$ because $\theta(w)$ is a product involving more than n copies of $\theta(x)$. □

We will say that a semigroup $\mathbf{S}$ is NFB with respect to a system of identities Σ if $\mathbf{S} \models \Sigma$ but no finite subset of $\mathrm{Id}(\mathbf{S})$ is sufficient to derive Σ.

Proposition 3.4. *Let* $\mathbf{S}$ *be an* n*-limited nilpotent monoid. Then* $\mathbf{S} \vee \mathrm{S}(\{a^n\})$ *has an irredundant basis. If* $\mathbf{S}$ *is NFB with respect to a system of balanced identities, then* $\mathbf{S} \vee \mathrm{S}(\{a^n\})$ *has an infinite irredundant basis of identities.*

Proof. It is clear that the identities of $\mathrm{S}(W)$ satisfy condition (1) of Lemma 3.1, and so by Lemma 3.2 the identities of $\mathbf{S} \vee \mathrm{S}(\{a^n\})$ are precisely those identities of $\mathbf{S}$ for which the second condition of Lemma 3.1 holds. Lemma 3.3 shows that the non-primitive identities of $\mathbf{S} \vee \mathrm{S}(\{a^n\})$ are the n-limited identities.

The remainder of this proof is similar to the proof of Proposition 2.7. Let $u \approx v$ be a primitive identity for $\mathbf{S} \vee \mathrm{S}(\{a^n\})$ and let Σ_{p} denote the closure of

$$\{x^{n+1} \approx x^{n+2}, xt_1xt_2x \cdots xt_nx \approx x^{n+1}t_1t_2 \cdots t_n, x^{n+1}t \approx tx^{n+1}\}$$

under deletion of subsets of $\{t_1, \ldots, t_{n+1}\}$. Both $\mathrm{S}(\{a^n\})$ and $\mathbf{S}$ satisfy Σ_{p} because x occurs more than n times in every participating word, and deletion of x leaves a tautology in each case. Moreover, Σ_{p} is a set of primitive identities with respect to $\mathbf{S} \vee \mathrm{S}(\{a^n\})$.

Using Σ_{p} we can derive the identity $u \approx u_1u_2$ and $v \approx v_1v_2$, where u_2 and v_2 are n-limited, u_1 and v_1 are of the form $x_1^{n+1} \cdots x_i^{n+1}$ for some i and $\mathrm{c}(u_1) \cap \mathrm{c}(u_2) = \emptyset$. Furthermore, property (2) of Lemma 3.1 shows that u_1 and v_1 are identical. Note that by deletion of the letters in $\mathrm{c}(u_1)$ we find that $\mathbf{S} \vee \mathrm{S}(\{a^n\}) \models u_2 \approx v_2$ and because both u_2 and v_2 are n-limited, we can use Lemma 3.3 to observe that $u_2 \approx v_2$ is non-primitive. Therefore the (finite) set Σ_{p} along with all non-primitive identities form a basis for the identities of $\mathbf{S} \vee \mathrm{S}(\{a^n\})$. By Theorem 2.6, $\mathbf{S} \vee \mathrm{S}(\{a^n\})$ has an irredundant basis of identities.

Now say that $\mathbf{S}$ is not finitely based with respect to a set Σ of balanced identities. By Lemma 3.1, $\mathrm{S}(\{a^n\})$, and hence $\mathbf{S} \vee \mathrm{S}(\{a^n\})$, also satisfies Σ. Let Φ be a finite subset of $\mathrm{Id}(\mathbf{S} \vee \mathrm{S}(\{a^n\}))$. Then Φ is a finite subset of $\mathrm{Id}(\mathbf{S})$ as well, and so we cannot derive Σ from Φ. Hence $\mathbf{S} \vee \mathrm{S}(\{a^n\})$ is not finitely based. □

It is not clear that every NFB nilpotent monoid $\mathbf{S}$ is NFB with respect to a system of balanced identities. The proof after Example 2.8 essentially shows that there are identities of nilpotent monoids that are necessarily non-balanced; such identities will be lost upon taking the $\{0,1\}$-direct join with $\mathrm{S}(\{a^n\})$ for suitable n. However, all of the non-finitely based monoids given in [5, 7, 15] are shown to be non-finitely based with respect to balanced identities. The methods in these papers are very general. For example, [5, Theorem 3.5] immediately shows that the potentially problematic monoid $\mathrm{S}(\{\sigma\})$ of Example 2.8 is NFB with respect to a system of balanced identities. In fact, if X is a fixed finite alphabet with $|X| > 1$, then almost all $\mathrm{S}(W)$ with W over X have the NFB-property with respect to a balanced system of identities ([3]; the identities used in this proof and other results in this direction can be found in [5]).

4. An Explicit Example

Theorem 2.6 is not sufficiently constructive to give any remotely tractable description of what an irredundant basis actually "looks like". Indeed most examples appear to have no easily describable basis of this kind. We now give an example with a very basic infinite irredundant basis and with the interesting property that this basis is unique within a certain finitely based variety of semigroups. We also find a similar example with uncountably many infinite irredundant identity bases. To get a really simple basis, we have found it necessary to move to more general nilpotent monoids than those of the form $\mathrm{S}(W)$.

Recall that if L is a subset of a free monoid, then the syntactic monoid of L is the largest congruence such that L is a union of congruence classes. This congruence $\sim_L$ is given by defining $u \sim_L v$ if and only if for all possibly empty words w_1, w_2 we have $w_1 u w_2 \in L \Leftrightarrow w_1 v w_2 \in L$. The quotient $X^*/{\sim_L}$, called the *syntactic monoid* of L, is denoted by $\mathrm{Syn}_{\mathrm{M}}(L)$; see [1] for details. The set L is often called a *language*. When W is a finite set of words, we can see from the definition of $\mathrm{S}(W)$ as a quotient of a free monoid that W is a union of congruence classes. Hence $\sim_W$ contains the congruence giving $\mathrm{S}(W)$, or in other words, $\mathrm{Syn}_{\mathrm{M}}(W)$ is a quotient of $\mathrm{S}(W)$; in particular, this means that syntactic monoids of finite languages are nilpotent monoids.

Throughout the remainder of this section we will denote the language $\{abba, abab, acabcb\}$ by the symbol T, the language

$$\{axyxayzz, xaayxyzz, xayaxyzz, xayxyazz,$$
$$xyaxayzz, xyxaayzz, xyxayazz\}$$

by U, the singleton language $\{abbacddc\}$ by V, and finally, the language $\{xaabbxyy, xbbaaxyy\}$ by W. We are going to consider the semigroup $\mathrm{S}(T \cup U \cup V) \vee \mathrm{Syn}_{\mathrm{M}}(W)$. We will denote this throughout by $\mathbf{A}$ and make free use of Lemma 3.2 and the comments preceding it throughout the remainder of the section.

Let Σ_{p} denote the set of identities

$$\{xt_1xt_2x \approx x^3t_1t_2, xxtx \approx x^3t, xtxx \approx x^3t, x^3t \approx tx^3, x^3 \approx x^4\}$$

and Φ the set $\{x_1x_2\cdots x_nx_n\cdots x_2x_1yy \approx yyx_1x_2\cdots x_nx_n\cdots x_2x_1 \colon n \in \mathbb{N}\}$.

The main result of this section is the following proposition.

Proposition 4.1. *The set* $\Sigma_{\mathrm{p}} \cup \Phi$ *is an irredundant basis of semigroup identities for* $\mathbf{A}$. *Furthermore, any identity basis for* $\mathbf{A}$ *within the variety defined by* Σ_{p} *contains a copy of each identity in* Φ; *hence* Φ *is the unique* (*up to a change of letter names and up to replacing* $p \approx q$ *by* $q \approx p$) *irredundant basis for* $\mathbf{A}$ *within the variety defined by* Σ_{p}.

The proof of Proposition 4.1 will be completed over a number of lemmas.

Lemma 4.2. $\mathrm{Syn}_{\mathrm{M}}(W)$ *satisfies* Φ *but not* $xx_1x_1x_2x_2xyy \approx yyxx_1x_1x_2x_2x$.

Proof. Consider the fully invariant congruence θ corresponding to Φ on the free monoid $\{a, b, x, y\}^*$. Most of the identities in Φ are too long to be applied to either of the words in W. Indeed, the only member of Φ which can be applied to a word in W is the identity $x_1x_1yy \approx yyx_1x_1$. Applying this to a word in W simply produces the other word in W. In other words, W is fixed under applications of the identities in Φ. Thus W is a union of congruence classes of θ (in fact it is a congruence class of θ) and by the definition of the syntactic monoid, we find that $\mathrm{Syn}_{\mathrm{M}}(W)$ is a quotient of $\{a,b,x,y\}^*/\theta$. In particular, $\mathrm{Syn}_{\mathrm{M}}(W)$ satisfies Φ.

On the other hand, one can apply $x_0x_1x_1x_2x_2x_0y_1y_1 \approx y_1y_1x_0x_1x_1x_2x_2x_0$ to the word $xaabbxyy$ to produce a word outside of W. Hence $\mathrm{Syn}_{\mathrm{M}}(W)$ fails this identity. $\square$

A similar though easier proof shows that $\mathrm{S}(T \cup U \cup V)$ also satisfies Φ. Using Lemma 2.4 and the fact that $\mathrm{Syn}_{\mathrm{M}}(W)$ is a quotient of $\mathrm{S}(W)$, it follows that $\mathbf{A} \models \Sigma_{\mathrm{p}}$ and hence we have the following lemma.

Lemma 4.3. $\mathbf{A}$ *satisfies* $\Phi \cup \Sigma_{\mathrm{p}}$.

Using Σ_{p}, every word w can be reduced to a word $x_1^3x_2^3\cdots x_n^3w'$ in which w' is 2-limited and $\mathrm{c}(w') \cap \{x_1,\ldots,x_n\} = \emptyset$. Note also that if u and v are 2-limited with $\{x_1,\ldots,x_n\} \cap (\mathrm{c}(u) \cup \mathrm{c}(v)) = \emptyset$ then $\mathbf{A} \models x_1^3\cdots x_n^3u \approx x_1^3\cdots x_n^3v$ if and only if $\mathbf{A} \models u \approx v$. This means that the set of all identities between 2-limited words together with Σ_{p} form a basis for the identities of $\mathbf{A}$. Note that 2-limited identities are non-primitive (because T contains a squared subword), while all members of Σ_{p} are primitive.

Before continuing with the next lemmas, we recall some concepts and notation from [7, 15]. For a word w and letters $x_1, x_2, \ldots, x_n$ we will let $w(x_1,\ldots,x_n)$ denote the word obtained from w by deleting all letters except those in the list $x_1,\ldots,x_n$. Now let $p \approx q$ be an identity. If $x, y \in \mathrm{c}(p)$ then the pair (x,y) will be said to be an *unstable occurrence pair* in $p \approx q$ if $p(x,y) \not\equiv q(x,y)$; otherwise (x,y) is *stable* in $p \approx q$. The pair (x,y) is unstable in the word p with respect to a semigroup $\mathbf{T}$ if it is unstable in some identity $p \approx q$ satisfied by $\mathbf{T}$; otherwise (x,y) is stable in p (with respect to $\mathbf{T}$). If w is a word and $x \in \mathrm{c}(w)$ then we use the symbols ${}_ix$ to denote the ith occurrence of x in w (if it exists). An easy fact is that every balanced identity $w \approx w'$ containing an unstable pair contains an unstable pair (x,y) for which there are i,j such that ${}_ix\,{}_jy$ is a subword of w but ${}_jy$ occurs before ${}_ix$ in w'. Such a pair is called a *critical pair*.

For a deeper analysis of the semigroup identities of monoids, one also needs the concept of an isoterm, as introduced by Perkins [10]. A word w is an *isoterm* for a semigroup $\mathbf{S}$ if $\mathbf{S} \models w \approx w'$ implies $w \equiv w'$. It follows from the definition of $\mathrm{S}(W')$ that if $w \in W'$ then w is an isoterm for $\mathrm{S}(W')$.

Lemma 4.4. *If x is a 2-occurring letter in a word w and t is linear in w then (x,t) is stable in w with respect to* $\mathbf{A}$.

Proof. This is because xxt, txx, xtx are all isoterms for $\mathrm{S}(T)$ and therefore for $\mathbf{A}$ also. $\square$

We will say that a subword u of a word w is *repeated* if w can be written as $w_1uw_2uw_3$ for some possibly empty words w_1, w_2, w_3. The word w will be said to be *without repeats* if its repeated subwords are single letters.

Lemma 4.5. *Let $p \approx q$ be a non-primitive identity satisfied by* $\mathbf{A}$ *such that p contains a repeated subword u other than a single letter. Let $p' \approx q'$ denote the identity obtained from $p \approx q$ by deleting all but one of the letters in* $\mathrm{c}(u)$. *Then $p' \approx q' \vdash p \approx q$.*

Proof. First note that $p \approx q$ is 2-limited and so u must be of the form $x_1 \cdots x_i$ for some distinct letters $x_1, \ldots, x_i$. Now $x_1 \cdots x_i x_1 \cdots x_i$ is an isoterm (because *abab* is in T) and so $p(x_1, \ldots, x_i) \equiv x_1 \cdots x_i x_1 \cdots x_i \equiv q(x_1, \ldots, x_i)$. Say that u does not appear as a repeated subword of q. So there is a letter z that occurs between the occurrences of x_j and x_{j+1} (for some $j < i$) in q. Now z cannot be a linear letter by Lemma 4.4. Also, because z does not appear between ${}_ix_j$ and ${}_ix_{j+1}$ in p (for $i = 1$ or 2), the word $p(x_j, x_{j+1}, z)$ must be one of the following words:

$$x_jx_{j+1}zzx_jx_{j+1}, \quad zx_jx_{j+1}zx_jx_{j+1}, \quad x_jx_{j+1}zx_jx_{j+1}z,$$
$$zx_jx_{j+1}x_jx_{j+1}z, \quad zzx_jx_{j+1}x_jx_{j+1}, \quad x_jx_{j+1}x_jx_{j+1}zz.$$

All except the last two are isoterms because of the words *abab* and *abba* in T. However, if $p(x_j, x_{j+1}, z)$ is one of the last two words, it follows that $q(x_j, x_{j+1}, z)$ is also one of the last two words (again, because *abab* and *abba* are isoterms). Thus we have a contradiction. Hence we have $p \equiv p_1x_1 \cdots x_ip_2x_1 \cdots x_ip_3$ and $q \equiv q_1x_1 \cdots x_iq_2x_1 \cdots x_iq_3$ for some words $p_1, p_2, p_3, q_1, q_2, q_3$.

Now it is easily seen that

$$p_1x_1p_2x_1p_3 \approx q_1x_1q_2x_1q_3 \vdash p_1x_1 \cdots x_ip_2x_1 \cdots x_ip_3 \approx q_1x_1 \cdots x_iq_2x_1 \cdots x_iq_3$$

as required. □

This lemma indicates that we may restrict our attention to identities whose words are without repeats.

Definition 4.6. A word u will be called *rigid* if every letter in $\mathrm{c}(u)$ occurs exactly twice in u and (up to a change in letter names) there are letters $z_1, z_2, \ldots, z_n$ such that for each $i \leq n-1$, $u(z_i, z_{i+1}) \equiv z_iz_{i+1}z_iz_{i+1}$, and z_1 is the first letter to appear in u and z_n is the rightmost letter to appear in u.

For example *abbcac* is rigid because we can choose $z_1 = a$ and $z_2 = c$ (with $n = 2$). If every letter appearing in a word w occurs exactly twice in w and $x \notin \mathrm{c}(w)$ then xwx is rigid.

Over the next two lemmas we are going to show that if $u \approx v$ is a 2-limited identity satisfied by $\mathbf{A}$, then u can be transformed into v by commuting a series of adjacent rigid subwords.

Lemma 4.7. *Let u and v be rigid words in disjoint alphabets and let $x \in \mathrm{c}(u)$ and $y \in \mathrm{c}(v)$. If (x, y) is unstable in an identity $uv \approx w$ satisfied by* $\mathbf{A}$ *then for all $z_1 \in \mathrm{c}(u)$ and $z_2 \in \mathrm{c}(v)$, we have $w(z_1, z_2) \equiv z_2z_2z_1z_1$.*

Proof. This follows because *abba* and *abab* are isoterms for $\mathbf{A}$. □

Lemma 4.8. *Let $w \approx w'$ be a 2-limited identity satisfied by* $\mathbf{A}$ *with unstable critical pair* (x, y) (*where x has its first occurrence before that of y*). *There are rigid words u and v in disjoint alphabets such that $w \equiv w_1uvw_2$ and u contains* (*both occurrences of*) *x and v contains* (*both occurrences of*) *y.*

Proof. Let (x, y) be a critical pair in a satisfied non-primitive identity $w \approx w'$. Since *abba*, *abab*, *abb*, *bba* and *aba* are isoterms, we can assume without loss of generality that $w(x, y) \equiv xxyy$; indeed since (x, y) is critical we have $w \equiv w_1xw_2xyw_3yw_4$. We will define a set fix_x inductively as follows: $x \in \mathrm{fix}_x$; if z_1 is in fix_x and z_2 is 2-occurring in w then $w(z_1, z_2) \in \{z_1z_2z_2z_1, z_2z_1z_2z_1\}$ implies $z_2 \in \mathrm{fix}_x$. Likewise we may define fix_y by setting $y \in \mathrm{fix}_y$ and if $z_1 \in \mathrm{fix}_y$ then $w(z_2, z_1) \in \{z_1z_2z_2z_1, z_1z_2z_1z_2\}$ implies $z_2 \in \mathrm{fix}_y$. The sets fix_x and fix_y are going to correspond to the letters in u and v respectively and these will be consecutive rigid subwords of w. It follows from the definition that if we delete all letters in $\mathrm{c}(w)$ except those in fix_x then the resulting word is rigid and likewise for fix_y. Lemma 4.7 then implies that if $z_1 \in \mathrm{fix}_x$ and $z_2 \in \mathrm{fix}_y$ then $w(z_1, z_2) \approx w'(z_1, z_2)$ is the identity $z_1z_1z_2z_2 \approx z_2z_2z_1z_1$. To complete the proof of Lemma 4.8 we need to show that the words $u = w(\mathrm{fix}_x)$ and $v = w(\mathrm{fix}_y)$ are actually subwords of w. That is, that every letter that appears in w between an occurrence of two letters contained in fix_x is itself contained in fix_x. We will say that a letter that has an occurrence in w between occurrences of two letters in fix_x, "occurs within the span of fix_x".

We will first show by contradiction that no linear letter occurs within the span of fix_x. Let t be linear and assume that it occurs within the span of fix_x. There must be a letter $z \in \mathrm{fix}_x$ such that $w(z, t) \equiv ztz$. However then $w(z, t, y) \equiv ztzyy$ which is an isoterm, contradicting the fact that (z, y) is unstable in w.

Now say z is 2-occurring and has an occurrence within the span of fix_x. If the second occurrence, ${}_2z$, of z occurs within the span of fix_x then there is a letter $z' \in \mathrm{fix}_x$ such that $w(z, z') \in \{zz'zz', z'zzz'\}$ showing that z is also in fix_x. If ${}_2z$ does not occur within the span of fix_x then it occurs to the right of ${}_1y$ (because this immediately succeeds ${}_2x$ in w). Since z has an occurrence within the span of fix_x there is a letter $z' \in \mathrm{fix}_x$ such that $w(z', z) \equiv z'zz'z$. But then $w(z', y, z) \in \{z'zz'yzy, z'zz'yyz\}$ and both of these are isoterms, contradicting the fact that (z', y) is unstable in w. □

This lemma shows that in order to derive a non-primitive identity $p \approx q$ for $\mathbf{A}$ it suffices to be able to commute certain rigid subwords.

Lemma 4.9. *Let $w \approx w'$ be a non-primitive identity satisfied by* $\mathbf{A}$. *Then $\Phi \vdash w \approx w'$.*

Proof. We may assume that $w \approx w'$ is non-trivial and that (x, y) is a critical pair. Let w_1, w_2, u and v be as in the statement of Lemma 4.8. These assumptions (and the fact that $\mathrm{Id}(\mathbf{A})$ is closed under the deletion of letters from identities) imply that $\mathbf{A} \models uv \approx vu$. We need to show that $\Phi \vdash uv \approx vu$, so that we will have

$\Phi \vdash w \approx w_1vuw_2$. By Lemma 4.7, the identity $w_1vuw_2 \approx w'$ has fewer unstable pairs than $w \approx w'$ and since there can be only finitely many unstable pairs, this will complete the proof.

First note that Lemma 4.5 implies that we may assume that w is without repeats. This will turn out to imply that uv is equivalent up to a change of letter names to a word that appears in an identity in Φ.

Claim 4.10. u is of the form $x_1x_2\cdots x_nx_n\cdots x_2x_1$.
Let $y \in \mathrm{c}(v)$. As $\mathbf{A} \models uv \approx vu$ we have that uyy is not an isoterm. To begin, we show that there is no pair of letters $z_1, z_2 \in \mathrm{c}(u)$ such that $u(z_1, z_2) \equiv z_1z_2z_1z_2$. This is where we use the words in language U. Assume that z_1 and z_2 exist and have been chosen such that the length of the subword between ${}_1z_1$ and ${}_1z_2$ is minimal amongst all such pairs. Since w contains no repeated subwords, there is a 2-occurring letter a such that $uv(z_1, z_2, a, y)$ is one of the following words:

$$az_1z_2z_1az_2y^2, z_1aaz_2z_1z_2y^2, z_1az_2az_1z_2y^2, z_1az_2z_1z_2ay^2,$$
$$z_1z_2az_1az_2y^2, z_1z_2z_1aaz_2y^2, z_1z_2z_1az_2ay^2.$$

(Note that we have omitted the cases where a occurs between between ${}_1z_1$ and ${}_1z_2$ and $u(z_1, a) \equiv z_1az_1a$, because these contradict the minimality of the length of the subword between ${}_1z_1$ and ${}_1z_2$.) Up to a change of letter names, each of these words is in U, and therefore is an isoterm. However (x, y) is unstable and u is a rigid word containing x and z_1, so by Lemma 4.7 the pair (z_1, y) is also unstable, a contradiction. Therefore there is no pair of letters $z_1, z_2 \in \mathrm{c}(u)$ such that $u(z_1, z_2) \equiv z_1z_2z_1z_2$.

Now recall the definition of rigid in Definition 4.6. We have shown that the sequence $z_1, \ldots, z_n$ in that definition must contain only one element. This letter can only be x — this is because (x, y) is critical in $w \approx w'$ and then x is the rightmost letter in u. Hence u can be written as $xu'x$, where u' is either empty, of the form z^2 (for some letter z) or satisfies the following property: for every pair of letters $z_1, z_2 \in \mathrm{c}(u')$, with ${}_1z_1$ occurring before ${}_1z_2$, $u'(z_1, z_2)$ is one of the words $z_1z_2z_2z_1$ or $z_1z_1z_2z_2$. It will suffice to show that u cannot be deleted to a word of the form $z_1z_1z_2z_2$, because then u is of the form $x_1x_2\cdots x_nx_n\cdots x_2x_1$. So let us now assume that there are letters z_1, z_2 such that u deletes to $z_1z_1z_2z_2$. Because x occurs first and last in u, it follows that $x \notin \{z_1, z_2\}$. Then uv deletes to $xz_1z_1z_2z_2xyy$ while (x, y) is unstable. This contradicts the second part of Lemma 4.2 and so the proof of the claim is complete.

Now $\mathbf{A} \models uv \approx vu$ and so we may also apply the claim to the subword v in vu, that is, v is of the form $y_1y_2\cdots y_my_m\cdots y_2y_1$ (again, we must have that $y \equiv y_1$ because (x, y) is critical). To complete the proof of the lemma it will suffice to prove that $1 \in \{n, m\}$. If both $n, m > 1$ then uv deletes to $x_1x_2x_2x_1y_1y_2y_2y_1$, which is an isoterm because of V. This contradicts the fact that vu deletes to $y_1y_2y_2y_1x_1x_2x_2x_1$ and so the lemma is proved. □

This lemma and the comments after Lemma 4.3 show that $\Phi \cup \Sigma_{\mathrm{p}}$ is a basis for $\mathrm{Id}(\mathbf{A})$. To complete the proof of Proposition 4.1 it remains to note that $\Phi \cup \Sigma_{\mathrm{p}}$ is irredundant and that Φ is essentially unique. Because $\Phi \cup \Sigma_{\mathrm{p}}$ is a basis, it follows that the only word w for which $x_1x_2\cdots x_nx_n\cdots x_2x_1yy \approx w$ is a non-trivial identity satisfied by $\mathbf{A}$ is the word $yyx_1x_2\cdots x_nx_n\cdots x_2x_1$. Hence any derivation of this identity from some set Φ' that is satisfied by $\mathbf{A}$ involves just one single application of an identity. It is easily seen that such an identity must be equivalent up to a change of letter names to $x_1x_2\cdots x_nx_n\cdots x_2x_1yy \approx yyx_1x_2\cdots x_nx_n\cdots x_2x_1$. Thus this identity is contained in any basis for $\mathbf{A}$. This also implies that the basis is irredundant within the variety defined by Σ_{p} since the only identity in $\Phi\cup\Sigma_{\mathrm{p}}$ that can be applied to $x_1x_2\cdots x_nx_n\cdots x_2x_1yy \approx yyx_1x_2\cdots x_nx_n\cdots x_2x_1$ is itself. The result now follows because Σ_{p} is an irredundant system of semigroup identities. □

To contrast the last statement of Proposition 4.1, we now note the following result.

Proposition 4.11. *The semigroup* $\mathrm{S}(T \cup U \cup V)$ *has uncountably many different* (*up to change of letter names and symmetry of identities*) *irredundant bases within the variety defined by* Σ_{p}.

Proof. We show that, for each $n \in \mathbb{N}$, any irredundant basis of identities for the semigroup $\mathrm{S}(T \cup U \cup V)$ contains (up to a change of letter names) *exactly one* of the identities

$$x_1x_2\cdots x_nz_1z_1z_2z_2x_n\cdots x_2x_1yy \approx yyx_1x_2\cdots x_nz_1z_1z_2z_2x_n\cdots x_2x_1 \tag{1}$$

or

$$x_1x_2\cdots x_nz_1z_1z_2z_2x_n\cdots x_2x_1yy \approx yyx_1x_2\cdots x_nz_2z_2z_1z_1x_n\cdots x_2x_1, \tag{2}$$

and that for each $n \in \mathbb{N}$, the choice of which of these is included is arbitrary. Both the identities can be seen to be satisfied by $\mathrm{S}(T \cup U \cup V)$, as can be the identity $xxyy \approx yyxx$. This last identity cannot be deduced from any shorter identity satisfied by $\mathrm{S}(T \cup U \cup V)$, because xxy and yxx are isoterms. Hence any basis for $\mathrm{S}(T \cup U \cup V)$ contains an identity equivalent to $xxyy \approx yyxx$. Similar arguments show that any basis for $\mathrm{S}(T \cup U \cup V)$ contains a non-trivial identity $p \approx q$ where p or q is equal up to a change of letter names to $x_1x_2\cdots x_nz_1z_1z_2z_2x_n\cdots x_2x_1yy$ and such that the pair corresponding to (x_1, y) is unstable. From this it easily follows that $p \approx q$ (or $q \approx p$) is equal up to a change of letter names to either identity (1) or identity (2). Therefore any basis for $\mathrm{S}(T \cup U \cup V)$ contains at least one of these identities. However $xxyy \approx yyxx$ and identity (1) imply identity (2), while $xxyy \approx yyxx$ and identity (2) imply identity (1). Hence an irredundant basis for $\mathrm{S}(T \cup U \cup V)$ contains exactly one of the two identities for any given $n \in \mathbb{N}$.

Theorem 2.6 shows that $\mathrm{S}(T \cup U \cup V)$ does have an irredundant basis (with Σ_{p} defined as for $\mathbf{A}$ above). Now let M be an arbitrary subset of $\mathbb{N}$. The length of the words in identities (1) and (2) for a given n is $2n + 6$, hence in the proof of Theorem 2.6 there are identities in Σ_{2n+6} that are equal up to a change of letter names to each of these identities. Now adjust the ordering of the sets Σ_{2n+6} such that for $n \in M$, a copy of identity (1) is the first listed identity and for $n \notin M$, a copy of identity (2) is the first listed identity. The above arguments now show that the resulting basis contains identity (1) for a given n if and only if $n \in M$. Hence, $\mathrm{S}(T \cup U \cup V)$ has uncountably many different irredundant bases. $\square$

The following lemma is folklore.

Lemma 4.12. *If* $\mathbb{V}_1$ *is a variety with an infinite irredundant basis of identities and* $\mathbb{V}_2$ *is a finitely based variety containing* $\mathbb{V}_1$ *then, in the lattice of varieties, the interval* $[\mathbb{V}_1, \mathbb{V}_2]$ *is uncountable.*

Proof. Let Σ be an infinite irredundant basis of identities for $\mathbb{V}_1$. Some cofinite subset Σ' of Σ fails on $\mathbb{V}_2$ and then each subset of Σ' defines a distinct subvariety of $\mathbb{V}_2$ containing $\mathbb{V}_1$. $\square$

In [7] it is shown that Σ_{p} of Proposition 4.1 is a basis for the identities of $\mathbb{V}(\mathrm{S}(\{abab, abba, aabb\}))$ and so this is a finitely based variety containing $\mathbf{A}$. By Lemma 4.12 we have the following theorem.

Theorem 4.13. *There are uncountably many semigroup varieties between* $\mathbb{V}(\mathrm{S}(\{abab, abba, aabb\}))$ *and* $\mathbb{V}(\mathbf{A})$.

It is known [7] that for every finite nilpotent monoid $\mathbf{S}$ there is a finite language P with $\mathrm{S}(P)$ being FB and such that $\mathbf{S}$ is in the semigroup (or monoid) variety of $\mathrm{S}(P)$. Hence Lemma 4.12 shows that to extend our irredundant basis results amongst nilpotent monoids to the language of monoids, one would find a finitely generated *monoid* variety of nilpotent monoids with uncountably many subvarieties. It is certainly easy to see that there are infinitely many monoid varieties between the monoid varieties $\mathbb{V}_{\mathrm{M}}(\mathrm{S}(\{abab, abba, aabb\}))$ and $\mathbb{V}_{\mathrm{M}}(\mathbf{A})$ but they are of a very restricted form. Indeed, with a little work one can verify that every variety in the interval $[\mathbb{V}_{\mathrm{M}}(\mathbf{A}), \mathbb{V}_{\mathrm{M}}(\mathrm{S}(\{abab, abba, aabb\}))]$ can be obtained by removing some final portion of the sequence of identities $x_1x_1yy \approx yyx_1x_1, x_1x_2x_2x_1yy \approx yyx_1x_2x_2x_1, \ldots$.

In fact, while there are many known finitely generated semigroup varieties with uncountably many subvarieties [4, 19], the first known finitely generated monoid varieties with this property have only very recently been found by the author and R. McKenzie [6]. (The corresponding problem for finitely generated inverse semigroup varieties in the signature $\{\cdot, {}^{-1}\}$ appears to be open and is also of some interest; see [11] for related results in this direction.)

As we now show, the monoid $\mathbf{A}$ *does not* have any irredundant basis of monoid identities.

Proposition 4.14. *In the language of monoids,* $\mathbf{A}$ *has no irredundant basis of identities.*

Proof. Suppose that Σ is an irredundant basis (necessarily infinite) for the identities of the monoid **A**. Let Σ'_{p} denote a minimal subset of Σ from which the identities Σ_{p} can be derived — this exists and is finite by the definition of equational deduction. Therefore there is an identity $p \approx q \in \Sigma \backslash \Sigma'_{\mathrm{p}}$. Consider a number n greater than the number of letters in $p \approx q$ and let Σ_1 be a minimal subset of Σ from which the identity $x_1x_2 \cdots x_nx_n \cdots x_1yy \approx yyx_1x_2 \cdots x_nx_n \cdots x_1$ can be derived. The arguments following the proof of Lemma 4.9 imply that Σ_1 contains only one identity, and that must delete to one of the form $x_1x_2 \cdots x_nx_n \cdots x_1yy \approx yyx_1x_2 \cdots x_nx_n \cdots x_1$. Hence $p \approx q \notin \Sigma_1$. However, for all $i \leq n$,

$$\begin{aligned} x_1x_2 \cdots x_nx_n \cdots x_1yy \approx yyx_1x_2 \cdots x_nx_n \cdots x_1 \vdash x_1x_2 \cdots x_ix_i \cdots x_1yy \\ \approx yyx_1x_2 \cdots x_ix_i \cdots x_1 \end{aligned}$$

in the language of monoids while the proof of Lemma 4.9 shows that these identities along with Σ_{p} can be used to derive every identity in at most n letters. Hence $\Sigma'_{\mathrm{p}} \cup \Sigma_1 \vdash p \approx q$, contradicting the assumption that Σ is irredundant. ☐

We finish with some questions and problems (problem (5) can be attributed to Gorbunov; see [2]).

(1) Is there a finite monoid with an infinite irredundant basis of monoid identities?
(2) Is there a finite nilpotent monoid with no irredundant basis of semigroup identities?
(3) Is there a finite algebra (or semigroup) of finite type with an infinite irredundant identity basis but with no recursive irredundant identity basis?
(4) Is there a finite algebra (or semigroup) with two different identity bases, one irredundant and the other containing no equivalent irredundant subset?
(5) Is there a finite algebra (or semigroup) with an infinite irredundant basis of quasi-identities?

With regard to question (3), we note that any finite nilpotent monoid that satisfies the conditions of Theorem 2.6 has a recursive irredundant identity basis. Indeed, when given a finite set of primitive identities for a finite nilpotent monoid **S** satisfying the conditions of Theorem 2.6, it is possible to decide when a given non-primitive identity is contained in the constructed basis; this is because Lemma 2.5 gives a computable upper bound on the length of a derivation of a given non-primitive identity from any given finite set of non-primitive identities. Thus if the conditions of Theorem 2.6 are satisfied, there is a choice of Σ_{p} (we do not necessarily know how to make this choice) such that the constructed basis is recursive.

We showed above that, up to a change of letter names, all irredundant identity bases for **A** within the variety $\mathbb{V}(\mathrm{S}(\{abba, abab, aabb\}))$ are recursive (there was only one possibility). In contrast however, Proposition 4.11 shows that $\mathrm{S}(T \cup U \cup V)$ has a non-recursive irredundant identity basis (there can be only countably many recursive bases).

With regard to (4), it is known that every set of first order sentences is equivalent to an irredundant set [12]. Hence if (4) is weakened to include arbitrary first order formulæ (rather than just identities), then any variety without an irredundant basis of identities is a solution.

References

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

[2] V. A. Gorbunov, *Algebraic Theory of Quasivarieties*, Siberian School of Algebra and Logic (Consultants Bureau, New York, 1998).

[3] M. Jackson, Small semigroup related structures with infinite properties, PhD thesis, University of Tasmania, Hobart (1999).

[4] M. Jackson, Finite semigroups whose varieties have uncountably many subvarieties, *J. Algebra* **228** (2000) 512–535.

[5] M. Jackson, The finite basis problem for finite Rees quotients of free monoids, *Acta Sci. Math.* (*Szeged*) **67** (2001) 121–159.

[6] M. Jackson and R. McKenzie, Interpreting graph colourability in finite semigroups, to appear in *Internat. J. Algebra Comput.*

[7] M. Jackson and O. Sapir, Finitely based, finite sets of words, *Internat. J. Algebra Comput.* **10** (2000) 683–708.

[8] J. Kad'ourek, On varieties of combinatorial inverse semigroups II, *Semigroup Forum* **44** (1992) 53–78.

[9] G. Mashevitsky, An example of a finite semigroup without irreducible basis in the class of completely 0-simple semigroups, *Uspekhi Mat. Nauk* **38** (1983) 211–213 (in Russian; English translation in *Russian Math. Surveys* **38**, 192–193).

[10] P. Perkins, Bases for equational theories of semigroups, *J. Algebra* **11** (1969) 298–314.

[11] N. Reilly, Large varieties generated by small inverse semigroups, *Acta Sci. Math.* (*Szeged*) **58** (1993) 25–41.

[12] I. Reznikoff, Tout ensemble de formules de la logique classique est equivalent a un ensemble independant, *C. R. Acad. Sci. Paris* **260** (1965) 2385–2388 (in French).

[13] M. Sapir, Sur la propiété de base finie pour les pseudovariétés de semigroupes finis, *C. R. Acad. Sci. Paris Sr. I Math.* **306**(20) (1988), 795–797 (in English and French).

[14] M. Sapir, On cross semigroup varieties and related questions, *Semigroup Forum* **42** (1991) 345–364.

[15] O. Sapir, Finitely based words, *Int. J. Algebra Comput.* **10** (2000) 457–480.

[16] L. N. Shevrin (ed.), *The Sverdlovsk Notebook. Unsolved Problems of the Theory of Semigroups*, 2nd edn. (Ural State University, Sverdlovsk, 1979) (in Russian).

[17] L. N. Shevrin and M. V. Volkov, Identities of semigroups, *Izv. Vyssh. Uchebn. Zaved. Mat.* **11** (1985) 3–47 (in Russian; English translation in *Soviet Math. Izv. VUZ* **29**, 1–64).

[18] H. Straubing, The variety generated by finite nilpotent monoids, *Semigroup Forum* **24** (1982) 25–38.

[19] A. N. Trahtman, Six-element semigroup generates a variety with uncountably many subvarieties, in *Algebraic Systems and their Varieties* (Sverdlovsk 1988), pp. 138–143 (in Russian).

[20] M. V. Volkov, The finite basis problem for finite semigroups, *Sci. Math. Jpn.* **53** (2001) 171–199.