Semigroup Forum OF1–OF8

DOI: 10.1007/s002330010009

RESEARCH ARTICLE

The Membership Problem for $\langle \mathbf{a}, \mathbf{b} : \mathbf{bab^2} = \mathbf{ab} \rangle$

D. A. Jackson

Communicated by Gerard J. Lallement

Throughout, $\mathcal{P}$ is the semigroup presentation $\langle a, b\colon\ bab^2 = ab \rangle$ for the semigroup S_1. Lallement and Rosaz, [5], have shown that the semigroups S_k having presentations $\langle a, b\colon\ b(ab)^k b = ab \rangle$ are residually finite. They also find normal forms for elements of S_k. Specialized to $k = 1$, every element of S_1 is either a power of a or else it can be represented uniquely by a word in one of the forms $a^\ell b^p a^n$ or $a^\ell b^p aba^n$ with $p > 0$. We begin by giving a new proof of this, which also establishes some invariants for the set of words that represent an element of S_1. Our main goal here is to prove that the membership problem is solvable for the presentation $\mathcal{P}$. It follows easily from work of Golubov that the semigroups S_k are not finitely separable.

Lemma 1. i) *Suppose $v \equiv b^{j_\ell} ab^{j_{\ell-1}} a \cdots ab^{j_1} ab^{j_0} a^n$ with $j_0 > 0$. Define q by*

$$q = \sum_{\text{even } i} j_i - \sum_{\text{odd } i} j_i.$$

If $q > 0$, then $v = a^\ell b^q a^n$ mod $\mathcal{P}$.
If $q \le 0$, then $\ell > 0$ and $v = a^{\ell-1} b^{1-q} aba^n$ mod $\mathcal{P}$.

ii) *Conversely, suppose that a word v on the alphabet $\{a, b\}$ has exactly k occurrences of the letter a and at least one occurrence the letter b so that we may write $v \equiv b^{t_k} ab^{t_{k-1}} a \cdots ab^{t_1} ab^{t_0}$ where at least one exponent t_i is nonzero. If $v = a^\ell b^p a^n$ modulo $\mathcal{P}$ or if $v = a^{\ell-1} b^p aba^n$ modulo $\mathcal{P}$ where $\ell \ge 1$ then $k = \ell + n$, $t_n > 0$ and $t_i = 0$ for $i < n$. For $0 \le i \le \ell$ write j_i for t_{n+i} and define q as in part* a) *using just the $\ell + 1$ exponents j_i. If $v = a^\ell b^p a^n$ modulo $\mathcal{P}$ where $p > 0$, then $p = q$. If $v = a^{\ell-1} b^p aba^n$ modulo $\mathcal{P}$ where $\ell \ge 1$ and $p > 0$, then $p = 1 - q$.*

Proof. *i)* Suppose $v \equiv b^{j_\ell} ab^{j_{\ell-1}} a \cdots ab^{j_1} ab^{j_0} a^n$ where $j_0 > 0$. Let r be the largest index such that $j_r > 0$, so $v \equiv a^{\ell-r} b^{j_r} ab^{j_{r-1}} a \cdots ab^{j_1} ab^{j_0} a^n$. We use induction on r for $0 \le r \le \ell$, to show that $v = a^\ell b^q a^n$ mod $\mathcal{P}$ if $q > 0$ and that $v = a^{\ell-1} b^{1-q} aba^n$ mod $\mathcal{P}$ if $q \le 0$.

Suppose first that $r=0$. Then $v \equiv a^\ell b^{j_0} a^n$ and we are done with $q = j_0 = \sum_{\text{even } i} j_i - \sum_{\text{odd } i} j_i$.

Similarly, if $r=1$, then $v \equiv a^{\ell-1} b^{j_1} a b^{j_0} a^n$. If we are in the case where $j_0 = 1$, then $\sum_{\text{even } i} j_i - \sum_{\text{odd } i} j_i \leq 0$ and we are done with $q = 1 - j_1$ and $j_1 = 1-q$. If $j_1 \geq j_0 > 1$, then $q = j_0 - j_1 \leq 0$, $v \equiv a^{\ell-1} b^{j_1} a b^{j_0} a^n = a^{\ell-1} b^{j_1 - j_0 + 1} a b a^n \bmod \mathcal{P}$ and we are done since $j_1 - j_0 + 1 = 1 - q$. If $j_1 < j_0$, then $q > 0$, $v \equiv a^{\ell-1} b^{j_1} a b^{j_0} a^n = a^\ell b^{j_0 - j_1} a^n \bmod \mathcal{P}$ and we are done with $q = j_0 - j_1$.

Assume then that $r \geq 2$. If $j_r < j_{r-1}$, then we can reduce the occurrence of $b^{j_r} a b^{j_{r-1}}$ within $v \equiv a^{\ell-r} \underline{b^{j_r} a b^{j_{r-1}}} a \cdots a b^{j-1} a b^{j_0} a^n$ to obtain $v = a^{\ell-r+1} b^{j_{r-1}-j_r} a b^{j_{r-2}} a \cdots a b^{j_1} a b^{j_0} a^n \bmod \mathcal{P}$ and we are done by the induction hypothesis. If $j_r \geq j_{r-1}$, let s be the largest index with $s < r-1$ and $j_s > 0$. If $s = r-2$, then

$$\begin{aligned} v &\equiv a^{\ell-r} b^{j_r} a \underline{b^{j_{r-1}} a b^{j_{r-2}}} a \cdots a b^{j_0} a^n \\ &= a^{\ell-r} b^{j_r} a b^{j_{r-1}+(j_r - j_{r-1}+1)} a b^{j_{r-2}+(j_r-j_{r-1}+1)} a \cdots a b^{j_0} a^n \bmod \mathcal{P} \\ &\equiv a^{\ell-r} \underline{b^{j_r} a b^{j_r+1}} a b^{j_{r-2}+j_r-j_{r-1}+1} a \cdots a b^{j_0} a^n \\ &= a^{\ell-r+1} b a b^{j_{r-2}+j_r-j_{r-1}+1} a \cdots a b^{j_0} a^n \bmod \mathcal{P} \end{aligned}$$

and we are done by the induction hypothesis. Similarly, if $s < r-2$, then

$$\begin{aligned} v &\equiv a^{\ell-r} b^{j_r} a b^{j_{r-1}} a^{r-s-2} \underline{a b^{j_s}} a b^{j_{s-1}} a \cdots a b^{j_0} a^n \\ &= a^{\ell-r} b^{j_r} a b^{j_{r-1}} a^{r-s-3} \underline{ab} a b^{j_s+1} a b^{j_{s-1}} a \cdots a b^{j_0} a^n \bmod \mathcal{P} \\ &= a^{\ell-r} b^{j_r} a b^{j_{r-1}} a^{r-s-3} b a b^2 a b^{j_s+1} a b^{j_{s-1}} a \cdots a b^{j_0} a^n \bmod \mathcal{P} \\ &= a^{\ell-r} b^{j_r} a \underline{b^{j_{r-1}} a b} (a b^2)^{r-s-3} a b^{j_s+1} a \cdots a b^{j_0} a^n \bmod \mathcal{P} \\ &= a^{\ell-r} \underline{b^{j_r} a b^{j_r+1}} a b^{1+(j_r-j_{r-1}+1)} (a b^2)^{r-s-3} a b^{j_s+1} a \cdots a b^{j_0} a^n \bmod \mathcal{P} \\ &= a^{\ell-r+1} a b a b^{j_r - j_{r-1}+2} (a b^2)^{r-s-3} a b^{j_s+1} a \cdots a b^{j_0} a^n \bmod \mathcal{P} \end{aligned}$$

and we are again done by the induction hypothesis.

ii) For the converse direction, we want to use induction on the length of a sequence of elementary transitions from $a^\ell b^p a^n$ to v or a sequence of elementary transitions from $a^{\ell-1} b^p a b a^n$ to v. For the base case, we need to observe that the conclusions are true when this sequence has length 0. If $v \equiv a^\ell b^p a^n$ in the free semigroup on $\{a, b\}$, then we do have $t_i = 0$ for $0 \leq i < n, t_n = p$ and $t_i = 0$ for $n < i \leq \ell + n = k$, so $q = \sum_{\text{even } i} j_i - \sum_{\text{odd } i} j_i = j_0 = t_n = p$. Similarly, if $v \equiv a^{\ell-1} b^p a b a^n$ in the free semigroup on $\{a, b\}$, then $t_i = 0$ for $0 \leq i < n$, $t_n = j_0 = 1$, $t_{n+1} = j_1 = p$ and $t_i = j_{i-n} = 0$ for $n+2 \leq i \leq \ell + n = k$, so $1 - q = 1 + \sum_{\text{odd } i} j_i - \sum_{\text{even } i} j_i = 1 + j_1 - j_0 = p$.

Suppose that $a^\ell b^p a^n = w_0 \to w_1 \to \cdots \to w_T = v$ is a sequence of elementary transitions from $a^\ell b^p a^n$ to v or that $a^{\ell-1} b^p a b a^n = w_0 \to w_1 \to \cdots \to w_T = v$ is a sequence of elementary transitions from $a^{\ell-1} b^p a b a^n$ to v. Since ab and bab^2 both contain just one occurrence of a, the number of occurrences of a in each w_i will be $\ell+n$. Observe that no elementary transition can ever involve a letter a from a^n (so we will have $t_i = 0$ for $0 \leq i < n$) or lower the rightmost nonzero exponent on a b to zero (so we will have $t_n = j_0 > 0$). Every elementary transition will either raise or lower two consecutive exponents on b's, so that $\sum_{\text{even } i} j_i$ and $\sum_{\text{odd } i} j_i$ will either both increase by one or else both decrease by one and the value of q is invariant under elementary transitions. ■

If v is a word on the alphabet in which both a and b occur, then v can be written in the form $b^{j_\ell} a b^{j_{\ell-1}} a \cdots a b^{j_1} a b^{j_0} a^n$ where $j_0 > 0$. We will define the **base** for any such word to be $\sum_{\text{even } i} j_i - \sum_{\text{odd } i} j_i$. By Lemma 1, this number, as well as ℓ and n will be the same for every word v' on $\{a, b\}$ which represents the same element of S_1 as v.

Given a set $\mathcal{B} = \{b^{x_1}, b^{x_2}, \ldots, b^{x_N}\}$ of powers of b in the free semigroup on $\{a, b\}$, it is clear that b^P is in the subsemigroup of $\{a, b\}^+$ generated by $\mathcal{B}$ if and only if there are nonnegative integers $m_1, m_2, \ldots, m_N$ such that $P = \sum m_i x_i$. The following lemma will be useful. This is a modest generalization of an exercise in [6].

Lemma 2. *Suppose that $x_1, x_2, \ldots, x_N$ are positive integers and that the greatest common divisor of this set of numbers is the number d. If z is any natural number that is divisible by d and z is at least as large as $x_1 x_2 \cdots x_N / d^N$, then there are nonnegative integers $m_1, m_2, \ldots m_N$ such that $z = \sum m_i x_i$.* ■

Theorem 3. *The membership problem is solvable for the semigroup presentation $\mathcal{P} = \langle a, b : bab^2 = ab \rangle$.*

Proof. Suppose that v is a word on the alphabet $\{a, b\}$ and that $\mathcal{U}$ is a set $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$ of words on the alphabet $\{a, b\}$. We need to exhibit an algorithm for deciding whether or not v is equivalent modulo $\mathcal{P}$ to some product of elements of $\mathcal{U}$.

Write the set $\mathcal{U}$ as the disjoint union $\mathcal{U} = \mathcal{U}_a \cup \mathcal{U}_b \cup \mathcal{U}_{mx}$ where $\mathcal{U}_a = \{u_i \in \mathcal{U} : |u_i|_b = 0\}$,$\mathcal{U}_b = \{u_i \in \mathcal{U} : |u_i|_a = 0\}$ and $\mathcal{U}_{mx} = \{u_i \in \mathcal{U} : |u_i|_a > 0 \text{ and } |u_i|_b > 0\}$.

If $v = b^p$, then v is not equivalent modulo $\mathcal{P}$ to any product of words from $\mathcal{U}$ if $\mathcal{U}_b$ is empty. Suppose then that $\mathcal{U}_b$ is nonempty and, for the sake of notation, describe $\mathcal{U}_b$ by $\mathcal{U}_b = \{b^{x_1}, b^{x_2}, \ldots, b^{x_N}\}$. Then $v = b^p$ is equivalent modulo $\mathcal{P}$ to a product of elements of $\mathcal{U}$ if and only if there are nonnegative integers $m_1, m_2, \ldots, m_N$ such that $p = \sum m_i x_i$. We can effectively determine whether or not this occurs.

Replacing $\mathcal{U}_b$ by $\mathcal{U}_a$, a very similar argument holds if $v = a^t$ for some $t > 0$.

Assume then that $|v|_a > 0$ and $|v|_b > 0$. Then, either we can write v in normal form as $v = a^\ell b^p a^n$ where $p > 0$ and $\ell + n > 0$ or else we can write

v in normal form as $v = a^{\ell-1}b^p aba^n$ where $p > 0$ and $\ell \geq 1$. We will regard the choice of form and ℓ, p and n as fixed and known for the remainder of this proof.

We will say that a finite sequence $(u_{i_1}, u_{i_2}, \ldots, u_{i_k})$ **has an interesting product** if the product $u_{i_1}u_{i_2}\cdots u_{i_k}$ is equivalent modulo $\mathcal{P}$ either to a word $a^\ell b^P a^n$ for some $P > 0$ or else, when $\ell \geq 1$, this product is equivalent modulo $\mathcal{P}$ to a word $a^{\ell-1}b^P aba^n$ for some $P > 0$ and all of the factors, with at most one exception, are either in $\mathcal{U}_a$ or in $\mathcal{U}_{mx}$.

Since, with at most one exception, we require that $u_{i_j} \in \mathcal{U}_a \cup \mathcal{U}_{mx}$ for every factor of an interesting product, we might have one factor which contains no occurrences of a, but every other factor must contain at least one occurrence of a. For every interesting product we have $|u_{i_1}u_{i_2}\cdots u_{i_k}|_a = \ell + n$, so the number k of factors in an interesting product can be at most $\ell+n+1$ and there are only a finite number of interesting products. We can effectively compute all of these and compute the base of each. The set of interesting products is defined for a fixed v in which both a and b occur. By construction and Lemma 1, each interesting product will have the same number of occurrences of a as v and will have the same number of occurrences of a to the right of the rightmost occurrence of b.

Roughly stated, we will determine whether or not v is equivalent modulo $\mathcal{P}$ to a product of words from $\mathcal{U}$ by inserting products of words from $\mathcal{U}_b$ between the factors of interesting products. By Lemma 1, we will never find v in this fashion if we insert a power of b between two of the rightmost n occurrences of a in an interesting product. If $u_{i_1}u_{i_2}\cdots u_{i_k}$ is an interesting product, we say that the product has an **insertion point between** u_{i_j} and $u_{i_{j+1}}$ if $|u_{i_{j+1}}\cdots u_{i_k}|_a \geq n$. This insertion point has **even parity** or **odd parity** according as $|u_{i_{j+1}}\cdots u_{i_k}|_a - n$ is even or odd. An interesting product may have no insertion points which occur between factors. An interesting product always has a **left-hand insertion point** to the left of u_{i_1} and this left-hand insertion point has even parity when ℓ is even and has odd parity when ℓ is odd. If $n = 0$, then an interesting product has a **right-hand insertion point** to the right of the rightmost factor. Right-hand insertion points, when they exist, always have even parity. When an interesting product has one of its factors in $\mathcal{U}_b$, then there will always be insertion points on both sides of this factor and these insertion points will have the same parity.

If v is equivalent modulo $\mathcal{P}$ to a product of factors from $\mathcal{U}$, then either we will obtain an interesting product if we delete all of the factors from $\mathcal{U}_b$ which occur in the product or else there is a factor from $\mathcal{U}_b$ in the product, positioned to the left of a^n, such that we will obtain an interesting product when we delete all of the factors from $\mathcal{U}_b$ except this one. If the set of interesting products is empty, then we know that v is not equivalent modulo $\mathcal{P}$ to a product of factors from $\mathcal{U}$. When the set of interesting products is nonempty, it will suffice to determine whether or not we can obtain a word equivalent to v by inserting words on $\mathcal{U}_b$ at insertion points of any one of these interesting products. By

Lemma 1, if we insert a word on $\mathcal{U}_b$ at an insertion point with even (odd) parity, it does not matter which insertion point with even (odd) parity is used.

We examine each interesting product and determine whether 1) it has both even and odd insertion points, 2) it has only even insertion points, or else 3) the product has only odd insertion points.

If $\mathcal{U}_b$ is empty, then v is equivalent to a product of words from $\mathcal{U}$ if and only if v is equivalent modulo $\mathcal{P}$ to one or more of the interesting products. Assume that $\mathcal{U}_b$ is nonempty and write again $\mathcal{U}_b = \{b^{x_1}, b^{x_2}, \ldots, b^{x_N}\}$. Write d for the greatest common divisor of the positive integers x_i.

Suppose first that we are examining an interesting product which has both even and odd insertion points. By Lemma 2, we can construct words b^{z_i} on $\mathcal{U}_b$ for every sufficiently large multiple, z_i, of d. Using this, given any integer multiple, z, of d, we can construct words b^{z_1} and b^{z_2} with $z = z_1 - z_2$. When $d = 1$, we can choose this difference to be the difference between the base of v and the base of the interesting product. We then insert b^{z_1} and b^{z_2} into appropriate insertion points with different parity and find that v is equivalent modulo $\mathcal{P}$ to a product of words from $\mathcal{U}$. If $d > 1$, then we see that we can use this interesting product to construct v as a product of words from $\mathcal{U}$ if and only if this interesting product has a base which is equivalent modulo d to the base of v.

Suppose then that we are examining an interesting product which has only even insertion points. (The case where the interesting product has only odd insertion points is similar.) If the base of this interesting product is greater than the base of v, then inserting powers of b at an even insertion points will construct a word with a still greater base, and we will not be able to use this interesting product to construct v as a product of words from $\mathcal{U}$. If the base of this interesting product is less than the base of v, then we can effectively determine whether or not the difference z can be written as a sum $\sum m_i x_i$ where the m_i are nonnegative integers. If this is possible, then we can insert $b^z = (b^{x_1})^{m_1}(b^{x_2})^{m_2} \cdots (b^{x_N})^{m_N}$ into the interesting product at any even insertion point and obtain a product of words on $\mathcal{U}$ which is equivalent to v modulo $\mathcal{P}$. If the difference z cannot be written as such a sum, then we may discard this interesting product from further considerations. ∎

Example 4. Let $\mathcal{U} = \{u_1 = a^4b^2a^7, u_2 = ab^5a^3, u_3 = a^5, u_4 = b^6, u_5 = b^{10}\}$. To illustrate the algorithm above, we will determine, for various words v whether or not v is in the subsemigroup H of S_1 that is generated by $\mathcal{U}$. We see easily that a^{15} and b^{32} are elements of H and that a^{34}, b^8 and b^{31} cannot be elements of H. Since $|u_1|_a = 11, |u_2|_a = 4, |u_3|_a = 5$ while $|u_4|_a = |u_5|_a = 0$, we cannot have that v is in H if v is any word with $|v|_a = 1, 2, 3, 6$ or 7.

We examine in more detail whether not v is in H for several cases where $|v|_a = 20$. In such cases, we can have $v \in H$ if and only if v is equal in S_1 to a product of elements of $\mathcal{U}$ in which the total number of occurrences of a in the factors is 20. We might have u_4 and u_5 occurring many times in such a product, but we must have that u_1, u_2 and u_3 each occur exactly once or else that u_3 occurs four times while u_1 and u_2 do not occur or else that u_2 occurs five times while u_1 and u_3 do not occur . We deduce that a word v with $|v|_a = 20$ can be in H if and only if it is equal to a product obtained by inserting powers of $u_4 = b^6$ and $u_5 = b^{10}$ between (or following or preceding) the factors in one of the eight products

$$\begin{array}{lll} u_1u_2u_3 = a^4b^2a^7 \cdot ab^5a^3 \cdot a^5 & & u_1u_3u_2 = a^4b^2a^7 \cdot a^5 \cdot ab^5a^3 \\ u_2u_1u_3 = ab^5a^3 \cdot a^4b^2a^7 \cdot a^5 & & u_2u_3u_1 = ab^5a^3 \cdot a^5 \cdot a^4b^2a^7 \\ u_3u_1u_2 = a^5 \cdot a^4b^2a^7 \cdot ab^5a^3 & & u_3u_2u_1 = a^5 \cdot ab^5a^3 \cdot a^4b^2a^7 \\ u_3^4 = a^5 \cdot a^5 \cdot a^5 \cdot a^5 & \text{or} & u_2^5 = ab^5a^3 \cdot ab^5a^3 \cdot ab^5a^3 \cdot ab^5a^3 \cdot ab^5a^3 \end{array}$$

If, for example, $v = a^{18}b^5a^2$, we see that no insertion of powers of b between, before, or after the factors in any of these eight products will yield a word which is equal to v in S_1. In every product, the rightmost occurrence of b is either too far to the left or too far to the right. We conclude that $a^{18}b^5a^2$ is not in H. The same argument shows that $a^{18}b^pa^2 \notin H$ and $a^{17}b^paba^2 \notin H$ for every natural number p.

In the proof of Theorem 3 above, we have defined, given $\mathcal{U}$ and v, a set of interesting products. For the set $\mathcal{U}$ of this example, we will always have that the set of interesting products is the empty set if $|v|_a = 7$ or if $v = a^{18}b^pa^2$ or $v = a^{17}b^paba^2$ for some natural number p.

If $v = a^8b^7a^{12}$, then we see that the set of interesting products is $\{u_2u_1u_3, u_4u_2u_1u_3, u_5u_2u_1u_3, u_2u_4u_1u_3, u_2u_5u_1u_3\}$. The only interesting product that we will need to consider in this case is $u_2u_1u_3$ since the other four are all obtained by inserting u_4 or u_5 at insertion points of this product. For $u_2u_1u_3 = ab^5a^3 \cdot a^4b^2a^7 \cdot a^5$, we have a left-hand insertion point and an insertion point between u_2 and u_1. Both of these insertion points have even parity. The base of $u_2u_1u_3$ is -3. For either of $u_5u_2u_1u_3$ or $u_2u_5u_1u_3$ the base is 7, so $a^8b^7a^{12} \in H$. It is not hard to see that $a^8b^pa^{12} \in H$ for p odd and $p \geq 13$. For every even natural number p, we will have $a^8b^pa^{12} \notin H$: since u_4 and u_5 are both even powers of b, when we insert powers of u_4 and u_5 into $u_2u_1u_3$, we can change the base value of -3 only by an even integer. With words v ending in a^{12}, we can insert powers of u_4 and u_5 into $u_2u_1u_3$ only to the left of u_2 or between u_2 and u_1. An insertion of b^m in either of these locations will raise the base by m. Since b^6 is the smallest power of b that we may insert, we see that $a^8ba^{12} \notin H$. Similarly, we see that $a^8b^pb^{12}$ is in H if $p = 3$ or $p = 9$, but is not in H if $p = 5$ or $p = 11$. We do have that $a^7b^4aba^{12} \in H$, since this is $u_2u_1u_3$. If $p \neq 4$, then $a^7b^paba^{12} \notin H$, since we can only raise and not lower the base of $u_2u_1u_3$ by inserting powers of u_4 and u_5.

If $v = a^{15}b^2a^5$, then none of the eight products displayed above are interesting products, but we should examine the products $u_1u_2u_3, u_2u_1u_3$ and u_3^4 in the display. To achieve the final a^5 factor, we will need to insert at least one factor u_4 or u_5 before the final u_3 in each of these, and our set of interesting products here will be $\{u_1u_2u_4u_3, u_1u_2u_5u_3, u_2u_1u_4u_3, u_2u_1u_5u_3, u_3^3u_4u_3, u_3^3u_5u_3\}$. The base for $u_3^3u_4u_3$ is 6. We can lower this by 4 if we insert another factor of u_4 before the final u_3 and an initial factor of u_5: the base for $u_5u_3^3u_4^2u_3$ is 2 so $a^{15}b^2a^5 \in H$. This generalizes to show that $a^{15}b^pa^5 \in H$ for every even p and that $a^{14}b^paba^5 \in H$ for every odd p. Similarly, the base for $u_1u_2u_5u_3$ is 3 and we can insert additional factors of u_4 and u_5 into this product to show that $a^{15}b^pa^5 \in H$ for every odd p and that $a^{14}b^paba^5 \in H$ for every even p.

Finite separability is a semigroup property that is stronger than residual finiteness. A definition is given in the next paragraph. If the semigroup S is finitely separable, then the membership problem is solvable for every finite presentation for S. An analogous result in group theory states that locally extended residually finite (LERF) groups have solvable membership problems. For both semigroups and groups, the proof that finite separability or LERF implies solvability of the membership problem is very much like a standard proof that residual finiteness implies solvability of the word problem.

A semigroup S is **finitely separable** if for every subsemigroup M of S and every element $s \in S-M$, there is a finite semigroup Q and a homomorphism Φ of S onto Q such that $\Phi(s) \notin \Phi(M)$. A semigroup S **has finitely separable subsets** if for every subset M of S and every element $s \in S-M$, there is a finite semigroup Q and a homomorphism Φ of S onto Q such that $\Phi(s) \notin \Phi(M)$. The monoid S^1 is obtained from S by adjoining a new identity element 1. Following Golubov, [2], [3], for elements $x, y \in S$, we define the set $[y:x]$ by $[y:x] = \{(u,v) \in S^1 \times S^1 : uxv = y\}$.

Theorem 5 (Golubov, [2], [3]). *The semigroup S has finitely separable subsets if and only if for every $y \in S$, there are only a finite number of distinct sets $[y:x]$ as x ranges over S.* ∎

For the semigroup S_1 presented by $\mathcal{P} = \langle a, b \ : \ bab^2 = ab\rangle$, it is fairly easy to see that we have $(b^p, 1) \in [ab : ab^r]$ if and only if $1+p = r$ We see from this that $[ab : ab^{r_1}] \neq [ab : ab^{r_2}]$ if $r_1 \neq r_2$, so by Golubov's characterization, S_1 does not have finitely separable subsets. For the semigroup S_k, [5], presented by $\langle a, b \ : \ b(ab)^kb = ab\rangle$, we see similarly that $(((ba)^{k-1}b)^p, 1) \in [ab : ab^r]$ if and only if $1+p = r$ and then that S_k does not have finitely separable subsets.

Theorem 6 (Golubov, [2], [3]). *Suppose that S is a semigroup without idempotents. Then S is finitely separable if and only if S has finitely separable subsets.* ∎

Theorem 7 (Golubov, [2], [3]). *Suppose that S is a nonregular semigroup which satisfies the left cancellation law. Then S is finitely separable if and only if S has finitely separable subsets.* ∎

It is easily seen that there are no idempotents in S_1, but it seems more difficult to prove that there are no idempotents in S_k for $k > 1$. It is apparent that the semigroups S_k are not regular. As Lallement and Rosaz remark, it is known, see [1], that the semigroups S_k are left cancellative. We thus see that the semigroups S_k are not finitely separable.

References

[1] Adjan, S.I., "Defining Relations and Algorithmic Problems for Groups and Semigroups", Proceedings of the Steklov Institute of Mathematics in the Academy of Sciences of the USSR **85**, American Mathematical Society, Providence, Rhode Island, (1967).

[2] Golubov, E.A., *On finite separability in semigroups* (Russian), Dokl. Akad. Nauk SSSR **189** (1969), 20–22. English transl. in Soviet Math. Dokl. **10** (1969), 1321–1323.

[3] Golubov, E.A., *Finite separability in semigroups* (Russian), Sibirsk. Mat. Ž. **11** (1970), 1247–1263. English transl. in Siberian Math. J. **11** (1970), 920–931.

[4] Lallement, G.J., "Semigroups and Combinatorial Applications", John Wiley & and Sons, New York, (1979).

[5] Lallement, G.J., and L. Rosaz *Residual finiteness of a class of semigroups presented by a single relation*, Semigroup Forum **48** (1994), 169–179.

[6] LeVeque, W.J., "Topics in Number Theory, vol. 1", Addison-Wesley Publishing Company, Inc., Reading, MA, (1956).

Department of Mathematics and
Mathematical Computer Science
Saint Louis University
220 N. Grand Ave.
St. Louis, MO 63103-2007

Received June 16, 2000