THE SOLVABILITY OF THE WORD PROBLEM FOR CERTAIN SEMIGROUPS

ANN YASUHARA

Abstract. This paper establishes the solvability of the word problem for semigroups with one defining relation if that relation is of the form $A \sim BtC$ where (1) $A$ and $BtC$ are words on the generators of the semigroup but the generator $t$ does not occur in $A$, $B$ or $C$ and (2) the length of $A$ is greater than the max(length $B$, length $C$).

This paper is a small contribution toward the long range goal of verifying the conjecture that the word problem for semigroups with one defining relation is solvable. In 1932 the corresponding problem for groups was shown to be solvable by Magnus [1]. However, in 1966 Matiyasevich [2] presented a semigroup with three defining relations for which the word problem is unsolvable. Here we show the solvability of the word problem for semigroups with one defining relation if that relation is of the form $A \sim BtC$ where (1) the generator $t$ does not occur in $A$, $B$ or $C$, and (2) the length of $A$ is greater than the max(length $B$, length $C$). The basic idea of the proof is to show that the lengths of words equivalent to a given word are bounded, and hence each set of equivalent words is finite. It will also be shown that condition (2) is necessary to insure that each set of equivalent words be finite.

We will be considering semigroup presentations rather than semigroups themselves. In order to define precisely what is meant by a semigroup presentation for the purposes of this paper we fix an enumerable sequence of symbols

(*) $a_0, a_1, a_2, \ldots$

We write $t$ for $a_0$ and sometimes write $a$ for $a_1$. A presentation $S$ is obtained by specifying an initial segment of (*) as the generators of $S$, and one defining relation $A \sim BtC$ where $A$, $B$ and $C$ are words on the generators of $S$ other than $t$ and all the generators of $S$ except $t$ occur in $A$, $B$ and/or $C$. If $W$ is a word on the generators of $S$, then we write $W \in S$. If $W$, $V \in S$ and $W$ and $V$ are equivalent under the defining relation of $S$ then we write $W \sim_s V$, or $W \sim V$ if there can be no con-

Received by the editors October 10, 1969.

AMS 1970 subject classifications. Primary 02F47, 20M05; Secondary 02F05.

Key words and phrases. Semigroup, one defining relation, generator, word problem, solvable.

1 This work was done under Air Force Grant AFOSR 68–1482.

645
The word problem for a semigroup which has presentation $S$ is solvable if there exists an algorithm which can determine of any pair of words $W$, $V \in S$ whether or not $W \sim_s V$.

Capital italic letters, except $S$, will be used as variables for words and those early in the alphabet for words in which $t$ does not occur. If words $W$ and $V$ are identical, symbol by symbol, we write $W \equiv V$. If $W$ is a word let $\lambda W$ be the length of $W$, let $\tau W$ be the number of occurrences of $t$ in $W$, and let $\alpha W = \lambda W - \tau W$, the number of occurrences of $a_i$'s ($i \geq 1$) in $W$. If $W$ is a word of the form $A_1A_2 \cdots A_\beta A_{\beta+1}$, where $\tau A_i = 0$ for all $i$ and any $A_i$ may be empty, we call the $A_i$ the factors of $W$. If $W \equiv UAV$ and $W' \equiv UBtCV$, we say: (1) $A \rightarrow BtC$ is applicable to $W$ ($BtC \rightarrow A$ is applicable to $W'$), and (2) that $W'$ is obtained from $W$ by the Type I operation ($W$ is obtained from $W'$ by the Type II operation); and further, we sometimes write $W_{\tau_1} \rightarrow W'_{\tau_2}$ ($W_{\tau_1}^1 \rightarrow W'_{\tau_2}^1$). If $W_{\tau_1} \rightarrow W_1$, $W_1 \rightarrow W_2$, $\cdots$, $W_{\tau_n} \rightarrow W'_n$, we also write $W_{\tau_1} \rightarrow \cdots \rightarrow W'_n$ ($W_{\tau_1}^1 \rightarrow \cdots \rightarrow W'_n^1$). $S$ is to refer to any semigroup presentation with the defining relation $A \sim BtC$. The letters $k$, $\mu$, $\nu$ will be used to refer to $\lambda A$, $\lambda B$ and $\lambda C$ respectively. Notice that if $W \sim_s V$, then $\alpha V = \alpha W + (\tau V - \tau W)(\mu + \nu - k)$. This relationship will be used often in the proof. If $S$ is a semigroup presentation with $\lambda A = k$, $\lambda B = \mu$, $\lambda C = \nu$, define $S^*$ to be the semigroup presentation with generators $\{t, a\}$ and defining relation $a^* \sim a^*a^*$. We define a mapping, $*$, of words in $S$ into words in $S^*$ by: $a^* = a$, $t^* = t$, and if $W \in S$ is of the form $A_1tA_2 \cdots A_\beta tA_{\beta+1}$, then $W^* = U^*a_1^* = U^*a$ and $W''^* = V^*t^* = V^*t$.

Lemma 1. If $W \sim_S V$, then $W^* \sim_{S^*} V^*$.

Proof. This is quite clear from the definition of $S^*$. If $BtC \rightarrow A$ is applicable to $W$ in $S$, then $B^*tC^* \rightarrow A^*$ (i.e. $a^*a^*t^* \rightarrow a^*$) is applicable to $W^*$ in $S^*$. Similarly for $A \rightarrow BtC$ applicable to $W$ in $S$.

If $W \in S$ is of the form $A_1tA_2 \cdots A_\beta tA_{\beta+1}$ where $\tau A_i = 0$, $1 \leq i \leq \beta + 1$, $\lambda A_1 \geq \min(k, \mu)$, $\lambda A_{\beta+1} \geq \min(k, \nu)$ and $\lambda A_i \geq \min(k, \mu, \nu)$ for $1 < i < \beta$, then we say $W$ is a live word (in $S$) and that the $t$'s occurring in $W$ are live occurrences of $t$. If $T \in S$ is a word of one of the following forms

1. $A_1tA_2 \cdots A_\beta tA_{\beta+1}$,
2. $tA_2 \cdots A_\beta tA_{\beta+1}$,
3. $A_1tA_2 \cdots A_\beta t$,
4. $tA_2 \cdots A_\beta t$,

where, in all cases, $\lambda A_i < \min(k, \mu)$, $A_{\beta+1} < \min(k, \nu)$ and $\lambda A_i < \min(k, \mu, \nu)$ for $1 < i < \beta$, then we say that $T$ is a dead word (in $S$) and all occurrences of $t$ in $T$ are dead occurrences. $T$ is also dead if it is
of the form $A_1$ where $\tau A_1 = 0$ and $\lambda A_1 < \kappa$. If $W$ is a word such that $\tau W > 0$ then we may write it uniquely in the form $W_1 T_1 W_2 \cdots W_i T_i W_{i+1}$ where all $W_i$ are live except possibly $W_1$ and $W_{i+1}$ which are either live or empty and all $T_i$ are dead and of form (4) above with the following possible exceptions:

1. if $W_1$ is empty then $T_1$ is either of form 3 or 4,
2. if $W_{i+1}$ is empty then $T_i$ is either of form 2 or 4,
3. if $W$ is itself dead, then $\delta = 1$, $W_1$ and $W_{i+1}$ are empty and $T_1$ (i.e. $W$) may be any of the four forms or $A_1$ for $\tau A_1 = 0$ and $\lambda A_1 < \kappa$.

When $W$ is written in the form just described we say that $W$ is written in the L-D form. For any $W \in S$ let $L_t W$ indicate the number of live occurrences of $t$ in $W$ and $D_t W$ the number of dead occurrences of $t$ in $W$.

**Lemma 2.** A. If $T \in S$ is dead and $T' \sim T$, then $T' \equiv T$.
B. If $V \sim W$ then $D_t W = D_t V$.
C. If $V \sim W$ and $W = W_1 T_1 W_2 \cdots W_i T_i W_{i+1}$ is in the L-D form, then the L-D form of $V$ is $V_1 T_1 V_2 \cdots V_i T_i V_{i+1}$ where for all $i$, $W_i \sim V_i$.

**Proof.** A. If $T$ is dead then all factors have length less than $\kappa$ so the Type I operation is not applicable to $T$. Further, no $t$ occurs in $T$ with a factor of length greater than or equal to $\nu$ on the right and a factor of length greater or equal to $\mu$ on the left, so the Type II operation is not applicable to $T$.

B. Let $W = UA U'$ and $V = UB t C U'$. The $t$ occurring in $V$ between $B$ and $C$ is live because $\lambda B = \mu$ and $\lambda C = \nu$ and so it is separated from any $t$’s occurring in $U$ or $U'$ by factors of length greater than or equal to the min$(\kappa, \mu, \nu)$. Further, in $W$ the rightmost $t$ in $U$ is separated from the leftmost $t$ of $U'$ by a factor of at least length $\kappa$. So, any $t$ occurring in $U$ or in $U'$ is either dead in both $W$ and in $V$, or live in both. Hence $D_t W = D_t V$. The proof for derivations of more than one step follows by induction.

C. Follows from parts A and B.

**Lemma 3.** If $V$ is live in $S^*$ then

$$a \stackrel{\alpha V}{\Rightarrow} \tau V(\mu + \nu + \kappa),$$

**Proof.** By hypothesis, $V = a^{e_1 a} \cdots a^{e_\beta} a^{e_{\beta+1}}$, where $e_1 \geq \min(\kappa, \mu)$, $e_{\beta+1} \geq \min(\kappa, \nu)$ and $e_i \geq \min(\kappa, \mu, \nu)$ for $1 < i \leq \beta$. Let

$$\delta = \alpha V - \tau V(\mu + \nu - \kappa),$$

and notice that $\tau V = \beta$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Case A. If $\mu \leq \nu$, examine $V$ from left to right to find the derivation

$$a^n \to U_1, \quad U_1 \to U_2, \ldots, \quad U_{\beta-1} \to U_\beta \equiv V.$$  

Since $e_1 \geq \mu$, $e_1 - \mu \geq 0$. Let $\gamma_1 = e_1 - \mu$ and consider $a^\delta$ as $a^n a^\delta a^\gamma a^{\gamma-\mu}$.

Then we have

$$U_1 \equiv a^n a^\delta a^{\gamma-\mu} a^{\gamma+\nu} \equiv a^n a^\delta.$$  

Continuing inductively, since $e_{\beta-1} \geq \min(\kappa, \mu, \nu)$, $e_{\beta-1} - \mu \geq 0$, so for $\gamma_{\beta-1} = e_{\beta-1} - \mu$, we have

$$U_{\beta-1} \equiv a^n a^\delta a^{\gamma_{\beta-1}+\nu}.$$  

Then $U_{\beta-1} = a^n a^\delta a^{\gamma_{\beta-1}+\nu} = a^n a^\delta a^{\gamma_{\beta-1}+\nu+\kappa} + (\delta-1)(\nu-k)$.

Case B. If $\nu < \mu$, start from the right end of $V$ and find the derivation in the analogous way.

If $V$ is live in $S^*$, then $a^n a^{\gamma-\nu+\delta} a^{\mu-\kappa}$ is the ancestor of $V$ and we write $aV$. If $V$ is in the L-D form so that $V = V_1 T_1 V_2 \cdots V_s T_s V_{s+1}$, then the ancestor of $V$ is $aV_1 T_1 aV_2 \cdots aV_s T_s aV_{s+1}$, which we also denote by $aV$.

Lemma 4. Let $W$ and $V$ be live words in $S^*$. $W \sim_s V$ if and only if $aW = aV$.

Proof. If $aW = aV$, then the lemma is obviously true. So, suppose that $W$ and $V$ are live in $S^*$ and that $W \sim_s V$. Since they are live, $W = a^n a^{t_1} a^{t_2} \cdots a^{t_s} a^{t_{s+1}}$ and $V = a^n a^{t_1} a^{t_2} \cdots a^{t_s} a^{t_{s+1}}$. Of course, $aW = \sum_{i=1}^{s} a_i$ and $aV = \sum_{i=1}^{s} a_i$. Let $\tau W = \beta$ and $\tau V = \beta'$. By Lemma 3, $aW = a^{\delta'}$ for $\delta = aW - \tau W (\mu+\nu-k)$, and $aV = a^{\delta'}$ for $\delta' = aV - \tau V (\mu+\nu-k)$. We will show that $\delta = \delta'$. $W \sim V$ implies that $\alpha V = aW + (\tau V - \tau W) (\mu+\nu-k)$.

Substituting for $\alpha V$ in $\delta'$,

$$\delta' = aW + (\tau V - \tau W)(\mu+\nu-k) - \tau V (\mu+\nu-k)$$

$$= aW - \tau W (\mu+\nu-k) = \delta.$$
Lemma 5. Let \( W = W_1T_1W_2 \cdots W_kT_kW_{k+1} \) and \( V = V_1T_1'V_2 \cdots V_kT_k'V_{k+1} \) be in L-D form in \( S^* \). \( W \sim_{s^*} V \) if and only if \( \delta = \delta', T_i = T_i' \) and \( e_i = e_i' \) for \( 1 \leq i \leq \delta + 1 = \delta' + 1 \), i.e. \( eW = eV \).

Proof. If \( eW = eV \), then the lemma is obviously true by Lemmas 3 and 4. If \( W \sim_{s^*} V \), then by Lemma 2, \( \delta = \delta', T_i = T_i' \) and \( W_i \sim_{s^*} V_i \) for \( 1 \leq i \leq \delta + 1 = \delta' + 1 \). Then by Lemma 3, \( eW_i = eV_i \) for \( 1 \leq i \leq \delta + 1 = \delta' + 1 \).

Theorem 1. For all \( \kappa, \mu, v \geq 0 \) the word problem for a semigroup presented by generators \( \{ t, a \} \) and defining relation \( a^* \sim a^nta^* \) is solvable.

Proof. Follows from Lemma 5.

Suppose \( A \rightarrow BtC \) (in \( S \)) is applicable to a word \( W \). If \( W \rightarrow W_1, W_1 \rightarrow W_2, \ldots, W_{n-1} \rightarrow W_n \), each by one application of the Type I operation, we say that \( W \rightarrow W_n \) by \( n \) consecutive applications of the Type I operation (of \( S \)) to \( W \). Define \( \xi_sW \) to be the maximum possible number of consecutive applications of the Type I operation (in \( S \)) to \( W \).

Lemma 6. If \( W \in S^* \), then \( \xi_sW \) is finite if and only if \( \kappa > \max(\mu, v) \).

Proof. Suppose that \( W = a^{\rho_1+\mu+v} \) and suppose that \( U \) is obtained from \( W \) by an application of the Type I operation. Then \( U = a^{\rho_1+\mu+v} \). If \( \kappa \leq \max(\mu, v) \), even if \( \rho_1 = \rho_2 = 0 \), the Type I operation is applicable to \( U \) and also to the result obtained from \( U \) by an application of the Type I operation, etc. On the other hand, if \( \kappa > \max(\mu, v) \), \( \rho_1 + \mu, \rho_2 + \mu < \rho_1 + \kappa + \rho_2 \). As the Type I operation is applied repeatedly, the lengths of the factors of the resulting words decrease and eventually are less than \( \kappa \); at that point the Type I operation is no longer applicable.

Lemma 7. If \( \kappa > \max(\mu, v) \) and \( W \sim_{s^*} V \), then both \( \lambda W \) and \( \lambda V \) are less than or equal to \( \alpha eW + (2\xi_sW - \tau eW)(\mu + v - \kappa) \).

Proof. By Lemma 5, \( W \sim_{s^*} V \), then \( eW = eV \). Since \( \kappa > \max(\mu, v) \), by Lemma 6 \( \xi_sW \) is finite, and, of course, \( \tau V, \tau W \leq \xi_sW \). \( \lambda W = eW + \tau W \) and \( \lambda W = eW + (\tau W - eW)(\mu + v - \kappa) \). Substituting for \( eW \) and \( \tau W \),

\[
\lambda W \leq \alpha eW + (\xi_sW - \tau eW)(\mu + v - \kappa) + \xi_sW eW.
\]

Since \( eW = eV \), it is easy to see that \( \lambda V \) is bounded in a similar fashion.

Lemma 8. If \( \kappa > \max(\mu, v) \) and \( W \sim_{s^*} V \), then both \( \lambda W \) and \( \lambda V \) are less than or equal to \( \alpha eW^* + (2\xi_sW^* - \tau eW^*)(\mu + v - \kappa) \).
Proof. \( W \sim_s V \), then by Lemma 1, \( W^* \sim_s V^* \). \( \lambda W = \lambda W^* \) and \( \lambda V = \lambda V^* \), and so the lemma follows from Lemma 7.

Theorem 2. For all \( k, \mu, \nu \geq 0 \), the cardinality of each set of words equivalent in \( S \) is finite if and only if \( k > \max(\mu, \nu) \).

Proof. Suppose \( k \leq \max(\mu, \nu) \). By Lemma 6, for any semigroup presentation \( S^* \) on generators \( \{ t, a \} \) with the defining relation \( a^r \sim a^t a^s \), there are words \( W \) (e.g. \( a^s \)) such that \( \xi_s \) is not finite. Thus the number of words \( V, W \rightarrow_s V \) is not finite. On the other hand, if \( k > \max(\mu, \nu) \), for any semigroup presentation, \( S \), with defining relation \( A \sim B t C \) where \( \lambda A = k, \lambda B = \mu \) and \( \lambda C = \nu \), there is a bound on the lengths of words in an equivalence class and hence the cardinality of that set is finite.

Theorem 3. If \( k > \max(\mu, \nu) \), then the word problem for \( S \) is solvable.

Proof. Follows from Theorem 2.

References