THE SOLVABILITY OF THE WORD PROBLEM FOR CERTAIN SEMIGROUPS[1]

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

$$(*) \qquad a_0, a_1, a_2, \cdots.$$

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.

fusion. 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 λW be the length of W, let τW 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 ($i \geqq 1$) in W. If W is a word of the form $A_1 t A_2 t \cdots A_\beta t A_{\beta+1}$, 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) $A \to BtC$ is applicable to W ($BtC \to A$ 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 $W \xrightarrow{\text{I}} W'$ ($W' \xrightarrow{\text{II}} W$). If $W \xrightarrow{\text{I}} W_1$, $W_1 \xrightarrow{\text{I}} W_2$, $\cdots$, $W_n \xrightarrow{\text{I}} W'$, we also write $W \xrightarrow{\text{I}} W'$ (or $W' \xrightarrow{\text{II}} W$). S is to refer to any semigroup presentation with the defining relation $A \sim BtC$. The letters κ, μ, ν will be used to refer to λA, λB and λC respectively. Notice that if $W \sim_S V$, then $\alpha V = \alpha W + (\tau V - \tau W)(\mu + \nu - \kappa)$. This relationship will be used often in the proof. If S is a semigroup presentation with $\lambda A = \kappa$, $\lambda B = \mu$, $\lambda C = \nu$, define S^* to be the semigroup presentation with generators $\{t, a\}$ and defining relation $a^\kappa \sim a^\mu t a^\nu$. We define a mapping, *, of words in S into words in S^* by: $a_i^* = a$, $t^* = t$, and if W and $W' \in S$ where $W \equiv Ua_i$ and $W' \equiv Vt$, then $W^* = U^* a_i^* \equiv U^* a$ and $W'^* = V^* t^* \equiv V^* t$.

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

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

If $W \in S$ is of the form $A_1 t A_2 t \cdots A_\beta t A_{\beta+1}$ where $\tau A_i = 0$, $1 \leqq i \leqq \beta+1$, $\lambda A_1 \geqq \min(\kappa, \mu)$, $\lambda A_{\beta+1} \geqq \min(\kappa, \nu)$ and $\lambda A_i \geqq \min(\kappa, \mu, \nu)$ for $1 < i \leqq \beta$, 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) $A_1 t A_2 \cdots A_\beta t A_{\beta+1}$,
(2) $t A_2 \cdots A_\beta t A_{\beta+1}$,
(3) $A_1 t A_2 \cdots A_\beta t$,
(4) $t A_2 \cdots A_\beta t$,

where, in all cases, $\lambda A_1 < \min(\kappa, \mu)$, $A_{\beta+1} < \min(\kappa, \nu)$ and $\lambda A_i < \min(\kappa, \mu, \nu)$ for $1 < i \leqq \beta$, 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 $W_1 T_1 W_2 \cdots W_\delta T_\delta W_{\delta+1}$ where all W_i are live except possibly W_1 and $W_{\delta+1}$ 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 $W_{\delta+1}$ is empty then T_δ is either of form 2 or 4,

(3) if W is itself dead, then $\delta = 1$, W_1 and $W_{\delta+1}$ 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 $L\tau W$ indicate the number of live occurrences of t in W and $D\tau W$ 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 $D\tau W = D\tau V$.*

C. *If $V \sim W$ and $W \equiv W_1 T_1 W_2 \cdots W_\delta T_\delta W_{\delta+1}$ is in the L-D form, then the L-D form of V is $V_1 T_1 V_2 \cdots V_\delta T_\delta V_{\delta+1}$ where for all i, $W_i \sim V_i$.*

PROOF. A. If T is dead then all factors have length less than κ 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 ν on the right and a factor of length greater or equal to μ on the left, so the Type II operation is not applicable to T.

B. Let $W \equiv UAU'$ and $V \equiv UBtCU'$. 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 κ. So, any t occurring in U or in U' is either dead in both W and in V, or live in both. Hence $D\tau W = D\tau V$. 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*

$$a^{\alpha V - \tau V(\mu+\nu+\kappa)} \xrightarrow{\mathrm{I}} V.$$

PROOF. By hypothesis, $V \equiv a^{\epsilon_1} t a^{\epsilon_2} \cdots a^{\epsilon_\beta} t a^{\epsilon_{\beta+1}}$, where $\epsilon_1 \geqq \min(\kappa, \mu)$, $\epsilon_{\beta+1} \geqq \min(\kappa, \nu)$ and $\epsilon_i \geqq \min(\kappa, \mu, \nu)$ for $1 < i \leqq \beta$. Let

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

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

Case A. If $\mu \leqq \nu$, examine V from left to right to find the derivation

$$a^{\delta} \overset{\mathrm{I}}{\longrightarrow} U_1, U_1 \overset{\mathrm{I}}{\longrightarrow} U_2, \cdots, U_{\beta-1} \overset{\mathrm{I}}{\longrightarrow} U_{\beta} \equiv V.$$

Since $\epsilon_1 \geqq \mu$, $\epsilon_1 - \mu \geqq 0$. Let $\gamma_1 = \epsilon_1 - \mu$ and consider a^{δ} as $a^{\gamma_1} a^{\kappa} a^{\delta-\gamma_1-\kappa}$. Then we let

$$U_1 \equiv a^{\gamma_1} a^{\mu} t a^{\nu} a^{\delta-\gamma_1-\kappa} \equiv a^{\epsilon_1} t a^{\delta-\gamma_1-\kappa+\nu}.$$

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

$$U_{\beta-1} \equiv a^{\epsilon_1} t a^{\epsilon_2} \cdots t a^{\epsilon_{\beta-1}} t a^{\delta-(\gamma_1+\cdots+\gamma_{\beta-1})+(\beta-1)(\nu-\kappa)}.$$

Then $U_{\beta} \equiv a^{\epsilon_1} t a^{\epsilon_2} \cdots t a^{\epsilon_{\beta-1}} t a^{\epsilon_{\beta}} t a^{\delta-(\gamma_1+\cdots+\gamma_{\beta})+\beta(\nu-\kappa)}$ for $\gamma_{\beta} = \epsilon_{\beta} - \mu$. If $\epsilon_{\beta+1} = \delta - \sum_{i=1}^{\beta} \gamma_i + \beta(\nu - \kappa)$, the lemma is proved. By definition, $\epsilon_{\beta+1} = \alpha V - \sum_{i=1}^{\beta} \epsilon_i$, and by the definition of δ, $\alpha V = \delta + \beta(\mu + \nu - \kappa)$, so

$$\begin{aligned} \epsilon_{\beta+1} &= \delta + \beta(\mu + \nu - \kappa) - \sum_{i=1}^{\beta} \epsilon_i \\ &= \delta + \beta(\nu - \kappa) - \sum_{i=1}^{\beta} (\epsilon_i - \mu) \\ &= \delta + \beta(\nu - \kappa) - \sum_{i=1}^{\beta} \gamma_i. \end{aligned}$$

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 $a^{\alpha V - \tau V(\mu+\nu-\kappa)}$ is the ancestor of V and we write $\mathfrak{A}V$. If V is in the L-D form so that $V \equiv V_1 T_1 V_2 \cdots V_{\delta} T_{\delta} V_{\delta+1}$, then the ancestor of V is $\mathfrak{A}V_1 T_1 \mathfrak{A}V_2 \cdots \mathfrak{A}V_{\delta} T_{\delta} \mathfrak{A}V_{\delta+1}$, which we also denote by $\mathfrak{A}V$.

LEMMA 4. *Let W and V be live words in S^*. $W \sim_{S^*} V$ if and only if $\mathfrak{A}W \equiv \mathfrak{A}V$.*

PROOF. If $\mathfrak{A}W \equiv \mathfrak{A}V$, 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, $W \equiv a^{\epsilon_1} t a^{\epsilon_2} \cdots a^{\epsilon_{\beta}} t a^{\epsilon_{\beta+1}}$ and $V \equiv a^{\epsilon'_1} t a^{\epsilon'_2} \cdots a^{\epsilon'_{\beta'}} t a^{\epsilon'_{\beta'+1}}$. Of course, $\alpha W = \sum_{i=1}^{\beta} \epsilon_i$, $\alpha V = \sum_{i=1}^{\beta'} \epsilon'_i$, $\tau W = \beta$, and $\tau V = \beta'$. By Lemma 3, $\mathfrak{A}W = a^{\delta}$ for $\delta = \alpha W - \tau W(\mu + \nu - \kappa)$, and $\mathfrak{A}V = a^{\delta'}$ for $\delta' = \alpha V - \tau V(\mu + \nu - \kappa)$. We will show that $\delta = \delta'$. $W \sim V$ implies that $\alpha V = \alpha W + (\tau V - \tau W)(\mu + \nu - \kappa)$. Substituting for αV in δ',

$$\begin{aligned} \delta' &= \alpha W + (\tau V - \tau W)(\mu + \nu - \kappa) - \tau V(\mu + \nu - \kappa) \\ &= \alpha W - \tau W(\mu + \nu - \kappa) = \delta. \end{aligned}$$

LEMMA 5. *Let* $W \equiv W_1T_1W_2 \cdots W_\delta T_\delta W_{\delta+1}$ *and* $V \equiv V_1T_1'V_2 \cdots V_{\delta'}T_{\delta'}'V_{\delta'+1}$ *be in L-D form in* S^*. $W \sim_{S^*} V$ *if and only if* $\delta = \delta'$, $T_i \equiv T_i'$ and $\mathfrak{A}V_i \equiv \mathfrak{A}W_i$ *for* $1 \leqq i \leqq \delta+1 = \delta'+1$, *i.e.* $\mathfrak{A}W \equiv \mathfrak{A}V$.

PROOF. If $\mathfrak{A}W \equiv \mathfrak{A}V$, then the lemma is obviously true by Lemmas 3 and 4. If $W \sim_{S^*} V$, then by Lemma 2, $\delta = \delta'$, $T_i \equiv T_i'$ and $W_i \sim_{S^*} V_i$ for $1 \leqq i \leqq \delta+1 = \delta'+1$. Then by Lemma 3, $\mathfrak{A}W_i \equiv \mathfrak{A}V_i$ for $1 \leqq i \leqq \delta+1 = \delta'+1$.

THEOREM 1. *For all* $\kappa, \mu, \nu \geqq 0$ *the word problem for a semigroup presented by generators* $\{t, a\}$ *and defining relation* $a^\kappa \sim a^\mu t a^\nu$ *is solvable.*

PROOF. Follows from Lemma 5.

Suppose $A \to BtC$ (in S) is applicable to a word W. If $W \xrightarrow{\mathrm{I}} W_1$, $W_1 \xrightarrow{\mathrm{I}} W_2, \cdots, W_{n-1} \xrightarrow{\mathrm{I}} W_n$, each by one application of the Type I operation, we say that $W \xrightarrow{\mathrm{I}} W_n$ by n consecutive applications of the Type I operation (of S) to W. Define $\zeta_S W$ 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* $\zeta_{S^*} W$ *is finite if and only if* $\kappa > \max(\mu, \nu)$.

PROOF. Suppose that $W \equiv a^{\rho_1+\kappa+\rho_2}$ and suppose that U is obtained from W by an application of the Type I operation. Then $U \equiv a^{\rho_1+\mu}ta^{\rho_2+\nu}$. If $\kappa \leqq \max(\mu, \nu)$, 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 $\kappa > \max(\mu, \nu)$, $\rho_1+\mu$, $\rho_2+\mu < \rho_1+\kappa+\rho_2$. As the Type I operation is applied repeatedly, the lengths of the factors of the resulting words decrease and eventually are less than κ; at that point the Type I operation is no longer applicable.

LEMMA 7. *If* $\kappa > \max(\mu, \nu)$ *and* $W \sim_{S^*} V$, *then both* λW *and* λV *are less than or equal to* $\alpha\mathfrak{A}W + (2\zeta_{S^*}W - \tau\mathfrak{A}W)(\mu+\nu-\kappa)$.

PROOF. By Lemma 5, $W \sim_{S^*} V$, then $\mathfrak{A}W \equiv \mathfrak{A}V$. Since $\kappa > \max(\mu, \nu)$, by Lemma 6 $\zeta_{S^*}\mathfrak{A}W$ is finite, and, of course, τV, $\tau W \leqq \zeta_{S^*}\mathfrak{A}W$. $\lambda W = \alpha W + \tau W$ and $\alpha W = \alpha\mathfrak{A}W + (\tau W - \tau\mathfrak{A}W)(\mu+\nu-\kappa)$. Substituting for αW and τW,

$$\lambda W \leqq \alpha\mathfrak{A}W + (\zeta_{S^*}\mathfrak{A}W - \tau\mathfrak{A}W)(\mu + \nu - \kappa) + \zeta_{S^*}\mathfrak{A}W.$$

Since $\mathfrak{A}W \equiv \mathfrak{A}V$, it is easy to see that λV is bounded in a similar fashion.

LEMMA 8. *If* $\kappa > \max(\mu, \nu)$ *and* $W \sim_S V$, *then both* λW *and* λV *are less than or equal to* $\alpha\mathfrak{A}W^* + (2\zeta_{S^*}\mathfrak{A}W^* - \tau\mathfrak{A}W^*)(\mu+\nu-\kappa)$.

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* $\kappa, \mu, \nu \geqq 0$, *the cardinality of each set of words equivalent in* S *is finite if and only if* $\kappa > \max(\mu, \nu)$.

PROOF. Suppose $\kappa \leqq \max(\mu, \nu)$. By Lemma 6, for any semigroup presentation S^* on generators $\{t, a\}$ with the defining relation $a^\kappa \sim a^\mu t a^\nu$, there are words W (e.g. a^κ) such that $\zeta_{S^*} W$ is not finite. Thus the number of words V, $W \to_{S^*} V$ is not finite. On the other hand, if $\kappa > \max(\mu, \nu)$, for any semigroup presentation, S, with defining relation $A \sim BtC$ where $\lambda A = \kappa$, $\lambda B = \mu$ 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* $\kappa > \max(\mu, \nu)$, *then the word problem for* S *is solvable.*

PROOF. Follows from Theorem 2.

REFERENCES

1. W. Magnus, A. Karrass and D. Solitar, *Combinatorial group theory: Presentations of groups in terms of generators and relations*, Pure and Appl. Math., vol. 13, Interscience, New York, 1966. MR **34** #7617.

2. Ju. V. Matijasevič, *Simple examples of undecidable associative calculi*, Dokl. Akad. Nauk SSSR **173** (1967), 1264–1266 = Soviet Math. Dokl. **8** (1967), 555–557.

NEW YORK UNIVERSITY AT UNIVERSITY HEIGHTS, BRONX, NEW YORK 10453