



---

The Word Problem for Cancellation Semigroups with Zero

Author(s): Yuri Gurevich and Harry R. Lewis

Source: *The Journal of Symbolic Logic*, Vol. 49, No. 1 (Mar., 1984), pp. 184-191

Published by: [Association for Symbolic Logic](#)

Stable URL: <http://www.jstor.org/stable/2274101>

Accessed: 05/02/2011 22:59

---

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=asl>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact [support@jstor.org](mailto:support@jstor.org).



*Association for Symbolic Logic* is collaborating with JSTOR to digitize, preserve and extend access to *The Journal of Symbolic Logic*.

<http://www.jstor.org>

## THE WORD PROBLEM FOR CANCELLATION SEMIGROUPS WITH ZERO

YURI GUREVICH AND HARRY R. LEWIS<sup>1</sup>

By the *word problem* for some class of algebraic structures we mean the problem of determining, given a finite set  $E$  of equations between words (i.e. terms) and an additional equation  $x = y$ , whether  $x = y$  must hold in all structures satisfying each member of  $E$ . In 1947 Post [P] showed the word problem for semigroups to be undecidable. This result was strengthened in 1950 by Turing, who showed the word problem to be undecidable for *cancellation semigroups*, i.e. semigroups satisfying the *cancellation property*

(1) If  $xy = xy'$  or  $yx = y'x$ , then  $y = y'$ .

Novikov [N] eventually showed the word problem for groups to be undecidable.

(Many flaws in Turing's proof were corrected by Boone [B]. Even after his corrections, at least one problem remains; the sentence on line 16 of p. 502 of [T] does not follow if one relation is principal and the other is a commutation relation. A corrected and somewhat simplified version of Turing's proof can be built on the construction given here.)

In 1966 Gurevich [G] showed the word problem to be undecidable for *finite* semigroups. However, this result on finite structures has not been extended to cancellation semigroups or groups;<sup>2</sup> indeed it is easy to see that a finite cancellation semigroup is a group, so both questions are the same. We do not here settle the word problem for finite groups, but we do show that the word problem is undecidable for finite semigroups with zero (that is, having an element  $0$  such that  $x0 = 0x = 0$  for all  $x$ ) satisfying an approximation to the cancellation property (1). Naturally, no nontrivial semigroup with zero can satisfy (1); instead, for a semigroup with zero which also has an identity, let the cancellation property be

(2) If  $xy = xy' \neq 0$  or  $yx = y'x \neq 0$ , then  $y = y'$ .

That is, any equation can be cancelled provided it is not an equation  $0 = 0$ . For a semigroup with zero but without identity, define the cancellation property to be the conjunction of (2) and

(3) If  $xy = x$  or  $yx = x$ , then  $x = 0$ .

---

Received March 12, 1982; revised May 25, 1982.

<sup>1</sup> Research supported by NSF Grant MCS80-05386.

<sup>2</sup> *Added in Proof.* Recently Slobodskoi [S] showed the word problem for finite groups to be decidable.

That is, if division by  $x$  'should' equate some semigroup element with a nonexistent identity, then  $x$  must be 0. Whether or not a semigroup with zero has an identity, we refer to it as a *cancellation semigroup with zero* if it satisfies the appropriate cancellation property.

It is a consequence of our main theorem that the word problem is undecidable for finite cancellation semigroups with zero; this holds for semigroups with identity, and also for semigroups without identity. However we find it technically easier to establish a stronger result: that the set of implications  $E \Rightarrow x = y$  holding in all semigroups is effectively inseparable from the set of such implications that fail in some finite cancellation semigroup with zero. Recall [R] that two sets  $A$  and  $B$  are *recursively inseparable* if there is no recursive set containing  $A$  and disjoint from  $B$ . Effective inseparability is stronger:  $A$  and  $B$  are *effectively inseparable* if there is a partial recursive function  $f$  of two variables such that if  $p$  and  $q$  are indices of disjoint r.e. sets  $W_p$  and  $W_q$  containing  $A$  and  $B$ , respectively, then  $f(p, q)$  is outside both  $W_p$  and  $W_q$  and hence bears witness to the fact that  $W_p$  and  $W_q$  do not form a complementary recursive pair separating  $A$  and  $B$ . Clearly the recursive or effective inseparability of  $A$  and  $B$  suffices for the nonrecursiveness of both  $A$  and  $B$ .

With the basic terminology defined we can state the main result.

**THEOREM.** *Let  $\Delta$  range over alphabets containing the symbols 0 and  $A_0$ , and let  $x_i$  and  $y_i$  range over words in  $\Delta^*$ . Let  $\phi$  range over formulas of the form  $x_1 = y_1 \wedge \cdots \wedge x_n = y_n \Rightarrow A_0 = 0$  such that for each  $A \in \Delta$  the equations  $A0 = 0$  and  $0A = 0$  appear among the antecedents. Then the following two sets are effectively inseparable:*

- $\{\phi: \phi \text{ holds in every } \Delta\text{-generated semigroup}\},$
- $\{\phi: \phi \text{ fails in some finite } \Delta\text{-generated cancellation semigroup with zero and without identity}\}.$

(As mentioned earlier, a similar result can be obtained for semigroups with identity. Indeed, adjoining an identity element to a semigroup with zero preserves the cancellation property.)

We have presented this work from the standpoint of its interest as an attack on the word problem for finite groups. Historically, however, it was motivated by an application in computer science: a decision problem in the theory of relational database dependencies [GL]. In addition, the present paper provides an independent proof, in a slightly stronger form, of the main result of [G], the undecidability of the word problem for finite semigroups. (The paper [G] contains a number of other results on decision problems in algebraic structures not directly related to the work presented here.) Our construction is fundamentally a combination and simplification of those in [G] and in [T].

The overall method of proof is to reduce a halting problem for Turing machines to the word problem in question. We adopt a specialized version of the Turing machine model similar to that used by Turing in [T]. Formally a *Turing machine* is an automaton consisting of a finite set  $Q$  of states, including the initial state  $q_0$ , a tape alphabet  $T$  containing the blank symbol  $a_0$ , and a partial transition function  $\delta$  giving the action of the machine for certain state-symbol combinations. The single tape should be viewed as unlimited in extent both to the left and to the right and with all but a finite number of the tape cells blank at any time during the machine's

computation. Following [T], we make the somewhat peculiar assumption that the tape head occupies a position *between* tape squares, and that, depending on the state, the head is looking to its left or to its right. That is,  $Q$  is the union of two disjoint sets—the set of ‘left-looking’ states and the set of ‘right-looking’ states. We assume that  $q_0$ , the initial state, is left-looking. The transition function  $\delta$  then takes certain elements of  $Q \times T$  to  $Q \times T \times \{0, 1\}$ , where if  $\delta(q, a) = \langle q', a', e \rangle$ , then

1.  $q'$  is the new state,
2. the scanned symbol  $a$  is rewritten as  $a'$ , and
3. (a) if  $e = 0$ , then the head does not move, and  
(b) if  $e = 1$ , then the head moves across the scanned square (i.e. left one tape square if  $q$  was a left-looking state, and right one square if  $q$  was a right-looking state).

A *halting state* of  $M$  is a state  $h$  such that  $\delta(h, a)$  is undefined for every  $a \in T$ . (As usual  $T^*$  is the set of words over the alphabet  $T$ .) A *configuration* is a member  $\langle x, q, y \rangle$  of  $T^* \times Q \times T^*$  such that  $x$  does not begin with a blank and  $y$  does not end with a blank; its interpretation as a physical arrangement of the tape and the head should be evident.

EXAMPLE. Suppose  $\langle x, q, cy \rangle$  is a configuration, where  $x, y \in T^*$  and  $c \in T$ . Suppose that  $q$  is a right-looking state and  $\delta(q, c) = \langle q', c', e \rangle$ , where  $c'$  is nonblank. If  $e = 0$  then the next configuration is  $\langle x, q', c'y \rangle$ ; if  $e = 1$  then the next configuration is  $\langle xc', q', y \rangle$ . However, if  $c'$  were the blank symbol,  $y$  were  $\lambda$ , and  $e = 0$ , then the next configuration would be  $\langle x, q', \lambda \rangle$ . (We use  $\lambda$  to denote the empty word.)

Every configuration has at most one successor configuration; we write  $C \vdash C'$  to indicate the (functional) relationship of a configuration  $C$  to its successor  $C'$  and write  $\vdash^*$  for the reflexive, transitive closure of  $\vdash$ .

We consider Turing machines with at least two distinguished halting states  $q_1$  and  $q_2$  in addition to their initial state  $q_0$ . The following is established by standard methods (see, for example, the proof of Theorem XII(c) on p. 94 of [R]).

LEMMA 1. *Let  $M_1$  be the class of Turing machines that eventually enter state  $q_1$ , having been started in the initial configuration  $\langle \lambda, q_0, \lambda \rangle$ . Let  $M_2$  be defined similarly for the halting state  $q_2$ . Then  $M_1$  and  $M_2$  are effectively inseparable.*

We prove our result by constructing, for any Turing machine  $M$ , a set  $E$  of equations and an equation  $A_0 = 0$ , such that if  $M \in M_1$  then  $A_0 = 0$  holds in any semigroup satisfying  $E$ , and if  $M \in M_2$  then  $A_0 = 0$  fails in a finite cancellation semigroup  $G'$  with zero and without identity. That such a reduction of a pair of sets to a pair of sets preserves effective inseparability is shown by Smullyan [Sm, p. 98].

In general terms, the encoding of  $M$  by  $E$  is achieved as follows. A configuration of  $M$  is represented by a word over the alphabet of  $E$ ; in fact several words may represent the same configuration. The computation by  $M$  is mimicked by the derivation of one word from another using the equations in  $E$ . The words representing configurations contain, among other symbols, the tape symbols of the configuration, in order, and a symbol to indicate the state of  $M$ ; this symbol is located among the tape symbols so as to mark the head position. The equations in  $E$  are intended to be used as derivation rules—the left-hand side of an equation is to be replaced by the corresponding right-hand side; we have to show in due course that replacing the right-hand side of such an equation by the corresponding left-hand

side does not cause problems. The derivation rules are of several kinds. Individual steps in the computation by  $M$  correspond to uses of the *transition rules* in  $E$ . In addition,  $E$  contains *commutation rules*. To explain their purpose, we must first explain that interspersed among the tape and state symbols in a word representing a configuration are *transition symbols*. Two transition symbols are introduced for each step for each simulated step by  $M$ ; their purpose is to ensure that it does no harm to apply a transition rule in reverse. However these transition symbols get in the way of the simulation, and the commutation rules are needed to enable the state symbol to jump across transition symbols. (The state symbol carries an extra bit of information, indicated in a superscript, which restricts the direction in which it can jump over a transition symbol.) The symbol  $\uparrow$  is an endmarker; two occurrences of it delimit the representation of the configuration. A special symbol  $\#$  is introduced outside the endmarkers solely for the purpose of ensuring that the cancellation property is satisfied.

In addition, the symbol  $A_0$  represents the initial configuration of  $M$  and  $0$  represents the zero element. As long as a computation by  $M$  continues without reaching a halting state, the equality of  $A_0$  and the word representing a configuration can be established by using the equations in  $E$ . If  $M$  ultimately reaches state  $q_1$ , then a state symbol corresponding to  $q_1$  eventually appears in the word; but  $q_1$  is specified to be equal to  $0$ , and so the entire word is annihilated. Thus in this case  $A_0$  is shown to equal  $0$  in the semigroup. On the other hand, if  $M$  ultimately reaches state  $q_2$ , then only finitely many different words can be derived from  $A_0$  in this way, and these words and their subwords form a finite model for the equations, a model in which  $A_0 = 0$  does not hold.

Let us fix some machine  $M$  and let it have state set  $Q = \{q_0, \dots, q_r\}$  (where  $q_0$  is the initial state and  $q_1, q_2$  are halting states), and symbol set  $T = \{a_0, \dots, a_p\}$  (where  $a_0$  is the blank). To recapitulate, the equations are written using the following symbols:

- $a_k$  ( $k = 0, \dots, p$ ; the *tape symbols*),
- $q_i^e$  ( $i = 0, \dots, r$ ;  $e = 0, 1$ ; the *state symbols*),
- $\sigma_m$  (for each pair  $m \in Q \times T$ , and for  $m = 0$ ; the *transition symbols*),
- $\uparrow$  (the *endmarker*),
- $\#$  (a special symbol needed only to ensure the cancellation property),
- $0$  (the *zero symbol*),
- $A_0$  (the *initial symbol*).

Let us call this set of symbols  $\Delta$ . The equations are derived from a semi-Thue system (system of one-way rewriting rules). The rules are as follows:

*Annihilation rules.*

- (1a)  $A0 \rightarrow 0$ , for each  $A \in \Delta$ ,
- (1b)  $0A \rightarrow 0$ , for each  $A \in \Delta$ ,
- (1c)  $q_i^e \rightarrow 0$ , for  $e = 0, 1$ .

*Transition rules.*

- (2.m)  $a_k q_i^e \rightarrow \sigma_m a_h q_j^1 \sigma_m$ , where  $e$  is 0 or 1,  $q_i$  is a left-looking state,  $\delta(q_i, a_k) = \langle q_j, a_h, 0 \rangle$ , and  $m = \langle q_i, a_k \rangle$ .
- (3.m)  $a_k q_i^e \rightarrow \sigma_m q_j^0 a_h \sigma_m$ , where  $e$  is 0 or 1,  $q_i$  is a left-looking state,  $\delta(q_i, a_k) = \langle q_j, a_h, 1 \rangle$ , and  $m = \langle q_i, a_k \rangle$ .

(4.m)  $q_i^e a_k \rightarrow \sigma_m a_h q_i^1 \sigma_m$ , where  $e$  is 0 or 1,  $q_i$  is a right-looking state,  $\delta(q_i, a_k) = \langle q_j, a_h, 1 \rangle$ , and  $m = \langle q_i, a_k \rangle$ .

(5.m)  $q_i^e a_k \rightarrow \sigma_m q_j^0 a_h \sigma_m$ , where  $e$  is 0 or 1,  $q_i$  is a right-looking state,  $\delta(q_i, a_k) = \langle q_j, a_h, 0 \rangle$ , and  $m = \langle q_i, a_k \rangle$ .

*Blank-creating rules.*

(6.i)  $\uparrow q_i^0 \rightarrow \# \uparrow \sigma_0 a_0 q_i^1 \sigma_0$ , where  $q_i$  is a left-looking state.

(7.i)  $q_i^1 \uparrow \rightarrow \sigma_0 q_i^0 a_0 \sigma_0 \uparrow \#$ , where  $q_i$  is a right-looking state.

*Commutation rules.*

(8.m, i)  $\sigma_m q_i^0 \rightarrow q_i^0 \sigma_m$ , for each  $m$ , and each left-looking state  $q_i$ .

(9.m, i)  $q_i^1 \sigma_m \rightarrow \sigma_m q_i^1$ , for each  $m$ , and each right-looking state  $q_i$ .

*Initialization rule.*

(10)  $A_0 \rightarrow \uparrow q_0^0 \uparrow$

Let  $E$  be the set of equations  $u = v$  derived from the rules  $u \rightarrow v$ . Then the Theorem will follow from these two lemmas:

LEMMA 2. *If  $M \in M_1$  then  $A_0 = 0$  holds in  $\Delta^*/E$ .*

LEMMA 3. *If  $M \in M_2$  then there is a finite cancellation semigroup with zero and without identity in which  $E$  holds but the equation  $A_0 = 0$  does not hold.*

Let us begin with some notation. If  $u$  and  $v$  are words in  $\Delta^*$ , then  $u \rightarrow v$  holds only if  $u \rightarrow v$  is one of the rules;  $u \Rightarrow v$  if there is a rule  $x \rightarrow y$  and there are words  $z$  and  $w$  such that  $u = zxw$  and  $v = zyw$ , that is, just in case  $v$  is derived from  $u$  by rewriting some one subword by means of a rule;  $u \Leftarrow v$  if and only if  $v \Rightarrow u$ ;  $u \Leftrightarrow v$  if and only if  $u \Rightarrow v$  or  $u \Leftarrow v$ ; and  $\overset{*}{\Rightarrow}$ ,  $\overset{*}{\Leftarrow}$ , and  $\overset{*}{\Leftrightarrow}$  are the reflexive, transitive closures of  $\Rightarrow$ ,  $\Leftarrow$ , and  $\Leftrightarrow$ , respectively.

PROOF OF LEMMA 2. Let  $H$  be the homomorphism on words in  $\Delta^*$  defined as follows:

$$H(A) = \begin{cases} \lambda & \text{if } A \text{ is a transition symbol, i.e. some } \sigma_m, \\ A & \text{otherwise.} \end{cases}$$

We show the following

*Claim.* For any configuration  $\langle w_1, q_i, w_2 \rangle$  such that  $\langle \lambda, q_0, \lambda \rangle \overset{*}{\Leftarrow} \langle w_1, q_i, w_2 \rangle$ , there are words  $x_1$  and  $x_2$  in  $\Delta^*$  and numbers  $s, t, s'$ , and  $t'$  such that  $H(x_1) = a_0^s w_1$ ,  $H(x_2) = w_2 a_0^{s'}$ , and  $A_0 \overset{*}{\Leftarrow} \#^t \uparrow x_1 q_i^e x_2 \uparrow \#^{t'}$ , a word we refer to as  $\xi$  below; and moreover if  $q_i$  is right-looking then  $e = 1$  and  $x_2$  begins with some  $a_k$ , and if  $q_i$  is left-looking then  $e = 0$  and  $x_1$  ends with some  $a_k$ .

The claim is proved by induction on the number  $c$  of steps required for  $M$  to reach the indicated configuration. If  $c = 0$  then the configuration is  $\langle \lambda, q_0, \lambda \rangle$  and  $\xi$  is  $\# \uparrow \sigma_0 a_0 q_0^1 \sigma_0 \uparrow$ , which is derived from  $A_0$  by one application of the initialization rule (10) and one application of the blank-creating rule (6.0). If  $c > 0$ , then let  $\langle w_1, q_i, w_2 \rangle$  be the configuration reached by  $M$  after  $c - 1$  steps, and let  $\xi$  be the word satisfying the claim at that point. Assume that  $q_i$  is right-looking (the case in which  $q_i$  is left-looking is symmetrical), that  $x_2$  begins with  $a_k$ , and that  $\delta(q_i, a_k) = \langle q_j, a_h, e' \rangle$ . Let  $m = \langle q_i, a_k \rangle$ . Then either rule (4.m) (if  $e' = 1$ ) or rule (5.m) (if  $e' = 0$ ) is applicable to  $\xi$ . Next, some series of applications of the commutation rules may be needed in order to bring the new state symbol contiguous with a tape symbol or one of the occurrences of the endmarker, and, in the latter case, rule (6.j) will have to be applied to introduce a blank symbol next to the endmarker. Note, however, that if

rule (4.m) was applied and  $q_j$  is left-looking, then no commutation rule will be needed (and in fact none will be applicable).

Since  $M$  reaches state  $q_1$  it follows by induction that there is a string  $\xi$  such that  $A_0 \xrightarrow{*} \xi$  and  $q_1^0$  or  $q_1^1$  occurs in  $\xi$ . From rules (1a), (b), (c) it then follows that  $A_0 \xrightarrow{*} 0$ .

We now prove Lemma 3, which follows from a sequence of sublemmas. Suppose that  $M \in M_2$ . Let  $W = \{w: A_0 \xrightarrow{*} w\}$ .

LEMMA 4. *The relations  $\Rightarrow$  and  $\Leftarrow$  are at most single valued on any member of  $W$  not containing an occurrence of 0. That is, if  $w \in W$  and 0 does not occur in  $w$ , then there are no distinct  $x, y \in \Delta^*$  such that either  $w \Rightarrow x$  and  $w \Rightarrow y$ , or  $x \Rightarrow w$  and  $y \Rightarrow w$ .*

PROOF. This will follow from the fact that any member of  $W$  except  $A_0$  contains exactly one occurrence of a state symbol, provided that it does not contain an occurrence of 0. Suppose that there is an  $n > 0$  and a sequence  $A_0 = u_0 \Leftrightarrow u_1 \Leftrightarrow \cdots \Leftrightarrow u_n$  such that  $w = u_n$ . It suffices to show that  $\Rightarrow$  and  $\Leftarrow$  are at most single valued on the  $u_i$ . This is clearly true for  $i = 0$ ; there can be no  $x$  such that  $x \Leftarrow u_0$ , and the only possibility is  $u_0 \Rightarrow u_1 = \uparrow q_0^0 \uparrow$ . Every rule except those involving  $A_0$  or 0 replaces a subword containing one state symbol by a subword with the same property, so we may assume that every  $u_i$  ( $i > 0$ ) contains exactly one state symbol. It is easy to check that  $\Rightarrow$  is single valued on such a word; no two different transition rules can apply to the same word, because of the determinacy of the machine (i.e. because  $\delta$  is a function); a blank-creating rule is applicable only when no transition rule is applicable, because the head is looking in a direction where the endmarker is seen rather than a tape symbol; and a commutation rule is applicable only when neither a transition rule nor a blank-creating rule is applicable, because the head is looking in a direction in which a transition symbol is seen rather than a tape symbol or an endmarker. It is only slightly more difficult to see that  $\Leftarrow$  is also single valued on words containing only one occurrence of a state symbol. No two transition rules can be applicable, in the reverse sense, to the same word, because the values of  $m$  are different for different rules; the same fact makes it impossible to apply a blank-creating rule, in the reverse sense, to a word to which a transition rule is applicable in the reverse sense. Likewise the commutation rules cannot be applied in the reverse sense if a transition rule could be so applied, because of the position of the transition symbol and the value of the upper index on the state symbol.

LEMMA 5. *If  $A_0 \xrightarrow{*} u$ , then  $A_0 \xrightarrow{*} u$  and either  $u = A_0$  or there are words  $w_1, w_2, x_1, x_2$  and numbers  $s, t, s',$  and  $t'$  such that  $u = \#^{t'} \uparrow x_1 q_j^e x_2 \uparrow \#^{t'}$ ,  $H(x_1) = a_0^s$ ,  $H(x_2) = w_2 a_0^s$ , and  $\langle \lambda, q_i, \lambda \rangle \stackrel{*}{\vdash} \langle w_1, q_i, w_2 \rangle$ .*

PROOF. Suppose that  $A_0 \xrightarrow{*} u$ , and let  $A_0 = u_0 \Leftrightarrow u_1 \Leftrightarrow \cdots \Leftrightarrow u_n = u$  be a shortest derivation of  $u$  from  $A_0$ . We prove the lemma by induction on  $n$ . It is obvious if  $n = 0$  or  $n = 1$ . So suppose that  $n > 1$  and that it has been established by induction that the lemma holds for  $u = u_{n-1}$ . Since  $u_{n-2} \Rightarrow u_{n-1}$  and  $\Leftarrow$  is single valued on  $u_{n-1}$ , it cannot happen that  $u_{n-1} \Leftarrow u_n$ , for then  $u_n = u_{n-2}$ , violating the assumption that  $n$  was minimal. So  $u_{n-1} \Rightarrow u_n$ ; but then it is easy to see that values of the variables mentioned in the statement of the lemma can be found so that the conditions are true for  $u_n$  as well.

It follows that the symbols  $q_1^e$  ( $e = 0, 1$ ) occur in no member of  $W$ , and hence neither does 0. Moreover the characterization provided by Lemma 5 can be used to bound the length of words in  $W$ . For at most two length-increasing rules—one

blank-creating rule and one transition rule—can be used in the portion of the derivation corresponding to a single step of  $M$ . These two rules increase the length of the derived word by 6 at most. So if  $M$  takes  $t$  steps to reach state  $q_2$  and halt, then the longest member of  $W$  has length  $6t + 3$  at most. This means that  $W$  is finite.

DEFINITION. Let us say that a word  $u$  in  $\Delta^*$  is a *divisor* of  $A_0$  if  $u \neq \lambda$  and there are (possibly empty) words  $x$  and  $y$  such that  $A_0 \stackrel{*}{\Leftrightarrow} xuy$ . In other words, a divisor of  $A_0$  is a nonempty subword of a word in  $W$ . Let  $X$  be the set of all divisors of  $A_0$ , and let  $K$  be the (finite) cardinality of  $X/E$ .

Note that  $X$  is closed under  $E$ ; that is, if  $x \in X$  and the equation  $x = y$  is in  $E$  then  $y \in X$ .

We can conclude from the preceding development that  $0$  is not a divisor of  $A_0$  and hence not a member of  $X$ . From  $X$  we can now construct a finite semigroup in which each equation in  $E$  holds. The idea is to identify each word not in  $X$  with  $0$ .

An *ideal* of a semigroup  $G$  is a set  $I$  such that if  $i \in I$  and  $g \in G$  then  $ig, gi \in I$ . We claim that  $(\Delta^*/E) - (X/E)$  is an ideal of  $\Delta^*/E$ . The reason is simple: the product of a nondivisor of  $A_0$  with any word must be another nondivisor. Then let  $G$  be the semigroup  $(X/E) \cup \{0\}$ , with the product  $(x/E)(y/E)$  defined to be  $(xy)/E$  provided that  $x, y$ , and their concatenation are all in  $X$ , and  $0$  otherwise. It follows easily from the fact that  $(\Delta^*/E) - (X/E)$  is an ideal that the operation so defined is associative.

$G$  is finite, having cardinality exactly  $K + 1$ .  $G$  has no identity since  $\lambda \notin X$ . It remains only to show that  $G$  has the cancellation property.

To prove (2), suppose that  $xA \stackrel{*}{\Leftrightarrow} yA$ , where  $A \in \Delta$  and  $xA, yA \in X$ ; the verification of the case  $Ax \stackrel{*}{\Leftrightarrow} Ay$  is symmetrical. We must show that  $x \stackrel{*}{\Leftrightarrow} y$ . By definition of  $X$  there are  $u_1, v_1, u_2, v_2$  in  $\Delta^*$  such that  $A_0 \stackrel{*}{\Leftrightarrow} u_1xAv_1$  and  $A_0 \stackrel{*}{\Leftrightarrow} u_2yAv_2$ . By Lemma 4 both  $\Rightarrow$  and  $\Leftarrow$  are at most single valued on  $u_1xAv_1$  and on  $u_2yAv_2$  and hence on  $xA$  and  $yA$ . It follows by induction that either  $xA \stackrel{*}{\Rightarrow} yA$  or  $yA \stackrel{*}{\Rightarrow} xA$ . By symmetry let us assume that  $xA \stackrel{*}{\Rightarrow} yA$ . If the indicated occurrence of  $A$  is not within the subword replaced at any stage of this derivation, then obviously  $x \stackrel{*}{\Rightarrow} y$  by application of the same rule. Otherwise, since no rule (except the annihilation rules) have the same symbol as the rightmost symbol of both the left and right sides, there must be some rule used in which  $A$  disappears ( $zA \rightarrow v$ , where  $v$  does not end in  $A$ ) and some other rule used in which  $A$  reappears ( $v' \rightarrow z'A$ , where  $v'$  does not end in  $A$ ). By inspection of the rules, the only symbol playing both roles is a transition symbol, and the rule  $zA \rightarrow v$  must be a commutation rule (9.m, i), which leaves a word with a right-looking state symbol at its right end. But this is impossible, since no rule can apply to a word containing a single state symbol which is right-looking and appears at the right end of the word. This completes the proof of (2).

To prove (3) we must show that if  $yx \stackrel{*}{\Leftrightarrow} x$  or  $xy \stackrel{*}{\Leftrightarrow} x$  then  $x \stackrel{*}{\Leftrightarrow} 0$ . Suppose that  $xy \stackrel{*}{\Leftrightarrow} x$  but it is not the case that  $x \stackrel{*}{\Leftrightarrow} 0$ ; the other case is symmetrical. By (2) we may assume that  $x$  is a single symbol; for example, if  $x = Az$ , where  $z$  is a nonempty word, then  $Azy \stackrel{*}{\Leftrightarrow} Az$  and by cancellation  $zy \stackrel{*}{\Leftrightarrow} z$ . So it remains to show that  $Az \stackrel{*}{\Leftrightarrow} A$  only if  $A \stackrel{*}{\Leftrightarrow} 0$ . But this is easy to see, since except for the annihilation rules the only rule with but a single symbol on one side is the initialization rule (10), so that  $A$  must be  $A_0$ , and then Lemma 5 implies that the only word  $w$  containing an occurrence of  $A_0$  such that  $A_0 \stackrel{*}{\Leftrightarrow} w$  is  $A_0$  itself.

This completes the proof.



## REFERENCES

- [B] WILLIAM W. BOONE, *An analysis of Turing's 'The word problem in semi-groups with cancellation'*, *Annals of Mathematics*, vol. 67 (1958), pp. 195–202.
- [G] YURI GUREVICH, *The word problem for certain classes of semigroups*, *Algebra and Logic*, vol. 5 (1966), pp. 25–35.
- [GL] YURI GUREVICH and HARRY R. LEWIS, *The inference problem for template dependencies*, *Proceedings of the ACM SIGACT-SIGMOD Conference on Principles of Database Systems, Los Angeles, 1982*, Association for Computing Machinery, New York, 1982; revised version, to appear in *Information and Control*.
- [N] P. S. NOVIKOV, *On the algorithmic unsolvability of the word problem in group theory*, *Trudy Matematicheskogo Instituta imeni V. A. Steklova*, vol. 44 (1955). (Russian)
- [P] EMIL L. POST, *Recursive unsolvability of a problem of Thue*, this JOURNAL, vol. 12 (1947), pp. 1–11.
- [R] HARTLEY ROGERS, *Theory of recursive functions and effective computability*, McGraw-Hill, New York, 1967.
- [S1] A. M. SLOBODSKOI, *Unsolvability of the universal theory of finite groups*, *Algebra and Logic*, vol. 20 (1981), pp. 139–156.
- [Sm] RAYMOND M. SMULLYAN, *Theory of formal systems*, Annals of Mathematics Studies, No. 47, Princeton University Press, Princeton, N.J., 1961.
- [T] ALAN M. TURING, *The word problem for semigroups with cancellation*, *Annals of Mathematics*, vol. 52 (1950), pp. 491–505.

COMPUTER AND COMMUNICATION SCIENCES DEPARTMENT  
UNIVERSITY OF MICHIGAN  
ANN ARBOR, MICHIGAN 48109

AIKEN COMPUTATION LABORATORY  
HARVARD UNIVERSITY  
CAMBRIDGE, MASSACHUSETTS 02138