PARTIAL RESULTS REGARDING WORD PROBLEMS AND RECURSIVELY ENUMERABLE DEGREES OF UNSOLVABILITY

BY WILLIAM W. BOONE[1]

Communicated by Deane Montgomery, July 30, 1962

Introduction and summary of results. With the settling of the Problem of Post by Friedburg and Mucnik[2] a question that naturally presents itself is whether or not unsolvability results about word problems and related problems can be paralleled for arbitrary recursively enumerable degrees of unsolvability, i.e., for any such degree, D, does there exist a problem of such-and-such a kind having degree D? The present results furnish a partial answer to this general question. Throughout our statement of results, existence is intended in the strong sense of the exhibition of a uniform procedure for constructing.

Corresponding to a well-known unsolvability result of Markov [12][3] and Post [20] we have the following.

RESULT A. *For any recursively enumerable degree of unsolvability, D, there exists a Thue system, $\mathfrak{T}_D$, such that the word problem for $\mathfrak{T}_D$ is of degree D.*

Corresponding to an unsolvability result noted by Marshall Hall [7], we have the following.

RESULT B. *Result* A *may be strengthened to require that $\mathfrak{T}_D$ be a Thue system on two symbols.*

The following result corresponds more closely to the unsolvability result of WP, §36, than to the unsolvability of the word problem for groups as usually formulated.

RESULT C. *For any recursively enumerable degree of unsolvability, D, there exists a group presentation, $\mathfrak{T}_D$, consisting of a finite number of generators and an infinite but recursive set of defining relations, such that the word problem for $\mathfrak{T}_D$ is of degree D.*

As elsewhere noted,[4] "arbitrary degree" analogues of the Markov-

---

[1] The author is an Associate Member of the Center for Advanced Study, University of Illinois. This research was supported earlier by the John Simon Guggenheim Memorial Foundation and the United States Office of Naval Research.

[2] E. L. Post, Bull. Amer. Math. Soc. **50** (1944), 314, lines 17–22; R. M. Friedburg, Proc. Nat. Acad. Sci. U.S.A. **43** (1957), 236–238; A. A. Mucnik, Dokl. Akad. Nauk SSSR (N.S.) **108** (1956), 194–197.

[3] "WP" indicates *The Word Problem*, Ann. of Math. **70** (1959), 207–265 and *numbers in square brackets refer to the bibliography of* WP.

[4] Meeting of the Association for Symbolic Logic, Leeds, August 1962. Result B and related results were presented to this meeting. Result A, to the International Congress of Mathematicians, Stockholm, August 1962. Result C, to the Internationales Kolloquium Über Endliche Gruppen, Oberwolfach, June, 1960. Result C was discovered independently by C. R. Clapham.

Addison-Feeney-Rabin-Adjan Theorems[5] follow: the analogue for Thue systems by Result A and a very easy modification of Markov's original argument; the analogue for group presentations of the type described in Result C, by Result C and a very easy modification of Rabin's argument. (As to the analogue for finitely presented groups, this would similarly be established by the existence of a finitely presented group with word problem of preassigned arbitrary recursively enumerable degree.)

PROOF OF RESULT A.[6] Let $\mathfrak{T}_1$ be any semi-Thue system having the form which we now stipulate. The semi-Thue systems $\mathfrak{T}_2$, $\mathfrak{T}_3$ and $\mathfrak{T}_4$ depend on $\mathfrak{T}_1$.

$\mathfrak{T}_1$

$\mathfrak{Z}_1$: $s_0, s_1, \cdots, s_M, h; q_1, q_2, \cdots q_N, q$.

$\mathfrak{U}_1$: $\Theta_1 \to \Theta_1', \Theta_2 \to \Theta_2', \cdots \Theta_P \to \Theta_P'$.

Here each $\Theta_\iota \to \Theta_\iota'$, $\iota = 1, 2, \cdots P$ is of the form $\mathbf{H}\Delta q_\alpha \Delta' \mathbf{H}' \to \mathbf{H}\Pi q_\beta \Pi' \mathbf{H}'$, where (1) Δ, Δ', Π, Π' are words on the s-symbols; (2) $\mathbf{H}$ is 1 or the word h; (3) $\mathbf{H}'$ is 1 or the word h; (4) q_α is $q_1, q_2, \cdots q_N$; (5) q_β is $q_2, q_3, \cdots q_N$, or q.

$\mathfrak{T}_2$

$\mathfrak{Z}_2$: All symbols of $\mathfrak{Z}_1$; $q_0; f_1, f_2, \cdots f_P$.

$\mathfrak{U}_2$: Where $\iota = 1, 2, \cdots, P$ and $\beta = 0, 1, \cdots, M$ the rules or rule pairs 2.1 through 2.9 are rules of $\mathfrak{U}_2$:

2.1 $hq_0 \leftrightarrow f_\iota h q_0$,
2.2 $q_0 s_1 \to s_1 q_0$,
2.3 $s_1 q_0 h \to s_1 q_1 h$,
2.4 $f_\iota \Theta_\iota \to \Theta_\iota' f_\iota$,
2.5 $f_\iota s_\beta \leftrightarrow s_\beta f_\iota$,
2.6 $f_\iota h \leftrightarrow h f_\iota$,
2.7 $hqhf_\iota \leftrightarrow hqh$,
2.8 $f_\iota hqh \leftrightarrow hqh$,
2.9 $hq_0 f_\iota \leftrightarrow hq_0$.

$\mathfrak{T}_3$

$\mathfrak{Z}_3$: All symbols of $\mathfrak{Z}_2$.

$\mathfrak{U}_3$: $\Theta \leftrightarrow \Theta'$ where $\Theta \to \Theta'$ or $\Theta' \to \Theta$ (or both) is a rule of $\mathfrak{U}_2$.

$\mathfrak{T}_4$

$\mathfrak{Z}_4$: $s_{0L}, s_{1L}, \cdots s_{ML}, h_L; s_{0R}, s_{1R}, \cdots s_{MR}, h_R; f_{1L}, f_{1R}, f_{2L}, f_{2R} \cdots f_{PL}, f_{PR}; q_0, q_1, \cdots q_N, q$.

[5] See, e.g., Markov [13], the review in English [16], or M. O. Rabin, Ann. of Math. 67 (1958), 172–194 (the latter lists references to the papers of the other authors).

[6] Only WP[3] §1 and the first paragraph of §2, are needed to understand the terminology and notation used here. The terms q-symbol, s-symbol, etc., defined on p. 220 of WP, seem self-explanatory.

$\mathfrak{U}_4$: $\check{\Theta}\leftrightarrow\check{\Theta}'$ is a rule couple of $\mathfrak{U}_4$ where $\Theta\leftrightarrow\Theta'$ is any rule couple of $\mathfrak{U}_3$ other than of $\mathfrak{U}_{2.5}$ or $\mathfrak{U}_{2.6}$ and $\check{\Theta}$ and $\check{\Theta}'$ are obtained from Θ and Θ' respectively by adding L as (additional) subscript to h and every s-symbol at each occurrence left of the q-symbol and adding R as (additional) subscript to h and every s-symbol at each occurrence right of the q-symbol. Where $\iota=1, 2, \cdots P$ and $\beta=0, 1, \cdots M$, $f_{\iota L}s_{\beta L}\leftrightarrow s_{\beta L}f_{\iota L}$, $f_{\iota R}s_{\beta R}\leftrightarrow s_{\beta R}f_{\iota R}$, $f_{\iota L}h_L\leftrightarrow h_L f_{\iota L}$, $f_{\iota R}h_R\leftrightarrow h_R f_{\iota R}$ are rule couples of $\mathfrak{U}_4$.

LEMMA 1.[7] *For any recursively enumerable set of natural numbers, S, there is a choice of $\mathfrak{T}_1$ such that $n\in S$ if and only if $hs_1^{n+1}q_1h\vdash_1 hqh$.*

Lemma 1 is well-known.[8]

EQUIVALENCE THEOREM 1. *For any choice of $\mathfrak{T}_1$, the problem to determine for two arbitrary words* **U** *and* **V** *on $\mathfrak{Z}_4$ whether or not* $\mathbf{U}\vdash_4\mathbf{V}$ *reduces to the problem to determine for arbitrary natural number n whether or not $hs_1^{n+1}q_1h\vdash_1 hqh$; and vice versa.*

Since $\mathfrak{T}_4$ is a Thue system, by Lemma 1 and Equivalence Theorem 1, Result A is immediate.

The following definitions apply to $\mathfrak{T}_1$, $\mathfrak{T}_2$, $\mathfrak{T}_3$. Both Δ and Π are variables for words on the s- and f-symbols; both Ξ and Ω, for words on the f-symbols; Σ is a variable for words of form[9] $\Xi h\Delta q_\alpha\Pi h\Omega$ (*special* words); $\dot{\mathbf{A}}$ is ($\tilde{\mathbf{A}}$ is) the word **A** with f-symbols (with all symbols but f-symbols) everywhere erased. The word **A** is *semi-special* if **A** or h**A** or **A**h or h**A**h is special; Θ is a variable for semi-special words. A word of form $\mathbf{A}hq_0\mathbf{B}$ is *initial.* We use Γ (We use Λ) as a variable for initial special (for initial semi-special) words. We use Φ as variable for words containing at most one occurrence of a q-symbol (*regular* words). With no Γ (no Λ) in the context, $\dot{\Gamma}$ is ($\dot{\Lambda}$ is) a variable for f-free special initial (for f-free semi-special initial) words. A special initial word of form $hq_0s_1^{n+1}h$ is *numerical.* The notation (?$\dot{\Gamma}$, $\dot{\Gamma}$ numerical) $\dot{\Gamma}\vdash_2 hqh$ indicates[10] the following decision problem: to determine for arbitrary $\dot{\Gamma}$, "Does $\dot{\Gamma}\vdash_2 hqh$?"

The plan of the argument for Equivalence Theorem 1 in the non-

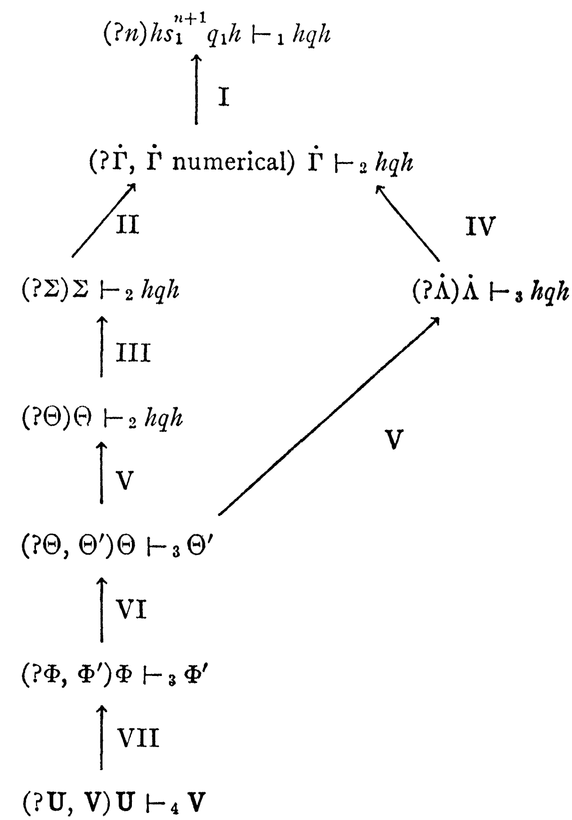
[7] Exponents are used in the usual way; within exponents, n is always a variable for natural numbers.

[8] See Kleene [9], §§68 and 71. Alternatively see the text book of Martin Davis (McGraw-Hill, 1958) or of Hans Hermes (Springer Verlag, 1961).

[9] Lower case Greek letters are variables for subscripts on symbols—including the blank subscript.

[10] By analogy, the notation (? – –, . . – – – . . .) . . . . – – – . . . . should be clear to the reader in general.

trivial direction is to show, in the diagrammatic arrangement below, that each decision problem P is reducible to the decision problem(s) at the head(s) of the arrow(s) issuing upward from P. Beside each arrow is written the number of the theorem asserting the reduction indicated.[11]



Outline of arguments for these theorems. Theorem I: Show $hq_0s_1^{n+1}h \vdash_2 hqh$ if and only if $hs_1^{n+1}q_1h \vdash_1 hqh$, $n=0, 1, 2, \cdots$. Theorem II: Call a special word *terminal* if of form $\Xi hqh\Omega$; *intermediate* if neither initial nor terminal. We have the following (recursive) possibilities for a given special word Σ. (a) Σ initial and $\dot{\Sigma}$ initial numerical; (b) Σ initial and $\dot{\Sigma}$ initial but not numerical; (c) Σ intermediate; (d) Σ terminal. If (a), apply assumed oracular process to determine if $\dot{\Sigma} \vdash_2 hqh$. By $\mathfrak{U}_{2.1}$, $\mathfrak{U}_{2.5}$, $\mathfrak{U}_{2.6}$, $\mathfrak{U}_{2.9}$, $\Sigma \vdash_2 hqh$ if and only if $\dot{\Sigma} \vdash_2 hqh$. If

[11] Theorem V asserts that a certain decision problem is reducible to the union of two other decision problems.

(b), not $\Sigma \vdash_2 hqh$. If (d), $\Sigma \vdash_2 hqh$ by rules $\mathfrak{U}_{2.7}$ and $\mathfrak{U}_{2.8}$. There remains only case (c) so it suffices to show (?Σ, Σ intermediate) $\Sigma \vdash_2 hqh$ is solvable. But this follows since an application of a rule of $\mathfrak{U}_{2.4}$ (a rule of $\mathfrak{U}_{2.5}$ or $\mathfrak{U}_{2.6}$) to a special word decreases by one (does not change) the number of occurrences of f-symbols left of the occurrence of the q-symbol;[12] and hence the number of applications of rules of $\mathfrak{U}_{2.2}$ and $\mathfrak{U}_{2.4}$ to a special word is bounded. Theorem III: If Θ is not special, then not $\Theta \vdash_2 hqh$. Theorem IV: By the method of "Post's Reduction"[13] show that $\dot{\Gamma} \vdash_3 hqh$ if and only if $\dot{\Gamma} \vdash_2 hqh$. Note that if $\dot{\Lambda}$ is not both special and numerical, then not $\dot{\Lambda} \vdash_3 hqh$. Theorem V: LEMMA 2. *Suppose not* $\dot{\Lambda} \vdash_3 hqh$. *Then* $\dot{\Lambda} \vdash_3 \dot{\Lambda}'$ *if and only if* $\dot{\Lambda}$ *is* $\dot{\Lambda}'$. LEMMA 3. *There is a recursive procedure*, R_0, *to determine for any* Θ *such that not* $\Theta \vdash_2 hqh$ *whether or not there is a* $\dot{\Lambda}$ *such that* $\Theta \vdash_3 \dot{\Lambda}$, *and if so to produce such a* $\dot{\Lambda}$, *say* $\dot{\Lambda}(\Theta)$. LEMMA 4. *There is a recursive procedure* R_1 *to determine for any pair* Θ, Θ' *such that not* $\Theta \vdash_2 hqh$ *and* $\dot{\Lambda}(\Theta)$ *does not exist, whether or not* $\Theta \vdash_3 \Theta'$. For Lemmas 2, 3 and 4, first show by the method of "Post's Reduction" that, for certain values of **A** and **B** given obviously by the statements of these lemmas, if $\mathbf{A} \vdash_3 \mathbf{B}$ then $\mathbf{A} \vdash_2 \mathbf{B}$ or $\mathbf{B} \vdash_2 \mathbf{A}$. For Lemmas 3 and 4 the argument proceeds, as for Case (c) of the argument for Theorem II, by showing the number of applications for the rules of $\mathfrak{U}_{2.2}$ and $\mathfrak{U}_{2.4}$ in these $\mathfrak{T}_2$ proofs is bounded and hence that the problems indicated are solvable. Now to show Theorem V, let R_2 be an oracular process to solve (?Θ)$\Theta \vdash_2 hqh$; R_3, to solve (?$\dot{\Lambda}$)$\dot{\Lambda} \vdash_3 hqh$. Then for any given pair of semi-special word Θ, Θ' to determine whether or not $\Theta \vdash_3 \Theta'$ apply R_2 to both Θ and Θ', consulting Table 1 about the answer—and subsequent tables as directed.[14]

TABLE 1

Is $\Theta \vdash_2 hqh$?	Is $\Theta' \vdash_2 hqh$?	Final Answer or Subsequent Action
Yes	Yes	$\Theta \vdash_3 \Theta'$
No	Yes	Apply R_0 to Θ consulting Table 2 about answer.
No	No	Apply R_0 to Θ and to Θ' consulting Table 3 about answers.

[12] Argue, similarly, for the rules $\mathfrak{U}_{2.2}$ and $\mathfrak{U}_{2.3}$ about the number of occurrences of s_1 right of q_0.

[13] I.e., the method of Lemma II of [20].

[14] The Yes-No row omitted from Table 1 is clear by symmetry.

TABLE 2

Does $\dot{\Lambda}(\Theta)$ exist?	Final Answer or Subsequent Action
Yes	Apply R_3 to $\dot{\Lambda}(\Theta)$; $\Theta \vdash_3 \Theta'$ if and only if $\dot{\Lambda}(\Theta) \vdash_3 hqh$.
No	Apply R_1 to the pair Θ, Θ' to determine whether or not $\Theta \vdash_3 \Theta'$.

TABLE 3

Do both $\dot{\Lambda}(\Theta)$ and $\dot{\Lambda}(\Theta')$ exist?	Final Answer or Subsequent Action
Yes	Apply R_3 to both $\dot{\Lambda}(\Theta)$ and $\dot{\Lambda}(\Theta')$ consulting Table 4 about answer.
No	Apply R_1 to Θ, Θ' to determine whether or not $\Theta \vdash_3 \Theta'$.

TABLE 4

Is $\dot{\Lambda}(\Theta) \vdash_3 hqh$?	Is $\dot{\Lambda}(\Theta') \vdash_3 hqh$?	Final Answer
Yes	Yes	$\Theta \vdash_3 \Theta'$
Yes	No	Not $\Theta \vdash_3 \Theta'$
No	Yes	Not $\Theta \vdash_3 \Theta'$
No	No	$\Theta \vdash_3 \Theta'$ if and only if $\dot{\Lambda}(\Theta)$ is $\dot{\Lambda}(\Theta')$.

Theorem VI: Consider the situation wherein Φ is $\mathbf{A}h\Delta q_\alpha \Pi h\mathbf{B}$ and Φ' is $\mathbf{A}'h\Delta' q_{\alpha'}\Pi' h\mathbf{B}'$: $\Phi \vdash_3 \Phi'$ if and only if $\tilde{\mathbf{A}}h\Delta q_\alpha \Pi h\tilde{\mathbf{B}} \vdash_3 \tilde{\mathbf{A}}'h\Delta' q_{\alpha'}\Pi' h\tilde{\mathbf{B}}'$, $\dot{\mathbf{A}}$ is $\dot{\mathbf{A}}'$, and $\dot{\mathbf{B}}$ is $\dot{\mathbf{B}}'$. All other cases are degenerate versions of this situation. Theorem VII: Demonstrate by means of Turing's barrier argument, [23],[15] defining barrier as Turing does on page 500 [23]. Given $\mathbf{U}$ and $\mathbf{V}$, words on $\mathfrak{Z}_4$ express them in the form $\mathbf{U}_1\mathbf{U}_2 \cdots \mathbf{U}_M$ and $\mathbf{V}_1\mathbf{V}_2 \cdots \mathbf{V}_N$ respectively where each $\mathbf{U}_i$ and $\mathbf{V}_i$ contain no barriers and M and N are minimal. Let $\mathbf{U}_i^\circ$ (Let $\mathbf{V}_i^\circ$) be $\mathbf{U}_i$ (be $\mathbf{V}_i$) with subscript L and R everywhere erased. Then show that $\mathbf{U} \vdash_4 \mathbf{V}$ if and only if both $M = N$ and $\mathbf{U}_i^\circ \vdash_3 \mathbf{V}_i^\circ$, $i = 1, 2, \cdots, M$.

We omit a discussion of the argument for Equivalence Theorem 1

[15] I.e., by the methods of Lemma 11 of [23], cf. [4].

in the trivial direction; all lemmas needed already occur in the argument for Equivalence Theorem 1 in the nontrivial direction.

PROOF OF RESULT B. Let $\mathfrak{T}_5$ be the Thue system whose symbols are a, b and whose operation rules are those of $\mathfrak{T}_4$ with the ith symbol of $\mathfrak{T}_4$ replaced by ab^ia. ($\mathfrak{T}_4$ is recursively embedded in $\mathfrak{T}_5$.) The word problem for $\mathfrak{T}_5$ reduces to the word problem for $\mathfrak{T}_4$; and vice versa. Note $\mathfrak{T}_4$ has no rules of form $\mathbf{A}\leftrightarrow 1$; the argument proceeds much like that for Theorem VII, above, used for Result A.

PROOF OF RESULT C. We consider the class of group presentations of WP, §36; viz., where S is any set of ordered pairs of positive integers let $\mathfrak{T}_S$ be the following group presentation.

$$\mathfrak{T}_S$$

$\mathfrak{Z}_S$: x_1, x_2, q, z

$\mathfrak{U}_S$: $z^m x_1^n q x_1^{-n} = x_2^n q x_2^{-n}$ for each (m, n) of S; $z=1$.

EQUIVALENCE THEOREM 2. *For any recursively enumerable set of positive integers, M, let S be the recursive set of ordered pairs of positive integers such that $d\in M$ if and only if there is a c such that $(c, d)\in S$. Then the word problem for $\mathfrak{T}_S$ reduces to the decision problem for M; and vice versa.*

Theorem XVI of WP shows Equivalence Theorem 2 in the trivial direction.[16] Now as in WP, let $\mathfrak{T}_S'$ be the presentation (isomorphic to $\mathfrak{T}_S$) with generators x_1, x_2, q and defining relations $x_1^n q x_1^{-n} = x_2^n q x_2^{-n}$, $n\in M$. Then to show the Equivalence Theorem 2 in the nontrivial direction it clearly suffices to show (†) *the word problem for $\mathfrak{T}_S'$ reduces to the decision problem for M.* The following fact seems to be well known: *Let P be the free product of groups G_1 and G_2 with the amalgamation wherein subgroup H_1 of G_1 is identified with subgroup H_2 of G_2. Suppose* (1) *the word problem is solvable in G_1 and in G_2*; (2) *the extended word problem is solvable in G_1 relative to H_1 and in G_2 relative to H_2. Then the word problem is solvable in P.* Now (the group presented by) $\mathfrak{T}_S'$ can be regarded as the free product of $F(x_1, q)$, the free group on x_1 and q and $F(x_2, q')$ with the correspondence $x_1^n q x_1^{-n} \rightarrow x_2^n q' x_2^{-n}$, $n=0$ or $\in M$ specifying the identification of subgroup V, of $F(x_1, q)$, generated by the $x_1^n q x_1^{-n}$ with the subgroup V', of $F(x_2,q')$, generated by the $x_2^n q' x_2^{-n}$, $n=0$ or $\in M$. Clearly to show (†) it is sufficient to assume an oracular process R to solve the decision problem for M and then show (1) and (2) hold where P, G_1, G_2, H_1, H_2 are

[16] If the group-theoretic version of the argument for Theorem XVI of WP, page 262 of WP—due to Graham Higman—then the entire argument for the present Equivalence Theorem 2 is a group-theoretic.

$\mathfrak{T}_S'$, $F(x_1, q)$, $F(x_2, q')$, V, V' respectively. Regarding (1) we need only note that $F(x_1, q)$ and $F(x_2, q')$ are free groups. To verify (2) suppose we are given any reduced word $\mathbf{W}$ on x_1, q. If $\mathbf{W}$ is 1 then $\mathbf{W}\in V$; if $\mathbf{W}$ is not 1 and $\mathbf{W}$ is q-free, $W\notin V$. Otherwise express $\mathbf{W}$ in the form $x_1^k q^e \mathbf{A}$, $e = \pm 1$. If $k \notin M$, (consult R) then $\mathbf{W}\notin V$. If $k\in M$, let $\mathbf{W}'$ be $(x_1^k q^{-e} x_1^{-k})(x_1^k q^e \mathbf{A})$ reduced and reapply this process to $\mathbf{W}'$; $\mathbf{W}\in V$ if and only if $\mathbf{W}'\in V$. Obviously, this is a recursive procedure to determine "Is $\mathbf{W}\in V$?" Similarly for $F(x_2, q')$ and V'.[17]

UNIVERSITY OF ILLINOIS

---

[17] This is essentially an argument due to J. Nielsen, Math. Scand. **3**, pp. 31–43, as pointed out to us by B. H. Neumann.