MATH. SCAND. 19 (1966), 185–192

ON A PROBLEM OF J. H. C. WHITEHEAD AND A PROBLEM OF ALONZO CHURCH

WILLIAM W. BOONE and HARTLEY ROGERS, Jr.

This paper was motivated by two questions, one raised by the late J. H. C. Whitehead and the other by Alonzo Church. Whitehead's question is this: Does there exist a recursive enumeration of all finite presentations of groups having a solvable word problem? Church's question is the following: Does there exist some one partial algorithm which solves the word problem for all finite presentations of groups having a solvable word problem? We shall state two general theorems which will furnish answers, in the negative, to both of these questions. (Whitehead raised his question informally with one of the authors in October, 1957; Church his, in August, 1958. Whitehead's question is noted in Boone [3] and the general setting is there explained.)

The naturalness of Whitehead's question arises from the result of Adjan [1] and Rabin [16] asserting that the meta- word problem for finitely presented groups is recursively unsolvable, i.e., that it is recursively unsolvable to determine of an arbitrary finite presentation of a group whether or not it has a solvable word problem. Knowing that the set of (Gödel numbers of) finitely presented groups with solvable word problem is not a recursive set, it is then natural, by analogy with the situation obtaining for other decision problems of group theory and number theory, to inquire if this set be recursively enumerable; or to ask more specifically exactly where this set is located in the Kleene–Mostowski Hierarchy. Since our answer to Whitehead's question is in the negative, the argument given is a new proof that the meta- word problem is unsolvable—a proof very different from that of Adjan or Rabin. This is the case simply because any recursive set is recursively enumerable[2].

Received December 18, 1965.

Research supported in part by the National Science Foundation of the U. S. A. under Grants No. GP-1568, GP-4646, and GP-4361.

[2] In settling Whitehead's question we automatically settle a variation whose naturalness springs from the fact that having a solvable word problem is an algebraic property, i.e., two finite presentations which are isomorphic either both do or both do not have a

Church's question is similarly a natural one to raise in view of the very diversity of methods used by mathematicians to solve word problems on the one hand, and the wide class of groups embraced by the methods of Dehn, Tartakovskii, Britton, Schiek, Greenlinger, Lipschutz, and Lyndon on the other. These methods are all concerned with cancellation between relators and have much in common[3].

We obtain analogous results for Thue systems on two generators, propositional calculi, Post normal systems, and finitely axiomatizable elementary theories—all as special cases, along with that of groups, of our Theorems 1 and 2. The mere fact that the meta- decision problem is unsolvable for Thue systems on two generators, Post normal systems, and finitely axiomatizable elementary theories would seem to be new.

As will be seen, Theorems 1 and 2 follow in a very immediate way from known results. But because the main purpose of this paper is to relate two different areas of mathematics, we shall attempt to make the presentation of the proofs of Theorems 1 and 2, taken together with Rogers [17], as self-contained as possible.

The only concepts of recursive function theory which we need to recall and which are not explained in Rogers [17] are those concerned with many-one reducibility. But the notions needed, $\leqq_m$, $\equiv_m$, and "many-one degrees" are defined exactly as $\leqq_1$, $\equiv_1$, and "1-degrees" are defined on p. 128 of Rogers [17] except that the f is no longer required to be one-one. Usually the standard notions and notations used in Rogers [17] will be assumed in this paper without mentions, e.g. Σ_n, Π_n. In using the more technical results and definitions of Rogers [17], our references as to where these are given in Rogers [17] will be quite specific.

LEMMA 1. *If $A \leqq_m B$, then according as B is in Σ_n or Π_n of the Kleene–Mostowski Hierarchy, so also is A.*

Suppose $B \in \Sigma_1$. Then for a certain binary recursive relation R,

$$x \in B \iff (\exists y) R(x,y) .$$

solvable word problem. One could ask: does there exist a recursive enumeration σ', made up of certain finite presentations of groups such that *each abstract group* which is finitely presentable and has a solvable word problem is presented by at least one presentation of σ'? This differs from Whitehead's question, as we interpret it, in that in the recursive enumeration σ, of Whitehead, *each presentation* with solvable word problem is required to appear at least once. But suppose σ' were to exist. Then, since all finite presentations of a group isomorphic to a given presentation are recursively enumerable (say by Tietze transforms), the existence of σ would follow by Cantor's argument for enumerating the rationals. Thus we shall have shown that neither σ nor σ' exists.

[3] See Lyndon [14] for references to these works. Lyndon [14] contains various results which are indicative of an inherent unity in these methods.

But for a certain recursive numerical function f,

$$u \in A \iff f(u) \in B .$$

Thus

$$u \in A \iff (\exists y) R(f(u), y);$$

so that, since $R(f(u), y)$ is a recursive relation in u and y, $A \in \Sigma_1$. All the other cases are shown in essentially the same way.

Lemma 1 in effect asserts that the Σ_n and Π_n of the hierarchy are well-defined with respect to many-one degrees, and are closed downward under many-one reducibility.

Where $M \in \Sigma_n$, M is called *maximal in* Σ_n, if

$$(\forall B)[B \in \Sigma_n \Rightarrow B \leqq_m M] .$$

And similarly for Π_n instead of Σ_n. The term "maximal in Σ_n" or "in Π_n" is also applied to the many-one degree of M and any set of that degree. Clearly by (2) and (3) of p. 127 of Rogers [17] and Lemma 1 of the present paper, if M is maximal in Σ_n, $n > 0$, then $M \notin \Pi_n$, $M \notin \Sigma_u$, $M \notin \Pi_u$ for $u < n$. And similarly with Σ and Π interchanged. Thus if a set S is determined to be maximal in Σ_n (or in Π_n) for a particular n, S has been located in the Kleene–Mostowski Hierarchy quite precisely indeed[4].

We assume as understood the notion of a *logical system* (or "canonical system" to use the term of Post) given in an effective way by *primitive symbols*, by a definition of *well-formed formula*, by *axioms*, and by *rules of inference*, as well as the notion of the *decision problem* (as to theoremhood) for such a system. Note that a Thue system, a finite presentation of a group, or a recursive presentation of a group is a logical system—the generators and equality sign being the primitive symbols, equations being well-formed formulas, the defining equations being the axioms, and the familiar rules of multiplication of an equation on the left (or right), reflexivity, symmetry, and transitivity being the rules of inference[5]. Of

---

[4] Using the term "maximal in ... with respect to $\leqq_m$" for what we have just called "maximal in ..." and assuming as understood the analogous "maximal in ... with respect to $\leqq_1$" we remark that by a construction parallel to that used in Myhill [15], a set is maximal in Σ_n (or Π_n) with respect to $\leqq_m$, if and only if it is maximal in Σ_n (or Π_n) with respect to $\leqq_1$.

[5] In the case of group presentations, read "generators with exponent $+1$ or -1 attached" for "generators". As described in Boone [2], pp. 213–214, one can also regard Thue systems and group presentations as Gentzen-type logical systems—so that well-formed formulas are words, etc.—rather than as Hilbert-type logical systems, our present point of view. For our purposes, the choice of point of view is quite inessential.

course partial propositional calculi, finitely axiomatizable elementary theories, and Turing Machines are frequently studied as logical systems.

We now use K as a variable for classes of logical systems; and $\mathrm{Cond}_1(K)$ is to mean the following: there exists a recursive construction such that for each (index for a) recursively enumerable set of natural numbers S, to which this construction is applied, the result is (a Gödel number for) a logical system of K, say k_S, such that the decision problem for k_S is reducible to S and such that S is uniformly many-one reducible to the set of (Gödel numbers for) theorems of k_S. Here "uniformly many-one reducible" means that there is a binary, recursive function f, such that for any recursively enumerable set S with index x, and for any natural number u, $u \in S$ if and only if $f(x,u)$ is (a Gödel number for) a theorem of k_S, the corresponding logical system[6]. (Of course this implies that the decision problem for k_S is solvable if and only if S is recursive.)

The situation in which one naturally demonstrates $\mathrm{Cond}_1(K)$ is in showing for some particular class K that for each recursively enumerable degree of unsolvability D, there exists a member of K whose decision problem is of degree D. This is exactly why we have already available in the literature, arguments that $\mathrm{Cond}_1(K)$ holds for this or that class K.

THEOREM 1. *Suppose* $\mathrm{Cond}_1(K)$. *Then* K', *the class of all (Gödel numbers of) systems of* K *possessing a solvable decision problem, is at least maximal in* Σ_3 *in the Kleene–Mostowski Hierarchy. Consequently* K' *is not recursively enumerable; a fortiori, the meta- decision problem for* K *is recursively unsolvable. In case* K *is a recursive class of systems,* K' *is exactly maximal in* Σ_3.[7]

As in the first paragraph of § 2, p. 127 of Rogers [17], let W_x be the recursively enumerable set with index x; and, as on p. 130 of Rogers [17], let A_1 be the set of x such that W_x is recursive.

Now Theorem 2 of Rogers [17] in effect asserts that A_1 is maximal in Σ_3. Thus to show our Theorem 1 it suffices to show that $A_1 \equiv_m K'$.

---

[6] Any of the standard ways of specifying, i.e., indexing, recursively enumerable sets will suffice. But for our application to Church's question it is best to regard a recursively enumerable set of natural numbers S as given by a Turing Machine $\mathfrak{M}_S$ that "semi-computes" S, i.e., if a given number is in S then this fact can be ascertained from $\mathfrak{M}_S$. See Boone [4], the machine $\mathfrak{M}$ described in (1.1), (1.2), and (1.3) following the statement of Equivalence Theorem 1. The gain is both in the simplicity of the form of group presentations being used to answer Church's question and the unity of the over-all argument.

[7] To say that K is recursive is to say that the set of all Gödel numbers for members of K is recursive. This is the case for all classes of finitely presented structures in the applications given below. See the remark before Theorem 2.

But since $\text{Cond}_1(K)$, $A_1 \leqq_m K'$. In case K is a recursive class, by the very definitions of A_1 and K', $K' \leqq_m A_1$. Hence we have Theorem 1.

REMARK. In applications of our theorems in which all sets of axioms for systems of K are finite, each system will have, essentially, only one Gödel number. In applications in which the systems of K may be infinite, recursive sets of axioms, each system will, in general, have infinitely many Gödel numbers,—in an essential way. These Gödel numbers may be taken to be Gödel numbers of (Turing Machines[6] or sets of recursion equations presenting) the recursive characteristic function of the set of axioms—"fully effective" Gödel numbers—or they may be taken to be indices for (Turing Machines, etc.) recursively enumerating the set of axioms—"semi-effective" Gödel numbers. Under either choice, our theorems apply.

THEOREM 2. *Suppose* $\text{Cond}_1(K)$. *Let K' be the class of all (Gödel numbers of) systems of K possessing a solvable decision problem. Then one can explicitly specify a recursive subclass of K', say K'', such that there does not exist some one algorithm, $\mathfrak{A}$, which solves the decision problem for all systems of K''. Thus, a fortiori, there does not exist some one algorithm which solves the decision problem for all systems of K'.*

In precise terms, what we mean by the $\mathfrak{A}$ of Theorem 2 is a binary, partial recursive function f, depending on K'', such that if y is the index of system k of K'' and if p is the Gödel number of well-formed formula W of k, then f is defined for the argument y, p, and $f(y, p) = 0$ or 1 according as W is a theorem of k or not.

We now assume some standard recursive enumeration of all Turing Machines: $\mathfrak{M}_0, \mathfrak{M}_1, \mathfrak{M}_2, \ldots$. We assume, too, that in some uniform way certain complete configurations of these machines are singled out as representing (natural) numbers so that each number has a unique representation. If $\mathfrak{M}_m$ is started in the initial complete configuration representing n, we say that "$\mathfrak{M}_m$ has input n". Finally, for each $\mathfrak{M}_m$ we single out a certain internal configuration, uniformly called q; and where $\mathfrak{M}_m$ with input n eventually enters internal configuration q with blank tape and stops we shall say "$\mathfrak{M}_m$ q-terminates for n". As is consistent with our earlier use of this notation, W_m is to be the set of n such that $\mathfrak{M}_m$ q-terminates for n. It is well-known that (*) *the problem to determine for arbitrary m and n whether or not $n \in W_m$ is recursively unsolvable.*

LEMMA 2. *For each pair of numbers, m and n, there is a Turing Machine $\mathfrak{D}_{m,n}$ such that:*

(2.1) $\mathfrak{O}_{m,n}$ *does not q-terminate for* i, $i \neq 1$;

(2.2) $\mathfrak{O}_{m,n}$ *q-terminates for* 1 *if and only if* $n \in W_m$;

(2.3) *Suppose notationally, that* $\mathfrak{O}_{m,n}$ *is* $\mathfrak{M}_{\eta(m,n)}$; *then* η *is a total recursive function*; *i.e., there is a recursive construction which, when applied to arbitrary* $\mathfrak{M}_m$ *and* n, *the result is* $\mathfrak{O}_{m,n}$;

(2.4) J, *the range of* η *is a recursive set*; *i.e., one can recursively determine for arbitrary* $\mathfrak{M}_j$ *whether or not it is* $\mathfrak{O}_{m,n}$ *for some* m *and* n, *and if so, for which* m *and* n.

In the first stage $\mathfrak{O}_{m,n}$ checks to determine whether or not it has input 1. If so, $\mathfrak{O}_{m,n}$ enters the second stage by which it passes into the complete configuration representing n. Finally, $\mathfrak{O}_{m,n}$ enters the third stage in which it behaves exactly like $\mathfrak{M}_m$ with input n. From this animistic description it should be easy for the reader to spell out the recursive construction of Lemma 2.3 in such fashion that Lemma 2.4 is verified.

We now show Theorem 2. Clearly

$$W_{\eta(m,n)} = \begin{cases} \{1\}, & \text{if } n \in W_m, \\ \emptyset & \text{otherwise}. \end{cases}$$

Thus each W_i, $i \in J$, is a recursive set. But in view of * and the fact that $1 \in W_{\eta(m,n)}$ if and only if $n \in W_m$, (**) *there does not exist some one algorithm which solves the decision problem for all* W_i, $i \in J$. In the notation of the definition of Cond_1, let the K'' of Theorem 2 be k_{W_i}, $i \in J$. Clearly, each of these systems does have a solvable decision problem by the first part of the definition of Cond_1. This shows Theorem 2, for the existence of an $\mathfrak{A}$ as described in Theorem 2 would contradict ** in view of the uniform many-one reducibility part of the definition of Cond_1.

We now list the applications of Theorems 1 and 2 which are known to us. These are given by the following table.[8]

K	*Source(s) verifying* $\text{Cond}_1(K)$
Thue systems	Céjtin [6]; Shepherdson [18]; Boone [4], Result A.
Thue systems on two generators	Boone [4], Result B.
Recursively presented groups	Clapham [7]; Boone [5], Result J.
Finitely presented groups	Fridman [9]; Clapham [7]; Boone [5], Result G.

K	*Source(s) verifying* $\mathrm{Cond}_1(K)$
Certain partial propositional calculi	Gladstone [10]; Ihrig [12]; Singletary [19].
Post normal systems and related systems	Ihrig [13].
Turing Machines	Shepherdson [18].
Recursively axiomatizable elementary theories	Feferman [8].
Finitely axiomatizable elementary theories	Hanf [11].

Each value of K noted may be qualified with "of a certain form". Read in this way, no one line of the table implies another. The corresponding value of K'' in Theorem 2 has an extremely simple form when constructed from the works of Ihrig, Singletary, and Boone listed. Indeed, with a notation for the $\mathfrak{M}_i$ of the proof of Theorem 2 assumed, a "generic member" of the class of finite presentations of groups, partial propositional calculi, etc., can, in a practical sense, actually be written down if these sources are used. It was for the sake of this simplicity that we used the q-terminating problem in the proof of Theorem 2 rather than say the halting problem.

We shall not go into the question here as to whether or not Theorems 1 and 2 are applicable to decision problems like the isomorphism problem and the homeomorphy problem, i.e., decision problems about properties of, or relations among, logical systems as a whole.

Finally, we note that there is no recursive enumeration of all finite presentations of groups having unsolvable word problem, since the collection of all such presentations is maximal in Π_3. Indeed, the analogous general theorem holds for any class of logical systems K, such that $\mathrm{Cond}_1(K)$.

---

[8] In listing the announcements Céjtin [6] and Fridman [9], we are simply assuming, on the basis of the kind of result announced, that in the proof intended by these mathematicians Cond_1 is verified for the indicated value of K. While we cannot assert unequivocally that Clapham [7] shows Cond_1 for finitely presented groups, we are rather convinced that this is so—with perhaps some trivial modification required. We have no reservations about the other entries. Thus in particular the case of finitely presented groups, which motivated the present paper, is settled by Boone [5].

REFERENCES

1. S. I. Adjan, *The algorithmic unsolvability of problems concerning certain properties of groups*, Dokl. Akad. Nauk SSSR 103 (1955), 533–535.
2. W. W. Boone, *The word problem*, Ann. of Math. 70 (1959), 207–265.
3. W. W. Boone, review of [16], Math. Reviews, Review # 1611, 22 (1961).
4. W. W. Boone, *Word problems and recursively enumerable degrees of unsolvability. A first paper on Thue systems*, Ann. of Math. 83 (1966), 520–571.
5. W. W. Boone, *Word problems and recursively enumerable degrees of unsolvability. A sequel on finitely presented groups*, Ann. of Math. 84 (1966), 49–83.
6. G. S. Céjtin, Oral announcement of P. S. Novikov in half-hour lecture at the International Congress of Mathematicians, Stockholm, August 1962, to the effect that Céjtin had shown the existence of Thue systems with word problem of arbitrary recursively enumerable degree of unsolvability.
7. C. R. J. Clapham, *Finitely presented groups with word problems of arbitrary degrees of insolvability*, Proc. London Math. Soc. (3) 14 (1964), 633–676.
8. S. Feferman, *Degrees of unsolvability associated with classes of formalized theories*, J. Symb. Logic 22 (1957), 161–175.
9. A. A. Fridman, *Degrees of unsolvability of the problem of identity in finitely presented groups*, Dokl. Akad. Nauk SSSR 147 (1962), 805–808 (= Soviet Math. 3 (1962), 1733–1737).
10. M. D. Gladstone, *Some ways of constructing a propositional calculus of any required degree of unsolvability*, Trans. Amer. Math. Soc. 118 (1965), 192–210. (Dissertation, University of Bristol, 1963).
11. W. Hanf, Dissertation, University of California at Berkely, 1962. Portion circulated by the International Business Machine Corporation under the title *Model Theoretic Methods in the Study of Elementary Logic*. See further Notices of the American Mathematical Society 9 (1962), Abstract 590-30, 127–128, and Abstract 62T-75, 146–147.
12. A. H. Ihrig, *The Post-Linial theorems for arbitrary recursively enumerable degrees of unsolvability*, Notre Dame J. Formal Logic 6 (1965), 54–72.
13. A. H. Ihrig, Notices of the American Mathematical Society 11 (1964), abstract 64T-9, 128. See further *A remark on Post Normal Systems*, to appear J. Association for Computing Machinery, under author's marriage name, A. Yasuhara. (This and [12] are in author's dissertation, University of Illinois, 1964.)
14. R. C. Lyndon, *On Dehn's algorithm*, Math. Ann. 166 (1966), 208–228.
15. J. Myhill, *Creative sets*, Z. math. Logik Grundlagen Math. 1 (1955), 97–108.
16. M. O. Rabin, *Recursive unsolvability of group theoretic problems*, Ann. of Math. 67 (1958), 172–194.
17. H. Rogers, Jr., *Computing degrees of unsolvability*, Math. Ann. 138 (1959), 125–140.
18. J. C. Shepherdson, *Machine configuration and word problems of given degree of unsolvability*, Z. math. Logik Grundlagen Math. 11 (1965), 149–175.
19. W. E. Singletary, *Recursive unsolvability of a complex of problems proposed by Post*, submitted to the J. Math. Soc. Japan. (Dissertation University of Illinois, 1964.)

UNIVERSITY OF ILLINOIS, URBANA, ILL.,
AND INSTITUTE FOR ADVANCED STUDY, PRINCETON, N. J., U.S.A.

AND

MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASS., U.S.A.