THE DECISION PROBLEM FOR RECURSIVELY ENUMERABLE DEGREES

BY J. R. SHOENFIELD

If I have any message today for mathematicians in general, it is that consideration of difficult problems can be useful even when the problem is at present beyond solution. The problem I will discuss is unlikely to be solved in the near future, but I hope to show how the study of it leads to many more accessible problems.

In order to state the problem, we need some definitions. To save words, we agree that *number* means *natural number* (nonnegative integer) and *set* means *set of numbers*.

A set A is *recursive* if there is an algorithm for determining whether any given number is in A. A set A is *recursive in* a set B if there is an algorithm by which we can decide whether any given number x is in A, provided we are supplied with answers to all questions we choose to ask of the form 'Is y in B?'.

As an example, let $A = \{2x : x \in B\}$. Then B is recursive in A; for $x \in B$ iff $2x \in A$. Also A is recursive in B; for $x \in A$ iff x is even and $\frac{1}{2}x \in B$. (All this is independent of the choice of B.)

Writing $A \leq_R B$ for A is recursive in B, we easily see that

$$(1) \qquad\qquad A \leq_R A,$$

$$(2) \qquad\qquad A \leq_R B \ \& \ B \leq_R C \to A \leq_R C.$$

Of course $A \leq_R B \ \& \ B \leq_R A$ does not imply $A = B$, as the above example shows. However, if we define

$$(3) \qquad\qquad A \sim B \text{ iff } A \leq_R B \ \& \ B \leq_R A,$$

then (1) and (2) show that $\sim$ is an equivalence relation. The equivalence class of A is the *degree* of A; it is written $\mathrm{dg}(A)$. Setting

$$(4) \qquad\qquad \mathrm{dg}(A) \leq \mathrm{dg}(B) \text{ iff } A \leq_R B,$$

we see from (1) and (2) that the set of degrees is a partially ordered set D.

The study of degrees was initiated by Kleene and Post [2] who observed two simple facts. (A) There is a smallest degree 0; it is the degree of every recursive set. (B) Every pair a, b of degrees has a least upper bound $a \cup b$. In fact, $\mathrm{dg}(A) \cup \mathrm{dg}(B) = \mathrm{dg}(A \oplus B)$, where $A \oplus B = \{2x : x \in A\} \cup \{2x+1 : x \in B\}$.

The main content of [2] and several subsequent papers is that D has very few nice properties other than (A) and (B). For example, it is shown in [2] that D is not a linearly ordered set, or even a lattice. In [11] it is shown that no strictly increasing sequence of degrees has a least upper bound.

One quickly reaches the conclusion that there is no good way to describe D completely. A logician, however, cannot feel satisfied with such a vague statement; he must replace it by a precise and provable statement. We will show how this is done.

We shall write *poset* for partially ordered set. The smallest member of a poset (if it exists) is designated by 0; the largest by 0′. If a and b are elements in a poset, their least upper bound (if it exists) is designated by $a \cup b$ and their greatest lower bound by $a \cap b$.

Now we describe a language L for making statements about any given poset. The language contains *variables* x, y, $z, \cdots$ which vary through the members of the poset. From these variables we form *atomic formulas* of the form $x \leq y$ or $x = y$. From these we build further formulas by means of propositional connectives (not, or, and, etc.) and quantifiers ($\forall x$ and $\exists x$).

The *decision problem* for a poset P is the following: find an algorithm for determining if a given sentence of L is true in P. Now the sentences of L can express only relatively simple facts about P, since we cannot say anything about all subsets of P. Hence a good description of P should provide a solution of the decision problem for P. However, Lachlan [5] has shown that the decision problem for D is unsolvable.

To approach our next definition, we consider an example. Let A be the set of n such that $x^n + y^n = z^n$ has a nontrivial solution. We do not know if A is recursive; certainly no algorithm is known for deciding if n is in A. However, given n, we can start testing all possible triples (x, y, z); and if n is in A, we will find that out. If n is not in A, the computation goes on forever.

A set A is *recursively enumerable* (abbreviated RE) if there is an algorithm which, applied to n, leads to the conclusion that n is in A when this conclusion is correct, but leads to no conclusion when n is not in A. A degree is RE if it is the degree of an RE set. (Caution: dg(A) may be RE even if A is not RE.) The set of RE degrees is designated by RED.

There is not room to explain why RE sets and degrees are important; please believe that they are. Investigations have shown that RED has many of the properties of D, but the proofs are generally much harder. The priority method of Friedberg [1] and Muchnik [7] was needed just to show that RED has more than two members, and the proof that RED is not a lattice was only given in [4].

The decision problem for RED is the difficult problem I will discuss. I propose to show that attempting either a positive or a negative solution leads to interesting and approachable problems.

Let us first see why Lachlan's negative solution for D does not work for RED. An *initial section* of a partially ordered set is a subset of the form $\{x : x \leq y\}$. The key fact proved by Lachlan is that every finite distributive lattice is isomorphic to an initial section of D. It follows easily that if we could decide which sentences of L are true in D, we could decide which sentences of L are true in all finite distributive lattices. But the latter is known to be impossible.

This procedure fails in RED because of the following theorem of Muchnik

[7]: the only finite initial section of RED is the set $\{0\}$. (This is a rare case in which RED behaves very differently from D.)

A subset of RED is *definable from* $a_1, \cdots, a_n \in$ RED if it is $\{x \in \text{RED} : \phi(x, a_1, \cdots, a_n)\}$ for some formula $\phi(x, y_1, \cdots, y_n)$ of L. Thus the initial section $\{x : x \leq y\}$ is definable from y. Perhaps the above will lead the reader to accept the following principle: the best method to get a negative solution of the decision problem for RED is to show that lots of finite subsets can be defined from few elements of RED.

Unfortunately, this method does not seem to work. Consider, for example, the definable subsets of RED (where *definable* means definable from zero members of RED). Only four finite definable subsets are known: the empty set, $\{0\}$, $\{0'\}$, and $\{0, 0'\}$. (It is fairly easy to prove that RED has a largest member.) It is a reasonable conjecture that these are the only finite definable sets. If we succeeded in proving this, we might understand enough to show that it is impossible to solve the decision problem negatively by what we called the best method.

How might we prove the conjecture? It is easy to see that automorphisms of RED take definable sets into definable sets. It would thus suffice to prove: if x, $y \in$ RED and neither is 0 or $0'$, then some automorphism of RED takes x into y. Unfortunately, we do not even know if RED has any automorphisms other than the identity. However, recent work by Soare and others on isomorphisms of RE sets lead one to think that this problem can be attacked.

How might we give a positive solution to the decision problem for RED? I suggested in [9] a conjecture which would give such a solution. Roughly speaking, it is this: if $\phi(x, y_1, \cdots, y_n)$ is a formula of L, and $a_1, \cdots, a_n \in$ RED, then there is a $b \in$ RED such that $\phi(b, a_1, \cdots, a_n)$, unless there is an obvious reason why no such b can exist.

Instead of making this precise, let us consider an example. Given a_1 and a_2, can we find b such that $b < a_1$, $b < a_2$, and $b \neq 0$? An obvious reason why not would be that $a_1 = 0$ or $a_2 = 0$. The conjecture implies that b exists whenever $a_1 \neq 0$ and $a_2 \neq 0$. In other words, no two nonzero RE degrees a and b have $a \cap b = 0$.

In [13], Yates produced two nonzero RE degrees a and b with $a \cap b = 0$. In [3], Lachlan gave another counterexample to the general conjecture. Both counterexamples have been improved in various ways.

Proud of the success of my conjecture in inspiring good work, I searched for another such conjecture. All I have produced is a conjecture which would solve a very special case of the decision problem. However, I think it has much more justification than my original conjecture.

One approach to a positive solution is to consider very simple sentences of L first. Since it is the quantifiers which cause all the difficulty, we should somehow restrict the way in which quantifiers appear.

A formula is *existential* if it has the form $\exists x_1 \cdots \exists x_n \phi(x_1, \cdots, x_n)$ where $\phi(x_1, \cdots, x_n)$ contain no quantifiers. In L, this class of formulas is too simple; the solution of the decision problem for these sentences in RED is trivial.

We therefore expand L to L' by adding three new kinds of atomic formulas: $x=0$, $x \cup y = z$, and $x \cap y = z$. Each of these formulas can be expressed in L also, but only by using quantifiers. Thus formulas of L' say no more than formulas of L; but existential formulas of L' say a good deal more than existential formulas of L.

Let me outline a program for solving the decision problem for existential formulas of L' (in RED). Let X and Y be posets having a smallest element. An L'-embedding of X in Y is a one-one mapping F of X into Y which is an isomorphism for all things mentioned in L'. Thus we must have $a = b \cap c$ iff $F(a) = F(b) \cap F(c)$ for a, b, $c \in X$.

EMBEDDING CONJECTURE. Every finite lattice has an L'-embedding in RED.

How would this solve our problem? Consider an existential formula $\exists x_1 \cdots \exists x_n \phi(x_1, \cdots, x_n)$ in L'. It is trivial to see that this is true in RED iff it is true in some finite subset of RED. It is easy to see that every finite poset with a smallest element can be L'-embedded in a finite lattice; so, by the Embedding Conjecture, it can be L'-embedded in RED. Thus we have only to see if $\exists x_1 \cdots \exists x_n \phi(x_1, \cdots, x_n)$ is true in some finite poset with a smallest element. It turns out that we can do this quite easily.

What justification is there for the Embedding Conjecture? Consider the case of the four element Boolean algebra. It consists of two atoms a and b plus $a \cup b$ and $a \cap b = 0$. An L'-embedding F in RED is clearly determined by $F(a)$ and $F(b)$; and it is easy to check that what we require of $F(a)$ and $F(b)$ is $F(a) \neq 0$, $F(b) \neq 0$, and $F(a) \cap F(b) = 0$. Thus, this case of the conjecture is just the theorem of Yates mentioned above.

The Embedding Conjecture has been proved for distributive lattices by Thomason [12] and for the two five-element nondistributive lattices by Lachlan [6]. Possibly one could prove the full conjecture by the methods of [6].

The main trouble with the Embedding Conjecture is that very simple extensions are false. Thus suppose we extend L' to L'' by adding $x=0'$ as a new atomic sentence. The extension of the Embedding Conjecture to L'' is false for the four element Boolean algebra. This theorem of Lachlan [4] is quite remarkable; it shows that something cannot happen in RED, even though there is no obvious reason why it should not happen. The only similar result I can think of is the Muchnik theorem on initial sections quoted above.

In [4], Lachlan conjectures the following extension of his result: if a, $b \in$ RED and $a \cup b = 0'$, then $a \cap b$ does not exist. Suppose for the moment that this is true and that the Embedding Conjecture is true. We can then characterize the finite lattices which can be L''-embedded in RED: they are those such that $0'$ is not the supremum of the elements other than $0'$. This in turn leads to a solution of the decision problem for existential sentences of L'' in RED.

By this time, even enthusiastic degree theorists have enough problems to keep them busy. I cannot promise that the solution to these problems will

lead to the solution of the decision problem; but it will certainly increase our understanding of RE degrees.

BIBLIOGRAPHY

The books [8] and [10] contain considerable information about the topics of this paper.

1. R. M. Friedberg, *Two recursively enumerable sets of incomparable degrees of unsolvability* (*solution of Post's problem*, 1944), Proc. Nat. Acad. Sci. U.S.A. **43** (1957), 236–238. MR **18**, 867.

2. S. C. Kleene and E. L. Post, *The upper semi-lattice of degrees of recursive unsolvability*, Ann. of Math. (2) **59** (1954), 379–407. MR **15**, 772.

3. A. H. Lachlan, *The impossibility of finding relative complements for recursively enumerable degrees*, J. Symbolic Logic **31** (1966), 434–454. MR **34** #5673.

4. ———, *Lower bounds for pairs of recursively enumerable degrees*, Proc. London Math. Soc. (3) **16** (1966), 537–569. MR **34** #4126.

5. ———, *Distributive initial segments of the degrees of unsolvability*, Z. Math. Logik Grundlagen Math. **14** (1968), 457–472. MR **38** #5620.

6. ———, *Embedding nondistributive lattices in the recursively enumerable degrees*, Conference in Mathematical Logic—London '70, Lecture Notes in Math., vol. 255, Springer-Verlag, New York, 1972, pp. 149–177.

7. A. A. Mučnik, *Negative answer to the problem of reducibility of the theory of algorithms*, Dokl. Akad. Nauk SSSR **108** (1956), 194–197. (Russian).

8. G. E. Sacks, *Degrees of unsolvability*, Ann. of Math. Studies, no. 55, Princeton Univ. Press, Princeton, N.J., 1963. MR **32** #4013.

9. J. R. Shoenfield, *Applications of model theory to degrees of unsolvability*, Theory of Models (Proc. 1963 Internat. Sympos., Berkeley), North-Holland, Amsterdam, 1965, pp. 359–363. MR **34** #53.

10. ———, *Degrees of unsolvability*, North-Holland, Amsterdam, 1971.

11. C. Spector, *On degrees of recursive unsolvability*, Ann. of Math. (2) **64** (1956), 581–592. MR **18**, 552, 1118.

12. S. K. Thomason, *Sublattices of the recursively enumerable degrees*, Z. Math. Logik Grundlagen Math. **17** (1971), 273–280. MR **45** #8523.

13. C. E. M. Yates, *A minimal pair of recursively enumerable degrees*, J. Symbolic Logic **31** (1966), 158–168. MR **34** #5677.