ON AUTO-REDUCIBILITY

MATHEMATICS

1970

SovietRxiv

Abstract

Full Text

UDC 51.01+518.5

MATHEMATICS

B. A. TRAKHTENBROT

ON AUTO-REDUCIBILITY

(Presented by Academician P. S. Novikov, 15 XII 1969)

1°. Introduction. In the present paper the concept of auto-reducibility (non-auto-reducibility) is defined and studied; this concept, as it seems to us, naturally refines the intuitive idea of the mutual dependence (of mutual independence) of the individual problems that make up a certain mass problem. Consider, for example, the problem of recognizing derivability in some formal theory T, constructed in the usual way by means of predicate logic. This problem may be algorithmically undecidable; however, there may exist an effective procedure (in our terminology, an auto-reduction) that gives the correct answer to each question "is the formula $\mathfrak{A}$ derivable?" provided only that the answers for other formulas, distinct from $\mathfrak{A}$, are regarded as known. For example, it is enough to use information about the derivability or non-derivability of $\neg\neg\mathfrak{A}$. Suppose now that for our theory T derivability is effectively recognizable and, consequently, the required answers can be found by means of direct computations (without auto-reduction). It might turn out, however, that in this case it is impossible to dispense with complicated computations (usually this is just how it is); the above-mentioned auto-reduction procedure, on the other hand, is very simple.

Of course, a priori there may exist algorithmically undecidable problems for which auto-reduction is impossible (non-auto-reducible problems), as well as algorithmically decidable problems for which no auto-reduction is possible that is substantially simpler than unconditional decision algorithms.

Such situations may be interpreted as a manifestation of the independence of the individual problems of a mass problem from one another.

In what follows, by a mass problem we mean, as is customary in the theory of algorithms, the problem of membership in some set G of natural numbers, and we devote our main attention to recursively enumerable (r.e.) sets or their complements. In Sec. 2° we give definitions connected with auto-reducibility, and also with the formalization of the concept of a random sequence (the Mises collective) due to A. N. Kolmogorov (2) and D. W. Loveland (3); from this it is seen that non-auto-reducibility is a weaker (and hence more general) property than randomness. In Sec. 3° it is clarified which auto-reducible and non-auto-reducible sets exist in the class of r.e. sets. In Sec. 4° for recursive sets the complexity of computation is compared with the complexity of auto-reduction.

Results close to Theorem 2 of this section, but of a more special character, are contained in the work of J. H. Hojaev (7). Finally, in Sec. 5° the connection of auto-reducibility with the notions of introreducibility* and uniform introreducibility (4) is briefly discussed.

2°. Let G be an arbitrary set of natural numbers, and let Γ be its characteristic function (predicate), or, equivalently, the corresponding sequence of ones and zeros:

$$\Gamma(1), \Gamma(2), \ldots, \Gamma(n), \ldots \tag{1}$$

* In RZhMat 7A72, 1969, the term "introreducible" is translated as self-reducible; we prefer the more accurate translation introreducible. (Self-reducible could be used as a synonym for auto-reducible.)

In terms of machines with an oracle ((1), p. 130), the notion of a guessing strategy (admissible system) and a selection strategy (admissible system) can be formalized as follows.

A guessing strategy is a machine $\mathfrak{M}$ with an oracle satisfying the following condition: whatever the oracle G and the natural number n, when run on the argument n, the machine $\mathfrak{M}$ never queries the oracle with the question "$n \in G$?" (although it may ask any questions "$v \in G$?" with $v \neq n$).

A selection strategy is a machine $\mathfrak{M}$ with an oracle which, when run on a blank tape, writes on it (in some standard code) an oracle-dependent sequence (finite or infinite) of nonrepeating natural numbers

$$i_1, i_2, \ldots, i_k, \ldots \tag{2}$$

subject to the condition: whatever the oracle G and the natural number k, up to the completion of the writing of the number i_k the machine does not query the oracle with the question "$i_k \in G$?" .

In this case, of the sequence of zeros and ones

$$\Gamma(i_1), \Gamma(i_2), \ldots, \Gamma(i_k), \ldots \tag{3}$$

one says that it is selected from the sequence (1) by means of the selection strategy $\mathfrak{M}$.

A set G is called autoreducible if it possesses self-information, i.e., a guessing strategy which, supplied with the oracle G, computes for each n the value $\Gamma(n)$; otherwise G is non-autoreducible.

As is known, in accordance with the Mises conception, the sequence (1) is declared to be a collective, or a random sequence, if the following conditions are fulfilled: 1) in it there exists the limit of the relative frequency of ones; 2) this

limit is preserved for every infinite subsequence (3) selected from (1) by means of a selection strategy.*

In what follows, when using the terminology indicated above, we shall not distinguish between the set G, the sequence (1), the predicate Γ, or the corresponding membership problem (for example, a random set G, an autoreducible sequence $\Gamma(1), \Gamma(2), ...$, etc.).

The following assertion is almost obvious:

If the sequence (1) is autoreducible, then there exists a selection strategy which selects from it an infinite subsequence (3) lying entirely in G or in its complement. Consequently, every random set is non-autoreducible.

3°. The property of autoreducibility is recursively invariant. However, it is not invariant with respect to m-equivalence. For any set G there exists a set G' m-equivalent to it which is autoreducible (and, moreover, the process of self-information is very simple). Namely, G' can be defined by the condition:

$$\forall n[2n \in G' \equiv 2n+1 \in G' \equiv n \in G]. \tag{4}$$

On the other hand, any assertion on the existence of random sets is automatically also a theorem on the existence of non-autoreducible sets. Thus, for example, in ([3]) it is established that in the Kleene–Mostowski class $\Sigma_2 \cap \Pi_2$ there exist random (and hence non-autoreducible) sets. However, since a random set cannot be recursively enumerable and cannot even be obtained from r.e. sets by means of Boolean operations, this gives us no information

---

* Let us recall that the original formalization of the Mises conception is due to Church; it is based on a definition of selection strategy different from the Kolmogorov–Loveland definition used by us and selects a narrower class of strategies.

with respect to r.e. sets (or, what is the same, with respect to sets with r.e. complements). In fact, by means of two suitable diagonal constructions one can discover the existence of non-autoreducible r.e. sets of two mutually exclusive types.

Theorem 1. (A). *There exists a non-autoreducible set G with r.e. complement which is not immune (i.e., G contains an infinite r.e. set).*

(B). *There exists a non-autoreducible set G with r.e. complement satisfying the condition: no selection strategy can single out from G an infinite r.e. subset.* $(*)$

Note that condition $(*)$ is stronger than ordinary immunity.

Unsolved problems. (I). Does there exist, for every nonrecursive set (and, in particular, for every nonrecursive r.e. set), an m-equivalent (truth-table-equivalent, Turing-equivalent, $\cdots$) set that is non-autoreducible?

(II). Describe "natural" mass problems that are non-autoreducible. (In the introduction the autoreducibility of recognizing logical derivability was already noted; this also applies to the identity problem for group theory, etc.)

4°. We shall estimate the complexity of computations and autoreductions by means of space signaling functions ([5]). Let us recall some definitions pertaining to ordinary Turing machines, and also to Turing machines with an oracle. The space signaling function $s_{\mathfrak{M}}(n)$ indicates, for an ordinary machine $\mathfrak{M}$, the number of cells used by $\mathfrak{M}$, provided it is started on the argument n, given in unary notation (n strokes). The analogous meaning is borne by $s_{\mathfrak{M}\Gamma}(n)$ for a machine supplied with an oracle Γ. An everywhere defined function $h(n)$ is called a space function if it coincides with $s_{\mathfrak{M}}(n)$ for some ordinary machine $\mathfrak{M}$.

Theorem 2. *For any space function h there exists a predicate Γ satisfying the following conditions:*

1) *(upper bound for computation). There exists a machine $\mathfrak{R}$, computing Γ, such that*
$$\forall n\,[s_{\mathfrak{R}}(n) = h(n)].$$

2) *(lower bound for autoreduction). Let a guessing strategy $\mathfrak{M}$ compute Γ; then there exists a constant c such that*
$$\forall n\,[s_{\mathfrak{M}\Gamma}(n) \geq ch(n)].$$

In other words, there exist effective mass problems of any complexity h which do not admit autoreductions substantially simpler than their unconditional computations.

It was already observed earlier (see the introduction and the sets G' defined by condition (4)) that there exist mass problems with a very simple autoreduction. However, this occurred in connection with a trivial mutual dependence of the individual problems (for example, the derivability of $\mathfrak{A}$, the derivability of $\neg\mathfrak{A}$, $2n \in G' \equiv 2n+1 \in G'$).

The following theorem, strengthening the result from ([6]), reveals a nontrivial situation of mutual dependence excluding "triples" of the above-mentioned type.

Theorem 3. *For every strictly monotone space function h there exists a predicate Γ satisfying the following conditions:*

(I) *(upper bound for computation). There exists a machine $\mathfrak{R}$, computing Γ, such that*
$$\forall n\,[s_{\mathfrak{R}}(n) = h(n)].$$

(II) *(lower bound for computation). For every machine* $\mathfrak{M}$*, computing* Γ*, there exists a constant* c *such that*

$$\forall n\,[s_{\mathfrak{M}}(n) \geq ch(n)].$$

(III) *(upper bound for autoreduction). There exist a guessing strategy* Ω*, computing* Γ*, and a constant* d *such that*

$$\forall n\,[s_{\Omega\Gamma}(n) \leq h(n)] \qquad \exists^{\infty} n\,[s_{\Omega\Gamma}(n) \leq dn].$$

It remains an open question whether Theorem 3 remains valid if the assertion $T \sim n[s_{\Omega\Gamma}(n) \leq dn]$ is replaced by the stronger assertion $\forall n[s_{\Omega\Gamma}(n) \leq dn]$.

5°. Let us recall the following definitions (see (4)).

A set M is called **introreducible** if it is reducible to each of its infinite subsets.

A set M is uniformly introreducible if there exists a reduction algorithm (an oracle machine) that reduces M to each of its infinite subsets.

Denote by $\mathfrak{R}_{\text{aut}}, \mathfrak{R}_{\text{intr}}, \mathfrak{R}_{\text{unif}}$ the classes of autoreducible, introreducible, and uniformly introreducible sets, respectively. Lachlan (4) proved that

$$\mathfrak{R}_{\text{intr}} \supset \mathfrak{R}_{\text{unif}}.$$

It is not hard to show that

$$\mathfrak{R}_{\text{aut}} \supset \mathfrak{R}_{\text{unif}}, \qquad \mathfrak{R}_{\text{intr}} \not\supset \mathfrak{R}_{\text{aut}}.$$

The following question remains open: $\mathfrak{R}_{\text{aut}} \supset \mathfrak{R}_{\text{intr}}$?

Institute of Mathematics
Siberian Branch of the Academy of Sciences of the USSR
Novosibirsk

Received
11 XII 1969

CITED LITERATURE

1. H. Rogers Jr., *Theory of Recursive Functions and Effective Computability*, 1967.

2. A. N. Kolmogorov, *Indian J. Statistics*, Ser. A, 25, No. 4, 369 (1963).

3. D. W. Loveland, *Trans. Am. Math. Soc.*, 125, No. 3, 497 (1966).

4. C. G. Jockusch, *J. Symb. Logic*, 33, No. 4, 521 (1968); RZhMat., 7A72 (1969).

5. B. A. Trakhtenbrot, *Complexity of Algorithms and Computations*, Novosibirsk, 1967.

6. B. A. Trakhtenbrot, *Algebra and Logic*, seminar, 4, no. 5, 79 (1965).

7. Dzh. Khodzhaev, All-Union Conf. on Problems of Theoretical Cybernetics, Abstracts of Reports, Novosibirsk, 1969, p. 111.

Note: Figure translations are in progress. See original paper for figures.