ON COMPUTABILITY ON PROBABILISTIC MACHINES

MATHEMATICS

1969

SovietRxiv

Abstract

Full Text

UDC 51.01:518.5

MATHEMATICS

Ya. M. BARZDIN'

ON COMPUTABILITY ON PROBABILISTIC MACHINES

(Presented by Academician A. N. Kolmogorov on 24 III 1969)

One of the aims of the present paper is to show that, under one formulation not considered in ([1]), probabilistic machines (using, for example, a binary random device with probability $p = 1/2$ of producing 1) can nevertheless do more than deterministic machines. In particular, it will be shown (Theorem 1) that for any set M having an m-universal complement, and for any number $\alpha < 1$, one can choose a probabilistic machine such that, if we set it in operation, then with probability $\geq \alpha$ the following event will occur: the set that it enumerates (this set depends on chance and therefore may turn out differently each time*) will, first, be contained in the set M, and, second, will not be contained in any recursively enumerable subset of the set M. We emphasize that many algorithmically undecidable mass problems can be formulated in the form of the following problem: given a certain set M having an m-universal (or, what is the same, creative) complement, it is required, for any natural number x, to determine whether x belongs to the set M or not (substantively, x denotes the number of an individual problem). In the case of such mass problems, our result may be interpreted as follows: using "coin tossing," with arbitrarily high probability $\alpha < 1$ we can solve an infinite set of individual problems that cannot be solved by any single deterministic method. This shows that, using random devices (for example, "coin tossing"), we can with high probability obtain new truths ("axioms") suitable for solving individual problems of mass problems.

In the second part of the paper an attempt is made to investigate the question of what the application of probabilistic machines can yield in the computation of recursive functions (we note that an analogous question, only in another formulation, is also considered in ([3])).

We proceed to precise formulations. In ([1]) the notion of a p-machine was introduced. Without loss of generality, by a p-machine we shall understand a Turing machine that has input and output channels using, respectively, the alphabets $\{0, 1\}$ and $\{0, 1, \Lambda\}$, and that is characterized by the fact that a binary random device with probability p of producing 1 is connected to its input channel (i.e., at each step the machine receives through the input channel either 0 or 1, the probability of the appearance of 1 being p, and at each step it outputs through

the output channel either 0, or 1, or Λ). If a device that always supplies the same symbol is connected to the input channel of the machine, then we shall call such a machine deterministic. In what follows, unless otherwise stated, we shall assume that the machine begins operation with a blank tape (the initial state of the head is assumed fixed). Let T be some p-machine. If we set it in operation, then through the output channel it will produce some

---

* This is precisely the difference between our formulation and the formulation of ([1]).

output sequence $\tau = (b_1, b_2, b_3, ...)$, $b_i \in \{0, 1, \Lambda\}$, depending, generally speaking, on the random sequence that the machine obtains from the random device. With each such sequence τ we shall associate a set $\mathcal{T}$ of natural numbers, of which we shall say that the machine enumerates it. For definiteness we shall assume that $x \in \mathcal{T}$ if and only if τ contains the binary notation for the number x, separated on the left and on the right by the symbol Λ. Thus, if we run a p-machine once, it will enumerate one set; if we run it another time, it will enumerate, generally speaking, another set, and so on. By a statement of the form "the p-machine T enumerates with probability α a set having property A," we shall mean the following: if we run the machine T, then with probability α an event will occur consisting in the fact that the set that the machine T enumerates (generally speaking, in operation to infinity) will have property A.

Theorem 1. *Let $0 < p < 1$. For any set M having an m-universal complement, and for any $\alpha < 1$, there exists a p-machine that with probability $\geq \alpha$ enumerates an infinite subset of the set M that is not contained in any recursively enumerable subset of the set M.*

The idea of the proof of Theorem 1 is as follows. First we construct a sufficiently "sparse" simple set M_0, namely, so "sparse" that, using the random device (it gives us the possibility, for any k, of randomly choosing one of the numbers $1, 2, ..., k$), we could with probability $\geq \alpha$ enumerate an infinite set of natural numbers, none of which belongs to the set M_0. The idea of constructing a "sparse" simple set is the same as the idea of constructing the simple set σ in § 8.3 ([2]), only instead of the function $2x$ (see the definition of the simple set σ in ([2])), one must take a sufficiently rapidly growing function $\varphi(x)$. Now let M be an arbitrary m-universal set and let $h(x)$ be a function that reduces M_0 to M, i.e. $h(M_0) \subset M$ and $h(\overline{M_0}) \subset \overline{M}$. Since M_0 is simple and, consequently, $\overline{M_0}$ is immune, it is not hard to verify that for any infinite set R, if $R \subseteq \overline{M_0}$, then $h(R)$, as well as any extension of $h(R)$ contained in $\overline{M}$, is not recursively enumerable. Therefore the required p-machine T can be defined as a machine consisting of two parts: the first part is a machine that with probability $\geq \alpha$ enumerates an infinite subset $\{x_1, x_2, x_3, ...\}$ of the set $\overline{M_0}$, and the second is a machine that successively computes $h(x_1), h(x_2), h(x_3), ...$ and sends them to the output channel.

Let us now consider, instead of sets having arbitrary m-universal complements,

those sets which have dense universal complements (we call a set densely universal if every recursively enumerable set is densely reducible to it; for the definition of dense reducibility see ([4])). Let $K(R;n)$, as in ([4]), denote the complexity of programs recognizing membership of numbers not exceeding n in the set R. Note that, according to ([4]), if the set M has a densely universal complement, then $K(M;n) \sim \log_2 n$. Using ([4]), one can prove the following refinement of Theorem 1:

Theorem 1′. *Let $0 < p < 1$. For any set M having a densely universal complement, and for any $\alpha < 1$, there exists a p-machine that with probability $\geq \alpha$ enumerates an infinite subset of the set M such that any extension R of it contained in M is not recursively enumerable and has $K(R;n) \approx \log_2 n$.*

Above we considered sets having m-universal complements. The question arises: does Theorem 1 remain valid if one considers sets M having merely recursively enumerable complements (not necessarily m-universal)? A negative answer to this question is given by

Theorem 2. *There exists a set U having a recursively enumerable complement such that for no $\alpha > 0$ does there exist a p-machi-*

with rational p, which with probability $\geq \alpha$ would enumerate an infinite subset of the set U.

Now consider the sets of an arbitrary projective-recursive class Σ_n, $n = 1, 2, 3, ...$ (recall that Σ_1 is the class of recursively enumerable sets, Σ_{n+1} is the class of sets of the form $\exists x_3 \forall x_{k-1} P(x_1, ..., x_k)$, where $P(x_1, ..., x_k) \in \Sigma_n$; for more details see, for example, in (5) the Kleene–Mostowski arithmetical hierarchy). Using the same considerations as above, one can prove an analogue of Theorem 1 in the case of an arbitrary projective-recursive class Σ_n. In a weaker form this analogue can be formulated as follows:

Theorem 3. Let $n \in \{1, 2, 3, ...\}$, $0 < p < 1$, and $\alpha < 1$. There exists a set M_n whose complement is of class Σ_n, and there exists a p-machine T which, with probability $\geq \alpha$, enumerates an infinite subset of the set M_n such that any extension of it contained in M_n does not belong to Σ_n.

Further, one can verify that this theorem can be strengthened in the sense that, for any rational $\alpha < 1$ and any natural n, the set M_n (more precisely, a formula of elementary arithmetic defining the set M_n) and the p-machine T can be constructed effectively. Hence, in particular, it follows that

Theorem 4. Let $0 < p < 1$. For any $\alpha < 1$ there exists a p-machine T which, with probability $\geq \alpha$, enumerates such an infinite set of true statements of elementary arithmetic that is not contained in any projective-recursive set of true statements of elementary arithmetic.

Now consider the computation of functions on deterministic machines and on p-machines. We shall naturally make precise the notion "the machine T transforms x into y" : this means that if we write x on the tape of the machine T and

start it, then after it stops y will be written on the tape. Let the machine T be a p-machine and let ξ be a random variable equal to the infinite sequence of zeros and ones produced by the random device of the machine T. Then the quantity into which the machine T transforms the number x is a random variable depending on ξ; denote it by $T_\xi(x)$. By $T^*_\xi(x)$ denote the number of steps used by the machine T in transforming x. In the case of a deterministic machine, instead of $T_\xi(x)$ and $T^*_\xi(x)$ we shall write $T_0(x)$ and $T^*_0(x)$; it is natural to call $T^*_0(x)$ the time signaling function of the machine T. Denote by $\exists^\infty x\, P(x)$ the assertion "there exist infinitely many values x for which $P(x)$." From Corollary 2 of Theorem 1 of the paper (6) it follows directly that

Theorem 5. Let $0 < p < 1$. Whatever general recursive function $g(x)$ we take, there exists a general recursive predicate $\Gamma(x)$ having the following properties:

1) for any deterministic machine T

$$\neg[\forall x\,(T_0(x) = \Gamma(x))\ \&\ \exists^\infty x\,(T^*_0(x) \leq g(x))];$$

2) for any $\alpha < 1$ there exists a p-machine T such that

$$P\{\forall x\,(T_\xi(x) = \Gamma(x))\ \&\ \exists^\infty x\,(T^*_\xi(x) \leq g(x))\} \geq \alpha.$$

We note that a special case of this theorem (if the second requirement is omitted) is Rabin' s theorem (see (7) or (8)).

The question arises: is there an analogue of Rabin' s theorem in the case of p-machines? A positive answer to this question is given by

Theorem 6. Whatever general recursive function $g(x)$ we take, there exists a general recursive predicate $\Gamma(x)$ such that, for any $\alpha > 0$ and any p-machine T with rational p,

$$P\{\forall x\,(T_\xi(x) = \Gamma(x))\ \&\ \exists^\infty x\,(T^*_\xi(x) \leq g(x))\} < \alpha.$$

The author expresses gratitude to B. A. Trakhtenbrot for valuable advice, as a result of which the proofs of Theorems 1 and 5 were considerably simplified.

Computing Center
of the Latvian State University
named after P. Stuchka
Riga

Received
5 I 1969

REFERENCES

[1] K. Leu, E. Moore et al., *Collection: Automata*, IL, 1956, p. 242. [2] A. I. Mal' tsev, *Algorithms and Recursive Functions*, "Nauka," 1965. [3] B. A. Trakhtenbrot,

Algebra and Logic, Seminar, 2, No. 1, 25 (1963). [4] Ya. M. Barzdin, DAN, 182, No. 6, 1249 (1968). [5] H. Rogers, *Theory of Recursive Functions and Effective Computability*, N. Y., 1967. [6] B. A. Trakhtenbrot, *Algebra and Logic*, Seminar, 4, No. 5, 81 (1965). [7] M. O. Rabin, Bull. Res. Council Israel. F. 8, No. 1, 69 (1959). [8] S. G. Matveeva, *Siberian Mathematical Journal*, 6, No. 3, 546 (1965).

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