ON ONE METHOD OF PROVING THE UNSOLVABILITY OF ALGORITHMIC PROBLEMS

MATHEMATICS

1969

SovietRxiv

Abstract

Full Text

UDC 51.01:518.5

MATHEMATICS

Yu. T. MEDVEDEV

ON ONE METHOD OF PROVING THE UNSOLVABILITY OF ALGORITHMIC PROBLEMS

(Presented by Academician A. N. Kolmogorov, 29 VIII 1968)

§ 1. To every predicate $P(t,x)$ over the domain of natural numbers one can associate the following algorithmic problem: to construct a general recursive function $f(t)$ such that $P(t,f(t))$ holds for all t. Problems of this kind will be called **parametric**. If the assertion $P(t_0,x_0)$ is true, then we shall say that x_0 is a **solution** of our problem **for the given value** $t=t_0$ of the parameter.

Many algorithmic problems admit a natural representation in parametric form. Among them are, for example, the problems of solvability and separation of sets, the problem of extension of functions, and the problem of realizability for formulas of the calculus of statements and formulas of the predicate calculus. A parametric problem determined by the predicate $P(t,x)$ (we shall denote it by P) will be called **effectively refutable** if, for every partial recursive function $f(t)$, one can effectively (i.e., by means of a general recursive function) indicate such a t_0 that, if $f(t)$ is defined for $t=t_0$, then $f(t_0)$ is not a solution of P for $t=t_0$. Obviously, effective refutability is a stronger property than simple unsolvability. In particular, effective refutability of the problem of solvability and separation for recursively enumerable sets is equivalent to the property of creativity and, correspondingly, effective inseparability.

In § 2 of the present paper a convenient criterion for effective refutability is established (Theorem 1), and certain operations on parametric problems are considered. An application of these results to the proof of nonrealizability of certain formulas of the calculus of statements is indicated. In § 3 an application is given to the notion of solvability of a composite finite problem. This section is also of independent significance, since it contains a certain refinement of the notion of a finite problem (1).

§ 2. We shall use a system of definition of partial recursive functions in which there exists the notion of a nullary function (as, for example, in the system using the schemes of primitive recursion and Kleene' s μ-operator). Every nullary partial recursive function will be called a **quasinumber**. Consequently, for every quasinumber one can speak of its being defined, and also, if it is defined, of its value. Substitution of a concrete number into a unary partial recursive function gives a certain quasinumber (it is defined simultaneously with the corresponding value of the given function and, in the case of definedness, has this same value). Just as in the case of ordinary functions, for quasinumbers there exists a universal partial recursive function $U(\tilde{x})$, where $\tilde{x}$ plays the role of the Gödel number of a quasinumber. If the quasinumber with number $\tilde{x}$ is defined, then its value will be denoted by x. In our exposition, expressions of the type "the quasinumber with number $\tilde{x}$" are sometimes replaced, for simplicity, by "the quasinumber $\tilde{x}$."

Theorem 1 (criterion of effective refutability). *In order that the parametric problem P be effectively refutable, it is neces-*

visible and sufficient that for each natural number $\tilde{x}$ one could effectively specify such a $t = \tau(\tilde{x})$ that the assertion holds: if the quasinumber $\tilde{x}$ is defined, then not $P(t, x)$.

We shall restrict ourselves to proving the sufficiency of the condition of the theorem. In order to distinguish functions from their values, in what follows we shall use λ-notations (see (2)).

Lemma 1. For every partial recursive function $\lambda z h(z)$ there exists a general recursive function $\lambda z \nu(z)$ such that, for every z, the number $\nu(z)$ is the number of the quasinumber $h(z)$.

Proof of the sufficiency of the condition of the theorem. Let $\lambda\tilde{x}\tau(\tilde{x})$ be a unary general recursive function satisfying the condition of Theorem 1 with respect to $P(t, x)$, and let $\lambda t f(t)$ be an arbitrary unary partial recursive function. Consider a function $\lambda z \lambda y V(z, y)$, universal for unary partial recursive functions, and denote by e the number that is the number of the partial recursive function $\lambda z f(\tau(\nu(z)))$, where $\lambda z \nu(z)$ is the function from Lemma 1, constructed for $h = \lambda z V(z, z)$. By virtue of the universality of V, for every natural z we have $f(\tau(\nu(z))) \simeq V(e, z)$ (the sign of conditional equality $\simeq$ refers in this case to nullary functions, i.e. to quasinumbers).

Let $t_0 = \tau(\nu(e))$. Suppose that f is defined at $t = t_0$ and that $P(t_0, f(t_0))$ is true; then $f(t_0) = f(\tau(\nu(e)))$ is defined, and, in accordance with the preceding, we have $f(\tau(\nu(e))) = V(e, e)$. Therefore $P(t_0, V(e, e))$, i.e. $P(\tau(\nu(e)), V(e, e))$. This contradicts the properties of the functions τ and ν. Consequently, if f is defined at $t = t_0$, then not $P(t_0, f(t_0))$. Thus everything has been proved, since t_0 is constructed effectively from the number of f.

The concept of effective refutability and Theorem 1 suggest introducing the following definitions. A **strong effective refutation** of a parametric problem $P(t, x)$ is a parametric problem $\sim P(t^*, x^*)$, where the predicate $\sim P(t^*, x^*)$, for any fixed t_0^*, x_0^*, is true if and only if t_0^* is the number of such a partial recursive function $\lambda t f(t)$ for which the assertion is true: if f is defined at $t = x_0^*$, then it is false that $P(x_0^*, f(x_0^*))$. A **weak effective refutation** for $P(t, x)$ is a parametric problem $-P(t^{**}, x^{**})$, where, for given t_0^{**}, x_0^{**}, the assertion $-P(t_0^{**}, x_0^{**})$ is true if and only if t_0^{**} is the number of such a quasinumber $\tilde{x}_0$ that, if $\tilde{x}_0$ is defined, then it is false that $P(x_0^{**}, x_0)$. Obviously, effective refutability of the problem P is equivalent to solvability of the problem $\sim P$. From Theorem 1 it follows that solvability of $\sim P$ is equivalent to solvability of $-P$.

For parametric problems P and Q one can introduce various definitions of reducibility of Q to P, and also define operations of reducing Q to P. In the present note we shall restrict ourselves, bearing in mind the application to realizability, to the simplest definition of a reduction operation. The operation $\supset_1$, which may be called the operation of reduction with respect to the corresponding parameter, assigns to the problems $P = P(t, x)$ and $Q = Q(t, y)$ the problem $R = P \supset_1 Q$, $R = R(t, z)$, where, for each t_0, z_0, the assertion $R(t_0, z_0)$ is true if and only if z_0 is the number of such a partial recursive function $r = \lambda x r(x)$ that, for all x_0, if $P(t_0, x_0)$, then r is defined at $x = x_0$ and $Q(t_0, r(x_0))$.

Lemma 2. For effective refutability of the problem $P \supset_1 Q$ it is sufficient that the following condition be fulfilled: for each quasinumber $\tilde{y}$ one can effectively construct such an ordered pair of numbers $\langle t, x \rangle$ that $P(t, x)$ is true and, if $\tilde{y}$ is defined, then not $Q(t, y)$.

We now pass to the question of the realizability of formulas of the propositional calculus. To each propositional formula $\Phi(a_1, \dots, a_m)$, constructed from the variables $a_1, \dots, a_m$ by means of the connectives $\&, \vee, \neg$ and $\supset$, we assign a parametric problem (the realization problem) $P_\Phi(t, x)$, where $P_\Phi(t_0, x_0)$ is true if and only if the condition is fulfilled: t_0 is

number of such an ordered system $S = \langle \varphi_1, \dots, \varphi_m \rangle$ of closed logico-arithmetical formulas for which x_0 realizes the result of substituting the system S into Φ, i.e., $x_0 r \Phi(\varphi_1, \dots, \varphi_m)$. By the definition of realizability of propositional formulas, the realizability of Φ is equivalent to the solvability of the problem P_Φ. Determining the question of realizability of concrete formulas Φ encounters great difficulties even in the case of formulas depending on one variable. The most nontrivial case of this kind was considered by V. A. Yankov (3), who proved that the formula

$$((\neg\neg a \supset a) \supset (\neg a \vee \neg\neg a)) \supset (\neg a \vee \neg\neg a)$$

is not realizable. It is known that every formula in one variable which is not intuitionistically derivable is intuitionistically equivalent to one of the formulas of the following recurrent sequence (4):

$$\Psi_0 = a \& \neg a, \quad \Psi_1 = a, \quad \Psi_2 = \neg a, \quad \Psi_3 = \neg a \vee a, \quad \Psi_{2n+1} = \Psi_{2n} \vee \Psi_{2n-2}, \quad \Psi_{2n+2} = \Psi_{2n} \supset \Psi_{2n-3} \quad \text{for } n > 1.$$

The formula of V. A. Yankov cited above coincides with Ψ_{10}. From V. A. Yankov' s result, as well as the results of Rose (5), F. L. Varnakhovskii (6), and M. M. Kipnis (7), it follows that the formulas Ψ_{11}, Ψ_{12}, and Ψ_{13} are also not realizable. With the aid of our method, using in particular Lemma 2, one can prove the following assertion.

Theorem 2. *For each of the formulas Ψ_k, with k from 0 to 15 inclusive, the corresponding realizability problem is effectively refutable.*

We note that in the proof of Theorem 2 one uses, for substitution into Φ_k ($0 \leq k \leq 15$), only such closed arithmetical formulas as have the form

$$\varphi = \exists z_1 \forall z_2 A(z_1, z_2),$$

where A expresses a primitive-recursive predicate.

§ 3. In the present section we investigate a certain refinement of the notion of a finitary problem (^{1}). First let us recall and somewhat refine the basic definitions. A finitary problem A is an ordered pair $\langle A^0, A^+\rangle$, the first element A^0 of which is a nonempty finite set, and the second element A^+ is a subset of the first: $A^+ \subseteq A^0$. By a finite set here we mean a finitary set in the sense of A. A. Markov, i.e., a set specified by a completed list of words in some alphabet. The set $A^+ \subseteq A^0$ (called the set of solutions of the problem A) is in general specified by means of some condition on the elements of the set A^0 (which is called the set of admissible possibilities of the problem A). Logical operations on finitary problems are defined as in (^{1}). Each propositional formula $\Phi(z_1, \dots, z_m)$ can be interpreted as a compound finitary problem, which is a function of the "variable" problems $A_1, \dots, A_m$ substituted into Φ in place of $z_1, \dots, z_m$. Fix some ordered system $S = \langle F_1, \dots, F_m\rangle$ of nonempty finitary sets. By a system of problems on S we shall mean any ordered system H of finitary problems $H = \langle A_1, \dots, A_m\rangle$ for which $A_k^0 = F_k$ for all $k = 1, \dots, m$. From the definition of the operations on problems it follows that the set of admissible possibilities for the problem

$$A_H = \Phi(A_1, \dots, A_m)$$

depends only on S. Therefore (since S is fixed), instead of A_H^0 we shall write A^0. If the intersection of all A_H^+ is nonempty, for those H on S for which $A_1^+, \dots, A_m^+$ are finitary sets, then the formula Φ is called solvable on S. Let r belong to the intersection of all such A_H^+. Classically, the solvability of Φ on S means that $r \in A_H^+$ for any H on S. Under what conditions is this assertion true constructively? Obviously, one must impose some restriction on the class of finitary problems; this is done, in particular, below.

A finitary problem A is called **deductive** if one of the assertions is true: (1) the set A^+ is recursively enumerable (^{2}); (2) the complement of the set A^+ is recursively enumerable; (3) the set A^+ is recursive. Depending on which of these conditions holds, A is called a deductive problem of type 1, 2, or type 3. An ordered system $H = \langle A_1, \dots, A_m\rangle$ of problems on S will be called a **deductive system of problems on** S, if all A_k are deductive. By the number of a deductive sys-

we shall call the number of an ordered system $\langle \alpha_1, \dots, \alpha_m\rangle$, where α_k is the number of the pair $\langle i_k, n_k\rangle$, with n_k the number of the set A_k^+, and i_k the type of A_k (a number equal to 1, 2, or 3), the number of the deductive system H.

Theorem 3. If the propositional formula $\Phi(z_1, \ldots, z_m)$ is solvable on S, then there exists an $r \in A_0$ such that, for any deductive system H of problems on S, $r \in A_H^+$.

The formula Φ and the system S define, in the following way, a parametric problem in the sense of § 1 of the present paper. The parameter of this problem is the number of an arbitrary deductive system H of finite problems on S, and the solution corresponding to this parameter is the number of such an $r \in A_0$ that $r \in A_H^+$. We denote this parametric problem by $P[\Phi, S]$. With the aid of Theorem 1 the following result is established.

Theorem 4. If the formula Φ is not solvable on the system S, then the parametric problem $P[\Phi, S]$ is effectively refutable.

Steklov Mathematical Institute
Academy of Sciences of the USSR

Received
20 VIII 1968

CITED LITERATURE

1. Yu. T. Medvedev, DAN, 142, No. 5, 1015 (1962).
2. S. K. Kleene, *Introduction to Metamathematics*, Moscow, 1957.
3. V. A. Yankov, DAN, 151, No. 5, 1035 (1963).
4. I. Nishimura, J. Symb. Logic, 25, 327 (1962).
5. G. F. Rose, Trans. Am. Math. Soc., 75, 1 (1953).
6. F. L. Varshavskii, DAN, 161, No. 6, 1257 (1965).
7. M. M. Kinnis, DAN, 174, No. 2, 277 (1967).

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

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.