ON THE COMPLEXITY OF ALGORITHMS CONNECTED WITH THE REALIZATION OF LOGICO-ARITHMETICAL AND PROPOSITIONAL FORMULAS

MATHEMATICS

1970

SovietRxiv

Abstract

Full Text

UDC 517.11

MATHEMATICS

V. I. KHOMICH

ON THE COMPLEXITY OF ALGORITHMS CONNECTED WITH THE REALIZATION OF LOGICO-ARITHMETICAL AND PROPOSITIONAL FORMULAS

(Presented by Academician P. S. Novikov on 9 IX 1969)

The paper establishes estimates for the complexity of algorithms recognizing the realizability of closed logico-arithmetical formulas of bounded length, and also of algorithms that boundedly realize certain propositional formulas, i.e., such algorithms which transform every set of closed logico-arithmetical formulas of bounded length into a number realizing the result of substituting this set into the propositional formula under consideration in place of its variables.

1. We shall use the terminology and notions introduced in papers ([1–6]), in particular the notion of the length of a word P (notation $[P^0]$) and the notion of the representation of a normal algorithm $\mathfrak{A}$ (notation $\mathfrak{A}^u$). By the complexity of a normal algorithm $\mathfrak{A}$ we shall mean the length of its representation, i.e. $[\mathfrak{A}^u]$ (notation $\mathfrak{A}_\zeta$). By the quasi-feasibility of an object with given properties we shall mean the possibility of deriving a contradiction from the assumption of its infeasibility. The alphabet of logico-arithmetical formulas (notation A) shall be the following list of elementary signs:

$$\& \vee \supset \neg \forall \exists 0' + \times ( ) t = .$$

The standard two-letter extension of the alphabet A will be denoted by the symbol A^+. By a logico-arithmetical formula we shall mean a formula of formal arithmetic, defined in ([2]), assuming that a variable is a word of the form $(t \dots t)$ (see ([3]), p. 27). We use the notion of realization of a logico-arithmetical formula introduced in ([5]).

2. Let $\mathfrak{A}$ be a normal algorithm over A, and let n be a natural number. We shall say that the **algorithm $\mathfrak{A}$ n-recognizes the realizability (nonrealizability) of closed logico-arithmetical formulas** if, for any closed

logico-arithmetical formula F such that $[F^0] \leq n$: a) the algorithm $\mathfrak{A}$ is applicable to F; b) F is realizable (nonrealizable) if and only if $\mathfrak{A}(F) \doteq \Lambda$.

Theorem 1. *There exist natural numbers C_1, C_2, and C_3 such that, for any natural number n and any normal algorithm $\mathfrak{A}$ in the alphabet A^+, if $\mathfrak{A}$ n-recognizes the nonrealizability of closed logico-arithmetical formulas, then*

$$\mathfrak{A}_\zeta \geq \frac{1}{C_1} \cdot 2^{\sqrt{n}/C_2} - C_3.$$

The proof of Theorem 1 is based on the following two lemmas.

Lemma 1. *One can construct a logico-arithmetical formula $F(x)$ with a single parameter x such that there exist natural numbers C_1 and C_2 such that, for any natural number n and any normal algorithm $\mathfrak{A}$ in the alphabet $0'abc$, if $\mathfrak{A}$ recognizes the nonrealizability of $F(m)$ for all natural numbers m such that $m \leq n$, then $\mathfrak{A}_\zeta \geq n/C_1 - C_2$.*

The formula $F(x)$ is constructed with the aid of the predicate μ, constructed by N. V. Petri (see ([7]), p. 37).

Lemma 2. *For any natural number n such that $n > 0$, one can construct a constant term T_n such that $z(T_n) = n$ and $[T_n^0] \leq 7([\log_2 n] + 1)^2$. (Here $z(T_n)$ denotes the value of the constant term T_n.)*

From Theorem 1 it is easy to obtain

Theorem 2. *There exist natural numbers C_1, C_2, and C_3 such that, for every natural number n and every normal algorithm $\mathfrak{A}$ in the alphabet A^+, if $\mathfrak{A}$ n-recognizes the realizability of closed logical-arithmetical formulas, then*

$$\mathfrak{A} \ \geq \ \frac{1}{C_1} \cdot 2^{\sqrt{n}/C_2} - C_3.$$

Theorem 2 gives a lower bound for the complexity of n-recognizing the realizability of closed logical-arithmetical formulas. From cardinality considerations the following upper bound may be obtained.

Theorem 3. *There exists a natural number C such that, for every natural number n, there quasi-exists a normal algorithm $\mathfrak{A}$ in the alphabet A^+ which n-recognizes the realizability of closed logical-arithmetical formulas and is such that*

$$\mathfrak{A} \ \leq \ {}^{14}/_{13} \cdot 14^n + C.$$

3. In what follows let p denote a propositional variable. Let G be a propositional formula in one variable p, and let n be a natural number. We shall say that a normal algorithm $\mathfrak{A}$ over the alphabet A n**-realizes the**

formula G if, for every closed logical-arithmetical formula H such that $[H^\circ] \leq n$: a) the algorithm $\mathfrak{A}$ is applicable to H; b) $\mathfrak{A}(H)$ realizes $G(H)$.

Let G be a propositional formula in one variable p. We shall say that the formula G **has no upper bound for the complexity of realizability** if, for every general recursive function f, there exists a natural number N such that, for every natural number m such that $m \geq N$, and every normal algorithm $\mathfrak{A}$ in the alphabet A^+ that m-realizes G, one has $\mathfrak{A} \geq f(m)$.

Consider the propositional formulas $\neg\neg p \supset p$, $p \vee \neg p$, $(\neg p \supset p) \supset p^*$. For each of these formulas it is true that, for every natural number n, there quasi-exists a normal algorithm n-realizing it. The following assertions hold, however.

Theorem 4. *The propositional formula $\neg\neg p \supset p$ has no upper bound for the complexity of realizability.*

Theorem 5. *Let F and G be propositional formulas in one variable p such that $F \vdash G$ in the intuitionistic propositional calculus, and suppose G has no upper bound for the complexity of realizability. Then F also has no upper bound for the complexity of realizability.*

From Theorems 4 and 5 one can obtain:

Corollary 1. *The propositional formulas $p \vee \neg p$, $(\neg p \supset p) \supset p$ have no upper bound for the complexity of realizability.*

Corollary 2. *The propositional formula $F \supset (\neg\neg p \supset p)$, where F is a formula in one variable p derivable in the intuitionistic propositional calculus, has no upper bound for the complexity of realizability.*

4. It is known that the formula $(p \vee \neg p) \supset (\neg\neg p \supset p)$ is derivable in the intuitionistic propositional calculus and, consequently, by Nelson’ s theorem is realizable. However, the following theorem holds.

Theorem 6. *There exist natural numbers C_1, C_2, and C_3 such that, for every natural number n and every normal algorithm $\mathfrak{A}$ in the alphabet A^+, if $\mathfrak{A}$ n-realizes the propositional formula $(\neg\neg p \supset p) \supset (p \vee \neg p)$, then*

$$\mathfrak{A} \geq \frac{1}{C_1} \cdot 2^{\sqrt{n}/C_2} - C_3.$$

This theorem, which may be obtained from Theorem 1, gives a lower bound for the complexity of realizability of the propositional formula $(\neg\neg p \supset p) \supset (p \vee \neg p)$. From cardinality considerations the following upper bound may be obtained.

Theorem 7. *There exists a natural number C such that, for every natural number n, there quasi-exists a normal algorithm $\mathfrak{A}$ in the alpha-*

* Here and below we use the generally accepted rules for omitting parentheses when writing propositional formulas.

where A^+ is such that $\mathfrak{A}$ n-realizes the propositional formula $(\neg\neg p \supset p) \supset (p \vee \neg p)$, and $\mathfrak{A}_3 \leq {}^{14}/_{13} \cdot 14^n + C$.

Analogous results hold for the "weakened" law of excluded middle:

Theorem 8. There exist natural numbers C_1, C_2, and C_3 such that, for any natural number n and any normal algorithm $\mathfrak{A}$ in the alphabet A^+, if $\mathfrak{A}$ n-realizes the propositional formula $\neg p \vee \neg\neg p$, then

$$\mathfrak{A}_3 \geq \frac{1}{C_1} \cdot 2^{\sqrt{n}/C_2} - C_3.$$

Theorem 9. There exists a natural number C such that, for any natural number n, there quasi-exists a normal algorithm $\mathfrak{A}$ in the alphabet A^+ such that $\mathfrak{A}$ n-realizes the propositional formula $\neg p \vee \neg\neg p$, and $\mathfrak{A}_3 \leq {}^{14}/_{13} \cdot 14^n + C$.

Theorems 8 and 9 and Corollary 1 show the relationship between the complexities of realizing the formulas $p \vee \neg p$ and $\neg p \vee \neg\neg p$.

The author expresses deep gratitude to N. M. Nagorny for his advice.

Moscow State University
named after M. V. Lomonosov

Received
4 IX 1969

CITED LITERATURE

[1] A. A. Markov, *Tr. Mat. inst. im. V. A. Steklova AN SSSR*, **42** (1954).
[2] S. K. Kleene, *Introduction to Metamathematics*, Moscow, 1957.
[3] N. A. Shanin, *Tr. Matem. inst. im. V. A. Steklova AN SSSR*, **43** (1955).
[4] A. A. Markov, *Izv. AN SSSR, ser. matem.*, **31**, No. 1, 161 (1967).
[5] S. C. Kleene, *J. Symbolic Logic*, **10**, 109 (1945).
[6] G. F. Rose, *Trans. Am. Math. Soc.*, **75**, 1 (1953).
[7] N. V. Petri, *DAN*, **185**, No. 1, 37 (1969).

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