A. Karatsuba and Yu. Ofman

1962

SovietRxiv

Abstract

Full Text

CYBERNETICS AND CONTROL THEORY

A. Karatsuba and Yu. Ofman

MULTIPLICATION OF MULTI-DIGIT NUMBERS ON AUTOMATA

(Presented by Academician A. N. Kolmogorov, 13 II 1962)

One of the aims of the present note, as also of the previously published note by Yu. Ofman ([1]), whose notation and definitions are also used here, is to consider the problem of finding lower estimates for the algorithmic complexity of discrete functions. As yet there are no nontrivial lower estimates. It is quite probable that a theory is possible which, by a single method, will estimate from below the number of operations on digits in the multiplication of multi-digit numbers and the number of operations on numbers in solving systems of linear equations, etc.

Two m-digit binary numbers are placed at the input of a binary automaton (an input of $k = 2m$ elements). At the output, from $2m + 1$ elements, the binary representation of the product must be obtained. For the function $y = d_s(x)$ thus defined, lower estimates for the complexity of the binary automata realizing it are obtained elementarily:

$$N_0 \succcurlyeq m, \qquad T_0 \succcurlyeq \log_2 m.$$

We next give the scheme of proof of two theorems.

Theorem 1 (Ofman). *For any s, $1 \leq s \leq m$, the function d_s can be realized by a binary automaton with characteristics which, as $m \to \infty$ (uniformly in s within the indicated limits), have the characteristics*

$$N \preccurlyeq \frac{m^2}{3}, \quad T \preccurlyeq s \log_2 m.$$

For $s = 1$ we obtain an automaton with characteristics

$$N \preccurlyeq m^2 \quad T \preccurlyeq \log_2 m, \tag{1}$$

for $s = m$, with characteristics

$$N \preccurlyeq m, \qquad T \preccurlyeq m \log m. \tag{2}$$

Theorem 2 (Karatsuba). *The function d_s can be realized by a binary automaton with characteristics*

$$N \preccurlyeq m^{\log_2 3}, \qquad T \preccurlyeq \log^2 m.$$

The authors of the note have not succeeded in advancing beyond these results. Obviously, N_0 and T_0 satisfy the estimates

$$N_0 \preccurlyeq m, \qquad T_0 \preccurlyeq \log_2 m,$$

but it is not known whether such orders of growth of N and T can be combined with one another.

The usual school method of multiplication, modified only in that the products of the multiplicand by each digit of the multiplier are obtained in parallel and added by automaton 3, leads to the estimates (1). If, however, one forms the products of the multiplicand by the separate digits of the multiplier successively and adds them to the accumulated sum of previously formed pro-

products, repeatedly using the automaton for addition from Theorem 2 of [1], then one can arrive at estimate (2). An auxiliary device which successively feeds new and new products into the adder is constructed without great difficulty within the requirements of the estimates (2).

To obtain the automaton whose existence is asserted in Theorem 1, the multiplier is divided into groups of digits, with s digits in each group. Multiplication by the digits of the multiplier from one digit group is performed sequentially, and the addition of the results of multiplication by each digit group is performed in parallel.

For the proof of Theorem 2, let us note that multiplication can be replaced by addition and squaring: $ab = \frac{1}{4}[(a+b)^2 - (a-b)^2]$. Division by four presents no great difficulty in the binary system. Thus, it suffices to estimate the orders of growth of N and T for the function $y = d_6(x)$, corresponding to the squaring of a $2m$-digit binary number

$$(x, x_2, \dots, x_{2m}) = x_1 2^{2m-1} + x_2 2^{2m-2} + \dots + x_{2m}.$$

The formula

$$(x_1 x_2 \dots x_{2m})^2 = 2^{m-4}\big[(x_1 x_2 \dots x_m) + (x_{m+1} \dots x_{2m})\big]^2 +$$

$$+(2^{2m} - 2^{m-4})(x_1 x_2 \dots x_m)^2 + (1 - 2^{m-4})(x_{m+1} x_{m+2} \dots x_{2m})^2$$

shows that the squaring of a $2m$-digit number is reduced to three squarings of m-digit numbers* and to operations (addition, multiplication by powers of two), whose execution can be carried out quite economically, using the methods indicated in [1].

Lemma. If the squaring of an r-digit number can be performed by an automaton with $N = N_r,\ T = T_r$, then for the squaring of a 2^{r+1}-digit number one can construct an automaton with $N = N_{r+1} = 3N_r + c \cdot 2^r,\ T = T_{r+1} = T_r + c_1 \cdot r$.

With the aid of the lemma, the inductive proof of Theorem 2 is easily carried out.

For representations by automata without feedback (superpositions), Theorem 2 and the special case of Theorem 1 corresponding to formula (1) are valid.

Received
9 II 1962

CITED LITERATURE

1. Yu. Ofman, DAN, **145**, No. 1 (1962).

---

* The sum $(x_1x_2 \ldots x_m)+(x_{m+1} \ldots x_{2m})$ may have $m+1$ digits, but the reduction of the squaring of an $(m+1)$-digit number to the squaring of an m-digit number is done by means of the formula $(2a + b)^2 = 4a^2 + 4ab + b^2$, where $b = 0, 1$.

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