CYBERNETICS AND CONTROL THEORY

MULTIPLICATION OF MULTIDIGIT NUMBERS ON AUTOMATA

A. Karatsuba and Yu. Ofman

(Presented by Academician A. N. Kolmogorov, February 13, 1962)
Translated from Doklady Akademii Nauk SSSR, Vol. 145, No. 2,
pp. 293-294, July, 1962
Original article submitted February 9, 1962

One of the problems studied in this paper, just as in the previously published paper by Yu. Ofman [1], whose notation and definitions are used here, is the problem of finding the lower estimates of the algorithmic complexity of discrete functions. So far no nontrivial lower estimates exist. It is very probable that a theory is possible for the number of operations on digits for multiplication of multidigit numbers and the number of operations performed on the numbers in solving systems of linear equations, etc.

Two m-digit binary numbers are applied to the input of a binary automaton (an input consisting of $k = 2m$ sections). At the output from the $2m + 1$ sections we must obtain the binary recording of the product. For the function $y = d_5(x)$ defined in this manner we obtain the lower estimates of the complexity of the binary automatons which realize them in elementary fashion: $N_0 \geq m$, $T_0 \geq \log_2 m$.

Below we present the scheme for proving two theorems.

Theorem 1 (Ofman). For any s, $1 \leq s \leq m$, the function d_5 can be realized by a binary automaton with characteristics that have the following characteristics for $m \to \infty$ (uniformly with respect to s within the indicated limits):

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

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

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

and for $s = m$ we obtain an automaton with the characteristics

$$N \asymp m, \quad T \asymp m \log m. \tag{2}$$

Theorem 2 (Karatsuba). The function d_5 can be realized by means of a binary automaton with the characteristics

$$N \asymp m^{\log_2 3}, \quad T \asymp \log^2 m.$$

The authors of this paper could not advance further than these results. It is obvious that N_0 and T_0 satisfy the estimates

$$N_0 \asymp m, \quad T_0 \asymp \log_2 m,$$

but it is not known whether such orders of growth for N and T can be connected to each other.

The conventional multiplication method (modified only in the sense that the product of the multiplicand by each place in the multiplier are obtained in parallel and added by the automaton 3) leads to the estimates (1). However, if we form the products of the multiplicand by the individual digits of the multiplier in sequence and add them to the accumulated sum of previously formed products, then it is possible to arrive at the estimate (2) by repeated use of the automaton for addition described in Theorem 2 of [1]. The auxiliary device which successively introduces new products into the adder is designed without great difficulty within the confines of the requirements posed by the estimates (2).

In order to obtain the automaton whose existence is postulated in Theorem 1 the multiplier is subdivided into groups of places with s places in each group. Multiplication by the digits of a multiplier from one group of places is performed in sequence, and the addition of the results obtained via multiplication by each group of places is performed in parallel.

In order to prove Theorem 2 we note that multiplication can be replaced by addition and squaring: $ab = \frac{1}{4}[(a + b)^2 - (a - b)^2]$. Division by four does not present great difficulties in the binary number system. Thus it is sufficient to estimate the orders of growth of N and T for the function $y = d_6(x)$ that corresponds to squaring a $2m$-digit binary number:

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

The formula

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

demonstrates that squaring a 2m-digit number reduces to three squaring operations performed on m-digit numbers* and operations (addition, multiplication by a power of two), whose realization can be achieved very economically if we use the devices indicated in [1].

Lemma. If squaring an r-digit number can be achieved by an automaton with $N = N_r$, $T = T_r$, then in order to square a 2^{r+1}-digit number it is possible to design an automaton with $N = N_{r+1} = 3N_r + c \cdot 2^r$, $T = T_{r+1} = T_r + c_1 \cdot r$.

By means of the lemma it is easy to perform the inductive proof of Theorem 2.

Theorem 2 and the particular case of Theorem 1 corresponding to formula (1) are valid for representations achieved by automata that have no feedback loops (superpositions).

LITERATURE CITED

1. Yu. Ofman, DAN, 145, No. 1 (1962) [Soviet Physics--Doklady, Vol. 7, p. 589].

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