Reports of the Academy of Sciences of the USSR

MATHEMATICS

1963

SovietRxiv

Abstract

Full Text

Reports of the Academy of Sciences of the USSR
1963. Vol. 150, No. 3

MATHEMATICS

A. L. TOOM

ON THE COMPLEXITY OF A CIRCUIT OF FUNCTIONAL ELEMENTS IMPLEMENTING MULTIPLICATION OF INTEGERS

(Presented by Academician P. S. Novikov on 30 I 1963)

1. Introduction. We consider the problem of constructing, in one sense or another, as simple as possible a circuit R_n of functional elements (for the definition see, for example, in ([1])), which, from the binary digits of two integer n-digit numbers M and N, $0 \leqslant M, N < 2^n$, computes all binary digits of their product MN. The complexity of the circuit R_n can be characterized by two parameters: the number of elements $f(R_n)$ and the depth of the circuit $t(R_n)$, i.e. the largest number of elements in a circuit $A_1, \ldots, A_{t(R_n)}$ such that the state of each of them, except the first, directly depends on the state of the preceding one. In content, the depth is the operating time of the circuit, if the operating time of each element is 1. It is assumed that the Boolean functions assigned to the elements of the circuit are taken from some finite basis. The choice of such a basis is arbitrary, since all estimates given below are up to multiplication by a constant.

Let l and m be two functions of the same variables. The fact that there exists a constant c such that $l \leqslant cm$ will be written as follows: $l \prec m$. Let S_n be a circuit which, from the n digits of a number N, $0 \leqslant N < 2^n$, gives the digits of the number N^2. Then the equality

$$MN = \tfrac{1}{4}\left[(M+N)^2 - (M-N)^2\right]$$

indicates a method for constructing a circuit R_n which gives, from the digits of M, N, where $0 \leqslant M, N < 2^n$, the digits of their product MN, and such that

$$f(R_n) \prec f(S_n), \qquad t(R_n) \prec t(S_n).$$

Therefore we shall construct a circuit S_n giving N^2 from N. The words "a circuit from the numbers A_i computes (or gives) the numbers B_j" here and below mean

that this circuit, from the binary digits of the numbers A_i, realizes the binary digits of the numbers B_j.

In ([2]) two constructions of circuits S_n^1 and S_n^2 are given, which compute N^2 from N, and for which, respectively,

$$f(S_n^1) \prec n^2, \qquad t(S_n^1) \prec \lg n,$$

$$f(S_n^2) \prec n^{\log_2 3}, \qquad t(S_n^2) \prec \lg^2 n.$$

In the present work a circuit S_n is constructed for which

$$f(S_n) \prec n^{1+\varepsilon}, \qquad t(S_n) \prec n^{\varepsilon}, \tag{1}$$

where ε is an arbitrary positive constant. More precisely, for sufficiently large c (for example, $c = 2^5$),

$$f(S_n) \prec nc^{\sqrt{\log_2 n}}, \qquad t(S_n) \prec c^{\sqrt{\log_2 n}}.$$

2. Description of the circuit. Let n binary digits of the number N be given:

$$\omega_0\omega_1 \dots \omega_{n-1}, \qquad \sum_{i=0}^{n-2} \omega_i 2^i = N,$$

where ω_i is equal to 0 or 1. Choose two natural numbers q and r so that

$$qr < n \leq q(r+1),$$

and in the case $n < q(r+1)$ put $\omega_n = \omega_{n+1} = \dots = \omega_{q(r+1)-1} = 0$.

Represent N in the form

$$N = \sum_{i=0}^{r} a_i 2^{iq}, \qquad \text{where } a_i = \sum_{j=0}^{q-1} \omega_{iq+j} 2^j.$$

Each a_i is a natural number containing q digits in binary notation. These digits $\omega_{iq} \dots \omega_{(i+1)q-1}$ are digits of the number N or identically zero. Thus, with each number N we have associated $r+1$ numbers: $a_0 \dots a_r$. Now associate with each number N the polynomial of degree r:

$$P(x) = \sum_{i=0}^{r} a_i x^i.$$

Obviously, $N = P(2^q)$, $N^2 = P^2(2^q)$.

Our circuit consists of 4 parts I_n, II_n, III_n, IV_n, whose order of connection is as follows:

$$N \to I_n \to II_n \to III_n \to IV_n \to N^2.$$

Part I_n, using the numbers $a_0, \dots, a_r$, which may be regarded as given, computes the values $P(x)$ for all integers x in the interval $-r \le x \le r$; denote these $2r+1$ numbers by $m_{-r}, \dots, m_r$, i.e.

$$m_i = P(i) \qquad \text{for } -r \le i \le r.$$

Part II_n squares all m_i, thereby obtaining the values of the polynomial $P^2(x)$ at the same points $-r, \dots, r$:

$$m_i^2 = P^2(i) \qquad \text{for } -r \le i \le r.$$

Part III_n, knowing the values of the polynomial $P^2(x)$ of degree $2r$ at $2r+1$ points, computes its coefficients by known formulas.

Part IV_n, knowing the coefficients of $P^2(x)$, computes its value at

$$x = 2^q.$$

Thus, the number $N^2 = P^2(2^q)$ has been obtained.

The method of constructing the circuit is inductive in the sense that parts II_n and III_n include circuits S_k for certain $k < n$ as their component parts.

3. **Estimate of the complexity of the circuit.** This estimate uses results (for proofs see ([3])), formulated here as Lemmas 1 and 2.

Lemma 1. There exists a circuit $T_{a,b}$, over b a-digit numbers $A_1, \dots, A_b$, computing the sum

$$\sum_{i=1}^{b} A_i 2^{k(i)},$$

where all $k(i)$ are integers, such that

$$f(T_{a,b}) < ab, \qquad t(T_{a,b}) < \lg a + \lg b.$$

Lemma 2. There exists a circuit $U_{a,b}$, over two numbers A and B, having a and b digits respectively, producing their product AB, such that

$$f(U_{a,b}) < ab, \qquad t(U_{a,b}) < \lg a + \lg b.$$

Let us describe in detail the computations performed by each part of the circuit, and estimate the complexities of these parts. To simplify the estimates, we shall assume in advance that for $k < n$ estimate (1) is valid and that $q^{1/5} > r > \lg\lg q$.

Part I_n: a) multiplies $\prec r^2$ numbers with $\prec q$ digits by numbers with $\prec r \lg r$ digits; b) computes $\prec r$ sums of $\prec r$ terms with $\prec q$ digits in each; hence $f(I_n) \prec qr^4,\ t(I_n) \prec \lg q$.

Part II_n squares $\prec r$ numbers with $\prec q$ digits; hence $f(II_n) \prec r \cdot f(S_q),\ t(II_n) \prec t(S_q)$.

Part III_n solves a system of linear equations with constant $\prec r \lg r$-digit coefficients, where the free terms m_i^2 have $\prec q$ digits and the solutions are integers. In other words, it: a) computes $\prec r$ linear combinations of $\prec q$-digit numbers m_i^2 with $\prec r^2 \lg r$-digit coefficients; b) divides (exactly) these linear combinations by the determinant of the system; since it is constant, this division can be reduced to multiplying these $\prec q$-digit linear combinations by a number (approximately the reciprocal determinant) with the same number of digits $\prec q$; hence $f(III_n) \prec qr^5 + r \cdot f(S_q),\ t(III_n) \prec \lg q + t(S_q)$.

Part IV_n substitutes $x = 2^q$ into a polynomial in x of degree r with $\prec q$-digit coefficients; hence

$$f(IV_n) \prec qr, \qquad t(IV_n) \prec \lg q.$$

Now let us estimate the complexity of the circuit S_n. Obviously,

$$f(S_n) = f(I_n) + f(II_n) + f(III_n) + f(IV_n),$$

$$t(S_n) \leqslant t(I_n) + t(II_n) + t(III_n) + t(IV_n).$$

Thus we arrive at the formulas

$$f(S_n) \prec r \cdot f(S_q) + qr^5,$$

$$t(S_n) \prec t(S_q) + \lg q,$$

where $qr \leqslant n$.

Putting $r = c_1\sqrt{\lg q}$, we obtain, for a sufficiently large constant c,

$$f(S_n) \prec nc^{\sqrt{\lg n}},$$

$$t(S_n) \prec c^{\sqrt{\lg n}}.$$

Moscow State University
named after M. V. Lomonosov

Received
16 I 1963

CITED LITERATURE

1. O. B. Lupanov, *Problems of Cybernetics*, vol. 7, 1962, p. 61.

2. A. Karatsuba, Yu. Ofman, DAN, 145, No. 2, 293 (1962).

3. Yu. Ofman, DAN, 145, No. 1, 48 (1962).

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