

THE COMPLEXITY OF A SCHEME OF FUNCTIONAL ELEMENTS REALIZING THE MULTIPLICATION OF INTEGERS

A. L. TOOM

1. **Introduction.** The problem to be considered concerns the construction of a scheme R_n , which is the simplest possible in some sense or another, from functional elements (for their definition see, for example, [1]) which if we are given the binary digits of two n -digit integers M and N , $0 \leq M, N < 2^n$, calculates all binary digits of their product MN . The complexity of a scheme in R_n can be characterized by two parameters: the number of elements $f(R_n)$ and the depth of the scheme $t(R_n)$, i. e. the greatest number of elements in the scheme $A_1, \dots, A_{t(R_n)}$ such that the state of each of them, except for the first, depends directly upon the state of the previous one. The depth contains the performance time of the scheme if the performance time of each element is 1. It is to be assumed that the Boolean functions assigned to the elements of the scheme are to be taken from a certain finite basis. The choice of such a basis is arbitrary since all estimates deduced below are given with accuracy up to multiplication by a constant.

Let l and m be two functions of one and the same variable. The fact that there exists a constant c such that $l \leq cm$ will be denoted in the following manner: $l \prec m$. Let S_n be a scheme with respect to n digits of a number N , $0 \leq N < 2^n$, which gives the digits of the number N^2 . Then the equality

$$MN = 1/4 [(M + N)^2 - (M - N)^2]$$

determines the manner of the construction of a scheme R_n which gives with respect to the digits of M, N where $0 \leq M, N < 2^n$, the digits of their product MN and such that

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

Therefore we will construct a scheme S_n giving N^2 according to N . The words "the scheme with respect to numbers A_i calculates (or gives) numbers B_j " here and in the sequel means that this scheme realizes the binary digits of numbers B_j according to the binary digits of the numbers A_i .

In paper [2] two constructions of schemes S_n^1 and S_n^2 were deduced giving N^2 according to N , for which respectively

$$\begin{aligned} f(S_n^1) &\prec n^2, & t(S_n^1) &\prec \lg n, \\ f(S_n^2) &\prec n^{\log_2 3}, & t(S_n^2) &\prec \lg^2 n. \end{aligned}$$

In the present paper a scheme S_n is constructed for which

$$f(S_n) \prec n^{1+\epsilon}, \quad t(S_n) \prec n^\epsilon,$$

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

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

2. **Description of the scheme.** Let there be a given n binary digits of a number N :

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

where ω_i equals 0 or 1. We select two natural numbers q and r such that

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

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

We represent N in the form

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

Each α_i is a natural number which contains 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, to each number N we associate $r + 1$ numbers: $\alpha_0, \dots, \alpha_r$. We now place in correspondence to each number N a polynomial of degree r :

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

Clearly, $N = P(2^n)$, $N^2 = P^2(2^q)$.

Our scheme consists of 4 parts I_n, II_n, III_n, IV_n , which are combined in the following order:

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

Part I_n with respect to numbers $\alpha_0, \dots, \alpha_r$, which can be assumed given, calculates the value of $P(x)$ for all integers x in the interval $-r \leq x \leq r$; we denote these $2r + 1$ numbers by m_{-r}, \dots, m_r , i. e.

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

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

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

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

Part IV_n , if we know the coefficients of $P^2(x)$, computes its value for $x = 2^q$.

Thus the number $N^2 = P^2(2^q)$ is obtained.

The method of construction of the scheme is inductive in the sense that parts II_n and III_n include schemes S_k for some $k < n$, in particular their component parts.

3. Estimate of the complexity of a scheme. This estimate utilizes results (for proofs of which, see [3]) stated here in the form of Lemmas 1 and 2.

Lemma 1. *There exists a scheme $T_{a, b}$ with respect to a -digit numbers A_1, \dots, A_b , which evaluates the sum $\sum_{i=1}^b A_i 2^{k(i)}$, where all $k(i)$ are integers, such that*

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

Lemma 2. *There exists a scheme $U_{a, b}$ with respect to two numbers A and B , having a and b digits respectively, which gives their product AB , such that*

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

Let us describe in detail the computation which each part of the scheme carries out and estimate the complexity of these parts. For simplifying the estimation we will assume beforehand that for $k < n$

estimate (1) is correct and $q^{1/5} \succ r \succ \lg \lg q$.

Part I_n a) multiplies $\prec r^2$ numbers with $\prec q$ digits by numbers with $\prec r \lg r$ digits; b) calculates $\prec r$ sums with respect to $\prec r$ composed of $\prec q$ digits in each; hence $f(I_n) \prec q r^4$, $t(I_n) \prec \lg q$.

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 numbers m_i^2 have $\prec q$ digits, and the solutions are integers. In other words this part: a) calculates $\prec r$ linear combinations from $\prec q$ -digit numbers m_i^2 with $\prec r^2 \lg r$ -digit coefficients; b) divides (without a remainder) these linear combinations by the determinant of the system; since it is a constant, this division can be reduced to multiplication of these $\prec q$ -digit linear combinations by a number (approximately the inverse of the determinant) with the same number of digits $\prec q$: hence $f(III_n) \prec q r^5 + r f(S_q)$, $t(III_n) \prec \lg q + t(S_q)$.

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

$$f(IV_n) \prec q r, \quad t(IV_n) \prec \lg g.$$

Now we will estimate the complexity of the scheme S_n . Clearly,

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

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

Thus we arrive at the formulas

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

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

where $q r \leq n$.

Setting $r = c_1 \sqrt[5]{\lg q}$, we obtain for a sufficiently large constant c

$$f(S_n) \prec n c^5 \sqrt[5]{\lg n},$$

$$t(S_n) \prec c \sqrt[5]{\lg n}.$$

Moscow State University

Received 16/JAN/63

BIBLIOGRAPHY

- [1] O. B. Lupanov, Probl. Kibernet. 7 (1962), 61.
- [2] A. Karabuca and Ju. Ofman, Dokl. Akad. Nauk SSSR 145 (1962), 293.
- [3] Ju. Ofman, Dokl. Akad. Nauk SSSR 145 (1962), 48.

Translated by:

N. Friedman