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 $A_1, \ldots, A_{t(R_n)}$ 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

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

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

$$f(S_n^1) \prec n^2, \qquad t(S_n^1) \prec \lg n,$$
$$f(S_n^2) \prec n^{\log_2 3} \qquad t(S_n^2) \prec \lg^2 n.$$

In the present paper a scheme S_n is constructed for which

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

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:

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

where ω_1 equals 0 or 1. We select two natural numbers q and r such that

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

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

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 $\omega_{iq} \ldots \omega_{(i+1)q-1}$ are digits of the number N or identically zero. Thus, to each number N we associate $r+1$ numbers: $\alpha_0, \ldots, \alpha_r$. We now place in correspondence to each number N a polynomial of degree r:

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

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:

$$N \to \mathrm{I}_n \to \mathrm{II}_n \to \mathrm{III}_n \to \mathrm{IV}_n \to N^2.$$

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

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

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 $A_1, \ldots, A_b$, which evaluates the sum $\Sigma_{i=1}^{b} A_i 2^{k(i)}$, where all $k(i)$ are integers, such that*

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

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*

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

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 $f(I_n) \prec' qr^4$, $t(I_n) \prec \lg q$.

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 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 $f(III_n) \prec qr^5 + rf(S_q)$, $t(III_n) \prec \lg q + t(S_q)$.

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

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

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

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

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

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 $qr \leq n$.

Setting $r = c_1^{\sqrt{\lg q}}$, 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

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

Доклады Академии наук СССР
1963. Том 150, № 3

МАТЕМАТИКА

А. Л. ТООМ

О СЛОЖНОСТИ СХЕМЫ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ, РЕАЛИЗИРУЮЩЕЙ УМНОЖЕНИЕ ЦЕЛЫХ ЧИСЕЛ

(Представлено академиком П. С. Новиковым 30 I 1963)

1. Введение. Рассматривается задача о построении возможно более простой в том или ином смысле схемы R_n из функциональных элементов определение см., например, в (1)), которая по двоичным разрядам двух целых n-разрядных чисел M и N, $0 \leqslant M, N < 2^n$, вычисляет все двоичные разряды их произведения MN. Сложность схемы R_n можно охарактеризовать двумя параметрами: числом элементов $f(R_n)$ и глубиной схемы $t(R_n)$, т. е. наибольшим количеством элементов в схеме $A_1, \ldots, A_{t(R_n)}$ таких, что состояние каждого из них, кроме первого, непосредственно зависит от состояния предыдущего. Содержательно глубина — это время работы схемы, если время работы каждого элемента 1. Считается, что булевские функции, приписываемые элементами схемы, берутся из некоторого конечного базиса. Выбор такого базиса произволен, так как все оценки, приводимые ниже, даны с точностью до умножения на константу.

Пусть l и m — две функции от одних и тех же переменных. Тот факт, что существует такая константа c, что $l \leqslant cm$ мы будем записывать следующим образом: $l \prec m$. Пусть S_n — схема по n разрядам числа N, $0 \leqslant N < 2^n$, дающая разряды числа N^2. Тогда равенство

$$MN = {}^1/_4 [(M + N)^2 - (M - N)^2]$$

указывает способ построения схемы R_n, дающей по разрядам M, N, где $0 \leqslant M, N < 2^n$, разряды их произведения MN и такой, что

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

Поэтому мы будем строить схему S_n, дающую N^2 по N. Слова «схема по числам A_i вычисляет (или дает) числа B_j» здесь и в дальнейшем означают, что эта схема по двоичным разрядам чисел A_i реализует двоичные разряды чисел B_j.

В работе (2) приведены две конструкции схем S_n^1 и S_n^2, дающие N^2 по N, для которых соответственно

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

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

В настоящей работе строится схема S_n, для которой

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

где ε — произвольная положительная константа. Точнее, при достаточно большом c (например, $c = 2^5$)

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

2. Описание схемы. Пусть даны n двоичных разрядов числа N:

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

где ω_i равно 0 или 1. Выберем два натуральных числа q и r так, чтобы

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

и в случае $n < q(r+1)$ положим $\omega_n = \omega_{n+1} = \ldots = \omega_{q(r+1)-1} = 0$.

Представим N в виде

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

Каждое α_i — натуральное число, содержащее в двоичной записи q разрядов. Эти разряды $\omega_{iq} \ldots \omega_{(i+1)q-1}$ — разряды числа N или тождественные нули. Итак, каждому числу N мы сопоставили $r+1$ чисел: $\alpha_0 \ldots \alpha_r$. Поставим теперь каждому числу N в соответствие многочлен степени r:

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

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

Наша схема состоит из 4 частей I_n, II_n, III_n, IV_n, порядок соединения которых таков:

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

Часть I_n по числам $\alpha_0 \ldots \alpha_r$, которые можно считать данными, вычисляет значения $P(x)$ при всех целых x в промежутке $-r \leqslant x \leqslant r$; обозначим эти $2r+1$ чисел через $m_{-r} \ldots m_r$, т. е.

$$m_i = P(i) \quad \text{при} -r \leqslant i \leqslant r.$$

Часть II_n возводит все m_i в квадрат, получая при этом значения многочлена $P^2(x)$ в тех же точках $-r, \ldots, r$:

$$m_i^2 = P^2(i) \quad \text{при} -r \leqslant i \leqslant r.$$

Часть III_n, зная значения многочлена $P^2(x)$ степени $2r$ в $2r+1$ точках, по известным формулам вычисляет его коэффициенты.

Часть IV_n, зная коэффициенты $P^2(x)$, вычисляет его значение при $x = 2^q$.

Итак, число $N^2 = P^2(2^q)$ получено.

Метод построения схемы индуктивен в том смысле, что части II_n и III_n включают схемы S_k при некоторых $k < n$ в качестве своих составных частей.

3. Оценка сложности схемы. Эта оценка использует результаты (доказательство которых см. (3)), сформулированные здесь в виде лемм 1 и 2.

Лемма 1. *Существует схема $T_{a,b}$ по a-разрядным числам $A_1, \ldots, A_b$, вычисляющая сумму $\sum_{i=1}^{b} A_i 2^{k(i)}$, где все $k(i)$ целые, такая, что*

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

Лемма 2. *Существует схема $U_{a,b}$, по двум числам A и B, имеющим a и b разрядов соответственно, дающая их произведение AB, такая, что*

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

Опишем подробно вычисления, которые производит каждая часть схемы, и оценим сложности этих частей. Для упрощения оценок будем считать заранее, что при $k < n$ оценка (1) верна и $q^{1/4} \succ r \succ \lg \lg q$.

Часть I_n: а) умножает $\prec r^2$ чисел с $\prec q$ разрядами на числа с $\prec r \lg r$ разрядами; б) вычисляет $\prec r$ сумм по $\prec r$ слагаемых с $\prec q$ разрядами в каждом; отсюда $f(I_n) \prec qr^4$, $t(I_n) \prec \lg q$.

Часть II_n возводит в квадрат $\prec r$ чисел с $\prec q$ разрядами; отсюда $f(II_n) \prec r \cdot f(S_q)$, $t(II_n) \prec t(S_q)$.

Часть III_n решает систему линейных уравнений с постоянными $\prec r \lg r$-разрядными коэффициентами, причем свободные члены m_i^2 имеют $\prec q$ разрядов, а решения — целые числа. Иными словами, она: а) вычисляет $\prec r$ линейных комбинаций от $\prec q$-разрядных чисел m_i^2 с $\prec r^2 \lg r$-разрядными коэффициентами; б) делит (нацело) эти линейные комбинации на определитель системы; так как он постоянен, то это деление можно свети к умножению этих $\prec q$-разрядных линейных комбинаций на число (приближенно обратное определителю) с таким же числом разрядов $\prec q$; отсюда $f(III_n) \prec qr^5 + r \cdot f(S_q)$, $t(III_n) \prec \lg q + t(S_q)$.

Часть IV_n в многочлен от x степени r с $\prec q$-разрядными коэффициентами подставляет $x = 2^q$; отсюда

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

Теперь оценим сложность схемы S_n. Очевидно,

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

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

Таким образом, приходим к формулам

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

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

где $qr \leqslant n$.

Положив $r = c_1^{\sqrt{\lg q}}$, получаем при достаточно большом постоянном c

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

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

Московский государственный университет
им. М. В. Ломоносова

Поступило
16 I 1963

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] О. Б. Лупанов, Проблемы кибернетики, в. 7, 1962, стр. 61. [2] А. Карабуца, Ю. Офман, ДАН, **145**, № 2, 293 (1962). [3] Ю. Офман, ДАН, **145**, № 1, 48 (1962).