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

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

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

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

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

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

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

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

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:

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

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 $\sum\limits_{i=1}^{b} A_i 2^{k\,(i)}$, 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 $q^{1/2} \succ r \succ \lg \lg q$.

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. Карацуба, Ю. Офман, ДАН, 145, № 2, 293 (1962). [3] Ю. Офман, ДАН, 145, № 1, 48 (1962).

Отзыв на работу А.Тоома "О сложности схемы из функциональных ~~[illegible]~~ элементов,реализующей умножение целых чисел".

Повидимому,для всех математиков явилось большой неожиданностью,что обычная схема умножения многозначных чисел,требующая

$$\asymp n^2$$

элементрарных операций при умножении друг на друга двух n-значных чисел,не является самой экономной.А.Карацуба в 1962-ом году показал,что для такого умножения достаточно

$$\asymp n^{1,58\ldots}$$

элементарных операций.Результат А.Карацубы замечателен своей неожиданностью ,но получен необычно простыми средствами – его можно рассказать разумному школьнику за двадцать минут.

Дальнейшее продвижение оказалось значительно более трудным и не удавалось целому ряду молодых исследователей,ухватившихся за эту тему ,соблазнительную своей неожиданностью и элементарностью.

По А.Тоому достаточно

$$\asymp n e^{\sqrt{\ln n}} < n^{1+\varepsilon}$$

операций / $\varepsilon>0$ любое /.Так как оценка

$$> n$$

тривиальна~~[illegible]~~ ,то с точки зрения показателя при n вопрос решен до конца.

Результат А.Тоома позволяет осуществить ~~[illegible]~~ решающее продвижение в вопросе с виду значительно более общем ~~[illegible]~~. Теперь можно доказать,что "сложность" вычисления любой аналитической на отрезке функции с точностью до h растет с ~~[illegible]~~ с убыванием h не быстрее

$$\left(\frac{1}{h}\right)^{2+\varepsilon},$$

при чем заменить показатель $2+\varepsilon$ показателем меньшим ~~[illegible]~~ чем 2 заведомо невозможно. В моем обзорном докладе на Стокгольмском съезде была указана лишь оценка

$$\lesssim \left(\frac{1}{h}\right)^{2,58\ldots}$$

Построения А.Тоома остроумны и неожиданны. Среди работ по реализации функций от большого числа дискретных /обычно двоичных/ переменных схемами из функциональных элементов, дискретными автоматами и т.п. работа А.Тоома принадлежит к числу самых интересных безотносительно к поколениям конкурирующих здесь математиков.

Изложение несколько сжато /заметка в ДАН не вместила бы полного освещения всех деталей/, но результат проверен многими. И сам результат и все промежуточные утверждения правильны. Работа заслуживает на студенческом конкурсе самой высокой оценки.

14 декабря 1963

А.Колмогоров

/А.Колмогоров/