A. Karatsuba, Yu. Ofman, Multiplication of many-digital numbers by automatic computers, *Dokl. Akad. Nauk SSSR*, 1962, Volume 145, Number 2, 293–294

Доклады Академии наук СССР
1962. Том 145, № 2

КИБЕРНЕТИКА И ТЕОРИЯ РЕГУЛИРОВАНИЯ

А. КАРАЦУБА и Ю. ОФМАН

УМНОЖЕНИЕ МНОГОЗНАЧНЫХ ЧИСЕЛ НА АВТОМАТАХ

(Представлено академиком А. Н. Колмогоровым 13 II 1962)

Одной из задач настоящей заметки, так же как ранее опубликованной заметки Ю. Офмана ([1]), обозначения и определения которой используются также здесь, является рассмотрение проблемы нахождения нижних оценок алгоритмической сложности дискретных функций. Пока никаких нетривиальных оценок снизу не существует. Весьма вероятно, что возможна теория, которая одним методом оценит снизу число операций над цифрами при умножении многозначных чисел и количество операций над числами при решении системы линейных уравнений и пр.

Два m-значных двоичных числа помещаются на вход двоичного автомата (вход из $k = 2m$ звеньев). На выходе из $2m + 1$ звеньев должна быть получена двоичная запись произведения. Для определенной таким образом функции $y = d_5(x)$ элементарно получаются нижние оценки сложности реализующих ее двоичных автоматов: $N_0 \geqslant m$, $T_0 \geqslant \log_2 m$.

Далее излагается схема доказательства двух теорем.

Т е о р е м а 1 (Офман). *При любом s, $1 \leqslant s \leqslant m$, функция d_5 может быть реализована двоичным автоматом с характеристиками, имеющими при $m \to \infty$ (равномерно по s в указанных пределах) характеристики*

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

При $s = 1$ получаем автомат с характеристиками

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

при $s = m$ с характеристиками

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

Т е о р е м а 2 (Карацуба). *Функция d_5 может быть реализована двоичным автоматом с характеристиками*

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

Далее этих результатов авторам заметки продвинуться не удалось. Очевидно, что N_0 и T_0 удовлетворяют оценкам

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

но неизвестно, соединимы ли такие порядки роста N и T между собой.

Обычный школьный способ умножения, измененный лишь в том, что произведения множимого на каждый разряд множителя получаются параллельно и складываются автоматом 3, приводит к оценкам (1). Если же образовывать произведения множимого на отдельные знаки множителя последовательно и прибавлять их к накопленной сумме ранее образованных про-

изведений, пользуясь многократно автоматом для сложения теоремы 2 работы ([1]), то можно прийти к оценке (2). Вспомогательное устройство, которое последовательно вводит в сумматор новые и новые произведения, конструируется без больших затруднений в пределах требований оценок (2).

Для получения автомата, существование которого утверждается в теореме 1, множитель делится на группы разрядов по s разрядов в группе. Умножение на знаки множителя из одной разрядной группы производится последовательно, а сложение результатов умножения на каждую разрядную группу производится параллельно.

Для доказательства теоремы 2 заметим, что умножение можно заменить сложением и возведением в квадрат: $ab = {}^1/_4\,[(a+b)^2 - (a-b)^2]$. Деление на четыре не представляет больших затруднений в двоичной системе счисления. Таким образом, оказывается достаточным оценить порядки роста N и T для функции $y = d_6(x)$, соответствующей возведению в квадрат $2m$-значного двоичного числа

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

Формула

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

показывает, что возведение в квадрат $2m$-значного числа сводится к трем возведениям в квадрат m-значных чисел * и операциям (сложение, умножение на степени двойки), осуществление которых можно произвести весьма экономно, пользуясь приемами, указанными в ([1]).

Лемма. *Если возведение в квадрат r-значного числа можно произвести автоматом с $N = N_r$, $T = T_r$, то для возведения в квадрат 2^{r+1}-значного числа можно построить автомат с $N = N_{r+1} = 3N_r + c \cdot 2^r$, $T = T_{r+1} = T_r + c_1 \cdot r$.*

При помощи леммы легко проводится индуктивное доказательство теоремы 2.

Для представлений автоматами без обратных связей (суперпозициями) верна теорема 2 и частный случай теоремы 1, соответствующий формуле (1).

Поступило
9 II 1962

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Ю. Офман, ДАН, 145, № 1 (1962).

* Сумма $(x_1 x_2 \ldots x_m) + (x_{m+1} \ldots x_{2m})$ может иметь $m+1$ знаков, но сведение возведения в квадрат $(m+1)$-значного числа к возведению в квадрат m-значного числа делается при помощи формулы $(2a+b)^2 = 4a^2 + 4ab + b^2$, где $b = 0{,}1$.