

Ю. В. БЕНДЕРСКИЙ

БЫСТРЫЕ ВЫЧИСЛЕНИЯ

(Представлено академиком И. М. Виноградовым 20 III 1975)

Первые постановки задач об оценке сложности вычислений различного вида функций (умножение многозначных чисел, вычисление определителя m -го порядка и т. д.) принадлежат А. Н. Колмогорову (1956 г.). В 1960 г. А. А. Карацуба на примере умножения многозначных чисел предложил общий метод решения задач об оценке сверху сложности вычислений широкого класса функций (опубликовано в ⁽¹⁾). Существо этого метода состоит в том, что вычисление функции от $2n$ -значного аргумента сводится к вычислению небольшого числа функций от n -значного аргумента и далее применяется итеративный процесс (быстрый итеративный метод). Обозначим через $M(n)$ сложность умножения двух n -значных чисел; в ⁽¹⁾ получено

$$M(n) = O(n^\alpha), \quad \alpha = \log_2 3.$$

Указанный метод применил в 1970 г. А. Штрассен ⁽³⁾ к оценке $V(n)$ — сложности вычисления определителя n -го порядка и доказал, что

$$V(n) = O(n^\beta), \quad \beta = \log_2 7.$$

В оценке сложности умножения n -значных чисел метод А. А. Карацубы усовершенствован А. Л. Тоомом ⁽²⁾ и Шенхаге и Штрассеном ⁽⁴⁾ (числа разбиваются не на два «блока», а на растущее с ростом n число «блоков»), которые получили соответственно оценки

$$M(n) = O(ne^{c\sqrt{\ln n}}), \quad M(n) = O(n \ln n \ln \ln n).$$

В настоящей статье быстрый итеративный метод применяется к оценке сложности вычисления элементарных алгебраических функций, т. е. функций вида $1/z$, $z^{1/k}$ и их суперпозиций. Введем ряд определений.

Определение 1. Пусть элементарная алгебраическая функция $s=f(z)$ задана на некоторой ограниченной области $D \subset \mathbb{C}$, не имеет в $\bar{D}$ особенностей и ограничена вместе со своей производной. Переменная и значение функции записываются парами двоичных последовательностей, т. е.

$$\begin{aligned} z &= (\overline{x_{-i} \dots x_0, x_1, \dots}; \overline{y_{-j} \dots y_0, y_1, \dots}), \\ s &= (\overline{u_{-v} \dots u_0, u_1, \dots}; \overline{v_{-\mu} \dots v_0, v_1, \dots}), \end{aligned}$$

где x_i, y_j, u_i, v_i равны 0 или 1.

Тогда вычислить $s=f(z)$ в точке $z=z_0 \in D$ с точностью до 2^{-n} означает найти такое s_n , что

$$|s_n - f(z_0)| = O(2^{-n})$$

с константой в O , не зависящей от n .

Очевидно, что вычисление $f(z)$ в точке $z=z_0$ можно заменить вычислением ее в точке $z=z_n$, где $|z_0 - z_n| < 2^{-n}$, так как $f'(z)$ ограничена в $\bar{D}$. Таким образом, все участвующие в вычислениях числа можно записать в виде конечных последовательностей.

Определение 2. Количество операций, достаточное для вычисления $f(z)$ с точностью до 2^{-n} , обозначается $s_f(n)$. Количество операций, достаточное для умножения двух n -значных чисел, обозначается $M(n)$.

Предполагается, что $M(n)$ — монотонно возрастающая функция, $M(n) > n$.

С помощью введенных определений основной результат формулируется следующим образом.

Для элементарной алгебраической функции $s=f(z)$, заданной в некоторой ограниченной области $D \subset \mathbb{C}$, ограниченной вместе с производной и не имеющей в $\bar{D}$ особенностей,

$$s_f(n) = O(M(n)),$$

причем константа зависит только от f и D , но не зависит от $z \in D$ и n .

Теорема 1. Пусть z — комплексное, $1/2 < |z| \leq 1$, $s=1/z$. Тогда

$$s_{1/z}(n) = O(M(n)).$$

Предварительно докажем следующее утверждение.

Лемма 1. Для s и z из условия теоремы 1 выполняется итерация: если $|s_n - s| < 2^{-n}$, то для

$$s_{2n} = z s_n^2 - 2s_n \quad (1)$$

справедливо неравенство

$$|s_{2n} - s| < 2^{-2n}.$$

Доказательство. Возводя обе части неравенства $|s_n - s| < 2^{-n}$ в квадрат, имеем

$$|s_n^2 - 2s_n/z + s^2| < 2^{-2n}.$$

Умножив на $|z| \leq 1$, получаем формулу (1).

Доказательство теоремы 1. Положив $s_1 = 3/2$, итерируем до получения требуемой точности. Сложность одного шага итерации равна $2M(n) + cn$. Обозначив $s_{1/z}(n) = I(n)$, имеем рекуррентное соотношение

$$I(2n) = I(n) + 2M(n) + cn,$$

откуда следует утверждение теоремы.

Замечания. а) Для произвольного $z \neq 0$ заменой $z' = 2^N z$ можно добиться выполнения условия $1/2 < |z'| \leq 1$.

б) На каждом шаге итерации для вычисления s_{2n} достаточно брать вместо z его приближение.

Следствие 1. Для $1/R < |z - z_i|$, $|z| < R$ сложность вычисления $R(z)$, где $R(z)$ — рациональная функция, z_i — ее полюсы, равна $O(M(n))$.

Следствие 2. Деление целых чисел с остатком можно свести к вычислению рациональных функций следующим образом. Пусть a и b — целые числа, меньшие 2^n ; требуется найти такие q и r целые, что $a = bq + r$ и $0 \leq r < q$. Тогда, вычислив s_n такое, что $|s_n - 1/b| < 2^{-n}$, имеем

$$q = [s_n b], \quad r = a - bq. \quad (2)$$

Сложность вычисления q и r по формулам (2) равна $O(M(n))$.

Теорема 2. Пусть $0 < r \leq |z| < R$,

$$s = f(z) = z^{1/k}, \quad 0 \leq \arg s < 2\pi/k,$$

k — натуральное. Тогда

$$s_f(n) = R(n) = O(M(n)).$$

Доказательство аналогично доказательству теоремы 1. Итерация проводится по формуле

$$s_{2n} = \frac{k+1}{k} s_n - \frac{s_n^{k+1}}{kz} \quad (3)$$

или

$$s_{2n} = \frac{k-1}{k} s_n + \frac{z}{k s_n^{k-1}}. \quad (4)$$

Тогда из неравенства

$$|s_n - s| < 2^{-n}$$

следует

$$|s_{2n} - s| < ck \cdot 2^{-2n}$$

и итерация сходится при

$$|s_0 - s| < 1/(ck), \quad c > 2.$$

s_0 можно вычислить, например, разложив $z^{1/k}$ в ряд Тейлора и взяв достаточное число членов.

Доказательство формул (3) и (4). Разложив правую часть (3) в ряд по s_n в точке $s = z^{1/k}$, имеем

$$F''(s_n)|_{s_n=s} = \frac{k+1}{s} < \frac{k+1}{r},$$

что и требовалось доказать.

Из доказанных теорем следует, что сложность вычисления элементарных алгебраических функций не превосходит $O(M(n))$ с константой, не зависящей от $z \in D$ и n .

По такой же схеме быстрый итеративный метод можно применять для быстрых вычислений элементарных трансцендентных функций, эллиптических функций, функций от матриц и др.

Всесоюзный научно-исследовательский
проектный институт экономики,
организации управления производством и информации
лесной, целлюлозно-бумажной и деревообрабатывающей промышленности
Москва

Поступило
18 III 1975

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- ¹ А. Карацуба, Ю. Офман, ДАН, т. 145, № 2, 293 (1962). ² А. Л. Тоом, ДАН, т. 150, № 3 (1963). ³ V. Strassen, Numerische Math., Bd. 13, H. 4, 354 (1969).
⁴ A. Schönhage, V. Strassen, Arch. f. elektronisches Rechnen. B. 7, Fasc. 3-4, 281 (1971).