Тема 5. Деление чисел. Арифметика многочленов.

С. Б. Гашков, И. С. Сергеев

1 Быстрое деление чисел

Поскольку операция деления сводится к инвертированию и умножению, достаточно рассмотреть операцию инвертирования. Пусть дано число $A \in [1/2, 1]$, и положим $R = 1/A$. Рассмотрим задачу вычисления числа R_n, такого, что $|R - R_n| \le 2^{-n}$. Иначе говоря, R_n есть приближение к R с точностью 2^{-n}. Общий случай, когда $A \notin [1/2, 1]$, сводится к рассмотренному при замене A на $2^k A$ и последующем умножении результата на 2^k (эти операции реализуются сдвигом позиции запятой, что в схемной модели выполняется бесплатно).

Пусть $a_{..k}$ обозначает число a с отсеченными разрядами после запятой младше k-го — это приближение к a с точностью 2^{-k}.

Пусть A известно с точностью до $n + O(1)$ знаков после запятой. Определим последовательность r_i следующим образом:

$$r_0 = 1, \qquad \tilde{r}_{i+1} = 2r_i - A_{..4+2^i} \cdot r_i^2, \qquad r_i = (\tilde{r}_i)_{..4+2^i}. \tag{1}$$

Лемма 1.

$$|1 - r_i A_{..4+2^i}| < 2^{-2^{i-1}-1/2}.$$

Доказательство. Очевидно, неравенство справедливо при $i = 0$. Докажем индуктивный переход от i к $i + 1$.

а) По индуктивному предположению, справедливо:

$$0 \le 1 - \tilde{r}_{i+1} A_{..4+2^i} = (1 - r_i A_{..4+2^i})^2 \le 2^{-2^i-1}.$$

Очевидно $r_{i+1} > 0$. Из левого неравенства дополнительно получаем, что $r_{i+1} \le A^{-1}_{..4+2^i} \le 2$.

б) Получим вспомогательную оценку:

$$\begin{aligned}|r_{i+1}A_{..4+2^{i+1}} - \tilde{r}_{i+1}A_{..4+2^i}| \leq \\ \leq |r_{i+1}A_{..4+2^{i+1}} - r_{i+1}A_{..4+2^i}| + |r_{i+1}A_{..4+2^i} - \tilde{r}_{i+1}A_{..4+2^i}| \leq \\ \leq r_{i+1}\,|A_{..4+2^{i+1}} - A_{..4+2^i}| + A_{..4+2^i}\,|r_{i+1} - \tilde{r}_{i+1}| \leq \\ \leq 2 \cdot 2^{-4-2^i} + 1 \cdot 2^{-4-2^{i+1}} < 2^{-3-2^i} + 2^{-4-2^i}.\end{aligned}$$

в) Окончательно, утверждение леммы следует из выкладки:

$$\begin{aligned}|1 - r_{i+1}A_{..4+2^{i+1}}| \leq \\ |r_{i+1}A_{..4+2^{i+1}} - \tilde{r}_{i+1}A_{..4+2^i}| + |1 - \tilde{r}_{i+1}A_{..4+2^i}| < \\ < 2^{-3-2^i} + 2^{-4-2^i} + 2^{-1-2^i} = \frac{11}{16}2^{-2^i} < 2^{-2^i-1/2}.\end{aligned}$$

Следствие 1. $|1 - r_iA| < 2^{-2^{i-1}}$.

Доказательство. Действительно,

$$|1 - r_iA| \leq |1 - r_iA_{..4+2^i}| + r_i\,|A - A_{..4+2^i}| < 2^{-2^{i-1}-1/2} + 2^{-3-2^i} < 2^{-2^{i-1}}.$$

Таким образом, число r_i есть приближение к R с точностью $2^{1-2^{i-1}}$.

1.1 Оценка сложности

Определим специальную функцию $M(n)$, которая, во-первых, не меньше сложности умножения n-разрядных чисел, а во-вторых для любых $x, y \in \mathbb{N}$ при $x \leq y$ выполнено

$$M(x)/x \leq M(y)/y. \tag{2}$$

Из этого неравенства вытекает суперлинейность: $M(x + y) \geq M(x) + M(y)$. Из метода Шёнхаге—Штрассена следует, что $M(n) = O(n \log n \log\log n)$.

Теорема 1. *Сложность инвертирования (с точностью 2^{-n}) составляет $I(n) = O(M(n))$.*

Доказательство. Для вычисления обратного числа с точностью 2^{-n} достаточно определить r_i вплоть до $i = \lceil \log_2 n \rceil + 1$. Вычисление r_{i+1}, отталкиваясь от r_i, можно выполнить за 2 умножения $(5+2^i)$-разрядных чисел

и одного вычитания со сложностью $2M(5+2^i)+O(2^i)$. Следовательно, для определения последнего r_i будет затрачено

$$\sum_{i=0}^{\lceil \log_2 n \rceil + 1} (2M(5+2^i)+O(2^i)) \leq$$

$$\leq 2M\left(2^{\lceil \log_2 n \rceil + 2} + 5\log_2 n + 10\right) + O(n) = O(M(n))$$

операций. Последний переход справедлив в силу $M(cn) = O(M(n))$, где c — константа.

Таким образом, фактически сложность инвертирования и, как следствие, деления, по порядку не выше сложности умножения.

Указанный метод инвертирования был предложен С. Куком около 1966 г. По существу, этот метод является переложением известного метода Ньютона—Рафсона на дискретный случай: в методе Ньютона—Рафсона для поиска решения уравнения $f(x) = 0$ предлагается итерация $x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$. В нашем случае $f(x) = A - 1/x$.

2 Арифметика многочленов

От чисел перейдем к изучению основных операций с многочленами. Будем рассматривать многочлены над коммутативным кольцом R с единицей без делителей нуля. Многочлен кодируется набором своих коэффициентов. При реализации арифметических операций с многочленами сложность будем измерять числом арифметических действий: сложений-вычитаний, умножений, делений, умножений в кольце R.

Очевидно, сложение или вычитание многочленов степени, меньшей n, имеет сложность n. Для умножения можно воспользоваться модификацией алгоритма Шёнхаге—Штрассена, который в случае многочленов имеет даже более простое строение, чем для чисел. Умножение выполняется в кольце $R[x]/(x^{2^m}+1)$, и также используется ДПФ. Правда, приходится отдельно рассматривать случай кольца R характеристики 2, т.к. ДПФ порядка степени двойки не определено в кольце $R[x]/(x^{2^m}+1)$. В этом случае предлагается умножать в кольцах $R[x]/(x^{2\cdot 3^m}+x^{3^m}+1)$ и использовать ДПФ порядка степени тройки.

Сложность умножения многочленов степени n методом Шёнхаге—Штрассена, как и в случае чисел, составляет $O(n\log n\log\log n)$, при этом для многочленов неизвестны методы с лучшим порядком сложности.

Роль точности в задаче инвертирования многочленов играет число известных коэффициентов. Пусть задан многочлен $f(x)$, младший коэффициент $f(0)$ которого отличен от нуля. Пусть $r_n(x)f(x) = 1 \bmod x^n$, т.е. $r_n(x) = f^{-1}(x) \bmod x^n$. Тогда очередное приближение $r_{2n}(x) = f^{-1}(x) \bmod x^{2n}$ может быть найдено из аналогичного (1) соотношения

$$r_{2n}(x) = 2r_n(x) - f(x)r_n^2(x). \tag{3}$$

Сложность $I(n)$ нахождения младших n коэффициентов обратного многочлена, таким образом, составляет $O(M(n))$, где $M(n)$ — функция сложности умножения многочленов степени $n-1$, дополненная, как и для чисел, условием $M(x)/x \le M(y)/y$ при $x \le y$.

2.1 Деление с остатком.

Рассмотрим задачу нахождения частного $q(x)$ и остатка $r(x)$ от деления многочлена $a(x)$, $\deg a < 2n$, на многочлен $b(x)$, $\deg b = n$. Описываемый далее способ вычислений был предложен Ф. Штрассеном.

Представим делимый многочлен в виде $a(x) = h(x)x^n + g(x)$, $\deg g < n$. Перепишем равенство $a(x) = q(x)b(x) + r(x)$ в виде

$$h(x)x^n = q(x)b(x) + r'(x), \tag{4}$$

где $r'(x) = r(x) - g(x)$.

Введем обозначение $\widetilde{c}(x) = x^{\deg c} c\left(\frac{1}{x}\right)$, которое означает, что коэффициенты многочлена $\widetilde{c}$ являются коэффициентами многочлена c, переписанными в обратном порядке.

Подставим в (4) $1/x$ вместо x и умножим на $x^{\deg h+n}$:

$$x^{\deg h+n} h\left(\frac{1}{x}\right) x^{-n} = x^{\deg h+n} q\left(\frac{1}{x}\right) b\left(\frac{1}{x}\right) + x^{\deg h+n} r'\left(\frac{1}{x}\right),$$

откуда, замечая, что $\deg h = \deg q$, получаем

$$\widetilde{h}(x) = \widetilde{q}(x)\widetilde{b}(x) + \widetilde{r'}(x)x^{n+\deg h-\deg r'},$$

и далее, домножением на $x^{n-1-\deg h}$:

$$\left(\widetilde{h}(x)x^{n-1-\deg h}\right) = \left(\widetilde{q}(x)x^{n-1-\deg h}\right)\widetilde{b}(x) + \left(\widetilde{r'}(x)x^{n-1-\deg r'}\right)x^n.$$

Многочлены в скобках обозначим через $\widehat{h}(x), \widehat{q}(x), \widehat{r}(x)$ соответственно. Очевидно, степени всех трех этих многочленов равны $n-1$. Приходим к равенству

$$\widehat{h}(x) = \widehat{q}(x)\widetilde{b}(x) + \widehat{r}(x)x^n, \tag{5}$$

которое приводит к следующему алгоритму.

Найдем многочлен $i(x) = \left(\widetilde{b}(x)\right)^{-1} \bmod x^n$. Из (5) следует, что $\widehat{q}(x) = i(x)\widehat{h}(x) \bmod x^n$, т.е. частное $q(x)$ определяется из произведения $i(x)\widehat{h}(x)$. Наконец, остаток находится по формуле $r(x) = (q(x)b(x) - a(x)) \bmod x^n$. Таким образом, сложность $D(n)$ рассмотренного алгоритма можно оценить как $I(n) + 2M(n) + O(n)$.

Дополнительные вопросы

1. Обосновать соотношение $M(cn) = O(M(n))$, которое использовалось при доказательстве теоремы 1.
2. Отталкиваясь от метода Ньютона—Рафсона, построить алгоритм приближенного вычисления квадратного корня, сложность которого по порядку равна $M(n)$.
3. Доказать формулу (3).