Тема 6.2. Арифметика чисел. Логарифм и экспонента.

С. Б. Гашков, И. С. Сергеев

1 Арифметико-геометрическое среднее

Пусть $a, b \geq 0$. Положим $a_0 = a$, $b_0 = b$ и при любом $k \geq 1$ положим $a_k = \frac{a_{k-1}+b_{k-1}}{2}$ и $b_k = \sqrt{a_{k-1}b_{k-1}}$. *Арифметико-геометрическим средним* чисел a и b называется предел введенных последовательностей:

$$\text{АГС}(a, b) = \lim_{k\to\infty} a_k = \lim_{k\to\infty} b_k.$$

Последовательности $\{a_k\}$ и $\{b_k\}$ сходятся к пределу очень быстро: разность $a_k - b_k$ становится величиной порядка 2^{-n} при $k \approx \log_2(n \log_2 |a-b|)$. Более точно скорость сходимости описывается следующей леммой. Для удобства всюду далее будем считать, что $a \geq b$.

Лемма 1. *Пусть* $1 \leq \frac{a}{b} \leq 1 + 2^{2^m}$. *Тогда*

а) $\frac{a_n}{b_n} \leq 1 + 2^{2^{m-n}}$;

б) при $n \geq m$ *справедливо* $\frac{a_n}{b_n} \leq 1 + 2^{3-2^{n+1-m}}$.

Доказательство. Докажем п. а) индукцией по n. При $n = 0$ соотношение гарантируется условием леммы. Индуктивный переход доказывает выкладка:

$$\frac{a_{n+1}}{b_{n+1}} = \frac{1}{2}\left(\sqrt{\frac{a_n}{b_n}} + \sqrt{\frac{b_n}{a_n}}\right) \leq \sqrt{\frac{a_n}{b_n}} \leq \sqrt{1 + 2^{2^{m-n}}} < 1 + 2^{2^{m-n-1}}.$$

Также индукцией докажем п. б). При $n = m$ имеем частный случай п. а). Положим $\frac{a_n}{b_n} = 1 + \varepsilon$, тогда

$$\left(\frac{a_{n+1}}{b_{n+1}}\right)^2 = \left(\frac{\sqrt{1+\varepsilon} + \frac{1}{\sqrt{1+\varepsilon}}}{2}\right)^2 = \frac{1 + \varepsilon + 2 + \frac{1}{1+\varepsilon}}{4} \leq \frac{4 + \varepsilon^2}{4} \leq \left(1 + \frac{\varepsilon^2}{8}\right)^2$$

в силу соотношения $\frac{1}{1+\varepsilon} \leq 1 - \varepsilon + \varepsilon^2$. Следовательно, $\frac{a_{n+1}}{b_{n+1}} \leq 1 + \frac{\varepsilon^2}{8}$, а из $\varepsilon \leq 2^{3-2^{n+1-m}}$ следует $\frac{\varepsilon^2}{8} \leq 2^{3-2^{n+2-m}}$. Лемма доказана.

2 Эллиптические интегралы. Теорема Гаусса

При $a, b > 0$ определим несобственный интеграл

$$I(a,b) = \int_0^{+\infty} \frac{dx}{\sqrt{(x^2+a^2)(x^2+b^2)}},$$

относящийся к семейству эллиптических интегралов. Справедлива

Теорема 1 (Гаусс)**.**

$$I(a,b) = \frac{\pi}{2\text{АГС}(a,b)}.$$

Теорема вытекает из следующих двух лемм.

Лемма 2. *При* $a \geq b$

$$\frac{\pi}{2a} \leq I(a,b) \leq \frac{\pi}{2b}.$$

Доказательство. Очевидно $I(a,a) \leq I(a,b) \leq I(b,b)$. Остается заметить, что

$$I(a,a) = \int_0^{+\infty} \frac{dx}{x^2+a^2} = \frac{1}{a}\int_0^{+\infty} \frac{dy}{y^2+1} = \frac{1}{a}\operatorname{arctg} y\Big|_0^{+\infty} = \frac{\pi}{2a}.$$

Лемма 3.

$$I(a,b) = I\left(\frac{a+b}{2}, \sqrt{ab}\right).$$

Доказательство. Пусть $u = \frac{1}{2}\left(x - \frac{ab}{x}\right)$. Заметим, что

$$(x^2+a^2)(x^2+b^2) = x^2(a+b)^2 + (x^2-ab)^2 = 4x^2\left(u^2 + \left(\frac{a+b}{2}\right)^2\right).$$

Кроме того,

$$x\,du = \frac{x}{2}\left(1 + \frac{ab}{x^2}\right)dx = \frac{1}{2}\left(x + \frac{ab}{x}\right)dx = \sqrt{u^2+ab}\,dx.$$

Тогда

$$I(a,b) = \frac{1}{2}\int_0^{+\infty} \frac{dx}{x\sqrt{u^2+\left(\frac{a+b}{2}\right)^2}} = \frac{1}{2}\int_{-\infty}^{+\infty} \frac{du}{\sqrt{\left(u^2+\left(\frac{a+b}{2}\right)^2\right)(u^2+ab)}} =$$

$$= \int_0^{+\infty} \frac{du}{\sqrt{\left(u^2+\left(\frac{a+b}{2}\right)^2\right)(u^2+ab)}} = I\left(\frac{a+b}{2}, \sqrt{ab}\right).$$

Далее нам понадобится еще одна простая лемма:

Лемма 4.

$$I(1,b) = 2\int_0^{\sqrt{b}} \frac{dx}{\sqrt{(x^2+1)(x^2+b^2)}}.$$

Доказательство.

$$\int_{\sqrt{b}}^{+\infty} \frac{dx}{\sqrt{(x^2+1)(x^2+b^2)}} = \int_{\sqrt{b}}^{0} \frac{-bdu}{u^2\sqrt{((b/u)^2+1)(b/u)^2+b^2)}} =$$

$$= \int_0^{\sqrt{b}} \frac{du}{\sqrt{(u^2+b^2)(u^2+1)}}.$$

Следующая лемма является ключевой — она устанавливает связь между эллиптическими интегралами и логарифмической функцией.

Лемма 5. *Если* $b \in (0,\, 1]$, *то*

$$0 \le I(1,b) - (2+b^2/2)\ln\left(\sqrt{\frac{1}{b}} + \sqrt{1+\frac{1}{b}}\right) + \frac{1}{2}b\sqrt{1+b} \le \frac{1}{5}b^{3/2}.$$

Доказательство. А) Для начала нам понадобятся простые соотношения: при $\alpha \ge 0$

$$1-\frac{\alpha}{2} \le \frac{1}{\sqrt{1+\alpha}} \le 1-\frac{\alpha}{2}+\frac{\alpha^2}{2}.$$

Левое неравенство верно в силу того, что при $\alpha \le 2$:

$$(1-\alpha/2)^2(1+\alpha) = (1-\alpha+\alpha^2/4)(1+\alpha) = 1-\alpha^2+\frac{\alpha^2}{4}(1+\alpha) = 1+\frac{\alpha^2}{4}(\alpha-3) \le 1.$$

Правое неравенство следует из

$$(1-\alpha/2+\alpha^2/2)^2 = 1-\alpha+\alpha^2+\frac{1}{4}(\alpha-\alpha^2)^2 \geq 1-\alpha+\alpha^2 \geq \frac{1}{1+\alpha}.$$

Б) Выпишем производные для следующих функций:

$$\ln\left(x+\sqrt{x^2+b^2}\right)' = \frac{1}{\sqrt{x^2+b^2}}, \qquad \left(x\sqrt{x^2+b^2}\right)' = \frac{2x^2+b^2}{\sqrt{x^2+b^2}}.$$

В) Нижняя оценка леммы доказывается как

$$\begin{aligned}
I(1,b) = 2\int_0^{\sqrt{b}} \frac{dx}{\sqrt{(x^2+1)(x^2+b^2)}} &\geq \int_0^{\sqrt{b}} \frac{2-x^2}{\sqrt{x^2+b^2}}dx = \\
&= \int_0^{\sqrt{b}} \frac{2+b^2/2}{\sqrt{x^2+b^2}}dx - \int_0^{\sqrt{b}} \frac{x^2+b^2/2}{\sqrt{x^2+b^2}}dx = \\
&= (2+b^2/2)\ln\left(x+\sqrt{x^2+b^2}\right)\Big|_0^{\sqrt{b}} - \frac{x}{2}\sqrt{x^2+b^2}\Big|_0^{\sqrt{b}} = \\
&= (2+b^2/2)\ln\left(\frac{\sqrt{b}+\sqrt{b+b^2}}{b}\right) - \frac{1}{2}b\sqrt{1+b}.
\end{aligned}$$

Г) Верхняя оценка следует из цепочки неравенств:

$$\begin{aligned}
&\int_0^{\sqrt{b}} \frac{1}{\sqrt{(x^2+b^2)}}\left(\frac{2}{\sqrt{x^2+1}}-(2-x^2)\right)dx \leq \\
&\qquad \leq \int_0^{\sqrt{b}} \frac{1}{\sqrt{(x^2+b^2)}}x^4dx \leq \frac{1}{b}\int_0^{\sqrt{b}} x^4dx = \frac{1}{5}b^{3/2}.
\end{aligned}$$

Лемма доказана.

3 Алгоритм Брента—Саламина

Пусть дано число X, и требуется вычислить $\ln X$ с точностью 2^{-2N}. Общую схему вычислений описывает диаграмма:

$$X \longrightarrow 2^n X = X_0 \in [2^{N+1}, 2^{N+2}) \longrightarrow$$
$$\longrightarrow b = \left(\frac{2X_0}{X_0^2 - 1}\right)^2,\ X_0 = \sqrt{1/b} + \sqrt{1+1/b} \longrightarrow$$
$$\longrightarrow \text{АГС}(1,b) \longrightarrow I(1,b) = \frac{\pi}{2\text{АГС}(1,b)} \longrightarrow$$
$$\longrightarrow \ln X_0 \approx I(1,b)/2 \longrightarrow \ln X = \ln X_0 - n \ln 2.$$

Предварительно домножением на подходящую степень двойки вход алгоритма приводится к интервалу $X_0 \in [2^{N+1}, 2^{N+2})$. Это гарантирует достаточную малость параметра b, такого, что $X_0 = \sqrt{1/b} + \sqrt{1+1/b}$. А именно, $b \leq 2^{-2N}$. Тогда, согласно лемме 5, $\ln X_0 = I(1,b)/2 + b/4 + \epsilon$. При этом ϵ по абсолютной величине можно оценить сверху как $\frac{b^{3/2}}{10} + \frac{b^2}{8} + \frac{b^2}{4} \ln X_0$. Если $N \geq 2$, то $\epsilon \leq b\left(\frac{1}{5 \cdot 2^{N+1}} + \frac{1}{2^{2N+3}} + \frac{N+2}{2^{2N+2}}\right) \leq b/4$, следовательно, $|\ln X_0 - I(1,b)/2| \leq b/2$.

Помимо вычисления АГС, алгоритм содержит несколько аддитивных операций, инвертирований и умножений, в том числе умножений на константы π и $\ln 2$, которые тоже нуждаются в вычислении. В действительности эти константы уже вычислены с точностью, по меньшей мере, до нескольких миллионов знаков — и этого достаточно для любых практических вычислений. Иначе, для вычисления указанных (и многих других) констант с точностью 2^{-n} известны алгоритмы сложности $O(\log n)M(n)$, их мы оставим за скобками.

Потребуем, чтобы интеграл $I(1,b)$ был вычислен с точностью $b/2$. Тогда точность, с которой вычисляется $\ln X_0$ оценивается как $3b/4$ и, при надлежащей точности заключительного вычитания точность вычисления $\ln X$ может быть оценена как b.

Оценим точность ϵ, с которой надо вычислить $\text{АГС}(1,b)$, чтобы обеспечить точность $b/2$ для $I(1,b)$. Для этого с точностью b надо вычислить отношение $\pi/\text{АГС}(1,b)$ (деление на 2 выполняется точно и при этом вдвое уменьшается погрешность). Так как некоторый запас точности (скажем, $b/2$) нужно оставить для инвертирования и умножения на π, то приближенное к АГС значение АГС* должно удовлетворять соотношению $|\pi/\text{АГС}^* - \pi/\text{АГС}(1,b)| \le b/2$. Это позволяет выписать соотношение для ϵ вида

$$\left|\frac{\pi}{\text{АГС}(1,b)-\epsilon} - \frac{\pi}{\text{АГС}(1,b)}\right| \le b/2.$$

Несложно получить оценку $\epsilon \le b(\text{АГС}(1,b)/\pi)^2$. Таким образом, можно положить $\epsilon = 2^{-2N-2\log_2 N - c_0}$ при подходящей константе c_0.

4 Точность вычисления АГС

Следует учесть, что выполняемые в ходе алгоритма действия дают приближенный результат (в случае квадратного корня, это в принципе неизбежно). Оценим рост абсолютной погрешности при вычислении АГС. Пусть в действительности вместо последовательностей $\{a_k\}$ и $\{b_k\}$ вычисляются последовательности $\{a'_k = a_k + e^a_k\}$ и $\{b'_k = b_k + e^b_k\}$. Обозначим $e_k = \max\{|e^a_k|, |e^b_k|\}$. Пусть E_M и E_Q обозначают погрешность выполнения умножения и вычисления квадратного корня соответственно.

Лемма 6.

$$e_{k+1} \le 2\frac{a_{k+1}}{b_{k+1}}e_k + \frac{e_k^2}{b_{k+1}} + E_Q + \sqrt{E_M}.$$

Доказательство. Ясно, что погрешность, вообще говоря, больше прирастает при вычислении b_k.

$$\begin{aligned}|b'_{k+1} - \sqrt{a_k b_k}| &= \left|\sqrt{a'_k b'_k + e^M_k} + e^Q_k - \sqrt{a_k b_k}\right| \le \\ &\le \left|\sqrt{a'_k b'_k + e^M_k} - \sqrt{a'_k b'_k}\right| + \left|\sqrt{a'_k b'_k} - \sqrt{a_k b_k}\right| + E_Q. \quad (1)\end{aligned}$$

Используя неравенство $|\sqrt{\alpha+\beta} - \sqrt{\alpha}| \le \sqrt{|\beta|}$, первое слагаемое в правой части (1) можно оценить как $\sqrt{E_M}$.

При помощи неравенства $|\sqrt{1+\epsilon} - 1| \le |\epsilon|$ второе слагаемое в правой части (1) оценим как

$$\left|\sqrt{(a_k+e_k^a)(b_k+e_k^b)}-\sqrt{a_kb_k}\right| \leq$$

$$\leq \sqrt{b'_k}\left|\sqrt{a_k+e_k^a}-\sqrt{a_k}\right|+\sqrt{a_k}\left|\sqrt{b_k+e_k^b}-\sqrt{b_k}\right| \leq$$

$$\leq \sqrt{\frac{b'_k}{a_k}}e_k+\sqrt{\frac{a_k}{b_k}}e_k = 2\frac{a_{k+1}}{b_{k+1}}e_k+e_k\sqrt{\frac{b_k}{a_k}}\left(\sqrt{b'_k/b_k}-1\right) \leq 2\frac{a_{k+1}}{b_{k+1}}e_k+\frac{e_k^2}{b_{k+1}}.$$

Лемма доказана.

Подбирая параметры $E_Q \leq e_k/3$, $E_M \leq e_k^2/9$ и, так как можно полагать (при надлежащем выборе e_0) $3e_k \leq b_{k+1}$, то имеем $e_{k+1} \leq \left(2\frac{a_{k+1}}{b_{k+1}}+1\right)e_k$ и, как следствие,

$$e_k \leq (2a_k/b_k+1)(2a_{k-1}/b_{k-1}+1)\cdot\ldots\cdot(2a_1/b_1+1)e_0.$$

В нашем случае

$$a_0/b_0 = 1/b = \left(\frac{X_0^2-1}{2X_0}\right)^2 \leq \left(\frac{2^{2N+4}-1}{2^{N+3}}\right)^2 < 2^{2N+2} < 1+2^{2^{1+\lceil\log_2(N+1)\rceil}}.$$

Пусть $m = \lceil\log_2(N+1)\rceil+1$. Тогда при помощи леммы 1 при $k \leq m-1$ можно оценить $2a_k/b_k+1$ как $3+2^{2^{m-k}+1} < 2^{2^{m-k}+2}$. А при $k \geq m$ указанное выражение оценим как $2a_m/b_m+1 \leq 2(1+2)+1 < 2^3$. Теперь при $k = L+m-1$ получаем

$$e_k \leq 2^{(2^{m-1}+2)+\ldots+(2^1+2)+3L}e_0 < 2^{2^m+2m+3L}e_0.$$

5 Сложность алгоритма

Оценим число итераций для вычисления АГС с необходимой точностью. Поскольку согласно лемме 1: $a_k-b_k \leq 2^{3-2^{k+1-m}}b_k$, то при $k \geq 2m+c_1$ погрешность, с которой любое из чисел a_k и b_k приближает АГС$(1,b)$, не превосходит $\epsilon/2 = 2^{-2N-2\log_2 N-c_0-1}$. Выбирая e_0 в виде $2^{-4N-7\log_2 N-c_2}$, получаем $e_k < \epsilon/2$ — это означает, что погрешность вычисления АГС в алгоритме не превосходит ϵ.

Таким образом, АГС вычисляется за $2\log_2 N + O(1)$ итераций, на каждой из которых выполняется умножение и извлечение корня с $(4+o(1))N$-разрядными числами. Поэтому общая сложность алгоритма составляет $O(\log N)M^*(N)$.

Заметим, что число b должно быть дано с точностью $2^{-(4+o(1))N}$, следовательно число X должно быть известно с точностью до $(2 + o(1))N$ знаков.