К-5. Асимптотика

3 ноября 2024 г. 23:19

O и другие буквы

- Умение сравнивать функции в окрестности какой-то предельной точки области определения — одно из базовых умений, прививаемых в курсе матанализа
- В дискретной математике/ компьютерных науках этот скилл востребован
- ★ В дискретной математике функции чаще всего заданы на $\mathbb{N}$, и сравнение проводится в окрестности единственной нетривиальной предельной точки ∞
  - т.е. «при больших n»
- Напомним базовые определения:
  - $f(n) = O(g(n))$, если существуют $n_0 \in \mathbb{N}, C > 0$: $|f(n)| \leqslant C|g(n)|$ для всех $n > n_0$
    - или $\overline{\lim}_{n\to\infty} \frac{|f(n)|}{|g(n)|} < \infty$

$f \nearrow$ медленнее g

  - $f(n) = o(g(n))$, если для любого $C > 0$ существует $n_0 \in \mathbb{N}$: $|f(n)| \leqslant C|g(n)|$ для всех $n > n_0$
    - или $\lim_{n\to\infty} \frac{|f(n)|}{|g(n)|} = 0$
  - $f(n) = \Omega(g(n))$, если существуют $n_0 \in \mathbb{N}, C > 0$: $|f(n)| \geqslant C|g(n)|$ для всех $n > n_0$
    - или $\underline{\lim}_{n\to\infty} \frac{|f(n)|}{|g(n)|} > 0$
  - $f(n) = \Theta(g(n))$, если $f(n) = O(g(n))$ и $f(n) = \Omega(g(n))$
    - или существуют $C_1, C_2 > 0$: $C_1 \leqslant \underline{\lim}_{n\to\infty} \frac{|f(n)|}{|g(n)|}, \overline{\lim}_{n\to\infty} \frac{|f(n)|}{|g(n)|} \leqslant C_2$

! В записях вида $f(n) = O(g(n))$ знак $=$ внезапно не означает равенства
  - иначе $n = O(n^2)$ и $n^2 = O(n^2)$ повлечет $n = n^2$

Учимся читать

- На примере O разберем, как правильно читать записи с асимптотическими обозначениями
- Пусть $g(n) : \mathbb{N} \to \mathbb{R}$
  - $O(g(n)) = \{f(n) \mid \exists n_0 \in \mathbb{N}, C > 0\ (\forall n > n_0)(|f(n)| \leqslant C|g(n)|)\}$
  - ★ $O(g(n))$ — множество функций
  - ★ мы отождествляем функцию $f(n)$ и множество $\{f(n)\}$
  - ★ запись $f(n) = O(g(n))$ означает $\{f(n)\} \subseteq O(g(n))$
  - ★ $O(n \log n) = O(n^2)$ — тоже включение множеств
  - синтаксис $f(n) = O(g(n))$ ничем не хуже, чем `n=n*n` в программировании
- Если S, T — два множества функций переменной n, то
  - ★ $S + T = \{f(n) + g(n) \mid f(n) \in S, g(n) \in T\}$
  - аналогично $S - T, ST, S/T, \sqrt{S}, e^S, \log S, \ldots$
- ★ Это позволяет выполнять преобразования выражений, например
  - $O(n^2)(n + O(\log n)) = O(n^3)$
- ★ Если вы понимаете описанный выше точный смысл O, то можете относится к записи $O(g(n))$ как к «почти» функции, определенной с точностью до несущественных деталей
- ★ Определение O можно распространить на функции нескольких переменных
  - например, $O(nm)$
  - подразумевается, что обе переменные стремятся к бесконечности: $\exists n_0, m_0, C \ldots$

! Как правильно интерпретировать O в записи $\sum_{k=1}^{n}(k^2 + O(k))$?

Учимся писать

- Простейшие O-преобразования:
  - ⋆ $f(n) = O(f(n))$
  - ⋆ $C \cdot O(f(n)) = O(f(n))$, если C — константа
  - ⋆ $O(O(f(n))) = O(f(n))$
  - ⋆ $O(f(n)) + O(g(n)) = O(|f(n)| + |g(n)|)$
  - ⋆ $O(f(n))O(g(n)) = O(f(n)g(n)) = f(n)O(g(n))$
  - ⋆ $\dfrac{1}{O(f(n))} = \Omega\Big(\dfrac{1}{f(n)}\Big)$

! В каких из приведенных формул $=$ действительно можно интерпретировать как равенство множеств?

Доказательство последней формулы:

- $O(f(n)) = \{h(n) \mid \exists n_0 \in \mathbb{N}, C > 0\, (\forall n > n_0)(|h(n)| \leqslant C|f(n)|)\}$

$\Rightarrow$ $\frac{1}{O(f(n))} = \left\{\frac{1}{h(n)} \mid \exists n_0 \in \mathbb{N}, C > 0\, (\forall n > n_0)(|h(n)| \leqslant C|f(n)|)\right\}$

- $|h(n)| \leqslant C|f(n)| \Leftrightarrow \left|\frac{1}{h(n)}\right| \geqslant \frac{1}{C} \cdot \frac{1}{|f(n)|}$

$\Rightarrow$ $\frac{1}{h(n)} = \Omega\left(\frac{1}{f(n)}\right)$ по определению □

Пример: $\sum_{k=1}^{n}(k^2 + O(k))$

- ⋆ $O(k)$ стоит под знаком суммирования, предел которого зависит от n

$\Rightarrow$ $O(k) = \{f(k,n) \mid \exists n_0 \in \mathbb{N}, C > 0\, (\forall n > n_0, k \leqslant n)(|f(k,n)| \leqslant Ck)\}$

$\Rightarrow$ $\sum_{k=1}^{n}(k^2 + O(k)) = \sum_{k=1}^{n} k^2 + \sum_{k=1}^{n} f(k,n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n + f(1,n) + \cdots + f(n,n)$

- $\left|\frac{1}{2}n^2 + \frac{1}{6}n + f(1,n) + \cdots + f(n,n)\right| \leqslant \frac{1}{2}n^2 + \frac{1}{6}n + C \cdot 1 + \cdots + C \cdot n \leqslant D \cdot n^2$

$\Rightarrow$ $\sum_{k=1}^{n}(k^2 + O(k)) = \frac{1}{3}n^3 + O(n^2)$

А. М. Шур (кф УрФУ) | O символика. Преобразования | Дискретная математика | 3 / 3

Учимся считать: уточнение формулы Стирлинга

Мы знаем формулу Стирлинга в виде $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

- Более точные варианты:
  - ⋆ $n! = \left(1 + O(\frac{1}{n})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$
  - ⋆ $n! = \left(1 + \frac{a}{n} + O(n^{-2})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$
  - ⋆ $n! = \left(1 + \frac{a}{n} + \frac{b}{n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ (1)
  - …
- Задача: уточнить формулу Стирлинга, найдя константу a
- Метод: шевеление (малое возмущение) формулы (1)
  - $n! = n(n-1)!$
  - $(n-1)! = \left(1 + \frac{a}{n-1} + \frac{b}{(n-1)^2} + O((n-1)^{-3})\right)\sqrt{2\pi(n-1)}\left(\frac{n-1}{e}\right)^{n-1}$
  - ⋆ заметим, что $\frac{n-1}{n} = 1 - n^{-1}$; $\frac{n}{n-1} = (1 - n^{-1})^{-1} = 1 + \frac{1}{n} + \frac{1}{n^2} + \cdots$ $\Rightarrow$
  - $\frac{a}{n-1} = \frac{a}{n} \cdot \frac{n}{n-1} = \frac{a}{n} + \frac{a}{n^2} + O(n^{-3})$
  - $\frac{b}{(n-1)^2} = \frac{b}{n^2} + O(n^{-3})$
  - $O((n-1)^{-3}) = O(n^{-3})$
  - $\sqrt{2\pi(n-1)} = \sqrt{2\pi n}(1 - n^{-1})^{1/2} = \sqrt{2\pi n}\left(1 - \frac{1}{2n} - \frac{1}{8n^2} + O(n^{-3})\right)$
    - формула Тейлора $(1+x)^\alpha = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2}x^2 + O(x^3)$ при $x = -\frac{1}{n}$, $\alpha = \frac{1}{2}$
- Имеем
  - $(n-1)! = \left(1 + \frac{a}{n} + \frac{a+b}{n^2} + O(n^{-3})\right)\left(1 - \frac{1}{2n} - \frac{1}{8n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n-1}{e}\right)^{n-1}$

Уточнение формулы Стирлинга (2)

$(n-1)! = \left(1 + \frac{a}{n} + \frac{a+b}{n^2} + O(n^{-3})\right)\left(1 - \frac{1}{2n} - \frac{1}{8n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n-1}{e}\right)^{n-1}$

- Оценим $(n-1)^{n-1}$:
  - $(n-1)^{n-1} = n^{n-1}(1-n^{-1})^{n-1} = n^{n-1}(1-n^{-1})^n(1+n^{-1}+n^{-2}+O(n^{-3}))$
  - $(1-n^{-1})^n = e^{n\cdot\ln(1-n^{-1})} =$ [Тейлор]
    $= e^{n\left(-\frac{1}{n}-\frac{1}{2n^2}-\frac{1}{3n^3}+o\left(\frac{1}{n^4}\right)\right)} = e^{-1-\frac{1}{2n}-\frac{1}{3n^2}+o\left(\frac{1}{n^3}\right)} =$ [Тейлор]
    $= e^{-1}\left(1 - \frac{1}{2n} + \frac{1}{8n^2} + O(n^{-3})\right)\left(1 - \frac{1}{3n^2} + O(n^{-3})\right)\left(1 + O(n^{-3})\right)$
    $= e^{-1}\left(1 - \frac{1}{2n} - \frac{5}{24n^2} + O(n^{-3})\right)$
- Перемножим все скобки вида $1 + o(1)$:

$$\left(1+\frac{a}{n}+\frac{a+b}{n^2}+O(n^{-3})\right)\left(1-\frac{1}{2n}-\frac{1}{8n^2}+O(n^{-3})\right)\left(1+\frac{1}{n}+\frac{1}{n^2}+O(n^{-3})\right)\cdot$$
$$\left(1-\frac{1}{2n}-\frac{5}{24n^2}+O(n^{-3})\right) = \left(1+\frac{a}{n}+\frac{a+b-1/12}{n^2}+O(n^{-3})\right)$$

- В итоге,
  - $n! = n(n-1)! = n\left(1 + \frac{a}{n} + \frac{a+b-1/12}{n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^{n-1}\cdot\frac{1}{e} =$
    $= \left(1 + \frac{a}{n} + \frac{a+b-1/12}{n^2} + O(n^{-3})\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \qquad (2)$
- Коэффициенты (2) равны коэффициентам исходной формулы Стирлинга (1)
  $\Rightarrow$ $a + b - \frac{1}{12} = b \Rightarrow a = \frac{1}{12}$

★ выражение $\left(1 + \frac{1}{12n}\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ дает очень хорошее приближение для n!

Учимся считать: n-е простое число

Пусть $\pi(n)$ — количество простых чисел, не превосходящих n

★ Одна из важнейших комбинаторных теорем утверждает, что $\pi(n) \sim \frac{n}{\ln n}$
  ★ более точно, $\pi(n) = \frac{n}{\ln n} + O\left(\frac{n}{\ln^2 n}\right)$

- Задача: найти асимптотическую формулу для n-го простого числа
- Решение: пусть $p = p(n)$ — n-е простое число, тогда $\pi(p) = n$
  $\Rightarrow$ $n = \frac{p}{\ln p} + O\left(\frac{p}{\ln^2 p}\right)$
    ⋆ надо решить это «уравнение» относительно p
  - $O\left(\frac{p}{\ln^2 p}\right) = o\left(\frac{p}{\ln p}\right) \Rightarrow \frac{p}{\ln p} = O(n)$

  $\Rightarrow$ $O\left(\frac{p}{\ln^2 p}\right) = O\left(\frac{n}{\ln p}\right) = O\left(\frac{n}{\ln n}\right)$ (т.к. $p > n$)
  $\Rightarrow$ $\frac{p}{\ln p} = n + O\left(\frac{n}{\ln n}\right) = n\left(1 + O\left(\frac{1}{\ln n}\right)\right) \Rightarrow p = n\ln p\left(1 + O\left(\frac{1}{\ln n}\right)\right)$
    ⋆ надо избавиться от $\ln p$ справа; логарифмируем обе части
  - $\ln p = \ln n + \ln\ln p + O\left(\frac{1}{\ln n}\right)$

  $\Rightarrow$ $p < n^2$ для больших $n \Rightarrow \ln p < 2\ln n \Rightarrow \ln\ln p < \ln\ln n + O(1)$
  $\Rightarrow$ $\ln p = \ln n + \ln\ln n + O(1)$
  $\Rightarrow$ $p = n(\ln n + \ln\ln n + O(1))\left(1 + O\left(\frac{1}{\ln n}\right)\right) = n\ln n + n\ln\ln n + O(n)$ □

! Начав с более точной формулы $\pi(n) = \frac{n}{\ln n} + \frac{n}{\ln^2 n} + O\left(\frac{n}{\ln^3 n}\right)$, выведите более точное приближение для p

Функции, часто встречающиеся под знаком O

- Рассматриваем только бесконечно большие (в $n = \infty$) функции
  - ★ бесконечно малые получаются как обратные к бесконечно большим

  Основные классы:
  - ★ $f(n) = n$ и полиномиальные функции
    - существуют $\alpha, \beta > 0$ такие, что $f(n) = O(n^\alpha)$ и $f(n) = \Omega(n^\beta)$
  - ★ $f(n) = 2^n$ и экспоненциальные функции
    - $f(n) = 2^{p(n)}$ для некоторой полиномиальной функции $p(n)$
  - ★ часто экспоненциальные функции понимаются в более узком смысле, как $2^{\Omega(n)}$
    - ★ получается, если в определении полиномиальной функции потребовать $\beta \geqslant 1$
  - ★ тогда функции вида $2^{\sqrt[3]{n}}$ или $2^{\frac{n}{\log n}}$ называют почти экспоненциальными
  - ★ $f(n) = \log n$ и полилогарифмические функции
    - $f(n) = p(\log n)$ для некоторой полиномиальной функции $p(n)$

★ полилогарифмические $<$ полиномиальные $<$ экспоненциальные

★ реже приходится иметь дело с функциями, которые растут
- быстрее экспоненциальных:
  - ★ число n-местных функций на двухэлементном множестве равно 2^{2^n}
- медленнее полилогарифмических:
  - ★ двоичная запись длины двоичного числа n содержит $\log\log n$ бит

★ В моей научной работе встречались
- ★ $\sqrt{\frac{\log\log n}{\log\log\log n}}$ (время обращения к некоторому словарю)
- ★ $\left.2^{2^{\cdot^{\cdot^{\cdot^{2^n}}}}}\right\}$ n двоек (оценка некоторой комбинаторной функции)

Время работы некоторых алгоритмов

- $O(\log n)$: двоичный поиск в упорядоченном массиве из n элементов
- $O(m)$: поиск в глубину или ширину в связном графе с m ребрами
- $O(n\log n)$: Mergesort и некоторые другие сортировки массива из n элементов
  - ★ для сортировки сравнением мы доказывали нижнюю оценку $\Omega(n\log n)$
- $O(n^2)$: умножение столбиком двух чисел по n цифр
- $O(n^3)$: поиск обратной матрицы методом Гаусса
- $O\left(p(n)(\sqrt{2})^n\right)$: проверка простоты n-битного числа перебором делителей
- $O(n!)$: переборное решение задачи коммивояжера
  - ★ можно понизить сложность до $O(n^2 2^n)$ алгоритмом Хелда–Карпа
- $O(m+n)$: поиск в глубину или ширину в произвольном графе
- $O(mn)$: редактирование строк минимальным числом вставок/удалений/замен
- $O(2^k n)$: поиск k-элементного вершинного покрытия в графе с n вершинами