toolkit

we will see how it goes.

authors: shaleen baral

Contents

i. asymptotics

i.i. introduction

For simplicity, all our functions are of the type $\mathbb{N} \longrightarrow \mathbb{R}$.

Definition 1.1.1: We say that $f(n)$ is *asymptotically equivalent* to $g(n)$ and write $f(n) \sim g(n)$ if $f(n)/g(n) \to 1$ as $n \to \infty$.

Definition 1.1.2: We write $f(n) \in O(g(n))$ when there is a $C > 0$ such that for all sufficiently large n,

$$|f(n)| \leq C|g(n)|.$$

Remark: Technically, $O(\cdot)$ represents a set of functions. Still, we may write an equation involving $O(\cdot)$ (for eg. $f = O(g)$) in which case $O(\cdot)$ just represents some function from this asymptotic class. This remark holds for all the other asymptotic classes we will define.

Definition 1.1.3: We write $f(n) \in \Omega(g(n))$ when there is a $c > 0$ such that for all sufficiently large n,

$$|f(n)| \geq c|g(n)|.$$

Lemma 1.1.1: Equivalently, $f(n) = O(g(n))$ if and only if $\limsup_{n \longrightarrow \infty} |f(n)|/|g(n)| < \infty$.

Proof: For convenience, let $Q(n) = |f(n)|/|g(n)|$. First, the foward direction. We note that we have $0 \leq Q(n) \leq C$. As $Q(n)$ is bounded, $\limsup Q(n)$ clearly exists and is finite (the sequence $\{\sup_{n \geq k} Q(n)\}_{k \in N}$ is decreasing and as it is bounded by below, must converge).

Conversely, assume $\limsup Q(n) < \infty$. Let $C = \limsup Q(n) + 1$. As $C > \limsup Q(n)$, it is an eventual upper bound for $Q(n)$. That is to say, there exists $N \in \mathbb{N}$ such that for all $n \geq N$

$$|f(n)| \leq C|g(n)|.$$

□

Lemma 1.1.2: Equivalently, $f(n) = \Omega(g(n))$ if and only if $\liminf_{n \longrightarrow \infty} |f(n)|/|g(n)| > 0$.

Proof: For convenience, let $Q(n) = |f(n)|/|g(n)|$. For the forward direction, we note that there exists $N \in \mathbb{N}$ and $c > 0$ such that for all $n \geq N$

$$\begin{aligned} |f(n)| &\geq c|g(n)| \\ \Longrightarrow Q(n) &\geq c. \end{aligned}$$

Note that c is a lower bound for $\{Q(n)\}_{n \in \mathbb{N}}$. Consequently, it must be a lower bound for the tailing sequences $\{Q(n)\}_{n \geq m}$ for any m. Then, we have

$$\liminf_{n \to \infty} Q(n) = \sup_{m \in \mathbb{N}} \inf_{n \geq m} Q(n) \geq c > 0.$$

Conversely, assume $\liminf Q(n) > 0$. Choose any $c \in (0, \liminf Q(n))$. Then, such a c is an eventual lower bound for $Q(n)$. That is, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, we have

$$|f(n)| \geq c|g(n)|.$$

□

Definition 1.1.4: We write $f(n) = \Theta(g(n))$ when there are constants $c, C > 0$ such that

$$c|g(n)| \leq f(n) \leq C|g(n)|.$$

Equivalently, $f(n) = \Theta(g(n))$ iff $f(n) = \Omega(g(n))$ and $f(n) = O(g(n))$.

Lemma 1.1.3: If $f_1, f_2 \in O(g)$ then $f_1 + f_2 \in O(g)$.

Proof: There exists $C_1, C_2, N_1, N_2 > 0$ such that for $n \geq N_1$ and $n \geq N_2$

$$|f_1| \leq C_1|g| \qquad \text{and} \qquad |f_2| \leq C_2|g|.$$

Then, for $N = \max(N_1, N_2)$, we can say that if $n \geq N$ then

$$|f_1 + f_2| \leq (C_1 + C_2)\ |g|.$$

□

Lemma 1.1.4: If $f_1, f_2 \in \Omega(g)$ then $f_1 + f_2 \in \Omega(g)$ too.

Proof: Same idea as above.

□

Remark: A stronger statement is possible: if $f_1 \in \Omega(g)$ and $f \geq f_1$ then $f \in \Omega(g)$.

Lemma 1.1.5: If $f_1, f_2 \in \Theta(g)$ then $f_1 + f_2 \in \Theta(g)$ too.

Proof: Follows from prior two lemmas and definition of Θ.

□

Definition 1.1.5: We write $f(n) \in (g(n))$ (or $f(n) \ll g(n)$) if $f(n)/g(n) \to 0$ as $n \to \infty$.

Definition 1.1.6: We write $f(n) \in \omega(g(n))$ (or $f(n) \gg g(n)$) if $f(n)/g(n) \to \infty$ as $n \to \infty$.

Lemma 1.1.6: If $f_1, f_2 \in o(g)$ then $f_1 + f_2 = o(g)$.

Proof:

$$\lim_{n\to\infty} \frac{f_1(n) + f_2(n)}{g(n)} = \lim_{n\to\infty} \frac{f_1(n)}{g(n)} + \lim_{n\to\infty} \frac{f_2(n)}{g(n)} = 0.$$

□

Lemma 1.1.7: If $f_1, f_2 \in \omega(g)$ then $f_1 + f_2 = \omega(g)$.

Proof: Same idea as above. □

Remark: A stronger statement is possible: if $f_1 \in \omega(g)$ and $f \geq f_1$ then $f \in \omega(g)$.

Remark: Note that $O(\cdot)$ and $\Omega(\cdot)$ both induce a *pre order* (a reflexive, transitive relation) on functions $\mathbb{N} \to \mathbb{R}$. Similarly, $o(\cdot)$ and $\omega(\cdot)$ induce a *strict partial order* (an irreflexive, transtive relation). Finally, $\Theta(\cdot)$ induces an *equivalence relation* (a reflexive, symmetric, transitive relation). Consequently, $O(\cdot)$ and $\Omega(\cdot)$ induce a *non-strict partial order* (an antisymmetric preorder) on these equivalence classes.

We think of $O(\cdot), \Omega(\cdot), \Theta(\cdot)$ as making claims about the *asymptotic bounds* of functions. We think of $o(\cdot), \omega(\cdot)$ as making claims about the *relative growth* of functions. The following lemmas should illustrate this point.

Lemma 1.1.8: If $f = o(g)$ then $f = O(g)$. In fact, any positive constant $C > 0$ can be used to satisfy the definition of $O(g)$.

Proof: By definition, we have $\lim_{n \longrightarrow \infty} \frac{f(n)}{g(n)} = 0$. So for any $C > 0$, there exists $N \in \mathbb{N}$ such that for all $n \geq N$, we have

$$\left|\frac{f(n)}{g(n)}\right| \leq C$$
$$\Rightarrow |f(n)| \leq C|g(n)|.$$

□

Lemma 1.1.9: If $f = \omega(g)$ then $f = \Omega(g)$. In fact, any positive constant $c > 0$ can be used to satisfy the definition of $\Omega(g)$.

Proof: By definition, we have $\lim_{n \longrightarrow \infty} \frac{f(n)}{g(n)} = \infty$. That is to say for every $c > 0$, there exists $N \in \mathbb{N}$ such that for all $n \geq \mathbb{N}$,

$$\left|\frac{f(n)}{g(n)}\right| \geq c$$
$$\Longrightarrow |f(n)| \geq c|g(n)|.$$

□

The following is a common way to denote asymptotic equivalence.

Lemma 1.1.10: $f \sim g$ if and only if $f(n) = g(n)(1 + o(1))$.

Proof:

$$\lim_{n \longrightarrow \infty} \frac{f(n)}{g(n)} = 1 \Longleftrightarrow \lim_{n \longrightarrow \infty} \left[\frac{f(n)}{g(n)} - 1\right] = 0 \Longleftrightarrow \frac{f(n)}{g(n)} - 1 = o(1)$$

.

□

A convenient result is that we can *sandwich* our function to obtain a result of asymptotic equivalence.

Lemma 1.1.11: Suppose there are functions $\mathrm{LB} \sim g, \mathrm{UB} \sim g$ such that

$$\mathrm{LB}(n) \leq f(n) \leq \mathrm{UB}(n).$$

Then, $f \sim g$.

Proof:

$$\lim_{n\to\infty}\frac{\mathrm{LB}(n)}{g(n)} \le \lim_{n\to\infty}\frac{f(n)}{g(n)} \le \lim_{n\to\infty}\frac{\mathrm{UB}(n)}{g(n)}$$
$$\Longrightarrow 1 \le \lim_{n\to\infty}\frac{f(n)}{g(n)} \le 1$$
$$\Longrightarrow \lim_{n\to\infty}\frac{f(n)}{g(n)} = 1.$$

□

Usually, we end up decomposing a function into two terms—one which is asymptotically equivalent to our target and one that is negligble with respect to it.

Lemma 1.1.12: If $f = f_1 + f_2$ where $f_1 \sim g$ and $f_2 = o(g)$, then $f \sim g$

Proof:

$$\lim_{n\to\infty}\frac{f(n)}{g(n)} = \lim_{n\to\infty}\frac{f_1(n)}{g(n)} + \lim_{n\to\infty}\frac{f_2(n)}{g(n)} = 1.$$

□

i.ii. the hierarchy

Here is the dream.

Definition 1.2.1: A function is $g(n)$ is said to be in *standard form* if it is the product of the following types

a. Constants (eg. $\sqrt{2\pi}, 6, e^{-2}$)
b. Constant powers of n (eg. $n, \sqrt{n}, n^{\frac{5}{2}}, n^{-3}$)
c. Constant powers of $\ln n$ (eg. $\ln n, \sqrt{\ln n}, \frac{1}{\ln n}$)
d. Exponentials (eg. $2^n, e^{-n}, 2^{\frac{n}{2}}$)
e. n^{cn} for constant c (eg. n^n)

Proposition 1.2.1: For all $K > 0$ and $\varepsilon > 0$

$$\ln^K n \ll n^{\varepsilon},$$
$$n^K \ll (1+\varepsilon)^n,$$
$$K^n \ll n^{\varepsilon n}.$$

Proof: Start with $f(n) = n^K$ and $g(n) = (1+\varepsilon)^n$. Note that,

$$\lim_{n\to\infty}\frac{f(n+1)}{f(n)} = \lim_{n\to\infty}\left(1+n^{-1}\right)^K = 1^K = 1.$$

Take any c such that $1 < c < 1+\varepsilon$. There exist n_0 such that for all $n > n_0$, $\frac{f(n+1)}{f(n)} < c$. Then,

$$\frac{f(n_0+m)}{g(n_0+m)} \le \frac{c^m f(n_0)}{(1+\varepsilon)^m g(n_0)} \to 0$$

as $m \to \infty$.

Note that under the parametrization $n = e^m$, $\ln^K n \ll n^{\varepsilon}$ becomes $m^K \ll (e^{\varepsilon})^m$. Note that from the above result,

$$m^K \ll (1+\varepsilon)^K \ll (e^{\varepsilon})^K$$

using the fact that $1 + x \leq e^x$.

Finally, for the last result, fix $c > K$ and n_0 with $n_0^\varepsilon \geq c$. For $n \geq n_0$, $n^{\varepsilon n} \geq c^n \gg K^n$.

□

Sometimes we see a $(1 + o(1))$ factor in the exponent. This gives very crude bounds. For example, $f(n) = g(n)^{1+o(1)}$ is equivalent to saying that

a. for any $\varepsilon > 0$, for n sufficiently large, $f(n) > g(n)^{1-\varepsilon}$.
b. for any $\varepsilon > 0$, for n sufficiently large, $f(n) < g(n)^{1+\varepsilon}$.

This is a much weaker claim then $f \sim g$. For example, if we have $g(n) = n^2$ then $f(n)$ could be any of $n^2, n^2 \ln n, n^2 \ln^5 n, n^2 \ln^{-3} n$.

Working with asymptotics can simplify issues quite a bit. Consider the following theorem.

Proposition 1.2.2: Let $a, c > 0$ and and $b \in \mathbb{R}$. Define, for $x > 1$, $f(x) = cx^a \ln^b x$. For y sufficiently large, there is a unique x with $y = f(x)$. Write $x = g(y)$ for such y. Asymptotically in y,

$$x \sim dy^{1/a} (\ln y)^{-b/a},$$

where $d = a^{a/b} c^{-1/a}$.

Proof: Start by noting that, eventually the x^a term dominates the polylogarithmic term to make f increasing. More formally, note that

$$\begin{aligned} f'(x) &= acx^{a-1} \ln^b x + bcx^{a-1} \ln^{b-1} x \\ &= cx^{a-1} \ln^b x \cdot \left(a + \frac{b}{\ln x}\right). \end{aligned}$$

There exists $x_0 > 1$ such that for all $x > x_0$, we have $\frac{|b|}{a} < \ln x$. So, for all $x > x_0$, we have $f'(x) > 0$. Thus, f' is eventually increasing.

For large x,

$$\ln y = \ln c + a \ln x + b \ln \ln x \sim a \ln x.$$

where the asymptotic equivalence is justified by $\ln c, \ln \ln x \in o(\ln x)$.

Now, consider

$$\begin{aligned} & y = cx^a \ln^b x \\ \Longrightarrow\ & x = c^{-1/a} y^{1/a} (\ln x)^{-b/a} \\ & \quad \sim a^{a/b} c^{-1/a} y^{1/a} (\ln y)^{-b/a}. \end{aligned}$$

□

Proposition 1.2.3: If $y = \Theta\left(x^a \ln^b x\right)$ then $x = \Theta\left(y^{1/a} \ln^{-b/a} x\right)$.

i.iii. stirling's approximation

The following is the main result also known as Stirling's formula.

Proposition 1.3.1:

$$n! \sim n^n e^{-n} \sqrt{2\pi n}.$$

The proof of this theorem is slightly technical and so, has been omitted in favor of weaker results with shorter proofs. I would still recommend studying a proof of this– I like the exposition in Spencer and Florescu's *Asymptopia* as well as Keith Conrad's notes.

We estimate the logarithm of $n!$ via the formula

$$S_n = \ln(n!) = \sum_{k=1}^{n} \ln k.$$

We expect S_n to be close to the integral of the function $\ln x$ between $x = 1$ and $x = n$. Define

$$I_n = \int_1^n \ln x \, dx = [x \ln x - x]_1^n = n \ln n - n + 1.$$

Let T_n be the value for the approximation of the integral I_n via the trapezoidal rule using step size 1. That is, estimate $\int_i^{i+1} f(x)dx$ by $\frac{1}{2}(f(i) + f(i+1))$. Summing up over $1 \leq i \leq n-1$,

$$T_n = \frac{1}{2} \ln 1 + \sum_{k=2}^{n-1} \ln k + \frac{1}{2} \ln n = S_n - \frac{1}{2} \ln n.$$

We estimate the error in this approximation by definine

$$E_n = I_n - T_n.$$

Furthermore, for $1 \leq k \leq n-1$, let S_k denote the *sliver* of area under the curve $y = \ln x$ for $k \leq x \leq k+1$ but over the straight line between $(k, \ln k)$ and $(k+1, \ln(k+1))$. As the curve $\ln x$ is concave, the curve is over the straight line and we have,

$$E_n = \sum_{k=1}^{n-1} \mu(S_k)$$

with μ denoting the area.

Lemma 1.3.1:

$$\lim_{n \to \infty} E_n = c < \infty.$$

Proof: Let $P = (k, \ln k)$ and let $Q = (k+1, \ln(k+1))$. Furthermore, let C denote the curve $f(x) = \ln x$ in the interval $[k, k+1]$. Furthermore, f has derivative between $\frac{1}{k}$ and $\frac{1}{k+1}$ on the interval $[k, k+1]$. Let U denote the straight line segment starting at P with slope $\frac{1}{k}$ and ending at $x = k+1$. Let L be the straight line segment starting at P with slope $\frac{1}{k+1}$, ending at $x = k+1$.

As the derivative of C is always between those of U and L, the curve C is under U and over L. That is to say, at $x = k+1$, L then is below the curve C, below the point Q. Thus, the straight line PQ lies above the line L and we can bound $\mu(S_k)$ by the area between U and L. The latter is a triangle with height being 1 and base being the line from U to L at $x = k+1$ which has length $\frac{1}{k} - \frac{1}{k+1}$. Thus,

$$\mu(S_k) \leq \frac{1}{2}\left(\frac{1}{k} - \frac{1}{k+1}\right).$$

This value is $O(k^{-2})$ and we achieve convergence. We even obtain the explicit upper bound,

$$\sum_{k=1}^{\infty} \mu(S_k) \leq \sum_{k=1}^{\infty} \frac{1}{2}\left(\frac{1}{k} - \frac{1}{k+1}\right) = \frac{1}{2}.$$

□

Proposition 1.3.2: There is some positive constant K, such that

$$n! \sim K n^n e^{-n} \sqrt{n}.$$

Proof: From the definitions above,

$$\begin{aligned} \ln(n!) &= T_n + \frac{1}{2} \ln n \\ &= I_n - E_n + \frac{1}{2} \ln n \end{aligned}$$

The lemma above gives us,

$$= n \ln n - n + \frac{1}{2} \ln n + 1 - c + o(1)$$

Exponentiating this gives us,

$$n! \sim n^n e^{-n} \sqrt{n} e^{1-c}.$$

□

We can get a more precise approximation by putting more effort into estimating the error and using the fact that $K = \sqrt{2\pi}$.

i.iv. taylor's theorem

ii. binomial coefficients

ii.i. introduction

ii.ii. bounds

iii. primes

iii.i. using asymptotics

iii.ii. prime number theorem

iii.iii. bertrand's postulate

iv. integrals

iv.i. approximating sums

iv.ii. harmonic numbers

v. just some beautiful results

Of course subjective, but for whatever reasons I think the results below are quite striking.

v.i. greshgorin's circles

simplicity

v.ii. amitsur-levitzki

shocking

v.iii. prüfer encoding

elegant

v.iv. dft

neat ‘things fit in’

v.v. mastering floors and ceilings

master theorem, also sunk cost