# tutorial2-2024

Thursday, September 12, 2024 11:10 AM

Notation In this course: $(\log n)^2 = (\log n)(\log n)$

$$\log^{(2)} n = \log(\log n)$$

Example: $\log^* 16 = ?$

$$\left.\begin{aligned} \log 16 &= 4 \\ \log 4 &= 2 \\ \log 2 &= 1 \end{aligned}\right\} \text{ so } \log^* 16 = 3$$

$\log^* n$ is the slowest growing function in this course for most algorithms

## Useful properties

$f(n) = 2^{n^2}$ $\quad g(n) = 3^n$ $\quad$ We want to calculate $\lim_{n\to\infty} \frac{2^{n^2}}{3^n}$

$\log a^b = b \log a$

log of limits

$$\log\left(\lim_{n\to\infty} \frac{2^{n^2}}{3^n}\right) = \lim_{n\to\infty}\left(\log \frac{2^{n^2}}{3^n}\right) = \lim_{n\to\infty} \frac{n^2 \log 2}{n \log 3} = \infty$$

Since $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 2^{\infty} = \infty$

then $f(n) = \Omega(g(n))$

## Order of functions

tutorial2-2024

# ECE345 Tutorial 2

Winston (Yuntao) Wu

Electrical & Computer Engineering



## Outline

1. Notations
2. Asymptotics
3. Proof Methods



## Notations

Sets:
$\mathbb{N} = \{1, 2, 3, ...\}$: all natural numbers (LaTeX: \mathbb{N})
$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$: all integers (LaTeX: \mathbb{Z})
$\mathbb{R}$ = all real numbers (LaTeX: \mathbb{R})
$\emptyset$: empty set (LaTeX: \emptyset)
$x \in S$: $x$ is an element of a set $S$ (LaTeX: x \in S)
$x \notin S$: $x$ is not an element of a set $S$ (LaTeX: x \notin S)
$A \subset B$: $A$ is a subset of $B$ i.e. all elements in $A$ is in $B$(LaTeX: A \subset B)
$A \not\subset B$: $A$ is not a subset of $B$ (LaTeX: A \not \subset B)
$\mathcal{P}(X) = \{Y : Y \subset X\}$: the power set of $X$, i.e. the set of all subset of $X$ (LaTeX: \mathcal{P}(X))

Set operations:
Union: $A \cup B = \{x : x \in A \text{ or } x \in B\}$ (LaTeX: A \cup B)
Intersection: $A \cap B = \{x : x \in A \text{ and } x \in B\}$ (LaTeX: A \cap B)
Difference: $A - B = A \backslash B = \{x : x \in A \text{ and } x \notin B\}$
Complement: Fix a universe $U$, $A \subset U$, $\bar{A} = C_U A = \{x \in U, x \notin A\}$ (LaTeX: \bar{A})
Cartesian product: $A \times B = \{(a, b) : a \in A, b \in B\}$

## Notations

Logics:
Negation: $\neg P$, $\sim P$, $\bar{P}$, (LaTeX: \lnot, \sim)
And: $P \land Q$ (LaTeX: \land)
Or: $P \lor Q$ (LaTeX: \lor)

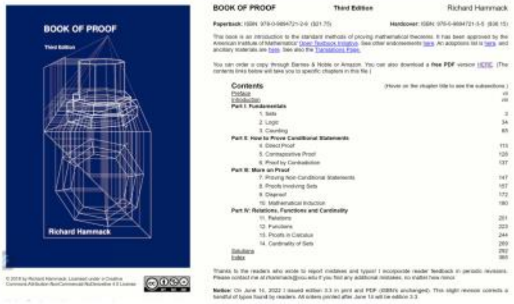
Quantifiers:
$\exists$ there exists (LaTeX: \exists)
$\forall$ for all, for any (LaTeX: \forall)

Other symbols:
s.t. such that
$\Leftarrow$ implies (LaTeX: \Leftarrow)
$\Leftrightarrow$ if and only if (equivalently) (LaTeX: \Leftrightarrow)
$\because$ because (LaTeX: \because)
$\therefore$ therefore (LaTeX: \therefore)
$[a, b] = \{x : a \leq x \leq b\}$, $(a, b) = \{x : a < x < b\}$
$(a, b] = \{x : a < x \leq b\}$, $[a, b) = \{x : a \leq x < b\}$



## Book of Proof

For more notations & examples of proof methods, please check the *Book of Proof* by Richard Hammack in the following link: `https://www.people.vcu.edu/~rhammack/BookOfProof/`






## Outline

1 Notations

2 Asymptotics

3 Proof Methods

## Definition

- $f(n) = \mathcal{O}(g(n)) \Leftrightarrow \exists c, n_0 > 0$ s.t. $0 \le f(n) \le cg(n)$, $\forall n \ge n_0$
- $f(n) = \Omega(g(n)) \Leftrightarrow \exists c, n_0 > 0$ s.t. $0 \le cg(n) \le f(n)$, $\forall n \ge n_0$
- $f(n) = \Theta(g(n)) \Leftrightarrow f(n) = \mathcal{O}(g(n))$ and $f(n) = \Omega(g(n) \Leftrightarrow \exists c_1, c_2, n_0 > 0$ s.t. $0 \le c_1 g(n) \le f(n) \le c_2 g(n)$, $\forall n \ge n_0$

e.g. (2022 final): What does it mean by $n! = n^n e^{-n}\sqrt{2\pi n}\left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right)$ (Stirling formula[1])?

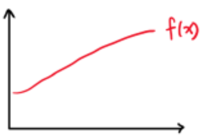
[1] For those who are interested, the Stirling's formula can be derived from the gamma function $\Gamma(z) = \int_0^\infty t^{z-1}e^{-t}dt$ for Re$(z) > 0$.
$n! = \Gamma(n+1) = \int_0^\infty t^n e^{-t}dt = n^n e^{-n}\sqrt{2\pi n}\left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right)$ by Laplace's method.



## Intuition

$\mathcal{O}$:

- $f \le g \Leftrightarrow f(n) \le g(n)$, $\forall n$
- $f$ **eventually** $\le g \Leftrightarrow \exists n_0 > 0$ s.t. $f(n) \le g(n)$, $\forall n \ge n_0$
- $f$ eventually grows **slower** than or the **same** as $g \Leftrightarrow \exists c, n_0 > 0$ s.t. $f(n) \le g(n) + c$, $\forall n \ge n_0$
- $f$ eventually grows **slower** than or **similar** to $g \Leftrightarrow \exists c, n_0 > 0$ s.t. $f(n) \le cg(n)$, $\forall n \ge n_0$




$\Omega$ is similar.
For $\Theta$, we can bound $f$ from below and above.



## Example

Prove that $2^{n+1} = \mathcal{O}(2^n)$.

Solution:

Prove that $2^{n+1} = \Omega(2^n)$.

Solution:

## Example

Prove that $(n+a)^b = \Theta(n^b)$.

Solution:



## Properties

Transitivity: $f(n) = \Theta(g(n))$ and $g(n) = \Theta(h(n)) \Rightarrow f(n) = \Theta(h(n))$

Transpose: $f(n) = \mathcal{O}(g(n)) \Leftrightarrow g(n) = \Omega(f(n))$

Symmetry: $f(n) = \Theta(g(n)) \Rightarrow g(n) = \Theta(f(n))$



## Limit Method

- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0 \Rightarrow f(n) = o(g(n))^2$ (The 2 and 3 here are refering to the footnote numbers.)
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} < \infty \Rightarrow f(n) = \mathcal{O}(g(n))$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty \Rightarrow f(n) = \omega(g(n))^3$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} > 0 \Rightarrow f(n) = \Omega(g(n))$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = c,\ c \in (0,\infty) \Rightarrow f(n) = \Theta(g(n))$

L'Hopital's rule: $\lim_{x\to a} \frac{f(x)}{g(x)} = \frac{0}{0}$ or $\frac{\infty}{\infty} \Rightarrow \lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)}$

[2] $f(n) = o(g(n))$ if and only if $\forall c > 0$, $\exists n_0 > 0$ such that $0 \le f(n) < cg(n)$ for all $n \ge n_0$.

[3] $f(n) = \omega(g(n))$ if and only if $\forall c > 0$, $\exists n_0 > 0$ such that $0 \le cg(n) < f(n)$ for all $n \ge n_0$.

## Limit Method (More Precisely)

- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0 \Rightarrow f(n) = o(g(n))$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = c \in [0,\infty) \Rightarrow f(n) = \mathcal{O}(g(n))$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = c \in (0,\infty) \Rightarrow f(n) = \Theta(g(n))$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = c \in (0,\infty] \Rightarrow f(n) = \Omega(g(n))$
- $\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty \Rightarrow f(n) = \omega(g(n))$



## Useful results

$n^a = \mathcal{O}(n^b) \Leftrightarrow a \leq b$

$\log_a n = \mathcal{O}(\log_b n), \forall a, b > 1$

$c^n = \mathcal{O}(d^n) \Leftrightarrow c \leq d$



## Bounded Functions

Polylogarithmically bounded: $\exists k > 0,\ f(n) = \mathcal{O}((\log n)^k)$
Polynomially bounded: $\exists k > 0,\ f(n) = \mathcal{O}(n^k)$
Exponentially bounded: $\exists k > 0,\ f(n) = \mathcal{O}(k^n)$

**Remark**

Notation (in this course): $(\log n)^2 = (\log n)(\log n)$ and $\log^{(2)} n = \log(\log n)$
$\log^* n = \min\{i \geq 0 : \log^{(i)} n \leq 1\}$

## Polynomially-Bounded Functions

**Theorem**

$f(n) = \mathcal{O}(n^k) \Leftrightarrow \log(f(n)) = \mathcal{O}(\log n)$

**Theorem**

All Logarithmically bounded functions are polynomically bounded. i.e. $f(n) = \mathcal{O}((\log n)^a) \Rightarrow f(n) = \mathcal{O}(n^b)$, $\forall a, b \geq 0$

**Theorem**

All polynomially bounded functions are exponentially bounded. i.e. $f(n) = \mathcal{O}(n^a) \Rightarrow f(n) = \mathcal{O}(b^n)$, $\forall a > 0, b > 1$

UNIVERSITY OF TORONTO



## Polynomially-Bounded Functions

**Theorem**

$f(n) = \mathcal{O}(n^k) \Leftrightarrow \log(f(n)) = \mathcal{O}(\log n)$

UNIVERSITY OF TORONTO



## Polynomially-Bounded Functions

**Theorem**

All Logarithmically bounded functions are polynomically bounded. i.e. $f(n) = \mathcal{O}((\log n)^a) \Rightarrow f(n) = \mathcal{O}(n^b)$, $\forall a, b \geq 0$

UNIVERSITY OF TORONTO

## Polynomially-Bounded Functions

**Theorem**

All polynomially bounded functions are exponentially bounded. i.e. $f(n) = \mathcal{O}(n^a) \Rightarrow f(n) = \mathcal{O}(b^n)$, $\forall a > 0, b > 1$



## Logarithm Method

Useful

Limit of logs: $\lim_{x \to a} (\log_b f(x)) = \log_b \left( \lim_{x \to a} f(x) \right)$ ($\log_b(\cdot)$ is continuous)

Suppose we want to compute $\lim_{n \to \infty} \frac{f(n)}{g(n)} = L$.

$$\log \left( \lim_{n \to \infty} \frac{f(n)}{g(n)} \right) = \log L$$

$$\lim_{n \to \infty} \left( \log \frac{f(n)}{g(n)} \right) = \log L$$

$$\lim_{n \to \infty} \frac{f(n)}{g(n)} = L = 2^{\lim_{n \to \infty} \left( \log \frac{f(n)}{g(n)} \right)}$$



## Example

$f(n) = 2^{n^2}$, $g(n) = 3^n$.

Solution:

## Example

$f(n) = 2^{n+1}$, $g(n) = 4^n$.

Solution:



## Comparing Functions

★ very useful slide

Short hand notation: $f(n) << g(n) \Leftrightarrow f(n) = \mathcal{O}(g(n))$
Assume $f$ and $h$ are eventually positive, i.e. $\lim_{n\to\infty} f(n) > 0$ and $\lim_{n\to\infty} h(n) > 0$

$1 << \log^*(n) << \log^{(i)} n << (\log n)^a << \sqrt{n} << n << n \log n << n^{1+b} << c^n << n!$, for all positive $i, a, b, c$

$f(n) << g(n) \Rightarrow h(n)f(n) << h(n)g(n)$

$f(n) << g(n) \Rightarrow f(n)^{h(n)} << g(n)^{h(n)}$

$f(n) << g(n)$ and $\lim_{n\to\infty} h(n) > 1 \Rightarrow h(n)^{f(n)} << h(n)^{g(n)}$



## Outline

1. Notations
2. Asymptotics
3. Proof Methods

## Direct Proofs (Book of Proof 4.3, p118)

skipped

1. Start with the givens
2. Mathematically manipulate the givens and/or reason about the givens to arrive at the conclusion

E.g. Prove $|a+b| \leq |a|+|b|$.



## Example

This is a direct proof; start from LHS get to RHS Will see this identity in heaps

E.g. Prove $\sum_{i=0}^{n-1} ia^i = \frac{a-a^n}{(1-a)^2} - \frac{(n-1)a^n}{1-a}$

i) Expand a few terms: $0(1) + 1a + 2a^2 + \ldots + (n-1)a^{n-1}$ ①

similar to adding $1+2+3+\ldots+n$

Multiply everything by the common ratio:

$a\sum_{i=0}^{n-1} = 0(a) + a^2 + 2a^3 + \ldots + (n-2)a^{n-1} + (n-1)a^n$ ②

① − ② $= (1-a)\sum_{i=0}^{n-1} ia^i = a + a^2 + a^3 + \ldots + a^{n-1} - (n-1)a^n = \frac{a-a^n}{1-a} - (n-1)a^n$

This is a geometric series sum

divide both sides by $1-a$

$\frac{a-a^n}{(1-a)^2} - \frac{(n-1)a^n}{(1-a)}$



## Disprove by counter-example (Book of Proof 9.1, p174)

Provide a case where the proposition is not true.
E.g. Prove or disprove: All primes are odd.

Side notes:
Pythagorean theorem: $a^2+b^2=c^2$ (Proved)
Fermat's last theorem: $a^n+b^n=c^n$ has no positive integer solutions for $n>2$ (Proved, Andrew Wiles, 1995)
Euler's conjecture: $\sum_{i=1}^{k} x_i^n = b^n$ has no positive integer solution for $b>2$
(Counter-example: $27^5+84^5+110^5+113^5=144^5$)

## Proof by contradiction (Book of Proof 6.1, p138)

1. Assume toward a contradiction $\neg P$/ $\bar{P}$(not P)
2. Make some argument
3. arrive at a contradiction
4. $\therefore P$ must be true

e.g. Prove that there are infinitely many prime number

P is prime if only factor of P is 1 and itself

Assume there are finitely many prime numbers ⇝ create a set $S = \{P_1, P_2, \dots, P_n\}$

Let $P$ = product of every individual element in S $+1 = P_1 \times P_2 \times P_3 \times \dots P_n + 1$

Then P is not in S and P is not divisible by any other prime. Then we have a contradiction since P is not in S and we said that there are infinitely many primes



## Weak Induction (Book of Proof 10.1, p182)

☆ Exam will have 1 induction question and 1 counting argument proof

Proof by induction: to show $P(n)$ (some boolean statement depending on $n$) is true $\forall n \geq n_0$.

Weak induction:

1. Basis: show $P(n_0)$ is true
2. Hypothesis: Assume $P(n)$ is true (**!!!Note:** You should not assume it is true for all $n$. This is what you need to prove. Assume $P(n)$ is true for all $n$ will cost you 2-3 marks in exams.)
3. Induction: Show $P(n) \Rightarrow P(n+1)$

☆ so do not write "P(n) is true for all n"
You must only write "P(n) is true"



## Weak induction examples

Prove $n! \leq n^n$, $\forall n \geq 1$

Base: $n=1$ $\quad 1! \leq 1^1$

IH: Assume $n! \leq n^n$

IS: WTP $(n+1)! \leq (n+1)^{n+1}$

⚠ Must use induction hypothesis in inductive step

so note $(n+1)! = (n+1)n! \leq (n+1)n^n$ by IH

$\leq (n+1)(n+1)^n = (n+1)^{n+1}$

so $(n+1)! \leq (n+1)^{n+1}$

## Weak induction examples

Prove $11^n - 6$ is divisible by 5, $\forall n \geq 1$



## Strong induction (Book of Proof 10.2, p187)

1. Basis: show $P(n_0), P(n_1), \ldots$ are true ← ☆ The key difference for strong induction
2. Hypothesis: Assume $P(k)$ is true, $\forall k \leq n$
3. Induction: Show $P(n_0) \wedge \cdots \wedge P(k) \wedge \cdots \wedge P(n) \Rightarrow P(n+1)$

e.g. The Fundamental Theorem of Arithmetic: all integers $n \geq 2$ can be expressed as the product of one or more prime numbers

Review solution from the book, TA did not go over it in the last three minutes of the lecture



## Strong induction example

Prove that using \$2 and \$5, we can make any amount $\geq$ \$4