

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

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

Examples:  $\log^* 16 = ?$

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

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

Useful properties

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

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

log of limits

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

$$\text{since } \lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 2^\infty = \infty$$

$$\text{then } f(n) = \Omega(g(n))$$

Order of functions



# ECE345 Tutorial 2

Winston (Yuntao) Wu

Electrical & Computer Engineering



Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

1 / 33

## Outline

### 1 Notations

### 2 Asymptotics

### 3 Proof Methods



Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

2 / 33

## Notations

Sets:

$\mathbb{N} = \{1, 2, 3, \dots\}$ : all natural numbers ( $\text{\LaTeX: } \mathbb{N}$ )

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ : all integers ( $\text{\LaTeX: } \mathbb{Z}$ )

$\mathbb{R}$  = all real numbers ( $\text{\LaTeX: } \mathbb{R}$ )

$\emptyset$ : empty set ( $\text{\LaTeX: } \emptyset$ )

$x \in S$ :  $x$  is an element of a set  $S$  ( $\text{\LaTeX: } x \in S$ )

$x \notin S$ :  $x$  is not an element of a set  $S$  ( $\text{\LaTeX: } x \notin S$ )

$A \subset B$ :  $A$  is a subset of  $B$  i.e. all elements in  $A$  is in  $B$  ( $\text{\LaTeX: } A \subset B$ )

$A \not\subset B$ :  $A$  is not a subset of  $B$  ( $\text{\LaTeX: } A \not\subset B$ )

$\mathcal{P}(X) = \{Y : Y \subset X\}$ : the power set of  $X$ , i.e. the set of all subset of  $X$  ( $\text{\LaTeX: } \mathcal{P}(X)$ )

Set operations:

Union:  $A \cup B = \{x : x \in A \text{ or } x \in B\}$  ( $\text{\LaTeX: } A \cup B$ )

Intersection:  $A \cap B = \{x : x \in A \text{ and } x \in B\}$  ( $\text{\LaTeX: } A \cap B$ )

Difference:  $A - B = A \setminus B = \{x : x \in A \text{ and } x \notin B\}$

Complement: Fix a universe  $U$ ,  $A \subset U$ ,  $\bar{A} = C_U A = \{x \in U, x \notin A\}$  ( $\text{\LaTeX: } \bar{A}$ )

Cartesian product:  $A \times B = \{(a, b) : a \in A, b \in B\}$



Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

3 / 33

## Notations

Logics:

Negation:  $\neg P, \sim P, \bar{P}$ , ( $\LaTeX$ :  $\backslash not, \backslash sim$ )

And:  $P \wedge Q$  ( $\LaTeX$ :  $\backslash land$ )

Or:  $P \vee Q$  ( $\LaTeX$ :  $\backslash lor$ )

Quantifiers:

$\exists$  there exists ( $\LaTeX$ :  $\backslash exists$ )

$\forall$  for all, for any ( $\LaTeX$ :  $\backslash forall$ )

Other symbols:

s.t. such that

$\Leftarrow$  implies ( $\LaTeX$ :  $\backslash Leftarrow$ )

$\Leftrightarrow$  if and only if (equivalently) ( $\LaTeX$ :  $\backslash Leftrightarrow$ )

$\because$  because ( $\LaTeX$ :  $\backslash because$ )

$\therefore$  therefore ( $\LaTeX$ :  $\backslash therefore$ )

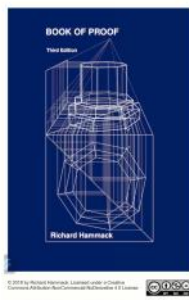
$[a, b] = \{x : a \leq x \leq b\}, (a, b) = \{x : a < x < b\}$

$[a, b) = \{x : a \leq x < b\}, (a, b] = \{x : a < x \leq b\}$



## 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/>



BOOK OF PROOF		Third Edition	Richard Hammack
Paperback ISBN: 978-0-9844271-0-4 (2017-75)	Hardcover ISBN: 978-0-9844271-0-5 (2018-15)		
This book is an introduction to the standard methods of proving mathematical theorems. It has been approved by the American Institute of Mathematics (AIM) as a textbook for its program in logic and foundations. It is available for free under a Creative Commons license.			
You can order or copy through Amazon, Barnes & Noble, or Amazon. You can also download a free PDF version (PDF). (The contents listed below will take you to specific chapters in this file.)			
<b>Contents</b>			
(Please use the chapter title to see the subsections.)			
0. Introduction			ix
<b>Part I: Fundamentals</b>			
1. Logic			1
2. Logic			34
3. Contradiction			45
<b>Part II: How to Prove Conditional Statements</b>			
4. Conditional			111
5. Contrapositive Proof			129
6. Proof by Contradiction			137
<b>Part III: More on Proof</b>			
7. Proving Non-Conditional Statements			147
8. Proofs Involving Sets			157
9. Natural			172
10. Mathematical Induction			180
<b>Part IV: Relations, Functions and Cardinality</b>			
11. Relations			201
12. Functions			223
13. Proofs in Cardinality			244
14. Cardinality of Sets			262
<b>Solutions</b>			
Solutions to the exercises in each chapter are provided in separate reader feedback in periodic updates. Please contact me at rhammack@vcu.edu if you find any additional mistakes, or submit new ones.			
Revised: 20 June 16, 2022. Please submit any errata or PDF updates accordingly. This revised version includes a number of updates found by readers. All updates posted after June 16 will be labeled 2.3.			



## Outline

### 1 Notations

### 2 Asymptotics

### 3 Proof Methods



## Definition

- $f(n) = \mathcal{O}(g(n)) \Leftrightarrow \exists c, n_0 > 0$  s.t.  $0 \leq f(n) \leq cg(n), \forall n \geq n_0$
- $f(n) = \Omega(g(n)) \Leftrightarrow \exists c, n_0 > 0$  s.t.  $0 \leq cg(n) \leq f(n), \forall n \geq n_0$
- $f(n) = \Theta(g(n)) \Leftrightarrow f(n) = \mathcal{O}(g(n))$  and  $f(n) = \Omega(g(n)) \Leftrightarrow \exists c_1, c_2, n_0 > 0$  s.t.  $0 \leq c_1g(n) \leq f(n) \leq c_2g(n), \forall n \geq n_0$

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

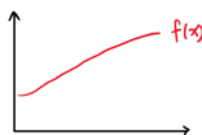
<sup>1</sup>For those who are interested, the Stirling's formula can be derived from the gamma function  $\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$  for  $\text{Re}(z) > 0$ .

$n! = \Gamma(n+1) = \int_0^\infty t^n e^{-t} dt = n^n e^{-n} \sqrt{2\pi n} (1 + \mathcal{O}(\frac{1}{n}))$  by Laplace's method.

## Intuition

$\mathcal{O}$ :

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



$\Omega$  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

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

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

<sup>2</sup> $f(n) = o(g(n))$  if and only if  $\forall c > 0, \exists n_0 > 0$  such that  $0 \leq f(n) < cg(n)$  for all  $n \geq n_0$ .

<sup>3</sup> $f(n) = \omega(g(n))$  if and only if  $\forall c > 0, \exists n_0 > 0$  such that  $0 \leq cg(n) < f(n)$  for all  $n \geq n_0$ .



## Limit Method (More Precisely)

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

## 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 polynomially 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.  $f(n) = \mathcal{O}(n^a) \Rightarrow f(n) = \mathcal{O}(b^n), \forall a > 0, b > 1$



## Polynomially-Bounded Functions

### Theorem

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



## Polynomially-Bounded Functions

### Theorem

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



## 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

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

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

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

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

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

Arsedl



## Example

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

Solution:





## Example

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

Solution:



## Comparing Functions

Short hand notation:  $f(n) \ll g(n) \Leftrightarrow f(n) = \mathcal{O}(g(n))$

Assume  $f$  and  $h$  are eventually positive, i.e.  $\lim_{n \rightarrow \infty} f(n) > 0$  and  $\lim_{n \rightarrow \infty} h(n) > 0$

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

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

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

$$f(n) \ll g(n) \text{ and } \lim_{n \rightarrow \infty} h(n) > 1 \Rightarrow h(n)f(n) \ll h(n)g(n)$$



## Outline

1 Notations

2 Asymptotics

3 Proof Methods



← *★ very useful slide*

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

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

skipped

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



Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

25 / 33

## Example

This is a direct proof: start from LHS get to RHS will see this identity in heaps  $\Delta$

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:  $0(1) + 1a + 2a^2 + \dots + (n-1)a^{n-1}$  ①

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

Multiply everything by the common ratio:

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

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

divide both sides by  $1-a$

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

this is a geometric series sum



Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

26 / 33

## 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:  $27^5 + 84^5 + 110^5 + 113^5 = 144^5$ )



Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

27 / 33

## 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  $\rightarrow$  create a set  $S = \{p_1, p_2, \dots, p_n\}$*

*Let  $P =$  product of every individual element in  $S + 1 = p_1 \times p_2 \times p_3 \times \dots \times p_n + 1$*

*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*



Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

28 / 33

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

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"*

*★ Exam will have  
1 induction question and 1  
counting argument proof*



Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

29 / 33

## Weak induction examples

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

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

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

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

*so note  $(n+1)! = (n+1)n! \leq (n+1)n^n$  by IH  $\triangleleft$  Must use induction hypothesis in inductive step*

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

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



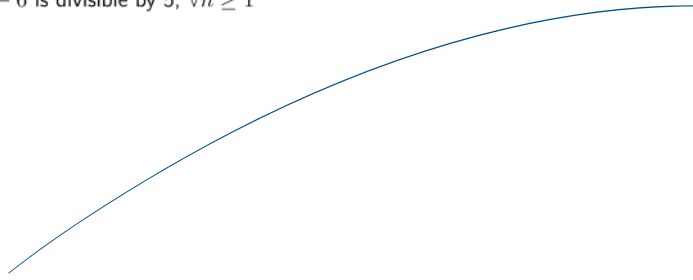
Winston (Yuntao) Wu (UofT)

ECE345 Tutorial 2

30 / 33

## 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  $P(n_0), P(n_1), \dots$  are true  $\leftarrow$  *★ The key difference for strong induction*
2. Hypothesis: Assume  $P(k)$  is true,  $\forall k \leq n$
3. Induction: Show  $P(n_0) \wedge \dots \wedge P(k) \wedge \dots \wedge P(n) \Rightarrow P(n+1)$

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  $\geq \$4$

