ECE345 Tutorial 2

Winston (Yuntao) Wu

Electrical & Computer Engineering

Outline

UNIVERSITY OF TORONTO

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

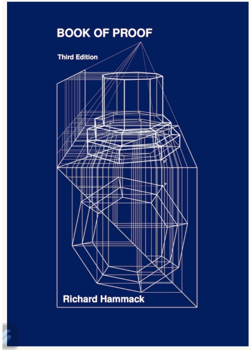
Logics:
Negation: $\neg P$, $\sim P$, $\bar{P}$, (LaTeX: \lnot, \sim)
And: $P \wedge Q$ (LaTeX: \land)
Or: $P \vee Q$ (LaTeX: \lor)

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/`



BOOK OF PROOF **Third Edition** Richard Hammack

Paperback: ISBN: 978-0-9894721-2-8 ($21.75) **Hardcover:** ISBN: 978-0-9894721-3-5 ($36.15)

This book is an introduction to the standard methods of proving mathematical theorems. It has been approved by the American Institute of Mathematics' Open Textbook Initiative. See other endorsements here. An adoptions list is here, and ancillary materials are here. See also the Translations Page.

You can order a copy through Barnes & Noble or Amazon. You can also download a **free PDF** version HERE. (The contents links below will take you to specific chapters in this file.)

Contents (Hover on the chapter title to see the subsections.)

Thanks to the readers who wrote to report mistakes and typos! I incorporate reader feedback in periodic revisions. Please contact me at rhammack@vcu.edu if you find any additional mistakes, no matter how minor.

Notice: On June 14, 2022 I issued edition 3.3 in print and PDF (ISBN's unchanged). This slight revision corrects a handful of typos found by readers. All orders printed after June 14 will be edition 3.3.

UNIVERSITY OF TORONTO

Outline

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. $0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n)$, $\forall n \geq n_0$

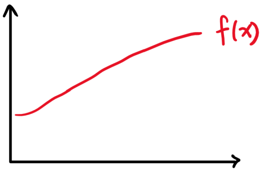
e.g. (2022 final): What does it mean by $n! = n^n e^{-n}\sqrt{2\pi n}\left(1 + \mathcal{O}\left(\frac{1}{n}\right)\right)$ (Stirling formula[1])?
Note here $f(n) = \frac{n!}{n^n e^{-n}\sqrt{2\pi n}} - 1$, $g(n) = \frac{1}{n}$,
So $\dfrac{n!}{n^n e^{-n}\sqrt{2\pi n}} - 1 \leq \dfrac{c}{n}$ for some $c, n_0 > 0$ and all $n \geq n_0$

[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

$\mathcal{O}$:

- $f \leq g \Leftrightarrow f(n) \leq g(n)$, $\forall n$
- 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. $f(n) \leq cg(n)$, $\forall n \geq n_0$



Ω is similar.

For Θ, we can bound f from below and above.

Example

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

Solution: $0 \leq 2^{n+1} = 2 \cdot 2^n \leq c \cdot 2^n$, $\forall n \geq 0$, if $c \geq 2$.
$\therefore$ we can choose $c = 2$, $n_0 = 1$, $0 \leq 2^{n+1} \leq c2^n$, $\forall n \geq n_0$.
$\therefore 2^{n+1} = \mathcal{O}(2^n)$.

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

Solution: $0 \leq c \cdot 2^n \leq 2 \cdot 2^n = 2^{n+1}$, $\forall n \geq 0$, if $c \leq 2$.
$\therefore$ we can choose $c = 1$, $n_0 = 1$, $0 \leq c2^n \leq 2^{n+1}$, $\forall n \geq n_0$.
$\therefore 2^{n+1} = \Omega(2^n)$.

Example

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

Solution:

Note: $|a| = a$ if $a \geq 0$ and $|a| = -a$ if $a < 0$, thus $-|a| \leq a \leq |a|$.

Observation: $n + a \leq n + |a| \leq 2n$, if $n \geq |a|$,

$n + a \geq n - |a| \geq \frac{1}{2}n$, if $n \geq 2|a|$.

Show that $(n+a)^b = \mathcal{O}(n^b)$: we need to show $0 \leq (n+a)^b \leq c \cdot n^b$, for some c and $\forall n \geq n_0$.

let $n_0 = |a| \Rightarrow 0 \leq (n+a)^b \leq (2n)^b = 2^b n^b$

Choose $c \geq 2^b$

Show that $(n+a)^b = \Omega(n^b)$: we need to show $0 \leq c \cdot n^b \leq (n+a)^b$, for some c and $\forall n \geq n_0$.

let $n_0 = 2|a| \Rightarrow 0 \leq \left(\frac{1}{2}\right)^b n^b = \left(\frac{1}{2}n\right)^b \leq (n+a)^b$

Choose $c \leq \left(\frac{1}{2}\right)^b$

$(n+a)^b = \mathcal{O}(n^b)$ and $(n+a)^b = \Omega(n^b) \Rightarrow (n+a)^b = \Theta(n^b)$

UNIVERSITY OF TORONTO

Transitivity: $f(n) = \Theta(g(n))$ and $g(n) = \Theta(h(n)) \Rightarrow f(n) = \Theta(h(n))$
Proof: $\exists c_1, c_2, n_1 > 0$ s.t. $0 \leq c_1 g(n) \leq f(n) \leq c_2 g(n)$, $\forall n \geq n_1$.
$\exists c_3, c_4, n_2 > 0$ s.t. $0 \leq c_3 h(n) \leq g(n) \leq c_4 h(n)$, $\forall n \geq n_2$.
$\therefore 0 \leq c_1 c_3 h(n) \leq c_1 g(n)$ and $c_2 g(n) \leq c_2 c_4 h(n)$, $\forall n \geq n_2$.
$\therefore 0 \leq c_1 c_3 h(n) \leq c_1 g(n) \leq f(n) \leq c_2 g(n) \leq c_2 c_4 h(n)$, $\forall n \geq \max(n_1, n_2)$.

Transpose: $f(n) = \mathcal{O}(g(n)) \Leftrightarrow g(n) = \Omega(f(n))$
Proof: $\exists c, n_0 > 0$ s.t. $0 \leq f(n) \leq cg(n)$, $\forall n \geq n_0 \Leftrightarrow \exists c, n_0 > 0$ s.t. $0 \leq \frac{1}{c} f(n) \leq g(n)$, $\forall n \geq n_0$

Symmetry: $f(n) = \Theta(g(n)) \Leftrightarrow g(n) = \Theta(f(n))$
Proof: $f(n) = \Theta(g(n)) \Leftrightarrow f(n) = \mathcal{O}(g(n))$ and $f(n) = \Omega(g(n)) \Leftrightarrow g(n) = \Omega(f(n))$ and $g(n) = \mathcal{O}(f(n))$

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 $0 \leq f(n) < cg(n)$ for all $n \geq n_0$.
[3] $f(n) = \omega(g(n))$ 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)

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

UNIVERSITY OF TORONTO

Useful results

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

Proof: $a \leq b \Leftrightarrow \lim_{n\to\infty} \frac{n^a}{n^b} = 0$ or $1 \Leftrightarrow n^a = \mathcal{O}(n^b)$

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

Proof: $\lim_{n\to\infty} \frac{\log_a n}{\log_b n} = \lim_{n\to\infty} \frac{\frac{\log_b n}{\log_b a}}{\log_b n} = \frac{1}{\log_b a} < \infty$

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

Proof: $c \leq d \Leftrightarrow \lim_{n\to\infty} \frac{c^n}{d^n} = \lim_{n\to\infty} \left(\frac{c}{d}\right)^n = 0$ or $1 < \infty \Leftrightarrow c^n = \mathcal{O}(d^n)$

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

Polynomially-Bounded Functions

Theorem

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

Proof: $(\Rightarrow)$ $f(n) = \mathcal{O}(n^k) \Rightarrow \exists c_1, n_0 > 0$ s.t. $f(n) = c_1 n^k$, $\forall n \geq n_0$
Take log on both sides, $\log(f(n)) = \log(c_1 n^k) = k \log(c_1 n) = k \log c_1 + k \log n \leq c_2 \log n$
We could choose any $c_2 \geq k \left(\frac{\log c_1}{\log n_0} - 1 \right)$ and any $n_0 \geq 2$, s.t. $\forall n \geq n_0$, with this c_2, we have $0 \leq \log(f(n)) \leq c_2 \log n$, i.e. $\log(f(n)) = \mathcal{O}(\log n)$

$(\Leftarrow)$ $\log(f(n)) = \mathcal{O}(\log n) \Rightarrow \exists c, n_0 > 0$ s.t. $\forall n \geq n_0$, $\log(f(n)) \leq c \log n = \log(n^c)$,
Take exponential of both sides, $f(n) \leq n^c \Rightarrow f(n) = \mathcal{O}(n^c)$, Here, c and k are indifferent as constants.

Polynomially-Bounded Functions

Theorem

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

Proof: To make sure the recursive L'Hopital ends, round up to the nearest integer $a \to \lceil a \rceil$ since $f(n) = \mathcal{O}((\log n)^a)$, $(\log n)^a = \mathcal{O}((\log n)^{\lceil a \rceil})$, $(\log n)^{\lceil a \rceil} = \mathcal{O}(n^b)$, then $f(n) = \mathcal{O}(n^b)$ by transitivity.

To show that $(\log n)^{\lceil a \rceil} = \mathcal{O}(n^b)$, we use the limit method. Here, let's assume $a \in \mathbb{N}$.

$$\lim_{n\to\infty} \frac{(\log n)^a}{n^b} = \frac{\infty}{\infty} \text{ (use L'Hopital)} = \lim_{n\to\infty} \frac{a(\log n)^{a-1}\frac{1}{n\ln 2}}{bn^{b-1}} = \lim_{n\to\infty} \frac{a}{b\ln 2}\frac{(\log n)^{a-1}}{n^b} =$$

$$\cdots \text{(Recursive L'Hopitals)} = \lim_{n\to\infty} \left(\frac{1}{b\ln 2}\right)^a \cdot a! \cdot \frac{1}{n^b} = 0$$

$\therefore (\log n)^a = \mathcal{O}(n^b)$

UNIVERSITY OF TORONTO

Polynomially-Bounded Functions

Theorem

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

Proof: Round up to the nearest integer $a \to \lceil a \rceil$
since $f(n) = \mathcal{O}(n^a)$, $n^a = \mathcal{O}(n^{\lceil a \rceil})$, $n^{\lceil a \rceil} = \mathcal{O}(b^n)$, then $n^a = \mathcal{O}(b^n)$ by transitivity.

To show that $n^a = \mathcal{O}(b^n)$, we use the limit method. Here, let's assume $a \in \mathbb{N}$.

$\lim_{n\to\infty} \frac{n^a}{b^n} = \frac{\infty}{\infty}$ (use L'Hopital)

$= \lim_{n\to\infty} \frac{an^{a-1}}{b^n \ln b} = \frac{a}{\ln b} \lim_{n\to\infty} \frac{n^{a-1}}{b^n} = \cdots$ (Recursive L'Hopitals) $= \frac{a!}{\ln^a b} \lim_{n\to\infty} \frac{1}{b^n} = 0$

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

Logarithm Method

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

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

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

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

Example

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

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

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

Example

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

Solution: $\log\left(\lim_{n\to\infty} \frac{2^{n+1}}{4^n}\right) = \lim_{n\to\infty}\left(\log\left(\frac{2^{n+1}}{4^n}\right)\right) = \lim_{n\to\infty}(n+1)\log 2 - n\log 4 = -\infty$

$\therefore \lim_{n\to\infty} \frac{f(n)}{g(n)} = 2^{-\infty} = 0$

Comparing Functions

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

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

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

Proof: $\lim\limits_{n\to\infty} \dfrac{h(n)f(n)}{h(n)g(n)} = \lim\limits_{n\to\infty} \dfrac{f(n)}{g(n)} = 0$

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

Proof: $\log\left(\lim\limits_{n\to\infty} \dfrac{f(n)^{h(n)}}{g(n)^{h(n)}}\right) = \lim\limits_{n\to\infty} h(n) \log \dfrac{f(n)}{g(n)} = \lim\limits_{n\to\infty} h \log \lim\limits_{n\to\infty} \dfrac{f}{g} = -\infty$, $\lim_{n\to\infty} \frac{f^h}{g^h} = 0$

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

Proof: $\log\left(\lim\limits_{n\to\infty} \dfrac{h(n)^{f(n)}}{h(n)^{g(n)}}\right) = \lim\limits_{n\to\infty} (f - g) \log h = -\infty$, $\lim_{n\to\infty} \frac{h^f}{h^g} = 0$

UNIVERSITY OF TORONTO

Outline

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

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

Proof: $(a+b)^2 = a^2 + b^2 + 2ab \leq a^2 + b^2 + 2|a||b| = (|a| + |b|)^2$

$\Rightarrow |a+b| \leq ||a| + |b|| = |a| + |b|$

Example

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

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

$a\sum_{i=0}^{n-1} ia^i = \quad 0 \cdot a + 1 \cdot a^2 + 2 \cdot a^3 + \cdots + (n-1) \cdot a^n$ ② (Multiply both sides by a)

①-② $\Rightarrow (1-a)\sum_{i=0}^{n-1} ia^i = a + a^2 + \cdots + a^{n-1} - (n-1)a^n \Rightarrow \sum_{i=0}^{n-1} ia^i = \frac{a-a^n}{(1-a)^2} - \frac{(n-1)a^n}{1-a}$

When $|a| < 1$ and $n \to \infty$, the sum converges to $\frac{a}{(1-a)^2}$, used to prove the Build-Heap runtime.

Side note: The same technique can be used to find the closed form for geometric series

$\sum_{i=0}^{n-1} a^i = \frac{a^n - 1}{a-1}$.

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.
Counter e.g. 2 is prime, but 2 is even.

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

Proof: Assume that there are a finite number of primes
Let S be the complete set of primes
let $P = \prod_{x \in S} x + 1$
$P \notin S$ because $P > x, \forall x \in S$
P is a prime because P is not divisible by any prime, $1 \equiv P \mod x, \forall x \in S$
P is a prime but not in S, contradiction.

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 $P(n) \Rightarrow P(n+1)$

Weak induction examples

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

Proof: **Base Step**: $n = 1$, $1! = 1 = 1^1$

(i) Using n only:

Induction Hypothesis: Assume $n! \leq n^n$

Induction Step: For $n+1$, $(n+1)! = (n+1)n! \leq (n+1)n^n$ by IH

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

(ii)Introducing a new variable k:

Induction Hypothesis: Assume when $n = k \geq 1$, $k! \leq k^k$

Induction Step: When $n = k+1$, $(k+1)! = (k+1)k! \leq (k+1)k^k$ by IH

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

Weak induction examples

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

Let $P(n) = 5|(11^n - 6)$ (5 divides $11^n - 6$)

Base Step: $n = 1$, $11^1 - 6 = 5$ $5|5$

Induction Hypothesis: Assume $P(n)$ is true

Induction Step: Check $P(n+1)$, $11^{n+1} - 6 = 11 \cdot 11^n - 6 = 11 \cdot (5m + 6 - 6)$

$= 55m + 66 - 6 = 55m + 60 = 5(11m + 12)$ for some m

So $5|11^{n+1} - 6$, $P(n+1)$ is true.

Strong induction (Book of Proof 10.2, p187)

1. Basis: show $P(n_0), P(n_1), \ldots$ are true
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

Proof: **Base Step**: $n = 2$, 2 is a prime

Induction Hypothesis: assume all $k \in [2, n]$ can be written as the product of one or more primes

Induction Step:

$n+1$ is prime. Then it can be expressed as the product of itself.

$n+1$ is not prime. Then $n+1 = k_1 k_2$ for some integers $k_1, k_2 < n+1$. By IH, k_1, k_2 can be written as product of primes. Thus $n+1$ can be written as product of primes

Strong induction example

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

Proof: **Base Step**: $n = 4$ can be made using \$2+\$2, $n = 5$ can be made using \$5

Induction Hypothesis: assume $\forall k \in [4, n]$, \$$k$ can be made using \$2 and \$5

Induction Step: $(n+1) = (n-1) + 2$ and $n-1$ can be made using \$2 and \$5 by IH