Proof techniques (cont’d), Truth tables
(if time) Infimum/Supreme

ROB 501

Course administration

- No lecture or discussion on Monday (Labor Day)
- Discussion sessions are starting today (review relevant to HW#1)
- HW#1 is posted
- GSI Office hours for this week:

  Andrew: F 4-5pm, T 1-2pm

  Ishank: F 3-4pm, T 2-3pm

  Location: FRB 3310

Quick review

Notation:

$\mathbb{N} = \{1, 2, 3, \cdots\}$ Natural numbers or counting numbers

$\mathbb{Z} = \mathcal{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ Integers or whole numbers

$\mathbb{Q} = \left\{\frac{m}{q} | m, q \in \mathbb{Z}, q \neq 0, \text{no common factors (reduce all fractions)}\right\}$ Rational numbers

$\mathbb{R}$ = Real numbers

$\mathbb{C} = \{\alpha + j\beta \mid \alpha, \beta \in \mathbb{R}, j^2 = \text{-}1\}$ Complex numbers

$\forall$ means "for every", "for all", "for each".

$\exists$ means "for some", "there exist(s)", "there is/are", "for at least one".

$\in$ means "element of" as in "$x \in A$" (x is an element of the set A)

"$\neg$": not "$\wedge$": and "$\vee$": or

Quick review

- Proof techniques
  - Direct proof
  - Proof by contrapositive
  - Proof by exhaustion

    <u>Proof by Exhaustion</u>: Reduce the proof to a finite # of cases and then check every one of them.

    <u>Ex:</u> Four color problem (Google it!)
  - (TODAY) Proof by induction
    - (TODAY) First principle of induction (standard induction)
    - (TODAY) Second principle of induction (strong induction)
  - (TODAY) Proof by contradiction

Proof by induction

$n \in \mathbb{N}$

First Principle of Induction (Standard Induction): Let $P(n)$ denote a statement about the natural numbers with the following properties:

(a) Base case: $P(1)$ is true   1. $P(1)$ true

(b) Induction part: If $P(k)$ is true, then $P(k+1)$ is true.   2. $P(k) \Rightarrow P(k+1)$

$1 \oplus 2 \Rightarrow$ $\therefore P(n)$ is true for all $n \geq 1$ ($n \geq$ base case)

Ex: Claim: For all $n \geq 1$, $1+3+5+\dots+(2n-1)=n^2$

Proof: $P(n): 1+3+5+\dots+(2n-1)=n^2$ (this is what we want to show to hold for all n)

Base case: $P(1)$: $1 \stackrel{?}{=} (1)^2$ ✓

Induction step: We assume $P(k)$ is true:

$P(k): 1+3+5+\ldots+(2k-1) = k^2$

and attempt to show $P(k+1)$ is also true:

$$P(k+1) = \underbrace{1+3+5+\ldots+(2k-1)}+(2(k+1)-1) =$$

$$= \quad k^2 + 2k + 2 - 1$$

$$= k^2+2k+1 = (k+1)^2 \quad \checkmark$$

$\Longrightarrow$ $P(n)$ is true for all $n \geq 1$

Q: What if we want our induction to start at 5 (i.e. you want show some $P(n)$ holds for all $n \geq 5$)

Take the base case as $P(5)$.

Define $\tilde{P}(n) := P(n+5-1)$,

and do an induction for $\tilde{P}(n)$.

Works for any $n_0 \neq 1$ (i.e. $\tilde{P}(n) := P(n+n_0-1)$)
$n_0 \in \mathbb{N}$

Second principle of Induction

Let $P(n)$ be a statement about $\mathbb{N}$ w/ the following properties:

a) Base case: $P(1)$ is true.

b) If $P(j)$ is true for all $1 \leq j \leq k$, then $P(k+1)$ true.

Then, $P(n)$ is true for all $n \geq 1$.

<u>Fact</u>: Two induction methods are equivalent! Sometimes 2^{nd} method is helpful b.c. assuming more in step b) makes it easier to prove b).

<u>Ex:</u>

<u>Def</u>: $n \in \mathbb{N}$, $n \geq 2$, is <u>composite</u> if $\exists\, a, b \in \mathbb{N}$ $2 \leq a, b \leq n-1$, such that $n = a \cdot b$. Otherwise, n is prime.

<u>Theorem</u>: (Fundamental Thm of Arithmetic)

Every natural number $n \geq 2$ can be written as the product of <u>one</u> or more primes.

<u>Proof</u>: $P(n)$: If $n \geq 2$, then n can be expressed as a product of one or more primes.

<u>Base case</u>: $P(2)$ is true because 2 is prime.

Induction step: Assume that $P(j)$ is true for $2 \leq j \leq k$ (i.e., we assume $P(2), P(3), \dots, P(k)$ are true). To show: $P(k+1)$ is true.

Two cases: $k+1$ is either prime or composite.

Case 1: $k+1$ is prime, then $P(k+1)$ is trivially true $(k+1 = \underbrace{k+1}_{\text{prime}})$

Case 2: $k+1$ is composite. (By def.)

$\exists \; a, b \in \mathbb{N} \quad 2 \leq a, b \leq k$ s.t. $k+1 = a \cdot b$.

By induction assumption $P(a)$ and $P(b)$ are true (because $a, b \leq k$), which means $\exists$ primes s.t.

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_\ell$$
$$b = q_1 \cdot q_2 \cdot \dots \cdot q_m$$

Therefore $k+1 = p_1 \cdot p_2 \cdot \dots \cdot p_\ell \cdot q_1 \cdot q_2 \cdot \dots \cdot q_m$

$k+1$ is written as a product of primes. ✓

$\Rightarrow P(n)$ is true for all $n \geq 2$.

Proof by contradiction

A contradiction is a logical statement that is both true and false.

Let R be a logical statement. Then, $R \wedge (\neg R)$ being true is a contradiction.

Ex: R = $m, n \in \mathbb{N}$ have no common factors and "m and n are even" $\Rightarrow$ R is a contradiction

Ex (proof by contradiction):

Theorem: $\sqrt{2}$ is irrational. (due to Euclid)

p : $\sqrt{2}$ is irrational.

$\neg p$: $\sqrt{2}$ is rational.

We will show $\neg p$ leads to a contradiction hence $\neg p$ must be false $\Rightarrow$ p is true.

Assume $\neg p$. ($\sqrt{2}$ is rational)

$\exists m, n \in \mathbb{Z}$ s.t.

R1: m, n have no common factors, $n \neq 0$

R2: $\sqrt{2} = \frac{m}{n}$

$R2 \Rightarrow 2 = \frac{m^2}{n^2} \Rightarrow 2n^2 = m^2$

we proved on Monday

$\Rightarrow m^2$ is even $\Rightarrow$ m is even

$\Rightarrow \exists k \in \mathbb{N}$ s.t. $m = 2k$

$\therefore 2n^2 = m^2 = (2k)^2 \Rightarrow n^2 = 2k^2$

$\Rightarrow n^2$ is even $\Rightarrow n$ is even.

$\therefore m, n$ have a common factor since they are both even, 2 is a common factor.

$\neg R1$ is true.

$\therefore$ Contradiction: because we "showed" $R_1 \wedge \neg R1$ is true from $\neg p$.

$\Rightarrow \neg p$ is false $\Rightarrow p$ is true.

$$\boxed{a \Rightarrow b \equiv \neg a \vee b}$$

Relation to contrapositive

$$(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p) \equiv \neg(p \wedge (\neg q))$$

"direct" — contrapositive — used in contradiction

A common use of contradiction (when proving implications) is Assuming $(p \wedge \neg q)$ is true and seeking a contradiction.

Truth tables

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Exercise :

p	q	$\neg q$	$p \wedge \neg q$	$\neg(p \wedge \neg q)$
T	T			
T	F			
F	T			
F	F			

OFFICE HOURS

① $A \in \mathbb{R}^{n \times m}$

$$A = \begin{bmatrix} a^1 \\ a^2 \\ \vdots \\ a^n \end{bmatrix}_{n \times m}$$

where $a^i \in \mathbb{R}^{1 \times m}$

$$B = \begin{bmatrix} b^1 & \cdots & b^p \end{bmatrix}_{m \times p} \quad b^i \in \mathbb{R}^{m \times 1}$$

② $K = [k^1, \ldots k^m]_{n \times m}$ $\quad k^i \in \mathbb{R}^{n \times 1}$

①
$$AB = \left[[AB]_1 \,\middle|\, [AB]_2 \,\middle|\, \cdots \,\middle|\, [AB]_p \right]$$

$$A [b^1 \vdots b^2 \vdots \ldots \vdots b^n]$$

AB

$[Ab^1 | \dots | Ab^p] = M$

To show $AB = M$,

we need to show

$$[AB]_{ij} = M_{ij} \quad \forall i j.$$

$[AB]_{ij}$ give by defn.

$=$ (1)

$M_{ij} =$ (2)

(1) = (2)