Lecture 2: Proofs (cont'd) + Propositional Logic

Date: **02-Dec-2021 (Thu)**

CS1010: Discrete Mathematics

IIT Hyderabad, Odd Semester (2021)

Start at 4:06 pm.

Last time

- Proofs, Importance of Proofs
  - Proof = Chain of logical deductions leading to a proposition starting from a set of axioms.

- Types of Proofs (Examples)
  - Direct (If $x \in [0,2]$ then $-x^3 + 4x + 1 \geq 0$) procedure.
  - Contradiction (Proof of correctness of algorithm to check primes)
  - Contrapositive (If r is irrational, then $\sqrt{r}$ is irrational)

- Terms: Proposition, Predicate, Axioms, Implication

$(P \Rightarrow Q)$

$P(n) :=$ n is a prime $\rightarrow$ If P then Q.

Today

- Some more Proof types
  - Proving an “If and only If”
  - Proof by Cases

- Good and Bad proofs

- **Propositional Logic**: The `math’ of propositions:

Reference: For Propositional Logic: Appropriate parts of Kenneth Rosen book.

Proving an Iff statement.
"If and only if"

Theorem = Important True proposition.

Theorem: $\underbrace{\text{An integer } n \text{ is even}}_{P} \Longleftrightarrow \underbrace{n^2 \text{ is even}}_{Q}$.

If P then Q
$\boxed{\text{and}}$ If Q then P.

(1) If n is even $\Rightarrow$ n^2 is even.
(2) If n^2 is even $\Rightarrow$ n is even.

Two distinct "direction" of implication.

Proof. (1) If n is even, then $n = 2k$ for some integer k.
$\Rightarrow n^2 = n \cdot n = (2k)^2 = 4k^2$, which is even.

(2) ~~If n^2 is even, $n^2 = 2k$.~~ Consider the contrapositive). → If n is odd then n^2 is odd
If n is odd; then let $n = 2k+1$ for some $k \in \mathbb{Z}$,
$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = \text{odd}$. ∎
or QED!

Proof (by contradiction):

Let n^2 be even. Suppose, for the sake of contradiction n is odd.

$n^2 = 4k^2 + 4k + 1$

Then . . . .

$4/6 \Rightarrow 2/3$.

Example of Proof by contradiction

Theorem: $\sqrt{2}$ is irrational

Proof (by contradiction): Assume not, for the sake of contradiction. Then $\sqrt{2} = \frac{p}{q}$. where $p, q \in \mathbb{Z}$

where $\frac{p}{q}$ is in the "lowest" form. (p, q don't have common factors).

$\sqrt{2} = p/q \Rightarrow 2q^2 = p^2 \Rightarrow p^2$ is even. $\Rightarrow p$ is even.

Let $p = 2k$, for some $k \in \mathbb{Z}$.

Then $2q^2 = 4k^2 \Rightarrow q^2 = 2k^2 \Rightarrow q^2$ is even $\Rightarrow q$ is even

$\Rightarrow$ p, q have 2 as a common factor.

$\downarrow$ a contradiction to p, q not having common factor. $\blacksquare$

$\square$.

"Thus proved" $\longrightarrow$ or Q.E.D.

Proof by cases.

Theorem. If $|x| > 2$ then $x^2 > 4$.

{ Cases should cover all possibilities. }

"Exhaustive".

Proof: Case 1: $x > 2 \rightarrow x^2 > 4$

Case 2: $x < -2 \rightarrow x^2 > 4$

Theorem: If n is an integer, then $p(n) := 3n^2 + n + 14$ is even.

Proof: Consider two cases:

Case 1: n is an odd integer. $n = 2k+1$, $p(n) = 2(6k^2 + 7k + 9)$

Case 2: n is even integer. $n = 2k$, $p(n) = 2(6k^2 + k + 7)$ $\square$

Consider $\big||a|-|b|\big| \leq |a-b|$. for real no. a, b.

assume say wlog $a \leq b$.

$b \geq a$ follows from above.

<u>Proofs by Induction</u> : in 2 lectures.

A *bogus* proof

$\nearrow$ AM $\geq$ GM ineq.

- Show that for all non-negative integers a, b: $\frac{a+b}{2} \geq \sqrt{ab}$

not an axiom!

(what is wrong?).

$$\frac{a+b}{2} \overset{?}{\geq} \sqrt{ab}, \qquad \text{so}$$
$$\Uparrow$$
$$a+b \overset{?}{\geq} 2\sqrt{ab}, \qquad \text{so}$$
$$\Uparrow$$
$$a^2+2ab+b^2 \overset{?}{\geq} 4ab, \qquad \text{so}$$
$$\Uparrow$$
$$a^2-2ab+b^2 \overset{?}{\geq} 0, \qquad \text{so}$$
$$\Uparrow$$
$$(a-b)^2 \geq 0 \qquad \text{which we know is true.}$$

start $\underbrace{(a-b)^2 \geq 0}_{\text{axiom}}$. and expand

What is a good proof?

- A proof that the number of primes is infinite by Sam Northshield

Suppose there are only finitely many primes and let P be their product. Then

$$0 < \underbrace{\prod_p \sin\left(\frac{\pi}{p}\right) = \prod_p \sin\left(\frac{\pi(1+2P)}{p}\right)}_{\text{Too cryptic.}} = 0$$

What is a good proof?

- Show that $\sqrt[3]{2}$ is irrational

By contradiction:

Let $\sqrt[3]{2} = \frac{p}{q}$. for $p, q \in \mathbb{Z}$.

$$2 = \frac{p^3}{q^3}$$

$a^n + b^n = c^n$.

$$\Rightarrow p^3 = q^3 + q^3.$$

{By Fermat's last theorem, such integers p, q cannot exist}

$\blacksquare$

Propositional Logic

Simple operations on Propositions

- $\neg := NOT$ eg: $\neg P$: T when P is F, F when P is T

  P: The sky is blue. $\neg P$: the sky is not blue.

  $0 \leq x \leq 2$ $x \leq 2$ and $x \geq 0$

P	$\neg P$
T	F
F	T

- $\wedge :=$ *AND* (conjunction) $\vee :=$ *OR* (disjunction)

$0 \leq 1 \leq 2 \to T$

$0 \leq 3 \leq 2 \to F$

P	Q	P∧Q
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	P ∨ Q
T	T	T
T	F	T
F	T	T
F	F	F

$P \vee Q$ is true when $\boxed{\text{atleast}}$ one of P, Q is true

Examples and Combinations

Find the conjunction of the propositions p and q where p is the proposition "Rebecca's PC has more than 16 GB free hard disk space" and q is the proposition "The processor in Rebecca's PC runs faster than 1 GHz."

Conjunction: Reb's PC has more than 16 GB and it's proc runs faster than 1 GHz.

$(\neg p) \vee q$ → also a proposition.

(PC has < 16 GB space) or (proc runs > 1 GHz)

$((\neg p) \wedge q) \vee (\neg q \vee p)$ → Logical expression, also a proposition.

p	q	r
T	T	T
T	F	
F	T	
F	F	

Truth table for r.

$r := (\neg p \wedge q) \vee (\neg q \vee p)$.

$p = T$, $q = T$.

$r = (F \wedge T) \vee (F \vee T)$.

$= F \vee T = T$.

$r := ((p \wedge w) \vee (q \wedge w)) \wedge (\neg (p \vee q) \vee w)$

[Base props: p, q, w]

p	q	w	r
			F
			F
			F
			F
			F

(Usual OR = inclusive OR)

Exclusive-Or (XOR)

- $p \oplus q$: XOR (**Exactly** one is true)

P	Q	$P \oplus Q$	r
T	T	F	F
T	F	T	T
F	T	T	T
F	F	F	F

Can XOR be expressed in terms of $\wedge$, $\vee$, $\neg$.

Suggestion: $r = (p \wedge \neg q) \vee (\neg p \wedge q)$.

"Claim": r "is the same" as $p \oplus q$.

$\boxed{\text{Logical equivalence}}$.

XOR in terms of AND, OR, NOT

$\neg$

General example?

p	q	r	output
T	T	T	F
T	T	F	T
T	F	T	T
T	F	F	F
F	T	T	F (T)
F	T	F	T
F	F	T	T
F	F	F	F

$(p \wedge q \wedge \neg r)$

$(p \wedge \neg q \wedge r)$

$\neg p \wedge q \wedge \neg r$

$(\neg p \wedge \neg q \wedge r)$

$q \oplus r$.

→ Can this be written as a $\wedge, \vee, \neg$ proposition.

→ $\boxed{\text{YES}}$!

Required Proposition $= (p \wedge q \wedge \neg r) \vee$
$(p \wedge \neg q \wedge r) \vee$
$(\neg p \wedge q \wedge \neg r) \vee$
$(\neg p \wedge \neg q \wedge r)$.

Proposition:

↓

Can do with rows of F also, flip positions of $\vee$ and $\wedge$ + negation

Logical Equivalences

$(P \Rightarrow Q)$

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

Implies (If-Then)

- $P \Rightarrow Q$

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T