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 <u>proposition</u> starting from a set of axioms.
- Types of Proofs (Examples)
 - Direct (If $x \in [0,2]$ then $-x^3 + 4x + 1 \ge 0$)
 - 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 = Q

 P(n) := n is a prime = J 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 If statement.

"If and only y" If P then Q and If Q then P. Theorem: An integer n is even $\Leftrightarrow n^2$ is even. QTwo distinct direction" of implication. (1) If n is even $\Rightarrow n^2$ is even. (2) If n° is even > n in even. $\frac{Rroof.(1)}{2}$ If n is un, then n=2k for some integer k. $\Rightarrow n^2 = n \cdot n = (2h)^2 = 4k^2$, which is even. If n is odd (2) If n^2 is err $n^2 = 2k$. Consider the contrapositive). If n is odd; then let n = 2k+1 for some $k \in \mathbb{Z}$ $N^2 = (2k+1)^2 = 4k^2 + 4k+1$ I then no is odd = odd . Z or QED!

Theorem = Important true proposition.

Proof (by contradiction): Let n² be even. Suppose, for the sale of contradiction n woodd. 4 -> 3 Example of Roof by contradiction Theorem: $\sqrt{2}$ is irrational for the sele of contradiction. Proof (by contradiction): Assume not; Then $\sqrt{2} = \frac{P}{q}$, where $P, q \in \mathbb{Z}$. where of is in the "lowest" form. (P, q, don't have common factors). $\sqrt{2} = \frac{1}{4}$ \Rightarrow $2q^2 = p^2$ \Rightarrow p^2 in even \Rightarrow p is even. Then $29^2 = 4k^2$ $\Rightarrow 9^2 = 2k^2 \Rightarrow 9^2$ is $e^2 = 9^2$ is $e^2 =$

⇒ P, q have 2 as a common factor.

a contradiction to P, q not having common factor. "Thus proved" - > or QED. Proof by cases. Theorem. If |x| > 2 then $x^2 > 4$. { Cases should cour} { all possibilities. } Proof: Cene 1: x>2. $\Rightarrow x^2>4$ "Exhaustive". Case 2: $\chi < -2$ $\rightarrow \chi^2 > 4$ then p(n)=3n2+n+14 is even. Theorem: If n is an integer, Proof: Conider two cases: Care 1: n = 2k+1, $p(n) = 2(6k^2 + 7k+9)$ Case 2: n 15 even integer. $p(n) = 2(6k^2 + k + 7)$ Consider $|a|-|b|| \le |a-b|$, for real no a,b.
assume say who $a \le b$.

bza follon for above.

Proofs by Induction in 2 lectures.

A bogus proof

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

what is
$$\frac{a+b}{2} \stackrel{?}{\geq} \sqrt{ab}$$
, so $\frac{a+b}{2} \stackrel{?}{\geq} \sqrt{ab}$, so $\frac{a+b}{2} \stackrel{?}{\geq} \sqrt{ab}$, so $\frac{a^2+2ab+b^2 \stackrel{?}{\geq} 4ab}{\wedge}$, so $\frac{a^2-2ab+b^2 \stackrel{?}{\geq} 0}{\wedge}$, so which we know is true.

Stat
$$(a-b)^2 > 0$$
. 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

$$0 < \prod_{p} \sin\left(\frac{\pi}{p}\right) = \prod_{p} \sin\left(\frac{\pi(1+2P)}{p}\right) = 0$$
Too cryptic

What is a good proof?

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

By contradiction.

Let
$$\Im Z = \frac{1}{8}$$
, for $p, q \in \mathbb{Z}$.

$$2 = \frac{1}{8}$$

$$2 = \frac{1}{8}$$

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

$$\text{By Fermat's lest theorem, such integers } p, q, \text{ cannot exist}$$

Propositional Logic

Simple operations on Propositions

$\bullet \land = AND$	(conjunction)	$\vee := OR$	(disjunction)
-----------------------	---------------	--------------	---------------

Р	Q	F∕Q
Т	Т	Т
Т	F	F
F	Т	F
F	F	F

		0	<1 < 2 >T
P	Q	PVQ	$0 \leq 3 \leq 2$
Т	Т	Т	T F.
Т	F	T	
F	Т	T	
F	F	F	
Praistrue when latlest one of P, a is true			

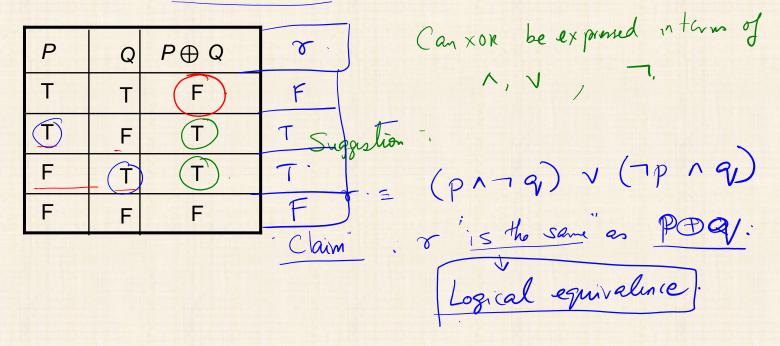
Examples and Combinations

Find the conjunction of the propositions \underline{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."

r= ((pnw) v(qnw)) A (¬(pvq) vw) [Base props: p, 2, w]

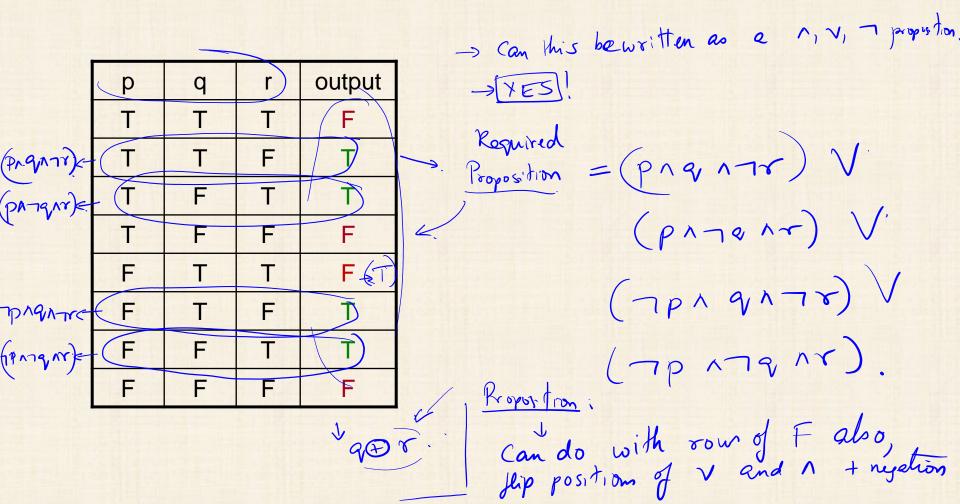
Exclusive-Or (XOR)

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



XOR in terms of AND, OR, NOT

General example?



Logical Equivalences

$$(P \Rightarrow q) = (P \cdot V \cdot q)$$

Implies (If-Then)

•
$$P \Rightarrow Q$$

P	Q	$P \Rightarrow Q$
Т	Т	Т
Т	F	F
F	Т	Т
F	F	Т