Lec 8. Methods of proof of $P \to Q$.

1. Direct $P \to Q$. ("vacuos" proof, $P = F$ always).
2. contrapositive $\neg Q \to \neg P$

   ("trivial" proof. if $Q = T$ always).

3. Contradiction.

- show that $\neg P \to (r \wedge \neg r)$

  Since $\neg P = F$ thus $P = T$.

- show $\neg(P \to Q) \to (P \wedge \neg P) \vee (Q \wedge \neg Q)$.

  $\neg(P \to Q) \equiv P \wedge \neg Q$

  since $\neg(P \to Q) = F$ thus $P \to Q = T$.

Assume $\left.\begin{array}{l} P \\ \neg Q \end{array}\right\}$ all defn's, lemmas, etc associated w P and $\neg Q$

$$\therefore \underbrace{(P \wedge \neg P)} \vee \underbrace{(Q \wedge \neg Q)}$$

sometimes direct proof of $\neg Q \to \neg P$ is simple

sometimes direct proof $P \to Q$ is simple.

4. Equivalence (iff) $P \leftrightarrow Q$.

Need to show (by some method of proof),

that both $P \to Q$ and $Q \to P$.

5. Exhaustive / proof by cases.

Show $P \to Q$ holds for all possible classes of arguments to P and Q.

e.g. $n \in \mathbb{Z}$ is either positive, negative, neutral

$n \in \mathbb{Z}$ is either odd or even

$n \in \mathbb{R}$ is either rational or irrational

etc.

Aside / memory jog.

Truth table for $\neg(P \to Q) \equiv P \land \neg Q$

P	Q	$P \to Q$	$\neg(P \to Q)$	$P \land \neg Q$
1	1	1	0	0
1	0	0	1	1
0	1	1	0	0
0	0	1	0	0

logically equivalent.

6. Constructive existence proofs of $\exists x\, P(x)$.

Find one $x \in \mathcal{U}$ for which $P(x) = T$.

7. Nonconstructive existence proof of $\exists x\, P(x)$.

Show there must exist an $x \in \mathcal{U}$ for which $P(x) = T$.

(Typically use proof by cases to show x must exist).

- Example from Lec 7 (next page).
- Proof that the set of prime numbers is infinite.

Example of
#7: Non constructive existence proof.

* Show there exists a value, but don't have to pin point it.

Prove: that there exists irrational x, y.
s.t. x^y is rational.

Recall rational # $r = l/m$, where $l, m \in \mathbb{Z}$ w. no common factors.

Need an instance where x, y are both irrational
but x^y is rational.

Try $x = \sqrt{2}$ and $y = \sqrt{2}$
consider $x^y = \sqrt{2}^{\sqrt{2}}$

case 1: if $\sqrt{2}^{\sqrt{2}}$ is rational $\longrightarrow$ done w/ existence proof.

case 2: if $\sqrt{2}^{\sqrt{2}}$ is irrational
let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

$$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2.$$

$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$ is rational

Example of nonconstructive existence proof.

Prove the proposition

Q = The set of prime numbers is infinite.

· Thus $\forall n \exists p > n$ where p is prime.
and $n \in \mathbb{Z}$

Defns:

· $p \in \mathbb{Z}$; $P = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$

· $p \in P$ has 2 and only 2 factors

factors$(p) = \{1, p\}$

(1 is not a prime number)

· $n \in \mathbb{Z}$ is composite if it is not prime.

Proof

Show by direct proof that $\neg Q = F$. Thus $Q = T$.

$\neg Q$ = There are a finite number of primes

Let n denote the largest prime.

Let $y = n! + 1$ Recall $n! = (n)(n-1)(n-2)\cdots 3\cdot 2\cdot 1$

case 1 y = prime. $\rightarrow$ $\neg Q = F$ (since $y > n$).

case 2 y = composite (and has more than 2 factors)

$$y = n! + 1$$
$$= \underbrace{n(n-1)(n-2)\cdots 1}_{\text{composite w/ factors every integer } x \leq n} + 1$$

composite w/ factors every integer $x \leq n$.

Factors of $y = \{1,\ n!+1,$ some additional number of factors which are greater than n and prime$\}$?

If y is composite $\exists p > n. \rightarrow \neg Q = F$ //

Class questions:

- why does a factor of $n!+1$ have to be greater than n?

$$y' = n! = \underbrace{n \cdot (n-1)(n-2) \cdots 1}_{n \text{ factors}}$$

- why do two consecutive integers not share a common factor? (other than 1)

Ideas discussed

$$y = y' + 1 \qquad \frac{y = y'+}{y'} \notin \mathbb{Z}$$

y is not divisible by (y'). $\Leftrightarrow \frac{y'+1}{y'} \notin \mathbb{Z}$

$$m = n + 1$$

$$\frac{y'+1}{y'} = 1 + \frac{1}{y'} = 1 + \frac{1}{n \cdot (n-1)(n-2) \cdots 1}$$

... the number theory to show this next lecture ...

Proof by contradiction that for all $x \in \mathbb{R}$

the mapping $\sqrt{x^2}$ is not a function.

$$P := \forall x \in \mathbb{R} \left(\sqrt{x^2} \text{ is not a function} \right)$$

Recall argument form; $\neg P \rightarrow (r \land \neg r)$

Defn of a function

$r =$ every $a \in A$ is mapped onto <u>one</u> $b \in B$.

(b does not have to be unique to a).

Assert $\neg P \equiv \sqrt{x^2}$ is a function for $x \in \mathbb{R} \rightarrow r$.

$\sqrt{x^2} = \pm x$ for $x \in \mathbb{R}$, $\rightarrow \neg r$

$\therefore (r \land \neg r)$

Sequences & summation (chap 2.4)

- A sequence is an ordered list

$$S = \{a_0, a_1, a_2, \ldots a_n\}$$

a_j is the j'th element.

a is just a variable name

$$S = \{b_0, b_1, b_2, \ldots b_n\}$$

b_j is the j'th element

Typically $j \in \mathbb{N} = \{0, 1, 2, 3, \ldots\}$

but often $j \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

A sequence: the order of appearance and repetition of elements matters (unlike a set)

Overload of notation! (curly brackets "context clarifies")

Set, $T = \{e_1, e_2, \ldots e_n\}$

where $e_j \neq e_i$ if $i \neq j$

sequence $S = \{a_0, a_1, a_2, \ldots\}$

but a_1 can be equal to a_2.