Methods of proof, Lec 7.

3. Proof by contradiction of a proposition p

a) Find a second proposition, r, that is implied from p. $p \to r$

Typically r is a definition associated w/ p.

e.g. Proof $\sqrt{2}$ is irrational

required defn r = rational number $r = l/m$

where $l, m \in \mathbb{Z}$ w/ no common factors

b) Show that $\neg p \to (r \wedge \neg r)$ a contradiction.

Thus $\neg p = F$ and $\neg\neg p = p = T$ //

(an indirect proof).

3. Proof by contradiction of an implication $p \to q$

Foundations

$\neg(p \to q) \equiv p \wedge \neg q$ ($p \to q$ only false if $p = T$ and $q = F$)

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

commutativity.

Need to show if $p \to q$ is False, this leads to a contradiction.

Proof: show $\neg(p \to q)$ leads to $(p \wedge \neg p)$ or $(q \wedge \neg q)$

$$\begin{array}{ll} p & \text{assert } p \\ \neg q & \text{assert } \neg q \\ \hline \therefore (P \wedge \neg P) \vee (Q \wedge \neg Q) & \end{array}$$

"Domination law" $p \vee T \equiv T$, show either $(P \wedge \neg P)$ or $(Q \wedge \neg Q)$

since $\neg(p \to q) \to (p \wedge \neg p) \vee (q \wedge \neg q)$

therefore $\neg(p \to q) = F$ and $p \to q = T$

<u>Example proof</u>: by contradiction of proposition

p = 4 is an odd number

If n is an odd number, $\to r = n = 2k+1$ for some $k \in \mathbb{Z}$

n is an even number $\to q = n = 2k$, for som $k \in \mathbb{Z}$

Argument form: $\neg p \to (r \wedge \neg r)$

Proof:

$$\begin{array}{ll} 4 = 2j & (\text{assert } \neg P) \\ \underline{\text{No integer can be both odd \& even.}} & \\ \therefore r \wedge \neg r & \end{array}$$

$4 = 2j$ and $4 = 2k+1$

Example: Proof by <u>contradiction</u> of $p \to q$

Proof: $\forall x, y \in \mathbb{R} \; \Big(\underbrace{(x+y) \geq 2}_{P(x,y)} \to \underbrace{(x \geq 1 \vee y \geq 1)}_{Q(x,y)} \Big)$

Recall argument form

$$\begin{array}{l} p \\ \neg q \\ \hline \therefore (p \wedge \neg p) \vee (q \wedge \neg q) \end{array}$$

$x + y \geq 2$	(assert P is true)
$\neg (x \geq 1 \vee y \geq 1)$	(assert $\neg q$)
$(\neg (x \geq 1) \wedge \neg (y \geq 1))$	DeMorgan's
$(x < 1) \wedge (y < 1)$	arthimetic.
$\therefore$	$p \wedge \neg p$

aside: $\left\{ \begin{array}{l} q = (x \geq 1) \vee (y \geq 1) \\ \neg q = (x < 1) \wedge (y < 1) \end{array} \right.$

$$\begin{array}{l} p = x + y \geq 2 \\ \text{if } (x < 1) \wedge (y < 1) \\ \hline \therefore \neg p \end{array}$$

since $x + y < 2$ if $(x<1) \wedge (y<1)$

Since $\neg (p \to q) \equiv p \wedge \neg q = F$

then $p \to q$ is true.

4. Equivalence proof (if and only if)

$p \leftrightarrow q$

Need to show $p \to q$ and $q \to p$.

Example: If $n \in \mathbb{Z}^+$ then n is odd ~~only~~ if and only if n^2 is odd.

1) $p \to q$ direct proof easy.

$n = 2k+1$ (assert p)

$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2j + 1$

$\therefore n^2$ is odd.

2) $q \to p$ try direct proof

$n^2 = 2k + 1$ (assert q)

$n = \sqrt{2k+1}$ ... ???

Try contrapositive $\neg p \to \neg q$

$n = 2k$ ($\neg p$ assert)

$n^2 = 4k^2 = 2(2k^2) = 2j$

$\therefore n^2$ is even; $\neg p \to \neg q \therefore q \to p$. //

5. Exhaustive proof / proof by cases.

* show that the implication is true for all $x \in U$.

Very often the elements x fall into classes:

e.g. • integers $\mathbb{Z}$; ~~odd~~ positive, ~~even~~ negative, zero (3 classes)

• real #'s $\mathbb{R}$; rational or irrational (2 classes)

Proof that $p \to q$ holds for each category.

(Challenge is to make sure you cover all the categories).

Example ; proof if n is an integer then $n^2 \geq n$.

Proove: $\forall n \in \mathbb{Z} \ (n^2 \geq n)$

3 classes of integers : - positive
- negative
- zero

• case 1 $n > 0$ then $n^2 \geq n$; $\therefore \dfrac{n \geq 0}{n^2 \geq n}$

• case 2 $n < 0$ then $n^2 > n$; $\dfrac{n < 0}{\therefore n^2 > n}$

• case 3 $n = 0$ then $n^2 = 0$ and $n^2 \geq n$. / $\dfrac{n = 0}{\therefore n^2 \geq n}$

Often proof by cases relies on integers being
• odd or even
• positive, negative, or zero.

Existence proofs

$\exists x\, P(x)$

$\exists x\, (P(x) \rightarrow Q(x))$

6. Constructive existence proofs ; find an x for which $P(x)$.

7. Nonconstructive existence proofs: show $P(x)$ must hold for some x but we don't need to specify the x precisely.

Example: constructive existence proof

Proove there exist an positive integer n that is the sum of cubes of positive integers in two ways.

$$\exists n \in \mathbb{Z}^+ \text{ s.t. } (n = i^3 + j^3) \wedge (n = k^3 + l^3)$$

$$\text{for } (i \neq k \neq l,\ j \neq k, l.)$$

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

in other words $i \neq k \neq l \neq j$

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