closure

Proof Techniques

Direct proof of P ⇒ Q

Let even(x): x is even

odd(x): x is odd

Procedure:

1. Assume that P is true
2. [Logical deductions to derive Q from P]
3. Therefore, Q is true

Example:
Prove that for all integers *n*, if *n* is even, then $n^2 + n$ is even.

$(\forall n \in \mathbb{Z})\ (\text{Even}(n) \Rightarrow \text{Even}(n^2+n))$

Explanation: given n is even $\rightarrow n = 2k$

want n^2+n is even $\rightarrow n^2+n = 2j$

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

Proof: assume n is an arbitary even integer (1)

then by def of even, $\exists k \in \mathbb{Z}$ s.t. $n = 2k$ (2)

so $n^2+n = (2k^{(2)})^2 + 2k = 4k^2 + 2k = 2(2k^2+k)$

since k is an integer ($k \in \mathbb{Z}$) by closure $2k^2+k \in \mathbb{Z}$

Thus, $n^2+n = 2j$ for some integer j (namely $j = 2k^2+k$)

∴ by definition, n^2+n is even (3)

Proof by contrapositive (of P ⇒ Q)

$\neg Q \Rightarrow \neg P \equiv P \Rightarrow Q$

Procedure:

1. State that we are using proof by contrapositive and what the contrapositive of the implication is
2. Use a proof technique to show that ¬Q ⇒ ¬P
3. Therefore, the original implication is proved

Example:
Prove that for all positive real numbers *x*, if *x* is not rational, then the square root of *x* is not rational.

$(\forall x \in \mathbb{R}^+)\ (x \notin \mathbb{Q} \rightarrow \sqrt{x} \notin \mathbb{Q})$

Exploration:

contra positive: $\neg(\sqrt{x} \notin \mathbb{Q}) \Rightarrow \neg(x \notin \mathbb{Q})$.

$(\sqrt{x} \notin \mathbb{Q}) \Rightarrow (x \in \mathbb{Q})$

$x \in \mathbb{Q}$ means $a = \frac{a}{b}$, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $b \neq 0$

want $x = \frac{c}{d}$, $c \in \mathbb{Z}$, $d \in \mathbb{Z}$, $d \neq 0$

$(\sqrt{x})^2 = \frac{a^2}{b^2}$

$x = \frac{a^2}{b^2} = \frac{c}{d}$, $b \neq 0$

if $xy \neq 0$, then $x \neq 0$ or $y \neq 0$

if $x \neq 0$ and $y \neq 0$, then $xy \neq 0$

prove: $(\forall x \in \mathbb{R}^+)(x \notin \mathbb{Q} \to \sqrt{x} \notin \mathbb{Q})$

proof: We do a proof by contra positive by showing

$(\forall x \in \mathbb{R}^+) \neg(\sqrt{x} \notin \mathbb{Q}) \to \neg(x \notin \mathbb{Q})$

or $\sqrt{x} \in \mathbb{Q} \to x \in \mathbb{Q}$

Let x be an arbitory elt of $\mathbb{R}^+$

Assume $\sqrt{x} \in \mathbb{Q}$

Then by definition, $\exists a \in \mathbb{Z}$ and $\exists b \in \mathbb{N}$, $b \neq 0$ s.t. $\sqrt{x} = \frac{a}{b}$

squaring each side, we get $x = \frac{a^2}{b^2}$

Since $a \in \mathbb{Z}$, $a^2 \in \mathbb{Z}$; since $b \in \mathbb{N}$, $b^2 \in \mathbb{N}$ (by closure)

since $b \neq 0$, $b^2 \neq 0$ (since $b^2 = 0 \to b = 0$)

So, $x = \frac{c}{d}$, for $c \in \mathbb{Z}$, $d \in \mathbb{N}$, $d \neq 0$.

So by definition, $x \in \mathbb{Q}$.

Thus $(\forall x \in \mathbb{R}^+)(\sqrt{x} \in \mathbb{Q} \to x \in \mathbb{Q})$

$\therefore$ the contrapositive, $(\forall x \in \mathbb{R}^+)(x \notin \mathbb{Q} \to \sqrt{x} \notin \mathbb{Q})$ is also true.

Proof Techniques (continued)

Proof by contradiction (of proposition P)

Note: if $P \equiv Q \to R$,
$\neg P \equiv \neg(Q \to R)$
$\equiv Q \wedge \neg R$

Procedure:

1. Assume that P is false i.e. assume $\neg P$ is true
   (so, to prove Q ⇒ R, assume Q is true and R is false)
2. [Logical deductions to come up with a contradiction]
3. Conclude that the assumption that P is false cannot hold.
   Therefore, P is true

Example: Pigeonhole Principle
Prove that if ~~m~~ objects are placed into *n* bins, where *m* > *n*,
then some bin must contain at least two objects.

Proof by contradiction
Assume m objects are placed into n bins, $m > n$
and it is not the case that one bin contains at least 2 objects
That means each bin contains 0 or 1 object
Since there are n bins, # objects is between 0..n (inclusive)
In other words, $0 \leq m \leq n$; But $m > n \Rightarrow \Leftarrow$ contradiction, the assumption is false.
So, there must be some bin contain at least 2 objects.

Proof of P ⇔ Q

Procedure:

1. State that we will prove the two implications
2. Prove P ⇒ Q (using proof technique of your choice)
3. Prove Q ⇒ P (using proof technique of your choice)
4. Conclude by stating what was proved

Example:
Prove that for all integers *m* and *n*,
mn is odd iff *m* is odd and *n* is odd.

$(\forall m, n \in \mathbb{Z})(Odd(m \cdot n) \Leftrightarrow odd(m) \wedge Odd(n))$

Prove: we'll prove $Odd(m \cdot n) \to odd(m) \wedge odd(n)$
and $odd(m) \wedge odd(n) \to Odd(m \cdot n)$

Prove: $(Odd(m) \wedge Odd(n)) \Rightarrow Odd(m \cdot n)$
Assume m, n are arbitrary odd integers
$Odd(m)$ means: $\exists a \in \mathbb{Z}$ s.t. $m = 2a+1$) def of odd
$Odd(n)$ means: $\exists b \in \mathbb{Z}$ s.t. $n = 2b+1$
(want to show $\exists c \in \mathbb{Z}$ s.t $m \cdot n = 2c+1$

$m \cdot n = (2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1$
Since $ab \in \mathbb{Z}$, by closure, $(2ab + a + b) \in \mathbb{Z}$
So, $m \cdot n = 2c+1$ for some $c \in \mathbb{Z}$
So, by definition, $m \cdot n$ is odd.

Prove: $Odd(m \cdot n) \Rightarrow (Odd(m) \wedge Odd(n))$

prove by contrapositive: prove $\neg(Odd(m) \wedge Odd(n)) \Rightarrow \neg Odd(m \cdot n)$

simplify: $(\neg Odd(m) \vee \neg Odd(n)) \Rightarrow \neg Odd(m \cdot n)$

$\equiv (Even(m) \vee Even(n)) \Rightarrow Even(m \cdot n)$

To prove: $(A \vee B) \Rightarrow C$, consider 2 cases: A true or B true

Suppose m is even, then by definition, $\exists k \in \mathbb{Z}$ s.t. $m = 2k$

Then $(m \cdot n) = (2k) \cdot n = 2(k \cdot n)$ (by associacivity)

Since $k, n \in \mathbb{Z}$, $k \cdot n \in \mathbb{Z}$ by closure

So. $m \cdot n = 2(kn)$ is even by definition

Suppose n is even. Since multiplication is commutative

so $n \cdot m = m \cdot n$, by similar reasoning, $m \cdot n$ is even

Thus $(Even(m) \vee Even(n)) \Rightarrow Even(m \cdot n)$

So, contrapositive also holds: $Odd(m \cdot n) \Rightarrow (Odd(m) \wedge Odd(n))$.

So $Odd(m \cdot n) \Leftrightarrow (Odd(m) \wedge Odd(n))$.

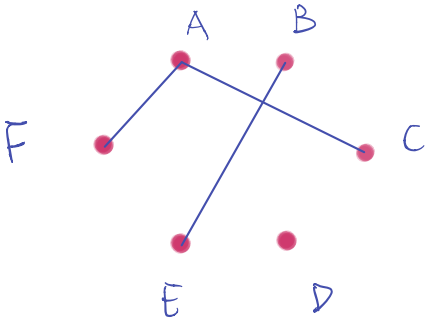
Note: if $P \Leftrightarrow Q$ and $Q \Leftrightarrow R$, then $P \Leftrightarrow R$

Proof by cases

Procedure:

1. Break up the analysis to two or more cases that collectively exhaust all the possibilities
2. For each case, prove that the desired statement holds

Example:
Prove that every group of 6 people contains a subgroup of 3 people who are mutual acquantances or a subgroup of 3 people who are mutual strangers.



edge between people means they know each other

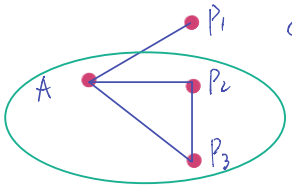
C, D, F are mutual strangers.

pick an arbitary person A.

Case 1: A knows at least 3 people (i.e. 3 or more)

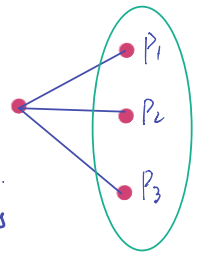
Case 2: A knows fews than 3 people (i.e. at most 2)

Case 1: A knows ≥ 3 people



Case 1a: at least 2 people I knows know each other

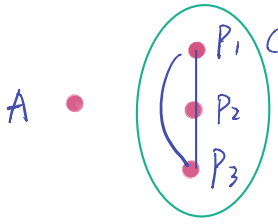
Then A & those 2 people are mutually aquaintances



Case 1b: nobody A knows is aquaintance of each other

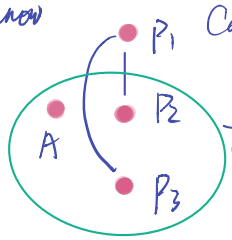
Then there are (at least) 3 people who are mutually strangers.

Case 2: A knows < 3 people; at least 3 people who A doesn't know.



Case 2a: 3 of people A doesn't know all know each other

This is a group of mutually acquaintances.



Case 2b: There are 2 people A doesn't know who don't know each other

Then there two people plus A are mutual strangers.