How to Prove Stuff!

Just follow these two easy steps!!

1. Translate the thing you want to prove into formal propositional logic.

2. Use a proof technique appropriate to the outermost symbol. (etc.)

$p \land q$ To prove $p \land q$, prove p, and prove q.

"To prove [$p \land q$], we will prove each separately.
- [proof of p]
- [proof of q]

Therefore, [$p \land q$]."

Example Prove $3 < 5 \land 8 \cdot 2 = 16$.

Proof. To show $3 < 5 \land 8 \cdot 2 = 16$, we will show each:
- $3 < 5$ because $3 + 2 = 5$.
- $8 \cdot 2 = 16$ because I saw a flash card once.

Therefore, $3 < 5 \land 8 \cdot 2 = 16$.

$p \lor q$ To prove $p \lor q$, you have options:
- Prove p, OR
- Prove q, OR
- Use a proof by contradiction (later).

"To prove $p \lor q$, we will prove p.
- [proof of p]

Therefore, $p \lor q$."

(not "assume")

$p \to q$ To prove $p \to q$, suppose p and prove q.

"To show that $p \to q$, let us suppose p. Then we must show q.

- [Proof of q, which gets to use p] } imaginary world where p is true

Therefore, since we proved q when we supposed p, then $p \to q$. } back to the real world.

Alternative technique: prove the contrapositive $\neg q \to \neg p$.

Example. Prove $(2n+1 > 6) \to (n > 2)$.

Proof. To prove $(2n+1 > 6)$ implies $n > 2$, suppose that $2n+1 > 6$. We must show $n > 2$.

- Starting from $2n+1 > 6$, we can reason as follows:

$$
\begin{aligned}
& 2n+1 > 6 \\
\to \quad & \{\text{subtract } 1 \text{ from both sides}\} \\
& 2n > 5 \\
\to \quad & \{\text{divide both sides by } 2\} \\
& n > 5/2 \\
\to \quad & \{5/2 > 2,\ > \text{ is transitive}\} \\
& n > 2
\end{aligned}
$$

Therefore, since we showed $n > 2$ under the supposition that $2n+1 > 6$, we have shown $(2n+1 > 6) \to (n > 2)$.

$p \leftrightarrow q$ To prove $p \leftrightarrow q$, prove $(p \to q) \wedge (q \to p)$.

"To prove p iff q, we must prove both directions.

- $(\to)$ [proof of $p \to q$]
- $(\leftarrow)$ [proof of $q \to p$]

Therefore, since p and q both imply the other, $p \leftrightarrow q$."

$\neg p$ To prove $\neg p$:

① Use a De Morgan law to "push the $\neg$ inward", then prove the result.

eg "To prove $\neg(p \wedge q)$, we can equivalently prove $\neg p \vee \neg q$ ..."

② Prove $p \to$ False. (Note $p \to F \equiv \neg p \vee F \equiv \neg p$.)

$\forall$ To prove $\forall x{:}D.\ P(x)$:

① Let d stand for some arbitrary element of the domain D, that is, don't assume anything about d other than fact that it is an element of the domain D.

Now, prove $P(d)$.

Caution: often people use x to stand for the arbitrary element. I'll try not to.

"To show $\forall x{:}D.\ P(x)$, let d be an arbitrary element of D. Then we will show $P(d)$.

- [Proof of $P(d)$]

Therefore, since $P(d)$ is true for an arbitrary d, in fact it is true for all d, that is, $\forall x{:}D.\ P(x)$."

② Use a proof by induction (later).

Example. Prove: If n is any natural number where $(2n+1>6)$, then $n>2$.

Translation: $\forall n{:}\mathbb{N}.\ (2n+1>6) \to (n>2)$.

Proof Let n be an arbitrary natural number. Then we must show $(2n+1>6) \to (n>2)$.

- [proof from before]

Therefore, $(2n+1>6) \to (n>2)$ for all natural #'s n.

$\exists$ To prove $\exists x : D.\ P(x)$;

1. Pick a specific element d in domain D, and prove $P(d)$.
2. Use a proof by contradiction.

"To show $\exists x : D.\ P(x)$, we will show specifically that $P(d)$.

- [proof of $P(d)$]

Therefore, since P is true for d, $\exists x : D.\ P(x)$."