Proofs!

<u>Def'n</u> A <u>proof</u> is a logically valid argument that establishes the truth of a proposition.

Proofs exist on a continuum from formal $\longrightarrow$ informal.

A <u>formal</u> proof:

- Uses only axioms (assumptions) and things previously proved
- Consists of a series of steps where each step is a valid <u>logical inference</u> from previous steps or assumptions.
- Is often expressed in formal notation.

An <u>informal</u> proof:

- Uses only axioms + things previously proved
- May omit or combine steps.
- Is often expressed in natural language.
- <u>In principle</u> could be expanded into a complete formal proof.
- Has other humans as its audience.

"<u>Logical inference</u>"

Rely on intuition!

eg. If $P \to Q$ is true and P is true, then Q is true.

(Why? intuitive; or make truth table; or show

$$((P \to Q) \wedge P) \longrightarrow Q \equiv T$$

). $\leftarrow$ practice for learning goal L3?

eg. If $A \wedge B$ is true, then A is true.

etc..

How To Prove Things

Just 3 easy steps!

1. Translate the statement to be proved into propositional logic (using $\wedge$, $\vee$, $\neg$, $\rightarrow$, $\forall$, $\exists$, ...)
2. Write a proof outline corresponding to the propositional logic formula.
3. Use your intuition/insight/ingenuity/content knowledge to fill in the missing pieces.

$p \wedge q$

To prove a conjunction $p \wedge q$, prove p, and then prove q.

> We must show $p \wedge q$, so we will prove both.
>
> > Proof of p
>
> > proof of q
>
> Therefore, $p \wedge q$.

eg. Prove $3 < 5 \wedge 2 \times 8 = 16$.

Proof. We must show $3 < 5 \wedge 2 \times 8 = 16$, so we will prove both seperately.

> First, $3 < 5$ because $3 + 2 = 5$.

> Second, $2 \times 8 = 16$ because ....
> ....

Therefore, $3 < 5 \wedge 2 \times 8 = 16$.

$p \vee q$

To prove $p \vee q$, you have options:

1. Prove p
2. Prove q
3. Use a proof by contradiction.

We must show $p \vee q$, which we will do by proving p.

Proof of p

So, since p is true, $p \vee q$ must be true.

$\boxed{p \to q}$ To prove $p \to q$, suppose p is true, then prove q in the hypothetical world where p is true.

We must show $P \to Q$, so suppose P.

Proof of Q (using P)

Since Q is true under the supposition P, therefore $P \to Q$.

OR prove the contrapositive $\neg q \to \neg p$.

We must show $P \to Q$, which we will do by proving the contrapositive, that is, $\neg q \to \neg p$.

Proof of $\neg q \to \neg p$.

We proved $\neg q \to \neg p$, which is equivalent to $p \to q$.

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

We must prove $p \leftrightarrow q$, so we will prove both directions.

($\to$) proof of $p \to q$.

($\leftarrow$) proof of $q \to p$.

Therefore, since $p \to q$ and $q \to p$, $p \leftrightarrow q$.

$\boxed{\neg p}$ To prove $\neg p$:

1. Use De Morgan laws to "push the $\neg$ inwards" first.

   eg. to prove $\neg(p \vee q)$, prove $\neg p \wedge \neg q$

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

<u>Example</u>. Write a proof outline for $P \to (Q \vee R)$.

To prove $P \to (Q \vee R)$, suppose P, then we will show $(Q \vee R)$.

> We will show $Q \vee R$ by proving Q.
>
> > Proof of Q (using P)
>
> Therefore, since Q is true, $Q \vee R$ is true.

Since we proved $Q \vee R$ under the supposition P, therefore $P \to (Q \vee R)$.

<u>Example</u>. Prove $(A \vee B) \to \neg C$ using a proof by contrapositive.

<u>Proof</u>. We will show $(A \vee B) \to \neg C$ via its contrapositive, that is, $C \to \neg(A \vee B)$. So <u>suppose C</u>; we will show $\neg(A \vee B)$.

> $\neg(A \vee B) \equiv \neg A \wedge \neg B$, we will prove each separately.
>
> > Proof of $\neg A$ (using C)
>
> > Proof of $\neg B$ (using C)
>
> Hence $\neg A \wedge \neg B$, that is, $\neg(A \vee B)$.

Therefore $C \to \neg(A \vee B)$, which is equivalent to $(A \vee B) \to \neg C$.

Recall $\text{Odd}(n) = \exists k : \mathbb{Z}.\ n = 2k+1.$

Example. Prove that if k is odd, so is k^2.

$$(\forall k : \mathbb{Z}.)\ \text{Odd}(k) \to \text{Odd}(k^2)$$

Proof. To show the implication $\text{Odd}(k) \to \text{Odd}(k^2)$, suppose $\text{Odd}(k)$, that is, there is some integer j such that $\boxed{k = 2j+1}$. KNOW

We must show $\text{Odd}(k^2)$, that is, we must find an integer p such that $k^2 = 2p+1$. WANT.

To show $k^2 = 2p+1$:

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

So we can pick $p = 2j^2 + 2j$, which is an integer since j is.

Therefore, since we showed k^2 is odd under the assumption that k is odd, $\text{Odd}(k) \to \text{Odd}(k^2)$.

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

① Prove $P(d)$ for an arbitrary d.

To prove $\forall x : D.\ P(x)$, let d be an arbitrary element in domain D, we will prove $P(d)$.

Proof of $P(d)$.

Since d was arbitrary, in fact $\forall x : D.\ P(x)$.

② Use induction. (later).

$\boxed{\exists x{:}D.\ P(x)}$ To prove an exists statement:

① Pick a specific value in domain D, call it d, and prove $P(d)$. (e.g. to prove $\exists n{:}\mathbb{N}.\ P(n)$, might prove $P(2)$).

② Use a proof by contradiction.

Ex. Prove $\forall n{:}\mathbb{Z}.\ \mathrm{Odd}(3n+2) \to \mathrm{Odd}(n)$.

Proof. (attempt)

KNOW

Let z be an arbitrary integer; we will show $\mathrm{Odd}(3z+2) \to \mathrm{Odd}(z)$.

KNOW

To show this implication, suppose $3z+2$ is odd; we will then show z is also odd.

WANT.

$\mathrm{Odd}(z) \equiv \boxed{\exists k{:}\mathbb{Z}.\ z = 2k+1}$. To prove this, we must give a specific value of k that makes $z = 2k+1$ true.

Since $3z+2$ is odd, there exists an integer j such that $3z+2 = 2j+1$. Solving for z,

$$\Rightarrow 3z = 2j-1$$

$$\Rightarrow z = \frac{2j-1}{3}.\ ?$$

STUCK! Want $z = 2\,?+1$ but this does not look like that.

Let's try contrapositive instead!

Ex. Prove $\forall n : \mathbb{Z}.\ Odd(3n+2) \to Odd(n)$.

Proof.

Let n be an arbitrary integer.

To show $Odd(3n+2) \to Odd(n)$, we will use the contrapositive, namely, $\neg Odd(n) \to \neg Odd(3n+2)$, that is,

$Even(n) \to \boxed{Even(3n+2)}$. So

WANT.

Suppose $\boxed{n \text{ is even}}$.

KNOW

We assume
$\neg Odd \equiv Even$
$\neg Even \equiv Odd$
we will prove later!

If n is even, $\underline{n = 2k}$ for some integer k.

$$
\begin{aligned}
3n+2 &= 3(2k)+2 \\
&= 6k+2 \\
&= 2(3k+1)
\end{aligned}
$$

Hence $3n+2$ is of the form $2 \times (\text{integer})$, so it is even.