Proof technique for proving propositions $P(n)$ about $n \in \mathbb{N}, \mathbb{Z}^+$

Three steps:

1) Assume $P(n)$ (all defns & associated axioms)

2) Use the defns of $P(n)$ to show that if $P(n)$ is true, then $P(n+1)$ is true.
   Direct proof $P(n) \rightarrow P(n+1)$.

3) Show $P(n)$ holds for some smallest element $\mathbb{Z}^+$ or $\mathbb{N}$, call it $n_{\text{min}}$.

\[ \forall n \geq n_{\text{min}}, P(n) = T. \]

Typically useful for:

- Summations
- Inequalities
- Division
- Sets
- Algorithms.
Proof by induction for summations

(General technique).

Example summations

\[ S_n = \sum_{i=1}^{n} i, \quad S_{\text{geo}}(n) = \sum_{i=0}^{n} ar^i, \quad \text{etc.} \]

Hypothesis \( P(n) := S_n = f(n) \)

\( \text{ raw sum } \)

\( \text{ simple, closed-form eqn.} \)

Need to show \( P(n) \rightarrow P(n+1) \)

i.e. if \( S_n = f(n) \) then \( S_{n+1} = f(n+1) \)

Steps:

- Write \( S_{n+1} \) and execute algebra to make it expressed in terms of \( S_n \).

- Substitute \( f(n) \) for \( S_n \) (i.e. assume \( P(n) \)).

- Use algebra to make r.h.s. in terms \( f(n+1) \).
For example, prove $P(n) \implies P(n+1)$

where $P(n) := \sum_{i=1}^{n} (2i-1) = n^2$

Write $S_{n+1}$ & show it in terms of $S_n$

\[
\sum_{i=1}^{n+1} (2i-1) = \sum_{i=1}^{n} (2i-1) + (2(n+1)-1)
\]

Substitute $f(n)$ for $P(n)$

\[
\sum_{i=1}^{n+1} (2i-1) = n^2 + (2(n+1)-1)
\]

Use algebra on r.h.s. to show it is $f(n+1)$

\[
\sum_{i=1}^{n+1} (2i-1) = n^2 + 2n + 1 = (n+1)^2
\]

We have proven inductive step $P(n) \implies P(n+1)$

Still need the basis step:

$P(1) = (1)^2 = 1 \checkmark$
Sum are easy! well defined methodology just shown.

Proof by induction for inequalities:

For example: $P(n) := n \leq 2^n$ for all $n \in \mathbb{Z}^+$

- Inductive hypothesis: $P(n)$
- Inductive proof step: $P(n) \rightarrow P(n+1)$
- Bases step: $P(n_{min}) = T$

- Hypothesis: $P(n) := n < \frac{2^n}{n} \forall n \in \mathbb{Z}^+$

- Inductive proof step

$$P(n): \quad n < 2^n$$

Wrote l.h.s of $P(n+1)$

$$n+1 < (2^n)+1 \leq 2 \cdot 2^n$$

$$= 2^{n+1}$$

$$\therefore \quad n+1 < 2^{n+1}$$

$(P(n) \rightarrow P(n+1))$

Lemma 1:
For $n > 0$, $2^n + 1 < 2^{n+1}$

\[ \begin{array}{c|c|c|c} n & 2^n+1 & 2 \cdot 2^n \\ \hline 1 & 3 & 4 \\ 2 & 5 & 8 \\ 3 & 9 & 16 \end{array} \]
Proof by induction on \( \text{sets} \)

For example:

\[ P(n) := \text{A set with } n \text{ elements has } 2^n \text{ subsets.} \]

Want to show \((1)\) \( P(n) \rightarrow P(n+1) \); \((2)\) \( P(n_{\text{min}}) = \top \)

1) \( P(n) \rightarrow P(n+1) \)

Assume \( P(n) \) a set of size \( n \) has \( 2^n \) subsets.

Let \( |S| = n \)

Let \( |B| = n+1 \) and \( B = S \cup \{b\} \) where \( b \not\in S \)

For every subset of \( S \), can make a new subset w/ \( \{b\} \) included.

\[ \text{# subsets of } B = 2 \times \text{# of subsets of } S \]

\[ = 2 \cdot 2^n = 2^{n+1}. \]

\[ \therefore \ P(n) := \text{# of subsets of } S \text{ is } 2^n. \]

\[ \therefore \ P(n) \rightarrow P(n+1) \]

2) Base step.

\( P(n) \) holds for some \( n_{\text{min}} \)

\[ P(n=0); \quad |\{\emptyset\}| = 0, \quad \text{# of subsets } \{\emptyset\} = 2^0 = 1. \]

\( P(n=0) \) is true (that a set with zero elements has \( 2^0 \) subsets).
More proofs for sub:

Hypothesis:

\[ P(n) := (A_1 \cup A_2 \cup \ldots \cup A_n) \cap B = (A_1 \cap B) \cup (A_2 \cap B) \cup \ldots \cup (A_n \cap B) \]

Basis step: try \( n = 1 \).

\[ P(1) : A_1 \cap B = A_1 \cap B \]

Inductive step: prove \( P(n) \Rightarrow P(n+1) \)

Use distributive law:

\[ (x \cup y) \cap z = (x \cap z) \cup (y \cap z) \]

Show \( P(n) \Rightarrow P(n+1) \)

\[ P(n+1) = ((A_1 \cup A_2 \cup \ldots \cup A_n) \cup A_{n+1}) \cap B \]

\[ = (x \cup y) \cap z \]

\[ \text{dist law} \]

\[ (A_1 \cup A_2 \cup \ldots \cup A_n) \cap B \cup (A_{n+1} \cap B) \]

\[ = P(n) \cup (A_{n+1} \cap B) \]

\[ = P(n+1) \]
Recap proof by induction

- Hypothesis $P(n)$ for $n \in \mathbb{N}, \mathbb{Z}^+$
- Inductive step $P(n) \rightarrow P(n+1)$
  (using def'n of $P(n)$ and algebra)
- Basis step $P(n) = T$ for some $n_{\min}$

$\therefore \forall n \geq n_{\min} P(n)$

Game plan for $P(n) \rightarrow P(n+1)$:

- Write the l.h.s. of $P(n+1)$, express it in terms of $P(n)$
- Substitute the expression for $P(n)$ with the hypothesis
- Show this results in appropriate formula for r.h.s. of $P(n+1)$
New topic: Recursion and iteration

- Build from top down.
- Build up from bottom.

Recursion: a general term for defining an object in terms of itself.

- An inductive proof establishes truth of \( P(k+1) \) due to truth of \( P(k) \).

- A recursive def'n of a func, predicate, set, etc. defines larger elements in terms of smaller elements.

For instance, consider the geometric sequence \( \{a_0, a_1, a_2, \ldots a_n\} \) where \( a_n = ar^n \) (for \( a, r \) consts)

A recursive def'n of geometric series:

\[
a_n = (a_{n-1})r
\]

For instance; arithmetic series: \( \{a_0, a_1, \ldots a_n\} \) where \( a_n = a_0 + nd \) for \( a_0, d \) constants.

Recursive defn:

\[
a_n = a_{n-1} + d
\]
A recursive function \( f(n) \) is defined in terms of smaller values of the function:

E.g., \( f(0), f(1), f(2) \ldots f(k) \) given

For \( n > k \), there is a rule for writing

\[ f(n) \text{ in } f(0), f(1), f(2) \ldots, f(n-1) . \]

Example recursive function:

Explicit function: Factorial function \( f(n) = n \cdot (n-1) \cdot (n-2) \ldots 2 \cdot 1 \)

Recursive factorial function:

\[ f(0) = 1 \quad \text{(Base case)} \]

\[ \forall n > 1 \quad f(n) = n \cdot f(n-1) \quad \text{Recursive definition} \]

Explicit function \( f(n) = a^n \)

Recursive definition: \( f(0) = 1 \)

\[ \forall n > 1 \quad f(n) = a \cdot f(n-1) \]