Proofs by Induction

The *Principle of Mathematical Induction* is an inference rule which is valid for proving assertions of the form $\forall n.\ P(n)$, where n ranges over the natural numbers:

$$\frac{P(0) \qquad \forall n.\ P(n) \rightarrow P(n+1)}{\forall n.\ P(n)}\ \texttt{(IND)}$$

$$\left|\ \begin{array}{ll} P(0) & \\ \forall n.\ P(n) \rightarrow P(n+1) & \\ \forall n.\ P(n) & \quad\quad\quad\quad \textbf{IND} \end{array}\right.$$

Idea: If $P(0)$ holds, and for all n, $P(n)$ implies $P(n+1)$, then $\forall n.\ P(n)$ holds by a "domino effect".

Usually, the induction step uses ($\forall\mathbf{I}$) and ($\rightarrow\mathbf{I}$):

$$
\begin{array}{|l}
P(0) \qquad\qquad\qquad\qquad \text{Basis} \\
\begin{array}{|l}
\begin{array}{|l}
\underline{P(k)} \qquad\qquad\qquad\qquad \text{Induction Hypothesis} \\
\vdots \\
P(k+1) \qquad\qquad\qquad \text{Induction Step}
\end{array} \\
\underline{P(k) \rightarrow P(k+1)} \qquad \rightarrow\mathbf{I} \\
\forall n.\ P(n) \rightarrow P(n+1) \quad \forall\mathbf{I}
\end{array} \\
\forall n.\ P(n) \qquad\qquad\quad \mathbf{IND}
\end{array}
$$

Writing it this way explicitly shows the scope of the induction hypothesis (a common source of confusion).

The variable n can be used as the “fresh” variable instead of k, but its scope has to be respected.

Induction: Example

Theorem: $\forall n.\ \sum_{i=0}^{n} i \;=\; n(n+1)/2$
Proof: Let $P(n)$ denote $\sum_{i=0}^{n} i \;=\; n(n+1)/2$.

- *(Basis)*: Show $P(0)$. $\sum_{i=0}^{0} i \;=\; 0 \;=\; 0(0+1)/2$.
- *(Induction Step):* We must show $\forall n.\ P(n) \rightarrow P(n+1)$. Let k be a *fixed but arbitrary* number, and *assume* $P(k)$ holds. Then

$$\begin{aligned}
\textstyle\sum_{i=0}^{k+1} i &= (k+1) + \textstyle\sum_{i=0}^{k} i \\
&= (k+1) + k(k+1)/2 \qquad \texttt{(by ind. hyp.)} \\
&= (k^2+3k+2)/2 \\
&= (k+1)(k+2)/2.
\end{aligned}$$

Thus $P(k) \rightarrow P(k+1)$. Since k *was arbitrary*, we conclude $\forall n.\ P(n) \rightarrow P(n+1)$. QED

$$\sum_{i=0}^{0} i \;=\; 0(0+1)/2 \qquad \text{Basis}$$

$$\sum_{i=0}^{k} i \;=\; k(k+1)/2 \qquad \text{Ind. Hyp.}$$

$$\vdots$$

$$\sum_{i=0}^{k+1} i \;=\; (k+1)(k+2)/2 \qquad \text{Ind. Step}$$

$$\left(\sum_{i=0}^{k} i \;=\; k(k+1)/2\right) \;\rightarrow\; \left(\sum_{i=0}^{k+1} i \;=\; (k+1)(k+2)/2\right) \qquad \rightarrow\mathbf{I}$$

$$\forall n.\; \left(\sum_{i=0}^{n} i \;=\; n(n+1)/2\right) \;\rightarrow\; \left(\sum_{i=0}^{n+1} i \;=\; (n+1)(n+2)/2\right) \qquad \forall\mathbf{I}$$

$$\forall n.\; \sum_{i=0}^{n} i \;=\; n(n+1)/2 \qquad \textbf{IND}$$

Complete Induction

There are other forms of induction for natural numbers. An example is *complete (or "course of values") induction*:

$$\frac{\forall n.\ (\forall m.\ m < n \to P(m)) \to P(n)}{\forall n.\ P(n)}$$

or, in Fitch style:

$\forall m.\ m < n \to P(m)$	Ind. Hyp.
$\vdots$	
$P(n)$	Ind. Step
$(\forall m.\ m < n \to P(m)) \to P(n)$	$\to$**I**
$\forall n.\ (\forall m.\ m < n \to P(m)) \to P(n))$	$\forall$**I**
$\forall n.\ P(n)$	**IND**

Notes:

- Complete induction "feels" stronger, because the induction hypothesis is $\forall m.\ m < n \rightarrow P(n)$ instead of just $P(n)$.
- Complete induction is easier when the induction step has to "go lower than $P(n-1)$" to prove $P(n)$.
- There is no explicit base case, but note that if $n = 0$ the induction hypothesis $\forall m.\ m < 0 \rightarrow P(0)$ is vacuous (*i.e.* of no help).
- Complete induction is actually equivalent in power to ordinary induction.
  Exercise: Use ordinary induction to prove:
  $(\forall n.\ (\forall m.\ m < n \rightarrow P(m)) \rightarrow P(n)) \rightarrow (\forall n.\ P(n))$.

Generalized Induction Rules

Induction can be used to prove theorems about things other than the natural numbers.
Note that Complete Induction mentions no arithmetic, only "less than" ($<$).

A valid form of induction for sets (as axiomatized by ZFC) is obtained by using $\in$ (element of) as $<$:

$$\frac{\forall A.\ (\forall B.\ B \in A \to P(B)) \to P(A)}{\forall A.\ P(A)}$$

In this form, it is called the *Principle of $\in$-Induction* (a variant form of the *Principle of Transfinite Induction*).

Well-Founded Induction

Induction can be applied in any situation in which the "less than" relation $<$ is *well-founded*.

Def: A binary relation $<$ on a set A is called *well-founded* if every nonempty subset of A has a minimal element with respect to $<$:

$$\forall B.\ B \subseteq A \wedge B \neq \phi \rightarrow (\exists x.\ x \in B \wedge (\forall x.\ x \in S \rightarrow y \not< x)).$$

Well-foundedness is equivalent to "$<$ has no infinite decreasing sequences".

Theorem: If $<$ is a well-founded relation on a set A, then the *Principle of Well-Founded (or Noetherian) Induction:*

$$\frac{\forall x.\ (\forall y.\ y < x \to P(y)) \to P(x)}{\forall x.\ P(x)}$$

is valid for proving assertions $\forall x.P(x)$ about elements of A.

Some examples of situations where this principle applies:

- *Natural numbers* with the "strictly less than" relation $<$.
- *Sets* with the "element of" relation $\in$.
- *Strings* with the "proper prefix of" relation.
- *Expression trees* with the "proper subexpression" relation.

It **does not apply**, *e.g.*, to real numbers with $<$.

Inductively Defined Sets

An *inductive definition* defines a set in terms of a set of *closure conditions*. For example, consider *expressions*:

1. A letter a standing alone is an expression.
2. If E_1 and E_2 are expressions, then $(E_1 + E_2)$ is an expression.
3. If E_1 and E_2 are expressions, then $(E_1 * E_2)$ is an expression.
4. The only expressions are those that can be shown to be so by a finite number of applications of (1-3).

The set of expressions is then the *smallest* (w.r.t. $\subseteq$) set that is *closed* under conditions (1-3).

Structural Induction

Inductively defined sets admit an induction principle, called *structural induction*. For the expression example:

To show that $P(E)$ holds for all expressions E, it is sufficient to show:

1. $P(a)$ holds for all letters a standing alone.
2. *If*, whenever $P(E_1)$ and $P(E_2)$ hold for expressions E_1 and E_2, *then* $P(E_1 + E_2)$ also holds.
3. *If*, whenever $P(E_1)$ and $P(E_2)$ hold for expressions E_1 and E_2, *then* $P(E_1 * E_2)$ also holds.

The validity of this principle can be proved by ordinary mathematical induction on the number of steps n required to construct an expression.