An Introduction to Induction Principles

Patricia HILL
School of Computing
University of Leeds, United Kingdom

Roberto BAGNARA
Department of Mathematics
University of Parma, Italy

Mathematical Induction

Let $P(n)$ be a property of natural numbers $n = 0, 1, 2, \ldots$ The principle of mathematical induction says that to show $P(n)$ holds for all natural numbers, it is sufficient to show:

- The base case: $P(0)$ holds.
- The step case: If $P(m)$ holds then so does $P(m+1)$, for any natural number m.

$P(m)$ is called inductive hypothesis.

Formally,

$$\Big(P(0) \wedge \big(\forall m \in \mathbb{N} : \underbrace{P(m)}_{\text{ind. hyp.}} \implies P(m+1)\big)\Big) \implies \forall n \in \mathbb{N} : P(n).$$

Mathematical Induction: Example 1

Let us show that $P(n) \equiv \big(0 + 2 + 4 + \cdots + 2n = n(n+1)\big)$:

- Inductive hypothesis: $P(m) \equiv \big(\sum_{i=0}^{m} 2i = m(m+1)\big)$.
- Base case, $m = 0$: $P(0) \equiv \big(0 = 0(0+1)\big)$.
- Step case, $m \geq 0$: Assume $P(m)$ holds.

$$
\begin{aligned}
\sum_{i=0}^{m+1} 2i &= 0 + 2 + \cdots + 2m + 2(m+1) \\
&= (0 + 2 + \ldots + 2m) + 2(m+1) && \text{[by rearranging]} \\
&= m(m+1) + 2(m+1) && \text{[by ind. hyp. } P(m)\text{]} \\
&= (m+1)(m+2) && \text{[by rearranging]}
\end{aligned}
$$

so that $P(m+1)$ holds.

Exercises

Prove the following identities by mathematical induction:

$$1 + 3 + 5 + \cdots + (2n + 1) = (n + 1)^2;$$

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots + \frac{1}{(n + 1)(n + 2)} = \frac{n + 1}{n + 2};$$

$$1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

Mathematical Induction: Example 2

Let $Q(n)$ be the property that, for all symbols $a, b, s_1, \ldots, s_n$, we have $(as_1 \cdots s_n = s_1 \cdots s_n b) \implies a = b$. We show that $\forall n \in \mathbb{N} : Q(n)$.

- Inductive hypothesis:
  $Q(m) \equiv \big((as_1 \cdots s_m = s_1 \cdots s_m b) \implies a = b\big)$.
- Base case, $m = 0$: $Q(0) \equiv (a = b \implies a = b)$.
- Step case, $m \geq 0$: Suppose

$$as_1 \cdots s_m s_{m+1} = s_1 \cdots s_m s_{m+1} b;$$

  then $b = s_{m+1}$ and therefore

$$as_1 \cdots s_m = s_1 \cdots s_m s_{m+1} = s_1 \cdots s_m b.$$

  By the inductive hypothesis, $a = b$, and thus $Q(m+1)$ holds.

COMPLETE MATHEMATICAL INDUCTION

Let $P(n)$ be a property of natural numbers $n = 0, 1, 2, \ldots$ The principle of complete mathematical induction says that to show $P(n)$ holds for all natural numbers, it is sufficient to show:

- The base case: $P(0)$ holds.
- The step case: If $P(k)$ holds for each $k = 0, 1, \ldots\ m$ then so does $P(m + 1)$, for any natural number m.

The conjunction $\bigwedge_{k=0}^{m} P(k)$ is called inductive hypothesis.

Formally,

$$\left(P(0) \wedge \left(\forall m \in \mathbb{N} : \underbrace{\left(\bigwedge_{k=0}^{m} P(k)\right)}_{\text{ind. hyp.}} \implies P(m+1)\right)\right) \implies \forall n \in \mathbb{N} : P(n).$$

Structural Induction

The principle of structural induction is:

> *In order to show that a property is true of all expressions, it suffices to show it is true of all atomic expressions and is preserved by all methods of forming the expressions.*

Structural Induction: Exercise

Definition:

1. "tt" and "ff" are boolean expressions;
2. If b is a boolean expression, "$(\mathrm{not}\ \ b)$" is a boolean expression;
3. If b_0 and b_1 are boolean expressions, "$(b_0 \text{ and } b_1)$" is a boolean expression;
4. If b_0 and b_1 are boolean expressions, "$(b_0 \text{ or } b_1)$" is a boolean expression.
5. Nothing is a boolean expression unless it is constructed by rules 1–4.

Prove using structural induction that in every boolean expression the number of '(' equals the number of ')'.

Well-Founded Induction: Introduction

Mathematical and structural induction are instances of well-founded induction.

- Mathematical induction relies on the fact that for any number n every descending sequence $n > n-1 > n-2 > \cdots$ is finite.
- Structural induction relies on the fact that for any expression a_0 every subexpression sequence of the form

$$a_0 \sqsupset a_1 \sqsupset a_2 \sqsupset \cdots$$

is finite. ($a' \sqsubset a$ denotes $a' \neq a$ is a subexpression of a.)

These rely on a well-founded relation.

Well-Founded Relations

A well-founded relation is a binary relation '$\prec$' on a set A such that there are no infinite "descending chains"

$$a_0 \succ a_1 \succ \cdots \succ a_i \succ \cdots$$

- When $a \prec b$, element a is called a predecessor of b.
- An equivalent definition of well-founded relation is:

  Every non-empty subset S of A has an element with no predecessors in S:

$$\forall S \subseteq A : (S \neq \emptyset \implies \exists m \in S \,.\, \forall s \in S : s \not\prec m)$$

Well-Founded Relations (cont.)

- If '$\prec$' is well-founded, then the transitive closure '$\prec^+$' is well-founded.
- We write '$\preceq$' for the reflexive closure of '$\prec$'.

$$a \preceq b \Longleftrightarrow a = b \vee a \prec b$$

Exercise: Show that '$\preceq$' is not a well-founded relation.

Partial Ordering

Suppose R is a binary relation on a set A. R is:

1. Reflexive: if, for all $a \in A$, $a \; R \; a$;
2. Transitive: if, for all $a_1, a_2, a_3 \in A$:
$$(a_1 \; R \; a_2 \wedge a_2 \; R \; a_3) \implies a_1 \; R \; a_3;$$
3. Antisymmetric: if, for all $a_1, a_2 \in A$:
$$(a_1 \; R \; a_2 \wedge a_2 \; R \; a_1) \implies a_1 = a_2.$$

A partial ordering is a binary relation that is reflexive, transitive and antisymmetric.

A total ordering on a set A is a partial ordering $\preceq$ on A such that, for all $a_1, a_2 \in A$, either $a_1 \preceq a_2$ or $a_2 \preceq a_1$.

WELL-FOUNDED RELATIONS AND PARTIAL ORDERINGS

Exercise: Let '$\prec$' a well-founded relation over a set A.

- Show that '$\prec^+$', the transitive closure of '$\prec$', is well-founded.
- Show that '$\prec^\star$', the reflexive and transitive closure of '$\prec$', is a partial ordering.

WELL-FOUNDED RELATIONS: EXAMPLES

- Let $A = \mathbb{N}$ be the set of natural numbers and '$\prec$' be the relation $m \prec n$ if and only if $n = m + 1$.

- Let $A = \mathbb{N}$ be the set of natural numbers and '$\prec$' be the relation '$<$'.

- Let $A = \mathrm{Aexp}$ be the set of all arithmetic expressions in IMP. Let $b \sqsubset a$ be defined to hold if and only if b is an immediate subexpression of a.

  Then '$\sqsubset$' is a well-founded relation.

- Let A be the set of all finite character strings.

  Let $t \lessdot s$ be defined to hold if and only if t is a proper substring of s.

  Then '$\lessdot$' is a well-founded relation.

Well-Founded Induction

The principle of well-founded induction is:

> *Let $\prec$ be a well-founded relation on a set A. Let P be a property. Then $P(a)$ holds for all a in A if and only if*
>
> $$\forall a \in A : \Big(\big(\forall b \prec a : P(b)\big) \implies P(a) \Big).$$

So, to prove that a property holds of all elements of a well-founded set (i.e., a set with a well-founded ordering) we just have to prove that if it holds for all predecessors of any $a \in A$ in this ordering, then it holds for a.

Definitions by Induction

Consider the following definition: for all $a \in \mathrm{Aexp}$ we define:

$$\mathrm{length}(a) \stackrel{\mathrm{def}}{=} \begin{cases} 1, & \text{if } a \equiv m; \\ 1, & \text{if } a \equiv x; \\ \mathrm{length}(a_0) + \mathrm{length}(a_1), & \text{if } a \equiv (a_0 + a_1); \\ \mathrm{length}(a_0) + \mathrm{length}(a_1), & \text{if } a \equiv (a_0 - a_1); \\ \mathrm{length}(a_0) + \mathrm{length}(a_1), & \text{if } a \equiv (a_0 * a_1). \end{cases}$$

Definitions of this form are often called inductive or recursive.