

Principle of well-founded induction

Justification	A theorem of set theory.
Prerequisites	Let A be a set, and let \prec be a well-founded relation on A . By definition, this means that there are no infinite descending chains $\dots \prec a_k \prec \dots \prec a_1 \prec a_0$ for elements $a_i \in A$. Finally, let P be a property of elements in A .
Rule	$\frac{\forall a \in A. (\forall b \prec a. P(b)) \Rightarrow P(a)}{\forall a \in A. P(a)}$
Application	For an arbitrary element $a \in A$, assume that the property holds for all elements $b \in A$ such that $b \prec a$. Prove that it is then the case that the property also holds of a . Often used in termination proofs.
Example	Let c be the the following IMP program:

$X := 0; \text{ while } \neg(Y = 0) \text{ do } X := X + 1; Y := Y - 1$

We wish to prove that c terminates for all initial states in $S = \{\sigma \mid \sigma \in \Sigma \wedge \sigma(Y) \geq 0\}$. Termination can be expressed as

$$\forall \sigma \in S. \exists \sigma' \in \Sigma. \langle c, \sigma \rangle \rightarrow \sigma'.$$

Let \prec be a binary relation over S such that, supposing $\sigma, \sigma' \in S$, $\sigma \prec \sigma' \iff \sigma(Y) < \sigma'(Y)$. Then \prec is well-founded, since we must always have $\sigma(Y) \geq 0$ for any $\sigma \in S$ in a chain. Now, as induction hypothesis, assume for some arbitrary $\sigma \in S$ that

$$\forall \sigma'' \prec \sigma. \exists \sigma' \in \Sigma. \langle c, \sigma'' \rangle \rightarrow \sigma'.$$

Assume $\sigma(Y) = 0$. If we let c_0 be the initial assignment and w be the while-loop in c , we have the following derivation in the big-step operational semantics:

$$\frac{\langle c_0, \sigma \rangle \rightarrow \sigma[0/X] \quad \langle w, \sigma[0/X] \rangle \rightarrow \sigma[0/X]}{\langle c, \sigma \rangle \rightarrow \sigma[0/X]}$$

Clearly, the execution terminates in a state $\sigma[0/X]$. Assume next $\sigma(Y) > 0$, let c_1 denote the composition of the two assignments in w and let $\sigma'' = \sigma[1/X, \sigma(Y) - 1/Y]$. This gives

$$\frac{\langle c_0, \sigma \rangle \rightarrow \sigma[0/X] \quad \frac{\langle c_1, \sigma[0/X] \rangle \rightarrow \sigma'' \quad \langle w, \sigma'' \rangle \rightarrow \sigma'}{\langle w, \sigma[0/X] \rangle \rightarrow \sigma'}}{\langle c, \sigma \rangle \rightarrow \sigma'}$$

Note that the induction hypothesis guarantees the existence of a σ' such that $\langle w, \sigma'' \rangle \rightarrow \sigma'$, since $\sigma'' \prec \sigma$. Hence, we have found the required terminating state, and our proof is done.

Principle of rule induction

Justification Special case of well-founded induction; \prec is the premise-conclusion relation.

Prerequisites Let R be a set of rules of the form (X/x) , where X is either the empty set or some set of premises, and x is the conclusion. Let $A = \{x \mid \Vdash_R x\}$, i.e. let A be the set defined by the rules. Let P be a property of elements in A .

Rule
$$\frac{\forall (\{x_0, \dots, x_n\}/x) \in R. (P(x_0) \wedge \dots \wedge P(x_n)) \Rightarrow P(x)}{\forall a \in A. P(a)}$$

Application Consider a rule, and assume the property holds of each premise. Show that this implies that the property holds of the conclusion. Repeat for every rule used in defining the set. Often used for relating different semantics.

Example We wish to prove $\Vdash \langle c, \sigma \rangle \rightarrow \sigma' \Rightarrow \mathcal{C}[\![c]\!](\sigma) = \sigma'$. Consider the non-trivial big-step operational semantics rule for while loops:

$$\frac{\langle b, \sigma \rangle \rightarrow \mathbf{true} \quad \langle c, \sigma \rangle \rightarrow \sigma'' \quad \langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma'' \rangle \rightarrow \sigma'}{\langle \mathbf{while} \ b \ \mathbf{do} \ c, \sigma \rangle \rightarrow \sigma'}$$

Assume $\Vdash \langle b, \sigma \rangle \rightarrow \mathbf{true}$. By a straightforward structural induction over boolean expressions, this implies that $\mathcal{B}[\![b]\!](\sigma) = \mathbf{true}$. Assume next as induction hypotheses $\mathcal{C}[\![c]\!](\sigma) = \sigma''$ and $\mathcal{C}[\![\mathbf{while} \ b \ \mathbf{do} \ c]\!](\sigma'') = \mathit{fix}(\Gamma)(\sigma'') = \sigma'$. By definition,

$$\begin{aligned} \mathcal{C}[\![\mathbf{while} \ b \ \mathbf{do} \ c]\!] &= \{(\sigma, \sigma') \mid \mathcal{B}[\![b]\!](\sigma) = \mathbf{true} \wedge \\ &\quad \exists \sigma''. \mathcal{C}[\![c]\!](\sigma) = \sigma'' \wedge \mathit{fix}(\Gamma)(\sigma'') = \sigma'\} \cup \\ &\quad \{(\sigma, \sigma) \mid \mathcal{B}[\![b]\!](\sigma) = \mathbf{false}\}. \end{aligned}$$

Simple application of the first assumption and the induction hypotheses now yields

$$\mathcal{C}[\![\mathbf{while} \ b \ \mathbf{do} \ c]\!](\sigma) = \sigma',$$

which is the result we want. Using this, and similar implications for the other rules, we use the principle of rule induction to conclude that our property of the denotational and operational semantics of **IMP** is indeed the case.

Principle of fixed-point induction

Justification A theorem of domain theory.

Prerequisites Let F_1, \dots, F_n be recursively defined functions over a domain D . Let Γ_i be a continuous functional $\Gamma_i: (D \rightarrow D) \rightarrow (D \rightarrow D)$ corresponding to the recursive definition of F_i , where $1 \leq i \leq n$. Let P be a property of n functions over D .

Rule
$$\frac{P(\emptyset, \dots, \emptyset) \wedge (P(F_1, \dots, F_n) \Rightarrow P(\Gamma_1(F_1), \dots, \Gamma_n(F_n)))}{P(\text{fix}(\Gamma_1), \dots, \text{fix}(\Gamma_n))}$$

Application Prove that the property holds of the empty function \emptyset , and assume it holds for F_1, \dots, F_n . From this assumption, derive that the property also holds of $\Gamma_1(F_1), \dots, \Gamma_n(F_n)$. Continuity then ensures that the property propagates to the fixed points. Often used for proving equalities in denotational semantics when while loops are involved.

Example Let Γ be the functional of $\mathcal{C}[\text{while } \neg b \text{ do } c]$. Define

$$\mathcal{C}[\text{repeat } c \text{ until } b] = \text{fix}(\Gamma')$$

where

$$\Gamma'(F') = \{(\sigma, \sigma') \mid \exists \sigma'' . \mathcal{B}[b](\sigma'') = \mathbf{false} \wedge (\sigma, \sigma'') \in \mathcal{C}[c] \wedge (\sigma'', \sigma') \in F'\} \cup \{(\sigma, \sigma') \mid \mathcal{B}[b](\sigma') = \mathbf{true} \wedge (\sigma, \sigma') \in \mathcal{C}[c]\}.$$

We wish to prove $\mathcal{C}[c; \text{while } \neg b \text{ do } c] = \mathcal{C}[\text{repeat } c \text{ until } b]$. Let $P(F, F')$ be the property that $\Gamma(F) \circ \mathcal{C}[c] = \Gamma'(F')$. Our problem then reduces to proving $P(\text{fix}(\Gamma), \text{fix}(\Gamma'))$, which opens the way for using fixed-point induction. First, consider $P(\emptyset, \emptyset)$. We have

$$\begin{aligned} \Gamma(\emptyset) \circ \mathcal{C}[c] &= \{(\sigma, \sigma) \mid \mathcal{B}[\neg b](\sigma) = \mathbf{false}\} \circ \mathcal{C}[c] = \\ &= \{(\sigma, \sigma') \mid \mathcal{B}[b](\sigma') = \mathbf{true} \wedge (\sigma, \sigma') \in \mathcal{C}[c]\} = \Gamma'(\emptyset). \end{aligned}$$

As induction hypothesis, assume $P(F, F')$. This gives

$$\begin{aligned} \Gamma(\Gamma(F)) \circ \mathcal{C}[c] &= \{(\sigma, \sigma') \mid \mathcal{B}[b](\sigma) = \mathbf{false} \wedge \\ &(\sigma, \sigma') \in \Gamma(F) \circ \mathcal{C}[c]\} \cup \{(\sigma, \sigma) \mid \mathcal{B}[b](\sigma) = \mathbf{true}\} \circ \mathcal{C}[c] = \\ &= \{(\sigma, \sigma') \mid \exists \sigma'' . \mathcal{B}[b](\sigma'') = \mathbf{false} \wedge (\sigma, \sigma'') \in \mathcal{C}[c] \wedge \\ &(\sigma'', \sigma') \in \Gamma'(F')\} \cup \{(\sigma, \sigma') \mid \mathcal{B}[b](\sigma') = \mathbf{true} \wedge \\ &(\sigma, \sigma') \in \mathcal{C}[c]\} = \Gamma'(\Gamma'(F')). \end{aligned}$$

Using the principle of fixed-point induction, we have now established the equivalence.

Principle of structural induction

Justification Special case of well-founded induction; \prec is the term-subterm relation.

Prerequisites Let A be the set defined by the grammar $G = (T, N, S, R)$, where T is the set of terminal symbols, N is the set of nonterminal symbols, S is the start symbol and where we have a set of rules $R \subseteq (T \cup N)^* \times (T \cup N)^*$. Let P be a property of elements in A .

Rule
$$\frac{\forall t \in T. P(t) \wedge \forall (x, y) \in R. P(x) \Rightarrow P(y)}{\forall a \in A. P(a)}$$

Application Assume that a property holds of the left side of a formation rule. Prove that this implies that the property holds of the right-side term. When this has been repeated for all rules, every possible way of forming terms in A is covered. Often used for proving relatively simple properties such as determinism.

Example Consider the grammar defining the set of arithmetic expressions **Aexp** in **IMP**, written in BNF:

$$a ::= n \mid X \mid a + a \mid a - a \mid a \times a$$

Note that the set of terminal symbols is the union of the set of numbers **N** and the set of locations **Loc**. Hence, if we wish to prove a property P , we must first prove it for all elements in **N** and **Loc**. We then assume P holds for the nonterminal symbol a , and show that it is then the case that it holds for any other right-side term. Consider now the termination property of arithmetic expressions under big-step operational semantics, i.e. consider

$$\forall a \in \mathbf{Aexp}. \forall \sigma \in \Sigma. \exists m \in \mathbf{N}. \langle a, \sigma \rangle \rightarrow m.$$

Proving this fact when a is member of **N** or **Loc** is trivial; in the first case, take the number itself, and in the second case, take $\sigma(X)$. Next, assume that there exists numbers m_0 and m_1 for some expressions a_0 and a_1 in state σ . From this we can conclude that there exists a number m such that $\langle a_0 \text{ op } a_1, \sigma \rangle \rightarrow m$; simply take $m = m_0 \text{ op } m_1$, where op is the arithmetic operation that **op** represents. Applying the principle of structural induction, the proof that the property holds is done.

Principle of mathematical induction

Justification Special case of well-founded induction; \prec is the predecessor-successor relation of natural numbers.

Prerequisites Let \mathbb{N} be the set of the natural numbers, and let P be a property of elements in \mathbb{N} .

Rule
$$\frac{P(0) \wedge \forall m \in \mathbb{N}. P(m) \Rightarrow P(m+1)}{\forall n \in \mathbb{N}. P(n)}$$

Application Prove that property holds of 0 and assume that it holds for some number m . Show that this implies that it holds for $m+1$. Used whenever natural numbers are involved.

Example Define

$$\begin{aligned} c_1 &\equiv \text{ while } X \geq 0 \text{ do } Y := 5; X := 3, \text{ and} \\ c_2 &\equiv Y := 5; \text{ while } X \geq 0 \text{ do } X := 3. \end{aligned}$$

We wish to prove that $c_1 \sim c_2$ when X is initially non-negative or Y is initially 5, under denotational semantics. Let Γ_1 and Γ_2 be the functionals of the while loops in c_1 and c_2 , respectively. Following the definitions we have

$$\begin{aligned} \Gamma_1(F) &= \{(\sigma, \sigma') \mid \sigma(X) \geq 0 \wedge (\sigma[5/Y, 3/X], \sigma') \in F\} \cup \\ &\quad \{(\sigma, \sigma) \mid \sigma(X) < 0\}, \text{ and} \\ \Gamma_2(F) &= \{(\sigma, \sigma') \mid \sigma(X) \geq 0 \wedge (\sigma[3/X], \sigma') \in F\} \cup \\ &\quad \{(\sigma, \sigma) \mid \sigma(X) < 0\}. \end{aligned}$$

By the fixed-point theorem, we know there exists fixed points for each of these functionals. Hence, it is sufficient to prove, for all natural numbers $i \in \mathbb{N}$, that

$$\begin{aligned} \forall \sigma. (\sigma(X) \geq 0 \vee \sigma(Y) = 5) &\Rightarrow \forall \sigma'. \\ (\sigma, \sigma') \in \Gamma_1^i(\emptyset) &\iff (\sigma[5/Y], \sigma') \in \Gamma_2^i(\emptyset). \end{aligned}$$

Trivially, this property holds for $i = 0$, since $\Gamma_1^0 = \Gamma_2^0 = \emptyset$. Assume next that it holds for $i = k$ when $\sigma(X) \geq 0$. Note that $\Gamma_j^{k+1}(\emptyset) = \Gamma_j(\Gamma_j^k(\emptyset))$ for $j = 1, 2$. We have

$$\begin{aligned} (\sigma, \sigma') \in \Gamma_1(\Gamma_1^k(\emptyset)) &\iff (\sigma[3/X, 5/Y], \sigma') \in \Gamma_1^k(\emptyset) \iff \\ (\sigma[3/X, 5/Y], \sigma') &\in \Gamma_2^k(\emptyset) \iff (\sigma[5/Y], \sigma') \in \Gamma_2(\Gamma_2^k(\emptyset)). \end{aligned}$$

To cover all cases, assume $\sigma(X) < 0 \wedge \sigma(Y) = 5$. Since we then have $\sigma = \sigma[5/Y]$, it is trivial that

$$(\sigma, \sigma) \in \Gamma_1(\Gamma_1^k(\emptyset)) \iff (\sigma[5/Y], \sigma) \in \Gamma_2(\Gamma_2^k(\emptyset)).$$

Thus, the property also holds for $i = k+1$, and we apply the principle of mathematical induction to conclude the proof.