university of groningen

Basic Approaches to the Semantics of Computation (BaSC)

Lecture 3: Well-Founded Induction and IMP

Jorge A. Pérez

Bernoulli Institute for Mathematics, Computer Science, and AI
University of Groningen, Groningen, the Netherlands

November 17, 2025

From Lecture 1

Suppose that we have expressions with variables, denoted $x, y, \ldots$:

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \mid \otimes \mathsf{E}$$

- How to evaluate expressions such as $(x \oplus 4) \otimes y$?
- Solution: We need some memories

$$\mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

- The states of the abstract machines and the interpretation function:

$$\langle \mathsf{E}, \sigma \rangle \qquad\qquad \mathcal{E}[\![\cdot]\!] : \mathit{Exp} \to (\mathbb{M} \to \mathbb{N})$$

From Lecture 1

Suppose that we have expressions with variables, denoted $x, y, \ldots$:

$$\mathsf{E} ::= x \mid \mathsf{N} \mid \mathsf{E} \oplus \mathsf{E} \mid \mathsf{E} \mid \;\otimes \mathsf{E}$$

- How to evaluate expressions such as $(x \oplus 4) \otimes y$?
- Solution: We need some memories

$$\mathbb{M} \triangleq \{\sigma \mid \sigma : X \to \mathbb{N}\}$$

- The states of the abstract machines and the interpretation function:

$$\langle \mathsf{E}, \sigma \rangle \qquad\qquad \mathcal{E}[\![\cdot]\!] : \mathit{Exp} \to (\mathbb{M} \to \mathbb{N})$$

Today: A proof technique (well-founded induction) and the syntax of IMP

Part I

Motivation

Proof Techniques

- How to prove an existential statement? $\exists x.\, P(x)$

Proof Techniques

- How to prove an existential statement? $\exists x \,.\, P(x)$
  $\rightarrow$ Exhibit a **witness**.

Proof Techniques

- How to prove an existential statement? $\exists x \,.\, P(x)$

  $\rightarrow$ Exhibit a **witness**.

Statement	**Witness**
$\exists n \in \mathbb{N}. n^2 \leq n$	$n = 0$

Proof Techniques

- How to prove an existential statement? $\exists x\,.\,P(x)$
  $\rightarrow$ Exhibit a **witness**.

Statement	**Witness**
$\exists n \in \mathbb{N}. n^2 \leq n$	$n = 0$

- How to disprove a universal statement? $\forall x\,.\,P(x) \equiv \exists x . \neg P(x)$

Proof Techniques

- How to prove an existential statement? $\exists x\,.\,P(x)$
  $\rightarrow$ Exhibit a **witness**.

Statement	**Witness**
$\exists n \in \mathbb{N}. n^2 \leq n$	$n = 0$

- How to disprove a universal statement? $\overline{\forall x\,.\,P(x)} \equiv \exists x\,.\neg P(x)$
  $\rightarrow$ Exhibit a **counter-example** to P.

Proof Techniques

- How to prove an existential statement? $\exists x.\, P(x)$
  $\rightarrow$ Exhibit a **witness**.

Statement	**Witness**
$\exists n \in \mathbb{N}. n^2 \leq n$	$n = 0$

- How to disprove a universal statement? $\forall x.\, P(x) \equiv \exists x. \neg P(x)$
  $\rightarrow$ Exhibit a **counter-example** to P.

Statement	**Counterexample**
$\forall n \in \mathbb{N}. n^2 \leq n$	$n = 2$

Proof Techniques

- How to prove an existential statement? $\exists x \,.\, P(x)$
  $\rightarrow$ Exhibit a **witness**.
- How to disprove a universal statement? $\forall x \,.\, P(x) \equiv \exists x \,.\, \neg P(x)$
  $\rightarrow$ Exhibit a **counter-example** to P.
- Prove a universal statement? $\forall x \,.\, P(x)$
  $\rightarrow$ Use **induction**!

Proof Techniques

- How to prove an existential statement? $\exists x \,.\, P(x)$
  $\rightarrow$ Exhibit a **witness**.
- How to disprove a universal statement? $\forall x \,.\, P(x) \equiv \exists x \,.\, \neg P(x)$
  $\rightarrow$ Exhibit a **counter-example** to P.
- Prove a universal statement? $\forall x \,.\, P(x)$
  $\rightarrow$ Use **induction**!

Today: Well-founded induction
Induction on well-founded relations

What is Common To

- natural numbers
- lists
- trees
- grammar languages
- terms of a signature
- theorems of a logic system
- derivations
- computations

What is Common To

- natural numbers
- lists
- trees
- grammar languages
- terms of a signature
- theorems of a logic system
- derivations
- computations

generated by
finite applications of
some given rules

What is Common To

- natural numbers
- lists
- trees
- grammar languages
- terms of a signature
- theorems of a logic system
- derivations
- computations

generated by
finite applications of
some given rules

base cases
inductive cases

What is Common To

	base case	inductive case
natural numbers		
lists		
trees		
grammar languages		
terms of a signature		
theorems of a logic system		
derivations		
computations		

What is Common To

	base case	inductive case
natural numbers	0	succ
lists		
trees		
grammar languages		
terms of a signature		
theorems of a logic system		
derivations		
computations		

What is Common To

	base case	inductive case
natural numbers	0	succ
lists	nil	cons
trees		
grammar languages		
terms of a signature		
theorems of a logic system		
derivations		
computations		

What is Common To

	base case	inductive case
natural numbers	0	succ
lists	nil	cons
trees	nil	node
grammar languages		
terms of a signature		
theorems of a logic system		
derivations		
computations		

What is Common To

	base case	**inductive case**
natural numbers	0	succ
lists	nil	cons
trees	nil	node
grammar languages	productions with terminal symbols only	productions with non-terminal symbols
terms of a signature		
theorems of a logic system		
derivations		
computations		

What is Common To

	base case	inductive case
natural numbers	0	succ
lists	nil	cons
trees	nil	node
grammar languages	productions with terminal symbols only	productions with non-terminal symbols
terms of a signature	constants	operators
theorems of a logic system		
derivations		
computations		

What is Common To

	base case	inductive case
natural numbers	0	succ
lists	nil	cons
trees	nil	node
grammar languages	productions with terminal symbols only	productions with non-terminal symbols
terms of a signature	constants	operators
theorems of a logic system	axioms	inference rules
derivations	axioms	inference rules
computations		

What is Common To

	base case	inductive case
natural numbers	0	succ
lists	nil	cons
trees	nil	node
grammar languages	productions with terminal symbols only	productions with non-terminal symbols
terms of a signature	constants	operators
theorems of a logic system	axioms	inference rules
derivations	axioms	inference rules
computations	single step	concatenation

Part II

Well-Founded Induction

Well-Founded Induction

Ingredients

- A set of elements A, possibly infinite.
- A predicate $P : A \to \mathbb{B}$. We want to prove $\forall a \in A.\, P(a)$.
- A binary relation of precedence $\prec \subseteq A \times A$, not necessarily transitive.

Well-Founded Induction

Ingredients

- A set of elements A, possibly infinite.
- A predicate $P : A \to \mathbb{B}$. We want to prove $\forall a \in A.\, P(a)$.
- A binary relation of precedence $\prec \subseteq A \times A$, not necessarily transitive.
  - $a \prec b$ reads 'a precedes b'
  - also written $b \succ a$
  - also written $a \to b$ (graph notation)

Well-Founded Induction

Ingredients

- A set of elements A, possibly infinite.
- A predicate $P : A \to \mathbb{B}$. We want to prove $\forall a \in A.\, P(a)$.
- A binary relation of precedence $\prec \subseteq A \times A$, not necessarily transitive.
  - $a \prec b$ reads 'a precedes b'
  - also written $b \succ a$
  - also written $a \to b$ (graph notation)
- To use induction, we must guarantee to reach some base cases.

Well-Founded Induction

Ingredients

- A set of elements A, possibly infinite.
- A predicate $P : A \to \mathbb{B}$. We want to prove $\forall a \in A.\, P(a)$.
- A binary relation of precedence $\prec \subseteq A \times A$, not necessarily transitive.
  - $a \prec b$ reads 'a precedes b'
  - also written $b \succ a$
  - also written $a \to b$ (graph notation)
- To use induction, we must guarantee to reach some base cases.
  Hence, no infinite descending chain is allowed in $\prec$.
  That is, $\prec$ must be well-founded.

Well-founded Induction Principle

Well-founded Induction

Let $\prec \subseteq A \times A$ be well-founded.

$$(\forall a \in A.\, P(a)) \Leftrightarrow (\forall a \in A.\, (\forall b \prec a.\, P(b)) \Rightarrow P(a))$$

Well-founded Induction Principle

Well-founded Induction

Let $\prec \subseteq A \times A$ be well-founded.

$$(\forall a \in A.\, P(a)) \Leftrightarrow (\forall a \in A.\, (\forall b \prec a.\, P(b)) \Rightarrow P(a))$$

Key ideas in the proof of the principle:

- A relation is well-founded iff its transitive closure is well-founded
- Well-founded relations are acyclic
- $\prec$ is well-founded iff any $Q \subseteq A$ has a minimal element

Well-founded Induction Principle

Well-founded Induction

Let $\prec \subseteq A \times A$ be well-founded.

$$(\forall a \in A.\, P(a)) \Leftrightarrow (\forall a \in A.\, (\forall b \prec a.\, P(b)) \Rightarrow P(a))$$

Key ideas in the proof of the principle:

- A relation is well-founded iff its transitive closure is well-founded
- Well-founded relations are acyclic
- $\prec$ is well-founded iff any $Q \subseteq A$ has a minimal element

Goal: Derive useful instances of the induction principle, to reason about IMP.

Well-founded Induction Principle

Well-founded Induction

Let $\prec \subseteq A \times A$ be well-founded.

$$(\forall a \in A.\, P(a)) \Leftrightarrow (\forall a \in A.\, (\forall b \prec a.\, P(b)) \Rightarrow P(a))$$

Key ideas in the proof of the principle:

- A relation is well-founded iff its transitive closure is well-founded
- Well-founded relations are acyclic
- $\prec$ is well-founded iff any $Q \subseteq A$ has a minimal element

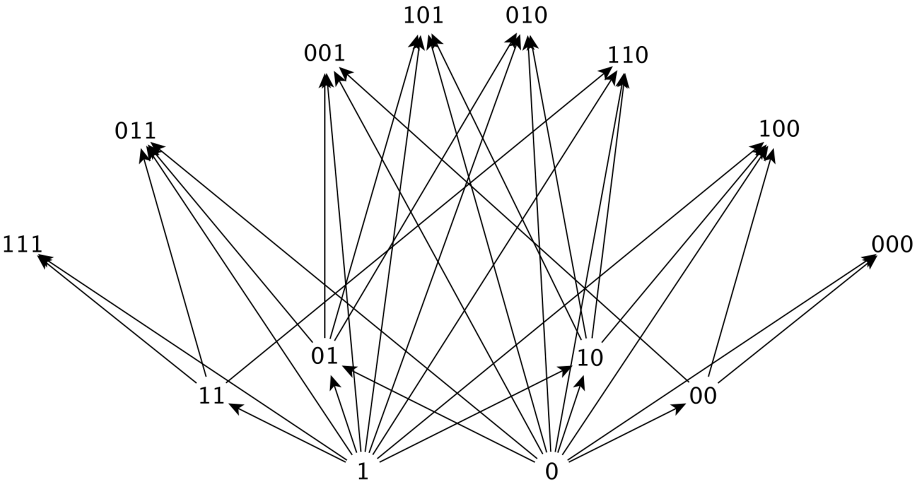
Goal: Derive useful instances of the induction principle, to reason about IMP.

Recall:

- $P \Rightarrow Q$ is equivalent to $\neg Q \Rightarrow \neg P$ (this is the contrapositive formulation).

Example: Graph of a Relation

$A = \mathbb{B}^*$, with $u \prec w$ if u appears in w (with $u \neq \epsilon$ and $u \neq w$)



Infinite Descending Chain

An infinite sequence $\{a_i\}_{i \in \mathbb{N}}$ of elements in A such that $\forall i \in \mathbb{N}. a_i \succ a_{i+1}$

Infinite Descending Chain

An infinite sequence $\{a_i\}_{i \in \mathbb{N}}$ of elements in A such that $\forall i \in \mathbb{N}.\, a_i \succ a_{i+1}$

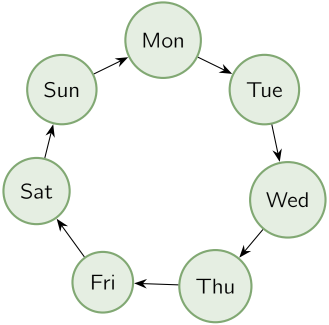
The sequence can also be seen as a function $a : \mathbb{N} \to A$, such that $a(i)$ decreases (in the sense of $\prec$) as i grows:

$$a(0) \succ a(1) \succ a(2) \succ \cdots$$

Infinite Descending Chain

Example

- $A = \{\text{Mon}, \text{Tue}, \text{Wed}, \text{Thu}, \text{Fri}, \text{Sat}, \text{Sun}\}$.
- Sat $\prec$ Sun $\prec$ Mon $\prec \cdots$
  (equivalently: Mon $\succ$ Sun $\succ$ Sat $\succ \cdots$)
- $a(n) = n$th day past



Well-founded Relations

A relation is called **well-founded**
if has no infinite descending chain.

		well-founded?
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	
$\mathbb{N}$	$n \prec m$ if $n < m$	
$\mathbb{Z}$	$n \prec m$ if $n < m$	
$\mathbb{N}$	$n \prec m$ if $n \leq m$	
$\mathbb{N}$	$n \prec m$ if $n = m$	

Well-founded Relations

A relation is called **well-founded** if has no infinite descending chain.

		well-founded?
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	✓
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	
$\mathbb{N}$	$n \prec m$ if $n < m$	
$\mathbb{Z}$	$n \prec m$ if $n < m$	
$\mathbb{N}$	$n \prec m$ if $n \leq m$	
$\mathbb{N}$	$n \prec m$ if $n = m$	

Well-founded Relations

A relation is called **well-founded**
if has no infinite descending chain.

		well-founded?
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	✓
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	✗
$\mathbb{N}$	$n \prec m$ if $n < m$	
$\mathbb{Z}$	$n \prec m$ if $n < m$	
$\mathbb{N}$	$n \prec m$ if $n \leq m$	
$\mathbb{N}$	$n \prec m$ if $n = m$	

Well-founded Relations

A relation is called **well-founded**
if has no infinite descending chain.

		well-founded?
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	✓
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	✗
$\mathbb{N}$	$n \prec m$ if $n < m$	✓
$\mathbb{Z}$	$n \prec m$ if $n < m$	
$\mathbb{N}$	$n \prec m$ if $n \leq m$	
$\mathbb{N}$	$n \prec m$ if $n = m$	

Well-founded Relations

A relation is called **well-founded**
if has no infinite descending chain.

		well-founded?
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	✓
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	✗
$\mathbb{N}$	$n \prec m$ if $n < m$	✓
$\mathbb{Z}$	$n \prec m$ if $n < m$	✗
$\mathbb{N}$	$n \prec m$ if $n \leq m$	
$\mathbb{N}$	$n \prec m$ if $n = m$	

Well-founded Relations

A relation is called **well-founded**
if has no infinite descending chain.

		well-founded?
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	✓
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	✗
$\mathbb{N}$	$n \prec m$ if $n < m$	✓
$\mathbb{Z}$	$n \prec m$ if $n < m$	✗
$\mathbb{N}$	$n \prec m$ if $n \leq m$	✗
$\mathbb{N}$	$n \prec m$ if $n = m$	

Well-founded Relations

A relation is called **well-founded**
if has no infinite descending chain.

		well-founded?
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	✓
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	✗
$\mathbb{N}$	$n \prec m$ if $n < m$	✓
$\mathbb{Z}$	$n \prec m$ if $n < m$	✗
$\mathbb{N}$	$n \prec m$ if $n \leq m$	✗
$\mathbb{N}$	$n \prec m$ if $n = m$	✗

Well-founded Relations

A relation is called **well-founded**
if has no infinite descending chain.

		well-founded?
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	✓
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	✗
$\mathbb{N}$	$n \prec m$ if $n < m$	✓
$\mathbb{Z}$	$n \prec m$ if $n < m$	✗
$\mathbb{N}$	$n \prec m$ if $n \leq m$	✗
$\mathbb{N}$	$n \prec m$ if $n = m$	✗

In general, a well-founded relation cannot be reflexive.

Transitive Closure

Given a relation $\prec$, its transitive closure $\prec^+$ is the least relation generated by the following rules:

$$\frac{a \prec b}{a \prec^+ b} \qquad\qquad \frac{a \prec^+ b \qquad b \prec^+ c}{a \prec^+ c}$$

Transitive Closure

Given a relation $\prec$, its transitive closure $\prec^+$ is the least relation generated by the following rules:

$$\frac{a \prec b}{a \prec^+ b} \qquad \frac{a \prec^+ b \qquad b \prec^+ c}{a \prec^+ c}$$

From this definition:

$$\prec \subseteq \prec^+$$
$$(\prec^+)^+ = \prec^+$$

Transitive and Reflexive Closure

Given a relation $\prec$, its transitive and reflexive closure $\prec^*$ is the least relation generated by the following rules:

$$\frac{a \in A}{a \prec^* a} \qquad \frac{a \prec b}{a \prec^* b} \qquad \frac{a \prec^* b \qquad b \prec^* c}{a \prec^* c}$$

Transitive and Reflexive Closure

Given a relation $\prec$, its transitive and reflexive closure $\prec^*$ is the least relation generated by the following rules:

$$\frac{a \in A}{a \prec^* a} \qquad \frac{a \prec b}{a \prec^* b} \qquad \frac{a \prec^* b \qquad b \prec^* c}{a \prec^* c}$$

From this definition:

$$\prec \subseteq \prec^+ \subseteq \prec^*$$
$$(\prec^*)^* = \prec^*$$

Closures and Induced Paths

Given $\prec$, we have:

$a \prec^+ b$ iff there is a non-empty, finite path from a to b in the graph of $\prec$
$\exists k > 0, \{c_i\}_{i \in [0,k]}. a = c_0 \prec c_1 \prec \cdots \prec c_k = b$

$a \prec^* b$ iff there is a possibly empty, finite path from a to b in the graph of $\prec$
$\exists k \geq 0, \{c_i\}_{i \in [0,k]}. a = c_0 \prec c_1 \prec \cdots \prec c_k = b$

Closures, By Example

		$\prec^+$	$\prec^*$
$\mathbb{N}$	$n \prec m$ if $m = n + 1$	$n < m$	$n \leq m$
$\mathbb{Z}$	$n \prec m$ if $m = n + 1$	$n < m$	$n \leq m$
$\mathbb{N}$	$n \prec m$ if $n < m$	$n < m$	$n \leq m$
$\mathbb{N}$	$n \prec m$ if $n \leq m$	$n \leq m$	$n \leq m$
$\mathbb{N}$	$n \prec m$ if $n = m$	$n = m$	$n = m$

Theorem 4.2

A relation $\prec$ is well-founded iff its transitive closure $\prec^+$ is well-founded.

Theorem 4.2

A relation $\prec$ is well-founded iff its transitive closure $\prec^+$ is well-founded.

There are two directions:

1. $\boxed{\prec^+ \text{ w.f.} \Rightarrow \prec \text{ w.f.}}$

2. $\boxed{\prec \text{ w.f.} \Rightarrow \prec^+ \text{ w.f.}}$

Theorem 4.2

A relation $\prec$ is well-founded iff its transitive closure $\prec^+$ is well-founded.

There are two directions:

1. $\boxed{\prec^+ \text{ w.f.} \Rightarrow \prec \text{ w.f.}}$

   Any descending chain for $\prec$ is a descending chain for $\prec^+$. By assumption, the descending chains for $\prec^+$ are finite, so are the descending chains for $\prec$.

2. $\boxed{\prec \text{ w.f.} \Rightarrow \prec^+ \text{ w.f.}}$

Theorem 4.2

A relation $\prec$ is well-founded iff its transitive closure $\prec^+$ is well-founded.

There are two directions:

1. $\boxed{\prec^+ \text{ w.f.} \Rightarrow \prec \text{ w.f.}}$

   Any descending chain for $\prec$ is a descending chain for $\prec^+$. By assumption, the descending chains for $\prec^+$ are finite, so are the descending chains for $\prec$.

2. $\boxed{\prec \text{ w.f.} \Rightarrow \prec^+ \text{ w.f.}}$

Theorem 4.2

A relation $\prec$ is well-founded iff its transitive closure $\prec^+$ is well-founded.

There are two directions:

1. $\boxed{\prec^+ \text{ w.f.} \Rightarrow \prec \text{ w.f.}}$

   Any descending chain for $\prec$ is a descending chain for $\prec^+$. By assumption, the descending chains for $\prec^+$ are finite, so are the descending chains for $\prec$.

2. $\boxed{\prec \text{ w.f.} \Rightarrow \prec^+ \text{ w.f.} \equiv \neg(\prec^+ \text{ w.f.}) \;\Rightarrow\; \neg(\prec \text{ w.f.})}$

Theorem 4.2

A relation $\prec$ is well-founded iff its transitive closure $\prec^+$ is well-founded.

There are two directions:

1. $\boxed{\prec^+ \text{ w.f.} \Rightarrow \prec \text{ w.f.}}$

   Any descending chain for $\prec$ is a descending chain for $\prec^+$. By assumption, the descending chains for $\prec^+$ are finite, so are the descending chains for $\prec$.

2. $\boxed{\prec \text{ w.f.} \Rightarrow \prec^+ \text{ w.f.} \equiv \neg(\prec^+ \text{ w.f.}) \;\Rightarrow\; \neg(\prec \text{ w.f.})}$

   Consider an infinite descending chain for $\prec^+$:

$$a_0 \succ^+ a_1 \succ^+ a_2 \succ^+ \cdots$$

   Recall that $a \succ^+ b$ iff there is a non-empty, finite path from a to b in the graph of $\prec$. Therefore, we derive the infinite descending chain in $\prec$:

$$a_0 \succ \cdots \succ a_1 \succ \cdots \succ a_2 \succ \cdots \succ \cdots$$

Acyclic Relations

- We say that the relation $\prec$ has a cycle if $a \prec^+ a$, for some $a \in A$.
- We say that $\prec$ is acyclic if it has no cycles: $\forall a \in A . a \not\prec^+ a$.
- Note that $\prec$ is acyclic iff $\prec^+$ is acyclic.

Theorem 4.3

If $\prec$ is well-founded then it is acyclic.

By contraposition:

Theorem 4.3

If $\prec$ is well-founded then it is acyclic.

By contraposition: we prove that if $\prec$ has a cycle then it is not well-founded.

- Take a $a \in A$ such that $a \prec^+ a$. We have an infinite descending chain:

$$a \succ^+ a \succ^+ a \succ^+ \cdots$$

- Hence, $\succ^+$ is not well-founded. By Theorem 4.2, then $\succ$ is not well-founded.

Minimal Element

Let $\prec$ be a relation over A.

- Given $Q \subseteq A$, we say $m \in Q$ is minimal if there is no $x \in Q$ such that $x \prec m$. That is, $\forall x \in Q . m \not\prec x$
- Q has no minimal element if $\forall m \in Q . \exists x \in Q . x \prec m$.

Lemma 4.1

$\prec$ is well-founded iff
every nonempty $Q \subseteq A$ contains a minimal element m.

Lemma 4.1

(1) $\prec$ has an infinite descending chain iff
(2) there is an non-empty $Q \subseteq A$ with no minimal element

Lemma 4.1

(1) $\prec$ has an infinite descending chain iff
(2) there is an non-empty $Q \subseteq A$ with no minimal element

- **(1)** $\Rightarrow$ **(2)**:
  Take an infinite descending chain $a_1 \succ a_2 \succ a_3 \succ \cdots$ and consider the associated set $Q = \{a_1, a_2, a_3, \ldots\}$. The set Q has no minimal element: for every $a_i \in Q$ we know that there is a $a_{i+1} \in Q$ such that $a_i \succ a_{i+1}$.

Lemma 4.1

(1) $\prec$ has an infinite descending chain iff
(2) there is an non-empty $Q \subseteq A$ with no minimal element

- **(1)** $\Rightarrow$ **(2)**:
  Take an infinite descending chain $a_1 \succ a_2 \succ a_3 \succ \cdots$ and consider the associated set $Q = \{a_1, a_2, a_3, \ldots\}$. The set Q has no minimal element: for every $a_i \in Q$ we know that there is a $a_{i+1} \in Q$ such that $a_i \succ a_{i+1}$.
- **(2)** $\Rightarrow$ **(1)**:
  We consider a non-empty set $Q \subseteq A$ with no minimal element.
  Take any $a_0 \in Q$: because it is not minimal, there is a a_1 such that $a_0 \succ a_1$.
  By a similar reasoning, a_1 is not minimal either; we construct an infinite descending chain by iterating the argument.

Theorem 4.5

Let $\prec$ be a well-founded relation over A.

$$\underbrace{\forall a \in A. P(a)}_{(1)} \Leftrightarrow \underbrace{(\forall a \in A. (\forall b \prec a. P(b)) \Rightarrow P(a))}_{(2)}$$

-

Theorem 4.5

Let $\prec$ be a well-founded relation over A.

$$\underbrace{\forall a \in A.P(a)}_{(1)} \Leftrightarrow \underbrace{(\forall a \in A.(\forall b \prec a.P(b)) \Rightarrow P(a))}_{(2)}$$

Set $H(a) \triangleq \forall b \prec a.P(b)$ and $S(a) \triangleq H(a) \Rightarrow P(a)$.

-

Theorem 4.5

Let $\prec$ be a well-founded relation over A.

$$\underbrace{\forall a \in A.P(a)}_{(1)} \Leftrightarrow \underbrace{(\forall a \in A.(\forall b \prec a.P(b)) \Rightarrow P(a))}_{(2)}$$

Set $H(a) \triangleq \forall b \prec a.P(b)$ and $S(a) \triangleq H(a) \Rightarrow P(a)$.

- **(1)** $\Rightarrow$ **(2)**:
  Assume $\forall a.P(a)$ and take an arbitrary $a \in A$. We have:

$$\begin{aligned} S(a) &\equiv H(a) \Rightarrow P(a) \\ &\equiv (\neg H(a) \vee P(a)) \\ &\equiv (\neg H(a) \vee \mathtt{true}) \\ &\equiv \mathtt{true} \end{aligned}$$

Theorem 4.5

Let $\prec$ be a well-founded relation over A.

$$\underbrace{\forall a \in A.P(a)}_{(1)} \Leftrightarrow \underbrace{(\forall a \in A.(\forall b \prec a.P(b)) \Rightarrow P(a))}_{(2)}$$

Set $H(a) \triangleq \forall b \prec a.P(b)$ and $S(a) \triangleq H(a) \Rightarrow P(a)$.

- **(2)** $\Rightarrow$ **(1)**: (This is the direction we really want!)
  We prove $\neg$**(1)** $\Rightarrow \neg$**(2)**. Assume $\exists a.\neg P(a)$.
  Let $Q = \{q \in A \mid \neg P(a)\} \neq \emptyset$.
  Since $\prec$ is well-founded, then Q has a minimal element $m \in Q$ (Lem. 4.1).
  Clearly, $\neg P(m)$. Because m is minimal, we have $\forall b \prec m.P(b) \equiv H(m)$.
  Thus, $H(m) \wedge \neg P(m) \equiv \neg(H(m) \Rightarrow P(m)) \equiv \neg S(m)$.
  Therefore, $\exists a \in A.\neg S(a)$.

Well-Founded Induction

Let $\prec \subseteq A \times A$ be a well-founded relation.

$$\frac{\forall a \in A.\big((\forall b \prec a. P(b)) \Rightarrow P(a)\big)}{\forall a \in A. P(a)}$$

- A general proof principle, aka Noetherian induction.

Well-Founded Induction

Let $\prec \subseteq A \times A$ be a well-founded relation.

$$\frac{\forall a \in A.\big((\forall b \prec a.P(b)) \Rightarrow P(a)\big)}{\forall a \in A.P(a)}$$

- A general proof principle, aka Noetherian induction.
- Derived from Theorem 4.5, direction **(2)** $\Rightarrow$ **(1)**.

Well-Founded Induction

Let $\prec \subseteq A \times A$ be a well-founded relation.

$$\frac{\forall a \in A.\big((\forall b \prec a.P(b)) \Rightarrow P(a)\big)}{\forall a \in A.P(a)}$$

- A general proof principle, aka Noetherian induction.
- Derived from Theorem 4.5, direction **(2)** $\Rightarrow$ **(1)**.
- When proving $P(a)$ for some a, we can exploit the assumption $\forall b \prec a.P(b)$.

Well-Founded Induction

Let $\prec \subseteq A \times A$ be a well-founded relation.

$$\frac{\forall a \in A. \big((\forall b \prec a. P(b)) \Rightarrow P(a) \big)}{\forall a \in A. P(a)}$$

- A general proof principle, aka Noetherian induction.
- Derived from Theorem 4.5, direction **(2)** $\Rightarrow$ **(1)**.
- When proving $P(a)$ for some a, we can exploit the assumption $\forall b \prec a. P(b)$.
- A base case is any element of A such that the set $\{b \in A \mid b \prec a\}$ is empty.

Well-Founded Induction

Let $\prec \subseteq A \times A$ be a well-founded relation.

$$\frac{\forall a \in A.\Big((\forall b \prec a.P(b)) \Rightarrow P(a)\Big)}{\forall a \in A.P(a)}$$

- A general proof principle, aka Noetherian induction.
- Derived from Theorem 4.5, direction **(2)** $\Rightarrow$ **(1)**.
- When proving $P(a)$ for some a, we can exploit the assumption $\forall b \prec a.P(b)$.
- A base case is any element of A such that the set $\{b \in A \mid b \prec a\}$ is empty.

We may now **instantiate the principle**, by choosing specific A and $\prec$.

Instance 1: Mathematical Induction

- Set: $A = \mathbb{N}$
- Well-founded relation: $\prec \; = \{(n, n+1) \mid n \in \mathbb{N}\}$ (immediate precedence)

$$\frac{\forall a \in A.\big((\forall b \prec a.P(b)) \Rightarrow P(a)\big)}{\forall a \in A.P(a)}$$

Instance 1: Mathematical Induction

- Set: $A = \mathbb{N}$
- Well-founded relation: $\prec \; = \{(n, n+1) \mid n \in \mathbb{N}\}$ (immediate precedence)

$$\frac{\forall a \in A.\Big((\forall b \prec a.P(b)) \Rightarrow P(a)\Big)}{\forall a \in A.P(a)}$$

Two cases:

1. Case $a = 0$: There is no $b \prec 0$ and so $(\forall b \prec 0.P(b)) \equiv \texttt{true}$ and

$$\begin{aligned}((\forall b \prec 0.P(b)) \Rightarrow P(0)) &\equiv \texttt{true} \Rightarrow P(0) \\ &\equiv \boxed{P(0)}\end{aligned}$$

Instance 1: Mathematical Induction

- Set: $A = \mathbb{N}$
- Well-founded relation: $\prec \; = \{(n, n+1) \mid n \in \mathbb{N}\}$ (immediate precedence)

$$\frac{\forall a \in A.\Big((\forall b \prec a.P(b)) \Rightarrow P(a)\Big)}{\forall a \in A.P(a)}$$

Two cases:

1. Case $a = 0$: There is no $b \prec 0$ and so $(\forall b \prec 0.P(b)) \equiv \texttt{true}$ and
$$\begin{aligned}((\forall b \prec 0.P(b)) \Rightarrow P(0)) &\equiv \texttt{true} \Rightarrow P(0)\\ &\equiv \boxed{P(0)}\end{aligned}$$
2. Case $a = n+1$: There is only one b such that $b \prec n+1$, i.e., $b = 1$, and
$$((\forall b \prec n+1.P(b)) \Rightarrow P(n+1)) \equiv \boxed{P(n) \Rightarrow P(n+1)}$$

Instance 1: Mathematical Induction

- Set: $A = \mathbb{N}$
- Well-founded relation: $\prec \, = \{(n, n+1) \mid n \in \mathbb{N}\}$ (immediate precedence)

$$\frac{\forall a \in A. \big((\forall b \prec a. P(b)) \Rightarrow P(a) \big)}{\forall a \in A. P(a)} \quad \rightsquigarrow \quad \frac{P(0) \qquad \forall n \in \mathbb{N}. \big(P(n) \Rightarrow P(n+1) \big)}{\forall a \in A. P(a)}$$

Instance 2: Strong Induction

- Set: $A = \mathbb{N}$
- Well-founded relation: $\prec \; = <$ (strictly-less than)

$$\frac{\forall a \in A.\Big((\forall b \prec a. P(b)) \Rightarrow P(a)\Big)}{\forall a \in A. P(a)}$$

Two cases:

1. Case $a = 0$: As before, there is no $b \prec 0$ and so $(\forall b \prec 0. P(b)) \equiv \texttt{true}$ and

$$((\forall b \prec 0. P(b)) \Rightarrow P(0)) \equiv \boxed{P(0)}$$

Instance 2: Strong Induction

- Set: $A = \mathbb{N}$
- Well-founded relation: $\prec \, = <$ (strictly-less than)

$$\frac{\forall a \in A.\big((\forall b \prec a.P(b)) \Rightarrow P(a)\big)}{\forall a \in A.P(a)}$$

Two cases:

1. Case $a = 0$: As before, there is no $b \prec 0$ and so $(\forall b \prec 0.P(b)) \equiv \texttt{true}$ and

$$((\forall b \prec 0.P(b)) \Rightarrow P(0)) \equiv \boxed{P(0)}$$

2. Case $a = n + 1$: There are multiple b such that $b \prec n + 1$ and

$$((\forall b \prec n+1.P(b)) \Rightarrow P(n+1)) \equiv \boxed{P(0) \wedge \cdots \wedge P(n) \Rightarrow P(n+1)}$$

Instance 2: Strong Induction

- Set: $A = \mathbb{N}$
- Well-founded relation: $\prec\; = <$ (strictly-less than)

$$\frac{P(0) \quad \forall n \in \mathbb{N}.\Big((P(0) \wedge \cdots \wedge P(n)) \Rightarrow P(n+1)\Big)}{\forall a \in A.P(a)}$$

Instance 3: Structural Induction

- Consider a signature $\Sigma = \{\Sigma_n\}_{n \in \mathbb{N}}$.
- Set $A = T_\Sigma$ (closed terms)
- Define the immediate subterm relation $\prec$:

$$\prec = \Big\{ (t_i, f(t_1, \ldots, t_n)) \mid f \in \Sigma_n, i \in [1..n] \Big\}$$

Instance 3: Structural Induction

- Consider a signature $\Sigma = \{\Sigma_n\}_{n \in \mathbb{N}}$.
- Set $A = T_\Sigma$ (closed terms)
- Define the immediate subterm relation $\prec$:

$$\prec = \left\{ (t_i, f(t_1, \ldots, t_n)) \mid f \in \Sigma_n, i \in [1..n] \right\}$$

Example

Let $\Sigma_0 = \{0\}$, $\Sigma_1 = \{\mathsf{succ}\}$, and $\Sigma_2 = \{\mathsf{plus}\}$. We have:

- $0 \prec \mathsf{succ}(0) \prec \mathsf{plus}(0, \mathsf{succ}(0))$

Instance 3: Structural Induction

- Consider a signature $\Sigma = \{\Sigma_n\}_{n \in \mathbb{N}}$.
- Set $A = T_\Sigma$ (closed terms)
- Define the immediate subterm relation $\prec$:

$$\prec = \Big\{ (t_i, f(t_1, \dots, t_n)) \mid f \in \Sigma_n, i \in [1..n] \Big\}$$

Example

Let $\Sigma_0 = \{0\}$, $\Sigma_1 = \{\mathsf{succ}\}$, and $\Sigma_2 = \{\mathsf{plus}\}$. We have:

- $0 \prec \mathsf{succ}(0) \prec \mathsf{plus}(0, \mathsf{succ}(0))$
- $0 \prec \mathsf{plus}(0, \mathsf{succ}(0))$

Instance 3: Structural Induction

- Consider a signature $\Sigma = \{\Sigma_n\}_{n \in \mathbb{N}}$.
- Set $A = T_\Sigma$ (closed terms)
- Define the immediate subterm relation $\prec$:

$$\prec = \left\{ (t_i, f(t_1, \ldots, t_n)) \mid f \in \Sigma_n, i \in [1..n] \right\}$$

Example

Let $\Sigma_0 = \{0\}$, $\Sigma_1 = \{\mathsf{succ}\}$, and $\Sigma_2 = \{\mathsf{plus}\}$. We have:

- $0 \prec \mathsf{succ}(0) \prec \mathsf{plus}(0, \mathsf{succ}(0))$
- $0 \prec \mathsf{plus}(0, \mathsf{succ}(0))$
- $0 \not\prec \mathsf{plus}(\mathsf{succ}(0), \mathsf{succ}(0))$

Instance 3: Structural Induction

- Consider a signature $\Sigma = \{\Sigma_n\}_{n \in \mathbb{N}}$.
- Set $A = T_\Sigma$ (closed terms)
- Define the immediate subterm relation $\prec$:

$$\prec = \Big\{(t_i, f(t_1, \ldots, t_n)) \mid f \in \Sigma_n, i \in [1..n]\Big\}$$

Example

Let $\Sigma_0 = \{0\}$, $\Sigma_1 = \{\mathsf{succ}\}$, and $\Sigma_2 = \{\mathsf{plus}\}$. We have:

- $0 \prec \mathsf{succ}(0) \prec \mathsf{plus}(0, \mathsf{succ}(0))$
- $0 \prec \mathsf{plus}(0, \mathsf{succ}(0))$
- $0 \not\prec \mathsf{plus}(\mathsf{succ}(0), \mathsf{succ}(0))$

Before instantiating the principle, we need to prove that $\prec$ is well founded.

Subterm Relation is Well Founded

In the proof, we relate $\prec$ to a known well-founded relation:

- Let $\mathit{depth} : T_\Sigma \to \mathbb{N}$ be defined as

$$\begin{aligned} \mathit{depth}(c) &\triangleq 1 && \text{if } c \in \Sigma_0 \\ \mathit{depth}(f(t_1, \ldots, t_n)) &\triangleq 1 + \max_{i \in [1..n]} \mathit{depth}(t_i) && \text{if } f \in \Sigma_n \end{aligned}$$

- By definition, if $t \prec t'$ then $\mathit{depth}(t) < \mathit{depth}(t')$.
- Any descending chain in $\prec$ induces a descending chain in $<$.
- Since $<$ is well-founded, so is $\prec$.

Corollary

- Because $\prec$ is well-founded, its transitive closure $\prec^+$ is well-founded.

Example

Let $\Sigma_0 = \{0\}$, $\Sigma_1 = \{\mathsf{succ}\}$, and $\Sigma_2 = \{\mathsf{plus}\}$. We have:

- $0 \prec^+ \mathsf{succ}(0) \prec^+ \mathsf{plus}(0, \mathsf{succ}(0))$
- $0 \prec^+ \mathsf{plus}(0, \mathsf{succ}(0))$
- $0 \prec^+ \mathsf{plus}(\mathsf{succ}(0), \mathsf{succ}(0))$

Instance 3: Structural Induction

- Set: $A = T_\Sigma$ (closed terms)
- Well-founded relation: $\prec = \{(t_i, f(t_1, \ldots, t_n)) \mid f \in \Sigma_n, i \in [1..n]\}$

$$\frac{\forall a \in A.\big((\forall b \prec a.P(b)) \Rightarrow P(a)\big)}{\forall a \in A.P(a)}$$

$$\rightsquigarrow$$

$$\frac{\forall n \in \mathbb{N}.\forall f \in \Sigma_n.\forall t_1, \ldots, t_n.(P(t_1) \wedge \cdots \wedge P(t_n)) \Rightarrow P(f(t_1, \ldots, t_n))}{\forall t \in T_\Sigma.P(t)}$$

Part III

Induction At Work

IMP: A Language in Three Layers

- Arithmetic expressions

$$a ::= x \mid n \mid a \text{ op } a$$

IMP: A Language in Three Layers

variables (or identifiers)

- **Arithmetic expressions**

integers

$$a ::= x \mid n \mid a \text{ op } a$$

binary expressions (op $\in \{+, -, \times\}$)

IMP: A Language in Three Layers

- **Arithmetic expressions**

$$a ::= x \mid n \mid a \; \mathsf{op} \; a$$

- **Boolean expressions**

true ($\mathtt{tt}$) or false ($\mathtt{ff}$)

binary expressions ($\mathsf{bop} \in \{\wedge, \vee\}$)

$$b ::= v \mid a \; \mathsf{cmp} \; a \mid \neg b \mid b \; \mathsf{bop} \; b$$

comparisons ($\mathsf{cmp} \in \{<, \leq, >, \geq, =, \neq\}$)

IMP: A Language in Three Layers

- **Arithmetic expressions**

  variables (or identifiers)

  integers

  $$a ::= x \mid n \mid a \text{ op } a$$

  binary expressions (op $\in \{+, -, \times\}$)

- **Boolean expressions**

  true ($\texttt{tt}$) or false ($\texttt{ff}$)

  binary expressions (bop $\in \{\wedge, \vee\}$)

  $$b ::= v \mid a \text{ cmp } a \mid \neg b \mid b \text{ bop } b$$

  comparisons (cmp $\in \{<, \leq, >, \geq, =, \neq\}$)

- **Commands**

  $$c ::= \textbf{skip} \mid x := a \mid \textbf{if } b \textbf{ then } c \textbf{ else } c \mid \textbf{while } b \textbf{ do } c$$

IMP: A Language in Three Layers

The syntax of IMP:

$$a ::= x \mid n \mid a \, \mathsf{op} \, a$$

$$b ::= v \mid a \, \mathsf{cmp} \, a \mid \neg b \mid b \, \mathsf{bop} \, b$$

$$c ::= \textbf{skip} \mid x := a \mid \textbf{if } b \textbf{ then } c \textbf{ else } c \mid \textbf{while } b \textbf{ do } c$$

Let's focus for the moment on arithmetic expressions and their properties.

Arithmetic Expressions

Syntax

$$x \in \mathsf{Ide} \qquad n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \mathsf{Ide} \to \mathbb{Z}\} \qquad \mathsf{op} \in \{+, -, \times\}$$

$$a ::= x \mid n \mid a \;\mathsf{op}\; a$$

Semantics

Arithmetic Expressions

Syntax

$$x \in \mathsf{Ide} \qquad n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \mathsf{Ide} \to \mathbb{Z}\} \qquad \mathsf{op} \in \{+, -, \times\}$$

$$a ::= x \mid n \mid a \;\mathsf{op}\; a$$

Semantics

$$\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$$

Arithmetic Expressions

Syntax

$$x \in \mathsf{Ide} \qquad n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \mathsf{Ide} \to \mathbb{Z}\} \qquad \mathsf{op} \in \{+, -, \times\}$$

$$a ::= \; x \mid n \mid a \;\mathsf{op}\; a$$

Semantics

$$\frac{}{\langle x , \sigma \rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n , \sigma \rangle \longrightarrow n}$$

Arithmetic Expressions

Syntax

$$x \in \mathsf{Ide} \qquad n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \mathsf{Ide} \to \mathbb{Z}\} \qquad \mathsf{op} \in \{+, -, \times\}$$

$$a ::= x \mid n \mid a \;\mathsf{op}\; a$$

Semantics

$$\frac{}{\langle x, \sigma\rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma\rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \;\mathsf{op}\; a_1, \sigma\rangle \longrightarrow n_0 \; op \; n_1}$$

Arithmetic Expressions

Syntax

$$x \in \mathsf{Ide} \qquad n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \mathsf{Ide} \to \mathbb{Z}\} \qquad \mathsf{op} \in \{+, -, \times\}$$

$$a ::= x \mid n \mid a \;\mathsf{op}\; a$$

Semantics

$$\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma \rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \;\mathsf{op}\; a_1, \sigma \rangle \longrightarrow n_0 \; op \; n_1}$$

A termination property:

- $P(a) \triangleq \forall \sigma \in \mathbb{M}. \exists m \in \mathbb{Z}. \langle a, \sigma \rangle \longrightarrow m.$
- $\forall a. P(a)$? Structural Induction!

Structural Induction

Given the syntax of arithmetic expressions:

$$a ::= x \mid n \mid a \text{ op } a$$

We have that structural induction is as follows:

$$\frac{\forall x \in \mathsf{Ide} \qquad \forall n \in \mathbb{Z} \qquad \forall a_0, a_1 .\, P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)}{\forall a . P(a)}$$

To establish termination we have two base cases, and one inductive case.

Termination: Base Case (1 of 2)

$$\forall x \in \mathsf{Ide}.\ P(x)$$

Termination: Base Case (1 of 2)

$$\forall x \in \mathsf{Ide}.\ P(x)$$

Take some arbitrary identifier $x \in \mathsf{Ide}$. We must prove:

$$P(x) \triangleq \forall \sigma.\ \exists m.\ \langle x, \sigma \rangle \longrightarrow m$$

Termination: Base Case (1 of 2)

$$\forall x \in \mathsf{Ide}.\, P(x)$$

Take some arbitrary identifier $x \in \mathsf{Ide}$. We must prove:

$$P(x) \triangleq \forall \sigma.\, \exists m.\, \langle x, \sigma \rangle \longrightarrow m$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle x, \sigma \rangle \longrightarrow m$, where m is the only variable.

Termination: Base Case (1 of 2)

$$\forall x \in \text{Ide}.\, P(x)$$

Take some arbitrary identifier $x \in \text{Ide}$. We must prove:

$$P(x) \triangleq \forall \sigma.\, \exists m.\, \langle x, \sigma \rangle \longrightarrow m$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle x, \sigma \rangle \longrightarrow m$, where m is the only variable.
- By rule $\dfrac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$ we have $\langle x, \sigma \rangle \longrightarrow m \nwarrow_{[m = \sigma(x)]}$ $\square$

Termination: Base Case (1 of 2)

$$\forall x \in \mathsf{Ide}.\, P(x)$$

Take some arbitrary identifier $x \in \mathsf{Ide}$. We must prove:

$$P(x) \triangleq \forall \sigma.\, \exists m.\, \langle x, \sigma \rangle \longrightarrow m$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle x, \sigma \rangle \longrightarrow m$, where m is the only variable.
- By rule $\dfrac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$ we have $\langle x, \sigma \rangle \longrightarrow m \nwarrow_{[m = \sigma(x)]} \square$
- We are done by taking $m = \sigma(x)$.

Termination: Base Case (2 of 2)

$$\forall n \in \mathbb{Z}.\, P(n)$$

We proceed similarly as before: Take some arbitrary $n \in \mathbb{Z}$. We must prove:

$$P(n) \triangleq \forall \sigma.\, \exists m.\, \langle n, \sigma \rangle \longrightarrow m$$

Termination: Base Case (2 of 2)

$$\forall n \in \mathbb{Z}.\, P(n)$$

We proceed similarly as before: Take some arbitrary $n \in \mathbb{Z}$. We must prove:

$$P(n) \triangleq \forall \sigma.\, \exists m.\, \langle n, \sigma \rangle \longrightarrow m$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle n, \sigma \rangle \longrightarrow m$, where m is the only variable.

Termination: Base Case (2 of 2)

$$\forall n \in \mathbb{Z}.\, P(n)$$

We proceed similarly as before: Take some arbitrary $n \in \mathbb{Z}$. We must prove:

$$P(n) \triangleq \forall \sigma.\, \exists m.\, \langle n, \sigma \rangle \longrightarrow m$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle n, \sigma \rangle \longrightarrow m$, where m is the only variable.
- By rule $\dfrac{}{\langle n, \sigma \rangle \longrightarrow n}$ we have $\langle n, \sigma \rangle \longrightarrow m \nwarrow_{[m=n]}$ $\square$

Termination: Base Case (2 of 2)

$$\forall n \in \mathbb{Z}.\, P(n)$$

We proceed similarly as before: Take some arbitrary $n \in \mathbb{Z}$. We must prove:

$$P(n) \triangleq \forall \sigma.\, \exists m.\, \langle n, \sigma \rangle \longrightarrow m$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle n, \sigma \rangle \longrightarrow m$, where m is the only variable.
- By rule $\dfrac{}{\langle n, \sigma \rangle \longrightarrow n}$ we have $\langle n, \sigma \rangle \longrightarrow m \nwarrow_{[m=n]} \square$
- We are done by taking $m = n$.

Termination: Inductive Case

$$\forall a_0, a_1 .\ P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \ \mathsf{op}\ a_1)$$

- Take some arbitrary expressions a_0, a_1. We assume:

$$P(a_0) \triangleq \forall \sigma .\ \exists m_0 .\ \langle a_0, \sigma \rangle \longrightarrow m_0$$
$$P(a_1) \triangleq \forall \sigma .\ \exists m_1 .\ \langle a_1, \sigma \rangle \longrightarrow m_1$$

We must prove $P(a_0 \ \mathsf{op}\ a_1) \triangleq \forall \sigma .\ \exists m .\ \langle a_0 \ \mathsf{op}\ a_1, \sigma \rangle \longrightarrow m$.

Termination: Inductive Case (cont.)

$$\forall a_0, a_1 \,.\, P(a_0) \land P(a_1) \;\Rightarrow\; P(a_0 \;\mathsf{op}\; a_1)$$

Termination: Inductive Case (cont.)

$$\forall a_0, a_1 \,.\, P(a_0) \wedge P(a_1) \;\Rightarrow\; P(a_0 \;\mathsf{op}\; a_1)$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle a_0 \,\mathsf{op}\, a_1 , \sigma \rangle \longrightarrow m$, where m is the only variable.

Termination: Inductive Case (cont.)

$$\forall a_0, a_1 .\, P(a_0) \wedge P(a_1) \;\Rightarrow\; P(a_0 \text{ op } a_1)$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle a_0 \,\text{op}\, a_1 , \sigma \rangle \longrightarrow m$, where m is the only variable.
- By rule $\dfrac{\langle a_0 , \sigma \rangle \longrightarrow n_0 \quad \langle a_1 , \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1 , \sigma \rangle \longrightarrow n_0 \ op\ n_1}$ we have
  $\langle a_0 \,\text{op}\, a_1 , \sigma \rangle \longrightarrow m \nwarrow_{[m = m_0\, op\, m_1]} \langle a_0 , \sigma \rangle \longrightarrow m_0 , \langle a_1 , \sigma \rangle \longrightarrow m_1$

Termination: Inductive Case (cont.)

$$\forall a_0, a_1 .\, P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle a_0 \text{ op } a_1 , \sigma \rangle \longrightarrow m$, where m is the only variable.
- By rule $\dfrac{\langle a_0 , \sigma \rangle \longrightarrow n_0 \quad \langle a_1 , \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1 , \sigma \rangle \longrightarrow n_0 \; op \; n_1}$ we have
  $\langle a_0 \text{ op } a_1 , \sigma \rangle \longrightarrow m \nwarrow_{[m = m_0 \, op \, m_1]} \langle a_0 , \sigma \rangle \longrightarrow m_0 , \langle a_1 , \sigma \rangle \longrightarrow m_1$
- By the inductive hypotheses, there are m_0, m_1 such that $\langle a_0 , \sigma \rangle \longrightarrow m_0$ and $\langle a_1 , \sigma \rangle \longrightarrow m_1$

Termination: Inductive Case (cont.)

$$\forall a_0, a_1 .\, P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \operatorname{op} a_1)$$

- Let $\sigma \in \mathbb{M}$ be some arbitrary memory.
  Consider the goal $\langle a_0 \operatorname{op} a_1 , \sigma \rangle \longrightarrow m$, where m is the only variable.
- By rule $\dfrac{\langle a_0 , \sigma \rangle \longrightarrow n_0 \quad \langle a_1 , \sigma \rangle \longrightarrow n_1}{\langle a_0 \operatorname{op} a_1 , \sigma \rangle \longrightarrow n_0 \; op \; n_1}$ we have
  $\langle a_0 \operatorname{op} a_1 , \sigma \rangle \longrightarrow m \;\nwarrow_{[m = m_0 \, op \, m_1]}\; \langle a_0 , \sigma \rangle \longrightarrow m_0 , \langle a_1 , \sigma \rangle \longrightarrow m_1$
- By the inductive hypotheses, there are m_0, m_1 such that $\langle a_0 , \sigma \rangle \longrightarrow m_0$ and $\langle a_1 , \sigma \rangle \longrightarrow m_1$
- We are done by taking $m = m_0 \; op \; m_1$.

Another Property of AExpressions

Syntax

$$x \in \mathsf{Ide} \qquad n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \mathsf{Ide} \to \mathbb{Z}\} \qquad \mathsf{op} \in \{+, -, \times\}$$

$$a ::= \; x \mid n \mid a \;\mathsf{op}\; a$$

Semantics

$$\frac{}{\langle x \,, \sigma \rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n \,, \sigma \rangle \longrightarrow n} \qquad \frac{\langle a_0 \,, \sigma \rangle \longrightarrow n_0 \quad \langle a_1 \,, \sigma \rangle \longrightarrow n_1}{\langle a_0 \;\mathsf{op}\; a_1 \,, \sigma \rangle \longrightarrow n_0 \; op \; n_1}$$

Another Property of AExpressions

Syntax

$$x \in \mathsf{Ide} \qquad n \in \mathbb{Z} \qquad \mathbb{M} \triangleq \{\sigma \mid \mathsf{Ide} \to \mathbb{Z}\} \qquad \mathsf{op} \in \{+, -, \times\}$$

$$a ::= \; x \mid n \mid a \;\mathsf{op}\; a$$

Semantics

$$\frac{}{\langle x, \sigma\rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma\rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \;\mathsf{op}\; a_1, \sigma\rangle \longrightarrow n_0 \;op\; n_1}$$

Determinacy:

- $P(a) \triangleq \forall \sigma \in \mathbb{M}. \forall m, m' \in \mathbb{Z}. (\langle a, \sigma\rangle \longrightarrow m \wedge \langle a, \sigma\rangle \longrightarrow m') \Rightarrow m = m'.$

Determinacy: Base Case (1 of 2)

$$\forall x \in \mathsf{Ide}.\, P(x)$$

Take some arbitrary identifier $x \in \mathsf{Ide}$. We must prove:

$$P(x) \triangleq \forall \sigma, m, m'.\, \langle x, \sigma \rangle \longrightarrow m \wedge \langle x, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

Consider arbitrary σ, m, m' such that $\langle x, \sigma \rangle \longrightarrow m$ and $\langle x, \sigma \rangle \longrightarrow m'$.
We want to prove $m = m'$.

Determinacy: Base Case (1 of 2)

$$\forall x \in \mathsf{Ide}.\ P(x)$$

Take some arbitrary identifier $x \in \mathsf{Ide}$. We must prove:

$$P(x) \triangleq \forall \sigma, m, m'.\ \langle x, \sigma \rangle \longrightarrow m \wedge \langle x, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

Consider arbitrary σ, m, m' such that $\langle x, \sigma \rangle \longrightarrow m$ and $\langle x, \sigma \rangle \longrightarrow m'$.
We want to prove $m = m'$.

- Consider the goal $\langle x, \sigma \rangle \longrightarrow m$.
  Only the rule $\dfrac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)}$ is applicable, hence $m = \sigma(x)$.
- Similarly, since $\langle x, \sigma \rangle \longrightarrow m'$, it must be that $m' = \sigma(x)$.
- We thus conclude that $m = m'$.

Determinacy: Base Case (2 of 2)

$$\forall n \in \mathbb{Z}.\, P(n)$$

Take some arbitrary $n \in \mathbb{Z}$. We must prove:

$$P(n) \triangleq \forall \sigma, m, m'.\, \langle n, \sigma \rangle \longrightarrow m \wedge \langle n, \sigma \rangle \longrightarrow m' \Rightarrow m = m'$$

Consider arbitrary σ, m, m' such that $\langle n, \sigma \rangle \longrightarrow m$ and $\langle n, \sigma \rangle \longrightarrow m'$.
We want to prove $m = m'$.

- Consider the goal $\langle n, \sigma \rangle \longrightarrow m$.
  Only the rule $\dfrac{}{\langle n, \sigma \rangle \longrightarrow n}$ is applicable, hence $m = n$.
- Similarly, since $\langle n, \sigma \rangle \longrightarrow m'$, it must be that $m' = n$.
- We thus conclude that $m = m'$.

Determinacy: Inductive Case

$$\forall a_0, a_1 .\, P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$$

Take some arbitrary expressions a_0, a_1. We assume (inductive hypotheses, $i \in \{0, 1\}$):

$$P(a_i) \triangleq \forall \sigma, m_i, m_i' .\, \langle a_i, \sigma \rangle \longrightarrow m_i \wedge \langle a_i, \sigma \rangle \longrightarrow m_i' \Rightarrow m_i = m_i'$$

We must prove

$$P(a_0 \,\text{op}\, a_1) \triangleq \forall \sigma, m, m' .\, (\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m \wedge \langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m') \Rightarrow m = m'$$

Consider generic σ, m, m' such that $\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m$ and $\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow m'$. We want to prove $m = m'$.

Inductive Case (cont.)

$$\forall a_0, a_1 .\, P(a_0) \land P(a_1) \Rightarrow P(a_0 \text{ op } a_1)$$

- Consider the goal $\langle a_0 \,\text{op}\, a_1, \sigma\rangle \longrightarrow m$.
  Only the rule $\dfrac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma\rangle \longrightarrow n_0 \; op \; n_1}$ is applicable.
  Hence $m = n_0 \, op \, n_1$ with $\langle a_0, \sigma\rangle \longrightarrow n_0$ and $\langle a_1, \sigma\rangle \longrightarrow n_1$.
- Similarly, since $\langle a_0 \,\text{op}\, a_1, \sigma\rangle \longrightarrow m'$, it must be $m' = n'_0 \, op \, n'_1$ with $\langle a_0, \sigma\rangle \longrightarrow n'_0$ and $\langle a_1, \sigma\rangle \longrightarrow n'_1$.
- By the inductive hypotheses, we have

Inductive Case (cont.)

$$\forall a_0, a_1 .\, P(a_0) \wedge P(a_1) \Rightarrow P(a_0 \,\mathrm{op}\, a_1)$$

- Consider the goal $\langle a_0 \,\mathrm{op}\, a_1, \sigma\rangle \longrightarrow m$.
  Only the rule $\dfrac{\langle a_0, \sigma\rangle \longrightarrow n_0 \quad \langle a_1, \sigma\rangle \longrightarrow n_1}{\langle a_0 \,\mathrm{op}\, a_1, \sigma\rangle \longrightarrow n_0 \,op\, n_1}$ is applicable.
  Hence $m = n_0 \,op\, n_1$ with $\langle a_0, \sigma\rangle \longrightarrow n_0$ and $\langle a_1, \sigma\rangle \longrightarrow n_1$.
- Similarly, since $\langle a_0 \,\mathrm{op}\, a_1, \sigma\rangle \longrightarrow m'$, it must be $m' = n_0' \,op\, n_1'$ with $\langle a_0, \sigma\rangle \longrightarrow n_0'$ and $\langle a_1, \sigma\rangle \longrightarrow n_1'$.
- By the inductive hypotheses, we have both $n_0 = n_0'$ and $n_1 = n_1'$.
- We thus conclude $m = n_0 \,op\, n_1 = n_0' \,op\, n_1' = m'$.

IMP: Big-step Semantics (1 of 2)

$$\frac{}{\langle x, \sigma \rangle \longrightarrow \sigma(x)} \qquad \frac{}{\langle n, \sigma \rangle \longrightarrow n} \qquad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ op } a_1, \sigma \rangle \longrightarrow n_0 \ op \ n_1}$$

$$\frac{}{\langle v, \sigma \rangle \longrightarrow v} \qquad \frac{\langle b, \sigma \rangle \longrightarrow v}{\langle b, \sigma \rangle \longrightarrow \neg v} \qquad \frac{\langle a_0, \sigma \rangle \longrightarrow n_0 \quad \langle a_1, \sigma \rangle \longrightarrow n_1}{\langle a_0 \text{ cmp } a_1, \sigma \rangle \longrightarrow n_0 \ cmp \ n_1}$$

$$\frac{\langle b_0, \sigma \rangle \longrightarrow v_0 \quad \langle b_1, \sigma \rangle \longrightarrow v_1}{\langle b_0 \text{ bop } b_1, \sigma \rangle \longrightarrow v_0 \ bop \ v_1}$$

IMP: Big-step Semantics (2 of 2)

$$\frac{}{\langle \mathbf{skip}, \sigma\rangle \longrightarrow \sigma} \qquad \frac{\langle a, \sigma\rangle \longrightarrow n}{\langle x := a, \sigma\rangle \longrightarrow \sigma[n/x]} \qquad \frac{\langle c_0, \sigma\rangle \longrightarrow \sigma'' \quad \langle c_1, \sigma''\rangle \longrightarrow \sigma'}{\langle c_0; c_1, \sigma\rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathtt{ff} \quad \langle c_1, \sigma\rangle \longrightarrow \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma'} \qquad \frac{\langle b, \sigma\rangle \longrightarrow \mathtt{tt} \quad \langle c_0, \sigma\rangle \longrightarrow \sigma'}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \longrightarrow \sigma'}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathtt{ff}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma}$$

$$\frac{\langle b, \sigma\rangle \longrightarrow \mathtt{tt} \quad \langle c, \sigma\rangle \longrightarrow \sigma'' \quad \langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma''\rangle \longrightarrow \sigma'}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \longrightarrow \sigma'}$$

The End