

# Induction

CS 152 (Spring 2020)

Harvard University

Thursday, February 6, 2020

# Today, we learn to

- ▶ define an inductive set
- ▶ derive the induction principle of an inductive set
- ▶ prove properties of programs by induction
- ▶ use Coq to check your proofs
- ▶ believe in induction!

# Expressing Program Properties

# Progress

$\forall e \in \mathbf{Exp}. \forall \sigma \in \mathbf{Store}.$

either  $e \in \mathbf{Int}$  or  $\exists e', \sigma'. \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$

# Termination

$\forall e \in \mathbf{Exp}. \forall \sigma_0 \in \mathbf{Store}. \exists \sigma \in \mathbf{Store}. \exists n \in \mathbf{Int}.$   
 $\langle e, \sigma_0 \rangle \longrightarrow^* \langle n, \sigma \rangle$

# Deterministic Result

$\forall e \in \mathbf{Exp}. \forall \sigma_0, \sigma, \sigma' \in \mathbf{Store}. \forall n, n' \in \mathbf{Int}.$   
if  $\langle e, \sigma_0 \rangle \longrightarrow^* \langle n, \sigma \rangle$  and  
 $\langle e, \sigma_0 \rangle \longrightarrow^* \langle n', \sigma' \rangle$  then  
 $n = n'$  and  $\sigma = \sigma'$ .

# Inductive Sets

# Inductive Set: Definition

Axiom:

$$\frac{}{a \in A}$$

Inductive Rule:

$$\frac{a_1 \in A \quad \dots \quad a_n \in A}{a \in A}$$



# Grammar for **Exp**

$$e ::= x \mid n \mid e_1 + e_2 \mid e_1 \times e_2 \mid x := e_1; e_2$$

# Inductive Set **Exp**

$$\text{VAR} \frac{}{x \in \mathbf{Exp}} x \in \mathbf{Var}$$

$$\text{INT} \frac{}{n \in \mathbf{Exp}} n \in \mathbf{Int}$$

$$\text{ADD} \frac{e_1 \in \mathbf{Exp} \quad e_2 \in \mathbf{Exp}}{e_1 + e_2 \in \mathbf{Exp}}$$

$$\text{MUL} \frac{e_1 \in \mathbf{Exp} \quad e_2 \in \mathbf{Exp}}{e_1 \times e_2 \in \mathbf{Exp}}$$

$$\text{ASG} \frac{e_1 \in \mathbf{Exp} \quad e_2 \in \mathbf{Exp}}{x := e_1; e_2 \in \mathbf{Exp}} x \in \mathbf{Var}$$

# Grammar Equivalent to Inductive Set

$$e ::= x \mid n \mid e_1 + e_2 \mid e_1 \times e_2 \mid x := e_1; e_2$$
$$\text{VAR} \frac{}{x \in \mathbf{Exp}} x \in \mathbf{Var} \qquad \text{INT} \frac{}{n \in \mathbf{Exp}} n \in \mathbf{Int}$$
$$\text{ADD} \frac{e_1 \in \mathbf{Exp} \quad e_2 \in \mathbf{Exp}}{e_1 + e_2 \in \mathbf{Exp}}$$
$$\text{MUL} \frac{e_1 \in \mathbf{Exp} \quad e_2 \in \mathbf{Exp}}{e_1 \times e_2 \in \mathbf{Exp}}$$
$$\text{ASG} \frac{e_1 \in \mathbf{Exp} \quad e_2 \in \mathbf{Exp}}{x := e_1; e_2 \in \mathbf{Exp}} x \in \mathbf{Var}$$

# Inductive Set **Exp**: Example Derivation

$$\text{MUL} \frac{\text{ADD} \frac{\text{VAR} \frac{}{\text{foo} \in \mathbf{Exp}} \quad \text{INT} \frac{}{3 \in \mathbf{Exp}}}{(\text{foo} + 3) \in \mathbf{Exp}} \quad \text{VAR} \frac{}{\text{bar} \in \mathbf{Exp}}}{(\text{foo} + 3) \times \text{bar} \in \mathbf{Exp}}$$

# Inductive Set $\mathbb{N}$ (Natural Numbers)

The natural numbers can be inductively defined:

$$\frac{}{0 \in \mathbb{N}} \quad \frac{n \in \mathbb{N}}{\text{succ}(n) \in \mathbb{N}}$$

where  $\text{succ}(n)$  is the successor of  $n$ .

# Inductive Set $\longrightarrow$ (Step Relation)

The small-step evaluation relation  $\longrightarrow$  is an inductively defined set. The definition of this set is given by the semantic rules.

# Inductive Set $\longrightarrow^*$ (Multi-Step Rel.)

$$\overline{\langle e, \sigma \rangle \longrightarrow^* \langle e, \sigma \rangle}$$

$$\frac{\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle \quad \langle e', \sigma' \rangle \longrightarrow^* \langle e'', \sigma'' \rangle}{\langle e, \sigma \rangle \longrightarrow^* \langle e'', \sigma'' \rangle}$$

# Inductive proofs



# Mathematical induction

# Mathematical induction

For any property  $P$ ,

**If**

- ▶  $P(0)$  holds
- ▶ For all natural numbers  $n$ , if  $P(n)$  holds then  $P(n + 1)$  holds

**then** for all natural numbers  $k$ ,  $P(k)$  holds.

# Mathematical induction

$$\frac{}{0 \in \mathbb{N}} \quad \frac{n \in \mathbb{N}}{\text{succ}(n) \in \mathbb{N}}$$

For any property  $P$ ,

**If**

- ▶  $P(0)$  holds
- ▶ For all natural numbers  $n$ , if  $P(n)$  holds then  $P(n + 1)$  holds

**then** for all natural numbers  $k$ ,  $P(k)$  holds.

# Induction on inductively-defined sets

# Induction on inductively-defined sets

For any property  $P$ ,

**If**

- ▶ **Base cases:** For each axiom

$$\frac{}{a \in A},$$

$P(a)$  holds.

- ▶ **Inductive cases:** For each inference rule

$$\frac{a_1 \in A \quad \dots \quad a_n \in A}{a \in A},$$

if  $P(a_1)$  and  $\dots$  and  $P(a_n)$  then  $P(a)$ .

**then** for all  $a \in A$ ,  $P(a)$  holds.

# Inductive reasoning principle for set **Exp**

For any property  $P$ ,

**If**

- ▶ For all variables  $x$ ,  $P(x)$  holds.
- ▶ For all integers  $n$ ,  $P(n)$  holds.
- ▶ For all  $e_1 \in \mathbf{Exp}$  and  $e_2 \in \mathbf{Exp}$ , if  $P(e_1)$  and  $P(e_2)$  then  $P(e_1 + e_2)$  holds.
- ▶ For all  $e_1 \in \mathbf{Exp}$  and  $e_2 \in \mathbf{Exp}$ , if  $P(e_1)$  and  $P(e_2)$  then  $P(e_1 \times e_2)$  holds.
- ▶ For all variables  $x$  and  $e_1 \in \mathbf{Exp}$  and  $e_2 \in \mathbf{Exp}$ , if  $P(e_1)$  and  $P(e_2)$  then  $P(x := e_1; e_2)$  holds.

**then** for all  $e \in \mathbf{Exp}$ ,  $P(e)$  holds.

# Case INT

$$\text{INT} \frac{\quad}{n \in \mathbf{Exp}} n \in \mathbf{Int}$$

For all integers  $n$ ,  
 $P(n)$  holds

## Case ADD

$$\text{ADD} \frac{e_1 \in \mathbf{Exp} \quad e_2 \in \mathbf{Exp}}{e_1 + e_2 \in \mathbf{Exp}}$$

For all  $e_1 \in \mathbf{Exp}$  and  $e_2 \in \mathbf{Exp}$ ,  
if  $P(e_1)$  and  $P(e_2)$   
then  $P(e_1 + e_2)$  holds.



# Inductive reasoning principle for set $\longrightarrow$

For any property  $P$ , **If**

- ▶ **VAR**: For all variables  $x$ , stores  $\sigma$  and integers  $n$  such that  $\sigma(x) = n$ ,  $P(\langle x, \sigma \rangle \longrightarrow \langle n, \sigma \rangle)$  holds.
- ▶ **ADD**: For all integers  $n, m, p$  such that  $p = n + m$ , and stores  $\sigma$ ,  $P(\langle n + m, \sigma \rangle \longrightarrow \langle p, \sigma \rangle)$  holds.
- ▶ **MUL**: For all integers  $n, m, p$  such that  $p = n \times m$ , and stores  $\sigma$ ,  $P(\langle n \times m, \sigma \rangle \longrightarrow \langle p, \sigma \rangle)$  holds.
- ▶ **ASG**: For all variables  $x$ , integers  $n$  and expressions  $e \in \mathbf{Exp}$ ,  $P(\langle x := n; e, \sigma \rangle \longrightarrow \langle e, \sigma[x \mapsto n] \rangle)$  holds.
- ▶ **LADD**: For all expressions  $e_1, e_2, e'_1 \in \mathbf{Exp}$  and stores  $\sigma$  and  $\sigma'$ , if  $P(\langle e_1, \sigma \rangle \longrightarrow \langle e'_1, \sigma' \rangle)$  holds then  $P(\langle e_1 + e_2, \sigma \rangle \longrightarrow \langle e'_1 + e_2, \sigma' \rangle)$  holds.
- ▶ **RADD**: For all integers  $n$ , expressions  $e_2, e'_2 \in \mathbf{Exp}$  and stores  $\sigma$  and  $\sigma'$ , if  $P(\langle e_2, \sigma \rangle \longrightarrow \langle e'_2, \sigma' \rangle)$  holds then  $P(\langle n + e_2, \sigma \rangle \longrightarrow \langle n + e'_2, \sigma' \rangle)$  holds.
- ▶ **LMUL**: For all expressions  $e_1, e_2, e'_1 \in \mathbf{Exp}$  and stores  $\sigma$  and  $\sigma'$ , if  $P(\langle e_1, \sigma \rangle \longrightarrow \langle e'_1, \sigma' \rangle)$  holds then  $P(\langle e_1 \times e_2, \sigma \rangle \longrightarrow \langle e'_1 \times e_2, \sigma' \rangle)$  holds.
- ▶ **RMUL**: For all integers  $n$ , expressions  $e_2, e'_2 \in \mathbf{Exp}$  and stores  $\sigma$  and  $\sigma'$ , if  $P(\langle e_2, \sigma \rangle \longrightarrow \langle e'_2, \sigma' \rangle)$  holds then  $P(\langle n \times e_2, \sigma \rangle \longrightarrow \langle n \times e'_2, \sigma' \rangle)$  holds.
- ▶ **ASG1**: For all variables  $x$ , expressions  $e_1, e_2, e'_1 \in \mathbf{Exp}$  and stores  $\sigma$  and  $\sigma'$ , if  $P(\langle e_1, \sigma \rangle \longrightarrow \langle e'_1, \sigma' \rangle)$  holds then  $P(\langle x := e_1; e_2, \sigma \rangle \longrightarrow \langle x := e'_1; e_2, \sigma' \rangle)$  holds.

**then** for all  $\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$ ,  
 $P(\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle)$  holds.

# Proving progress

# Progress (Statement)

**Progress:** For each store  $\sigma$  and expression  $e$  that is not an integer, there exists a possible transition for  $\langle e, \sigma \rangle$ :

$$\forall e \in \mathbf{Exp}. \forall \sigma \in \mathbf{Store}.$$

either  $e \in \mathbf{Int}$  or  $\exists e', \sigma'. \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$

# Progress (Rephrased)

$$P(e) = \forall \sigma. (e \in \mathbf{Int}) \vee (\exists e', \sigma'. \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle)$$

# Progress (Rephrased)

$\forall e \in \mathbf{Exp}. \forall \sigma \in \mathbf{Store}.$

either  $e \in \mathbf{Int}$  or  $\exists e', \sigma'. \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$

$$P(e) = \forall \sigma. (e \in \mathbf{Int}) \vee (\exists e', \sigma'. \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle)$$

## Example: Proving progress

by “structural induction on the expressions  $e$ ”

We will prove by structural induction on expressions **Exp** that for all expressions  $e \in \mathbf{Exp}$  we have

$$P(e) = \forall \sigma. (e \in \mathbf{Int}) \vee (\exists e', \sigma'. \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle).$$

Consider the possible cases for  $e$ .

## Proving progress: Case $e = x$

By the VAR axiom, we can evaluate  $\langle x, \sigma \rangle$  in any state:  $\langle x, \sigma \rangle \longrightarrow \langle n, \sigma \rangle$ , where  $n = \sigma(x)$ . So  $e' = n$  is a witness that there exists  $e'$  such that  $\langle x, \sigma \rangle \longrightarrow \langle e', \sigma \rangle$ , and  $P(x)$  holds.

## Proving progress: Case $e = x$

$$\text{VAR} \frac{}{\langle x, \sigma \rangle \longrightarrow \langle n, \sigma \rangle} \text{ where } n = \sigma(x)$$

By the VAR axiom, we can evaluate  $\langle x, \sigma \rangle$  in any state:  $\langle x, \sigma \rangle \longrightarrow \langle n, \sigma \rangle$ , where  $n = \sigma(x)$ . So  $e' = n$  is a witness that there exists  $e'$  such that  $\langle x, \sigma \rangle \longrightarrow \langle e', \sigma \rangle$ , and  $P(x)$  holds.



Proving progress: Case  $e = n$

Then  $e \in \mathbf{Int}$ , so  $P(n)$  trivially holds.

## Proving progress: Case $e = e_1 + e_2$

This is an inductive step. The inductive hypothesis is that  $P$  holds for subexpressions  $e_1$  and  $e_2$ . We need to show that  $P$  holds for  $e$ . In other words, we want to show that  $P(e_1)$  and  $P(e_2)$  implies  $P(e)$ . Let's expand these properties. We know that the following hold:

$$P(e_1) = \forall \sigma. (e_1 \in \mathbf{Int}) \vee (\exists e', \sigma'. \langle e_1, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle)$$

$$P(e_2) = \forall \sigma. (e_2 \in \mathbf{Int}) \vee (\exists e', \sigma'. \langle e_2, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle)$$

and we want to show:

$$P(e) = \forall \sigma. (e \in \mathbf{Int}) \vee (\exists e', \sigma'. \langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle)$$

We must inspect several subcases.

## Proving progress: Case $e = e_1 + e_2$ , $e_1, e_2 \in \mathbf{Int}$

First, if both  $e_1$  and  $e_2$  are integer constants, say  $e_1 = n_1$  and  $e_2 = n_2$ , then by rule **ADD** we know that the transition  $\langle n_1 + n_2, \sigma \rangle \longrightarrow \langle n, \sigma \rangle$  is valid, where  $n$  is the sum of  $n_1$  and  $n_2$ . Hence,  $P(e) = P(n_1 + n_2)$  holds (with witness  $e' = n$ ).

## Proving progress: Case $e = e_1 + e_2$ , $e_1 \notin \text{Int}$

Second, if  $e_1$  is not an integer constant, then by the inductive hypothesis  $P(e_1)$  we know that  $\langle e_1, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$  for some  $e'$  and  $\sigma'$ . We can then use rule LADD to conclude  $\langle e_1 + e_2, \sigma \rangle \longrightarrow \langle e' + e_2, \sigma' \rangle$ , so  $P(e) = P(e_1 + e_2)$  holds.

Proving progress: Case  $e = e_1 + e_2$ ,  
 $e_1 \in \mathbf{Int}$ ,  $e_2 \notin \mathbf{Int}$

Third, if  $e_1$  is an integer constant, say  $e_1 = n_1$ , but  $e_2$  is not, then by the inductive hypothesis  $P(e_2)$  we know that  $\langle e_2, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$  for some  $e'$  and  $\sigma'$ . We can then use rule  $\mathbf{R}_{\text{ADD}}$  to conclude  $\langle n_1 + e_2, \sigma \rangle \longrightarrow \langle n_1 + e', \sigma' \rangle$ , so  $P(e) = P(n_1 + e_2)$  holds.

## Proving progress: Remaining cases

Case  $e = e_1 \times e_2$  and case  $e = x := e_1; e_2$ . These are also inductive cases, and their proofs are similar to the previous case. [Note that if you were writing this proof out for a homework, you should write these cases out in full.]

# Incremental update

For all expressions  $e$  and stores  $\sigma$ , if  
 $\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$  then  
either  $\sigma = \sigma'$  or  
there is some variable  $x$  and integer  $n$  such that  
 $\sigma' = \sigma[x \mapsto n]$ .

# Proving incremental update

We proceed by induction on the derivation of  $\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$ . Suppose we have  $e, \sigma, e'$  and  $\sigma'$  such that  $\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$ . The property  $P$  that we will prove of  $e, \sigma, e'$  and  $\sigma'$ , which we will write as  $P(\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle)$ , is that either  $\sigma = \sigma'$  or there is some variable  $x$  and integer  $n$  such that  $\sigma' = \sigma[x \mapsto n]$ :

$$P(\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle) \triangleq \\ \sigma = \sigma' \vee (\exists x \in \mathbf{Var}, n \in \mathbf{Int}. \sigma' = \sigma[x \mapsto n]).$$

Consider the cases for the derivation of  $\langle e, \sigma \rangle \longrightarrow \langle e', \sigma' \rangle$ .



## Proving incremental update: Case ADD

This is an axiom. Here,  $e \equiv n + m$  and  $e' = p$  where  $p$  is the sum of  $m$  and  $n$ , and  $\sigma' = \sigma$ . The result holds immediately.

# Proving incremental update: Case LADD

This is an inductive case. Here,  $e \equiv e_1 + e_2$  and  $e' \equiv e'_1 + e_2$  and  $\langle e_1, \sigma \rangle \longrightarrow \langle e'_1, \sigma' \rangle$ . By the inductive hypothesis, applied to  $\langle e_1, \sigma \rangle \longrightarrow \langle e'_1, \sigma' \rangle$ , we have that either  $\sigma = \sigma'$  or there is some variable  $x$  and integer  $n$  such that  $\sigma' = \sigma[x \mapsto n]$ , as required.

## Proving incremental update: Case ASG

This is an axiom. Here  $e \equiv x := n; e_2$  and  $e' \equiv e_2$  and  $\sigma' = \sigma[x \mapsto n]$ . The result holds immediately.

# Proving incremental update: remaining cases

We leave the other cases (VAR, RADD, LMUL, RMUL, MUL, and ASG1) as exercises. Seriously, try them. Make sure you can do them. Go on.

Interlude: What if induction weren't true?

# Peano Axioms

$$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow \dots$$

1. zero is a number.
2. If  $a$  is a number, the successor of  $a$  is a number.
3. zero is not the successor of a number.
4. Two numbers of which the successors are equal are themselves equal.
5. (induction axiom.) If a set  $S$  of numbers contains zero and also the successor of every number in  $S$ , then every number is in  $S$ .

# Monster Chains

$$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow \dots$$

$$\dots \rightarrow -a_1 \rightarrow a_0 \rightarrow a_1 \rightarrow a_2' \rightarrow a_3' \rightarrow \dots$$

$$\dots \rightarrow -b_1 \rightarrow b_0 \rightarrow b_1' \rightarrow b_2' \rightarrow b_3' \rightarrow \dots$$