Fixed-point Induction

CS 6371: Advanced Programming Languages

Kevin W. Hamlen

February 15, 2024

Structural Induction

- Induction over $\mathbb{N}$:
  - Weak induction (over $\mathbb{N}$):
    1. Prove that $P(0)$ holds (called the **base case**).
    2. For arbitrary $n \geq 1$, prove $P(n-1) \Rightarrow P(n)$. (Assumption $P(n-1)$ called the **(weak) inductive hypothesis (IH)**.)
  - Strong induction (over $\mathbb{N}$):

    For arbitrary $n \in \mathbb{N}$, prove $(\forall n_0 < n, P(n_0)) \Rightarrow P(n)$. (Assumption $\forall n_0 < n, P(n_0)$ called the **(strong) IH**).
- Structural Induction
  1. Base case(s): Prove that $P(\mathcal{D})$ holds for "minimal" structure(s) $\mathcal{D}$.
  2. Inductive case(s): Assume (IH) that $P(\mathcal{D}_0)$ holds for all structures $\mathcal{D}_0$ "smaller than" $\mathcal{D}$, and prove $P(\mathcal{D})$.
- These are all actually special cases of a much more general inductive principle called **fixed-point induction**.

Fixed-point Induction

To prove that a **recursively defined function** $f : A \rightharpoonup A$ satisfies a property P:

1. Define a non-recursive *functional* $F : (A \rightharpoonup A) \to (A \rightharpoonup A)$ such that $\mathit{fix}(F) = f$.
2. **Base Case:** Prove $P(\bot_A)$.
3. **Inductive Case:** Assume $P(g)$ holds for some *arbitrary* function $g : A \rightharpoonup A$ (IH), and prove that this implies $P(F(g))$.

Lecture Outline:

- Do an example fixed-point induction proof for a simple f.
- Show how the same technique can be used to prove things about loops.
- Big picture: how this approach generalizes structural induction and motivates denotational semantics

First Example Proof

Theorem (recursive factorial definition correctness):

Define $f : \mathbb{Z} \rightharpoonup \mathbb{Z}$ as follows:

$$f(x) = (x{=}0 \rightarrow 1 \mid x{>}0 \rightarrow x f(x-1))$$

For all $x \in \mathbb{Z}$, $f(x)$ is either undefined or equals $x!$.

(Turns out $f(x)$ is defined for all $x \geq 0$, but we won't prove that here.)

Defining a Non-recursive Functional

Theorem (recursive factorial definition correctness):

Define $f : \mathbb{Z} \rightharpoonup \mathbb{Z}$ as follows:

$$f(x) = (x{=}0 \rightarrow 1 \mid x{>}0 \rightarrow xf(x-1))$$

For all $x \in \mathbb{Z}$, $f(x)$ is either undefined or equals $x!$.

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \rightarrow (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \rightarrow 1 \mid x{>}0 \rightarrow xg(x-1))$$

Notation $\lambda v, \ldots$ means “function that accepts v as input and returns …”.

Functional F’s definition must be a **verbatim copy** of f, but with all recursive calls to f replaced with calls of new parameter g.

Least Fixed Point of Functional

Theorem (recursive factorial definition correctness):

Define $f : \mathbb{Z} \rightharpoonup \mathbb{Z}$ as follows:

$$f(x) = (x{=}0 \to 1 \mid x{>}0 \to x f(x-1))$$

For all $x \in \mathbb{Z}$, $f(x)$ is either undefined or equals $x!$.

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to x g(x-1))$$

By construction, $\mathit{fix}(F) = f$.

Q: How do we know this?

A: This is actually the mathematical definition of recursion! When we write a recursive function in math class, we're actually referring to the least fixed point of the functional defined in this way.

Setting up the Induction

Theorem (recursive factorial definition correctness):

Define $f : \mathbb{Z} \rightharpoonup \mathbb{Z}$ as follows:

$$f(x) = (x{=}0 \to 1 \mid x{>}0 \to x f(x-1))$$

For all $x \in \mathbb{Z}$, $f(x)$ is either undefined or equals $x!$.

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to x g(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Remember, always tell me:

- what kind of induction (fixed-point in this case).
- what the induction is over (functional F in this case).

Base Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: ?

(We need to prove $P(\perp_{\mathbb{Z}})$ here.)

Base Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot_{\mathbb{Z}})$ holds vacuously.

Look at the defintion of P. Property $P(\bot)$ asserts that something is true of all members of $\bot^{\leftarrow}$, but $\bot^{\leftarrow}$ is the empty set. So $\bot$ trivially ("vacuously") satisfies this P.

Base case almost always vacuously true, but not guaranteed so always check P.

Inductive Hypothesis

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Don't invent a different IH! In a fixed-point induction, IH is always exactly $P(g)$, and g must be **arbitrary** (not f, not F, has no relation to them).

Strongly recommended that you **write out** definition of $P(g)$. Otherwise I must guess whether you really know what the IH is (which can come into doubt if your proof has flaws).

Inductive Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Inductive Case: ?

We must prove $P(F(g))$ here. What does $P(F(g))$ say?

Inductive Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to x g(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Inductive Case: Let $x \in F(g)^{\leftarrow}$ be given. ...

$P(F(g)) \equiv \forall x \in F(g)^{\leftarrow}, F(g)(x) = x!$, so we must prove $F(g)(x) = x!$ now. What is $F(g)(x)$?

Inductive Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Inductive Case: Let $x \in F(g)^{\leftarrow}$ be given.

Case 1: Assume $x = 0$. ...
Case 2: Assume $x > 0$. ...

$P(F(g)) \equiv \forall x \in F(g)^{\leftarrow}, F(g)(x) = x!$, so we must prove $F(g)(x) = x!$ now.
Definition of $F(g)(x)$ has two cases, so let's take one at a time...

Inductive Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to x g(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Inductive Case: Let $x \in F(g)^{\leftarrow}$ be given.

Case 1: If $x = 0$ then $F(g)(x) = 1$ by definition of F. ...
Case 2: Assume $x > 0$. ...

$P(F(g)) \equiv \forall x \in F(g)^{\leftarrow}, F(g)(x) = x!$, so we must prove $F(g)(x) = x!$ now.
Definition of $F(g)(x)$ has two cases, so let's take one at a time...

Inductive Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Inductive Case: Let $x \in F(g)^{\leftarrow}$ be given.

Case 1: If $x = 0$ then $F(g)(x) = 1$ by definition of F. And $0! = 1$.
Case 2: Assume $x > 0$. ...

$P(F(g)) \equiv \forall x \in F(g)^{\leftarrow}, F(g)(x) = x!$, so we must prove $F(g)(x) = x!$ now.
Definition of $F(g)(x)$ has two cases, so let's take one at a time...

Inductive Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Inductive Case: Let $x \in F(g)^{\leftarrow}$ be given.

Case 1: If $x = 0$ then $F(g)(x) = 1$ by definition of F. And $0! = 1$.
Case 2: If $x > 0$ then $F(g)(x) = xg(x-1)$ by definition of F. ...

Need to prove $xg(x-1) = x!$. How?
Remember, g is a **completely arbitrary** function. May not assume it's f (circular reasoning)!

Inductive Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\perp)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Inductive Case: Let $x \in F(g)^{\leftarrow}$ be given.

Case 1: If $x = 0$ then $F(g)(x) = 1$ by definition of F. And $0! = 1$.
Case 2: If $x > 0$ then $F(g)(x) = xg(x-1)$ by definition of F. By IH (with $x_0 = x - 1$), $g(x-1) = (x-1)!$.

Inductive Case

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = x!$. We wish to prove $P(f)$.
Define functional $F : (\mathbb{Z} \rightharpoonup \mathbb{Z}) \to (\mathbb{Z} \rightharpoonup \mathbb{Z})$ as follows:

$$F(g) = \lambda x, (x{=}0 \to 1 \mid x{>}0 \to xg(x-1))$$

By construction, $\mathit{fix}(F) = f$. To prove $P(f)$, we will prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \mathbb{Z} \rightharpoonup \mathbb{Z}$ be an arbitrary function satisfying $P(g)$. That is, assume $\forall x_0 \in g^{\leftarrow}, g(x_0) = x_0!$.

Inductive Case: Let $x \in F(g)^{\leftarrow}$ be given.

Case 1: If $x = 0$ then $F(g)(x) = 1$ by definition of F. And $0! = 1$.
Case 2: If $x > 0$ then $F(g)(x) = xg(x-1)$ by definition of F. By IH (with $x_0 = x - 1$), $g(x-1) = (x-1)!$. Therefore, $F(g)(x) = x(x-1)! = x!$.

Note: At no point did we say anything like, “Function f keeps multiplying consecutive integers until it eventually reaches x.” That’s not a proof.

If you find yourself using the word “eventually” (or synonyms), you’ve abandoned the induction and are appealing to intuition instead of math.

Proof for a Looping Program

Now let's apply the same strategy to prove something about a program that loops:

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program `while 2 <= x do (y := y * x ; x := x - 1)` and property P is defined by
$P(f) \equiv \forall(\sigma, \sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \wedge \sigma(\mathtt{y}) = 1) \implies \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Setting up the Induction

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program `while` 2 `<=` `x` `do` $($`y := y * x ; x := x - `$1)$ and property P is defined by $P(f) \equiv \forall(\sigma,\sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \wedge \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) &= \{(\sigma,\sigma) \mid (\sigma,F) \in \mathcal{B}[\![2 \,\texttt{<=}\, \mathtt{x}]\!]\} \cup \\ &\qquad \{(\sigma, f(\mathcal{C}[\![\mathtt{y := y * x ; x := x -} 1]\!]\sigma)) \mid (\sigma,T) \in \mathcal{B}[\![2 \,\texttt{<=}\, \mathtt{x}]\!]\} \\ &= \{(\sigma,\sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ &\qquad \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Must expand (very carefully!) the definition of Γ for this c. Write it out!

Base Case

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program `while` 2 `<=` `x` `do` $($`y := y * x; x := x - 1`$)$ and property P is defined by $P(f) \equiv \forall(\sigma,\sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \wedge \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) &= \{(\sigma,\sigma) \mid (\sigma,F) \in \mathcal{B}[\![2 \mathtt{<=} \mathtt{x}]\!]\} \cup \\ &\quad\ \{(\sigma, f(\mathcal{C}[\![\mathtt{y := y * x; x := x - 1}]\!]\sigma)) \mid (\sigma,T) \in \mathcal{B}[\![2 \mathtt{<=} \mathtt{x}]\!]\} \\ &= \{(\sigma,\sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ &\quad\ \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: ?

Must prove $P(\bot)$.

Base Case

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program `while 2<=x do (y:=y*x;x:=x-1)` and property P is defined by $P(f) \equiv \forall(\sigma,\sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \wedge \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) &= \{(\sigma,\sigma) \mid (\sigma, F) \in \mathcal{B}[\![\mathtt{2 <= x}]\!]\} \cup \\ &\qquad \{(\sigma, f(\mathcal{C}[\![\mathtt{y := y * x ; x := x - 1}]\!]\sigma)) \mid (\sigma, T) \in \mathcal{B}[\![\mathtt{2 <= x}]\!]\} \\ &= \{(\sigma,\sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ &\qquad \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P(\perp)$ holds vacuously.

Base Case

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program
$\texttt{while}\ 2\,\texttt{<=}\,\texttt{x}\ \texttt{do}\ (\texttt{y}:=\texttt{y}*\texttt{x};\texttt{x}:=\texttt{x}-1)$ and property P is defined by
$P(f) \equiv \forall(\sigma,\sigma') \in f, \big((\sigma(\texttt{x}) \geq 1 \wedge \sigma(\texttt{y}) = 1) \implies \sigma'(\texttt{y}) = \sigma(\texttt{x})!\big)$.

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = {} & \{(\sigma,\sigma) \mid (\sigma,F) \in \mathcal{B}[\![2\,\texttt{<=}\,\texttt{x}]\!]\} \cup \\ & \{(\sigma, f(\mathcal{C}[\![\texttt{y}:=\texttt{y}*\texttt{x};\texttt{x}:=\texttt{x}-1]\!]\sigma)) \mid (\sigma,T) \in \mathcal{B}[\![2\,\texttt{<=}\,\texttt{x}]\!]\} \\ = {} & \{(\sigma,\sigma) \mid 2 > \sigma(\texttt{x})\} \cup \\ & \{(\sigma, f(\sigma[\texttt{y} \mapsto \sigma(\texttt{y})\sigma(\texttt{x})][\texttt{x} \mapsto \sigma(\texttt{x}) - 1])) \mid 2 \leq \sigma(\texttt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume
$\forall(\sigma_0,\sigma_0') \in g, \big((\sigma_0(\texttt{x}) \geq 1 \wedge \sigma_0(\texttt{y}) = 1) \implies \sigma_0'(\texttt{y}) = \sigma_0(\texttt{x})!\big)$.

Inductive Case

Theorem

... where $P(f) \equiv \forall(\sigma,\sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \wedge \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{&(\sigma,\sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ &\{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0,\sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \geq 1 \wedge \sigma_0(\mathtt{y}) = 1) \Longrightarrow \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: ?

We must prove $P(\Gamma(g))$ now. What does it say?

Inductive Case

Theorem

… where $P(f) \equiv \forall(\sigma, \sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \land \sigma(\mathtt{y}) = 1) \implies \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = {} & \{(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ & \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \geq 1 \land \sigma_0(\mathtt{y}) = 1) \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: ?

We must prove $P(\Gamma(g))$ now, which says $\forall(\sigma, \sigma') \in \Gamma(g), \ldots$

Inductive Case

Theorem

… where $P(f) \equiv \forall(\sigma, \sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \land \sigma(\mathtt{y}) = 1) \implies \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = {} & \{(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ & \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \geq 1 \land \sigma_0(\mathtt{y}) = 1) \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given.

We must now prove $(\sigma(\mathtt{x}) \geq 1 \land \sigma(\mathtt{y}) = 1) \implies \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!$.

Inductive Case

Theorem

… where $P(f) \equiv \forall(\sigma, \sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \wedge \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = {} & \{(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ & \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P(\perp)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \geq 1 \wedge \sigma_0(\mathtt{y}) = 1) \Longrightarrow \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ and $\sigma(\mathtt{y}) = 1$.

Goal: Must now prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{x})!$.

(Hint: Use assumption $(\sigma, \sigma') \in \Gamma(g)$ first.)

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \geq 1 \land \sigma_0(\mathtt{y}) = 1) \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ and $\sigma(\mathtt{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathtt{x})$. ...

Case 2: Assume $2 \leq \sigma(\mathtt{x})$. ...

Goal: Must prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{x})!$.

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{&(\sigma,\sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ &\{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \geq 1 \land \sigma_0(\mathtt{y}) = 1) \Longrightarrow \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ and $\sigma(\mathtt{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. ...

Case 2: Assume $2 \leq \sigma(\mathtt{x})$. ...

Goal: Must prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{x})!$.

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = {} & \{(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ & \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \geq 1 \wedge \sigma_0(\mathtt{y}) = 1) \Longrightarrow \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ and $\sigma(\mathtt{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathtt{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathtt{x}) = 1$. ...

Case 2: Assume $2 \leq \sigma(\mathtt{x})$. ...

Goal: Must prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{x})!$.

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = {} & \{(\sigma, \sigma) \mid 2 > \sigma(\mathrm{x})\} \cup \\ & \{(\sigma, f(\sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1])) \mid 2 \leq \sigma(\mathrm{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathrm{x}) \geq 1 \wedge \sigma_0(\mathrm{y}) = 1) \Longrightarrow \sigma_0'(\mathrm{y}) = \sigma_0(\mathrm{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathrm{x}) \geq 1$ and $\sigma(\mathrm{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathrm{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathrm{x}) = 1$. Thus, $\sigma'(\mathrm{y}) = \sigma(\mathrm{y}) = 1 = 1! = \sigma(\mathrm{x})!$.

Case 2: Assume $2 \leq \sigma(\mathrm{x})$. ...

Goal: Must prove $\sigma'(\mathrm{y}) = \sigma(\mathrm{x})!$.

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{(\sigma,\sigma) \mid 2 > \sigma(\mathrm{x})\} \cup \\ \{(\sigma, f(\sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1])) \mid 2 \leq \sigma(\mathrm{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathrm{x}) \geq 1 \land \sigma_0(\mathrm{y}) = 1) \Longrightarrow \sigma_0'(\mathrm{y}) = \sigma_0(\mathrm{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathrm{x}) \geq 1$ and $\sigma(\mathrm{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathrm{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathrm{x}) = 1$. Thus, $\sigma'(\mathrm{y}) = \sigma(\mathrm{y}) = 1 = 1! = \sigma(\mathrm{x})!$.

Case 2: Assume $2 \leq \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1]$. ...

Goal: Must prove $\sigma'(\mathrm{y}) = \sigma(\mathrm{x})!$.

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{(\sigma,\sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \le \sigma(\mathtt{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \ge 1 \wedge \sigma_0(\mathtt{y}) = 1) \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \ge 1$ and $\sigma(\mathtt{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \le \sigma(\mathtt{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathtt{x}) = 1$. Thus, $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) = 1 = 1! = \sigma(\mathtt{x})!$.

Case 2: Assume $2 \le \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$. ...

Goal: Must prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{x})!$.

Saying $\sigma' = g(\sigma_2)$ is the same as saying $(\sigma_2, \sigma') \in g$. (Recall: Partial functions are sets of input-output pairs.)

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{&(\sigma,\sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ &\{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \le \sigma(\mathtt{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathtt{x}) \ge 1 \wedge \sigma_0(\mathtt{y}) = 1) \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \ge 1$ and $\sigma(\mathtt{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \le \sigma(\mathtt{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathtt{x}) = 1$. Thus, $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) = 1 = 1! = \sigma(\mathtt{x})!$.

Case 2: Assume $2 \le \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$.

- $\sigma_2(\mathtt{x}) \ge 1$ because ...?
- $\sigma_2(\mathtt{y}) = 1$ because ...?

Goal: Must prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{x})!$.

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{(\sigma, \sigma) \mid 2 > \sigma(\mathrm{x})\} \cup \\ \{(\sigma, f(\sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1])) \mid 2 \leq \sigma(\mathrm{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma'_0) \in g, \big((\sigma_0(\mathrm{x}) \geq 1 \land \sigma_0(\mathrm{y}) = 1) \Longrightarrow \sigma'_0(\mathrm{y}) = \sigma_0(\mathrm{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathrm{x}) \geq 1$ and $\sigma(\mathrm{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathrm{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathrm{x}) = 1$. Thus, $\sigma'(\mathrm{y}) = \sigma(\mathrm{y}) = 1 = 1! = \sigma(\mathrm{x})!$.

Case 2: Assume $2 \leq \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma'_0 = \sigma'$.

- $\sigma_2(\mathrm{x}) \geq 1$ because $\sigma_2(\mathrm{x}) = \sigma(\mathrm{x}) - 1$ and $\sigma(\mathrm{x}) \geq 2$.
- $\sigma_2(\mathrm{y}) = 1$ because ...?

Goal: Must prove $\sigma'(\mathrm{y}) = \sigma(\mathrm{x})!$.

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{(\sigma, \sigma) \mid 2 > \sigma(\mathrm{x})\} \cup \\ \{(\sigma, f(\sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1])) \mid 2 \leq \sigma(\mathrm{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathrm{x}) \geq 1 \land \sigma_0(\mathrm{y}) = 1) \implies \sigma_0'(\mathrm{y}) = \sigma_0(\mathrm{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathrm{x}) \geq 1$ and $\sigma(\mathrm{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathrm{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathrm{x}) = 1$. Thus, $\sigma'(\mathrm{y}) = \sigma(\mathrm{y}) = 1 = 1! = \sigma(\mathrm{x})!$.

Case 2: Assume $2 \leq \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$.

- $\sigma_2(\mathrm{x}) \geq 1$ because $\sigma_2(\mathrm{x}) = \sigma(\mathrm{x}) - 1$ and $\sigma(\mathrm{x}) \geq 2$.
- $\sigma_2(\mathrm{y}) = 1$ because $\sigma_2(\mathrm{y}) = \sigma(\mathrm{y})\sigma(\mathrm{x})$ and ... ?

Goal: Must prove $\sigma'(\mathrm{y}) = \sigma(\mathrm{x})!$.

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{(\sigma,\sigma) \mid 2 > \sigma(\mathrm{x})\} \cup \\ \{(\sigma, f(\sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1])) \mid 2 \leq \sigma(\mathrm{x})\}\end{aligned}$$

...

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big((\sigma_0(\mathrm{x}) \geq 1 \land \sigma_0(\mathrm{y}) = 1) \implies \sigma_0'(\mathrm{y}) = \sigma_0(\mathrm{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathrm{x}) \geq 1$ and $\sigma(\mathrm{y}) = 1$.

Case 1: Assume $2 > \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathrm{x}) < 2$ (and $\sigma^{\to} = \mathbb{Z}$), we infer $\sigma(\mathrm{x}) = 1$. Thus, $\sigma'(\mathrm{y}) = \sigma(\mathrm{y}) = 1 = 1! = \sigma(\mathrm{x})!$.

Case 2: Assume $2 \leq \sigma(\mathrm{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathrm{y} \mapsto \sigma(\mathrm{y})\sigma(\mathrm{x})][\mathrm{x} \mapsto \sigma(\mathrm{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$.

- $\sigma_2(\mathrm{x}) \geq 1$ because $\sigma_2(\mathrm{x}) = \sigma(\mathrm{x}) - 1$ and $\sigma(\mathrm{x}) \geq 2$.
- $\sigma_2(\mathrm{y}) = 1$ because $\sigma_2(\mathrm{y}) = \sigma(\mathrm{y})\sigma(\mathrm{x})$ and ... ?

Hmm. This looks bad. I think we're stuck.

Mathematical Rigor

Essential skill for faithfully verifying software:

Don't blindly "force" a proof forward (usually by just stating what you want to be true) when the assumptions don't support it!

The theorem might be false! The code might be wrong! Lives could be at stake!

- Recognizing a proof failure and pointing it out will earn you maximal partial credit.
- Unmarked false proof steps (where you really didn't know how to prove it but just pretended it was proved) solicit maximal point deductions.

Generalizing the Theorem

Back to our problem... How to fix?

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program
`while` 2 `<= x do` $($`y := y * x;x := x - `$1)$ and property P is defined by
$P(f) \equiv \forall(\sigma, \sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \wedge \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big).$

This theorem has an assumption that is true at the start of the loop but does not remain true as the loop iterates. What is it?

Generalizing the Theorem

Back to our problem... How to fix?

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program `while 2 <= x do (y := y * x; x := x - 1)` and property P is defined by $P(f) \equiv \forall(\sigma, \sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \land \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

This theorem has an assumption that is true at the start of the loop but does not remain true as the loop iterates. What is it?

Generalizing the Theorem

Back to our problem... How to fix?

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program
`while` 2 `<=` `x` `do` $($`y := y * x;x := x - `$1)$ and property P is defined by
$P(f) \equiv \forall(\sigma, \sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \land \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

This theorem has an assumption that is true at the start of the loop but does not remain true as the loop iterates.

This is a problem because when we start our induction, we get a "weak" inductive hypothesis (assumptions are too "strong") that we cannot apply.

Solution: Can we formulate a different theorem that **implies** this one, but without that assumption or generalized in some way? If so, we can prove that instead to get this theorem.

Generalizing the Theorem

Back to our problem... How to fix?

Lemma

Property $P'(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program `while 2<=x do (y:=y*x;x:=x-1)` and property P' is defined by $P'(f) \equiv \forall(\sigma,\sigma') \in f, \big((\sigma(\mathrm{x}) \geq 1 ~~\wedge \sigma(\mathrm{y}) = 1~~) \implies \sigma'(\mathrm{y}) = \sigma(\mathrm{y}) \cdot \sigma(\mathrm{x})!\big)$.

This theorem has an assumption that is true at the start of the loop but does not remain true as the loop iterates.

This is a problem because when we start our induction, we get a “weak” inductive hypothesis (assumptions are too “strong”) that we cannot apply.

Solution: Can we formulate a different theorem that **implies** this one, but without that assumption or generalized in some way? If so, we can prove that instead to get this theorem.

Generalizing the Theorem

Theorem

Property $P(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program `while` 2 `<=` `x` `do` $($`y` `:=` `y` `*` `x` `;` `x` `:=` `x` `-` $1)$ and property P is defined by $P(f) \equiv \forall(\sigma, \sigma') \in f, \big((\sigma(\mathtt{x}) \geq 1 \wedge \sigma(\mathtt{y}) = 1) \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{x})!\big)$.

Lemma

Property $P'(\mathcal{C}[\![c]\!])$ holds, where c is SIMPL program `while` 2 `<=` `x` `do` $($`y` `:=` `y` `*` `x` `;` `x` `:=` `x` `-` $1)$ and property P' is defined by $P'(f) \equiv \forall(\sigma, \sigma') \in f, \big(\sigma(\mathtt{x}) \geq 1 \Longrightarrow \sigma'(\mathtt{y}) = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!\big)$.

Proof

Property $P'(f)$ implies $P(f)$ because P is merely the special case of P' when $\sigma(\mathtt{y}) = 1$. Proving $P'(\mathcal{C}[\![c]\!])$ therefore suffices to prove $P(\mathcal{C}[\![c]\!])$. We will prove $P'(\mathcal{C}[\![c]\!])$ by fixed-point induction over Γ. ...

Generalizing the Theorem

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{&(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ &\{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P'(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P'(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P'. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big(\sigma_0(\mathtt{x}) \geq 1 \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{y}) \cdot \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ ~~and $\sigma(\mathtt{y}) = 1$~~.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathtt{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathtt{x}) = 1$. Thus, $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) = \sigma(\mathtt{y}) \cdot 1! = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

Case 2: Assume $2 \leq \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$.

- $\sigma_2(\mathtt{x}) \geq 1$ because $\sigma_2(\mathtt{x}) = \sigma(\mathtt{x}) - 1$ and $\sigma(\mathtt{x}) \geq 2$.
- ~~$\sigma_2(\mathtt{y}) = 1$ because ...~~

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{(\sigma,\sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P'(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P'(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P'. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big(\sigma_0(\mathtt{x}) \geq 1 \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{y}) \cdot \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ ~~and $\sigma(\mathtt{y}) = 1$~~.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathtt{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathtt{x}) = 1$. Thus, $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) = \sigma(\mathtt{y}) \cdot 1! = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

Case 2: Assume $2 \leq \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$.

- $\sigma_2(\mathtt{x}) \geq 1$ because $\sigma_2(\mathtt{x}) = \sigma(\mathtt{x}) - 1$ and $\sigma(\mathtt{x}) \geq 2$.

From IH we infer that $\sigma'(\mathtt{y}) = \sigma_2(\mathtt{y}) \cdot \sigma_2(\mathtt{x})!$.

Goal: Prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = {} & \{(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ & \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P'(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P'(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P'. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big(\sigma_0(\mathtt{x}) \geq 1 \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{y}) \cdot \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ ~~and $\sigma(\mathtt{y}) = 1$~~.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathtt{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathtt{x}) = 1$. Thus, $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) = \sigma(\mathtt{y}) \cdot 1! = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

Case 2: Assume $2 \leq \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$.

- $\sigma_2(\mathtt{x}) \geq 1$ because $\sigma_2(\mathtt{x}) = \sigma(\mathtt{x}) - 1$ and $\sigma(\mathtt{x}) \geq 2$.

From IH we infer that $\sigma'(\mathtt{y}) = \sigma_2(\mathtt{y}) \cdot \sigma_2(\mathtt{x})! = (\sigma(\mathtt{y})\sigma(\mathtt{x})) \cdot (\sigma(\mathtt{x}) - 1)!$.

Goal: Prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = {} & \{(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ & \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P'(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P'(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P'. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big(\sigma_0(\mathtt{x}) \geq 1 \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{y}) \cdot \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ ~~and $\sigma(\mathtt{y}) = 1$~~.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathtt{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathtt{x}) = 1$. Thus, $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) = \sigma(\mathtt{y}) \cdot 1! = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

Case 2: Assume $2 \leq \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$.

- $\sigma_2(\mathtt{x}) \geq 1$ because $\sigma_2(\mathtt{x}) = \sigma(\mathtt{x}) - 1$ and $\sigma(\mathtt{x}) \geq 2$.

From IH we infer that $\sigma'(\mathtt{y}) = \sigma_2(\mathtt{y}) \cdot \sigma_2(\mathtt{x})! = (\sigma(\mathtt{y})\sigma(\mathtt{x})) \cdot (\sigma(\mathtt{x}) - 1)! = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

Goal: Prove $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$

Inductive Case

Proof

By definition of $\mathcal{C}$, $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ where Γ is defined by:

$$\begin{aligned}\Gamma(f) = \{(\sigma, \sigma) \mid 2 > \sigma(\mathtt{x})\} \cup \\ \{(\sigma, f(\sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1])) \mid 2 \leq \sigma(\mathtt{x})\}\end{aligned}$$

We can therefore prove $P'(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Base Case: $P'(\bot)$ holds vacuously.

IH: Let $g : \Sigma \rightharpoonup \Sigma$ be an arbitrary function satisfying P'. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \big(\sigma_0(\mathtt{x}) \geq 1 \implies \sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{y}) \cdot \sigma_0(\mathtt{x})!\big)$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given. Assume $\sigma(\mathtt{x}) \geq 1$ ~~and $\sigma(\mathtt{y}) = 1$~~.

Case 1: Assume $2 > \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = \sigma$. Since $1 \leq \sigma(\mathtt{x}) < 2$ (and $\sigma^{\rightarrow} = \mathbb{Z}$), we infer $\sigma(\mathtt{x}) = 1$. Thus, $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) = \sigma(\mathtt{y}) \cdot 1! = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

Case 2: Assume $2 \leq \sigma(\mathtt{x})$. By definition of Γ, $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1]$. Apply IH with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$.

- $\sigma_2(\mathtt{x}) \geq 1$ because $\sigma_2(\mathtt{x}) = \sigma(\mathtt{x}) - 1$ and $\sigma(\mathtt{x}) \geq 2$.

From IH we infer that $\sigma'(\mathtt{y}) = \sigma_2(\mathtt{y}) \cdot \sigma_2(\mathtt{x})! = (\sigma(\mathtt{y})\sigma(\mathtt{x})) \cdot (\sigma(\mathtt{x}) - 1)! = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

□

Big Picture

- Denotational Semantics
    - The fact that loops in imperative languages denote least fixed points gives us a powerful tool for mathematically proving things about them.
    - Fixed-point induction much nicer than infinite unions once you get the hang of it.
- “Turning the crank” of the induction
    - Choosing the right generalization of the theorem is key to carrying out all forms of induction.
    - Intuition: Remove/generalize theorem assumptions that are not invariant (always true) throughout the loop’s iterations.
    - Wrong choice will lead to proof stuck point, which will reveal new theorem generalization ...
    - ... but only if you don’t “force” proofs by blowing past stuck points pretending they’re proved!

Fixed-point Induction Generalizes Structural Induction

Why is fixed-point induction a generalization of structural induction?

Goal: Prove $\forall \mathcal{D}, P(\mathcal{D})$ (i.e., some property P holds for all derivations).

Two options:

1. Let $\mathcal{D}$ be given and prove $P(\mathcal{D})$ by structural induction.
2. Define $\boldsymbol{\mathcal{D}}$ to be the (countably infinite) set of all derivations, and define $\mathbf{P}(\boldsymbol{\mathcal{D}}_0) \equiv \forall \mathcal{D} \in \boldsymbol{\mathcal{D}}_0, P(\mathcal{D})$. Prove $\mathbf{P}(\boldsymbol{\mathcal{D}})$ by fixed-point induction.

Turns out $\boldsymbol{\mathcal{D}}$ is the least fixed point of a functional.
Optional Exercise: Define the appropriate functional!

Eliminating Recursion

Exercise

Consider the following recursively defined function $f : \mathbb{Z} \to \mathbb{Z}$.

$$f(x) = \big(x{=}0 \to 0 \mid x{>}0 \to 2 - f(1-x) \mid x{<}0 \to f(-x)\big)$$

Find a closed-form definition of f and prove your answer.

Definition (closed form): A *closed-form* definition of a function is a definition that contains no recursion, or references to fixpoints or other recursively defined functions.

How to guess a closed-form definition of a recursively defined function?

- A Just plug many numbers in and see if a pattern emerges.
- B Use the functional and try to discern a pattern.

Neither is a proof; they just give you a hypothesis to prove/disprove.

Functional Approach to Closed-form Discovery

$$f(x) = \big(x{=}0 \to 0 \mid x{>}0 \to 2 - f(1-x) \mid x{<}0 \to f(-x)\big)$$

$$F(g) = \lambda x.\big(x{=}0 \to 0 \mid x{>}0 \to 2 - g(1-x) \mid x{<}0 \to g(-x)\big)$$

Functional Approach to Closed-form Discovery

$$f(x) = \big(x{=}0 \rightarrow 0 \mid x{>}0 \rightarrow 2 - f(1-x) \mid x{<}0 \rightarrow f(-x)\big)$$

$$F(g) = \lambda x.\big(x{=}0 \rightarrow 0 \mid x{>}0 \rightarrow 2 - g(1-x) \mid x{<}0 \rightarrow g(-x)\big)$$

$$F^0(\perp) = \{\}$$

Functional Approach to Closed-form Discovery

$$f(x) = \big(x{=}0 \to 0 \mid x{>}0 \to 2 - f(1-x) \mid x{<}0 \to f(-x)\big)$$

$$F(g) = \lambda x.\big(x{=}0 \to 0 \mid x{>}0 \to 2 - g(1-x) \mid x{<}0 \to g(-x)\big)$$

$$\begin{aligned} F^0(\bot) &= \{\} \\ F^1(\bot) &= \lambda x.\big(x{=}0 \to 0 \mid x{>}0 \to 2 - F^0(\bot)(1-x) \mid x{<}0 \to F^0(\bot)(-x)\big) \\ &= \{(0,0)\} \end{aligned}$$

Functional Approach to Closed-form Discovery

$$f(x) = \big(x{=}0 \to 0 \mid x{>}0 \to 2 - f(1-x) \mid x{<}0 \to f(-x)\big)$$

$$F(g) = \lambda x.\big(x{=}0 \to 0 \mid x{>}0 \to 2 - g(1-x) \mid x{<}0 \to g(-x)\big)$$

$$\begin{aligned}
F^0(\bot) &= \{\} \\
F^1(\bot) &= \{(0,0)\} \\
F^2(\bot) &= \lambda x.\big(x{=}0 \to 0 \mid x{>}0 \to 2 - F^1(\bot)(1-x) \mid x{<}0 \to F^1(\bot)(-x)\big) \\
&= \{(0,0),(1,2)\}
\end{aligned}$$

Functional Approach to Closed-form Discovery

$$f(x) = \big(x{=}0 \to 0 \mid x{>}0 \to 2 - f(1-x) \mid x{<}0 \to f(-x)\big)$$

$$F(g) = \lambda x.\big(x{=}0 \to 0 \mid x{>}0 \to 2 - g(1-x) \mid x{<}0 \to g(-x)\big)$$

$$\begin{aligned}
F^0(\bot) &= \{\} \\
F^1(\bot) &= \{(0,0)\} \\
F^2(\bot) &= \{(0,0),(1,2)\} \\
F^2(\bot) &= \lambda x.\big(x{=}0 \to 0 \mid x{>}0 \to 2 - F^2(\bot)(1-x) \mid x{<}0 \to F^2(\bot)(-x)\big) \\
&= \{(-1,2),(0,0),(1,2)\}
\end{aligned}$$

Functional Approach to Closed-form Discovery

$$f(x) = \big(x{=}0 \rightarrow 0 \mid x{>}0 \rightarrow 2 - f(1-x) \mid x{<}0 \rightarrow f(-x)\big)$$

$$F(g) = \lambda x.\big(x{=}0 \rightarrow 0 \mid x{>}0 \rightarrow 2 - g(1-x) \mid x{<}0 \rightarrow g(-x)\big)$$

$$\begin{aligned}
F^0(\bot) &= \{\} \\
F^1(\bot) &= \{(0,0)\} \\
F^2(\bot) &= \{(0,0),(1,2)\} \\
F^2(\bot) &= \{(-1,2),(0,0),(1,2)\} \\
&\vdots \\
F^7(\bot) &= \{(-3,2),(-2,0),(-1,2),(0,0),(1,2),(2,0),(3,2)\}
\end{aligned}$$

Hypothesis (unproved):

$$f(x) = \begin{cases} 2 & \text{if } x \text{ is odd} \\ 0 & \text{if } x \text{ is even} \end{cases}$$

Proving Function Equivalence

Theorem

Consider the following recursively defined function $f : \mathbb{Z} \to \mathbb{Z}$.

$$f(x) = \big(x{=}0 \to 0 \mid x{>}0 \to 2 - f(1-x) \mid x{<}0 \to f(-x)\big)$$

Function f is equal to hypothesis function h defined by

$$h(x) = \begin{cases} 2 & \text{if } x \text{ is odd} \\ 0 & \text{if } x \text{ is even} \end{cases}$$

Proof

Define property $P(g) \equiv \forall x \in g^{\leftarrow}, g(x) = h(x)$. We wish to prove $P(f)$. Define functional F as on the previous slide and observe that $\mathit{fix}(F) = f$ by construction. Thus, to prove $P(f)$ it suffices to prove $P(\mathit{fix}(F))$ by fixed-point induction over F. …

Note: This actually only proves $f \subseteq h$. To complete the proof you would also have to prove $h \subseteq f$, but we won't do that in this class.

Other Kinds of Recursive Functions

What if f is a multi-argument function (e.g., $f(x, y) = \cdots$)?

- Same procedure except elements of f look like $((x, y), z)$.
- See sample exercise #2 in the online notes.

What if we have a nest of mutually recursive functions?

$$\begin{aligned} f(x) &= \big(P_1(x) \to \cdots \mid P_2(x) \to \cdots g(x-1) \cdots\big) \\ g(x) &= \big(P_3(x) \to \cdots \mid P_4(x) \to \cdots f(x-5) \cdots\big) \end{aligned}$$

Trick: Turn it into a single function by adding an extra argument:

$$\begin{aligned} h(s, x) = \big(&s = 1 \wedge P_1(x) \to \cdots \mid s = 1 \wedge P_2(x) \to \cdots h(2, x-1) \cdots \\ \mid\, &s = 2 \wedge P_3(x) \to \cdots \mid s = 2 \wedge P_4(x) \to \cdots h(1, x-5) \cdots\big) \end{aligned}$$

So now $f(x) = h(1, x)$ and $g(x) = h(2, x)$. Can prove things about f and g by proving things about h.