Lecture #8–9: Fixed-point Induction

CS 6371: Advanced Programming Languages

February 11–13, 2014

Suppose we want to prove that some property P holds for a recursively defined function $f : A \rightharpoonup A$. We can prove $P(f)$ by fixed-point induction via the following three steps:

1. Define a non-recursive functional $F : (A \rightharpoonup A) \to (A \rightharpoonup A)$ whose least fixed point is f.
2. **Base Case:** Prove that property P holds for the function whose preimage is empty. That is, prove that $P(\bot_{A \rightharpoonup A})$ holds.
3. **Inductive Case:** Assume as the inductive hypothesis that P holds for some arbitrary function g, and prove that this implies that P holds for function $F(g)$. That is, prove $P(g) \Rightarrow P(F(g))$.

Here is an example of such a proof:

Exercise 1. *Consider the following recursive definition of the factorial function $f : \mathbb{N}_0 \to \mathbb{N}_0$.*

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

Prove that for all $x \in \mathbb{Z}$, $f(x)$ is either undefined or $f(x) = x!$. (It also turns out that $f(x)$ is defined for all $x \geq 0$, but we won't prove that here.)

Proof. The property P to be proved can be formally expressed as $P(g) \equiv \forall x \in g^{\leftarrow} \,.\, g(x) = x!$. We wish to prove $P(f)$. Define functional $F : (\mathbb{N}_0 \rightharpoonup \mathbb{N}_0) \to (\mathbb{N}_0 \rightharpoonup \mathbb{N}_0)$ as follows:

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

Observe that $\mathit{fix}(F) = f$. Thus, to prove $P(f)$ it suffices to prove $P(\mathit{fix}(F))$ by fixed-point induction.

Base Case: $P(\bot_{\mathbb{N}_0 \rightharpoonup \mathbb{N}_0})$ holds vacuously. That is, $P(\bot_{\mathbb{N}_0 \rightharpoonup \mathbb{N}_0})$ requires us to prove something about all members of ${\bot_{\mathbb{N}_0 \rightharpoonup \mathbb{N}_0}}^{\leftarrow}$, but ${\bot_{\mathbb{N}_0 \rightharpoonup \mathbb{N}_0}}^{\leftarrow}$ has no members, so there is nothing to prove.

Inductive Case: Assume that $P(g)$ holds for some arbitrary function g. That is, assume that $\forall x{\in}g^{\leftarrow} \,.\, g(x){=}x!$. We will prove that $P(F(g))$ holds. That is, we will prove that $\forall x{\in}F(g)^{\leftarrow} \,.\, F(g)(x){=}x!$. Let an arbitrary $x \in F(g)^{\leftarrow}$ be given. Looking at the definition of F, there are two cases to consider:

Case 1: Suppose $x = 0$. Then by definition of F, $F(g)(x) = 1 = x!$.

Case 2: Suppose $x > 0$. Then by definition of F, $F(g)(x) = xg(x-1)$. By inductive hypothesis, $g(x-1) = (x-1)!$. Hence, $F(g)(x) = x(x-1)! = x!$. $\square$

The same general technique can be used to prove a property P of the denotation of a while loop. First, define a non-recursive functional Γ whose least fixed point is $\mathcal{C}[\![\texttt{while } b \texttt{ do } c]\!]$.

$$\begin{aligned}\Gamma(f) = &\{(\sigma, (f \circ \mathcal{C}[\![c]\!])(\sigma)) \mid (\sigma, T) \in \mathcal{B}[\![b]\!]\} \cup \\ &\{(\sigma, \sigma) \mid (\sigma, F) \in \mathcal{B}[\![b]\!]\}\end{aligned}$$

We can now prove that P holds for $\mathit{fix}(\Gamma)$ using fixed-point induction. The induction has two steps:

1. As the base case of the induction, prove $P(\perp_{\Sigma \rightharpoonup \Sigma})$.
2. Assume as the inductive hypothesis that $P(f)$ holds, and prove that $P(\Gamma(f))$ holds.

To prove a property P by induction it is often easier to prove a stronger property P' that implies P. The stronger P' yields a stronger inductive hypothesis. Here is an example:

Exercise 2. *Define c to be the SIMPL program* `while 2<=x do (y:=y * x; x:=x - 1)`. *Define property P by $P(f) \equiv \forall(\sigma, \sigma') \in f$, if $\sigma(\mathtt{x}) \geq 1$ and $\sigma(\mathtt{y}) = 1$ then $\sigma'(\mathtt{y}) = \sigma(\mathtt{x})!$. Prove $P(\mathcal{C}[\![c]\!])$.*

Proof. We will instead prove a different property $P'(\mathcal{C}[\![c]\!])$, where P' is defined as follows:

$$P'(f) \;\equiv\; \forall(\sigma, \sigma') \in f, \text{ if } \sigma(\mathtt{x}) \geq 1 \text{ then } \sigma'(\mathtt{y}) = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$$

Notice that $P'(f)$ implies $P(f)$. That is, since we know by assumption that $\sigma(\mathtt{y}) = 1$, $P'(f)$ implies that $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})! = \sigma(\mathtt{x})!$. Thus, proving $P'(\mathcal{C}[\![c]\!])$ suffices to prove the theorem.

We begin by defining a functional Γ whose least fixed point is $\mathcal{C}[\![c]\!]$:

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

We shall prove by fixed-point induction that property $P'(\mathit{fix}(\Gamma))$ holds.

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

Inductive Case: Assume as the inductive hypothesis that property $P'(f)$ holds. That is, assume that for all $(\sigma_0, \sigma_0') \in f$, if $\sigma_0(\mathtt{x}) \geq 1$ then $\sigma_0'(\mathtt{y}) = \sigma_0(\mathtt{y}) \cdot \sigma_0(\mathtt{x})!$. We wish to prove that property $P'(\Gamma(f))$ holds.

Let $(\sigma, \sigma') \in \Gamma(f)$ be given and assume that $\sigma(\mathtt{x}) \geq 1$. We must prove that $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

Case 1: Assume that $2 \leq \sigma(\mathtt{x})$. From the definition of Γ we conclude that $\sigma' = f(\sigma_2)$ where $\sigma_2 = \sigma[\mathtt{y} \mapsto \sigma(\mathtt{y})\sigma(\mathtt{x})][\mathtt{x} \mapsto \sigma(\mathtt{x}) - 1]$. Writing $\sigma' = f(\sigma_2)$ is the same as writing $(\sigma_2, \sigma') \in f$. Therefore, we intend to apply the inductive hypothesis with $\sigma_0 = \sigma_2$ and $\sigma_0' = \sigma'$. To do so, we must first prove that $\sigma_2(\mathtt{x}) \geq 1$. From the definition of σ_2 we infer that $\sigma_2(\mathtt{x}) = \sigma(\mathtt{x}) - 1$. Since $2 \leq \sigma(\mathtt{x})$ by assumption, it follows that $\sigma_2(\mathtt{x}) \geq 1$. By inductive hypothesis, $\sigma'(\mathtt{y}) = \sigma_2(\mathtt{y}) \cdot \sigma_2(\mathtt{x})! = (\sigma(\mathtt{y})\sigma(\mathtt{x})) \cdot (\sigma(\mathtt{x}) - 1)! = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

Case 2: Assume that $2 > \sigma(\mathtt{x})$. From the definition of Γ we conclude that $\sigma' = \sigma$, so $\sigma'(\mathtt{y}) = \sigma(\mathtt{y})$. Since we have assumed both that $\sigma(\mathtt{x}) \geq 1$ and that $2 > \sigma(\mathtt{x})$, it follows that $\sigma(\mathtt{x}) = 1$. Hence, $\sigma'(\mathtt{y}) = \sigma(\mathtt{y}) = \sigma(\mathtt{y}) \cdot \sigma(\mathtt{x})!$.

We have therefore proved by fixed-point induction that property $P'(\mathit{fix}(\Gamma))$ holds. Since $\mathit{fix}(\Gamma) = \mathcal{C}[\![c]\!]$, it follows that $P'(\mathcal{C}[\![c]\!])$ holds. Since property P' implies the theorem, this proves the theorem. $\square$