

# Lecture #9: Fixed-point Induction

CS 6371: Advanced Programming Languages

September 18, 2008

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

1. Define a non-recursive functional  $F : (A \rightarrow A) \rightarrow (A \rightarrow A)$  whose least fixed point is  $f$ .
2. **Base Case:** Prove that property  $P$  holds for the empty set. That is, prove that  $P(\perp_{A \rightarrow A})$  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  $f : \mathbb{N} \rightarrow \mathbb{N}$ :

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

Prove that  $f$  is the factorial function.

*Proof.* The property  $P$  of being the factorial function can be defined as  $P(g) \equiv \forall x \in \text{Dom}(g). g(x) = x!$ . We wish to prove  $P(f)$ . Define functional  $F : (\mathbb{N} \rightarrow \mathbb{N}) \rightarrow (\mathbb{N} \rightarrow \mathbb{N})$  as follows:

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

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

**Base Case:**  $P(\perp_{\mathbb{N} \rightarrow \mathbb{N}})$  holds vacuously. That is,  $P(\perp_{\mathbb{N} \rightarrow \mathbb{N}})$  requires us to prove something about all members of  $\text{Dom}(\perp_{\mathbb{N} \rightarrow \mathbb{N}})$ , but  $\text{Dom}(\perp_{\mathbb{N} \rightarrow \mathbb{N}})$  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  $\forall x \in \text{Dom}(g). g(x) = x!$ . We will prove that  $P(F(g))$  holds. That is, we will prove that  $\forall x \in \text{Dom}(F(g)). F(g)(x) = x!$ . Let an arbitrary  $x \in \text{Dom}(F(g))$  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  $\Gamma$  whose least fixed point is  $\mathcal{C}[\text{while } b \text{ do } c]$ .

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

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

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

Often in order to prove a property  $P$  by fixed-point induction it is easier to prove a stronger property  $P'$  that implies  $P$ . Here is an example:

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

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

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

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

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

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

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

**Base Case:** Property  $P'(\perp)$  holds vacuously. That is, since  $P'$  requires us to prove something for all  $(\sigma, \sigma') \in \perp$  but  $\perp$  is empty, there is nothing to prove.

**Inductive Case:** Assume as the inductive hypothesis that property  $P'(f)$  holds. That is, assume that for all  $(\sigma_0, \sigma_1) \in f$ , if  $\sigma_0(x) \geq 1$  then  $\sigma_1(y) = \sigma_0(y) \cdot \sigma_0(x)!$ . We wish to prove that property  $P'(\Gamma(f))$  holds.

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

**Case 1:** Assume that  $2 \leq \sigma(\mathbf{x})$ . From the definition of  $\Gamma$  we conclude that  $\sigma' = f(\sigma_2)$  where  $\sigma_2 = \sigma[\mathbf{y} \mapsto \sigma(\mathbf{y})\sigma(\mathbf{x})][\mathbf{x} \mapsto \sigma(\mathbf{x}) - 1]$ . Writing  $\sigma' = f(\sigma_2)$  is the same as writing  $(\sigma_2, \sigma') \in f$ . Therefore, we intend to apply the induction hypothesis with  $\sigma_0 = \sigma_2$  and  $\sigma_1 = \sigma'$ . To do so, we must first prove that  $\sigma_2(\mathbf{x}) \geq 1$ . From the definition of  $\sigma_2$  we infer that  $\sigma_2(\mathbf{x}) = \sigma(\mathbf{x}) - 1$ . Since  $2 \leq \sigma(\mathbf{x})$  by assumption, it follows that  $\sigma_2(\mathbf{x}) \geq 1$ . By inductive hypothesis,  $\sigma'(\mathbf{y}) = \sigma_2(\mathbf{y}) \cdot \sigma_2(\mathbf{x})! = (\sigma(\mathbf{y})\sigma(\mathbf{x})) \cdot (\sigma(\mathbf{x}) - 1)! = \sigma(\mathbf{y}) \cdot \sigma(\mathbf{x})!$ .

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

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