

Lecture #9: Fixed-point Induction

CS 6371: Advanced Programming Languages

September 19, 2007

To prove that some property P holds for function $f = \mathcal{C}[\text{while } b \text{ do } c]$, first rewrite the while-loop as the following recursive function:

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

Next, consider the non-recursive functional Γ whose least fixed-point is f :

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

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

1. As the base case of the induction, prove that P holds for $\perp_{\Sigma \rightarrow \Sigma} = \{\}$, or prove that P holds for $\Gamma(\perp_{\Sigma \rightarrow \Sigma})$.
2. As the inductive hypothesis, assume that P holds for g . Prove that P holds for $\Gamma(g)$.

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:

Theorem. Define c to be the IMP program `while $2 \leq x$ do $(y := y * x; x := x - 1)$` . For all $(\sigma, \sigma') \in \mathcal{C}[c]$, if $\sigma(x) \geq 1$ and $\sigma(y) = 1$ then $\sigma'(y) = \sigma(x)!$ (where $!$ is the mathematical symbol for factorial).

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

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

Notice that $P'(\mathcal{C}[c])$ implies the theorem. That is, if $\sigma(y) = 1$ and $\sigma'(y) = \sigma(y) \cdot \sigma(x)!$ then $\sigma'(y) = \sigma(x)!$. Thus, proving $P'(\mathcal{C}[c])$ suffices to prove the theorem.

We begin by rewriting $\mathcal{C}[c]$ as a recursive function f :

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

Next, we consider the functional Γ whose least fixed-point is f :

$$\Gamma(g) = \{(\sigma, g(\sigma[y \mapsto \sigma(y)\sigma(x)][x \mapsto \sigma(x) - 1])) \mid \sigma \in \Sigma, 2 \leq \sigma(x)\} \cup \{(\sigma, \sigma) \mid \sigma \in \Sigma, 2 > \sigma(x)\}$$

We shall prove by fixed-point induction that property $P'(fix(\Gamma))$ 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 $P'(g)$ holds. That is, assume that for all $(\sigma_0, \sigma_1) \in g$, if $\sigma_0(x) \geq 1$ then $\sigma_1(y) = \sigma_0(y) \cdot \sigma_0(x)!$. We wish to prove that property $P'(\Gamma(g))$ holds.

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

Case 1: Assume that $2 \leq \sigma(x)$. From the definition of Γ we conclude that $\sigma' = g(\sigma_2)$ where $\sigma_2 = \sigma[y \mapsto \sigma(y)\sigma(x)][x \mapsto \sigma(x) - 1]$. Writing $\sigma' = g(\sigma_2)$ is the same as writing $(\sigma_2, \sigma') \in g$. 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 $\sigma_2(x) \geq 1$. From the definition of σ_2 we infer that $\sigma_2(x) = \sigma(x) - 1$. Since $2 \leq \sigma(x)$ by assumption, it follows that $\sigma_2(x) \geq 1$. By inductive hypothesis, $\sigma'(y) = \sigma_2(y) \cdot \sigma_2(x)! = (\sigma(y)\sigma(x)) \cdot (\sigma(x) - 1)! = \sigma(y) \cdot \sigma(x)!$.

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

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