Semantic Equivalence

CS 4301/6371: Advanced Programming Languages

Kevin W. Hamlen

February 27, 2024

Formal Semantics

- Three styles of formal semantics:
  1. Large-step operational: $\langle c, \sigma \rangle \Downarrow \sigma'$
  2. Small-step operational: $\langle c, \sigma \rangle \rightarrow_1 \langle c', \sigma' \rangle$
  3. Denotational: $\mathcal{C}[\![c]\!]\sigma = \sigma'$
- Each has strengths, so often must define more than one
- Danger: multiple semantics must be mutually consistent
- Can we prove that our SIMPL semantics are all consistent?

Semantic Equivalence

Theorem: Semantic Equivalence

The following assertions are all equivalent (each implies the others):

1. $\langle c, \sigma \rangle \Downarrow \sigma'$
2. $\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$ where $\rightarrow^*$ is the reflexive transitive closure of $\rightarrow_1$
3. $\mathcal{C}[\![c]\!]\sigma = \sigma'$

Semantic Equivalence

Theorem: Semantic Equivalence

The following assertions are all equivalent (each implies the others):

1. $\langle c, \sigma \rangle \Downarrow \sigma'$
2. $\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$ where $\rightarrow^*$ is the reflexive transitive closure of $\rightarrow_1$
3. $\mathcal{C}[\![c]\!]\sigma = \sigma'$

Proof strategy: Prove three implications:

- (1) $\Rightarrow$ (2)
- (2) $\Rightarrow$ (3)
- (3) $\Rightarrow$ (1)

Theorem follows from transitivity of implication.

Large-step implies Small-step

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Assume $\langle c, \sigma \rangle \Downarrow \sigma'$. ...

What next?

Structural Induction Setup

Lemma

$\langle c, \sigma\rangle \Downarrow \sigma' \implies \langle c, \sigma\rangle \rightarrow^* \langle \mathtt{skip}, \sigma'\rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma\rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

Let's just state the IH upfront, so we don't have to predict which are the base cases.

Structural Induction Setup

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \Longrightarrow \langle c, \sigma \rangle \rightarrow^* \langle \mathtt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \mathtt{skip}, \sigma_0' \rangle$.

Skip Case

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \Longrightarrow \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 1: Suppose $\mathcal{D}$ ends in Rule L1:

$$\mathcal{D} = \frac{}{\langle \texttt{skip}, \sigma \rangle \Downarrow \sigma}\text{(L1)}$$

Skip Case

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 1: Suppose $\mathcal{D}$ ends in Rule L1:

$$\mathcal{D} = \frac{}{\langle \texttt{skip}, \sigma \rangle \Downarrow \sigma}\text{(L1)}$$

Hence $c = \texttt{skip}$ and $\sigma' = \sigma$.

Skip Case

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \Longrightarrow \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 1: Suppose $\mathcal{D}$ ends in Rule L1:

$$\mathcal{D} = \frac{}{\langle \texttt{skip}, \sigma \rangle \Downarrow \sigma}\text{(L1)}$$

Hence $c = \texttt{skip}$ and $\sigma' = \sigma$. Since $\rightarrow^*$ is reflexive, we conclude that $\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$.

Sequence Case

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \Longrightarrow \langle c, \sigma \rangle \rightarrow^* \langle \mathtt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \mathtt{skip}, \sigma_0' \rangle$.

Case 2: Suppose $\mathcal{D}$ ends in Rule L2:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle c_1 \,, \sigma \rangle \Downarrow \sigma_2} \qquad \cfrac{\mathcal{D}_2}{\langle c_2 \,, \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1 \,; c_2 \,, \sigma \rangle \Downarrow \sigma'}\text{(L2)}$$

Sequence Case

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \to^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \to^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 2: Suppose $\mathcal{D}$ ends in Rule L2:

$$\mathcal{D} = \frac{\dfrac{\mathcal{D}_1}{\langle c_1 \,, \sigma \rangle \Downarrow \sigma_2} \qquad \dfrac{\mathcal{D}_2}{\langle c_2 \,, \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1 \,; c_2 \,, \sigma \rangle \Downarrow \sigma'}\text{(L2)}$$

Hence $c = c_1 \,; c_2$.

Sequence Case

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \Longrightarrow \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 2: Suppose $\mathcal{D}$ ends in Rule L2:

$$\mathcal{D} = \dfrac{\dfrac{\mathcal{D}_1}{\langle c_1, \sigma \rangle \Downarrow \sigma_2} \qquad \dfrac{\mathcal{D}_2}{\langle c_2, \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1 ; c_2, \sigma \rangle \Downarrow \sigma'} \text{(L2)}$$

Hence $c = c_1 ; c_2$.
Apply IH with $\mathcal{D}_0 = \mathcal{D}_1$, $c_0 = c_1$, $\sigma_0 = \sigma$, and $\sigma_0' = \sigma_2$. Since $\mathcal{D}_1 < \mathcal{D}$, we infer that $\langle c_1, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma_2 \rangle$.

Sequence Case

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 2: Suppose $\mathcal{D}$ ends in Rule L2:

$$\mathcal{D} = \dfrac{\dfrac{\mathcal{D}_1}{\langle c_1\,, \sigma \rangle \Downarrow \sigma_2} \qquad \dfrac{\mathcal{D}_2}{\langle c_2\,, \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1\,; c_2, \sigma \rangle \Downarrow \sigma'}\text{(L2)}$$

Hence $c = c_1\,; c_2$.
Apply IH with $\mathcal{D}_0 = \mathcal{D}_1$, $c_0 = c_1$, $\sigma_0 = \sigma$, and $\sigma_0' = \sigma_2$. Since $\mathcal{D}_1 < \mathcal{D}$, we infer that $\langle c_1\,, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma_2 \rangle$.
Apply IH with $\mathcal{D}_0 = \mathcal{D}_2$, $c_0 = c_2$, $\sigma_0 = \sigma_2$, and $\sigma_0' = \sigma'$. Since $\mathcal{D}_2 < \mathcal{D}$, we infer that $\langle c_2\,, \sigma_2 \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$.

Need to somehow prove that $\langle c_1\,; c_2, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$ ... ?

Sequence Case

Lemma

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 2: Suppose $\mathcal{D}$ ends in Rule L2:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle c_1, \sigma \rangle \Downarrow \sigma_2} \qquad \cfrac{\mathcal{D}_2}{\langle c_2, \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1 ; c_2, \sigma \rangle \Downarrow \sigma'} \text{(L2)}$$

Hence $c = c_1 ; c_2$.
Apply IH with $\mathcal{D}_0 = \mathcal{D}_1$, $c_0 = c_1$, $\sigma_0 = \sigma$, and $\sigma_0' = \sigma_2$. Since $\mathcal{D}_1 < \mathcal{D}$, we infer that $\langle c_1, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma_2 \rangle$.
Apply IH with $\mathcal{D}_0 = \mathcal{D}_2$, $c_0 = c_2$, $\sigma_0 = \sigma_2$, and $\sigma_0' = \sigma'$. Since $\mathcal{D}_2 < \mathcal{D}$, we infer that $\langle c_2, \sigma_2 \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$.

Need to somehow prove that $\langle c_1 ; c_2, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$
Idea: Prove $\langle c_1 ; c_2, \sigma \rangle \rightarrow^* \langle \texttt{skip} ; c_2, \sigma_2 \rangle \rightarrow_1 \langle c_2, \sigma_2 \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle \Longrightarrow \langle c \texttt{;} c', \sigma \rangle \rightarrow^* \langle \texttt{skip} \texttt{;} c', \sigma' \rangle$

Proof

Assume $\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$.

How to prove this?

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle \Longrightarrow \langle c\texttt{;}c', \sigma \rangle \rightarrow^* \langle \texttt{skip;}c', \sigma' \rangle$

Proof

Assume $\langle c, \sigma \rangle \rightarrow_n \langle \texttt{skip}, \sigma' \rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma\rangle \rightarrow^* \langle \texttt{skip}, \sigma'\rangle \Longrightarrow \langle c\texttt{;}c', \sigma\rangle \rightarrow^* \langle \texttt{skip;}c', \sigma'\rangle$

Proof

Assume $\langle c, \sigma\rangle \rightarrow_n \langle \texttt{skip}, \sigma'\rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Base Case: Suppose $n = 0$.

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma\rangle \rightarrow^* \langle \texttt{skip}, \sigma'\rangle \Longrightarrow \langle c\texttt{;}c', \sigma\rangle \rightarrow^* \langle \texttt{skip;}c', \sigma'\rangle$

Proof

Assume $\langle c, \sigma\rangle \rightarrow_n \langle \texttt{skip}, \sigma'\rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Base Case: If $n = 0$ then $c = \texttt{skip}$ and $\sigma = \sigma'$ (by reflexivity). It follows that $\langle c\texttt{;}c', \sigma\rangle \rightarrow^* \langle \texttt{skip;}c', \sigma'\rangle$ (also by reflexivity).

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma\rangle \rightarrow^* \langle \texttt{skip}, \sigma'\rangle \Longrightarrow \langle c;c', \sigma\rangle \rightarrow^* \langle \texttt{skip};c', \sigma'\rangle$

Proof

Assume $\langle c, \sigma\rangle \rightarrow_n \langle \texttt{skip}, \sigma'\rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Base Case: If $n = 0$ then $c = \texttt{skip}$ and $\sigma = \sigma'$ (by reflexivity). It follows that $\langle c;c', \sigma\rangle \rightarrow^* \langle \texttt{skip};c', \sigma'\rangle$ (also by reflexivity).

IH: Assume if $\langle c_0, \sigma_0\rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma_0'\rangle$ then $\langle c_0;c_0', \sigma_0\rangle \rightarrow_{n-1} \langle \texttt{skip};c', \sigma_0'\rangle$ (for all $c_0, \sigma_0, \sigma_0', c_0'$).

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle \Longrightarrow \langle c\texttt{;}c', \sigma \rangle \rightarrow^* \langle \texttt{skip;}c', \sigma' \rangle$

Proof

Assume $\langle c, \sigma \rangle \rightarrow_n \langle \texttt{skip}, \sigma' \rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Base Case: If $n = 0$ then $c = \texttt{skip}$ and $\sigma = \sigma'$ (by reflexivity). It follows that $\langle c\texttt{;}c', \sigma \rangle \rightarrow^* \langle \texttt{skip;}c', \sigma' \rangle$ (also by reflexivity).

IH: Assume if $\langle c_0, \sigma_0 \rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma_0' \rangle$ then $\langle c_0\texttt{;}c_0', \sigma_0 \rangle \rightarrow_{n-1} \langle \texttt{skip;}c', \sigma_0' \rangle$ (for all $c_0, \sigma_0, \sigma_0', c_0'$).

Inductive Case: Assume $n \geq 1$.

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma\rangle \rightarrow^* \langle \texttt{skip}, \sigma'\rangle \Longrightarrow \langle c;c', \sigma\rangle \rightarrow^* \langle \texttt{skip};c', \sigma'\rangle$

Proof

Assume $\langle c, \sigma\rangle \rightarrow_n \langle \texttt{skip}, \sigma'\rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Base Case: If $n = 0$ then $c = \texttt{skip}$ and $\sigma = \sigma'$ (by reflexivity). It follows that $\langle c;c', \sigma\rangle \rightarrow^* \langle \texttt{skip};c', \sigma'\rangle$ (also by reflexivity).

IH: Assume if $\langle c_0, \sigma_0\rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma_0'\rangle$ then $\langle c_0;c_0', \sigma_0\rangle \rightarrow_{n-1} \langle \texttt{skip};c', \sigma_0'\rangle$ (for all $c_0, \sigma_0, \sigma_0', c_0'$).

Inductive Case: If $n \geq 1$ then we have $\langle c, \sigma\rangle \rightarrow_1 \langle c_2, \sigma_2\rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma'\rangle$ for some $\langle c_2, \sigma_2\rangle$.

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle \Longrightarrow \langle c\,\texttt{;}\,c', \sigma \rangle \rightarrow^* \langle \texttt{skip}\,\texttt{;}\,c', \sigma' \rangle$

Proof

Assume $\langle c, \sigma \rangle \rightarrow_n \langle \texttt{skip}, \sigma' \rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Base Case: If $n = 0$ then $c = \texttt{skip}$ and $\sigma = \sigma'$ (by reflexivity). It follows that $\langle c\,\texttt{;}\,c', \sigma \rangle \rightarrow^* \langle \texttt{skip}\,\texttt{;}\,c', \sigma' \rangle$ (also by reflexivity).

IH: Assume if $\langle c_0, \sigma_0 \rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma_0' \rangle$ then $\langle c_0\,\texttt{;}\,c_0', \sigma_0 \rangle \rightarrow_{n-1} \langle \texttt{skip}\,\texttt{;}\,c', \sigma_0' \rangle$ (for all $c_0, \sigma_0, \sigma_0', c_0'$).

Inductive Case: If $n \geq 1$ then we have $\langle c, \sigma \rangle \rightarrow_1 \langle c_2, \sigma_2 \rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma' \rangle$ for some $\langle c_2, \sigma_2 \rangle$. By IH (with $c_0 = c_2$, $\sigma_0 = \sigma_2$, $\sigma_0' = \sigma'$, $c_0' = c'$) we infer $\langle c_2\,\texttt{;}\,c', \sigma_2 \rangle \rightarrow_{n-1} \langle \texttt{skip}\,\texttt{;}\,c', \sigma' \rangle$.

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle \Longrightarrow \langle c\texttt{;}c', \sigma \rangle \rightarrow^* \langle \texttt{skip;}c', \sigma' \rangle$

Proof

Assume $\langle c, \sigma \rangle \rightarrow_n \langle \texttt{skip}, \sigma' \rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Base Case: If $n = 0$ then $c = \texttt{skip}$ and $\sigma = \sigma'$ (by reflexivity). It follows that $\langle c\texttt{;}c', \sigma \rangle \rightarrow^* \langle \texttt{skip;}c', \sigma' \rangle$ (also by reflexivity).

IH: Assume if $\langle c_0, \sigma_0 \rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma_0' \rangle$ then $\langle c_0\texttt{;}c_0', \sigma_0 \rangle \rightarrow_{n-1} \langle \texttt{skip;}c', \sigma_0' \rangle$ (for all $c_0, \sigma_0, \sigma_0', c_0'$).

Inductive Case: If $n \geq 1$ then we have $\langle c, \sigma \rangle \rightarrow_1 \langle c_2, \sigma_2 \rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma' \rangle$ for some $\langle c_2, \sigma_2 \rangle$. By IH (with $c_0 = c_2$, $\sigma_0 = \sigma_2$, $\sigma_0' = \sigma'$, $c_0' = c'$) we infer $\langle c_2\texttt{;}c', \sigma_2 \rangle \rightarrow_{n-1} \langle \texttt{skip;}c', \sigma' \rangle$. Rule S1 allows us to derive

$$\frac{\langle c, \sigma \rangle \rightarrow_1 \langle c_2, \sigma_2 \rangle}{\langle c\texttt{;}c', \sigma \rangle \rightarrow_1 \langle c_2\texttt{;}c', \sigma_2 \rangle}\text{(S1)}$$

Sequence Lemma

Subsequence Lemma:

$\langle c, \sigma\rangle \rightarrow^* \langle \texttt{skip}, \sigma'\rangle \Longrightarrow \langle c\texttt{;}c', \sigma\rangle \rightarrow^* \langle \texttt{skip;}c', \sigma'\rangle$

Proof

Assume $\langle c, \sigma\rangle \rightarrow_n \langle \texttt{skip}, \sigma'\rangle$. Proof is by weak natural number induction on $n \in \mathbb{N}$.

Base Case: If $n = 0$ then $c = \texttt{skip}$ and $\sigma = \sigma'$ (by reflexivity). It follows that $\langle c\texttt{;}c', \sigma\rangle \rightarrow^* \langle \texttt{skip;}c', \sigma'\rangle$ (also by reflexivity).

IH: Assume if $\langle c_0, \sigma_0\rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma_0'\rangle$ then $\langle c_0\texttt{;}c_0', \sigma_0\rangle \rightarrow_{n-1} \langle \texttt{skip;}c', \sigma_0'\rangle$ (for all $c_0, \sigma_0, \sigma_0', c_0'$).

Inductive Case: If $n \geq 1$ then we have $\langle c, \sigma\rangle \rightarrow_1 \langle c_2, \sigma_2\rangle \rightarrow_{n-1} \langle \texttt{skip}, \sigma'\rangle$ for some $\langle c_2, \sigma_2\rangle$. By IH (with $c_0 = c_2$, $\sigma_0 = \sigma_2$, $\sigma_0' = \sigma'$, $c_0' = c'$) we infer $\langle c_2\texttt{;}c', \sigma_2\rangle \rightarrow_{n-1} \langle \texttt{skip;}c', \sigma'\rangle$. Rule S1 allows us to derive

$$\frac{\langle c, \sigma\rangle \rightarrow_1 \langle c_2, \sigma_2\rangle}{\langle c\texttt{;}c', \sigma\rangle \rightarrow_1 \langle c_2\texttt{;}c', \sigma_2\rangle}\text{(S1)}$$

Putting these together yields $\langle c\texttt{;}c', \sigma\rangle \rightarrow_1 \langle c_2\texttt{;}c', \sigma_2\rangle \rightarrow_{n-1} \langle \texttt{skip;}c', \sigma'\rangle$. □

Sequence Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Subsequence Lemma:

$\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle \implies \langle c ; c', \sigma \rangle \rightarrow^* \langle \texttt{skip} ; c', \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 2: Suppose $\mathcal{D}$ ends in Rule L2:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle c_1 , \sigma \rangle \Downarrow \sigma_2} \qquad \cfrac{\mathcal{D}_2}{\langle c_2 , \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1 ; c_2 , \sigma \rangle \Downarrow \sigma'} \text{(L2)}$$

Apply IH with $\mathcal{D}_0 = \mathcal{D}_1$, $c_0 = c_1$, $\sigma_0 = \sigma$, and $\sigma_0' = \sigma_2$. Since $\mathcal{D}_1 < \mathcal{D}$, we infer that $\langle c_1 , \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma_2 \rangle$.
Apply IH with $\mathcal{D}_0 = \mathcal{D}_2$, $c_0 = c_2$, $\sigma_0 = \sigma_2$, and $\sigma_0' = \sigma'$. Since $\mathcal{D}_2 < \mathcal{D}$, we infer that $\langle c_2 , \sigma_2 \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$.

Idea: Prove $\langle c_1 ; c_2 , \sigma \rangle \rightarrow^* \langle \texttt{skip} ; c_2 , \sigma_2 \rangle \rightarrow_1 \langle c_2 , \sigma_2 \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Sequence Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Subsequence Lemma:

$\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle \implies \langle c ; c', \sigma \rangle \rightarrow^* \langle \texttt{skip} ; c', \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma'_0$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma'_0 \rangle$.

Case 2: Suppose $\mathcal{D}$ ends in Rule L2:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle c_1 , \sigma \rangle \Downarrow \sigma_2} \qquad \cfrac{\mathcal{D}_2}{\langle c_2 , \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1 ; c_2 , \sigma \rangle \Downarrow \sigma'} \text{(L2)}$$

Apply IH with $\mathcal{D}_0 = \mathcal{D}_1$, $c_0 = c_1$, $\sigma_0 = \sigma$, and $\sigma'_0 = \sigma_2$. Since $\mathcal{D}_1 < \mathcal{D}$, we infer that $\langle c_1 , \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma_2 \rangle$. The subsequence lemma implies that $\langle c_1 ; c_2 , \sigma \rangle \rightarrow^* \langle \texttt{skip} ; c_2 , \sigma_2 \rangle$. Apply IH with $\mathcal{D}_0 = \mathcal{D}_2$, $c_0 = c_2$, $\sigma_0 = \sigma_2$, and $\sigma'_0 = \sigma'$. Since $\mathcal{D}_2 < \mathcal{D}$, we infer that $\langle c_2 , \sigma_2 \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$.

Idea: Prove $\langle c_1 ; c_2 , \sigma \rangle \rightarrow^* \langle \texttt{skip} ; c_2 , \sigma_2 \rangle \rightarrow_1 \langle c_2 , \sigma_2 \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Sequence Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \to^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma'_0$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \to^* \langle \texttt{skip}, \sigma'_0 \rangle$.

Case 2: Suppose $\mathcal{D}$ ends in Rule L2:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle c_1\,, \sigma \rangle \Downarrow \sigma_2} \qquad \cfrac{\mathcal{D}_2}{\langle c_2\,, \sigma_2 \rangle \Downarrow \sigma'}}{\langle c_1\,; c_2\,, \sigma \rangle \Downarrow \sigma'}\text{(L2)}$$

Apply IH with $\mathcal{D}_0 = \mathcal{D}_1$, $c_0 = c_1$, $\sigma_0 = \sigma$, and $\sigma'_0 = \sigma_2$. Since $\mathcal{D}_1 < \mathcal{D}$, we infer that $\langle c_1\,, \sigma \rangle \to^* \langle \texttt{skip}, \sigma_2 \rangle$. The subsequence lemma implies that $\langle c_1\,; c_2\,, \sigma \rangle \to^* \langle \texttt{skip}; c_2\,, \sigma_2 \rangle$. Moreover, Rule S2 derives

$$\cfrac{}{\langle \texttt{skip}; c_2\,, \sigma_2 \rangle \to_1 \langle c_2\,, \sigma_2 \rangle}\text{(S2)}$$

Apply IH with $\mathcal{D}_0 = \mathcal{D}_2$, $c_0 = c_2$, $\sigma_0 = \sigma_2$, and $\sigma'_0 = \sigma'$. Since $\mathcal{D}_2 < \mathcal{D}$, we infer that $\langle c_2, \sigma_2 \rangle \to^* \langle \texttt{skip}, \sigma' \rangle$. This yields $\langle c_1\,; c_2\,, \sigma \rangle \to^* \langle \texttt{skip}; c_2\,, \sigma_2 \rangle \to_1 \langle c_2\,, \sigma_2 \rangle \to^* \langle \texttt{skip}, \sigma' \rangle$.

Assignment Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 3: Suppose $\mathcal{D}$ ends in Rule L3:

$$\mathcal{D} = \frac{\dfrac{\mathcal{D}_1}{\langle a, \sigma \rangle \Downarrow n}}{\langle v := a, \sigma \rangle \Downarrow \sigma[v \mapsto n]}\text{(L3)}$$

Assignment Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \Longrightarrow \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 3: Suppose $\mathcal{D}$ ends in Rule L3:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle a, \sigma \rangle \Downarrow n}}{\langle v := a, \sigma \rangle \Downarrow \sigma[v \mapsto n]}\text{(L3)}$$

So $c = (v := a)$ and $\sigma' = \sigma[v \mapsto n]$.

Need to somehow prove that $\langle v := a, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma[v \mapsto n] \rangle$.

Assignment Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 3: Suppose $\mathcal{D}$ ends in Rule L3:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle a, \sigma \rangle \Downarrow n}}{\langle v := a, \sigma \rangle \Downarrow \sigma[v \mapsto n]}\text{(L3)}$$

So $c = (v := a)$ and $\sigma' = \sigma[v \mapsto n]$.

Need to somehow prove that $\langle v := a, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma[v \mapsto n] \rangle$.
Idea: Prove $\langle v := a, \sigma \rangle \rightarrow^* \langle v := n, \sigma \rangle \rightarrow_1 \langle \texttt{skip}, \sigma[v \mapsto n] \rangle$.

Assignment Case

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma\rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0\rangle \to^* \langle \texttt{skip}, \sigma_0'\rangle$.

Case 3: Suppose $\mathcal{D}$ ends in Rule L3:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle a, \sigma\rangle \Downarrow n}}{\langle v := a, \sigma\rangle \Downarrow \sigma[v \mapsto n]}\text{(L3)}$$

So $c = (v := a)$ and $\sigma' = \sigma[v \mapsto n]$.

Need to somehow prove that $\langle v := a, \sigma\rangle \to^* \langle \texttt{skip}, \sigma[v \mapsto n]\rangle$.
Idea: Prove $\langle v := a, \sigma\rangle \to^* \langle v := n, \sigma\rangle \to_1 \langle \texttt{skip}, \sigma[v \mapsto n]\rangle$.
Two challenges:

- Must prove $\langle a, \sigma\rangle \Downarrow n \Longrightarrow \langle a, \sigma\rangle \to^* \langle n, \sigma\rangle$.
- Must prove $\langle a, \sigma\rangle \to^* \langle n, \sigma\rangle \Longrightarrow \langle v := a, \sigma\rangle \to^* \langle v := n, \sigma\rangle$.

Semantic Equivalence

Theorem: Arithmetic Semantic Equivalence

The following assertions are all equivalent:

1. $\langle a, \sigma\rangle \Downarrow n$
2. $\langle a, \sigma\rangle \rightarrow^* \langle n, \sigma\rangle$
3. $\mathcal{A}[\![a]\!]\sigma = n$

Theorem: Boolean Semantic Equivalence

The following assertions are all equivalent ($p \in \{T, F\}$):

1. $\langle b, \sigma\rangle \Downarrow p$
2. $\langle b, \sigma\rangle \rightarrow^* \langle \texttt{true}, \sigma\rangle$ if $p = T$ and $\langle b, \sigma\rangle \rightarrow^* \langle \texttt{false}, \sigma\rangle$ if $p = F$
3. $\mathcal{B}[\![b]\!]\sigma = p$

Theorem: Command Semantic Equivalence

The following assertions are all equivalent (each implies the others):

1. $\langle c, \sigma\rangle \Downarrow \sigma'$
2. $\langle c, \sigma\rangle \rightarrow^* \langle \texttt{skip}, \sigma'\rangle$ where $\rightarrow^*$ is the reflexive transitive closure of $\rightarrow_1$
3. $\mathcal{C}[\![c]\!]\sigma = \sigma'$

Subassignment Lemma

Subassignment Lemma

$\langle a, \sigma \rangle \rightarrow^* \langle n, \sigma \rangle \implies \langle v := a, \sigma \rangle \rightarrow^* \langle v := n, \sigma \rangle$

Proof

Assume $\langle a, \sigma \rangle \rightarrow_i \langle n, \sigma \rangle$. Proof is by weak natural number induction over $i \in \mathbb{N}$.

Base Case: If $i = 0$ then $a = n$ (by reflexivity). It follows that $\langle a, \sigma \rangle \rightarrow^* \langle n, \sigma \rangle$ (also by reflexivity).

IH: Assume if $\langle a_0, \sigma_0 \rangle \rightarrow_{i-1} \langle n_0, \sigma_0 \rangle$ then $\langle v := a_0, \sigma_0 \rangle \rightarrow_{i-1} \langle v := n_0, \sigma_0 \rangle$.

Inductive Case: If $i \geq 1$ then we have $\langle a, \sigma \rangle \rightarrow_1 \langle a_2, \sigma \rangle \rightarrow_{i-1} \langle n, \sigma \rangle$ for some a_2. By IH (with $a_0 = a_2$, $\sigma_0 = \sigma$, $n_0 = n$) we infer $\langle v := a, \sigma \rangle \rightarrow_{i-1} \langle v := n, \sigma \rangle$. Rule S3 allows us to derive

$$\frac{\langle a, \sigma \rangle \rightarrow_1 \langle a_2, \sigma \rangle}{\langle v := a, \sigma \rangle \rightarrow_1 \langle v := a_2, \sigma \rangle}\text{(S3)}$$

Putting these together yields $\langle v := a, \sigma \rangle \rightarrow_1 \langle v := a_2, \sigma \rangle \rightarrow_{i-1} \langle v := n, \sigma \rangle$. □

Assignment Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 3: Suppose $\mathcal{D}$ ends in Rule L3:

$$\mathcal{D} = \frac{\dfrac{\mathcal{D}_1}{\langle a, \sigma \rangle \Downarrow n}}{\langle v := a, \sigma \rangle \Downarrow \sigma[v \mapsto n]}\text{(L3)}$$

So $c = (v := a)$ and $\sigma' = \sigma[v \mapsto n]$. By arithmetic semantic equivalence, $\mathcal{D}_1$ implies $\langle a, \sigma \rangle \rightarrow^* \langle n, \sigma \rangle$. The subassignment lemma therefore implies $\langle v := a, \sigma \rangle \rightarrow^* \langle v := n, \sigma \rangle$. Moreover, Rule S4 derives

$$\frac{}{\langle v := n, \sigma \rangle \rightarrow_1 \langle \texttt{skip}, \sigma' \rangle}\text{(S4)}$$

We conclude that $\langle v := a, \sigma \rangle \rightarrow^* \langle v := n, \sigma \rangle \rightarrow_1 \langle \texttt{skip}, \sigma' \rangle$.

Conditional Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \to^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \to^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 4: Suppose $\mathcal{D}$ ends in Rule L4:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle b, \sigma \rangle \Downarrow T} \qquad \cfrac{\mathcal{D}_2}{\langle c_1, \sigma \rangle \Downarrow \sigma'}}{\langle \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2, \sigma \rangle \Downarrow \sigma'} \text{(L4)}$$

By boolean semantic equivalence, $\mathcal{D}_1$ implies $\langle b, \sigma \rangle \to^* \langle \texttt{true}, \sigma \rangle$. A subconditional lemma proves $\langle \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2, \sigma \rangle \to^* \langle \texttt{if true then } c_1 \texttt{ else } c_2, \sigma \rangle$. Rule S6 derives $\langle \texttt{if true then } c_1 \texttt{ else } c_2, \sigma \rangle \to_1 \langle c_1, \sigma \rangle$. Applying the IH (with $\mathcal{D}_0 = \mathcal{D}_2 < \mathcal{D}$, $c_0 = c_1$, $\sigma_0 = \sigma$, $\sigma_0' = \sigma'$) implies $\langle c_1, \sigma \rangle \to^* \langle \texttt{skip}, \sigma' \rangle$. Putting these together yields $\langle \texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2, \sigma \rangle \to^* \langle \texttt{if true then } c_1 \texttt{ else } c_2, \sigma \rangle \to_1 \langle c_1, \sigma \rangle \to^* \langle \texttt{skip}, \sigma' \rangle$.

Case 5: The case where $\mathcal{D}$ ends in Rule L5 is similar.

Loop Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \Longrightarrow \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 6: Suppose $\mathcal{D}$ ends in Rule L6:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle \texttt{if } b \texttt{ then } (c_1 \texttt{;while } b \texttt{ do } c_1) \texttt{ else skip}, \sigma \rangle \Downarrow \sigma'}}{\langle \texttt{while } b \texttt{ do } c_1, \sigma \rangle \Downarrow \sigma'} \text{(L6)}$$

Optional exercise: You should try this one yourself. Turns out it's not very hard! (Answer on next slide.)

Loop Case

Lemma: (1)⇒(2)

$\langle c, \sigma \rangle \Downarrow \sigma' \implies \langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$

Proof

Let $\mathcal{D}$ be a derivation of $\langle c, \sigma \rangle \Downarrow \sigma'$. Proof is by structural induction over $\mathcal{D}$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$ has a derivation $\mathcal{D}_0 < \mathcal{D}$, then $\langle c_0, \sigma_0 \rangle \rightarrow^* \langle \texttt{skip}, \sigma_0' \rangle$.

Case 6: Suppose $\mathcal{D}$ ends in Rule L6:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle \texttt{if } b \texttt{ then } (c_1\,\texttt{;while } b \texttt{ do } c_1) \texttt{ else skip}, \sigma \rangle \Downarrow \sigma'}}{\langle \texttt{while } b \texttt{ do } c_1, \sigma \rangle \Downarrow \sigma'} \text{(L6)}$$

Rule S8 derives $\langle \texttt{while } b \texttt{ do } c_1, \sigma \rangle \rightarrow_1 \langle \texttt{if } b \texttt{ then } (c_1\,\texttt{;while } b \texttt{ do } c_1) \texttt{ else skip} \rangle$. Applying the IH (with $\mathcal{D}_0 = \mathcal{D}_1 < \mathcal{D}$, $c_0 = \texttt{if } b \texttt{ then } (c_1\,\texttt{;while } b \texttt{ do } c_1) \texttt{ else skip}$, $\sigma_0 = \sigma$, $\sigma_0' = \sigma'$) yields $\langle \texttt{if } b \texttt{ then } (c_1\,\texttt{;while } b \texttt{ do } c_1) \texttt{ else skip}, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$. Putting these together yields $\langle \texttt{while } b \texttt{ do } c_1, \sigma \rangle \rightarrow_1 \langle \texttt{if } b \texttt{ then } (c_1\,\texttt{;while } b \texttt{ do } c_1) \texttt{ else skip} \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$. □

Small-step implies Denotational

Lemma: (2)⇒(3)

$\langle c, \sigma \rangle \to^* \langle \texttt{skip}, \sigma' \rangle \Longrightarrow \mathcal{C}[\![c]\!]\sigma = \sigma'$

Proof

Assume $\langle c, \sigma \rangle \to^* \langle \texttt{skip}, \sigma' \rangle$.

What should be our proof strategy for this one?

Small-step implies Denotational

Lemma: (2)⇒(3)

$\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle \Longrightarrow \mathcal{C}[\![c]\!]\sigma = \sigma'$

Proof

Assume $\langle c, \sigma \rangle \rightarrow^* \langle \texttt{skip}, \sigma' \rangle$.

What should be our proof strategy for this one?

Clever idea: Let's instead prove $\langle c, \sigma \rangle \rightarrow_1 \langle c', \sigma' \rangle \Longrightarrow \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c']\!]\sigma'$.

Do you see why this suffices to prove the theorem?

Small-step implies Denotational

Lemma: (2)⇒(3)

$\langle c, \sigma \rangle \rightarrow_1 \langle c', \sigma' \rangle \Longrightarrow \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c']\!]\sigma'$

Proof

Proof is by structural induction on the derivation $\mathcal{D}$ of $\langle c, \sigma \rangle \rightarrow_1 \langle c', \sigma' \rangle$.

Inductive Sequence Case

Lemma: (2)⇒(3)

$\langle c, \sigma \rangle \rightarrow_1 \langle c', \sigma' \rangle \implies \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c']\!]\sigma'$

Proof

Proof is by structural induction on the derivation $\mathcal{D}$ of $\langle c, \sigma \rangle \rightarrow_1 \langle c', \sigma' \rangle$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \rightarrow_1 \langle c_0', \sigma_0' \rangle$ has a derivation $\mathcal{D}_0 < \mathcal{D}$ then $\mathcal{C}[\![c_0]\!]\sigma = \mathcal{C}[\![c_0']\!]\sigma_0'$.

Case 1: Suppose $\mathcal{D}$ ends in Rule S1:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle c_1, \sigma \rangle \rightarrow_1 \langle c_1', \sigma' \rangle}}{\langle c_1 ; c_2, \sigma \rangle \rightarrow_1 \langle c_1' ; c_2, \sigma' \rangle}\text{(S1)}$$

Inductive Sequence Case

Lemma: (2)⇒(3)

$\langle c, \sigma\rangle \rightarrow_1 \langle c', \sigma'\rangle \Longrightarrow \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c']\!]\sigma'$

Proof

Proof is by structural induction on the derivation $\mathcal{D}$ of $\langle c, \sigma\rangle \rightarrow_1 \langle c', \sigma'\rangle$.

IH: Assume if $\langle c_0, \sigma_0\rangle \rightarrow_1 \langle c_0', \sigma_0'\rangle$ has a derivation $\mathcal{D}_0 < \mathcal{D}$ then $\mathcal{C}[\![c_0]\!]\sigma = \mathcal{C}[\![c_0']\!]\sigma_0'$.

Case 1: Suppose $\mathcal{D}$ ends in Rule S1:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle c_1, \sigma\rangle \rightarrow_1 \langle c_1', \sigma'\rangle}}{\langle c_1 ; c_2, \sigma\rangle \rightarrow_1 \langle c_1' ; c_2, \sigma'\rangle}\text{(S1)}$$

Applying the IH (with $\mathcal{D}_0 = \mathcal{D}_1 < \mathcal{D}$, $c_0 = c_1$, $\sigma_0 = \sigma$, $c_0' = c_1'$, $\sigma_0' = \sigma'$) implies $\mathcal{C}[\![c_1]\!]\sigma = \mathcal{C}[\![c_1']\!]\sigma'$.

Must prove $\mathcal{C}[\![c_1 ; c_2]\!]\sigma = \mathcal{C}[\![c_1' ; c_2]\!]\sigma'$.

Inductive Sequence Case

Lemma: (2)⇒(3)

$\langle c, \sigma \rangle \to_1 \langle c', \sigma' \rangle \Longrightarrow \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c']\!]\sigma'$

Proof

Proof is by structural induction on the derivation $\mathcal{D}$ of $\langle c, \sigma \rangle \to_1 \langle c', \sigma' \rangle$.

IH: Assume if $\langle c_0, \sigma_0 \rangle \to_1 \langle c_0', \sigma_0' \rangle$ has a derivation $\mathcal{D}_0 < \mathcal{D}$ then $\mathcal{C}[\![c_0]\!]\sigma = \mathcal{C}[\![c_0']\!]\sigma_0'$.

Case 1: Suppose $\mathcal{D}$ ends in Rule S1:

$$\mathcal{D} = \cfrac{\cfrac{\mathcal{D}_1}{\langle c_1\,, \sigma \rangle \to_1 \langle c_1'\,, \sigma' \rangle}}{\langle c_1\,; c_2\,, \sigma \rangle \to_1 \langle c_1'\,; c_2\,, \sigma' \rangle}\text{(S1)}$$

Applying the IH (with $\mathcal{D}_0 = \mathcal{D}_1 < \mathcal{D}$, $c_0 = c_1$, $\sigma_0 = \sigma$, $c_0' = c_1'$, $\sigma_0' = \sigma'$) implies $\mathcal{C}[\![c_1]\!]\sigma = \mathcal{C}[\![c_1']\!]\sigma'$. From the denotational definition of sequence, we conclude that $\mathcal{C}[\![c_1\,; c_2]\!]\sigma = \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma) = \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1']\!]\sigma') = \mathcal{C}[\![c_1'\,; c_2]\!]\sigma'$.

Other Cases

Optional exercise: Try some of the other cases on your own. Most are pretty feasible (no new lemmas needed other than semantic equivalence of expressions, which we already assumed).

The case for while-loops is challenging though!

Which Proof Approach?

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma \rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. ...

How do we approach this one? (No derivation in the assumptions to induct over!)

Setting Up the Induction

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \Longrightarrow \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

Danger: We might be in trouble when we hit the while loop, but let's proceed for now. What's the IH?

Setting Up the Induction

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma \rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$.

What does “smaller” ($c_0 < c$) mean for commands?

Same idea as derivations: Any reasonable metric will do, but we’ll just compare the heights of the ASTs.

Skip Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 1: Suppose $c = \texttt{skip}$.

Skip Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 1: If $c = \mathtt{skip}$ then $\sigma' = \mathcal{C}[\![c]\!]\sigma = \sigma$. Thus, we can derive

$$\frac{}{\langle c, \sigma\rangle \Downarrow \sigma'}\text{(L1)}$$

Sequence Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 2: Suppose $c = c_1\,;c_2$.

Sequence Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \Longrightarrow \langle c, \sigma \rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$.

Case 2: If $c = c_1 ; c_2$ then $\sigma' = \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c_1 ; c_2]\!]\sigma = \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma)$.

Sequence Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 2: If $c = c_1\,;c_2$ then $\sigma' = \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c_1\,;c_2]\!]\sigma = \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma)$.
The IH (with $c_0 = c_1 < c$, $\sigma_0 = \sigma$, $\sigma_0' = \mathcal{C}[\![c_1]\!]\sigma$) implies that $\langle c_1, \sigma\rangle \Downarrow \mathcal{C}[\![c_1]\!]\sigma$.

Sequence Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \Longrightarrow \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 2: If $c = c_1 ; c_2$ then $\sigma' = \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c_1 ; c_2]\!]\sigma = \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma)$.
The IH (with $c_0 = c_1 < c$, $\sigma_0 = \sigma$, $\sigma_0' = \mathcal{C}[\![c_1]\!]\sigma$) implies that $\langle c_1, \sigma\rangle \Downarrow \mathcal{C}[\![c_1]\!]\sigma$.
The IH (with $c_0 = c_2 < c$, $\sigma_0 = \mathcal{C}[\![c_1]\!]\sigma$, $\sigma_0' = \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma)$) implies that $\langle c_2, \mathcal{C}[\![c_1]\!]\sigma\rangle \Downarrow \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma)$.

Sequence Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 2: If $c = c_1 ; c_2$ then $\sigma' = \mathcal{C}[\![c]\!]\sigma = \mathcal{C}[\![c_1 ; c_2]\!]\sigma = \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma)$.
The IH (with $c_0 = c_1 < c$, $\sigma_0 = \sigma$, $\sigma_0' = \mathcal{C}[\![c_1]\!]\sigma$) implies that $\langle c_1, \sigma\rangle \Downarrow \mathcal{C}[\![c_1]\!]\sigma$.
The IH (with $c_0 = c_2 < c$, $\sigma_0 = \mathcal{C}[\![c_1]\!]\sigma$, $\sigma_0' = \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma)$) implies that
$\langle c_2, \mathcal{C}[\![c_1]\!]\sigma\rangle \Downarrow \mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma)$.
Since $\mathcal{C}[\![c_2]\!](\mathcal{C}[\![c_1]\!]\sigma) = \mathcal{C}[\![c_1 ; c_2]\!]\sigma$ (by the definition of $\mathcal{C}$), we can therefore derive:

$$\frac{\langle c_1, \sigma\rangle \Downarrow \mathcal{C}[\![c_1]\!]\sigma \qquad \langle c_2, \mathcal{C}[\![c_1]\!]\sigma\rangle \Downarrow \mathcal{C}[\![c_1 ; c_2]\!]\sigma}{\langle c_1 ; c_2, \sigma\rangle \Downarrow \mathcal{C}[\![c_1 ; c_2]\!]\sigma}\text{(L2)}$$

Other Cases

Lemma: (3)⇒(1)

$$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma \rangle \Downarrow \sigma'$$

Let's skip to the `while` case, since that's the dangerous one.

(Other cases left as exercise to the reader.)

While Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \Longrightarrow \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 6: If $c = \texttt{while}\ b\ \texttt{do}\ c_1$ then $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$.

We must now prove $\langle c, \sigma\rangle \Downarrow \mathit{fix}(\Gamma)\sigma$. How?

Hint: The theorem just became a property of a fixed point.

While Case

Lemma: (3)⇒(1)

$\mathcal{C}[\![c]\!]\sigma = \sigma' \implies \langle c, \sigma\rangle \Downarrow \sigma'$

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma'_0$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma'_0$.

Case 6: If $c = \texttt{while}\ b\ \texttt{do}\ c_1$ then $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$. Define property $P(f) \equiv \forall(\sigma, \sigma') \in f, \langle c, \sigma\rangle \Downarrow \sigma'$, and observe that $P(\mathcal{C}[\![c]\!])$ is the theorem statement. Since $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ we can prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

Fixed point induction to the rescue!

While Case

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0 \rangle \Downarrow \sigma_0'$.

Case 6: If $c = \texttt{while}\ b\ \texttt{do}\ c_1$ then $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$. Define property $P(f) \equiv \forall (\sigma, \sigma') \in f, \langle c, \sigma \rangle \Downarrow \sigma'$, and observe that $P(\mathcal{C}[\![c]\!])$ is the theorem statement. Since $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ we can prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

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

While Case

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH1: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 6: If $c = \texttt{while}\ b\ \texttt{do}\ c_1$ then $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$. Define property $P(f) \equiv \forall(\sigma, \sigma') \in f, \langle c, \sigma\rangle \Downarrow \sigma'$, and observe that $P(\mathcal{C}[\![c]\!])$ is the theorem statement. Since $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ we can prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

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

IH2: Assume $P(g)$ for some arbitrary g. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \langle c, \sigma_0\rangle \Downarrow \sigma_0'$.

Goal: Prove $P(\Gamma(g))$.

Practice Exercise: See if you can prove this on your own. (Solution on next two slides.)

While Case

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH1: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 6: If $c = \texttt{while}\ b\ \texttt{do}\ c_1$ then $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$. Define property $P(f) \equiv \forall(\sigma, \sigma') \in f, \langle c, \sigma\rangle \Downarrow \sigma'$, and observe that $P(\mathcal{C}[\![c]\!])$ is the theorem statement. Since $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ we can prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

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

IH2: Assume $P(g)$ for some arbitrary g. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \langle c, \sigma_0\rangle \Downarrow \sigma_0'$.

Inductive Case: Let $(\sigma, \sigma') \in \Gamma(g)$ be given.
Case 6.1: If $\mathcal{B}[\![b]\!]\sigma = F$ then $\sigma' = \sigma$ by definition of Γ. Since $\mathcal{B}[\![b]\!]\sigma = F$, the boolean semantic equivalence lemma implies that $\langle b, \sigma\rangle \Downarrow F$ is derivable. We can therefore derive:

$$\dfrac{\dfrac{\langle b, \sigma\rangle \Downarrow F \qquad \dfrac{}{\langle \texttt{skip}, \sigma\rangle \Downarrow \sigma'}\,\text{(L1)}}{\langle \texttt{if}\ b\ \texttt{then}\ (c_1\,;c)\ \texttt{else skip}, \sigma\rangle \Downarrow \sigma'}\,\text{(L5)}}{\langle c, \sigma\rangle \Downarrow \sigma'}\,\text{(L6)}$$

Case 6.2: If $\mathcal{B}[\![b]\!]\sigma = T$ then ... *(next slide)*

While Case

Proof

Assume $\mathcal{C}[\![c]\!]\sigma = \sigma'$. Proof is by structural induction over c.

IH1: Assume if $\mathcal{C}[\![c_0]\!]\sigma_0 = \sigma_0'$ and $c_0 < c$ then $\langle c_0, \sigma_0\rangle \Downarrow \sigma_0'$.

Case 6: If $c = \texttt{while}\ b\ \texttt{do}\ c_1$ then $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$. Define property $P(f) \equiv \forall(\sigma, \sigma') \in f, \langle c, \sigma\rangle \Downarrow \sigma'$, and observe that $P(\mathcal{C}[\![c]\!])$ is the theorem statement. Since $\mathcal{C}[\![c]\!] = \mathit{fix}(\Gamma)$ we can prove $P(\mathcal{C}[\![c]\!])$ by fixed point induction over Γ.

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

IH2: Assume $P(g)$ for some arbitrary g. That is, assume $\forall(\sigma_0, \sigma_0') \in g, \langle c, \sigma_0\rangle \Downarrow \sigma_0'$.

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

Case 6.1: If $\mathcal{B}[\![b]\!]\sigma = F$ then ... *(previous slide)*

Case 6.2: If $\mathcal{B}[\![b]\!]\sigma = T$ then $\sigma' = g(\mathcal{C}[\![c_1]\!]\sigma)$ by definition of Γ. Since $\mathcal{B}[\![b]\!]\sigma = T$, the boolean semantic equivalence lemma implies that $\langle b, \sigma\rangle \Downarrow T$ is derivable. From IH1 (with $c_0 = c_1 < c$, $\sigma_0 = \sigma$) we have $\langle c_1, \sigma\rangle \Downarrow \mathcal{C}[\![c_1]\!]\sigma$. From IH2, $(\mathcal{C}[\![c_1]\!]\sigma, \sigma') \in g$ implies $\langle c, \mathcal{C}[\![c_1]\!]\sigma\rangle \Downarrow \sigma'$. This allows us to derive

$$\dfrac{\dfrac{\langle b, \sigma\rangle \Downarrow T \qquad \dfrac{\langle c_1, \sigma\rangle \Downarrow \mathcal{C}[\![c_1]\!]\sigma \quad \langle c, \mathcal{C}[\![c_1]\!]\sigma\rangle \Downarrow \sigma'}{\langle c_1 ; c, \sigma\rangle \Downarrow \sigma'}\text{(L2)}}{\langle \texttt{if}\ b\ \texttt{then}\ (c_1 ; c)\ \texttt{else skip}, \sigma\rangle \Downarrow \sigma'}\text{(L4)}}{\langle c, \sigma\rangle \Downarrow \sigma'}\text{(L6)}$$

□

Large Proofs

- This was/is a huge proof even for a small language.
  - We didn't even prove equivalence of arithmetic and boolean expression semantics (must prove (1)⇒(2), (2)⇒(3), and (3)⇒(1) for each!).
  - And we skipped many cases just for commands.
- Good news: If you want to practice structural induction, try some of the (many, many) cases we left out!
- Bad news: How can we trust a proof this large? What if there's a mistake?
  - Modern language designers don't write proofs like this by hand. They use **Automated Theorem Provers**.
  - (But we'll stick with writing them manually in this class, because that teaches the foundational skills you need to do it in a theorem prover.)