CSE 505, Fall 2003, Lecture 5 Proofs

Dan Grossman

Note: The proofs for Theorems 1–4 assume our language is deterministic. That is, we're really proving only one direction of the "if and only if" nature of equivalence. You can prove the other direction on your own.

Theorem 1: Informally, $e*4$ can be replaced with $(e+(e+e))+e$. Formally, for all H and e, if $H\ ;\ e * 4 \Downarrow c$, then $H\ ;\ (e+(e+e))+e \Downarrow c$.

Proof: The derivation of $H\ ;\ e * 4 \Downarrow c$ must end with the Times rule:

$$\frac{H\ ;\ e \Downarrow c' \qquad H\ ;\ 4 \Downarrow 4}{H\ ;\ e * 4 \Downarrow c}$$

where c' is one fourth of c. In particular, we know there exists a derivation of $H\ ;\ e \Downarrow c'$. Therefore, we can derive:

$$\frac{\dfrac{H\ ;\ e \Downarrow c' \qquad \dfrac{H\ ;\ e \Downarrow c' \qquad H\ ;\ e \Downarrow c'}{H\ ;\ e+e \Downarrow c'+c'}}{H\ ;\ e+(e+e) \Downarrow c'+c'+c'} \qquad H\ ;\ e \Downarrow c'}{H\ ;\ (e+(e+e))+e \Downarrow c'+c'+c'+c'}$$

Recall the + characters in the conclusion of the Plus rule are the mathetical plus. So the result of the derivation is c. (Note: The other direction—if $H\ ;\ (e+(e+e))+e \Downarrow c$ then $H\ ;\ e*4 \Downarrow c$—is basically this argument backwards.)

Theorem 2: Informally, if 1 s_1 s_2 is equivalent to s_1. Formally, for all H, s_1, and s_2:

(a) For all n, if $H\ ;\ \mathsf{if}\ 1\ s_1\ s_2 \rightarrow^n H'\ ;\ \mathsf{skip}$, then there exist H'' and n' such that $H\ ;\ s_1 \rightarrow^{n'} H''\ ;\ \mathsf{skip}$ and $H''(ans) = H'(ans)$.

(b) If for all n there exist H' and s' such that $H\ ;\ \mathsf{if}\ 1\ s_1\ s_2 \rightarrow^n H'\ ;\ s'$, then for all n there exist H'' and s'' such that $H\ ;\ s_1 \rightarrow^n H''\ ;\ s''$.

Lemma: For all H, s_1, s_2, and $n \geq 1$, if $H\ ;\ \mathsf{if}\ 1\ s_1\ s_2 \rightarrow^n H'\ ;\ s'$, then $H\ ;\ s_1 \rightarrow^{n-1} H'\ ;\ s'$.
Lemma implies theorem:

(a) For $n \geq 1$, it's stronger (true for any s' not just skip and uses H' and $n-1$ for H'' and n'). The case $n = 0$ is impossible because if 1 s_1 s_2 is not skip.

(b) Assume the lemma and for all n there exist H' and s' such that $H\ ;\ \mathsf{if}\ 1\ s_1\ s_2 \rightarrow^n H'\ ;\ s'$. Then to show the conclusion of part (b), just use the lemma with $n+1$.

Proof of the lemma: By induction on n. For the base case, $n = 1$, i.e., $H\ ;\ \mathsf{if}\ 1\ s_1\ s_2 \rightarrow H'\ ;\ s'$. Only rule If1 applies, so H' is H and s' is s_1. So we need $H\ ;\ s_1 \rightarrow^0 H\ ;\ s_1$, which is immediate. For the inductive case, $n > 1$, i.e., $H\ ;\ \mathsf{if}\ 1\ s_1\ s_2 \rightarrow^n H'\ ;\ s'$. That means $H\ ;\ \mathsf{if}\ 1\ s_1\ s_2 \rightarrow^{n-1} H''\ ;\ s''$ and $H''\ ;\ s'' \rightarrow H'\ ;\ s'$ for some H'' and s''. Because $n-1 < n$, induction ensures $H\ ;\ s_1 \rightarrow^{n-2} H''\ ;\ s''$. With that and $H''\ ;\ s'' \rightarrow H'\ ;\ s'$, we get $H\ ;\ s_1 \rightarrow^{n-1} H'\ ;\ s'$.

Theorem 3: Informally, the statement-sequence operator is associative. Formally, for all H, s_1, s_2, and s_3:

(a) For all n, if $H\ ;\ s_1; (s_2; s_3) \rightarrow^n H'\ ;\ \mathsf{skip}$ then there exist H' and n' such that $H\ ;\ (s_1; s_2); s_3 \rightarrow^{n'} H''\ ;\ \mathsf{skip}$ and $H''(ans) = H'(ans)$.

(b) If for all n there exist H' and s' such that $H\ ;\ s_1; (s_2; s_3) \rightarrow^n H'\ ;\ s'$, then for all n there exist H'' and s'' such that $H\ ;\ (s_1; s_2); s_3 \rightarrow^n H''\ ;\ s''$.

Lemma For all n, if $H \;;\; s_1; (s_2; s_3) \;\rightarrow^n\; H' \;;\; s'$, then either (1) s' has the form $s_1'; (s_2; s_3)$ and $H \;;\; (s_1; s_2); s_3 \;\rightarrow^n\; H' \;;\; (s_1'; s_2); s_3$ or (2) $H \;;\; (s_1; s_2); s_3 \;\rightarrow^n\; H' \;;\; s'$.

Lemma implies theorem: It's stronger because if s' is skip, then only (2) applies and we have $H'' = H'$ and $n' = n$.

Proof of the lemma: By induction on n. For the base case $n = 0$, so (1) holds with $s_1' = s_1$. For the inductive case $n > 0$, so $H \;;\; s_1; (s_2; s_3) \;\rightarrow^n\; H' \;;\; s'$, which means $H \;;\; s_1; (s_2; s_3) \;\rightarrow^{n-1}\; H'' \;;\; s''$ and $H'' \;;\; s'' \rightarrow H' \;;\; s'$ for some H'' and s''. So by induction either (1) s'' has the form $s_1''; (s_2; s_3)$ and $H \;;\; (s_1; s_2); s_3 \;\rightarrow^{n-1}\; H'' \;;\; (s_1''; s_2); s_3$ or (2) $H \;;\; (s_1; s_2); s_3 \;\rightarrow^{n-1}\; H'' \;;\; s''$.

If (1), then the derivation of $H'' \;;\; s'' \rightarrow H' \;;\; s'$ ends with either Seq1 or Seq2. If Seq1, then H'' is H', s_1'' is skip and s' is $s_2; s_3$. Furthermore, we can derive:

$$\frac{H'' \;;\; \mathsf{skip}; s_2 \rightarrow H'' \;;\; s_2}{H'' \;;\; (\mathsf{skip}; s_2); s_3 \rightarrow H'' \;;\; s_2; s_3}$$

So (2) holds. If Seq2, then the derivation of $H'' \;;\; s'' \rightarrow H' \;;\; s'$ must have the form:

$$\frac{H'' \;;\; s_1'' \rightarrow H' \;;\; s_1'}{H'' \;;\; s_1''; (s_2; s_3) \rightarrow H' \;;\; s_1'; (s_2; s_3)}$$

So there must be a derivation of $H'' \;;\; s_1'' \rightarrow H' \;;\; s_1'$. So we can derive:

$$\frac{\dfrac{H'' \;;\; s_1'' \rightarrow H' \;;\; s_1'}{H'' \;;\; s_1''; s_2 \rightarrow H' \;;\; s_1'; s_2}}{H'' \;;\; (s_1''; s_2); s_3 \rightarrow H' \;;\; (s_1'; s_2); s_3}$$

So (1) holds.

If (2), then $H'' \;;\; s'' \rightarrow H' \;;\; s'$ ensures $H \;;\; (s_1; s_2); s_3 \rightarrow H' \;;\; s'$, so (2) holds.

Theorem 4: Informally, the semantics with the rule

$$\frac{}{H \;;\; x := x; s \rightarrow H \;;\; s}$$

is equivalent to the semantics without it. More formally, if $H \;;\; s \rightarrow^* H' \;;\; \mathsf{skip}$ with the rule, then $H \;;\; s \rightarrow^* H'' \;;\; \mathsf{skip}$ without it (and vice-versa!) for some H'' such that $H''(ans) = H'(ans)$. (We'll skip termination equivalence for this one, though it's not hard.)

Proof (sketch): It is trivial to show that if $H \;;\; s \rightarrow^* H'' \;;\; \mathsf{skip}$ without the rule then $H \;;\; s \rightarrow^* H'' \;;\; \mathsf{skip}$ with the rule because we never "have to" use the rule.

For the other direction, the interesting lemma is: If $H_1 \;;\; s \rightarrow H_2 \;;\; s'$ with the new rule and $H_1(x) = H_3(x)$ for all x then $H_3 \;;\; s \rightarrow^* H_4 \;;\; s'$ without the new rule and $H_2(x) = H_4(x)$ for all x. The proof of the lemma is by induction on the derivation of $H \;;\; s \rightarrow H' \;;\; s'$, proceeding by cases on the last rule used in the derivation. Several cases use this auxiliary lemma (prove it!): If $H(x) = H'(x)$ for all x, then $H \;;\; e \Downarrow c$ if and only if $H' \;;\; e \Downarrow c$. Here are the cases:

Seq1: s has the form $\mathsf{skip}; s''$ and we have a derivation of $H_1 \;;\; \mathsf{skip}; s'' \rightarrow H_1 \;;\; s''$. We can also use Seq1 to derive $H_3 \;;\; \mathsf{skip}; s'' \rightarrow H_3 \;;\; s''$ and we already know H_1 and H_3 agree on all variables.

While: Just like the Seq1 case except s and s' have different forms.

If1: s has the form $\mathsf{if}\; e\; s_1\; s_2$ and our derivation ensures s' is s_1, H_2 is H_1, and $H_1 \;;\; e \Downarrow c$ for some $c > 0$. Our auxiliary lemma ensures $H_3 \;;\; e \Downarrow c$, so we can use If1 to derive $H_3 \;;\; \mathsf{if}\; e\; s_1\; s_2 \rightarrow H_3 \;;\; s_1$ and we already know H_1 and H_3 agree on all variables.

If2: Analogous to the previous case.

Assign: s has the form $x := e$, H_2 is $H_1, x \mapsto c$, s' is skip and $H_1 \;;\; e \Downarrow c$. Our auxiliary lemma ensures $H_3 \;;\; e \Downarrow c$. So we can use Assign to derive $H_3 \;;\; s \rightarrow H_3, x \mapsto c \;;\; \mathsf{skip}$. So we just need that $H_1, x \mapsto c$ and $H_3, x \mapsto c$ return the same constant for all variables. This is easy to show with the two cases of x and $y \neq x$.

Seq2: s has the form $s_1; s_2$ and s' has the form $s_1'; s_2$ and $H_1 \;;\; s_1 \rightarrow H_2 \;;\; s_1'$ with the new rule. So by induction, $H_3 \;;\; s_1 \rightarrow^* H_4 \;;\; s_1'$ without the new rule and H_3,H_4 agree on all variables. So using the Seq Lemma we proved in class, $H_3 \;;\; s_1; s_2 \rightarrow^* H_4 \;;\; s_1'; s_2$ without the new rule.

"New Rule": s has the form $x := x; s'$ and $H_2 = H_1$. Without the new rule, we can use Seq2, Assign, and Seq1 to derive $H_3 \;;\; x := x; s' \;\rightarrow^2\; H_3, x \mapsto H_3(x) \;;\; s'$ (prove it!). So we just need that H_3 and $H_3, x \mapsto H_3(x)$ are the same for all variables, which is easy to show.

Theorem 5: Our large-step semantics for expressions is equivalent to this small-step semantics (omitting multiplication and using the math plus in the result of the second rule):

$$\frac{}{H;\, x \rightarrow H(x)} \qquad \frac{}{H;\, c_1 + c_2 \rightarrow c_1{+}c_2} \qquad \frac{H;\, e_1 \rightarrow e_1'}{H;\, e_1 + e_2 \rightarrow e_1' + e_2} \qquad \frac{H;\, e_2 \rightarrow e_2'}{H;\, e_1 + e_2 \rightarrow e_1 + e_2'}$$

Formally, $H \;;\; e \Downarrow c$ if and only if $H;\, e \rightarrow^* c$.

Proof: We prove the two directions separately. First assume $H \;;\; e \Downarrow c$. We need this lemma (prove it!): If $H;\, e \rightarrow^n e'$, then $H;\, e_1 + e \rightarrow^n e_1 + e'$ and $H;\, e + e_2 \rightarrow^n e' + e_2$. Given the lemma, the proof is by induction on the derivation of $H \;;\; e \Downarrow c$, proceeding by cases on the last rule used in the derivation:

- Const: In this case $H;\, e \rightarrow^0 c$.
- Var: In this case $H;\, e \rightarrow^1 c$.
- Plus: In this case, we know e has the form $e_1 + e_2$, $H \;;\; e_1 \Downarrow c_1$, $H \;;\; e_2 \Downarrow c_2$, and c is the sum of c_1 and c_2. By induction $H;\, e_1 \rightarrow^{n_1} c_1$ and $H;\, e_2 \rightarrow^{n_2} c_2$ for some n_1 and n_2. So our lemma ensures $H;\, e_1 + e_2 \rightarrow^{n_1} c_1 + e_2$ and $H;\, c_1 + e_2 \rightarrow^{n_2} c_1 + c_2$. Therefore, using the small-step rule for adding constants, we can derive $H;\, e_1 + e_2 \rightarrow^{n_1+n_2+1} c$.

Now assume $H;\, e \rightarrow^n c$ for some n. We prove $H \;;\; e \Downarrow c$ by induction on n. For $n = 0$, e is c and the Const rule lets us derive $H \;;\; c \Downarrow c$. For $n > 0$, there exists an e' such that $H;\, e \rightarrow e'$ and $H;\, e' \rightarrow^{n-1} c$. By induction $H \;;\; e' \Downarrow c$. So the following lemma suffices: If $H;\, e \rightarrow e'$ and $H \;;\; e' \Downarrow c$, then $H \;;\; e \Downarrow c$. We prove the lemma by induction on the derivation of $H;\, e \rightarrow e'$, proceeding by cases on the last rule used in the derivation:

- If e is some x, then e' and c are $H(x)$. Using Var, we can derive $H \;;\; x \Downarrow H(x)$.
- If e has the form $c_1 + c_2$, then e' and c are the sum of c_1 and c_2. Using Plus lets us derive the result.
- If e has the form $e_1 + e_2$ and e' has the form $e_1' + e_2$, then the assumed derivations end like this:

  $$\frac{H;\, e_1 \rightarrow e_1'}{H;\, e_1 + e_2 \rightarrow e_1' + e_2} \qquad\qquad \frac{H \;;\; e_1' \Downarrow c_1 \qquad H \;;\; e_2 \Downarrow c_2}{H \;;\; e_1' + e_2 \Downarrow c_1{+}c_2}$$

  Using $H;\, e_1 \rightarrow e_1'$, $H \;;\; e_1' \Downarrow c_1$, and the induction hypothesis, $H \;;\; e_1 \Downarrow c_1$. Using this fact, $H \;;\; e_2 \Downarrow c_2$, and the Plus rule, we can derive $H \;;\; e_1 + e_2 \Downarrow c_1{+}c_2$.
- If e has the form $e_1 + e_2$ and e' has the form $e_1 + e_2'$, the argument is analogous to the previous case (prove it!).