CSE505, Lecture 5 Supplement, Fall 2005
Dan Grossman

By popular demand, here are proofs for theorems only sketched in the lecture-5 slides. (The equivalence proof for small-step and large-step expression semantics is complete enough in the slides I think. I wrote these very quickly, so corrections are welcome.

Theorem: $H \ ; e * 2 \Downarrow c$ if and only if $H \ ; e + e \Downarrow c$.
Proof: (Does not use induction)

- First assume $H \ ; e * 2 \Downarrow c$ and show $H \ ; e + e \Downarrow c$. Any derivation of $H \ ; e * 2 \Downarrow c$ must end with the MULT rule, which means there must exist derivations of $H \ ; e \Downarrow c'$ and $H \ ; 2 \Downarrow 2$, and c must be $2c'$. That is, there must be a derivation that looks like this:

$$\dfrac{\dfrac{\vdots}{H \ ; e \Downarrow c'} \qquad \dfrac{}{H \ ; 2 \Downarrow 2}}{H \ ; e * 2 \Downarrow 2c'}$$

  So given that there exists a derivation of $H \ ; e \Downarrow c'$, we can use ADD to derive:

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

  Math provides $c' + c' = 2c'$, so the conclusion of this derivation is what we need.

- Now assume $H \ ; e + e \Downarrow c$ and show $H \ ; e * 2 \Downarrow c$. Any derivation of $H \ ; e + e \Downarrow c$ must end with the ADD rule, which means there exists a derivation that looks like this (where $c = c_1 + c_2$):

$$\dfrac{\dfrac{\vdots}{H \ ; e \Downarrow c_1} \qquad \dfrac{\vdots}{H \ ; e \Downarrow c_2}}{H \ ; e + e \Downarrow c_1 + c_2}$$

  In fact, we earlier proved determinacy (there is at most one c such that $H \ ; e \Downarrow c$), so the derivation must have this form (where $c = c_1 + c_1$):

$$\dfrac{\dfrac{\vdots}{H \ ; e \Downarrow c_1} \qquad \dfrac{\vdots}{H \ ; e \Downarrow c_1}}{H \ ; e + e \Downarrow c_1 + c_1}$$

  So given that there exists a derivation of $H \ ; e \Downarrow c_1$, we can use MULT to derive:

$$\dfrac{H \ ; e \Downarrow c_1 \qquad \dfrac{}{H \ ; 2 \Downarrow 2}}{H \ ; e * 2 \Downarrow 2c_1}$$

  Math provides $c_1 + c_1 = 2c_1$, so the conclusion of this derivation is what we need.

$$C ::= [\cdot] \mid C + e \mid e + C \mid C * e \mid e * C$$

Formal definition of "filling the hole":

$$\begin{array}{rcl} ([\cdot])[e] & = & e \\ (C + e_1)[e] & = & C[e] + e_1 \\ (e_1 + C)[e] & = & e_1 + C[e] \\ (C * e_1)[e] & = & C[e] * e_1 \\ (e_1 * C)[e] & = & e_1 * C[e] \end{array}$$

Theorem: $H \; ; \; C[e * 2] \Downarrow c$ if and only if $H \; ; \; C[e + e] \Downarrow c$.
Proof: By induction on (the height of) the structure of C:

- If the height is 1, then C is $[\cdot]$, so $C[e * 2] = e * 2$ and $C[e + e] = e + e$. So the previous theorem is exactly what we need.
- If the height is greater than 1, then C has one of four forms:
  - If C is $C' + e'$ for some C' and e', then $C[e * 2]$ is $C'[e * 2] + e'$ and $C[e + e]$ is $C'[e + e] + e'$. Since C' is shorter than C, induction ensures that for any constant c', $H \; ; \; C'[e * 2] \Downarrow c'$ if and only if $H \; ; \; C'[e + e] \Downarrow c'$.

    Assume $H \; ; \; C'[e * 2] + e' \Downarrow c$ and show $H \; ; \; C'[e + e] + e' \Downarrow c$: Any derivation of $H \; ; \; C'[e * 2] + e' \Downarrow c$ must end with ADD, i.e., it looks like this (where $c = c' + c''$):

    $$\dfrac{\dfrac{\vdots}{H \; ; \; C'[e * 2] \Downarrow c'} \qquad \dfrac{\vdots}{H \; ; \; e' \Downarrow c''}}{H \; ; \; C'[e * 2] + e' \Downarrow c}$$

    As argued above, the existence of a derivation of $H \; ; \; C'[e * 2] \Downarrow c'$ ensures the existence of a derivation of $H \; ; \; C'[e + e] \Downarrow c'$. So using ADD and the existence of a derivation of $H \; ; \; e' \Downarrow c''$, we can derive:

    $$\dfrac{H \; ; \; C'[e + e] \Downarrow c' \qquad H \; ; \; e' \Downarrow c''}{H \; ; \; C'[e + 2] + e' \Downarrow c}$$

    Now assume $H \; ; \; C'[e + e] + e' \Downarrow c$ and show $H \; ; \; C'[e * 2] + e' \Downarrow c$: Any derivation of $H \; ; \; C'[e + 2] + e' \Downarrow c$ must end with ADD, i.e., it looks like this (where $c = c' + c''$):

    $$\dfrac{\dfrac{\vdots}{H \; ; \; C'[e + e] \Downarrow c'} \qquad \dfrac{\vdots}{H \; ; \; e' \Downarrow c''}}{H \; ; \; C'[e + 2] + e' \Downarrow c}$$

    As argued above, the existence of a derivation of $H \; ; \; C'[e + e] \Downarrow c'$ ensures the existence of a derivation of $H \; ; \; C'[e * 2] \Downarrow c'$. So using ADD and the existence of a derivation of $H \; ; \; e' \Downarrow c''$, we can derive:

    $$\dfrac{H \; ; \; C'[e * 2] \Downarrow c' \qquad H \; ; \; e' \Downarrow c''}{H \; ; \; C'[e * 2] + e' \Downarrow c}$$

  - The other 3 cases are similar. (Try them out.)

Theorem: Informally, the statement-sequence operator is associative. Formally:

(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.