CSE505, Lecture 5 Supplement, Fall 2006
Dan Grossman

In class we sketched several proofs but Dan's handwriting is bad and there were probably typos as we went along. Here are the proofs more carefully laid out, as one might do on a homework assignment. There may still be bugs; 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:

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

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

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

    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.

Theorem: The two semantics below are equivalent, i.e., $H\ ;\ e \Downarrow c$ if and only if $H;\ e \to^* c$.

$$\frac{}{H\ ;\ c \Downarrow c}\ \textsc{const} \qquad \frac{}{H\ ;\ x \Downarrow H(x)}\ \textsc{var} \qquad \frac{H\ ;\ e_1 \Downarrow c_1 \qquad H\ ;\ e_2 \Downarrow c_2}{H\ ;\ e_1 + e_2 \Downarrow c_1{+}c_2}\ \textsc{add}$$

$$\frac{}{H;\ x \to H(x)}\ \textsc{svar} \qquad \frac{}{H;\ c_1 + c_2 \to c_1{+}c_2}\ \textsc{sadd} \qquad \frac{H;\ e_1 \to e_1'}{H;\ e_1 + e_2 \to e_1' + e_2}\ \textsc{sleft} \qquad \frac{H;\ e_2 \to e_2'}{H;\ e_1 + e_2 \to e_1 + e_2'}\ \textsc{sright}$$

Proof: We prove the two directions separately.
First assume $H\ ;\ e \Downarrow c$; show $\exists n.\ H;\ e \to^n c$. By induction on the height h of derivation of $H\ ;\ e \Downarrow c$:

- $h = 1$: Then the derivation must end with CONST or VAR. For CONST, e is c and trivially $H;\ e \to^0 c$. For VAR, e is some x where $H(x) = c$, so using SVAR, $H;\ e \to^1 c$.
- $h > 1$: Then the derivation must end with ADD, so e is some $e_1 + e_2$ where $H\ ;\ e_1 \Downarrow c_1$, $H\ ;\ e_2 \Downarrow c_2$, and c is $c_1{+}c_2$. By induction $\exists n_1, n_2.\ H;\ e_1 \to^{n_1} c_1$ and $H;\ e_2 \to^{n_2} c_2$. Therefore, using the lemma below, $H;\ e_1 + e_2 \to^{n_1} c_1 + e_2$ and $H;\ c_1 + e_2 \to^{n_2} c_1 + c_2$, so ADD lets us derive $H;\ e_1 + e_2 \to^{n_1+n_2+1} c$.

Lemma: If $H;\ e \to^n e'$, then $H;\ e_1 + e \to^n e_1 + e'$ and $H;\ e + e_2 \to^n e' + e_2$.

Proof: By induction on n. If $n = 0$, the result is trivial because $e = e_1 = e_2$. If $n > 0$, then there exists some e'' such that $H;\ e \to^{n-1} e''$ and $H;\ e'' \to^1 e'$. So by induction $H;\ e_1 + e \to^{n-1} e_1 + e''$ and $H;\ e + e_2 \to^{n-1} e'' + e_2$. So using SLEFT and SRIGHT respectively, $H;\ e_1 + e \to^n e_1 + e'$ and $H;\ e + e_2 \to^n e' + e_2$.

Now assume $\exists n.\ H;\ e \to^n c$; show $H\ ;\ e \Downarrow c$. By induction on n:

- $n = 0$: e is c and CONST lets us derive $H\ ;\ c \Downarrow c$.
- $n > 0$: So $\exists e'.\ H;\ e \to e'$ and $H;\ e' \to^{n-1} c$. By induction $H\ ;\ e' \Downarrow c$. So this lemma suffices: If $H;\ e \to e'$ and $H\ ;\ e' \Downarrow c$, then $H\ ;\ e \Downarrow c$. Prove the lemma by induction on height h of derivation of $H;\ e \to e'$:
  - $h = 1$: Then the derivation ends with SVAR or SADD. For SVAR, e is some x and $e' = H(x) = c$. So with VAR we can derive $H\ ;\ x \Downarrow H(x)$, i.e., $H\ ;\ e \Downarrow c$. For SADD, e is some $c_1 + c_2$ and $e' = c = c_1{+}c_2$. Wo with ADD, we can derive $H\ ;\ c_1 + c_2 \Downarrow c_1{+}c_2$, i.e., $H\ ;\ e \Downarrow c$.
  - $h > 1$: Then the derivation ends with SLEFT or SRIGHT. For SLEFT, the assumed derivations ends like this:

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

    Using $H;\ e_1 \to e_1'$, $H\ ;\ e_1' \Downarrow c_1$, and the induction hypothesis, $H\ ;\ e_1 \Downarrow c_1$. Using this fact, $H\ ;\ e_2 \Downarrow c_2$, and ADD, we can derive $H\ ;\ e_1 + e_2 \Downarrow c_1{+}c_2$.

    For SRIGHT, the assumed derivations ends like this:

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

    Using $H;\ e_2 \to e_2'$, $H\ ;\ e_2' \Downarrow c_2$, and the induction hypothesis, $H\ ;\ e_2 \Downarrow c_2$. Using this fact, $H\ ;\ e_1 \Downarrow c_1$, and ADD, we can derive $H\ ;\ e_1 + e_2 \Downarrow c_1{+}c_2$.