1.

1999 CST Part IB Semantics of Prog. Langs., paper 5, q 9 AMP

The relation $C, s \Downarrow s'$ is inductively defined by the following axioms and rules:

1 (1) $\quad \mathrm{skip}, s \Downarrow s$

2 (2) $\quad \ell := E, s \Downarrow s[\ell \mapsto n] \quad$ if $\; E, s \Downarrow n$

where $s[\ell \mapsto n]$ is the state s' with $\mathrm{dom}(s') = \mathrm{dom}(s) \cup \{\ell\}$ and for all $\ell' \in \mathrm{dom}(s')$

$$s'(\ell') = \begin{cases} n & \text{if } \ell' = \ell \\ s(\ell') & \text{otherwise.} \end{cases}$$

1 (3)
$$\frac{C_1, s \Downarrow s' \qquad C_2, s' \Downarrow s''}{C_1 ; C_2, s \Downarrow s''}$$

(4)
$$\frac{C_1, s \Downarrow s'}{\mathrm{if}\ B\ \mathrm{then}\ C_1\ \mathrm{else}\ C_2, s \Downarrow s'} \quad \text{if } B, s \Downarrow \mathrm{true}$$

1

(5)
$$\frac{C_2, s \Downarrow s'}{\mathrm{if}\ B\ \mathrm{then}\ C_1\ \mathrm{else}\ C_2, s \Downarrow s'} \quad \text{if } B, s \Downarrow \mathrm{false}$$

1 (6)
$$\frac{C, s \Downarrow s' \qquad \mathrm{while}\ B\ \mathrm{do}\ C, s' \Downarrow s''}{\mathrm{while}\ B\ \mathrm{do}\ C, s \Downarrow s''} \quad \text{if } B, s \Downarrow \mathrm{true}$$

1 (7) $\quad \mathrm{while}\ B\ \mathrm{do}\ C, s \Downarrow s \quad$ if $\; B, s \Downarrow \mathrm{false}$

3 (8)
$$\frac{C[\ell'/\ell], s[\ell' \mapsto n] \Downarrow s'[\ell' \mapsto n']}{\mathrm{begin}\ \mathrm{loc}\ \ell := E ; C\ \mathrm{end}, s \Downarrow s'} \quad \text{if } E, s \Downarrow n$$

and $\ell' \notin \mathrm{dom}(s) \cup \mathrm{dom}(s') \cup \mathrm{loc}(E)$

where $C[\ell'/\ell]$ means C with all occurrences of ℓ replaced by ℓ'.

<u>Claim</u>: $\ell := 0;\ \text{begin loc}\ \ell := 1;\ \text{skip end},\ s \Downarrow s[\ell \mapsto 0]$

For

(9) $\ell := 0, s \Downarrow s[\ell \mapsto 0]$ by (2) [assuming $0, s \Downarrow 0$]

and since $\text{skip}[\ell'/\ell] = \text{skip}$, by (1) we have

2 $\text{skip}[\ell'/\ell], s[\ell \mapsto 0][\ell' \mapsto 1] \Downarrow s[\ell \mapsto 0][\ell' \mapsto 1]$

so by (8)

(10) $\text{begin loc}\ \ell := 1;\ \text{skip end},\ s[\ell \mapsto 0] \Downarrow s[\ell \mapsto 0]$

12 Finally (3) on (9)+(10) yields the desired conclusion.

Two commands are <u>semantically equivalent</u>, $C \cong C'$, if for all states s, s'

1 $$C, s \Downarrow s' \iff C', s \Downarrow s'.$$

Suppose $\ell' \neq \ell$ and that

(11) $\text{begin loc}\ \ell := E;\ \ell' := !\ell\ \text{end},\ s \Downarrow s'$

holds. This can only have been proved by an application of (8) to

$$(\ell' := !\ell)[\ell''/\ell], s[\ell'' \mapsto n] \Downarrow s'[\ell'' \mapsto n']$$

i.e. to

(12) $\ell' := !\ell'', s[\ell'' \mapsto n] \Downarrow s'[\ell'' \mapsto n']$

where $E, s \Downarrow n$.

Now (12) could only have been proved by (2), so $n' = n$ and $s' = s[\ell' \mapsto n]$. Hence by (2) again

(13) $\ell' := E, s \Downarrow s'$

holds. Conversely, if (13) does hold, it was proved by (2), so $E, s \Downarrow n$ for some n and $s' = s[\ell' \mapsto n]$.

In that case (12) also holds by (2) (with $n'=n$) and then (8) on (12) yields (11).
Thus we have proved (11) $\Leftrightarrow$ (13) for all s, s'.
4 Therefore (begin loc $\ell := E$; $\ell' := !\ell$ end) $\cong$ ($\ell' := E$).

If $\ell' = \ell$, then

1 $$\text{begin loc } \ell := E;\ \ell := !\ell \text{ end} \not\cong \ell := E.$$

for example, taking $E = 1$, we can calculate that

$$\text{begin loc } \ell := 0;\ \ell := !\ell \text{ end}, \{\ell \mapsto 0\} \Downarrow \{\ell \mapsto 0\}$$

whereas

$$\ell := 1, \{\ell \mapsto 0\} \Downarrow \{\ell \mapsto 1\}.$$

Contrary to what one might expect, the above definition of semantic equivalence means that when $\ell \notin loc(C)$, begin loc $\ell := E$; C end is
2 <u>not</u> necessarily $\cong$ to C. The problem is that evaluation of E may not yield a result.
For example, with

$$E = !\ell \quad , \quad s = \{\ell' \mapsto 0\} \ , \ \ell' \neq \ell$$

we have $E, s \not\Downarrow n$ for any n;
so begin loc $\ell := E$; C end, $s \not\Downarrow s'$ for any s'
whereas we may well have

$$C, s \Downarrow s'$$

8 (e.g. when $C = \text{Skip}$ and $s = s'$).