Exercise sheet 5

CS242 Formal Specification and Verification

Autumn term 2006

4.3.5 Use the proof rule for assignment and logical implication as appropriate to show the validity of

(a) $\vdash_{\mathsf{par}} (\!|x > 0|\!)\ \mathtt{y} = \mathtt{x} + \mathtt{1}\ (\!|y > 1|\!)$

(c) $\vdash_{\mathsf{par}} (\!|x > 1|\!)\ \mathtt{a} = \mathtt{1}; \mathtt{y} = \mathtt{x}; \mathtt{y} = \mathtt{y} - \mathtt{a}\ (\!|y > 0 \wedge x > y|\!)$

4.3.10 Prove the validity of the sequent $\vdash_{\mathsf{par}} (\!|\top|\!)\ P\ (\!|z = \min(x, y)|\!)$, where $\min(x, y)$ is the smallest number of x and y and the code of P is given by

```
if (x > y) {
   z = y;
} else {
   z = x;
}
```

4.3.11 For each of the specifications below, write code for P and prove the partial correctness of the specified input/output behaviour:

(a) $(\!|\top|\!)\ P\ (\!|z = \max(w, x, y)|\!)$, where $\max(w, x, y)$ denotes the largest of w, x and y.

(b) $(\!|\top|\!)\ P\ (\!|(x = 5 \rightarrow y = 3) \wedge (x = 3 \rightarrow y = -1)|\!)$.

4.3.14 Show that $\vdash_{\mathsf{par}} (\!|y \geq 0|\!)\ \mathtt{Multi1}\ (\!|z = x \cdot y|\!)$ is valid, where `Multi1` is:

```
a = 0;
z = 0;
while (a != y) {
  z = z + x;
  a = a + 1;
}
```

4.4.1 Prove the validity of the following total-correctness sequent:

(b) $\vdash_{\mathsf{tot}} (\!|y \geq 0|\!)\ \mathtt{Multi1}\ (\!|z = x \cdot y|\!)$