How to typeset verification problems

Gernot Salzer

May 6, 2011

This document explains how to typeset verification problems when solving the exercises for the course "Formal Methods in Computer Science".

1 Annotation calculus

The LaTeX code in the left column produces the output shown in the right column.

```
\documentclass{scrartcl}
\usepackage{fvsw}
\begin{document}
\begin{ALG}
\ASSERT F\\                                          { F }
\ASSERTN1\INV                          \quad(wh)\\   { 1: Inv }  (wh)
\WHILE\ $e$ \DO\\                                    while e do
\>\ASSERTN2{\INV\land e}               \quad(wh)\\     { 2: Inv ∧ e }  (wh)
\>\IF\ $e'$ \THEN\\                                    if e' then
\>\>\ASSERTN6{\INV\land e\land e'}     \quad(if)$\da$\\  { 6: Inv ∧ e ∧ e' }  (if)↓
\>\>\ASSERTN{10}{\INV\sub{x<-x+1}}     \quad(sk)$\ua$\\  { 10: Inv[x/x+1] }  (sk)↑
\>\>\SKIP\\                                            skip
\>\>\ASSERTN8{\INV\sub{x<-x+1}}        \quad(fi)$\ua$\\  { 8: Inv[x/x+1] }  (fi)↑
\>\ELSE\\                                            else
\>\>\ASSERTN7{\INV\land e\land\lnot e'} \quad(if)$\da$\\  { 7: Inv ∧ e ∧ ¬e' }  (if)↓
\>\>\ASSERTN{11}\TRUE                  \quad(ab)$\ua$\\  { 11: true }  (ab)↑
\>\>\ABORT\\                                           abort
\>\>\ASSERTN9{\INV\sub{x<-x+1}}        \quad(fi)$\ua$\\  { 9: Inv[x/x+1] }  (fi)↑
\>\FI;\\                                             fi;
\>\ASSERTN5{\INV\sub{x<-x+1}}          \quad(as)$\ua$\\  { 5: Inv[x/x+1] }  (as)↑
\>\ASS x{x+1}\\                                        x := x+1
\>\ASSERTN3\INV                        \quad(wh)\\     { 3: Inv }  (wh)
\OD\\                                                od
\ASSERTN4{\INV\land\lnot e}            \quad(wh)\\   { 4: Inv ∧ ¬e }  (wh)
\ASSERT G                                            { G }
\end{ALG}
\end{document}
```

2 Hoare calculus

The same verification task as above, but this time presented as derivation in the Hoare calculus. The output can be found on the next page.

```
\documentclass{scrartcl}
\usepackage{fullpage,rotating}
\advance\textheight20pt
\usepackage{fvsw}
\begin{document}
\begin{sideways}
\small\infertrue
$
\La{\CA F{\WHILE\ e\ \DO\ \IF\ e'\ \THEN\ \SKIP\ \ELSE\ \ABORT\ \FI;\ \ASS x{x+1}\ \OD}G}%
   {\FRM{1}{F\lfi\INV}\hspace{-5em}}%
   {\WH{\CA\INV
           {\WHILE\ e\ \DO\ \IF\ e'\ \THEN\ \SKIP\ \ELSE\ \ABORT\ \FI;\ \ASS x{x+1}\ \OD}%
           {\INV\land\lnot e}%
       }%
       {\SC{\CA{\INV\land e}{\IF\ e'\ \THEN\ \SKIP\ \ELSE\ \ABORT\ \FI;\ \ASS x{x+1}}\INV}%
           {\Ia{\CA{\INV\land e}%
                   {\IF\ e'\ \THEN\ \SKIP\ \ELSE\ \ABORT\ \FI}%
                   {\INV\sub{x<-x+1}}%
               }%
               {\Lb{\CA{\INV\land e\land e'}\SKIP{\INV\sub{x<-x+1}}}%
                   {\FRM{2}{\INV\land e\land e'\lfi\INV\sub{x<-x+1}}}%
                   {\SK{\CA{\INV\sub{x<-x+1}}\SKIP{\INV\sub{x<-x+1}}}}%
               }%
               {\AB{\CA{\INV\land e\land \lnot e'}\ABORT{\INV\sub{x<-x+1}}}}%
           }%
           {\Aa{\CA{\INV\sub{x<-x+1}}{\ASS x{x+1}}\INV}}%
       }%
   }%
   {\hspace{-8.8em}\FRM{3}{\INV\land\lnot e\lfi G}}
$
\end{sideways}
\end{document}
```

$$\dfrac{\dfrac{Inv \wedge e \wedge e' \overset{(2)}{\Rightarrow} Inv[x/x+1] \quad \{\, Inv[x/x+1] \,\}\, \mathsf{skip}\, \{\, Inv[x/x+1] \,\}^{(sk)}}{\{\, Inv \wedge e \wedge e' \,\}\, \mathsf{skip}\, \{\, Inv[x/x+1] \,\}}\,(lc) \quad \{\, Inv \wedge e \wedge \neg e' \,\}\, \mathsf{abort}\, \{\, Inv[x/x+1] \,\}^{(ab)}}{\{\, Inv \wedge e \,\}\, \mathsf{if}\ e'\ \mathsf{then\ skip\ else\ abort\ fi}\, \{\, Inv[x/x+1] \,\}}\,(if) \quad \{\, Inv[x/x+1] \,\}\, x := x+1\, \{\, Inv \,\}^{(as)}}{\{\, Inv \wedge e \,\}\, \mathsf{if}\ e'\ \mathsf{then\ skip\ else\ abort\ fi};\ x := x+1\, \{\, Inv \,\}}\,(sc)$$

$$\dfrac{F \overset{(1)}{\Rightarrow} Inv \qquad \dfrac{\{\, Inv \,\}\, \mathsf{while}\ e\ \mathsf{do\ if}\ e'\ \mathsf{then\ skip\ else\ abort\ fi};\ x := x+1\ \mathsf{od}\, \{\, Inv \wedge \neg e \,\}}\,(wh) \qquad Inv \wedge \neg e \overset{(3)}{\Rightarrow} G}{\{\, F \,\}\, \mathsf{while}\ e\ \mathsf{do\ if}\ e'\ \mathsf{then\ skip\ else\ abort\ fi};\ x := x+1\ \mathsf{od}\, \{\, G \,\}}\,(lc)$$