A7.1 Gelte $\mathcal{I} \vdash \{B\}\, c_2\, \{C\}$.

Zeige: $sat_n(c_1, s, h, \mathcal{I}, B) \Rightarrow sat_n(c_1; c_2, s, h, \mathcal{I}, C)$ f.a. c_1, s, h

IA: $n = 0$

Nach Definition gilt $sat_0(c_1; c_2, s, h, \mathcal{I}, C)$ für alle c_1, s, h

IV: $\forall c_1, s, h.\ sat_n(c_1, s, h, \mathcal{I}, B) \Rightarrow sat_n(c_1; c_2, s, h, \mathcal{I}, C)$

IS: $n \to n+1$

① Es gelte $sat_{n+1}(c_1, s, h, \mathcal{I}, B)$. // Ansonsten nichts zu zeigen

Wir zeigen: $sat_{n+1}(c_1; c_2, s, h, \mathcal{I}, C)$ gilt. Dazu:

a) zeige: $c_1; c_2 = skip \Rightarrow [\![C]\!]\, s\, h$

Gilt, da seq. Komposition $c_1; c_2$ nicht skip ist, $c_1; c_2 \neq skip$.

b) zeige: $\exists h_\mathcal{I}, h_F.\ satH(s, h_\mathcal{I}, c_1; c_2, \mathcal{I}) \wedge (c_1; c_2, s, h \uplus h_\mathcal{I} \uplus h_F) \to abort$

Seien $h_\mathcal{I}, h_F$ bel. und gelte $satH(s, h_\mathcal{I}, c_1; c_2)$.

Angenommen $(c_1; c_2, s, h \uplus h_\mathcal{I} \uplus h_F) \to abort$.

Nach SOS-Semantik erhalten wir: $(c_1, s, h \uplus h_\mathcal{I} \uplus h_F) \to abort$.

Also zusammen:

$$\neg\left(\exists h_\mathcal{I}\, h_F.\ satH(s, h_\mathcal{I}, c_1) \wedge (c_1, s, h \uplus h_\mathcal{I} \uplus h_F) \to abort\right)$$

$\rightsquigarrow$ Widerspruch zu $sat_{n+1}(c_1, s, h, \mathcal{I}, B)$ aus ①.

↳ Wichtig, dass $sat_n(\ldots)$ nichts aussagt.

A7.1

c) zeige: $\forall h_J, h_F, c', s', h'.$

$$satU(s, h_J, c_1;c_2, J) \wedge (c_1;c_2, s, h \uplus h_J \uplus h_F) \to (c', s', h')$$
$$\Longrightarrow \exists h'', h_J'.\ h' = h'' \uplus h_J' \uplus h_F.\ satU(s', h_J', c', J)$$
$$\wedge\ sat_n(c', s', h'', J, \mathbf{C})$$

Wir beobachten, dass die Transition von $c_1;c_2$ nach c' nur von den Regeln (SEQ1) und (SEQ2) stammen kann.

Seien h_J, h_F, c', s', h' bel. mit $\underbrace{satU(s, h_J, c_1;c_2, J)}_{②}$ und $(c_1;c_2, s, h \uplus h_J \uplus h_F) \longrightarrow (c', s', h')$.

Fall 1: (SEQ1) wurde angewendet.

Nach Definition gilt: $c_1 = skip$ und $(c', s', h') = (c_2, s, h \uplus h_J \uplus h_F)$.

Wähle also $h'' = h$ und $h_J' = h_J$. Damit erhalten wir sofort:

- $satU(s', h_J', c', J)$ aus ② und $locked(c_1;c_2) = locked(c_1) = 0$ und $locked(c_2) = 0$ // noch kein atomic
- $sat_n(c_2, s', h'', J, \mathbf{C})$ aus Vor. $J \vdash \{B\}\ c_2\ \{C\}$ und weil ① gilt $[\![B]\!]\, s\, h = [\![B]\!]\, s'\, h''$

Fall 2: (SEQ2) wurde angewendet.

Nach Definition: $c' = c_1';c_2$ und $(c_1, s, h \uplus h_J \uplus h_F) \longrightarrow (c_1', s', h')$.

Nach ① ex. h'' und h_J' mit $h' = h'' \uplus h_J' \uplus h_F$ und
$satU(s', h_J', c_1', J)$ und
$sat_n(c_1', s', h'', J, B)$.

Letzteres gibt nach IV: $sat_n(c_1';c_2, s', h'', J, \mathbf{C})$.

Des Weiteren $satU(s', h_J', c_1';c_2, J)$ weil $locked(c_1') = locked(c_1';c_2)$.

A7.2 Wähle:

$R = \text{false}$

$G_1(x,y,x',y') = y' \geq y \wedge x = x'$

$G_2(x,y,x',y') = y' = y \wedge (x' = x \vee x' = y)$

Idee!

$\{x>0 \wedge y>0\}$

$\{x>0 \wedge y>0\}$ $\quad\|\quad$ $\{x>0 \wedge y>0\}$

(1) $y = y+1;$ $\{x>0 \wedge y>0\}$ — (2) assume $x>0;$ $\{\text{true}\}$

(3) assume $(y>0)$ $\{x>0 \wedge y>0\}$ — (4) $x := y$ $\{\text{true}\}$

$\{\text{true}\}$

Ansatz

(1) Zeige: $y := y+1 : (x>0 \wedge y>0,\ R \vee G_2,\ G_1,\ x>0, y>0)$

- $\{x>0 \wedge y>0 \wedge x_0 = x \wedge y_0 = y\}\ y := y+1\ \{x>0 \wedge y>0 \wedge \underbrace{G_1(x_0,y_0,x,y)}_{y \geq y_0 \wedge x = x_0}\}$

  ist valides Hoare Triple ✓

- $x>0 \wedge y>0 \wedge \overbrace{y' = y \wedge (x' = x \vee x' = y)}^{(R \vee G_2)(x,y,x',y')} \Longrightarrow x'>0 \wedge y'>0$ ✓

  $\rightsquigarrow$ $x>0 \wedge y>0$ ist stabil unter $R \vee G_2$

(2) Zeige: assume $x>0 : (x>0 \wedge y>0,\ R \vee G_2,\ G_1,\ \text{true})$

- $\{x>0 \wedge y>0 \wedge x_0 = x \wedge y_0 = y\}$ assume $x>0$ $\{\text{true} \wedge \underbrace{G_1(x_0,y_0,x,y)}_{y \geq y_0 \wedge x = x_0}\}$

  ist valides Hoare-Tripel ✓

- $x>0 \wedge y>0$ stabil unter $R \vee G_2$ wie oben

- $\text{true} \wedge (R \vee G_2)(x,y,x',y') \Longrightarrow \text{true}$

  $\rightsquigarrow$ true stabil unter $R \vee G_2$

(3) Zeige: assume $y>0$: $(x>0 \wedge y>0, R \vee G_1, G_2, x>0 \wedge y>0)$

- $\{x>0 \wedge y>0 \wedge x_0=x \wedge y_0=y\}$ assume $y>0$ $\{x>0 \wedge y>0 \wedge \underbrace{G_2(x_0,y_0,x,y)}_{y=y_0 \wedge (x=x_0 \vee x=y_0)}\}$
  ist valides Hoare-Tripel

- $x>0 \wedge y>0 \wedge \underbrace{y' \geq y \wedge x=x'}_{(R \vee G_1)(x,y,x',y')} \Rightarrow x'>0 \wedge y'>0$

  $\rightsquigarrow$ $x>0 \wedge y>0$ stabil unter $R \vee G_1$

(4) Zeige: $x := y$: $(x>0 \wedge y>0, R \vee G_1, G_2, \text{true})$

- $\{x>0 \wedge y>0 \wedge x_0=x \wedge y_0=y\}$ $x:=y$ $\{\text{true} \wedge \underbrace{G_2(x_0,y_0,x,y)}_{y=y_0 \wedge (x=x_0 \vee x=y_0)}\}$
  ist valides Hoare-Tripel

- $x>0 \wedge y>0$ stabil unter $R \vee G_1$ wie oben

- $\text{true} \wedge (R \vee G_1)(x,y,x',y') \Rightarrow \text{true}$ ✓

  $\rightsquigarrow$ true stabil unter $R \vee G_1$

Zusamen:

C : $(x>0 \wedge y>0, R, G_1 \vee G_2, \text{true})$

mittels Anwendung von (PAR) und (SEQ).