$\boxed{A8.1}$

a) Widerlege mit:

$$A \equiv x \mapsto 1 * \text{true} \qquad B \equiv x \mapsto 1$$

Seien s bel., $h = \{x \mapsto 1, y \mapsto 1\}$, $h' = \{x \mapsto 1\}$

Dann gilt: $\llbracket A \rrbracket s h = 1$

$\llbracket A -\!\circledast B \rrbracket_s \emptyset = 1$ weil $\llbracket A \rrbracket s h' = 1$

und $\llbracket B \rrbracket_s h' \uplus \emptyset = 1$

Zusammen: $\llbracket A * (A -\!\circledast B) \rrbracket_s h = 1$ aber $\llbracket B \rrbracket_s h = 0$

b) Widerlege mit:

$$A \equiv x \mapsto 1 * y \mapsto 2 \qquad B \equiv x \mapsto 1$$

Seien s, h bel. mit $\llbracket B \rrbracket s h = 1$. Dann gilt: $h = \{x \mapsto 1\}$.

Also $\llbracket A \rrbracket s h' = 0$ für alle $h' \subseteq h$.

Damit $\llbracket A * (A -\!\circledast B) \rrbracket s h = 0$.

c) Seien s, h bel. mit $\llbracket A -\!\circledast B \rrbracket s h$.

Nach Definition ex. h_1 mit $h_1 \perp h$ und $\llbracket A \rrbracket s h_1$ und $\llbracket B \rrbracket_s h \uplus h_1$.

<u>zz</u>: $\llbracket \neg(A -\!* \neg B) \rrbracket_s h = 1$ <u>gzz</u>: $\llbracket A -\!* \neg B \rrbracket s h = 0$

<u>gzz</u>! $\exists h'.\ \llbracket A \rrbracket_s h' = 1$ und $\underbrace{\llbracket \neg B \rrbracket_s h \uplus h' = 0}_{\Leftrightarrow\ \llbracket B \rrbracket s h \uplus h' = 1}$.

Wähle $h' = h_1$. ✓

$\boxed{A8.1}$

d) Sei s,h bel. mit $[\![\neg(A -\!\!* \neg B)]\!] s\, h$. Also $[\![A -\!\!* \neg B]\!] s\, h = 0$.

Nach Def gilt:

$$\neg \forall h_1.\ h_1 \perp h \wedge [\![A]\!] s\, h_1 \Rightarrow [\![\neg B]\!] s\, h_1 \uplus h$$

$$\Leftrightarrow \exists h_1.\ h_1 \perp h \wedge [\![A]\!] s\, h_1 \wedge \underbrace{[\![\neg B]\!] s\, h_1 \uplus h = 0}_{\Leftrightarrow\ [\![B]\!] s\, h_1 \uplus h = 1}$$

$\overset{\text{Def}}{\Leftrightarrow} A -\!\circledast B$ ✓

e) Widerlege mit:

$A \equiv x \mapsto 1 \qquad B \equiv x \mapsto 2$

$[\![B]\!] s\, h$ liefert $h = \{x \mapsto 2\}$.

D.h. $\nexists h_1.\ h_1 \perp h$ und $[\![A]\!] s\, h_1 = 1$

Also $[\![A -\!\circledast (A * B)]\!] s\, h = 0$.

Damit $B \not\Rightarrow (A -\!\circledast (A * B))$. ✓

f) • Seien s,h bel. mit $[\![x \mapsto y -\!\circledast (x \mapsto y * B)]\!] s\, h$.

Also ex. h_1 mit $h \perp h_1$ und $[\![x \mapsto y]\!] s\, h_1$ und $[\![x \mapsto y * B]\!] s\, h \uplus h_1$.

Es muss gelten: $h_1 = \{x \mapsto y\}$. Damit $x \notin dom(h)$ nach $h \perp h_1$.

Wir erhalten sofort $[\![B]\!] s\, h$, da Separation $x \mapsto y * \ldots$ hier h_1 für $x \mapsto y$ abspalten muss.

Des Weiteren: $[\![x \hookrightarrow c]\!] s\, h = 0$ für alle c, da $x \notin dom(h)$.

Zusammen: $[\![B \backslash x]\!] s\, h = 1$

• Seien s,h bel. mit $[\![B \backslash x]\!] s\, h$. Nach Def: $[\![B]\!] s\, h$ und $x \notin dom(h)$.

Wähle $h_1 = \{x \mapsto y\}$. Dann $[\![x \mapsto y]\!] s\, h_1 = 1$ und $h_1 \perp h$.

Ferner gilt: $[\![B * x \mapsto y]\!] s\, h \uplus h_1$ sofort.

Zusammen: $[\![x \mapsto y -\!\circledast (x \mapsto y * B \backslash x)]\!] s\, h = 1$. ✓

$\boxed{\text{A8.2:}}$

a) Zeige:

$$\forall s,h,a,b,c,d.\ [\![a \mapsto b \circledast ls(c,d)]\!]\, s\,h \Rightarrow [\![ls(c,a) * ls(b,d)]\!]\, s\,h$$

per Induktion nach $|dom(h)|$

<u>IA</u>: $|dom(h)| = 0$.

Ex. h_1 mit $[\![a \mapsto b]\!]\, s\, h_1$ und $\underline{[\![ls(c,d)]\!]\, s\, h_1 \uplus \emptyset}$

$h_1 \neq \emptyset$ $\quad \Rightarrow [\![\exists e.\ c \mapsto e * ls(e,d)]\!]\, s\, h_1$ da $h_1 \neq \emptyset$

Dann folgt: $[\![c \mapsto e * ls(e,d)]\!]\, s' h_1$ mit $s' = s \cup \{e \mapsto v\}$ für ein v

Def h_1 liefert: $[\![c \mapsto e]\!]\, s' h_1 = 1$ und somit $s(c) = s(a)$ und $v = s(b)$.

Ferner gilt: $[\![ls(e,d)]\!]\, s' \emptyset = 1$ und somit $[\![e = d]\!]\, s' \emptyset$

also auch $[\![b = d]\!]\, s' \emptyset$

Zusammen bekommen wir:

$$[\![ls(c,a) * ls(b,d)]\!]\, s\, \underset{h}{\underset{\|}{\emptyset}} \quad \checkmark$$

<u>IV</u>: Beh. gilt für alle h mit $|dom(h)| \leq n$.

<u>IS</u> $n \to n+1$.

Es gelte $[\![a \mapsto b \circledast ls(c,d)]\!]\, s\, h$. Also ex h_1 mit:

$h_1 \perp h$ und $[\![a \mapsto b]\!]\, s\, h_1$ und $[\![ls(c,d)]\!]\, s\, h \uplus h_1$

Da $h \uplus h_1 \neq \emptyset$ folgt: $[\![c \neq d \wedge \exists e.\ c \mapsto e * ls(e,d)]\!]\, s\, h \uplus h_1$

$\Rightarrow s(c) \neq s(d)$ und $[\![c \mapsto e * ls(e,d)]\!]\, s' h \uplus h_1$ mit $s' = s \uplus \{e \mapsto v\}$ für ein v.

Fall 1: $[\![a=c]\!]s$

Damit ist $c \mapsto e$ durch h_1 erfüllt. Also:

$$[\![ls(e,d)]\!]s'\,h \quad \text{und} \quad [\![e=b]\!]s'$$

$$\Rightarrow [\![a=c \wedge emp * ls(b,d)]\!]s\,h$$

$$\Rightarrow [\![ls(c,a) * ls(b,d)]\!]s\,h$$

Fall 2: $[\![a\neq c]\!]s$

Dann ex. h_2, h_3 mit $h = h_2 \uplus h_3$ und $[\![c \mapsto e]\!]s'h_2 = 1$.

Wir erhalten:

$$[\![ls(e,d)]\!]s'\,h_1 \uplus h_3$$

$$\Rightarrow [\![a \mapsto b -\!\!\circledast\, ls(e,d)]\!]s'\,h_3$$

Jetzt liefert IV für $h_3 \subsetneq h$:

$$[\![ls(e,a) * ls(b,d)]\!]s'\,h_3$$

$$\Rightarrow [\![c \mapsto e * ls(e,a) * ls(b,d)]\!]s'\,h$$

$$\Rightarrow [\![a\neq c \wedge \exists e.\, c \mapsto e * ls(e,a) * ls(b,d)]\!]s\,h$$

$$\Rightarrow [\![ls(c,a) * ls(b,d)]\!]s\,h$$

$\blacksquare$

$\boxed{A8.2}$

b) <u>zz.</u> $\text{sem\_stable}(\, ls(K, nil),\, R_1 \,)$

$$\Leftrightarrow \quad (x \mapsto y \multimap\!\!\circledast\; ls(K, nil)) * x \mapsto z * z \mapsto y \implies ls(K, nil)$$

<u>Es folgt nach a)</u> $x \mapsto y \multimap\!\!\circledast\; ls(K, nil)$

$$\implies ls(K, x) * ls(y, nil)$$

Also erhalten wir:

$$ls(K, x) * x \mapsto z * z \mapsto y * ls(y, nil)$$

$$\implies ls(K, x) * x \mapsto z * ls(z, nil)$$

$$\implies ls(K, x) * ls(x, nil)$$

$$\implies ls(K, nil) \quad \checkmark$$

$\boxed{A8.2}$

c) $((x \mapsto z * z \mapsto y) -\!\circledast\, ls(K, nil)) * x \mapsto y$

$\overset{VL}{\Longrightarrow} (z \mapsto y -\!\circledast (x \mapsto z -\!\circledast\, ls(K, nil))) * x \mapsto y$

$\overset{a)}{\Longrightarrow} (z \mapsto y -\!\circledast (ls(K, x) * ls(z, nil))) * x \mapsto y$

$\overset{VL}{\Longrightarrow} ((z \mapsto y -\!\circledast\, ls(K,x)) * ls(z,nil)\upharpoonright_z * x \mapsto y)$ ①

$\vee ((z \mapsto y -\!\circledast\, ls(z,nil)) * ls(K,x)\upharpoonright_z * x \mapsto y)$ ②

② $\overset{a)}{\Longrightarrow} ls(z,z) * ls(y, nil) * ls(K,x)\upharpoonright_z * x \mapsto y$

$\Longrightarrow ls(x, nil) * ls(K, x) \Longrightarrow ls(K, nil)$ ✓

① Betrachte $ls(z, nil)\upharpoonright_z$. Nach Def $\upharpoonright_z$ ist z nicht alloziert.
Dann erhalten wir:

$$ls(z, nil)\upharpoonright_z \Longrightarrow emp \wedge z = nil.$$

D.h. $\nexists h_1 : [\![z \mapsto y]\!]\, s\, h_1$ wobei hier s bel. mit $s(z) = nil$.
Damit ist $(z \mapsto y -\!\circledast \dots)$ nicht erfüllbar, sodass wir erhalten:

$$① \Rightarrow false$$

① $\vee$ ② $\Longrightarrow$ ② $\Longrightarrow ls(K, nil)$ ✓

d) Wir hätten in ① keinen Widerspruch/false erhalten, sondern

$ls(K, m) * ls(y, x) * z = m * x \mapsto y$

$\Longrightarrow \underline{ls(K, m)}$ ✓ $* \underline{ls(y,x) * x \mapsto y}$ f

↳ Wir hätten explizit Kreise verbieten müssen.

$\boxed{\text{A8.3}}$

$$\dfrac{\begin{array}{c} c_1 : \boxed{x \mapsto 0,0,0}, G_2, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1} \\ c_2 : \boxed{x \mapsto 0,0,0}, G_1, G_2, \boxed{x \mapsto 1,0,1} \vee \boxed{x \mapsto 2,1,1} \end{array}}{\dfrac{c_1 \| c_2 : \boxed{x \mapsto 0,0,0}, \emptyset, G_1 \cup G_2, \begin{array}{l} (\boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1}) \wedge \\ (\boxed{x \mapsto 1,0,1} \vee \boxed{x \mapsto 2,1,1}) \end{array}}{c_1 \| c_2 : \boxed{x \mapsto 0,0,0}, \emptyset, G_1 \cup G_2, \boxed{x \mapsto 2,1,1}}\,(\text{CONS})}\,(\text{PAR})$$

Zum Nachweis für c_1:

$$\dfrac{\dfrac{\checkmark}{\vdash_{SL} \{x \mapsto 0,0,0\}\, c_1' \,\{x \mapsto 1,1,0\}} \qquad \dfrac{\checkmark}{\vdash_{SL} \{x \mapsto 1,0,1\}\, c_1' \,\{x \mapsto 2,1,1\}}}{c_1' : x \mapsto 0,0,0, \emptyset, G_1, x \mapsto 1,1,0 \qquad c_1' : x \mapsto 1,0,1, \emptyset, G_1, x \mapsto 2,1,1}\,(\text{SEQ+CON})$$

': ohne atomic

$$\dfrac{\begin{array}{cc} c_1' : x \mapsto 0,0,0, \emptyset, G_1, x \mapsto 1,1,0 & c_1' : x \mapsto 1,0,1, \emptyset, G_1, x \mapsto 2,1,1 \\ x \mapsto 0,0,0 \rightsquigarrow x \mapsto 1,1,0 \subseteq G_1 & x \mapsto 1,0,1 \rightsquigarrow x \mapsto 2,1,1 \subseteq G_1 \end{array}}{\begin{array}{c} c_1 : \boxed{x \mapsto 0,0,0}, \emptyset, G_1, \boxed{x \mapsto 1,1,0} \\ c_1 : \boxed{x \mapsto 1,0,1}, \emptyset, G_1, \boxed{x \mapsto 2,1,1} \end{array}}\,(\text{ATOM})$$

$$\dfrac{\begin{array}{c} c_1 : \boxed{x \mapsto 0,0,0}, \emptyset, G_1, \boxed{x \mapsto 1,1,0} \\ c_1 : \boxed{x \mapsto 1,0,1}, \emptyset, G_1, \boxed{x \mapsto 2,1,1} \end{array}}{\begin{array}{c} c_1 : \boxed{x \mapsto 0,0,0}, \emptyset, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1} \\ c_1 : \boxed{x \mapsto 1,0,1}, \emptyset, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1} \end{array}}\,(\text{CONS})^{*}_{2x}$$

$$\dfrac{\begin{array}{c} c_1 : \boxed{x \mapsto 0,0,0}, \emptyset, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1} \\ c_1 : \boxed{x \mapsto 1,0,1}, \emptyset, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1} \end{array}}{c_1 : \boxed{x \mapsto 0,0,0} \vee \boxed{x \mapsto 1,0,1}, \emptyset, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1}}\,(\text{DISJ})^{*}$$

$$\dfrac{\begin{array}{c} c_1 : \boxed{x \mapsto 0,0,0} \vee \boxed{x \mapsto 1,0,1}, \emptyset, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1} \\ \underline{\text{stable}}(\boxed{x \mapsto 0,0,0} \vee \boxed{x \mapsto 1,0,1}, G_2) \quad \underline{\text{stable}}(\boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1}, G_2) \end{array}}{\dfrac{c_1 : \boxed{x \mapsto 0,0,0} \vee \boxed{x \mapsto 1,0,1}, G_2, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1}}{c_1 : \boxed{x \mapsto 0,0,0}, G_2, G_1, \boxed{x \mapsto 1,1,0} \vee \boxed{x \mapsto 2,1,1}}\,(\text{CONS})^{**}}\,(\text{ATOMR})$$

* Diese Regelanwendungen sind nötig, um $\ldots \subseteq G_1$ nachweisen zu können.

** Diese Regelanwendung ist nötig, um stable für die Vorbedingung nachweisen zu können.

Wählen nun Garantien:

$$G_1 = \{ \; x \mapsto 0,0,0 \rightsquigarrow x \mapsto 1,1,0, \quad x \mapsto 1,0,1 \rightsquigarrow x \mapsto 2,1,1 \; \}$$

$$G_2 = \{ \; x \mapsto 0,0,0 \rightsquigarrow x \mapsto 1,0,1, \quad x \mapsto 1,1,0 \rightsquigarrow x \mapsto 2,1,1 \; \}$$

- $x \mapsto 0,0,0 \rightsquigarrow x \mapsto 1,1,0 \subseteq G_1$ ✓
- $x \mapsto 1,0,1 \rightsquigarrow x \mapsto 2,1,1 \subseteq G_1$ ✓
- stable($\boxed{x \mapsto 0,0,0 \vee x \mapsto 1,0,1}$, G_2) :
  - sem-stable($x \mapsto 0,0,0 \vee x \mapsto 1,0,1$, $x \mapsto 0,0,0 \rightsquigarrow x \mapsto 1,0,1$):

    $$(x \mapsto 0,0,0 \mathrel{-\!\circledast} (x \mapsto 0,0,0 \vee x \mapsto 1,0,1)) * x \mapsto 1,0,1$$
    $$\overset{VL}{\Rightarrow} ((x \mapsto 0,0,0 \mathrel{-\!\circledast} x \mapsto 0,0,0) * x \mapsto 1,0,1)$$
    $$\vee (x \mapsto 0,0,0 \mathrel{-\!\circledast} x \mapsto 1,0,1) * x \mapsto 1,0,1)$$
    $$\Rightarrow x \mapsto 1,0,1 \vee \text{false} \Rightarrow x \mapsto 1,0,1 \Rightarrow x \mapsto 1,0,1 \vee x \mapsto 0,0,0$$ ✓

  - sem-stable($x \mapsto 0,0,0 \vee x \mapsto 1,0,1$, $x \mapsto 1,1,0 \rightsquigarrow x \mapsto 2,1,1$):

    $$(x \mapsto 1,1,0 \mathrel{-\!\circledast} (x \mapsto 0,0,0 \vee x \mapsto 1,0,1)) * x \mapsto 2,1,1$$
    $$\Rightarrow \text{false} \Rightarrow x \mapsto 0,0,0 \vee x \mapsto 1,0,1$$ ✓

- stable($\boxed{x \mapsto 1,1,0 \vee x \mapsto 2,1,1}$, G_2)
  - $$(x \mapsto 0,0,0 \mathrel{-\!\circledast} (x \mapsto 1,1,0 \vee x \mapsto 2,1,1)) * x \mapsto 1,0,1$$
    $$\Rightarrow \text{false} \Rightarrow$$ ✓
  - $$(x \mapsto 1,1,0 \mathrel{-\!\circledast} (x \mapsto 1,1,0 \vee x \mapsto 2,1,1)) * x \mapsto 2,1,1$$
    $$\Rightarrow x \mapsto 2,1,1$$ ✓