A6.1

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\{x = x' \land a \mapsto z\}\ x := [a]\ \{x = z \land a[x/x'] \mapsto z\}}\ (\text{LLOOKV})}{\{x = x' \land a \mapsto z * B(x', z)\}\ x := [a]\ \{x = z \land a[x/x'] \mapsto z * B(x', z)\}}\ (\text{FRAME})^{*}}{\{\exists x', z.\ x = x' \land a \mapsto z * B(x', z)\}\ x := [a]\ \{\exists x', z.\ x = z \land a[x/x'] \mapsto z * B(x', z)\}}\ (\text{AUX})^{**}}{\{\exists z.\ a \mapsto z * B(x, z)\}\ x := [a]\ \{\exists x'.\ a[x/x'] \mapsto x * B(x', x)\}}\ (\text{CONS})
$$

(GLOOKV) hat Nebenbed. : $*$ $z, x', x \notin fv(B)$

$**$ z, x', x verschieden , $z, x' \notin fv(a)$

$\Rightarrow z, x' \notin fv(x := [a])$

$\boxed{\text{A6.2}}$

procedure GETLAST(x)

local y, z ;

$$\{\, list(x) \,\}$$

y := x ;

$$\{\, y = x * list(x) \,\}$$

$$\{\, y = x * \exists \alpha .\ \alpha \neq \varepsilon * lseg_{\alpha}(x, nil) \,\}$$

$$\{\, y = x * \exists u, \alpha, K .\ x \mapsto u, K * lseg_{\alpha}(K, nil) \,\}$$

z = [x + 1] ;

$$\{\, \exists u, \alpha, K .\ x \mapsto u, K * lseg_{\alpha}(k, nil) * y = x * z = k \,\}$$

$$\boxed{I} \quad \{\, \exists \alpha, u, \beta .\ \underbrace{lseg_{\alpha}(x, y)}_{\alpha = \varepsilon \wedge x = y} * y \mapsto u, z * lseg_{\beta}(z, nil) \,\}$$

while z ≠ nil do // Invariante ist I

$$\{\, z \neq nil * Inv \,\}$$

$$\{\, z \neq nil * \exists \alpha, \beta .\ lseg_{\alpha}(x, z) * lseg_{\beta}(z, nil) \,\}$$

y := z ;

$$\{\, z \neq nil * y = z * \exists \alpha, \beta .\ lseg_{\alpha}(x, z) * lseg_{\beta}(z, nil) \,\}$$

$$\{\, \exists \alpha, u, \beta, K .\ lseg_{\alpha}(x, y) * \underbrace{y \mapsto u, K * lseg_{\beta}(K, nil)}_{\text{aus } lseg_{\alpha\beta}(z, nil) \wedge z \neq nil} \,\}$$

z := [y + 1] ;

$$\{\, \exists \alpha, u, \beta .\ lseg_{\alpha}(x, y) * y \mapsto u, z * lseg_{\beta}(z, nil) \,\}$$

$$\{\, I \,\}$$

od

$$\{\, Inv * z = nil \,\}$$

$$\{\, \exists \alpha, u, \beta .\ lseg_{\alpha}(x, y) * y \mapsto u, nil * \underbrace{lseg_{\beta}(nil, nil)}_{\beta = \varepsilon * emp} \,\}$$

$$\{\, \exists \alpha, u .\ lseg_{\alpha}(x, y) * lseg_{u}(y, nil) \,\}$$

return y;

$\boxed{A6.3}$ Aus Aufgabe 6.2 erhalten wir:

$$T(\text{GETLAST}) = \{\ list(x) \mapsto \{\underbrace{\exists \alpha\, \exists u.\ lseg_\alpha(x,y) * lseg_u(y, nil)}_{Q(x,y)}\}\}$$

Betrachte nun MERGE. Da wir noch keine Information berechnet haben, starten wir mit der Vorbedingung emp und aktuellen Heap emp.

1. Schritt:

- berechne $[\![z = \text{GETLAST}(x)]\!]_T (emp, emp)$
- löse BI-ABD$(emp * X,\ list(x) * Y)$

  $\rightsquigarrow\ X \equiv list(x)\ ,\ Y \equiv emp$
- füge $(list(x), Q(x,z))$ zu $[\![z = \text{GETLAST}]\!]_T (emp, emp)$ hinzu

2. Schritt:

- berechne $[\![[z+1] := y]\!]_T (list(x), Q(x,z))$
- wissen dass Spec der Anweisung ist: $\{z+1 \mapsto \_\}\ [z+1] := y\ \{z+1 \mapsto y\}$
- löse BI-ABD$(Q(x,z) * X,\ x+1 \mapsto _ * Y)$

  $\rightsquigarrow\ X \equiv emp\ ,\ Y \equiv \exists \alpha\, \exists u.\ lseg_\alpha(x,z) * z \mapsto u$
- beachte: $z+1 \mapsto y * \exists \alpha\, \exists u.\ lseg_\alpha(x,z) * z \mapsto u$

  $\models \exists \alpha\, \exists u.\ lseg_\alpha(x,z) * lseg_u(z,y) \models \exists \alpha.\ lseg_\alpha(x,y) * \underline{\alpha \neq \varepsilon}$
- füge $(list(x), \exists \alpha.\ lseg_\alpha(x,y) * \alpha \neq \varepsilon)$ zu $[\![[z+1] := y]\!]_T (list(x), Q(x,z))$ hinzu

Schritt 3:

- Füge Schritte zusammen (Sequenz)
- also füge $(list(x), \exists \alpha .\ lseg_{\alpha}(x,y) * \alpha \neq \varepsilon)$

  zu $[\![③ ; ④]\!]_T \ (emp, emp)$ hinzu

- bekommen:

$$T(MERGE) = \{ list(x) \mapsto \{ \exists \alpha .\ lseg_{\alpha}(x,y) * \alpha \neq \varepsilon \} \}$$

Schritt 4:

- Verstärke Nachbedingung zur gewünschten.
- löse $\text{BI-ABD}(\exists \alpha .\ lseg_{\alpha}(x,y) * \alpha \neq \varepsilon * X, \underbrace{list(x)}_{\text{Ziel}} * Y)$

$$\rightsquigarrow X \equiv \exists \beta .\ lseg_{\beta}(y, nil), \quad Y \equiv emp$$

- können Ergebnis zu T hinzufügen:

$$T(MERGE) = \{ list(x) \mapsto \{ \exists \alpha .\ lseg_{\alpha}(x,y) * \alpha \neq \varepsilon \},$$
$$list(x) * \exists \beta\, lseg_{\beta}(y, nil) \mapsto \{ list(x) \} \}$$

- Zusammengefasst haben wir:

$$\{ list(x) * \exists \beta\, lseg_{\beta}(y, nil) \} \ MERGE(x,y) \ \{ list(x) \}$$

nachgewiesen.

A6.4

a) Sei I bel.

Wähle $R \equiv (\ell \mapsto 0 * I) \vee (\ell \mapsto 1 * emp)$

$R \vdash$

$\{emp\}$

atomic $\{$

$\{R * emp\}$

$\{\exists a.\ \ell \mapsto a * ((a=0 \wedge I) \vee (a=1 \wedge emp))\}$

$t_i := [\ell];$

$\{\exists a.\ \ell \mapsto a * t_i = a * ((a=0 \wedge I) \vee (a=1 \wedge emp))\}$

assume $t_i = 0;$

$\{\ell \mapsto 0 * t_i = 0 * ((0=0 \wedge I) \vee (0=1 \wedge emp))\}$

$\{\ell \mapsto 0 * t_i = 0 * I\}$

$[\ell] := 1;$

$\{\ell \mapsto 1 * t_i = 0 * I\}$

$\{\ell \mapsto 1 * I\}$

$\{R * I\}$

$\}$

$\{I\}$

$\boxed{A6.4}$

zu a)

$R \vdash$

$\{I\}$

atomic {

$\{R * I\}$

$\{\exists a.\ \ell \mapsto a * ((a = 0 \land I) \lor (a = 1 \land emp)) * I\}$

$t_i := [\ell];$

$\{\exists a.\ \ell \mapsto a * t_i = a * ((a = 0 \land I) \lor (a = 1 \land emp)) * I\}$

assume $t_i = 1;$

$\{\ell \mapsto 1 * t_i = 1 * emp * I\}$

$[\ell] := 0;$

$\{\ell \mapsto 0 * t_i = 1 * I\}$

$\{\ell \mapsto 0 * I\}$

$\{R\}$

$\{R * emp\}$

}

$\{emp\}$

b)

$$\dfrac{\dfrac{\dfrac{}{R \vdash \{emp\}\ lock_i\ \{I\}}\,(a)}{R \vdash \{P\}\ lock_i\ \{P * I\}}\,(FRAME) \qquad \dfrac{\dfrac{Vor.}{R \vdash \{P * I\}\ C\ \{Q * I\}} \quad \dfrac{\dfrac{}{R \vdash \{I\}\ unlock_i\ \{emp\}}\,(a)}{R \vdash \{Q * I\}\ unlock_i\ \{Q\}}\,(FRAME)}{R \vdash \{P * I\}\ C; unlock_i\ \{Q\}}\,(SEQ)}{R \vdash \{P\}\ lock_i; C; unlock_i\ \{Q\}}\,(SEQ)$$

$\boxed{A6.5}$ $\quad x \mapsto 0,0,0 \rightsquigarrow J \vdash \{A\}\ c\ \{B\} \rightsquigarrow x \mapsto 2,1,1$

<u>Idee 1:</u> Verwende Invariante $J \equiv \exists a,b,c.\ x \mapsto a,b,c \wedge a = b+c$

- $x \mapsto 0,0,0$ impliziert die Invariante
- Problem:
  - tatsächliche Werte a,b,c nicht bekannt
  - atomarer Block kann $+1$ für a rechnen, kann aber nicht $b=0$ etablieren

    $\Rightarrow$ Invariante kann nicht wieder hergestellt werden!

<u>Idee 2:</u> Verwende Invariante $J \equiv \exists a,b.\ x \mapsto a+b * X(a,b)$, wobei $X(a,b)$ eine Korrelation zwischen a und b bzgl. Speicherzellen $x+1$ und $x+2$ herstellt.

z.B.: $X(a,b) \equiv \forall k.\ x+1 \mapsto k \mathrel{-\!\!*} x+1 \mapsto k \wedge a=k$
$\quad * \ \forall k.\ x+2 \mapsto k \mathrel{-\!\!*} x+2 \mapsto k \wedge b=k$

Wichtig: $X(a,b)$ owned $x+1$ und $x+2$ <u>nicht</u>. Stattdessen geben wir $x+1 \mapsto 0$ bzw. $x+2 \mapsto 0$ in die Teilbeweise der (PAR) Regel.

Zeige: $\{J * x+1 \mapsto 0\}\ c_1\ \{J * x+1 \mapsto 1\}$
$\{J * x+2 \mapsto 0\}\ c_2\ \{J * x+2 \mapsto 1\}$

Mit (PAR) und (ATOM) dann:

$$J \vdash \{\underbrace{x+1 \mapsto 0 * x+2 \mapsto 0}_{A}\}\ c_1 \| c_2\ \{\underbrace{x+1 \mapsto 1 * x+2 \mapsto 1}_{B}\}$$

und $J * B \vdash x \mapsto 2,1,1$

<u>Problem</u> $\quad x \mapsto 0,0,0 \nvdash J * A$