

E Substitution theorems for $BI^{\mu\nu}$

Theorem 9.

If $\llbracket Y \rrbracket$ and $\llbracket P \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}$ exist

$$\llbracket P \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]} = \llbracket P\{Y/X_v\} \rrbracket_{\rho}$$

Proof (Theorem 9). By induction on the formula P .

- Case P as the form $E = E'$, $E \mapsto E_1, e_2$, **false**, **emp**
 $P\{Y/X_v\} = P$ and $\forall \rho. \llbracket P \rrbracket_{\rho} = \llbracket P \rrbracket$ so

$$\begin{aligned} & \llbracket P \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]} \\ &= \llbracket P \rrbracket \\ &= \llbracket P\{Y/X_v\} \rrbracket \\ &= \llbracket P\{Y/X_v\} \rrbracket_{\rho} \end{aligned}$$
- $\llbracket P \Rightarrow Q \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}$

$$\begin{aligned} &= (\top \setminus \llbracket P \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}) \cup \llbracket Q \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]} \\ &= (\top \setminus \llbracket P\{Y/X_v\} \rrbracket_{\rho}) \cup \llbracket Q\{Y/X_v\} \rrbracket_{\rho} \quad (\text{ind. hyp.}) \\ &= \llbracket P\{Y/X_v\} \Rightarrow Q\{Y/X_v\} \rrbracket_{\rho} \\ &= \llbracket (P \Rightarrow Q)\{Y/X_v\} \rrbracket_{\rho} \end{aligned}$$
- $\llbracket \exists x. P \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}$

$$\begin{aligned} &= \{s, h \mid \exists v \in \text{Val}. [s \mid x \mapsto v], h \in \llbracket P \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}\} \\ &= \{s, h \mid \exists v \in \text{Val}. [s \mid x \mapsto v], h \in \llbracket P\{Y/X_v\} \rrbracket_{\rho}\} \quad (\text{ind. hyp.}) \\ &= \llbracket \exists x. (P\{Y/X_v\}) \rrbracket_{\rho} \\ &= \llbracket (\exists x. P)\{Y/X_v\} \rrbracket_{\rho} \end{aligned}$$
- $\llbracket P * Q \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}$

$$\begin{aligned} &= \{s, h \mid \exists h_0, h_1. h_0 \# h_1, h = h_0.h_1 \\ &\quad s, h_0 \in \llbracket P \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]} \text{ and } s, h_1 \in \llbracket Q \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}\} \\ &= \{s, h \mid \exists h_0, h_1. h_0 \# h_1, h = h_0.h_1 \\ &\quad s, h_0 \in \llbracket P\{Y/X_v\} \rrbracket_{\rho} \text{ and } s, h_1 \in \llbracket Q\{Y/X_v\} \rrbracket_{\rho}\} \quad (\text{ind. hyp.}) \\ &= \llbracket P\{Y/X_v\} * Q\{Y/X_v\} \rrbracket_{\rho} \\ &= \llbracket (P * Q)\{Y/X_v\} \rrbracket_{\rho} \end{aligned}$$
- $\llbracket P \multimap Q \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}$

$$\begin{aligned} &= \{s, h \mid \forall h'. \text{ if } h' \# h \text{ and } s, h' \in \llbracket P \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]} \text{ then} \\ &\quad s, h.h' \in \llbracket Q \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}\} \\ &= \{s, h \mid \forall h'. \text{ if } h' \# h \text{ and } s, h' \in \llbracket P\{Y/X_v\} \rrbracket_{\rho} \text{ then} \\ &\quad s, h.h' \in \llbracket Q\{Y/X_v\} \rrbracket_{\rho}\} \quad (\text{ind. hyp.}) \\ &= \llbracket P\{Y/X_v\} \multimap Q\{Y/X_v\} \rrbracket_{\rho} \\ &= \llbracket (P \multimap Q)\{Y/X_v\} \rrbracket_{\rho} \end{aligned}$$
- $\llbracket X_v \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}$

$$\begin{aligned} &= \llbracket Y \rrbracket \\ &= \llbracket Y \rrbracket_{\rho} \\ &= \llbracket X_v\{Y/X_v\} \rrbracket_{\rho} \end{aligned}$$
- $\llbracket Z_v \rrbracket_{\rho[X_v \mapsto \llbracket Y \rrbracket]}$ with $Z_v \neq X_v$

$$\begin{aligned} &= \llbracket Z_v \rrbracket_{\rho} \\ &= \llbracket Z_v\{Y/X_v\} \rrbracket_{\rho} \end{aligned}$$

$$\begin{aligned}
& - \llbracket \mu X_v.P \rrbracket_{[\rho|X_v \mapsto \llbracket Y \rrbracket]} \\
& = \text{lfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P \rrbracket_{[[\rho|X_v \mapsto \llbracket Y \rrbracket]|X_v \mapsto Z]} \\
& = \text{lfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P \rrbracket_{[\rho|X_v \mapsto Z]} \\
& = \text{lfp}_{\emptyset}^{\subseteq} \lambda X. \llbracket P \rrbracket_{[\rho|X_v \mapsto X]} \\
& = \llbracket \mu X_v.P \rrbracket_{\rho} \\
& = \llbracket (\mu X_v.P)\{Y/X_v\} \rrbracket_{\rho} \\
& - \llbracket \mu Z_v.P \rrbracket_{[\rho|X_v \mapsto \llbracket Y \rrbracket]} \text{ with } X \neq Z \\
& = \text{lfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P \rrbracket_{[[\rho|X_v \mapsto \llbracket Y \rrbracket]|Z_v \mapsto Z]} \\
& = \text{lfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P \rrbracket_{[[\rho|Z_v \mapsto Z]|X_v \mapsto \llbracket Y \rrbracket]} \\
& = \text{lfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P\{Y/X_v\} \rrbracket_{[\rho|Z_v \mapsto Z]} \quad (\text{ind. hyp.}) \\
& = \llbracket \mu Z_v.(P\{Y/X_v\}) \rrbracket_{\rho} \\
& = \llbracket (\mu Z_v.P)\{Y/X_v\} \rrbracket_{\rho} \\
& - \llbracket \nu X_v.P \rrbracket_{[\rho|X_v \mapsto \llbracket Y \rrbracket]} \\
& = \text{gfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P \rrbracket_{[[\rho|X_v \mapsto \llbracket Y \rrbracket]|X_v \mapsto Z]} \\
& = \text{gfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P \rrbracket_{[\rho|X_v \mapsto Z]} \\
& = \text{gfp}_{\emptyset}^{\subseteq} \lambda X. \llbracket P \rrbracket_{[\rho|X_v \mapsto X]} \\
& = \llbracket \nu X_v.P \rrbracket_{\rho} \\
& = \llbracket (\nu X_v.P)\{Y/X_v\} \rrbracket_{\rho} \\
& - \llbracket \nu Z.P \rrbracket_{[\rho|X_v \mapsto \llbracket Y \rrbracket]} \text{ with } X \neq Z \\
& = \text{gfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P \rrbracket_{[[\rho|X_v \mapsto \llbracket Y \rrbracket]|Z_v \mapsto Z]} \\
& = \text{gfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P \rrbracket_{[[\rho|Z_v \mapsto Z]|X_v \mapsto \llbracket Y \rrbracket]} \\
& = \text{gfp}_{\emptyset}^{\subseteq} \lambda Z. \llbracket P\{Y/X_v\} \rrbracket_{[\rho|Z_v \mapsto Z]} \quad (\text{ind. hyp.}) \\
& = \llbracket \nu Z.(P\{Y/X_v\}) \rrbracket_{\rho} \\
& = \llbracket (\nu Z.P)\{Y/X_v\} \rrbracket_{\rho} \\
& - \llbracket P[E'/x] \rrbracket_{[\rho|X_v \mapsto \llbracket Y \rrbracket]} \\
& = \{s, h \mid [s \mid x \mapsto \llbracket E' \rrbracket^s], h \in \llbracket P \rrbracket_{[\rho|X_v \mapsto \llbracket Y \rrbracket]}\} \\
& = \{s, h \mid [s \mid x \mapsto \llbracket E' \rrbracket^s], h \in \llbracket P\{Y/X_v\} \rrbracket_{\rho}\} \quad (\text{ind. hyp.}) \\
& = \llbracket P\{Y/X_v\}[E'/x] \rrbracket_{\rho} \\
& = \llbracket (P[E'/x])\{Y/X_v\} \rrbracket_{\rho} \\
& \square
\end{aligned}$$

Lemma 7. *If $\llbracket Y \rrbracket$ exists*

$$sp(P, C)\{Y/X_v\} = sp(P\{Y/X_v\}, C)$$

Proof (Lemma 7). Proof by induction on C .

$$\begin{aligned}
& - \text{Case } x := E \\
& \quad (sp(P, C)\{Y/X_v\}) \\
& = (\exists x'. P[x'/x] \wedge x = E[x'/x])\{Y/X_v\} \\
& = (\exists x'. (P\{Y/X_v\})[x'/x] \wedge x = E[x'/x]) \\
& = sp(P\{Y/X_v\}, C) \\
& - \text{Case } x := E.i \\
& \quad (sp(P, C)\{Y/X_v\}) \\
& = (\exists x'. P[x'/x] \wedge x = (E[x'/x].i))\{Y/X_v\} \\
& = (\exists x'. (P\{Y/X_v\})[x'/x] \wedge x = (E[x'/x].i)) \\
& = sp(P\{Y/X_v\}, C)
\end{aligned}$$

- Case $E.1 := E'$

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= (\exists x_1, x_2. (E \mapsto E', x_2) * ((E \mapsto x_1, x_2) \multimap P)\{Y/X_v\}) \\
&= (\exists x_1, x_2. (E \mapsto E', x_2) * ((E \mapsto x_1, x_2) \multimap (P\{Y/X_v\}))) \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$
- Case $E.2 := E'$

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= (\exists x_1, x_2. (E \mapsto E', x_2) * ((E \mapsto x_1, x_2) \multimap P)\{Y/X_v\}) \\
&= (\exists x_1, x_2. (E \mapsto x_1, E') * ((E \mapsto x_1, x_2) \multimap (P\{Y/X_v\}))) \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$
- Case $x := \text{cons}(E_1, E_2)$

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= \exists x'. (P[x'/x] * (x \mapsto E_1[x'/x], E_2[x'/x]))\{Y/X_v\} \\
&= \exists x'. ((P\{Y/X_v\})[x'/x] * (x \mapsto E_1[x'/x], E_2[x'/x])) \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$
- Case $\text{dispose}(E)$

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= \exists x_1, x_2. ((E \mapsto x_1, x_2) \multimap P)\{Y/X_v\} \\
&= \exists x_1, x_2. ((E \mapsto x_1, x_2) \multimap (P\{Y/X_v\})) \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$
- Case $C_1; C_2$

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= sp(sp(P, C_1), C_2)\{Y/X_v\} \\
&= sp(sp(P, C_1)\{Y/X_v\}, C_2) \text{ (ind.hyp)} \\
&= sp(sp(P\{Y/X_v\}, C_1), C_2) \text{ (ind.hyp)} \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$
- Case $\text{if } E \text{ then } C_1 \text{ else } C_2$

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= (sp(P \wedge E = \text{true}, C_1) \vee sp(P \wedge E = \text{false}, C_2))\{Y/X_v\} \\
&= sp(P \wedge E = \text{true}, C_1)\{Y/X_v\} \vee sp(P \wedge E = \text{false}, C_2)\{Y/X_v\} \\
&= sp(P\{Y/X_v\} \wedge E = \text{true}, C_1) \vee sp(P\{Y/X_v\} \wedge E = \text{false}, C_2) \text{ (ind. hyp.)} \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$
- Case **skip**

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= P\{Y/X_v\} \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$
- Case $\text{while } E \text{ do } C_1$

Case X_v not free in P

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= ((\mu X_v. sp(X_v \wedge E = \text{true}, C_1) \vee P) \wedge (E = \text{false}))\{Y/X_v\} \\
&= ((\mu X_v. sp(X_v \wedge E = \text{true}, C_1) \vee P) \wedge (E = \text{false})) \\
&= ((\mu X_v. sp(X_v \wedge E = \text{true}, C_1) \vee P\{Y/X_v\}) \wedge (E = \text{false})) \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$

Case X_v free in P

$$\begin{aligned}
& (sp(P, C)\{Y/X_v\}) \\
&= ((\mu Z_v.sp(Z_v \wedge E = \mathbf{true}, C_1) \vee P) \wedge (E = \mathbf{false}))\{Y/X_v\} \\
&= ((\mu Z_v.sp(Z_v \wedge E = \mathbf{true}, C_1) \vee P\{Y/X_v\}) \wedge (E = \mathbf{false})) \\
&= ((\mu W_v.sp(W_v \wedge E = \mathbf{true}, C_1) \vee P\{Y/X_v\}) \wedge (E = \mathbf{false})) \\
&= sp(P\{Y/X_v\}, C)
\end{aligned}$$

We have the equality between the case Z_v and W_v since $\llbracket Y \rrbracket$ exists so there is no free formula variables in Y , so neither Z_v or W_v can become bounded in some Y placed in P .

□