C Variable Renaming Theorem for $BI^{\mu\nu}$

Theorem 5. $\boxed{\begin{array}{l} \text{- } P \text{ is } v\text{-closed} \\ \textit{If} \text{ - } z \notin Var(P) \quad \textit{then } P \equiv P\{[z/y]\} \text{ .} \\ \text{- } y \notin FV(P) \end{array}}$

Lemma 1. $[\![E\{E'/x\}]\!]^s = [\![E]\!]^{[s|x\rightarrow [\![E']\!]^s]}$ *if* $[\![E']\!]^s$ *exists*

Proof. Lemma 1

- $[\![x\{E'/x\}]\!]^s = [\![E']\!]^s = [\![x]\!]^{[s|x\rightarrow [\![E']\!]^s]}$
- $[\![y\{E'/x\}]\!]^s = [\![y]\!]^s = [\![y]\!]^{[s|x\rightarrow [\![E']\!]^s]}$
- $[\![True\{E'/x\}]\!]^s = [\![True]\!]^s = true = [\![True]\!]^{[s|x\rightarrow [\![E']\!]^s]}$
- $[\![False\{E'/x\}]\!]^s = [\![False]\!]^s = false = [\![False]\!]^{[s|x\rightarrow [\![E']\!]^s]}$
- $[\![42\{E'/x\}]\!]^s = [\![42]\!]^s = 42 = [\![42]\!]^{[s|x\rightarrow [\![E']\!]^s]}$
- $[\![(E_1 \ op \ E_2)\{E'/x\}]\!]^s = [\![E_1\{E'/x\} \ op \ E_2\{E'/x\}]\!]^s = [\![E_1\{E'/x\}]\!]^s \ \ op \ \ [\![E_2\{E'/x\}]\!]^s = [\![E_1]\!]^{[s|x\rightarrow [\![E']\!]^s]} \ op \ [\![E_2]\!]^{[s|x\rightarrow [\![E']\!]^s]} = [\![E_1 \ op \ E_2]\!]^{[s|x\rightarrow [\![E']\!]^s]}$

Lemma 2. $[\![E\{z/y\}]\!]^s = [\![E]\!]^{[s|y\rightarrow s(z)]}$ *if* $z \in dom(s)$

Proof. Lemma 2 By Lemma 1. □

Lemma 3. $[\![E\{E'/x\}]\!]^s = [\![E]\!]^s$ *if* $[\![E']\!]^s$ *doesn't exists but* $[\![E\{E'/x\}]\!]^s$ *does*

Proof. Lemma 3 $[\![x\{E'/x\}]\!]^s = [\![E']\!]^s$
So $x \notin Var(E)$ and we directly have $E\{E'/x\} = E$

Lemma 4. $[\![E\{z/y\}]\!]^s = [\![E]\!]^s$ *if* $z \not\in dom(s)$

Proof. Lemma 4 By Lemma 3. □

Let $s^\bullet \triangleq \begin{cases} [s \mid y \rightarrow s(z)] & \text{if } z \in dom(s) \\ s & \text{if } z \notin dom(s) \end{cases}$
Let $\rho^\bullet$ be $[\forall X_v \in dom(\rho).\ X_v \rightarrow \{s, h \mid s^\bullet, h \in \rho(X_v)\}]$

Lemma 5. $[\![E\{z/y\}]\!]^s = [\![E]\!]^{s^\bullet}$

Proof. Lemma 5 By Lemma 2 and 4. □

Remember that in case P is $E = E'$, $E \mapsto E_1, E_2$, `false` and `emp` we have $\forall \rho. [\![P]\!]_\rho = [\![P]\!]$ since they are v-closed, see Lemma 6.
Remember $P \equiv Q$ iff $\forall \rho$. either ($[\![P]\!]_\rho$ and $[\![Q]\!]_\rho$ do not exist) either $[\![P]\!]_\rho = [\![Q]\!]_\rho$.

Proof (Th. 5). By Th. 6, $[\![P\{[z/y]\}]\!]_{\rho^\bullet} = \{s, h \mid s^\bullet, h \in [\![P]\!]_\rho\}$ in case $nodep(z, \rho)$ and $z \notin Var(P)$, then $[\![P\{[z/y]\}]\!] = \{s, h \mid s^\bullet, h \in [\![P]\!]\}$ if $z \notin Var(P)$.
Which is if $z \notin dom(s)$ then $s, h \in [\![P\{[z/y]\}]\!]iffs, h \in [\![P]\!]$ and if $z \in dom(s)$ we have $s, h \in [\![P\{[z/y]\}]\!]iff[s \mid y \rightarrow s(z)], h \in [\![P]\!]$.
Then since $y \notin FV(P)$ with the stack extension theorem 4 we have $nodep(y, P)$ and so $s, h \in$ so $[s \mid y \rightarrow s(z)], h \in [\![P]\!]iffs, h \in [\![P]\!]$.
We then have $[\![P\{[z/y]\}]\!] = [\![P]\!]$ which is what we wanted since P is v-closed (see Lemma 6). □

Theorem 6. *If* $\begin{array}{l}\text{- } nodep(z,\rho)\\ \text{- } z \notin Var(P)\end{array}$ *then* $[\![P\{[z/y]\}]\!]_{\rho^\bullet} = \{s,h \mid s^\bullet, h \in [\![P]\!]_\rho\}$

Proof (Th. 6). THE PROOF IS ONLY MADE IF ALL THE lfp and gpf are for MONOTONIC FUNCTIONS. But this is the case for the *wlp* and *sp* formulas and for the example in the paper.

We will prove by structural induction on P:
(recall that for $E1 = E2, E \mapsto E_1, E_2, \texttt{false}, \texttt{emp}$ $\forall\rho.[\![P]\!]_\rho = [\![P]\!]$*)*

– $[\![(E_1 = E_2)\{[z/y]\}]\!]$
$= [\![(E_1\{z/y\} = E_2\{z/y\}]\!]$
$= \{s,h \mid [\![E_1\{z/y\}]\!]^s = [\![E_2\{z/y\}]\!]^s\}$
$= \{s,h \mid [\![E_1]\!]^{s^\bullet} = [\![E_2]\!]^{s^\bullet}\}$
$= \{s,h \mid s^\bullet, h \in [\![E_1 = E_2]\!]\}$

– $[\![(E \mapsto E_1, E_2)\{[z/y]\}]\!]$
$= [\![E\{z/y\} \mapsto E_1\{z/y\}, E_2\{z/y\}]\!]$
$= \{s,h \mid dom(h) = \{[\![E\{z/y\}]\!]^s\}$ and $h([\![E\{z/y\}]\!]^s) = \langle [\![E_1\{z/y\}]\!]^s, [\![E_2\{z/y\}]\!]^s\rangle$
$= \{s,h \mid dom(h) = \{[\![E]\!]^{s^\bullet}\}$ and $h([\![E]\!]^{s^\bullet}) = \langle [\![E_1]\!]^{s^\bullet}, [\![E_2]\!]^{s^\bullet}\rangle\}$
$= \{s,h \mid s^\bullet, h \in [\![E \mapsto E_1, E_2]\!]\}$

– $[\![\texttt{false}\{[z/y]\}]\!]$
$= [\![\texttt{false}]\!]$
$= \emptyset$
$= \{s,h \mid s^\bullet, h \in [\![\texttt{false}]\!]$

– If $[\![P \Rightarrow Q]\!]_\rho$ exists then
$[\![(P \Rightarrow Q)\{[z/y]\}]\!]_{\rho^\bullet}$
$= [\![P\{[z/y]\} \Rightarrow Q\{[z/y]\}]\!]_{\rho^\bullet}$
$= (\top \setminus [\![P\{[z/y]\}]\!]_{\rho^\bullet}) \cup [\![Q\{[z/y]\}]\!]_{\rho^\bullet}$
$= (\top \setminus \{s,h \mid s^\bullet, h \in [\![P]\!]_\rho\}) \cup \{s,h \mid s^\bullet \in [\![Q]\!]_\rho\}$ *(ind.hyp.)*
$= \{s,h \mid s^\bullet, h \in (\top \setminus [\![P]\!]_\rho) \cup [\![Q]\!]_\rho\}$
$= \{s,h \mid s^\bullet, h \in [\![P \Rightarrow Q]\!]_\rho\}$

– $[\![(\exists x.\ P)\{[z/y]\}]\!]_{\rho^\bullet}$ when $x \neq y$
$= [\![\exists x.\ (P\{[z/y]\})]\!]_{\rho^\bullet}$
$= \{s,h \mid \exists v.[s \mid x \to v], h \in [\![P\{[z/y]\}]\!]_{\rho^\bullet}\}$
$= \{s,h \mid \exists v.[s \mid x \to v], h \in \{s,h \mid s^\bullet, h \in [\![P]\!]_\rho\}\}$ (ind.)
$= \{s,h \mid \exists v.[s \mid x \to v]^\bullet, h \in [\![P]\!]_\rho\}$
$= \{s,h \mid \exists v.[s^\bullet \mid x \to v], h \in [\![P]\!]_\rho\}$ (since $x \neq y, z$)
$= \{s,h \mid s^\bullet, h \in [\![\exists x.P]\!]_\rho\}$

– $[\![(\exists y.\ P)\{[z/y]\}]\!]_{\rho^\bullet}$
$= [\![\exists z.\ (P\{[z/y]\})]\!]_{\rho^\bullet}$
$= \{s,h \mid \exists v.[s \mid z \to v], h \in [\![P\{[z/y]\}]\!]_{\rho^\bullet}\}$
$= \{s,h \mid \exists v.[s \mid z \to v], h \in \{s,h \mid s^\bullet, h \in [\![P]\!]_\rho\}\}$ (ind.)
$= \{s,h \mid \exists v.[s \mid z \to v]^\bullet, h \in [\![P]\!]_\rho\}$
$= \{s,h \mid \exists v.[s \mid z \to v \mid y \to v], h \in [\![P]\!]_\rho\}$
$= \{s,h \mid \exists v.[s \mid y \to v \mid z \to v], h \in [\![P]\!]_\rho\}$ (since $z \neq y$)
$= \{s,h \mid \exists v.[s \mid y \to v], h \in [\![P]\!]_\rho\}$ (from stack extension theorem)
$= \{s,h \mid \exists v.[s^\bullet \mid y \to v], h \in [\![P]\!]_\rho\}$
$= \{s,h \mid s^\bullet, h \in [\![\exists y.P]\!]_\rho\}$

– $[\![\texttt{emp}\{[z/y]\}]\!]$
$= [\![\texttt{emp}]\!]$
$= \{s, h \mid h = []\}$
$= \{s, h \mid s^\bullet, h \in [\![emp]\!]\}$
– $[\![(P * Q)\{[z/y]\}]\!]_{\rho^\bullet}$
$= [\![(P\{[z/y]\} * Q\{[z/y]\})]\!]_{\rho^\bullet}$
$= \{s, h \mid \exists h_0, h_1.\ h_0 \sharp h_1, h_0.h_1 = h, s, h_0 \in [\![P\{[z/y]\}]\!]_{\rho^\bullet}$ and $s, h_1 \in [\![Q\{[z/y]\}]\!]_{\rho^\bullet}\}$
$= \{s, h \mid \exists h_0, h_1.\ h_0 \sharp h_1, h_0.h_1 = h, s^\bullet, h_0 \in [\![P]\!]_\rho$ and $s^\bullet, h_1 \in [\![Q]\!]_\rho\}$ (ind. hyp.)
$= \{s, h \mid s^\bullet, h \in [\![P * Q]\!]_\rho\}$
– $[\![(P -\!\!* Q)\{[z/y]\}]\!]_{\rho^\bullet}$
$= [\![P\{[z/y]\} -\!\!* Q\{[z/y]\}]\!]_{\rho^\bullet}$
$= \{s, h \mid \forall h'.$ if $h' \sharp h$ and $s, h' \in [\![P\{[z/y]\}]\!]_{\rho^\bullet}$ then $s, h.h' \in [\![Q\{[z/y]\}]\!]_{\rho^\bullet}\}$
$= \{s, h \mid \forall h'.$ if $h' \sharp h$ and $s^\bullet, h' \in [\![P]\!]_\rho$ then $s^\bullet, h.h' \in [\![Q]\!]_\rho\}$ (ind. hyp.)
$= \{s, h \mid s^\bullet, h \in [\![P -\!\!* Q]\!]_\rho\}$
– $[\![X_v\{[z/y]\}]\!]_{\rho^\bullet}$
$= [\![X_v]\!]_{\rho^\bullet}$
$= \rho^\bullet(X_v)$
$= \{s, h \mid s^\bullet, h \in \rho(X_v)\}$
$= \{s, h \mid s^\bullet, h \in [\![X_v]\!]_\rho\}$
– $[\![P[E/x]\{[z/y]\}]\!]_{\rho^\bullet}$ if $x \neq y$
$= [\![(P\{[z/y]\})[E\{z/y\}/x]]\!]_{\rho^\bullet}$
$= \{s, h \mid [s \mid x \to [\![E\{[z/y]\}]\!]^s], h \in [\![P\{[z/y]\}]\!]_{\rho^\bullet}\}$
$= \{s, h \mid [s \mid x \to [\![E]\!]^{s^\bullet}], h \in [\![P\{[z/y]\}]\!]_{\rho^\bullet}\}$
$= \{s, h \mid [s \mid x \to [\![E]\!]^{s^\bullet}], h \in \{s, h \mid s^\bullet, h \in [\![P]\!]_\rho\}\}$ (ind.)
$= \{s, h \mid ([s \mid x \to [\![E]\!]^{s^\bullet}])^\bullet, h \in [\![P]\!]_\rho\}$
$= \{s, h \mid [s^\bullet \mid x \to [\![E]\!]^{s^\bullet}], h \in [\![P]\!]_\rho\}$ (since $x \neq y, z$)
$= \{s, h \mid s^\bullet, h \in [\![P[E/x]]\!]_\rho\}$
– $[\![P[E/y]\{[z/y]\}]\!]_{\rho^\bullet}$
$= [\![(P\{[z/y]\})[E\{z/y\}/z]]\!]_{\rho^\bullet}$
$= \{s, h \mid [s \mid z \to [\![E\{[z/y]\}]\!]^s], h \in [\![P\{[z/y]\}]\!]_{\rho^\bullet}\}$
$= \{s, h \mid [s \mid z \to [\![E]\!]^{s^\bullet}], h \in [\![P\{[z/y]\}]\!]_{\rho^\bullet}\}$
$= \{s, h \mid [s \mid z \to [\![E]\!]^{s^\bullet}], h \in \{s, h \mid s^\bullet, h \in [\![P]\!]_\rho\}\}$ (ind.)
$= \{s, h \mid ([s \mid z \to [\![E]\!]^{s^\bullet}])^\bullet, h \in [\![P]\!]_\rho\}$
$= \{s, h \mid [s \mid z \to [\![E]\!]^{s^\bullet} \mid y \to [\![E]\!]^{s^\bullet}], h \in [\![P]\!]_\rho\}$
$= \{s, h \mid [s \mid y \to [\![E]\!]^{s^\bullet}], h \in [\![P]\!]_\rho\}$ (from stack extension th.)
$= \{s, h \mid [s^\bullet \mid y \to [\![E]\!]^{s^\bullet}], h \in [\![P]\!]_\rho\}$
$= \{s, h \mid s^\bullet, h \in [\![P[E/y]]\!]_\rho\}$
– If $[\![\mu X.P]\!]_\rho$ exists:
$[\![(\mu X.P)\{[z/y]\}]\!]_{\rho^\bullet}$
$= [\![\mu X.P\{[z/y]\}]\!]_{\rho^\bullet}$
$= \text{lfp}^{\subseteq}_{\emptyset}\ \lambda X.[\![P\{[z/y]\}]\!]_{[\rho^\bullet | X_v \to X]}$
see proof below
$= \{s, h \mid s^\bullet, h \in \text{lfp}^{\subseteq}_{\emptyset}\ \lambda X.[\![P]\!]_{[\rho | X_v \to X]}\}$
$= \{s, h \mid s^\bullet, h \in [\![\mu X.P]\!]_\rho\}$
Let

$F \triangleq \lambda X.[\![P\{[z/y]\}]\!]_{[\rho^\bullet|X_v \to X]}$
$A \triangleq \text{lfp}^{\subseteq}_{\emptyset} F$
$G \triangleq \lambda X.[\![P]\!]_{[\rho|X_v \to X]}$
$B \triangleq \text{lfp}^{\subseteq}_{\emptyset} G$
$C \triangleq \{s, h \mid s^\bullet, h \in B\}$
We want then $A = C$.
We know that B exists.
Notice that $([\rho \mid X_v \to B])^\bullet = [\rho^\bullet \mid X_v \to C]$.
First we prove that $A \subseteq C$, we prove it by proving that $C = F(C)$.
Since $B = [\![\mu X.P]\!]_{[\rho|X_v \to X]}$, by the stack extension theorem, we have $nodep(z, B)$ so $nodep(z, [\rho \mid X_v \to B])$ and we can use the induction.
By definition, $B = G(B)$, so $B = [\![P]\!]_{[\rho|X_v \to B]}$
and then $C = \{s, h \mid s^\bullet, h \in [\![P]\!]_{[\rho|X_v \to B]}\}$
by induction we then have $C = [\![P\{z/y\}]\!]_{([\rho|X_v \to B])^\bullet}$, which is $C = [\![P\{z/y\}]\!]_{[\rho^\bullet|X_v \to C]}$,
we then have $C = F(C)$ and so A exists and $A \subseteq C$.
Now we want to prove that $C \subseteq A$.
Let D be the biggest set such that $nodep(z, D)$ and $\{s, h \mid s^\bullet, h \in D\} \subseteq A$.
By the stack extension theorem, $nodep(z, [\![P]\!]_{[\rho|X_v \to D]})$ and we can use the induction.
Since we said we are working with monotonic functions, we have $F(\{s, h \mid s^\bullet, h \in D\}) \subseteq F(A)$
since A is a fix point we have then $F(\{s, h \mid s^\bullet, h \in D\}) \subseteq A$
which is $[\![P\{[z/y]\}]\!]_{[\rho^\bullet|X_v \to \{s,h|s^\bullet, h \in D\}]} \subseteq A$
by induction we have then $\{s, h \mid s^\bullet, h \in [\![P]\!]_{[\rho|X_v \to D]}\} \subseteq A$
which is $\{s, h \mid s^\bullet, h \in G(D)\} \subseteq A$
Then by construction of D as the biggest set we have $G(D) \subseteq D$
and then D is a postfixpoint of G and then $B \subseteq D$ and then $\{s, h \mid s^\bullet, h \in B\} \subseteq \{s, h \mid s^\bullet, h \in D\}$ which is $C \subseteq A$.

– If $[\![\nu X.P]\!]_\rho$ exists:
$[\![(\nu X.P)\{[z/y]\}]\!]_{\rho^\bullet}$
$= [\![\nu X.P\{[z/y]\}]\!]_{\rho^\bullet}$
$= \text{gfp}^{\subseteq}_{\emptyset}\ \lambda X.[\![P\{[z/y]\}]\!]_{[\rho^\bullet|X_v \to X]}$
see proof below
$= \{s, h \mid s^\bullet, h \in \text{gfp}^{\subseteq}_{\emptyset}\ \lambda X.[\![P]\!]_{[\rho|X_v \to X]}\}$
$= \{s, h \mid s^\bullet, h \in [\![\nu X.P]\!]_\rho\}$
Let
$F \triangleq \lambda X.[\![P\{[z/y]\}]\!]_{[\rho^\bullet|X_v \to X]}$
$A \triangleq \text{gfp}^{\subseteq}_{\emptyset} F$
$G \triangleq \lambda X.[\![P]\!]_{[\rho|X_v \to X]}$
$B \triangleq \text{gfp}^{\subseteq}_{\emptyset} G$
$C \triangleq \{s, h \mid s^\bullet, h \in B\}$
We want then $A = C$.
We know that B exists.
Notice that $([\rho \mid X_v B])^\bullet = [\rho^\bullet \mid X_v \to C]$.
First we prove that $A \supseteq C$, we prove it by proving that $C = F(C)$.

Since $B = [\![\nu X.P]\!]_{[\rho|X_v \to X]}$, by the stack extension theorem, we have $nodep(z, B)$ so $nodep(z, [\rho \mid X_v \to B])$ and we can use the induction.
By definition, $B = G(B)$, so $B = [\![P]\!]_{[\rho|X_v \to B]}$
and then $C = \{s, h \mid s^\bullet, h \in [\![P]\!]_{[\rho|X_v \to B]}\}$
by induction we then have $C = [\![P\{z/y\}]\!]_{([\rho|X_v \to B])^\bullet}$, which is $C = [\![P\{z/y\}]\!]_{[\rho^\bullet|X_v \to C]}$,
we then have $C = F(C)$ and so A exists and $A \supseteq C$.

Now we want to prove that $C \supseteq A$.
Let D be the smallest set such that $nodep(z, D)$ and $\{s, h \mid s^\bullet, h \in D\} \supseteq A$.
By the stack extension theorem, $nodep(z, [\![P]\!]_{[\rho|X_v \to D]})$ and we can use the induction.
Since we said we are working with monotonic functions, we have $F(\{s, h \mid s^\bullet, h \in D\}) \supseteq F(A)$
since A is a fix point we have then $F(\{s, h \mid s^\bullet, h \in D\}) \supseteq A$
which is $[\![P\{[z/y]\}]\!]_{[\rho^\bullet|X_v \to \{s,h|s^\bullet,h \in D\}]} \supseteq A$
by induction we have then $\{s, h \mid s^\bullet, h \in [\![P]\!]_{[\rho|X_v \to D]}\} \supseteq A$
which is $\{s, h \mid s^\bullet, h \in G(D)\} \supseteq A$
Then by construction of D as the smallest set we have $G(D) \supseteq D$
and then D is a prefixpoint of G and then $B \supseteq D$ and then $\{s, h \mid s^\bullet, h \in B\} \supseteq \{s, h \mid s^\bullet, h \in D\}$ which is $C \supseteq A$.
□

Lemma 6. *If P is v-closed formula: $\forall \rho. [\![P]\!]_\rho = [\![P]\!]$.*

Proof (Lemma 6). The simple case are direct from the definition of $[\![\cdot]\!]_\rho$, the others come by induction. □