Blame and Coercion: Together Again for the First Time

Supplementary Material

Jeremy Siek
Indiana University, USA
jsiek@indiana.edu

Peter Thiemann
Universität Freiburg, Germany
thiemann@informatik.uni-freiburg.de

Philip Wadler
University of Edinburgh, UK
wadler@inf.ed.ac.uk

PLDI'15, June 13–17, 2015, Portland, OR, USA.

http://dx.doi.org/10.1145/—

A. Positive and negative subtyping

Lemma 1 (Positive and negative subtyping)**.**

1. $A <:^+ B$ *iff* $|A \stackrel{p}{\Longrightarrow} B|^{\mathsf{BC}}\ \mathsf{safe_C}\ p$.
2. $A <:^- B$ *iff* $|A \stackrel{p}{\Longrightarrow} B|^{\mathsf{BC}}\ \mathsf{safe_C}\ \overline{p}$.

Proof. $A <:^+ B$ implies $|A \stackrel{p}{\Longrightarrow} B|^{\mathsf{BC}}\ \mathsf{safe_C}\ p$ and $A <:^- B$ implies $|A \stackrel{p}{\Longrightarrow} B|^{\mathsf{BC}}\ \mathsf{safe_C}\ \overline{p}$ is proved by mutual induction on the definition of $|A \stackrel{p}{\Longrightarrow} B|^{\mathsf{BC}}$.

Cases for positive subtyping:

Case $|\iota \stackrel{p}{\Longrightarrow} \iota|^{\mathsf{BC}} = \mathtt{id}_\iota$ satisfies $\iota <:^+ \iota$ and $\mathtt{id}_\iota\ \mathsf{safe_C}\ p$.

Case $|A \to B \stackrel{p}{\Longrightarrow} A' \to B'|^{\mathsf{BC}} = |A' \stackrel{\overline{p}}{\Longrightarrow} A|^{\mathsf{BC}} \to |B \stackrel{p}{\Longrightarrow} B'|^{\mathsf{BC}}$. From the assumption $A \to B <:^+ A' \to B'$, we obtain $A' <:^- A$ and $B <:^+ B'$. By induction, we get that $|A' \stackrel{\overline{p}}{\Longrightarrow} A|^{\mathsf{BC}}\ \mathsf{safe_C}\ \overline{\overline{p}}$ and $|B \stackrel{p}{\Longrightarrow} B'|^{\mathsf{BC}}\ \mathsf{safe_C}\ p$, which proves the claim.

Case $|\star \stackrel{p}{\Longrightarrow} \star|^{\mathsf{BC}} = \mathtt{id}_\star$ satisfies $\star <:^+ \star$ and $\mathtt{id}_\star\ \mathsf{safe_C}\ p$.

Case $|G \stackrel{p}{\Longrightarrow} \star|^{\mathsf{BC}} = G\mathtt{!}$. Immediate because $G <:^+ \star$.

Case $|A \stackrel{p}{\Longrightarrow} \star|^{\mathsf{BC}} = |A \stackrel{p}{\Longrightarrow} G|^{\mathsf{BC}}\ ;G\mathtt{!}$ where $A \neq \star$, $A \neq G$, and $A \sim G$. Hence, it must be that $G = \star \to \star$ and $A = A' \to B'$ so that $|A \stackrel{p}{\Longrightarrow} G|^{\mathsf{BC}} = |A' \to B' \stackrel{p}{\Longrightarrow} \star \to \star|^{\mathsf{BC}} = |\star \stackrel{\overline{p}}{\Longrightarrow} A'|^{\mathsf{BC}} \to |B' \stackrel{p}{\Longrightarrow} \star|^{\mathsf{BC}}$. Since $\star <:^- A'$ and $B' <:^+ \star$, the result holds by induction.

Case $|\star \stackrel{p}{\Longrightarrow} G|^{\mathsf{BC}}$. Not applicable because $\star \not<:^+ G$.

Case $|\star \stackrel{p}{\Longrightarrow} A|^{\mathsf{BC}}$ where $A \neq \star$, $A \neq G$, and $A \sim G$. Not applicable because $\star \not<:^+ A$.

Cases for negative subtyping:

Case $|\iota \stackrel{p}{\Longrightarrow} \iota|^{\mathsf{BC}} = \mathtt{id}_\iota$ satisfies $\iota <:^- \iota$ and $\mathtt{id}_\iota\ \mathsf{safe_C}\ \overline{p}$.

Case $|A \to B \stackrel{p}{\Longrightarrow} A' \to B'|^{\mathsf{BC}} = |A' \stackrel{\overline{p}}{\Longrightarrow} A|^{\mathsf{BC}} \to |B \stackrel{p}{\Longrightarrow} B'|^{\mathsf{BC}}$. From the assumption $A \to B <:^- A' \to B'$, we obtain $A' <:^+ A$ and $B <:^- B'$. By induction, we get that $|A' \stackrel{\overline{p}}{\Longrightarrow} A|^{\mathsf{BC}}\ \mathsf{safe_C}\ \overline{p}$ and $|B \stackrel{p}{\Longrightarrow} B'|^{\mathsf{BC}}\ \mathsf{safe_C}\ \overline{p}$, which proves the claim.

Case $|\star \stackrel{p}{\Longrightarrow} \star|^{\mathsf{BC}} = \mathtt{id}_\star$ satisfies $\star <:^- \star$ and $\mathtt{id}_\star\ \mathsf{safe_C}\ \overline{p}$.

Case $|G \stackrel{p}{\Longrightarrow} \star|^{\mathsf{BC}} = G\mathtt{!}$. Immediate because $G <:^- \star$.

Case $|A \stackrel{p}{\Longrightarrow} \star|^{\mathsf{BC}} = |A \stackrel{p}{\Longrightarrow} G|^{\mathsf{BC}}\ ;G\mathtt{!}$. If $A <:^- \star$, then it must be that $A <:^- G$. Hence, the claim holds by induction.

Case $|\star \stackrel{p}{\Longrightarrow} G|^{\mathsf{BC}} = G\mathtt{?}^p$ is safe for $\overline{p}$ and $\star <:^- G$ holds.

Case $|\star \stackrel{p}{\Longrightarrow} B|^{\mathsf{BC}} = G\mathtt{?}^p\ ; |G \stackrel{p}{\Longrightarrow} B|^{\mathsf{BC}}$ (where $B \neq \star$, $B \neq G$, and $G \sim B$). $\star <:^- B$ is satisfied regardless of B. Hence, it must be that $G = \star \to \star$ so that $B = A' \to B'$ and we need to examine $|\star \to \star \stackrel{p}{\Longrightarrow} A' \to B'|^{\mathsf{BC}} = |A' \stackrel{\overline{p}}{\Longrightarrow} \star|^{\mathsf{BC}} \to |\star \stackrel{p}{\Longrightarrow} B'|^{\mathsf{BC}}$. As $A' <:^+ \star$ and $\star <:^- B'$ we can argue by induction that $|A' \stackrel{\overline{p}}{\Longrightarrow} \star|^{\mathsf{BC}}\ \mathsf{safe_C}\ \overline{p}$ and $|\star \stackrel{p}{\Longrightarrow} B'|^{\mathsf{BC}}\ \mathsf{safe_C}\ \overline{p}$.

The reverse implication is proved by similar mutual induction on the definition of the translation. □

B. Bisimulation between coercions and threesomes

Here we give the full proof of Proposition 16.

Lemma 2 (Compose Identity Threesomes)**.** $s \mathbin{;} |\mathtt{id}_A|^{\mathsf{CS}} = s$ *and* $|\mathtt{id}_A|^{\mathsf{CS}} \mathbin{;} s = s$

Proof. The proof is a straightforward induction on s and A. □

Lemma 3. *If* $M\langle s\rangle \longrightarrow^* V_1$ *and* $V_1\langle t\rangle \longrightarrow^* V_2$*,*
then $M\langle s \mathbin{;} t\rangle \longrightarrow^* V_2$.

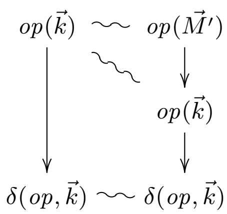
Proof of Proposition 16. Part 1 and 2. We proceed by case analysis on $M \approx M'$, in each case proving the two statements:

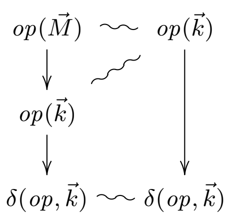
1. If $M \longrightarrow_{\mathsf{C}} N$ then $M' \longrightarrow^*_{\mathsf{S}} N'$ and $N \approx N'$ for some N'.
2. If $M' \longrightarrow_{\mathsf{S}} N'$ then $M \longrightarrow^*_{\mathsf{C}} N$ and $N \approx N'$ for some N.

(Here we assume parts 3 and 4, which we later prove independently.)

Case $\dfrac{}{k \approx k}$ Both statements are vacuously true because k cannot reduce.

Case $\dfrac{\vec{M} \approx \vec{M}'}{op(\vec{M}) \approx op(\vec{M}')}$

1.


2.


Case $\dfrac{}{x \approx x}$

Both statements are vacuously true because x cannot reduce.

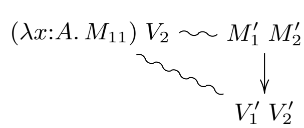
Case $\dfrac{M \approx M'}{\lambda x{:}A.\, M \approx \lambda x{:}A.\, M'}$

Both statements are vacouously true because lambda terms cannot reduce.

Case $\dfrac{M_1 \approx M_1' \qquad M_2 \approx M_2'}{M_1\ M_2 \approx M_1'\ M_2'}$

1. We proceed by case analysis on $M = M_1\ M_2 \longrightarrow_{\mathsf{C}} N$. So either M_1 reduces, M_2 reduces, or they are both values.
   Suppose M_1 reduces, i.e., $M_1 \longrightarrow_{\mathsf{C}} M_3$. From $M_1\ M_2 \approx M'$, we have $M' = M_1'\ M_2'$ and $M_1 \approx M_1'$ and $M_2 \approx M_2'$. By the induction hypothesis, $M_1' \longrightarrow^*_{\mathsf{S}} M_3'$ and $M_3 \approx M_3'$. So $M_1'\ M_2' \longrightarrow^*_{\mathsf{S}} M_3'\ M_2'$ and $M_3\ M_2 \approx M_3'\ M_2'$.
   The case for M_2 reducing is essentialy the same as for M_1 reducing.
   Suppose M_1 and M_2 are values. We proceed by cases on M_1.
   - $M_1 = k$: M cannot reduce;
   - $M_1 = \lambda x{:}A.\, M_{11}$: part of beta redex, see (a) below;
   - $M_1 = V\langle c \to d\rangle$: part of coercion redex, see (b) below;
   - $M_1 = V\langle G!\rangle$: M cannot reduce.

   Let $V_2 = M_2$.
   (a) $(\lambda x{:}A.\, M_{11})\ V_2 \longrightarrow_{\mathsf{C}} M_{11}[x := V]$ We have



   then proceed by case analysis on $(\lambda x{:}A.\, M_{11}) \approx V_1'$.

Subcase $\dfrac{M_{11} \approx M'_{11}}{\lambda x{:}A.\, M_{11} \approx \lambda x{:}A.\, M'_{11}}$

$$\begin{array}{ccc}
(\lambda x{:}A.\, M_{11})\ V_2 & \sim\!\sim & (\lambda x{:}A.\, M'_{11})\ V'_2 \\
\downarrow & & \downarrow \\
M_{11}[x := V_2] & \sim\!\sim\!\sim & M'_{11}[x := V'_2]
\end{array}$$

Subcase $\dfrac{\lambda x{:}A.\, M_{11} \approx U'}{\lambda x{:}A.\, M_{11} \approx U'\langle |\mathtt{id}_{A\to B}|^{\mathsf{CS}}\rangle}$

$$\begin{array}{ccc}
(\lambda x{:}A.\, M_{11})\ V_2 & \sim\!\sim\!\sim\!\sim\!\sim\!\sim & U'\langle |\mathtt{id}_{A\to B}|^{\mathsf{CS}}\rangle\ V'_2 \\
\Big\downarrow & & \downarrow \\
 & & (U'\ V'_2\langle |\mathtt{id}_A|^{\mathsf{CS}}\rangle)\langle |\mathtt{id}_B|^{\mathsf{CS}}\rangle \\
 & & \| \\
 & & ((\lambda x{:}A.\, M'_{11})\ V'_2\langle |\mathtt{id}_A|^{\mathsf{CS}}\rangle)\langle |\mathtt{id}_B|^{\mathsf{CS}}\rangle \\
 & & \downarrow \\
M_{11}[x := V_2] & \sim\!\sim\!\sim & M'_{11}[x := V'_2\langle |\mathtt{id}_A|^{\mathsf{CS}}\rangle]\langle |\mathtt{id}_B|^{\mathsf{CS}}\rangle
\end{array}$$

(b) $(V\langle c \to d\rangle)\ W \longrightarrow_{\mathsf{C}} (V\ W\langle c\rangle)\langle d\rangle$
We proceed by induction on $V\langle c \to d\rangle \approx M'_1$. There are two cases to consider. (Rule (iii) does not apply because the premise would relate a value to a function application.)
Subcase rule (i).

$$\frac{V\langle c{\to}d\rangle \approx M'_{11} \qquad \vdash V\langle c{\to}d\rangle : A{\to}B}{V\langle c \to d\rangle \approx M'_{11}\langle \mathtt{id}_A{\to}\mathtt{id}_B\rangle}$$

We have $M'_{11} \longrightarrow^* V'_{11}$ and $V\langle c \to d\rangle \approx V'_{11}$ by induction. So we have $V'_{11} = U'\langle (s_1 \to s_2)\,;\,|c \to d|^{\mathsf{CS}}\rangle$ and $V \approx U'\langle s_1 \to s_2\rangle$.

$$\begin{array}{ccc}
(V\langle c \to d\rangle)\ W & \sim\!\sim\!\sim\!\sim\!\sim\!\sim\!\sim & (M'_{11}\langle \mathtt{id}_A{\to}\mathtt{id}_B\rangle)\ M'_2 \\
\Big\downarrow & & \downarrow \\
 & & U'\langle (s_1 \to s_2)\,;\,|c \to d|^{\mathsf{CS}}\rangle\langle \mathtt{id}_A{\to}\mathtt{id}_B\rangle\ V'_2 \\
 & & \downarrow \\
 & & U'\langle (s_1 \to s_2)\,;\,|c \to d|^{\mathsf{CS}}\,;\,(\mathtt{id}_A{\to}\mathtt{id}_B)\rangle\ V'_2 \\
 & & \|\ \text{Lemma 2} \\
(V\ W\langle c\rangle)\langle d\rangle & \sim\!\sim\!\sim\!\sim\!\sim & (U'\langle (s_1 \to s_2)\,;\,|c \to d|^{\mathsf{CS}}\rangle)\ V'_2
\end{array}$$

The left is related to the right by rule (iii).
Subcase rule (ii).

$$\begin{array}{ccc}
(V\langle c \to d\rangle)\ W & \sim\!\sim & (M'_{11}\langle s\,;\,|c|^{\mathsf{CS}} \to |d|^{\mathsf{CS}}\rangle)\ M'_2 \\
\downarrow & \swarrow\!\sim\!\sim\!\sim & \\
(V\ W\langle c\rangle)\langle d\rangle & &
\end{array}$$

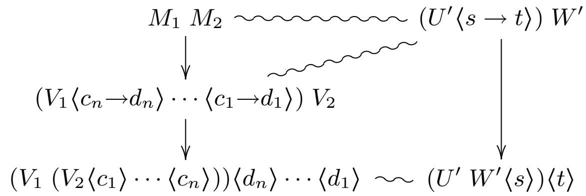
because

$$\dfrac{\dfrac{V \approx M'_{11}\langle s\rangle \qquad \dfrac{W \approx M'_2}{W\langle c\rangle \approx M'_2\langle |c|^{\mathsf{CS}}\rangle}}{V\ W\langle c\rangle \approx (M'_{11}\langle s\rangle)\ (M'_2\langle |c|^{\mathsf{CS}}\rangle)}}{(V\ W\langle c\rangle)\langle d\rangle \approx (M'_{11}\langle s\,;\,|c|^{\mathsf{CS}} \to |d|^{\mathsf{CS}}\rangle)\ M'_2}$$

2. We proceed by case analysis on $M'_1\ M'_2 \longrightarrow_{\mathsf{S}} N'$.
 (a) Case $(\lambda x{:}A.\, M'_{11})\ V'_2 \longrightarrow_{\mathsf{S}} M'_{11}[x := V'_2]$

$$\begin{array}{ccc}
M_1\ M_2 & \sim\!\sim\!\sim\!\sim & (\lambda x{:}A.\, M'_{11})\ V'_2 \\
\downarrow & \swarrow\!\sim\!\sim\!\sim & \Big\downarrow \\
(\lambda x{:}A.\, M_{11})\ V_2 & & \\
\downarrow & & \\
M_{11}[x := V_2] & \sim\!\sim\!\sim & M'_{11}[x := V'_2]
\end{array}$$

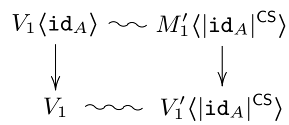
(b) Case $(U'\langle s \to t\rangle)\ W' \longrightarrow_{\mathsf{S}} (U'\ W'\langle s\rangle)\langle t\rangle$



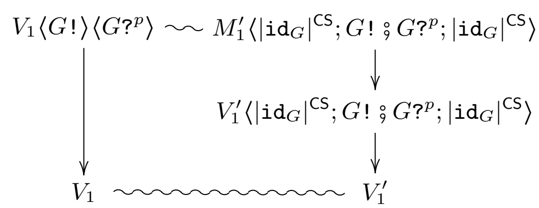
Case $\dfrac{M_1 \approx M_1' \qquad |c|^{\mathsf{CS}} = s}{M_1\langle c\rangle \approx M_1'\langle s\rangle}$

1. We proceed by case analysis on $M_1\langle c\rangle \longrightarrow_{\mathsf{C}} N$.

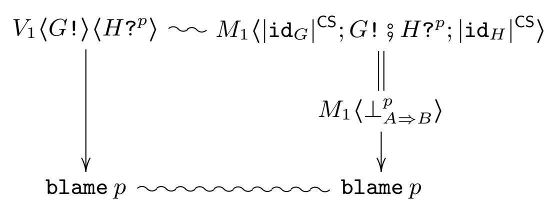
   (a) Case $V_1\langle \mathtt{id}_A\rangle \longrightarrow_{\mathsf{C}} V_1$



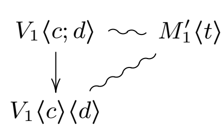
   (b) Case $V_1\langle G!\rangle\langle G?^p\rangle \longrightarrow_{\mathsf{C}} V_1$



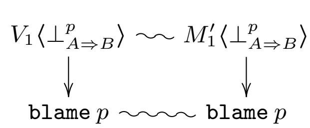
   (c) Case $V_1\langle G!\rangle\langle H?^p\rangle \longrightarrow_{\mathsf{C}} \mathtt{blame}\ p$



   (d) Case $V_1\langle c; d\rangle \longrightarrow_{\mathsf{C}} V_1\langle c\rangle\langle d\rangle$

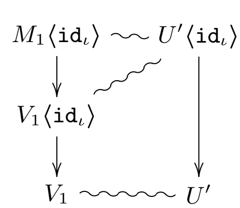


   (e) Case $V_1\langle \bot^p_{A \Rightarrow B}\rangle \longrightarrow_{\mathsf{C}} \mathtt{blame}\ p$

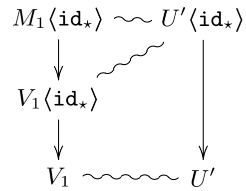


2. We proceed by case analysis on $M_1'\langle t\rangle \longrightarrow_{\mathsf{S}} N'$.

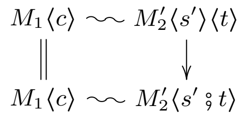
   (a) Case $U'\langle \mathtt{id}_\iota\rangle \longrightarrow_{\mathsf{S}} U'$



(b) Case $U'\langle \mathtt{id}_\star \rangle \longrightarrow_{\mathsf{S}} U'$

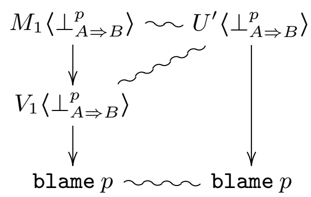


(c) Case $M_2'\langle s' \rangle\langle t \rangle \longrightarrow_{\mathsf{S}} M_2'\langle s' \mathbin{⨟} t \rangle$



We have $M_1 \approx M_2'\langle s' \rangle$ and therefore $M_1\langle c \rangle \approx M_2'\langle s' \mathbin{⨟} t \rangle$.

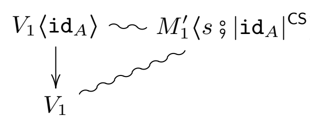
(d) Case $U'\langle \bot^p_{A \Rightarrow B} \rangle \longrightarrow_{\mathsf{S}} \mathtt{blame}\, p$



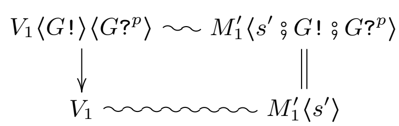
Case $\dfrac{M_1 \approx M_1'\langle s \rangle \qquad |c|^{\mathsf{CS}} = t}{M_1\langle c \rangle \approx M_1'\langle s \mathbin{⨟} t \rangle}$

1. We proceed by case analysis on $M_1\langle c \rangle \longrightarrow_{\mathsf{C}} N$.

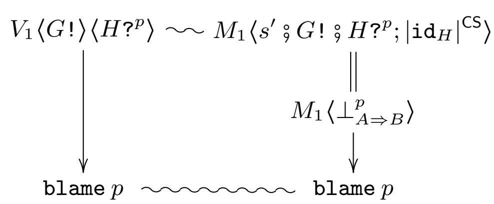
(a) Case $V_1\langle \mathtt{id}_A \rangle \longrightarrow_{\mathsf{C}} V_1$



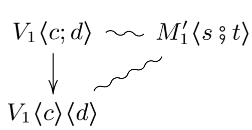
(b) Case $V_1\langle G! \rangle\langle G?^p \rangle \longrightarrow_{\mathsf{C}} V_1$



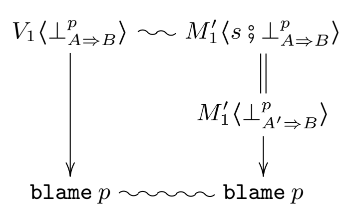
(c) Case $V_1\langle G! \rangle\langle H?^p \rangle \longrightarrow_{\mathsf{C}} \mathtt{blame}\, p$



(d) Case $V_1\langle c ; d \rangle \longrightarrow_{\mathsf{C}} V_1\langle c \rangle\langle d \rangle$



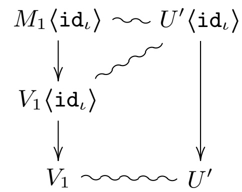
(e) Case $V_1\langle \bot^p_{A \Rightarrow B} \rangle \longrightarrow_{\mathsf{C}} \mathtt{blame}\, p$



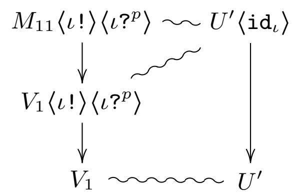
2. We proceed by case analysis on $M'_1\langle s \mathbin{⨾} t\rangle \longrightarrow_{\mathsf{S}} N'$.

(a) Case $U'\langle \mathtt{id}_\iota\rangle \longrightarrow_{\mathsf{S}} U'$.
There are two cases for $s \mathbin{⨾} t = \mathtt{id}_\iota$:

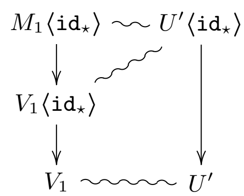
i. $s = t = \mathtt{id}_\iota$



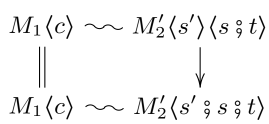
ii. $s = \mathtt{id}_\iota; \iota!$ and $t = \iota?^p; \mathtt{id}_\iota$. In that case, the assumption is $M_1 \approx U'\langle \mathtt{id}_\iota; \iota!\rangle$. By inversion, $M_1 = M_{11}\langle \iota!\rangle$ and $M_{11} \approx U'\langle \mathtt{id}_\iota\rangle$. By further inversion, $M_{11} \approx U'$. Hence:



(b) Case $U'\langle \mathtt{id}_\star\rangle \longrightarrow_{\mathsf{S}} U'$



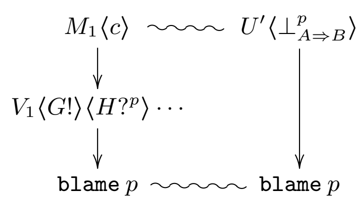
(c) Case $M'_2\langle s'\rangle\langle s \mathbin{⨾} t\rangle \longrightarrow_{\mathsf{S}} M'_2\langle s' \mathbin{⨾} s \mathbin{⨾} t\rangle$



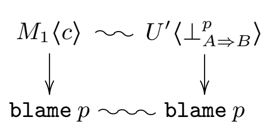
We have $M_1 \approx M'_2\langle s'\rangle\langle s\rangle$ and therefore $M_1 \approx M'_2\langle s' \mathbin{⨾} s\rangle$. With $|t|^{\mathsf{CS}} = c$ we conclude $M_1\langle c\rangle \approx M'_2\langle s' \mathbin{⨾} s \mathbin{⨾} t\rangle$.

(d) Case $U'\langle \bot^p_{A\Rightarrow B}\rangle \longrightarrow_{\mathsf{S}} \mathtt{blame}\ p$
There are three ways that we could have $s \mathbin{⨾} t = \bot^p_{A\Rightarrow B}$.

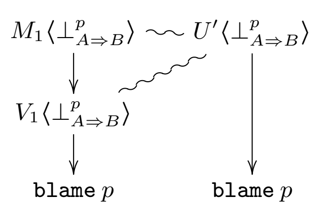
i. $s = (g; G!), t = (H?^p; i)$



ii. $s = \bot^p_{A\Rightarrow B}$
We have $M_1 \approx U'\langle \bot^p_{A\Rightarrow B}\rangle$ so by the induction hypothesis $M_1 \longrightarrow^* \mathtt{blame}\ p$.

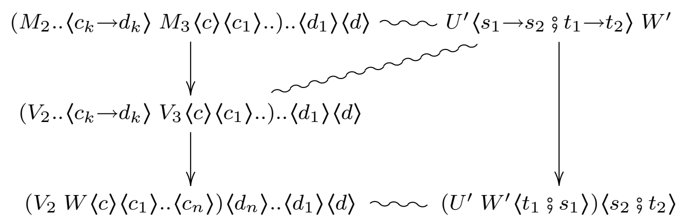


iii. $t = \bot^p_{A\Rightarrow B}$

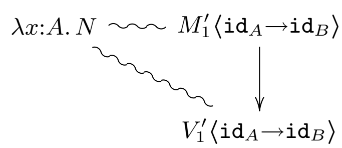


Case $\dfrac{M_1 \approx M_1'\langle s\rangle\ M_2'\langle t_1\rangle \qquad |d|^{\mathsf{CS}} = t_2}{M_1\langle d\rangle \approx M_1'\langle s \mathbin{⨟} (t_1{\to}t_2)\rangle\ M_2'}$

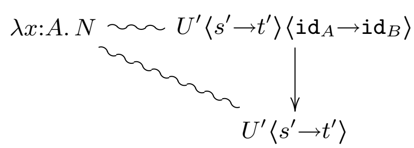
1. We proceed by case analysis on $M_1\langle d\rangle \longrightarrow_{\mathsf{C}} N$, but every case is vacuously true because they require M_1 to be a value, but M_1 corresponds to a function application.
2. We proceed by cases on $M_1'\langle s \mathbin{⨟} (t_1{\to}t_2)\rangle\ M_2' \longrightarrow_{\mathsf{S}} N'$.
   We have $M_1 \approx U'\langle s_1{\to}s_2\rangle\ W'\langle t_1\rangle$.
   So $M_1 = (M_2 \cdots\ M_3\langle c\rangle\langle c_1\rangle \cdots) \cdots \langle d_1\rangle$
   where $|c{\to}d|^{\mathsf{CS}} = t_1{\to}t_2$
   and $|c_1{\to}d_1; \cdots ; c_n{\to}d_n|^{\mathsf{CS}} = s_1{\to}s_2$.



Part 3. We show that the term M' on the right can become a value V' that corresponds to V. We proceed by induction on V.
Case $V = k$. We proceed by cases on $k \approx M'$, but we only have one case to consider.
Subcase $\dfrac{}{k \approx k}$ Take $V' = k$.
Case $V = \lambda x{:}A.\, N$. We proceed by induction on $(\lambda x{:}A.\, N) \approx M'$.
Subcase $\dfrac{N \approx N'}{\lambda x{:}A.\, N \approx \lambda x{:}A.\, N'}$
We take $V' = \lambda x{:}A.\, N'$.
Subcase $\dfrac{\lambda x{:}A.\, N \approx M_1' \qquad |\mathtt{id}_{A\to B}|^{\mathsf{CS}} = \mathtt{id}_A \to \mathtt{id}_B}{\lambda x{:}A.\, N \approx M_1'\langle \mathtt{id}_A \to \mathtt{id}_B\rangle}$
By the inner induction hypothesis we have the following.

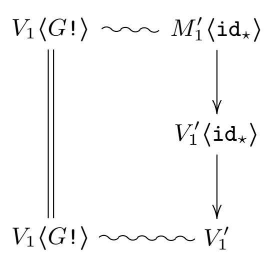


Now suppose $V_1' = \lambda x{:}A.\, N'$. Then $V_1'\langle \mathtt{id}_A{\to}\mathtt{id}_B\rangle$ is a value.
On the other hand, suppose $V_1' = U'\langle s'{\to}t'\rangle$.



Case $V = V_1\langle G!\rangle$. We proceed by induction on $V_1\langle G!\rangle \approx M'$. There is one case to consider. (Rule (iii) does not apply because the premises would relate a value to a function application.)
Subcase rule (i)

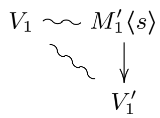
$$\frac{V_1\langle G!\rangle \approx M_1'}{V_1\langle G!\rangle \approx M_1'\langle |\mathtt{id}_\star|^{\mathsf{CS}}\rangle}$$



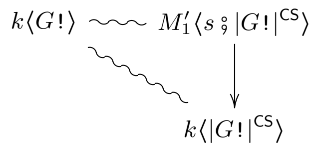
Subcase rule (ii)

$$\frac{V_1 \approx M_1'\langle s\rangle}{V_1\langle G!\rangle \approx M_1'\langle s \mathbin{⨟} |G!|^{\mathsf{CS}}\rangle}$$

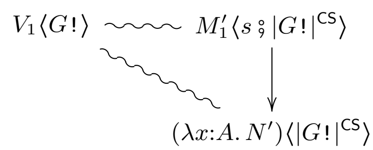
The inner induction hypothesis gives us



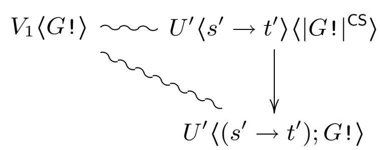
Suppose $V_1' = k$. Then $k\langle |G!|^{\mathsf{CS}}\rangle$ is a value. By Lemma 3 we have



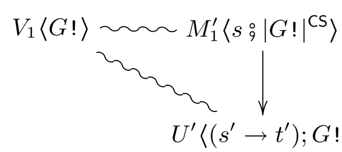
Suppose $V_1' = \lambda x{:}A.\, N'$. Then $(\lambda x{:}A.\, N')\langle |G!|^{\mathsf{CS}}\rangle$ is a value. By Lemma 3 we have



Suppose $V_1' = U'\langle g; H!\rangle$. Then V_1' has type $\star$, but that contradicts it having type G.
Suppose $V_1' = U'\langle s' \to t'\rangle$. We have



By Lemma 3 we conclude



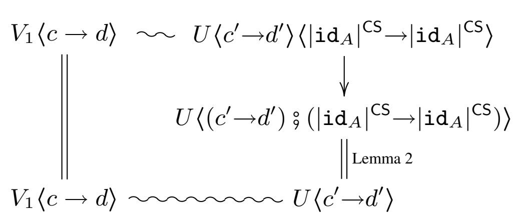
Case $V = V_1\langle c \to d\rangle$. We proceed by induction on $V_1\langle c \to d\rangle \approx M'$. There are three cases to consider. (Rule (iii) does not apply because the premise would relate a value to a function application.)

Subcase rule (i)

$$\frac{V_1\langle c \to d\rangle \approx M_1' \qquad \vdash V_1\langle c{\to}d\rangle : A{\to}B \qquad |\mathtt{id}_{A\to B}|^{\mathsf{CS}} = t}{V_1\langle c \to d\rangle \approx M_1'\langle t\rangle}$$

We have $M_1' \longrightarrow^* V_1'$ and $V_1\langle c \to d\rangle \approx V_1'$ by the inner induction hypothesis. We proceed by cases on V_1' with the knowledge that it is of function type.

Suppose $V_1' = \lambda x{:}A.\, e$. Then $V_1'\langle \mathtt{id}_A \to \mathtt{id}_B\rangle$ is a value and we relate the left to the right by rule (i).
Suppose $V_1' = U\langle c'{\to}d'\rangle$.



Subcase rule (ii)

$$\frac{V_1 \approx M_1'\langle s\rangle \qquad |c \to d|^{\mathsf{CS}} = t}{V_1\langle c \to d\rangle \approx M_1'\langle s \mathbin{;} t\rangle}$$

We have $M_1'\langle s\rangle \longrightarrow^* V_1'$ and $V_1 \approx V_1'$ by the inner induction hypothesis. Then applying some case analysis on V_1' we have $V_1'\langle |c|^{\mathsf{CS}} \to |d|^{\mathsf{CS}}\rangle \longrightarrow V'$ and $V_1\langle c \to d\rangle \approx V'$ for some V'.

Part 4. We show that the term M on the left can become a value that corresponds to V'. We proceed by induction on V'.

Case $V' = k$. By inversion on $M \approx k$ we have $M = k$, which is already a value, so we take $V = M$.

Case $V' = \lambda x{:}A.\ N$. By inversion on $M \approx \lambda x{:}A.\ N$ we have $M = \lambda x{:}A.\, N'$ and take $V = M$.

Case $V' = U'\langle s \to t\rangle$. Inversion of $M \approx U'\langle s \to t\rangle$ gives us two cases to consider.

Subcase for rule (i)

$$\frac{M \approx U' \qquad \vdash M : A \qquad |\mathtt{id}_A|^{\mathsf{CS}} = s \to t}{M \approx U'\langle s \to t\rangle}$$

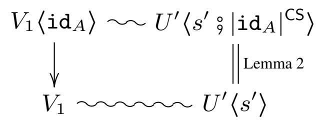
By the induction hypothesis, $M \longrightarrow_{\mathsf{C}}^{*} V$ where $V \approx U'$. Then the left and right sides are related by rule (i).

Subcase for rule (ii).

$$\frac{M_1 \approx U'\langle s'\rangle \qquad |c|^{\mathsf{CS}} = t'}{M_1\langle c\rangle \approx U'\langle s' \mathbin{⨾} t'\rangle}$$

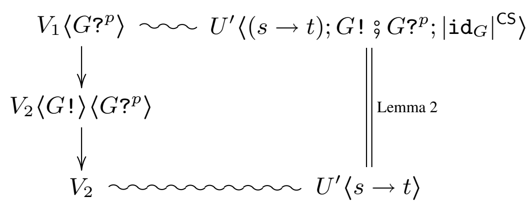
We have $M = M_1\langle c\rangle$ and $(s' \mathbin{⨾} t') = s \to t$. By the induction hypothesis, $M_1 \longrightarrow_{\mathsf{C}}^{*} V_1$ where $V_1 \approx U'\langle s'\rangle$. We proceed with a nested induction on c.

Suppose $c = \mathtt{id}_A$.



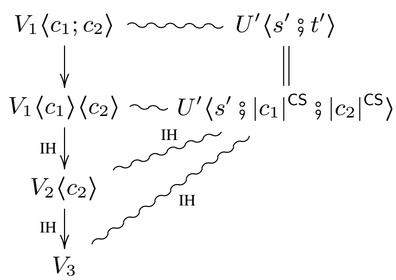
Suppose $c = G!$. Then $t' = |G!|^{\mathsf{CS}} = |\mathtt{id}_G|^{\mathsf{CS}}; G!$, but that contradicts $(s' \mathbin{⨾} t') = s \to t$.

Suppose $c = G?^p$. Then $t' = G?^p; |\mathtt{id}_G|^{\mathsf{CS}}$. With $(s' \mathbin{⨾} t') = s \to t$, we have $s' = (s \to t); G!$. Then from $V_1 \approx U'\langle (s \to t); G!\rangle$ we have $V_1 = V_2\langle G!\rangle$ with $V_2 \approx U'\langle s \to t\rangle$ for some V_2. So we obtain:



Next suppose $c = c_1 \to c_2$, then $V_1\langle c_1 \to c_2\rangle$ is already a value. From $V_1 \approx U'\langle s'\rangle$ and $|c|^{\mathsf{CS}} = t'$ we have $V_1\langle c\rangle \approx U'\langle s' \mathbin{⨾} t'\rangle$ by rule (ii).

Suppose $c = (c_1; c_2)$. We have $t' = |c_1|^{\mathsf{CS}} \mathbin{⨾} |c_2|^{\mathsf{CS}}$. We obtain the following with two uses of the the inner induction hypothesis.



Suppose $c = \bot^p_{A\Rightarrow B}$. Then $t' = \bot^p_{A\Rightarrow B}$ and $(s' \mathbin{⨾} t') = \bot^p_{-\Rightarrow B}$, but $(s' \mathbin{⨾} t') = s \to t$ so we have a contradiction.

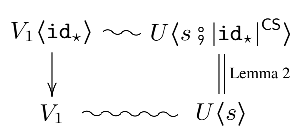
Case $V' = U\langle g; G!\rangle$. Considering $M \approx U\langle g; G!\rangle$, only rule (ii) applies.

Subcase (ii):

$$\frac{M_1 \approx U\langle s\rangle \qquad |c|^{\mathsf{CS}} = t}{M_1\langle c\rangle \approx U\langle s \mathbin{⨾} t\rangle}$$

By the induction hypothesis, we have $M_1 \longrightarrow_{\mathsf{C}}^{*} V_1$ and $V_1 \approx U\langle s\rangle$. We proceed by nested induction on c.

Suppose $c = \mathtt{id}_\star$.

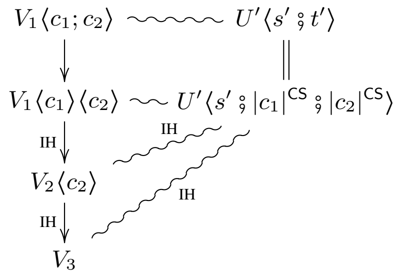


Suppose $c = H!$. Then we have $V_1\langle H!\rangle \approx U\langle s \mathbin{⨾} |H!|^{\mathsf{CS}}\rangle$.

Suppose $c = H?^p$. Then $t = |H?^p|^{\mathsf{CS}} = H?^p; |\mathtt{id}_H|^{\mathsf{CS}}$. But that contradicts $(s \mathbin{⨾} t) = (g; G!)$.

Suppose $c = c_1 \to c_2$. Then $t = |c_1 \to c_2|^{\mathsf{CS}} = |c_1|^{\mathsf{CS}} \to |c_2|^{\mathsf{CS}}$. But that contradicts $(s \mathbin{⨾} t) = (g; G!)$.

Suppose $c = (c_1; c_2)$. We use the same reasoning as for the corresponding case in $V' = U\langle s \to t\rangle$, that is, we obtain the following with two uses of the the inner induction hypothesis.



Suppose $c = \bot^p_{A \Rightarrow B}$. Then $t' = \bot^p_{A \Rightarrow B}$ and $(s' \mathbin{⨾} t') = \bot^p_{- \Rightarrow B}$, but $(s' \mathbin{⨾} t') = (g; G!)$ so we have a contradiction.

Part 5 and 6.

Case $\dfrac{}{\texttt{blame}\ p \approx \texttt{blame}\ p}$

□

C. Translation is bisimilar

Here we sketch the proof of Proposition 17.

Proposition 17. $M \approx |M|^{\mathsf{CS}}$.

Proof. (Sketch). By induction on M. The only non-trivial case is for $M\langle c\rangle$ where we need to apply rules (i) and (ii) to establish $\approx$. In all other cases, the congruence rules are sufficient. □