

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

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

PLDI'15, June 13–17, 2015, Portland, OR, USA.
Copyright © 2015 ACM 978-1-4503-3468-6/15/06...\$15.00.
[http://dx.doi.org/10.1145/—](http://dx.doi.org/10.1145/)

A. Positive and negative subtyping

Lemma 1 (Positive and negative subtyping).

1. $A <:^+ B$ iff $|A \xRightarrow{p} B|^{\text{BC}} \text{ safe}_C p$.
2. $A <:^- B$ iff $|A \xRightarrow{p} B|^{\text{BC}} \text{ safe}_C \bar{p}$.

Proof. $A <:^+ B$ implies $|A \xRightarrow{p} B|^{\text{BC}} \text{ safe}_C p$ and $A <:^- B$ implies $|A \xRightarrow{p} B|^{\text{BC}} \text{ safe}_C \bar{p}$ is proved by mutual induction on the definition of $|A \xRightarrow{p} B|^{\text{BC}}$.

Cases for positive subtyping:

Case $|\iota \xRightarrow{p} \iota|^{\text{BC}} = \text{id}_\iota$ satisfies $\iota <:^+ \iota$ and $\text{id}_\iota \text{ safe}_C p$.

Case $|A \rightarrow B \xRightarrow{p} A' \rightarrow B'|^{\text{BC}} = |A' \xRightarrow{\bar{p}} A|^{\text{BC}} \rightarrow |B \xRightarrow{p} B'|^{\text{BC}}$. From the assumption $A \rightarrow B <:^+ A' \rightarrow B'$, we obtain $A' <:^- A$ and $B <:^+ B'$. By induction, we get that $|A' \xRightarrow{\bar{p}} A|^{\text{BC}} \text{ safe}_C \bar{p}$ and $|B \xRightarrow{p} B'|^{\text{BC}} \text{ safe}_C p$, which proves the claim.

Case $|\star \xRightarrow{p} \star|^{\text{BC}} = \text{id}_\star$ satisfies $\star <:^+ \star$ and $\text{id}_\star \text{ safe}_C p$.

Case $|G \xRightarrow{p} \star|^{\text{BC}} = G!$. Immediate because $G <:^+ \star$.

Case $|A \xRightarrow{p} \star|^{\text{BC}} = |A \xRightarrow{p} G|^{\text{BC}} ; G!$ where $A \neq \star$, $A \neq G$, and $A \sim G$. Hence, it must be that $G = \star \rightarrow \star$ and $A = A' \rightarrow B'$ so that $|A \xRightarrow{p} G|^{\text{BC}} = |A' \rightarrow B' \xRightarrow{p} \star \rightarrow \star|^{\text{BC}} = |\star \xRightarrow{\bar{p}} A'|^{\text{BC}} \rightarrow |B' \xRightarrow{p} \star|^{\text{BC}}$. Since $\star <:^- A'$ and $B' <:^+ \star$, the result holds by induction.

Case $|\star \xRightarrow{p} G|^{\text{BC}}$. Not applicable because $\star \not<:^+ G$.

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

Cases for negative subtyping:

Case $|\iota \xRightarrow{p} \iota|^{\text{BC}} = \text{id}_\iota$ satisfies $\iota <:^- \iota$ and $\text{id}_\iota \text{ safe}_C \bar{p}$.

Case $|A \rightarrow B \xRightarrow{p} A' \rightarrow B'|^{\text{BC}} = |A' \xRightarrow{\bar{p}} A|^{\text{BC}} \rightarrow |B \xRightarrow{p} B'|^{\text{BC}}$. From the assumption $A \rightarrow B <:^- A' \rightarrow B'$, we obtain $A' <:^+ A$ and $B <:^- B'$. By induction, we get that $|A' \xRightarrow{\bar{p}} A|^{\text{BC}} \text{ safe}_C \bar{p}$ and $|B \xRightarrow{p} B'|^{\text{BC}} \text{ safe}_C \bar{p}$, which proves the claim.

Case $|\star \xRightarrow{p} \star|^{\text{BC}} = \text{id}_\star$ satisfies $\star <:^- \star$ and $\text{id}_\star \text{ safe}_C \bar{p}$.

Case $|G \xRightarrow{p} \star|^{\text{BC}} = G!$. Immediate because $G <:^- \star$.

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

Case $|\star \xRightarrow{p} G|^{\text{BC}} = G?^p$ is safe for \bar{p} and $\star <:^- G$ holds.

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

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). $s \mathbin{\text{\$}} |\text{id}_A|^{\text{CS}} = s$ and $|\text{id}_A|^{\text{CS}} \mathbin{\text{\$}} s = s$

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 $M \langle s \mathbin{\text{\$}} t \rangle \longrightarrow^* V_2$.

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

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

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

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

$$1. \begin{array}{ccc} op(\vec{k}) & \rightsquigarrow & op(\vec{M}') \\ \downarrow & \rightsquigarrow & \downarrow \\ & & op(\vec{k}) \\ \downarrow & & \downarrow \\ \delta(op, \vec{k}) & \rightsquigarrow & \delta(op, \vec{k}) \end{array}$$

$$2. \begin{array}{ccc} op(\vec{M}) & \rightsquigarrow & op(\vec{k}) \\ \downarrow & \rightsquigarrow & \downarrow \\ & & op(\vec{k}) \\ \downarrow & & \downarrow \\ \delta(op, \vec{k}) & \rightsquigarrow & \delta(op, \vec{k}) \end{array}$$

Case $\frac{x \approx x}{x \approx x}$

Both statements are vacuously true because x cannot reduce.

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

Both statements are vacuously true because lambda terms cannot reduce.

Case $\frac{M_1 \approx M'_1 \quad M_2 \approx M'_2}{M_1 M_2 \approx M'_1 M'_2}$

1. We proceed by case analysis on $M = M_1 M_2 \longrightarrow_{\text{C}} N$. So either M_1 reduces, M_2 reduces, or they are both values.
Suppose M_1 reduces, i.e., $M_1 \longrightarrow_{\text{C}} M_3$. 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, $M'_1 \longrightarrow_{\text{S}}^* M'_3$ and $M_3 \approx M'_3$. So $M'_1 M'_2 \longrightarrow_{\text{S}}^* M'_3 M'_2$ and $M_3 M_2 \approx M'_3 M'_2$.

The case for M_2 reducing is essentially 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;
- $M_1 = V \langle c \rightarrow d \rangle$: part of coercion redex, see (b) below;
- $M_1 = V \langle G! \rangle$: M cannot reduce.

Let $V_2 = M_2$.

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

$$\begin{array}{ccc} (\lambda x:A. M_{11}) V_2 & \rightsquigarrow & M'_1 M'_2 \\ & \rightsquigarrow & \downarrow \\ & & V'_1 V'_2 \end{array}$$

then proceed by case analysis on $(\lambda x:A. M_{11}) \approx V'_1$.

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

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

$$\text{Subcase } \frac{\lambda x:A. M_{11} \approx U'}{\lambda x:A. M_{11} \approx U' \langle |\text{id}_{A \rightarrow B}|^{\text{CS}} \rangle}$$

$$\begin{array}{ccc} (\lambda x:A. M_{11}) V_2 & \rightsquigarrow & U' \langle |\text{id}_{A \rightarrow B}|^{\text{CS}} \rangle V'_2 \\ \downarrow & & \downarrow \\ M_{11}[x := V_2] & \rightsquigarrow & M'_{11}[x := V'_2 \langle |\text{id}_A|^{\text{CS}} \rangle \langle |\text{id}_B|^{\text{CS}} \rangle] \\ & & \downarrow \\ & & ((\lambda x:A. M'_{11}) V'_2 \langle |\text{id}_A|^{\text{CS}} \rangle \langle |\text{id}_B|^{\text{CS}} \rangle) \langle |\text{id}_B|^{\text{CS}} \rangle \\ & & \downarrow \\ & & M'_{11}[x := V'_2 \langle |\text{id}_A|^{\text{CS}} \rangle \langle |\text{id}_B|^{\text{CS}} \rangle] \end{array}$$

(b) $(V \langle c \rightarrow d \rangle) W \rightarrow_c (V W \langle c \rangle) \langle d \rangle$

We proceed by induction on $V \langle c \rightarrow d \rangle \approx M'_1$. 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).

$$\frac{V \langle c \rightarrow d \rangle \approx M'_{11} \quad \vdash V \langle c \rightarrow d \rangle : A \rightarrow B}{V \langle c \rightarrow d \rangle \approx M'_{11} \langle \text{id}_A \rightarrow \text{id}_B \rangle}$$

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

$$\begin{array}{ccc} (V \langle c \rightarrow d \rangle) W & \rightsquigarrow & (M'_{11} \langle \text{id}_A \rightarrow \text{id}_B \rangle) M'_2 \\ \downarrow & & \downarrow \\ (V W \langle c \rangle) \langle d \rangle & \rightsquigarrow & U' \langle (s_1 \rightarrow s_2) \ ; \ |c \rightarrow d|^{\text{CS}} \rangle \langle \text{id}_A \rightarrow \text{id}_B \rangle V'_2 \\ & & \downarrow \\ & & U' \langle (s_1 \rightarrow s_2) \ ; \ |c \rightarrow d|^{\text{CS}} \ ; \ (\text{id}_A \rightarrow \text{id}_B) \rangle V'_2 \\ & & \parallel \text{Lemma 2} \\ & & U' \langle (s_1 \rightarrow s_2) \ ; \ |c \rightarrow d|^{\text{CS}} \rangle V'_2 \end{array}$$

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

Subcase rule (ii).

$$\begin{array}{ccc} (V \langle c \rightarrow d \rangle) W & \rightsquigarrow & (M'_{11} \langle s \ ; \ |c|^{\text{CS}} \rightarrow |d|^{\text{CS}} \rangle) M'_2 \\ \downarrow & & \downarrow \\ (V W \langle c \rangle) \langle d \rangle & \rightsquigarrow & \end{array}$$

because

$$\frac{\frac{V \approx M'_{11} \langle s \rangle \quad \frac{W \approx M'_2}{W \langle c \rangle \approx M'_2 \langle |c|^{\text{CS}} \rangle}}{V W \langle c \rangle \approx (M'_{11} \langle s \rangle) (M'_2 \langle |c|^{\text{CS}} \rangle)}}{(V W \langle c \rangle) \langle d \rangle \approx (M'_{11} \langle s \ ; \ |c|^{\text{CS}} \rightarrow |d|^{\text{CS}} \rangle) M'_2}$$

2. We proceed by case analysis on $M'_1 M'_2 \rightarrow_S N'$.

(a) Case $(\lambda x:A. M'_{11}) V'_2 \rightarrow_S M'_{11}[x := V'_2]$

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

(b) Case $(U'(s \rightarrow t)) W' \longrightarrow_S (U' W'(s)) \langle t \rangle$

$$\begin{array}{ccc}
 M_1 M_2 \rightsquigarrow (U'(s \rightarrow t)) W' & & \\
 \downarrow & \rightsquigarrow & \downarrow \\
 (V_1 \langle c_n \rightarrow d_n \rangle \cdots \langle c_1 \rightarrow d_1 \rangle) V_2 & & \\
 \downarrow & & \downarrow \\
 (V_1 (V_2 \langle c_1 \rangle \cdots \langle c_n \rangle)) \langle d_n \rangle \cdots \langle d_1 \rangle \rightsquigarrow (U' W'(s)) \langle t \rangle
 \end{array}$$

Case $\frac{M_1 \approx M'_1 \quad |c|^{\text{CS}} = s}{M_1 \langle c \rangle \approx M'_1 \langle s \rangle}$

1. We proceed by case analysis on $M_1 \langle c \rangle \longrightarrow_C N$.

(a) Case $V_1 \langle \text{id}_A \rangle \longrightarrow_C V_1$

$$\begin{array}{ccc}
 V_1 \langle \text{id}_A \rangle \rightsquigarrow M'_1 \langle |\text{id}_A|^{\text{CS}} \rangle & & \\
 \downarrow & \rightsquigarrow & \downarrow \\
 V_1 \rightsquigarrow V'_1 \langle |\text{id}_A|^{\text{CS}} \rangle
 \end{array}$$

(b) Case $V_1 \langle G! \rangle \langle G?^p \rangle \longrightarrow_C V_1$

$$\begin{array}{ccc}
 V_1 \langle G! \rangle \langle G?^p \rangle \rightsquigarrow M'_1 \langle |\text{id}_G|^{\text{CS}}; G! \ ; G?^p; |\text{id}_G|^{\text{CS}} \rangle & & \\
 \downarrow & \rightsquigarrow & \downarrow \\
 V_1 \rightsquigarrow V'_1 & & V'_1 \langle |\text{id}_G|^{\text{CS}}; G! \ ; G?^p; |\text{id}_G|^{\text{CS}} \rangle \\
 & & \downarrow
 \end{array}$$

(c) Case $V_1 \langle G! \rangle \langle H?^p \rangle \longrightarrow_C \text{blame } p$

$$\begin{array}{ccc}
 V_1 \langle G! \rangle \langle H?^p \rangle \rightsquigarrow M_1 \langle |\text{id}_G|^{\text{CS}}; G! \ ; H?^p; |\text{id}_H|^{\text{CS}} \rangle & & \\
 \downarrow & \rightsquigarrow & \parallel \\
 \text{blame } p \rightsquigarrow \text{blame } p & & M_1 \langle \perp_{A \Rightarrow B}^p \rangle \\
 & & \downarrow
 \end{array}$$

(d) Case $V_1 \langle c; d \rangle \longrightarrow_C V_1 \langle c \rangle \langle d \rangle$

$$\begin{array}{ccc}
 V_1 \langle c; d \rangle \rightsquigarrow M'_1 \langle t \rangle & & \\
 \downarrow & \rightsquigarrow & \\
 V_1 \langle c \rangle \langle d \rangle
 \end{array}$$

(e) Case $V_1 \langle \perp_{A \Rightarrow B}^p \rangle \longrightarrow_C \text{blame } p$

$$\begin{array}{ccc}
 V_1 \langle \perp_{A \Rightarrow B}^p \rangle \rightsquigarrow M'_1 \langle \perp_{A \Rightarrow B}^p \rangle & & \\
 \downarrow & \rightsquigarrow & \downarrow \\
 \text{blame } p \rightsquigarrow \text{blame } p
 \end{array}$$

2. We proceed by case analysis on $M'_1 \langle t \rangle \longrightarrow_S N'$.

(a) Case $U' \langle \text{id}_i \rangle \longrightarrow_S U'$

$$\begin{array}{ccc}
 M_1 \langle \text{id}_i \rangle \rightsquigarrow U' \langle \text{id}_i \rangle & & \\
 \downarrow & \rightsquigarrow & \downarrow \\
 V_1 \langle \text{id}_i \rangle & & \\
 \downarrow & & \downarrow \\
 V_1 \rightsquigarrow U'
 \end{array}$$

(b) Case $U' \langle \text{id}_* \rangle \longrightarrow_S U'$

$$\begin{array}{ccc} M_1 \langle \text{id}_* \rangle & \rightsquigarrow & U' \langle \text{id}_* \rangle \\ \downarrow & \rightsquigarrow & \downarrow \\ V_1 \langle \text{id}_* \rangle & & \\ \downarrow & & \\ V_1 & \rightsquigarrow & U' \end{array}$$

(c) Case $M'_2 \langle s' \rangle \langle t \rangle \longrightarrow_S M'_2 \langle s' \ ; t \rangle$

$$\begin{array}{ccc} M_1 \langle c \rangle & \rightsquigarrow & M'_2 \langle s' \rangle \langle t \rangle \\ \parallel & & \downarrow \\ M_1 \langle c \rangle & \rightsquigarrow & M'_2 \langle s' \ ; t \rangle \end{array}$$

We have $M_1 \approx M'_2 \langle s' \rangle$ and therefore $M_1 \langle c \rangle \approx M'_2 \langle s' \ ; t \rangle$.

(d) Case $U' \langle \perp_{A \Rightarrow B}^p \rangle \longrightarrow_S \text{blame } p$

$$\begin{array}{ccc} M_1 \langle \perp_{A \Rightarrow B}^p \rangle & \rightsquigarrow & U' \langle \perp_{A \Rightarrow B}^p \rangle \\ \downarrow & \rightsquigarrow & \downarrow \\ V_1 \langle \perp_{A \Rightarrow B}^p \rangle & & \\ \downarrow & & \\ \text{blame } p & \rightsquigarrow & \text{blame } p \end{array}$$

Case $\frac{M_1 \approx M'_1 \langle s \rangle \quad |c|^{\text{CS}} = t}{M_1 \langle c \rangle \approx M'_1 \langle s \ ; t \rangle}$

1. We proceed by case analysis on $M_1 \langle c \rangle \longrightarrow_C N$.

(a) Case $V_1 \langle \text{id}_A \rangle \longrightarrow_C V_1$

$$\begin{array}{ccc} V_1 \langle \text{id}_A \rangle & \rightsquigarrow & M'_1 \langle s \ ; |\text{id}_A|^{\text{CS}} \rangle \\ \downarrow & \rightsquigarrow & \\ V_1 & & \end{array}$$

(b) Case $V_1 \langle G! \rangle \langle G?^p \rangle \longrightarrow_C V_1$

$$\begin{array}{ccc} V_1 \langle G! \rangle \langle G?^p \rangle & \rightsquigarrow & M'_1 \langle s' \ ; G! \ ; G?^p \rangle \\ \downarrow & & \parallel \\ V_1 & \rightsquigarrow & M'_1 \langle s' \rangle \end{array}$$

(c) Case $V_1 \langle G! \rangle \langle H?^p \rangle \longrightarrow_C \text{blame } p$

$$\begin{array}{ccc} V_1 \langle G! \rangle \langle H?^p \rangle & \rightsquigarrow & M_1 \langle s' \ ; G! \ ; H?^p \ ; |\text{id}_H|^{\text{CS}} \rangle \\ \downarrow & & \parallel \\ \text{blame } p & \rightsquigarrow & M_1 \langle \perp_{A \Rightarrow B}^p \rangle \\ & & \downarrow \\ & & \text{blame } p \end{array}$$

(d) Case $V_1 \langle c; d \rangle \longrightarrow_C V_1 \langle c \rangle \langle d \rangle$

$$\begin{array}{ccc} V_1 \langle c; d \rangle & \rightsquigarrow & M'_1 \langle s \ ; t \rangle \\ \downarrow & \rightsquigarrow & \\ V_1 \langle c \rangle \langle d \rangle & & \end{array}$$

(e) Case $V_1 \langle \perp_{A \Rightarrow B}^p \rangle \longrightarrow_C \text{blame } p$

$$\begin{array}{ccc} V_1 \langle \perp_{A \Rightarrow B}^p \rangle & \rightsquigarrow & M'_1 \langle s \ ; \perp_{A \Rightarrow B}^p \rangle \\ \downarrow & & \parallel \\ \text{blame } p & \rightsquigarrow & M'_1 \langle \perp_{A \Rightarrow B}^p \rangle \\ & & \downarrow \\ & & \text{blame } p \end{array}$$

2. We proceed by case analysis on $M_1'(s \ ; \ t) \longrightarrow_S N'$.

(a) Case $U' \langle \text{id}_i \rangle \longrightarrow_S U'$.

There are two cases for $s \ ; \ t = \text{id}_i$:

i. $s = t = \text{id}_i$,

$$\begin{array}{ccc} M_1 \langle \text{id}_i \rangle & \rightsquigarrow & U' \langle \text{id}_i \rangle \\ \downarrow & \rightsquigarrow & \downarrow \\ V_1 \langle \text{id}_i \rangle & & \\ \downarrow & & \downarrow \\ V_1 & \rightsquigarrow & U' \end{array}$$

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

$$\begin{array}{ccc} M_{11} \langle \iota! \rangle \langle \iota^{?P} \rangle & \rightsquigarrow & U' \langle \text{id}_i \rangle \\ \downarrow & \rightsquigarrow & \downarrow \\ V_1 \langle \iota! \rangle \langle \iota^{?P} \rangle & & \\ \downarrow & & \downarrow \\ V_1 & \rightsquigarrow & U' \end{array}$$

(b) Case $U' \langle \text{id}_* \rangle \longrightarrow_S U'$

$$\begin{array}{ccc} M_1 \langle \text{id}_* \rangle & \rightsquigarrow & U' \langle \text{id}_* \rangle \\ \downarrow & \rightsquigarrow & \downarrow \\ V_1 \langle \text{id}_* \rangle & & \\ \downarrow & & \downarrow \\ V_1 & \rightsquigarrow & U' \end{array}$$

(c) Case $M_2'(s') \langle s \ ; \ t \rangle \longrightarrow_S M_2'(s' \ ; \ s \ ; \ t)$

$$\begin{array}{ccc} M_1 \langle c \rangle & \rightsquigarrow & M_2'(s') \langle s \ ; \ t \rangle \\ \parallel & & \downarrow \\ M_1 \langle c \rangle & \rightsquigarrow & M_2'(s' \ ; \ s \ ; \ t) \end{array}$$

We have $M_1 \approx M_2'(s') \langle s \rangle$ and therefore $M_1 \approx M_2'(s' \ ; \ s)$. With $|t|^{\text{CS}} = c$ we conclude $M_1 \langle c \rangle \approx M_2'(s' \ ; \ s \ ; \ t)$.

(d) Case $U' \langle \perp_{A \Rightarrow B}^p \rangle \longrightarrow_S \text{blame } p$

There are three ways that we could have $s \ ; \ t = \perp_{A \Rightarrow B}^p$.

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

$$\begin{array}{ccc} M_1 \langle c \rangle & \rightsquigarrow & U' \langle \perp_{A \Rightarrow B}^p \rangle \\ \downarrow & & \downarrow \\ V_1 \langle G! \rangle \langle H^{?P} \rangle \dots & & \\ \downarrow & & \downarrow \\ \text{blame } p & \rightsquigarrow & \text{blame } p \end{array}$$

ii. $s = \perp_{A \Rightarrow B}^p$

We have $M_1 \approx U' \langle \perp_{A \Rightarrow B}^p \rangle$ so by the induction hypothesis $M_1 \longrightarrow^* \text{blame } p$.

$$\begin{array}{ccc} M_1 \langle c \rangle & \rightsquigarrow & U' \langle \perp_{A \Rightarrow B}^p \rangle \\ \downarrow & & \downarrow \\ \text{blame } p & \rightsquigarrow & \text{blame } p \end{array}$$

iii. $t = \perp_{A \Rightarrow B}^p$

$$\begin{array}{ccc} M_1 \langle \perp_{A \Rightarrow B}^p \rangle & \rightsquigarrow & U' \langle \perp_{A \Rightarrow B}^p \rangle \\ \downarrow & \rightsquigarrow & \downarrow \\ V_1 \langle \perp_{A \Rightarrow B}^p \rangle & & \\ \downarrow & & \downarrow \\ \text{blame } p & & \text{blame } p \end{array}$$

$$\text{Case } \frac{M_1 \approx M'_1 \langle s \rangle M'_2 \langle t_1 \rangle \quad |d|^{CS} = t_2}{M_1 \langle d \rangle \approx M'_1 \langle s \rangle \langle t_1 \rightarrow t_2 \rangle M'_2}$$

1. We proceed by case analysis on $M_1 \langle d \rangle \rightarrow_C N$, 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 $M'_1 \langle s \rangle \langle t_1 \rightarrow t_2 \rangle M'_2 \rightarrow_S N'$.
We have $M_1 \approx U' \langle s_1 \rightarrow s_2 \rangle W' \langle t_1 \rangle$.
So $M_1 = (M_2 \cdots M_3 \langle c \rangle \langle c_1 \rangle \cdots) \cdots \langle d_1 \rangle$
where $|c \rightarrow d|^{CS} = t_1 \rightarrow t_2$
and $|c_1 \rightarrow d_1; \cdots; c_n \rightarrow d_n|^{CS} = s_1 \rightarrow s_2$.

$$\begin{array}{ccc} (M_2 \cdots \langle c_k \rightarrow d_k \rangle M_3 \langle c \rangle \langle c_1 \rangle \cdots \langle d_1 \rangle \langle d \rangle \rightsquigarrow U' \langle s_1 \rightarrow s_2 \rangle \langle t_1 \rightarrow t_2 \rangle W' & & \\ \downarrow & \rightsquigarrow & \downarrow \\ (V_2 \cdots \langle c_k \rightarrow d_k \rangle V_3 \langle c \rangle \langle c_1 \rangle \cdots \langle d_1 \rangle \langle d \rangle & & \\ \downarrow & & \downarrow \\ (V_2 W \langle c \rangle \langle c_1 \rangle \cdots \langle c_n \rangle \langle d_n \rangle \cdots \langle d_1 \rangle \langle d \rangle \rightsquigarrow (U' W' \langle t_1 \rangle \langle s_1 \rangle) \langle s_2 \rangle \langle t_2 \rangle \end{array}$$

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 $\frac{k \approx k}{\text{Take } V' = k.}$

Case $V = \lambda x:A. N$. We proceed by induction on $(\lambda x:A. N) \approx M'$.

Subcase $\frac{N \approx N'}{\lambda x:A. N \approx \lambda x:A. N'}$

We take $V' = \lambda x:A. N'$.

Subcase $\frac{\lambda x:A. N \approx M'_1 \quad |\text{id}_{A \rightarrow B}|^{CS} = \text{id}_A \rightarrow \text{id}_B}{\lambda x:A. N \approx M'_1 \langle \text{id}_A \rightarrow \text{id}_B \rangle}$

By the inner induction hypothesis we have the following.

$$\begin{array}{ccc} \lambda x:A. N \rightsquigarrow M'_1 \langle \text{id}_A \rightarrow \text{id}_B \rangle & & \\ \rightsquigarrow & \downarrow & \\ & V'_1 \langle \text{id}_A \rightarrow \text{id}_B \rangle & \end{array}$$

Now suppose $V'_1 = \lambda x:A. N'$. Then $V'_1 \langle \text{id}_A \rightarrow \text{id}_B \rangle$ is a value.

On the other hand, suppose $V'_1 = U' \langle s' \rightarrow t' \rangle$.

$$\begin{array}{ccc} \lambda x:A. N \rightsquigarrow U' \langle s' \rightarrow t' \rangle \langle \text{id}_A \rightarrow \text{id}_B \rangle & & \\ \rightsquigarrow & \downarrow & \\ & U' \langle s' \rightarrow t' \rangle & \end{array}$$

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)

$$\begin{array}{ccc} \frac{V_1 \langle G! \rangle \approx M'_1}{V_1 \langle G! \rangle \approx M'_1 \langle |\text{id}_*|^{CS} \rangle} & & \\ V_1 \langle G! \rangle \rightsquigarrow M'_1 \langle \text{id}_* \rangle & & \downarrow \\ \parallel & & V'_1 \langle \text{id}_* \rangle \\ & & \downarrow \\ V_1 \langle G! \rangle \rightsquigarrow V'_1 & & \end{array}$$

Subcase rule (ii)

$$\frac{V_1 \approx M'_1 \langle s \rangle}{V_1 \langle G! \rangle \approx M'_1 \langle s \rangle \langle G! \rangle^{CS}}$$

The inner induction hypothesis gives us $V_1 \rightsquigarrow M'_1 \langle s \rangle$

$$\begin{array}{c} V_1 \rightsquigarrow M'_1 \langle s \rangle \\ \swarrow \downarrow \\ V'_1 \end{array}$$

Suppose $V'_1 = k$. Then $k \langle |G!|^{\text{CS}} \rangle$ is a value. By Lemma 3 we have

$$\begin{array}{c} k \langle G! \rangle \rightsquigarrow M'_1 \langle s \ ; \ |G!|^{\text{CS}} \rangle \\ \swarrow \downarrow \\ k \langle |G!|^{\text{CS}} \rangle \end{array}$$

Suppose $V'_1 = \lambda x:A. N'$. Then $(\lambda x:A. N') \langle |G!|^{\text{CS}} \rangle$ is a value. By Lemma 3 we have

$$\begin{array}{c} V_1 \langle G! \rangle \rightsquigarrow M'_1 \langle s \ ; \ |G!|^{\text{CS}} \rangle \\ \swarrow \downarrow \\ (\lambda x:A. N') \langle |G!|^{\text{CS}} \rangle \end{array}$$

Suppose $V'_1 = U' \langle g; H! \rangle$. Then V'_1 has type \star , but that contradicts it having type G .
Suppose $V'_1 = U' \langle s' \rightarrow t' \rangle$. We have

$$\begin{array}{c} V_1 \langle G! \rangle \rightsquigarrow U' \langle s' \rightarrow t' \rangle \langle |G!|^{\text{CS}} \rangle \\ \swarrow \downarrow \\ U' \langle (s' \rightarrow t'); G! \rangle \end{array}$$

By Lemma 3 we conclude

$$\begin{array}{c} V_1 \langle G! \rangle \rightsquigarrow M'_1 \langle s \ ; \ |G!|^{\text{CS}} \rangle \\ \swarrow \downarrow \\ U' \langle (s' \rightarrow t'); G! \rangle \end{array}$$

Case $V = V_1 \langle c \rightarrow d \rangle$. We proceed by induction on $V_1 \langle c \rightarrow d \rangle \approx M'$. 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)

$$\frac{V_1 \langle c \rightarrow d \rangle \approx M'_1 \quad \vdash V_1 \langle c \rightarrow d \rangle : A \rightarrow B \quad |\text{id}_{A \rightarrow B}|^{\text{CS}} = t}{V_1 \langle c \rightarrow d \rangle \approx M'_1 \langle t \rangle}$$

We have $M'_1 \rightarrow^* V'_1$ and $V_1 \langle c \rightarrow d \rangle \approx V'_1$ 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 $V'_1 \langle \text{id}_A \rightarrow \text{id}_B \rangle$ is a value and we relate the left to the right by rule (i).

Suppose $V'_1 = U \langle c' \rightarrow d' \rangle$.

$$\begin{array}{c} V_1 \langle c \rightarrow d \rangle \rightsquigarrow U \langle c' \rightarrow d' \rangle \langle |\text{id}_A|^{\text{CS}} \rightarrow |\text{id}_A|^{\text{CS}} \rangle \\ \parallel \downarrow \\ U \langle (c' \rightarrow d') \ ; \ (|\text{id}_A|^{\text{CS}} \rightarrow |\text{id}_A|^{\text{CS}}) \rangle \\ \parallel \text{Lemma 2} \\ V_1 \langle c \rightarrow d \rangle \rightsquigarrow U \langle c' \rightarrow d' \rangle \end{array}$$

Subcase rule (ii)

$$\frac{V_1 \approx M'_1 \langle s \rangle \quad |c \rightarrow d|^{\text{CS}} = t}{V_1 \langle c \rightarrow d \rangle \approx M'_1 \langle s \ ; \ t \rangle}$$

We have $M'_1 \langle s \rangle \rightarrow^* V'_1$ and $V_1 \approx V'_1$ by the inner induction hypothesis. Then applying some case analysis on V'_1 we have $V'_1 \langle |c|^{\text{CS}} \rightarrow |d|^{\text{CS}} \rangle \rightarrow V'$ and $V_1 \langle c \rightarrow d \rangle \approx V'$ 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 $V' = U' \langle s \rightarrow t \rangle$. Inversion of $M \approx U' \langle s \rightarrow t \rangle$ gives us two cases to consider.

Subcase for rule (i)

$$\frac{M \approx U' \quad \vdash M : A \quad |\text{id}_A|^{\text{CS}} = s \rightarrow t}{M \approx U' \langle s \rightarrow t \rangle}$$

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

Subcase for rule (ii).

$$\frac{M_1 \approx U' \langle s' \rangle \quad |c|^{\text{CS}} = t'}{M_1 \langle c \rangle \approx U' \langle s' \ ; \ t' \rangle}$$

We have $M = M_1 \langle c \rangle$ and $(s' \ ; \ t') = s \rightarrow t$. By the induction hypothesis, $M_1 \xrightarrow{*}_C V_1$ where $V_1 \approx U' \langle s' \rangle$. We proceed with a nested induction on c .

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

$$\begin{array}{ccc} V_1 \langle \text{id}_A \rangle & \rightsquigarrow & U' \langle s' \ ; \ | \text{id}_A |^{\text{CS}} \rangle \\ \downarrow & & \parallel \text{Lemma 2} \\ V_1 & \rightsquigarrow & U' \langle s' \rangle \end{array}$$

Suppose $c = G!$. Then $t' = |G!|^{\text{CS}} = |\text{id}_G|^{\text{CS}}; G!$, but that contradicts $(s' \ ; \ t') = s \rightarrow t$.

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

$$\begin{array}{ccc} V_1 \langle G?^p \rangle & \rightsquigarrow & U' \langle (s \rightarrow t); G! \ ; \ G?^p; |\text{id}_G|^{\text{CS}} \rangle \\ \downarrow & & \parallel \text{Lemma 2} \\ V_2 \langle G! \rangle \langle G?^p \rangle & & \\ \downarrow & & \\ V_2 & \rightsquigarrow & U' \langle s \rightarrow t \rangle \end{array}$$

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

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

$$\begin{array}{ccc} V_1 \langle c_1; c_2 \rangle & \rightsquigarrow & U' \langle s' \ ; \ t' \rangle \\ \downarrow & & \parallel \\ V_1 \langle c_1 \rangle \langle c_2 \rangle & \rightsquigarrow & U' \langle s' \ ; \ |c_1|^{\text{CS}} \ ; \ |c_2|^{\text{CS}} \rangle \\ \text{IH} \downarrow & \rightsquigarrow & \text{IH} \\ V_2 \langle c_2 \rangle & & \\ \text{IH} \downarrow & \rightsquigarrow & \text{IH} \\ V_3 & & \end{array}$$

Suppose $c = \perp_{A \Rightarrow B}^p$. Then $t' = \perp_{A \Rightarrow B}^p$ and $(s' \ ; \ t') = \perp_{A \Rightarrow B}^p$, but $(s' \ ; \ t') = s \rightarrow t$ 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):

$$\frac{M_1 \approx U \langle s \rangle \quad |c|^{\text{CS}} = t}{M_1 \langle c \rangle \approx U \langle s \ ; \ t \rangle}$$

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

Suppose $c = \text{id}_*$.

$$\begin{array}{ccc} V_1 \langle \text{id}_* \rangle & \rightsquigarrow & U \langle s \ ; \ | \text{id}_* |^{\text{CS}} \rangle \\ \downarrow & & \parallel \text{Lemma 2} \\ V_1 & \rightsquigarrow & U \langle s \rangle \end{array}$$

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

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

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

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

$$\begin{array}{ccc}
 V_1\langle c_1; c_2 \rangle & \rightsquigarrow & U'\langle s' \circledast t' \rangle \\
 \downarrow & & \parallel \\
 V_1\langle c_1 \rangle \langle c_2 \rangle & \rightsquigarrow & U'\langle s' \circledast |c_1|^{\text{CS}} \circledast |c_2|^{\text{CS}} \rangle \\
 \text{IH} \downarrow & \rightsquigarrow & \text{IH} \\
 V_2\langle c_2 \rangle & & \text{IH} \\
 \text{IH} \downarrow & & \text{IH} \\
 V_3 & &
 \end{array}$$

Suppose $c = \perp_{A \Rightarrow B}^p$. Then $t' = \perp_{A \Rightarrow B}^p$ and $(s' \circledast t') = \perp_{\rightarrow B}^p$, but $(s' \circledast t') = (g; G!)$ so we have a contradiction.
Part 5 and 6.

Case $\frac{\text{blame } p \approx \text{blame } p}{\text{blame } p \approx \text{blame } p}$

□

C. Translation is bisimilar

Here we sketch the proof of Proposition 17.

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

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. \square