TRINITY COLLEGE DUBLIN
COLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH

Uniqueness Typing for Resource Management in Message-Passing Concurrency

Technical Appendix

Edsko de Vries, Adrian Francalanza and Matthew Hennessy

Computer Science Department Technical Report **TCD-CS-2010-03**
Foundations and Methods Research Group **April 30, 2010**

Uniqueness Typing for Resource Management in Message-Passing Concurrency

Technical Appendix

Edsko de Vries,* Adrian Francalanza and Matthew Hennessy*

April 30, 2010

Abstract

This technical appendix contains the soundness proofs of the lemmas in *Uniqueness Typing for Resource Management in Message-Passing Concurrency* published at Linearity 2009 in Coimbra, Portugal. It is meant as a companion to that paper and is not written to be read independently. We prove soundness for a simplified language (without explicit allocation and deallocation) first. The semantics of this language is the standard pi-calculus semantics. Even in this simpler language the proof is non-trivial due to the support for strong update on unique channels, and the proof for the simpler language is easier to understand. We then extend the proof to the full language with explicit allocation and deallocation of channels.

1 Preliminaries

1.1 Properties of splitting

Lemma 1 (Type splitting). *If* $[\vec{T}]^a = [\vec{T}_1]^{a_1} \circ [\vec{T}_2]^{a_2}$ *then*

1. *The original channel is not affine, and the split channels are not (immediately) unique:*

$$a \prec_s 1 \quad \bullet \prec_s a_1 \quad \bullet \prec_s a_2$$

2. *The split channels both carry objects of the same type:*

$$\vec{T}_1 = \vec{T}_2$$

3. *Both split types are subtypes of the original:*

$$[\vec{T}]^a \preceq_s [\vec{T}_1]^{a_1} \quad [\vec{T}]^a \preceq_s [\vec{T}_2]^{a_2}$$

4. *Only one of the split channels can be unique:*

$$\textit{if } a_1 \prec_s 1 \textit{ and } a_2 \prec_s 1 \textit{ then } a_1 = a_2 = \omega$$

Proof. Immediate from the definition of $(\circ)$. □

1.2 Consistency

To define consistency, we define a relation that models the effect of the structural operations on the environment: $(\prec)$ is the smallest preorder that satisfies

$$\frac{\mathbf{T} = \mathbf{T}_1 \circ \mathbf{T}_2}{\Gamma, u : \mathbf{T} \prec \Gamma, u : \mathbf{T}_1, u : \mathbf{T}_2} \qquad \frac{}{\Gamma, u : \mathbf{T} \prec \Gamma}$$

$$\frac{\mathbf{T}_1 \prec_s \mathbf{T}_2}{\Gamma, u : \mathbf{T}_1 \prec \Gamma, u : \mathbf{T}_2} \qquad \frac{}{\Gamma, u : [\vec{T}_1]^\bullet \prec \Gamma, u : [\vec{T}_2]^\bullet}$$

*The financial support of SFI is gratefully acknowledged.

Lemma 2. *The following typing rule is admissible.*

$$\frac{\Gamma' \vdash P \qquad \Gamma \prec \Gamma'}{\Gamma \vdash P}\ \textsc{tStr}$$

Proof. By definition of $(\prec)$. □

We can now formally define consistency.

Definition 3 (Consistency)**.** *An environment Γ' is consistent if and only if there exists an environment Γ such that $\Gamma \prec \Gamma'$ and Γ is a partial function.*

Corollary 4.

If Γ is consistent and $\Gamma \prec \Gamma'$ then Γ' is consistent.

Proof. Follows from transitivity of $(\prec)$. □

Lemma 5. *If $\Gamma \vdash P$ and Γ is consistent, then there exists an Γ' such that $\Gamma' \vdash P$ and Γ' is a partial function.*

Proof. Follows from the definition of consistency and Lemma 2 (tStr). □

1.3 Properties of Consistency

Lemma 6 ($(\prec)$ does not increase domains)**.**

$$\textit{If } c \in \boldsymbol{dom}(\Gamma') \textit{ and } \Gamma \prec \Gamma' \textit{ then } c \in \boldsymbol{dom}(\Gamma)$$

Lemma 7 (Consistency and Uniqueness)**.**

$$\textit{If } \Gamma, c : [\,\overrightarrow{\mathbf{T}}\,]^{\bullet} \textit{ is consistent then } c \notin \boldsymbol{dom}(\Gamma)$$

Lemma 8 (Consistency and Uniqueness (cont.))**.**

$$\textit{If } \Gamma \textit{ is consistent and } \Gamma \prec \Gamma', c : [\,\overrightarrow{\mathbf{T}}\,]^{\bullet} \textit{ then } \exists \Gamma'' \textit{ such that } \Gamma = \Gamma'', c : [\overrightarrow{\mathbf{T'}}]^{\bullet} \textit{ and } \Gamma'' \prec \Gamma'$$

Lemma 9. *If $u \notin \boldsymbol{dom}(\Gamma)$ and*

$$\Gamma, u : [\vec{T'}]^{a} \prec \Gamma, u : [\vec{T}]^{a_1}, u : [\vec{T}]^{a_2}$$

then

$$\Gamma, u : [\vec{T'}]^{a} \prec \Gamma, u : [\vec{T}]^{a_1 - 1}, u : [\vec{T}]^{a_2 - 1}$$

Proof. We must have

$$u : [\vec{T'}]^{a} \prec u : [\vec{T}]^{a'}$$

where

$$[\vec{T}]^{a'} = [\vec{T}]^{a_1'} \circ [\vec{T}]^{a_2'}$$

and

$$[\vec{T}]^{a_1'} \preceq_s [\vec{T}]^{a_1}, [\vec{T}]^{a_2'} \preceq_s [\vec{T}]^{a_2}$$

By Lemma 1, we have

$$a' \prec_s 1 \quad \bullet \prec_s a_1' \preceq_s a_1 \quad \bullet \prec_s a_2' \preceq_s a_2$$

which means that the conclusion of the lemma is defined. Moreover, we know that $a' \preceq_s a_1'$ and $a' \preceq_s a_2'$. We take cases on a_1, a_2.

- $a_1 = a_2 = 1$. Follows from weakening.
- $a_1 = 1, a_2 = \omega$. We have to show that $a' \preceq_s a_2 - 1 = a_2$; immediate.

- $a_1 = \omega, a_2 = \omega$. Trivial.
- $a_1 = 1, a_2 = (\bullet, i+1)$. We have $a'_1 \preceq_s a_1$ and $a'_2 \preceq_s a_2$. By inversion on type splitting, this means that $a' = (\bullet, j)$ with $j \leq i$; $a' \preceq_s a_2 - 1 = (\bullet, i)$ follows.

The missing cases are symmetric. □

Lemma 10. *Every sub-environment of a consistent environment is consistent.*

Proof. Suppose that $\Gamma = \Gamma_1, \Gamma_2$ and Γ is consistent: there exists a partial function Γ' such that $\Gamma' \prec \Gamma$. But $\Gamma \prec \Gamma_1$ because of weakening; hence, $\Gamma' \prec \Gamma_1$ because of transitivity, and Γ_1 is therefore consistent. □

1.4 Minimality

We introduce another property of environments which will be useful in proofs.

Definition 1 (Minimality). *An environment* Γ *is* minimal *iff*

- Γ *is consistent, and*
- *If* $u : [\vec{T}]^{(\bullet, i)} \in \Gamma$ *or* $u : [\vec{T}]^{\omega} \in \Gamma$*, this is the only assumption about* u *in* Γ.

For example, $\Gamma_1 = u : [\vec{T}]^{(\bullet,1)}, u : [\vec{T}]^1$ is consistent but not minimal: it is not minimal in the sense that there is a smaller environment $\Gamma'_1 = u : [\vec{T}]^\bullet$ such that $\Gamma'_1 \prec \Gamma_1$ and Γ'_1 effectively gives us the same information as Γ_1.

Conversely, $\Gamma_2 = u : [\vec{T}]^1, u : [\vec{T}]^1$ is minimal, because although there is a smaller environment Γ'_2 such that $\Gamma'_2 \prec \Gamma_2$ (for instance, $u : [\vec{T}]^\omega$), all such environments include a strictly stronger assumption about u.

Minimality generalizes the property of being a partial function; it would coincide with being a partial function if we generalize affinity.

Lemma 11. *Any partial function* Γ *is minimal.*

Proof. Trivial. □

Minimality has the following property which we will need in the subterm typing lemma.

Lemma 12. *If* $\Gamma \prec \Gamma_1, \Gamma_2$ *and* Γ *is minimal, then there exist minimal environments* Γ'_1, Γ'_2 *such that* $\Gamma \prec \Gamma'_1, \Gamma'_2$ *and* $\Gamma'_1 \prec \Gamma_1$ *and* $\Gamma'_2 \prec \Gamma_2$.

Proof. We consider three cases for Γ_1 (Γ_2 is dealt with analogously).

1. The only assumptions about u in Γ_1 are affine. In that case, Γ_1 is minimal and we are done.
2. We have $u : [\vec{T}]^\omega \in \Gamma_1$. Since Γ_1 must be consistent (Lemma 10), all assumptions about u in Γ_1 must be unrestricted or affine. Remove all these assumptions, leaving only the assumption $u : [\vec{T}]^\omega$. Since this new environment can be obtained by applying weakening ($\Gamma_1 \prec \Gamma'_1$) we have $\Gamma \prec (\Gamma_1, \Gamma_2) \prec (\Gamma'_1, \Gamma_2)$ by transitivity, and $\Gamma'_1 \prec \Gamma_1$ by splitting and subtyping.
3. We have $u : [\vec{T}]^{(\bullet, i)}$ in Γ_1. Because of consistency all other assumptions about u in Γ_1 and Γ_2 must be affine. Suppose that there are j such assumptions in Γ_1 and k such assumptions in Γ_2 (where $j + k \leq i$). This means that we must have $u : [\vec{T}]^{(\bullet, i')} \in \Gamma$ with $i' \leq i - (j+k)$. Leave Γ_2 as is (because it is already minimal with respect to u), but remove all j affine assumptions about u from Γ_1 and leave only $u : [\vec{T}]^{(\bullet, i-j)}$. We know that Γ can be split as these two new environments Γ_1, Γ'_2 because

$$u : [\vec{T}]^{i'} \prec u : [\vec{T}]^{(\bullet, i-j)}, \underbrace{u : [\vec{T}]^1, \cdots, u : [\vec{T}]^1}_{k}$$

and moreover $\Gamma'_1 \prec \Gamma_1$ because

$$u : [\vec{T}]^{i-j} \prec u : [\vec{T}]^{(\bullet, i)}, \underbrace{u : [\vec{T}]^1, \cdots, u : [\vec{T}]^1}_{j}$$

□

Minimality allows us to prove the following proposition which is a generalization of Lemma 9 and is essential for the communication case of the subject reduction proof.

Proposition 13. *If* Γ *is minimal and*

$$\Gamma \prec \Gamma', u : [\vec{T}]^{a_1}, u : [\vec{T}]^{a_2}$$

then

$$\Gamma \prec \Gamma', u : [\vec{T}]^{a_1 - 1}, u : [\vec{T}]^{a_2 - 1}$$

Proof. If a_1, a_2 are only affine or unrestricted, the lemma follows from weakening (unrestricted assumptions are not affected by the decrement operation). The only interesting case is where one of $a_1 = (\bullet, i)$ and $a_2 = 1$ (or vice versa). Since Γ is minimal, this means that we must have that the two assumptions were contracted from a single assumption

$$\Gamma \prec \Gamma', u : [\vec{T}]^{(\bullet, i-1)} \prec \Gamma', u : [\vec{T}]^{(\bullet, i)}, u : [\vec{T}]^{1}$$

and the property follows because

$$\Gamma \prec \Gamma', u : [\vec{T}]^{a_1 - 1}, u : [\vec{T}]^{a_2 - 1} = \Gamma', u : [\vec{T}]^{(\bullet, i-1)}$$

□

1.5 Inversion

In between every two applications of logical rules there are zero or more applications of the structural rules (subtyping, revision and contraction). We can use the relation ($\prec$) to conveniently state inversion principles. For example,

Lemma 14 (Inversion for output)**.** *If* $\Gamma \vdash c!\vec{d}.P$ *then*

$$\Gamma \prec \Gamma', u : [\vec{T}]^{a}, \overrightarrow{d : T}$$

and $\Gamma', u : [\vec{T}]^{a-1} \vdash P$*.*

The inversion lemmas for the other constructs are similar.

2 Soundness of the Language without Allocation and Deallocation

In this section we consider soundness for the language without allocation and deallocation, i.e., of the type system when applied to the standard pi-calculus, with the standard pi-calculus reduction relation, structural equivalence, etc (we do not reproduce these definitions here; they can be found in any textbook on the pi-calculus). The type system is the one described in the paper, excluding obviously the rules for allocation and deallocation. The soundness proof is non-trivial because we still support strong update (revision), which makes essential use of uniqueness typing.

2.1 Safety

Lemma 15 (Preservation of types under structural equivalence)**.** *If* $\Gamma \vdash P$ *and* $P \equiv P'$ *then* $\Gamma \vdash P'$*.*

Proof. Since the typing relation is not sensitive to the order of the assumptions in the typing environment, reordering parallel processes and extrusion do not affect typing. Removing or adding nil processes and adding or removing a restriction around the nil process do not affect typing because nil can be typed in any environment. Finally, alpha-renaming bound names does not affect typing because those bound names are not in the (original) typing environment. □

Lemma 16 (Subterm typing)**.** *If* $\Gamma \vdash \mathcal{C}[P]$ *and* Γ *is minimal then there exists a minimal* Γ' *such that* $\Gamma' \vdash P$*, and for every* P' *such that* $\Gamma' \vdash P'$*,* $\Gamma \vdash \mathcal{C}[P']$*.*

Proof. By induction on $\mathcal{C}$.

- Case $\mathcal{C} = []$. Immediate (take $\Gamma' = \Gamma$).
- Case $\mathcal{C} = Q \,||\, \mathcal{C}'$. By inversion on the typing relation[1],

  $$\begin{array}{c} \Gamma_1 \vdash Q \quad \Gamma_2 \vdash \mathcal{C}'[P] \\ \hline\hline \Gamma \vdash Q \,||\, \mathcal{C}'[P] \end{array}\; \Gamma \prec \Gamma_1, \Gamma_2$$

  By Lemma 12 there exist minimal environments Γ_1', Γ_2' such that $\Gamma \prec \Gamma_1', \Gamma_2'$ and $\Gamma_1' \prec \Gamma_1$, $\Gamma_2' \prec \Gamma_2$. By rule tSTR (Lemma 2) we have that $\Gamma_1' \vdash Q$ and $\Gamma_2' \vdash \mathcal{C}'[P]$.

  By the induction hypothesis at $\Gamma_2' \vdash \mathcal{C}'[P]$ there exists a Γ'' such that $\Gamma'' \vdash P$ and for every P' such that $\Gamma'' \vdash P'$ we have $\Gamma_2' \vdash \mathcal{C}'[P']$. Take $\Gamma' = \Gamma''$. The proof is completed by

  $$\begin{array}{c} \Gamma_1' \vdash Q \quad \Gamma_2' \vdash \mathcal{C}'[P'] \\ \hline\hline \Gamma \vdash Q \,||\, \mathcal{C}'[P'] \end{array}\; \text{tPAR}(\Gamma \prec \Gamma_1', \Gamma_2')$$

- Case $\mathcal{C} = \mathcal{C}' \,||\, Q$. Analogous.
- Case $\mathcal{C} = (\nu c)\mathcal{C}'$. By inversion on the typing relation, we have

  $$\begin{array}{c} \Gamma_1, c\!:\!T \vdash \mathcal{C}'[P] \\ \hline\hline \Gamma \vdash (\nu c)\mathcal{C}'[P] \end{array}\; \Gamma \prec \Gamma_1$$

  We therefore also have

  $$\frac{\Gamma_1, c\!:\!T \vdash \mathcal{C}'[P]}{\Gamma, c\!:\!T \vdash \mathcal{C}'[P]}\; \text{tSTR}$$

  where $\Gamma, c\!:\!T$ is minimal because by Barendregt we can assume that $c \notin \mathbf{dom}(\Gamma)$ (effectively, this is saying that there is no need to apply any of the structural rules before applying tRST).

  By the induction hypothesis at $\Gamma, c : T \vdash \mathcal{C}'[P]$, there exists a Γ'' such that $\Gamma'' \vdash P$ and for all P' such that $\Gamma'' \vdash P$ we have $\Gamma, c\!:\!T \vdash \mathcal{C}'[P]$. Take $\Gamma' = \Gamma''$. The proof is completed by

  $$\frac{\Gamma, c\!:\!T \vdash \mathcal{C}'[P']}{\Gamma \vdash (\nu c)\mathcal{C}'[P']}\; \text{tREST}$$

□

Theorem 17 (Type safety). *If* $\Gamma \vdash P$ *and* Γ *is minimal then* $P \not\rightarrow^{err}$.

Proof. By induction on $P \xrightarrow{\text{err}}$.

- Case

  $$\frac{|\vec{d}| \neq |\vec{x}|}{c!\vec{d}.P \parallel c?\vec{x}.Q \xrightarrow{\text{err}}}\; \text{ECOM}$$

  By inversion on $\Gamma \vdash c!\vec{d}.P \parallel c?\vec{x}.Q$ we must have that $\Gamma \prec \Gamma_1, \Gamma_2$ where

  $$\begin{array}{c} \Gamma_1', c\!:\![\vec{T}]^{a-1} \vdash P \\ \hline\hline \Gamma_1 \vdash c!\vec{d}.P \end{array}\; \Gamma_1 \prec \Gamma_1', c\!:\![\vec{T}]^a, \overrightarrow{d\!:\!T}$$

  and

  $$\begin{array}{c} \Gamma_2', c\!:\![\vec{T}']^{a'-1}, \overrightarrow{x\!:\!T'} \vdash Q \\ \hline\hline \Gamma_2 \vdash c?\vec{x}.Q \end{array}\; \Gamma_2 \prec \Gamma_2', c\!:\![\vec{T}']^{a'}$$

  From the rules for input and output, we have that $|\vec{d}| = |\vec{T}|$ and $|\vec{x}| = |\vec{T}'|$. Remains to show that $\vec{T} = \vec{T}'$, which follows from Lemma 1.

[1] We use a double line to indicate an arbitrary (but finite) number of applications of the structural rules.

- Case

$$\frac{P \equiv P' \quad P' \xrightarrow{\text{err}}}{P \xrightarrow{\text{err}}}\ \textsc{eStr}$$

Since $\Gamma \vdash P$, by preservation of types under structural equivalence $\Gamma \vdash P'$, at which point we can apply the induction hypothesis to complete the proof.

- Case

$$\frac{P \xrightarrow{\text{err}}}{\mathcal{C}[P] \xrightarrow{\text{err}}}$$

Since $\Gamma \vdash \mathcal{C}[P]$, by the subterm typing lemma we know that there exists a minimal $\Gamma' \vdash P$. The induction hypothesis completes the proof.

□

Corollary 18 (Type safety for partial functions)**.** *If* $\Gamma \vdash P$ *and* Γ *is a partial functions then* $P \not\rightarrow^{err}$.

Proof. Follows immediately from type safety since all partial functions are minimal. □

2.2 Substitution

Lemma 19 (Process substitution)**.** *If* $\Gamma_1, X\!:\!\mathbf{proc} \vdash P$ *and* $\Gamma_2^{\omega} \vdash Q$ *then* $\Gamma_1, \Gamma_2^{\omega} \vdash P\{Q/X\}$.

Proof. By induction on P followed by inversion on the typing relation.

- Case nil. Immediate.

- Case

$$\frac{\Gamma_1', X\!:\!\mathbf{proc}, a\!:\!\mathbf{T} \vdash P}{\Gamma_1, X\!:\!\mathbf{proc} \vdash (\nu a)P}\ \textsc{tRest}$$

where

$$\Gamma_1, X\!:\!\mathbf{proc} \prec \Gamma_1', X\!:\!\mathbf{proc}$$

Induction hypothesis establishes the premise of

$$\frac{\Gamma_1', a\!:\!\mathbf{T}, \Gamma_2^{\omega} \vdash P\{Q/X\}}{\Gamma_1, \Gamma_2^{\omega} \vdash (\nu a)P\{Q/X\}}\ \textsc{tRest}$$

- Case

$$\frac{\Gamma_1', X\!:\!\mathbf{proc}, u\!:\![\,\overrightarrow{\mathbf{T}}\,]^{a-1} \vdash P}{\Gamma_1, X\!:\!\mathbf{proc} \vdash u!\vec{v}.P}\ \textsc{tOut}$$

where

$$\Gamma_1, X\!:\!\mathbf{proc} \prec \Gamma_1', X\!:\!\mathbf{proc}, u\!:\![\,\overrightarrow{\mathbf{T}}\,]^{a}, \overrightarrow{v\!:\!\mathbf{T}}$$

The induction hypothesis gives us the premise of

$$\dfrac{\dfrac{\Gamma_1', u\!:\![\,\overrightarrow{\mathbf{T}}\,]^{a-1}, \Gamma_2^{\omega} \vdash P\{Q/X\}}{\Gamma_1', u\!:\![\,\overrightarrow{\mathbf{T}}\,]^{a}, \overrightarrow{v\!:\!\mathbf{T}}, \Gamma_2^{\omega} \vdash u!\vec{v}.P\{Q/X\}}\ \textsc{tOut}}{\Gamma_1, \Gamma_2^{\omega} \vdash u!\vec{v}.P\{Q/X\}}\ \textsc{tStr}$$

- Case

$$\frac{\Gamma_1', X\!:\!\mathbf{proc}, u\!:\![\,\overrightarrow{\mathbf{T}}\,]^{a-1}, \overrightarrow{x\!:\!T} \vdash P}{\Gamma_1, X\!:\!\mathbf{proc} \vdash u?\vec{x}.P}\ \textsc{tIn}$$

where

$$\Gamma_1, X\!:\!\mathbf{proc} \prec \Gamma_1', X\!:\!\mathbf{proc}, u\!:\![\,\overrightarrow{\mathbf{T}}\,]^{a}$$

Induction hypothesis gives us the premise of

$$\dfrac{\dfrac{\Gamma_1', u : [\,\overrightarrow{\mathbf{T}}\,]^{a-1}, \overrightarrow{x : T}, \Gamma_2^\omega \vdash P\{Q/X\}}{\Gamma_1', u : [\,\overrightarrow{\mathbf{T}}\,]^{a}, \Gamma_2^\omega \vdash P\{Q/X\}}\;\textsc{tIn}}{\Gamma_1, \Gamma_2^\omega \vdash u?\vec{x}.P\{Q/X\}}\;\textsc{tStr}$$

- Case

$$\dfrac{\Gamma_a, X : \mathbf{proc} \vdash P_a \quad \Gamma_b, X : \mathbf{proc} \vdash P_b}{\Gamma_1, X : \mathbf{proc} \vdash P_a \parallel P_b}\;\textsc{tPar}$$

where

$$\Gamma_1, X : \mathbf{proc} \prec (\Gamma_a, X : \mathbf{proc}), (\Gamma_b, X : \mathbf{proc})$$

(we only treat the case where $X \in \mathrm{fv}\, P_a \cup \mathrm{fv}\, P_b$; the other cases are similar but easier).

We use the induction hypothesis twice to establish the premises of

$$\dfrac{\dfrac{\Gamma_a, \Gamma_2^\omega \vdash P_a\{Q/X\} \quad \Gamma_b, \Gamma_2^\omega \vdash P_b\{Q/X\}}{\Gamma_a, \Gamma_2^\omega, \Gamma_b, \Gamma_2^\omega \vdash (P_a\{Q/X\}) \parallel (P_b\{Q/X\})}\;\textsc{tPar}}{\Gamma_1, \Gamma_2^\omega \vdash (P_a\{Q/X\}) \parallel (P_b\{Q/X\})}\;\textsc{tStr}$$

Crucially, we take advantage of the fact that $\Gamma^\omega \prec \Gamma^\omega, \Gamma^\omega$ for any unrestricted environment Γ^ω.

- Case

$$\begin{array}{c} \Gamma_1^\omega, X : \mathbf{proc}, Y : \mathbf{proc} \vdash P \\ \hline\hline \Gamma_1, X : \mathbf{proc} \vdash \mathsf{rec}\, Y.P \end{array}\;\textsc{tRec}$$

where

$$\Gamma_1, X : \mathbf{proc} \prec (\Gamma_1^\omega, X : \mathbf{proc})$$

(again, we treat only the case where $X \in \mathrm{fv}\, P$; we assume without loss of generality that $X \neq Y$).

The induction hypothesis establishes the premise of

$$\dfrac{\dfrac{\Gamma_1^\omega, Y : \mathbf{proc}, \Gamma_2^\omega \vdash P\{Q/X\}}{\Gamma_1^\omega, \Gamma_2^\omega \vdash \mathsf{rec}\, Y.P\{Q/X\}}\;\textsc{tRec}}{\Gamma_1, \Gamma_2^\omega \vdash \mathsf{rec}\, Y.P\{Q/X\}}\;\textsc{tStr}$$

- Case

$$\dfrac{}{\Gamma_1', X : \mathbf{proc}, Y : \mathbf{proc} \vdash Y}\;\textsc{tVar}$$

where

$$\Gamma_1, X : \mathbf{proc} \prec \Gamma_1', X : \mathbf{proc}, Y : \mathbf{proc}$$

If $X = Y$, weakening establishes the premise of

$$\dfrac{\Gamma_1', Y : \mathbf{proc}, \Gamma_2^\omega \vdash Q}{\Gamma_1, \Gamma_2^\omega \vdash Q}\;\textsc{tStr}$$

Otherwise, we have

$$\dfrac{\dfrac{}{\Gamma_1', Y : \mathbf{proc}, \Gamma_2^\omega \vdash Y}\;\textsc{tVar}}{\Gamma_1, \Gamma_2^\omega \vdash Y}\;\textsc{tStr}$$

- Case

$$\begin{array}{c} \Gamma_1', X : \mathbf{proc} \vdash P \quad \Gamma_1', X : \mathbf{proc} \vdash Q \\ \hline\hline \Gamma_1, X : \mathbf{proc} \vdash \mathsf{if}\ u = v\ \mathsf{then}\ P\ \mathsf{else}\ Q \end{array}\;\textsc{tIf}$$

where

$$\Gamma_1, X : \mathbf{proc} \prec \Gamma_1', X : \mathbf{proc}$$

The induction hypothesis establishes the premises of

$$\begin{array}{c} \Gamma_1', \Gamma_2^\omega \vdash P\{Q/X\} \quad \Gamma_1', \Gamma_2^\omega \vdash Q\{Q/X\} \\ \hline\hline \Gamma_1, \Gamma_2^\omega \vdash \mathsf{if}\ u = v\ \mathsf{then}\ P\{Q/X\}\ \mathsf{else}\ Q\{Q/X\} \end{array}\;\textsc{tIf}$$

□

Lemma 20 (Identifier substitution)**.** *If* $\Gamma, \overrightarrow{x\!:\!T} \;\vdash\; P$*, where the* $\vec{x}$ *are pairwise disjoint and do not occur in the domain of* Γ*, then* $\Gamma, \overrightarrow{u : T} \vdash Q\{\vec{u}/\vec{x}\}$*.*

Proof. This is a simple renaming of variables throughout the typing derivation. □

2.3 Preservation

Theorem 21 (Subject reduction)**.** *If* $\Gamma \vdash P$*,* Γ *is minimal and* $P \longrightarrow P'$ *then* $\Gamma \vdash P'$*.*

Proof. By induction on $P \longrightarrow P'$.

- Case
  $$\frac{}{c!\vec{d}.P \parallel c?\vec{x}.Q \longrightarrow P \parallel Q\{\vec{d}/\vec{x}\}}\ \textsc{rCom}$$
  As in the type safety lemma, by inversion on
  $$\Gamma \vdash c!\vec{d}.P \parallel c?\vec{x}.Q$$
  we must have that $\Gamma \prec \Gamma_p, \Gamma_q$ where
  $$\begin{array}{c} \Gamma_1, c : [\vec{T}]^{a_1-1} \vdash P \\ \hline\hline \Gamma_p \vdash c!\vec{d}.P \end{array}\ \textsc{tOut}$$
  where
  $$\Gamma_p \prec \Gamma_1, c : [\vec{T}]^{a_1}, \overrightarrow{d\!:\!T}$$
  Similarly,
  $$\begin{array}{c} \Gamma_2, c : [\vec{T}]^{a_2-1}, \overrightarrow{x\!:\!T} \vdash Q \\ \hline\hline \Gamma_q \vdash c?\vec{x}.Q \end{array}$$
  where
  $$\Gamma_q \prec \Gamma_2, c : [\vec{T}]^{a_2}$$
  (as in Theorem 28, the types carried by both channels must be the same since Γ is consistent.) By the name substitution lemma, we have that
  $$\Gamma_2, c : [\vec{T}]^{a_2-1}, \overrightarrow{d\!:\!T} \vdash Q\{\vec{d}/\vec{x}\}$$
  We now construct the required type derivation as follows:
  $$\dfrac{\dfrac{\overline{\Gamma_1, c : [\vec{T}]^{a_1-1} \vdash P} \quad \overline{\Gamma_2, c : [\vec{T}]^{a_2-1}, \overrightarrow{d\!:\!T} \vdash Q\{\vec{d}/\vec{x}\}}}{(\Gamma_1, c : [\vec{T}]^{a_1-1}), (\Gamma_2, c : [\vec{T}]^{a_2-1}, \overrightarrow{d\!:\!T}) \vdash P \parallel Q\{\vec{d}/\vec{x}\}}\ \textsc{tPar}}{\Gamma \vdash P \parallel Q\{\vec{d}/\vec{x}\}}\ \textsc{tStr}$$
  Remains to show that the last step is justified, i.e., that
  $$\Gamma \prec (\Gamma_1, c : [\vec{T}]^{a_1-1}), (\Gamma_2, c : [\vec{T}]^{a_2-1}, \overrightarrow{d\!:\!T})$$
  Since environment are unordered, this follows from Proposition 13.

- Case
  $$\frac{}{\mathsf{rec}\, X.P \longrightarrow P\{\mathsf{rec}\, X.P/X\}}\ \textsc{rRec}$$
  We must have that $\Gamma \prec \Gamma^\omega$ where
  $$\begin{array}{c} \Gamma^\omega, X : \mathbf{proc} \vdash P \\ \hline\hline \Gamma \vdash \mathsf{rec}\, X.P \end{array}\ \textsc{tRec}$$
  It follows that $\Gamma^\omega \vdash \mathsf{rec}\, X.P$. The process substitution lemma then establishes the premise of
  $$\frac{\Gamma^\omega, \Gamma^\omega \vdash P\{\mathsf{rec}\, X.P/X\}}{\Gamma \vdash P\{\mathsf{rec}\, X.P/X\}}\ \textsc{tStr}$$
  (note that $\Gamma^\omega \prec \Gamma^\omega, \Gamma^\omega$ for any environment Γ^ω containing only unrestricted assumptions).

- Case
$$\frac{}{\textsf{if } c\!=\!c \textsf{ then } P \textsf{ else } Q \longrightarrow P}\ \textsc{rThen}$$
By inversion on the typing relation, we must have that
$$\frac{\Gamma' \vdash P \quad \Gamma' \vdash Q}{\Gamma \vdash \textsf{if } c\!=\!c \textsf{ then } P \textsf{ else } Q}\ \textsc{tIf}$$
where $\Gamma \prec \Gamma'$. The conclusion is immediate. The case for rELSE is analogous.

- Case
$$\frac{P \equiv P' \quad P' \longrightarrow Q' \quad Q' \equiv Q}{P \longrightarrow Q}\ \textsc{rStr}$$
Follows from the induction hypothesis and preservation of types under structural equivalence.

- Case
$$\frac{P \longrightarrow P'}{\mathcal{C}[P] \longrightarrow \mathcal{C}[P']}\ \textsc{rCtxt}$$
Since $\Gamma \vdash \mathcal{C}[P]$, by the subterm typing lemma there exists a minimal Γ' such that $\Gamma' \vdash P$ and for all P' such that $\Gamma' \vdash P'$, $\Gamma \vdash \mathcal{C}[P']$. Since the induction hypothesis gives us $\Gamma' \vdash P'$, there is nothing left to show.

□

Corollary 22 (Subject reduction for partial functions)**.** *If* $\Gamma \vdash P$, Γ *is a partial function and* $P \rightarrow P'$ *then* $\Gamma \vdash P'$.

Proof. Follows immediately from subject reduction since all partial functions are minimal. □

3 Soundness for the Full Language

We extend the type soundness results to our extended language. Most cases carry forward smoothly from earlier proofs. In what follows, we outline the cases that are different.

3.1 Subterm Typing

The following lemmas lead to a refined sub-term lemma 27 , which is central to prove the contextual cases for both safety and subject reduction.

Proposition 23. $\Gamma \vdash \sigma \triangleright P$ *and* $\sigma(c) = \bot$ *implies* $c \notin \boldsymbol{dom}(\Gamma)$

Proposition 24. $\Gamma \prec \Gamma_1, \Gamma_2$ *and* $\Gamma_2 \prec \Gamma_3$ *implies* $\Gamma \prec \Gamma_1, \Gamma_3$

Lemma 25 (Sub-Environment Consolidation)**.** $\Gamma, c : \mathbf{T} \prec \Gamma'$ *where* $c \notin \boldsymbol{dom}(\Gamma)$ *implies* $\exists \Gamma''$ *such that:*

- $(\Gamma, c : \mathbf{T}) \prec (\Gamma'', c : \mathbf{T}) \prec \Gamma'$
- $\boldsymbol{dom}(\Gamma'', c : \mathbf{T}) = \boldsymbol{dom}(\Gamma')$.

Lemma 26. *If* $\Gamma \prec (\Gamma_1, \Gamma_2)$ *and* $\Gamma_2 \prec \Gamma_3$ *where* $\Gamma, \Gamma_1, \Gamma_2, \Gamma_3$ *are all minimal then* $\exists$ *a minimal* Γ_4 *such that:*

- $\Gamma \prec \Gamma_4$ *and* $\Gamma \prec \Gamma_4 \prec (\Gamma_1, \Gamma_3)$
- $\boldsymbol{dom}(\Gamma_4) = \boldsymbol{dom}(\Gamma_1) \cup \boldsymbol{dom}(\Gamma_3)$

Definition 2 (Sub Environments)**.** σ' *is a sub-environment of* σ wrt. Γ, *denoted as* $\sigma \prec_\Gamma \sigma'$ *iff:*

- $\boldsymbol{dom}(\sigma) = \boldsymbol{dom}(\sigma')$
- $\sigma(c) = \bot$ *implies* $\sigma'(c) = \bot$
- $\sigma(c) = \top$ *and* $\sigma'(c) = \bot$ *implies* $\Gamma = \Gamma', c : [\overrightarrow{\mathbf{T}}]^{\bullet}$

Lemma 27 (Sub-term Typing 2)**.** $\Gamma \vdash \mathcal{C}[\sigma \triangleright P]$ *implies:*

1. *$\exists$ a minimal Γ_1 such that $\Gamma \prec \Gamma_1$ and $\Gamma_1 \vdash \sigma \triangleright P$*
2. *When $\Gamma_1 \vdash \sigma \triangleright P$ and there exist $\Gamma' \vdash \sigma' \triangleright P'$ where:*
   - *$\sigma \prec_{\Gamma_1} \sigma'$,*
   - *$\Gamma_1 \prec \Gamma'$ and Γ' is minimal*

   implies $\exists$ minimal $\Gamma_2 . \Gamma_2, \Gamma \prec \Gamma_2$ and $\Gamma_2 \vdash \mathcal{C}[\sigma' \triangleright P']$

Proof. By induction on the structure of $\mathcal{C}$. We here consider two main cases:

$\mathcal{C} = (\nu c)\mathcal{C}'$**:** We have three subcases:

$c \notin \mathbf{dom}(\sigma)$: Then for $(\nu c)\mathcal{C}'[\sigma \triangleright P] = \sigma'' \triangleright P''$, by the condition of well-formed configurations, we know that $c \notin \mathrm{fn}\, P''$. Thus, by the structural equivalence $P'' \equiv (\nu c)P''$ (whenever $c \notin \mathrm{fn}\, P''$), we know $\mathcal{C}$ acts as the context $\mathcal{C}'$ and the proof follows immediately by I.H.

$\sigma(c) = \top$: Let $(\nu c)\mathcal{C}'[\sigma \triangleright P] = \sigma'' \triangleright (\nu c\!:\!\top)P''$. By tCONF we know

$$d \in \mathbf{dom}(\Gamma) \text{ implies } \sigma''(d) = \top \tag{1}$$

and by the respective Inversion Lemma we know

$$\frac{\Gamma_1, c\!:\!\mathbf{T} \vdash P''}{\Gamma \vdash (\nu c\!:\!\top)P''}\ \Gamma \prec \Gamma_1 \tag{2}$$

Since we assume alpha renaming for bound names, $c \notin \mathbf{dom}(\Gamma)$ (and also $c \notin \mathbf{dom}(\Gamma_1)$) which means that if Γ minimal, then $\Gamma, c\!:\!\mathbf{T}$ is minimal too. Thus by $\Gamma, c\!:\!\mathbf{T} \prec \Gamma_1, c\!:\!\mathbf{T}$, tSTR and (2) we know

$$\Gamma, c\!:\!\mathbf{T} \vdash P'' \tag{3}$$

By (3), (1), tCONF we deduce that

$$\Gamma, c\!:\!\mathbf{T} \vdash (\sigma'', c\!:\!\top \triangleright P'') \tag{4}$$

and by I.H. we deduce that there exists Γ_1 such that $\Gamma_1 \vdash \sigma \triangleright P$, proving the first clause.

If we assume $\Gamma' \vdash \sigma' \triangleright P'$ for $\sigma \prec_{\Gamma_1} \sigma'$ and $\Gamma_1 \prec \Gamma'$ (Γ' minimal) then by (4) and I.H. we know that there exists a minimal Γ_3 such that $\Gamma, c\!:\!\mathbf{T} \prec \Gamma_3$ and

$$\Gamma_3 \vdash \mathcal{C}'[\sigma' \triangleright P'] \tag{5}$$

Let $\mathcal{C}'[\sigma' \triangleright P'] = \sigma''' \triangleright P'''$. We have two cases to consider resulting form $\sigma \prec_{\Gamma_1} \sigma'$:

$\sigma'''(c) = \bot$**:** By tCONF we must have

$$\forall d \in \mathbf{dom}(\Gamma_3).\sigma'''(d) = \top \text{ and thus } c \notin \mathbf{dom}(\Gamma_3) \tag{6}$$

$$\Gamma_3 \vdash P''' \tag{7}$$

We also know that $\mathcal{C}[\sigma' \triangleright P'] = (\sigma''' \setminus c) \triangleright (\nu c\!:\!\bot)P'''$. By (7) and tRST2 we obtain

$$\Gamma_3 \vdash (\nu c\!:\!\bot)P''' \tag{8}$$

and by (6), (8) and tCONF we obtain $\Gamma_3 \vdash (\sigma''' \setminus c) \triangleright (\nu c\!:\!\bot)P'''$ as required.

$\sigma'''(c) = \top$**:** By tCONF we must have

$$\forall d \in \mathbf{dom}(\Gamma_3).\sigma'''(d) = \top \tag{9}$$

$$\Gamma_3 \vdash P''' \tag{10}$$

We also know that $\mathcal{C}[\sigma' \triangleright P'] = (\sigma''' \setminus c) \triangleright (\nu c\!:\!\top)P'''$. Since both Γ_3 and $\Gamma, c\!:\!\mathbf{T}$ are minimal, by Lemma 25 there exists a minimal Γ_4 such that $(\Gamma, c\!:\!\mathbf{T}) \prec (\Gamma_4, c\!:\!\mathbf{T}) \prec \Gamma_3$ where $\mathbf{dom}(\Gamma_4) = \mathbf{dom}(\Gamma_3) \setminus \{c\}$. Thus by tSTR and (10) we have $\Gamma_4, c : \mathbf{T} \vdash P'''$ and by tRST1 we obtain $\Gamma_4 \vdash (\nu c\!:\!\top)P'''$. Finally, by tCONF and (9) we obtain $\Gamma_4 \vdash (\sigma''' \setminus c) \triangleright (\nu c\!:\!\top)P'''$.

$\sigma(c) = \bot$: Similar to the case above but simpler.

$\mathcal{C} = Q \parallel \mathcal{C}'$**:** We know $\mathcal{C}[\sigma \triangleright P] = \sigma'' \triangleright Q \,||\, P''$ where $\mathcal{C}'[\sigma \triangleright P] = \sigma'' \triangleright P''$. By TCONF we know

$$c \in \mathbf{dom}(\Gamma) \text{ implies } \sigma''(c) = \top \tag{11}$$

$$\Gamma \vdash Q \,||\, P'' \tag{12}$$

By (12) and the respective Inversion Lemma we know

$$\frac{\Gamma_1 \vdash Q \quad \Gamma_2 \vdash P''}{\Gamma \vdash Q \,||\, P''} \; \Gamma \prec \Gamma_1, \Gamma_2 \tag{13}$$

By $\Gamma \prec \Gamma_1, \Gamma_2$, the fact that Γ is minimal and Lemma 12 there exist minimal Γ_1' and Γ_2' such that $\Gamma \prec (\Gamma_1', \Gamma_2')$, $\Gamma_1' \prec \Gamma_1$ and $\Gamma_2' \prec \Gamma_2$. Thus by (13) and rtittStr we have

$$\Gamma_1' \vdash Q \tag{14}$$

$$\Gamma_2' \vdash P'' \tag{15}$$

Since $\Gamma \prec \Gamma_2'$, by (11), (15), TCONF and I.H. we deduce that $\exists$ minimal Γ_3 such that

$$\Gamma_2' \prec \Gamma_3 \text{ and } \Gamma_3 \vdash \sigma \triangleright P \tag{16}$$

and by $\Gamma \prec \Gamma_2'$ and $\Gamma_2' \prec \Gamma_3$ we deduce $\Gamma \prec \Gamma_3$ as required by the first clause.

If we assume $\Gamma' \vdash \sigma' \triangleright P'$ for $\sigma \prec_{\Gamma_3} \sigma'$ and $\Gamma_3 \prec \Gamma'$ (Γ' minimal), then by (15), (16) and I.H. we obtain that there exists a minimal Γ_4 such that

$$\Gamma_2' \prec \Gamma_4 \text{ and } \Gamma_4 \vdash \mathcal{C}'[\sigma' \triangleright P'] \tag{17}$$

Let $\mathcal{C}'[\sigma' \triangleright P'] = \sigma''' \triangleright P'''$. By TCONF we know that forall c

$$\sigma'''(c) = \bot \text{ implies } c \notin \mathbf{dom}(\Gamma_4) \tag{18}$$

By definition of $\sigma \prec_{\Gamma_3} \sigma'$, these constitute the only possible discrepancies between σ''' and σ''. More specifically, for all the discrepancies between the two states σ''' and σ'', *i.e.*,

$$\sigma''(c) = \top \text{ and } \sigma'''(c) = \bot$$

we know $\Gamma_3 = \Gamma_3', c : [\overrightarrow{\mathbf{T}}]^\bullet$ and by $\Gamma_2' \prec \Gamma_3$ we deduce also that $\Gamma_2' = \Gamma_2'', c : [\overrightarrow{\mathbf{T}}]^\bullet$. From this and $\Gamma \prec (\Gamma_1', \Gamma_2')$ we deduce that

$$\sigma''(c) = \top \text{ and } \sigma'''(c) = \bot \text{ implies } c \notin \mathbf{dom}(\Gamma_1') \tag{19}$$

Moreover, from (17) and TCONF we have

$$\sigma'''(c) = \bot \text{ implies } c \notin \mathbf{dom}(\Gamma_4) \tag{20}$$

. Thus by Lemma 26 there exists a minimal Γ_5 such that

$$\Gamma \prec \Gamma_5 \prec (\Gamma_1', \Gamma_4) \text{ and } \mathbf{dom}(\Gamma_5) = \mathbf{dom}(\Gamma_1') \cup \mathbf{dom}(\Gamma_4) \tag{21}$$

which means that

$$\sigma'''(c) = \bot \text{ implies } c \notin \mathbf{dom}(\Gamma_5) \tag{22}$$

Thus by (14), (17), (21), TSTR, (22) and TCONF we obtain $\Gamma_5 \vdash \sigma''' \triangleright Q \,||\, P''' = \Gamma_5 \vdash \mathcal{C}[\sigma' \triangleright P']$ as required.

□

3.2 Safety

Theorem 28 (Type safety)**.** *If* $\Gamma \vdash \sigma \triangleright P$ *and* Γ *is minimal then* $\sigma \triangleright P \not\rightarrow^{err}$*.*

Proof. We assume $\sigma \triangleright P \rightarrow^{\text{err}}$ and show that this leads to a contradiction. There are two new case from Theorem 28. We here consider the first; the second case, relating to rule eIn is analogous:

eOut: By the hypothesis of this rule we know

$$\sigma(c) = \bot \tag{23}$$

Moreover we know $P = c!\vec{d}.Q$ for some Q. Thus if $\Gamma \vdash \sigma \triangleright c!\vec{d}.Q$, by tConf, we know

$$d \in \mathbf{dom}(\Gamma) \text{ implies } \sigma(d) = \top \tag{24}$$

$$\Gamma \vdash c!\vec{d}.Q \tag{25}$$

By (25) and the respective Inversion Lemma we know $\exists\Gamma_1$ such that:

$$\frac{\Gamma_1, c:[\vec{\mathbf{T}}]^a, \overrightarrow{d:\mathbf{T}} \vdash c!\vec{d}.Q}{\Gamma \vdash c!\vec{d}.Q}\ \Gamma \prec (\Gamma_1, c:[\vec{\mathbf{T}}]^a, \overrightarrow{d:\mathbf{T}}) \tag{26}$$

From (26) we know $c \in \mathbf{dom}(\Gamma)$ and by (24) we must also have $\sigma(c) = \top$, which constradicts (23).

□

4 Subject Reduction

Lemma 29. $\Gamma \vdash P$ *and* $c \notin \text{fn}\, P$ *implies* $\Gamma \setminus c \vdash P$ *where* $\Gamma \setminus c = \{u:\mathbf{T} \mid u:\mathbf{T} \in \Gamma$ *and* $u \neq c\}$

Lemma 30 (Sub environments and Reduction)**.** $\Gamma \vdash \sigma \triangleright P$ *and* $\sigma \triangleright P \longrightarrow \sigma' \triangleright P'$ *then* $\sigma \prec_\Gamma \sigma'$

Theorem 31 (Subject Reduction)**.** *If* $\Gamma \vdash \sigma \triangleright P$*,* Γ *is minimal and* $\sigma \triangleright P \rightarrow \sigma' \triangleright P'$ *then* $\exists$ *minimal* Γ' *such that* $\Gamma \prec \Gamma'$*, and* $\Gamma' \vdash \sigma' \triangleright P'$*.*

Proof. By rule induction on $\sigma \triangleright P \rightarrow \sigma \triangleright P'$.

rFree: From the rule conclusion we know:

$$\sigma = \sigma_1, c:\top \text{ and } \sigma' = \sigma_1, c:\bot \tag{27}$$

$$P = \mathsf{free}\, c.Q \text{ and } P' = Q \tag{28}$$

By $\Gamma \vdash \sigma \triangleright P$, tConf,(28) and the respective Inversion Lemma, we know that $\exists\Gamma'$ such that

$$d \in \mathbf{dom}(\Gamma) \text{ implies } \sigma(d) = \top \tag{29}$$

$$\Gamma \prec \Gamma', c:[\overrightarrow{\mathbf{T}}]^\bullet \tag{30}$$

$$\Gamma' \vdash Q \tag{31}$$

Now (30) and Lemma 8 implies

$$\exists\Gamma''.\ \Gamma' = \Gamma'', c:[\overrightarrow{\mathbf{T}'}]^\bullet \text{ and } \Gamma'' \prec \Gamma' \tag{32}$$

By tStr, (31) and (32) we obtain

$$\Gamma'' \vdash Q$$

By (32) we know $c \notin \mathbf{dom}(\Gamma'')$. Moreover, by (29), (27) we obtain

$$d \in \mathbf{dom}(\Gamma'') \text{ implies } \sigma'(d) = \top$$

which by tConf and (28) gives $\Gamma'' \vdash \sigma' \triangleright P'$. Moreover, by (32) we deduce that $\Gamma \prec \Gamma''$.

RSALL: From the rule conclusion we know:

$$\sigma = \sigma' \tag{33}$$

$$P = \mathsf{alloc}(x).Q \tag{34}$$

$$P' = (\nu c : \top) Q[{}^{c}/_{x}] \text{ where } c \notin \mathbf{dom}(\sigma) \tag{35}$$

From (35) and the definition of a configuration we deduce that $c \notin \mathsf{fn}\, P$. By (34) TCONF and the respective Inversion Lemma we have:

$$d \in \mathbf{dom}(\Gamma) \text{ implies } \sigma(d) = \top \tag{36}$$

$$\Gamma \prec \Gamma' \tag{37}$$

$$\Gamma', x : [\overrightarrow{\mathbf{T}}]^{\bullet} \vdash Q \tag{38}$$

Since $c \notin \mathsf{fn}\, Q$, by (38) and Lemma 29 we know

$$(\Gamma' \setminus c), x : [\overrightarrow{\mathbf{T}}]^{\bullet} \vdash Q \tag{39}$$

and by (37) we obtain also $\Gamma \prec \Gamma' \setminus c$. Now by (39) and Lemma 20 we deduce:

$$(\Gamma' \setminus c), c : [\overrightarrow{\mathbf{T}}]^{\bullet} \vdash Q[{}^{c}/_{x}] \tag{40}$$

Clearly, by definition of $\Gamma' \setminus c$, $c \notin \mathbf{dom}(\Gamma' \setminus c)$ and by TRST1 and (35) we obtain

$$\Gamma' \setminus c \vdash P'$$

By $\Gamma \prec \Gamma' \setminus c$ and TSTR we derive $\Gamma \vdash P'$ and by (33), (36) and TCONS we conclude $\Gamma \vdash \sigma' \triangleright P'$.

TCTXT: Follows from Lemma 30 and from Lemma 27.

□