Appendix: Complete proofs

Lemma 4.6 (*Termination of Type Filtering*) For any well-formed type environment E, and types T and U, the backward application of the type rules to $E \vdash T :: \mathit{NodeTest} \Rightarrow U$ terminates.

Proof
l-guardedness of E avoids infinite applications of rule (VarFilt), the only one that could make rules diverge. □

Lemma 4.7 (*Type Filtering Checking*) For any well-formed type environment E and type T well-formed in E:

$$E \vdash T :: \mathit{NodeTest} \Rightarrow U \;\Leftrightarrow\; [\![U]\!]_E = \{f :: \mathit{NodeTest} \mid f \in [\![T]\!]_E\}$$

Proof
By induction on the proof of $E \vdash T :: \mathit{NodeTest} \Rightarrow U$. □

Lemma 4.9 For any E well-formed and T such that $E \vdash T$ Def and for each tree t:

$$(\exists f \in [\![T]\!]_E.\ t \in_{st} f) \;\Leftrightarrow\; (\exists U.\ T \rightarrow_e^E U \;\wedge\; t \in [\![U]\!]_E \;\wedge\; (U \equiv l[T'] \vee U \equiv B))$$

Proof
($\Rightarrow$) follows by induction on the structure of t. ($\Leftarrow$) follows by induction on the length of e. □

Lemma 4.10 For any E well-formed and T such that $E \vdash T$ Def, and for any U:

$$T \rightarrow_e^E U \;\wedge\; (U \equiv l[T'] \vee U \equiv B) \;\Leftrightarrow\; U \in \mathit{SubTrees}_E(T)$$

Proof
($\Rightarrow$) follows by induction on the length of e, while ($\Leftarrow$) follows by induction on $|\mathit{SubTrees}_E(T)|$. □

Lemma 4.11 For any well-formed E and T such that $E \vdash T$ Def, for each tree t:

$$(\exists f \in [\![T]\!]_E.\ t \in_{st} f) \;\Leftrightarrow\; (\exists U.\ U \in \mathit{SubTrees}_E(T) \wedge t \in [\![U]\!]_E)$$

Proof
By Lemma 4.9 and Lemma 4.10. □

Lemma 4.12 (*Soundness of DOS Type*) For any well-formed E and T such that $E \vdash T$ Def and

$$\begin{aligned} \mathit{SubTrees}_E(T) &= \{U_1, \ldots, U_n\} \\ U &\equiv (U_1 \mid \ldots \mid U_n)* \end{aligned}$$

then:

$$\forall f \in [\![T]\!]_E.\ \mathit{dos}(f) \in [\![U]\!]_E$$

Proof
Consider $f \in [\![T]\!]_E$ with $\mathit{dos}(f) = t_1, \ldots, t_m$. We have $t_j \in_{st} f$ for each $j = 1 \ldots m$ (Definition 4.8). Hence, we can apply Lemma 4.11, obtaining that there exists $\{U_{i_1}, \ldots, U_{i_m}\} \subseteq \mathit{SubTrees}_E(T)$ such that $t_j \in [\![U_{i_j}]\!]_E$ for $j = 1 \ldots m$. Now, since

$$\begin{aligned} &\mathit{SubTrees}_E(T) = \{U_1, \ldots, U_n\} \\ &U \equiv (U_1 \mid \ldots \mid U_n)* \end{aligned}$$

we have that $[\![U]\!]_E$ contains all the forests obtained by combinations and repetitions of trees belonging to $U_i \in SubTrees_E(T)$, and in particular it contains the forest $dos(f) = t_1, \ldots, t_m$, as $t_j \in [\![U_{i_j}]\!]_E$ with $U_{i_j} \in SubTrees_E(T)$, for $j = 1 \ldots m$.

□

Theorem 4.14 (*Upper Bound*) For any well-formed environment E, Γ well-formed in E, and query Q:

$$E;\ \Gamma \vdash_\beta\ Q : (U;\ \_)\ \wedge\ \rho \in \mathscr{R}(E,\Gamma)\ \Rightarrow\ [\![Q]\!]_\rho \in [\![U]\!]_E$$

Proof
We prove the statements:

- $\forall \rho \in \mathscr{R}(E,\Gamma)$.
  $E;\ \Gamma \vdash_\beta\ Q : (U;\ \_)\ \Rightarrow\ [\![Q]\!]_\rho \in [\![U]\!]_E$
- $\forall \rho \in \mathscr{R}(E,\Gamma).\ \forall f \in [\![T]\!]_E$.
  $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{in}\ T \to Q : (U;\ \_)\ \Rightarrow\ \prod_{t \in trees(f)} [\![Q]\!]_{\rho, \overline{x} \to t} \in [\![U]\!]_E$

We proceed by induction on the proof tree and by cases on the last applied rule. We only consider the main cases; the others are easier.

(TypeForest) In this case, we have $E;\ \Gamma \vdash_\beta\ Q_1, Q_2 : (U_1, U_2;\ \_)$ and the following hypothesis:

$$\begin{array}{ll} E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (U_1;\ \_) & (1)\\ E;\ \Gamma \vdash_{\beta.1}\ Q_2 : (U_2;\ \_) & (2)\\ \forall \rho \in \mathscr{R}(E,\Gamma).\ [\![Q_1]\!]_\rho \in [\![U_1]\!]_E & (3)\\ \forall \rho \in \mathscr{R}(E,\Gamma).\ [\![Q_2]\!]_\rho \in [\![U_2]\!]_E & (4) \end{array}$$

We want to prove:

$$\forall \rho \in \mathscr{R}(E,\Gamma).[\![Q_1, Q_2]\!]_\rho \in [\![U_1, U_2]\!]_E$$

Observe that $\forall \rho \in \mathscr{R}(E,\Gamma)$:

$$[\![Q_1, Q_2]\!]_\rho = [\![Q_1]\!]_\rho, [\![Q_2]\!]_\rho$$

Therefore the thesis follows from (3) and (4).

(TypeLetSplitting) Recall that we are assuming $Split_E(T) = \{T\}$. We have $E;\ \Gamma \vdash_\beta$ $\texttt{let}\ x := Q_1\ \texttt{return}\ Q_2 : (U;\ \_)$ and, by induction:

$$\begin{array}{ll} E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \_) & (1)\\ E;\ \Gamma,\ x : T_1 \vdash_{\beta.1}\ Q_2 : (U;\ \_) & (2)\\ \forall \rho \in \mathscr{R}(E,\Gamma).\ [\![Q_1]\!]_\rho \in [\![T_1]\!]_E & (3)\\ \forall \rho \in \mathscr{R}(E,(\Gamma, x : T_1)).\ [\![Q_2]\!]_\rho \in [\![U]\!]_E & (4) \end{array}$$

We want to prove that

$$\forall \rho \in \mathscr{R}(E,\Gamma).\ [\![\texttt{let}\ x := Q_1\ \texttt{return}\ Q_2]\!]_\rho \in [\![U]\!]_E$$

To this aim, we recall that:

$$\forall \rho \in \mathscr{R}(E,\Gamma).\ [\![\texttt{let}\ x := Q_1\ \texttt{return}\ Q_2]\!]_\rho = [\![Q_2]\!]_{\rho, x \mapsto [\![Q_1]\!]_\rho}\ \ (*)$$

where, by (3), $[\![Q_1]\!]_\rho \in [\![T_1]\!]_E$. Hence $\rho, x \mapsto [\![Q_1]\!]_\rho \in \mathscr{R}(E,(\Gamma, x : T_1))$, from which,

by (4) and induction,

$$[\![Q_2]\!]_{\rho,x\mapsto[\![Q_1]\!]_\rho} = [\![\texttt{let } x := Q_1 \texttt{ return } Q_2]\!]_\rho \in [\![U]\!]_E$$

(TypeFor) In this case we have $E;\ \Gamma \vdash_\beta \ \texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2 : (U;\ \_)$ and the following hypothesis:

$$E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (U_1;\ \_) \quad (1)$$
$$\forall \rho \in \mathscr{R}(E,\Gamma).[\![Q_1]\!]_\rho \in [\![U_1]\!]_E \quad (2)$$
$$E;\ \Gamma \vdash_{\beta.1}\ \overline{x} \texttt{ in } U_1 \to Q_2 : (U;\ \_) \quad (3)$$
$$\forall \rho \in \mathscr{R}(E,\Gamma).\ \forall f \in [\![U_1]\!]_E.\ \prod_{t\in trees(f)} [\![Q_2]\!]_{\rho,\overline{x}\mapsto t} \in [\![U]\!]_E \quad (4)$$

We want to prove:

$$\forall \rho \in \mathscr{R}(E,\Gamma).\ [\![\texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2]\!]_\rho \in [\![U]\!]_E$$

Recall that $\forall \rho \in \mathscr{R}(E,\Gamma)$:

$$[\![\texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2]\!]_\rho = \prod_{t\in trees(f)} [\![Q_2]\!]_{\rho,\overline{x}\mapsto t}$$

with

$$f = [\![Q_1]\!]_\rho$$

By (2) we have $f \in [\![U_1]\!]_E$, hence the case follows by (4).

(TypeInConc) In this case we have $E;\ \Gamma \vdash_\beta \ \overline{x} \texttt{ in } T_1, T_2 \to Q : (T_1', T_2';\ \_)$ and the following hypothesis:

$$E;\ \Gamma \vdash_\beta \ \overline{x} \texttt{ in } T_1 \to Q : (T_1';\ \_) \quad (1)$$
$$E;\ \Gamma \vdash_\beta \ \overline{x} \texttt{ in } T_2 \to Q : (T_2';\ \_) \quad (2)$$
$$\forall \rho \in \mathscr{R}(E,\Gamma).\ \forall f \in [\![T_1]\!]_E.\ \textstyle\prod_{t\in trees(f)} [\![Q]\!]_{\rho,x\mapsto t} \in [\![T_1']\!]_E \quad (3)$$
$$\forall \rho \in \mathscr{R}(E,\Gamma).\ \forall f \in [\![T_2]\!]_E.\ \textstyle\prod_{t\in trees(f)} [\![Q]\!]_{\rho,x\mapsto t} \in [\![T_2']\!]_E \quad (4)$$

We want to prove:

$$\forall \rho \in \mathscr{R}(E,\Gamma).\ \forall f \in [\![T_1, T_2]\!]_E.\ \prod_{t\in trees(f)} [\![Q]\!]_{\rho,\overline{x}\mapsto t} \in [\![T_1', T_2']\!]_E$$

For any $\rho \in \mathscr{R}(E,\Gamma)$ and $f = (f_1, f_2) \in [\![T_1, T_2]\!]_E$ with $f_i \in [\![T_i]\!]_E$:

$$\prod_{t\in trees(f_1,f_2)} [\![Q]\!]_{\rho,\overline{x}\mapsto t} = \prod_{t\in trees(f_1)} [\![Q]\!]_{\rho,\overline{x}\mapsto t}\ ,\ \prod_{t\in trees(f_2)} [\![Q]\!]_{\rho,\overline{x}\mapsto t}$$

By (3) and (4) we have

$$\prod_{t\in trees(f_i)} [\![Q]\!]_{\rho,\overline{x}\mapsto t} \in [\![T_i']\!]_E$$

and this proves the case since

$$[\![T_1', T_2']\!]_E = \{f_1, f_2 \mid\ f_i \in [\![T_i']\!]_E\}$$

(TypeInElSplitting) Similar to (TypeLetSplitting) .

(TypeChild) It follows from Lemma 4.7.

(TypeDos) We have $J \equiv E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{dos} :: \mathit{NodeTest} : (U';\ \mathscr{S})$ and the following hypothesis:

$$\begin{aligned}
&\mathit{WF}(J) && (1)\\
&\overline{x} : T \in \Gamma\ \wedge\ (T \equiv m[T'] \vee T \equiv B) && (2)\\
&\{U_1, \ldots, U_n\} = \mathit{SubTrees}_E(T) && (3)\\
&U \equiv (U_1 \mid \ldots \mid U_n)* && (4)\\
&E \vdash\ U :: \mathit{NodeTest} \Rightarrow U' && (5)
\end{aligned}$$

By (1) we can apply Lemma 4.12, from which

$$\forall f \in [\![T]\!]_E.\ \mathit{dos}(f) \in [\![U]\!]_E$$

and by Lemma 4.7

$$\forall f \in [\![U]\!]_E.\ \mathit{dos}(f) :: \mathit{NodeTest} \in [\![U']\!]_E$$

Hence, the case is proved since

$$\forall \rho \in \mathscr{R}(E,\Gamma).\ [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_\rho = \mathit{dos}(\rho(\overline{x})) :: \mathit{NodeTest}$$

with $\rho(\overline{x}) \in [\![T]\!]_E$.

□

Theorem 4.15 (*Soundness of Existential Error-Checking*) For any well-formed environment E, Γ well-formed in E, and query Q:

$$E;\ \Gamma \vdash_\beta\ Q : (U;\ \mathscr{S})\ \wedge\ \beta.\alpha \in \mathscr{S}\ \Rightarrow Q \textit{ has an error at } \alpha \textit{ w.r.t. } \mathscr{R}(E,\Gamma)$$

Proof
We prove the following statements:

- $E;\ \Gamma \vdash_\beta\ Q : (U;\ \mathscr{S})\ \Rightarrow$
  $\gamma \in \mathscr{S}\ \Rightarrow\ (\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q) \wedge Q \textit{ has an error at } \alpha)$
- $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{in}\ T \to Q : (U;\ \mathscr{S}) \Rightarrow$
  $\gamma \in \mathscr{S}\ \Rightarrow\ (\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q) \wedge$
  $(\forall \overline{f} \in [\![T]\!]_E.\ \texttt{for}\ \overline{x}\ \texttt{in}\ \overline{f}\ \texttt{return}\ Q\ \textit{ has an error at }\ 1.\alpha))$ [8]

We proceed by induction on the proof tree and by case distinction on the last rule applied. We prove only some of the main cases (see the Appendix for more cases).

(TypeForest) We have $E;\ \Gamma \vdash_\beta\ Q_1, Q_2 : (T_1, T_2;\ \mathscr{S}_1 \cup \mathscr{S}_2)$ and the following hypothesis

$$\begin{aligned}
&E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \mathscr{S}_1) && (1)\\
&E;\ \Gamma \vdash_{\beta.1}\ Q_2 : (T_2;\ \mathscr{S}_2) && (2)\\
&\gamma \in \mathscr{S}_1 \Rightarrow (\gamma \equiv \beta.0.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_1) \wedge\ Q_1 \textit{ has an error at } \alpha) && (3)\\
&\gamma \in \mathscr{S}_2 \Rightarrow (\gamma \equiv \beta.1.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_2) \wedge\ Q_2 \textit{ has an error at } \alpha) && (4)
\end{aligned}$$

We want to prove that

$$\gamma \in \mathscr{S}_1 \cup \mathscr{S}_2 \Rightarrow (\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_1, Q_2) \wedge Q_1, Q_2 \textit{ has an error at } \alpha)$$

[8] To be formally precise $\overline{f}$ should be defined as a term of a subgrammar $() \mid b \mid l[f] \mid f, f'$. Although inelegant, for the sake of simplicity, we allow here a notation that mixes up syntax and semantics.

By $\gamma \in \mathscr{S}_1 \cup \mathscr{S}_2$, (3) and (4):

$$\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_1, Q_2)$$

It remains to prove that Q_1, Q_2 has an error at α. To this end, observe that by $\gamma \equiv \beta.\alpha \in \mathscr{S}_1 \cup \mathscr{S}_2$, we have that either $\alpha \equiv 0.\alpha' \wedge \alpha' \in \mathscr{S}_1$ or $\alpha \equiv 1.\alpha' \wedge \alpha' \in \mathscr{S}_2$. Suppose we are in the first case (the second one is similar). In this case, by (3), Q_1 has an error at α', and this means that Q_1, Q_2 has an error at $\alpha \equiv 0.\alpha'$.

(TypeFor) We have $E;\ \Gamma \vdash_\beta\ \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2 : (T_2;\ \mathscr{S}_1 \cup \mathscr{S}_2 \cup \mathscr{S})$ and the following hypothesis:

$$E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \mathscr{S}_1) \quad (1)$$
$$E;\ \Gamma \vdash_{\beta.1}\ \overline{x}\ \texttt{in}\ T_1 \to Q_2 : (T_2;\ \mathscr{S}_2) \quad (2)$$
$$\mathscr{S} = \text{ if } T_1 \sim_E () \text{ then } \{\beta.0\} \text{ else } \emptyset \quad (3)$$
$$\gamma \in \mathscr{S}_1 \Rightarrow (\gamma \equiv \beta.0.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_1) \wedge Q_1 \textit{ has an error at } \alpha) \quad (4)$$
$$\gamma \in \mathscr{S}_2 \Rightarrow (\gamma \equiv \beta.1.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_2) \wedge (\forall f \in [\![T_1]\!]_E. \quad (5)$$
$$\texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q_2 \textit{ has an error at } 1.\alpha))$$

We want to prove that $\forall\ \gamma$

$$\gamma \in (\mathscr{S} \cup \mathscr{S}_1 \cup \mathscr{S}_2) \ \Rightarrow\ (\gamma \equiv \beta.\alpha' \wedge \alpha' \in \mathit{CriticalLocs}(\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2)$$
$$\wedge\ \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2 \textit{ has an error at } \alpha'$$

For any

$$\gamma \in (\mathscr{S} \cup \mathscr{S}_1 \cup \mathscr{S}_2)$$

$\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2)$ follows from (3), (4) and (5). To prove that $\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2$ has an error at α we distinguish three possible cases: (i) $\alpha \equiv 0$, (ii) and $\alpha \equiv 0.\alpha'$ and $\alpha' \in \mathit{CriticalLocs}(Q_1)$, and (iii) $\alpha \equiv 1.\alpha'$ and $\alpha' \in \mathit{CriticalLocs}(Q_2)$. Case (ii) does not pose particular problems (proceed as for case (TypeForest)). In case (i) we have $T_1 \sim_E ()$, hence, by Lemma 4.5 and Theorem 4.14, we have $[\![Q_1]\!]_\rho = ()$ for each $\rho \in \mathscr{R}(E, \Gamma)$, which proves the case. It remains case (iii). We want to prove that

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ \forall \rho' \in \left(\bigcup_{t \in trees([\![Q_1]\!]_\rho)} \mathit{Ext}((\rho, \overline{x} \mapsto t),\ Q_2,\ \alpha') \right).\ [\![(Q_2)_{|\alpha'}]\!]_{\rho'} = ()$$

To prove it we exploit hypothesis (5), and expand it as follows

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ \forall f \in [\![T_1]\!]_E.$$
$$\forall \rho' \in \textstyle\bigcup_{t \in trees(f)} \mathit{Ext}((\rho, \overline{x} \mapsto t),\ Q_2,\ \alpha').\ [\![(Q_2)_{|\alpha'}]\!]_{\rho'} = ()$$

This, together with $[\![Q_1]\!]_\rho \in [\![T]\!]_E$ (Theorem 4.14), proves the case.

(TypeDos) We have $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{dos} :: \mathit{NodeTest} : (U;\ \mathscr{S})$ and the following hypothesis:

$$WF(E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{dos} :: \mathit{NodeTest} : (U;\ \mathscr{S})) \quad (1)$$
$$\overline{x} : T \in \Gamma\ \wedge\ (T \equiv m[T] \vee T \equiv B) \quad (2)$$
$$\{U_1, \ldots, U_n\} = \mathit{SubTrees}_E(T) \quad (3)$$
$$U' \equiv (U_1 \mid \ldots \mid U_n)* \quad (4)$$
$$E \vdash\ U' :: \mathit{NodeTest} \Rightarrow U \quad (5)$$
$$\mathscr{S} = \text{ if } U \sim_E () \text{ then } \{\beta\} \text{ else } \emptyset \quad (6)$$

We want to prove that

$$\gamma \in \mathscr{S} \;\Rightarrow\; (\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(\overline{x}\ \texttt{dos} :: \mathit{NodeTest}) \wedge (\overline{x}\ \texttt{dos} :: \mathit{NodeTest} \;\; \mathit{has\ an\ error\ at} \;\; \alpha))$$

We first observe that it may be $\mathscr{S} = \{\beta\}$ or $\mathscr{S} = \emptyset$. Moreover, $\mathit{CriticalLocs}(\overline{x}\ \texttt{dos} :: \mathit{NodeTest}) = \{\epsilon\}$, which proves

$$\gamma \in \mathscr{S} \;\Rightarrow\; (\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(\overline{x}\ \texttt{dos} :: \mathit{NodeTest}))$$

It remains to prove that $\mathscr{S} = \{\beta\}$ entails that $\overline{x}\ \texttt{dos} :: \mathit{NodeTest}$ has an error at ϵ. $\overline{x}\ \texttt{dos} :: \mathit{NodeTest}$ has an error at ϵ if and only if

$$\forall \rho \in \mathscr{R}(E, \Gamma). \forall \rho' \in \mathit{Ext}(\epsilon, \overline{x}\ \texttt{dos} :: \mathit{NodeTest}, \rho).\ [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho'} = ()$$

Since $\mathit{Ext}(\epsilon, \overline{x}\ \texttt{dos} :: \mathit{NodeTest}, \rho) = \{\rho\}$, we have that $\overline{x}\ \texttt{dos} :: \mathit{NodeTest}$ has an error at ϵ if and only if

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho} = ()$$

Hence, we have to prove that

$$\mathscr{S} = \{\beta\} \;\Rightarrow\; \forall \rho \in \mathscr{R}(E, \Gamma).\ [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho} = ()$$

We have $\mathscr{S} = \{\beta\}$ if and only if $U \sim_E ()$, which, by Lemma 4.5, implies that

$$[\![U]\!]_E = \{()\}$$

Therefore, by Theorem 4.14, we have proved the case.

□

Lemma 5.3 For each $*$-guarded environment E and type T defined in E:

$$[\![T]\!]_E \;=\; \bigcup_{A \in \mathit{Split}_E(T)} [\![A]\!]_E$$

Proof
By induction on the cardinality of $\mathit{Split}_E(T)$ and by case distinction on the shape of T. □

Lemma 5.6 (*Monotonicity of Filtering, Childr and DOS*)

1. $\forall f, f'.\ f \sqsubseteq f' \;\Rightarrow\; f :: \mathit{NodeTest} \sqsubseteq f' :: \mathit{NodeTest}$, $\mathit{dos}(f) \sqsubseteq \mathit{dos}(f')$
2. $\forall t, t'.\ t \sqsubseteq t' \;\Rightarrow\; \mathit{childr}(t) \sqsubseteq \mathit{childr}(t')$

Proof
Property 1. follows by induction on the structure of f, while 2. easily follows by definition of childr(t). □

Lemma 5.7 (*Query Monotonicity*)

$$\forall Q, \rho, \rho'.\ \rho \sqsubseteq \rho' \;\Rightarrow\; [\![Q]\!]_{\rho} \sqsubseteq [\![Q]\!]_{\rho'}$$

Proof
By case distinction and induction on the structure of Q. We consider only the main cases.

$Q \equiv \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2$. For substitutions ρ and ρ' such that $\rho \sqsubseteq \rho'$, we want to prove

$$[\![\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2]\!]_\rho \sqsubseteq [\![\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2]\!]_{\rho'}$$

By induction, we assume

$$[\![Q_1]\!]_\rho \sqsubseteq [\![Q_1]\!]_{\rho'}\ (*)$$

This means

$$\forall t \in \mathit{trees}([\![Q_1]\!]_\rho).\exists t' \in \mathit{trees}([\![Q_1]\!]_{\rho'}).\ t \sqsubseteq t'$$

By definition of query semantics, the property to prove can be rewritten as:

$$\prod_{t \in \mathit{trees}([\![Q_1]\!]_\rho)} [\![Q_2]\!]_{\rho,\overline{x}\to t} \sqsubseteq \prod_{t \in \mathit{trees}([\![Q_1]\!]_{\rho'})} [\![Q_2]\!]_{\rho',\overline{x}\to t}$$

that is

$$\forall \overline{t} \in \mathit{trees}(\prod_{t \in \mathit{trees}([\![Q_1]\!]_\rho)} [\![Q_2]\!]_{\rho,\overline{x}\to t}).\ \exists \overline{t}' \in \mathit{trees}(\prod_{t \in \mathit{trees}([\![Q_1]\!]_{\rho'})} [\![Q_2]\!]_{\rho',\overline{x}\to t}).\ \overline{t} \sqsubseteq \overline{t}'$$

Consider

$$\overline{t} \in \mathit{trees}(\prod_{t \in \mathit{trees}([\![Q_1]\!]_\rho)} [\![Q_2]\!]_{\rho,\overline{x}\to t}).$$

For such a $\overline{t}$ we have that $\exists\ t' \in \mathit{trees}([\![Q_1]\!]_\rho)$ such that $\overline{t} \in \mathit{trees}([\![Q_2]\!]_{\rho,\overline{x}\to t'})$. By (*), for such a t' there exists $t'' \in \mathit{trees}([\![Q_1]\!]_{\rho'})$ with $t' \sqsubseteq t''$. This entails $(\rho, \overline{x} \mapsto t') \sqsubseteq (\rho', \overline{x} \mapsto t'')$, hence by induction we can assume

$$[\![Q_2]\!]_{\rho,\overline{x}\to t'} \sqsubseteq [\![Q_2]\!]_{\rho',\overline{x}\to t''}$$

which, since $\overline{t} \in \mathit{trees}([\![Q_2]\!]_{\rho,\overline{x}\to t'})$, gives us

$$\exists \overline{t}' \in \mathit{trees}([\![Q_2]\!]_{\rho',\overline{x}\to t''}).\ \overline{t} \sqsubseteq \overline{t}'$$

Hence the case is proved by observing that $t'' \in \mathit{trees}([\![Q_1]\!]_{\rho'})$ and that

$$\overline{t}' \in \mathit{trees}([\![Q_2]\!]_{\rho',\overline{x}\to t''}) \ \Rightarrow\ \overline{t}' \in \mathit{trees}(\prod_{t \in \mathit{trees}([\![Q_1]\!]_{\rho'})} [\![Q_2]\!]_{\rho',\overline{x}\to t})$$

$Q \equiv \overline{x}\ \texttt{child} :: \mathit{NodeTest}$. Directly follows from Lemma 5.6.
$Q \equiv \overline{x}\ \texttt{dos} :: \mathit{NodeTest}$. Directly follows from Lemma 5.6.
□

Corollary 5.8 Given a well formed query Q and a substitution ρ such that $FV(Q) \subseteq \mathit{dom}(\rho) \cup \{\chi\}$:

$$f_1 \sqsubseteq f_2\ \Rightarrow \prod_{t \in \mathit{trees}(f_1)} [\![Q]\!]_{\rho,\chi\to t}\ \sqsubseteq \prod_{t \in \mathit{trees}(f_2)} [\![Q]\!]_{\rho,\chi\to t}$$

Proof
By Lemma 5.7. □

Lemma 5.9 (*Extension Monotonicity*) For any Q and pair of substitutions ρ_1 and ρ_2 such that $FV(Q) \subseteq \mathit{dom}(\rho_1) = \mathit{dom}(\rho_2)$ and $\rho_1 \sqsubseteq \rho_2$, $\forall \beta \in \mathit{Locs}(Q)$.

$$\forall \rho' \in \mathit{Ext}(\rho_1, Q, \beta).\ \exists \rho'' \in \mathit{Ext}(\rho_2, Q, \beta).\ \rho' \sqsubseteq \rho''$$

Proof
By induction on the structure of Q, Lemma 5.7, and Corollary 5.8. □

Lemma 5.10 (*Closure of Split Types*) For any $*$-guarded environment E and type T well-formed in E, for any $A \in Split_E(T)$:

$$\forall f_1,\ f_2 \in [\![A]\!]_E.\ \exists f \in [\![A]\!]_E.\ f_i \sqsubseteq f\ i = 1,2$$

Proof
We first observe that for each $A \in Split_E(T)$

$$Split_E(A) = \{A\}$$

This entails that we can define a measure $d^*(A)$, over types obtained by splitting, as follows:

$$\begin{array}{lcl} d^*(()) & = & 0 \\ d^*(B) & = & 0 \\ d^*(T'*) & = & 0 \\ d^*(l[T']) & = & 1 + d^*(T') \\ d^*(T', U') & = & 1 + d^*(T') + d^*(U') \end{array}$$

Observe that $d^*(A)$ is not defined over union types, since A can not be a union type. We then proceed by induction on $d^*(A)$.

If $d^*(A) = 0$, the case $A \equiv B$ is obvious, as, by definition of $\sqsubseteq$, $\forall b_1, b_2, b_3 \in [\![B]\!]_E$ we have $b_1 \sqsubseteq b_3$ and $b_2 \sqsubseteq b_3$. Here, the only interesting case is $A \equiv T'*$. For this case, given f_1 and f_2 in $[\![A]\!]_E$, observe that their composition f_1, f_2 still is in $[\![A]\!]_E$ and that $f_1 \sqsubseteq f_1, f_2$ and $f_2 \sqsubseteq f_1, f_2$.

If $d^*(A) > 0$ the only interesting case is $A \equiv T', U'$. Consider f_1 and f_2 in $[\![T', U']\!]_E$. We have

$$\begin{array}{l} f_1 = f_1^1, f_1^2\ \wedge\ f_1^1 \in [\![T']\!]_E\ \wedge f_1^2 \in [\![U']\!]_E \\ f_2 = f_2^1, f_2^2\ \wedge f_2^1 \in [\![T']\!]_E\ \wedge f_2^2 \in [\![U']\!]_E \end{array}$$

By induction we have that there exists $f' \in [\![T']\!]_E$ and $f'' \in [\![U']\!]_E$ such that

$$\begin{array}{l} f_1^1, f_2^1 \sqsubseteq f' \\ f_1^2, f_2^2 \sqsubseteq f'' \end{array}$$

hence $f_1^1, f_2^1, f_1^2, f_2^2 \sqsubseteq f', f''$. Since $f_1, f_2 \sqsubseteq f_1^1, f_2^1, f_1^2, f_2^2$ by transitivity of $\sqsubseteq$ we have that $f_1, f_2 \sqsubseteq f', f''$. □

Lemma 5.11 For any type A defined in a $*$-guarded environment E, if $Split_E(A) = \{A\}$ then,

$$\forall f_1, \ldots, f_n \in [\![A]\!]_E.\ \exists f \in [\![A]\!]_E.\ f_i \sqsubseteq f\ i = 1 \ldots n$$

Proof
By induction on n, Lemma 5.10, and transitivity of $\sqsubseteq$. □

Lemma 5.14 (*Query Variables Environment Splitting*) For each $*$-guarded type environment E and Γ well-formed in E:

$$\bigcup_{\Gamma' \in SplitVEnv(\Gamma, E)} \mathscr{R}(E, \Gamma') = \mathscr{R}(E, \Gamma)$$

Proof
By induction on the length of Γ and by Lemma 5.3. $\square$

Lemma 5.15 For any strongly-$*$-guarded and well-formed Γ in a $*$-guarded type environment E, and $\rho_1, \ldots, \rho_n \in \mathscr{R}(E, \Gamma)$, there exists $\rho \in \mathscr{R}(E, \Gamma)$ such that $\rho_i \sqsubseteq \rho$ for $i = 1 \ldots n$.

Proof
By induction on the length of Γ and by Lemma 5.11. $\square$

Lemma 5.17 (*Invariance of Well-Formation*) For any well-formed judgement $E;\ \Gamma \vdash_\beta Q : (U;\ \mathscr{S})$ with Γ strongly-$*$-guarded, the backward application of the rules produces judgements that are well-formed as well, and containing strongly-$*$-guarded environments.

Proof
It directly follows by the way rules (TypeInElSplitting) and (TypeLetSplitting) are defined. $\square$

Lemma 5.18 (*Soundness and Completeness of DOS Type*) For any E well-formed and T such that $E \vdash T$ Def and

$$\begin{aligned} SubTrees_E(T) &= \{U_1, \ldots, U_n\} \\ U &\equiv (U_1 \mid \ldots \mid U_n)* \end{aligned}$$

then:

(1) $\forall f \in [\![T]\!]_E.\ dos(f) \in [\![U]\!]_E$

(2) $\forall f \in [\![U]\!]_E.\ \exists \{f'_1, \ldots, f'_m\} \subseteq [\![T]\!]_E.\ f \sqsubseteq dos(f'_1, \ldots, f'_m)$

(3) $Split_E(T) = T \ \Rightarrow\ \forall f \in [\![U]\!]_E.\ \exists f' \in [\![T]\!]_E.\ \ f \sqsubseteq dos(f')$

Proof
(1) Similar to Lemma 4.12.
(2) Consider $f \in [\![U]\!]_E$ with $f = t_1, \ldots, t_m$. This implies that for each $i = 1 \ldots m$ there exists $U^i \in SubTrees_E(T)$ such that $t_i \in [\![U^i]\!]_E$. By Lemma 4.11 we have $t_i \in_{st} f'_i$ with $f'_i \in [\![T]\!]_E$ for each $i = 1 \ldots m$. Therefore, by observing that

$$dos(f'_1, \ldots, f'_m) = dos(f'_1), \ldots, dos(f'_m),$$

and by $t_i \in_{st} f'_i$, we have that each $dos(f'_i)$ can be decomposed in f^1_i, t_i, f^2_i (Definition 4.8). Hence, each t_i is at the top level of $dos(f'_1, \ldots, f'_n)$ and this implies

$$f = t_1, \ldots, t_m \sqsubseteq dos(f'_1, \ldots, f'_n)$$

(3) By (2) we know that for $f \in [\![U]\!]_E$ there exist $f'_1, \ldots, f'_m \in [\![T]\!]_E$ such that

$$f \sqsubseteq dos(f'_1, \ldots, f'_m)$$

Since $Split_E(T) = T$, by Lemma 5.11 there exists $f' \in [\![T]\!]_E$ such that $f'_i \sqsubseteq f'$ for $i = 1 \ldots m$. From this it easily follows that

$$f'_1, \ldots, f'_m \sqsubseteq f'$$

Therefore, by Lemma 5.6, we have

$$f \sqsubseteq dos(f'_1, \ldots, f'_m) \sqsubseteq dos(f')$$

then by transitivity of $\sqsubseteq$ we conclude $f \sqsubseteq dos(f')$.
$\square$

Lemma 5.19 (*Upper Bound*) In the type splitting system, for each Q, $*$-guarded E, and Γ strongly-$*$-guarded and well-formed in E:

$$E;\ \Gamma \vdash_\beta\ Q : (U;\ \_)\ \wedge\ \rho \in \mathscr{R}(E,\Gamma)\ \Rightarrow\ [\![Q]\!]_\rho \in [\![U]\!]_E$$

Proof
We prove the statements:

- $\forall \rho \in \mathscr{R}(E,\Gamma)$.
  $E;\ \Gamma \vdash_\beta\ Q : (U';\ \_)\ \Rightarrow\ [\![Q]\!]_\rho \in [\![U']\!]_E$
- $\forall \rho \in \mathscr{R}(E,\Gamma).\ \forall f \in [\![T]\!]_E$.
  $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{in}\ T \to Q : (U';\ \_)\ \Rightarrow\ \prod_{t \in trees(f)} [\![Q]\!]_{\rho,\overline{x}\to t} \in [\![U']\!]_E$

We proceed by induction on the proof tree and by cases on the last applied rule. We only consider the case (TypeLetSplitting). Case (TypeInElSplitting) is similar to (TypeLetSplitting), while the other cases are essentially the same as in the proof of Theorem 4.14.

(TypeLetSplitting) We have $E;\ \Gamma \vdash_\beta\ \texttt{let}\ x := Q_1\ \texttt{return}\ Q_2 : (U';\ \_)$ and, by induction:

$$\begin{array}{ll}
E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ _) & (1)\\
Split_E(T_1) = \{A_1, \ldots, A_n\} & (2)\\
E;\ \Gamma,\ x : A_i \vdash_{\beta.1}\ Q_2 : (U_i;\ __i)\ \ i = 1 \ldots n & (3)\\
U' \equiv U_1 \mid \ldots \mid U_n & (4)\\
\forall \rho \in \mathscr{R}(E,\Gamma).\ [\![Q_1]\!]_\rho \in [\![T_1]\!]_E & (5)\\
\forall \rho \in \mathscr{R}(E,(\Gamma, x : A_i)).\ [\![Q_2]\!]_\rho \in [\![U_i]\!]_E\ \ i : 1, \ldots, n & (6)
\end{array}$$

We prove that

$$\forall \rho \in \mathscr{R}(E,\Gamma).\ [\![\texttt{let}\ x := Q_1\ \texttt{return}\ Q_2]\!]_\rho \in [\![U']\!]_E$$

To this aim we recall that

$$\forall \rho \in \mathscr{R}(E,\Gamma).\ [\![\texttt{let}\ x := Q_1\ \texttt{return}\ Q_2]\!]_\rho = [\![Q_2]\!]_{\rho, x \to [\![Q_1]\!]_\rho}\ \ (*)$$

where, by (5), $[\![Q_1]\!]_\rho \in [\![T_1]\!]_E$. Since (Lemma 5.3)

$$[\![T_1]\!]_E = \bigcup_{i=1\ldots n} [\![A_i]\!]_E$$

we have that $[\![Q_1]\!]_\rho \in [\![A_j]\!]_E$ for some $j = 1 \ldots n$. Hence $(\rho, x \mapsto [\![Q_1]\!]_\rho) \in \mathscr{R}(E,(\Gamma, x : A_j))$, from which, by (6), (4) and induction,

$$[\![Q_2]\!]_{\rho, x \to [\![Q_1]\!]_\rho} \in [\![U_j]\!]_E\ \Rightarrow\ [\![Q_2]\!]_{\rho, x \to [\![Q_1]\!]_\rho} \in [\![U']\!]_E$$

□

Theorem 5.20 (*Upper Bound for the Type-Splitting System*) For each Q, $*$-guarded and well-formed E, and Γ well-formed in E:

$$E;\ \Gamma \Vdash_\beta\ Q : (U;\ \_)\ \wedge\ \rho \in \mathscr{R}(E,\Gamma)\ \Rightarrow\ [\![Q]\!]_\rho \in [\![U]\!]_E$$

Proof
We first observe that, by Lemma 5.14, $\rho \in \mathscr{R}(E,\Gamma)$ implies

$$\rho \in \mathscr{R}(E,\Gamma')$$

with $\Gamma' \in SplitVEnv(\Gamma, E)$, and also observe that, by Definition 5.16, $U \equiv U' \mid U''$ with $E;\ \Gamma' \vdash_\beta\ Q : (U';\ \_)$. Hence, by Lemma 5.19 we have that $[\![Q]\!]_\rho \in [\![U']\!]_E$ which entails $[\![Q]\!]_\rho \in [\![U]\!]_E$, as $[\![U']\!]_E \subseteq [\![U]\!]_E$.

□

Lemma 5.21 (*Lower Bound*) In the type-splitting system, for each Q, $*$-guarded E, and Γ strongly-$*$-guarded and well-formed in E:

$$E;\ \Gamma \vdash_\beta\ Q : (U;\ \_)\ \ \Rightarrow\ \ \forall f \in [\![U]\!]_E.\ \exists \rho \in \mathscr{R}(E, \Gamma).\ f \sqsubseteq [\![Q]\!]_\rho$$

Proof
We prove the following statements:

- $\forall f \in [\![U]\!]_E.\ \exists \rho \in \mathscr{R}(E, \Gamma).$
  $E;\ \Gamma \vdash_\beta\ Q : (U;\ \_)\ \Rightarrow\ f \sqsubseteq [\![Q]\!]_\rho$
- $\forall f \in [\![U]\!]_E.\ \exists \rho \in \mathscr{R}(E, \Gamma).\ \exists f \in [\![T]\!]_E.$
  $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{in}\ T \to Q : (U;\ \_)\ \Rightarrow\ f \sqsubseteq \prod_{t \in trees(f)} [\![Q]\!]_{\rho, x \to t}$

We proceed by induction on the proof tree of the proved judgement and by cases on the last rule applied. We only prove main cases.

(TypeLetSplitting) We have $E;\ \Gamma \vdash_\beta\ \texttt{let}\ x := Q_1\ \texttt{return}\ Q_2 : (U;\ \_)$ and

$$\begin{array}{ll}
E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ _) & (1)\\
Split_E(T_1) = \{A_1, \ldots, A_n\} & (2)\\
E;\ \Gamma,\ x : A_i \vdash_{\beta.1}\ Q_2 : (U_i;\ _)\ \ i = 1 \ldots n & (3)\\
U \equiv U_1 \mid \ldots \mid U_n & (4)\\
\forall f \in [\![T_1]\!]_E.\ \exists \rho \in \mathscr{R}(E, \Gamma).\ f \sqsubseteq [\![Q_1]\!]_\rho & (5)\\
\forall f \in [\![U_i]\!]_E.\ \exists \rho \in \mathscr{R}(E, (\Gamma, x : A_i)).\ f \sqsubseteq [\![Q_2]\!]_\rho\ \ i = 1 \ldots n & (6)
\end{array}$$

We want to prove

$$\forall f \in [\![U]\!]_E.\ \exists \rho \in \mathscr{R}(E, \Gamma).\ f \sqsubseteq [\![\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2]\!]_\rho$$

For any $f \in [\![U]\!]_E$, by (4) we have that $f \in [\![U_i]\!]_E$ for some $i = 1 \ldots n$. Moreover, by (6):

$$(\exists \rho^2 \in \mathscr{R}(E, (\Gamma, x : A_i)).\ f \sqsubseteq [\![Q_2]\!]_{\rho^2})\ \ (7)$$

Since $\rho^2 \in \mathscr{R}(E, (\Gamma, x : A_i))$, we have

$$\rho^2 = \overline{\rho}^2, x \mapsto f'\ \ (8)$$

with $f' \in [\![A_i]\!]_E$ and $\overline{\rho}^2 \in \mathscr{R}(E, \Gamma)$.
Now, since $f' \in [\![A_i]\!]_E\ \Rightarrow\ f' \in [\![T]\!]_E$ (Lemma 5.3), and by (5) we have that:

$$\exists \rho^1 \in \mathscr{R}(E, \Gamma).\ \ f' \sqsubseteq [\![Q_1]\!]_{\rho^1}\ \ (9)$$

Hence, (7) and (8) imply that

$$f \sqsubseteq [\![Q_2]\!]_{\rho^2} = [\![Q_2]\!]_{\overline{\rho}^2, x \to f'}\ \ (10)$$

while (9) and (10) and Lemma 5.7 imply that

$$f \sqsubseteq [\![Q_2]\!]_{\overline{\rho}^2, x \to [\![Q_1]\!]_{\rho^1}}$$

Now, by Lemma 5.15 there exists $\rho \in \mathscr{R}(E,\Gamma)$ such that $\rho^1 \sqsubseteq \rho$ and $\overline{\rho}^2 \sqsubseteq \rho$, hence, by Lemma 5.7, we have:

$$f \sqsubseteq [\![Q_2]\!]_{\overline{\rho}^2, x \to [\![Q_1]\!]_{\rho^1}} \sqsubseteq [\![Q_2]\!]_{\overline{\rho}^2, x \to [\![Q_1]\!]_{\rho}} \sqsubseteq [\![Q_2]\!]_{\rho, x \to [\![Q_1]\!]_{\rho}}$$

By $[\![\texttt{let } x ::= Q_1 \texttt{ return } Q_2]\!]_\rho = [\![Q_2]\!]_{\rho, x \to [\![Q_1]\!]_\rho}$ the case is proved.

(TypeFor) We have $E;\ \Gamma \vdash_\beta \ \texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2 : (T_2;\ \_)$ and the following hypothesis:

$$E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \_) \tag{1}$$
$$E;\ \Gamma \vdash_{\beta.1}\ \overline{x} \texttt{ in } T_1 \to Q_2 : (T_2;\ \_) \tag{2}$$
$$\forall f \in [\![T_1]\!]_E . \exists \rho \in \mathscr{R}(E,\Gamma).\ f \sqsubseteq [\![Q_1]\!]_\rho \tag{3}$$
$$\forall f \in [\![T_2]\!]_E .\ \exists \rho \in \mathscr{R}(E,\Gamma).\ \exists f' \in [\![T_1]\!]_E .\ f \sqsubseteq \textstyle\prod_{t \in trees(f')} [\![Q_2]\!]_{\rho, \overline{x} \to t} \tag{4}$$

We want to prove that

$$\forall f \in [\![T_2]\!]_E .\ \exists \rho \in \mathscr{R}(E,\Gamma).\ f \sqsubseteq [\![\texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2]\!]_\rho$$

For any $f \in [\![T_2]\!]_E$, by (4) we have

$$\exists \rho^2 \in \mathscr{R}(E,\Gamma).\ \exists f' \in [\![T_1]\!]_E .\ f \sqsubseteq \textstyle\prod_{t \in trees(f')} [\![Q_2]\!]_{\rho^2, \overline{x} \to t} \tag{5}$$

Since $f' \in [\![T_1]\!]_E$, by (3) we have:

$$(\exists \rho^1 \in \mathscr{R}(E,\Gamma). f' \sqsubseteq [\![Q_1]\!]_{\rho^1}) \tag{6}$$

From (5) and (6) and Corollary 5.8 it follows

$$f \sqsubseteq \prod_{t \in trees(f')} [\![Q_2]\!]_{\rho^2, \overline{x} \to t} \sqsubseteq \prod_{t \in trees([\![Q_1]\!]_{\rho^1})} [\![Q_2]\!]_{\rho^2, \overline{x} \to t}$$

As in the previous case, by Lemma 5.15 there exists $\rho \in \mathscr{R}(E,\Gamma)$ such that $\rho^1 \sqsubseteq \rho$, $\rho^2 \sqsubseteq \rho$. Therefore, by Lemma 5.7 and Corollary 5.8, we have:

$$\begin{aligned} f \sqsubseteq \ & \textstyle\prod_{t \in trees([\![Q_1]\!]_{\rho^1})} [\![Q_2]\!]_{\rho^2, \overline{x} \to t} \sqsubseteq \\ & \textstyle\prod_{t \in trees([\![Q_1]\!]_{\rho})} [\![Q_2]\!]_{\rho^2, \overline{x} \to t} \sqsubseteq \\ & \textstyle\prod_{t \in trees([\![Q_1]\!]_{\rho})} [\![Q_2]\!]_{\rho, \overline{x} \to t} \end{aligned}$$

By $[\![\texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2]\!]_\rho = \prod_{t \in trees([\![Q_1]\!]_\rho)} [\![Q_2]\!]_{\rho, \overline{x} \to t}$ the case is proved.

(TypeInStar) We have $E;\ \Gamma \vdash_\beta \ \overline{x} \texttt{ in } T* \to Q : (U*;\ \_)$ and the following hypothesis:

$$E;\ \Gamma \vdash_\beta \ \overline{x} \texttt{ in } T \to Q : (U;\ \_)$$

We want to prove that:

$$(\forall f \in [\![U*]\!]_E .\ \exists \rho \in \mathscr{R}(E,\Gamma).\ \exists f' \in [\![T*]\!]_E .\ f \sqsubseteq \prod_{t \in trees(f')} [\![Q]\!]_{\rho, \overline{x} \to t})$$

Consider $f \in [\![U*]\!]_E$; this entails that $f = f_1, \ldots, f_n$ with $f_i \in [\![U]\!]_E$, for $i = 1 \ldots n$. For each f_i, by induction on $E;\ \Gamma \vdash_\beta \ \overline{x} \texttt{ in } T \to Q : (U;\ \_)$, we have

$$\exists \rho^i \in \mathscr{R}(E,\Gamma).\ \exists f_i' \in [\![T]\!]_E .\ f_i \sqsubseteq \prod_{t \in trees(f_i')} [\![Q]\!]_{\rho^i, \overline{x} \to t}$$

By Lemma 5.15, there exists $\rho \in \mathscr{R}(E,\Gamma)$ such that $\rho^i \sqsubseteq \rho$, for $i = 1 \ldots n$. Hence, by Lemma 5.7:

$$f_i \sqsubseteq \prod_{t \in trees(f_i')} [\![Q]\!]_{\rho^i, \overline{x} \to t} \sqsubseteq \prod_{t \in trees(f_i')} [\![Q]\!]_{\rho, \overline{x} \to t}$$

Therefore we have:

$$f = f_1, \ldots, f_n \sqsubseteq \prod_{t \in trees(f_1')} [\![Q]\!]_{\rho, \overline{x} \to t}, \ldots, \prod_{t \in trees(f_n')} [\![Q]\!]_{\rho, \overline{x} \to t}$$

and the case is proved by observing that $f_1', \ldots, f_n' \in [\![T*]\!]_E$ and that

$$\prod_{t \in trees(f_1')} [\![Q]\!]_{\rho, \overline{x} \to t}, \ldots, \prod_{t \in trees(f_n')} [\![Q]\!]_{\rho, \overline{x} \to t} = \prod_{t \in trees(f_1', \ldots, f_n')} [\![Q]\!]_{\rho, \overline{x} \to t}$$

(TypeChild) It follows by Lemma 4.7.

(TypeDos) We have $J \equiv E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{dos} :: NodeTest : (U';\ \_)$ and the following hypothesis:

$$\begin{array}{ll} WF(J) & (1) \\ \overline{x} : T \in \Gamma\ \wedge\ (T \equiv m[T'] \vee T \equiv B) & (2) \\ \{U_1, \ldots, U_n\} = SubTrees_E(T) & (3) \\ U \equiv (U_1 \mid \ldots \mid U_n)* & (4) \\ E \vdash\ U :: NodeTest \Rightarrow U' & (5) \end{array}$$

We prove that $\forall f \in [\![U']\!]_E$ there exists ρ such that

$$f \sqsubseteq [\![\overline{x}\ \texttt{dos} :: NodeTest]\!]_\rho$$

Since $\overline{x} : T \in \Gamma$ and Γ is strongly-$*$-guarded (Lemma 5.17) we have $Split_E(T) = \{T\}$. Consider $f \in [\![U']\!]_E$; since $E \vdash\ U :: NodeTest \Rightarrow U'$, by Lemma 4.7 we have

$$\exists f' \in [\![U]\!]_E.\ f' :: NodeTest = f$$

For such f', since $Split_E(T) = \{T\}$, by Lemma 5.18(3) we have that there exists $f'' \in [\![T]\!]_E$ such that $f' \sqsubseteq dos(f'')$. Now we apply filtering and Lemma 5.6 to obtain

$$f = f' :: NodeTest \sqsubseteq dos(f'') :: NodeTest$$

hence it remains to observe that $f'' \in [\![T]\!]_E$ and, since Γ is not empty, there exists a $\rho \in \mathscr{R}(E,\Gamma)$ such that $\rho(\overline{x}) = f''$ and that $[\![\overline{x}\ \texttt{dos} :: NodeTest]\!]_\rho = dos(f'') :: NodeTest$, which gives

$$f \sqsubseteq [\![\overline{x}\ \texttt{dos} :: NodeTest]\!]_\rho.$$

□

Theorem 5.22 (*Lower Bound for the Type-Splitting System*) For each Q, $*$-guarded E, and Γ well-formed in E:

$$E;\ \Gamma \Vdash_\beta\ Q : (U;\ \_)\ \Rightarrow\ \forall f \in [\![U]\!]_E.\ \exists \rho \in \mathscr{R}(E,\Gamma).\ f \sqsubseteq [\![Q]\!]_\rho$$

Proof
By hypothesis we have $E;\ \Gamma \Vdash_\beta\ Q : (U;\ \_)$, that is

$$\begin{array}{ll} (1) & \mathit{SplitVEnv}(\Gamma, E) = \{\Gamma_1, \ldots, \Gamma_n\} \\ (2) & E;\ \Gamma_i \vdash_\beta\ Q : (U_i;\ \_) \quad i = 1 \ldots n \\ (3) & U \equiv U_1 \mid \ldots \mid U_n \end{array}$$

Therefore, for each $f \in [\![U]\!]_E$, there exists U_i and Γ_i strongly-$*$-guarded such that $f \in [\![U_i]\!]_E$ and $E;\ \Gamma_i \vdash_\beta\ Q : (U_i;\ \_)$. Hence, by Lemma 5.21 we have

$$\exists \rho \in \mathscr{R}(E, \Gamma_i).\ f \sqsubseteq [\![Q]\!]_\rho$$

Now, the thesis follows from $\mathscr{R}(E, \Gamma_i) \subseteq \mathscr{R}(E, \Gamma)$ (Lemma 5.14). □

Corollary 5.23 (*( )-precision*) In the type splitting system, for each Q, $*$-guarded E, and Γ strongly-$*$-guarded and well-formed in E, if $E;\ \Gamma \vdash_\beta\ Q : (U;\ \_)$ then:

$$[\![U]\!]_E = \{()\} \ \Leftrightarrow\ \forall \rho \in \mathscr{R}(E, \Gamma).\ [\![Q]\!]_\rho = ()$$

Proof
$\Rightarrow$ follows from Lemma 5.19. To prove $\Leftarrow$ we observe that by $E;\ \Gamma \vdash_\beta\ Q : (U;\ \_)$ and Lemma 5.21

$$\forall f \in [\![U]\!]_E.\ \exists \rho \in \mathscr{R}(E, \Gamma).\ f \sqsubseteq [\![Q]\!]_\rho$$

That is, by the hypothesis $\forall \rho \in \mathscr{R}(E, \Gamma).\ [\![Q]\!]_\rho = ()$:

$$\forall f \in [\![U]\!]_E.\ f \sqsubseteq ()$$

and this means $[\![U]\!]_E = \{()\}$, since $f \sqsubseteq ()$ if and only if $f = ()$. □

Lemma 5.24 In the type-splitting system, for each query Q, $*$-guarded E, Γ strongly-$*$-guarded and well-formed in E:

$$E;\ \Gamma \vdash_\beta\ Q : (\_;\ \mathscr{S}) \ \Rightarrow\ (\beta.\alpha \in \mathscr{S} \ \Rightarrow\ Q \textit{ has an error at } \alpha \textit{ w.r.t. } \mathscr{R}(E, \Gamma))$$

Proof
We prove the following statement:

- $E;\ \Gamma \vdash_\beta\ Q : (U;\ \mathscr{S}) \ \Rightarrow$
  $\gamma \in \mathscr{S} \ \Rightarrow\ (\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q) \wedge Q \textit{ has an error at } \alpha)$
- $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{in}\ T \to Q : (U;\ \mathscr{S}) \Rightarrow$
  $\gamma \in \mathscr{S} \ \Rightarrow\ (\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q) \wedge$
  $(\forall f \in [\![T]\!]_E.\ \texttt{for}\ \overline{x}\ \texttt{in}\ \overline{f}\ \texttt{return}\ Q \textit{ has an error at } 1.\alpha))$

We proceed by induction on the proof tree and by case distinction on the last rule applied. The proof differs from Theorem 4.15 only for cases (TypeLetSplitting) and (TypeInElSplitting), which we prove below.

(TypeLetSplitting) We have

$$E;\ \Gamma \vdash_\beta\ \texttt{let}\ x := Q_1\ \texttt{return}\ Q_2 : (U;\ \mathscr{S} \cup \bigcap_{i=1\ldots n} \mathscr{S}_i)$$

and

$$E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \mathscr{S}) \quad (1)$$
$$Split_E(T_1) = \{A_1, \ldots, A_n\} \quad (2)$$
$$E;\ \Gamma,\ x : A_i \vdash_{\beta.1}\ Q_2 : (U_i;\ \mathscr{S}_i)\ \ i = 1 \ldots n \quad (3)$$
$$U \equiv U_1 \mid \ldots \mid U_n \quad (4)$$
With respect to E and Γ: (5)
$\gamma \in \mathscr{S} \Rightarrow (\gamma \equiv \beta.0.\alpha \wedge \alpha \in CriticalLocs(Q_1) \wedge Q_1$ has an error at $\alpha)$
For $i = 1 \ldots n$ with respect to E and $\Gamma, x : A_i$: (6)
$\gamma \in \mathscr{S}_i \Rightarrow (\gamma \equiv \beta.1.\alpha \wedge \alpha \in CriticalLocs(Q_2) \wedge Q_2$ has an error at $\alpha)$

We want to prove that $\forall\ \gamma$

$$\gamma \in \mathscr{S} \cup \textstyle\bigcap_{i=1\ldots n} \mathscr{S}_i \Rightarrow (\gamma \equiv \beta.\alpha \wedge \alpha \in CriticalLocs(\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2) \\ \wedge\ \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2\ \textit{has an error at}\ \ \alpha)$$

For any

$$\gamma \in \mathscr{S} \cup \bigcap_{i=1\ldots n} \mathscr{S}_i$$

$\gamma \equiv \beta.\alpha \wedge \alpha \in CriticalLocs(\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2)$ follows from (5) and (6). To prove that $\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2$ has an error at α, we distinguish two possible cases: (i) $\alpha \equiv 0.\alpha'$ and $\alpha' \in CriticalLocs(Q_1)$, and (ii) $\alpha \equiv 1.\alpha'$ and $\alpha' \in CriticalLocs(Q_2)$. Case (i) is easy. We prove case (ii). To this end we use hypothesis (6) and expand it as follows, for $i = 1 \ldots n$:

$$\forall \rho \in \mathscr{R}(E, \Gamma, x : A_i).\ \forall \rho' \in Ext(\rho,\ Q_2,\ \alpha').\ [\![(Q_2)_{|\alpha'}]\!]_{\rho'} = ()\ \ (7)$$

moreover, we have $\beta.1.\alpha' \in \mathscr{S}_i$.
We want to prove that $\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2$ has an error at $\alpha \equiv 1.\alpha'$:

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ \forall \rho' \in Ext((\rho, x \mapsto [\![Q_1]\!]_\rho),\ Q_2,\ \alpha').\ [\![(Q_2)_{|\alpha'}]\!]_{\rho'} = ()$$

By (7) we have just to prove that,

$$\rho \in \mathscr{R}(E, \Gamma), \rho' \in Ext((\rho, x \mapsto [\![Q_1]\!]_\rho),\ Q_2,\ \alpha')\ \Rightarrow \\ \exists i.\ \exists \overline{\rho} \in \mathscr{R}(E, \Gamma, x : A_i).\ \rho' \in Ext(\overline{\rho},\ Q_2,\ \alpha')$$

This reduces to prove that,

$$\rho \in \mathscr{R}(E, \Gamma)\ \Rightarrow\ \exists i.\ \rho, x \mapsto [\![Q_1]\!]_\rho \in \mathscr{R}(E, \Gamma, x : A_i).$$

Such statement follows from Lemma 5.19:

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ [\![Q_1]\!]_\rho \in [\![T_1]\!]_E$$

and by Lemma 5.3

$$[\![T_1]\!]_E = \bigcup_{i=1\ldots n} [\![A_i]\!]_E$$

(TypeInElSplitting) We have $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{in}\ m[T] \to Q : (U;\ \bigcap_{i=1\ldots n} \mathscr{S}_i)$ and the following hypothesis

$$
\begin{array}{ll}
Split_E(m[T]) = \{A_1, \ldots, A_n\} & (1)\\
E;\ \Gamma,\ \overline{x} : A_i \vdash_\beta\ Q : (U_i;\ \mathscr{S}_i) & (2)\\
U \equiv U_1 \mid \ldots \mid U_n & (3)\\
\gamma \in \mathscr{S}_i\ \Rightarrow & (4)\\
\quad \gamma \equiv \beta.\alpha\ \wedge & \\
\quad \alpha \in CriticalLocs(Q)\ \wedge & \\
\quad \forall f \in [\![A_i]\!]_E.\ \texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q\ \ \textit{has an error at}\ \ 1.\alpha &
\end{array}
$$

We want to prove that

$$
\begin{array}{l}
\gamma \in \bigcap_{i=1\ldots n} \mathscr{S}_i\ \Rightarrow\quad (\gamma \equiv \beta.\alpha \wedge \alpha \in CriticalLocs(Q) \wedge\ (\forall f \in [\![m[T]]\!]_E.\\
\qquad\qquad \texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q\ \ \textit{has an error at}\ \ 1.\alpha))
\end{array}
$$

By Lemma 5.3,

$$f \in [\![m[T]]\!]_E\ \Rightarrow\ \exists i.\ f \in [\![A_i]\!]_E$$

Thus, for such i it holds that,

$$\gamma \in \bigcap_{j=1\ldots n} \mathscr{S}_j\ \Rightarrow\ \gamma \in \mathscr{S}_i$$

and the thesis follows by (4).

□

Theorem 5.25 (*Soundness of Error-Checking for the Type-Splitting System*) For each Q, $*$-guarded E, and Γ well-formed in E:

$$E;\ \Gamma \Vdash_\beta\ Q : (U;\ \mathscr{S})\ \wedge\ \beta.\alpha \in \mathscr{S}\ \Rightarrow Q \textit{ has an error at } \alpha \textit{ w.r.t. } \mathscr{R}(E, \Gamma)$$

Proof
By hypothesis we have

$$
\begin{array}{ll}
(1) & SplitVEnv(\Gamma, E) = \{\Gamma_1, \ldots, \Gamma_n\}\\
(2) & E;\ \Gamma_i \vdash_\beta\ Q : (U_i;\ \mathscr{S}_i) \quad i = 1 \ldots n\\
(3) & \mathscr{S} = \bigcap_{i=1\ldots n} \mathscr{S}_i
\end{array}
$$

and $\beta.\alpha \in \mathscr{S}$, hence $\beta.\alpha \in \mathscr{S}_i$ for $i = 1 \ldots n$. Thus, by Lemma 5.24 we have that, for $i = 1 \ldots n$

$$Q \textit{ has an error at } \alpha \textit{ w.r.t. } \mathscr{R}(E, \Gamma_i))$$

that is

$$\exists \alpha \in CriticalLocs(Q).\ \forall \rho \in \mathscr{R}(E, \Gamma_i).\ \forall \rho' \in Ext(\rho, Q, \beta).\ [\![(Q)_{|\alpha}]\!]_{\rho'} = ()$$

Therefore, the thesis follows by Lemma 5.14:

$$\bigcup_{\Gamma' \in SplitVEnv(\Gamma, E)} \mathscr{R}(E, \Gamma') = \mathscr{R}(E, \Gamma)$$

□

Lemma 5.26 In the type-splitting system, for each Q, $*$-guarded E, and Γ strongly-$*$-guarded and well-formed in E:

$$E;\ \Gamma \vdash_\beta\ Q : (\_;\ \mathscr{S})\ \ \Rightarrow\ \ (Q \textit{ has an error at } \alpha \textit{ w.r.t. } \mathscr{R}(E, \Gamma)\ \Rightarrow\ \beta.\alpha \in \mathscr{S})$$

Proof
We prove the statements:

- $E;\ \Gamma \vdash_\beta\ Q : (U;\ \mathscr{S})\ \Rightarrow$

$$(\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q) \wedge Q \textit{ has an error at } \alpha)\ \Rightarrow\ \gamma \in \mathscr{S}$$

- $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{in}\ T \to Q : (U;\ \mathscr{S}) \Rightarrow$

$$(\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q) \wedge$$
$$(\forall f \in [\![T]\!]_E.\ \texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q \textit{ has an error at } 1.\alpha))\ \Rightarrow\ \gamma \in \mathscr{S}$$

We proceed by induction on the proof tree and by cases on the last rule applied. We prove only some of the main cases (more cases can be found in the Appendix).

(TypeForest) We have $E;\ \Gamma \vdash_\beta\ Q_1, Q_2 : (T_1, T_2;\ \mathscr{S}_1 \cup \mathscr{S}_2)$ and the following hypothesis

$$E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \mathscr{S}_1) \quad (1)$$
$$E;\ \Gamma \vdash_{\beta.1}\ Q_2 : (T_2;\ \mathscr{S}_2) \quad (2)$$
$$(\gamma \equiv \beta.0.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_1) \wedge\ Q_1 \textit{ has an error at } \alpha)\ \Rightarrow\ \gamma \in \mathscr{S}_1 \quad (3)$$
$$(\gamma \equiv \beta.1.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_2) \wedge Q_2 \textit{ has an error at } \alpha)\ \Rightarrow\ \gamma \in \mathscr{S}_2 \quad (4)$$

We want to prove that

$$(\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(Q_1, Q_2) \wedge Q_1, Q_2 \textit{ has an error at } \alpha) \quad (5)$$

implies

$$\gamma \in \mathscr{S}_1 \cup \mathscr{S}_2$$

We proceed by contradiction. Suppose that

$$(*)\ \gamma \equiv \beta.\alpha \notin \mathscr{S}_1 \cup \mathscr{S}_2$$

By $\alpha \in \mathit{CriticalLocs}(Q_1, Q_2)$, we have two possible cases

$$(a)\quad \alpha \equiv 0.\alpha'\ \wedge\ \alpha' \in \mathit{CriticalLocs}(Q_1)$$
$$(b)\quad \alpha \equiv 1.\alpha'\ \wedge\ \alpha' \in \mathit{CriticalLocs}(Q_2)$$

We only consider case (a), the other one is similar. By (*) we have

$$\beta.0.\alpha' \notin \mathscr{S}_1$$

and this by $\gamma \equiv \beta.0.\alpha' \wedge \alpha' \in \mathit{CriticalLocs}(Q_1)$ and the inductive hypothesis (3), entails

$$(**)\ Q_1 \textit{ has no error at } \alpha'$$

This entails that

$$Q_1, Q_2 \textit{ has no error at } \alpha$$

by contradicting (5). Indeed, (**) means that $\exists \rho \in \mathscr{R}(E, \Gamma)$ and $\exists \rho' \in \mathit{Ext}(\rho,\ Q_1,\ \alpha')$ such that

$$[\![(Q_1)_{|\alpha'}]\!]_{\rho'} \neq ()$$

and since,

$$\mathit{Ext}(\rho,\ Q_1,\ \alpha') = \mathit{Ext}(\rho,\ (Q_1, Q_2),\ 0.\alpha')$$
$$[\![(Q_1)_{|\alpha'}]\!]_{\rho'} = [\![(Q_1, Q_2)_{|0.\alpha'}]\!]_{\rho'}$$

we have that

$$Q_1, Q_2 \textit{ has no error at } 0.\alpha'.$$

(TypeLetSplitting) We have $E;\ \Gamma \vdash_\beta \texttt{let}\ x := Q_1\ \texttt{return}\ Q_2 : (U;\ \mathscr{S} \cup \bigcap_{i=1\ldots n} \mathscr{S}_i)$ and

$$E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \mathscr{S}) \quad (1)$$
$$Split_E(T_1) = \{A_1, \ldots, A_n\} \quad (2)$$
$$E;\ \Gamma,\ x : A_i \vdash_{\beta.1}\ Q_2 : (U_i;\ \mathscr{S}_i)\ \ i = 1 \ldots n \quad (3)$$
$$U \equiv U_1 \mid \ldots \mid U_n \quad (4)$$
$$\text{With respect to } E \text{ and } \Gamma: \quad (5)$$
$$(\alpha \in CriticalLocs(Q_1) \wedge Q_1 \text{ has an error at } \alpha) \ \Rightarrow\ \beta.0.\alpha \in \mathscr{S}$$
$$\text{For } i = 1 \ldots n \text{ with respect to } E \text{ and } \Gamma, x : A_i: \quad (6)$$
$$(\alpha \in CriticalLocs(Q_2) \wedge Q_2 \text{ has an error at } \alpha) \ \Rightarrow\ \ \beta.1.\alpha \in \mathscr{S}_i$$

We want to prove that $\forall\ \gamma$

$$(\gamma \equiv \beta.\alpha' \wedge \alpha' \in CriticalLocs(\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2) \\ \wedge\ \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2 \textit{ has an error at } \alpha') \quad \Rightarrow\ \ \gamma \in (\mathscr{S} \cup \textstyle\bigcap_{i=1\ldots n} \mathscr{S}_i)$$

We proceed by contradiction. Assume that

$$\gamma \equiv \beta.\alpha' \wedge \alpha' \in CriticalLocs(\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2) \\ \wedge\ \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2\ \textit{ has an error at } \alpha'$$

and that:

$$\gamma \equiv \beta.\alpha' \notin (\mathscr{S} \cup \bigcap_{i=1\ldots n} \mathscr{S}_i) \quad (7)$$

Since $\alpha' \in CriticalLocs(\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2)$, we can distinguish the following two cases

$$(a)\quad \alpha' = 0.\alpha''\ \wedge\ \alpha'' \in CriticalLocs(Q_1)$$
$$(b)\quad \alpha' = 1.\alpha''\ \wedge\ \alpha'' \in CriticalLocs(Q_2)$$

In what follows, we consider each case separately and prove that in each one we have a contradiction.

(a) We have $\alpha' = 0.\alpha''\ \wedge \alpha'' \in CriticalLocs(Q_1)$. Moreover, we have assumed that $\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2$ has an error at location $0.\alpha''$. This means that $\forall \rho \in \mathscr{R}(E, \Gamma). \forall \rho' \in Ext(\rho, \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2, 0.\alpha'')$.

$$[\![(\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2)_{|0.\alpha''}]\!]_{\rho'} = ()$$

Since

$$Ext(\rho, \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2, 0.\alpha'') = Ext(\rho, Q_1, \alpha'')$$

and

$$(\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2)_{|0.\alpha''} = (Q_1)_{|\alpha''}$$

we have that Q_1 has an error at α''. This, by the inductive hypothesis (5) entails that

$$\beta.0.\alpha'' \in \mathscr{S}$$

which in turn entails

$$\beta.0.\alpha'' \in (\mathscr{S} \cup \bigcap_{i=1\ldots n} \mathscr{S}_i)$$

which contradicts the assumption (7).

(b) We have $\alpha' = 1.\alpha'' \ \wedge \ \alpha'' \in \mathit{CriticalLocs}(Q_2)$. Moreover, (7) entails

$$1.\alpha'' \notin \bigcap_{i=1\ldots n} \mathscr{S}_i$$

This means that there exists $j \in \{1, \ldots, n\}$ such that

$$1.\alpha'' \notin \mathscr{S}_j$$

With respect to this j, by the inductive hypothesis (6) and with respect to environments E and $\Gamma, x : A_j$, it follows that

$$Q_2 \ \textit{has no error at} \ \alpha''$$

This is equivalent to saying that there exists $\rho \in \mathscr{R}(E, (\Gamma, x : A_j))$ and $\rho' \in \mathit{Ext}(\rho, Q_2, \alpha'')$ such that

$$[\![(Q_2)_{|\alpha''}]\!]_{\rho'} \neq ()$$

Since $\rho \in \mathscr{R}(E, (\Gamma, x : A_j))$ and $[\![A_j]\!]_E \subseteq [\![T_1]\!]_E$(Lemma 5.3) we have

$$\rho = \overline{\rho}, x \mapsto f \ \wedge \ f \in [\![T_1]\!]_E$$

By hypothesis (1) and lower bound Lemma 5.21, we have

$$\exists \overline{\rho}' \in \mathscr{R}(E, \Gamma).\ f \sqsubseteq [\![Q_1]\!]_{\overline{\rho}'}$$

Since Γ is strongly-*-guarded (Lemma 5.17), by Lemma 5.15 there exists $\overline{\overline{\rho}} \in \mathscr{R}(E, \Gamma)$ such that $\overline{\rho} \sqsubseteq \overline{\overline{\rho}}$ and $\overline{\rho}' \sqsubseteq \overline{\overline{\rho}}$.
Now, if we consider the substitution

$$\rho_1 = \overline{\overline{\rho}}, x \mapsto [\![Q_1]\!]_{\overline{\overline{\rho}}}$$

we have

$$\rho \ \sqsubseteq \ \rho_1$$

since $[\![Q_1]\!]_{\overline{\rho}'} \sqsubseteq [\![Q_1]\!]_{\overline{\overline{\rho}}}$, which follows by $\overline{\rho}' \sqsubseteq \overline{\overline{\rho}}$ and Lemma 5.7. Since $\rho' \in \mathit{Ext}(\rho, Q_2, \alpha'')$ by assumption, by Lemma 5.9 there exists $\rho'' \in \mathit{Ext}(\rho_1, Q_2, \alpha'')$ such that $\rho' \sqsubseteq \rho''$. Therefore by Lemma 5.7, we have

$$[\![(Q_2)_{|\alpha''}]\!]_{(\rho')} \sqsubseteq [\![(Q_2)_{|\alpha''}]\!]_{(\rho'')}$$

Hence, $[\![(Q_2)_{|\alpha''}]\!]_{\rho'} \neq ()$, and Lemma 5.5 imply that

$$[\![(Q_2)_{|\alpha''}]\!]_{\rho''} \neq ()$$

Now we observe that $\rho'' \in \mathit{Ext}(\rho_1, Q_2, \alpha'')$ and $\rho_1 = \overline{\overline{\rho}}, x \mapsto [\![Q_1]\!]_{\overline{\overline{\rho}}}$ entail

$$\rho'' \in \mathit{Ext}(\overline{\overline{\rho}}, \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2, 1.\alpha'')$$

hence

$$\mathit{Ext}(\rho_1, Q_2, \alpha'') = \mathit{Ext}(\overline{\overline{\rho}}, \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2, 1.\alpha'') \quad (8)$$

Hence, the hypothesis that

$$\text{for } \alpha' = 1.\alpha'', \ \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2 \ \textit{has an error at} \ \alpha'$$

is contradicted by (8) and by

$$[\![(Q_2)_{|\alpha''}]\!]_{\rho''} = [\![(\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2)_{|1.\alpha''}]\!]_{\rho''} \neq ()$$

with $\rho'' \in \mathit{Ext}(\overline{\overline{\rho}}, \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2, 1.\alpha'')$.

(TypeFor) We have $E;\ \Gamma \vdash_\beta \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2 : (T_2;\ \mathscr{S}_1 \cup \mathscr{S}_2 \cup \mathscr{S})$ and the following hypothesis:

$$E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \mathscr{S}_1) \tag{1}$$
$$E;\ \Gamma \vdash_{\beta.1}\ \overline{x}\ \texttt{in}\ T_1 \to Q_2 : (T_2;\ \mathscr{S}_2) \tag{2}$$
$$\mathscr{S} = \text{ if } T_1 \sim_E () \text{ then } \{\beta.0\} \text{ else } \emptyset \tag{3}$$
$$(\gamma \equiv \beta.0.\alpha\ \wedge \alpha \in \mathit{CriticalLocs}(Q_1) \wedge Q_1 \textit{ has an error at } \alpha) \Rightarrow \gamma \in \mathscr{S}_1 \tag{4}$$
$$(\gamma \equiv \beta.1.\alpha\ \wedge\ \alpha \in \mathit{CriticalLocs}(Q_2) \wedge \tag{5}$$
$$\wedge\ (\forall f \in [\![T_1]\!]_E.\texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q_2\ \textit{ has an error at }\ 1.\alpha)) \Rightarrow \gamma \in \mathscr{S}_2$$

We want to prove that $\forall\ \gamma$

$$(\gamma \equiv \beta.\alpha' \wedge \alpha' \in \mathit{CriticalLocs}(\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2) \wedge$$
$$\wedge\ \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2 \textit{ has an error at } \alpha' \quad \Rightarrow \gamma \in (\mathscr{S} \cup \mathscr{S}_1 \cup \mathscr{S}_2)$$

We proceed by contradiction. Suppose that for a γ it holds:

$$\gamma \equiv \beta.\alpha' \wedge \gamma'' \in \mathit{CriticalLocs}(\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2)$$
$$\wedge\ \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2\ \textit{ has an error at }\ \alpha'$$

and that,

$$\gamma \equiv \beta.\alpha' \notin \mathscr{S} \cup \mathscr{S}_1 \cup \mathscr{S}_2 \tag{6}$$

Since $\alpha' \in \mathit{CriticalLocs}(\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2)$, we can distinguish three cases

$$(a)\quad \alpha' = 0$$
$$(b)\quad \alpha' = 0.\alpha''\ \wedge\ \alpha'' \in \mathit{CriticalLocs}(Q_1)$$
$$(c)\quad \alpha' = 1.\alpha''\ \wedge\ \alpha'' \in \mathit{CriticalLocs}(Q_2)$$

We now consider each case separately and prove that in each one we have a contradiction.

(a) In this case, we have that $\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2$ has an error at location 0. This means that $\forall \rho \in \mathscr{R}(E, \Gamma)$

$$\forall \rho' \in \mathit{Ext}(\rho, \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2, 0).$$
$$[\![(\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2)_{|0}]\!]_{\rho'} = ()$$

Since

$$\mathit{Ext}(\rho, \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2, 0) = \{\rho\}$$

and

$$(\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2)_{|0} = Q_1$$

by Corollary 5.23 we have that $\forall \rho \in \mathscr{R}(E, \Gamma)$

$$[\![Q_1]\!]_\rho = ()$$

and this, by lower bound Lemma 5.21, entails $[\![T_1]\!]_E = \{()\}$. This, by Lemma 4.5, entails

$$\mathscr{S} = \text{ if } T_1 \sim_E () \text{ then } \{\beta.0\} \text{ else } \emptyset = \{\beta.0\}$$

which in turn entails

$$\beta.0 \in \mathscr{S}_1 \cup \mathscr{S}_2\ \cup \mathscr{S}$$

which contradicts the assumption (6).

(b) We have $\alpha' = 0.\alpha'' \ \wedge \alpha'' \in \mathit{CriticalLocs}(Q_1)$. Moreover, we have assumed that $\texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2$ has an error at location $0.\alpha''$. This means that $\forall \rho \in \mathscr{R}(E, \Gamma)$

$$\forall \rho' \in \mathit{Ext}(\rho, \texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2, 0.\alpha'').$$
$$[\![(\texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2)_{|0.\alpha''}]\!]_{\rho'} = ()$$

Since

$$\mathit{Ext}(\rho, \texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2, 0.\alpha'') = \mathit{Ext}(\rho, Q_1, \alpha'')$$

and

$$(\texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2)_{|0.\alpha''} = (Q_1)_{|\alpha''}$$

we have that Q_1 has an error at α''. This, by the inductive hypothesis (4) entails that

$$\beta.0.\alpha'' \in \mathscr{S}_1$$

which in turn entails

$$\beta.0.\alpha'' \in \mathscr{S}_1 \cup \mathscr{S}_2 \ \cup \mathscr{S}$$

which contradicts the assumption (6).

(c) We have $\alpha' = 1.\alpha'' \ \wedge \ \alpha'' \in \mathit{CriticalLocs}(Q_2)$. Moreover, (*) entails

$$1.\alpha'' \notin \mathscr{S}_2$$

From this, by the inductive hypothesis (5), it follows

$$(\exists f \in [\![T_1]\!]_E.\ \texttt{for } \overline{x} \texttt{ in } f \texttt{ return } Q_2 \ \ \textit{has no error at} \ \ \alpha)$$

Hence there exists an $f \in [\![T_1]\!]_E$ such that

$$\exists \rho \in \mathscr{R}(E, \Gamma).\ \exists \rho' \in \mathit{Ext}(\rho, \texttt{for } \overline{x} \texttt{ in } f \texttt{ return } Q_2, 1.\alpha'').$$
$$[\![(\texttt{for } \overline{x} \texttt{ in } f \texttt{ return } Q_2)_{|1.\alpha''}]\!]_{\rho'} \neq ()$$

By $f \in [\![T_1]\!]_E$, hypothesis (1), and lower bound Lemma 5.21, we obtain

$$\exists \rho'' \in \mathscr{R}(E, \Gamma).\ f \sqsubseteq [\![Q_1]\!]_{\rho''}$$

By Lemma 5.15 there exists $\overline{\rho} \in \mathscr{R}(E, \Gamma)$ such that $\rho \sqsubseteq \overline{\rho}, \rho'' \sqsubseteq \overline{\rho}$, hence, by Lemma 5.7, we have:

$$f \sqsubseteq [\![Q_1]\!]_{\rho''} \sqsubseteq [\![Q_1]\!]_{\overline{\rho}}$$

We consider the following two sets of substitutions obtained by extension as follows:

$$\begin{array}{lcl} \mathit{Ext}(\rho, \texttt{for } \overline{x} \texttt{ in } f \texttt{ return } Q_2, 1.\alpha'') & = & \bigcup_{t \in \mathit{trees}(f)} \mathit{Ext}((\rho, x \mapsto t), Q_2, \alpha'') \\ \mathit{Ext}(\overline{\rho}, \texttt{for } \overline{x} \texttt{ in } Q_1 \texttt{ return } Q_2, 1.\alpha'') & = & \bigcup_{t \in \mathit{trees}([\![Q_1]\!]_{\overline{\rho}})} \mathit{Ext}((\overline{\rho}, x \mapsto t), Q_2, \alpha'') \end{array}$$

Since $f \sqsubseteq [\![Q_1]\!]_{\overline{\rho}}$, we have that for each $t \in \mathit{trees}(f)$ there exists $t' \in \mathit{trees}([\![Q_1]\!]_{\overline{\rho}})$ such that

$$t \sqsubseteq t' \quad (7).$$

Now, we recall that for $\rho' \in \mathit{Ext}(\rho, \texttt{for } \overline{x} \texttt{ in } f \texttt{ return } Q_2, 1.\alpha'')$ we have

$$[\![(\texttt{for } \overline{x} \texttt{ in } f \texttt{ return } Q_2)_{|1.\alpha''}]\!]_{\rho'} \neq ()$$

that is equivalent to say that there exists $t_1 \in \mathit{trees}(f)$ such that

$$\rho' \in \mathit{Ext}((\rho, x \mapsto t_1), Q_2, \alpha'') \quad (8)$$

and

$$[\![(Q_2)_{|\alpha''}]\!]_{\rho'} \neq ()$$

Given $t_2 \in trees([\![Q_1]\!]_{\overline{\rho}})$ such that $t_1 \sqsubseteq t_2$, by $\rho \sqsubseteq \overline{\rho}$, (7), (8), and Lemma 5.9, there exists $\overline{\rho}' \in Ext((\overline{\rho}, x \mapsto t_2), Q_2, \alpha'')$ such that $\rho' \sqsubseteq \overline{\rho}'$. Therefore by Lemma 5.7,

$$[\![(Q_2)_{|\alpha''}]\!]_{\rho'} \sqsubseteq [\![(Q_2)_{|\alpha''}]\!]_{\overline{\rho}'}$$

From this inclusion, $[\![(Q_2)_{|\alpha''}]\!]_{\rho'} \neq ()$, and Lemma 5.5, it follows that

$$[\![(Q_2)_{|\alpha''}]\!]_{(\overline{\rho}')} \neq ()$$

and this contradicts the hypothesis stating that for $\alpha' = 1.\alpha''$ it holds

$$\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2 \quad \textit{has an error at} \quad \alpha'$$

since $t_2 \in trees([\![Q_1]\!]_{\rho})$ implies that

$$\overline{\rho}' \in Ext((\overline{\rho}, x \mapsto t_2), Q_2, \alpha'') \subseteq Ext(\overline{\rho}, \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2, 1.\alpha'') = \\ = \bigcup_{t \in trees([\![Q_1]\!]_{\rho})} Ext((\overline{\rho}, x \mapsto t_2), Q_2, \alpha'')$$

(TypeInConc) We have $E;\ \Gamma \vdash_{\beta}\ \overline{x}\ \texttt{in}\ T, U \to Q : (T, U;\ \mathscr{S}_1 \cap \mathscr{S}_2)$ and

$$E;\ \Gamma \vdash_{\beta}\ \overline{x}\ \texttt{in}\ T \to Q : (T;\ \mathscr{S}_1) \tag{1}$$
$$E;\ \Gamma \vdash_{\beta}\ \overline{x}\ \texttt{in}\ U \to Q : (U;\ \mathscr{S}_2) \tag{2}$$
$$(\gamma \equiv \beta.\alpha\ \wedge\ \alpha \in CriticalLocs(Q)\ \wedge \\ \wedge\ (\forall f \in [\![T]\!]_E.\ \texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q\ \ \textit{has an error at}\ \ 1.\alpha))\ \Rightarrow\ \gamma \in \mathscr{S}_1 \tag{3}$$
$$(\gamma \equiv \beta.\alpha\ \wedge\ \alpha \in CriticalLocs(Q)\ \wedge \\ \wedge\ (\forall f \in [\![U]\!]_E.\ \texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q\ \ \textit{has an error at}\ \ 1.\alpha))\ \Rightarrow\ \gamma \in \mathscr{S}_2 \tag{4}$$

We want to prove that

$$(\gamma \equiv \beta.\alpha\ \wedge\ \alpha \in CriticalLocs(Q)\ \wedge \\ \wedge\ (\forall f \in [\![T, U]\!]_E.\texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q\ \ \textit{has an error at}\ \ 1.\alpha))\ \ \Rightarrow\ \ \gamma \in \mathscr{S}_1 \cap \mathscr{S}_2$$

We proceed by contradiction. We assume that

$$(\gamma \equiv \beta.\alpha \wedge \alpha \in CriticalLocs(Q) \wedge\ (\forall f \in [\![T, U]\!]_E.\ \ (*) \\ \texttt{for}\ \overline{x}\ \texttt{in}\ f\ \texttt{return}\ Q\ \ \textit{has an error at}\ \ 1.\alpha))$$

and a contradiction that:

$$\gamma \equiv \beta.\alpha \notin \mathscr{S}_1 \cap \mathscr{S}_2$$

This last assumption means that $\beta.\alpha \notin \mathscr{S}_1\ \vee\ \beta.\alpha \notin \mathscr{S}_2$ and this by (3) and (4) implies that

$$(\exists f_1 \in [\![T]\!]_E.\ \texttt{for}\ \overline{x}\ \texttt{in}\ f_1\ \texttt{return}\ Q\ \ \textit{has no error at}\ \ 1.\alpha)\ \ \vee \\ (\exists f_2 \in [\![U]\!]_E.\ \texttt{for}\ \overline{x}\ \texttt{in}\ f_2\ \texttt{return}\ Q\ \ \textit{has no error at}\ \ 1.\alpha)$$

Suppose that the first statement is true. Consider any $f' \in [\![U]\!]_E$;[9] we have $f_1, f' \in [\![T, U]\!]_E$ and

$$\texttt{for}\ \overline{x}\ \texttt{in}\ f_1, f'\ \texttt{return}\ Q\ \ \textit{has no error at}\ \ 1.\alpha$$

[9] Such f' exists as our type system does not feature types U such that $[\![U]\!]_E = \emptyset$.

which contradicts (*). The other case is similar.

(TypeDos) We have $E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{dos} :: \mathit{NodeTest} : (U';\ \mathscr{S})$ and the following hypothesis:

$$
\begin{array}{ll}
(1) & \mathit{WF}(E;\ \Gamma \vdash_\beta\ \overline{x}\ \texttt{dos} :: \mathit{NodeTest} : (U';\ \mathscr{S})) \\
(2) & \overline{x} : T \in \Gamma\ \wedge\ (T \equiv m[T'] \vee T \equiv B) \\
(3) & \{U_1, \ldots, U_n\} = \mathit{SubTrees}_E(T) \\
(4) & U \equiv (U_1 \mid \ldots \mid U_n)* \\
(5) & E \vdash\ U :: \mathit{NodeTest} \Rightarrow U' \\
(6) & \mathscr{S} =\ \text{if } U' \sim_E () \text{ then } \{\beta\} \text{ else } \emptyset
\end{array}
$$

We want to prove that

$$
\begin{array}{l}
(\gamma \equiv \beta.\alpha \wedge \alpha \in \mathit{CriticalLocs}(\overline{x}\ \texttt{dos} :: \mathit{NodeTest}) \wedge \\
\quad (\overline{x}\ \texttt{dos} :: \mathit{NodeTest}\ \ \textit{has an error at}\ \ \alpha) \Rightarrow \gamma \in \mathscr{S}
\end{array}
$$

We first observe that it may be $\mathscr{S} = \{\beta\}$ or $\mathscr{S} = \emptyset$. Moreover, $\mathit{CriticalLocs}(\overline{x}\ \texttt{dos} :: \mathit{NodeTest}) = \{\epsilon\}$ and $\overline{x}\ \texttt{dos} :: \mathit{NodeTest}$ has an error at ϵ if and only if

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ \forall \rho' \in \mathit{Ext}(\epsilon, \overline{x}\ \texttt{dos} :: \mathit{NodeTest}, \rho).\ [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho'} = ()$$

Since $\mathit{Ext}(\epsilon, \overline{x}\ \texttt{dos} :: \mathit{NodeTest}, \rho) = \{\rho\}$, $\overline{x}\ \texttt{dos} :: \mathit{NodeTest}$ has an error at ϵ if and only if

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho} = ()$$

Hence, what we have to prove is

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho} = ()\ \Rightarrow\ \mathscr{S} = \{\beta\}$$

We proceed by contradiction and assume

$$\forall \rho \in \mathscr{R}(E, \Gamma).\ [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho} = ()\ \ (*)$$

and

$$\mathscr{S} = \emptyset$$

This last assumption means that $U' \sim_E () = \texttt{false}$. By Lemma 4.5, $[\![U']\!]_E \neq \{()\}$. Let f be a non empty forest in $[\![U']\!]_E$. By lower bound Lemma 5.21, we have

$$\exists \rho' \in \mathscr{R}(E, \Gamma).\ f \sqsubseteq [\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho'}$$

and this by Lemma 5.5 implies

$$[\![\overline{x}\ \texttt{dos} :: \mathit{NodeTest}]\!]_{\rho'} \neq ()$$

which contradicts (*).

□

Theorem 5.27 (*Completeness of Error-Checking for the Type-Splitting System*) For each Q, $*$-guarded E, and Γ well-formed in E:

$$E;\ \Gamma \Vdash_\beta\ Q : (U;\ \mathscr{S})\ \wedge Q\ \textit{has an error at}\ \alpha\ \textit{w.r.t.}\ \mathscr{R}(E, \Gamma)\ \Rightarrow \beta.\alpha \in \mathscr{S}$$

Proof
By hypothesis we have

$$\exists \alpha \in \mathit{CriticalLocs}(Q).\ \forall \rho \in \mathscr{R}(E,\Gamma).\ \forall \rho' \in \mathit{Ext}(\rho, Q, \alpha).\ [\![(Q)_{|\alpha}]\!]_{\rho'} = ()$$

and

(1) $\mathit{SplitVEnv}(\Gamma, E) = \{\Gamma_1, \ldots, \Gamma_n\}$
(2) $E;\ \Gamma_i \vdash_\beta\ Q : (U_i;\ \mathscr{S}_i) \quad i = 1 \ldots n$
(3) $\mathscr{S} = \bigcap_{i=1\ldots n} \mathscr{S}_i$

We want to prove that $\beta.\alpha \in \mathscr{S}$. To this aim, we prove that $\beta.\alpha \in \mathscr{S}_i$ for $i = 1 \ldots n$. This follows by observing that the hypothesis implies, for $i = 1 \ldots n$:

$$\forall \rho \in \mathscr{R}(E,\Gamma_i).\ \forall \rho' \in \mathit{Ext}(\rho, Q, \beta).\ [\![(Q)_{|\beta}]\!]_{\rho'} = ()$$

as $\mathscr{R}(E,\Gamma_i) \subseteq \mathscr{R}(E,\Gamma)$ (Lemma 5.14). This means that Q has an error at α with respect to $\mathscr{R}(E,\Gamma_i)$ for $i = 1 \ldots n$. Therefore, by Lemma 5.26 we have $\beta.\alpha \in \mathscr{S}_i$ for $i = 1 \ldots n$. □

Lemma 6.5 Assume $E;\ \Gamma \vdash_\beta\ Q : (T;\ \_)$, (E, Γ) is label-deterministic and

$$Q = \chi\ \mathit{Step}_1\ \mathit{Step}_2 \ldots \mathit{Step}_n$$

where Step_i is either $/l_i$ or $//l_i$. Then T is label-deterministic. Moreover,

$$\mathrm{UpperTrees}_E(T) \subseteq \{l_n[T']\}$$

for some T', where l_n is the label of Step_n.

Proof
By induction on n. □

Lemma 6.6 If E is $*$-guarded and T is well-defined and label-deterministic with respect to E, then each $A \in \mathit{Split}_E(T)$ is label-deterministic with respect to E.

Proof
Assume, toward a contradiction, that

$$A \rightarrow_e^E m[U]\ \wedge\ A \rightarrow_e^E m[U']\ \wedge\ U' \neq U$$

and then, by exploiting $A \in \mathit{Split}_E(T)$, conclude that T is not label-deterministic with respect to E, which contradicts the hypothesis. □

Lemma 6.7 If $E;\ \Gamma \vdash_\beta\ Q : (T;\ \_)$, (E, Γ) is label-deterministic and Q is left-path, then for each judgement of shape

$$E';\ \Gamma' \vdash_\beta\ Q' : (T'';\ \mathscr{S})$$

or

$$E';\ \Gamma' \vdash_\beta\ \overline{x}\ \texttt{in}\ T_1 \rightarrow Q' : (T'';\ \mathscr{S})$$

in the proof tree of $E;\ \Gamma \vdash_\beta\ Q : (T;\ \_)$, the pair (E', Γ') is label-deterministic and Q' is left-path. Moreover, in the second case, T_1 is label-deterministic.

Proof
It is sufficient to prove that the above properties are preserved by backward application of type rules. The main cases are (TypeLetSplitting), (TypeFor) and (TypeInElSplitting), which we prove below.

(TypeLetSplitting) We have $E;\ \Gamma \vdash_{\beta}\ \texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2 : (T;\ \_)$ which reduces to

$$\begin{array}{l} E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \_) \\ \mathit{Split}_E(T_1) = \{A_1, \ldots, A_n\} \\ E;\ \Gamma, x : A_i \vdash_{\beta.1}\ Q_2 : (U_i;\ \_) \\ T \equiv U_1 \mid \ldots \mid U_n \end{array}$$

with (E, Γ) label-deterministic. Queries Q_1 and Q_2 are left-path since the query $\texttt{let}\ x ::= Q_1\ \texttt{return}\ Q_2$ is. Moreover, we have

$$Q_1 \equiv \chi\ \mathit{Step}_1\ \mathit{Step}_2 \ldots \mathit{Step}_n \quad (*)$$

where Step_i is either $/l$ or $//l$.
Therefore, we only have to prove that $(E, (\Gamma, x : A_i))$ is label-deterministic, for each $i = 1 \ldots n$. Since (E, Γ) is label-deterministic, by (*) and by Lemma 6.5, we have that T_1 is label-deterministic. Then it suffices to apply Lemma 6.6 to prove that $(E, (\Gamma, x : A_i))$ is label-deterministic as well.

(TypeFor) We have $E;\ \Gamma \vdash_{\beta}\ \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2 : (T;\ \_)$ which reduces to

$$\begin{array}{l} E;\ \Gamma \vdash_{\beta.0}\ Q_1 : (T_1;\ \_)\ (*) \\ E;\ \Gamma \vdash_{\beta.1}\ \overline{x}\ \texttt{in}\ T_1 \rightarrow Q_2 : (T;\ \_) \end{array}$$

with (E, Γ) label-deterministic. Moreover, we have

$$Q_1 \equiv \chi\ \mathit{Step}_1\ \mathit{Step}_2 \ldots \mathit{Step}_n \quad (**)$$

where Step_i is either $/l$ or $//l$.
Queries Q_1 and Q_2 are left-path since $\texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2$ is. Finally, by this, (*), (**) and Lemma 6.5, we have that T_1 is label-deterministic with respect to E.

(TypeInElSplitting) We have $E;\ \Gamma \vdash_{\beta}\ \overline{x}\ \texttt{in}\ l[T_1] \rightarrow Q_2 : (T;\ \_)$ which reduces to

$$\begin{array}{l} \mathit{Split}_E(l[T_1]) = \{A_1, \ldots, A_n\} \\ E;\ \Gamma, x : A_i \vdash_{\beta.1}\ Q_2 : (U_i;\ \_) \\ T \equiv U_1 \mid \ldots \mid U_n \end{array}$$

Moreover, by hypothesis, we have that Q_2 is left-path and that $l[T_1]$ is label-deterministic with respect to E (*). Hence we only have to prove that $(E, (\Gamma, \overline{x} : A_i))$ is label-deterministic. This follows by the fact that $(E, (\Gamma))$ is label-deterministic, $l[T_1]$ is label-deterministic with respect to E, $A_i \in \mathit{Split}_E(l[T_1])$, and Lemma 6.6.

□

Lemma 6.8 (*Label-Deterministic Analysis*) If $E;\ \Gamma \vdash_{\beta}\ Q : (T;\ \_)$, $(\Gamma,\ E)$ is label-deterministic and Q is left-path, then for each judgement

$$E';\ \Gamma' \vdash_{\beta}\ \texttt{for}\ \overline{x}\ \texttt{in}\ Q_1\ \texttt{return}\ Q_2 : (T';\ \mathscr{S})$$

in the proof tree of $E;\ \Gamma \vdash_{\beta}\ Q : (T;\ \mathscr{S})$, we have

$$E';\ \Gamma' \vdash_{\beta}\ Q_1 : (T_1;\ \_)\ \wedge\ \mathrm{UpperTrees}_{E'}(T_1) \subseteq \{m[U]\}\ \text{ for some } m, U$$

Proof
By Lemma 6.7 we have that (E', Γ') is label-deterministic and that the query `for` $\overline{x}$ `in` Q_1 `return` Q_2 is left-path. Hence

$$Q_1 \equiv \chi\ Step_1\ Step_2 \ldots Step_n \quad (*)$$

Moreover, since $E;\ \Gamma \vdash_\beta\ Q : (T;\ \_)$ holds, we have that $E';\ \Gamma' \vdash_\beta\ Q_1 : (T_1;\ \mathscr{S})$ holds as well. It remains to prove that $\text{UpperTrees}_{E'}(T_1) \subseteq \{m[U]\}$. This follows by the fact that (E', Γ') is label-deterministic, by (*) and Lemma 6.5. □