Proof of type preservation

Vitor Fernandes

Theorem 1 (Classical substitution)**.** *If* $\Gamma, x : C \vdash \mathtt{P}$ *then* $\Gamma \vdash \mathtt{P}\{v/x\}$ *for any real number* v*.*

Proof. Follows routinely by induction over the type derivation system. □

Theorem 2 (Quantum substitution)**.** *If* $\Gamma, q : Q \vdash \mathtt{P}$ *then* $\Gamma, r : Q \vdash \mathtt{P}\{r/q\}$ *for every quantum variable* $r : Q$ *not in* Γ*.*

Proof. Follows routinely by induction over the type derivation system. □

Theorem 3 (Type preservation)**.** *If there exists a transition* $\langle\, \mathtt{P},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{Q},\, \sigma \,\rangle$ *with probability greater than zero and* $\Gamma \vdash \mathtt{P}$ *then* $\Delta \vdash \mathtt{Q}$ *for some typing context* Δ*.*

Proof. The proof follows by induction over the transition rules. Moreover, we strengthen the induction invariant in the following way: if there exists a transition $\langle\, \mathtt{P},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{Q},\, \sigma \,\rangle$ with probability greater than zero and $\Gamma \vdash \mathtt{P}$ then $\Delta \vdash \mathtt{Q}$ such that

$$\Delta^Q \subseteq \begin{cases} \Gamma^Q & \text{if } \alpha \neq \mathtt{c}?q \text{ and } \alpha \neq \mathtt{c}!q \\ \Gamma^Q, q : Q & \text{if } \alpha = \mathtt{c}?q \\ \Gamma^Q \setminus \{q : Q\} & \text{otherwise} \end{cases}$$

The proofs for invisible actions, classical output, quantum output, and super-operators are direct. The proof for classical input is a consequence of Theorem 1 and the proof for quantum input is a consequence of Theorem 2. For the other cases, we proceed in the following way.

1. Consider the case of measuring qubits. The transition derivation system tells that the process $\mathtt{M}[q; x].\mathtt{P}$ can only reduce to $\mathtt{P}$ with probability greater than zero. Moreover, we know that $\Gamma, q : Q \vdash \mathtt{M}[q; x].\mathtt{P}$ entails $\Gamma, x : C \vdash \mathtt{P}$. Both properties together prove our claim.

2. Consider now the case of relabelling. Assume that $\langle\, \mathtt{P}[\mathtt{f}],\, \rho \,\rangle \xrightarrow{f(\alpha)} \langle\, \mathtt{Q}[\mathtt{f}],\, \psi \,\rangle$ with probability greater than zero. Then it is also true that $\langle\, \mathtt{P},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{Q},\, \psi \,\rangle$ with probability greater than zero. The proof then follows by the induction hypothesis.

3. The case of restrictions follows an analogous reasoning to the previous one.

4. The case of conditionals follows an analogous reasoning to the previous one.

5. We now consider the sum operator. Assume that $\langle\, \mathtt{P} + \mathtt{Q},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{R},\, \psi \,\rangle$ with probability greater than zero. This entails that either $\langle\, \mathtt{P},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{R},\, \psi \,\rangle$ with probability greater than zero or $\langle\, \mathtt{Q},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{R},\, \psi \,\rangle$ with probability greater than zero. We consider only the first case. By assumption $\Gamma \vdash \mathtt{P} + \mathtt{Q}$ and therefore $\Gamma \vdash \mathtt{P}$. By the induction hypothesis $\Delta \vdash \mathtt{R}$ for some Δ which proves our claim.

6. Next, we consider constant processes. Assume that $\langle\, \mathtt{A}(\tilde{q}),\, \rho \,\rangle \xrightarrow{\alpha} \langle \mathtt{P},\, \psi \rangle$ with probability greater than zero and that $\Gamma \vdash \mathtt{A}(\tilde{q})$. Moreover, assume the existence of a defining equation $\mathtt{A}(\tilde{q}) \stackrel{def}{=} \mathtt{Q}$ and recall that $\Gamma \vdash \mathtt{A}(\tilde{q})$ entails $\Gamma \vdash \mathtt{Q}$ (a restriction put on defining equations). The transition derivation system ensures that $\langle\, \mathtt{Q},\, \rho \,\rangle \xrightarrow{\alpha} \langle \mathtt{P},\, \psi \rangle$. The proof then follows by the induction hypothesis.

7. We now consider the rule **Q-Com** in Table 1. Assume that $\langle \mathtt{P} \mid\mid \mathtt{Q},\, \rho \rangle \xrightarrow{\tau} \langle \mathtt{P}' \mid\mid \mathtt{Q}',\, \rho \rangle$ with probability greater than zero. This then entails that $\langle \mathtt{P}, \rho \rangle \xrightarrow{\mathtt{c}?r} \langle \mathtt{P}',\, \rho \rangle$ and $\langle \mathtt{Q},\, \rho \rangle \xrightarrow{\mathtt{c}!r} \langle \mathtt{Q}',\, \rho \rangle$ in both cases with probability greater than zero. By assumption we obtain $\Gamma_1 \vdash \mathtt{P}$ and $\Gamma_2 \vdash \mathtt{Q}$ with $\Gamma_1 \cap \Gamma_2 = \emptyset$. Moreover, by the induction hypothesis we obtain $\Delta_1 \vdash \mathtt{P}'$ and $\Delta_2 \vdash \mathtt{Q}'$ with $\Delta_1 = \Gamma_1, r : Q$ and $\Gamma_2 = \Delta_2, r : Q$. Since $\Gamma_1 \cap \Gamma_2 = \emptyset$ we obtain $\Delta_1 \cap \Delta_2 = \emptyset$ and therefore $\Delta_1 \cup \Delta_2 \vdash \mathtt{P}' \mid\mid \mathtt{Q}'$. The rules **C-Com**, **Inp-Int**, and **Oth-Int** follow in a similar fashion.

□

$$\textbf{Tau:}\quad \frac{}{\langle \tau.\mathtt{P},\rho\rangle \xrightarrow{\tau} \langle \mathtt{P},\rho\rangle}$$

$$\textbf{C-Inp:}\quad \frac{}{\langle\ c?x.\mathtt{P},\ \rho\ \rangle \xrightarrow{c?v} \langle\ \mathtt{P}\{v/x\},\ \rho\ \rangle}\ v \in \text{Real}$$

$$\textbf{C-Outp:}\quad \frac{}{\langle\ c!e.\mathtt{P},\rho\ \rangle \xrightarrow{c!v} \langle\ \mathtt{P},\rho\ \rangle}\ v = [\![e]\!]$$

$$\textbf{C-Com:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{c?v} \langle\ \mathtt{P}',\ \rho\ \rangle \qquad \langle\ \mathtt{Q},\ \rho\ \rangle \xrightarrow{c!v} \langle\ \mathtt{Q}',\ \rho\ \rangle}{\langle\ \mathtt{P} \,||\, \mathtt{Q},\ \rho\ \rangle \xrightarrow{\tau} \langle\ \mathtt{P}' \,||\, \mathtt{Q}',\ \rho\ \rangle}$$

$$\textbf{Q-Inp:}\quad \frac{}{\langle\ \mathtt{c}?q.\mathtt{P},\ \rho\ \rangle \xrightarrow{\mathtt{c}?r} \langle\ \mathtt{P}\{r/q\},\ \rho\ \rangle}\ r \notin qv(\mathtt{c}?q.\mathtt{P})$$

$$\textbf{Q-Outp:}\quad \frac{}{\langle\ \mathtt{c}!q.\mathtt{P},\ \rho\ \rangle \xrightarrow{\mathtt{c}!q} \langle\ \mathtt{P},\ \rho\ \rangle}$$

$$\textbf{Q-Com:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{\mathtt{c}?r} \langle\ \mathtt{P}',\ \rho\ \rangle \qquad \langle\ \mathtt{Q},\ \rho\ \rangle \xrightarrow{\mathtt{c}!r} \langle\ \mathtt{Q}',\ \rho\ \rangle}{\langle\ \mathtt{P} \,||\, \mathtt{Q},\ \rho\ \rangle \xrightarrow{\tau} \langle\ \mathtt{P}' \,||\, \mathtt{Q}',\ \rho\ \rangle}$$

$$\textbf{Oper:}\quad \frac{}{\langle\ \varepsilon[\tilde{r}].\mathtt{P},\ \rho\ \rangle \xrightarrow{\tau} \langle\ \mathtt{P},\ \varepsilon_{\tilde{r}}(\rho)\ \rangle}$$

$$\textbf{Meas:}\quad \frac{}{\langle\ \mathtt{M}[\tilde{r};x].\mathtt{P},\rho\ \rangle \xrightarrow{\tau} \sum_{i\in I} p_i \langle\ \mathtt{P}\{\lambda_i/x\}, E^i_{\tilde{r}}\rho E^i_{\tilde{r}}/p_i\ \rangle}$$

where $\mathtt{M}$ has the spectral decomposition $\mathtt{M} = \sum_{i\in I} \lambda_i E^i$ and $p_i = tr(E^i_{\tilde{r}}\rho)$

$$\textbf{Sum:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{\alpha} \mu}{\langle \mathtt{P}+\mathtt{Q},\rho\rangle \xrightarrow{\alpha} \mu}$$

$$\textbf{Rel:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle\ \mathtt{P_i},\ \rho_i\ \rangle}{\langle\ \mathtt{P}[\mathtt{f}],\ \rho\ \rangle \xrightarrow{f(\alpha)} \boxplus p_i \bullet \langle\ \mathtt{P_i}[\mathtt{f}],\ \rho_i\ \rangle}$$

$$\textbf{Res:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle\ \mathtt{P_i},\ \rho_i\ \rangle}{\langle\ \mathtt{P}\backslash\mathtt{L},\ \rho\ \rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle\ \mathtt{P_i}\backslash\mathtt{L},\ \rho_i\ \rangle}\ cn(\alpha) \not\subseteq L$$

$$\textbf{Cho:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{\alpha} \mu}{\langle \textbf{if } b \textbf{ then } \mathtt{P},\ \rho\rangle \xrightarrow{\alpha} \mu}\ [\![b]\!] = true$$

$$\textbf{Def:}\quad \frac{\langle\ \mathtt{P}\{\tilde{r}/\tilde{q}\},\ \ \rho\ \rangle \xrightarrow{\alpha} \mu}{\langle \mathtt{A}(\tilde{r}),\ \ \rho\rangle \xrightarrow{\alpha} \mu}\ \mathtt{A}(\tilde{q}) \stackrel{def}{=} \mathtt{P}$$

$$\textbf{Inp-Int:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{\mathtt{c}?r} \langle\ \mathtt{P}',\ \rho\ \rangle}{\langle\ \mathtt{P} \,||\, \mathtt{Q},\ \rho\ \rangle \xrightarrow{\mathtt{c}?r} \langle\ \mathtt{P}' \,||\, \mathtt{Q},\ \rho\ \rangle}\ r \notin qv(\mathtt{Q})$$

$$\textbf{Oth-Int:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle\ \mathtt{P'_i},\ \rho_i\ \rangle}{\langle\ \mathtt{P} \,||\, \mathtt{Q},\ \rho\ \rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle\ \mathtt{P'_i} \,||\, \mathtt{Q},\ \rho_i\ \rangle}\ \alpha \neq \mathtt{c}?r$$

Table 1: *SOS* rules *qCCS*

$$\text{(NIL)}\quad \frac{}{\Gamma \vdash nil} \qquad \text{(CONST)}\quad \frac{\Delta \subseteq \Gamma}{\Gamma \vdash \mathtt{A}(\Delta)}$$

$$\text{(INV)}\quad \frac{\Gamma \vdash \mathtt{P}}{\Gamma \vdash \tau.\mathtt{P}} \qquad \text{(OP)}\quad \frac{\Gamma \vdash \mathtt{P} \quad X \subseteq \Gamma^Q}{\Gamma \vdash \varepsilon[X].\mathtt{P}}$$

$$\text{(C-OUT)}\quad \frac{\Gamma \vdash \mathtt{P} \quad fv(e) \subseteq \Gamma^C}{\Gamma \vdash c!e.\mathtt{P}} \qquad \text{(C-IN)}\quad \frac{\Gamma, x : C \vdash \mathtt{P}}{\Gamma \vdash c?x.\mathtt{P}}$$

$$\text{(Q-IN)}\quad \frac{\Gamma, r : Q \vdash \mathtt{P}}{\Gamma \vdash \mathtt{c}?r.\mathtt{P}} \qquad \text{(Q-OUT)}\quad \frac{\Gamma \vdash \mathtt{P}}{\Gamma, r : Q \vdash \mathtt{c}!r.\mathtt{P}}$$

$$\text{(MEAS)}\quad \frac{\Gamma, x : C \vdash \mathtt{P}}{\Gamma, r : Q \vdash \mathtt{M}[r;x].\mathtt{P}} \qquad \text{(SUM)}\quad \frac{\Gamma_1 \vdash \mathtt{P} \qquad \Gamma_2 \vdash \mathtt{Q}}{\Gamma_1 \cup \Gamma_2 \vdash \mathtt{P} + \mathtt{Q}}$$

$$\text{(REL)}\quad \frac{\Gamma \vdash \mathtt{P}}{\Gamma \vdash \mathtt{P}[f]} \qquad \text{(RES)}\quad \frac{\Gamma \vdash \mathtt{P}}{\Gamma \vdash \mathtt{P}\backslash\mathtt{L}}$$

$$\text{(IF)}\quad \frac{\Gamma \vdash \mathtt{P} \quad \Delta \vdash\ b}{\Gamma, \Delta \vdash \textbf{if } b \textbf{ then } \mathtt{P}} \qquad \text{(COMM)}\quad \frac{\Gamma_1 \vdash \mathtt{P} \quad \Gamma_2 \vdash \mathtt{Q} \quad \Gamma_1^Q \cap \Gamma_2^Q = \emptyset}{\Gamma_1 \cup \Gamma_2 \vdash \mathtt{P} \,||\, \mathtt{Q}}$$

Table 2: $qCCS$ typing rules