Proof of type preservation

Vítor Fernandes[1], Renato Neves[2], and Luís Barbosa[2]

[1] University of Minho, Braga, Portugal
`vegf17@gmail.com`
[2] International Iberian Nanotechnology Laboratory, INESC-TEC & University of Minho, Braga, Portugal
`{nevrenato,lsb}@di.uminho.pt`

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 derivation system. We also 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 proof for invisible actions, classical output, quantum output, and super-operators is 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 be reduced (i.e. reduce with probability greater than zero) to the simpler process $\mathtt{P}$. 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 $\langle\, \mathtt{P}[\mathtt{f}],\, \rho \,\rangle \xrightarrow{f(\alpha)} \langle\, \mathtt{Q}[\mathtt{f}],\, \sigma \,\rangle$ with probability greater than zero. Then it is also true that $\langle\, \mathtt{P},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{Q},\, \sigma \,\rangle$ with probability greater than zero. The proof then follows directly by the induction hypothesis. The case of restrictions and conditionals follow an analogous reasoning to the previous one.

3. We now consider the sum operator. Assume that $\langle\, \mathtt{P} + \mathtt{Q},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{R},\, \sigma \,\rangle$ with probability greater than zero. This entails that either $\langle\, \mathtt{P},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{R},\, \sigma \,\rangle$ with probability greater than zero or $\langle\, \mathtt{Q},\, \rho \,\rangle \xrightarrow{\alpha} \langle\, \mathtt{R},\, \sigma \,\rangle$ with probability greater than zero. We consider only the first case because the other is analogous. By assumption $\Gamma \vdash \mathtt{P} + \mathtt{Q}$ and therefore $\Gamma \vdash \mathtt{P}$. By the induction hypothesis we obtain $\Delta \vdash \mathtt{R}$ for some Δ and then our claim follows directly.

4. Next, we consider constant processes. Assume that $\langle\ \mathtt{A}(\tilde{q}),\ \rho\ \rangle \xrightarrow{\alpha} \langle \mathtt{P},\ \sigma\rangle$ 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 $\Gamma \vdash \mathtt{Q}$ (an existing restriction over defining equations). The transition derivation system ensures that $\langle\ \mathtt{Q},\ \rho\ \rangle \xrightarrow{\alpha} \langle \mathtt{P},\ \sigma\rangle$. The proof then follows by the induction hypothesis.

5. 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 entails that $\langle \mathtt{P},\rho\rangle \xrightarrow{\mathtt{c}?r} \langle \mathtt{P}',\ \rho\rangle$ and that $\langle \mathtt{Q},\ \rho\rangle \xrightarrow{\mathtt{c}!r} \langle \mathtt{Q}',\ \rho\rangle$ 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 $\Delta_1^Q \subseteq \Gamma_1^Q, r : Q$ and $\Delta_2^Q \subseteq \Gamma_2 \backslash \{r : Q\}$. Since $\Gamma_1^Q \cap \Gamma_2^Q = \emptyset$ we obtain $\Delta_1^Q \cap \Delta_2^Q = \emptyset$ and therefore $\Delta_1 \cup \Delta_2 \vdash \mathtt{P}' \mid\mid \mathtt{Q}'$. The proof for the rules **C-Com**, **Inp-Int**, and **Oth-Int** follows a similar reasoning.

$\square$

To make it easier for the reader to follow the proof, the transition rules of qCCS [1] are presented in Table 1.

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

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

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

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

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

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

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

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

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

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

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

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

$$\textbf{Res:}\quad \frac{\langle\ \mathtt{P},\ \rho\ \rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle\ \mathtt{P_i},\ \rho_i\ \rangle}{\langle\ \mathtt{P}\backslash\mathtt{L},\ \rho\ \rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle\ \mathtt{P_i}\backslash\mathtt{L},\ \rho_i\ \rangle}\ cn(\alpha) \nsubseteq L$$

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

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

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

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

Table 1: SOS rules QCCS

With the same purpose as previously, the type system developed for QCCS [2] is presented in Table 2.

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

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

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

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

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

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

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

Table 2: QCCS type rules

Remark. The rule (C-OUT) presented in Table 2, is different of the one in [2].

References

[1] Yuan Feng, Runyao Duan, and Mingsheng Ying. Bisimulation for quantum processes. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 34(4):17, 2012.

[2] Vitor Fernandes. Integration of time in a quantum process algebra. Master's thesis, Dep. Informatica, Universidade do Minho, 2019. Available at https://github.com/vegf17/dissertation.