Symbolic SOS for CIF

M.A. Reniers D.E. Nadales Agut

May 9, 2011

Abstract

1 Symbolic rules

A symbolic action has the form

$$\langle p \rangle \xrightarrow{a,b,g,u,n,n',W,C,r} \langle p' \rangle$$

where:

- a is an action label, $a \in \mathcal{A}$
- b is boolean that indicates whether action is synchronizing, $b \in \mathbb{B}$
- g (guard), u (initialization expression), and n (invariant) are the predicates that have to be satisfied by the initial valuation, $g, u, n \in \mathcal{P}$
- n' is the invariant expression that has to be satisfied in the new valuation, $n' \in \mathcal{P}$
- W and C are the sets of jumping and control variables, respectively, associated to action a, $W, C \subseteq \mathcal{V}$
- r is the predicate that determines how the values of variables change in the new valuation (with regard to the old valuation), $r \in \mathcal{P}$

A symbolic time transition has the form

$$\langle p \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p' \rangle$$

where:

- u is initialization predicate that has to be satisfied at the beginning of the time delay, $u \in \mathcal{P}$
- n (invariant) and w (tcp) are the predicates that have to be satisfied during the time delay, $n, w \in \mathcal{P}$
- G is the dynamic type mapping, which associates a dynamic type to each variable in its domain, $G \in \mathcal{V} \rightharpoonup 2^{(\mathbb{T} \rightharpoonup \Lambda) \times (\mathbb{T} \rightharpoonup \Lambda)}$
- A is the set of synchronizing actions of composition p (and p'), $A \subseteq \mathcal{A}$
- P is a set of pairs of guards and enabled actions, $P \subseteq \mathcal{P} \times \mathcal{A}$
- U is a set of urgent guards, $U \subseteq \mathcal{P}$

A symbolic environment transition has the form

$$\langle p \rangle \overset{u,n,C,A}{\dashrightarrow} \langle p' \rangle$$

where:

- u (initialization expression) and n (invariant) are the predicates that must be satisfied by the initial valuation, $u, n \in \mathcal{P}$
- C is the set of controlled variables of composition p (and p'), $C \subseteq \mathcal{V}$

- A is the set of synchronizing actions of composition p (and p'), $A \subseteq \mathcal{A}$

Theorem 1 (Soundness of action transitions)**.** *For all p, p', a, b, g, u, n, n', W, C, r, X σ, and σ' we have that if the following conditions hold:*

1. $\langle p \rangle \xrightarrow{a,b,g,u,n,n',W,C,r} \langle p' \rangle$
2. $\sigma \models g$
3. $\sigma \models u$
4. $\sigma \models n$
5. $\sigma' \models n'$
6. $\sigma \restriction_{(C \cup X) \setminus W} = \sigma' \restriction_{(C \cup X) \setminus W}$
7. $\sigma'^{+} \cup \sigma \models r$

then, there is a concrete action transition:

$$(p, \sigma) \xrightarrow{a,b,X} (p', \sigma')$$

Theorem 2 (Soundness of environment transitions)**.** *For all p, p', u, n, C, A σ, and σ' we have that if the following conditions hold:*

1. $\langle p \rangle \overset{u,n,C,A}{\dashrightarrow} \langle p' \rangle$
2. $\sigma \models u$
3. $\sigma \models n$
4. $\sigma' \models n$
5. $\sigma \restriction_C = \sigma' \restriction_C$

then, there is a concrete environment transition:

$$(p, \sigma) \overset{A}{\dashrightarrow} (p', \sigma')$$

Theorem 3 (Soundness of time transitions)**.** *For all p, p', u, n, w, G, A, P, U, ρ, θ, and t we have that if the following conditions hold:*

1. $\langle p \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p' \rangle$
2. $\mathrm{dom}(\rho) = \mathrm{dom}(\theta) = [0, t] \wedge 0 < t$
3. $\rho(0) \models u$
4. $\langle \forall s : s \in [0, t] : \rho(s) \models n \rangle$
5. $\langle \forall s : s \in [0, t) : \rho(s) \models w \rangle$
6. $\langle \forall x : x \in \mathrm{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle$
7. $\langle \forall s : s \in [0, t] : \theta(s) = \{a \mid (g, a) \in P \wedge \rho(s) \models g\} \rangle$

8. $\langle \forall s : s \in [0,t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle$

then there is a concrete time transition:

$$(p, \rho(0)) \xrightarrow{\rho, A, \theta} (p', \rho(t))$$

Theorem 4 (Completeness of action transitions)**.** *For all p, p', a, b, X, σ, and σ' we have that if there is a concrete transition:*

$$(p, \sigma) \xrightarrow{a,b,X} (p', \sigma')$$

then there exists g, u, n, n', W, C, and r such that the following conditions hold:

1. $\langle p \rangle \xrightarrow{a,b,g,u,n,n',W,C,r} \langle p' \rangle$
2. $\sigma \models g$
3. $\sigma \models u$
4. $\sigma \models n$
5. $\sigma' \models n'$
6. $\sigma \restriction_{(C \cup X) \setminus W} = \sigma' \restriction_{(C \cup X) \setminus W}$
7. $\sigma'^{+} \cup \sigma \models r$

Theorem 5 (Completeness of environment transitions)**.** *For all p, p', A, σ, and σ' we have that if there is a concrete environment transition:*

$$(p, \sigma) \xrightarrow{A} (p', \sigma)$$

then there exists u, n, and C such that the following holds:

- $\langle p \rangle \overset{u,n,C,A}{\dashrightarrow} \langle p' \rangle$
- $\sigma \models u$
- $\sigma \models n$
- $\sigma' \models n$
- $\sigma \restriction_C = \sigma' \restriction_C$

Theorem 6 (Completeness of time transitions)**.** *For all p, p', ρ, A, and t we have that if there is a concrete time transition:*

$$(p, \rho(0)) \xrightarrow{\rho, A, \theta} (p', \rho(t))$$

then there exists u, n, w, G, P, and U such that the following conditions hold:

1. $\langle p \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p' \rangle$
2. $\rho(0) \models u$
3. $\langle \forall s : s \in [0,t] : \rho(s) \models n \rangle$

4. $\langle \forall s : s \in [0,t) : \rho(s) \models w \rangle$

5. $\langle \forall x : x \in \mathrm{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle$

6. $\langle \forall s : s \in [0,t] : \theta(s) = \{a \mid (g,a) \in P \wedge \rho(s) \models g\} \rangle$

7. $\langle \forall s : s \in [0,t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle$

1.1 Automata

Symbolic rules for automata.

Action transitions.

$$\frac{(v, g, a, (W, r), v') \in E}{\langle (V, \mathrm{init}, \mathrm{inv}, \mathrm{tcp}, E, \mathrm{var}_C, \mathrm{act}_S, \mathrm{dtype}) \rangle \xrightarrow{a, a \in \mathrm{act}_S, g, \mathrm{init}(v), \mathrm{inv}(v), \mathrm{inv}(v'), W, \mathrm{var}_C, r} \langle (V, \mathrm{id}_{v'}, \mathrm{inv}, \mathrm{tcp}, E, \mathrm{var}_C, \mathrm{act}_S, \mathrm{dtype}) \rangle} \; 1$$

Environment transitions.

$$\frac{v \in V}{\langle (V, \mathrm{init}, \mathrm{inv}, \mathrm{tcp}, E, \mathrm{var}_C, \mathrm{act}_S, \mathrm{dtype}) \rangle \overset{\mathrm{init}(v), \mathrm{inv}(v), \mathrm{var}_C, \mathrm{act}_S}{\dashrightarrow} \langle (V, \mathrm{id}_v, \mathrm{inv}, \mathrm{tcp}, E, \mathrm{var}_C, \mathrm{act}_S, \mathrm{dtype}) \rangle} \; 2$$

Time transitions.

$$\frac{v \in V}{\langle (V, \mathrm{init}, \mathrm{inv}, \mathrm{tcp}, E, \mathrm{var}_C, \mathrm{act}_S, \mathrm{dtype}) \rangle \overset{\mathrm{init}(v), \mathrm{inv}(v), \mathrm{tcp}(v), \mathrm{dtype}, \mathrm{act}_S, \{(g,a) \mid (v,g,a,u,v') \in E\}, \emptyset}{\longmapsto} \langle (V, \mathrm{id}_v, \mathrm{inv}, \mathrm{tcp}, E, \mathrm{var}_C, \mathrm{act}_S, \mathrm{dtype}) \rangle} \; 3$$

1.2 Parallel composition

Symbolic rule for synchronizing actions.

$$\frac{\langle p \rangle \xrightarrow{a, \mathrm{true}, g_p, u_p, n_p, n'_p, W_p, C_p, r_p} \langle p' \rangle, \langle q \rangle \xrightarrow{a, \mathrm{true}, g_q, u_q, n_q, n'_q, W_q, C_q, r_q} \langle q' \rangle}{\langle p \parallel q \rangle \xrightarrow{a, \mathrm{true}, g_p \wedge g_q, u_p \wedge u_q, n_p \wedge n_q, n'_p \wedge n'_q, W_p \cap W_q, (C_p \setminus W_p) \cup (C_q \setminus W_q), r_p \wedge r_q} \langle p' \parallel q' \rangle} \; 4$$

Symbolic rules for interleaving actions.

$$\frac{\langle p \rangle \xrightarrow{a, b, g_p, u_p, n_p, n'_p, W_p, C_p, r} \langle p' \rangle, \langle q \rangle \overset{u_q, n_q, C_q, A}{\dashrightarrow} \langle q' \rangle, a \notin A}{\langle p \parallel q \rangle \xrightarrow{a, b, g_p, u_p \wedge u_q, n_p \wedge n_q, n'_p \wedge n_q, W_p \setminus C_q, C_p \cup C_q, r} \langle p' \parallel q' \rangle} \; 5$$

$$\frac{\langle q \rangle \xrightarrow{a, b, g_q, u_q, n_q, n'_q, W_q, C_q, r} \langle q' \rangle, \langle p \rangle \overset{u_p, n_p, C_p, A}{\dashrightarrow} \langle p' \rangle, a \notin A}{\langle p \parallel q \rangle \xrightarrow{a, b, g_q, u_q \wedge u_p, n_q \wedge n_p, n'_q \wedge n_p, W_q \setminus C_p, C_q \cup C_p, r} \langle p' \parallel q' \rangle} \; 6$$

Rule for environment transitions.

$$\frac{\langle p \rangle \overset{u_p, n_p, C_p, A_p}{\dashrightarrow} \langle p' \rangle, \langle q \rangle \overset{u_q, n_q, C_q, A_q}{\dashrightarrow} \langle q' \rangle}{\langle p \parallel q \rangle \overset{u_p \wedge u_q, n_p \wedge n_q, C_p \cup C_q, A_p \cup A_q}{\dashrightarrow} \langle p' \parallel q' \rangle} \; 7$$

For defining the rule for time transitions, we make use of the operators $\fatbslash$, $\cap_2$, and $\setminus_2$, which are defined next.

Definition 1 (Join)**.** *Given two partial functions* $f : A \rightharpoonup 2^B$ *and* $g : A \rightharpoonup 2^B$*,* $f \fatbslash g$ *is the function such that* $\mathrm{dom}(f \fatbslash g) = \mathrm{dom}(f) \cup \mathrm{dom}(g)$ *and for all* $x \in \mathrm{dom}(f \fatbslash g)$*:*

$$(f \fatbslash g)(x) = \begin{cases} f(x) \cap g(x) & \text{if } x \in \mathrm{dom}(f) \cap \mathrm{dom}(g) \\ f(x) & \text{if } x \in \mathrm{dom}(f) \setminus \mathrm{dom}(g) \\ g(x) & \text{if } x \in \mathrm{dom}(g) \setminus \mathrm{dom}(f) \end{cases}$$

Definition 2 (Second component intersection)**.** *Given two sets* $A, B \subseteq C \times D$*:*

$$A \cap_2 B \triangleq \{(c_a \wedge c_b, d) \mid (c_a, d) \in A \wedge (c_b, d) \in B\}$$

Definition 3 (Second component difference)**.** *Given a set* $A \subseteq B \times C$ *and a set* $D \subseteq C$*:*

$$A \setminus_2 D \triangleq \{(a, b) \mid (a, b) \in A \wedge b \notin D\}$$

Rule for time transitions.

$$\frac{\langle p \rangle \overset{u_p, n_p, w_p, G_p, A_p, P, U_p}{\longmapsto} \langle p' \rangle, \langle q \rangle \overset{u_q, n_q, w_q, G_q, A_q, Q, U_q}{\longmapsto} \langle q' \rangle}{\langle p \parallel q \rangle \overset{u_p \wedge u_q, n_p \wedge n_q, w_p \wedge w_q, G_p \fatbslash G_q, A_p \cup A_q, (P \cap_2 Q) \cup (P \setminus_2 A_q) \cup (Q \setminus_2 A_p), U_p \cup U_q}{\longmapsto} \langle p' \parallel q' \rangle} \; 8$$

1.3 Control variable

Symbolic rule for actions.

$$\frac{\langle p \rangle \xrightarrow{a, b, g, u, n, n', W, C, r} \langle p' \rangle}{\langle \mathrm{ctrl}_x(p) \rangle \xrightarrow{a, b, g, u, n, n', W, C \cup \{x\}, r} \langle \mathrm{ctrl}_x(p') \rangle} \; 9$$

Symbolic rule for environment transitions[1]:

$$\frac{\langle p \rangle \overset{u, n, C, A}{\dashrightarrow} \langle p' \rangle}{\langle \mathrm{ctrl}_x(p) \rangle \overset{u, n, C \cup \{x\}, A}{\dashrightarrow} \langle \mathrm{ctrl}_x(p') \rangle} \; 10$$

$$\frac{\langle p \rangle \overset{u, n, w, G, A, P, U}{\longmapsto} \langle p' \rangle}{\langle \mathrm{ctrl}_x(p) \rangle \overset{u, n, w, G, A, P, U}{\longmapsto} \langle \mathrm{ctrl}_x(p') \rangle} \; 11$$

1.4 Urgency

$$\frac{\langle p \rangle \xrightarrow{a, b, g, u, n, n', W, C, r} \langle p' \rangle}{\langle \upsilon_{a'}(p) \rangle \xrightarrow{a, b, g, u, n, n', W, C, r} \langle \upsilon_{a'}(p') \rangle} \; 12$$

$$\frac{\langle p \rangle \overset{u, n, C, A}{\dashrightarrow} \langle p' \rangle}{\langle \upsilon_a(p) \rangle \overset{u, n, C, A}{\dashrightarrow} \langle \upsilon_a(p') \rangle} \; 13$$

[1]The rule for environment transition should also work if we add condition $x = x^+$ in the reset predicate, instead of adding x to the set of control variables in the conclusion.

$$\frac{\langle p\rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p'\rangle}{\langle \upsilon_a(p)\rangle \overset{u,n,w,G,A,P,U\cup\{g|(g,a)\in P\}}{\longmapsto} \langle \upsilon_a(p')\rangle}\ 14$$

1.5 Dynamic type

$$\frac{\langle p\rangle \xrightarrow{a,b,g,u,n,n',W,C,r} \langle p'\rangle}{\langle \mathrm{D}_{x:G}(p)\rangle \xrightarrow{a,b,g,u,n,n',W,C,r} \langle \mathrm{D}_{x:G}(p')\rangle}\ 15$$

$$\frac{\langle p\rangle \overset{u,n,C,A}{\dashrightarrow} \langle p'\rangle}{\langle \mathrm{D}_{x:G}(p)\rangle \overset{u,n,C,A}{\dashrightarrow} \langle \mathrm{D}_{x:G}(p')\rangle}\ 16$$

$$\frac{\langle p\rangle \overset{u,n,w,D,A,P,U}{\longmapsto} \langle p'\rangle}{\langle \mathrm{D}_{x:G}(p)\rangle \overset{u,n,w,D\uplus\{(x,G)\},A,P,U}{\longmapsto} \langle \mathrm{D}_{x:G}(p')\rangle}\ 17$$

1.6 Initialization

$$\frac{\langle p\rangle \xrightarrow{a,b,g,u,n,n',W,C,r} \langle p'\rangle}{\langle u' \gg p\rangle \xrightarrow{a,b,g,u\wedge u',n,n',W,C,r} \langle p'\rangle}\ 18$$

$$\frac{\langle p\rangle \overset{u,n,C,A}{\dashrightarrow} \langle p'\rangle}{\langle u' \gg p\rangle \overset{u\wedge u',n,C,A}{\dashrightarrow} \langle p'\rangle}\ 19$$

$$\frac{\langle p\rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p'\rangle}{\langle u' \gg p\rangle \overset{u\wedge u',n,w,G,A,P,U}{\longmapsto} \langle p'\rangle}\ 20$$

1.7 Synchronization

$$\frac{\langle p\rangle \xrightarrow{a,b,g,u,n,n',W,C,r} \langle p'\rangle}{\langle \gamma_{a'}(p)\rangle \xrightarrow{a,b\vee a=a',g,u,n,n',W,C,r} \langle \gamma_{a'}(p')\rangle}\ 21$$

$$\frac{\langle p\rangle \overset{u,n,C,A}{\dashrightarrow} \langle p'\rangle}{\langle \gamma_a(p)\rangle \overset{u,n,C,A\cup\{a\}}{\dashrightarrow} \langle \gamma_a(p')\rangle}\ 22$$

$$\frac{\langle p\rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p'\rangle}{\langle \gamma_a(p)\rangle \overset{u,n,w,G,A\cup\{a\},P,U}{\longmapsto} \langle \gamma_a(p')\rangle}\ 23$$

2 Proofs

2.1 Soundness of Symbolic Action Rules

For proving Theorem 1 we need the following lemmas.

Lemma 1. *For all sets C_0, X, W_0, C_1, W_1 the following equality holds:*

$$((C_0 \cup X) \setminus W_0) \cup ((C_1 \cup X) \setminus W_1) = ((C_0 \setminus W_0) \cup (C_1 \setminus W_1) \cup X) \setminus (W_0 \cap W_1)$$

Proof. We make the following derivation:

$$((C_0 \cup X) \setminus W_0) \cup ((C_1 \cup X) \setminus W_1)$$

$$= \{\text{Set algebra}\}$$

$$((C_0 \cup X) \cap \overline{W_0}) \cup ((C_1 \cup X) \cap \overline{W_1})$$

$$= \{\text{Set algebra}\}$$

$$(C_0 \cap \overline{W_0}) \cup (X \cap \overline{W_0}) \cup (C_1 \cap \overline{W_1}) \cup (X \cap \overline{W_1})$$

$$= \{\text{Set algebra}\}$$

$$(X \cap (\overline{W_0} \cup \overline{W_1})) \cup (C_0 \cap \overline{W_0}) \cup (C_1 \cap \overline{W_1})$$

$$= \{\text{Set algebra}\}$$

$$((X \cup (C_0 \cap \overline{W_0}) \cup (C_1 \cap \overline{W_1})) \cap ((\overline{W_0} \cup \overline{W_1}) \cup (C_0 \cap \overline{W_0}) \cup (C_1 \cap \overline{W_1}))$$

$$= \{\text{Set algebra (associativity of } \cup\text{, absorption)}\}$$

$$((X \cup (C_0 \cap \overline{W_0}) \cup (C_1 \cap \overline{W_1})) \cap (\overline{W_0} \cup \overline{W_1})$$

$$= \{\text{Set algebra}\}$$

$$((C_0 \setminus W_0) \cup (C_1 \setminus W_1) \cup X) \setminus (W_0 \cap W_1)$$

□

Lemma 2. *For all σ, σ', C_0, X, W_0, C_1, W_1 the following equivalence holds:*

$$\sigma \restriction_{((C_0 \setminus W_0) \cup (C_1 \setminus W_1) \cup X) \setminus (W_0 \cap W_1)} = \sigma' \restriction_{((C_0 \setminus W_0) \cup (C_1 \setminus W_1) \cup X) \setminus (W_0 \cap W_1)} \Leftrightarrow$$
$$\sigma \restriction_{((C_0 \cup X) \setminus W_0)} = \sigma' \restriction_{((C_0 \cup X) \setminus W_0)} \wedge$$
$$\sigma \restriction_{((C_1 \cup X) \setminus W_1)} = \sigma' \restriction_{((C_1 \cup X) \setminus W_1)}$$

Proof. In the proof of the theorem we make use of the following equivalence:

$$\sigma \restriction_A = \sigma' \restriction_A \Leftrightarrow \langle \forall x :: x \in A \Rightarrow \sigma(x) = \sigma'(x) \rangle \tag{1}$$

for all σ, σ', A.

Then we make the following derivation:

$$\sigma \restriction_{((C_0 \setminus W_0) \cup (C_1 \setminus W_1) \cup X) \setminus (W_0 \cap W_1)} = \sigma' \restriction_{((C_0 \setminus W_0) \cup (C_1 \setminus W_1) \cup X) \setminus (W_0 \cap W_1)}$$

$$\Leftrightarrow \{(1)\}$$

$$\langle \forall x :: x \in ((C_0 \setminus W_0) \cup (C_1 \setminus W_1) \cup X) \setminus (W_0 \cap W_1) \Rightarrow \sigma(x) = \sigma'(x) \rangle$$

$$\Leftrightarrow \{\text{Lemma 1}\}$$

$$\langle \forall x :: x \in ((C_0 \cup X) \setminus W_0) \cup ((C_1 \cup X) \setminus W_1) \Rightarrow \sigma(x) = \sigma'(x) \rangle$$

$$\Leftrightarrow \{\text{Set algebra and predicate calculus}\}$$

$$\langle \forall x :: x \in ((C_0 \cup X) \setminus W_0) \Rightarrow \sigma(x) = \sigma'(x) \rangle \wedge$$
$$\langle \forall x :: x \in ((C_1 \cup X) \setminus W_1) \Rightarrow \sigma(x) = \sigma'(x) \rangle$$
$$\Leftrightarrow \{(1)\}$$
$$\sigma \restriction_{((C_0 \cup X) \setminus W_0)} = \sigma' \restriction_{((C_0 \cup X) \setminus W_0)} \wedge \sigma \restriction_{((C_1 \cup X) \setminus W_1)} = \sigma' \restriction_{((C_1 \cup X) \setminus W_1)}$$

□

Proof of Theorem 1.
We prove Theorem 1 via structural induction on CIF compositions.

Base Case Assume there is an automaton:

$$p \triangleq (V, \text{init}, \text{inv}, \text{tcp}, E, \text{var}_C, \text{act}_S, \text{dtype})$$

and p', p', a, b, g, u, n, n', W, C, r, X, σ, and σ' such that the following holds:

$$\begin{aligned}
&\langle p \rangle \xrightarrow{a,b,g,u,n,n',W,C,r} \langle p' \rangle \\
&\sigma \models g \\
&\sigma \models u \\
&\sigma \models n \\
&\sigma' \models n' \\
&\sigma \restriction_{(C \cup X) \setminus W} = \sigma' \restriction_{(C \cup X) \setminus W} \\
&\sigma'^{+} \cup \sigma \models r
\end{aligned} \tag{2}$$

By inspecting the symbolic rule 1, we know that there must be an edge $(v, g, a, (W, r), v')$ such that:

$$\begin{aligned}
&b \equiv a \in \text{act}_S \\
&u \equiv \text{init}(v) \\
&n \equiv \text{inv}(v) \\
&n' \equiv \text{inv}(v') \\
&C \equiv \text{var}_C \\
&p' \equiv (V, \text{id}_{v'}, \text{inv}, \text{tcp}, E, \text{var}_C, \text{act}_S, \text{dtype})
\end{aligned} \tag{3}$$

Replacing the previous equivalences in (2), and simplifying the conjunctions yields:

$$\begin{aligned}
&\sigma \models \text{init}(v) \\
&\sigma \models \text{inv}(v) \\
&\sigma' \models \text{inv}(v') \\
&\sigma \restriction_{(\text{var}_C \cup X) \setminus W} = \sigma' \restriction_{(\text{var}_C \cup X) \setminus W}
\end{aligned} \tag{4}$$

Using (2), (4), and the concrete rule for atomic automata, we get that there is a concrete transition:

$$(p, \sigma) \xrightarrow{a,b,X} (p', \sigma')$$

which concludes the proof for the base case.

Induction Step

Parallel composition

Assume there are compositions q, r such that:

$$p \triangleq q \parallel r$$

and p', a, b, g, u, n, n', W, C, s, X σ, and σ' such that the following holds:

$$\begin{aligned}
&\langle p \rangle \xrightarrow{a,b,g,u,n,n',W,C,s} \langle p' \rangle \\
&\sigma \models g \\
&\sigma \models u \\
&\sigma \models n \\
&\sigma' \models n' \\
&\sigma \restriction_{(C \cup X) \setminus W} = \sigma' \restriction_{(C \cup X) \setminus W} \\
&\sigma'^{+} \cup \sigma \models s
\end{aligned} \tag{5}$$

By inspecting the symbolic rules, we know that the previous symbolic transition was originated by the application of Rule 4, Rule 5, or Rule 6. Then we make a case analysis depending on the last rule that was applied.

Rule 4 was applied last In this case there must be g_i, u_i, n_i, n'_i, W_i, C_i, r_i, with $i \in \{q, r\}$, such that:

$$\begin{aligned}
&\langle q \rangle \xrightarrow{a,\text{true},g_q,u_q,n_q,n'_q,W_q,C_q,r_q} \langle q' \rangle \\
&\langle r \rangle \xrightarrow{a,\text{true},g_r,u_r,n_r,n'_r,W_r,C_r,r_r} \langle r' \rangle \\
&b \equiv \text{true} \\
&g \equiv g_q \wedge g_r \\
&u \equiv u_q \wedge u_r \\
&n \equiv n_q \wedge n_r \\
&n' \equiv n'_q \wedge n'_r \\
&W \equiv W_q \cap W_r \\
&C \equiv (C_q \setminus W_q) \cup (C_r \setminus W_r) \\
&s \equiv r_q \wedge r_r \\
&p' \equiv q' \parallel r'
\end{aligned} \tag{6}$$

Replacing the equivalent terms in (5), and using the fact that for all predicates e, e' $(\sigma \models e \wedge e') \Leftrightarrow (\sigma \models e) \wedge (\sigma \models e')$ we get:

$$\begin{aligned}
&\sigma \models g_i \\
&\sigma \models u_i \\
&\sigma \models n_i \\
&\sigma' \models n'_i \\
&\sigma \cup \sigma'^{+} \models r_i
\end{aligned} \tag{7}$$

for $i \in \{q, r\}$.
From (5) and (6) we know that:

$$\begin{aligned} &\sigma \restriction_{(((C_q \setminus W_q) \cup (C_r \setminus W_r)) \cup X) \setminus (W_q \cap W_r)} = \\ &\sigma' \restriction_{(((C_q \setminus W_q) \cup (C_r \setminus W_r)) \cup X) \setminus (W_q \cap W_r)} \end{aligned} \tag{8}$$

Using Lemma 2, we get:

$$\sigma \restriction_{(C_i \cup X) \setminus W_i} = \sigma' \restriction_{(C_i \cup X) \setminus W_i} \tag{9}$$

for $i \in \{q, r\}$.
Using (6), (7), and (9) we can apply the induction hypothesis, to infer that there are concrete transitions:

$$(q, \sigma) \xrightarrow{a, \text{true}, X} (q', \sigma') \text{ and } (r, \sigma) \xrightarrow{a, \text{true}, X} (r', \sigma') \tag{10}$$

Using the previous equation, and the concrete rule for parallel composition, synchronizing actions case, we get that there is a transition:

$$(q \parallel r, \sigma) \xrightarrow{a, \text{true}, X} (q' \parallel r', \sigma')$$

And this concludes the proof for this case.

Rule 5 was applied last In this case there must be u_i, n_i, n'_q, W_q, and C_i, with $i \in \{q, r\}$, such that:

$$\begin{aligned} &\langle q \rangle \xrightarrow{a, b, g, u_q, n_q, n'_q, W_q, C_q, s} \langle q' \rangle \\ &\langle r \rangle \overset{u_r, n_r, C_r, A}{\dashrightarrow} \langle r' \rangle \\ &u \equiv u_q \wedge u_r \\ &n \equiv n_q \wedge n_r \\ &n' \equiv n'_q \wedge n_r \\ &W \equiv W_q \setminus C_r \\ &C \equiv C_q \cup C_r \\ &a \notin A \\ &p' \equiv q' \parallel r' \end{aligned} \tag{11}$$

Replacing the equivalent terms in (11), and applying predicate calculus we infer:

$$\begin{aligned} &\sigma \models u_q \\ &\sigma \models n_q \\ &\sigma' \models n'_q \\ &\sigma \restriction_{(C_q \cup C_r \cup X) \setminus (W_q \setminus C_r)} = \sigma' \restriction_{(C_q \cup C_r \cup X) \setminus (W_q \setminus C_r)} \end{aligned} \tag{12}$$

Using the last equation, set algebra, and predicate calculus we obtain:

$$\begin{aligned} &\sigma \restriction_{(C_q \cup X) \setminus W_q} = \sigma' \restriction_{(C_q \cup X) \setminus W_q} \wedge \\ &\sigma \restriction_{C_r} = \sigma' \restriction_{C_r} \end{aligned} \tag{13}$$

Using (5), (12), and (13), we can apply induction hypothesis and infer that there is a concrete action transition:

$$(q, \sigma) \xrightarrow{a,b,X} (q', \sigma') \tag{14}$$

From (5) and the equivalences of (11) we get:

$$\begin{aligned} &\sigma \models u_r \\ &\sigma \models n_r \\ &\sigma' \models n_r \end{aligned} \tag{15}$$

Then, using (13), the environment transition of (11), and the soundness of environment transitions (Lemma 2) we infer that there is an environment transition:

$$(r, \sigma) \xrightarrow{A} (r', \sigma') \tag{16}$$

Using these two transitions, and the fact that $a \notin A$ we can apply the concrete rule for parallel composition to obtain a concrete transition:

$$(q \parallel r, \sigma) \xrightarrow{a,b,X} (q' \parallel r', \sigma')$$

And this concludes the proof for this case.

Rule 6 was applied last This case is symmetrical to the previous one.

Urgency Case Straightforward using the symbolic rule for urgency, induction hypothesis, and the concrete rule for urgency.

Dynamic type Straightforward using the symbolic rule for dynamic type, induction hypothesis, and the concrete rule for dynamic type.

Synchronization Case Straightforward using the symbolic rule for synchronization, induction hypothesis, and the concrete rule for synchronization.

Control variable Assume there is a composition q and a variable x such that:

$$p \equiv \mathrm{ctrl}_x(q) \tag{17}$$

and p', a, b, g, u, n, n', W, C, s, X σ, and σ' such that the following holds:

$$\begin{aligned} &\langle p \rangle \xrightarrow{a,b,g,u,n,n',W,C,s} \langle p' \rangle \\ &\sigma \models g \\ &\sigma \models u \\ &\sigma \models n \\ &\sigma' \models n' \\ &\sigma \restriction_{(C \cup X) \setminus W} = \sigma' \restriction_{(C \cup X) \setminus W} \\ &\sigma \cup \sigma'^{+} \models s \end{aligned} \tag{18}$$

By inspecting at the symbolic rule for control (Rule 9), we know that there must exist q', and C' such that:

$$\begin{aligned} & p' \equiv \mathrm{ctrl}_x(q') \\ & \langle q \rangle \xrightarrow{a,b,g,u,n,n',W,C',s} \langle q' \rangle \\ & C \equiv C' \cup \{x\} \end{aligned} \tag{19}$$

Replacing C by its equivalent term in (18) we obtain:

$$\sigma \restriction_{(C' \cup \{x\} \cup X) \setminus W} = \sigma' \restriction_{(C' \cup \{x\} \cup X) \setminus W} \tag{20}$$

Using (18), (20), and the symbolic transition of (19) we can apply induction hypothesis and obtain that there is a concrete action transition:

$$(q, \sigma) \xrightarrow{a,b,X \cup \{x\}} (q', \sigma') \tag{21}$$

And using the previous transition, and applying the concrete rule for control variable we can conclude that there is a concrete transition:

$$(\mathrm{ctrl}_x(q), \sigma) \xrightarrow{a,b,X} (\mathrm{ctrl}_x(q'), \sigma')$$

Initialization Straightforward using the symbolic rule for initialization, the fact that $(\sigma \models e \wedge e') \Leftrightarrow (\sigma \models e) \wedge (\sigma \models e')$, for all σ, e, and e', induction hypothesis, and the concrete rule for initialization.

□

2.2 Soundness of Symbolic Environment Rules

Proof of Theorem 2. The proof of Theorem 2 goes via structural induction on CIF compositions.

Base Case Assume there is an automaton:

$$p \triangleq (V, \mathrm{init}, \mathrm{inv}, \mathrm{tcp}, E, \mathrm{var}_C, \mathrm{act}_S, \mathrm{dtype})$$

and p', u, n, C, A, σ, and σ' such that the following holds:

$$\begin{aligned} & \langle p \rangle \overset{u,n,C,A}{\dashrightarrow} \langle p' \rangle \\ & \sigma \models u \\ & \sigma \models n \\ & \sigma' \models n \\ & \sigma \restriction_C = \sigma' \restriction_C \end{aligned} \tag{22}$$

By inspecting the symbolic rule for atomic automata (Rule 2), we know that there must be a location $v \in V$ such that:

$$\begin{aligned} & p' \equiv (V, \mathrm{id}_v, \mathrm{inv}, \mathrm{tcp}, E, \mathrm{var}_C, \mathrm{act}_S, \mathrm{dtype}) \\ & u \equiv \mathrm{init}(v) \\ & n \equiv \mathrm{inv}(v) \\ & C \equiv \mathrm{var}_C \\ & A \equiv \mathrm{act}_S \end{aligned} \tag{23}$$

Using the equivalences above in (22) we obtain:

$$\begin{aligned}
&\sigma \models \text{init}(v) \\
&\sigma \models \text{inv}(v) \\
&\sigma' \models \text{inv}(v) \\
&\sigma \restriction_{\text{var}_C} = \sigma' \restriction_{\text{var}_C}
\end{aligned} \tag{24}$$

Then applying the concrete rule for atomic automata, we can infer that there is a concrete environment transition:

$$(p, \sigma) \xrightarrow{A} (p', \sigma')$$

which concludes the proof for this case.

Induction Step Parallel Composition Case Assume there are compositions q, r such that:

$$p \triangleq q \parallel r$$

and p', u, n, C, A, σ, and σ' such that the following holds:

$$\begin{aligned}
&\langle p \rangle \xrightarrow{u,n,C,A} \langle p' \rangle \\
&\sigma \models u \\
&\sigma \models n \\
&\sigma' \models n \\
&\sigma \restriction_C = \sigma' \restriction_C
\end{aligned} \tag{25}$$

Inspecting the symbolic rule for parallel composition, we know that there must be u_i, n_i, C_i, A_i, q', and r', for $i \in \{q, r\}$ such that:

$$\begin{aligned}
&p' \equiv q' \parallel r' \\
&\langle q \rangle \xrightarrow{u_q,n_q,C_q,A_q} \langle q' \rangle \\
&\langle r \rangle \xrightarrow{u_r,n_r,C_r,A_r} \langle r' \rangle \\
&u \equiv u_q \wedge u_r \\
&n \equiv n_q \wedge n_r \\
&C \equiv C_q \cup C_r \\
&A \equiv A_q \cup A_r
\end{aligned} \tag{26}$$

Using the equivalences above in (25), predicate calculus, and set algebra, allows us to infer:

$$\begin{aligned}
&\sigma \models u_i \\
&\sigma \models n_i \\
&\sigma' \models n_i \\
&\sigma \restriction_{C_i} = \sigma' \restriction_{C_i}
\end{aligned} \tag{27}$$

for $i \in \{q, r\}$.

Then we can apply induction hypothesis to obtain two environment transitions:

$$(q, \sigma) \overset{A_q}{\dashrightarrow} (q', \sigma') \text{ and } (r, \sigma) \overset{A_r}{\dashrightarrow} (r', \sigma') \tag{28}$$

Using the concrete rule for parallel composition we know that there is a transition:

$$(q \parallel r, \sigma) \overset{A_q \cup A_r}{\dashrightarrow} (q' \parallel r', \sigma)$$

which concludes the proof for this case.

Urgency Case Straightforward using the symbolic rule for urgency, induction hypothesis, and the concrete rule for urgency.

Dynamic Type Case Straightforward using the symbolic rule for dynamic type, induction hypothesis, and the concrete rule for dynamic type.

Synchronization Case Straightforward using the symbolic rule for synchronization, induction hypothesis, and the concrete rule for synchronization.

Control Variable Case Straightforward using the symbolic rule for control variable, the fact that:

$$\sigma \restriction_{C \cup \{x\}} = \sigma' \restriction_{C \cup \{x\}} \Leftrightarrow \sigma \restriction_C = \sigma' \restriction_C \wedge \sigma(x) = \sigma'(x)$$

induction hypothesis, and the concrete rule for control variable.

Initialization Case Straightforward using the symbolic rule for initialization, induction hypothesis, the fact that:

$$(\sigma \models u \wedge u') \Leftrightarrow (\sigma \models u) \wedge (\sigma \models u')$$

and the concrete rule for initialization.

□

2.3 Soundness of Symbolic Time Rules

In the proofs we need the following lemmas.

Lemma 3 (First Term Rule for Join)**.** *For all* $F \in A \rightharpoonup 2^B$ *and* $G \in A \rightharpoonup 2^B$*, and for all* $P \in (A \times 2^B) \rightharpoonup \mathbb{B}$ *we have that:*

$$\langle \forall x :: x \in \mathrm{dom}(F \uplus G) \Rightarrow P(x, (F \uplus G)(x)) \rangle$$

if and only if all of the following predicates hold:

1. $\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, F(x) \cap G(x)) \rangle$
2. $\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \notin \mathrm{dom}(G) \Rightarrow P(x, F(x)) \rangle$
3. $\langle \forall x :: x \notin \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, G(x)) \rangle$

Proof. Straightforward using Definition 1 and Leibniz rule for predicates[2]. □

[2]Leibniz rule states that $A = B \Rightarrow (P(A) \Leftrightarrow P(B))$.

Lemma 4 (Second Term Rule for Join)**.** *For all* $F \in A \rightharpoonup 2^B$ *and* $G \in A \rightharpoonup 2^B$*, and for all* $P \in (A \times 2^B) \rightharpoonup \mathbb{B}$*, such that:*

$$\langle \forall x, X, y, Y :: P(x, X \cap Y) \Leftrightarrow P(x, X) \wedge P(x, Y) \rangle$$

we have that:

$$\langle \forall x :: x \in \mathrm{dom}(F \Cap G) \Rightarrow P(x, (F \Cap G)(x)) \rangle$$

if and only if

$$\langle \forall :: x \in \mathrm{dom}(F) \Rightarrow P(x, F(x)) \rangle \wedge \langle \forall :: x \in \mathrm{dom}(G) \Rightarrow P(x, G(x)) \rangle$$

Proof. Assume $P(x, X \cap Y) \Leftrightarrow P(x, X) \wedge P(x, Y)$, then we make the following derivation:

$\langle \forall x :: x \in \mathrm{dom}(F \Cap G) \Rightarrow P(x, (F \Cap G)(x)) \rangle$

$\Leftrightarrow$ {Lemma 3}

$\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, F(x) \cap G(x)) \rangle \wedge$

$\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \notin \mathrm{dom}(G) \Rightarrow P(x, F(x)) \rangle \wedge$

$\langle \forall x :: x \notin \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, G(x)) \rangle$

$\Leftrightarrow$ {Hypothesis}

$\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, F(x)) \wedge P(x, G(x)) \rangle \wedge$

$\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \notin \mathrm{dom}(G) \Rightarrow P(x, F(x)) \rangle \wedge$

$\langle \forall x :: x \notin \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, G(x)) \rangle$

$\Leftrightarrow$ {Predicate calculus}

$\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, F(x)) \rangle \wedge$

$\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, G(x)) \rangle \wedge$

$\langle \forall x :: x \in \mathrm{dom}(F) \wedge x \notin \mathrm{dom}(G) \Rightarrow P(x, F(x)) \rangle \wedge$

$\langle \forall x :: x \notin \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G) \Rightarrow P(x, G(x)) \rangle$

$\Leftrightarrow$ {Predicate calculus}

$\langle \forall x :: (x \in \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G)) \vee (x \in \mathrm{dom}(F) \wedge x \notin \mathrm{dom}(G)) \Rightarrow P(x, F(x)) \rangle \wedge$

$\langle \forall x :: (x \in \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G)) \vee (x \notin \mathrm{dom}(F) \wedge x \in \mathrm{dom}(G)) \Rightarrow P(x, G(x)) \rangle$

$\Leftrightarrow$ {Predicate calculus}

$\langle \forall x :: x \in \mathrm{dom}(F) \Rightarrow P(x, F(x)) \rangle \wedge \langle \forall x :: x \in \mathrm{dom}(G) \Rightarrow P(x, G(x)) \rangle$

□

Proof of Theorem 3.
We prove Theorem 3 via structural induction on CIF compositions.

Base Case Assume there is an automaton:

$$p \triangleq (V, \text{init}, \text{inv}, \text{tcp}, E, \text{var}_C, \text{act}_S, \text{dtype})$$

and p', u, n, w, G, A, P, U, ρ, θ, and t, such that the following holds:

$$\begin{aligned}
&\langle p \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p' \rangle \\
&\text{dom}(\rho) = \text{dom}(\theta) = [0, t] \wedge 0 < t \\
&\rho(0) \models u \\
&\langle \forall s : s \in [0, t] : \rho(s) \models n \rangle \\
&\langle \forall s : s \in [0, t) : \rho(s) \models w \rangle \\
&\langle \forall x : x \in \text{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle \\
&\langle \forall s : s \in [0, t] : \theta(s) = \{a \mid (g, a) \in P \wedge \rho(s) \models g\} \rangle \\
&\langle \forall s : s \in [0, t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{29}$$

By inspecting the symbolic Rule 3, we have that there must be a $v \in V$ such that:

$$\begin{aligned}
u &\equiv \text{init}(v) \\
n &\equiv \text{inv}(v) \\
w &\equiv \text{tcp}(v) \\
G &\equiv \text{dtype} \\
A &\equiv \text{act}_S \\
P &\equiv \{(g, a) \mid (v, g, a, u, v') \in E\} \\
U &\equiv \emptyset \\
p' &\equiv (V, \text{id}_v, \text{inv}, \text{tcp}, E, \text{var}_C, \text{act}_S, \text{dtype})
\end{aligned} \tag{30}$$

Replacing the equivalences of Equation (30) in Equation (29) yields:

$$\begin{aligned}
&\text{dom}(\rho) = \text{dom}(\theta) = [0, t] \wedge 0 < t \\
&\rho(0) \models \text{init}(v) \\
&\langle \forall s : s \in [0, t] : \rho(s) \models \text{inv}(v) \rangle \\
&\langle \forall s : s \in [0, t) : \rho(s) \models \text{tcp}(v) \rangle \\
&\langle \forall x : x \in \text{dom}(\text{dtype}) : (\rho_x, \rho_{\dot{x}}) \in \text{dtype}(x) \rangle \\
&\langle \forall s : s \in [0, t] : \theta(s) = \\
&\{a \mid (g, a) \in \{(g', a') \mid (v, g', a', u, v') \in E\} \wedge \rho(s) \models g\} \rangle \\
&\langle \forall s : s \in [0, t) : \{g \mid g \in \emptyset \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{31}$$

Using basic properties of set comprehensions we have that:

$$\begin{aligned}
&\{a \mid (g, a) \in \{(g', a') \mid (v, g', a', u, v') \in E\} \wedge \rho(s) \models g\} = \\
&\{a \mid (v, g, a, u, v') \in E \wedge \rho(s) \models g\}
\end{aligned} \tag{32}$$

Thus, using (31) and (32), and concrete rule for time, we can infer that there is a transition:

$$(p, \rho(0)) \overset{\rho, A, \theta}{\longmapsto} (p', \rho(t))$$

which concludes the proof for the base case.

Induction Step

Parallel Composition Case Assume there are compositions q, r such that:

$$p \triangleq q \parallel r$$

and p', u, n, w, G, A, P, U, ρ, and θ, such that the following holds:

$$\begin{aligned}
&\langle p \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p' \rangle \\
&\mathrm{dom}(\rho) = \mathrm{dom}(\theta) = [0, t] \wedge 0 < t \\
&\rho(0) \models u \\
&\langle \forall s : s \in [0, t] : \rho(s) \models n \rangle \\
&\langle \forall s : s \in [0, t) : \rho(s) \models w \rangle \\
&\langle \forall x : x \in \mathrm{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle \\
&\langle \forall s : s \in [0, t] : \theta(s) = \{a \mid (g, a) \in P \wedge \rho(s) \models g\} \rangle \\
&\langle \forall s : s \in [0, t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{33}$$

By inspecting the symbolic Rule 8 for parallel composition, we know that there must be u_i, n_i, w_i, G_i, A_i, P_i, U_i, $i \in \{q, r\}$ such that:

$$\begin{aligned}
&\langle q \rangle \overset{u_q,n_q,w_q,G_q,A_q,P_q,U_q}{\longmapsto} \langle q' \rangle \\
&\langle r \rangle \overset{u_r,n_r,w_r,G_r,A_r,P_r,U_r}{\longmapsto} \langle r' \rangle \\
&p' \equiv q' \parallel r' \\
&u \equiv u_q \wedge u_r \\
&n \equiv n_q \wedge n_r \\
&w \equiv w_q \wedge w_r \\
&G = G_q \barwedge G_r \\
&A = A_q \cup A_r \\
&P \equiv (P_q \cap_2 P_r) \cup (P_q \setminus_2 A_r) \cup (P_r \setminus_2 A_q) \\
&U = U_q \cup U_r
\end{aligned} \tag{34}$$

Replacing in 33 using the equivalences of 34 we get:

$$\begin{aligned}
&\mathrm{dom}(\rho) = \mathrm{dom}(\theta) = [0,t] \wedge 0 < t\\
&\rho(0) \models u_q \wedge u_r\\
&\langle \forall s : s \in [0,t] : \rho(s) \models n_q \wedge n_r \rangle\\
&\langle \forall s : s \in [0,t) : \rho(s) \models w_q \wedge n_r \rangle\\
&\langle \forall x : x \in \mathrm{dom}(G_q \Cap G_r) : (\rho_x, \rho_{\dot{x}}) \in (G_q \Cap G_r)(x) \rangle\\
&\langle \forall s : s \in [0,t] : \theta(s) =\\
&\{a \mid (g,a) \in (P_q \cap_2 P_r) \cup (P_q \setminus_2 A_r) \cup (P_r \setminus_2 A_q) \wedge \rho(s) \models g\} \rangle\\
&\langle \forall s : s \in [0,t) : \{g \mid g \in U_q \cup U_r \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{35}$$

Since:

$$(\rho_x, \rho_{\dot{x}}) \in G_q(x) \cap G_r(x) \Leftrightarrow (\rho_x, \rho_{\dot{x}}) \in G_q(x) \wedge (\rho_x, \rho_{\dot{x}}) \in G_r(x)$$

we can use Lemma 4, and (35) we get:

$$\begin{aligned}
&\langle \forall x : x \in \mathrm{dom}(G_q) : (\rho_x, \rho_{\dot{x}}) \in G_q(x) \rangle \wedge\\
&\langle \forall x : x \in \mathrm{dom}(G_r) : (\rho_x, \rho_{\dot{x}}) \in G_r(x) \rangle
\end{aligned} \tag{36}$$

Using (35), predicate calculus, and set algebra ($A \cup B = \emptyset$ iff $A = \emptyset \wedge B = \emptyset$) we get:

$$\begin{aligned}
&\langle \forall s : s \in [0,t) : \{g \mid g \in U_q \wedge \rho(s) \models g\} = \emptyset \rangle \wedge\\
&\langle \forall s : s \in [0,t) : \{g \mid g \in U_r \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{37}$$

Next, we *define* guard trajectories θ_q, and θ_r such that $\mathrm{dom}(\theta_i) = [0,t]$, and:

$$\langle \forall s : s \in [0,t] : \theta_i(s) = \{a \mid (g,a) \in P_i \wedge \rho(s) \models g\} \rangle \tag{38}$$

where $i \in \{q, r\}$.
Then, using the symbolic transitions of (34), Equations (35), (36), (37), (38), and predicate calculus, we can apply induction hypothesis to infer that there are concrete time transitions:

$$(q, \rho(0)) \overset{\rho, A_q, \theta_q}{\longmapsto} (q', \rho(t)) \wedge (r, \rho(0)) \overset{\rho, A_r, \theta_r}{\longmapsto} (r', \rho(t)) \tag{39}$$

Using the concrete rule for time, and the previous transitions, we can infer that there is a concrete transition:

$$(q \parallel r, \rho(0)) \overset{\rho, A_q \cup A_r, (\theta_q \cap \theta_r) \cup (\theta_q \setminus A_r) \cup (\theta_r \setminus A_q)}{\longmapsto} (q' \parallel r', \rho(t)) \tag{40}$$

Now, in order to conclude the proof for the parallel composition case, we need to show that for all $s \in [0,t]$:

$$\theta(s) = (\theta_p(s) \cap \theta_q(s)) \cup (\theta_p(s) \setminus A_q) \cup (\theta_q(s) \setminus A_q) \tag{41}$$

For proving the precedent equation we derive the following identities. On the one hand we have:

$\theta(s)$
$= \{$Equation (35)$\}$
$\{a \mid (g,a) \in (P_q \cap_2 P_r) \cup (P_q \setminus_2 A_r) \cup (P_r \setminus_2 A_q) \wedge \rho(s) \models g\}$
$= \{$Set algebra (Properties of set builder operators) $\}$
$\{a \mid (g,a) \in (P_q \cap_2 P_r) \wedge \rho(s) \models g\} \cup$
$\{a \mid (g,a) \in (P_q \setminus_2 A_r) \wedge \rho(s) \models g\} \cup$
$\{a \mid (g,a) \in (P_r \setminus_2 A_q) \wedge \rho(s) \models g\}$

On the other hand we have:

$\theta_q(s) \cap \theta_r(s)$
$= \{$Equation (38) (Definition of θ_q and θ_r)$\}$
$\{a \mid (g,a) \in P_q \wedge \rho(s) \models g\} \cap \{a \mid (g,a) \in P_r \wedge \rho(s) \models g\}$
$= \{$Set algebra (Properties of set builder operators) $\}$
$\{a \mid (g_q,a) \in P_q \wedge \rho(s) \models g_q \wedge (g_r,a) \in P_r \wedge \rho(s) \models g_r\}$
$= \{$Predicate calculus$\}$
$\{a \mid (g_q,a) \in P_q \wedge (g_r,a) \in P_r \wedge \rho(s) \models (g_q \wedge g_r)\}$
$= \{$Definition of second component intersection (Definition 2)$\}$
$\{a \mid (g_q \wedge g_r,a) \in (P_q \cap_2 P_r) \wedge \rho(s) \models (g_q \wedge g_r)\}$

Finally we have that:

$\theta_q(s) \setminus A_r$
$= \{$Equation (38) (Definition of θ_q and θ_r)$\}$
$\{a \mid (g,a) \in P_q \wedge \rho(s) \models g\} \setminus A_r$
$= \{$Set algebra (Properties of set builder operators), and definition of second component difference (Definition 3)$\}$
$\{a \mid (g,a) \in (P_q \setminus_2 A_r) \wedge \rho(s) \models g\}$

Similarly it is possible to prove that:

$$\theta_r(s) \setminus A_q = \{a \mid (g,a) \in (P_r \setminus_2 A_q) \wedge \rho(s) \models g\}$$

Putting the last three equalities together we get as a result that Equation (41) holds, and this concludes the proof of soundness for the parallel composition case.

Urgency Case Assume there is a composition q, and an action a such that:

$$p \triangleq \upsilon_a(q)$$

and p', u, n, w, G, A, P, U, ρ, and θ, such that the following holds:

$$\begin{aligned}
&\langle \upsilon_a(q) \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p' \rangle \\
&\mathrm{dom}(\rho) = \mathrm{dom}(\theta) = [0,t] \wedge 0 < t \\
&\rho(0) \models u \\
&\langle \forall s : s \in [0,t] : \rho(s) \models n \rangle \\
&\langle \forall s : s \in [0,t) : \rho(s) \models w \rangle \\
&\langle \forall x : x \in \mathrm{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle \\
&\langle \forall s : s \in [0,t] : \theta(s) = \{a \mid (g,a) \in P \wedge \rho(s) \models g\} \rangle \\
&\langle \forall s : s \in [0,t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{42}$$

By inspecting the symbolic Rule 14 for urgency, the know that there must be a set U' such that:

$$U \equiv U' \cup \{g \mid (g,a) \in P\} \tag{43}$$

And similarly, for some composition q', we have:

$$p' = \upsilon_a(q')$$

Replacing U by its equivalent term in Equation (42), and simplifying (the conjunctions) we obtain:

$$\langle \forall s : s \in [0,t) : \{g \mid g \in U' \cup \{g' \mid (g',a) \in P\} \wedge \rho(s) \models g\} = \emptyset \rangle \tag{44}$$

Using set algebra and predicate calculus we obtain an expression equivalent to the previous equation:

$$\begin{aligned} &\langle \forall s : s \in [0,t) : \{g \mid g \in U' \wedge \rho(s) \models g\} = \emptyset \rangle \wedge \\ &\langle \forall s : s \in [0,t) : \{g \mid g \in \{g' \mid (g',a) \in P\} \wedge \rho(s) \models g\} = \emptyset \rangle \end{aligned} \tag{45}$$

Simplifying further the nested set builder operator yields:

$$\begin{aligned} &\langle \forall s : s \in [0,t) : \{g \mid g \in U' \wedge \rho(s) \models g\} = \emptyset \rangle \wedge \\ &\langle \forall s : s \in [0,t) : \{g \mid (g,a) \in P \wedge \rho(s) \models g\} = \emptyset \rangle \end{aligned} \tag{46}$$

Examining the symbolic rule for urgency we have that there *must* be a transition:

$$\langle q \rangle \overset{u,n,w,G,A,P,U'}{\longmapsto} \langle q' \rangle \tag{47}$$

Using Equation (42), and (46), and induction hypothesis we get that there is a concrete time transition:

$$(q, \rho(0)) \overset{\rho,A,\theta}{\longmapsto} (q', \rho(t)) \tag{48}$$

Next we show that:

$$\begin{aligned} &\langle \forall s : s \in [0,t) : \{g \mid (g,a) \in P \wedge \rho(s) \models g\} = \emptyset \rangle \Leftrightarrow \\ &\langle \forall s : s \in [0,t) : a \notin \theta(s) \rangle \end{aligned} \tag{49}$$

To prove the equivalence above we make the following derivation. Let $s \in [0,t)$, then:

$a \notin \theta(s)$
$\Leftrightarrow$ { Equation (42) (Definition of $\theta(s)$)}
$a \notin \{x \mid (g,x) \in P \wedge \rho(s) \models g\}$
$\Leftrightarrow$ { Set algebra}
$\{a\} \cap \{x \mid (g,x) \in P \wedge \rho(s) \models g\} = \emptyset$
$\Leftrightarrow$ {Set algebra}
$\{x \mid x = a\} \cap \{x \mid (g,x) \in P \wedge \rho(s) \models g\} = \emptyset$
$\Leftrightarrow$ {Set algebra}
$\{x \mid (g,a) \in P \wedge \rho(s) \models g\} = \emptyset$

$\Leftrightarrow$ {Set algebra}
$\{g \mid (g, a) \in P \wedge \rho(s) \models g\} = \emptyset$

Using the transition of (48), Equation (46), and the concrete rule for urgency, we conclude that there is a time transition:

$$(\upsilon_a(q), \rho(0)) \overset{\rho, A, \theta}{\longmapsto} (\upsilon_a(q'), \rho(t))$$

Or equivalently:

$$(\upsilon_a(q), \rho(0)) \overset{\rho, A, \theta}{\longmapsto} (p', \rho(t))$$

Which concludes the proof for this case.

Dynamic type Assume there is a composition q, a variable x, and a dynamic type G such that:

$$p \triangleq \mathrm{D}_{x:G}(q)$$

and p', u, n, w, G, A, P, U, ρ, and θ, such that the following holds:

$$\begin{aligned}
&\langle \mathrm{D}_{x:G}(q) \rangle \overset{u, n, w, G', A, P, U}{\longmapsto} \langle p' \rangle \\
&\mathrm{dom}(\rho) = \mathrm{dom}(\theta) = [0, t] \wedge 0 < t \\
&\rho(0) \models u \\
&\langle \forall s : s \in [0, t] : \rho(s) \models n \rangle \\
&\langle \forall s : s \in [0, t) : \rho(s) \models w \rangle \\
&\langle \forall x : x \in \mathrm{dom}(G') : (\rho_x, \rho_{\dot{x}}) \in G'(x) \rangle \\
&\langle \forall s : s \in [0, t] : \theta(s) = \{a \mid (g, a) \in P \wedge \rho(s) \models g\} \rangle \\
&\langle \forall s : s \in [0, t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{50}$$

By inspecting the symbolic rule for the dynamic type operator (17), we know that there must be a composition q', and a dynamic type D such that:

$$\begin{aligned}
&p' \equiv \mathrm{D}_{x:G}(q') \\
&G' = D \Cap \{(x, G)\} \\
&\langle q \rangle \overset{u, n, w, D, A, P, U}{\longmapsto} \langle q' \rangle
\end{aligned} \tag{51}$$

Using the above equivalences and (50), we get:

$$\langle \forall y : y \in \mathrm{dom}(D \Cap \{(x, G)\}) : (\rho_y, \rho_{\dot{y}}) \in (D \Cap \{(x, G)\})(y) \rangle \tag{52}$$

Applying Lemma 4, the equation above is equivalent to:

$$\begin{aligned}
&\langle \forall y : y \in \mathrm{dom}(D) : (\rho_y, \rho_{\dot{y}}) \in D(y) \rangle \\
&\langle \forall y : y \in \mathrm{dom}(D \Cap \{(x, G)\}) : (\rho_y, \rho_{\dot{y}}) \in (D \Cap \{(x, G)\})(y) \rangle
\end{aligned} \tag{53}$$

Using predicate calculus, the expression above can be simplified to:

$$(\rho_x, \rho_{\dot{x}}) \in G \tag{54}$$

Using (50), (51), (53), and applying induction hypothesis we obtain that there is a concrete transition:

$$(q, \rho(0)) \overset{\rho, A, \theta}{\longmapsto} (q', \rho(t)) \tag{55}$$

and then using (54), and the concrete rule for the dynamic type operator we obtain a concrete transition:

$$(\mathrm{D}_{x:G}(q), \rho(0)) \overset{\rho, A, \theta}{\longmapsto} (\mathrm{D}_{x:G}(q'), \rho(t)) \tag{56}$$

and this concludes the proof for this case.

Synchronization Case Assume there is a composition q, and an action a such that:

$$p \triangleq \gamma_a(q)$$

and p', u, n, w, G, A, P, U, ρ, and θ, such that the following holds:

$$\begin{aligned}
&\langle \gamma_a(q) \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p' \rangle \\
&\mathrm{dom}(\rho) = \mathrm{dom}(\theta) = [0, t] \wedge 0 < t \\
&\rho(0) \models u \\
&\langle \forall s : s \in [0, t] : \rho(s) \models n \rangle \\
&\langle \forall s : s \in [0, t) : \rho(s) \models w \rangle \\
&\langle \forall x : x \in \mathrm{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle \\
&\langle \forall s : s \in [0, t] : \theta(s) = \{a \mid (g, a) \in P \wedge \rho(s) \models g\} \rangle \\
&\langle \forall s : s \in [0, t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{57}$$

By inspecting the symbolic Rule 23 for the synchronization operator, the know that there must be a set A' such that:

$$A \equiv A' \cup \{a\} \tag{58}$$

And similarly, for some composition q', we have:

$$p' = \gamma_a(q')$$

Using the above equivalence, the symbolic transition of (42), and inspecting at the symbolic Rule 23 for the synchronization operator, we get that there is a symbolic transition:

$$\langle q \rangle \overset{u,n,w,G,A',P,U}{\longmapsto} \langle q' \rangle \tag{59}$$

Using the above transition, the predicates of Equation (42), and induction hypothesis we infer that there is a concrete time transition:

$$(q, \rho(0)) \overset{\rho, A', \theta}{\longmapsto} (q', \rho(t)) \tag{60}$$

Applying the concrete rule for synchronization operator we obtain the following time transition:

$$(\gamma_a(q), \rho(0)) \overset{\rho, A' \cup \{a\}, \theta}{\longmapsto} (\gamma_a(q')', \rho(t))$$

Or, equivalently:

$$(\gamma_a(q), \rho(0)) \overset{\rho, A', \theta}{\longmapsto} (p', \rho(t))$$

Which concludes the proof for this case.

Control variable Straightforward using the symbolic rule for control variable, induction hypothesis, and the concrete rule for control variable.

Initialization Straightforward using the symbolic rule for initialization, induction hypothesis, the fact that:

$$(\rho(0) \models u \wedge u') \Leftrightarrow (\rho(0) \models u) \wedge (\rho(0) \models u') \tag{61}$$

and the concrete rule for initialization.

□

2.4 Completeness of Symbolic Action Rules

Proof of Theorem 4. The proof of Theorem 4 goes via structural induction on CIF compositions.

Base Case Assume there is an automaton:

$$p \triangleq (V, \text{init}, \text{inv}, \text{tcp}, E, \text{var}_C, \text{act}_S, \text{dtype})$$

and a, b, X p', σ, and σ', such that there is a transition:

$$(p, \sigma) \xrightarrow{a,b,X} (p', \sigma') \tag{62}$$

Using the previous fact, and inspecting the concrete rules for atomic automata, we know that there exists an edge $(v, g, a, (W, r), v')$ such that:

$$\begin{aligned}
&p' \equiv (V, \text{id}_{v'}, \text{inv}, \text{tcp}, E, \text{var}_C, \text{act}_S, \text{dtype}) \\
&b \equiv a \in \text{act}_S \\
&\sigma \models \text{init}(v) \\
&\sigma \models g \\
&\sigma \models \text{inv}(v) \\
&\sigma' \models \text{inv}(v') \\
&\sigma \restriction_{(\text{var}_C \cup X) \setminus W} = \sigma' \restriction_{(\text{var}_C \cup X) \setminus W} \\
&\sigma'^{+} \cup \sigma \models r
\end{aligned} \tag{63}$$

Using the symbolic rule for atomic automata (Rule 1), we get that there is a symbolic transition:

$$\langle p \rangle \xrightarrow{a, a \in \text{act}_S, g, \text{init}(v), \text{inv}(v), \text{inv}(v'), W, \text{var}_C, r} \langle p' \rangle$$

which concludes the proof for the base case.

Induction Step Parallel Composition Case Assume there are compositions q, r such that:

$$p \triangleq q \parallel r$$

and a, b, X p', σ, and σ' such that there is a concrete transition:

$$(p, \sigma) \xrightarrow{a,b,X} (p', \sigma') \tag{64}$$

We make a case analysis depending on the rule that was applied last.

Concrete rule 4 was applied last Then we know that:

$$\begin{aligned} & p' \equiv q' \parallel r' \\ & b \equiv \text{true} \\ & (q, \sigma) \xrightarrow{a,\text{true},X} (q', \sigma') \\ & (r, \sigma) \xrightarrow{a,\text{true},X} (r', \sigma') \end{aligned} \tag{65}$$

Applying induction hypothesis, we know that there are g_i, u_i, n_i, n'_i, W_i, C_i, r_i, with $i \in \{q, r\}$, such that:

$$\begin{aligned} & \langle q \rangle \xrightarrow{a,\text{true},g_q,u_q,n_q,n'_q,W_q,C_q,r_q} \langle q' \rangle \\ & \langle r \rangle \xrightarrow{a,\text{true},g_r,u_r,n_r,n'_r,W_r,C_r,r_r} \langle r' \rangle \\ & \sigma \models g_i \\ & \sigma \models u_i \\ & \sigma \models n_i \\ & \sigma' \models n'_i \\ & \sigma \restriction_{(C_i \cup X) \setminus W_i} = \sigma' \restriction_{(C_i \cup X) \setminus W_i} \\ & \sigma \cup \sigma'^{+} \models r_i \end{aligned} \tag{66}$$

Using Lemma 2, predicate calculus, and the symbolic rule for synchronizing parallel composition we get:

$$\begin{aligned} & \langle q \parallel r \rangle \xrightarrow{a,\text{true},g_q \wedge g_r,u_q \wedge u_r,n_q \wedge n_r,n'_q \wedge n'_r,W_q \cap W_r,(C_q \setminus W_q) \cup (C_r \setminus W_r),r_q \wedge r_r} \\ & \langle q' \parallel r' \rangle \\ & \sigma \models g_q \wedge g_r \\ & \sigma \models u_q \wedge u_r \\ & \sigma \models n_q \wedge n_r \\ & \sigma' \models n'_q \wedge n'_r \\ & \sigma \restriction_{((C_q \setminus W_q) \cup (C_r \setminus W_r) \cup X) \setminus (W_q \cap W_r)} = \\ & \sigma' \restriction_{((C_q \setminus W_q) \cup (C_r \setminus W_r) \cup X) \setminus (W_q \cap W_r)} \\ & \sigma'^{+} \cup \sigma \models r_q \wedge r_r \end{aligned} \tag{67}$$

which concludes the proof for this case.

Concrete rule 5 was applied last Then we know that for some A:

$$\begin{aligned} & p' \equiv q' \parallel r' \\ & (q, \sigma) \xrightarrow{a,\text{true},X} (q', \sigma') \\ & (r, \sigma) \overset{A}{\dashrightarrow} (r', \sigma') \\ & a \notin A \end{aligned} \tag{68}$$

Applying induction hypothesis we know that there are g, u_q, n_q, n'_q, W, C_q, and s such that:

$$\begin{aligned} & \langle q \rangle \xrightarrow{a,b,g,u_q,n_q,n'_q,W,C_q,s} \langle q' \rangle \\ & \sigma \models g \\ & \sigma \models u_q \\ & \sigma \models n_q \\ & \sigma' \models n'_q \\ & \sigma \restriction_{(C_q \cup X) \setminus W} = \sigma' \restriction_{(C_q \cup X) \setminus W} \\ & \sigma'^{+} \cup \sigma \models s \end{aligned} \tag{69}$$

Using the completeness of environment transitions (Theorem 5), we know that there exists u_r, n_r, and C_r such that:

$$\begin{aligned} & \langle r \rangle \overset{u_r,n_r,C_r,A}{\dashrightarrow} \langle r' \rangle \\ & \sigma \models u_r \\ & \sigma \models n_r \\ & \sigma' \models n_r \\ & \sigma \restriction_{C_r} = \sigma' \restriction_{C_r} \end{aligned} \tag{70}$$

Using predicate calculus, set algebra, and the symbolic rule for interleaving parallel composition (Rule 5) we get:

$$\begin{aligned} & \langle q \parallel r \rangle \xrightarrow{a,b,g,u_q \wedge u_r,n_q \wedge n_r,n'_q \wedge n_r,W \setminus C_r,C_q \cup C_r,s} \langle q' \parallel r' \rangle \\ & \sigma \models u_q \wedge u_r \\ & \sigma \models n_q \wedge n_r \\ & \sigma' \models n'_q \wedge n_r \\ & \sigma \restriction_{(C_q \cup C_r \cup X) \setminus (W \setminus C_r)} = \sigma' \restriction_{(C_q \cup C_r \cup X) \setminus (W \setminus C_r)} \end{aligned} \tag{71}$$

which concludes the proof for this case.

Concrete rule 6 was applied last The proof for this case is symmetrical to the previous one.

Urgency Case Straightforward using the concrete rule for urgency, induction hypothesis, and the symbolic rule for urgency.

Dynamic Type Case Straightforward using the concrete rule for dynamic type, induction hypothesis, and the symbolic rule for dynamic type.

Synchronization Case Straightforward using the concrete rule for synchronization, induction hypothesis, and the symbolic rule for synchronization.

Control Variable Case Straightforward using the concrete rule for control variable, induction hypothesis, and the symbolic rule for control variable.

Initialization Case Straightforward using the concrete rule for initialization, induction hypothesis, the fact that:

$$(\rho(0) \models u \wedge u') \Leftrightarrow (\rho(0) \models u) \wedge (\rho(0) \models u') \tag{72}$$

and the symbolic rule for initialization.

□

2.5 Completeness of Symbolic Environment Rules

Proof of Theorem 5. The proof of Theorem 5 is symmetrical to the proof of soundness given in Section 2.2. □

2.6 Completeness of Symbolic Time Rules

Proof of Theorem 6. The proof of Theorem 6 goes via structural induction on CIF compositions.

Base Case Assume there is an automaton:

$$p \triangleq (V, \text{init}, \text{inv}, \text{tcp}, E, \text{var}_C, \text{act}_S, \text{dtype})$$

and p', ρ, and θ, such that there is a transition:

$$(p, \rho(0)) \overset{\rho, A, \theta}{\longmapsto} (p', \rho(t)) \tag{73}$$

Using the previous fact, and inspecting the concrete rules for atomic automata, we know that there exists $v \in V$ such that:

$$\begin{aligned}
&\rho(0) \models \text{init}(v) \\
&\langle \forall s : s \in [0, t] : \rho(s) \models \text{inv}(v) \rangle \\
&\langle \forall s : s \in [0, t) : \rho(s) \models \text{tcp}(v) \rangle \\
&\langle \forall x : x \in \text{dom}(\text{dtype}) : (\rho_x, \rho_{\dot{x}}) \in \text{dtype}(x) \rangle \\
&\langle \forall s : s \in [0, t] : \theta(s) = \{a | (v, g, a, (W, r), v') \in E \wedge \rho(s) \models g\} \rangle
\end{aligned} \tag{74}$$

We define:

$$P \equiv \{(g, a) \mid \langle \exists u, v' :: (v, g, a, u, v') \in E \rangle\} \tag{75}$$

Then we have that:

$$\{a \mid (v, g, a, (W, r), v') \in E \wedge \rho(s) \models g\} = \{a \mid (g, a) \in P \wedge \rho(s) \models g\} \tag{76}$$

And using predicate calculus, we know that:

$$\langle \forall s : s \in [0,t) : \{g \mid g \in \emptyset \wedge \rho(s) \models g\} = \emptyset \rangle \tag{77}$$

Thus, using the following equivalences:

$$\begin{aligned} u &\equiv \text{init} \\ n &\equiv \text{inv}(v) \\ w &\equiv \text{tcp}(v) \\ G &\equiv \text{dtype} \\ U &\equiv \emptyset \end{aligned}$$

And using (74), (76), (77), and the symbolic rule 3, we get:

$$\begin{aligned} &\langle p \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle p' \rangle \\ &\rho(0) \models u \\ &\langle \forall s : s \in [0,t] : \rho(s) \models n \rangle \\ &\langle \forall s : s \in [0,t) : \rho(s) \models w \rangle \\ &\langle \forall x : x \in \text{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle \\ &\langle \forall s : s \in [0,t] : \theta(s) = \{a \mid (g,a) \in P \wedge \rho(s) \models g\} \rangle \\ &\langle \forall s : s \in [0,t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle \end{aligned}$$

Induction Step Parallel Composition Case Assume there are compositions q, r such that:

$$p \triangleq q \parallel r$$

and p', A, ρ, and θ, such that there is a concrete transition:

$$(p, \rho(0)) \overset{\rho,A,\theta}{\longmapsto} (p', \rho(t)) \tag{78}$$

Inspecting the concrete rule for parallel composition we know that there must be A_q, A_r, θ_q, θ_r, q', r' such that the following holds:

$$\begin{aligned} &(q, \rho(0)) \overset{\rho,A_q,\theta_q}{\longmapsto} (q', \rho(t)) \\ &(r, \rho(0)) \overset{\rho,A_r,\theta_r}{\longmapsto} (r', \rho(t)) \\ &A \equiv A_q \cup A_r \\ &\theta = (\theta_q \cap \theta_r) \cup (\theta_q \setminus A_r) \cup (\theta_r \setminus A_q) \\ &p' = q' \parallel r' \end{aligned} \tag{79}$$

Using induction hypothesis we know that there exists u_i, n_i, w_i, G_i,

P_i, and U_i, where $i \in \{q, r\}$ such that the following conditions hold:

$$\begin{aligned}
&\langle q \rangle \overset{u_q, n_q, w_q, G_q, A_q, P_q, U_q}{\longmapsto} \langle q' \rangle \\
&\langle r \rangle \overset{u_r, n_r, w_r, G_r, A_r, P_r, U_r}{\longmapsto} \langle r' \rangle \\
&\rho(0) \models u_i \\
&\langle \forall s : s \in [0, t] : \rho(s) \models n_i \rangle \\
&\langle \forall s : s \in [0, t) : \rho(s) \models w_i \rangle \\
&\langle \forall x : x \in \mathrm{dom}(G_i) : (\rho_x, \rho_{\dot{x}}) \in G_i(x) \rangle \\
&\langle \forall s : s \in [0, t] : \theta_i(s) = \{a \mid (g, a) \in P_i \wedge \rho(s) \models g\} \rangle \\
&\langle \forall s : s \in [0, t) : \{g \mid g \in U_i \wedge \rho(s) \models g\} = \emptyset \rangle
\end{aligned} \tag{80}$$

Applying the symbolic rule for time (Rule 8) we know that there is a symbolic transition:

$$\begin{aligned}
&\langle p \parallel q \rangle \overset{u_p \wedge u_q, n_p \wedge n_q, w_p \wedge w_q, G_p \barwedge G_q, A_p \cup A_q, (P \cap_2 Q) \cup (P \setminus_2 A_q) \cup (Q \setminus_2 A_p), U_p \cup U_q}{\longmapsto} \\
&\langle p' \parallel q' \rangle
\end{aligned} \tag{81}$$

So we have to prove conditions 2-7 of the completeness theorem. Using Lemma 4, and (80) we get that:

$$\langle \forall x : x \in \mathrm{dom}(G_q \barwedge G_r) : (\rho_x, \rho_{\dot{x}}) \in G_q(x) \barwedge G_r \rangle \tag{82}$$

In Section 2.3 we have seen that:

$$\begin{aligned}
&(\theta_q \cap \theta_r) \cup (\theta_q \setminus A_r) \cup (\theta_r \setminus A_q)(s) = \\
&\{a \mid (g, a) \in ((P_q \cap_2 P_r) \cup (P_q \setminus_2 A_r) \cup (P_r \setminus_2 A_q)) \wedge \rho(s) \models g\}
\end{aligned} \tag{83}$$

when:

$$\langle \forall s : s \in [0, t] : \theta_i(s) = \{a \mid (g, a) \in P_i \wedge \rho(s) \models g\} \rangle \tag{84}$$

for $i \in \{p, r\}$. Since this is the case, Equation (83) holds in this case, and therefore we can infer that:

$$\begin{aligned}
&\langle \forall s : s \in [0, t] : \theta(s) = \\
&\{a \mid (g, a) \in (P_q \cap_2 P_r) \cup (P_q \setminus_2 A_r) \cup (P_r \setminus_2 A_q) \wedge \rho(s) \models g\} \rangle
\end{aligned} \tag{85}$$

Using (80), predicate calculus, and set algebra we have that:

$$\langle \forall s : s \in [0, t) : \{g \mid g \in U_q \cup U_r \wedge \rho(s) \models g\} = \emptyset \rangle \tag{86}$$

The remaining conditions are straightforward to verify, and this concludes the proof of completeness for the parallel composition case.

Urgency Case Assume there is a composition q, and an action a such that:

$$p \triangleq \upsilon_a(q)$$

and p', ρ, A, θ such that there is a concrete transition:

$$(p, \rho(0)) \overset{\rho,A,\theta}{\longmapsto} (p', \rho(t)) \tag{87}$$

Inspecting the concrete rule for urgency, we know that there must be another transition:

$$(q, \rho(0)) \overset{\rho,A,\theta}{\longmapsto} (q', \rho(t)) \tag{88}$$

such that:

$$\begin{aligned} & p' = \upsilon_a(q') \\ & \langle \forall s : s \in [0,t) : a \notin \theta(s) \rangle \end{aligned} \tag{89}$$

Applying inductive hypothesis, we know that there exists u, n, w, G, P, U, and t such that the following conditions hold:

$$\begin{aligned} & \langle q \rangle \overset{u,n,w,G,A,P,U}{\longmapsto} \langle q' \rangle \\ & \rho(0) \models u \\ & \langle \forall s : s \in [0,t] : \rho(s) \models n \rangle \\ & \langle \forall s : s \in [0,t) : \rho(s) \models w \rangle \\ & \langle \forall x : x \in \mathrm{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle \\ & \langle \forall s : s \in [0,t] : \theta(s) = \{a \mid (g,a) \in P \wedge \rho(s) \models g\} \rangle \\ & \langle \forall s : s \in [0,t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle \end{aligned} \tag{90}$$

Using the symbolic rule for urgency 14, we obtain the following transition:

$$\langle \upsilon_a(q) \rangle \overset{u,n,w,G,A,P,U \cup \{g \mid (g,a) \in P\}}{\longmapsto} \langle \upsilon_a(q') \rangle \tag{91}$$

Thus we have all the conditions needed, except for:

$$\langle \forall s : s \in [0,t) : \{g \mid g \in U \cup \{g | (g,a) \in P\} \wedge \rho(s) \models g\} = \emptyset \rangle \tag{92}$$

As we prove in Section 2.3, the previous expression is equivalent to:

$$\begin{aligned} & \langle \forall s : s \in [0,t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle \wedge \\ & \langle \forall s : s \in [0,t) : \{g \mid (g,a) \in P \wedge \rho(s) \models g\} = \emptyset \rangle \end{aligned} \tag{93}$$

The first part of the previous conjunction can be inferred from (90), and then we only need to prove the last part of the conjunction to complete the proof for this case.
In Section 2.3 we proved that:

$$\begin{aligned} & \langle \forall s : s \in [0,t) : \{g \mid (g,a) \in P \wedge \rho(s) \models g\} = \emptyset \rangle \Leftrightarrow \\ & \langle \forall s : s \in [0,t) : a \notin \theta(s) \rangle \end{aligned} \tag{94}$$

provided that:

$$\langle \forall s : s \in [0,t] : \theta(s) = \{a \mid (g,a) \in P \wedge \rho(s) \models g\} \rangle \tag{95}$$

Since this is ensured by (90), and since we assumed (89) we conclude that the second part of the conjunction in (93) is valid, and this completes the case for the urgent operator case.

Dynamic Type Case The proof for this case is symmetrical to the one given for the dynamic type case of the proof of soundness.

Synchronization Case Assume there is a composition q, and an action a such that:

$$p \triangleq \gamma_a(q)$$

and p', ρ, A, θ such that there is a concrete transition:

$$(p, \rho(0)) \overset{\rho, A, \theta}{\longmapsto} (p', \rho(t)) \tag{96}$$

Inspecting the concrete rule for synchronization, we know that there must be a concrete transition:

$$(q, \rho(0)) \overset{\rho, A', \theta}{\longmapsto} (q', \rho(t)) \tag{97}$$

such that:

$$\begin{aligned} p' &= \gamma_a(q') \\ A &= A' \cup \{a\} \end{aligned} \tag{98}$$

By induction hypothesis we know that there exists u, n, w, G, P, U, and t such that the following conditions hold:

$$\begin{aligned} &\langle q \rangle \overset{u, n, w, G, A', P, U}{\longmapsto} \langle q' \rangle \\ &\rho(0) \models u \\ &\langle \forall s : s \in [0, t] : \rho(s) \models n \rangle \\ &\langle \forall s : s \in [0, t) : \rho(s) \models w \rangle \\ &\langle \forall x : x \in \mathrm{dom}(G) : (\rho_x, \rho_{\dot{x}}) \in G(x) \rangle \\ &\langle \forall s : s \in [0, t] : \theta(s) = \{a \mid (g, a) \in P \wedge \rho(s) \models g\} \rangle \\ &\langle \forall s : s \in [0, t) : \{g \mid g \in U \wedge \rho(s) \models g\} = \emptyset \rangle \end{aligned} \tag{99}$$

And using the symbolic rule for synchronization (Rule 23), we know that there is a symbolic transition:

$$\langle \gamma_a(q) \rangle \overset{u, n, w, G, A' \cup \{a\}, P, U}{\longmapsto} \langle \gamma_a(q') \rangle \tag{100}$$

Which concludes the proof for this case.

Control Variable Case Straightforward using the concrete rule for control variable, induction hypothesis, and the symbolic rule for control variable.

Initialization Case Straightforward using the concrete rule for initialization, induction hypothesis, Equation 72, and the symbolic rule for initialization.

□

References