1 SOS rules for top level CIF models

To prove the main theorem we need to define SOS rules for translatable CIF compositions.

We use notation $M_{p,u}$ to refer to the CIF composition:

|[disc control xs
; disc ys
; clock ys
; init u
; urgent as
:: p]|

For action transitions we define the following rule.

$$\frac{(p,\sigma) \xrightarrow{a,b,(xs +\!\!+ cs)} (p',\sigma'), \sigma \models u}{(M_{p,u},\sigma) \xrightarrow{a,b,\emptyset} (M_{p',\mathrm{true}},\sigma')}\ 1$$

For time transitions we define the following rule.

$$\frac{\begin{array}{c}(p,\sigma) \overset{\rho,A,\theta}{\longmapsto} (p',\sigma'),\\ \langle \forall s : s \in \mathrm{dom}(\theta) : as \cap \theta(s) = \emptyset \rangle,\\ \langle \forall x : x \in xs \cup ys : (\rho_x, \rho_{\dot{x}}) \in G_{disc} \rangle,\\ \langle \forall c : c \in cs : (\rho_c, \rho_{\dot{c}}) \in G_{clock} \rangle,\\ \sigma \models u\end{array}}{(M_{p,u},\sigma) \overset{\rho,A,\theta}{\longmapsto} (M_{p'\mathrm{true}},\sigma')}\ 2$$

Environment transitions are not relevant in the context of the present work.

2 Additional notations

Given a composition p, function application $actv(p)$ returns a sequence $xs +\!\!+ [l_u]$, where xs is the sequence of all the active locations of the automata contained in p, and l_u is the unique location of the receptive automaton.

In what follows, given a list xs we use also notation xs as a shorthand for $\mathrm{ran}(xs)$ when no confusion arises.

Given a list of variables $xs = [x_0, \ldots, x_{n-1}]$ and a list of expressions $es = [e_0, \ldots, e_{n-1}]$, we use notation $xs = es$ to refer to the predicate

$$\langle \forall i : 0 \leq i < n : x_i = e_i \rangle$$

Similarly, $xs^+ = es$ denotes the predicate

$$\langle \forall i : 0 \leq i < n : x_i^+ = e_i \rangle$$

Making some abuse of notation, we use expression $xs = es$ to refer to the sequence of assignments

$$[x_0 = e_0, \ldots, x_{n-1} = e_{n-1}]$$

and expression $xs = es^-$ to refer to the sequence of assignments

$$[x_0 = e_0^-, \ldots, x_{n-1} = e_{n-1}^-]$$

In the present work it clear when one or the other is intended.

3 Additional properties

In this section we present additional properties needed for proving the main theorem.

Lemma 1 (Translatable updates and assignments)**.** *For any translatable update of the form* $(zs, zs^+ = es)$*, for any valuations* σ*,* σ'*, such that* $\mathrm{dom}(\sigma) = \mathrm{dom}(\sigma')$ *and* $\langle \forall x : x \in \mathrm{dom}(\sigma) : \sigma(x) = \sigma'(x) \rangle$*, we have that*

$$\sigma'^+ \cup \sigma \models zs^+ = es \Leftrightarrow (zs = es^-)(\sigma) = \sigma'$$

4 The proof of the theorem

Let $M_{p,u}$ be a translatable composition. Then $M_{p,u}$ is of the form

|[disc control xs
; disc ys
; clock ys
; init u
; urgent as
:: $\alpha_{0_0} \parallel \ldots \parallel \alpha_{0_{n-1}}$]|

We have to show $M_{p,u} \leftrightarrows \mathcal{T}(M_{p,u})$. For this we need to find a bisimulation relation R such that:

$$(M_{p,u}, actv(\mathcal{T}(M_{p,u})))$$

Or equivalently, by definition of function $actv()$ for CIF compositions, and by definition of $\mathcal{T}$:

$$(M_{p,u}, actv(M_{p,u}))$$

We define relation R as follows.

$$\begin{aligned} R \triangleq & \{(M_{p,u}, actv(M_{p,u}))\} \cup \\ & \{(p, actv(p)) \mid \langle \exists \sigma, \sigma', n, p_0, \rho, A, \theta :: [\![M_{p,u}]\!] \vdash (p_0, \sigma) \overset{\rho, A, \theta}{\longmapsto} (p, \sigma') \rangle\} \cup \\ & \{(p, actv(p)) \mid \langle \exists \sigma, \sigma', n, p_0, a, b :: [\![M_{p,u}]\!] \vdash (p_0, \sigma) \xrightarrow{a, b, \emptyset} (p, \sigma') \rangle\} \end{aligned}$$

Next we prove that R is indeed a bisimulation relation (as defined in our paper). We do so by checking that the for transfer conditions are satisfied.

Condition 1 Assume $(p, actv(p)) \in R$, and

$$[\![M_{p,u}]\!] \vdash (p, \sigma) \xrightarrow{a,b,\emptyset} (p', \sigma') \tag{1}$$

Note that since p is in the transition system induced by $M_{p,u}$, p is of the form

|[disc control xs
; disc ys
; clock ys
; init u
; urgent as
:: $\alpha_0 \parallel \ldots \parallel \alpha_{n-1}$]|

where α_i and α_{i_0} may differ only in their initial locations.

Assume $\mathcal{T}(M_{p,u}) = \langle \overline{A}, [l_0, \ldots, l_{n-1}], V, C, H, T_H, \mathcal{T}_i(u) \rangle$, where all the components are as in the definition of $\mathcal{T}$.

We have to do a case analysis depending on whether a is declared as urgent in $M_{p,u}$, and depending on the value of b.

Case a is urgent and $\neg b$ Under this assumption, given that the model consists of a parallel composition of n automata (the model is translatable), we know that only one of these could have performed the action. Thus we get the following facts.

There is an index i, such that $0 \leq i < n$, α_i is of the shape

$$(L_i, \mapsto l_i, \mathrm{inv}_i, \mathrm{tcp}_i, E_i, \mathrm{var}_{Ci}, \mathrm{act}_{Si}, \mathrm{dtype}_i)$$

and the following holds.

$$\begin{aligned} (l_i, g, a, (zs, zs^+ = es), l_i') &\in E_i \\ \sigma &\models g \\ \sigma &\models \mathrm{inv}_i(l_i') \\ \sigma'^+ \cup \sigma &\models zs^+ = es \\ \langle \forall x : x \in (xs \cup \mathrm{var}_{Ci}) \setminus zs : \sigma(x) = \sigma'(x) \rangle & \end{aligned} \tag{2}$$

All the remaining automata performed an environment transition. This is, for all j, $0 \leq j < n$ such that $j \neq i$, assuming α_j is of the shape

$$(L_j, \mapsto l_j, \mathrm{inv}_j, \mathrm{tcp}_j, E_j, \mathrm{var}_{Cj}, \mathrm{act}_{Sj}, \mathrm{dtype}_j)$$

we have that

$$\begin{aligned} \sigma' &\models \mathrm{inv}_i(l_j) \\ \langle \forall x : x \in \mathrm{var}_{Cj} : \sigma(x) = \sigma'(x) & \end{aligned} \tag{3}$$

Using the above facts, we have that $actv(p') = actv(p)[l'_i/l_i]$.

According to the definition of the transformation function, we have an edge $(l_i, g, a!, zs = es^-, l'_i) \in E'_i$, where the UPPAAL automaton A_i is of the shape $(L_i, l_{i_0}, E'_i, \text{inv}_i, T_{L_i})$.

Since a is an urgent action, we know that there is an edge $(l_u, \text{true}, a?, [], l_u)$ in the receptive automaton.

From (2) we know that[1]:

$$\langle \forall x : x \in \text{dom}(\sigma) \setminus zs : \sigma(x) = \sigma'(x) \rangle \tag{4}$$

Thus using Lemma 1 we get that:

$$(zs = es^-)(\sigma) = \sigma' \tag{5}$$

Since guard g is satisfied in σ, all the invariants of locations $\text{init}(M_{p,u})$ are satisfied in σ', there are no committed locations, and the assignment in the edge $(l_i, g, a!, zs = es^-, l'_i)$ transform σ into σ', we have communication with the receptive automaton can take place, and thus we get:

$$[\![\mathcal{T}(M_{p,u})]\!] \vdash (actv(p), \sigma) \xrightarrow{a} (actv(p'), \sigma')$$

Case a is urgent and b In this case we have that the synchronizing action a was executed synchronously by exactly two partners, by definition of translatable model. The proof that there is a transition

$$[\![\mathcal{T}(M_{p,u})]\!] \vdash (actv(p), \sigma) \xrightarrow{a} (actv(p'), \sigma')$$

goes very much along the lines of the previous case.

Case a is not urgent The proof for this case is similar to the previous ones. For non-synchronizing actions we use UPPAAL rules for internal transitions instead of rules for channels.

Condition 2 Assume there is a transition

$$[\![\mathcal{T}(M_{p,u})]\!] \vdash (actv(p), \sigma') \xrightarrow{a} (l', \sigma')$$

We have to do a case analysis depending on whether a is an (internal) action or a channel.

Internal action Then we have that there is an atomic UPPAAL automaton A_i, $A_i = (L_i, l_{i_0}, E'_i, \text{inv}'_i, T_{L_i})$, such that

$$\begin{aligned} (l_i, g, a, zs = es) &\in E_i \\ \sigma &\models g \\ (zs = es)(\sigma) = \sigma' &\models \text{inv}_i(l'_i) \\ \langle \forall j : 0 \leq j < n \wedge j \neq i : \sigma' \models \text{inv}_j(l_j) \rangle l' &= \text{init}(p)[l'_i/l_i] \end{aligned} \tag{6}$$

[1]Remember that $\text{dom}(\sigma)$ contains exactly all variables declared in the model

Where we assume l_j to be the active location if automaton A_j, for all j, such that $0 \leq j < n$.

According (6), we know that there must be an edge $(l_i, g, a, zs^+ = es')$ in α_i, where $es'^- = es$.

By definition of UPPAAL assignment, we know that only the clocks and variables being assigned change, thus we can use Lemma 1 to infer:

$$\sigma'^+ \cup \sigma \models zs^+ = es' \tag{7}$$

Thus, automaton α_i can perform an action transition

$$(\alpha_i, \sigma) \xrightarrow{a,\text{false},xs \cup cs} (\alpha_i', \sigma')$$

where α_i' is the same automaton as α_i, except that the initial location is changed to l_i'.

Since, by definition of translatable model, all assigned variables in automaton α_i are not controlled in the other automata, and since, by (6), the invariants of all the active locations in p are satisfied, we have that all the other automata α_j, $j \neq i$ can perform environment transitions

$$(\alpha_j, \sigma) \overset{\text{act}_{S_j}}{\dashrightarrow} (\alpha_j, \sigma')$$

As a consequence, p can perform an action transition

$$(p, \sigma) \xrightarrow{a,\text{false},\emptyset} (p', \sigma')$$

where $p' = p[\alpha_i'/\alpha_i]$, and thus $actv(()p') = l'$, thus $(p', l') \in R$, which concludes the proof.

Communication If the receptive automaton is involved in the communication action, then one of the A_i's performed a send action. The conditions for this send action are similar to those of (6), and thus, using a similar reasoning as in the precious case we can conclude that there is a corresponding action transition in p.

If the receptive automaton is not involved, then we have a communication action between two UPPAAL automata A_i and A_j, and the proofs is similar to the case of synchronizing actions for the CIF automata.

Condition 3 Assume there is a transition

$$[\![M_{p,u}]\!] \vdash (p, \sigma) \overset{\rho,A,\theta}{\longmapsto} (p', \sigma')$$

where $\text{dom}(\rho) = [0, t]$ for some $t \in \mathbb{T}$.

As stated before, note that since p is in the transition system induced by $M_{p,u}$, p is of the form

|[disc control xs
; disc ys
; clock ys
; init u
; urgent as
:: $\alpha_0 \parallel \ldots \parallel \alpha_{n-1}$]|

where α_i and α_{i_0} may differ only in their initial locations.

According to the SOS rules defined in Section 1, we have that

$$\begin{aligned}(\alpha_0 \parallel \ldots \parallel \alpha_{n-1}, \sigma) \overset{\rho, A, \theta}{\longmapsto} (\alpha_0 \parallel \ldots \parallel \alpha_{n-1}, \sigma') \\ \langle \forall s : s \in [0, t] : as \cap \theta(s) = \emptyset \rangle \\ \langle \forall x : x \in xs \cup ys : (\rho_x, \rho_{\dot{x}}) \in G_{disc} \rangle \\ \langle \forall c : c \in cs : (\rho_c, \rho_{\dot{c}}) \in G_{clock} \rangle \end{aligned} \tag{8}$$

Note that the time transition does not change the active locations of the automata involved in the parallel composition.

Consider state $(actv(p), \sigma)$. From the definition of function $\mathcal{T}$, we know that there are no automata in an committed location. Similarly, from (8), given the fact that a time transition is possible in the parallel composition of automata, we know that there cannot be any UPPAAL automaton in an urgent location, since that would imply that there is a corresponding CIF in which the tcp predicate is false.

Next, we show that synchronization over urgent channels is not possible. If we assume in the UPPAAL automaton there are 2 edges $(l_i, g_i, a!, r_s, l_i') \in E_i'$ and $(l_j, g_j, a!, r_s, l_j') \in E_j'$ such that $\sigma \models g_i \wedge g_j$. But this implies that $a \in \theta(0)$[2], which contradicts the fact that a p did a time transition. Thus, synchronization between urgent channels cannot take place.

Furthermore, from (8) and the facts that the invariants are preserved by the transformation function, it is easy to see that the invariants of the active locations in $actv(p)$ are satisfied during the time delay.

Finally, we have to see that in the new valuation the clocks are incremented by t time units, and that the values of variables remain constant during the delay. This follows easily from Rule 2, and the definition of the dynamic types G_{disc} and G_{clock}. This is, for every clock c we have $\sigma'(c) = \sigma(c) + t$, and for every variable x we have $\sigma(x) = \sigma'(x)$.

Putting these facts together, we have that in the transition systems induced by $\mathcal{T}(M_{p,u})$ a time transition of t time units is possible, since all the requirements are satisfied. This is, we have a transition

$$[\![\mathcal{T}(M_{p,u})]\!] \vdash (actv(p), \sigma) \overset{t}{\longmapsto} (actv(p), \sigma')$$

which concludes the proof of transfer condition 3.

[2]Note that we are also taking into account the receptive automaton case.

Condition 4 Assume there is a transition

$$[\![\mathcal{T}(M_{p,u})]\!] \vdash (actv(p), \sigma) \xrightarrow{t} (actv(p'), \sigma')$$

Considering the definition of function $\mathcal{T}$, this means that in the network of automata $\mathcal{T}(M_{p,u})$ we have that:

1. No process is in a committed location.
2. No process is in an urgent location.
3. No synchronization is possible over an urgent channel.
4. All invariants are satisfied during the time delay.
5. The new valuation advances the clocks t time units, and the values of variables are not changed.

From the above we get that, since no process is in a urgent location, the tcp predicate is true for all the corresponding locations in p. Similarly, we have that all the invariants are satisfied in the active locations of p during the delay.

Thus, every $\alpha_i \in p$ can do a time delay

$$(\alpha_i, \sigma) \overset{\rho, \mathrm{act}_{Si}, \theta}{\longmapsto} (\alpha_i, \sigma')$$

where

$$\begin{aligned} \mathrm{dom}(\rho) &= [0, t] \\ \langle \forall s, s', x : s, s' \in [0, t] \wedge x \in V : \rho(s)(x) = \rho(s')(x) \rangle & \\ \langle \forall s, c : s \in [0, t] \wedge c \in C : \rho(s)(c) == \rho(0)(c) + s \rangle & \end{aligned} \tag{9}$$

and θ is constructed from ρ, using the SOS rules for atomic automata.

Since no urgent channel is enabled in valuation $\sigma = \rho(0)$, we have that

$$as \cap (\theta(0)) = \emptyset \tag{10}$$

Given the fact that the guard for urgent trajectories do not change over time (since it is not allowed to contain clocks), from (10) we conclude that

$$\langle \forall s : s \in [0, t] : as \cap (\theta(s)) = \emptyset \rangle$$

It is also clear from (9) that ρ satisfies the dynamic type constraints. Thus, from the above facts we can conclude that there is a time transition

$$[\![\mathcal{T}(M_{p,u})]\!] \vdash (p, \sigma) \overset{\rho, A, \theta}{\longmapsto} (p, \sigma')$$

where $A = \mathrm{act}_{S0} \cup \ldots \cup \mathrm{act}_{Sn-1}$. And this concludes the proof.