A Omitted Proofs

We present the proof for Theorem 2 in the TACAS submission. We first need to define several definitions.

Given a parameterized system instance $sys(\bar{k}_t)$ and state $s \in S$ where S is the set of states in $sys(\bar{k}_t)$, we use $q_{i_p}(s)$ and $e_{i_p}(s)$ to denote the state of process i_p in the system state s, and the set of outstanding events of process i_p in the system state s, respectively, where $p \in [1,t]$ and $i \in [1,k_p]$.

Definition 1 (Projection on Processes). *Given a system specification $\Lambda = \{\Lambda_1,\ldots,\Lambda_t\}$ with t types of processes and a parameterized system instance $sys(\bar{k}_t) = (S, S_I, T, \Gamma(\bar{k}_t))$ where $\bar{k}_t = k_1,\ldots,k_t$, k_l denotes the number of processes of type $l \in [1,t]$ and given a set $R \subseteq \{i_p \mid i \in [1,k_p] \ \wedge\ p \in [1,t]\}$, the projected behavior of $sys(\bar{k}_t)$ w.r.t. R is denoted by $sys(\bar{k}_t){\downarrow}R = (S{\downarrow}R, S_I{\downarrow}R, T{\downarrow}R, \Gamma(\bar{k}_t))$, such that:*

- ◇ $S{\downarrow}R \subseteq \bigcup_{i_p\in R, s\in S} \{q_{i_p}(s)\} \times \bigcup_{i_p\in R, s\in S} \{e_{i_p}(s)\}$
- ◇ $S_I{\downarrow}R \subseteq \bigcup_{i_p\in R, s\in S_I} \{q_{i_p}(s)\} \times \bigcup_{i_p\in R, s\in S_I} \{e_{i_p}(s)\}$
- ◇ $s{\downarrow}R \overset{e/e'}{\rightarrow} s'{\downarrow}R \in T{\downarrow}R$ *if* $s \overset{e/e'}{\rightarrow} s' \in T \ \wedge\ q_{i_p}(s) \neq q_{i_p}(s') \ \wedge\ i_p \in R$.
- ◇ $s{\downarrow}R \overset{\tau}{\rightarrow} s'{\downarrow}R \in T{\downarrow}R$ *if* $s \overset{e/e'}{\rightarrow} s' \in T \ \wedge\ q_{i_p}(s) = q_{i_p}(s') \ \wedge\ i_p \in R$.

Given a path of receive/send actions with τ events, the corresponding sequence $\pi_{-\tau}$ is obtained by removing τ events from π as follows: $\forall i \geq 0, \pi_{-\tau}[i] = \pi[g(i)]$ where

$$g(i) = \begin{cases} 0 \text{ if } i < 0 \\ k \text{ otherwise; } g(i-1) \leq j < k : \pi[j] = \tau \wedge \pi[k] \neq \tau \end{cases} \tag{1}$$

We define $\textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}R, S_I)$ as the path of receive/send actions filtered from any τ events. Formally, $\textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}R, S_I) = \{\pi_{-\tau} \mid \pi \in \textsc{Path}(sys(\bar{k}_t){\downarrow}R, S_I) \ \wedge\ \forall i \geq 0, \pi_{-\tau}[i] = \pi[g(i)]\}$.

In the following, we define the sequence of states in a system as $s_0 s_1 \ldots$. We will use $s[i]$ to denoted the i-th state in the sequence of states.

Given a path $\pi \in sys(\bar{k}_t)$, we define the set of corresponding sequence of states as $\mathtt{Seq}(\pi) = \{s_0 s_1 \ldots \mid s_0 \in S_I \ \wedge\ \forall i \geq 0, s_i \overset{\pi[i]}{\rightarrow} s_{i+1} \in T\}$.

Given a path $\pi_{-\tau} \in \textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}R, S_I)$, we define the corresponding sequence of states in $sys(\bar{k}_t)$ as $\mathtt{Seq}(\pi_{-\tau}) = \{\gamma_0\gamma_1 \ldots \mid \gamma_0 = s_0 \in S_I{\downarrow}R \ \wedge\ \forall i \geq 0, \gamma[i] = s[h(i)] \in S{\downarrow}R\}$ where

$$h(i) = \begin{cases} 0 \text{ if } i < 0 \\ k \text{ otherwise; } g(i-1) \leq j < k : s[j] \overset{\tau}{\rightarrow} s[j+1] \in T{\downarrow}R \wedge \\ \qquad\qquad s[k] \overset{e/e'}{\rightarrow} s[k+1] \in T{\downarrow}R \ \wedge\ \pi[i]_{-\tau} = e/e' \end{cases} \tag{2}$$

Proposition 1. *Given a parameterized system instance $sys(\bar{k}_t) = (S, S_I, T, \Gamma(\bar{k}_t))$ with t different types of processes, where $\bar{k}_t = k_1,\ldots,k_t$, k_l denotes the number of* *processes of type $l \in [1,t]$ and given a set $R \subseteq \{i_p \mid i \in [1,k_p] \ \wedge \ p \in [1,t]\}$, let $\pi \in \textsc{Path}(sys(\bar{k}_t), S_I)$ be a sequence of receive/send events and $\pi_{-\tau}$ the corresponding sequence of events in $\textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}R, S_I{\downarrow}R)$. The following holds for all $\mathtt{LTL}\backslash\mathtt{X}$ properties φ defined over the states of processes with indexes in R: $\mathtt{Seq}(\pi) \models \varphi \Leftrightarrow \mathtt{Seq}(\pi_{-\tau})$.*

Proof. For every sequence of states in $\mathtt{Seq}(\pi)$, the same sequence of states exists in $\mathtt{Seq}(\pi_{-\tau})$ except from the states where the states of the processes in R are not affected. Therefore, every sequence of states existing in $\mathtt{Seq}(\pi)$ that satisfies a property φ, there will be the same sequence of states in $\mathtt{Seq}(\pi_{-\tau})$ but filtered from states not affecting the satisfaction of the property. Similarly, for every sequence of states in $\mathtt{Seq}(\pi_{-\tau})$, there will exist a sequence in $\mathtt{Seq}(\pi)$ with more states that do not affect the states of the processes in R. Therefore $\mathtt{Seq}(\pi) \models \varphi \Leftrightarrow \mathtt{Seq}(\pi_{-\tau})$. ∎

Proposition 2. *Given a system specification $\Lambda = \{\Lambda_1, \ldots, \Lambda_t\}$ with t types of processes, let $R = \{i_{p_1}, j_{p_2}\}$ such that i_{p_1} and j_{p_2} are adjacent processes in $\Gamma(\bar{k}_t)$ and $i \in [1, k_{p_1}]$, $j \in [1, k_{p_2}]$ and $p_1, p_2 \in [1,t]$. For all property φ defined over the states of adjacent processes of type p_1 and p_2, the following holds for any two parameterized system instances, $sys(\bar{k}_t)$ and $sys(\bar{k}'_t)$, where $\bar{k'}_t \geq \bar{k}_t$, for any $R' = \{i'_{p_1}, j'_{p_2}\}$, where $i' \in [1, k'_{p_1}]$, $j' \in [1, k'_{p_2}]$ and i'_{p_1}, j'_{p_2} are adjacent processes in $\Gamma(\bar{k'}_t)$*

$$\textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}R, S_I^{\bar{k}_t}) = \textsc{Path}_{-\tau}(sys(\bar{k}'_t){\downarrow}R', S_I^{\bar{k}'_t}) \Rightarrow \\ sys(\bar{k}_t) \models \varphi \ \Leftrightarrow \ sys(\bar{k}'_t) \models \varphi$$

In the above, $\bar{k}_t = k_1, \ldots, k_t$, $\bar{k'}_t = k'_1, \ldots, k'_t$, $\bar{k'}_t \geq \bar{k}_t = k'_1 \geq k_1, \ldots, k'_t \geq k_t$, and $S_I^{\bar{k}_t}$ and $S_I^{\bar{k}'_t}$ are the initial state-sets of $sys(\bar{k}_t)$ and $sys(\bar{k}'_t)$, respectively.

Proof. Let $\pi_{-\tau}$, $\pi'_{-\tau}$ be sequences of receive/send actions of adjacent processes in $\textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}\{i_{p_1}, j_{p_2}\}, S_I^{\bar{k}_t})$, and $\textsc{Path}_{-\tau}(sys(\bar{k'}_t){\downarrow}\{i'_{p_1}, j'_{p_2}\}, S_I^{\bar{k}_t})$, respectively. Since the adjacent processes in both system instances performed the exact sequence of receive/send actions in both $\pi_{-\tau}$ and $\pi'_{-\tau}$, their corresponding sequences of states will also be the same (same behavioral automata followed to perform the same actions). Therefore $\mathtt{Seq}(\pi_{-\tau}) = \mathtt{Seq}(\pi'_{-\tau})$. If the sequence of state of adjacent processes is the same in $sys(\bar{k}_t)$ and $sys(\bar{k'}_t)$, we can conclude using Proposition 1 that $sys(\bar{k}_t)$ and $sys(\bar{k'}_t)$ satisfy the same property φ defined over states of adjacent processes. ∎

Theorem 2 (Soundness) Given a prameterized system with t types of processes, if $sys(\bar{k}_t)$ is a cut-off instance, then for all $\mathtt{LTL}\backslash\mathtt{X}$ properties φ defined over the states of one process or two adjacent processes, for all $\bar{k}_t < \bar{k'}_t$, $sys(\bar{k}_t) \models \varphi \Leftrightarrow sys(\bar{k'}_t) \models \varphi$.

Proof. Using Proposition 2, we want to prove that if $sys(\bar{k}_t)$ is the cut-off instance, then $\textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}R, S_I^{\bar{k}_t}) = \textsc{Path}_{-\tau}(sys(\bar{k}'_t){\downarrow}R', S_I^{\bar{k}'_t})$ for any larger instance $sys(\bar{k'}_t)$. Proof is by the cases of definition 12. We start by the case 1 (b).

Let $\pi'_{-\tau}$ be a sequence of receive/send actions in $\textsc{Path}_{-\tau}(sys(\bar{k'}_t){\downarrow}R', S_I^{\bar{k'}_t})$, such that, for all $\pi_{-\tau}$ in $\textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}R, S_I^{\bar{k}_t})$, $\pi'_{-\tau} \neq \pi_{-\tau}$. Assume that $\pi'_{-\tau}$ has the same sequence of receive/send events as $\pi_{-\tau}$ up to an index l, where $\pi'_{-\tau}[l] \neq \pi_{-\tau}[l]$.

Let $\pi'_{-\tau}[l] = e/e'$, where $\exists\sigma \in \mathcal{CY}(\ddot{p})$ such that $\langle(e,q),(e',q')\rangle$ is a subsequence in σ. If for all $\pi_{-\tau}$ in $\textsc{Path}_{-\tau}(sys(\bar{k}_t){\downarrow}R, S_I^{\bar{k}_t})$, $\pi_{-\tau}[l] \neq e/e'$, this means that for cycle σ, $[\sigma] \cap \mathcal{L}(sys(\bar{k}_t)) = \emptyset$ (some events in the cycle are not executed in $sys(\bar{k}_t)$), therefore $sys(\bar{k}_t)$ is not a cut-off instance. On the other hand, since $\bar{k'}_t > \bar{k}_t$, it may be the case that e/e' occurred more than once in $\pi'_{-\tau}$ while e/e' occurred only once in $\pi_{-\tau}$. This means that adjacent processes performed the sequences of receive/send actions presented in parameter-dependent cycles more than once in the larger instance, while this is not true in the cut-off instance. This contradicts the fact that the cycle is due to parameter-dependent behavior. Therefore this case is also not possible.

Proof for case 1 (b) [1]. Consider the same assumption as above, where $\pi'_{-\tau}[l] \neq \pi_{-\tau}[l]$ and $\pi'_{-\tau}[l] = e/e'$.

If $e = \epsilon$, this means that neither of the processes in $sys(\bar{k}_t)$ could do an autonomous move (move with no input). As every path in $\ddot{p}$ starts with an autonomous move ϵ/e', this means that $\mathcal{L}(\ddot{p})_1 \not\subseteq \mathcal{L}(sys(\bar{k}_t))$ for $p = p_1$ or $p = p_2$.

If $e \neq \epsilon$, this means that a process of type p' was capable of sending the event e in $sys(\bar{k'}_t)$ while no process of that type in $sys(\bar{k}_t)$ was capable of doing so. For this to happen, the process of type p' in $sys(\bar{k'}_t)$ must have performed the receive/send action e_0/e that no process of that type in p' in $sys(\bar{k}_t)$ was capable of performing. If $e_0 = \epsilon$, this means either $\mathcal{L}(\ddot{p'})_1 \not\subseteq \mathcal{L}(sys(\bar{k}_t))$. If not, we check the previous receive/send action that lead to e/e_0. We repeat inductively on the length of the diverging point between the two paths and eventually reach the base case. ∎

References

1. Hanna, Y., Samuelson, D., Basu, S., Rajan, H.: Automating cut-off for multi-parameterized systems. In: ICFEM. (2010) 338–354