The equivalence between verifying a stutter-invariant LTL formula on a Modular Petri net or on its related RDSS

Sawsen Khlifa
Mediatron Lab
Higher School of Communications of Tunis
University of Carthage Tunisia
Sawsen.khlifa@supcom.tn

Chiheb Ameur Abid
Mediatron Lab
Faculty of Sciences of Tunis,
University of Tunis El Manar, Tunis, Tunisia
chiheb.abid@fst.utm.tn

Belhassan Zouari
ICL, Junia
Université Catholique de Lille
LITL, F-59000 Lille, France
belhassen.zouari@univ-catholille.fr

To check a property on a metagraph, we have to prove the stuttering equivalence [1] between checking the property on the metagraph, and checking it on the original reachability graph of the MPnet. It is ensured by the preservation of maximal paths (i.e. finite paths leading to a dead state and infinite paths).
In the following, we demonstrate that a MPnet satisfies an $LTL\backslash X$ property if and only if its corresponding RDSS does.

Theorem 1: Let $\mathcal{P}$ be a MPnet where $\mathcal{P} = (S, TF)$ and let $\mathcal{R}$ be its corresponding RDSS where $\mathcal{R} == \{RG_s = (\widehat{\mathcal{N}_s}, \widehat{\mathcal{A}_s}) | s \in S\}$. Let ϕ be an $LTL\backslash X$ formula on a subset of T_s the set of the local and synchronized transitions of a module s. Then $\mathcal{P} \vDash \phi \iff \mathcal{R} \vDash \phi$
To prove this Theorem, we will prove that the RDSS preserves the maximal paths of the associated MPnet. For that purpose, we present first, two lemmas about the correspondence between paths of $\mathcal{P}$ and those of $\mathcal{R}$.

lemma 1: Let $\pi = p_1 \xrightarrow{t_2} p_2 \xrightarrow{t_3} ... \xrightarrow{t_n} p_n$ be a path of a module s of $\mathcal{P}$ and $\widehat{\mathcal{M}_1}$ a metastate of the corresponding module s of $\mathcal{R}$ such that $p_1 \in \widehat{\mathcal{M}_1}.Q$. Then, there exists a path $\pi' = \widehat{\mathcal{M}_1} \xrightarrow{t'_2} \widehat{\mathcal{M}_2} \xrightarrow{t'_3} .... \xrightarrow{t'_l} \widehat{\mathcal{M}_l}$ and and a strictly increasing sequence of integers $i_1 = 1 < i_2 < \ldots < i_{l+1} = n + 1$ satisfying

$\{p_{i_k}, p_{i_k+1}, \ldots, p_{i_{k+1}-1}\} \subseteq \widehat{\mathcal{M}_k}.Q$ for all $1 \leq k \leq l$.

proof 1: We reason by induction on the length of π.
If $n = 1$, as $p_1 \in \widehat{\mathcal{M}_1}$ the lemma is verified for n=1.
For $n > 1$ we assume that :
$\pi = \widehat{\mathcal{M}_1} \xrightarrow{t'_2} \widehat{\mathcal{M}_2} \xrightarrow{t'_3} .... \xrightarrow{t'_{l-1}} \widehat{\mathcal{M}_{l-1}}$
and a strictly increasing sequence of integers
$i_1 = 1 < i_2 < \ldots < i_l = n$ align with the conditions outlined in the lemma for the path $\pi = p_1 \xrightarrow{t_2} p_2 \xrightarrow{t_3} ... \xrightarrow{t_{n-1}} p_{n-1}$.
Thus $p_{n-1} \in \widehat{\mathcal{M}_{l-1}}$.

- If $t_n \in T_{l,s}$
  By definition of the metastate, $p_n \in \widehat{\mathcal{M}_{l-1}}$ So the path and the sequence remain valid for the path of length n
- If $t_n \in T_{sync,s}$
  By definition of the RDSS $\exists \widehat{\mathcal{M}_l} \in RG_s$ s.t $\widehat{\mathcal{M}_{l-1}} \xrightarrow{t_n} \widehat{\mathcal{M}_l}$

Therefore, the path $\pi = \widehat{\mathcal{M}_1} \xrightarrow{t'_2} \widehat{\mathcal{M}_2} \xrightarrow{t'_3} .... \xrightarrow{t'_{l-1}} \widehat{\mathcal{M}_{l-1}} \xrightarrow{t'_l = t_n} \widehat{\mathcal{M}_l}$ and the sequence $i_1, i_2, \ldots, i_{l+1} i_l$
The subsequent lemma demonstrates the converse.

lemma 2: Let $\pi = \widehat{\mathcal{M}_1} \xrightarrow{t_2} \widehat{\mathcal{M}_2} \xrightarrow{t_3} .... \xrightarrow{t_n} \widehat{\mathcal{M}_n}$ be a path of $\mathcal{R}$. Then, there exists a path $p_1 \xrightarrow{\sigma_1} p'_1 \xrightarrow{t_2} p_2 \xrightarrow{\sigma_2} p'_2 \xrightarrow{t_3} ... \xrightarrow{t_n} p_n \xrightarrow{\sigma_n} p'_n$ of $\mathcal{P}$ in such a way that $\forall i = 1...n, \sigma_i \in T^*_{l,s}$ and $p_i, p'_i \in \widehat{\mathcal{M}_i}.Q$ as well as all traversed states from p_i to p'_i.

proof 2: The firing of a synchronised transition t_{i+1} from $\widehat{\mathcal{M}_i}$ to $\widehat{\mathcal{M}_{i+1}}$ is possible from a set of states in the starting metastate $\widehat{\mathcal{M}_i}$ activating this transition which we denote as $In_\pi(\widehat{\mathcal{M}_i})$, leading to a set of states reachable by crossing the same transition which we call $Out_\pi(\widehat{\mathcal{M}_i})$. This set will serve as the starting point for determining all states constructing the destination metastate $\widehat{\mathcal{M}_{i+1}}$ by adding all their successors through local transitions. Formally, we can define these two sets as follows:

$$In_\pi(\widehat{\mathcal{M}_i}) = \begin{cases} \{p' \in \widehat{\mathcal{M}_i}.Q \mid \\ \quad \exists p \in \widehat{\mathcal{M}_{i-1}}.Q : p \xrightarrow{t_i} p'\}, & \text{if } i \neq 1; \\ Out_\pi\ (a_i), & \text{otherwise.} \end{cases}$$

$$Out_\pi(\widehat{\mathcal{M}_i}) = \begin{cases} \{p \in \widehat{\mathcal{M}_i}.Q : s \xrightarrow{t_{i+1}}\}, & \text{if } i \neq n-1; \\ In_\pi(a_i), & \text{otherwise.} \end{cases}$$

we have $\widehat{\mathcal{M}_{n-1}} \xrightarrow{t_n} \widehat{\mathcal{M}_n}$ so there is at least one state $p_n \in In_\pi(\widehat{\mathcal{M}_n})$, that is reachable by firing t_n:

- case1: p_n has immediate or non-immediate successor through local transitions, Thus, we have $p_n \xrightarrow{\sigma_n} p'_n / \sigma_n \in T^*_{l,s}$.
- case2: p_n as no successors, then $p_n = p'_n$

Similarly, there is at least one element $p_{n-1} \in Out_\pi(\widehat{\mathcal{M}_{n-1}})$ that fire the synchronised transition t_n, resulting in $p_{n-1} \xrightarrow{t_n} p_n$. $p_{n-1}$is either an immediate or non-immediate successor of an element $p'_{n-1} \in In_\pi(\widehat{\mathcal{M}_{n-1}})$ through local transitions of $\widehat{\mathcal{M}_{n-1}}$ this results in $p_{n-1} \xrightarrow{\sigma_{n-1}} p'_{n-1}$.
In the case where p_{n-1} has no predecessor through local

transitions $\widehat{\mathcal{M}_{n-1}}$, $p_{n-1} = p'_{n-1}$.
Iterating this reasoning from a metastate to its predecessor, we can construct the path $p_1 \xrightarrow{\sigma_1} p'_1 \xrightarrow{t_2} p_2 \xrightarrow{\sigma_2} p'_2 \xrightarrow{t_3} ... \xrightarrow{t_n} p_n \xrightarrow{\sigma_n} p'_n$ in a reverse way starting from the end, going from $\widehat{\mathcal{M}_n}$to $\widehat{\mathcal{M}_1}$."

So far, we have demonstrated the correspondence between paths of $\mathcal{P}$ and those of $\mathcal{R}$. In the following, we will propose two lemmas to prove the correspondence of maximal paths for the two structures.

lemma 3: Let $\pi = p_0 \xrightarrow{t_1} ... \xrightarrow{t_n} p_n$ be a maximal path of a module s of $\mathcal{P}$. Then, there exists a

maximal path $\pi' = \widehat{\mathcal{M}_0} \xrightarrow{t'_1} .... \xrightarrow{t'_l} \widehat{\mathcal{M}_l}$ of $\mathcal{R}$ such that there exists a sequence of integers $i_0 = 0 < i_1 < \ldots < i_{l+1} = n+1$ satisfying $\{p_{i_k}, p_{i_k+1}, \ldots, p_{i_{k+1}-1}\} \subseteq \widehat{\mathcal{M}_k}.Q$ for all $0 \leq k \leq l$

proof 3:

- If p_n is a dead marking and knowing that $p_o \in \widehat{\mathcal{M}_0}$ we can build using lemma 1 a path $\pi' = \widehat{\mathcal{M}_0} \xrightarrow{t'_1} .... \xrightarrow{t'_l} \widehat{\mathcal{M}_l}$ and the associated integer sequence corresponding to π. As the last visited state of π belongs to $\widehat{\mathcal{M}_l}$. So p_n, which is a dead marking that does not enable any local transition, is a trivial terminal strongly connected component (SCC). This SCC is Sync-closed [2] and π' is a maximal path of $\mathcal{R}$.
- If p_n is not a dead marking the path π can be decomposed as follows: $\pi = \pi_1\pi_2$ s.t $\pi_1 = p_0 \xrightarrow{t_1} p_1 ... \xrightarrow{t_k} p_k$ and $\pi_2 = p_k \xrightarrow{t_{k+1}} p_{k+1} ... \xrightarrow{t_n} p_k$ so that π_2 is a circuit.
  Applying lemme 1 starting from p_0 the corresponding paths of π_1 and π_2 are consecutively π'_1 and π'_2 in $\mathcal{R}$
  $\pi'_1 = \widehat{\mathcal{M}_0} \xrightarrow{t'_1} .... \xrightarrow{t'_{m-1}} \widehat{\mathcal{M}_m}$ and π'_2 must be built starting from $\widehat{\mathcal{M}_m}$ as $p_k \in \widehat{\mathcal{M}_m}$.
  - If π_2 contains only local transitions: all states traversed to go from p_k to p_k forming the circuit are in $\widehat{\mathcal{M}_m}$. These states then form a terminal SCC containing a cycle. We conclude that this SCC is sync-closed.
  - If π_2 involves local or synchronized transitions, we choose the sub-paths such that t_{k+1} is a synchronized transition. By definition of th RDSS, as $p_k \in \widehat{\mathcal{M}_m}$ there exists an metastate $\widehat{\mathcal{M}_{0_1}}$ successor of $\widehat{\mathcal{M}_m}$ by the transition t_{k+1}. By using Lemma 1 , and the definition of the RDSS, let $\pi'_1 = \widehat{\mathcal{M}_0} \xrightarrow{t'_1} .... \xrightarrow{t'_{m-1}} \widehat{\mathcal{M}_m}$ and $\pi'_2 = \widehat{\mathcal{M}_{0_1}} \xrightarrow{t_{p_1}} .... \xrightarrow{t_l} \widehat{\mathcal{M}_{q_1}}$ with $s_k \in \widehat{\mathcal{M}_{q_l}}.Q$. If $\widehat{\mathcal{M}_{k_1}} \xrightarrow{t_{k+1}} \widehat{\mathcal{M}_{0_1}}$ then π'_2 is a circuit of $\mathcal{R}$ and $\pi'_1\pi'_2$ is a maximal path of $\mathcal{R}$ satisfying the lemma 3. Otherwise, by construction of the RDSS, there exists an other successor of $\widehat{\mathcal{M}_{q_l}}$ containing p_k. Applying again Lemma 1 from this metastate, we can construct a new path in $\mathcal{R}$ corresponding to pi_2. Let $\widehat{\mathcal{M}_{0_2}} \xrightarrow{t_{p_1}} .... \xrightarrow{t_l} \widehat{\mathcal{M}_{q_2}}$ be this path. If $\widehat{\mathcal{M}_{q_2}} \xrightarrow{t_{k+1}} \widehat{\mathcal{M}_{0_2}}$ we can then deduce a path of $\mathcal{R}$ which concludes the proof. Or else, we can construct a new path corresponding to π_2 starting from a successor of $\widehat{\mathcal{M}_{0_2}}$ or we continue the path decomposition in a recursive way. As the number of metastates in $\mathcal{R}$ is finite and particularly the number of metstates to which p_k can belong is limited by 2^N where N is number of places in the original graph of the MPnet related to the concerned module, a circuit will be necessarily obtained.

lemma 4: Let $\pi = \widehat{\mathcal{M}_0} \xrightarrow{t_1} \widehat{\mathcal{M}_1} \xrightarrow{t_2} .... \xrightarrow{t_n} \widehat{\mathcal{M}_n}$ be a maximal path of $\mathcal{R}$. Then, it exists a maximal path $p_1 \xrightarrow{\sigma_1} p'_0 \xrightarrow{t_1} p_1 \xrightarrow{\sigma_1} p'_1 \xrightarrow{t_2} ... \xrightarrow{t_n} p_n \xrightarrow{\sigma_n} p'_n$ of $\mathcal{P}$ s.t $\forall i = 1...n, \sigma_i \in T^*_{l,s}$ and $p_i, p'_i \in \widehat{\mathcal{M}_i}.Q$

proof 4:

- π is a maximal path reaching the metastate $\widehat{\mathcal{M}_n}$ such that $\widehat{\mathcal{M}_n}$ contains a sync-closed terminal SCC. If this SCC is trivial it contains a local deadlock marking or it contains a cycle.
  If the path π is composed from a single metastate, the proof is trivial because the deadlock marking or the SCC containing the cycle is necessarily reachable from p_0. Otherwise, using the same reasoning as in proof 2, we can demonstrate the existence of the maximal path on $\mathcal{P}$. by defining $In_\pi(\widehat{\mathcal{M}_0}) = p_0$ and $Out_\pi(\widehat{\mathcal{M}_n})$ is either the dead state or the set of sates forming the circuit.
- If $\widehat{\mathcal{M}_n}$ do not contain a terminal sync-closed SCC. π can be written as $\pi = \widehat{\mathcal{M}_0} \xrightarrow{t_1} ...\widehat{\mathcal{M}_l} \xrightarrow{t_{l+1}} .... \xrightarrow{t_n} \widehat{\mathcal{M}_n}$ s.t $\widehat{\mathcal{M}_l} \xrightarrow{t_{l+1}} .... \xrightarrow{t_n} \widehat{\mathcal{M}_n}$ is a circuit of $\mathcal{R}$ i.e $\widehat{\mathcal{M}_n} = \widehat{\mathcal{M}_l}$.
  Once again, using the same argumentation of the proof 2 by defining $In_\pi(\widehat{\mathcal{M}_0}) = p_0$ and $Out_\pi(\widehat{\mathcal{M}_n})$ as the set of states in $\widehat{\mathcal{M}_n}$ enabling t_{l+1}. Thus, by backward construction, we build the maximal path of $\mathcal{P}$that satisfies Lemma 4.

We have thus established the matching between the maximal paths of a module in the MPnet and those of the same one in the associated RDSS.

REFERENCES

[1] E. M. Clarke, O. Grumberg, D. A.Peled. Model checking the mit press, 1999, Cambridge, Massachusetts, London, UK, 988.

[2] H. Ouni, C.A. Abid and B. Zouari, *A distributed state space for modular Petri nets*, in 7th International Conference on Modelling, Identification and Control, 2015.