On-the-fly CSL Property Monitoring in STAMINA

The approach described below closely monitors CSL property checking, and uses basic decision procedures to quickly terminate state expansion as soon as sufficient conclusion can be drawn. This approach can potentially improve STAMINA's performance.

Assumptions:

- Verify a single non-nested CSL property in the form of $\mathsf{P}_{=?}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$, where $p \in [0,1]$.
- The approach described below assumes round-off errors in probability are properly handled to guarantee termination.
- Standard BFS is used for state space expansion. Note that state exploration assumes standard BSF for all states implemented in STAMINA before, not including the work Brett is doing now on incremental state expansion and verification. DFS will not work as it violates assumptions for Theorem 0.1.

Background: Path satisfiability for formula $\Phi\ \mathcal{U}\ \Psi$ is determined if either of the following conditions holds: (1) If a state on a path is found to satisfy Ψ for the first time, then satisfiability of $\Phi\ \mathcal{U}\ \Psi$ can be determined without needing all its successor states on this path; and (2) a path starting from a given initial state can never satisfy $\Phi\ \mathcal{U}\ \Psi$, if it includes a state satisfying $\neg\Phi \wedge \neg\Psi$. These conditions allow a search path to terminate during state exploration as soon as satisfiability of $\Phi\ \mathcal{U}\ \Psi$ is determined. A finite path ρ is a state-transition sequence starting with an initial state and ending with the last state $last(\rho)$. A path is an *early-terminated path*, denoted as $\underline{\rho}$, if $last(\underline{\rho})$ satisfies either $\neg\Phi \wedge \neg\Psi$ or Ψ. On the other hand, all states on a *non-early-terminated path*, denoted as ρ, must satisfy $\Phi \wedge \neg\Psi$.

Methods: Currently, STAMINA shortens each early-terminated path by making its last state *absorbing*, where its only outgoing transition a self-loop with probability 1. For each non-early-terminated path, it truncates it by directing the last state's outgoing transitions to a *single* abstract absorbing state.

In this improved approach, we create three different abstract absorbing states instead to collect probabilities of satisfying $\Phi\ \mathcal{U}^{[0,T]}\ \Psi$, failing it, and unknown, respectively. Note that we only redirect those outgoing transitions to an abstract state if such transition leads to an unexplored state. For the last state of each early-terminated path, the choice of abstract state to redirect such transitions depends on the satisfiability of $\Phi\ \mathcal{U}\ \Psi$ of the last state. Conditions for these three abstract absorbing states are listed below.

- $\mathbf{abs}_{sat}$: Absorbing state for all early-terminated path whose last state satisfies Ψ.
- $\mathbf{abs}_{unsat}$: Absorbing state for all early-terminated path whose last state satisfies $\neg\Phi \wedge \neg\Psi$.
- $\mathbf{abs}_{?}$: Absorbing state for all non-early-terminated but truncated paths. Satisfiability of $\Phi\ \mathcal{U}\ \Psi$ cannot be determined yet. The last state of a non-early-terminated path satisfies $\Phi \wedge \neg\Psi$.
- $\mathsf{P}^r_{\mathbf{abs}_{sat}}$, $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$, and $\mathsf{P}^r_{\mathbf{abs}_{?}}$ represent state reachability probabilities for the above three absorbing states, which are computed by PRISM's CTMC analysis, in iteration r.

Algorithm sketch: **Main algorithm:**

1. Start with a relatively large $\varkappa$ value (e.g., 10^{-4}). Set iteration counter r to 0.
2. Increment round counter: $r = r + 1$.
3. Apply property-guided state expansion with early-path-termination and create three abstract absorbing states as state above.
4. Perform PRISM's CTMC analysis up to the upper time bound T in the CSL property. On the resulting state space, we know the following state reachability probability equation holds: $\mathsf{P}^r_{\mathbf{abs}_{unsat}} + \mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_{?}} + \mathsf{P}^r_{\mathbf{X}} = 1$, where $\mathsf{P}^r_{\mathbf{X}}$ is the sum of probabilities of all explored states in iteration r, *excluding* $\mathsf{P}^r_{\mathbf{abs}_{sat}}$, $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$, and $\mathsf{P}^r_{\mathbf{abs}_{?}}$.

5. Calculate $\mathsf{P}^r_{\mathbf{abs}_{sat}}$, $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$, $\mathsf{P}^r_{\mathbf{abs}_?}$, and $\mathsf{P}^r_{\mathbf{X}}$.
6. Go to "Procedure for checking $\mathsf{P}^r_{\mathbf{abs}_{sat}}$".

Procedure for checking $\mathsf{P}^r_{\mathbf{abs}_{sat}}$:

1. **If CSL property is $\mathsf{P}_{=?}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$.**
   (a) Simulate the model first to get an estimated value for p. Let $p_u = p + \varepsilon$ and $p_l = p - \varepsilon$, where $0 < \varepsilon \ll 1$ and $p_l, p_u \in [0, 1]$.
   (b) Formulate $prop_1 = \mathsf{P}_{<p_u}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$ and then **go to step 2**: "If CSL property is $\mathsf{P}_{<p}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$". Formulate $prop_2 = \mathsf{P}_{>p_l}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$ and then **go to step 3**: "If CSL property is $\mathsf{P}_{>p}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$".
      i. The case $(\neg prop_1 \wedge \neg prop_2)$ should not occur as long as $p_l \leqslant p_u$.
      ii. If $(prop_1 \wedge prop_2)$, then terminate by concluding that the probability of the property is within $[p - \varepsilon, p + \varepsilon]$. So $\mathsf{P}_{=?}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi) = \mathsf{P}^r_{\mathbf{abs}_{sat}}$. **Terminate.**
      iii. Else:
         A. If $(prop_1 \wedge \neg prop_2)$, we know that $\mathsf{P}_{\leqslant p_l}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$. If $\mathsf{P}^r_{\mathbf{abs}_{sat}} = p_l$, then $\mathsf{P}_{=?}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi) = \mathsf{P}^r_{\mathbf{abs}_{sat}}$. **Terminate.** Otherwise, $\mathsf{P}_{<p_l}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$. Then perform the following updates in order: $p = p_l - \varepsilon$; $p_l = max\{p - \varepsilon, 0\}$; and $p_u = min\{p + \varepsilon, 1\}$. **Go to step 1b.**
         B. If $(\neg prop_1 \wedge prop_2)$, then we know that $\mathsf{P}_{\geqslant p_u}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$. If $\mathsf{P}^r_{\mathbf{abs}_{sat}} = p_u$, then $\mathsf{P}_{=?}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi) = \mathsf{P}^r_{\mathbf{abs}_{sat}}$. **Terminate.** Otherwise, $\mathsf{P}_{>p_u}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$. Then perform the following updates in order: $p = p_u + \varepsilon$; $p_l = max\{p - \varepsilon, 0\}$; and $p_u = min\{p + \varepsilon, 1\}$. **Go to step 1b.**
2. **If CSL property is $\mathsf{P}_{<p}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$.**
   (a) If $\mathsf{P}^r_{\mathbf{abs}_{sat}} \geqslant p$, then property fails. Because $\mathsf{P}^r_{\mathbf{abs}_{sat}}$ won't decrease in future state expansion iterations (see Theorem 0.1). **Return false.**
   (b) Else (i.e., $\mathsf{P}^r_{\mathbf{abs}_{sat}} < p$):
      i. If $\mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} < p$, then property satisfies according to Theorem 0.3. **Return true.**
      ii. Else (i.e., $\mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} \geqslant p$): Go to "Procedure for checking $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$".
3. **If CSL property is $\mathsf{P}_{>p}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$.**
   (a) If $\mathsf{P}^r_{\mathbf{abs}_{sat}} > p$, then property satisfies. Because $\mathsf{P}^r_{\mathbf{abs}_{sat}}$ won't decrease in future iterations (see Theorem 0.1). **Return true.**
   (b) Else (i.e., $\mathsf{P}^r_{\mathbf{abs}_{sat}} \leqslant p$):
      i. If $\mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} < p$, then property fails according to Theorem 0.3. **Return false.**
      ii. Else (i.e., $\mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} \geqslant p$): Go to "Procedure for checking $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$".

Procedure for checking $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$:

Note that this procedure is assumed to be called within "Procedure for checking $\mathsf{P}^r_{\mathbf{abs}_{sat}}$". So it is called only if property satisfiability cannot be determined. We use this procedure to filter out cases that can be determined by comparing $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$ with $1 - p$, before continue to expand the state space.

1. **If CSL property is $\mathsf{P}_{<p}(\Phi\ \mathcal{U}^{[0,T]}\ \Psi)$.**
   (a) If $\mathsf{P}^r_{\mathbf{abs}_{unsat}} > 1 - p$, which implies $\mathsf{P}^r_{\mathbf{abs}_{sat}} < p$, the property satisfies. **Return true.**. This is because $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$ can not decrease in future iterations, and it is already large enough to keep $\mathsf{P}^r_{\mathbf{abs}_{sat}} < p$ from after the current iteration r, $\mathsf{P}^r_{\mathbf{abs}_{sat}} < p$ holds for all future iterations.
   (b) Else (i.e., $\mathsf{P}^r_{\mathbf{abs}_{unsat}} \leqslant 1 - p$): **Go to step 2 of the main algorithm.**

2. **If CSL property is $\mathsf{P}_{>p}(\Phi\, \mathcal{U}^{[0,T]}\ \Psi)$.**
   (a) If $\mathsf{P}^r_{\mathbf{abs}_{unsat}} \leqslant 1-p$, then $\mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} \geqslant p$. Need more states to determine property satisfiability. **Go to step 2 of the main algorithm.**
   (b) If $\mathsf{P}^r_{\mathbf{abs}_{unsat}} > 1-p$, then $\mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} < p$, and property fails due to Theorem 0.3. **Return false.**

Theorem 0.1 *Let $\mathsf{P}^r_{\mathbf{abs}_{sat}}$ and $\mathsf{P}^{r+1}_{\mathbf{abs}_{sat}}$ be the probabilities accumulated in the abstract absorbing state $\mathbf{abs}_{sat}$ after iteration r and $r+1$, respectively, where $r \in \mathbb{Z}^+$. Then $\mathsf{P}^{r+1}_{\mathbf{abs}_{sat}} \geqslant \mathsf{P}^r_{\mathbf{abs}_{sat}}$.*

Theorem 0.2 *Let $\mathsf{P}^r_{\mathbf{abs}_{unsat}}$ and $\mathsf{P}^{r+1}_{\mathbf{abs}_{unsat}}$ be the probabilities accumulated in the abstract absorbing state $\mathbf{abs}_{unsat}$ after iteration r and $r+1$, respectively, where $r \in \mathbb{Z}^+$. Then $\mathsf{P}^{r+1}_{\mathbf{abs}_{unsat}} \geqslant \mathsf{P}^r_{\mathbf{abs}_{unsat}}$.*

Correctness Argument of Theorem 0.1 and 0.2 : After further state expansion in iteration $r+1$, $\mathsf{P}^r_{\mathbf{abs}_{sat}}$ obtained from iteration r either remains the same or increases. Because both early-terminated-paths redirected to $\mathbf{abs}_{sat}$, denoted as $\underline{\rho}^r_{sat}$, and their probability contribution in this state $\mathsf{P}^r_{\mathbf{abs}_{sat}}$ in iteration r remain unchanged going into the next iteration $r+1$. Note that state expansion in iteration $r+1$ only expands non-early-terminated paths and keep early-terminated-ones unchanged. Since BFS is used for state expansion, all explored states in iteration r already have all of their outgoing transitions expanded. So during iteration $r+1$, there won't be new outgoing transitions from any explored states obtained in iteration r. For each $\underline{\rho}^r_{sat}$, every explored state on this path cannot have new outgoing transitions diverting state reachability probabilities to other paths. Therefore, as long as CTMC analysis runs to the same upper time bound in both iterations r and $r+1$, $\mathsf{P}^{r+1}_{\mathbf{abs}_{sat}} \not< \mathsf{P}^r_{\mathbf{abs}_{sat}}$. Secondly, state expansion in iteration $r+1$ only extends non-early-terminated paths from r. So it is possible to create new paths leading to states on path $\underline{\rho}^r_{sat}$. This may potentially increase $\mathsf{P}^r_{\mathbf{abs}_{sat}}$ after the CTMC analysis in iteration $r+1$. Therefore, $\mathsf{P}^{r+1}_{\mathbf{abs}_{sat}} \geqslant \mathsf{P}^r_{\mathbf{abs}_{sat}}$. Similar argument can be made for Theorem 0.2.

Theorem 0.3 *Given $\mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} < p$ in iteration r, for any iteration l where $(l > r)$, $\mathsf{P}^l_{\mathbf{abs}_{sat}} < p$.*

Theorem 0.4 *Given $\mathsf{P}^r_{\mathbf{abs}_{unsat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} < p$ in iteration r, for any iteration l where $(l > r)$, $\mathsf{P}^l_{\mathbf{abs}_{unsat}} < p$.*

Correctness Argument of Theorem 0.3 and 0.4: Since $\mathsf{P}^r_{\mathbf{abs}_{sat}} + \mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}} < p$ in the current iteration r, the best case is where the entire probability sum $(\mathsf{P}^r_{\mathbf{abs}_?} + \mathsf{P}^r_{\mathbf{X}})$ contributes to $\mathsf{P}^l_{\mathbf{abs}_{sat}}$ in a future iteration $(l > r)$. However, this sum is still insufficient to bring $\mathsf{P}^l_{\mathbf{abs}_{sat}}$ equal or above p. Similar argument can be made for Theorem 0.4.