TreeLexPSM

Daniel Eduardo Contro

A.Y. 2024/2025

1 Introduction

In order to improve the expressiveness of the original *LexPSM* template, we introduce a generalization of it called *TreeLexPSM*. Given a reactive system $System^\phi = \langle S, TI, Init^\phi, \mathcal{G}^\phi \rangle$ and a parity automaton $\mathcal{A} = \langle Q, \Sigma, \delta, q_0, c \rangle$ with $c : Q \to \mathbb{N}_{<d}$ the associated coloring function, we define the product as $Product^\phi = \langle S \times Q, \Sigma, \mathcal{G}^\phi_\times, (q_0, Init^\phi), c \rangle$ where $\mathcal{G}^\phi_\times =$ "$\delta \times \mathcal{G}^\phi$", A *TreeLexPSM* is a family $\Pi = (\Pi_p)_{p \in \mathbb{N}_{<d}}$ of complete binary decision trees of height h, where every node is associated to a linear constraint and each leaf has a unique *LexPSM* related to it.

This induces a family $\mathcal{P} = (\mathcal{P}_p)_{p \in \mathbb{N}_{<d}}$ of families $\mathcal{P}_p = (P_{p,n})_{n \in \mathbb{N}_{<2^h}}$, where any family $P_{p,i}$ can possibly be empty, which is a partition of the state space $S \times Q$. Furthermore every $P_{p,i} \in P_p$ is associated with a *LexPSM* $\lambda_{p,i} : S \to \mathbb{R}^d$.

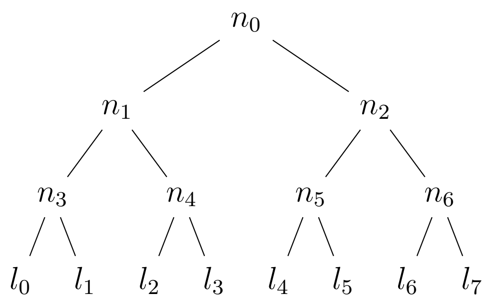

Figure 1: Example of a *TreeLexPSM* τ_0 for parity level 0 of height 3.

2 Proof Rule

The introduction of this new template requires the rewriting of the proof rule for the synthesis of a *TreeLexPSM*. The original proof rule for *LexPSM* is as follows:

$$\begin{array}{l}
\forall\phi : I(q_0, \mathit{Init}^\phi) \geq 0 \\
\forall\phi\forall x \in S \times Q \forall(g, U) \in \mathcal{G}^\phi_\times \forall u \in U : \\
\qquad TI(x) \wedge I(x) \geq 0 \wedge g(x) \Rightarrow I(u(x)) \geq 0 \\
\forall\phi\forall \,\text{even}\, p \in \mathbb{N}_{<d} \forall x \in S \times Q \forall(g, U) \in \mathcal{G}^\phi_\times : \\
\qquad O_p(x) \wedge TI(x) \wedge I(x) \geq 0 \wedge g(x) \Rightarrow \operatorname{Post} V^\phi(x) \preceq^\varepsilon_p V^\phi(x) \\
\forall\phi\forall \,\text{odd}\, p \in \mathbb{N}_{<d} \forall x \in S \times Q \forall(g, U) \in \mathcal{G}^\phi_\times : \\
\qquad O_p(x) \wedge TI(x) \wedge I(x) \geq 0 \wedge g(x) \Rightarrow \operatorname{Post} V^\phi(x) \prec^\varepsilon_p V^\phi(x) \\
\hline
\forall\phi : \Pr\big(\mathit{System}^\phi \vDash \mathit{Spec}\big) = 1
\end{array}$$

Figure 2: Proof rule of *LexPSM*.

Let us define $ith^{\phi,\Pi} : \mathbb{N}_{<d} \times \mathbb{N}_{<2^h} \to \wp(S \times Q) \times ((S \times Q) \times \mathbb{N}_{<d} \to \mathbb{R}^d)$ as the function that maps an index to a pair of a partition of the state space and the associated *LexPSM*

$$ith^{\phi,\Pi}(p, i) = (P_{p,i}, \lambda_{p,i}) \tag{1}$$

$V^{\phi,\Pi} : (S \times Q) \times \mathbb{N}_{<d} \to \mathbb{R}^d$:

$$V^{\phi,\Pi}(x, p) = \begin{cases} \lambda^\phi_{p,0}(x) & \text{if } x \in P^\phi_{p,0} \\ \vdots & \\ \lambda^\phi_{p,2^h-1}(x) & \text{if } x \in P^\phi_{p,2^h-1} \end{cases} \tag{2}$$

the $\operatorname{Post}_{(g,U)} : (S \times Q) \times \mathbb{N}_{<d} \to (\mathbb{R}^d)_{n \in \mathbb{N}_{<2^{|U|+h}}}$ operator for *TreeLexPSM* is defined as:

$$\begin{aligned} \mathit{Posts}_U = \prod_{(p,u) \in U} \{p \cdot \lambda^\phi_{p,i}(u(x)) \mid \\ i \in \mathbb{N}_{<2^h} P^\phi_{p,i}, \lambda^\phi_{p,i} = ith^{\phi,\Pi}(p, i) P^\phi_{p,i} \cap u(x) \neq \emptyset\} \end{aligned} \tag{3}$$

$$\operatorname{Post}_{(g,U)} V^{\phi,\Pi}(x, p) = \left\{ \sum_{x' \in \mathit{Posts}_u} x' \mid \mathit{Posts}_u \in \mathit{Posts}_U \right\} \tag{4}$$

Now we can rewrite the proof rule for the synthesis of a *TreeLexPSM*:

$$
\begin{array}{l}
\forall\phi : I(q_0, Init^\phi) \geq 0 \\
\forall\phi\forall x \in S \times Q \forall(g,U) \in \mathcal{G}_\times^\phi \forall u \in U : \\
\qquad TI(x) \wedge I(x) \geq 0 \wedge g(x) \Rightarrow I(u(x)) \geq 0 \\
\forall\phi\forall\, \text{even}\, p \in \mathbb{N}_{<d} \forall x \in S \times Q \forall(g,U) \in \mathcal{G}_\times^\phi \forall i \in \mathbb{N}_{<2^h} : \\
\qquad O_p(x) \wedge TI(x) \wedge I(x) \geq 0 \wedge g(x) \wedge P_{p,i}^\phi(x) \Rightarrow \bigvee_{post \in \mathrm{Post}_{(g,U)}\, V^{\phi,\Pi}(x,p)} post \preceq_p^\varepsilon V^{\phi,\Pi}(x,p) \\
\forall\phi\forall\, \text{odd}\, p \in \mathbb{N}_{<d} \forall x \in S \times Q \forall(g,U) \in \mathcal{G}_\times^\phi \forall i \in \mathbb{N}_{<2^h} : \\
\qquad O_p(x) \wedge TI(x) \wedge I(x) \geq 0 \wedge g(x) \wedge P_{p,i}^\phi(x) \Rightarrow \bigvee_{post \in \mathrm{Post}_{(g,U)}\, V^{\phi,\Pi}(x,p)} post \prec_p^\varepsilon V^{\phi,\Pi}(x,p) \\
\hline
\forall\phi : \Pr\left(System^\phi \vDash Spec\right) = 1
\end{array}
$$

Figure 3: Proof rule of *TreeLexPSM*.

3 Future Work

For the time being a *TreeLexPSM* has d binary decision trees each one of height h; one possible improvement would be to allow different heights for each tree. This refinement would need further studies in order to be able to understand which of the binary trees requires a greater expressivity (height) or if it's the overall invariant I that has to be refined in an CEGIS based guess-check algorithm implementation.