Specification Mining for Cyber-physical Systems

Alexandre Donzé and Sanjit Seshia (UCB), Xiaoqing Jin (UCR), Jyotirmoy Deshmukh (Toyota)
Problem formulation

What specifications does this system satisfy?

Modeling an Automatic Transmission Controller

- Documentation of legacy code/model
- Mining specifications of prototype models can lead to bugs or undesired behaviors discoveries
Formalizing Specifications

Parametric Signal Temporal Logic (PSTL)

- “The speed never exceeds 120 and RPM never exceeds 4500”
  \[
  \square(speed \leq \pi_{\text{speed}}) \land \square(RPM \leq \pi_{\text{rpm}})
  \]
  where, e.g., \((\pi_{\text{speed}} \mapsto 120, \pi_{\text{rpm}} \mapsto 4500)\)

- “Eventually between time 0 and some unspecified time \(\tau_1\), the signal \(x\) is less than some value \(\pi_1\), and from that point for some \(\tau_2\) seconds, it remains less than some value \(\pi_2\)”
  \[
  \square[0,\tau_1](x < \pi_1) \land \square[0,\tau_2](x < \pi_2)
  \]

- “Whenever the system shifts to gear 2, it dwells in gear 2 for at least \(\tau\) seconds”
  \[
  \square\left(\left(\text{gear} \neq 2 \land \square[0,\varepsilon]\text{gear} = 2\right) \Rightarrow \square[\varepsilon,\tau]\text{gear} = 2\right)
  \]
Mining Algorithm

Iterative procedure alternating synthesis and falsification of candidate specifications

Exploits the quantitative satisfaction of STL formulas

\[ \rho(\varphi, \mathbf{x}, t) \geq 0 \text{ iff } (\mathbf{x}, t) \models \varphi \]
Falsification of STL

Looking for an input of the system leading to a violation of candidate specifications

Minimizing of the quantitative satisfaction function over the space of input signals

\[ \min_{\mathbf{u} \in \mathcal{U}} \rho(\varphi, S(\mathbf{u}), 0) \]
Parameter Synthesis

Looking for parameters values for a candidate specification

- Exploits monotonicity of formulas with respect to its parameters
  \[ \forall v, v', x : [x \models \psi(v(\tau)) \land v(\tau) \leq v'(\tau)] \Rightarrow x \models \psi(v'(\tau)) \]

- We developed an SMT-based approach to check monotonicity
  => Enables dramatically efficient binary search of parameters

- Avoids over-conservative specifications by tightening around the satisfaction boundary
Implementation and Results

Approach implemented as an extension of Breach toolbox

- Provides Simulink models with a sophisticated test harness supporting PSTL formulas and now specification mining

- Approach validated on an industrial model from Toyota (~4000 blocks)

- We found a suspicious behavior in a closed-loop prototype model of a diesel engine and an actual bug that was causing it