Verimag - TEMA Toyota

2017- 2018

October 23, 2018

Falsification of Cyber-Physical Systems (CPS)

Problem: Finding behaviors that do not satisfy a specification
Approach: Falsification formulated as black-box optimization

Black-box optimization

- Existing search methods (Genetic Algorithms, Evolutionary Strategies, Simulated Annealing, ***etc.***)
- Pros: no gradient information required, large classes of problems (continuous/discrete), practical efficiency
- Cons: local optimum traps, no guarantee of global optimality

Our goal: exploit the advantages (CPS as black boxes) and propose a method to detect and escape local optima

Coverage-based Combination of Search Methods

Two (orthogonal) measures defined on the search space

- *Coverage* to quantify search ”exploration” progress (diversity of tested behaviors)
- *Robustness* to quantify ”exploitation” progress (improvement of objective values)

Results

- *Detection of local optima* by monitoring evolution of these measures
- Strategies to *combine search methods*, based on their exploration/exploitation features
- *Experiments*: on vehicle control benchmarks, the combination is more efficient (than search algorithms used individually)

Coverage of Temporal Specifications

- Timed automata (TA) as temporal properties of input signals of interest. Note that STL can be translated to TA
- Method of generating *uniformly* traces of TA $\Rightarrow$ generating signals satisfying a temporal specification with statistical guarantee of coverage

Implementation

- Using the tool *Cosmos*[1] for uniform generation
- *Matlab interface* with *Breach* to automatically test uniformly generated input signals
- *Case study*: detecting saturation in a Delta-Sigma Analog-to-Digital Converters (TA used to model uncertainty in the signal period)

[1] **`http://cosmos.lacl.fr`** [Benoît Barbot (Univ Paris-Est), Nicolas Basset (VERIMAG), et al]