Robustness-Guided Temporal Logic Testing for Stochastic Hybrid Systems

Houssam Abbas(1), Bardh Hoxha(1), Georgios Fainekos(1) and Koichi Ueda(2)

(1) ASU CPS Lab Arizona State University
(2) MBD TOYOTA TECHNICAL CENTER

Problem Formulation

Model: A Stochastic Cyber-Physical System $\Sigma$ whose output is modeled as a parameterized stochastic process $Y(t; \theta)$. The parameter $\theta$ is a couple $(x_0, u)$. Where $x_0$ is the initial condition of the system, and $u$ parameterizes the input signal to $\Sigma$. The randomness can be the result of sensor noise and other physical factors. All testing happens within a bounded time domain $R$.

Specification: A metric temporal logic (MTL) formula $\phi$ that captures the system’s desired behavior.

Problem: For an MTL specification $\phi$, the falsification problem for SCPS consists of finding a parameter value $\theta = (x_0, u)$ of the system $\Sigma$ such that, on average, $\Sigma$ driven by $\theta$ does not satisfy specification $\phi$.

Average MTL robustness

The formulas are built from a finite number of atomic propositions which label regions of interest in the state space. The propositional formulas are formed using the traditional operators of conjunction ($\wedge$), disjunction ($\vee$), negation ($\neg$), implication ($\Rightarrow$), and equivalence ($\Leftrightarrow$). MTL formulas are obtained from the standard propositional logic by adding temporal operators such as eventually ($\text{eventually}$), always ($\text{always}$), and until ($\text{until}$). MTL also allows timing constraints.

MTL intuition

Robustness of MTL formulae

$Robustness$ is a functional that associates a real extended number to each sample path $y$ of $Y$. A positive robustness indicates that the signal satisfies the formula, and a negative value indicates that it falsifies it.

$\rho_\phi : (y, \omega, \theta) \mapsto \rho_\phi (y, \omega, \theta) \equiv \rho_\phi (\omega, \theta) \in [\infty, \infty]$.

The average robustness $\bar{U}(\theta)$ captures the average behavior of the system for that $\theta$. We minimize $\bar{U}(\theta)$ to find worst-case average behavior.

$\bar{U}(\theta) = \mathbb{E}[\rho_\phi (\omega, \theta)] = \int \rho_\phi (\omega, \theta) dP(\omega)$

Minimization and guarantees

$U_* = \inf \{ U(\theta) | \theta \in \Theta \}$

Use a variant of Simulated Annealing adapted to minimizing expectations.

$U(\theta)$

Example guarantee: for a given $\varepsilon > 0$ and $\delta > 0$, find number of samples $s.t.$

$Pr[|U(\theta_f) - U(\theta_i)| < \varepsilon] > \delta$


Implemented in the S-TaLiRo Toolbox

Specification: the normalized air-to-fuel ratio is always within $[0.9, 1.1]$.

Robustness minimization and Statistical MC

Prob[failure] = 0.3

Modeling from physics

56 state variables and black boxes

Finding Falsifying Trajectories for Deterministic Cyber Physical Systems

- Minimum Expected Robustness for Stochastic Cyber Physical Systems
- Parameter Estimation of MTL Formulas for Cyber Physical Systems

www.tinyurl.com/Staliro

Verification results

$U(\theta) = 0.948$

$U(\theta) = 0.048$

$Pr[\text{failure}] = 0.9956$

Recent examples of Automotive Recalls due to CPS Errors (2011-2012)

- No downshifting from 6th to 4th under certain operating conditions
- Rough idling or stalling due to compromised adaptive ECU
- Cruise control does not disengage unless turning off the ignition

Simulation and Stateflow engine models

Find values for the parameter vector $\theta$ such that $\phi$ is falsified:

Formal Specification $\phi$

Whenever the normalized air-to-fuel ratio is outside $[0.9, 1.1]$, it will settle back inside the range within 1 sec, and stay there for at least 1 sec.

$\phi = G_{[0.9, 1.1]}(\text{OutOfBounds}) \rightarrow F_{[0.9, 1.1]}(\text{InBounds})$