Falsification Problems

CPS Lab, ASU

1 Powertrain Control Verification Benchmark

The benchmark is from the HSCC 2014 paper:

Jin, Xiaoqing, et al. "Powertrain control verification benchmark." Proceedings of the 17th international conference on Hybrid systems: computation and control. ACM, 2014.

The model is presented there in detail. There is a slight modification made so that falsification of the requirements is a bit easier. To make the falsification problem more interesting, we extend the search space so that the amplitude and period of the input pulse signal can be varying throughout the simulation. Furthermore, the timing in the occurrences when the signal rises/falls may be included in the search space.

Attached is a simulink model. Note that the attached model was recently tested with Matlab 2016b.

Requirements for the model as listed in the paper:

1. Closed-loop transient requirement (formula 26)'
2. Closed-loop settling time requirement (formula 27)'
3. Error tolerance (formula 29)'
4. Rich case excursion (formula 30)'
5. Lean case excursion (formula 31)'
6. Transition out of power mode (formula 32)'
7. Power mode performance (formula 33)'
8. Startup and sensor_fail modes performance (formula 34)'

2 Falsification of Properties of an Electro-Mechanical Braking System

The model of an Electro-mechanical braking system is described in the following paper:

Thomas Strathmann and Jens Oehlerking, "Verifying Properties of an Electro-Mechanical Braking System", EPiC Series in Computer Science, Volume 34,

2015, Pages 49–56 ARCH14-15. 1st and 2nd International Workshop on Applied veRification for Continuous and Hybrid Systems

The attached Simulink model will simulates this system's behavior for different input values. For the system to be well behaved we require some specifications to hold for all the possible values of vibration/noise, some of these requirements are mentioned below:

1. The position of the brake disc (x) reaches the set point x_0 with a tolerance ϵ within t_0 seconds and stays there.

$$\phi_1 = \Diamond_{[0,t_0]}\Box(x \geq x_0 - \epsilon \wedge x \leq x_0 + \epsilon)$$

2. the velocity of the caliper (v) should stay below 2 mm/s upon contact with the brake disc.

$$\phi_2 = \Box(x > x_0 \wedge X(x < x_0) \rightarrow v \leq 0.2$$

We need the following informal requirements to hold, too:

1. After a positive braking force is requested, it should be reached with an error margin of 10 percent within 0.02 time units.

2. For braking forces between 0 and 500, the current I should always stay below 2500.

3. If disk wiping is requested and the requested braking force is 0, contact with the brake disk ($F > 0$) should be achieved within 0.02 time units.

4. If no braking force is requested, the actual braking force should return to a value below 150 within 0.02 time units (even when disk wiping is requested).

5. For an input signal where the requested braking force is constant at 0, if disk wiping is continuously requested for at least 0.1 time units, the average braking force over this interval should be below 30.

All the aforementioned specifications should hold for the inputs InitialBrakeForce and BrackforceJump in the intervals [0 500] and [100 200] respectively.