Region Stable Hybrid Systems

Andreas Podelski[1] and Silke Wagner[2]

[1]Universität Freiburg, Germany
[2]Max-Planck-Institut für Informatik, Saarbrücken, Germany

We present our benchmarks which are typical instances of the verification problem that "every trajectory of a given hybrid system stabilizes w.r.t. a given region". This means that every trajectory eventually comes to a point where it lies within the region and never goes out again. Before this point the trajectory can run either inside or outside of the region; i.e., it can reach and leave the region any number of times.

Each of the next eight benchmarks is to illustrate a particular aspect of the verification problem. The other three benchmarks describe three well-known scenarios.

1 Monotonic System

Our first example (Fig. 1) is a hybrid system with one location and one continuous variable x. Initially the value of x is greater than 0; the flow condition is given by $\dot{x} = -1$. The region φ with respect to which we want to proof stability is given by $x \leq 0$.

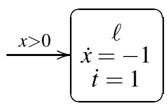

Fig. 1. Example 1.

Intuitively it is clear that all trajectories of the system must end up in the region φ (since the value of x is strictly monotonically decreasing by -1). For every single trajectory the amount of time that the trajectory can spend outside of the region φ is finite. However, the time that a trajectory can spend outside of φ is unbounded.

2 Simple Heating System

In our second example we consider a well-known heating system for a room ([1]), see Fig. 2.

This system is not stable in the classical sense (with respect to an equilibrium point). We want to show stability with respect to the region $x \in [65, 82]$.

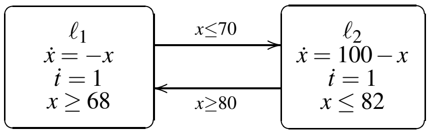

Fig. 2. Simple heating system.

3 More Complex Heating System

Our next example is a modification of the heating system that we have seen before. The modified heating system (Fig. 3) consists of three continuous variables x_p, x_e and t; x_p stands for the temperature of the room and x_e for the temperature of an internal engine.

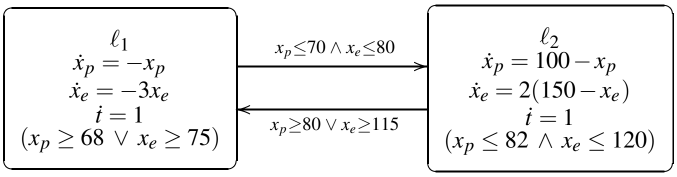

Fig. 3. Modified heating system.

The internal engine may overheat and switch off the heater temporarily, even though the desired temperature for the room (again given by $x_p \in [65, 82]$) is not yet reached. This means that, starting from low, the temperature will not increase strictly monotonically but it will also decrease during some periods of time. A side effect of this behavior is that a trajectory can reach the desired region but leaves it again for some time before it stabilizes.

4 One-tank Water System

In the following example we consider a one-tank water system (Fig. 4) with a constant inflow of water. The volume of water in the tank is denoted by x. The tank has a pipe such that water can also flow out of the tank again. The pipe can be opened for at most 8 seconds; after that the pipe must be closed again for 10 seconds. We want to know whether the tank can be drained, no matter what the initial volume of water is; i.e. we must check whether the system is stable with respect to $x \leq 0$.

As in the first example (Fig. 1), the time that a trajectory of this system can spend outside of the desired region is unbounded. Furthermore we prove in this example stability with respect to the equilibrium point $x = 0$. (Since the invariants of the system assure that $x \geq 0$, stability with respect to $x \leq 0$ implies stability with respect to the equilibrium point $x = 0$.)

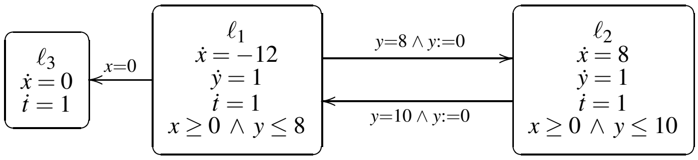

Fig. 4. One-tank water system.

5 Two-tank Water System

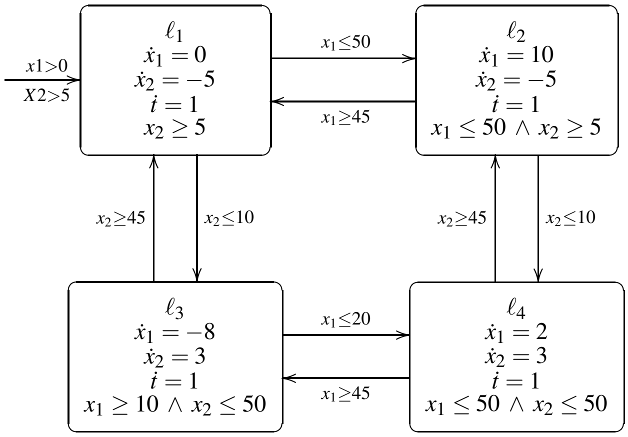

Fig. 5. Two-tank water system

Now we consider a two-tank water system consisting of two tanks one upon the other. The variables x_1 and x_2 denote the volume of water in the upper tank 1 and the lower tank 2, respectively. Water flows constantly out of the system from the lower tank. The system can switch on or off the inflow of water into the upper tank, and the flow of water from the upper to the lower tank; but both tanks must not overflow. The objective is to keep the water volume of the lower tank above 6, i.e. we are interested in stability with respect to the region $x_2 > 6$. The hybrid system that models this scenario consists of three continuous variables and four locations, see Fig. 5.

6 Distance Controller

The next example is a model of a distance controller, see Fig. 6. We consider two cars driving one after another. The leading car has a constant speed $v_1 > 0$. The second car is governed by a controller that continuously senses the distance between the two cars. If the distance is greater than a given value D_{acc} the second car speeds up; if the distance is smaller than D_{dec} it slows down. The second car has a maximum speed of $v_{\max}$ and a minimum speed of 0. The goal is to prove that the distance x between the two cars is always > 0 (this means that the two cars do not crash).

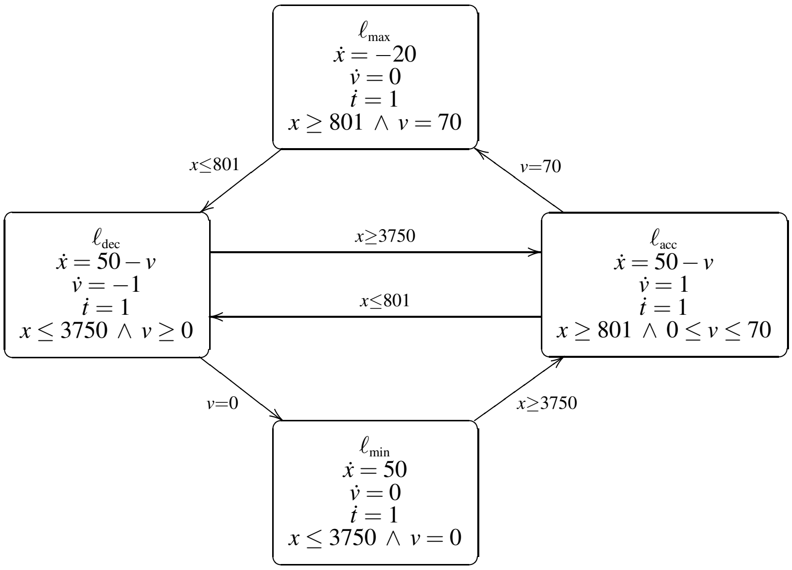

Fig. 6. Distance controller.

7 Bouncing Ball

This example is a modification of the well-known bouncing ball, see Fig. 7. A ball (thought of as a point-mass) is thrown horizontally against a wall. The distance between the wall and the thrower is denoted by x_t, the distance between the wall and the ball is denoted by x_b. We assume that the ball has a constant speed and does not lose any energy with a bounce. As soon as the thrower has thrown the ball he moves towards the wall until the ball returns to him; then he throws the ball again.

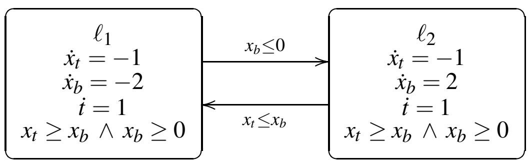

Fig. 7. Modified bouncing ball.

Each execution of the hybrid system in Fig. 7 is a Zeno execution, this means a solution of the system having infinitely many discrete jumps in finite time. Nevertheless we can show that the thrower can come arbitrarily close to the wall, i.e. we can prove stability of the system with respect to the region $x_t \leq \varepsilon$ for every $\varepsilon > 0$.

8 Train Breaks

In our next example we consider the braking behavior of a train, see Fig. 8. Initially the train is moving with a constant speed v. Eventually it starts braking, either with one break (if the speed is ≤ 200) or with two brakes (if the speed is > 200). There is a time delay between ordering the brake application and reaching the full brake effort. The braking capacity of the train depends on the speed. If the train is decelerated to a speed between 180 and 200 the second brake is released again. We want to prove stability of the system with respect to $v \leq 0$, i.e. we want to show that the train can always stop.

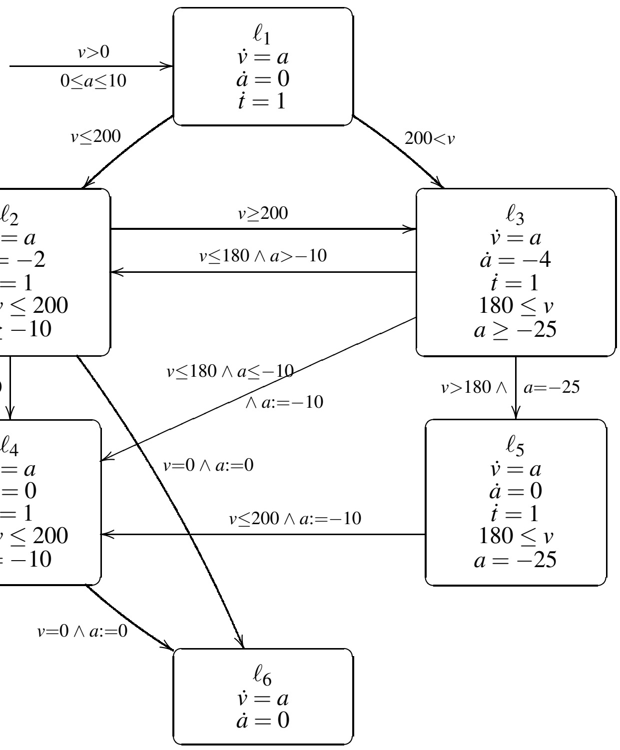

Fig. 8. Train brakes.

9 RLC circuit

We consider a series RLC circuit ([2]) with three branches, one resistor R, one inductor L and one capacitor C, see Fig. 9. Let x be the current through the inductor, and y be the current through the capacitor, respectively. We will prove that the system in Fig. 9 is stable for every $\varepsilon-$ball around the origin.

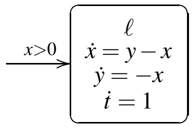

Fig. 9. Model of a series RLC circuit.

10 Pendulum

A simple gravity pendulum is a weight x on the end of a massless string, which, when given an initial push, will swing back and forth under the influence of gravity over its central (lowest) point. Its motion can be described as damped harmonic oscillation. We prove that the corresponding system (Fig. 10) is stable with respect to the region $x \leq \varepsilon$ for every $\varepsilon > 0$.

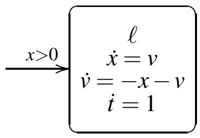

Fig. 10. Pendulum.

11 Chemical Reaction

We consider the energy E of an exothermic chemical reaction, namely the transformation from hydrogen and oxygen into water. During the reaction, the energy will first increase before it starts decreasing towards 0. The behavior of the energy is modelled by the hybrid system in Fig. 11. We prove stability of this system with respect to a small region around $E = 0$.

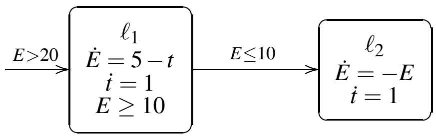

Fig. 11. Chemical reaction.

Results

The application of our tool to the examples listed above is fully automatic. There is no manual intervention. The table in Fig. 12 gives a comparison between numbers of variables, numbers of location, and the run times of our examples.

System	# Variables	# Locations	Run Time
Monotonic System	2	1	0.191s
Simple heater	3	2	0.490s
Complex heater	3	2	1.920s
Bouncing ball	3	2	4.209s
One tank system	3	3	1.813s
Distance controller	3	4	1.186s
Two tank system	3	4	16.545s
Train brake	3	6	2.589s
RLC circuit	2	2	0.449s
Pendulum	2	2	0.264s
Exothermic reaction	2	3	0.428s

Fig. 12. Experimental results (on a Pentium M 1,7GHz processor running Debian Linux 2.6.7)

References

1. T.A. Henzinger. The Theory of Hybrid Automata. In Logic in Computer Science (LICS), 1996.

2. M. Hirsch, and S. Smale. Differential Equations, Dynamical Systems, and Linear Algebra. In Academic Press, 1974.

3. A. Podelski, and S. Wagner. Model Checking of Hybrid Systems: From Reachability towards Stability. In Hybrid Systems: Computation and Control (HSCC), 2006.

4. A. Podelski, and S. Wagner. A Method and a Tool for Automatic Verification of Region Stability for Hybrid Systems. In MPI-I-2007-2-001 technical report, 2007. (See http://www.mpi-inf.mpg.de/~swagner/MPI-TechRep_07.pdf)

5. A. Podelski, and S. Wagner. A Sound and Complete Proof Rule for Region Stability of Hybrid Systems. In Hybrid Systems: Computation and Control (HSCC), 2007.

6. A. Podelski, and S. Wagner. Region Stability Proofs for Hybrid Systems. In Formal Modelling and Analysis of Timed Systems (FORMATS), 2007, to appear.