Thermostat (CAV 2010)

AVACS H4
Phase 2

July 28, 2011

1 Description of the Model

We consider in this test case an extension of the thermostat example described in [1]. A sketch of the model is depicted in Figure 1 There are four modes: *Cool*, *Heat*, *Check* and *Error*. The latter mode models the occurence of a failure, where the temperature sensor gets stuck at the last checked temperature.The set of variables $\{t,\ x,\ T\}$ where T represents the temperature, t represents a local timer and x is used to measure the total time passed so far. Thus, in all modes it holds that $x = 1$ and $t = 1$. In each mode there is also an invariant constraint restricting the set of state space for this mode. Invariant constraints are only for the sake of convenience and comparison with [1]. The

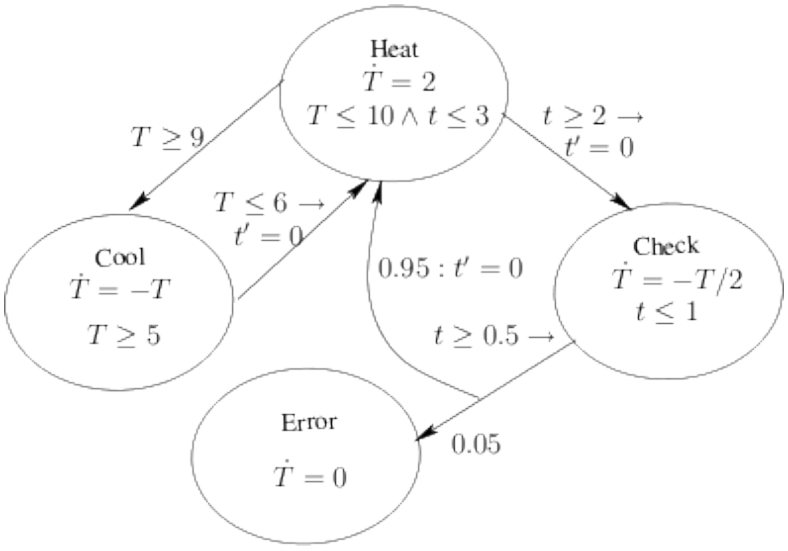

Figure 1: Sketch of the Thermostat model

initial condition is assumed to be $m = Heat \wedge t = 0 \wedge x = 0 \wedge 9 \leq T \leq 10$. The unsafe constraint is $m = Error \wedge x \leq 5$. We can interpret the probability of reaching the set of unsafe states as the probability of reaching the *Error* mode within time 5. Assume that

Time bound	Interval 2 Probability	Build (s)	Abstract states
2	0	0	11
4	0.050	0	43
5	0.097	1	58
20	0.370	20	916
40	0.642	68	2207
50	0.884	134	4916
120	0.940	159	4704
160	0.986	322	10195
180	0.986	398	10760

Time bound	Interval 10 Probability	Build (s)	Abstract states
2	0	0	8
4	1	0	12
5	1	0	13
20	1	1	95
40	0.512	30	609
50	1	96	1717
120	0.878	52	1502
160	0.954	307	4260
180	0.961	226	3768

Table 1: Peformance Statistics for Thermostat

the threshold for this risk is 0.1. In general, the verification of this property is not trivial (For time bound 5, we show in section 2 that the safety property is indeed satisfied by analysing the system analytically and illustrate how a safe upper bound can be otained by abstraction).

2 Results

ProHVer [3] can verify previouly mentioned property on the thermostat within 10 seconds after building the abstract state space. Here, we only give the building time for the abstraction of the automata, as the time to compute the upper bounds for the reachability probabilities is negligible. In Table 1 we give probability bounds and performance statistics for different time bounds. For the upper table, we used a partioning interval of length 2 but 10 for the one on the right side for variable x. We observe that the time needed for the analysis as well as the number of states of the abstract transition system grows about linearly in the time bound, though with large oscillations. Comparing the

Time bound	Interval 2	Interval 4	Interval 6	Interval 8	Interval 10
2	0	0	0	0	0
4	**0.050**	1	1	1	1
5	0.097	**0.050**	1	1	1
20	0.370	0.337	**0.302**	**0.302**	1
40	0.642	0.560	**0.512**	0.537	**0.512**
80	0.884	0.796	0.796	**0.774**	1
120	0.940	1	1	1	**0.878**
160	0.986	0.961	0.954	**0.952**	0.954
180	0.986	0.962	**0.958**	0.961	0.961

Table 2: Different Intervals for Thermostat

upper and lower table, we see that for the larger interval we need less resources, as was to be expected.

Due to the way *PHAVer* [2] splits locations among intervals, for some table entries, we see somewhat counter-intuitive behaviour. We observe that bounds do not necessarily improve with decreasing interval length. This is because *PHAVer* does not guarantee abstractions with smaller intervals to be an improvement, though they are in most cases. Furthermore, the abstractions we obtain from *PHAVer* can not guarantee probability bounds to increase monotonically with the time bound. This is because a slightly increased time bound might induce an entirely different abstraction, leading to a tighter probability bound and thus giving the impression of a decrease in probability, even though the actual maximal probability indeed stays the same or increases. In Table 2 we give the upper bounds for different interval widths. An interesting observation is that, even though smaller interval widths lead to better result on average, the tightest bounds (in bold fonts) are obtained via different interval widths for different time bounds. This might be due to the complicated form of the continuous dynamics in this case study: the temperature drops exponentially fast. In *PHAVer*, a new angle for the polygon-bounded overapproximation of the reachable states is chosen at each point a new abstract state is started due to the end of the interval length being reached. We conjecture that in some cases when choosing a smaller interval length, due to different angles being selected, we include different actually unreachable behaviour. Under unfavorable conditions, we include behaviour which allows reaching the unsafe state with a higher probability than in the case of a larger interval length. More measurings including not only the upper bounds for different interval widths, but also lower bounds are given in Appendix A.

It therefore seems worthwhile to explore techniques more adapted to the generation of transition systems for probabilistic hybrid automata, especially by adjusting the splitting of states to a method better adapted to our needs.

3 Solving the Thermostat Analytically

First, we observe that the initial constraint of T is $t = 0$ and $9 \leq T \leq 10$. The system cannot stay in the mode *Heat* for 2 time units, as this would increase the temperature by 4 units which violates the invariant $T \leq 10$ at *Heat*. This means that the system must switch to mode *Cool* to decrease the temperature. It would take some amount of time (approximately 0.41) units to decrease the temperature until 6, such that the system can go back to *Heat*. Note that switching back to *Heat* would reset the local timer which implies that $t = 0$ and that $x \geq 0.41$. To reach the unsafe mode *Error*, the intermediate mode *Check* must be touched. Because of the guard $t \geq 2$ between *Heat* and *Check*, once the mode *Check* is reached, it holds that $t = 0$ and $x \geq 2.41$. Then, the system waits in *Check* at least 0.5 time units. After the probabilistic jump from *Check* is triggered, it holds that $x \geq 2.91$. Then, the unsafe state could be reached with probability 0.05. With probability 0.95 the system goes back to mode *Heat* and it holds that $t = 0$ and $x \geq 2.91$. Reiterating the above analysis, reaching *Error* from *Heat* would again take at least 2.5 time units, which implies that there is only one chance to hit the unsafe mode *Error* within time 5. Thus, the probability is bounded by *0.05*, which implies that the saftey property is indeed satisfied. Now, we consider an abstraction of

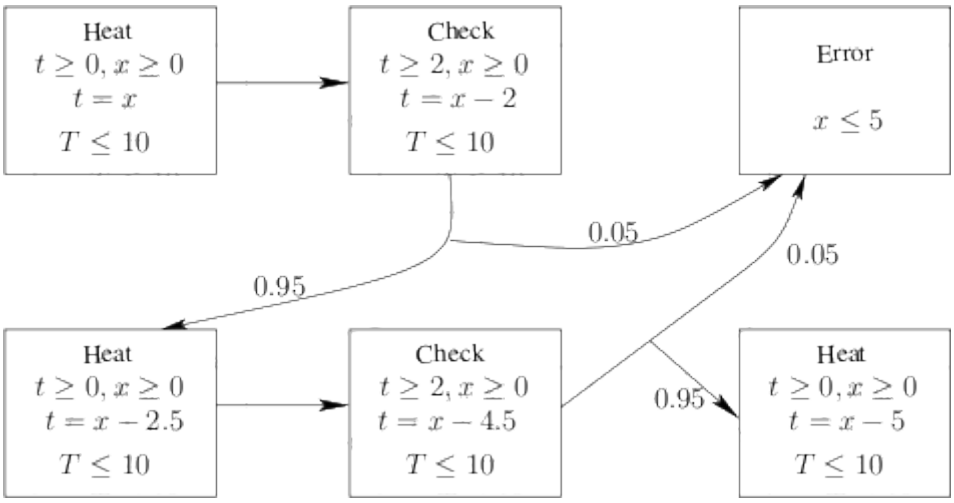

Figure 2: Abstraction of the Thermostat

the thermostat example. The initial abstract state is $(Heat,\ B)$, where B represents concrete valuations satisfying the constraint $t \geq 0$, $x \geq 0$, $t = x$ and $T \leq 10$. In Figure 2 we depicted fragments of the abstract states and of those abstract transitions which lead to abstract unsafe states. Notably, in this abstraction there are two chances to touch abstract unsafe states, thus the probability amounts to $0.05 + 0.95 \cdot 0.05 = 0.0975$. The reason is that from the initial state *Heat* the abstract automaton does not need to go back to *Cool* to let the temperature decrease. Instead, it can immediately switch to *Check*. This is due to the over-approximation of the abstract initial states. However, the computed probability for the threshold 0.1 is still good enough to prove the safety

property. If instead the threshold were set between 0.05 and 0.0975, refinement would have been needed.

References

[1] Rajeev Alur, Thao Dang, and Franjo Ivancic. Predicate abstraction for reachability analysis of hybrid systems. *ACM Transactions on Embedded Computing Systems*, 5(1):152–199, 2006.

[2] Goran Frehse. PHAVer: Algorithmic Verification of Hybrid Systems Past HyTech. pages 258–273. Springer, 2005.

[3] Lijun Zhang, Zhikun She, Stefan Ratschan, Holger Hermanns, and Ernst Moritz Hahn. Safety Verification for Probabilistic Hybrid Systems. In *CAV*, volume 6174 of *LNCS*, pages 196–211. Springer, 2010.

A Appendix

Time bound	Interval 0.5 Prob. Interval	Build (s)	Abstract states
1	[0.000, 0.000]	0	20
4	[0.000, 0.700]	10	917
5	[0.000, 0.910]	14	1051
10	[0.910, 0.992]	81	4330
15	[0.973, 0.999]	50	3216
20	[0.998, 1.000]	214	10676
25	[0.999, 1.000]	160	8671

Time bound	Interval 0.2 Prob. Interval	Build (s)	Abstract states
1	[0.000, 0.000]	0	79
4	[0.000, 0.700]	44	3590
5	[0.700, 0.910]	54	4066
10	[0.910, 0.992]	413	16773
15	[0.992, 0.999]	2578	53289
20	[0.999, 1.000]	1435	41313
25	[1.000, 1.000]	928	32864

Table 3: Additional Measurings with Lower- & Upper-Bounds of the Probabilities