MPRI - Course 2-8: verification of real-time systems

TD2 - undecidability

1 Stopwatch automata

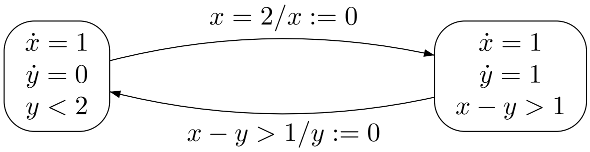

Figure 1: An example of an SA

Object of study. A stopwatch is a real variable which can have one of two dynamics: in some states it is $\dot{x} = 1$, in other states $\dot{x} = 0$. Intuitively it is a clock that can be stopped.

Stopwatch automata (SA) are hybrid automata where

- all continuous variables are stopwatches, there are finitely many of them;
- guards and invariants are boolean combinations of constraints $x < c$, $x \leq c$, $x - y < c$, $x - y \leq c$, where x, y are stopwatches, and c - integer constants;
- resets are as in timed automata: at a transition some stopwatches are reset to 0, while others stay unchanged.

We are mainly interested in the decidability of the predicate R, which is defined as follows: given an SA A and two of its control locations p and q, the predicate $R(A, p, q)$ is true if and only if there exists a run of A, starting at p with all the stopwatches at 0 and terminating at q with arbitrary values of clocks.

Undecidability proof

We suggest to encode a counter value n by two stopwatches x and y such that $x - y = n$.

- Give a black-box description (characterize the input-output relations) of gadget SAs that you need in order to simulate one counter.
- Build these gadgets.
- Give a black-box description (characterize the input-output relations) of gadget SAs that you need in order to simulate two counters.
- Build these gadgets.
- Terminate the proof of undecidability of R by simulation of a Minsky Machine.

Homework: Irrational Timed Automata

Object of study We consider the class of Irrational timed automata (ITA) which are just timed automata with the only difference that irrational constants of the form $k + j\sqrt{2}$ (with $k, j \in \mathbb{Z}$) are allowed in the guards. We are mainly interested in the decidability of the predicate R, which is defined as follows: given an ITA A and two of its control locations p and q, the predicate $R(A, p, q)$ is true if and only if there exists a run of A, starting at p with all the clocks at 0 and terminating at q with arbitrary values of clocks.

Undecidability

We suggest to choose an irrational number α (you are free to impose some restrictions on it) to encode a value of a counter $C = n$ by a clock value $x = \{n\alpha\}$ (curly brackets $\{,\}$ denote the fractional part).

- Establish that this encoding is injective: different values of n always give different values of x.
- Give a black-box description (characterize the input-output relations) of gadget ITAs that you need in order to simulate one counter.
- Build these gadgets.
- Give a black-box description (characterize the input-output relations) of gadget ITAs that you need in order to simulate two counters.
- Build these gadgets.
- Terminate the proof of undecidability of R by simulation of a Minsky Machine.