Model Checking Real-Time Systems

Written Abstract for the Seminar “Recent Advances in Model Checking”

Vincent Trélat

Organizational information

1 Introduction

2 Preliminaries

In this chapter, time values are equated with non-negative real numbers of $\mathbb{R}_{\geq 0}$. A *time sequence* is a finite or infinite non-decreasing sequence of time values. A *timed word* over some alphabet Σ is a finite or infinite sequence of pairs of $\Sigma \times \mathbb{R}_{\geq 0}$ such that the sequence formed with the second components of each pair is a time sequence. If the time sequence of a timed word is upper-bounded or converging, the timed word is said to be *converging*.

Let C be a finite set of variables called *clocks*. A *valuation* over C is a mapping $v\colon C \to \mathbb{R}_{\geq 0}$. The set of valuations over C is denoted by $\mathbb{R}_{\geq 0}^C$ and $\mathbf{0}_C$ denoted the valuation assigning 0 to every clock of C.

For any valuation v and any time value t, the valuation $v + t$ denotes the valuation obtained by shifting all values of v by t. For any subset r of C, $v[r]$ is the valuation obtained by resetting all clocks of r in v (i.e. set them to 0).

A *constraint* φ over C is recursively defined as follows:

- if $x \in C$, $k \in \mathbb{Z}$ and $\odot \in \{<, \leq, =, \geq, >\}$, then $x \odot k$ is a constraint over C,
- if φ_1 and φ_2 are constraints over C, then $\varphi_1 \wedge \varphi_2$ is a constraint over C.

The set of constraints over C is denoted by $\Phi(C)$. We say that a valuation v over C satisfies $x \odot k$ when $v(x) \odot k$, and when v satisfies a constraint φ, we write $v \models \varphi$. The set of valuations satisfying a constraint φ is denoted by $[\![\varphi]\!]_C$.

3 Timed Automata

Definition 1. A *Timed Automaton* (TA) is a tuple $\mathcal{A} = (L, l_0, C, \Sigma, I, E)$ where:

- L is a finite set of *locations* with initial location $l_0 \in L$;
- C is a finite set of *clocks*;
- Σ is a finite set of *actions*;
- $I\colon L \to \Phi(C)$ is an *invariant mapping*;
- $E \subseteq L \times \Phi(C) \times \Sigma \times 2^C \times L$ is a set of edges.

Any edge $(\ell, \varphi, a, r, \ell') \in E$ is denoted by $\ell \xrightarrow{\varphi, a, r} \ell'$ where φ is a *guard*, and r is a subset of clocks that are set to zero after taking the transition.