Real-Timed Automata

Lecture 4, 12.05.2014

Karin Quaas

Universität Leipzig, Germany

Lemma 3.4 There exists some $k \in \mathbb{N}$ such that for all timed words w we have $\mathsf{rotation}^k(w) = \mathsf{rotation}^m(w)$ for all $m \geq k$.

Proof. (Sketch) At some point of time all clocks have an integer value greater than cmax, hence the "last" region word is of the form $\emptyset \cdot \{(x, \infty) \mid x \in X\}$.

Lemma 3.5 Let r, r' be two clock regions. Further, let $w \in (2^{(X \times \mathsf{MAX})})^+$ be the word that represents r. Then r' is a time successor of r if, and only if, r' is represented by a word w' for which $w' \in \mathsf{rotation}^*(w)$.

The Region Graph Construction The *region graph* (also called *region automaton*) of a given timed automaton $\mathcal{A} = (\Sigma, \mathcal{L}, \mathcal{L}_0, \mathcal{L}_f, X, E)$, denoted by $\mathcal{R}(\mathcal{A})$, is a tuple $(\Sigma \cup \{\varepsilon\}, Q^{\mathcal{R}}, Q_0^{\mathcal{R}}, Q_f^{\mathcal{R}}, \to_{\mathcal{R}})$, where

- $Q^{\mathcal{R}} = \mathcal{L} \times \{r \mid r \text{ is a clock region over } X\}$,
- $Q_0^{\mathcal{R}} = \mathcal{L}_0 \times \{[\nu_0]\}$, where $\nu_0(x) = 0$ for every $x \in X$,
- $Q_f^{\mathcal{R}} = \mathcal{L}_f \times \{r \mid r \text{ is a clock region over } X\}$,
- $(l, r) \xrightarrow{\varepsilon}_{\mathcal{R}} (l, r')$ iff r' is a time successor of r,
- $(l, r) \xrightarrow{a}_{\mathcal{R}} (l', r')$ iff there exists t $\nu \in r$, $\nu' \in r'$ such that $(l, \nu) \xrightarrow{a}_D (l', \nu')$.

Recall that we want to reduce the reachability problem for timed automata to the reachability problem for *finite* graphs. That $\mathcal{R}(\mathcal{A})$ consists of *finitely* many nodes follows from Lemma 3.2. In the following we prove that the reduction of the reachability problem for timed automata to the reachability problem for the region graph is *correct*: The state (l, ν) (for some arbitrary clock valuation ν) is reachable in $\mathcal{A}$ if, and only if, (l, r) (for some arbitrary clock region r) is reachable in $\mathcal{R}(\mathcal{A})$. For this we use the theoretical concept of *bisimilarity*: we prove that $\mathcal{S}(\mathcal{A})$ and $\mathcal{R}(\mathcal{A})$ are *bisimilar*.

Correctness of the Reduction We define $(l, \nu) \equiv (l', \nu')$ iff $l = l'$ and $\nu \equiv \nu'$. We prove: $\equiv$ is a *time-abstract bisimulation relation*.

Lemma 3.6 [Bisimulation lemma]

1. If $(l_1, \nu_1) \equiv (l_1', \nu_1')$ and $(l_1, \nu_1) \xrightarrow{\delta}_T (l_2, \nu_2)$ for some $\delta \in \mathbb{R}_{\geq 0}$, then there exist $\delta' \in \mathbb{R}_{\geq 0}$ and (l_2', ν_2') such that $(l_1', \nu_1') \xrightarrow{\delta'}_T (l_2', \nu_2')$ and $(l_2, \nu_2) \equiv (l_2', \nu_2')$.

2. If $(l_1, \nu_1) \equiv (l_1', \nu_1')$ and $(l_1, \nu_1) \xrightarrow{a}_D (l_2, \nu_2)$ for some $a \in \Sigma$, then there exists (l_2', ν_2') such that $(l_1', \nu_1') \xrightarrow{a}_D (l_2', \nu_2')$ and $(l_2, \nu_2) \equiv (l_2', \nu_2')$.
3. If $(l_1, \nu_1) \equiv (l_1', \nu_1')$ and $(l_1', \nu_1') \xrightarrow{\delta}_T (l_2', \nu_2')$ for some $\delta' \in \mathbb{R}_{\geq 0}$, then there exist $\delta \in \mathbb{R}_{\geq 0}$ and (l_2, ν_2) such that $(l_1, \nu_1) \xrightarrow{\delta}_T (l_2, \nu_2)$ and $(l_2, \nu_2) \equiv (l_2', \nu_2')$.
4. If $(l_1, \nu_1) \equiv (l_1', \nu_1')$ and $(l_1', \nu_1') \xrightarrow{a}_D (l_2', \nu_2')$ for some $a \in \Sigma$, then there exists (l_2, ν_2) such that $(l_1, \nu_1) \xrightarrow{a}_D (l_2, \nu_2)$ and $(l_2, \nu_2) \equiv (l_2', \nu_2')$.

Proof. 1. – $(l_1, \nu_1) \equiv (l_1', \nu_1')$ implies $l_1 = l_1'$, and $\nu_1 \equiv \nu_1'$ (by definition of $\equiv$).
– $l_2 = l_1$ (by definition of $\rightarrow_T$), hence also $l_2 = l_1'$ (1)
– $\nu_2 = \nu_1 + \delta$ (2) (by definition of $\rightarrow_T$)
– By Lemma 3.1(a) there exists $\delta' \in \mathbb{R}_{\geq 0}$ such that $\nu_1 + \delta \equiv \nu_1' + \delta'$ (3).
– Hence there exists a timed transition $(l_1', \nu_1') \xrightarrow{\delta'}_T (l_2', \nu_2')$ where $l_2' = l_1'$ and $\nu_2' = \nu_1' + \delta'$ by definition of $\rightarrow_T$.
– By (1) we have $l_2' = l_2$, and by (2) and (3) we have $\nu_2' \equiv \nu_2$.

2. – $(l_1, \nu_1) \equiv (l_1', \nu_1')$ implies $l_1 = l_1'$ (1), and $\nu_1 \equiv \nu_1'$ (2) (by definition of $\equiv$).
– By $(l_1, \nu_1) \xrightarrow{a}_D (l_2, \nu_2)$ there exists $e = (l_1, a, \phi, \lambda, l_2) \in E$ with $\nu_1 \models \phi$ and $\nu_2 = \nu_1[\lambda := 0]$.
– By Lemma 3.1(b) and (2) we have $\nu_1' \models \phi$, we hence can also execute the edge e from (l_1', ν_1').
– By Lemma 3.1(c) we have in $(l_1', \nu_1') \xrightarrow{a}_D (l_2', \nu_2')$ with $\nu_2' = \nu_1'[\lambda := 0]$ also $\nu_2 \equiv \nu_2'$.

3. Analogously.
4. Analogously.

Let $(S, \rightarrow)$ und $(S', \rightarrow')$ be two directed graphs, not necessarily finite. Further let $s \in S$ und $s' \in S'$. Let $R \subseteq (S \times S')$ be a relation with $(s, s') \in R$. We say that R is a *bisimulation with respect to* (s, s') if for all $(s_1, s_1') \in R$ we have: (i) If $s_1 \rightarrow s_2$, then there exists $s_2' \in S'$ with $s_1' \rightarrow' s_2'$ and $(s_2, s_2') \in R$, (ii) If $s_1' \rightarrow' s_2'$, then there exists $s_2 \in S$ with $s_1 \rightarrow s_2$ such that $(s_2, s_2') \in R$. We say that $(S, \rightarrow)$ and $(S', \rightarrow')$ are *bisimilar with respect to s and s'* if there exists a bisimulation $R \subseteq (S \times S')$ with respect to (s, s') .

Next we prove that the two directed graphs $\mathcal{S}(\mathcal{A})$ and $\mathcal{R}(\mathcal{A})$ are bisimilar.

Lemma 3.7 $\mathcal{S}(\mathcal{A})$ and $\mathcal{R}(\mathcal{A})$ are bisimilar with respect to (l_0, ν_0) and $(l_0, [\nu_0])$.

Proof. Define $R = \{((l, \nu), (l, [\nu])) \mid \nu \text{ is a clock valuation for } X\}$. We prove that R is a bisimulation with respect to (l_0, ν_0) and $(l_0, [\nu_0])$. Clear: $((l_0, \nu_0), (l_0, [\nu_0])) \in R$. The following two cases are easy:

1. Assume $((l, \nu), (l, [\nu])) \in R$ and $(l, \nu) \xrightarrow{\delta}_T (l', \nu')$ for some $\delta \in \mathbb{R}_{\geq 0}$. Hence $\nu' = \nu + \delta$. Thus $[\nu']$ is a time successor of $[\nu]$. Hence by definition of $\rightarrow_{\mathcal{R}}$ we have $(l, [\nu]) \xrightarrow{\varepsilon}_{\mathcal{R}} (l, [\nu'])$.
2. Assume $((l, \nu), (l, [\nu])) \in R$ and $(l, \nu) \xrightarrow{a}_D (l', \nu')$ for some $a \in \Sigma$. By definition of $\rightarrow_D$ there exists some $e = (l, a, \phi, \lambda, l') \in E$ such that $\nu \models \phi$ and $\nu' = \nu[\lambda := 0]$. By definition of $\rightarrow_{\mathcal{R}}$ we also have: $(l, [\nu]) \xrightarrow{a}_{\mathcal{R}} (l', [\nu'])$.

Now we treat the two harder cases. For them we need the bisimulation lemma.

1. Assume $((l,\nu),(l,r)) \in R$ and $(l,r) \xrightarrow{\varepsilon}_{\mathcal{R}} (l,r')$. Hence r' is a time successor of r. Hence there exists $\nu_1 \in r$ and $\delta_1 \in \mathbb{R}_{\geq 0}$ such that $(\nu_1 + \delta_1) \in r'$ (by the definition of time successors). By definition of $\rightarrow_T$: $(l,\nu_1) \xrightarrow{\delta_1}_T (l,\nu_1+\delta_1)$. We have $\nu \in r$ and $\nu_1 \in r$, hence $\nu \equiv \nu_1$. Thus $(l,\nu) \equiv (l,\nu_1)$. By the bisimulation lemma there exists $\delta \in \mathbb{R}_{\geq 0}$ such that $(l,\nu) \xrightarrow{\delta}_T (l,\nu+\delta)$ and $(l,\nu+\delta) \equiv (l,\nu_1+\delta_1)$. Hence $(\nu+\delta) \in r'$. Hence $((l,\nu+\delta),(l,r')) \in R$.
2. Exercise.

We obtain the correctness of the reduction (use the definition of bisimulation!):

Corollary 1. *(l,ν) is reachable in $\mathcal{A}$ for some ν if, and only if, (l,r) is reachable in $\mathcal{R}(A)$ for some r.*

Next we consider the relation between timed languages recognized by a timed automaton and the (untimed) language recognized by the corresponding region automaton. Observe that the region graph contains transitions with so-called *ε-transitions*. From the theory of finite automata we know that for every finite automaton $\mathcal{A}$ *with ε-transitions* there exists a finite automaton $\mathcal{A}'$ without ε-transitions such that $L(\mathcal{A}) = L(\mathcal{A}')$. Let $\mathcal{B}$ be the finite automaton over Σ such that $L(\mathcal{B}) = L(\mathcal{R}(\mathcal{A}))$.

Corollary 2. $L(\mathcal{B}) = \mathsf{Untime}(L(\mathcal{A}))$

Proof. Let $w = a_1 \dots a_n \in L(\mathcal{B})$. Then $w \in L(\mathcal{R}(\mathcal{A}))$. Hence there is a successful run $(l_0,r_0) \xrightarrow{\varepsilon}_{\mathcal{R}} (l_0,r_0') \xrightarrow{a_1}_{\mathcal{R}} \cdots \xrightarrow{a_n}_{\mathcal{R}} (l_n,r_n)$ of $\mathcal{R}(\mathcal{A})$ on w, i.e., $l_0 \in \mathcal{L}_0$, $r_0 = 0^{|X|}$ and $l_n \in \mathcal{L}_F$. From the bisimulation lemma it follows that there exist $\delta_1,\dots,\delta_n \in \mathbb{R}_{\geq 0}$ such that the run of the form $(l_0,\nu_0) \xrightarrow{\delta_1}_T (l_0,\nu_0+\delta_1) \xrightarrow{a_1}_D \cdots \xrightarrow{a_n}_{\mathcal{R}} (l_n,\nu_n)$ with $\nu_i \in r_i$, $\nu_i + \delta_{i+1} \in r_i'$ for all $i \in \{0,\dots,n\}$ is a run of $\mathcal{A}$ over the timed word $u = (a_1,t_1)\dots(a_n,t_n)$, where $t_i = \sum_{j=1}^{n} \delta_j$. This run is successful, hence $w \in L(\mathcal{A})$. Further we have $w = \mathsf{Untime}(u)$. Hence $w \in \mathsf{Untime}(L(\mathcal{A}))$.

Let $w = a_1 \dots a_n \in \mathsf{Untime}(L(\mathcal{A}))$. Then there exists a timed word $u = (a_1,t_1)\dots(a_n,t_n) \in L(\mathcal{A})$ for some $t_1,\dots,t_n \in \mathbb{R}_{\geq 0}$. Then there exists a successful run of $\mathcal{A}$ on u, e.g., of the form $(l_0,\nu_0) \xrightarrow{\delta_1}_T (l_0,\nu_0+\delta_1) \xrightarrow{a_1} (l_1,\nu_1)\dots(l_n,\nu_n)$, where $t_i = \sum_{1\leq j\leq i} \delta_j$ for every $i \in \{1,\dots,n\}$. By the bisimulation lemma there exists a run of the form $(l_0,[\nu_0]) \xrightarrow{\varepsilon}_{\mathcal{R}} (l_0,[\nu_0+\delta_1]) \xrightarrow{a_1}_{\mathcal{R}} \dots (l_0,[\nu_{n-1}+\delta_n]) \xrightarrow{a_n}_{\mathcal{R}}$ of $\mathcal{R}$ on w. This run is successsful, hence $w \in L(\mathcal{R}(\mathcal{A}))$. Thus $w \in L(\mathcal{B})$.

(Alternatively, you can find in the literature a direct construction that constructs from a timed automaton $\mathcal{A}$ a region graph that does not use ε-transitions. Hence, in this construction time successor transitions are not explicitly considered.)