Region Graphs

Another approach to the analysis of dense-time finite-state CTS's is based on the definition of an equivalence relation among the states. Let $\mathcal{D}$ be a CTS whose timed guards and progress conditions are boolean combinations of inequalities of the forms $t_i < c_i$ and $t_j > d_j$, where all constants c_i, d_j are non-negative and strictly smaller than K. We denote by $\lfloor t_i \rfloor$ the integer part of t_i, i.e., the largest integer not greater than t_i, and by $fr(t_i)$ the fractional part of t_i given by $fr(t_i) = t_i - \lfloor t_i \rfloor$. Obviously, $0 \leq fr(t_i) < 1$.

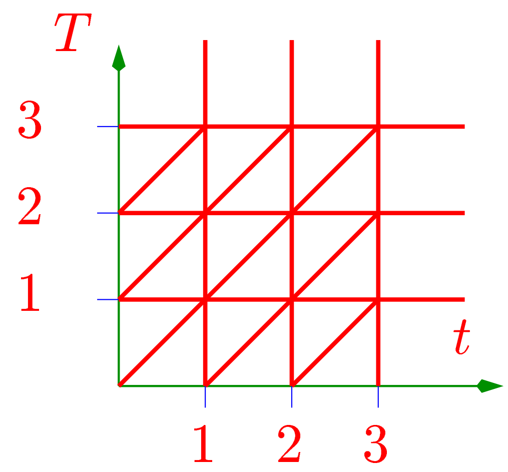
We say that states $(\overline{d}, \overline{t})$ and $(\overline{d}^*, \overline{t}^*)$ are equivalent, denoted $(\overline{d}, \overline{t}) \sim (\overline{d}^*, \overline{t}^*)$, if

- $\overline{d} = \overline{d}^*$. That is, the two states have an identical discrete part.
- For every $t_i \in C$, either $t_i > K$ and $t_i^* > K$, or $0 \leq \lfloor t_i \rfloor = \lfloor t_i^* \rfloor \leq K$.
- For every $t_i \geq t_j \in C$, either $t_i - t_j > K$ and $t_i^* - t_j^* > K$, or $0 \leq \lfloor t_i - t_j \rfloor = \lfloor t_i^* - t_j^* \rfloor \leq K$ and $fr(t_i - t_j) > 0 \leftrightarrow fr(t_i^* - t_j^*) > 0$.
- For every $t_i, t_j \in C$ such that $t_i \leq K$ and $t_j \leq K$, $sign(fr(t_i) - fr(t_j)) = sign(fr(t_i^*) - fr(t_j^*))$, including the case that $t_j = t_j^* = t_0 = 0$.

Let $[(\overline{d}, \overline{t})]$ denote the equivalence class of all states which are equivalent to $(\overline{d}, \overline{t})$. Obviously there is a finite number of equivalence classes which is bounded by $|D| K^n n!$, where $|D|$ is the number of all the different valuations of the discrete part of the state and n is the number of clocks.

Properties of Regions

Following is the partition of timed states into regions for the case of two clocks $C = \{t, T\}$ and $K = 3$.



In this diagram, there are 25 2-dimensional regions, $41 = 16+16+9$ 1-dimensional regions, and 16 0-dimensional regions.

The equivalence underlying the region definition is a bi-simulation relation. This is established by the following claims.

Claim 13. *Let $(\overline{d}, \overline{t})$ and $(\overline{d}^*, \overline{t}^*)$ be two states such that $(\overline{d}, \overline{t}) \sim (\overline{d}^*, \overline{t}^*)$, and let φ be an assertion formed as a positive boolean combination of inequalities $t_i - t_j \prec c_i$ and $t_i - t_j \succ d_i$, for $0 \leq c_i, d_j \leq K$, $i > 0$, $j \geq 0$. Then*

$$(\overline{d}, \overline{t}) \models \varphi \qquad \textit{iff} \qquad (\overline{d}^*, \overline{t}^*) \models \varphi$$

According to the definition of $\sim$, either $t_i > K$ and $t_i^* > K$, or $0 \leq \lfloor t_i \rfloor = \lfloor t_i^* \rfloor \leq K$ and $fr(t_i) > 0$ iff $fr(t_i^*) > 0$. In the first case, both states satisfy any constraint of the form $t_j > d_j$ and do not satisfy any constraint of the form $t_i < c_i$.

In the second case, also both states satisfy the same comparisons with any integer constant not exceeding K. A similar argument can be applied to clock differences of the form $t_i - t_j$. ∎

Continuation of Proof that $\sim$ is a Bi-Simulation

Claim 14. *For every states* $(\overline{d},\overline{t})$, $(\overline{d}^*,\overline{t}^*)$, *and* $(\overline{d}',\overline{t}')$, *such that* $(\overline{d},\overline{t}) \sim (\overline{d}^*,\overline{t}^*)$ *and* $(\overline{d}',\overline{t}')$ *is a* ρ_T*-successor of* $(\overline{d},\overline{t})$, *there exists a state* $(\overline{d}^{*\prime},\overline{t}^{*\prime})$, *such that* $(\overline{d}',\overline{t}') \sim (\overline{d}^{*\prime},\overline{t}^{*\prime})$ *and* $(\overline{d}^{*\prime},\overline{t}^{*\prime})$ *is a* ρ_T*-successor of* $(\overline{d}^*,\overline{t}^*)$.

$$\begin{array}{ccc}
\forall(\overline{d}^*,\overline{t}^*) & \xrightarrow{\rho_T} & \exists(\overline{d}^{*\prime},\overline{t}^{*\prime}) \\
\sim & & \sim \\
\forall(\overline{d},\overline{t}) & \xrightarrow{\rho_T} & \forall(\overline{d}',\overline{t}')
\end{array}$$

For the proof we consider separately the different types of transitions.

Consider the case that $(\overline{d}',\overline{t}')$ is obtained by applying a discrete transition to $(\overline{d},\overline{t})$, moving from discrete state d_i to discrete state d_j. In this case, $\overline{d} = d_i$, $\overline{d}' = d_j$, $\overline{t}$ satisfies g_{ij}, and $\overline{t}' = r_{ij}(\overline{t})$. We take $(\overline{d}^{*\prime},\overline{t}^{*\prime})$ to be $(d_j, r_{ij}(\overline{t}^*))$ and claim that, due to the equivalence $(\overline{d},\overline{t}) \sim (\overline{d}^*,\overline{t}^*)$, $\overline{d}^* = d_i$ and $\overline{t}^*$ satisfies g_{ij}. It follows that $(d_j, r_{ij}(\overline{t}^*))$ is a ρ_T-successor of $(\overline{d}^*,\overline{t}^*)$ and is equivalent to $(\overline{d}',\overline{t}')$.

Proof Continued

Next consider the case that $(\overline{d}', \overline{t}')$ is obtained by applying a $tick$ transition to $(\overline{d}, \overline{t})$, letting time increase by $\Delta > 0$. We define a state to be transient if $fr(t_i) = 0$ for some $t_i \in C$. The state is stable if $fr(t_i) > 0$ for all $t_i \in C$. Every $tick$ step can be broken into a finite sequence of $tick$-steps $(\overline{d}, \overline{t}) \rightarrow (\overline{d}, \overline{t} + \Delta_i)$, where $(\overline{d}, \overline{t} + \tau)$ is stable for every τ, $0 < \tau < \Delta_i$. Let t^*_m be a clock with the maximal fractional part in $\overline{t}^*$. We consider two cases:

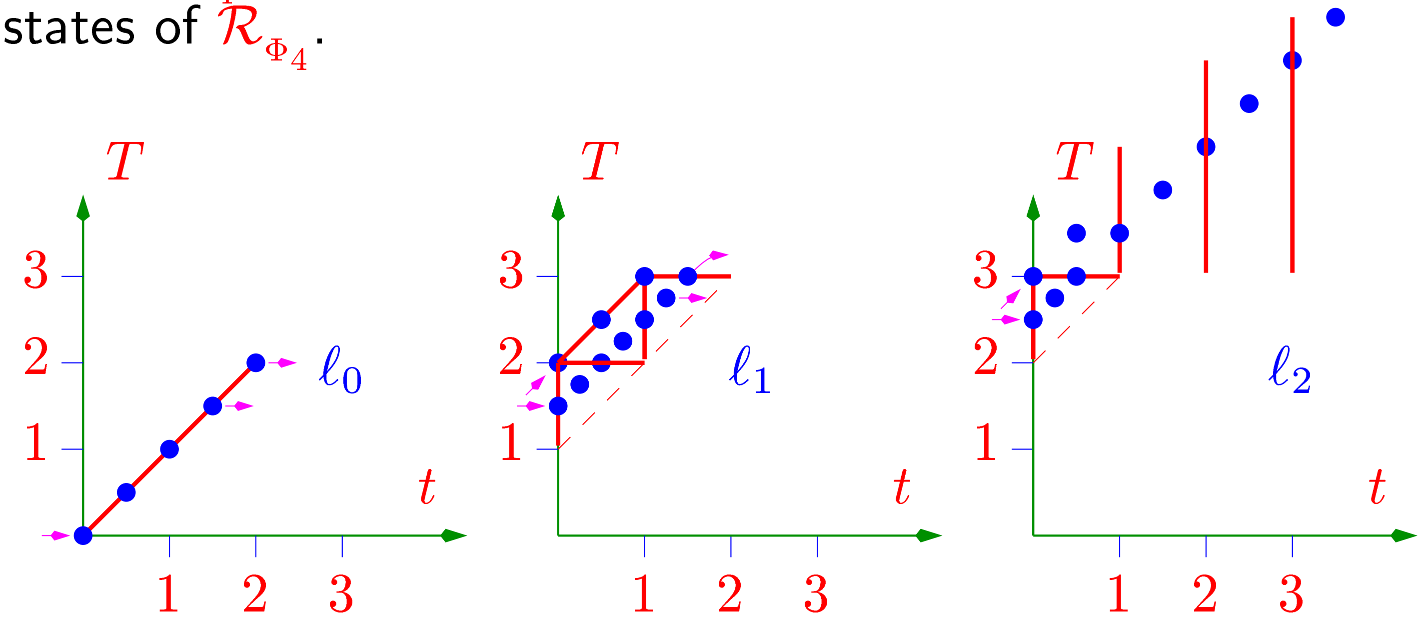
$(\overline{d}, \overline{t}+\Delta)$ **is stable**: We take Δ^* to be any number satisfying $0 < \Delta^* < 1 - fr(t^*_m)$. It can be shown that $(\overline{d}^{*\prime}, \overline{t}^{*\prime}) = (\overline{d}^*, \overline{t}^* + \Delta^*)$ is a stable state, equivalent to $(\overline{d}', \overline{t}') = (\overline{d}, \overline{t} + \Delta)$ and a $tick$-successor of $(\overline{d}^*, \overline{t}^*)$.

$(\overline{d}, \overline{t} + \Delta)$ **is transient**: We take $\Delta^* = 1 - fr(t^*_m)$. It can be shown that $(\overline{d}^{*\prime}, \overline{t}^{*\prime}) = (\overline{d}^*, \overline{t}^* + \Delta^*)$ is a transient state, equivalent to $(\overline{d}', \overline{t}') = (\overline{d}, \overline{t} + \Delta)$ and a $tick$-successor of $(\overline{d}^*, \overline{t}^*)$.

The Region Graph Automaton

For every finite-state CTS $\mathcal{D}$, we can construct a region-graph automaton $\mathcal{R}_\mathcal{D}$ whose locations are the different K-regions corresponding to the clock space of $\mathcal{D}$. There exists a transition from region r_i to region r_j iff there exist states $(\overline{d}, \overline{t})$, $(\overline{d}', \overline{t}')$ such that $(\overline{d}, \overline{t}) \in r_i$, $(\overline{d}', \overline{t}') \in r_j$, and $(\overline{d}', \overline{t}')$ is a ρ_T-successor of $(\overline{d}, \overline{t})$.

For example, $\mathcal{R}_{\Phi_4}$ is an automaton consisting of 82 regions. Below are all the reachable states of $\mathcal{R}_{\Phi_4}$.



$$\sigma_\mathcal{R} : \quad r_0, r_1, r_2, \ldots$$

is a run of $\mathcal{R}_\mathcal{D}$ iff there exists $\sigma : s_0, s_1, s_2, \ldots$ a run of $\mathcal{D}$ such that $r_i = [s_i]$ for every $i \geq 0$. The run $\sigma_\mathcal{R}$ is initialized iff the run σ is.

In most cases, σ is time-divergent iff it contains infinitely many states $(\overline{d}, \overline{t})$ such that $fr(t_i) = 0$ but $0 < t_i \leq K$ for some $t_i \in C$. For these cases, it is possible to define a set of accepting regions, which are the regions corresponding to such states. A computation of $\mathcal{R}_\mathcal{D}$ is then required to visit accepting regions infinitely often.

Region Equivalence Between Systems

A region-observation corresponding to a computation $s_0, s_1, \ldots$ is the infinite sequence of regions $[s_0], [s_1], \ldots$.

The finite-state CTS $\mathcal{D}_1$ is said to be region-equivalent to the finite-state CTS $\mathcal{D}_2$ if every observation $r_0, r_1, r_2, \ldots$ is equal, up to stuttering, to an observation of $\mathcal{D}_2$, and vice versa.

Obviously, if $\mathcal{D}_1$ is region-equivalent to $\mathcal{D}_2$, and φ is a K-bounded next-free LTL formula, then

$$\mathcal{D}_1 \models \varphi \qquad \text{iff} \qquad \mathcal{D}_2 \models \varphi$$