Verification of Real Time Systems - CS5270 7th lecture

Hugh Anderson

National University of Singapore
School of Computing

March, 2007

A warning...

Outline

1. Administration
   - Assignment 2
   - The road map...
2. Reducing complexity
   - Quotienting
3. Quotiented systems...
   - Regional equivalence

Outline

1. Administration
   - Assignment 2
   - The road map...
2. Reducing complexity
   - Quotienting
3. Quotiented systems...
   - Regional equivalence

Outline

1. Administration
   - Assignment 2
   - The road map...
2. Reducing complexity
   - Quotienting
3. Quotiented systems...
   - Regional equivalence

Outline

1. Administration
   - Assignment 2
   - The road map...
2. Reducing complexity
   - Quotienting
3. Quotiented systems...
   - Regional equivalence

Assignment 2

Assignment number 2:

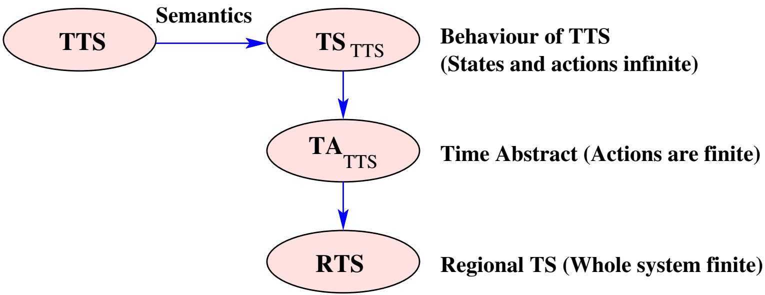
- On the web site
- Due on 22nd March

Outline

1. Administration
   - Assignment 2
   - The road map...
2. Reducing complexity
   - Quotienting
3. Quotiented systems...
   - Regional equivalence

The process...

Three steps...



The immediate road map

The topics:

- **TTS: Timed transition systems**
    - formal definition
    - parallel composition
    - Reduction of a TTS (which has possibly infinite states and actions) to $\mathrm{TA}_{\mathrm{TTS}}$ (which has infinite states and finite actions)$\mathrm{TTS} \longrightarrow \mathrm{TS}_{\mathrm{TTS}} \longrightarrow \mathrm{TA}_{\mathrm{TTS}}$

- Reduction of a $\mathrm{TA}_{\mathrm{TTS}}$ to a finite RTS by quotienting? $\mathrm{TA}_{\mathrm{TTS}} \longrightarrow \mathrm{RTS}$

- **Efficiency in TTS**
    - Regions
    - zones

Outline

1. Administration
   - Assignment 2
   - The road map...
2. Reducing complexity
   - Quotienting
3. Quotiented systems...
   - Regional equivalence

From TTS to $\mathrm{TS}_{\mathrm{TTS}}$ to $\mathrm{TA}_{\mathrm{TTS}}$ to quotiented TS

The reduction steps...

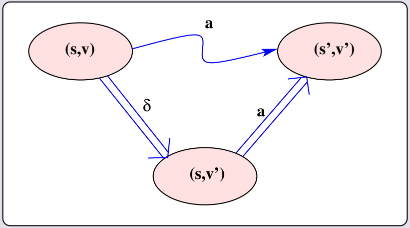
- $\mathrm{TTS} = (S, S_{\mathrm{in}}, \mathrm{Act}, X, I, \rightarrow)$
- $\mathrm{TS}_{\mathrm{TTS}} = (\mathcal{S}, \mathcal{S}_0, \mathrm{Act} \cup \mathbb{R}, \Longrightarrow)$
- $\mathrm{TA}_{\mathrm{TTS}} = (\mathcal{S}, \mathcal{S}_0, \mathrm{Act}, \rightsquigarrow)$
- $\mathrm{QTS}_{\mathrm{TTS}} = (\mathrm{QS}, \mathrm{QS}_0, \mathrm{Act}, \longrightarrow)$

Note that RTS and ZTS are examples of QTS.

Time abstract system

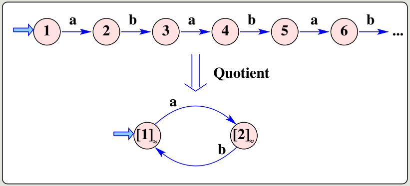
The view:

We derive a time-abstract transition system $\mathrm{TA}_{\mathrm{TTS}} = (\mathcal{S}, \mathcal{S}_0, \mathrm{Act}, \rightsquigarrow)$ from $\mathrm{TS}_{\mathrm{TTS}} = (\mathcal{S}, \mathcal{S}_0, \mathrm{Act} \cup \mathbb{R}, \Longrightarrow)$ where $(s, V) \overset{a}{\rightsquigarrow} (s', V')$ if and only if there exists a $\delta \in \mathbb{R}$ such that $(s, V) \overset{\delta}{\Longrightarrow} (s, V + \delta) \overset{a}{\Longrightarrow} (s', V')$



Quotienting to reduce TA to QTS

Infinite into finite



A suitable stable equivalence relation of finite index is *odd* and *even*. $i \approx j$ iff both i and j are odd, or if both i and j are even:

$$\begin{array}{lcll} \{1,3,5,\ldots\} & = & [1]_{\approx} & (= [3]_{\approx} = [5]_{\approx} = [7]_{\approx} \ldots) \\ \{2,4,6,\ldots\} & = & [2]_{\approx} & (= [4]_{\approx} = [6]_{\approx} = [6]_{\approx} \ldots) \end{array}$$

Stable equivalence relation of finite index

Or ... a finite index bisimulation ...

- Given $\mathrm{TA}_{\mathrm{TTS}} = (\mathcal{S}, \mathcal{S}_0, \mathrm{Act}, \rightsquigarrow)$, with $\approx \subseteq \mathcal{S} \times \mathcal{S}$ then
  - $s \approx s$ for every $s \in \mathcal{S}$ (i.e.$\approx$ is *reflexive*)
  - $s \approx s'$ implies $s' \approx s$ (i.e.$\approx$ is *symmetric*)
  - $s \approx s'$ and $s' \approx s''$ implies $s \approx s''$ (i.e.$\approx$ is *transitive*)
- $s \approx t$ and $s \overset{a}{\rightsquigarrow} s'$ implies that there exists t' such that $t \overset{a}{\rightsquigarrow} t'$ and $s' \approx t'$.
- $s \approx t$ and $t \overset{a}{\rightsquigarrow} t'$ implies that there exists s' such that $s \overset{a}{\rightsquigarrow} s'$ and $s' \approx t'$

$$\begin{tikzcd} s \arrow[r, phantom, "\approx"] \arrow[d, "a"] & t \arrow[d, "a"] \\ s' \arrow[r, phantom, "\approx"] & t' \end{tikzcd}$$

Quotiented $\mathrm{QTS}_{\mathrm{TTS}}$

The construction:

- Given $\mathrm{TA}_{\mathrm{TTS}} = (\mathcal{S}, \mathcal{S}_0, \mathrm{Act}, \rightsquigarrow)$
- Then given $\approx$ a (finite) quotient of $\mathrm{TA}_{\mathrm{TTS}}$, we have $\mathrm{QTS}_{\mathrm{TTS}} = (\mathrm{QS}, \mathrm{QS}_0, \mathrm{Act}, \longrightarrow)$
  - $\mathrm{QS} = \{[s]_\approx \mid s \in \mathcal{S}\}$
  - $\mathrm{QS}_0 = \{[s]_\approx \mid s \in \mathcal{S}_0\}$
  - $[s] \longrightarrow [s']$ if there exists $s_1 \in [s]$ and $s_1' \in [s']$ such that $s_1 \rightsquigarrow s_1'$ in $\mathrm{TA}_{\mathrm{TTS}}$
- Everything is now finite!

Quotiented QTS_{TTS} ... RTS? ZTS?

Skipped over...

- We have defined the quotiented transition system, without examining the particular form of quotienting to use.
- There are various quotients - we will examine
  - Regional equivalence
  - Zone eqivalence

Outline

1. Administration
   - Assignment 2
   - The road map...
2. Reducing complexity
   - Quotienting
3. Quotiented systems...
   - Regional equivalence

First step - rationals to integers...

Remember the definition of clock constraints?

- $I : S \rightarrow \Phi(X)$ assigns a clock invariant to each state. The clock constraints are limited to constraints of the form

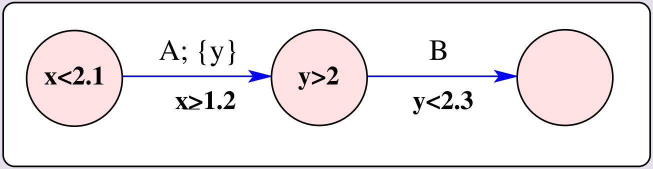
$$\Phi(X) = x \leq c \mid x \geq c \mid x < c \mid x > c \mid \phi_1 \wedge \phi_2$$

where $c \in \mathbb{Q}$ $\Longleftarrow$!

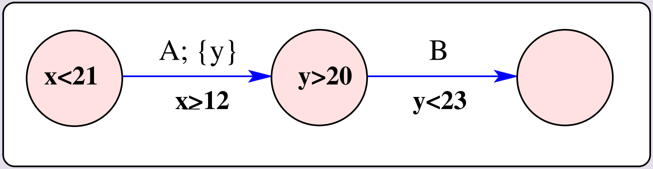
- There are only a finite number of rationals in any finite timed transition system.
- We can compute the least common multiple (LCM) k of all the denominators of all the (rational) constants in the original TTS, and then transform our system into a new one TTS' where every term like $x \leq c$ is changed to $x \leq k \cdot c$.

First step - rationals to integers...

Take the LCM of denominators of the time constants...



System TTS' has the same reachability properties...



$(s, V) \approx (s', V')$ based on regional equivalence

Assume we have this new TTS'...

- In this new transition system TTS', s is reachable if and only if it was reachable in the original TTS, and
- we have $(s, V) \approx (s', V')$ if and only if $s = s'$ and $V \equiv_{\mathrm{REG}} V'$ (V is regionally equivalent to V', or V belongs to the same region as V').

Second step - regional equivalence

Construct a stable equivalence relation of finite index $\equiv$

For any clock variable x, let C_x be the largest integer appearing in constraints involving x. We now construct a stable equivalence relation of finite index $\equiv_{\mathrm{REG}}$:

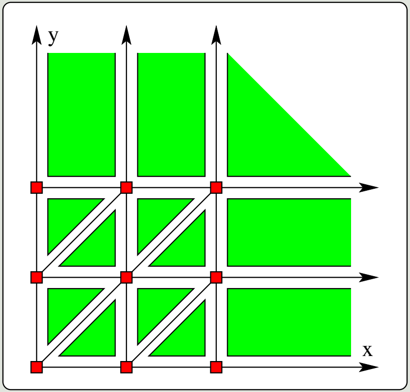
- $V \equiv_{\mathrm{REG}} V'$ if and only if the following three conditions are met for all clock variables, x and y:
  - $\lfloor V(x) \rfloor = \lfloor V'(x) \rfloor$, or $V(x) > C_x$ and $V'(x) > C_x$.
  - if $V(x) \leq C_x$ and $V(y) \leq C_y$ then $\mathrm{frac}(V(x)) \leq \mathrm{frac}(V(y))$ if and only if $\mathrm{frac}(V'(x)) \leq \mathrm{frac}(V'(y))$.
  - if $V(x) \leq C_x$, then $\mathrm{frac}(V(x)) = 0$ if and only if $\mathrm{frac}(V'(x)) = 0$.

What does this mean?

Regional equivalence

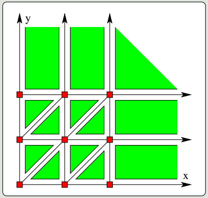
Consider a *TTS'* system

with two clocks $\{x, y\}$ with $C_x = 2$ and $C_y = 2$.



Regional equivalence

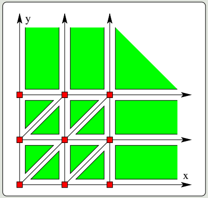
Consider the TTS' system



- Since we have two variables in the system, the regions can be of dimension 0, 1 or 2, i.e. points, lines or areas.
- We can visualize the regions by looking at the diagram where the points are marked with small shaded boxes, the lines are given as lines, and the areas are shaded.

Regional equivalence

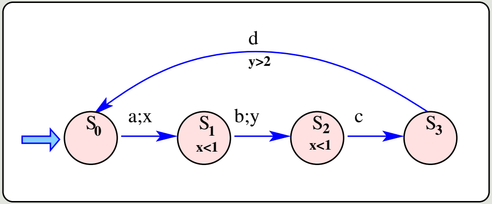
Consider the TTS' system

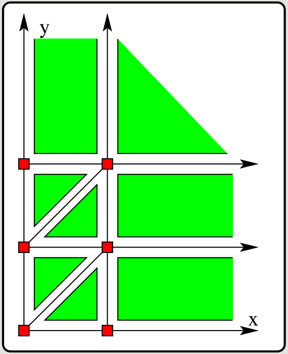


- 9 Points: $\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$
- 22 Lines: $\left\{ \begin{array}{cc} \{(x,y) \mid y = 0 \wedge 0 < x < 1\} & \{(x,y) \mid y = 0 \wedge 1 < x < 2\} \\ \{(x,y) \mid y = 1 \wedge 0 < x < 1\} & \{(x,y) \mid y = 1 \wedge 1 < x < 2\} \\ \ldots & \ldots \end{array} \right.$
- 13 Areas: $\left\{ \begin{array}{cc} \{(x,y) \mid 0 < x < y < 1\} & \{(x,y) \mid 0 < y < x < 1\} \\ \{(x,y) \mid 1 < x < y < 2\} & \{(x,y) \mid 1 < y < x < 2\} \\ \ldots & \ldots \end{array} \right.$

Regional equivalence

Regions for simple TTS





- In this example, $C_x = 1$ and $C_y = 2$.

Regional equivalence

Regions for simple TTS