Timed Automata

Lecture 11

GOALS OF TODAY'S LECTURE

- 1. Recall zone graphs

- 2. Simulations between zones

  ↳ Finite zone graphs for reachability

X : a set of clocks.

Zones: a set of valuations given by a conjunction of constraints:

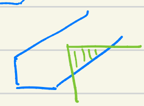
$$x - y \sim c \qquad\qquad c \in \mathbb{N}$$
$$x \sim c \qquad\qquad \sim \in \{<, \leq, =, \geq, >\}$$

Eg: $x - y \geq 14 \wedge y \leq 5$

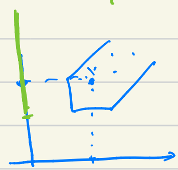
Operations on Zones:

Time-elapse: $\overrightarrow{Z} = \{ v + \delta \mid v \in Z, \ \delta \geq 0 \}$

Intersection: $Z \cap g = \{ v \mid v \in Z \text{ and } v \in g \}$



Reset : $[R]\, Z = \{ [R]v \mid v \in Z \}$



$$[R]v\,(x) = 0 \quad \text{if} \quad x \in R$$
$$= v(x) \quad\quad x \notin R$$

Symbolic transitions:

Suppose $t := q \xrightarrow[R]{g} q'$ is a transition

we have:

$$\boxed{(q, Z) \xrightarrow{t} (q', Z') \qquad \text{where: } Z' = \overrightarrow{[R](Z \cap g)}}$$

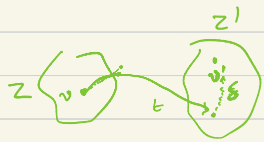
$$\boxed{Z \xrightarrow{g} Z \cap g \xrightarrow[R]{} [R](Z \cap g) \xrightarrow{\text{time}} \overrightarrow{[R](Z \cap g)}}$$

An important property of the symbolic transitions:

Lemma: Suppose $(q, Z) \xrightarrow{t} (q', Z')$ is a symbolic transition.

For every valuation $v' \in Z'$, there exists a valuation $v \in Z$ and a $\delta \geq 0$ s.t.

$$(q, v) \xrightarrow{\boxed{t, \delta}} (q', v')$$



Proof: $Z' = \overrightarrow{[R](Z \cap g)}$

Pick $v' \in Z'$

$\exists v_1 \in [R](Z \cap g)$ s.t. $v_1 \xrightarrow{\delta} v'$

$- \exists v_2 \in (Z \cap g)$ s.t. $v_2 \xrightarrow[{[R]}]{} v_1$

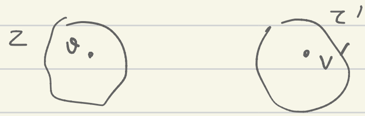
$v = v_2$

$(q, v) \xrightarrow{t} (q', v_1) \xrightarrow{\delta} (q', v')$

Is it true that $\forall v \in Z$,

$\exists v' \in Z'$

s.t. $(q, v) \xrightarrow{t, \delta} (q', v')$



$\rightarrow$ Not true. $-$ $Z \longrightarrow$ only $Z \cap g$ pass the transition.

Zone graphs are sound and complete:

Soundness:

Lemma: For every run on zones:

$Z_0 = \{v_0\}$

$$(q_0, Z_0) \xrightarrow{t_0} (q_1, Z_1) \xrightarrow{t_1} (q_2, Z_2) \xrightarrow{t_2} \cdots \xrightarrow{t_{n-1}} (q_n, Z_n)$$

there exists a corresponding timed run over valuations:

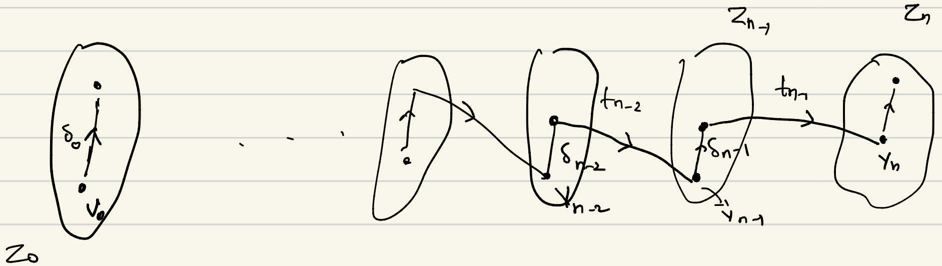
$$(q_0, v_0) \xrightarrow{\delta_0, t_0} (q_1, v_1) \xrightarrow{\delta_1, t_1} (q_2, v_2) \longrightarrow \cdots \xrightarrow{\delta_{n-1}, t_{n-1}} (q_n, v_n)$$

such that $v_i \in Z_i$

Proof: Pick some $v_n' \in Z_n$

From the symbolic transition $(q_{n-1}, Z_{n-1}) \xrightarrow{t_{n-1}} (q_n, Z_n)$
we have from previous lemma:

$$(q_{n-1}, v_{n-1}') \xrightarrow{t_{n-1}} \underset{\in Z_n}{(q_n, v_n)} \xrightarrow{\delta_n} (q_n, v_n')$$



Completeness:

Lemma: For every timed run

$$(q_0, v_0) \xrightarrow{\delta_0, t_0} (q_1, v_1) \xrightarrow{\delta_1, t_1} \cdots \xrightarrow{\delta_{n-1}, t_{n-1}} (q_n, v_n)$$

there exists a run over zones:

$$(q_0, Z_0) \xrightarrow{t_0} (q_1, Z_1) \xrightarrow{t_1} \cdots \xrightarrow{t_{n-1}} (q_n, Z_n)$$

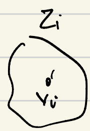
such that $v_i \in Z_i$

Proof: First: $Z_0 = \overrightarrow{\{v_0\}}$. Therefore $v_0 \in Z_0$

Assume that we have constructed a zone-run for i steps:

$$(q_0, Z_0) \xrightarrow{t_0} (q_1, Z_1) \xrightarrow{t_1} \cdots (q_i, Z_i)$$

s.t. $v_i \in Z_i$



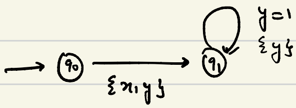
We know from the run that $v_i + \delta_i \models$ guard of t_i (g_i)

$$v_i + \delta_i \in Z_i \cap g_i$$

$$(q_i, Z_i) \xrightarrow{t_i} (q_{i+1}, Z_{i+1})$$

$\hookrightarrow$ non-empty and it contains v_{i+1}.

Zone graphs could be infinite:



$q_0, \; 0 \leq x = y$

$\downarrow$

$q_1, \; 0 \leq x = y$

$\downarrow$

$q_1, \; x - y = 1, \; (x, y \geq 0)$

$\downarrow$

$q_1. \; x - y = 2$

$\downarrow$

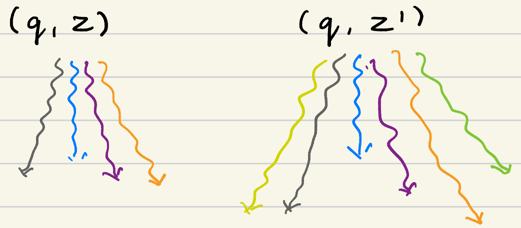
$\vdots$

Our main goal is to solve the reachability problem. We need an object that can detect all "reachable states" of the automaton.

Question: How do we get a finite "object" that is sound and complete for reachability?

Coming next: A framework for solving this question.

Simulations between zones:



Core idea: (q, z) is simulated by (q, z') if

> every path from (q,z) has a "corresponding" path from (q,z')

Formalizing this idea:

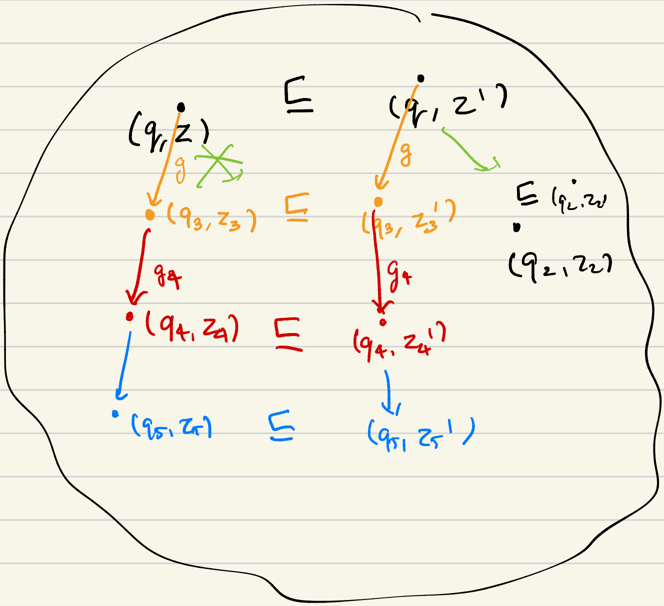
Define a binary relation which is "reflexive and transitive" $\sqsubseteq$ between nodes (q,z) and (q,z')

same discrete state q.

- that satisfies the following condition:

$$\begin{array}{ccc} (q, z) & \sqsubseteq & (q, z') \\ \forall \quad t \big\downarrow & & \exists . \big\downarrow t \\ (q_1, z_1) & \sqsubseteq & (q_1, z_1') \end{array}$$

For every transition $(q,z) \xrightarrow{t} (q_1, z_1)$ there exist a transition $(q, z') \xrightarrow{t} (q_1, z_1')$ s.t. $(q_1, z_1) \sqsubseteq (q_1, z_1')$



For example let us define $(q, Z) \sqsubseteq (q, Z')$

when $Z \subseteq Z'$

→ This is a simulation. But this need not give finiteness.

We want a simulation which is finite.

A particular simulation relation:

Let M be the maximum constant appearing in the automaton

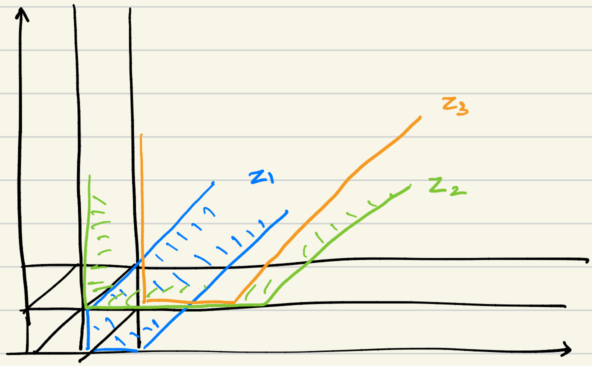
Regions $(Z) \subseteq$ Regions (Z')

$$(q, Z) \preccurlyeq_M (q, Z') \quad \text{if}$$

$$\boxed{\forall v \in Z, \quad \exists v' \in Z' \ \text{ s.t. } \ v \sim_M v'}$$

$\sim_M$ denotes region equivalence

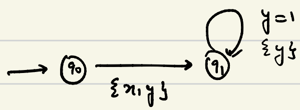
Theorem: $\preccurlyeq_M$ is a simulation relation on nodes.



$M = 2$

1. $Z_1 \preceq_M Z_2$? False
2. $Z_2 \preceq_M Z_1$? False
3. $Z_1 \preceq_M Z_3$? False
4. $Z_3 \preceq_M Z_1$? False. $(x=2, y>1)$

Example 1:



$q_0,\ 0 \le x = y$

$\downarrow$

$q_1,\ 0 \le x = y$ $\quad Z_1$

$\downarrow$

$q_1,\ x - y = 1,\ (x, y \ge 0)$ $\quad Z_1$

$\downarrow$

$q_1,\ x - y = 2$ $\quad Z_2$

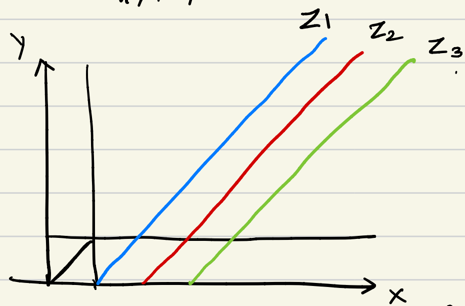
$\downarrow$

$\vdots$

$q_1,\ x - y = 3$

$M = 1$

Regions:



Regions intersected by red: $\{(x>1, y=0), (x>1, 0<y<1), (x>1, y=1), (x>1, y>1)\}$ → Regions(Z_1)

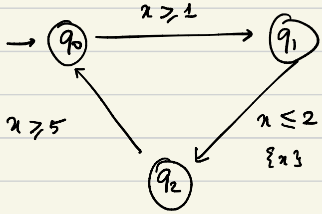
—— blue: $\{(x=1, y=0), (x>1, 0<y<1), (x>1, y=1), (x>1, y>1)\}$ → Regions(Z_2)

—— green: $\{(x>1, y=0), (x>1, 0<y<1), (x>1, y=1), (x>1, y>1)\}$ → Regions(Z_3)

$Z_2 \preccurlyeq_M Z_3$ and $Z_3 \preccurlyeq_M Z_2$

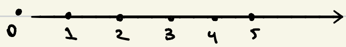
Regions(Z_2) $\subseteq$ Regions(Z_3)

Example 2:



$M = 5$, single clock.

Build the zone graph and draw the simulation edges.



$$q_0, \ x \geq 0 \longrightarrow q_1, \ x \geq 1 \longrightarrow q_2, \ x \geq 0 \longrightarrow q_0, \ x \geq 5$$

Summary:

- We have seen a relation $\preccurlyeq_M$ between zones:

$$Z \preccurlyeq_M Z' \text{ if}$$

$$\underset{\substack{\downarrow \\ \text{set of regions} \\ \text{that } Z \text{ intersects}}}{\text{Regions}(Z)} \subseteq \text{Regions}(Z')$$

$$(q, Z) \preccurlyeq_M (q, Z') \quad \text{if} \quad Z \preccurlyeq_M Z'$$

- What we have not seen:

  → $\preccurlyeq_M$ is a simulation

$$\begin{tikzcd} \bullet \arrow[r, phantom, "\preccurlyeq_M"] \arrow[d] & \bullet \arrow[d] \\ \bullet \arrow[r, phantom, "\preccurlyeq_M"] & \bullet \end{tikzcd}$$

  → $\preccurlyeq_M$ is "finite"

In every sequence of zones: $Z_1, Z_2, Z_3, \ldots\ldots Z_j \ldots Z_i$

$$\exists\, i > j \text{ s.t. } Z_i \preccurlyeq_M Z_j$$