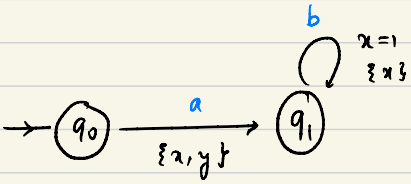
TIMED AUTOMATA

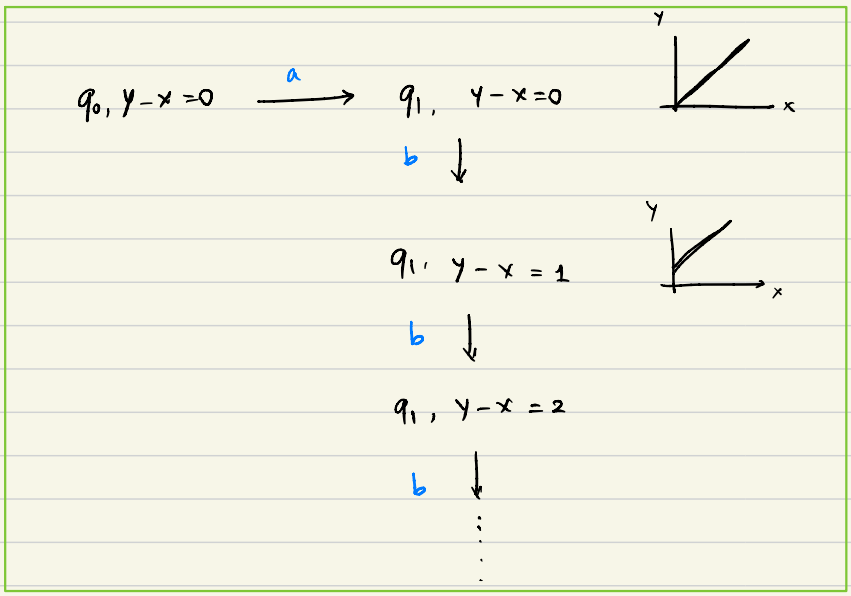
LECTURE 13

Plan for today:

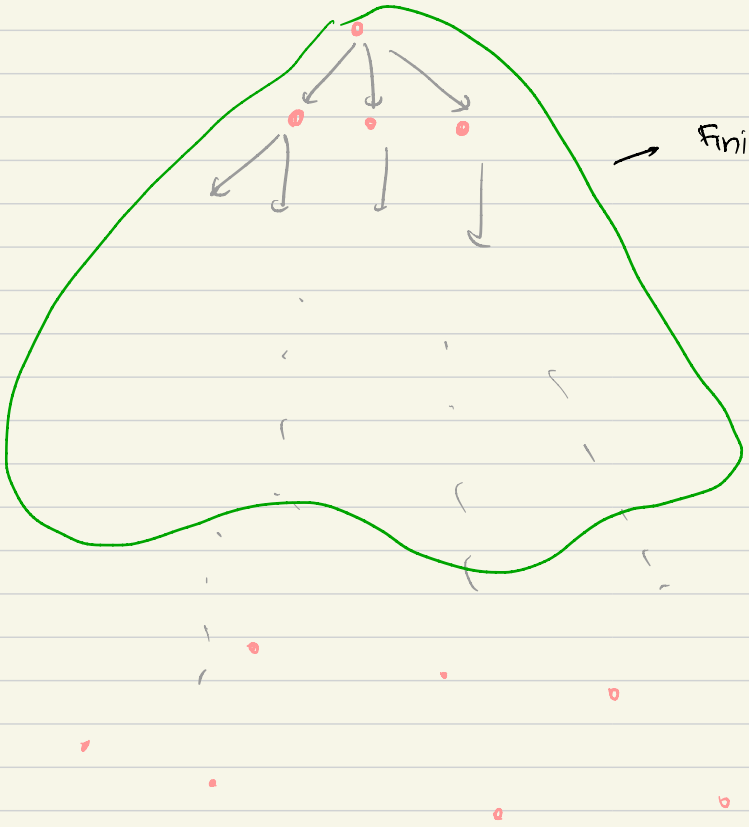
- Getting a finite truncation of the zone graph that is sound and complete for reachability

Recall:





← zone graph



→ Finite truncation that is correct for reachability

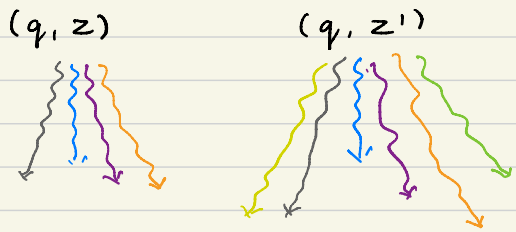
→ should contain all reachable states

Goal: 1. Get finiteness

2. Get a small finite truncation

Main idea: Use simulations between zones

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:

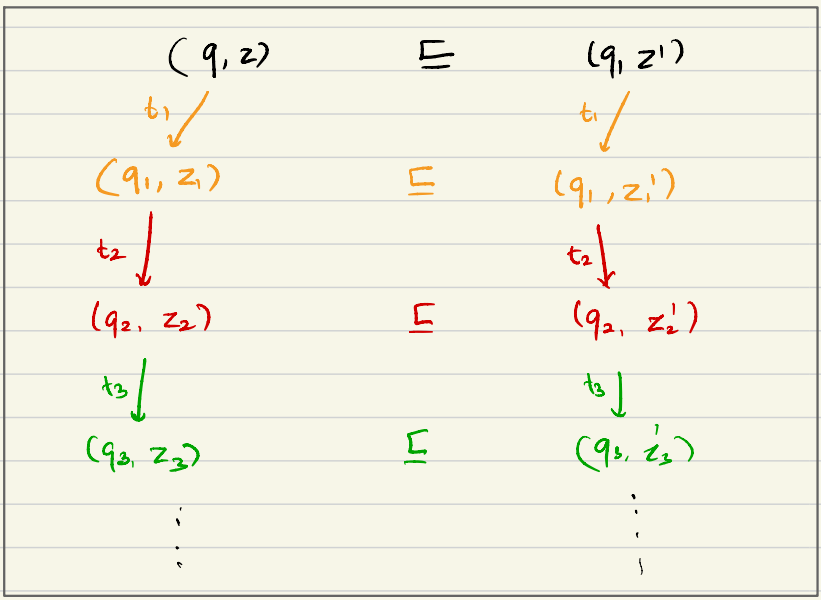
We will define a relation over nodes in the zone graph:

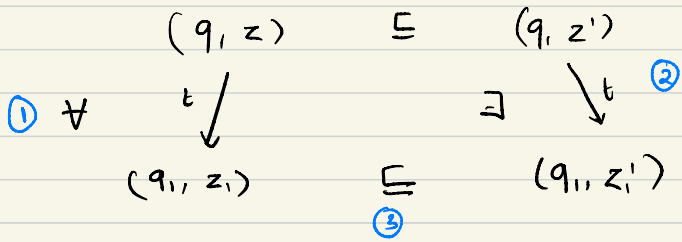
$$(q, z) \sqsubseteq (q, z')$$

The relation $\sqsubseteq$ satisfies the following properties:

- 1. $\sqsubseteq$ is reflexive and transitive.
- 2.

$$\begin{array}{ccc} (q, z) & \sqsubseteq & (q, z') \\ \textcircled{1}\ \forall \quad \downarrow t & & \exists \quad \downarrow t \ \textcircled{2} \\ (q_1, z_1) & \sqsubseteq & (q_1, z_1') \\ & \textcircled{3} & \end{array}$$





For every transition $(q,z) \xrightarrow{t} (q_1, z_1)$

there exists transition $(q, z') \xrightarrow{t} (q_1, z_1')$

such that $(q_1, z_1) \sqsubseteq (q_1, z_1')$

Find a simulation relation:

$(q, z) \quad \sqsubseteq \quad (q, z')$

relating nodes which have same control state

So we will consider relation $\sqsubseteq$ on zones.

$(q, z) \sqsubseteq (q, z')$ if $z \sqsubseteq z'$

- Task is to find a relation $\sqsubseteq$ on zones which will induce a simulation relation on nodes.

A first attempt at a simulation:

$Z \sqsubseteq Z'$ if $Z \subseteq Z'$

set inclusion

Is this a simulation?

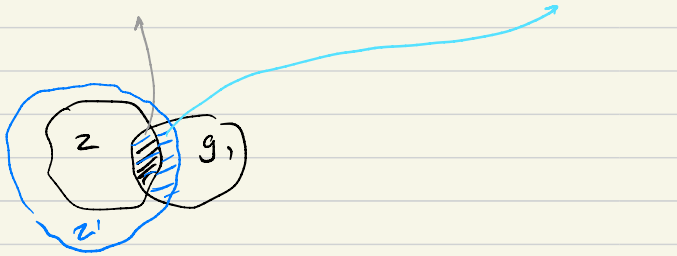
$(q_1, Z) \quad \sqsubseteq \quad (q_1, Z')$ when $Z \subseteq Z'$

symbolic transition from last lecture

$\xrightarrow{t_1, g_1, R_1}$ $\xrightarrow{t_1, g_1, R_1}$

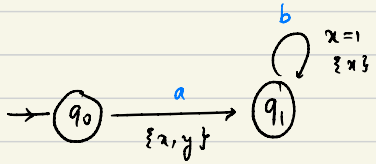
$(q_1, Z_1) \quad \sqsubseteq \quad (q_1, Z_1')$ $\quad Z_1 \subseteq Z_1'$

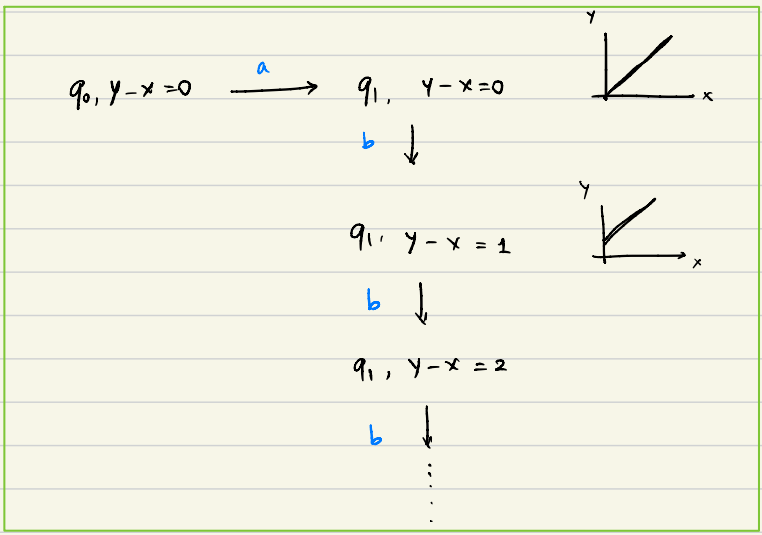
$Z_1 = \overrightarrow{[R_1](Z \cap g_1)}$ $\quad Z_1' = \overrightarrow{[R_1](Z_1' \cap g_1)}$



- Set inclusion is a simulation.

- So, are we done?





← zone graph

No pair $(q_1, y-x=i)$ $(q_1, y-x=j)$ $i \neq j$

is included in the other

- this gives no simulation in the above graph if we use set inclusion.

- Task is to get a "finite" simulation.

finite simulation:

A relation $Z \subseteq Z'$ is finite if:

for every sequence:

$$z_1 \quad z_2 \quad \ldots\ldots$$

$$\exists\ j > i \quad \text{s.t.}$$

$$\boxed{z_j \sqsubseteq z_i}$$

Simulation using regions: M- simulation

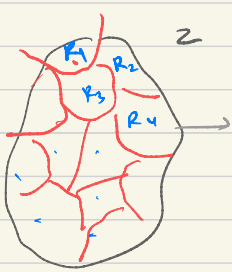
Let M be a max. bounds function attaching to each clock x the maximum constant appearing in a guard involving x.

$$Z \leq_M Z' \quad \text{if}$$

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

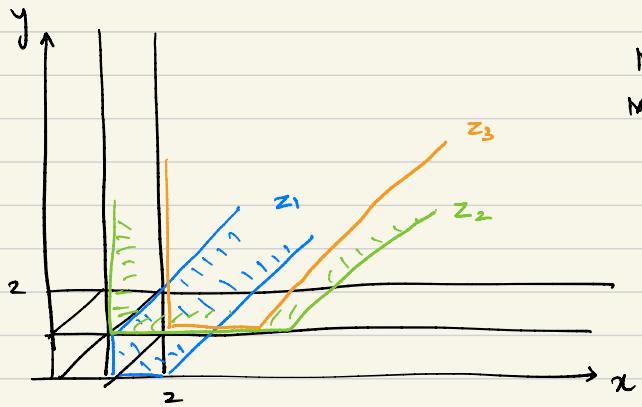
$\sim_M$ denotes region equivalence

$\text{Regions}_M(Z) \leq \text{Regions}_M(Z')$



$$\text{Regions}_M(Z) = \{ [v]_M \mid v \in Z \}$$

Recall: $z \preceq_M z'$ if $\text{Regions}_M(z) \subseteq \text{Regions}_M(z')$



$M_x = 2$

$M_y = 2$

1. $z_1 \preceq_M z_2$? No, $(1 < x < 2,\ 0 < y < 1,\ x < y) \in z_1 \notin z_2$.
2. $z_2 \preceq_M z_1$? No, $(1 < x < 2,\ y > 2) \in z_2, \notin z_1$
3. $z_1 \preceq_M z_3$? No, same as (1)
4. $z_3 \preceq_M z_1$?

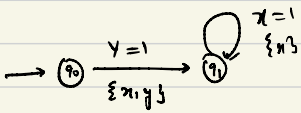
z_3: $x \geq 2$ (orange line coincide with black line)

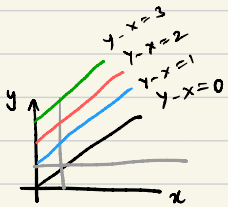
- $z_3 \not\preceq_M z_1$ $\quad y > 2,\ x = 2$

z_3: $x > 2$

- $z_3 \preceq_M z_1$

Example 1:





$(q_0, y-x=0) \longrightarrow q_1, y-x=0$

$\downarrow$

$q_1, y-x=1$

$\downarrow$

$q_1, y-x=2$ $\quad x=0, y>1$

$\preceq_M$

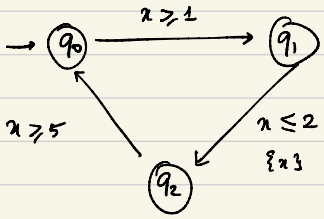
$\downarrow$

$q_1, y-x=3$

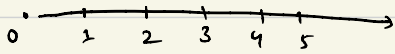
$y-x=3 \preceq_M y-x=2$

Using $\preceq_M$ gives a finite truncation.

Example 2:



$M = 5$, single clock.



$\simeq$ and $\leq_M$

$(q_0, x \geq 0) \longrightarrow (q_1, x \geq 1) \longrightarrow (q_2, x \geq 0)$

$(q_0, x \geq 5)$

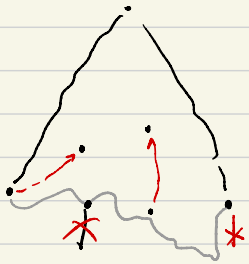
Simulation graph:

It is a finite truncation of the zone graph computed using the following algorithm.

- The algorithm maintains two lists: Passed & Waiting.

1) Add initial node (q_0, Z_0) to Waiting.
2) While Waiting $\neq \phi$ do.
3) - Pick (q, Z) from Waiting
4) - Add it to Passed.
5) - For every successor $(q, Z) \xrightarrow{t} (q_1, Z_1)$:
6) if $\exists (q_1, Z_1')$ in (Passed $\cup$ Waiting) s.t. $Z_1 \preceq_M Z_1'$
7) skip
8) else add (q_1, Z_1) to Waiting

↳ This algorithm computes a finite truncation of the zone graph.



Every leaf in the finite truncation is

either a deadlock (no enabled actions from this node)

or a covered node (there is a non-leaf node that simulates this)

Theorem: $(q, z) \preceq_M (q, z')$ is a simulation on the nodes of the zone graph.

(Exercise)

Theorem: $\preceq_M$ is finite.

(Exercise)

Theorem: $z \preceq_M z'$ can be done in $O(|X|^2)$

X is the no. of clocks.

↪ Ref: Better abstractions for timed automata
Herbreteau, Srivathsan, Walukiewicz '16.

This is as efficient as checking inclusion betn. zones.

Summary:

- We have given an algorithm to compute a finite truncation of the zone graph.
- This is based on: simulation: $Z \leq_M Z'$ when

$$\text{Regions}_M(Z) \subseteq \text{Regions}_M(Z')$$

Remark: Current tools use more sophisticated simulations. (out of scope for our course).