TIMED AUTOMATA

LECTURE 12

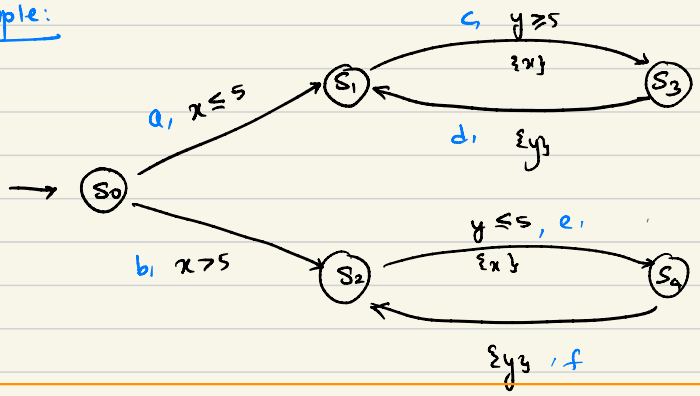
TODAY'S LECTURE:

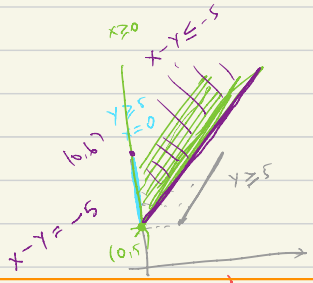
- Zone graphs
  - 1. More examples
  - 2. Formal definition
  - 3. Properties

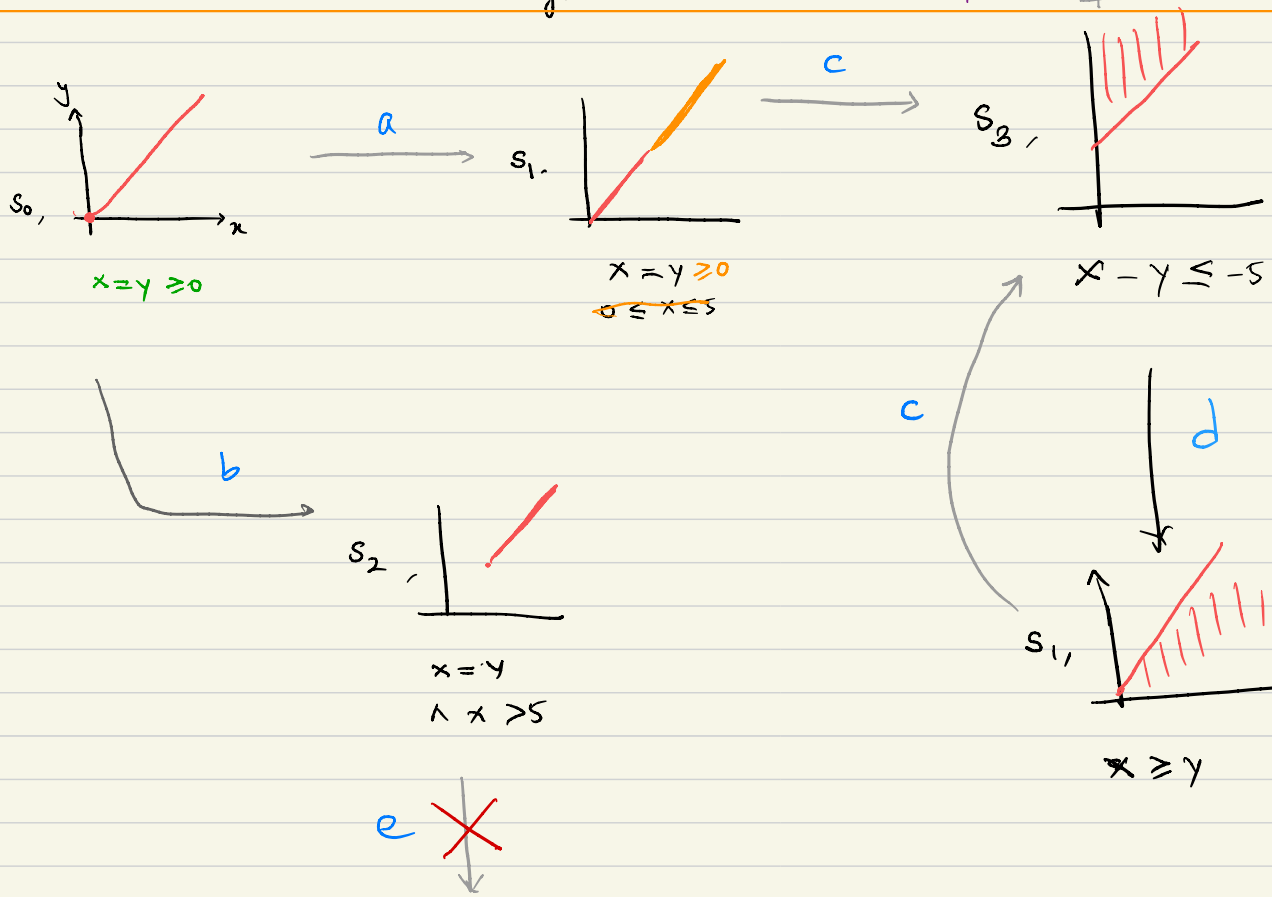
Zone graphs were introduced in the following paper:

Model-checking of real-time reachability properties using abstractions
Dawes & Tripakis, TACAS' 1998

Example:



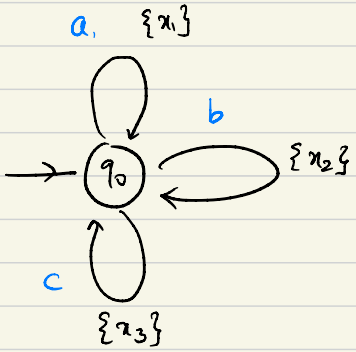




↓

Zone graph.

Example:



3 3 3
$x_1 = x_2 = x_3$ $\xrightarrow{\{x_1\}}$ 0, 3, 3
$x_2 = x_3 \geq 0$
$x_1 = 0$
↓ elapse 5
$0 \leq x_1 \leq x_2 = x_3$
5 8 8

0 0 0
q_0, $0 \leq x_1 = x_2 = x_3$

1 a → 0 1 1 q_0, $0 \leq x_1 \leq x_2 = x_3$

b → q_0, $0 \leq x_2 \leq x_1 = x_3$

c → q_0, $0 \leq x_3 \leq x_1 = x_2$

elapse 4 t.u. b

$x_1 = 4$
$x_2 = 5$
$x_3 = 5$
$\xrightarrow{\{x_2\}}$
$x_1 = 4$
$x_2 = 0$
$x_3 = 5$

elapse 3 t.u.

q_0, $0 \leq x_2 \leq x_1 \leq x_3$
3 7 8

a ↓

q_0, $0 \leq x_1 \leq x_2 \leq x_3$

Continuing this exploration, we get nodes with all different orderings of clocks.

abc $\xrightarrow{b}$ acb $\xrightarrow{a}$ cba

acb

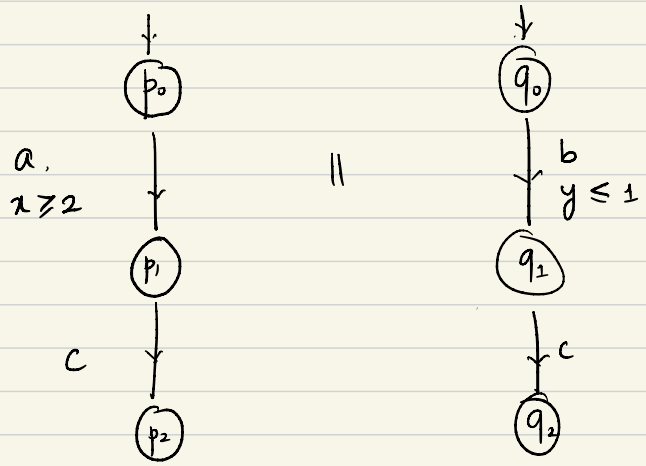
bac

bca

cab

cba

Example:



$\langle p_0, q_0 \rangle, \quad x = y \geq 0$

a

b

$\langle p_1, q_0 \rangle, \quad x = y \geq 2$

b ✗

disabled

$\langle p_0, q_1 \rangle, \quad x = y \geq 0$

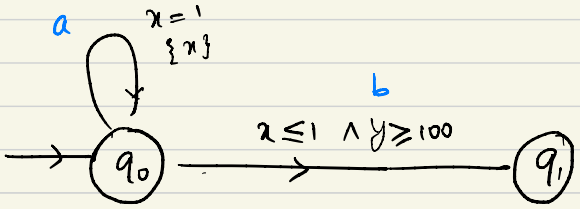
a

$\langle p_1, q_1 \rangle, \quad x = y \geq 2$

c

$\langle p_2, q_2 \rangle, \quad x = y \geq 2$

Example:



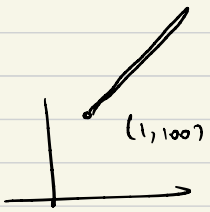
a

a

$q_0,\ y - x = 2$

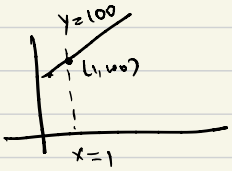
⋮

$q_0,\ y - x = 99$ —b→ $q_0,$



$y - x = 99$

$\wedge\ x \geq 1$



a

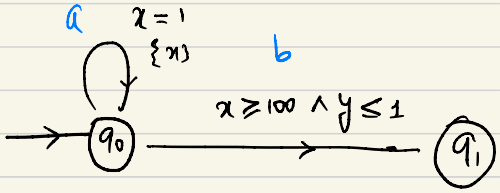
$q_0,\ y - x = 100$ —b→

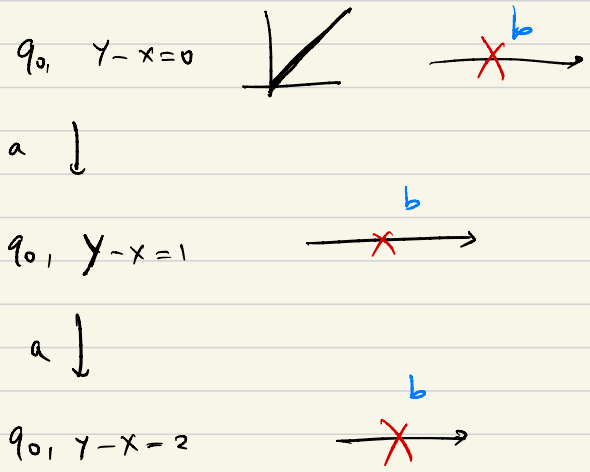
a

⋮

Zone graph is infinite!

Example:





Zone graph is infinite!

Zone graphs: formal definition:

Let X be a finite set of clocks.

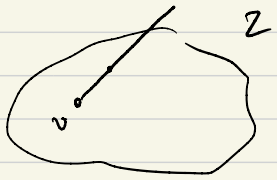
- A zone is a set of valuations over $\mathbb{R}_{\geq 0}^{|X|}$ given by conjunctions of two kinds of constraints:

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

Operations on zones:

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

(Z-elapse)



Guard intersection: Z, g (Z: zone, g: guard)

$$Z \wedge g = \{ v \mid v \in Z, v \models g \}$$

Reset: R: a set of clocks. Z, a zone

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

$$[R]v(x) = 0 \quad x \in R$$
$$= v(x) \quad x \notin R$$

Theorem: $\overrightarrow{Z}$, $Z \wedge g$, $[R]Z$ are all zones.

Symbolic transition:

$q \xrightarrow[R]{a,\ g} q'$ in the automaton.

$$(q, Z) \xrightarrow{a} (q', Z')$$

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

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

From the previous theorem, each of the intermediate sets of valuations is a zone.

Zone graph: definition

Nodes: (q, Z) q is a state of the automaton

Z is a zone.

Edges: for every $q \xrightarrow[R]{a,\ g} q'$

there exists a symbolic transition:

$$(q, Z) \xrightarrow{a} (q', Z')$$

$$Z' = \overrightarrow{[R][Z \cap g]}$$

Initial nodes: (q_0, Z_0) q_0 is an initial state of the automaton

$$Z_0 = \overrightarrow{\{v_0\}} \qquad v_0(x) = 0 \quad \forall x \in X$$

An important property of the symbolic transitions: (Post property)

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

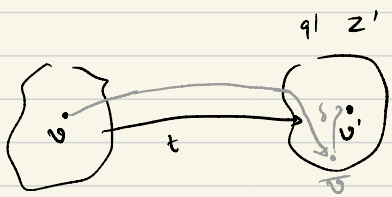
For every valuation $v' \in Z'$, there exists a valuation $v \in Z$ and a $\delta \geq 0$ s.t.

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

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

Proof:

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



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

For every $v' \in Z'$, there exists a $\bar{v} \in [R](Z \cap g)$ s.t.

$v' = \bar{v} + \delta$ for some $\delta \geq 0$.

For $\bar{v}$, there exists a $v \in Z$ s.t.

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

Question: Is this true? $\forall v \in Z \quad \exists v' \in Z'$ s.t.

$(q, v) \xrightarrow{t, \delta} (q', v')$? Not true

Zone graphs are sound and complete:

Soundness:

Lemma: For every run on zones:

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

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:

Completeness:

Lemma: For every timed run

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

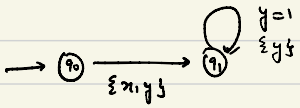
there exists a run over zones:

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

such that $v_i \in Z_i$

Proof: follows by definition of symbolic transition.

Zone graphs could be infinite:



q_0, $0 \le x = y$

↓

q_1, $0 \le x = y$

↓

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

↓

q_1, $x - y = 2$

↓

⋮

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?

Next lecture: A framework for solving this question.