Decidable Reachability for Initialized *Almost* Rectangular Hybrid Automata

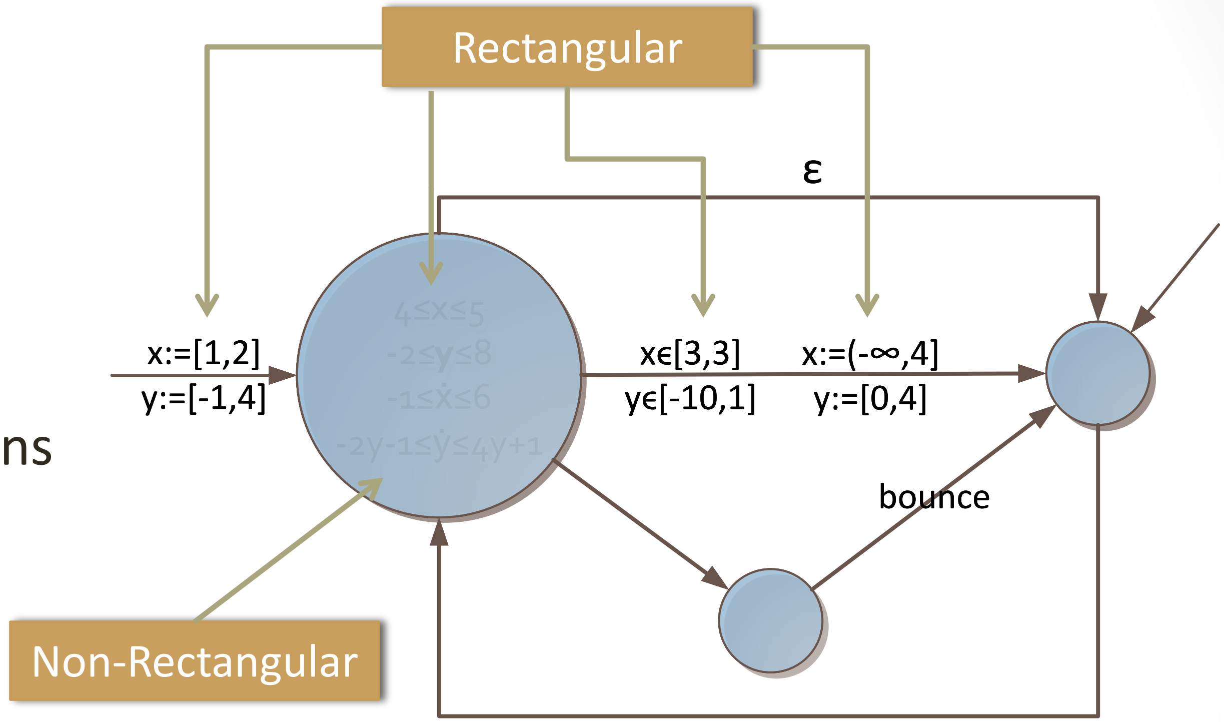
Nima Roohi
University of Illinois Urbana Champaign

Outline

- Define (Initialized) Almost Rectangular Hybrid Automata
- Problem 1
  - Solution (two transformations)
- What Transformations We Use
- Problem 2
  - Partitioning
    - Finite
    - Decidable

Almost Rectangular HA

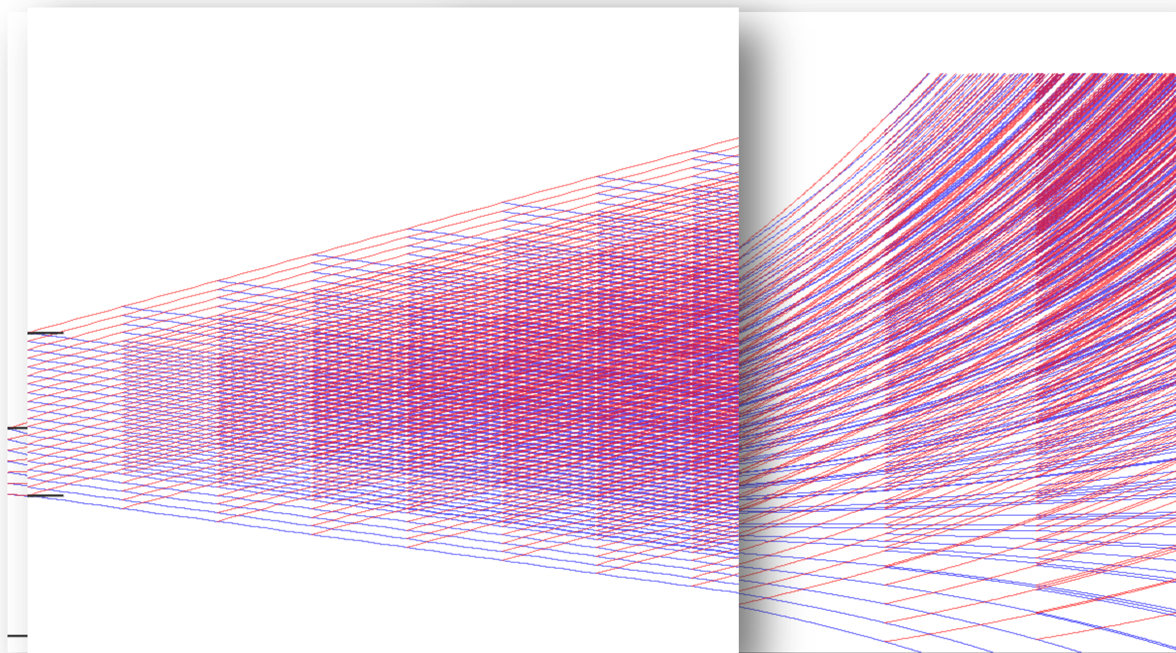
- Locations
- Variables
- Invariants
- Flows
- Init. Locations
- Init. Values
- Edges
  - Labels
  - Guards
  - Resets



Initialization is Defined as Before
(different flows enforces strong reset)

What is New in the Problem?

- Existence of a valid flow for *x* is not depend on the value of *x*
- Upper flow is never smaller than lower flow
    - Upper bound curve is never smaller than the lower bound curve

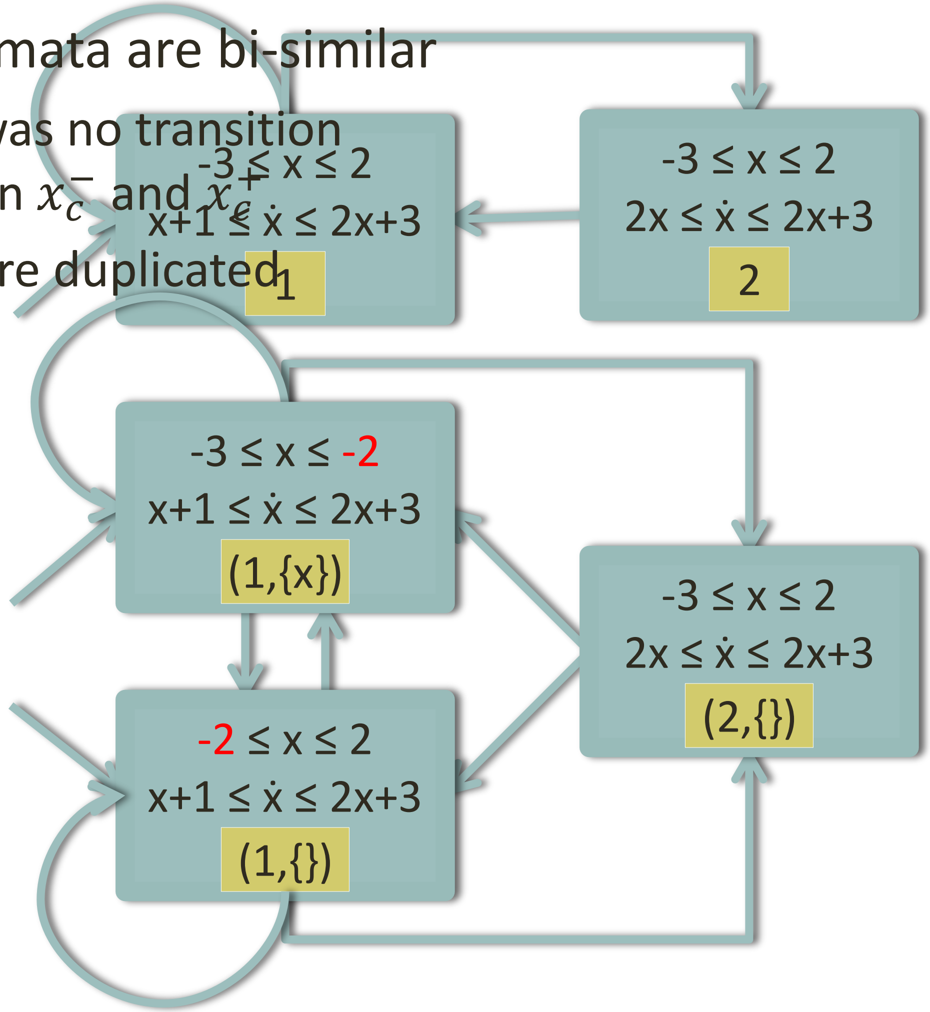


x:=[-1, 1]; x:=[1, 10]
-2x-1 ≤ ẋ ≤ 4x+1; 2 ≤ ẋ ≤ 4

x:=[-1, 1]
3x+1 ≤ ẋ ≤ 2x+8

Split the Location Invariants

- Number of locations will be increased by $2^{|Vars|}$
- Two automata are bi-similar
  - There was no transition between x_c^- and x_c^+
  - Edges are duplicated



Dec 16, 2012

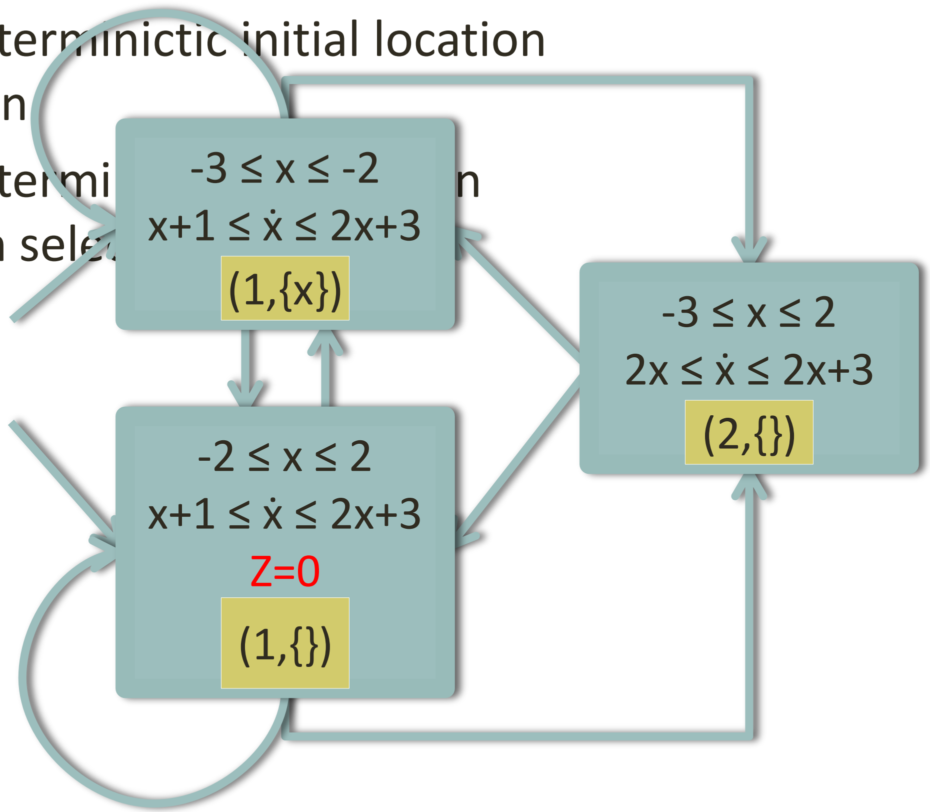
Problem is NOT Solved

- We just guaranteed x_c^- and x_c^+ cannot be in one invariant
  - But one of them is enough for the problem

x:=[0, 1]
$4x \le \dot{x} \le 2x$

Restrict Invariants

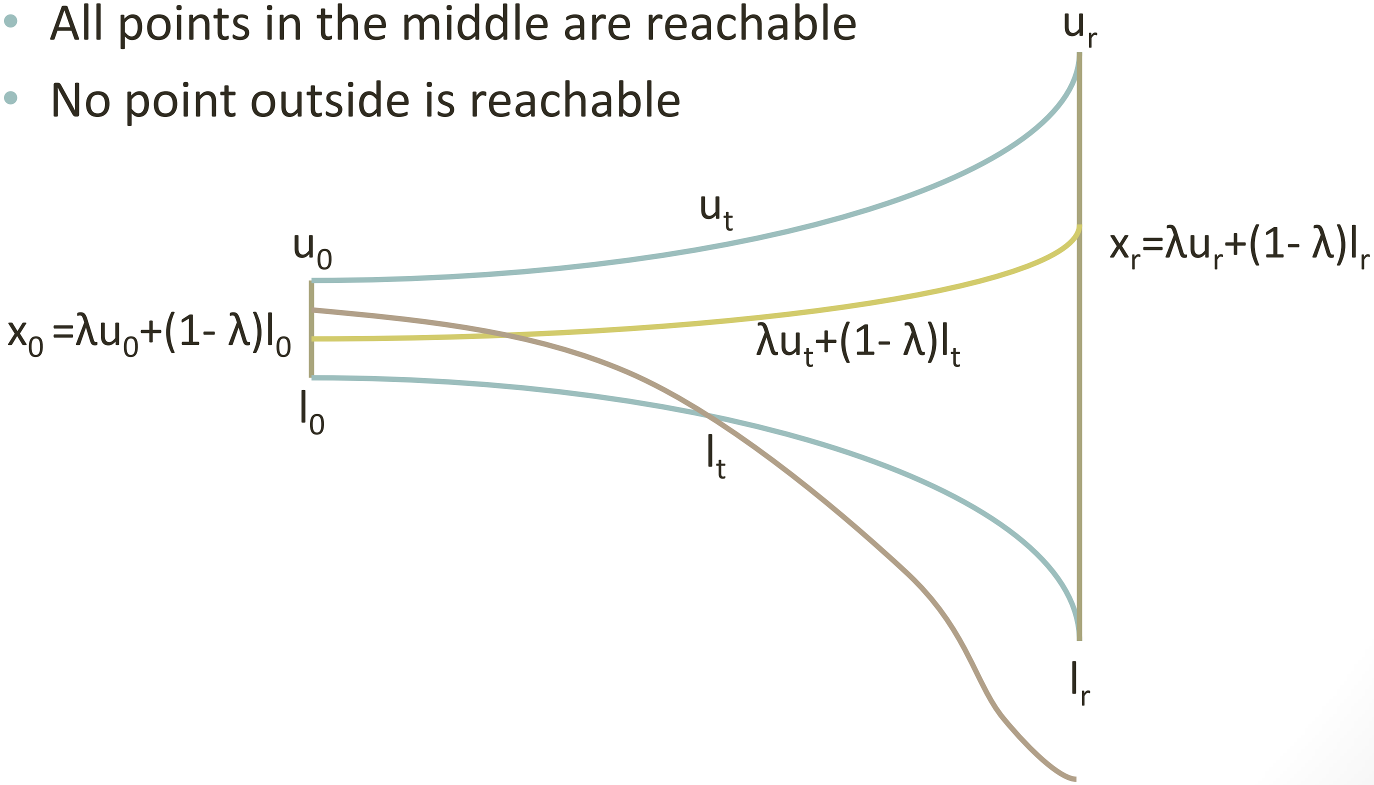
- Add one new variable (z) to each Hybrid Automaton
- Add $z = 0$ to the invariant of all such locations
- Two automata are bi-similar
  - Non-determinictic initial location selection
  - Non-determi n location sele



Dec 16, 2012

Restrict Invariants II

- Now we can assume after any positive amount of time, reachable points are defined by lower and upper bound curves.
  - All points in the middle are reachable
  - No point outside is reachable

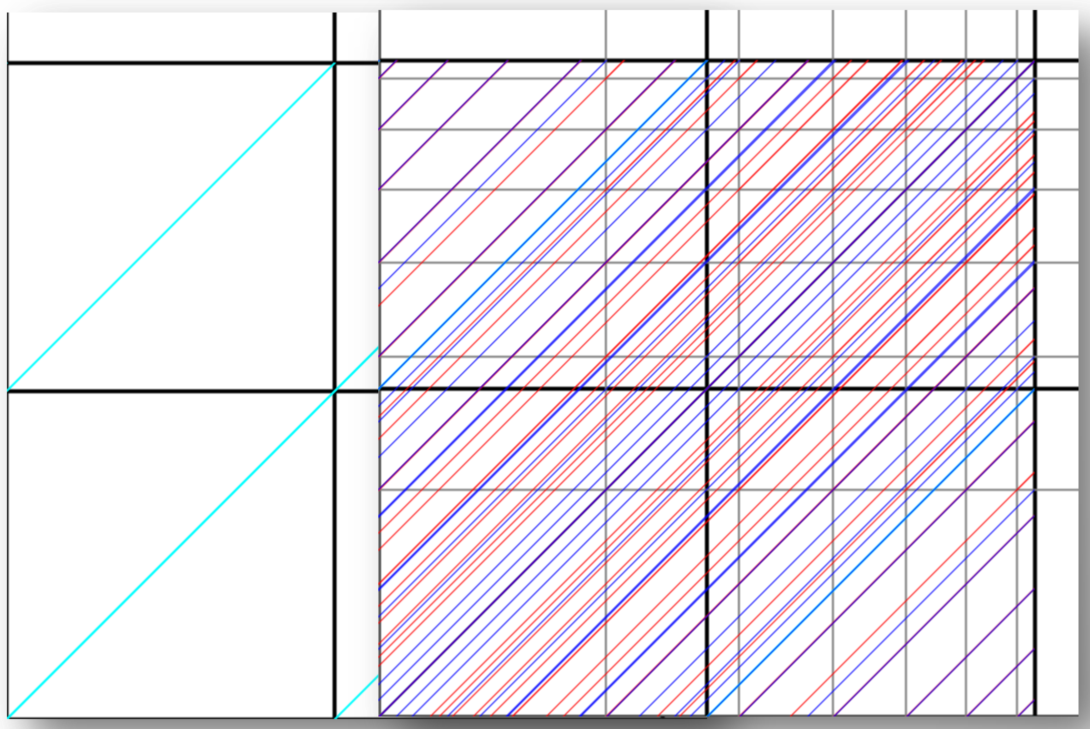


Transformations

- Split Locations
- Restrict Invariants
- Replace each variable x by two variables l_x and u_x
  - Flows will be in the form of $\dot{x} = ax + b$
- Clock Transformation
  - x_0 is known and is only one value
  - $\dot{x} = ax + b$
  - $x = x_0 e^{at} + \frac{be^{at} - b}{a}$
  - Clock transformation replace x by t_x
    - Constants will be changed accordingly
  - Constant will be in $\mathbb{Q} \cup \mathbb{Q}\ln\mathbb{Q}^+$
- Transform Initialized Singular automata to Initialized Stopwatch automata
- Transform Initialized Stopwatch automata to Timed automata
- Constants will be in $\mathbb{Q} \cup \mathbb{Q}\ln\mathbb{Q}^+$

What is New in the Problem?

- More Complex Regions
- Exponentially more Regions

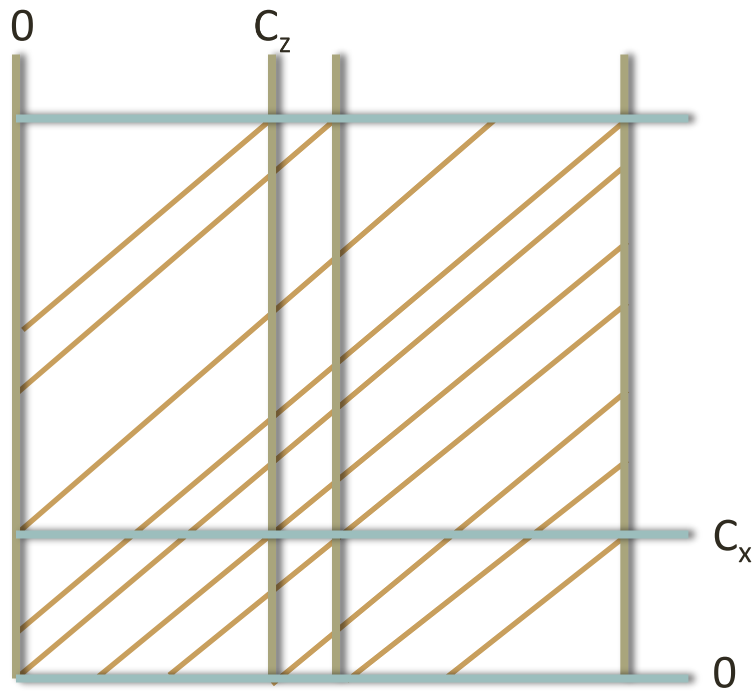


Rational Timed Automaton

Almost Rational Timed Automaton

Partitioning

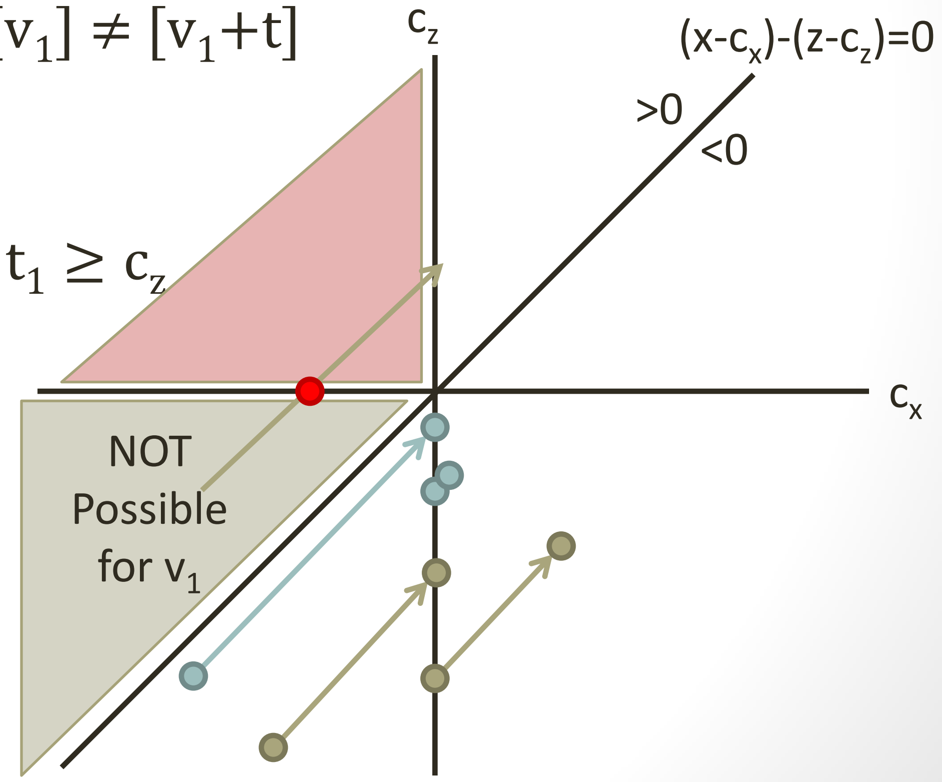
- Directly Considering Rational Constants Instead of Integers
- Only Considering Used Constants Instead of All Possible Constants



- Finite Number of Partitions (same order)

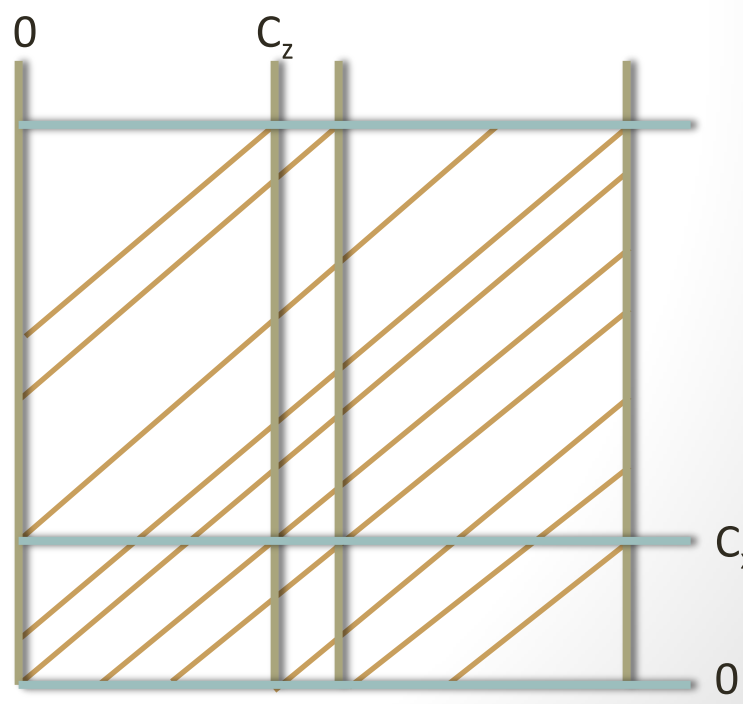
Equivalent Classes are Bisimilar

- Any t satisfy diagonal conditions
- We can assume $t_1 > 0$
  - Otherwise $t_2=0$ is the obvious answer
- We can assume between $[v_1] \neq [v_1+t]$ there is no other class
  - Induction Hypothesis
- Suppose $z_1 \leq c_z$ and $z_1 + t_1 \geq c_z$
  - Such z must exist
  - $z_1 < c_z \Rightarrow t_2 = c_z - z_2$
  - $z_1 = c_z \Rightarrow t_2 = 0^+$
- $t_2>0$



Regions are Computable

- All constants are in $\mathbb{Q} \cup \mathbb{Q}\ln\mathbb{Q}^{+}$
  - Closed under addition
  - Closed under multiplication by a rational number
- We can sort all horizontal and vertical lines (?)
- We can also sort all diagonal lines (?)
- If we can find empty regions then we can enumerate all regions (?)
- We also need to find whether
  - a region and invariant of a location intersect (?)
  - an edge connects two regions (?)
  - A time transition connects two regions (?)
    - Regions and constraints are convex



Dec 16, 2012

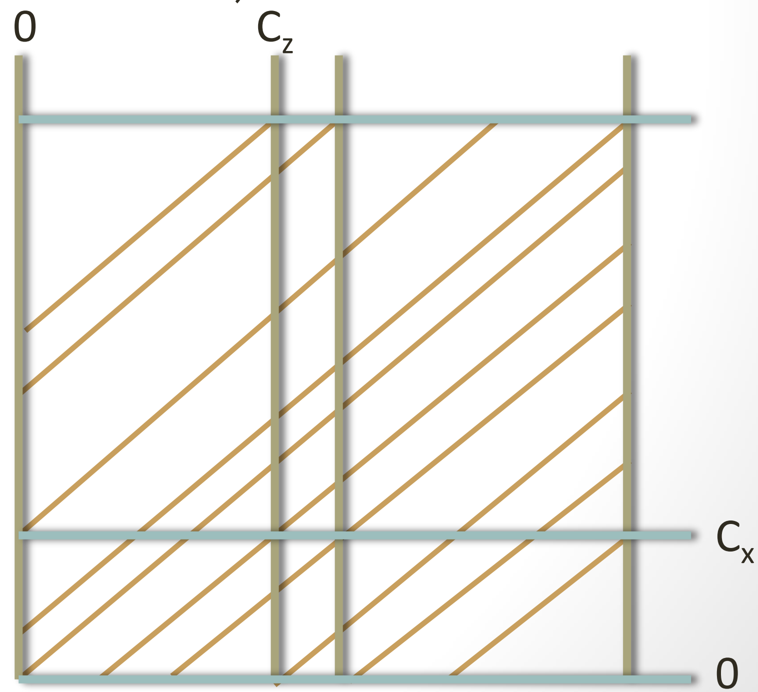
Regions are Computable II

- All these problems can be reduced to a more general decidability problem

$$\mathrm{I} = \bigwedge_{i \in m} \left(\left(\sum_{j \in n} a_{i,j} x_j \right) \sim_i r_i + \ln v_i \right)$$

  - $m, n \in \mathbb{N}^+$
  - $a_{i,j}, ri \in \mathbb{Q}$
  - $v_i \in \mathbb{Q}^+$
  - $\sim_i \in \{<, \leq\}$
- Variable Elimination Method like

Fourier–Motzkin



The Fourier–Motzkin Method

- Divide I into three sub-system of inequalities

$$\mathrm{I}_{-} \quad \mathrm{I}_{+} \quad \mathrm{I}_{0}$$

- For every pair of inequalities in I_{-} and I_{+} like
  - $2x - y < 3 \quad -3x - 5y \leq 4$
  - Define $3(2x - y) + 2(-3x - 5y) < 3 \times 3 + 2 \times 4$ or

$$-13y < 17$$

- Do the same until no variable remains!
- Therefore decidability of I is reduced to

$$\bigwedge_{i \in m'} (0 \sim_i r_i + \mathrm{ln} v_i)$$

Dec 16, 2012

Decidability of $r \sim \ln v$

- $r \sim \ln v$ is true if and only if $e^r \sim v$
- We know $e^r \notin \mathbb{Q}$ (r≠0)
  - Therefore $e^r \sim v$ if and only if $e^r < v$
- We can find rational lower (l_i) and upper (u_i) bounds of e^r that are equal to it up to at least first i number of digits
  - If $v \leq l_i$ then $e^r < v$ is false
  - If $v \geq u_i$ then $e^r < v$ is true
- i must exists, otherwise
  - $l_\infty \leq e^r \leq u_\infty$ and $l_\infty = u_\infty$ which implies $e^r \in \mathbb{Q}$

THANK YOU