ECE/CS 584: Verification of Embedded Computing Systems
Timed to Hybrid Automata

Sayan Mitra

Lecture 10

Announcements

- HW2 released
  - start soon

Last lecture

- Focus on specific classes of Hybrid Automata for which safety properties (invariants) can be verified completely automatically
  - Alur-Dill's Integral Timed Automata (ITA)
  - Control State Reachability (CSR) problem
  - Construction of Region Automaton (FSM)
- Today
  - How far can we generalize ITAs while preserving decidability of CSR

Clocks and **Rational** Clock Constraints

- A **clock variable** x is a continuous (analog) variable of type real such that along any trajectory τ of x, for all t ∈ $\tau.dom, (\tau \downarrow x)(t) = t.$
- For a set X of clock variables, the set Φ(X) of **integral clock constraints** are expressions defined by the syntax:

  g ::= x $\leq q \mid x \geq q \mid \neg\, g \mid g_1 \wedge g_2$

  where $x \in X$ and $q \in \mathbb{Q}$
- Examples: x = 10.125; x ∈ [2.99, 5); true are valid rational clock constraints
- Semantics of clock constraints $[g]$

Step 1. Rational Timed Automata

- **Definition.** A **rational timed automaton** is a HIOA A = $\langle V, Q, \Theta, A, \mathcal{D}, \mathcal{T} \rangle$ where
  - V = X ∪ $\{loc\}$, where X is a set of n clocks and l is a discrete state variable of finite type Ł
  - A is a finite set
  - $\mathcal{D}$ is a set of transitions such that
    - The guards are described by **rational** clock constraings $\Phi(X)$
    - $\langle x, l \rangle - a \rightarrow \langle x', l' \rangle$ implies either $x' = x$ or $x = 0$
  - $\mathcal{T}$ set of clock trajectories for the clock variables in X

Example: Rational Light switch

- Switch can be turned on whenever at least 2.25 time units have elapsed since the last turn off. Switches off automatically 15.5 time units after the last on.

automaton Switch

- **internal** push; pop
- **variables**

  internal x, y:Real := 0, loc:{on,off} := off
- **transitions**
- **internal** push

  pre x $\geq$ 2.25

  eff if loc = on **then** y := 0 **fi;** x := 0; loc := off
- **internal** pop

  pre y = 15.5 /\ loc = off

  eff x := 0
- **trajectories**

  invariant loc = on \/ loc = off

  stop when y = 15.5 /\ loc = off

  evolve d(x) = 1; d(y) = 1

Control State (Location) Reachability Problem

- Given an RTA, check if a particular location is reachable from the initial states
- Is problem is decidable?
- Key idea:
  - Construct a ITA that is bisimilar to the given RTA
  - Check CSR for ITA

Construction of ITA from RTA

- Multiply all rational constants by a factor q that make them integral
- Make d(x) = q for all the clocks

- RTA Switch is bisimilar to ITA Iswitch
- Simulation relation R is given by (**u,s**) $\in R$ iff **u.**x = 4 **s.**x and **u.**y = 4 **s.**y

automaton ISwitch
- **internal** push; pop
- **variables**
  - **internal** x, y:Real := 0, loc:{on,off} := off
- **transitions**
- **internal** push
  - **pre** x $\geq$ 9
  - **eff if** loc = on **then** y := 0 **fi;** x := 0; loc := off
- **internal** pop
  - **pre** y = 62 /\ loc = off
  - **eff** x := 0
- **trajectories**
  - **invariant** loc = on \/ loc = off
  - **stop when** y = 62 /\ loc = off
  - **evolve** d(x) = 4; d(y) = 4

Step 2. Multi-Rate Automaton

- **Definition.** A **multirate automaton** is a HIOA A = $\langle V, Q, \Theta, A, \mathcal{D}, \mathcal{T} \rangle$ where
  - V = X ∪ $\{loc\}$, where X is a set of n **continuous variables** and loc is a discrete state variable of finite type Ł
  - A is a finite set
  - $\mathcal{D}$ is a set of transitions such that
    - The guards are described by **rational** clock constrainqs $\Phi(X)$
    - $\langle x, l \rangle - a \rightarrow \langle x', l' \rangle$ implies either $x' = c$
  - $\mathcal{T}$ set of trajectories such that for each $x \in \ X\ \exists k\ such\ that\ \tau \in \mathcal{T}, t \in \tau.dom$

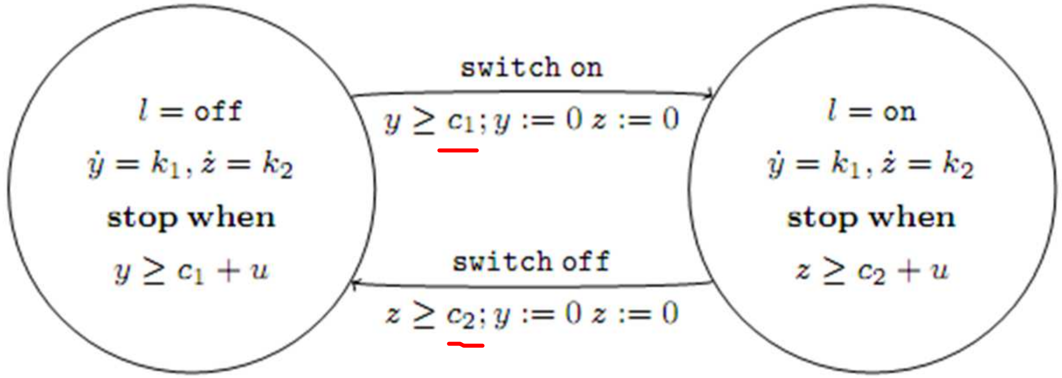
$$\tau(t).x = \tau(0).x + k\ t$$

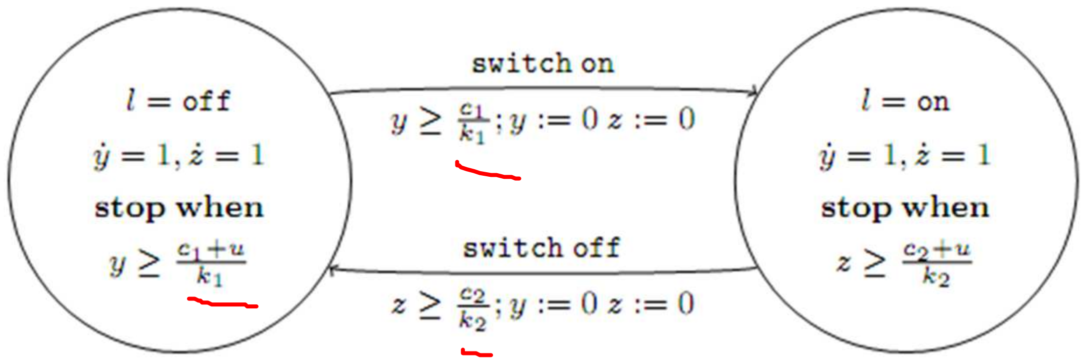
$d(x) = k \quad \dot{x} = k$

Control State (Location) Reachability Problem

- Given an MRA, check if a particular location is reachable from the initial states
- Is problem is decidable?
- Key idea:
  - Construct a RTA that is bisimilar to the given MRA

Example


$l = \text{off}$
$\dot{y} = k_1, \dot{z} = k_2$
stop when
$y \geq c_1 + u$
switch on
$y \geq c_1; y := 0\ z := 0$
switch off
$z \geq c_2; y := 0\ z := 0$
$l = \text{on}$
$\dot{y} = k_1, \dot{z} = k_2$
stop when
$z \geq c_2 + u$


$l = \text{off}$
$\dot{y} = 1, \dot{z} = 1$
stop when
$y \geq \frac{c_1+u}{k_1}$
switch on
$y \geq \frac{c_1}{k_1}; y := 0\ z := 0$
switch off
$z \geq \frac{c_2}{k_2}; y := 0\ z := 0$
$l = \text{on}$
$\dot{y} = 1, \dot{z} = 1$
stop when
$z \geq \frac{c_2+u}{k_2}$

Step 3. Initialized Rectangular HA

- **Definition.** An **initialized rectangular hybrid automaton (IRHA)** is a HIOA A = $\langle V, Q, \Theta, A, \mathcal{D}, \mathcal{T} \rangle$ where
  - V = X ∪ $\{loc\}$, where X is a set of n **continuous variables** and loc is a discrete state variable of finite type Ł
  - A is a finite set
  - $\mathcal{D}$ is a set of transitions such that
    - The guards are described by **rational** clock constrains $\Phi(X)$
    - $\langle x, l \rangle - a \rightarrow \langle x', l' \rangle$ implies
    - If the dynamics of x changes from l to l' then x' ∈ $[a, b]$
    - Otherwise $x' = x$
  - $\mathcal{T}$ set of trajectories such that for each

    $l \in L, x_i \in X,\ \dot{x}_i \in [a_{il}, b_{il}]$

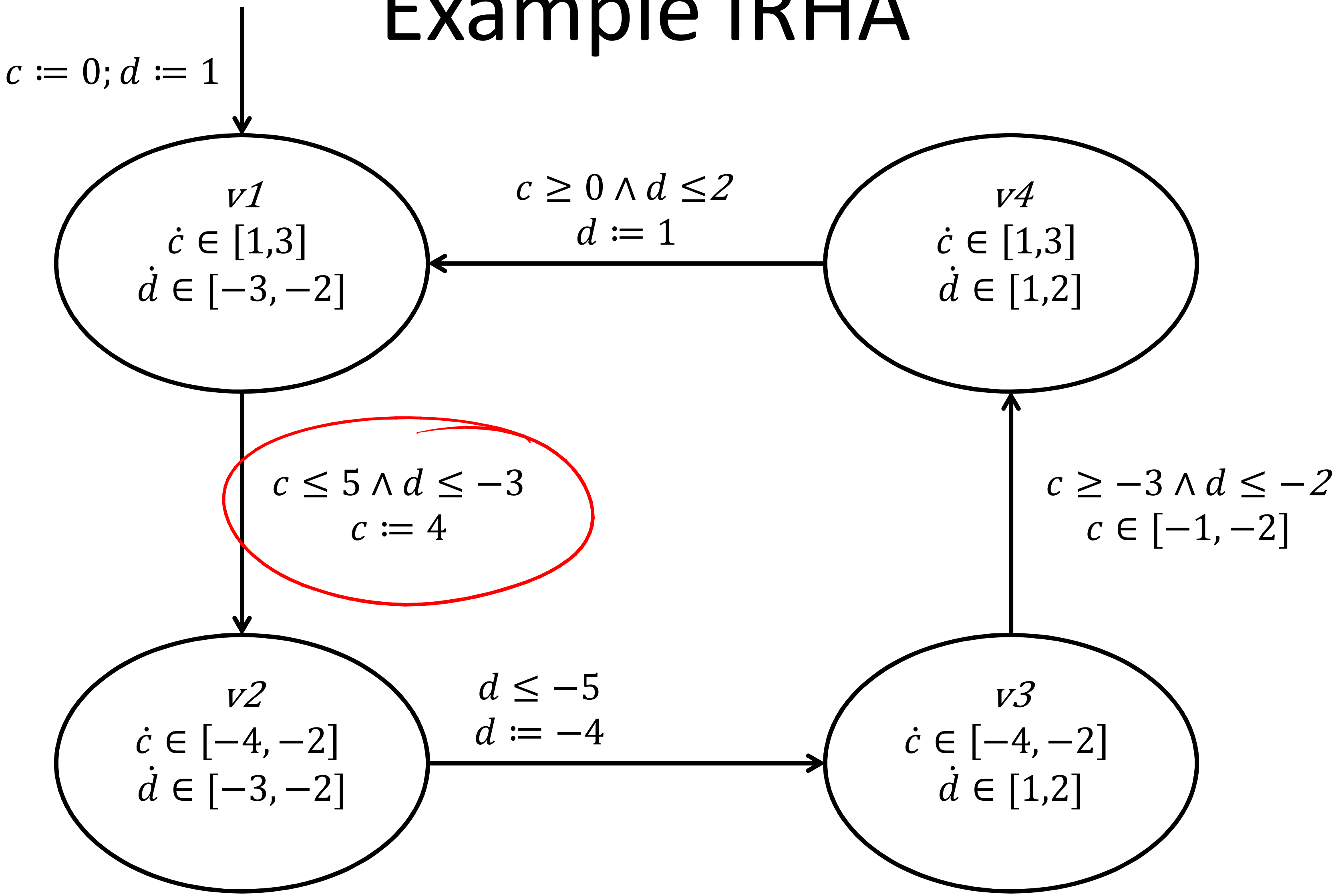
    That is, for any $\tau \in \mathcal{T}, t \in \tau.dom$

    $$\tau(0).x_i + a_{il}\, t \leq \tau(t).x_i \leq \tau(0).x_i + b_{il}\, t$$

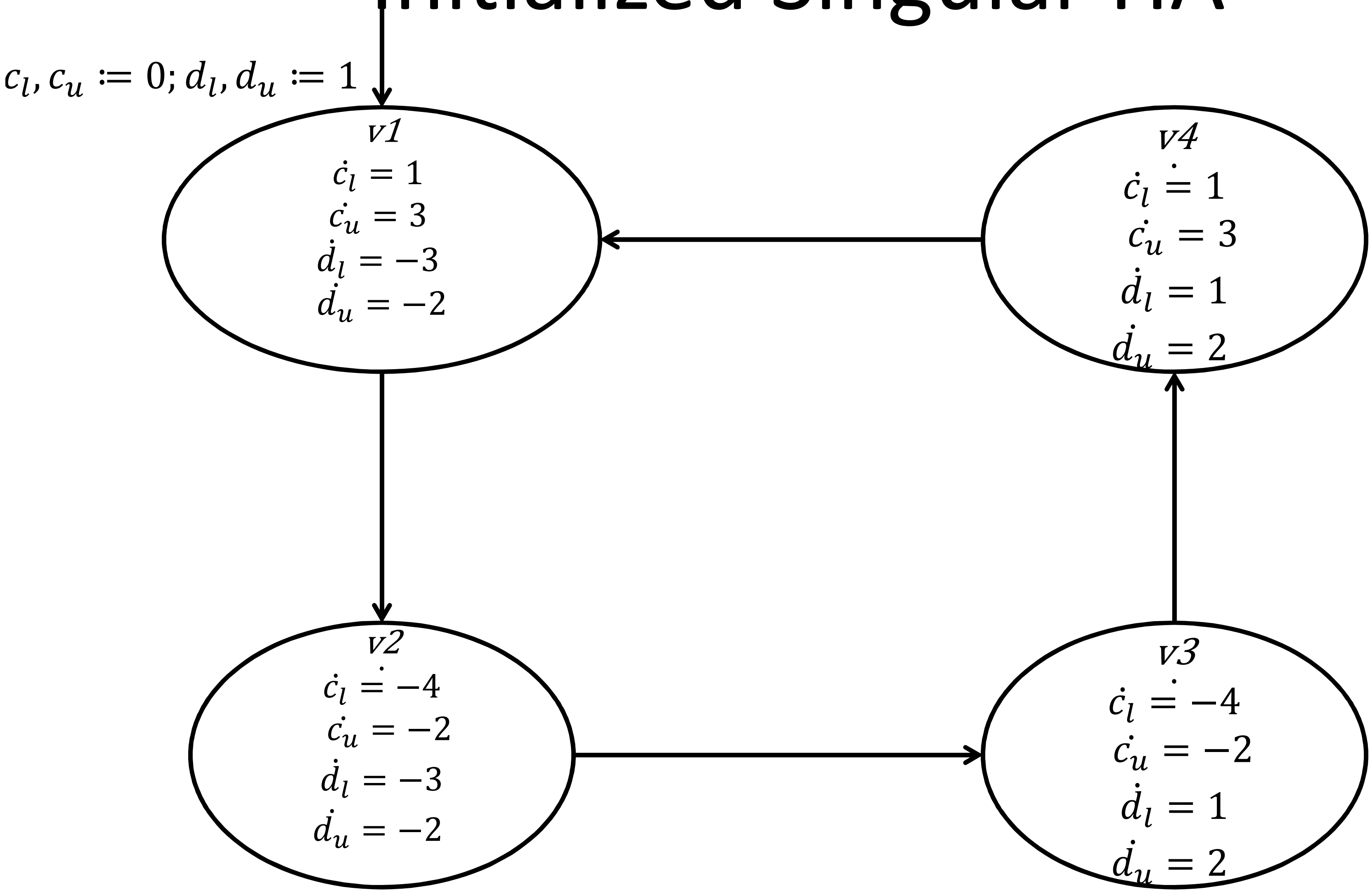
CSR Decidable for IRHA?

- Given an IRHA, check if a particular location is reachable from the initial states
- Is problem is decidable?
- Key idea:
  - Construct a 2n-dimensional **initialized Singular** automaton (Multi-rate automaton) that is bisimilar to the given IRHA
  - Construct a ITA that is bisimilar to the Singular TA

Example IRHA



Initialized Singular HA



Transitions

$v1$

$\dot{c}_l = 1$

$\dot{c}_u = 3$

$\dot{d}_l = -3$

$\dot{d}_u = -2$

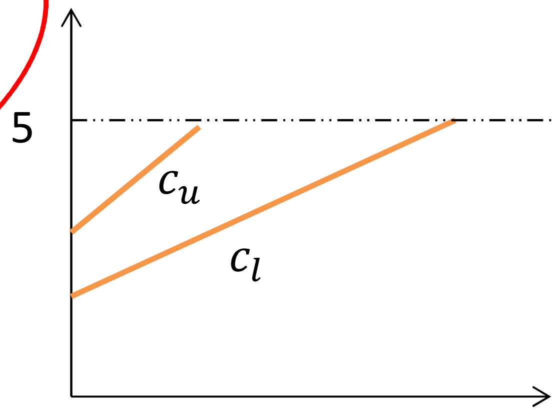
$c_l \leq 5$

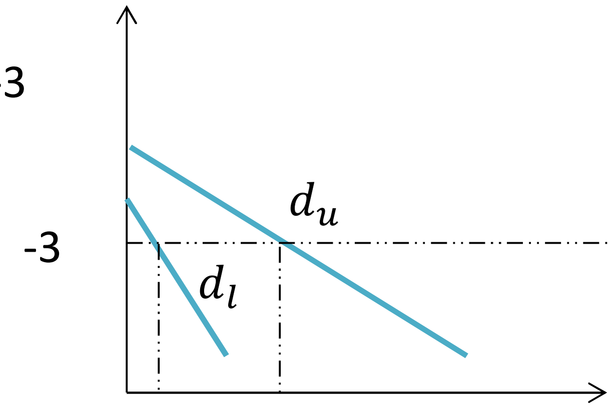
$c_l, c_u \coloneqq 4$

$d_u \leq -3$ *no reset*

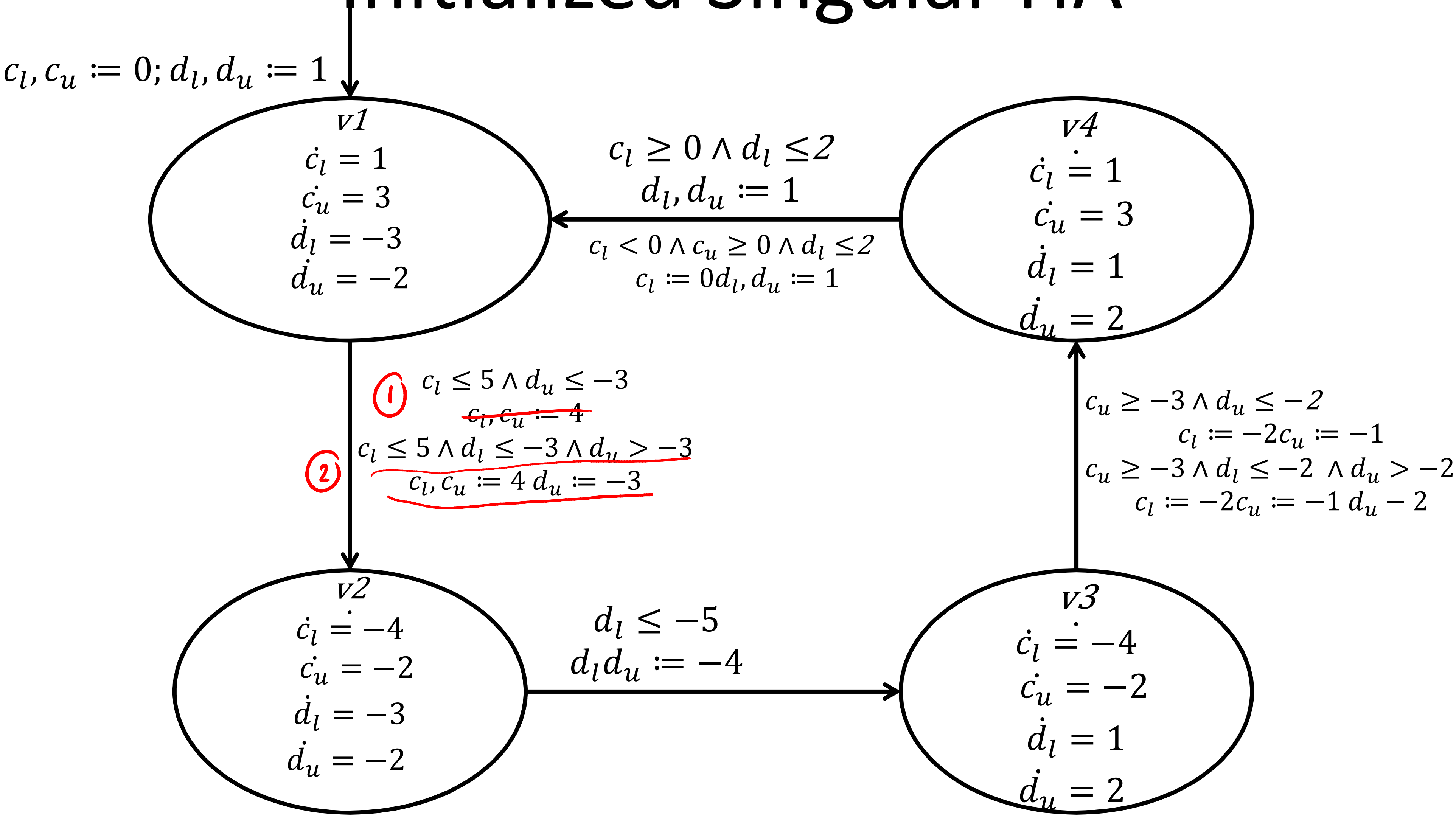
$d_u > -3 \wedge d_l \leq -3$ $d_u \coloneqq -3$

$$\frac{c \leq 5 \wedge d \leq -3}{c := 4}$$





Initialized Singular HA

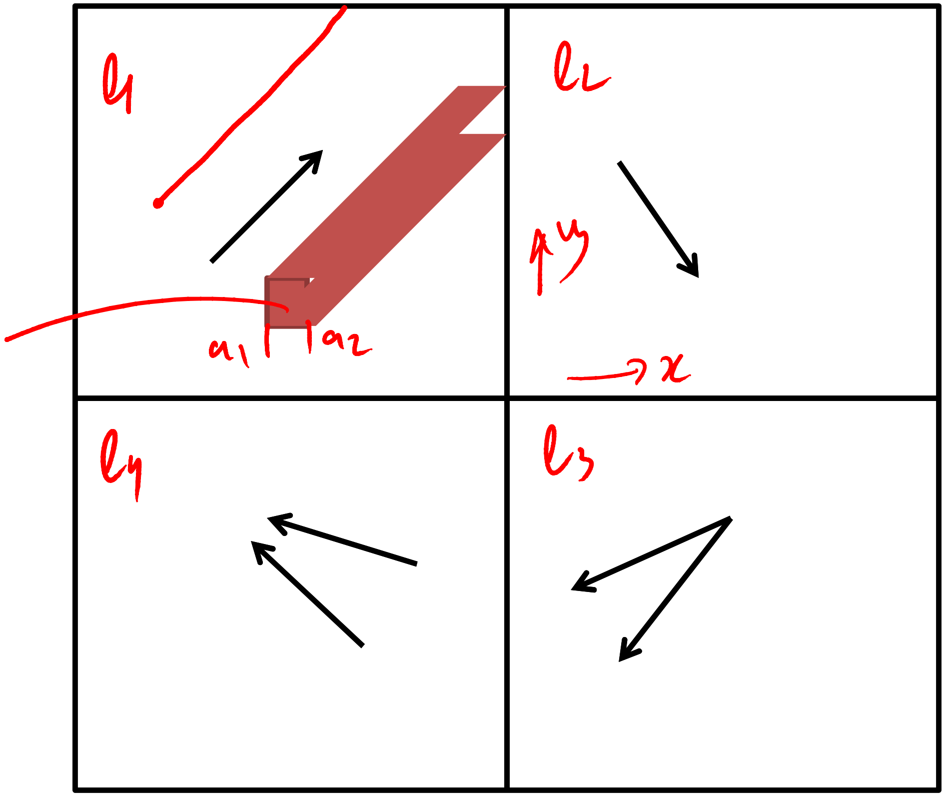


Can this be further generalized ?

- For initialized Rectangular HA, control state reachability is decidable
  - Can we drop the initialization restriction?
  - Can we drop the rectangular restriction?
  - Tune in in a week

Reachability Computation with polyhedra

Navigation Benchmark



- A set of states is represented by disjunction of linear inequalities
  - $(loc = l_1 \wedge A_1 x \leq b_1) \vee$
    $(loc = l_2 \wedge A_2 x \leq b_2) \vee$
    $\ldots$
- Post(,) computation performed symbolically using quantifier elimination

$(loc = l_1) \wedge a_1 \leq x \leq a_2 \wedge b_1 \leq y \leq b_2$

$\dot{x} = k \quad post([a_1, a_2]) = \exists t \; [a_1 + kt, a_2 + kt]$

$= [a_1, \infty]$

Summary

- ITA: (very) Restricted class of hybrid automata
  – Clocks, integer constraints
  – No clock comparison, linear
- Control state reachability with Alur-Dill's algorithm (region automaton construction)
- Rational coefficients
- Multirate Automata
- Initialized Rectangular Hybrid Automata
- HyTech, PHAVer use polyhedral reachability computations