Lecture 19: Timed automata and its reachability

Huan Zhang
huan@huan-zhang.com
Timed Automata & Reachability

• We have studied hybrid automaton

  **automaton** Bouncingball(c,h,g)

  **variables**: x: Reals := h, v: Reals := 0

  **actions**: bounce

  **transitions**:

  bounce

  **pre** \( x = 0 \land v < 0 \)

  **eff** \( v := -cv \)

  **trajectories**:

  freefall

  **evolve** \( d(x) = v; d(v) = -g \)

  **invariant** \( x \geq 0 \)
Timed Automata & Reachability

• We have studied hybrid automaton
• However, verification for general hybrid automaton is in general difficult

• Special classes of hybrid automaton:
  • (Alur-Dill’s) Timed Automata
  • Rectangular initialized hybrid automata
  • Linear hybrid automata

• Verification is feasible for these classes
  • Today and next a few lectures
Clocks and Clock Constraints

• A **clock variable** \( x \) is a continuous (analog) variable of type real such that along any trajectory \( \tau \) of \( x \), for all \( t \in \tau. \text{dom} \), \((\tau \downarrow x)(t) = t\).

• In other words, \( d(x) = 1 \)

• For a set \( X \) of clock variables, the set \( \Phi(X) \) of **integral clock constraints** are expressions defined by the syntax:

\[
g ::= x \leq q \mid x \geq q \mid \neg g \mid g_1 \land g_2
\]

where \( x \in X \) and \( q \in \mathbb{Z} \)

• Examples: \( x = 10 \); \( x \in [2, 5] \) are valid clock constraints

• What do clock constraints look like?
Example: “smart” light switch

automaton Switch
variables x, y:Real := 0, loc: {on,off} := off

transitions
push
  pre x ≥ 2
  eff if loc = off then x,y := 0; loc := on
  else x := 0
pop
  pre y = 15 \ loc = on
  eff x := 0; loc = off

integral clock constraints

trajectories

invariant loc = off ∨ y ≤ 15

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

Description
Switch can be turned on whenever at least 2 time units have elapsed since the last turn off. Switches can be turned off 15 time units after the last on.

clock guard

integral clock constraints

clock variables
Integral Timed Automata (ITA)

• **Definition.** A *integral timed automaton* $\mathcal{A} = \langle V, \Theta, A, \mathcal{D}, \mathcal{T} \rangle$ where
  
  • $V = X \cup \{l\}$, where $X$ is a set of $n$ clocks and $l$ is a discrete state variable of finite type $L$. The **state space** is $\text{val}(V) \times L$
  
  • $A$ is a finite set
  
  • $\mathcal{D}$ is a set of transitions such that
    
    • The preconditions are described by clock constraints $\Phi(X)$
    
    • $\langle x, l \rangle_a \rightarrow \langle x', l' \rangle$ implies either $x' = x$ or $x' = 0$ (time is reset to 0, or no change)
    
    • $\mathcal{T}$ set of clock trajectories for the clock variables in $X$
Control State (mode) Reachability Problem

• Given an ITA $\mathcal{A}$, check if a particular (mode) control state $l^* \in L$ is **reachable** from the initial states

• cannot just enumerate all states - uncontable many states!
Control State (mode) Reachability Problem

• Given an ITA $\mathcal{A}$, check if a particular (mode) control state $l^* \in L$ is reachable from the initial states
  • How many states in $\mathcal{A}$?
Model Reachability of Integral Timed Automata is Decidable [Alur Dill 94]

That is, there is an algorithm that takes in $\mathcal{A}, l^*$ and terminates with the correct answer.

Key idea:

- Construct a finite automaton $B$ that is a **time-abstract bisimilar** to the given ITA $\mathcal{A}$
- That is, FA $B$ behaves identically to ITA $\mathcal{A}$ w.r.t. control state reachability, but does not preserve timing information
- Check reachability of FA $B$
An equivalence relation with a finite quotient

Under what conditions do two states $x_1$ and $x_2$ of the automaton $\mathcal{A}$ behave identically with respect to control state reachability (CSR)?

When do they satisfy the same set of clock constraints?
When would they continue to satisfy the same set of clock constraints?

Goal: infinite number of states -> finite number of states
(possible because some states are identical)
An equivalence relation with a finite quotient

Under what conditions do two states \( x_1 \) and \( x_2 \) of the automaton \( \mathcal{A} \) behave identically with respect to mode reachability?

\[ x_1.\text{loc} = x_2.\text{loc} \]

and

\( x_1 \) and \( x_2 \) satisfy the same set of clock constraints:

For all clock \( y \):

- \( \text{int}(x_1.y) = \text{int}(x_2.y) \), or \( \text{int}(x_1.y) \geq c_{\mathcal{A}y} \) and \( \text{int}(x_2.y) \geq c_{\mathcal{A}y} \). (\( c_{\mathcal{A}y} \) is the maximum clock guard of \( y \))
- For all clock \( y \): with \( x_1.y \leq c_{\mathcal{A}y} \), \( \text{frac}(x_1.y) = 0 \) iff \( \text{frac}(x_2.y) = 0 \)
- For any two clocks \( y \) and \( z \): with \( x_1.y \leq c_{\mathcal{A}y} \) and \( x_1.z \leq c_{\mathcal{A}z} \), \( \text{frac}(x_1.y) \leq \text{frac}(x_1.z) \) iff \( \text{frac}(x_2.y) \leq \text{frac}(x_2.z) \)

**Lemma.** This is an equivalence relation on \( \text{val}(V) \) (the states of \( \mathcal{A} \))

The partition of \( \text{val}(V) \) induced by this relation is are called clock regions
An equivalence relation with a finite quotient

For all clock $y$: \( \text{int}(x_1.y) = \text{int}(x_2.y) \) or \( \text{int}(x_1.y) \geq c_{Ay} \) and \( \text{int}(x_2.y) \geq c_{Ay} \). \((c_{Ay} \text{ is the maxium clock guard of } y)\)

For all clock $y$: with $x_1.y \leq c_{Ay}$, \( \text{frac}(x_1.y) = 0 \) iff \( \text{frac}(x_2.y) = 0 \)

For any two clocks $y$ and $z$: with $x_1.y \leq c_{Ay}$ and $x_1.z \leq c_{Az}$, \( \text{frac}(x_1.y) \leq \text{frac}(x_1.z) \) iff \( \text{frac}(x_2.y) \leq \text{frac}(x_2.z) \)

Example of Two Clocks

\[ X = \{ y, z \} \]
\[ c_{Ay} = 2 \]
\[ c_{Az} = 3 \]
Complexity

**Lemma.** The number of clock regions is bounded by 
\[ |L| |X|! 2^{|X|} \prod_{z \in X} (2c_{\mathcal{A}z} + 2). \]

\( X \) is a set of clocks
\( L \) is the type of discrete states
\( c_{\mathcal{A}z} \) is the clock guard
Region automaton $R(\mathcal{A})$

Given an ITA $\mathcal{A} = \langle V, \Theta, D, T \rangle$, we construct the corresponding **Region Automaton** $R(\mathcal{A}) = \langle Q_R, \Theta_R, D_R \rangle$.

(i) $R(\mathcal{A})$ visits the same set of modes (but does not have timing information) and

(ii) $R(\mathcal{A})$ is finite state machine.

• ITA (clock constants) defines a set of clock regions, say $C_{\mathcal{A}}$. The set of states $Q_R = C_{\mathcal{A}} \times L$

• $Q_0 \subseteq Q$ is the set of states contain initial set $\Theta$ of $\mathcal{A}$

• $D$: We add the transitions between $Q$ (regions)
  - **Time successors**: Consider two clock regions $\gamma$ and $\gamma'$, we say that $\gamma'$ is a time successor of $\gamma$ if there exits a trajectory of ITA starting from $\gamma$ that ends in $\gamma'$
  - **Discrete transitions**: Same as the ITA

**Theorem.** A mode of ITA $\mathcal{A}$ is reachable iff it is also reachable in $R(\mathcal{A})$.

(we say that $R(\mathcal{A})$ is *time abstract bisimilar* to $\mathcal{A}$)
Time successors

The clock regions in green are time successors of the clock region in red.
Example 1: Region Automata

ITA

Corresponding FA
Example 2

ITA

Clock

Regions
Corresponding FA

\[ |X|! 2^{|X|} \prod_{x \in X} (2c_{\mathcal{A}_x} + 2) \]

Drastically increasing with the number of clocks
Special Classes of Hybrid Automata

- Finite Automata
- Integral Timed Automata
- Rational time automata
- Multirate automata
- Rectangular Initialized HA

- Rectangular HA

- Linear HA

- Nonlinear HA

Slides adapted from Prof. Sayan Mitra's slides in Fall 2021
Clocks and **Rational** Clock Constraints

- A **clock variable** $x$ is a continuous (analog) variable of type real such that along any trajectory $\tau$ of $x$, for all $t \in \tau.\ dom$, $(\tau \downarrow x)(t) = t$.

- For a set $X$ of clock variables, the set $\Phi(X)$ of **rational clock constraints** are expressions defined by the syntax:
  
  $$g ::= x \leq q \mid x \geq q \mid \neg g \mid g_1 \land g_2$$

  where $x \in X$ and $q \in \mathbb{Q}$

- Examples: $x = 10.125$; $x \in [2.99, 5)$; true are valid rational clock constraints

- Semantics of clock constraints $[g]$
Step 1. Rational Timed Automata

**Definition.** A *rational timed automaton* is a HA $\mathcal{A} = \langle V, \Theta, A, \mathcal{D}, \mathcal{T} \rangle$ where

- $V = X \cup \{loc\}$, where $X$ is a set of $n$ clocks and $l$ is a discrete state variable of finite type $L$
- $A$ is a finite set
- $\mathcal{D}$ is a set of transitions such that
  - The guards are described by rational clock constraints $\Phi(X)$
  - $\langle x, l \rangle \rightarrow a \rightarrow \langle x', l' \rangle$ implies either $x' = x$ or $x = 0$
- $\mathcal{T}$ set of clock trajectories for the clock variables in $X$

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
Example: **Rational** Light switch

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

automaton Switch

internal push; pop

variables

internal x, y:Real := 0, loc:{on,off} := off

transitions

push

pre x >= 2.25

eff if loc = on then y := 0 fi; x := 0;
loc := off

pop

pre y = 15.5 ∧ loc = off

eff x := 0; loc := off

trajectories

invariant loc = on ∨ loc = off

stop when y = 15.5

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

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
Control State (Location) Reachability Problem

• Given an RTA, check if a particular mode is reachable from the initial states
• Is problem decidable?
  • Yes
• Key idea:
  • Construct a ITA that has exactly same mode reachability behavior as the given RTA (timing behavior may be different)
  • Check mode reachability 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 reaches the same control locations as the ITA $I_{\text{switch}}$

```plaintext
automaton ISwitch

internal push; pop
variables
  internal $x, y: \text{Real} := 0$, $\text{loc}: \{\text{on, off}\} := \text{off}$

transitions
  push
    pre $x \geq 9$
    eff if $\text{loc} = \text{on}$ then $y := 0$ fi;
    $x := 0$; $\text{loc} := \text{off}$

  pop
    pre $y = 62 \land \text{loc} = \text{off}$
    eff $x := 0$

trajectories
  invariant $\text{loc} = \text{on} \lor \text{loc} = \text{off}$
  stop when $y = 62$
  evolve $d(x) = 4$; $d(y) = 4$
```

Slides adapted from Prof. Sayan Mitra's slides in Fall 2021
Step 2. Multi-Rate Automaton

• **Definition.** A multirate automaton is $\mathcal{A} = \langle V, Q, \Theta, A, D, T \rangle$ where
  
  • $V = X \cup \{loc\}$, where $X$ is a set of $n$ continuous variables and $loc$ is a discrete state variable of finite type $L$
  
  • $A$ is a finite set of actions
  
  • $\mathcal{D}$ is a set of transitions such that
    
    • The guards are described by rational clock constraints $\Phi(X)$
    
    • $\langle x, l \rangle \rightarrow a \rightarrow \langle x', l' \rangle$ implies either $x' = c$ or $x' = x$
  
  • $\mathcal{T}$ set of trajectories such that
    
    for each variable $x \in X$ there exists $\exists k$ such that $\tau \in \mathcal{T}$, $t \in \tau.\text{dom}$
    
    $\tau(t).x = \tau(0).x + k.t$
Control State (Location) Reachability Problem

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

\[ l = \text{off} \quad \hat{y} = k_1, \hat{z} = k_2 \quad \text{stop when} \quad y \geq c_1 + u \]

\[ l = \text{on} \quad \hat{y} = k_1, \hat{z} = k_2 \quad \text{stop when} \quad z \geq c_2 + u \]

\[ l = \text{off} \quad \hat{y} = 1, \hat{z} = 1 \quad \text{stop when} \quad y \geq \frac{c_1}{k_1} + u \]

\[ l = \text{on} \quad \hat{y} = 1, \hat{z} = 1 \quad \text{stop when} \quad z \geq \frac{c_2}{k_2} + u \]

Slides adapted from Prof. Sayan Mitra's slides in Fall 2021
Step 3. Rectangular HA

Definition. A rectangular hybrid automaton (RHA) is a HA \( \mathcal{A} = \langle V, A, T, D \rangle \) where

- \( V = X \cup \{ loc \} \), where \( X \) is a set of \( n \) continuous variables and \( loc \) is a discrete state variable of finite type \( L \)
- \( A \) is a finite set
- \( T = \bigcup_\ell T_\ell \) set of trajectories for \( X \)
  - For each \( \tau \in T_\ell \), \( x \in X \) either (i) \( d(x) = k_\ell \) or (ii) \( d(x) \in [k_{\ell 1}, k_{\ell 2}] \)
  - Equivalently, (i) \( \tau(t)[x = \tau(0) + k_\ell t] \)
    (ii) \( \tau(0)[x + k_{\ell 1} t \leq \tau(t)[x \leq \tau(0)[x + k_{\ell 2} t] \)
- \( D \) is a set of transitions such that
  - Guards are described by rational clock constraints
  - \( \langle x, l \rangle \xrightarrow{a} \langle x', l' \rangle \) implies \( x' = x \) or \( x' \in [c_1, c_2] \)

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
CSR Decidable for RHA?

• Given an RHA, check if a particular location is reachable from the initial states?

• Is this problem decidable? No
  

  • CSR for RHA reduction to Halting problem for 2 counter machines
  
  • Halting problem for 2CM known to be undecidable

  • Reduction in next lecture
Step 4. Initialized Rectangular HA

Definition. An initialized rectangular hybrid automaton (IRHA) is a RHA $\mathcal{A}$ where

- $V = X \cup \{\text{loc}\}$, where $X$ is a set of $n$ continuous variables and $\{\text{loc}\}$ is a discrete state variable of finite type $\mathcal{L}$
- $A$ is a finite set
- $\mathcal{T} = \bigcup_{\ell} \mathcal{T}_\ell$ set of trajectories for $X$
  - For each $\tau \in \mathcal{T}_\ell$, $x \in X$ either (i) $d(x) = k_\ell$ or (ii) $d(x) \in [k_{\ell_1}, k_{\ell_2}]$
  - Equivalently, (i) $\tau(t)[x = \tau(0)[x + k_\ell t$
    
  (ii) $\tau(0)[x + k_{\ell_1} t \leq \tau(t)[x \leq \tau(0)[x + k_{\ell_2} t$
- $\mathcal{D}$ is a set of transitions such that
  - Guards are described by rational clock constraints
  - $\langle x, l \rangle \rightarrow_{\alpha} \langle x', l' \rangle$ implies if dynamics changes from $\ell$ to $\ell'$ then $x' \in [c_1, c_2]$, otherwise $x' = x$

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
Example: Rectangular Initialized HA

Pre $x_1 \geq G \land x_2 \leq G$  Eff $x_1: = x_2: = 0$

1
\[ d(x_1) = k_1 \]
\[ d(x_2) = k_2 \]

2
\[ d(x_1) = k_1' \]
\[ d(x_2) = k_2 \]

3
\[ d(x_1) \in [a, b] \]
\[ d(x_2) = k_3 \]

Both $x_1$, $x_2$ have to be reset

Eff $x_1$, $x_2 \in [c, d]$

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
CSR Decidable for IRHA?

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

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021
Takeaway messages

• For restricted classes of HA, e.g., ITA, IRHA, Control state reachability is decidable (Alur-Dill)

• The problem becomes undecidable for RHA (Henzinger et al.)
  • Important message to re-focus on relaxed problem
  • Bounded time, approximate reachability

Slides adapted from Prof. Sayan Mitra’s slides in Fall 2021