Lecture 2.
Decidability and Verification
Advantages
Automated formal verification, Effective debugging tool

Moderate industrial success
In-house groups: Intel, Microsoft, Lucent, Motorola…
Commercial model checkers: FormalCheck by Cadence

Obstacles
Scalability is still a problem (about 100 state vars)
Effective use requires great expertise
Model Checking of Hybrid Systems

Is finite state analysis possible?
Is reachability problem decidable?

gives rise to the infinite transition system:

Is finite state analysis possible?
Is reachability problem decidable?
Finite Partitioning

Goal: To partition state-space into finitely many equivalence classes so that equivalent states exhibit similar behaviors
Talk Outline

- Preliminaries: Transition Systems
- Timed Automata and Region Graphs
- Equivalences and Finite Quotients
- Decidable Problems
Labeled Transition System $T$

- Set $Q$ of states
- Set $I$ of initial states
- Set $L$ of labels
- Set $\rightarrow$ of labeled transitions of the form $q \xrightarrow{a} q'$
Partitions and Quotients

- Let $T = (Q, I, L, \rightarrow)$ be a transition system and $\equiv$ be a partitioning of $Q$ (i.e. an equivalence relation on $Q$)

- Quotient $T/\equiv$ is transition system:
  1. States are equivalence classes of $\equiv$
  2. A state $P$ is initial if it contains a state in $I$
  3. Set of labels is $L$
  4. Transitions: $P \xrightarrow{a} P'$ if $q \xrightarrow{a} q'$ for some $q$ in $P$ and some $q'$ in $P'$
Language Equivalence

- Language of T: Set of possible finite strings over L that can be generated starting from initial states
- T and T’ are language-equivalent iff they generate the same language
- Roughly speaking, language equivalent systems satisfy the same set of “safety” properties
Bisimulation

- Relation $\equiv$ on $Q \times Q'$ is a bisimulation iff whenever $q \equiv q'$ then
  
  if $q \xrightarrow{a} u$ then for some $u'$, $u \equiv u'$ and $q' \xrightarrow{a} u'$, and
  
  if $q' \xrightarrow{a} u'$ then for some $u$, $u \equiv u'$ and $q \xrightarrow{a} u$.

- Transition systems $T$ and $T'$ are bisimilar if there exists bisimulation $\equiv$ on $Q \times Q'$ such that
  
  For every $q$ in $I$, there is $q'$ in $I'$, $q \equiv q'$ and vice versa.

- Many equivalent characterizations (e.g. game-theoretic)

- Roughly speaking, bisimilar systems satisfy the same set of branching-time properties (including safety)
Bisimulation Vs Language equivalence

Language equivalent but not bisimilar
Bisimilarity -> Language equivalence
Timed Vs Time-Abstract Relations

- Transition system associated with a timed/hybrid automaton:
  - Labels on continuous steps are delays in \( \mathbb{R} \)
  - Actual delays are suppressed (all continuous steps have same label): **Time-abstract**

- Two versions of language equivalence and two versions of bisimulation

- Time-abstract relations enough to capture untimed properties (e.g. reachability, safety)
Time-abstract Vs Timed

Time-abstract equivalent but not timed equivalent
Timed equivalence $\rightarrow$ Time-abstract equivalence
Talk Outline

✓ Preliminaries: Transition Systems
💰 Timed Automata and Region Graphs
☐ Equivalences and Finite Quotients
☐ Decidable Problems
Timed Automata (Recap)

- Only continuous variables are timers
- Invariants and Guards: $x <\text{const}, x \geq \text{const}$
- Actions: $x := 0$
- Can express lower and upper bounds on delays
Regions
Finite partitioning of state space

**Definition**

An equivalence class (i.e. a *region*) in fact there is only a finite number of regions!!

\[ w \equiv w' \text{ iff they satisfy the same set of constraints of the form} \]
\[ x_i < c, x_i = c, x_i - x_j < c, x_i - x_j = c \]
\[ \text{for } c \leq \text{ largest const relevant to } x_i \]

An equivalence class (i.e. a *region*)
in fact there is only a *finite* number of regions!!
Region Operations

An equivalence class (i.e. a region)

Successor regions, Succ(r)

Reset regions

{x}r

{y}r
Properties of Regions

- The region equivalence relation $\equiv$ is a time-abstract bisimulation:
  - Action transitions: If $w \equiv v$ and $(l,w) -a-> (l',w')$ for some $w'$, then $\exists v' \equiv w'$ s.t. $(l,v) -a-> (l',v')$
  - Delay transitions: If $w \equiv v$ then for all real numbers $d$, there exists $d'$ s.t. $w+d \equiv v+d'$

- If $w \equiv v$ then $(l,w)$ and $(l,v)$ satisfy the same temporal logic formulas
Region graph of a simple timed automata
Region Graphs (Summary)

- Finite quotient of timed automaton that is time-abstract bisimilar
- Number of regions: (\# of locations) times (product of all constants) times (factorial of number of clocks)
- Precise complexity class of reachability problem: PSPACE (basically, exponential dependence of clocks/constants unavoidable)
Talk Outline

✓ Preliminaries: Transition Systems
✓ Timed Automata and Region Graphs
/tcp Equivalences and Finite Quotients
/tcp Decidable Problems
Multi-rate Automata

- Modest extension of timed automata
  - Dynamics of the form $dx = \text{const}$ (rate of a clock is same in all locations)
  - Guards and invariants: $x < \text{const}$, $x > \text{const}$
  - Resets: $x := \text{const}$

- Simple translation to timed automata that gives time-abstract bisimilar system by scaling

\begin{align*}
  dx &= 2 \\
  dy &= 3 \\
  x > 5 \text{ and } y < 1 \\
  du &= 1 \\
  dv &= 1 \\
  u > 5/2 \text{ and } v < 1/3
\end{align*}
Rectangular Automata

- Interesting extension of timed automata
  - Dynamics of the form $dx$ in const interval (rate-bounds of a clock same in all locations)
  - Guards/invariants/resets as before
- Translation to multi-rate automata that gives time-abstract language-equiv system

\[
\begin{align*}
\text{dx in } [2,3] & \quad x < 2 \\
\text{v} & > 5, \text{ u} := 5 \\
\text{du} & = 2 \\
\text{dv} & = 3 \\
\end{align*}
\]
Rectangular Automata may not have finite bismilar quotients!

\[ \begin{align*}
&dx = 1, \quad dy \in [1, 2] \\
&x = 1, \quad a, \quad x := 0 \\
&y = 1, \quad b, \quad y := 0
\end{align*} \]
Continuous systems

- Given an initial partitioning $P$ of $\mathbb{R}^k$ and continuous dynamics $dX = F(X)$, is there a refinement of $P$ that is time-abstract bisimilar to the original system?

- Counter-example: Spiral. Initial partition: $-5 \leq x < 0$ and $0 < x \leq 5$
O-minimal Structures

A structure over $\mathbb{R}$ is order-minimal if every definable subset is a finite union of points and open intervals.

O-minimal structures

- $\mathbb{R}$ with $<, +, -, 0, 1$ (polyhedral sets)
- $\mathbb{R}$ with $<, +, -, *, e^x, 0, 1$ (semialgebraic sets and exponential trajectories)
- And many more such as sub-analytic
O-minimal Hybrid Systems

- Guards, Flows, Invariants definable in the same o-minimal structure
- Edges reset all variables (to constants or intervals)
- Thm: O-minimal hybrid systems have finite time-abstract bisimilarity quotients
Talk Outline

✓ Preliminaries: Transition Systems
✓ Timed Automata and Region Graphs
✓ Equivalences and Finite Quotients
☞ Decidable Problems
Decidable Problems

- Model checking branching-time properties of timed automata
- Reachability in rectangular automata
- Timed bisimilarity: are given two timed automata bisimilar?
- Optimization: Compute shortest paths (e.g. minimum time reachability) in timed automata with costs on locations and edges
- Controller synthesis: Computing winning strategies in timed automata with controllable and uncontrollable transitions
Undecidable Reachability Problems

- Timed automata + linear expressions as guards
- Multi-rate automata with comparisons among clocks as guards
- Timed automata + stop-watches (i.e. clocks that can have rates 0 or 1)

Many such results
Proofs by encoding Turing machines/2-counter machines
Sharp boundary for decidability understood
Air-traffic Control Problem as Weighted timed automaton

\[
\begin{align*}
\text{Start} & : c_0 \\
\text{wait1} & : w_1: y < 2, c_1: x < 1, y < 1 \\
\text{hold1} & : w'_1, c_3: x = 0, y = 0 \\
\text{land2} & : c_0 + w_1, 1 < x < 2, y > 1 \\
\text{wait2} & : w_2: x < 2, c_2: x < 1, y < 1 \\
\text{hold2} & : w'_2, c_4: y = 0 \\
\text{Land1} & : c_0 + w_2, 1 < y < 2, x > 1 \\
\text{Done} & \\
\end{align*}
\]
Shortest Paths in WTA

- Optimum solution may only be a limit
- Region graph construction not enough
- Algorithm
  1. Reduce to Parametric Shortest Path Problem on graphs (PSP)
  2. Solve PSP
From WTA to Weighted Graphs

- Augmented Region Automaton

  - Regions are split in boundary sub-regions

\[ \begin{align*}
  w_1(\theta_2 + \theta_3) & \quad \text{wait1} \quad 0 < x < 1 \quad (1,2) \\
  \text{hold1} & \quad x = 0 \quad (1) \\
  \text{hold1} & \quad y > 0 \quad (1,2)
\end{align*} \]
Summary

- Decidability only when simple dynamics or decoupled dynamics
- Theory of equivalences useful in understanding structural properties