Cyberphysical Systems: Invariants

Sayan Mitra

Verifying cyberphysical systems

mitras@illinois.edu

How to prove invariants of hybrid automata

Theorem 7.1. Given an HIOA $\mathcal{A} = \langle X, \Theta, A, \boldsymbol{D}, \boldsymbol{T} \rangle$, if a set of states $I \subseteq val(X)$ satisfies the following:

- (Start condition) For any starting state $\boldsymbol{x} \in \Theta, \boldsymbol{x} \in I$ and
- (Transition closure) For any action $\mathrm{a} \in A$, if and $\boldsymbol{x} \rightarrow_{\boldsymbol{a}} \boldsymbol{x}'$ and $\boldsymbol{x} \in I$ then $\boldsymbol{x}' \in I$, and
- (Trajectory closure) For any trajectory $\tau \in \boldsymbol{T}$ if $\tau.fstate \in I$ then $\tau.lstate \in I$

Then I is an inductive invariant of $\mathcal{A}$.

How to prove invariants of hybrid automata

Theorem 7.1. Given an HIOA $\mathcal{A} = \langle X, \Theta, A, \boldsymbol{D}, \boldsymbol{T} \rangle$, if a set of states $I \subseteq val(X)$ satisfies the following:

- (Start condition) For any starting state $\boldsymbol{x} \in \Theta, \boldsymbol{x} \in I$ and
- (Transition closure) For any action a $\in A$, if and $\boldsymbol{x} \rightarrow_{\boldsymbol{a}} \boldsymbol{x}'$ and $\boldsymbol{x} \in I$ then $\boldsymbol{x}' \in I$, and
- (Trajectory closure) For any trajectory $\tau \in \boldsymbol{T}$ if $\tau.fstate \in I$ then $\tau.lstate \in I$

Then I is an inductive invariant of $\mathcal{A}$.

Proof. Consider any reachable state $x \in Reach_{\mathcal{A}}$. By the definition of a reachable state, there exists an execution α of $\mathcal{A}$ with $\alpha.lstate = x$. We proceed by induction on the length of the execution α. For the base case, α consists of a single starting state $\boldsymbol{x} \in \Theta$, and, by the *start condition*, $\boldsymbol{x} \in I$. For the inductive step, we consider two subcases:

Case 1: $\alpha = \alpha' a\, p(\boldsymbol{x})$, where $a \in A$ and $p(\boldsymbol{x})$ is a point trajectory at $\boldsymbol{x}$.

By the induction hypothesis, we know that $\alpha'.lstate \in I$.

By invoking the *transition closure*, we obtain $\boldsymbol{x} \in I$.

Case 2: $\alpha = \alpha' \tau$, where τ is a trajectory of $\mathcal{A}$ and $\tau.lstate = \boldsymbol{x}$

By the *induction hypothesis*, $\alpha'.lstate \in I$ and by

invoking the *trajectory closure*, we deduce that $\tau.lstate = \boldsymbol{x} \in I$

An application

automaton Bouncingball(c,h,g)

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

actions: bounce

transitions:

bounce

pre *x = 0 /\ v < 0*

eff v := -cv

trajectories:

Loc1

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

invariant $\boldsymbol{x \geq 0}$

Candidate invariant: ``stays above ground''

$I_0: x \geq 0 \equiv \{\boldsymbol{u} \in val(\{x, v\}) | \, \boldsymbol{u}\lceil x \geq 0 \}$

Applying Theorem 7.1:

- Consider any initial state $\boldsymbol{u} \in \Theta; \boldsymbol{u}\lceil x = h \geq 0$
  - $\boldsymbol{u} \in I_0$
- Consider any transition $\boldsymbol{u} \rightarrow_{bounce} \boldsymbol{u}'$
  - From precondition we know $\boldsymbol{u}\lceil x = 0$; from effect we know $\boldsymbol{u}'.x = \boldsymbol{u}.x$ therefore $\boldsymbol{u}'\lceil x = 0 \geq 0$
  - $\boldsymbol{u}' \in I_0$
- Consider any trajectory $\tau \in T$
  - From mode invariant we know that for $\forall t \in \tau.dom\, , \tau(t)\lceil x \geq 0$
  - It follows that $\tau.lstate\lceil x \geq 0$
- What part of Bouncingball was used ? What could be changed?

An application

automaton Bouncingball(c,h,g)

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

actions: bounce

transitions:

bounce

pre *x = 0 /\ v < 0*

eff v := -cv

trajectories:

Loc1

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

invariant $\boldsymbol{x \geq 0}$

Candidate invariant: ``stays above ground and below h''

$I_h: h \geq x \geq 0$

Applying Theorem 7.1:

- Consider any initial state $\boldsymbol{u} \in \Theta$; $\boldsymbol{u}\lceil x = h$
  - $\boldsymbol{u} \in I_h$
- Consider any transition $\boldsymbol{u} \rightarrow_{bounce} \boldsymbol{u}'$
  - From precondition we know $\boldsymbol{u}\lceil x = 0$; from effect we know $\boldsymbol{u}'.x = \boldsymbol{u}.x$ therefore $\boldsymbol{u}'\lceil x = 0$
  - $\boldsymbol{u}' \in I_h$
- Consider any trajectory $\tau \in T$
  - From mode invariant and inductive hypothesis we know that for $\forall t \in \tau.dom$, $\tau(t)\lceil x \geq 0$ **and** , $\tau(0)\lceil x \in [0, h]$ and that τ is a solution of d(x) = v; d(v) = -g
  - Is this adequate to infer $\tau.lstate \in I_h$?

Strengthened invariant

automaton Bouncingball(c,h,g)

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

k: Nat := 0

actions: bounce

transitions:

bounce

pre *x = 0 /\ v < 0*

eff v := -cv; k:= k + 1

trajectories:

Loc1

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

invariant $\boldsymbol{x \geq 0}$

Candidate invariant: ``stays above ground and below h''

$I_v: v^2 - 2g\left(hc^{2k} - x\right) = 0$

Applying Theorem 7.1:

- Consider any initial state $\boldsymbol{u} \in \Theta$; $\boldsymbol{u}\lceil x = h; \boldsymbol{u}\lceil k = 0$
  - $\boldsymbol{u} \in I_v$
- **Exercise**: Finish the rest

Summary

- Theorem 7.1 gives a sufficient condition for proving **inductive** invariants
- Not all invariants are inductive
- We often have to **strengthen** invariants to make them inductive
- Read examples in Chapter 7

Floyd-Hoare Proofs

The core idea of inductive invariants dates back to the classical program analysis technique called **Floyd-Hoare logic**

The logic provides a set of rules for deducing correctness of automata, programs

The logic is built on **Hoare triples**, which describes how the execution of a statement (or line of code) changes the state of the automaton:

$P\ c\ Q$ where

- P and Q are predicates on the program variables and are called the **precondition** and **postcondition**
- c is a statement describing program variable change

The triple implies that when the precondition P is met, execution of c establishes the postcondition Q

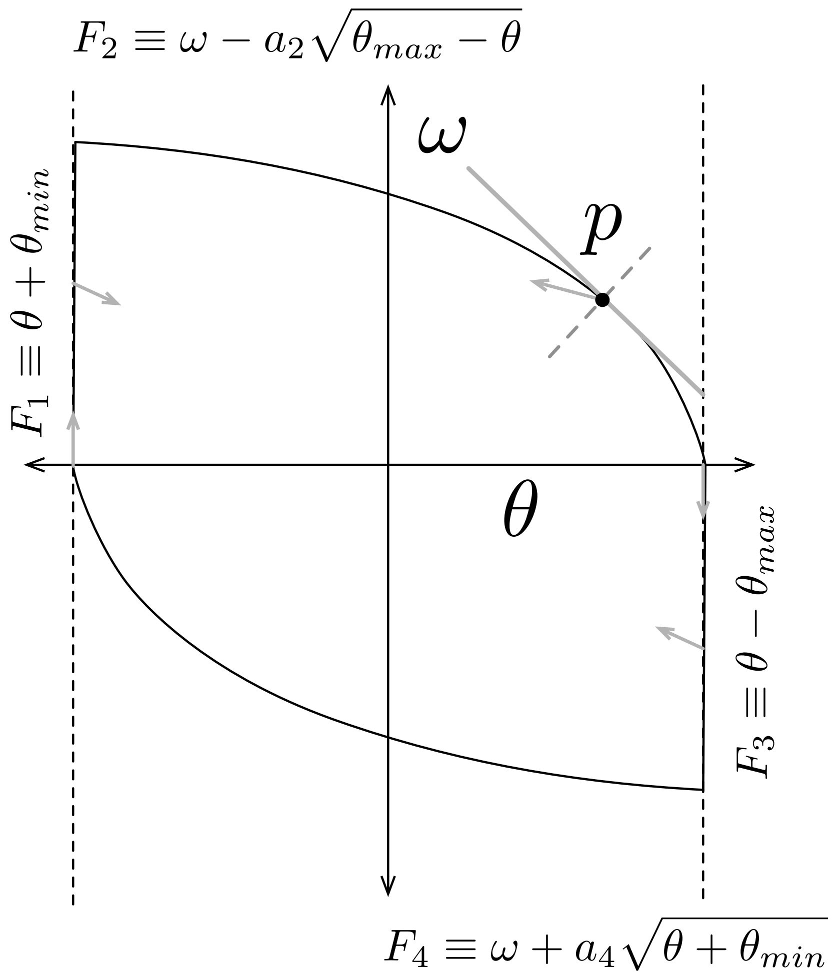
Sub-tangential conditions. Checking trajectory conditions without solving ODEs

(Trajectory closure) For any trajectory $\tau \in \boldsymbol{T}$ if $\tau.fstate \in I$ then $\tau.lstate \in I$

Lemma. Consider the ODE $\dot{x} = f(x)$ for state variable x, describing $\boldsymbol{T}$

Let I be a compact set containing the initial set Θ. Then, I is an inductive invariant of the above ODE if at every state $\boldsymbol{x}$ on the boundary of I, the vector $f(x)$ is pointing inwards from the boundary. That is $\frac{\partial P(\boldsymbol{x})}{\partial \boldsymbol{x}}.f(x) \geq 0$**,** where the boundary of I is defined by $\mathrm{P}(\boldsymbol{x}) = 0$

Checking sub-tangential condition



Assignments

- Chapter 7
  - Examples: Mutual exclusion, helicopter model
  - Barrier certificates
- Project proposals due thursday