Lecture 24: Progress Verification; Stability of Hybrid Systems

Huan Zhang

huan@huan-zhang.com

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

Due dates & deadlines

- Final **project presentations**: Week of **4/29** and **5/1**
- **Presentation slides due: 4/29 at 11 am (before class, hard deadline)**
- Same presentation schedule as the mid-term presentation:
  - People who presented mid-term on Tuesday will present on Thursday
  - People who presented mid-term on Thursday will present on Tuesday
  - Schedule will be posted on Canvas
- Attendence required, for each lecture, choose 2 projects that you are mostly interested in and submit two **feedback forms** (template will be posted on Canvas) to Canvas, due **72 hours after class**
- Feedback forms will be distributed to your peers to help them finalize their report
- No regular class on 5/6 (will become an office hour for final project; come to the classroom if you have questions)
- **HW4** will be posted on 4/26, due **5/10**
- **Final report** due **5/18**

Proving termination for automata

- Automaton $\mathcal{A} = (V, \Theta,\ \boldsymbol{D})$
- Recall $\boldsymbol{D} \subseteq val(V) \times val(V)$
- Automaton terminates if it does not have any infinite executions

- **Definition:** A **well-founded relation** < on a set S is a binary relation $< \ \subseteq S\ \times S$ such that every subset $S' \subseteq S$ has a **least** element.
- In other words, there are no infinite decreasing chains of elements s_0, s_1, ..., with $s_{i+1} < s_i$.
- Example: totally order set, e.g., {1, 2, 3, ...} with the usual order
- Example: $S = \mathbb{Z}^+$ a < b iff a divides b and a ≠ b (b mod a = 0, b ≠ a)
- Example: $S = \{0,1\}^*$ a < b iff a is a proper substring of b
- Example: $S = \{-1,\ -2,\ -3, \ldots\}$, < is the usual order, then < is **not** a well-founded relation

Proving termination for automata

Theorem. Automaton $\mathcal{A} = (V, \Theta, \boldsymbol{D})$ terminates iff there exists a well-founded **relation** R such that $\boldsymbol{D} \cap Reach_{\mathcal{A}} \times Reach_{\mathcal{A}} \subseteq R$.

Proof. If there exists R and automaton does not terminate.

Then there exists an infinite sequence of states $s_0, s_1, \ldots,$ with $s_i \, \boldsymbol{D} \, s_{i+1}$. Since these are reachable states, $s_i \, R \, s_{i+1}$. This violates the definition of a well-founded relation.

Suppose $\mathcal{A}$ is terminating, we define

$R = \boldsymbol{D} \cap Reach_{\mathcal{A}} \times Reach_{\mathcal{A}}$

check that R is indeed well-founded (because $\boldsymbol{D}$ does not permit infinite sequences)

Ranking functions

Often the well-founded relation is defined in terms of a ***ranking function*** $f\colon \mathrm{val}(V) \rightarrow \mathbb{N}$ such that for any reachable $\boldsymbol{v} \in val(V)$ and $\boldsymbol{v}'$ $such\ that$ $(\boldsymbol{v}, \boldsymbol{v}') \in D,\ f(\boldsymbol{v}') < f(\boldsymbol{v})$

Here < is a the usual comparison on integers

Instead of $\mathbb{N}$, the ranking function could use any other range set with a lower bound

Example

```
automaton UpDown
  signature
    internal up(d:Nat), down

  variables
    internal x, y : Int

  transitions
    internal up(d) where d = 1
      pre x > 0 ∧ y > 0
      eff x := x -1
          y := y + d

    internal down
      pre y > 0
      eff y := y -1
```

Example

```
automaton UpDown
  signature
    internal up(d:Nat), down

  variables
    internal x, y : Int

  transitions
    internal up(d) where d = 1
      pre x > 0 ∧ y > 0
      eff x := x -1
        y := y + d

    internal down
      pre y > 0
      eff y := y -1
```

Consider the ranking function $f(x, y) = 2x + y$

Check that for any transition $(x, y) \rightarrow (x', y')$

Up(1) $2x' + y' = 2(x - 1) + y + 1 = 2x + y - 1 = f(x, y) - 1 < f(x, y)$

Down: $2x' + y' = 2x + y - 1 = f(x, y) - 1 < f(x, y)$

Hence, the automaton terminates

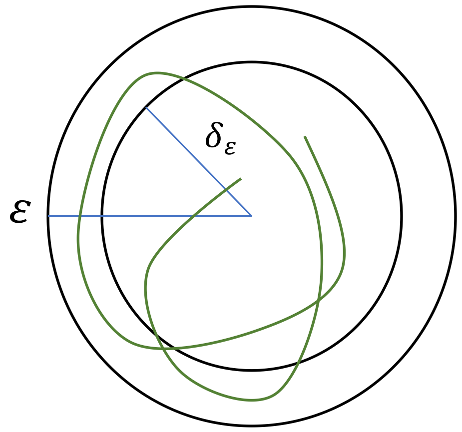
What if d > 1 ?

Recall Stability

- Time invariant autonomous systems (closed systems, systems without inputs)
- $\dot{x}(t) = f\big(x(t)\big),\ x_0 \in \mathbb{R}^n,\ t_0 = 0$ *(Eq. 1)*
- $\xi(t)$ is the solution
- $|\xi(t)|$ norm
- $x^* \in \mathbb{R}^n$ is an **equilibrium point** if $f(x^*) = 0$.
- For analysis we will assume **0** to be an equilibrium point of (1) with out loss of generality

Lyapunov stability

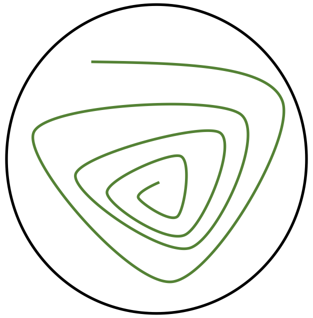
Lyapunov stability: The system (1) is said to be ***Lyapunov stable*** (at the origin) if for every $\varepsilon > 0$ there exists $\delta_\varepsilon > 0$ such that for every if $|\xi(0)| \leq \delta_\varepsilon$ then for all t ≥ 0, $|\xi(t)| \leq \varepsilon$.



Asymptotically stability

The system (1) is said to be ***Asymptotically stable*** *(at the origin)* if it is Lyapunov stable and there exists $\delta_2 > 0$ such that for every if $|\xi(0)| \leq \delta_2$ then t $\rightarrow \infty$, $|\xi(t)| \rightarrow \mathbf{0}$.

If the property holds for any δ_2 then **Globally Asymptotically Stable**



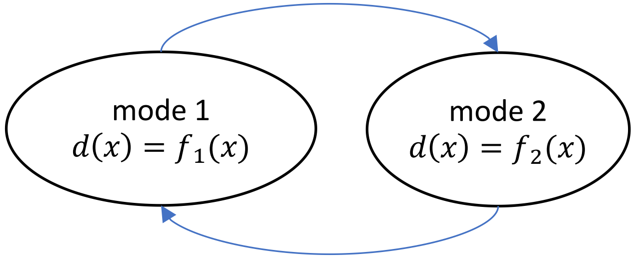
Verifying Stability for one dynamical system

Theorem. (Lyapunov) Consider the system (1) with state space $\xi(t) \in \mathbb{R}^n$ and suppose there exists a positive definite, continuously differentiable function $V: \mathbb{R}^n \to \mathbb{R}$. The system is:

1. Lyapunov stable if $\dot{V}\big(\xi(t)\big) := \frac{\partial V}{\partial x} f(x) \leq 0$, for all $x \neq 0$
2. Asymptotically stable if $\dot{V}\big(\xi(t)\big) < 0$, for all $x \neq 0$
3. It is globally AS if *V* is also radially unbounded.

(V is radially unbounded if $\big||x|\big| \to \infty \Rightarrow V(x) \to \infty$)

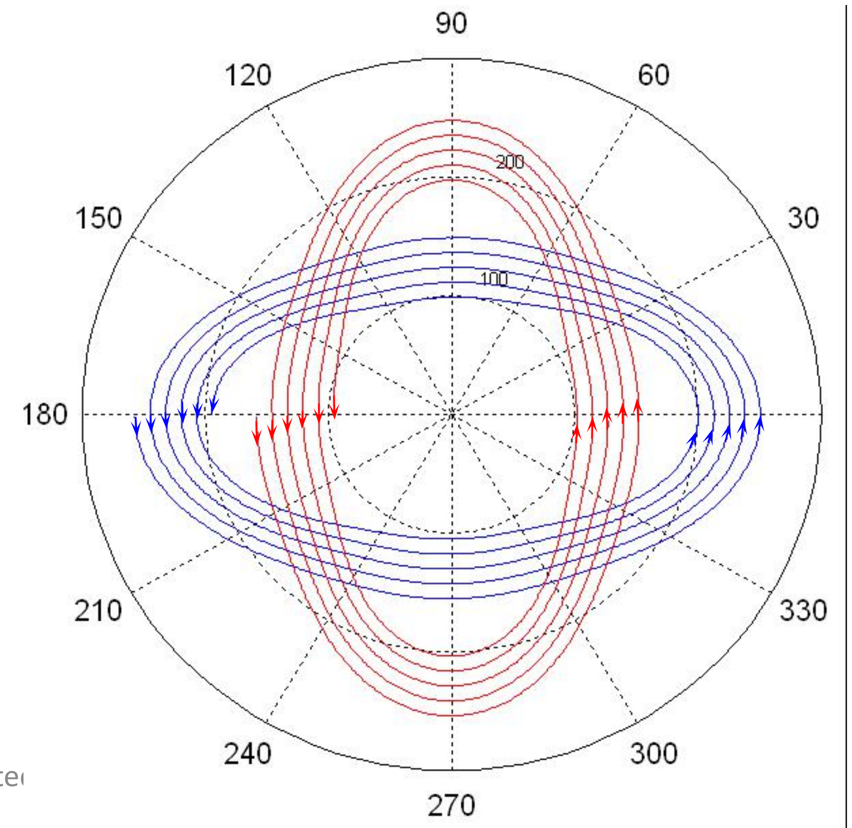
Defining stability of hybrid systems



- Hybrid automaton: $\mathbf{A} = \langle V, A,\ D, \mathrm{T}\rangle$
  - $V = X \cup \{\ell\}$
- Execution $\alpha = \tau_0 a_1 \tau_1 a_2 \ldots$
- Notation $\alpha(t)$: denotes the valuation $\beta.lstate$ where β is the longest prefix with $\beta.\mathrm{ltime} = t$
- $|\alpha(t)|$: norm of the continuous state X
- ***A*** is ***Lyapunov stable*** (at the origin) if for every $\varepsilon > 0$ there exists $\delta_\varepsilon > 0$ such that for every if $|\alpha(0)| \leq \delta_\varepsilon$ then for all t $\geq 0,\ |\alpha(t)| \leq \varepsilon$.
- ***Asymptotically stable*** if it is Lyapunov stable and there exists $\delta_2 > 0$ such that for every if $|\alpha(0)| \leq \delta_2$ then t $\rightarrow \infty,\ |\alpha(t)| \rightarrow \mathbf{0}$.

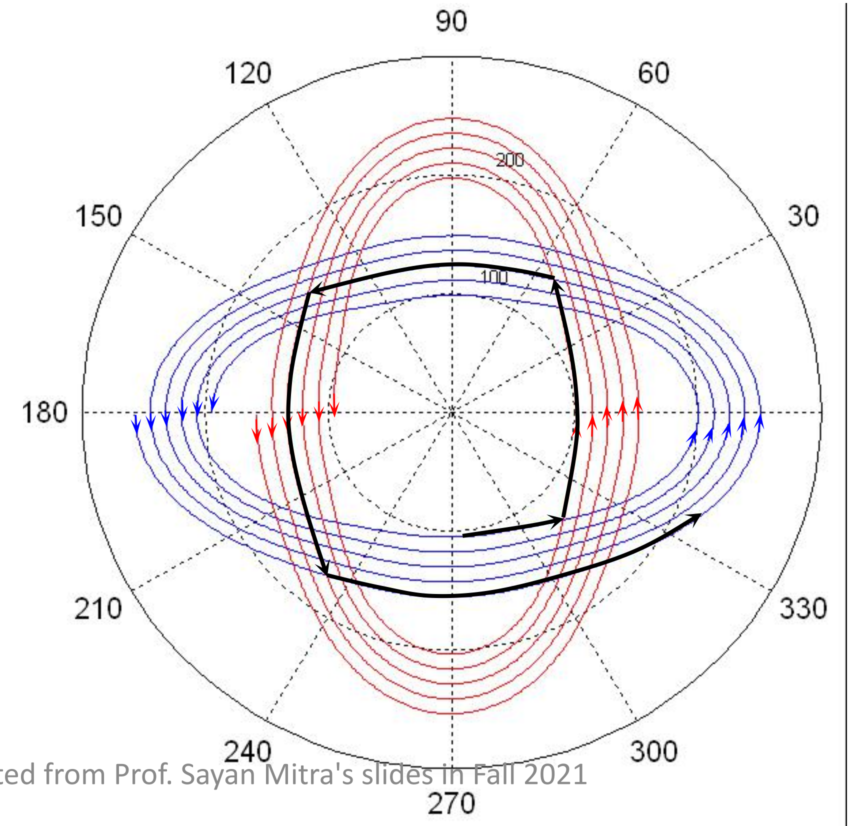
Question:Stability Verification

- If each mode is asymptotically stable then is ***A*** *also asymptotically stable?*



Question: Stability Verification

- If each mode is asymptotically stable then is ***A*** *also asymptotically stable?*
- ***No***



Common Lyapunov Function

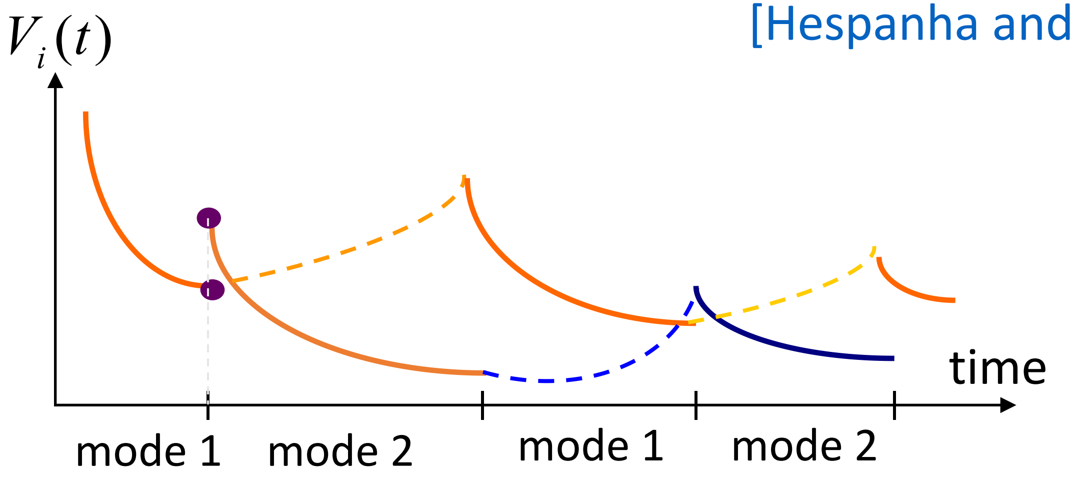
- If there exists positive definite continuously differentiable function $V: \mathbb{R}^n \rightarrow \mathbb{R}$ and a positive definite function W: $\mathbb{R}^n \rightarrow \mathbb{R}$ such that for each mode $i, \frac{\partial V}{\partial t} f_i(x) <- W(x)$ for all $x \neq 0$ then V is called a common Lyapunov function for A.

- V is called a common Lyapunov function

- **Theorem.** A is globally asymptotically stable if there exists a common Lyapunov function.

Stability Under Slow Switching

[Hespanha and Morse`99]



- Average Dwell Time (ADT) characterizes rate of mode switches
- Definition: H has ADT T if there exists a constant N_o such that for every execution α, the number of mode switches in α:

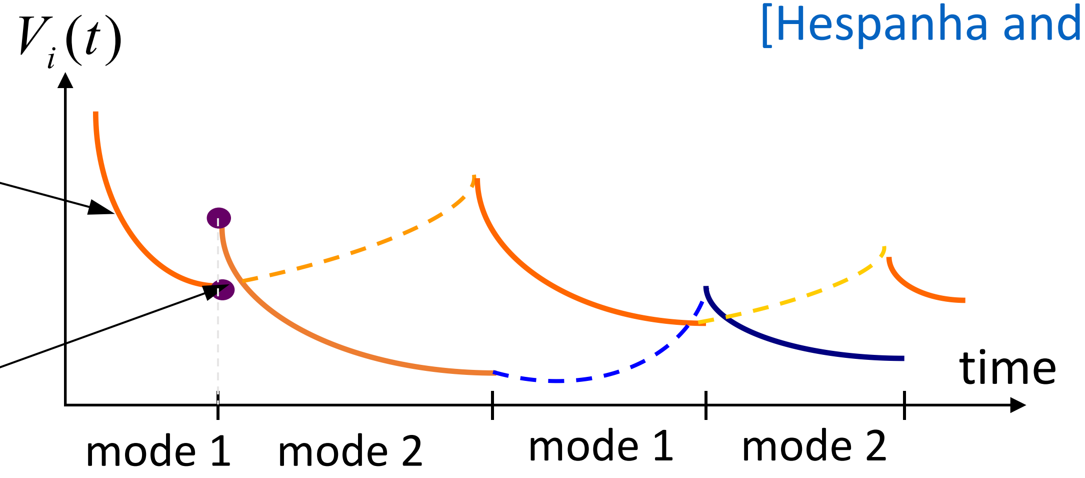
$$N(\alpha) \leq N_o + \text{duration}(\alpha)/T.$$

Stability Under Slow Switching

[Hespanha and Morse`99]

Stable in each mode $\frac{\partial V_i}{\partial x} \leq -2\lambda_0 V_i(x)$

"Energy" may increase when switch but up to a factor of μ $V_2 \leq \mu\ V_1$



- Average Dwell Time (ADT) characterizes rate of mode switches
- Definition: H has ADT T if there exists a constant N_o such that for every execution α, the number of mode switches in α: $N(\alpha) \leq N_o + \text{duration}(\alpha)/T$.

N(α): **Theorem** [HM`99] H is asymptotically stable if its modes have a set of Lyapunov functions (μ, λ_0) and ADT(H) > log μ/λ_0 .

Dwell time is long enough so energy can decrease sufficiently in each mode

Remarks about ADT theorem assumptions

1. If f_i is globally asymptotically stable, then there exists a Lyapunov function V_i that satisfies $\frac{\partial V_i}{\partial x} \leq -2\lambda_i V_i(x)$ for appropriately chosen $\lambda_i > 0$
2. If the set of modes is finite, choose λ_0 independent of i
3. The other assumption restricts the maximum increase in the value of the current Lyapunov functions over any mode switch, by a factor of μ.
4. We will also assume that there exist strictly increasing functions β_1 and β_2 such that $\beta_1(|x|) \leq V_i(x) \leq \beta_2(|x|)$

Our goals in this course

Write programs (tools) that prove correctness

- *Understand fundamental limits of creating such tools*
- *Learn models of CPS at different levels of abstractions*
- *Gain research experience*

What we have learned in this course

- Satisifiability problems:
  - SAT (DPLL)
  - SMT (DPLL-T)
  - Neural network verification (CROWN bound propagation, branch-and-bound)
- Computation Tree Logic
  - CTL model checking
- Dynamical systems (reachability & invariance):
  - Linear/nonlinear systems, LTI systems
  - stability verification, Lyapunov functions
- Verification of hybrid automata and timed automata
  - Abstractions
  - Composition
  - Progress Analysis
  - Common/Multiple Lyapunov functions