Progress verification

Sayan Mitra
Verifying cyberphysical systems
mitras@illinois.edu

Progress properties

- Every behavior system $\mathcal{A}$ will *eventually* reach a goal **goal**
- CTL: **AF goal**
- Dijkstra: From any state, (possibly >1 tokens) all executions get to a state with 1 token

Invariance/safety

- No behavior of **A** goes outside of **unsafe**
- CTL: **AG unsafe**
- Dijkstra: Starting a state with a 1 token, all executions have 1 token
- Finding a counterexample to safety does <u>not</u> prove progress

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 $s_0, s_1, \ldots$, with $s_{i+1} < s_i$.
- Example: $S = \mathbb{Z}$ a < b iff a divides b and a ≠ b
- Example: $S = \{0,1\}^*$ a < b iff a is a proper substring of b

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, $s_i \ R \ s_{i+1}$ which 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*** $f\colon \mathrm{val}(V) \to \mathbb{N}$ 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
```

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

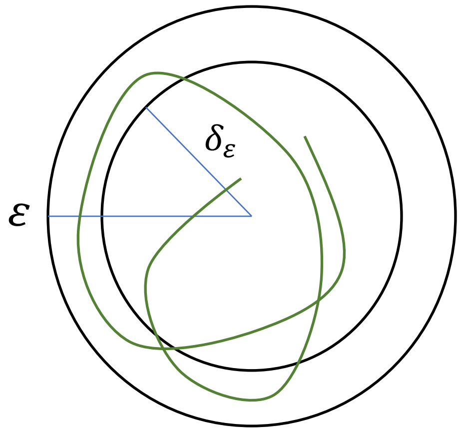
What if d > 1 ?

Recall Stability

- Time invariant autonomous systems (closed systems, systems without inputs)
- $\dot{x}(t) = f\big(x(t)\big), x_0 \in \mathbb{R}^n, t_0 = 0$ *–(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

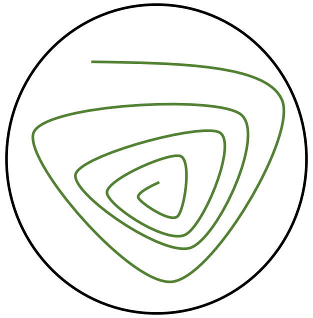
Lyapunov stability: The system (1) is said to be ***Lyapunov stable*** (at the origin) if for every $\varepsilon > 0$ there exists $\delta_\varepsilon > 0$ such that for every if $|\xi(0)| \leq \delta_\varepsilon$ then for all t $\geq 0, |\xi(t)| \leq \varepsilon$.



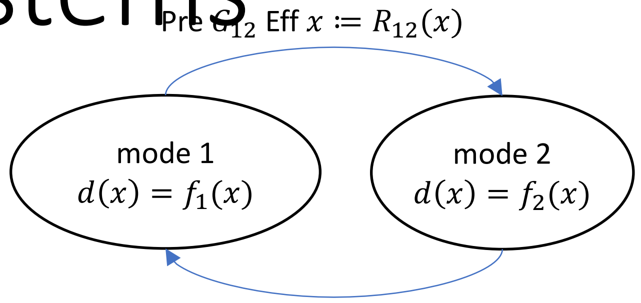
Asymptotically stability

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**



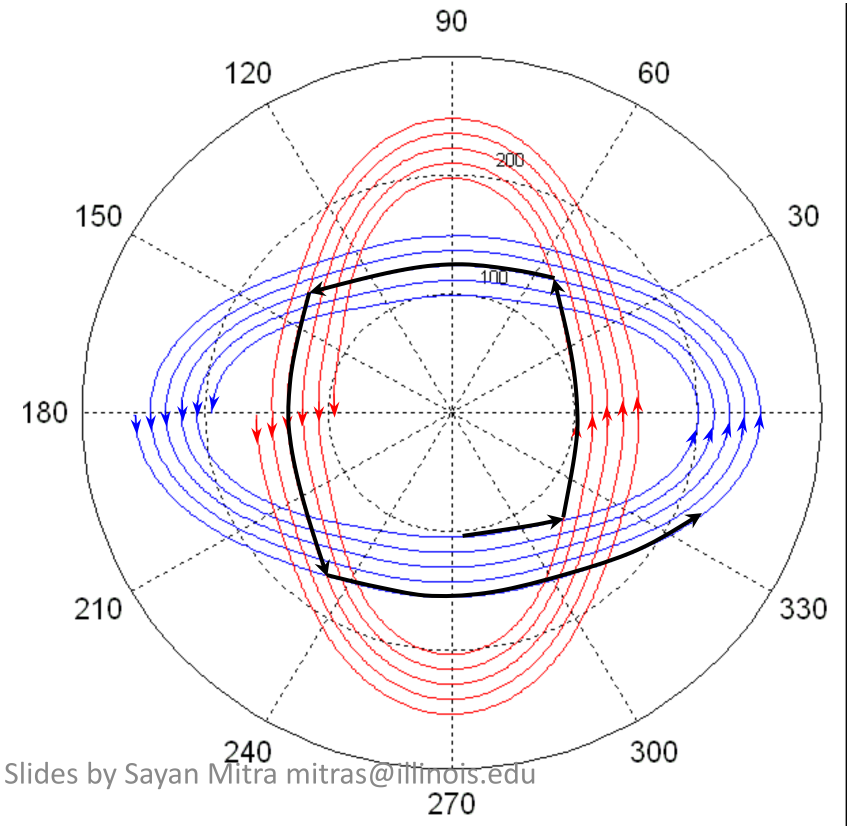
Defining stability of hybrid systems



- 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 $|\alpha(0)| \le \delta_\varepsilon$ then for all t $\geq 0, |\alpha(t)| \le \varepsilon$.
- ***Asymptotically stable*** if it is Lyapunov stable and there exists $\delta_2 > 0$ such that for every if $|\alpha(0)| \le \delta_2$ then t $\rightarrow \infty, |\alpha(t)| \rightarrow \mathbf{0}$.

Question:Stability Verification

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

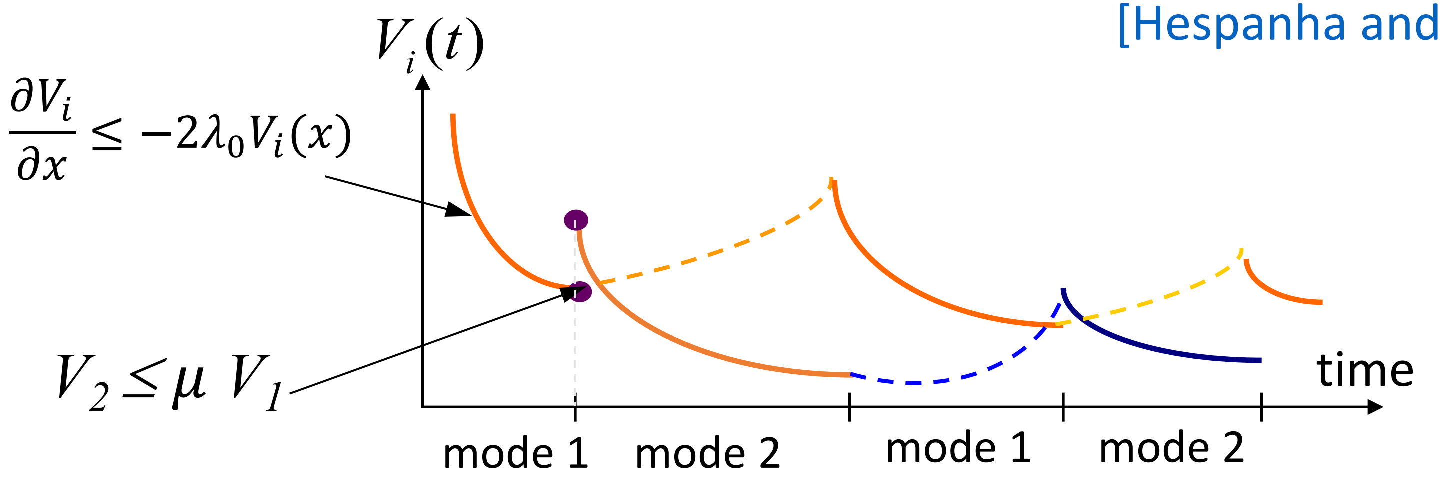
- **Theorem.** ***A*** is GUAS if there exists a common Lyapunov function.

Multiple Lyapunov Functions

- In the absence of a common lyapunov function the stability verification has to rely of the discrete transitions.
- The following theorem gives such a stability in terms of *multiple Lyapunov function*.
- **Theorem** [Branicky] If there exists a family of positive definite continuously differentiable **Lyapunov** functions $V_i: \mathbb{R}^n \to \mathbb{R}$ and a positive definite function $\mathrm{W_i}: \mathbb{R}^n \to \mathbb{R}$ such that for any execution α and for any time t_1 t_2 $\alpha(t_1).\ell = \alpha(t_2).\ell = i$ and for all time $t \in (t_1, t_2), \alpha(t).\ell \neq i$
  - $V_i(\alpha(t_2).x) - V_i(\alpha(t_1).x) \leq -W_i(\alpha(t_1).x)$

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_0 such that for every execution α,

$$N(\alpha) \leq N_0 + \text{duration}(\alpha)/T.$$

N(α): number of mode switches in α

- **Theorem** [HM`99] H is asymptotically stable if its modes have a set of Lyapunov functions (μ, λ_0) and $\boxed{\text{ADT}(H) > \log \mu/\lambda_0}$.

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 $\beta_1(|x|) \leq V_i(x) \leq \beta_2(|x|)$

Proof sketch

Suppose α is any execution of A.

Let $T = \alpha.ltime$ and $t_1, \ldots, t_{N(\alpha)}$ be instants of mode switches in α.

We will find an upper-bound on the value of $V_{\alpha(T).l}(\alpha(T).x)$

Define $W(t) = e^{2\lambda_0 t} V_{\alpha(t).l}(\alpha(t).x)$

W is non-increasing between mode switches $\left[\frac{\partial V_i}{\partial x} \leq -2\lambda_0 V_i(x)\right]$

That is, $W(t_{i+1}^-) \leq W(t_i \ )$

$W(t_{i+1}) \leq \mu W(t_{i+1}^-) \leq \mu W(t_i)$

Iterating this $N(\alpha)$ times: $W(T) \leq \mu^{N(\alpha)} W(0)$

$$e^{2\lambda_0 T} V_{\alpha(T).l}(\alpha(T).x) \leq \mu^{N(\alpha)} V_{\alpha(0).l}(\alpha(0).x)$$

$$V_{\alpha(T).l}(\alpha(T).x) \leq \mu^{N(\alpha)} e^{-2\lambda_0 T} V_{\alpha(0).l}(\alpha(0).x) = e^{-2\lambda_0 T + N(\alpha) \log \mu} V_{\alpha(0).l}(\alpha(0).x)$$

If α has ADT τ_a then, recall, $N(\alpha) \leq N_0 + T/\tau_a$ and $V_{\alpha(T).l}(\alpha(T).x) \leq e^{-2\lambda_0 T + (N_0 + T/\tau_a) \log \mu} V_{\alpha(0).l}(\alpha(0).x) \leq C\ e^{T(-2\lambda_0 + \log \mu / \tau_a)}$

If $\tau_a > \log \mu / 2\lambda_0$ then second term converges to 0 as $T \to \infty$ then from assumption 4 it follows that α converges to 0.

Further reading

- More general conditions for termination proofs of automata (Disjunctive unions of well-founded relations) [Podelski and Rybalchenko]
- Verification of dwell time [Mitra and Liberzon]
- Abstractions for stability proofs [Prabhakar et al., Duggirala et al.]