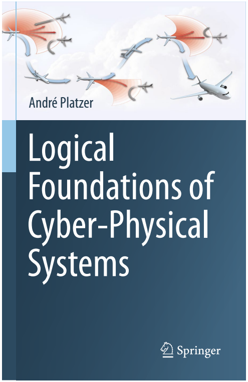
Stability & Switched Systems

Logical Foundations of Cyber-Physical Systems



Stefan Mitsch

Carnegie Mellon University
Computer Science Department

Outline

Outline

1. Beyond Safety
2. Stability
3. Switched Systems
4. Summary

What Else Could Possibly Go Wrong?

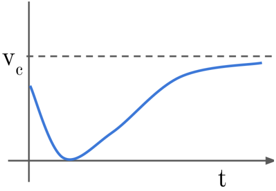
Proposition (System Proved Safe)

$$v \le v_c + \delta \to [(ctrl; ode)^*] v \le v_c + \delta$$

What Else Could Possibly Go Wrong?

Proposition (System Proved Safe)

$$v \le v_c + \delta \to [(ctrl; ode)^*] v \le v_c + \delta$$

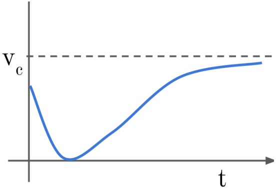


What Else Could Possibly Go Wrong?

Proposition (System Proved Safe)

$$v \leq v_c + \delta \rightarrow [(ctrl; ode)^*]v \leq v_c + \delta$$

↯ Not close to v_c

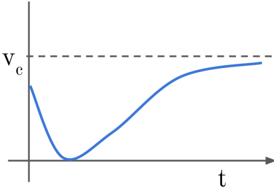


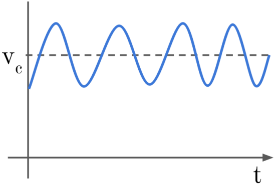
What Else Could Possibly Go Wrong?

Proposition (System Proved Safe)

$$v \leq v_c + \delta \rightarrow [(ctrl; ode)^*]v \leq v_c + \delta$$

↯ Not close to v_c



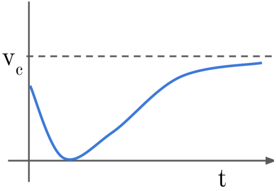


What Else Could Possibly Go Wrong?

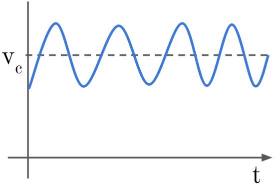
Proposition (System Proved Safe)

$$v \le v_c + \delta \rightarrow [(ctrl; ode)^*] v \le v_c + \delta$$

↯ Not close to v_c



↯ Not converging to v_c

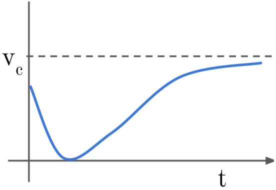


What Else Could Possibly Go Wrong?

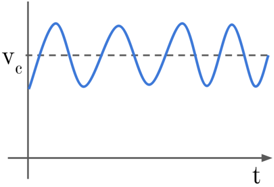
Proposition (System Proved Safe)

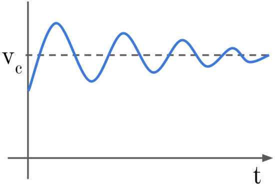
$$v \leq v_c + \delta \rightarrow [(ctrl; ode)^*] v \leq v_c + \delta$$

Not close to v_c



Not converging to v_c



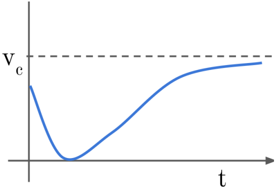


What Else Could Possibly Go Wrong?

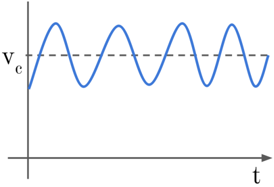
Proposition (System Proved Safe)

$$v \leq v_c + \delta \rightarrow [(ctrl; ode)^*] v \leq v_c + \delta$$

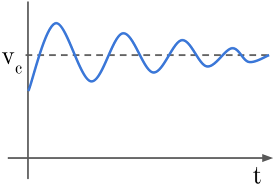
Not close to v_c



Not converging to v_c



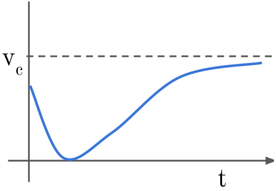
Stable



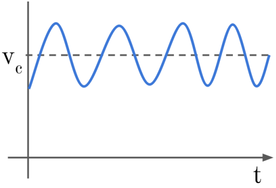
Proposition (System Proved Safe)

$$v \leq v_c + \delta \rightarrow [(ctrl; ode)^*] v \leq v_c + \delta$$

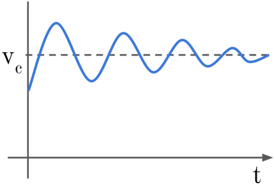
Not close to v_c



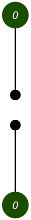
Not converging to v_c



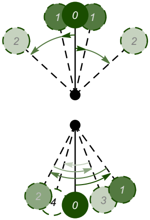
Stable



Theory



Practice

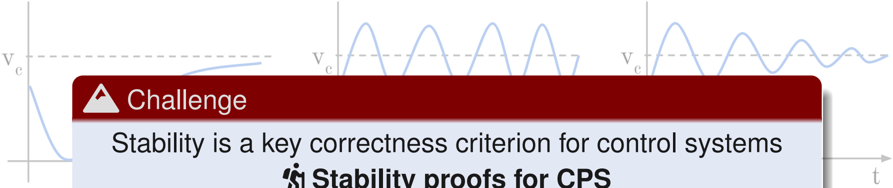


What Else Could Possibly Go Wrong?

Proposition (System Proved Safe)

$$v \le v_c + \delta \rightarrow [(ctrl; ode)^*] v \le v_c + \delta$$

Not close to v_c | Not converging to v_c | Stable



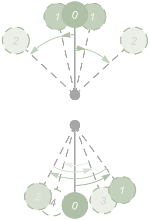
Challenge

Stability is a key correctness criterion for control systems

Stability proofs for CPS

Theory

Practice



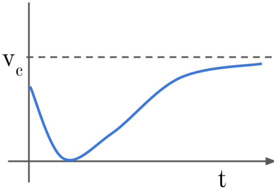
Outline

Asymptotic Stability in dL

- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed

Asymptotic Stability in dL

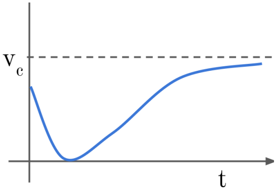
- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed



Asymptotic Stability in dL

- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed

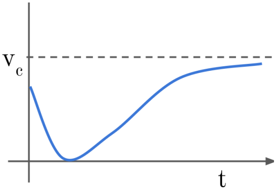
↯ Stable ✔ Attractive

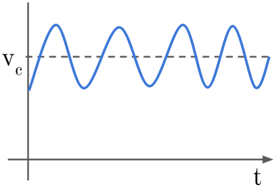


Asymptotic Stability in dL

- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed

↯ Stable ✔ Attractive

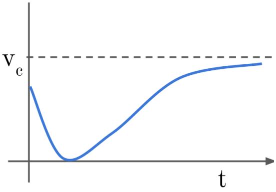




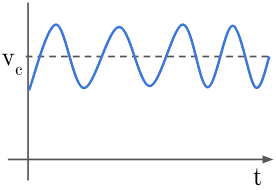
Asymptotic Stability in dL

- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed

↯ Stable ✔ Attractive



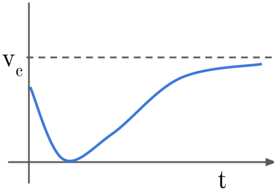
✔ Stable ↯ Attractive



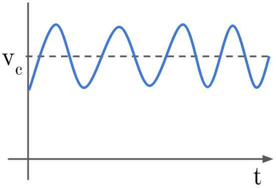
Asymptotic Stability in dL

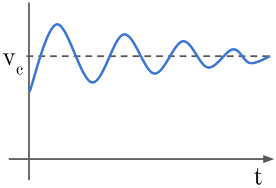
- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed

↯ Stable ✔ Attractive



✔ Stable ↯ Attractive

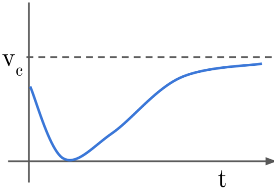




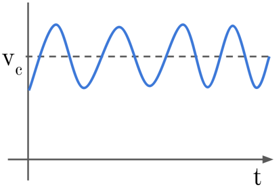
Asymptotic Stability in dL

- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed

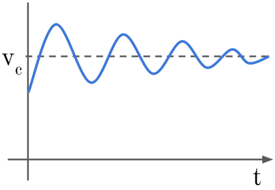
↯ Stable ✔ Attractive



✔ Stable ↯ Attractive



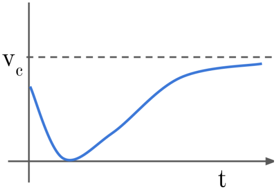
✔ Stable ✔ Attractive



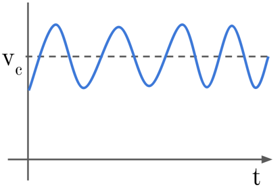
Asymptotic Stability in dL

- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed

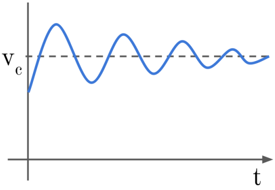
↯ Stable ✓ Attractive



✓ Stable ↯ Attractive

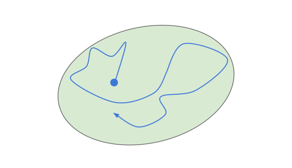


✓ Stable ✓ Attractive

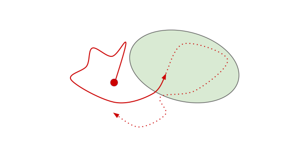


Safety and Liveness

Stability: $[\alpha]P$



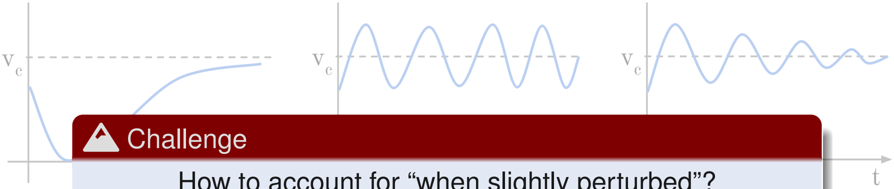
Attractivity: $\langle\alpha\rangle P$



Asymptotic Stability in dL

- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed

⚡ Stable ✔ Attractive | ✔ Stable ⚡ Attractive | ✔ Stable ✔ Attractive

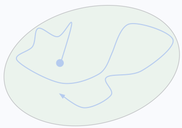


Challenge

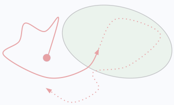
How to account for “when slightly perturbed”?

Safety and Liveness

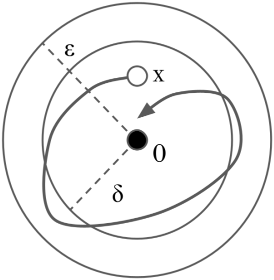
Stability: $[\alpha]P$



Attractivity: $\langle\alpha\rangle P$



- **Stability** stay close to origin when slightly perturbed



Origin 0 of an ODE $x' = f(x)$ with solution $x(t) : [0, T) \to \mathbb{R}^n$ is stable if

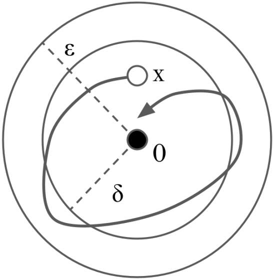
- for all $\varepsilon > 0$
- there exists $\delta > 0$
- s.t. for all $\|x(0)\| < \delta$
- $\|x(t)\| < \varepsilon$ for all t

Stability in dL

- **Stability** stay close to origin when slightly perturbed

Origin 0 of an ODE $x' = f(x)$ with solution $x(t) : [0, T) \to \mathbb{R}^n$ is stable if

- for all $\varepsilon > 0$
- there exists $\delta > 0$
- s.t. for all $\|x(0)\| < \delta$
- $\|x(t)\| < \varepsilon$ for all t

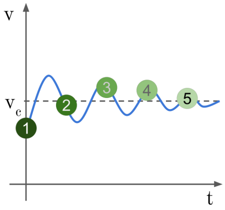


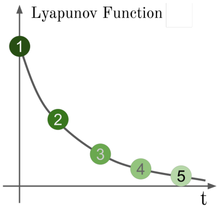
Stability

$$\forall \varepsilon > 0 \, \exists \delta > 0 \, \forall x \, (\|x\| < \delta \to [x' = f(x)] \|x\| < \varepsilon)$$

Lyapunov-functions V are energy-like functions to certify asymptotic stability

- V, V' are continuous
- $V(0) = 0$
- $V(x) > 0$ for all $\|x\| > 0$
- $V' \leq 0$





Lemma (Lyapunov Proof Rule)

Rule $\text{Lyap}_{\geq}$ is derivable in dL

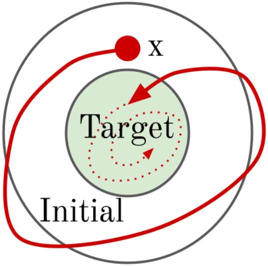
$$\text{Lyap}_{\geq}\ \frac{\vdash f(0) = 0 \land V(0) = 0 \quad 0 < \|x\|^2 \vdash V > 0 \land V' \leq 0}{\vdash \forall \varepsilon{>}0\, \exists \delta{>}0\, \forall x\, (\|x\|^2 < \delta^2 \rightarrow [x' = f(x)]\|x\|^2 < \varepsilon^2)}$$

Attractivity in dL

- **Attractivity** dissipate energy when slightly perturbed

Origin 0 of an ODE $x' = f(x)$ with solution $x(t) : [0, T) \to \mathbb{R}^n$ is attractive if

- there exists $\delta > 0$
- s.t. for all $\|x(0)\| < \delta$
- $\lim_{t \to T} x(t) = 0$

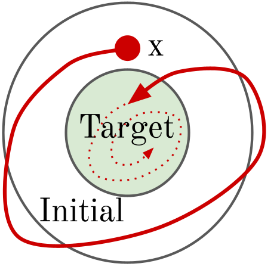


Attractivity in dL

- **Attractivity** dissipate energy when slightly perturbed

Origin 0 of an ODE $x' = f(x)$ with solution $x(t) : [0, T) \to \mathbb{R}^n$ is attractive if

- there exists $\delta > 0$
- s.t. for all $\|x(0)\| < \delta$
- $\lim_{t \to T} x(t) = 0$



Attractivity

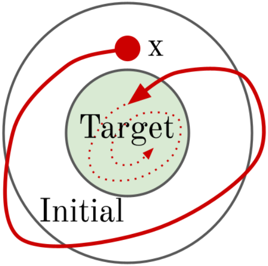
$$\exists \delta > 0 \, \forall x \, (\|x\| < \delta \to \forall \varepsilon > 0 \langle x' = f(x) \rangle [x' = f(x)] \|x\| < \varepsilon)$$

Attractivity in dL

- **Attractivity** dissipate energy when slightly perturbed

Origin 0 of an ODE $x' = f(x)$ with solution $x(t) : [0, T) \to \mathbb{R}^n$ is attractive if

- there exists $\delta > 0$
- s.t. for all $\|x(0)\| < \delta$
- $\lim_{t \to T} x(t) = 0$



Attractivity

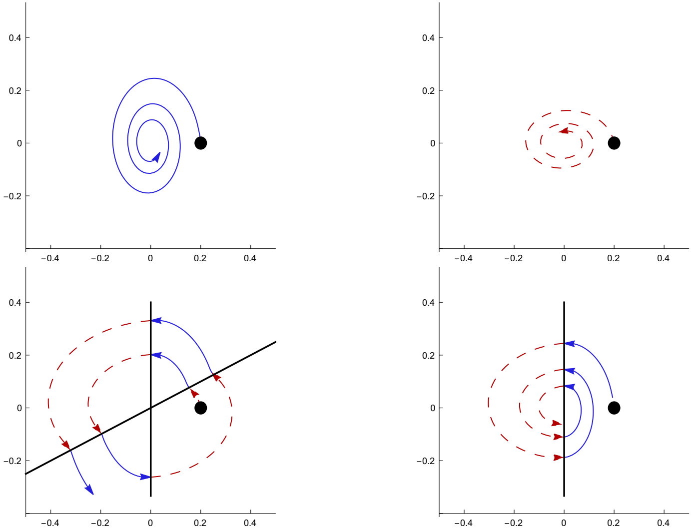
$$\exists \delta > 0 \, \forall x \, (\|x\| < \delta \to \forall \varepsilon > 0 \langle x' = f(x) \rangle [x' = f(x)] \|x\| < \varepsilon)$$

Pre-attractivity

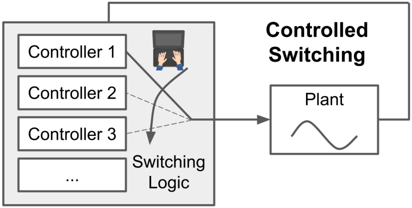
$$\forall \varepsilon > 0 \, \forall \delta > 0 \, \exists T \geq 0 \, \forall x \, (\|x\| < \delta \to [t := 0; \{x' = f(x), t' = 1\}](t \geq T \to \|x\| < \varepsilon))$$

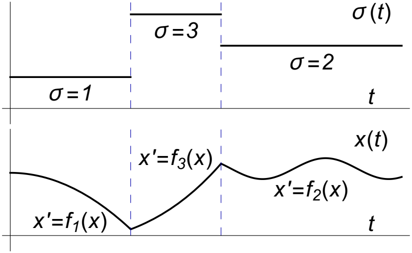
Outline

Switching between stable ODEs can be unstable

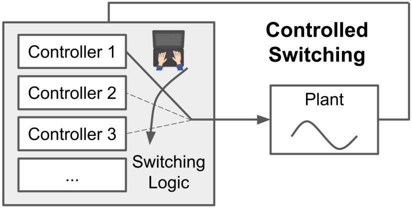


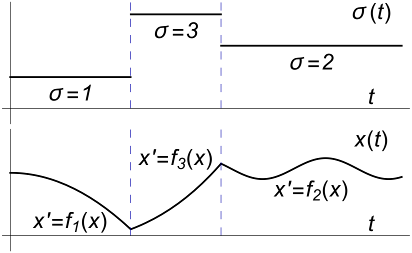
- Family $\mathscr{P}$ of ODEs $x' = f_p(x), p \in \mathscr{P}$
- Switching signal $\sigma(t)$ chooses ODE





- Family $\mathscr{P}$ of ODEs $x' = f_p(x), p \in \mathscr{P}$
- Switching signal $\sigma(t)$ chooses ODE

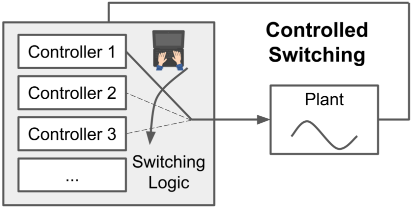


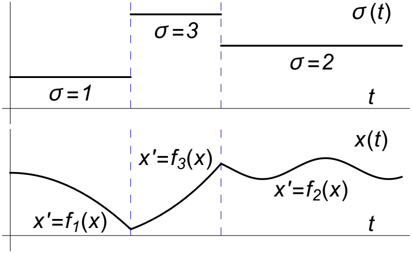


Arbitrary Switching as Hybrid Program

Non-deterministic choice between all ODEs: $\left(\bigcup_{p\in\mathscr{P}} x' = f_p(x)\right)^*$

- Family $\mathscr{P}$ of ODEs $x' = f_p(x), p \in \mathscr{P}$
- Switching signal $\sigma(t)$ chooses ODE





Arbitrary Switching as Hybrid Program

Non-deterministic choice between all ODEs: $\left(\bigcup_{p\in\mathscr{P}} x' = f_p(x)\right)^*$

Controlled Switching as Hybrid Program

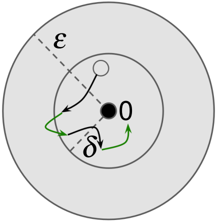
Controlled choice between ODEs: $(p := \mathrm{ctrl}(x); x' = f_p(x))^*$

Construct loop invariants that imply stability

Arbitrary Switching: Common Lyapunov Function

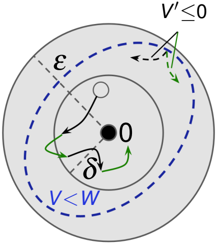
$$\alpha_{\text{arb}} \equiv \left(\bigcup_{p\in\mathscr{P}} x' = f_p(x)\right)^*$$

$$\forall\varepsilon{>}0\,\exists\delta{>}0\,\forall x\,(\|x\|{<}\delta \to [\alpha_{\text{arb}}]\|x\|{<}\varepsilon)$$



Construct loop invariants that imply stability

Arbitrary Switching: Common Lyapunov Function



$$\alpha_{\text{arb}} \equiv \left(\bigcup_{p\in\mathscr{P}} x' = f_p(x)\right)^*$$

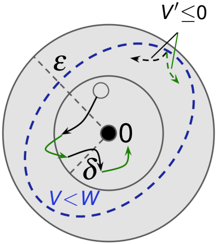
$$\forall \varepsilon{>}0\, \exists \delta{>}0\, \forall x\, (\|x\|{<}\delta \rightarrow [\alpha_{\text{arb}}]\|x\|{<}\varepsilon)$$

Construct loop invariants that imply stability

Arbitrary Switching: Common Lyapunov Function

$$\alpha_{\text{arb}} \equiv \left(\bigcup_{p\in\mathscr{P}} x' = f_p(x)\right)^*$$

$$\forall \varepsilon > 0 \, \exists \delta > 0 \, \forall x \, (\|x\| < \delta \rightarrow [\alpha_{\text{arb}}] \|x\| < \varepsilon)$$



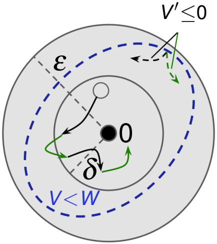
$Inv \equiv \|x\| < \varepsilon \land V < W$

Construct loop invariants that imply stability

Arbitrary Switching: Common Lyapunov Function

$$\alpha_{\text{arb}} \equiv \left(\bigcup_{p\in\mathscr{P}} x' = f_p(x)\right)^*$$

$$\forall\varepsilon{>}0\,\exists\delta{>}0\,\forall x\,(\|x\|{<}\delta \to [\alpha_{\text{arb}}]\|x\|{<}\varepsilon)$$



$$Inv \equiv \|x\| < \varepsilon \land \bigvee_{p\in\mathscr{P}} (u{=}p \land V_p{<}W)$$

Controlled Switching: Multiple Lyapunov Functions

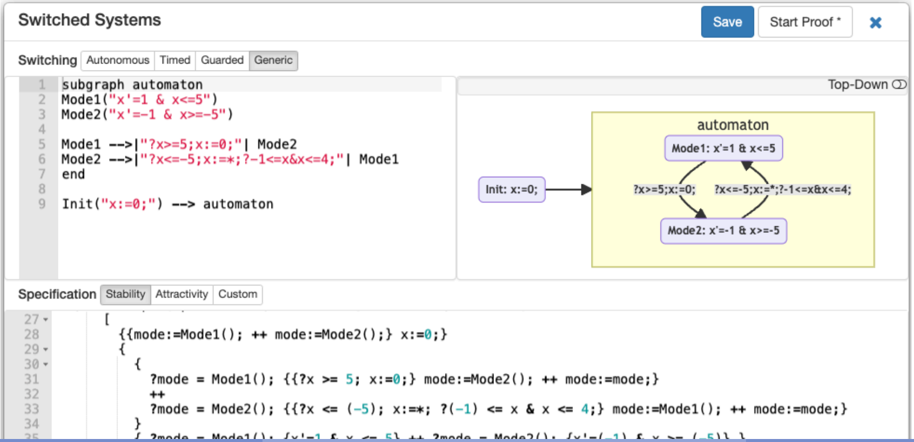
$$\alpha_{\text{ctrl}} \equiv (u := \text{ctrl}(x); x' = f_u(x))^*$$

$$\forall\varepsilon{>}0\,\exists\delta{>}0\,\forall x\,(\|x\|{<}\delta \to [\alpha_{\text{ctrl}}]\|x\|{<}\varepsilon)$$

Outline

Stability is a key correctness criterion for real-world safety

- **Stability** stay close to origin when slightly perturbed
- **Attractivity** dissipate energy when slightly perturbed
- **Lyapunov functions** certify stability
- **Switching** needs care to not cause instability



Yong Kiam Tan and André Platzer.
Deductive stability proofs for ordinary differential equations.
In *Tools and Algorithms for the Construction and Analysis of Systems - 27th International Conference, TACAS 2021, Luxembourg City, Luxembourg, March 27 - April 1, 2021, Proceedings, Part II*, pages 181–199, 2021.
doi:10.1007/978-3-030-72013-1_10.

Yong Kiam Tan and André Platzer.
Switched systems as hybrid programs.
In *7th IFAC Conference on Analysis and Design of Hybrid Systems, ADHS 2021, Brussels, Belgium, July 7-9, 2021*, pages 247–252, 2021.
doi:10.1016/j.ifacol.2021.08.506.

Yong Kiam Tan, Stefan Mitsch, and André Platzer.
Verifying switched system stability with logic.
In *HSCC '22: 25th ACM International Conference on Hybrid Systems: Computation and Control, Milan, Italy, May 4 - 6, 2022*, pages 2:1–2:11, 2022.
doi:10.1145/3501710.3519541.