Deductive Stability Proofs for Ordinary Differential Equations

Yong Kiam Tan André Platzer

Computer Science Department, Carnegie Mellon University

TACAS, Online, 1 Apr 2021

Outline

Outline

Motivation : Cyber-Physical Systems (CPSs)

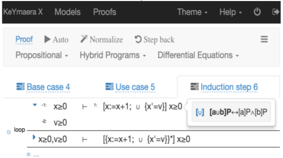


Challenge: How can we formally ensure correctness for cyber-physical systems that feature interacting discrete and continuous dynamics?

Motivation : Cyber-Physical Systems (CPSs)



Model as hybrid system & specify correctness



Hybrid system model:

$$\texttt{if}(v > \mathit{limit}) \quad x' = v, v' = \mathit{brake}$$

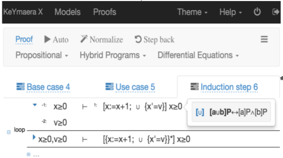
$$\texttt{else} \quad x' = v, v' = \mathit{accel}$$

Discrete + Continuous

Challenge: How can we formally ensure correctness for cyber-physical systems that feature interacting discrete and continuous dynamics?

Motivation : Cyber-Physical Systems (CPSs)

Model as hybrid system & specify correctness



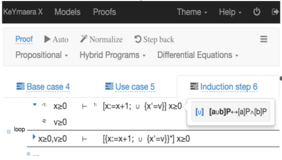
✓Deductive hyb. sys. safety proofs

✓Deductive hyb. sys. liveness proofs

Challenge: How can we formally ensure correctness for cyber-physical systems that feature interacting discrete and continuous dynamics?

Motivation : Cyber-Physical Systems (CPSs)

Model as hybrid system & specify correctness



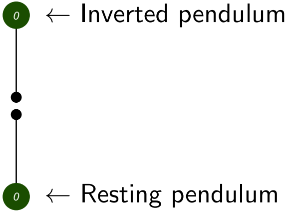
✓Deductive hyb. sys. safety proofs

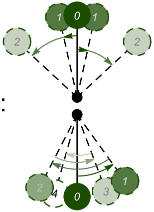
✓Deductive hyb. sys. liveness proofs

✓**Deductive ODE stability proofs**

This work: Deductive proofs of stability for continuous dynamics described by ordinary differential equations (ODEs).

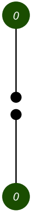
Why Stability?

Theoretically: 

In Practice: 

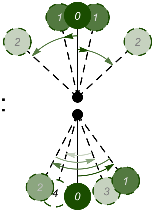
Stability shows robustness with respect to real world perturbations around a system's desired operating states.

Why Stability?

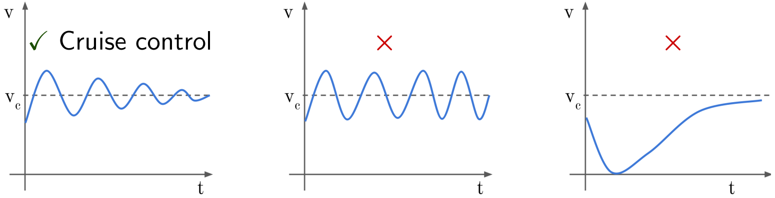
Theoretically: 

← Inverted pendulum

← Resting pendulum

In Practice: 

Stability shows robustness with respect to real world perturbations around a system's desired operating states.



Stability is often **the** correctness criterion for control system designs.

Which Stability?

- **Lyapunov stability**: classical stability for equilibria, Lyapunov (1892).

Which Stability?

- **Lyapunov stability**: classical stability for equilibria, Lyapunov (1892).
- **Asymptotic stability**: Lyapunov stability & asymptotic convergence to an equilibrium point from nearby states, Lyapunov (1892).

Which Stability?

- **Lyapunov stability**: classical stability for equilibria, Lyapunov (1892).
- **Asymptotic stability**: Lyapunov stability & asymptotic convergence to an equilibrium point from nearby states, Lyapunov (1892).
- **Exponential stability**: exponential convergence to an equilibrium point from nearby states, various authors.

Which Stability?

- **Lyapunov stability**: classical stability for equilibria, Lyapunov (1892).
- **Asymptotic stability**: Lyapunov stability & asymptotic convergence to an equilibrium point from nearby states, Lyapunov (1892).
- **Exponential stability**: exponential convergence to an equilibrium point from nearby states, various authors.
- **Global stability**: convergence to an equilibrium from all states of the system, Barbashin and Krasovskii (1952).
- **Set stability**: stability with respect to a subset of the state space, Zubov (1957), Yoshizawa (1966), Bhatia and Szegö (1967).
- **Input-to-state stability**: stability with respect to disturbances of continuous dynamics, Sontag (1989).
- **Region stability**: stability-like notion for hybrid systems, Podelski and Wagner (2007).
- ε**-stability**: relaxed notion of Lyapunov stability, suitable for applying numerically-driven decision procedures, Gao et al. (2019).

Contributions

- **Lyapunov stability**: classical stability for equilibria, Lyapunov (1892).
- **Asymptotic stability**: Lyapunov stability & asymptotic convergence to an equilibrium point from nearby states, Lyapunov (1892).
- **Exponential stability**: exponential convergence to an equilibrium

This work: Formal specification of various stability properties in differential dynamic logic (dL), enabling:

- Rigorous proofs of ODE stability from sound dL foundations.
- Formalization of logical relationships between stability notions.
- Practical deployment of stability proofs in KeYmaera X, a hybrid systems prover based on dL.

- **Region stability**: stability-like notion for hybrid systems, Podelski and Wagner (2007).
- **ε-stability**: relaxed notion of Lyapunov stability, suitable for applying numerically-driven decision procedures, Gao et al. (2019).

Outline

Background: Differential Dynamic Logic

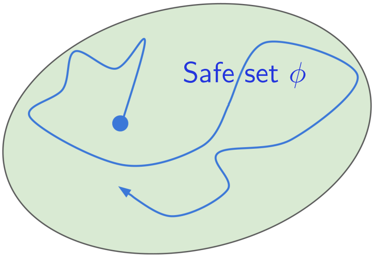
Specifications: $\phi, \psi ::= e \sim \tilde{e} \mid \phi \wedge \psi \mid \phi \vee \psi \mid \neg\phi \mid \cdots \mid \forall x\, \phi \mid \exists x\, \phi$

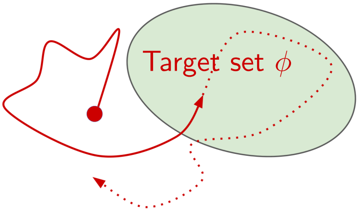
$\mid \underbrace{[\alpha]\phi \mid \langle\alpha\rangle\phi}$

α is a hybrid system modeled using dL's language of hybrid programs

Semantics: $[x' = f(x)]\phi$ iff $x' = f(x)$ solution always stays in ϕ.

$\langle x' = f(x)\rangle\phi$ iff $x' = f(x)$ solution eventually reaches ϕ.





Background: Differential Dynamic Logic

Specifications: $\phi, \psi ::= e \sim \tilde{e} \mid \phi \land \psi \mid \phi \lor \psi \mid \neg\phi \mid \cdots \mid \forall x\, \phi \mid \exists x\, \phi$

$$\mid \underbrace{[\alpha]\phi \mid \langle\alpha\rangle\phi}$$

α is a hybrid system modeled using dL's language of hybrid programs

Semantics: $[x' = f(x)]\phi$ iff $x' = f(x)$ solution always stays in ϕ.

$\langle x' = f(x)\rangle\phi$ iff $x' = f(x)$ solution eventually reaches ϕ.

Axiomatics:

[JACM'20] provides sound and complete dL ODE invariance reasoning for proving ODE safety properties $[x' = f(x)]\phi$.

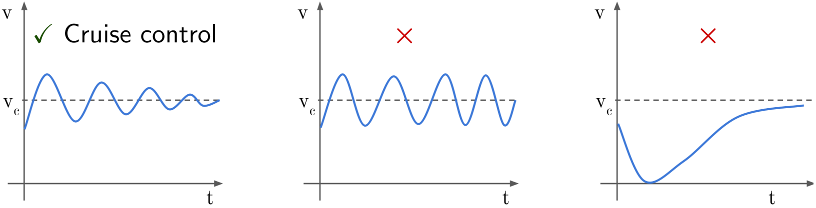
[FAC'21] provides a general, dL refinement-based approach for proving ODE liveness properties $\langle x' = f(x)\rangle\phi$.

Asymptotic Stability for ODEs

Stability: Stable systems stay close to their desired operating state(s) when slightly perturbed from those state(s).

Attractivity: Attractive systems dissipate small initial perturbations from their desired operating state(s).

Example: Cruise controllers stabilize car's velocity v at targeted value v_c.



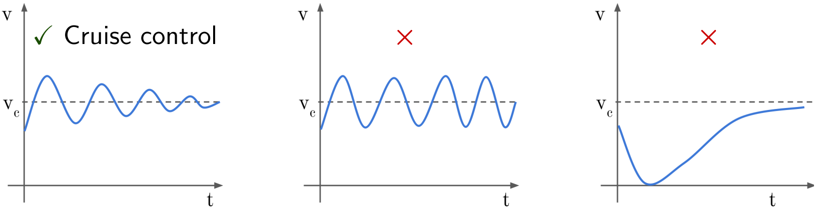
✓ Stable + Attractive → **Asymptotic Stability**

✓ Stable
× Not attractive

✓ Attractive
× Not stable

Asymptotic Stability for ODEs

Stability: Stable systems stay close to their desired operating state(s) when slightly perturbed from those state(s).
Attractivity: Attractive systems dissipate small initial perturbations from their desired operating state(s).
Example: Cruise controllers stabilize car's velocity v at targeted value v_c.



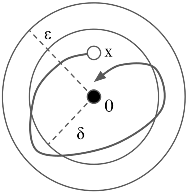
Key Idea: Specify ODE stability in dL, then derive stability proof rules by combining dL's ODE safety and liveness reasoning.

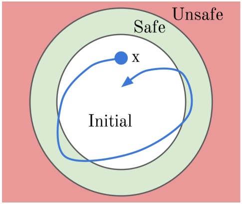
Formal Specification & Deduction (Stability)

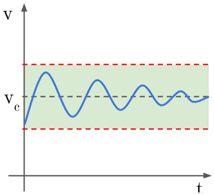
Definition (Stability)

The origin $0 \in \mathbb{R}^n$ of the n-dimensional ODE $x' = f(x)$ is:
stable if for all $\varepsilon{>}0$, there exists $\delta{>}0$ s.t. for all $x{=}x(0)$ with $\|x\|{<}\delta$, the ODE solution $x(t) : [0, T) \to \mathbb{R}^n$ always satisfies $\|x(t)\|{<}\varepsilon$.

$$\text{Stab}(x' = f(x)) \equiv \forall \varepsilon{>}0\, \exists \delta{>}0\, \forall x \left(\|x\|^2 < \delta^2 \to [x' = f(x)]\, \|x\|^2 < \varepsilon^2\right)$$





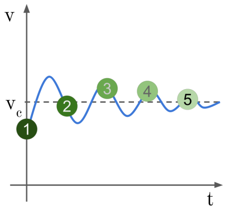


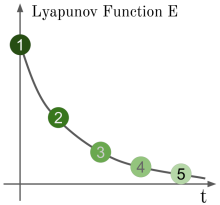
Formal Specification & Deduction (Stability)

Lemma (Lyapunov Function Proof Rule)

The following Lyapunov function proof rule is derivable in dL.

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





Lyapunov functions are an energy-like auxiliary measure used to certify (asymptotic) stability for a given system.

Formal Specification & Deduction (Stability)

Lemma (Lyapunov Function Proof Rule)

The following Lyapunov function proof rule is derivable in dL.

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

$$\vdash f(0) = 0 \land E(0) = 0$$

$$\text{Lyap}_{\geq}\ \frac{\dfrac{0 < \|x\|^2 \vdash E > 0 \land E' \leq 0}{\vdots}}{\vdash \text{Stab}(x' = f(x))}$$

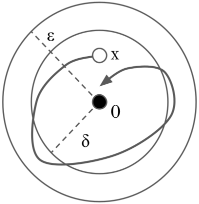
Deductive reasoning over $\forall, \exists$
& ODE safety reasoning [JACM'20]

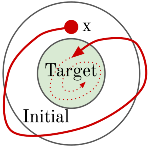
Formal Specification & Deduction (Attractivity)

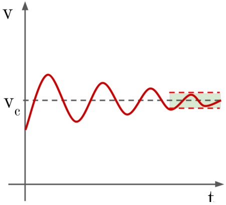
Definition (Attractivity)

The origin $0 \in \mathbb{R}^n$ of the n-dimensional ODE $x' = f(x)$ is:
attractive if there exists $\delta > 0$ s.t. for all $x = x(0)$ with $\|x\| < \delta$, the ODE solution $x(t) : [0, T) \to \mathbb{R}^n$ satisfies $\lim_{t \to T} x(t) = 0$.

$$\mathrm{Attr}(x' = f(x)) \equiv \exists \delta{>}0\, \forall x \left(\|x\|^2 < \delta^2 \to \underbrace{\mathrm{Asym}(x' = f(x), x = 0)}_{\forall \varepsilon > 0\, \langle x' = f(x) \rangle [x' = f(x)]\, \|x\|^2 < \varepsilon^2}\right)$$





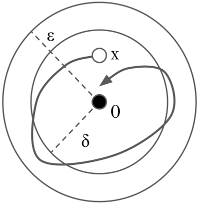


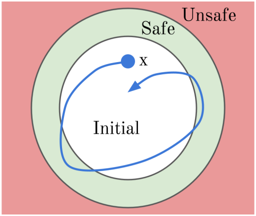
Formal Specification & Deduction (Asymptotic Stability)

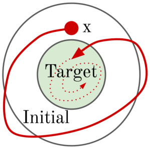
Definition (Asymptotic stability)

The origin $0 \in \mathbb{R}^n$ of the n-dimensional ODE $x' = f(x)$ is:
asymptotically stable if it is stable and attractive.

$$\mathrm{AStab}(x' = f(x)) \equiv \mathrm{Stab}(x' = f(x)) \wedge \mathrm{Attr}(x' = f(x))$$







Formal Specification & Deduction (Asymptotic Stability)

Definition (Asymptotic stability)

The origin $0 \in \mathbb{R}^n$ of the n-dimensional ODE $x' = f(x)$ is:
asymptotically stable if it is stable and attractive.

$$\text{AStab}(x' = f(x)) \equiv \text{Stab}(x' = f(x)) \land \text{Attr}(x' = f(x))$$

$$\text{Lyap}_{>}\ \dfrac{\vdash f(0) = 0 \land E(0) = 0 \qquad 0 < \|x\|^2 \vdash E > 0 \land E' < 0}{\vdash \text{AStab}(x' = f(x))}$$

Deductive reasoning over $\forall, \exists$
& ODE safety reasoning [JACM'20]
& ODE liveness reasoning [FAC'21]

Key Idea: Specify ODE stability in dL, then derive stability proof rules by combining dL's ODE safety and liveness reasoning.

Outline

Which Stability?

- ✓ **Lyapunov stability**: classical stability for equilibria, Lyapunov (1892).
- ✓ **Asymptotic stability**: Lyapunov stability & asymptotic convergence to an equilibrium point from nearby states, Lyapunov (1892).
- ✓ **Exponential stability**: exponential convergence to an equilibrium point from nearby states, various authors.
- ✓ **Global stability**: convergence to an equilibrium from all states of the system, Barbashin and Krasovskii (1952).
- ✓ **Set stability**: stability with respect to a subset of the state space, Zubov (1957), Yoshizawa (1966), Bhatia and Szegö (1967).
- **Input-to-state stability**: stability with respect to disturbances of continuous dynamics, Sontag (1989).
- **Region stability**: stability-like notion for hybrid systems, Podelski and Wagner (2007).
- ✓ ε-**stability**: relaxed notion of Lyapunov stability, suitable for applying numerically-driven decision procedures, Gao et al. (2019).

Which Stability?

- ✓ **Lyapunov stability**: classical stability for equilibria, Lyapunov (1892).
- ✓ **Asymptotic stability**: Lyapunov stability & asymptotic convergence to an equilibrium point from nearby states, Lyapunov (1892).
- ✓ **Exponential stability**: exponential convergence to an equilibrium

In paper: Proofs of logical relationships between stability notions in dL and various verified stability examples in KeYmaera X:

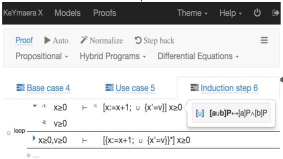
- Asymptotic stability of a PD inverted pendulum controller.
- Set stability for the axes of a 3D rigid body.
- ϵ-stability and other stability examples from verification literature (nonlinear ODEs, up to 6 dimensions) [CAV'19, TACAS'20].

- **Region stability**: stability-like notion for hybrid systems, Podelski and Wagner (2007).
- ✓ ε**-stability**: relaxed notion of Lyapunov stability, suitable for applying numerically-driven decision procedures, Gao et al. (2019).

Outline

Conclusion and Future Work

Model as hybrid system & specify correctness



✓Deductive hyb. sys. safety proofs

✓Deductive hyb. sys. liveness proofs

✓**Deductive ODE stability proofs**

Future work: stability with respect to continuous ODE disturbances, hybrid systems stability, and KeYmaera X automation for stability proofs.

References

[1] Ahmed, D., Peruffo, A., and Abate, A. (2020). Automated and sound synthesis of Lyapunov functions with SMT solvers. In Biere, A. and Parker, D., editors, TACAS, volume 12078 of LNCS, pages 97–114. Springer.

[2] Gao, S., Kapinski, J., Deshmukh, J. V., Roohi, N., Solar-Lezama, A., Aréchiga, N., and Kong, S. (2019). Numerically-robust inductive proof rules for continuous dynamical systems. In Dillig, I. and Tasiran, S., editors, CAV, volume 11562 of LNCS, pages 137–154. Springer.

[3] Platzer, A. and Tan, Y. K. (2020). Differential equation invariance axiomatization. J. ACM, 67(1):6:1–6:66.

[4] Tan, Y. K. and Platzer, A. (to appear). An axiomatic approach to existence and liveness for differential equations. Formal Aspects Comput.