# An Axiomatic Approach to Liveness for Differential Equations

**Yong Kiam Tan** André Platzer

Computer Science Department, Carnegie Mellon University

FM, 10th Oct 2019

# Outline

# Outline

# Motivation : Cyber-Physical Systems (CPSs)

Hybrid system models enable formal analysis of safety-critical CPSs:

**Discrete control:**

```
if (v > speed_limit)
  a := -1; //apply brakes
else
  a := 0;  //cruise
```

# Motivation : Cyber-Physical Systems (CPSs)

Hybrid system models enable formal analysis of safety-critical CPSs:

**Discrete control:**

```
if (v > speed_limit)
  a := -1; //apply brakes
else
  a := 0;  //cruise
```

**Continuous dynamics:**

$$\underbrace{x' = v, v' = a}_{\textbf{Ordinary Differential Equations (ODEs)}}$$

# Motivation : Cyber-Physical Systems (CPSs)

Hybrid system models enable formal analysis of safety-critical CPSs:

**Discrete control:**

```
if (v > speed_limit)
  a := -1; //apply brakes
else
  a := 0;  //cruise
```

**Continuous dynamics:**

$$\underbrace{x' = v, v' = a}_{\textbf{ODEs need proofs too!}}$$

# Correctness Specifications for CPSs


✓Safely under speed limit

# Correctness Specifications for CPSs


✓Safely under speed limit


✓Safely under speed limit

# Correctness Specifications for CPSs


✓Safely under speed limit
✓Gets to destination

System is safe and **live**

✓Safely under speed limit
✗Not moving at all!

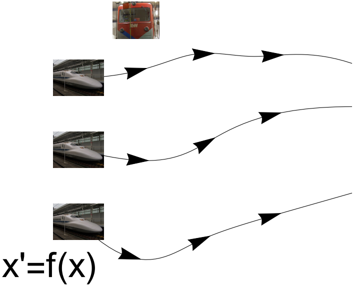
System is safe but not **live**

# ODEs and Domain Constraints

Ordinary Differential Equation (ODE)

$$\overbrace{x' = f(x)}$$

**ODE**: Models continuous physics of the system

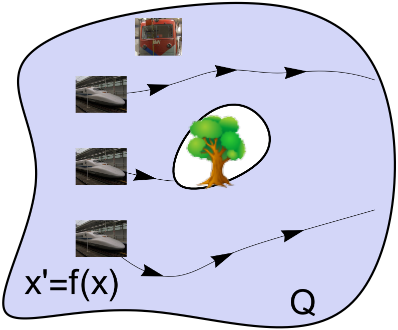



Trains drive on tracks prescribed by the ODEs.

# ODEs and Domain Constraints

$$\overbrace{x' = f(x) \,\&\, Q}^{\text{ODE with domain } Q}$$

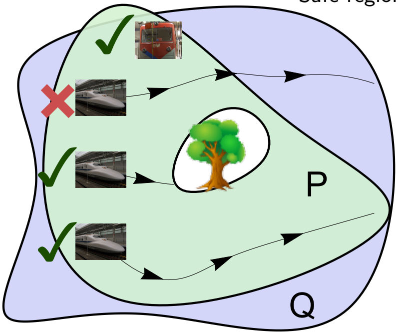
**Domain**: Specifies the domain of definition for ODEs




There are no train tracks across the national park!

# Safety & Liveness for ODEs

$$\textbf{Safety:}\ [\overbrace{x' = f(x)\,\&\,Q}^{\text{ODE with domain } Q}]\underbrace{P}_{\text{Safe region}}$$

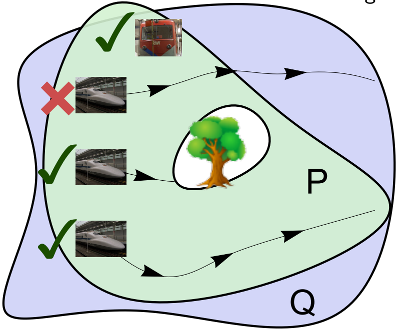


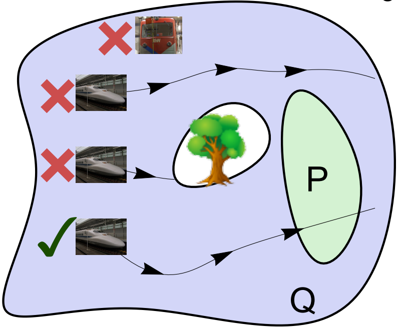

✓Trains stay in Porto ($P$) while driving on tracks.

# Safety & Liveness for ODEs

**Safety:** $\overbrace{[x' = f(x) \,\&\, Q]}^{\text{ODE with domain } Q}\ \underbrace{P}_{\text{Safe region}}$

**Liveness:** $\overbrace{\langle x' = f(x) \,\&\, Q \rangle}^{\text{ODE with domain } Q}\ \underbrace{P}_{\text{Goal region}}$



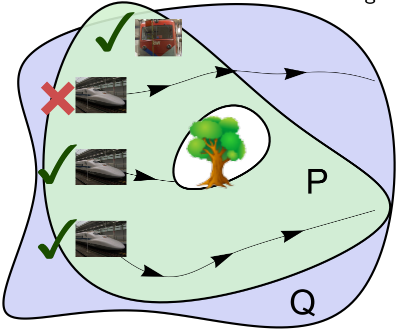




✓Trains stay in Porto ($P$) while driving on tracks.

✓Trains reach Porto ($P$) by driving on tracks.

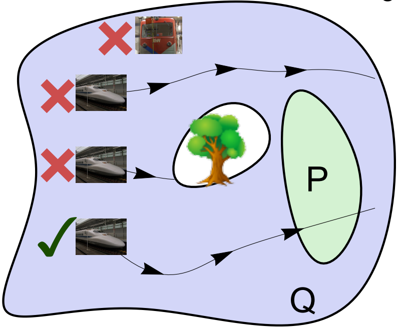
# Safety & Liveness for ODEs

**Safety:** $[\overbrace{x' = f(x) \,\&\, Q}^{\text{ODE with domain } Q}]\underbrace{P}_{\text{Safe region}}$



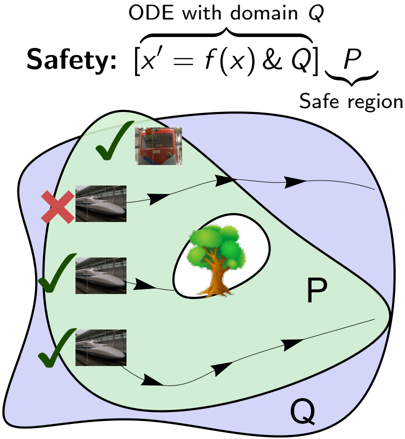

**Prior work:** complete invariance proofs for ODE safety [LICS'18]

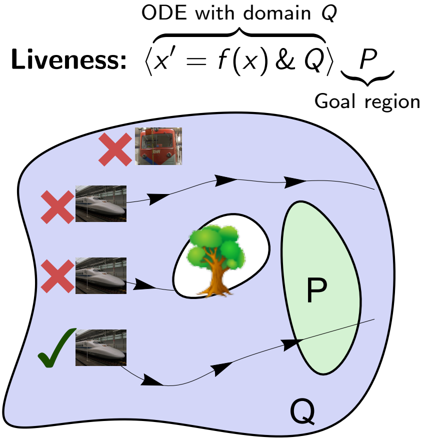
**Liveness:** $\langle\overbrace{x' = f(x) \,\&\, Q}^{\text{ODE with domain } Q}\rangle\underbrace{P}_{\text{Goal region}}$




✓Trains reach Porto ($P$) by driving on tracks.

# Safety & Liveness for ODEs




**Prior work:** complete invariance proofs for ODE safety [LICS'18]

**This talk:** proving ODE liveness in differential dynamic logic (dL)

# An Axiomatic Approach to Liveness for ODEs

Why take a **logical** approach?

| Surveyed Liveness Arguments | Goals of surveyed paper |
|---|---|
| Differential Variants [1] | Liveness proofs for inequalities |
| Bounded/Compact Eventuality [3, 4] | Automatic SOS liveness proofs |
| Set Lyapunov Functions [5] | Finding basin of attraction |
| Staging Sets + Progress [6] | Indirect liveness proofs for $P$ |
| Eq. Differential Variants [7] | Synthesizing switching logic |

Liveness arguments in the literature are used for a wide variety of purposes.

# An Axiomatic Approach to Liveness for ODEs

Why take a **logical** approach?

| Surveyed Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Differential Variants [1] | | × |
| Bounded/Compact Eventuality [3, 4] | × | × |
| Set Lyapunov Functions [5] | × | × |
| Staging Sets + Progress [6] | | |
| Eq. Differential Variants [7] | × | × |

Several arguments have technical glitches, making them unsound (×).

# An Axiomatic Approach to Liveness for ODEs

Why take a **logical** approach?

| Surveyed Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Differential Variants [1] | ✓ | ✗ ⇝ ✓ |
| Bounded/Compact Eventuality [3, 4] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |
| Set Lyapunov Functions [5] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |
| Staging Sets + Progress [6] | ✓ | ✓ |
| Eq. Differential Variants [7] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |

Our approach formalizes the underlying liveness arguments in a sound (✓), foundational, and uniform framework. It also corrects (✗ ⇝ ✓) the technical glitches.

# An Axiomatic Approach to Liveness for ODEs

Why take a **logical** approach?

- Understand the core principles behind ODE liveness proofs.

| Surveyed Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Differential Variants [1] | ✓ | ✗ $\rightsquigarrow$ ✓ |
| Bounded/Compact Eventuality [3, 4] | ✗ $\rightsquigarrow$ ✓ | ✗ $\rightsquigarrow$ ✓ |
| Set Lyapunov Functions [5] | ✗ $\rightsquigarrow$ ✓ | ✗ $\rightsquigarrow$ ✓ |
| Staging Sets + Progress [6] | ✓ | ✓ |
| Eq. Differential Variants [7] | ✗ $\rightsquigarrow$ ✓ | ✗ $\rightsquigarrow$ ✓ |

# An Axiomatic Approach to Liveness for ODEs

Why take a **logical** approach?

- Understand the core principles behind ODE liveness proofs.

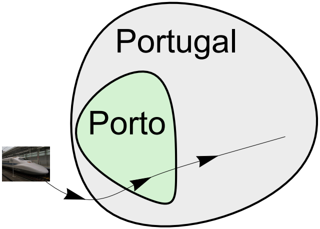
| Surveyed Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Differential Variants [1] | ✓ | ✗ ⇝ ✓ |
| Bounded/Compact Eventuality [3, 4] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |
| Set Lyapunov Functions [5] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |
| Staging Sets + Progress [6] | ✓ | ✓ |
| Eq. Differential Variants [7] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |

- Yields generalizations of existing liveness arguments "for free".

| New Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Higher Differential Variants | ✓ | - |
| [1] + [3, 4] + [6] | ✓ | - |
| [1] + [3, 4] + [6] + Higher Diff. Var. | - | ✓ |

# Outline

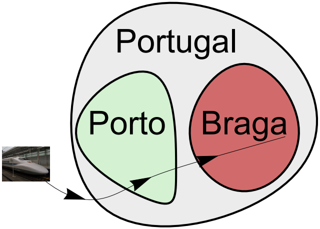
# A Simple Liveness Refinement




Trains that reach Porto also reach Portugal since Porto is part of Portugal.

✓ $\langle x' = f(x)\rangle \texttt{Porto} \rightarrow \langle x' = f(x)\rangle \texttt{Portugal}$

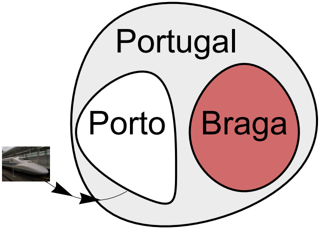
# A Simple Liveness Refinement




Can train reach Porto if it reaches Braga? Not true for **all** trains.

$$? \quad \langle x' = f(x) \rangle \texttt{Braga} \rightarrow \langle x' = f(x) \rangle \texttt{Porto}$$

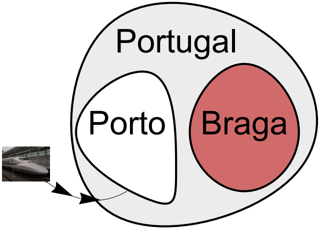
# A Simple Liveness Refinement




Must use specific properties of the ODE / train track.

$$[x' = f(x) \,\&\, \neg\texttt{Porto}]\neg\texttt{Braga} \rightarrow \big(\langle x' = f(x)\rangle\texttt{Braga} \rightarrow \langle x' = f(x)\rangle\texttt{Porto}\big)$$

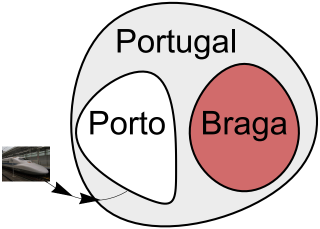
# A Simple Liveness Refinement




Must use specific properties of the ODE / train track.

$$[x' = f(x) \,\&\, \neg\texttt{Porto}]\neg\texttt{Braga} \rightarrow \big(\underbrace{\langle x' = f(x)\rangle \texttt{Braga}}_{\text{Known liveness property}} \rightarrow \underbrace{\langle x' = f(x)\rangle \texttt{Porto}}_{\text{Desired liveness property}}\big)$$

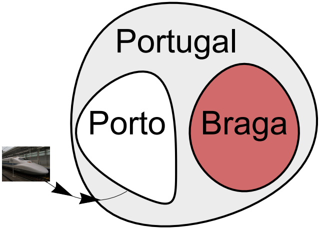
# A Simple Liveness Refinement




Must use specific properties of the ODE / train track.

$$\underbrace{[x' = f(x) \,\&\, \neg\mathtt{Porto}]\neg\mathtt{Braga}}_{\text{Need to show}} \rightarrow \big(\underbrace{\langle x' = f(x)\rangle\mathtt{Braga}}_{\text{Known liveness property}} \rightarrow \underbrace{\langle x' = f(x)\rangle\mathtt{Porto}}_{\text{Desired liveness property}}\big)$$

# A Simple Liveness Refinement




**Key Idea:** Liveness arguments can and should be understood using liveness refinement steps.

$$\underbrace{[x' = f(x) \,\&\, \neg\mathtt{Porto}]\neg\mathtt{Braga}}_{\text{Need to show}} \rightarrow \underbrace{(\langle x' = f(x)\rangle\mathtt{Braga}}_{\text{Known liveness property}} \rightarrow \underbrace{\langle x' = f(x)\rangle\mathtt{Porto})}_{\text{Desired liveness property}}$$

# Diamond Refinement Axioms

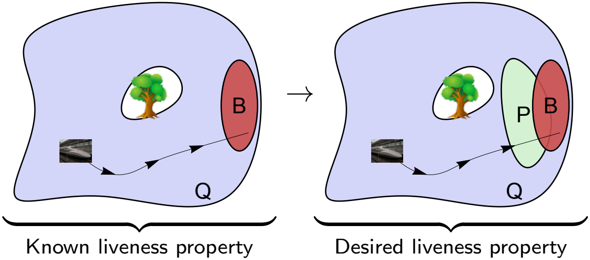
$$\underbrace{[x' = f(x) \,\&\, \neg\texttt{Porto}]\neg\texttt{Braga}}_{\text{Need to show}} \rightarrow \big(\underbrace{\langle x' = f(x)\rangle\texttt{Braga}}_{\text{Known liveness property}} \rightarrow \underbrace{\langle x' = f(x)\rangle\texttt{Porto}}_{\text{Desired liveness property}}\big)$$

# Diamond Refinement Axioms

$$[x' = f(x) \,\&\, \neg P]\neg B \rightarrow \big(\langle x' = f(x)\rangle B \rightarrow \langle x' = f(x)\rangle P\big)$$

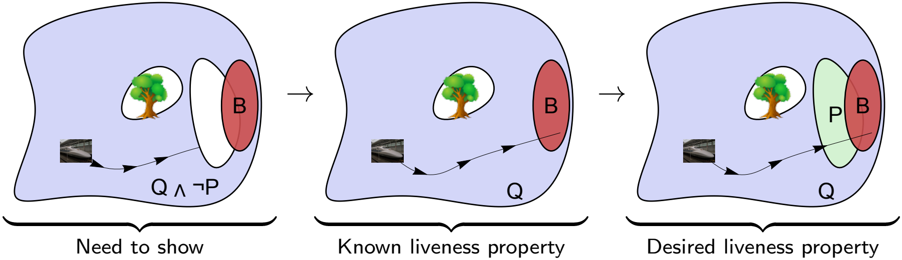
# Diamond Refinement Axioms

$$\mathrm{K}\langle\&\rangle\ [x' = f(x)\,\&\,Q \land \neg P]\neg B \rightarrow \big(\langle x' = f(x)\,\&\,Q\rangle B \rightarrow \langle x' = f(x)\,\&\,Q\rangle P\big)$$



# Diamond Refinement Axioms

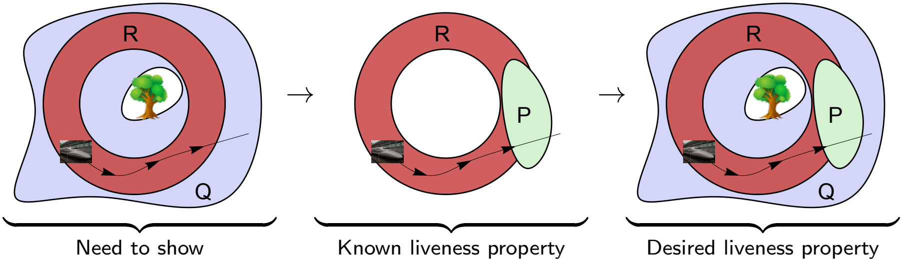
$$K\langle\&\rangle\ [x' = f(x)\,\&\, Q \land \neg P]\neg B \rightarrow (\langle x' = f(x)\,\&\, Q\rangle B \rightarrow \langle x' = f(x)\,\&\, Q\rangle P)$$



# Diamond Refinement Axioms

K⟨&⟩ $[x' = f(x) \,\&\, Q \land \neg P]\neg B \rightarrow \big(\langle x' = f(x) \,\&\, Q\rangle B \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

DR⟨·⟩ $[x' = f(x) \,\&\, R]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$



# Diamond Refinement Axioms

K$\langle\&\rangle$ $[x' = f(x) \,\&\, Q \land \neg P]\neg B \rightarrow \big(\langle x' = f(x) \,\&\, Q\rangle B \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

DR$\langle\cdot\rangle$ $[x' = f(x) \,\&\, R]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

**Idea 1:** ODE safety has effective reasoning principles [LICS'18], so use ODE safety to justify refinement steps.

# Diamond Refinement Axioms

K⟨&⟩ $[x' = f(x) \,\&\, Q \wedge \neg P]\neg B \rightarrow \big(\langle x' = f(x) \,\&\, Q\rangle B \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

DR⟨·⟩ $[x' = f(x) \,\&\, R]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

**Idea 1:** ODE safety has effective reasoning principles [LICS'18], so use ODE safety to justify refinement steps.

$$\langle x' = f(x) \,\&\, Q\rangle B \overbrace{\rightarrow}^{\substack{\mathrm{K}\langle\&\rangle \\ [x'=f(x)\,\&\,\neg P]\neg B}} \langle x' = f(x) \,\&\, Q\rangle P$$

# Diamond Refinement Axioms

K⟨&⟩ $[x' = f(x) \,\&\, Q \wedge \neg P]\neg B \rightarrow \big(\langle x' = f(x) \,\&\, Q\rangle B \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

DR⟨·⟩ $[x' = f(x) \,\&\, R]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

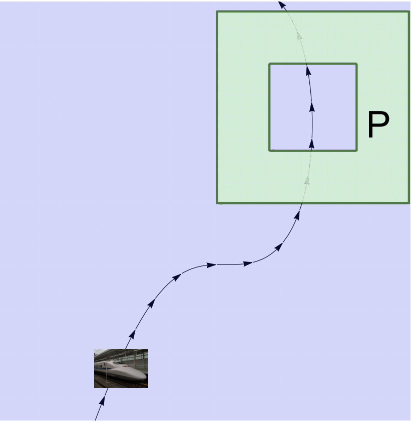
**Idea 1:** ODE safety has effective reasoning principles [LICS'18], so use ODE safety to justify refinement steps.

$$\langle x' = f(x) \,\&\, R\rangle B \overbrace{\rightarrow}^{\substack{\text{DR}\langle\cdot\rangle \\ [x'=f(x)\,\&\,R]Q}} \langle x' = f(x) \,\&\, Q\rangle B \overbrace{\rightarrow}^{\substack{\text{K}\langle\&\rangle \\ [x'=f(x)\,\&\,\neg P]\neg B}} \langle x' = f(x) \,\&\, Q\rangle P$$

**Idea 2:** Implication chains build complicated liveness arguments from simple building blocks.

# Outline

# ODE Liveness Example




**Example:** Train reaches Porto suburbs ($P$).
For simplicity, no domain constraint.

**Model ODE:**

$$x' = -y, y' = 4x^2$$

# Equational Differential Variants

| Surveyed Liveness Arguments | Goals of surveyed paper |
|---|---|
| Eq. Differential Variants [7] | Synthesizing switching logic |

Derived proof rule:

$$\mathrm{dV}^{M}_{=}\ \frac{p = 0 \vdash P \quad p < 0 \vdash p' \geq \varepsilon()}{\Gamma, \varepsilon() > 0, p \leq 0 \vdash \langle x' = f(x) \rangle P}$$

# Equational Differential Variants

| Surveyed Liveness Arguments | Goals of surveyed paper |
|---|---|
| Eq. Differential Variants [7] | Synthesizing switching logic |

Derived proof rule:

$$\mathrm{dV}^{M}_{=}\ \frac{p = 0 \vdash P \quad p < 0 \vdash p' \geq \varepsilon()}{\Gamma, \varepsilon() > 0, p \leq 0 \vdash \langle x' = f(x) \rangle P}$$

**Additional condition for soundness** ✓:
Either solution exists for sufficient duration or $x' = f(x)$ is globally Lipschitz continuous.

# Equational Differential Variants

| Surveyed Liveness Arguments | Goals of surveyed paper |
|---|---|
| Eq. Differential Variants [7] | Synthesizing switching logic |

Derived proof rule:

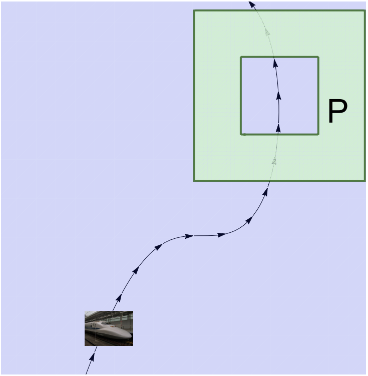
$$\mathrm{dV}^{M}_{=}\ \frac{\overbrace{p = 0 \vdash P}^{\text{Step 3}} \quad \overbrace{p < 0 \vdash p' \geq \varepsilon()}^{\text{Step 1}}}{\Gamma, \varepsilon() > 0, \underbrace{p \leq 0}_{\text{Step 2}} \vdash \langle x' = f(x) \rangle P}$$

Underlying refinement chain:

$$\langle x' = f(x), t' = 1 \rangle t > c() \overset{\substack{\text{Step 1}\\ \mathrm{K}\langle\&\rangle}}{\overbrace{\rightarrow}} \langle x' = f(x) \rangle p \geq 0 \overset{\substack{\text{Step 2}\\ \mathrm{K}\langle\&\rangle}}{\overbrace{\rightarrow}} \langle x' = f(x) \rangle p = 0 \overset{\substack{\text{Step 3}\\ \mathrm{K}\langle\&\rangle}}{\overbrace{\rightarrow}} \langle x' = f(x) \rangle P$$

# Proving Liveness for Train

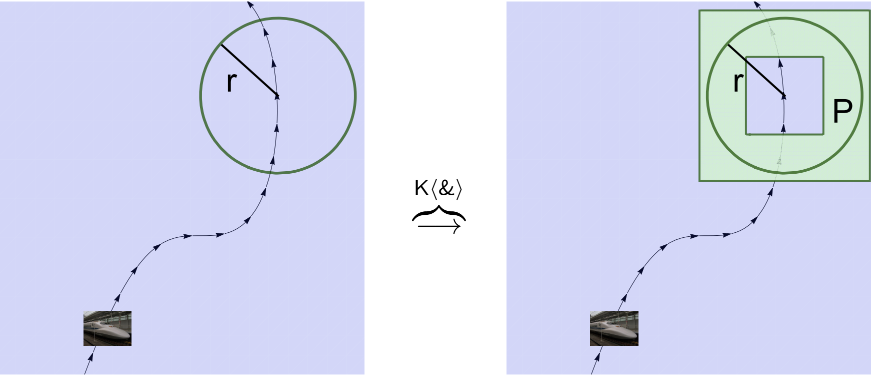
$$\langle x' = f(x), t' = 1\rangle t > 1.4 \overbrace{\rightarrow}^{\substack{\text{Step 1}\\ K\langle\&\rangle}} \langle x' = f(x)\rangle r \leq 1 \overbrace{\rightarrow}^{\substack{\text{Step 2}\\ K\langle\&\rangle}} \langle x' = f(x)\rangle r = 1 \overbrace{\rightarrow}^{\substack{\text{Step 3}\\ K\langle\&\rangle}} \langle x' = f(x)\rangle P$$




**Intuition:** Reduce liveness for (complicated) region $P$ to (simple) circle.

# Proving Liveness for Train

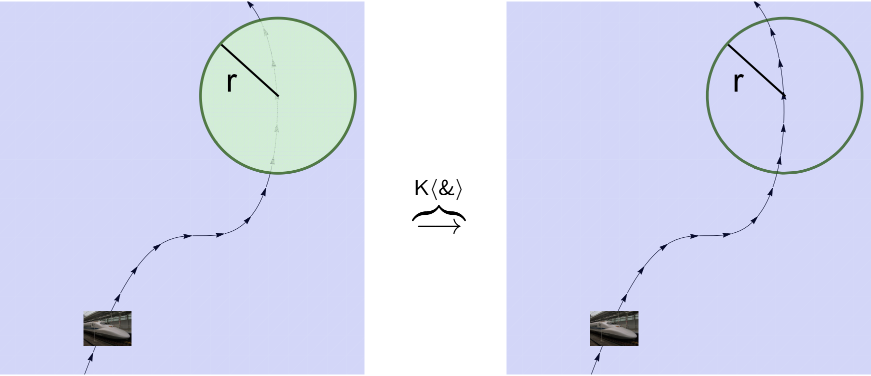
$$\langle x' = f(x), t' = 1\rangle t > 1.4 \overset{\text{Step 1}}{\overset{K\langle\&\rangle}{\overbrace{\rightarrow}}} \langle x' = f(x)\rangle r \leq 1 \overset{\text{Step 2}}{\overset{K\langle\&\rangle}{\overbrace{\rightarrow}}} \langle x' = f(x)\rangle r = 1 \overset{\text{Step 3}}{\overset{K\langle\&\rangle}{\overbrace{\rightarrow}}} \langle x' = f(x)\rangle P$$




**Intuition:** Reduce liveness for (complicated) region $P$ to (simple) circle.

# Proving Liveness for Train

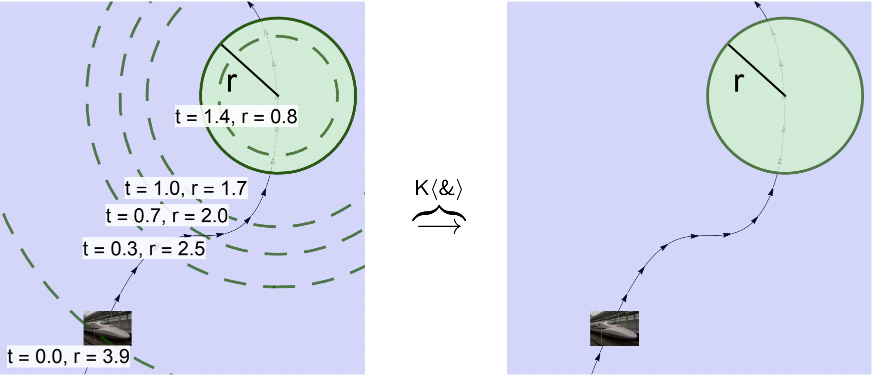
$$\langle x' = f(x), t' = 1\rangle t > 1.4 \overset{\text{Step 1}}{\overset{\text{K}\langle\&\rangle}{\overbrace{\to}}} \langle x' = f(x)\rangle r \le 1 \overset{\text{Step 2}}{\overset{\text{K}\langle\&\rangle}{\overbrace{\to}}} \langle x' = f(x)\rangle r = 1 \overset{\text{Step 3}}{\overset{\text{K}\langle\&\rangle}{\overbrace{\to}}} \langle x' = f(x)\rangle P$$




**Intuition:** Since train starts outside circle, reduce further to liveness for disk.

# Proving Liveness for Train

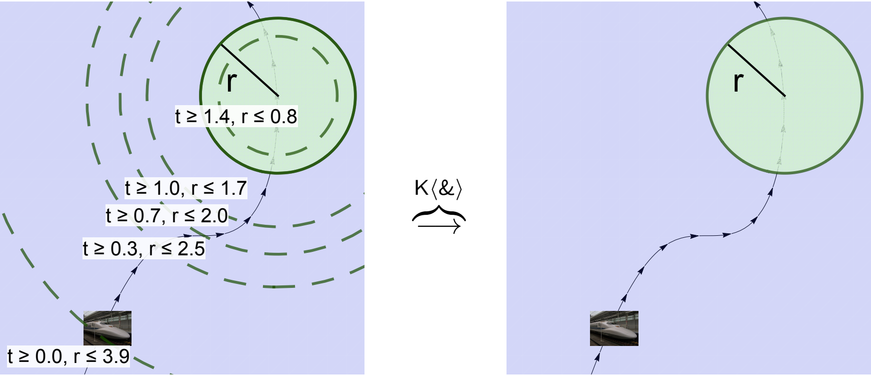
$$\langle x' = f(x), t' = 1\rangle t > 1.4 \overset{\text{Step 1}}{\overset{K\langle\&\rangle}{\overbrace{\rightarrow}}} \langle x' = f(x)\rangle r \leq 1 \overset{\text{Step 2}}{\overset{K\langle\&\rangle}{\overbrace{\rightarrow}}} \langle x' = f(x)\rangle r = 1 \overset{\text{Step 3}}{\overset{K\langle\&\rangle}{\overbrace{\rightarrow}}} \langle x' = f(x)\rangle P$$




**Intuition:** Symbolically analyze derivatives to lower bound time required to reach disk for the train.

# Proving Liveness for Train

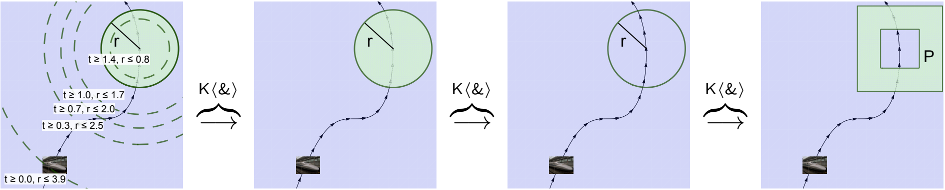
$$\langle x' = f(x), t' = 1 \rangle t > 1.4 \overset{\text{Step 1}\ \mathsf{K}\langle\&\rangle}{\overbrace{\rightarrow}} \langle x' = f(x) \rangle r \leq 1 \overset{\text{Step 2}\ \mathsf{K}\langle\&\rangle}{\overbrace{\rightarrow}} \langle x' = f(x) \rangle r = 1 \overset{\text{Step 3}\ \mathsf{K}\langle\&\rangle}{\overbrace{\rightarrow}} \langle x' = f(x) \rangle P$$




**Intuition:** Symbolically analyze derivatives to lower bound time required to reach disk for the train.

# Proving Liveness for Train

$$\langle x' = f(x), t' = 1\rangle t > 1.4 \overset{\text{Step 1}}{\overset{K\langle\&\rangle}{\overbrace{\to}}} \langle x' = f(x)\rangle r \leq 1 \overset{\text{Step 2}}{\overset{K\langle\&\rangle}{\overbrace{\to}}} \langle x' = f(x)\rangle r = 1 \overset{\text{Step 3}}{\overset{K\langle\&\rangle}{\overbrace{\to}}} \langle x' = f(x)\rangle P$$




The train reaches Porto ($P$) if it is driven for $> 1.4$ hours:

$$\langle x' = f(x), t' = 1\rangle t > 1.4 \to \langle x' = f(x)\rangle P$$

# Existence Properties

**Idea 3:** Basic liveness properties of ODEs can be justified by a small number of simple axioms.

GEx $\langle x' = f(x), t' = 1 \rangle t > c()$ (if $x' = f(x)$ globally Lipschitz)

# Existence Properties

**Idea 3:** Basic liveness properties of ODEs can be justified by a small number of simple axioms.

$$\text{GEx}\ \langle x' = f(x), t' = 1\rangle t > c() \quad \text{(if } x' = f(x) \text{ globally Lipschitz)}$$

Apply to ODE example:

$$\dfrac{\overbrace{\langle x' = f(x), t' = 1\rangle t > 1.4}^{\text{GEx}} \qquad \overbrace{\langle x' = f(x), t' = 1\rangle t > 1.4 \rightarrow \langle x' = f(x)\rangle P}^{\text{Train reaches Porto } (P) \text{ if driven for } > 1.4 \text{ hours}}}{\langle x' = f(x)\rangle P}$$

# Existence Properties

**Idea 3:** Basic liveness properties of ODEs can be justified by a small number of simple axioms.

$$\text{GEx } \langle x' = f(x), t' = 1\rangle t > c() \quad \text{(if } x' = f(x) \text{ globally Lipschitz)}$$

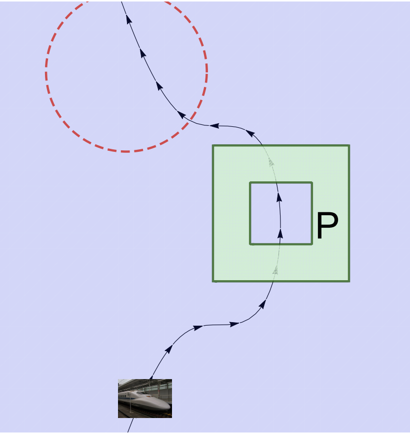
Apply to ODE example:

$$\frac{\overbrace{\cancel{\langle x' = f(x), t' = 1\rangle t > 1.4}}^{\text{Not for } x' = -y,\, y' = 4x^2} \qquad \overbrace{\langle x' = f(x), t' = 1\rangle t > 1.4 \rightarrow \langle x' = f(x)\rangle P}^{\text{Train reaches Porto } (P) \text{ if driven for } > 1.4 \text{ hours}}}{\cancel{\langle x' = f(x)\rangle P}}$$

# Existence Properties

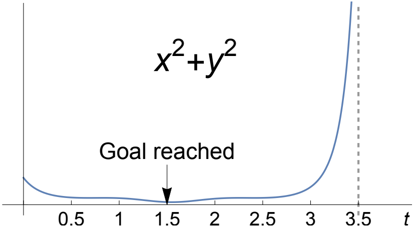
**Idea 3:** Basic liveness properties of ODEs can be justified by a small number of simple axioms.

GEx $\langle x' = f(x), t' = 1 \rangle t > c()$ (if $x' = f(x)$ globally Lipschitz)




**Problem:** Finite time blowup may prevent solutions from reaching goal.

$$\underbrace{x' = -y, y' = 4x^2}_{\text{This non-linear ODE is not globally Lipschitz!}}$$



# Equational Differential Variants

| Surveyed Liveness Arguments | Goals of surveyed paper |
|---|---|
| Eq. Differential Variants [7] | Synthesizing switching logic |

Derived proof rule:

$$\mathrm{dV}_{=}^{M}\ \frac{p = 0 \vdash P \quad p < 0 \vdash p' \geq \varepsilon()}{\Gamma, \varepsilon() > 0, p \leq 0 \vdash \langle x' = f(x) \rangle P}$$

**Additional condition for soundness** ✓:
Either solution exists for sufficient duration or $x' = f(x)$ is globally Lipschitz continuous.

# A Common Technical Glitch

Several errors ($\times$) due to insufficient technical assumptions about existence of solutions.

| Surveyed Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Differential Variants [1] | | |
| Bounded/Compact Eventuality [3, 4] | $\times$ | |
| Set Lyapunov Functions [5] | $\times$ | $\times$ |
| Staging Sets + Progress [6] | | |
| Eq. Differential Variants [7] | $\times$ | $\times$ |

# A Common Technical Glitch

Other errors ($\times$) were due to more subtle issues but they were also caught by our approach.

| Surveyed Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Differential Variants [1] | | $\times$ |
| Bounded/Compact Eventuality [3, 4] | | $\times$ |
| Set Lyapunov Functions [5] | | |
| Staging Sets + Progress [6] | | |
| Eq. Differential Variants [7] | | |

# Outline

# More Diamond Refinement Axioms

K⟨&⟩ $[x' = f(x) \,\&\, Q \land \neg P]\neg B \rightarrow (\langle x' = f(x) \,\&\, Q\rangle B \rightarrow \langle x' = f(x) \,\&\, Q\rangle P)$

DR⟨·⟩ $[x' = f(x) \,\&\, R]Q \rightarrow (\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P)$

COR $\neg P \land [x' = f(x) \,\&\, R \land \neg P]Q \rightarrow (\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P)$

SAR $[x' = f(x) \,\&\, R \land \neg(P \land Q)]Q \rightarrow (\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P)$

GEx $\langle x' = f(x), t' = 1\rangle t > c()$ (if $x' = f(x)$ globally Lipschitz)

BEx $\langle x' = f(x), t' = 1\rangle(\neg B(x) \lor t > c())$

# More Diamond Refinement Axioms

**Idea 1:** ODE safety has effective reasoning principles [LICS'18], so use ODE safety to justify refinement steps.

COR $\neg P \wedge [x' = f(x) \,\&\, R \wedge \neg P]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

SAR $[x' = f(x) \,\&\, R \wedge \neg(P \wedge Q)]Q \rightarrow \big(\langle x' = f(x) \,\&\, R\rangle P \rightarrow \langle x' = f(x) \,\&\, Q\rangle P\big)$

GEx $\langle x' = f(x), t' = 1\rangle t > c()$ (if $x' = f(x)$ globally Lipschitz)

BEx $\langle x' = f(x), t' = 1\rangle(\neg B(x) \vee t > c())$

# More Diamond Refinement Axioms

**Idea 1:** ODE safety has effective reasoning principles [LICS'18], so use ODE safety to justify refinement steps.

**Idea 2:** Implication chains build complicated liveness arguments from simple building blocks.

GEx $\langle x' = f(x), t' = 1 \rangle t > c()$ (if $x' = f(x)$ globally Lipschitz)

BEx $\langle x' = f(x), t' = 1 \rangle (\neg B(x) \vee t > c())$

# More Diamond Refinement Axioms

**Idea 1:** ODE safety has effective reasoning principles [LICS'18], so use ODE safety to justify refinement steps.

**Idea 2:** Implication chains build complicated liveness arguments from simple building blocks.

**Idea 3:** Basic liveness properties of ODEs can be justified by a small number of simple axioms.

# More Diamond Refinement Axioms

**Idea 1:** ODE safety has effective reasoning principles [LICS'18], so use ODE safety to justify refinement steps.

**Idea 2:** Implication chains build complicated liveness arguments from simple building blocks.

**Idea 3:** Basic liveness properties of ODEs can be justified by a small number of simple axioms.

**Idea 4:** Reducing ODE liveness arguments to basic liveness refinements isolates and minimizes the possibility of soundness errors.

# More Diamond Refinement Axioms

**Idea 1:** ODE safety has effective reasoning principles [LICS'18], so use ODE safety to justify refinement steps.

**Idea 2:** Implication chains build complicated liveness arguments from simple building blocks.

**Idea 3:** Basic liveness properties of ODEs can be justified by a small number of simple axioms.

**Idea 4:** Reducing ODE liveness arguments to basic liveness refinements isolates and minimizes the possibility of soundness errors.

**Key Idea:** Liveness arguments can and should be understood using liveness refinement steps.

# An Axiomatic Approach to Liveness for ODEs

Why take a **logical** approach?

- Understand the core principles behind ODE liveness proofs.

| Surveyed Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Differential Variants [1] | ✓ | ✗ ⇝ ✓ |
| Bounded/Compact Eventuality [3, 4] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |
| Set Lyapunov Functions [5] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |
| Staging Sets + Progress [6] | ✓ | ✓ |
| Eq. Differential Variants [7] | ✗ ⇝ ✓ | ✗ ⇝ ✓ |

- Yields generalizations of existing liveness arguments "for free".

| New Liveness Arguments | Without Domains | With Domains |
|---|---|---|
| Higher Differential Variants | ✓ | - |
| [1] + [3, 4] + [6] | ✓ | - |
| [1] + [3, 4] + [6] + Higher Diff. Var. | - | ✓ |

[1] André Platzer. 2010. Differential-algebraic Dynamic Logic for Differential-algebraic Programs. J. Log. Comput. 20, 1 (2010), 309–352. https://doi.org/10.1093/logcom/exn070

[2] André Platzer and Yong Kiam Tan. 2018. Differential Equation Axiomatization: The Impressive Power of Differential Ghosts. In LICS, Anuj Dawar and Erich Grädel (Eds.). ACM, New York, 819–828. https://doi.org/10.1145/3209108.3209147

[3] Stephen Prajna and Anders Rantzer. 2005. Primal-Dual Tests for Safety and Reachability. In HSCC (LNCS), Manfred Morari and Lothar Thiele (Eds.), Vol. 3414. Springer, Heidelberg, 542–556. https://doi.org/10.1007/978-3-540-31954-2_35

[4] Stephen Prajna and Anders Rantzer. 2007. Convex Programs for Temporal Verification of Nonlinear Dynamical Systems. SIAM J. Control Optim. 46, 3 (2007), 999–1021. https://doi.org/10.1137/050645178

# References II


[5] Stefan Ratschan and Zhikun She. 2010. Providing a Basin of Attraction to a Target Region of Polynomial Systems by Computation of Lyapunov-Like Functions. SIAM J. Control Optim. 48, 7 (2010), 4377–4394. https://doi.org/10.1137/090749955

[6] Andrew Sogokon and Paul B. Jackson. 2015. Direct Formal Verification of Liveness Properties in Continuous and Hybrid Dynamical Systems. In FM (LNCS), Nikolaj Bjørner and Frank S. de Boer (Eds.), Vol. 9109. Springer, Cham, 514–531. https://doi.org/10.1007/978-3-319-19249-9_32

[7] Ankur Taly and Ashish Tiwari. 2010. Switching logic synthesis for reachability. In EMSOFT, Luca P. Carloni and Stavros Tripakis (Eds.). ACM, New York, 19–28. https://doi.org/10.1145/1879021.1879025