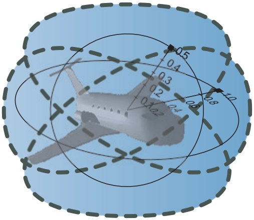
The Logical Path to Autonomous Cyber-Physical Systems

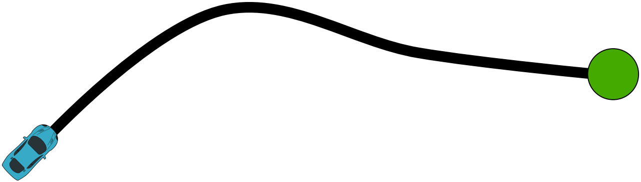
André Platzer

Carnegie Mellon University



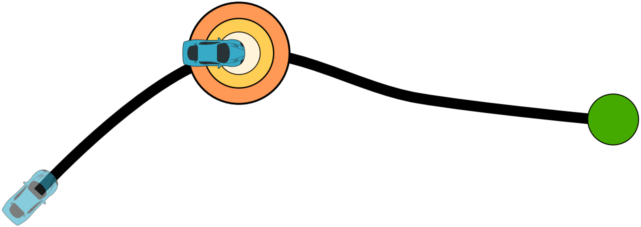
Outline

Outline



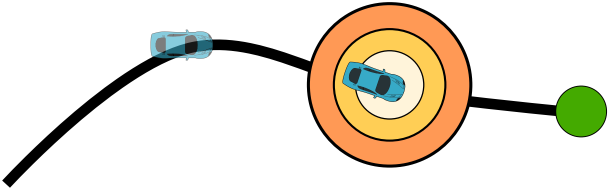
Cyber-Physical Systems

CPSs combine cyber capabilities with physical capabilities
to solve problems that neither part could solve alone.



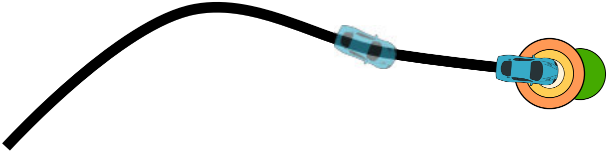
Cyber-Physical Systems

CPSs combine cyber capabilities with physical capabilities
to solve problems that neither part could solve alone.



Cyber-Physical Systems

CPSs combine cyber capabilities with physical capabilities to solve problems that neither part could solve alone.



Cyber-Physical Systems

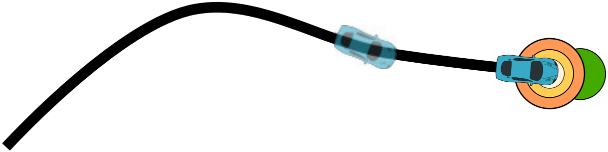
CPSs combine cyber capabilities with physical capabilities
to solve problems that neither part could solve alone.

CPS Analysis

- Simple control
- ODE model
- Strong predictions
- Nondet decisions

AI Learning

- Flexible responses
- "No" model*
- Hard to predict
- Optimal decision ($t \to \infty$)



Cyber-Physical Systems

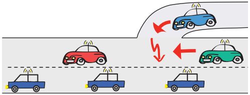
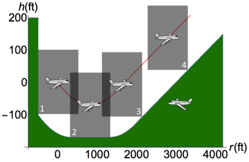
CPSs combine cyber capabilities with physical capabilities to solve problems that neither part could solve alone.

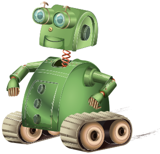
Autonomous CPSs Are on the Rise Everywhere

Prospects: Safety & Efficiency & Autonomy

Autonomous cars — Autonomous pilots — Robots near humans



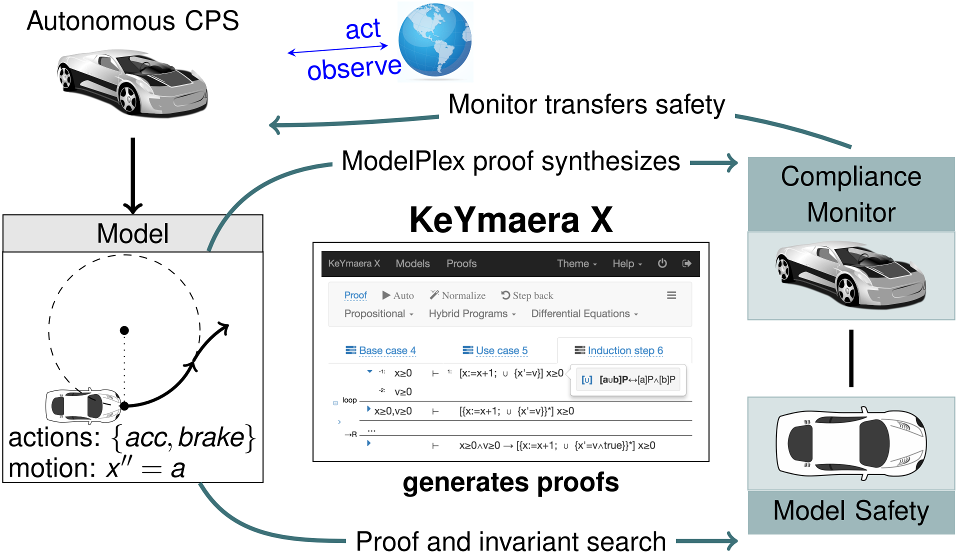


Objective

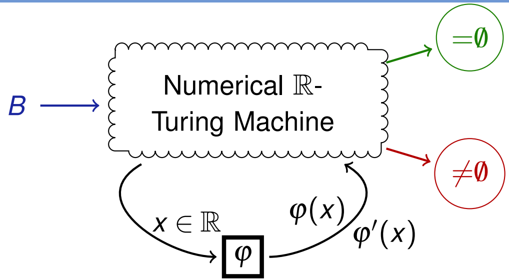
Best of both worlds: safety from CPS + flexibility from AI

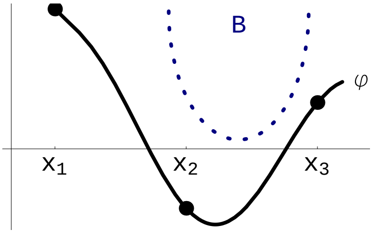
Outline

Approach: Safety Proofs for Autonomous CPS



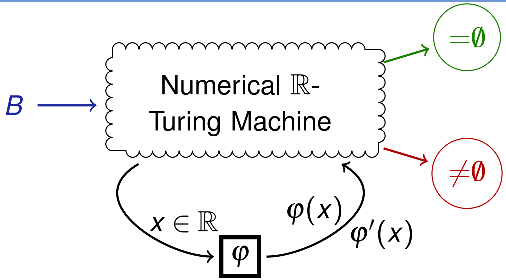
Model Requirements

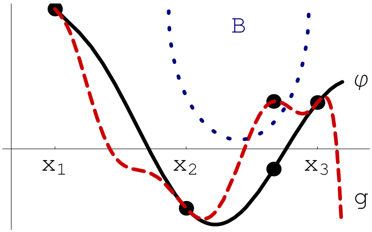




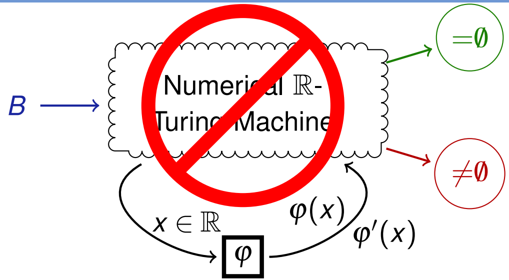
HSCC'07

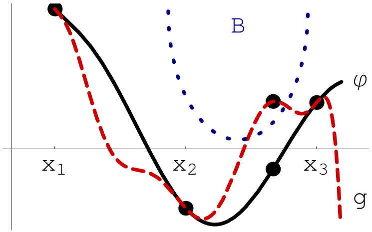
Model Requirements





HSCC'07





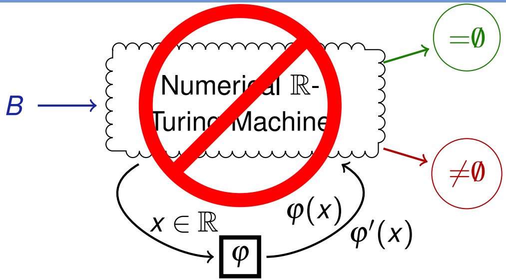
Proposition (Continuous image computation undecidable)

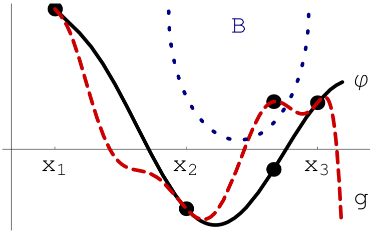
$\varphi(D) \cap B \stackrel{?}{=} \emptyset$ is undecidable by evaluating $\varphi(x)$ for

- *arbitrarily effective flow $\varphi \in C^k(D \subseteq \mathbb{R}^n, \mathbb{R}^m)$ with effective D, B*
- *even if tolerating error $\varepsilon > 0$ in decisions*

HSCC'07

Model Requirements: Symbolic/Intensional!



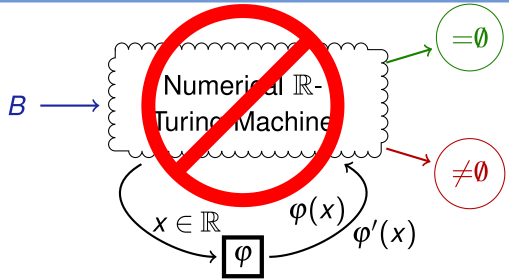


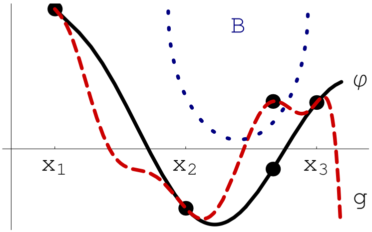
Proposition (Continuous image computation undecidable)

$\varphi(D) \cap B \stackrel{?}{=} \emptyset$ is undecidable by evaluating $\varphi(x)$ for

- *arbitrarily effective flow $\varphi \in C^k(D \subseteq \mathbb{R}^n, \mathbb{R}^m)$ with effective D, B*
- *even if tolerating error $\varepsilon > 0$ in decisions*
- *even φ smooth polynomial function with $\mathbb{Q}$-coefficients*
- *even in Blum-Shub-Smale “real Turing machines”*

HSCC’07





Proposition (Continuous image computation undecidable)

$\varphi(D) \cap B \stackrel{?}{=} \emptyset$ is undecidable by evaluating $\varphi(x)$ for

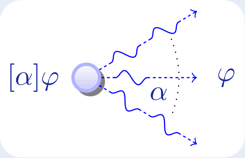
- *arbitrarily effective flow $\varphi \in C^k(D \subseteq \mathbb{R}^n, \mathbb{R}^m)$ with effective D, B*
- *even if tolerating error $\varepsilon > 0$ in decisions*
- *even φ smooth polynomial function with $\mathbb{Q}$-coefficients*
- *even in Blum-Shub-Smale "real Turing machines"*

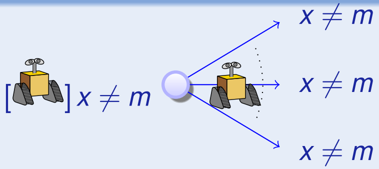
The promise of "no model" is a myth

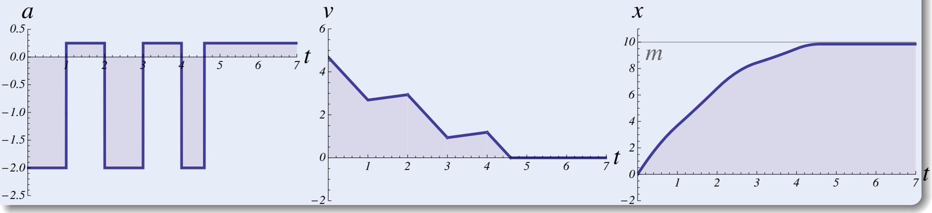
HSCC'07

CPS Analysis

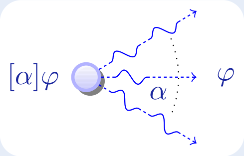
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)

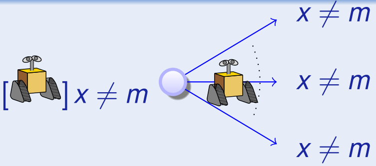






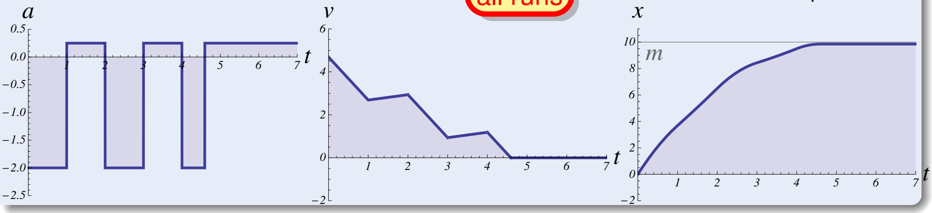
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





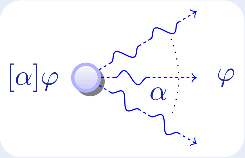
$$[\big((\text{if}(SB(x,m)) \quad a := -b)\ ;\ x' = v, v' = a\big)^*]\underbrace{x \neq m}_{\text{post}}$$

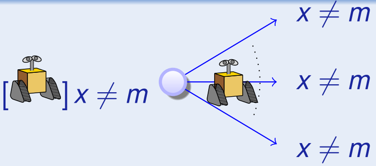
all runs



CPS Analysis

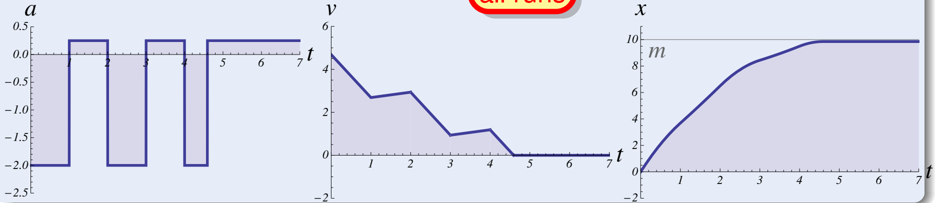
Concept (Differential Dynamic Logic) (JAR'08,LICS'12)





$$\underbrace{x \neq m \land b > 0}_{\text{init}} \rightarrow \Big[\Big(\big(\text{if}(SB(x,m)) \quad a := -b\big)\ ;\ x' = v, v' = a\Big)^*\Big]\underbrace{x \neq m}_{\text{post}}$$

all runs



Differential Dynamic Logic dL: Axiomatization

equations of truth

[:=] $[x := e]P(x) \leftrightarrow P(e)$

[?] $[?Q]P \leftrightarrow (Q \rightarrow P)$

['] $[x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P$ $\quad (y'(t) = f(y))$

[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$

[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

[*] $[\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$

K $[\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$

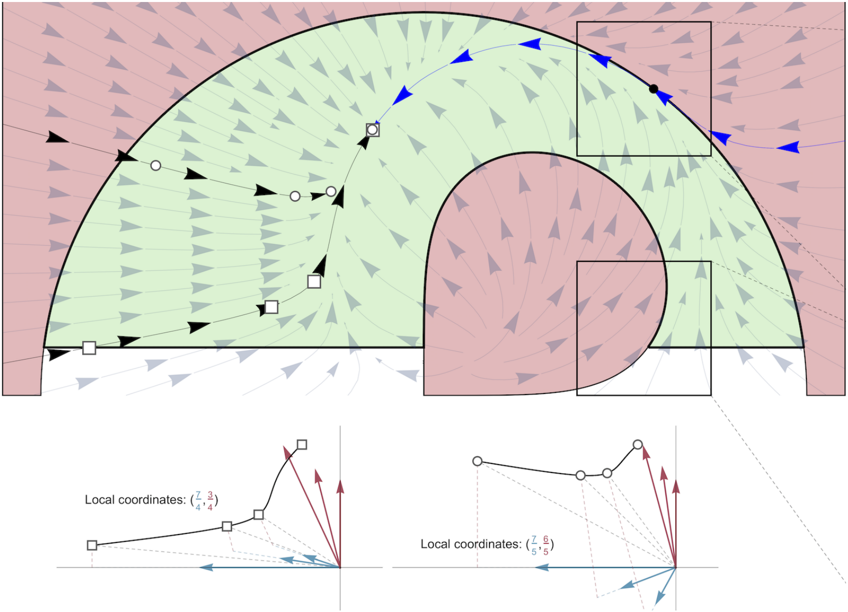
I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

C $[\alpha^*]\forall v{>}0\, (P(v) \rightarrow \langle\alpha\rangle P(v-1)) \rightarrow \forall v\, (P(v) \rightarrow \langle\alpha^*\rangle \exists v{\leq}0\, P(v))$

laws of logic of
laws of physics

LICS'12,JAR'17

Completeness for Differential Equation Invariants



LICS'18,JACM'20

Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18,JACM'20)

dL *calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations. They are decidable by DI,DC,DG in* dL.

Theorem (Semialgebraic Completeness) (LICS'18,JACM'20)

dL *calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations. They are decidable in* dL.

Differential Equation Axiomatization

Theorem (Algebraic Completeness) (LICS'18,JACM'20)

dL *calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations. They are decidable*

$$\text{DRI} \quad [x' = f(x)\,\&\,Q]e = 0 \leftrightarrow \big(Q \rightarrow e'^{*} = 0\big) \qquad (Q \text{ open})$$

Theorem (Semialgebraic Completeness) (LICS'18,JACM'20)

dL *calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations. They are decidable*

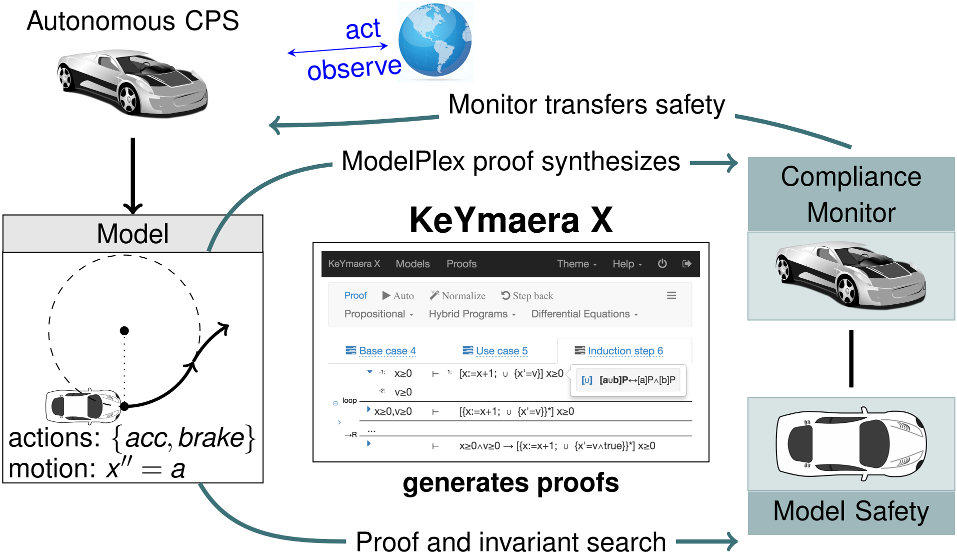
$$\text{SAI} \ \forall x\,(P \rightarrow [x' = f(x)]P) \leftrightarrow \forall x\,\big(P \rightarrow P'^{*}\big) \land \forall x\,\big(\neg P \rightarrow (\neg P)'^{*-}\big)$$

Definable e'^{*} is short for *all/significant* Lie derivative w.r.t. ODE
Definable e'^{*-} is w.r.t. backwards ODE $x' = -f(x)$. Also for P.

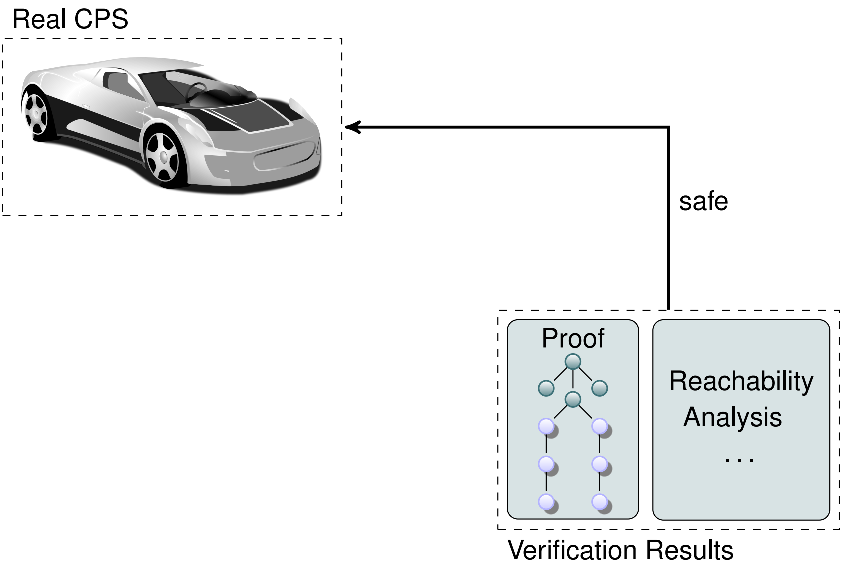
$$e'^{*} = 0 \equiv e{=}0 \land (e')'^{*}{=}0 \qquad (P \land Q)'^{*} \equiv P'^{*} \land Q'^{*}$$
$$e'^{*} \geq 0 \equiv e{\geq}0 \land (e{=}0{\rightarrow}(e')'^{*}{\geq}0) \qquad (P \lor Q)'^{*} \equiv P'^{*} \lor Q'^{*}$$

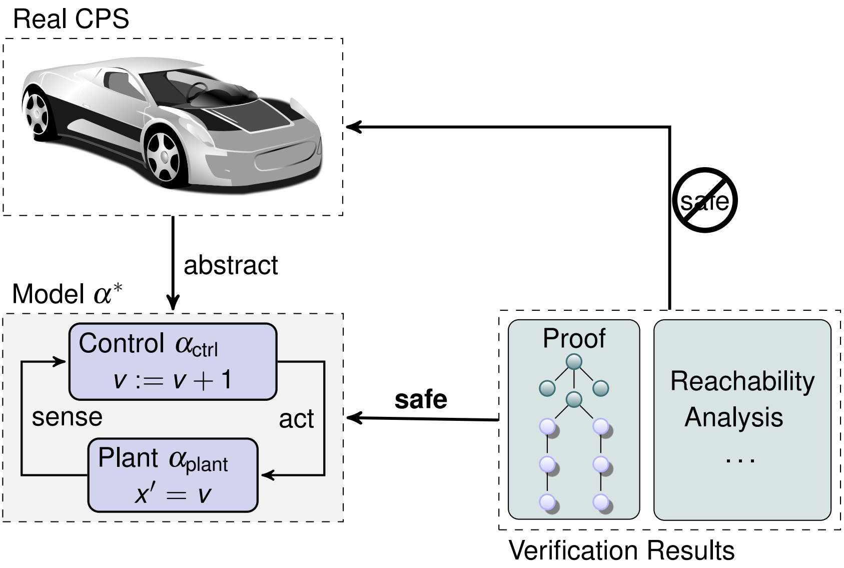
Outline

Approach: Safety Proofs for Autonomous CPS

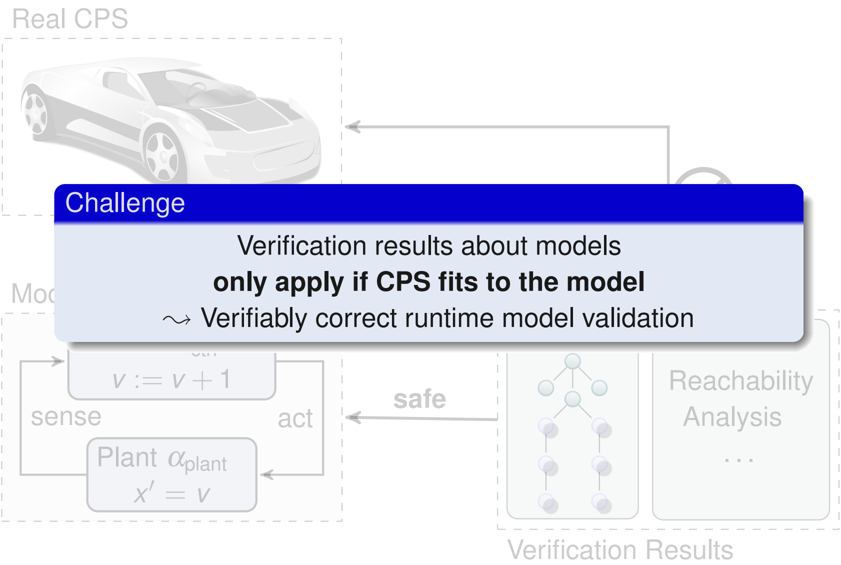


Formal Verification in CPS Development




Real CPS
abstract
Model α^*
Control α_{ctrl}
$v := v + 1$
sense
act
Plant α_{plant}
$x' = v$
safe
safe
Proof
Reachability Analysis
...
Verification Results

Formal Verification in CPS Development



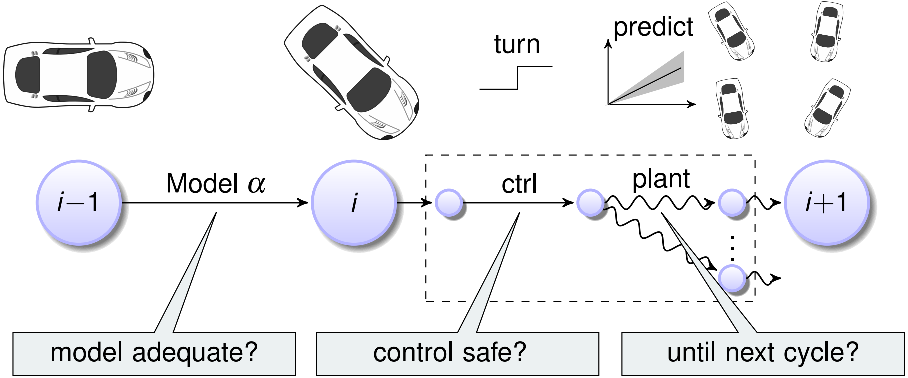
Challenge

Verification results about models

only apply if CPS fits to the model

$\rightsquigarrow$ Verifiably correct runtime model validation

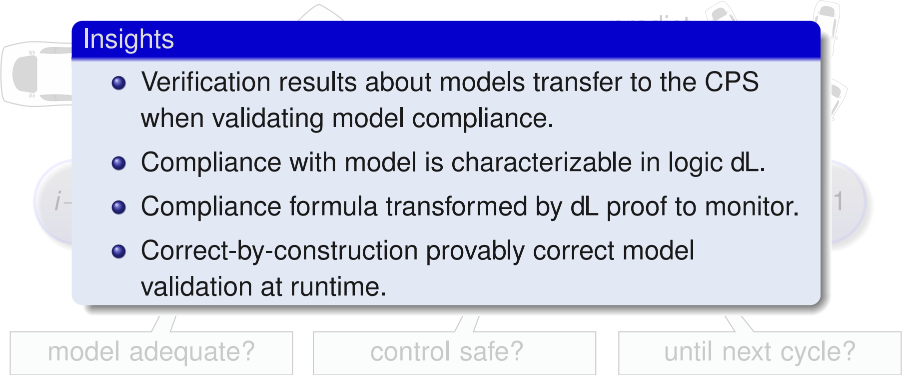
ModelPlex **ensures that verification results** about models **apply to CPS** implementations



FMSD'16

ModelPlex Runtime Model Validation

ModelPlex **ensures that verification results** about models **apply to CPS** implementations



Insights

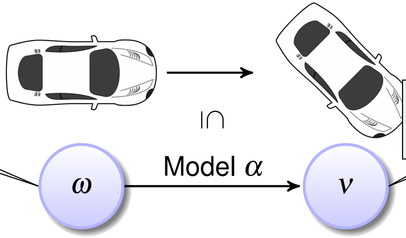
- Verification results about models transfer to the CPS when validating model compliance.
- Compliance with model is characterizable in logic dL.
- Compliance formula transformed by dL proof to monitor.
- Correct-by-construction provably correct model validation at runtime.

FMSD'16

Characterizing State Relations in Logic

When are two states linked through a run of model α?

a prior state characterized by x^-



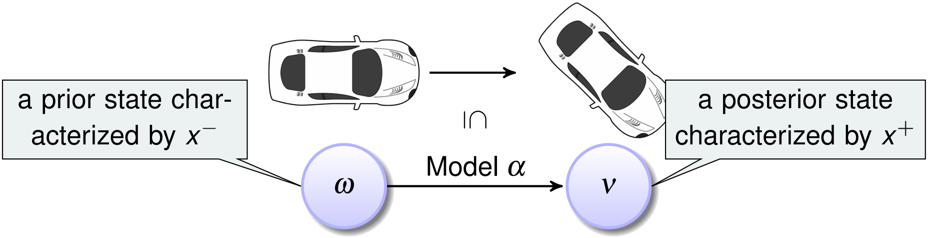
a posterior state characterized by x^+

Semantical: $(\omega, \nu) \in [\![\alpha]\!]$

reachability relation of α

FMSD'16

When are two states linked through a run of model α?



Offline

Semantical: $(\omega, \nu) \in [\![\alpha]\!]$

$\Updownarrow$ Lemma

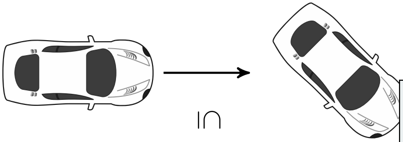
Logical dL: $(\omega, \nu) \models \langle\alpha\rangle(x = x^+)$

exists a run of α to a state where $x = x^+$

FMSD'16

Characterizing State Relations in Logic

When are two states linked through a run of model α?



a prior state characterized by x^-

$\omega \xrightarrow{\text{Model } \alpha} \nu$

a posterior state characterized by x^+

Offline

Semantical: $(\omega, \nu) \in [\![\alpha]\!]$

$\Updownarrow$ Lemma

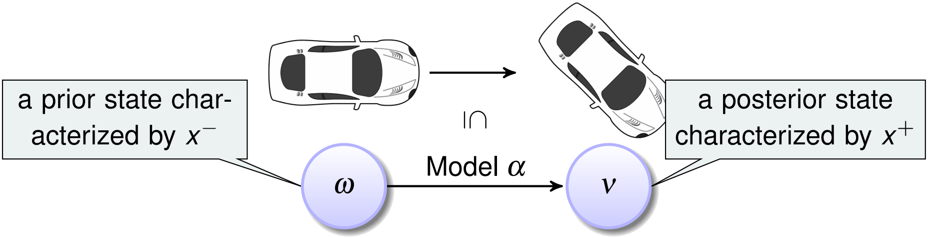
Logical dL: $(\omega, \nu) \models \langle\alpha\rangle(x = x^+)$ — exists a run of α to a state where $x = x^+$

$\Updownarrow$ dL proof

Arithmetical: $(\omega, \nu) \models F(x^-, x^+)$ — check at runtime (efficient)

FMSD'16

When are two states linked through a run of model α?



Offline

Semantical: $(\omega, \nu) \in [\![\alpha]\!]$

$\Updownarrow$ Lemma

Logical dL: $(\omega, \nu) \models \langle\alpha\rangle(x = x^+)$ — exists a run of α to a state where $x = x^+$

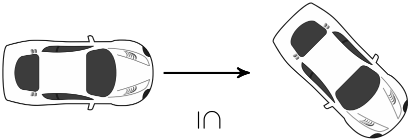
$\Uparrow$ dL proof

Arithmetical: $(\omega, \nu) \models F(x^-, x^+)$ — check at runtime (efficient)

FMSD'16

Logical Reductions for Model Safety Transfer

Logic reduces CPS safety to runtime monitor with offline proof



dL proof $A \rightarrow [\alpha]S$ — ω —Model α→ ν

Offline

Init $\omega \in [\![A]\!]$ Safe $\nu \in [\![S]\!]$

Semantical: $(\omega, \nu) \in [\![\alpha]\!]$

$\Updownarrow$ Lemma

Logical dL: $(\omega, \nu) \models \langle\alpha\rangle(x = x^+)$

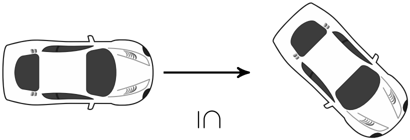
$\Uparrow$ dL proof

Arithmetical: $(\omega, \nu) \models F(x^-, x^+)$

check at runtime (efficient)

FMSD'16

Logic reduces CPS safety to runtime monitor with offline proof



dL proof $A \rightarrow [\alpha]S$ ω —Model α→ ν

Offline

Init $\omega \in [\![A]\!]$ Safe $\nu \in [\![S]\!]$

Semantical: $(\omega, \nu) \in [\![\alpha]\!]$

$\Updownarrow$ Lemma

Logical dL: $(\omega, \nu) \models \langle\alpha\rangle(x = x^+)$

$\Uparrow$ dL proof

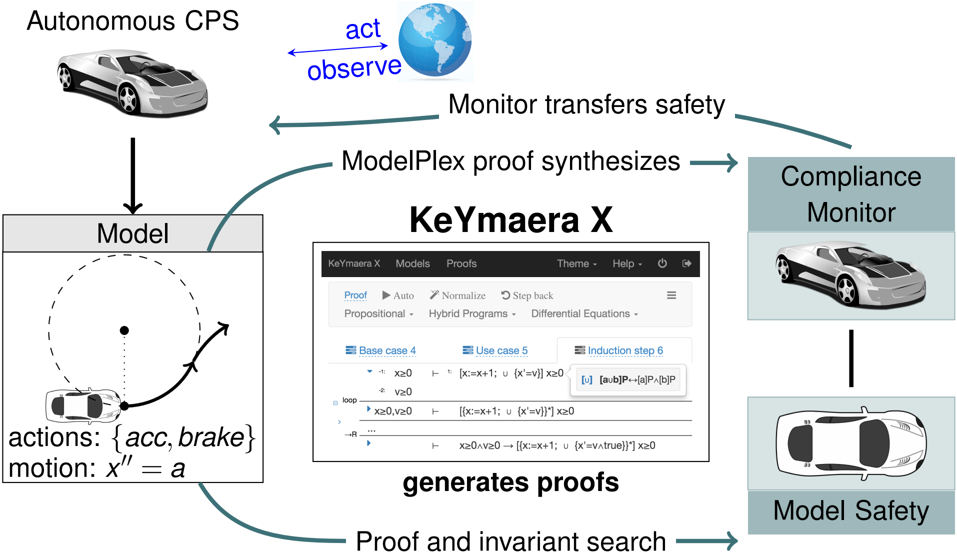
Arithmetical: $(\omega, \nu) \models F(x^-, x^+)$

check at runtime (efficient)

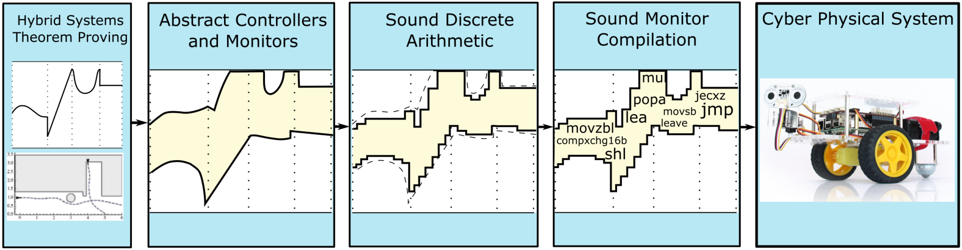
FMSD'16

Outline

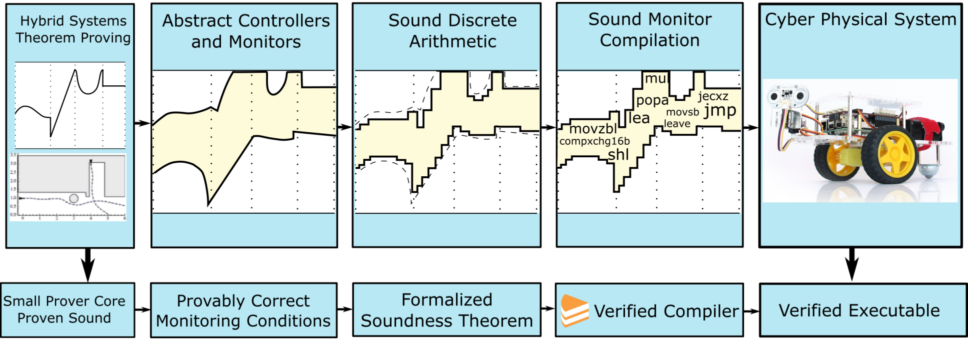
Approach: Safety Proofs for Autonomous CPS



VeriPhy: Automatic, Verified EXEs from Controllers

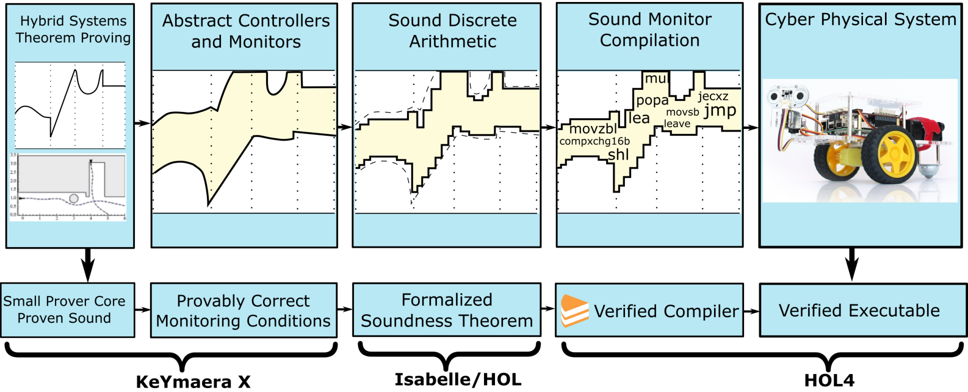


PLDI'18


Hybrid Systems Theorem Proving
Abstract Controllers and Monitors
Sound Discrete Arithmetic
Sound Monitor Compilation
mul
popa
jecxz
lea
movsb
jmp
movzbl
leave
compxchg16b
shl
Cyber Physical System
Small Prover Core Proven Sound
Provably Correct Monitoring Conditions
Formalized Soundness Theorem
Verified Compiler
Verified Executable

PLDI’18

VeriPhy: Automatic, Verified EXEs from Controllers

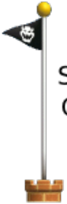


PLDI'18

VeriPhy: Takeaway Metaphor

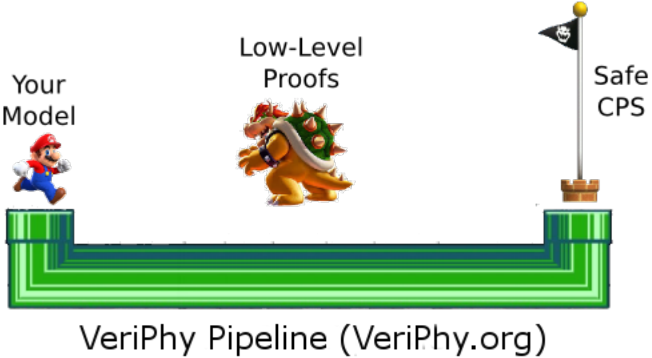
Your Model

Low-Level Proofs



Safe CPS

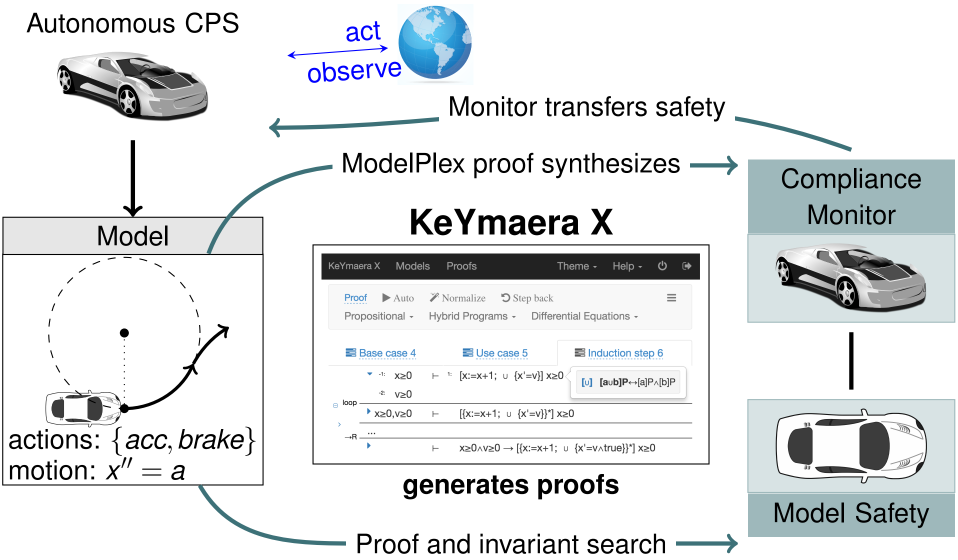
VeriPhy: Takeaway Metaphor

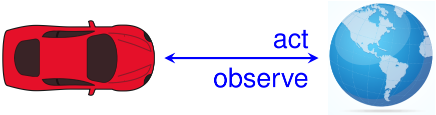


Outline

1. Autonomous Cyber-Physical Systems
2. Foundation: Differential Dynamic Logic
3. ModelPlex: Model Safety Transfer
4. VeriPhy: Executable Proof Transfer
5. **Safe Learning in CPSs**
6. Applications
   - Airborne Collision Avoidance System
   - Ground Robot Navigation
7. Summary

Approach: Safety Proofs for Autonomous CPS

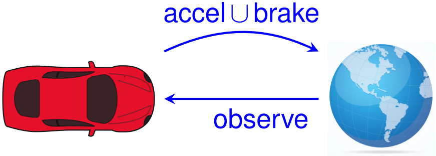




Reinforcement Learning learns from experience of trying actions

AAAI'18,ITC'18,TACAS'19,QEST'19

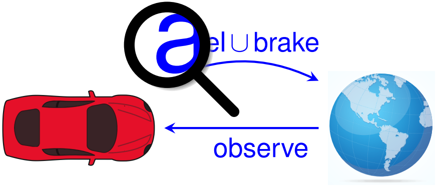
Learning to Act in a CPS



RL chooses an action, observes outcome, reinforces in policy if successful

AAAI'18,ITC'18,TACAS'19,QEST'19

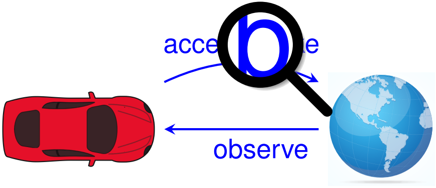
Learning to Act Safely in a CPS



ModelPlex monitor inspects each decision, vetoes if unsafe

AAAI'18,ITC'18,TACAS'19,QEST'19

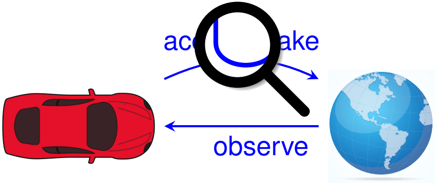
Learning to Act Safely in a CPS



ModelPlex monitor gives early feedback about possible future problems.
No need to wait till disaster strikes and propagate back.

AAAI'18,ITC'18,TACAS'19,QEST'19

Learning to Act Safely in a CPS

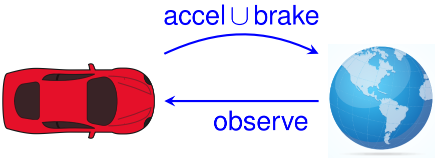


dL benefits from RL optimization.

RL benefits from dL safety signal.

AAAI'18,ITC'18,TACAS'19,QEST'19

Learning to Act Safely in a CPS



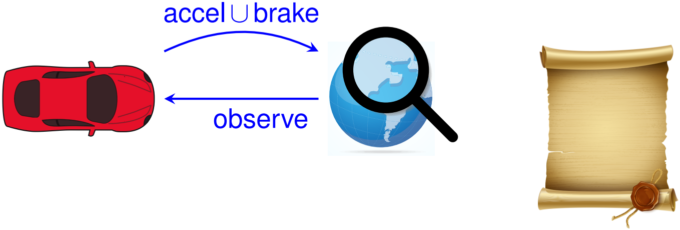
Theorem Safe policy if ODE accurate

Experiment Graceful recovery outside ODE ⇜ quantitative ModelPlex

Detect modeled versus unmodeled state space ⇜ ModelPlex

AAAI'18,ITC'18,TACAS'19,QEST'19

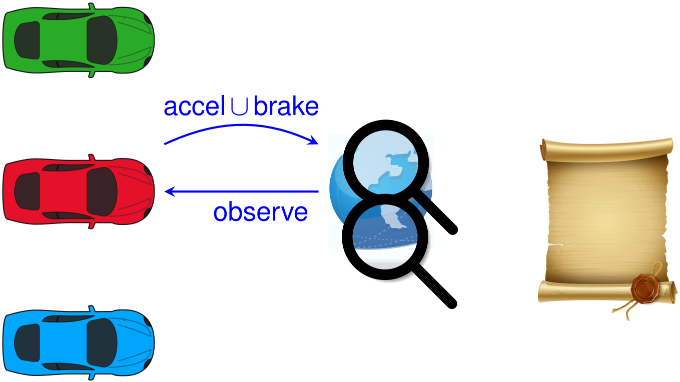
Learning to Act Safely in a CPS



What's safe when off model?

AAAI'18,ITC'18,TACAS'19,QEST'19

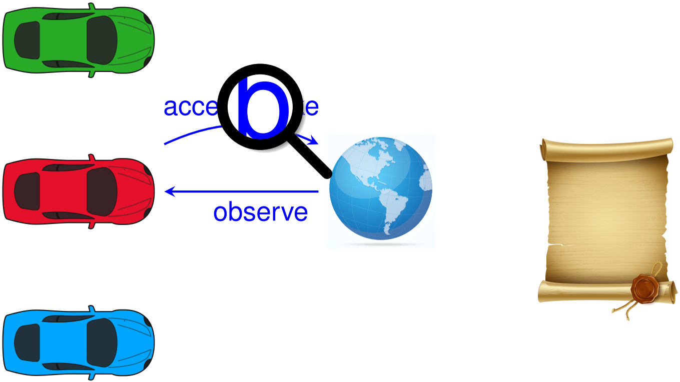
Learning to Act Safely in a CPS with Multiple Models



What's safe with multiple possible models?

AAAI'18,ITC'18,TACAS'19,QEST'19

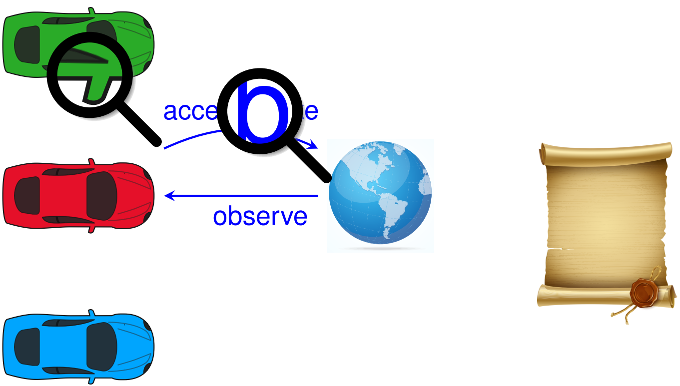
Learning to Act Safely in a CPS with Multiple Models



ModelPlex monitors conjunction of all plausible models

AAAI'18,ITC'18,TACAS'19,QEST'19

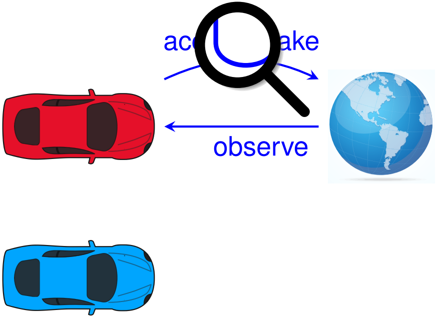
Learning to Act Safely in a CPS with Multiple Models



Remove incompatible models after contradictory observation

AAAI'18,ITC'18,TACAS'19,QEST'19

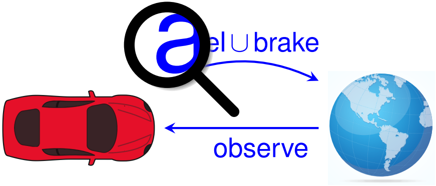
Learning to Act Safely in a CPS with Multiple Models



Plan differentiating experiment $\leftsquigarrow$ predictive monitor distinctions

AAAI'18,ITC'18,TACAS'19,QEST'19

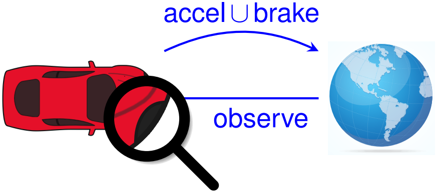
Learning to Act Safely in a CPS with Multiple Models



Convergence Plausible models converge to true model a.s., if possible

AAAI'18,ITC'18,TACAS'19,QEST'19

Learning to Act Safely in a CPS with Multiple Models

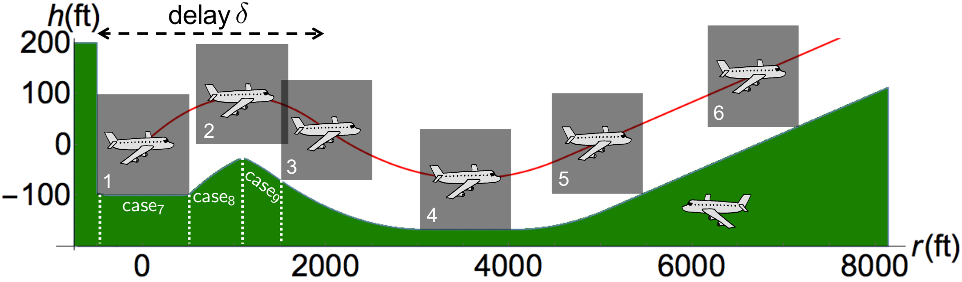


Modify model to fit observations by verification-preserving model update.
Safety proofs reified: modify model + proof tactic to preserve fit + safety

AAAI'18,ITC'18,TACAS'19,QEST'19

Outline

- Developed by the FAA to replace current TCAS in aircraft
- Approximately optimizes Markov Decision Process on a grid
- Advisory from lookup tables with numerous 5D interpolation regions

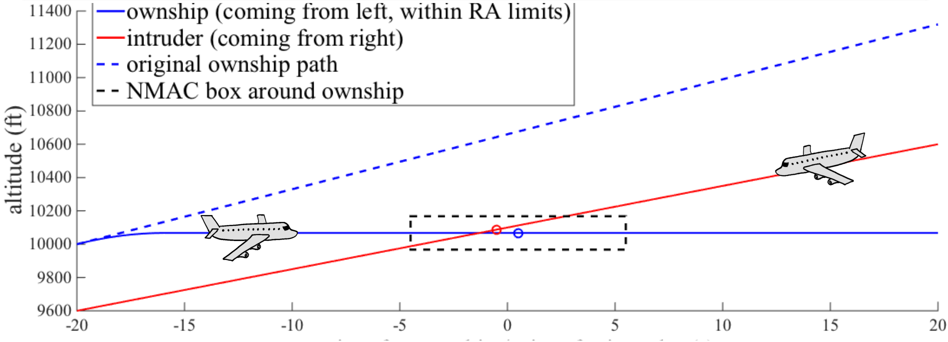


1. Identified safe region for each advisory symbolically
2. Proved safety for hybrid systems flight model in KeYmaera X

STTT'17

Airborne Collision Avoidance System ACAS X: Compare

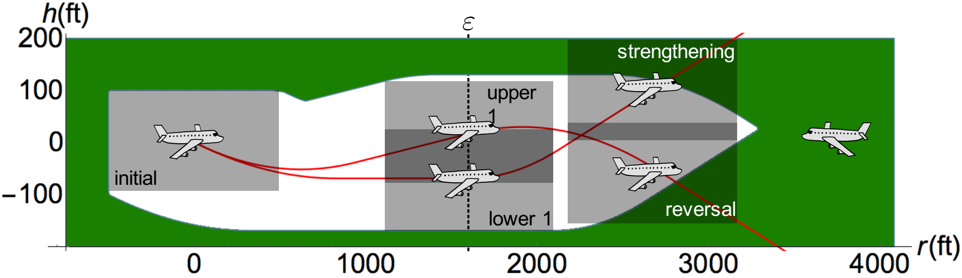
ACAS X table comparison shows safe advisory in 97.7% of the 648,591,384,375 states compared (15,160,434,734 counterexamples).



ACAS X issues DNC advisory, which induces collision unless corrected

STTT'17

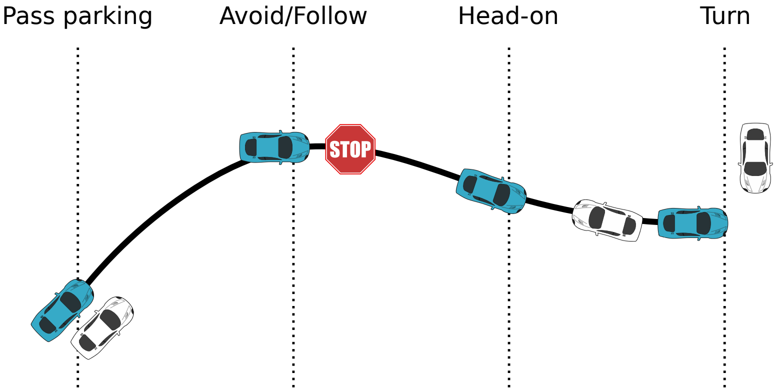
- Conservative, so too many counterexamples
- Settle for: safe for a little while, with safe future advisory possibility
- Safeable advisory: a subsequent advisory can safely avoid collision



1. Identified safeable region for each advisory symbolically
2. Proved safety for hybrid systems flight model in KeYmaera X

STTT'17

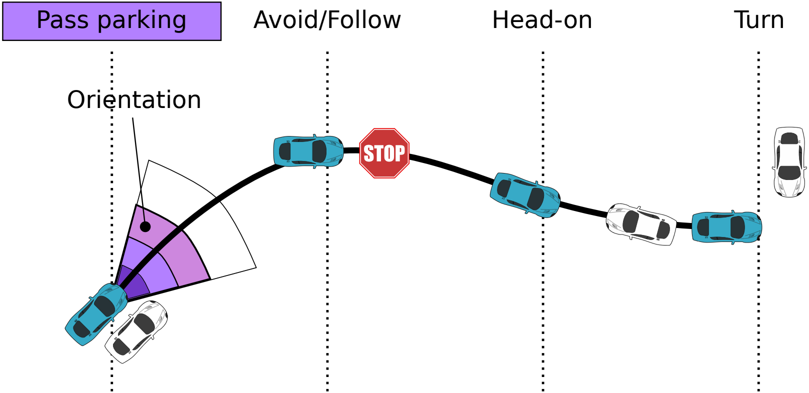
- Fundamental safety question for ground robot navigation IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Obstacle Avoidance: Verify

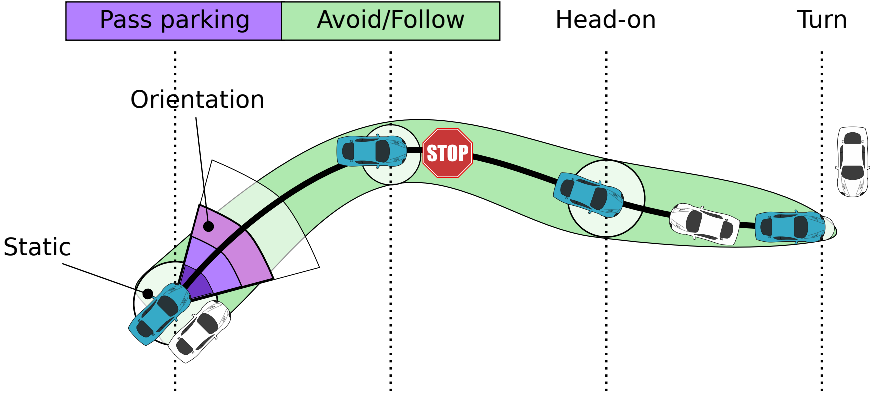
- Fundamental safety question for ground robot navigation — IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Obstacle Avoidance: Verify

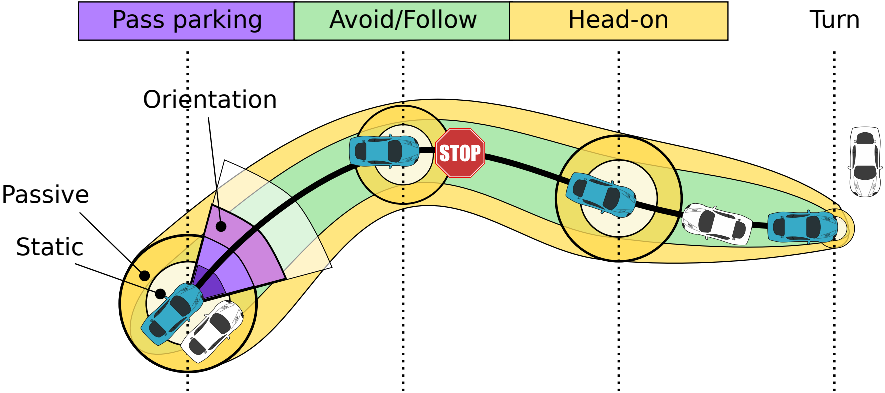
- Fundamental safety question for ground robot navigation — IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Obstacle Avoidance: Verify

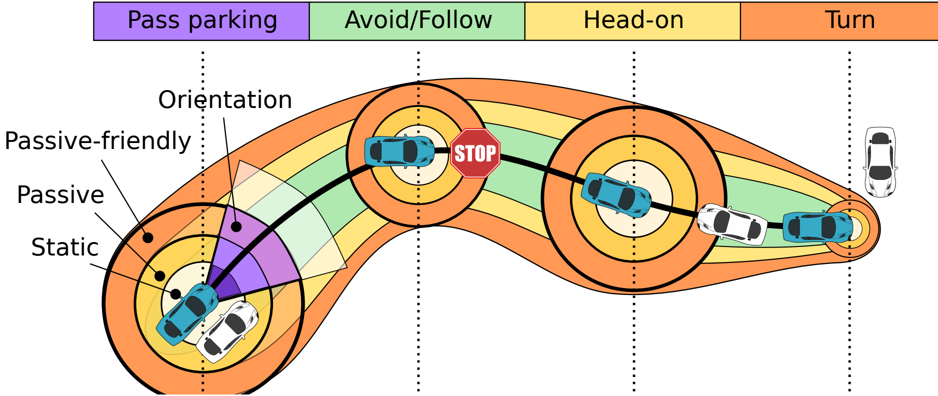
- Fundamental safety question for ground robot navigation — IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Obstacle Avoidance: Verify

- Fundamental safety question for ground robot navigation — IJRR'17
- When will which control decision avoid obstacles?
- Depends on safety objective, physical capabilities of robot + obstacle



1. Identified safe region for each safety notion symbolically
2. Proved safety for hybrid systems ground robot model in KeYmaera X

Ground Robot Invariants and Safe Control Constraints

Safety	Invariant + Safe Control
static	$\|p-o\|_\infty > \frac{s^2}{2b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon s\right)$
passive	$s \neq 0 \to \|p-o\|_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$
+ sensor	$\|\hat{p}-o\|_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right) + \Delta_p$
+ disturb.	$\|p-o\|_\infty > \frac{s^2}{2b\Delta_a} + V\frac{s}{b\Delta_a} + \left(\frac{A}{b\Delta_a}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$
+ failure	$\|\hat{p}-o\|_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(v+V)\right) + \Delta_p + g\Delta$
friendly	$\|p-o\|_\infty > \frac{s^2}{2b} + \frac{V^2}{2b_o} + V\left(\frac{s}{b}+\tau\right) + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$

$\vdots$

IJRR'17

Safety	Invariant + Safe Control
static	$\lVert p-o\rVert_\infty > \frac{s^2}{2b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon s\right)$
passive	$s\neq 0 \rightarrow \lVert p-o\rVert_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$
+ sensor	[illegible] $V)\big) + \Delta_p$
+ disturb.	$\lVert p-o\rVert_\infty >$ [illegible] $2b\Delta_a$ $+ V$ [illegible] $b\Delta_a$ $+ ($ [illegible] $b\Delta_a$ $+1)($ [illegible] $\varepsilon^2 + \varepsilon(s+V))$
+ failure	$\lVert \hat{p}-o\rVert_\infty > \frac{s^2}{2b} + V\frac{s}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(v+V)\right) + \Delta_p + g\Delta$
friendly	$\lVert p-o\rVert_\infty > \frac{s^2}{2b} + \frac{V^2}{2b_o} + V\left(\frac{s}{b}+\tau\right) + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2+\varepsilon(s+V)\right)$

⋮

Question

How to find and justify constraints? Proof!

IJRR'17

Outline

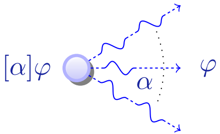
Acknowledgments

Logical Systems Lab at Carnegie Mellon University, Computer Science
Yong Kiam Tan, Brandon Bohrer, Nathan Fulton, Sarah Loos, Katherine Cordwell
Stefan Mitsch, Khalil Ghorbal, Jean-Baptiste Jeannin, Andrew Sogokon

Unterstützt von / Supported by
Alexander von Humboldt
Stiftung / Foundation

differential dynamic logic

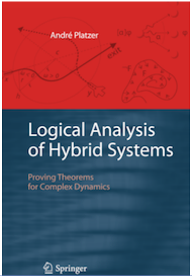
dL = DL + HP



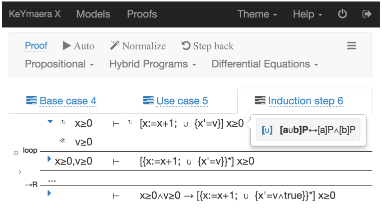
Logical Triumvirate of Technologies for Transitioning Trustworthiness

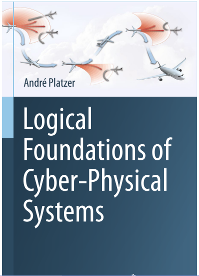
1. KeYmaera X: safe action in CPS model
2. ModelPlex: safe model $\rightsquigarrow$ safe impl
3. VeriPhy: sandbox $\rightsquigarrow$ safe executable

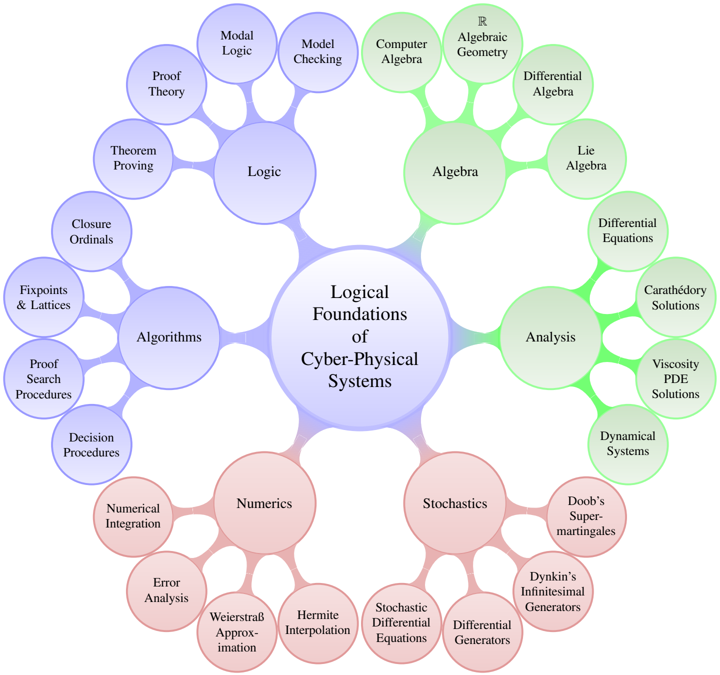
1. RL optimizes action choice
2. ModelPlex: safe reward for RL
3. VeriPhy: CPS sandbox for RL

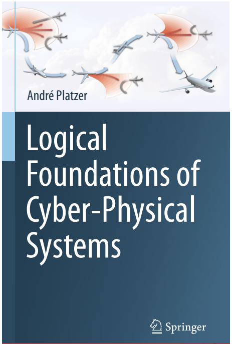


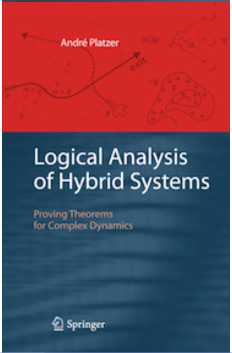
KeYmaera X






Logical Foundations of Cyber-Physical Systems
Logic
Modal Logic
Model Checking
Proof Theory
Theorem Proving
Algebra
Computer Algebra
ℝ Algebraic Geometry
Differential Algebra
Lie Algebra
Analysis
Differential Equations
Carathédory Solutions
Viscosity PDE Solutions
Dynamical Systems
Algorithms
Closure Ordinals
Fixpoints & Lattices
Proof Search Procedures
Decision Procedures
Numerics
Numerical Integration
Error Analysis
Weierstraß Approx-imation
Hermite Interpolation
Stochastics
Doob's Super-martingales
Dynkin's Infinitesimal Generators
Differential Generators
Stochastic Differential Equations


André Platzer
Logical Foundations of Cyber-Physical Systems
Springer


André Platzer
Logical Analysis of Hybrid Systems
Proving Theorems for Complex Dynamics
Springer

Differential Dynamic Logic dL: Syntax

Definition (Hybrid program α)

$$x := f(x) \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^*$$

Definition (dL Formula P)

$$e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle\alpha\rangle P$$

JAR'08,LICS'12,JAR'17

Discrete Assign | Test Condition | Differential Equation | Nondet. Choice | Seq. Compose | Nondet. Repeat

Definition (Hybrid program α)

$$x := f(x) \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^*$$

Definition (dL Formula P)

$$e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle\alpha\rangle P$$

All Reals | Some Reals | All Runs | Some Runs

JAR'08,LICS'12,JAR'17

Differential Dynamic Logic dL: Semantics

Definition (Hybrid program semantics) ($[\![\cdot]\!] : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S})$)

$$
\begin{aligned}
[\![x := e]\!] &= \{(\omega, \nu) \,:\, \nu = \omega \text{ except } \nu[\![x]\!] = \omega[\![e]\!]\} \\
[\![?Q]\!] &= \{(\omega, \omega) \,:\, \omega \in [\![Q]\!]\} \\
[\![x' = f(x)]\!] &= \{(\varphi(0), \varphi(r)) \,:\, \varphi \models x' = f(x) \text{ for some duration } r\} \\
[\![\alpha \cup \beta]\!] &= [\![\alpha]\!] \cup [\![\beta]\!] \\
[\![\alpha ; \beta]\!] &= [\![\alpha]\!] \circ [\![\beta]\!] \\
[\![\alpha^*]\!] &= [\![\alpha]\!]^* = \bigcup_{n \in \mathbb{N}} [\![\alpha^n]\!]
\end{aligned}
$$

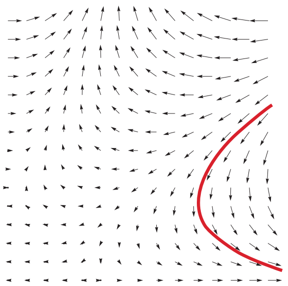
compositional semantics

Definition (dL semantics) ($[\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathscr{S})$)

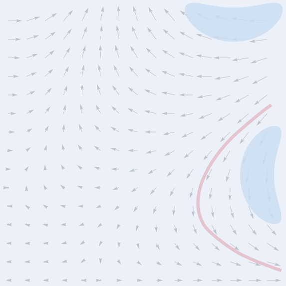
$$
\begin{aligned}
[\![e \geq \tilde{e}]\!] &= \{\omega \,:\, \omega[\![e]\!] \geq \omega[\![\tilde{e}]\!]\} \\
[\![\neg P]\!] &= [\![P]\!]^{\complement} \\
[\![P \wedge Q]\!] &= [\![P]\!] \cap [\![Q]\!] \\
[\![\langle\alpha\rangle P]\!] &= [\![\alpha]\!] \circ [\![P]\!] = \{\omega \,:\, \nu \in [\![P]\!] \text{ for some } \nu : (\omega, \nu) \in [\![\alpha]\!]\} \\
[\![[\alpha] P]\!] &= [\![\neg\langle\alpha\rangle\neg P]\!] = \{\omega \,:\, \nu \in [\![P]\!] \text{ for all } \nu : (\omega, \nu) \in [\![\alpha]\!]\} \\
[\![\exists x\, P]\!] &= \{\omega \,:\, \omega_x^r \in [\![P]\!] \text{ for some } r \in \mathbb{R}\}
\end{aligned}
$$

Differential Invariants for Differential Equations

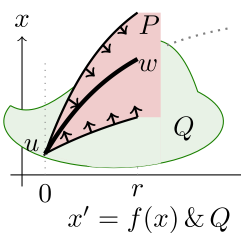
Differential Invariant

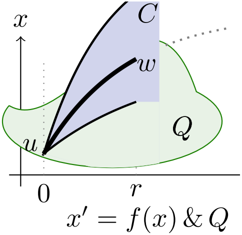


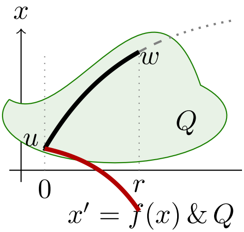
Differential Cut



Differential Ghost

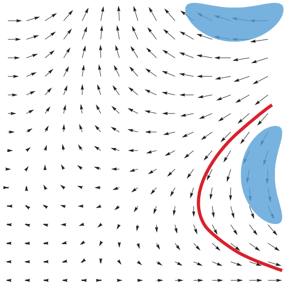




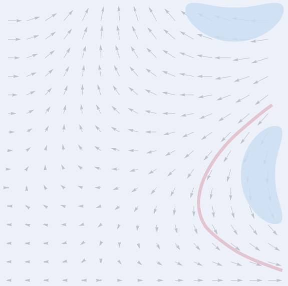


Differential Invariants for Differential Equations

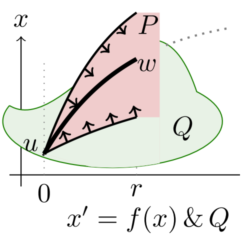
Differential Invariant

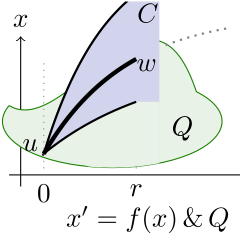


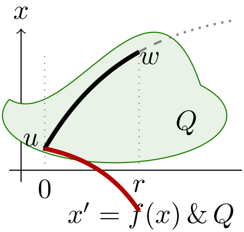
Differential Cut



Differential Ghost

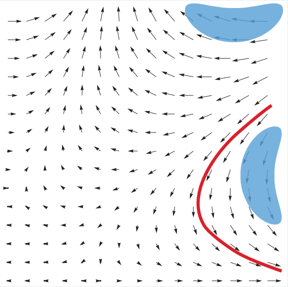




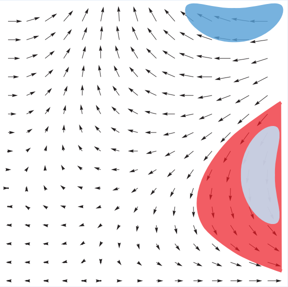


Differential Invariants for Differential Equations

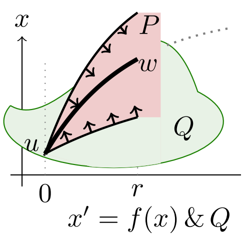
Differential Invariant

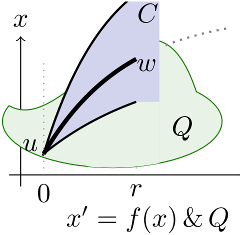


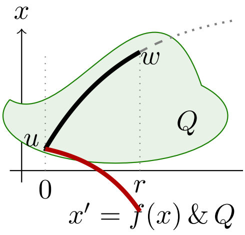
Differential Cut



Differential Ghost

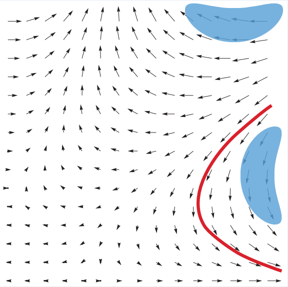




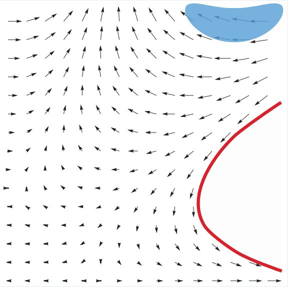


Differential Invariants for Differential Equations

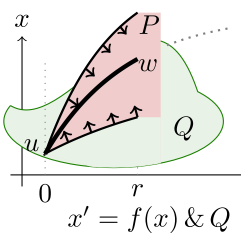
Differential Invariant

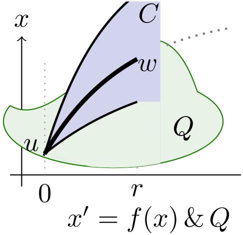


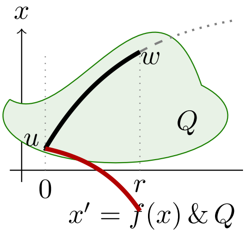
Differential Cut



Differential Ghost

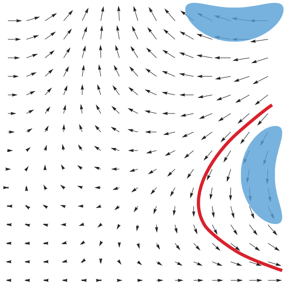




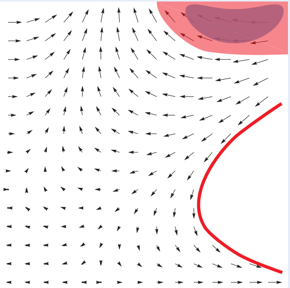


Differential Invariants for Differential Equations

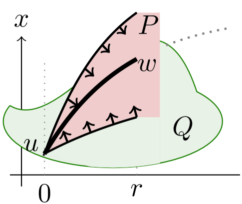
Differential Invariant



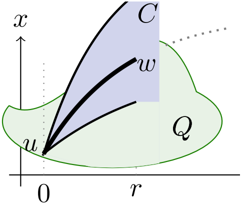
Differential Cut



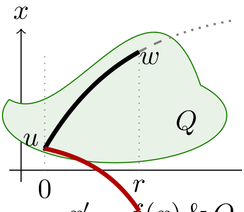
Differential Ghost



$x' = f(x) \,\&\, Q$



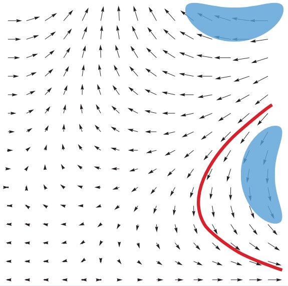
$x' = f(x) \,\&\, Q$

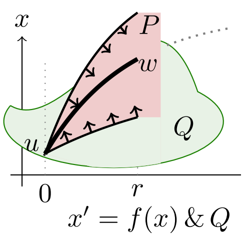


$x' = f(x) \,\&\, Q$

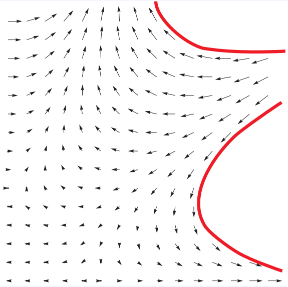
Differential Invariants for Differential Equations

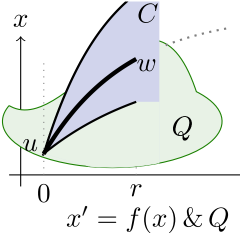
Differential Invariant



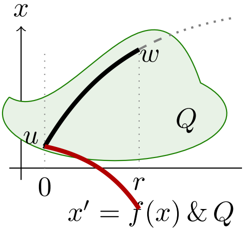


Differential Cut



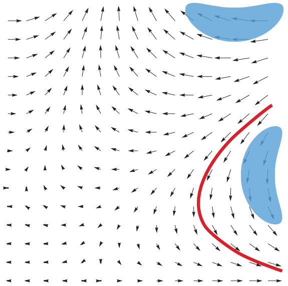


Differential Ghost

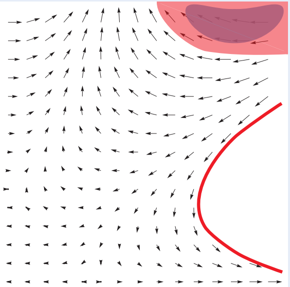


Differential Invariants for Differential Equations

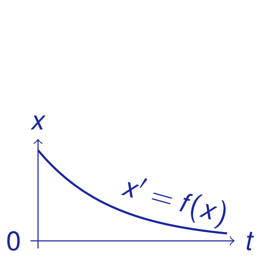
Differential Invariant

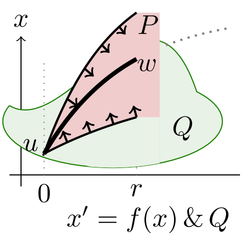


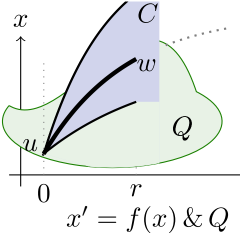
Differential Cut

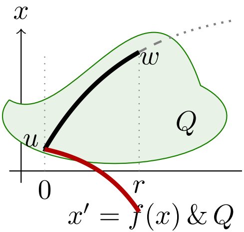


Differential Ghost



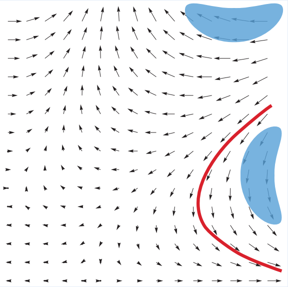




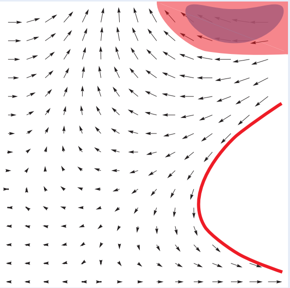


Differential Invariants for Differential Equations

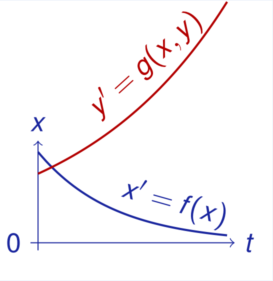
Differential Invariant

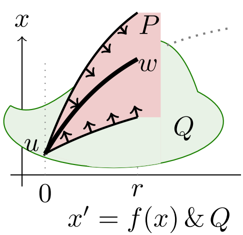


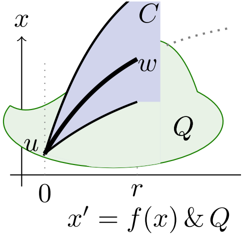
Differential Cut

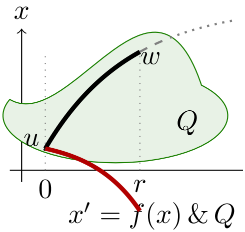


Differential Ghost



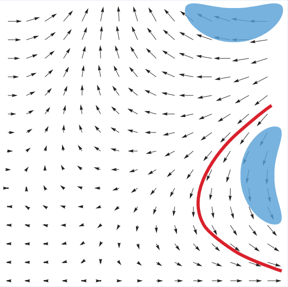




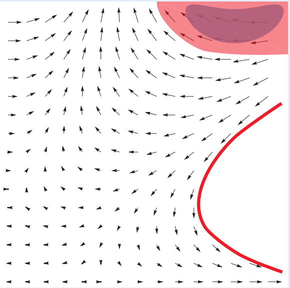


Differential Invariants for Differential Equations

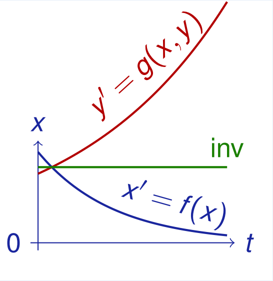
Differential Invariant

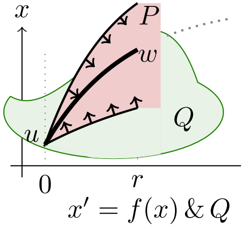


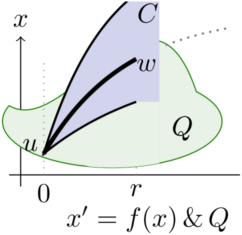
Differential Cut

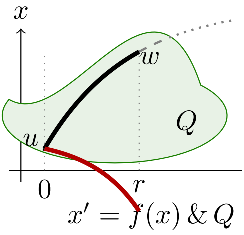


Differential Ghost









Differential Invariant

$$\frac{Q \vdash [x' := f(x)](P)'}{P \vdash [x' = f(x) \,\&\, Q]P}$$

Differential Cut

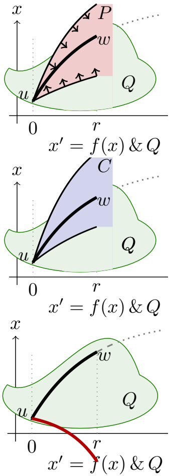
$$\frac{P \vdash [x' = f(x) \,\&\, Q]C \quad P \vdash [x' = f(x) \,\&\, Q \land C]P}{P \vdash [x' = f(x) \,\&\, Q]P}$$

Differential Ghost

$$\frac{P \leftrightarrow \exists y\, G \quad G \vdash [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \vdash [x' = f(x) \,\&\, Q]P}$$

deductive power added DI $\prec$ DI+DC $\prec$ DI+DC+DG

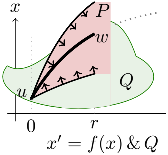
$$\omega[\![(e)']\!] = \sum_x \omega(x') \frac{\partial [\![e]\!]}{\partial x}(\omega)$$



Springer'10, LMCS'12, LICS'12,JAR'17,LICS'18,JACM'20

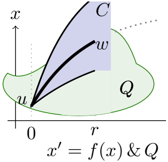
Differential Invariant

$$\frac{Q \vdash [x' := f(x)](P)'}{P \vdash [x' = f(x) \,\&\, Q]P}$$



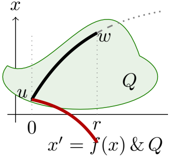
Differential Cut

$$\frac{P \vdash [x' = f(x) \,\&\, Q]C \quad P \vdash [x' = f(x) \,\&\, Q \land C]P}{P \vdash [x' = f(x) \,\&\, Q]P}$$



Differential Ghost

$$\frac{P \leftrightarrow \exists y\, G \quad G \vdash [x' = f(x), y' = g(x,y) \,\&\, Q]G}{P \vdash [x' = f(x) \,\&\, Q]P}$$



if $g(x,y) = a(x)y + b(x)$, so has long solution!

Springer'10, LMCS'12, LICS'12,JAR'17,LICS'18,JACM'20

André Platzer.
Logical Foundations of Cyber-Physical Systems.
Springer, Cham, 2018.
doi:10.1007/978-3-319-63588-0.

André Platzer.
The logical path to autonomous cyber-physical systems.
In David Parker and Verena Wolf, editors, *QEST*, volume 11785 of *LNCS*, pages 25–33. Springer, 2019.
doi:10.1007/978-3-030-30281-8_2.

Nathan Fulton and André Platzer.
Safe reinforcement learning via formal methods: Toward safe control through proof and learning.
In Sheila A. McIlraith and Kilian Q. Weinberger, editors, *AAAI*, pages 6485–6492. AAAI Press, 2018.

Nathan Fulton and André Platzer.
Verifiably safe off-model reinforcement learning.
In Tomas Vojnar and Lijun Zhang, editors, *TACAS, Part I*, volume 11427 of *LNCS*, pages 413–430. Springer, 2019.

doi:10.1007/978-3-030-17462-0_28.

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.
doi:10.1007/s10817-008-9103-8.

André Platzer.
Logics of dynamical systems.
In LICS [17], pages 13–24.
doi:10.1109/LICS.2012.13.

André Platzer.
A complete uniform substitution calculus for differential dynamic logic.
J. Autom. Reas., 59(2):219–265, 2017.
doi:10.1007/s10817-016-9385-1.

André Platzer.
The complete proof theory of hybrid systems.
In LICS [17], pages 541–550.
doi:10.1109/LICS.2012.64.

André Platzer and Yong Kiam Tan.
Differential equation axiomatization: The impressive power of differential ghosts.
In Anuj Dawar and Erich Grädel, editors, *LICS*, pages 819–828, New York, 2018. ACM.
doi:10.1145/3209108.3209147.

André Platzer and Yong Kiam Tan.
Differential equation invariance axiomatization.
J. ACM, 67(1):6:1–6:66, 2020.
doi:10.1145/3380825.

Stefan Mitsch and André Platzer.
ModelPlex: Verified runtime validation of verified cyber-physical system models.
Form. Methods Syst. Des., 49(1-2):33–74, 2016.
Special issue of selected papers from RV'14.
doi:10.1007/s10703-016-0241-z.

Jean-Baptiste Jeannin, Khalil Ghorbal, Yanni Kouskoulas, Aurora Schmidt, Ryan Gardner, Stefan Mitsch, and André Platzer.

A formally verified hybrid system for safe advisories in the next-generation airborne collision avoidance system.
STTT, 19(6):717–741, 2017.
doi:10.1007/s10009-016-0434-1.

Stefan Mitsch, Khalil Ghorbal, David Vogelbacher, and André Platzer.
Formal verification of obstacle avoidance and navigation of ground robots.
I. J. Robotics Res., 36(12):1312–1340, 2017.
doi:10.1177/0278364917733549.

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, Heidelberg, 2010.
doi:10.1007/978-3-642-14509-4.

André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput., 20(1):309–352, 2010.
doi:10.1093/logcom/exn070.

André Platzer.
The structure of differential invariants and differential cut elimination.
Log. Meth. Comput. Sci., 8(4:16):1–38, 2012.
doi:10.2168/LMCS-8(4:16)2012.

Logic in Computer Science (LICS), 2012 27th Annual IEEE Symposium on, Los Alamitos, 2012. IEEE.