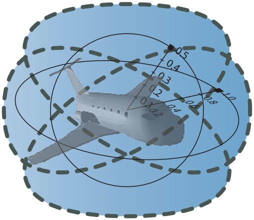
Logical Foundations of Cyber-Physical Systems

André Platzer

aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA

http://symbolaris.com/



Outline

Can you trust a computer to control physics?

Can you trust a computer to control physics?

Rationale

1. Safety guarantees require analytic foundations
2. Foundations revolutionized digital computer science & society
3. Need even stronger foundations when software reaches out into our physical world

Cyber-physical Systems

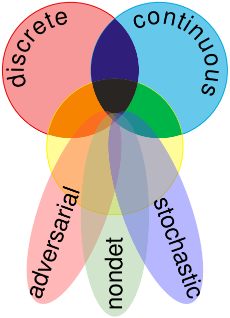
CPS combine cyber capabilities with physical capabilities to solve problems that neither part could solve alone.

How can we provide people with cyber-physical systems they can bet their lives on? — Jeannette Wing

CPS are Multi-Dynamical Systems

CPS Dynamics

CPS are characterized by multiple facets of dynamical systems.



CPS Compositions

CPS combine multiple simple dynamical effects.

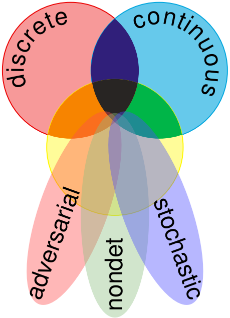
Tame Parts

Exploiting compositionality tames CPS complexity.

CPS are Multi-Dynamical Systems

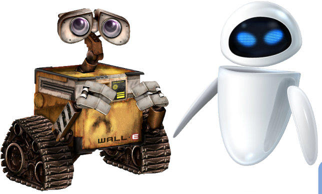
hybrid systems

HS = discrete + ODE



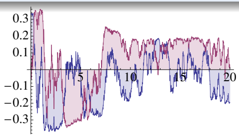
hybrid games

HG = HS + adversary



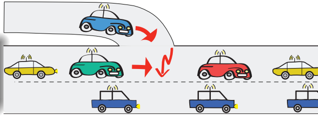
stochastic hybrid sys.

SHS = HS + stochastics



distributed hybrid sys.

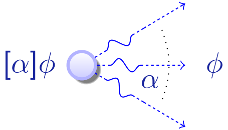
DHS = HS + distributed

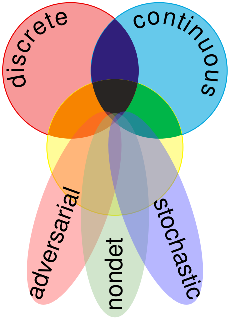


Family of Differential Dynamic Logics

differential dynamic logic

$\mathsf{d}\mathcal{L} = \mathsf{DL} + \mathsf{HP}$



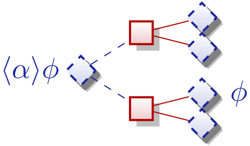


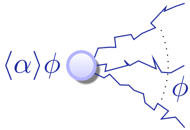
differential game logic

$\mathsf{dG}\mathcal{L} = \mathsf{GL} + \mathsf{HG}$

stochastic differential DL

$\mathsf{Sd}\mathcal{L} = \mathsf{DL} + \mathsf{SHP}$





quantified differential DL

$\mathsf{Qd}\mathcal{L} = \mathsf{FOL} + \mathsf{DL} + \mathsf{QHP}$

JAR'08,CADE'11,LMCS'12,LICS'12,LICS'12

Differential Dynamic Logic: Axiomatization

equations of truth

$[:=]$ $[x := \theta]\phi(x) \leftrightarrow \phi(\theta)$

$[?]$ $[?H]\phi \leftrightarrow (H \rightarrow \phi)$

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

$[\cup]$ $[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \land [\beta]\phi$

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

$[^*]$ $[\alpha^*]\phi \leftrightarrow \phi \land [\alpha][\alpha^*]\phi$

K $[\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$

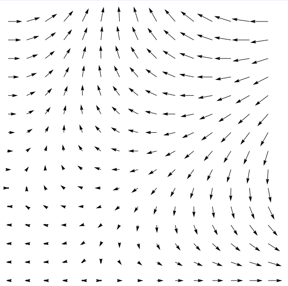
I $[\alpha^*](\phi \rightarrow [\alpha]\phi) \rightarrow (\phi \rightarrow [\alpha^*]\phi)$

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

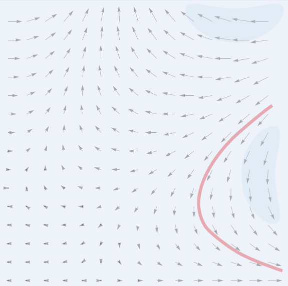
LICS'12

Differential Invariants for Differential Equations

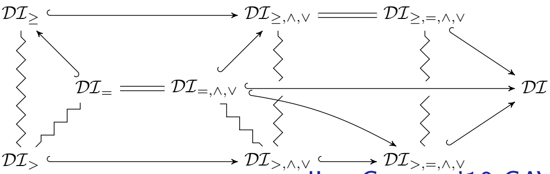
Differential Invariant



Differential Cut



Differential Ghost



Logic

Provability theory

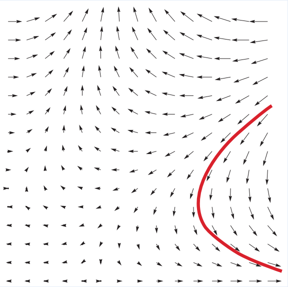
Math

Character-istic PDE

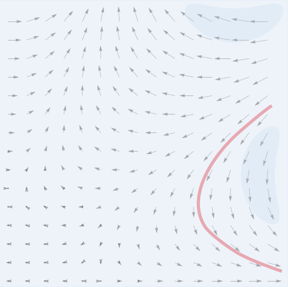
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

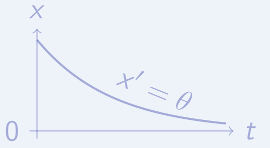
Differential Invariant

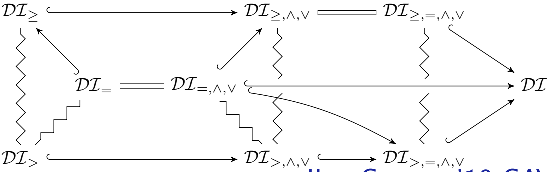


Differential Cut



Differential Ghost





Logic

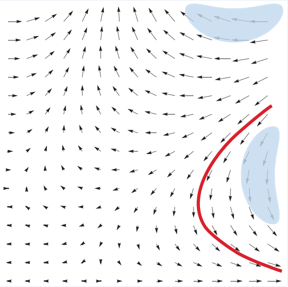
Provability theory

Math

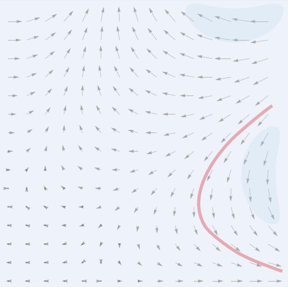
Characteristic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

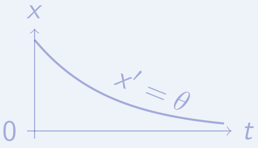
Differential Invariant

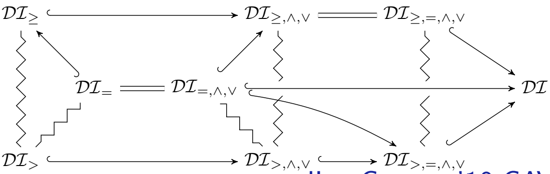


Differential Cut



Differential Ghost





Logic

Provability theory

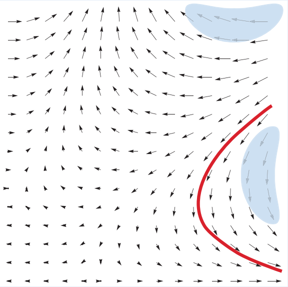
Math

Character-istic PDE

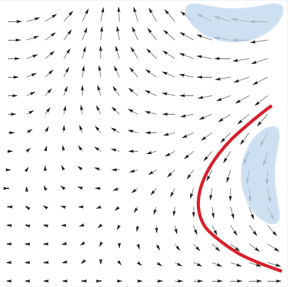
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

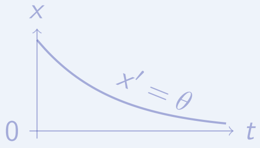
Differential Invariant

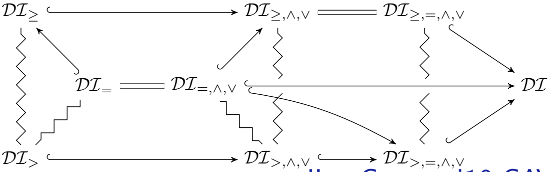


Differential Cut



Differential Ghost





Logic

Provability theory

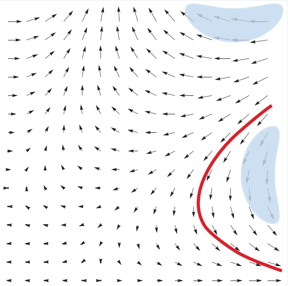
Math

Character-istic PDE

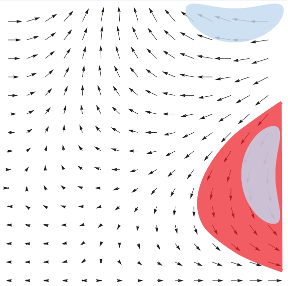
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

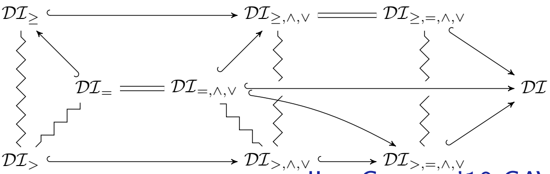
Differential Invariant



Differential Cut



Differential Ghost



Logic

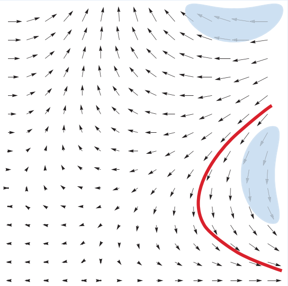
Provability theory

Math

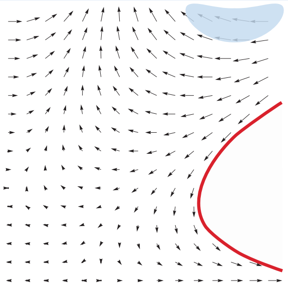
Characteristic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

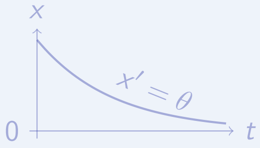
Differential Invariant

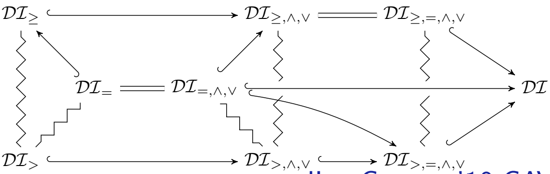


Differential Cut



Differential Ghost





Logic

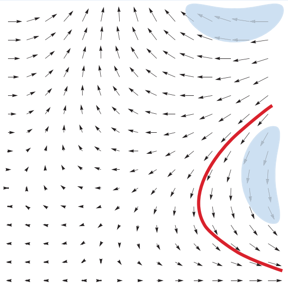
Provability theory

Math

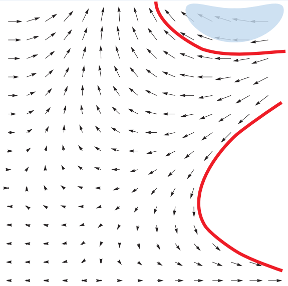
Character-istic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

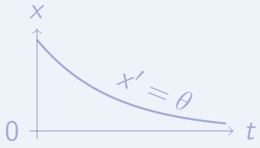
Differential Invariant

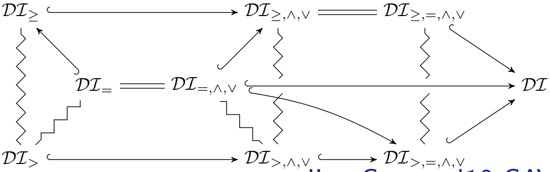


Differential Cut



Differential Ghost





Logic

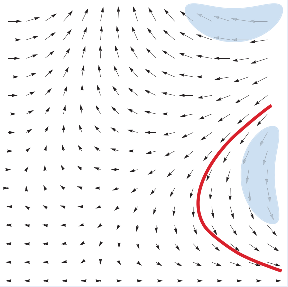
Provability theory

Math

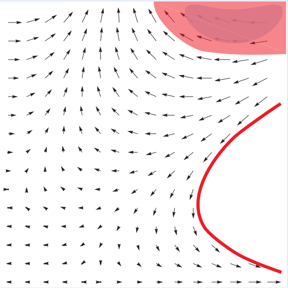
Character-istic PDE

JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

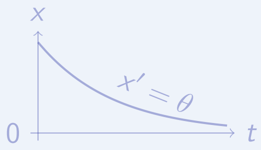
Differential Invariant

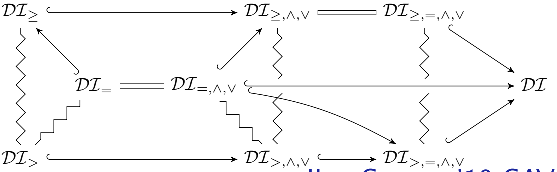


Differential Cut



Differential Ghost





Logic

Provability theory

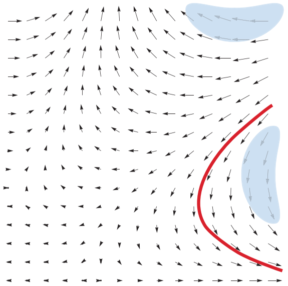
Math

Character-istic PDE

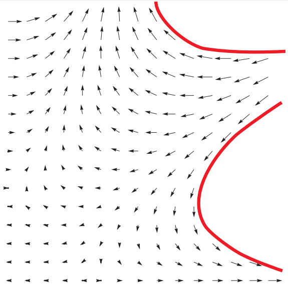
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

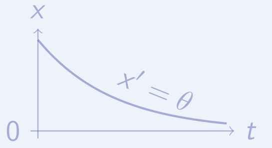
Differential Invariant

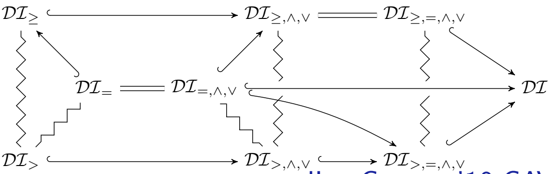


Differential Cut



Differential Ghost





Logic

Provability theory

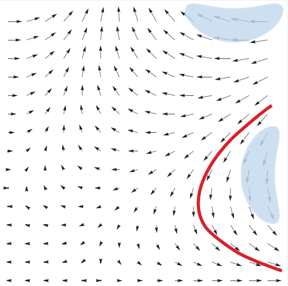
Math

Characteristic PDE

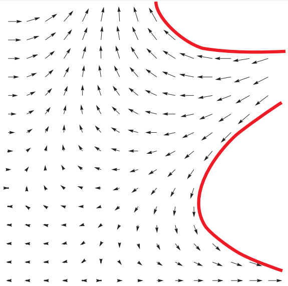
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

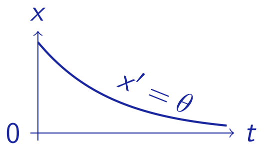
Differential Invariant

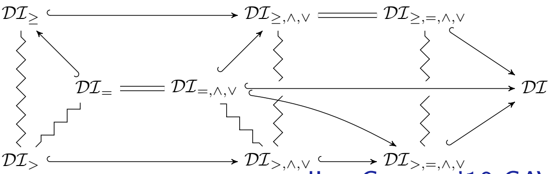


Differential Cut



Differential Ghost





Logic

Provability theory

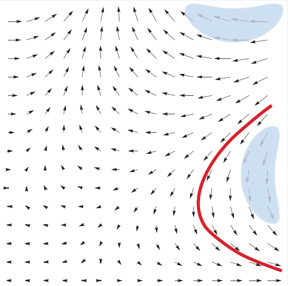
Math

Character-istic PDE

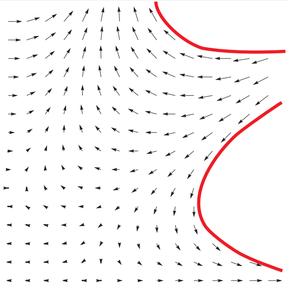
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

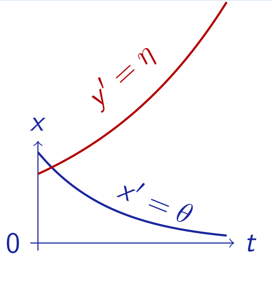
Differential Invariant

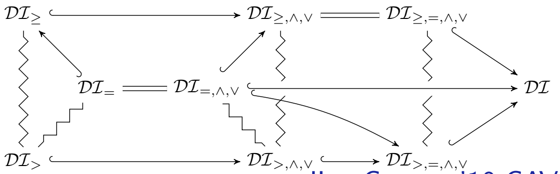


Differential Cut



Differential Ghost





Logic

Provability theory

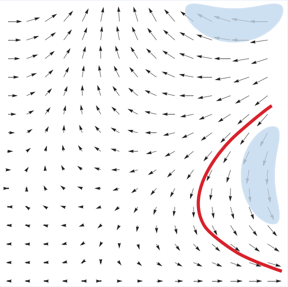
Math

Character-istic PDE

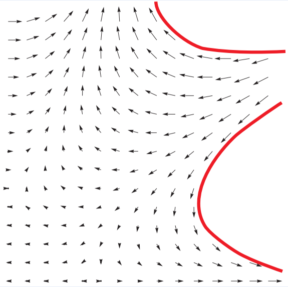
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Differential Invariants for Differential Equations

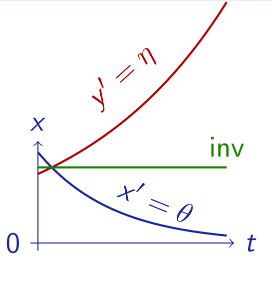
Differential Invariant



Differential Cut



Differential Ghost



$$
\begin{tikzcd}
\mathcal{DI}_{\geq} \arrow[rrr, hook] \arrow[dd, squiggly, dash] & & & \mathcal{DI}_{\geq,\wedge,\vee} \arrow[r, equal] \arrow[dd, squiggly, dash] & \mathcal{DI}_{\geq,=,\wedge,\vee} \arrow[dr, hook] \arrow[dd, squiggly, dash] & \\
& \mathcal{DI}_{=} \arrow[ul, hook] \arrow[r, equal] & \mathcal{DI}_{=,\wedge,\vee} \arrow[ur, hook] \arrow[rrr, hook] \arrow[drr, hook] & & & \mathcal{DI} \\
\mathcal{DI}_{>} \arrow[rrr, hook] & & & \mathcal{DI}_{>,\wedge,\vee} \arrow[r, hook] & \mathcal{DI}_{>,=,\wedge,\vee} \arrow[ur, hook] &
\end{tikzcd}
$$

Logic

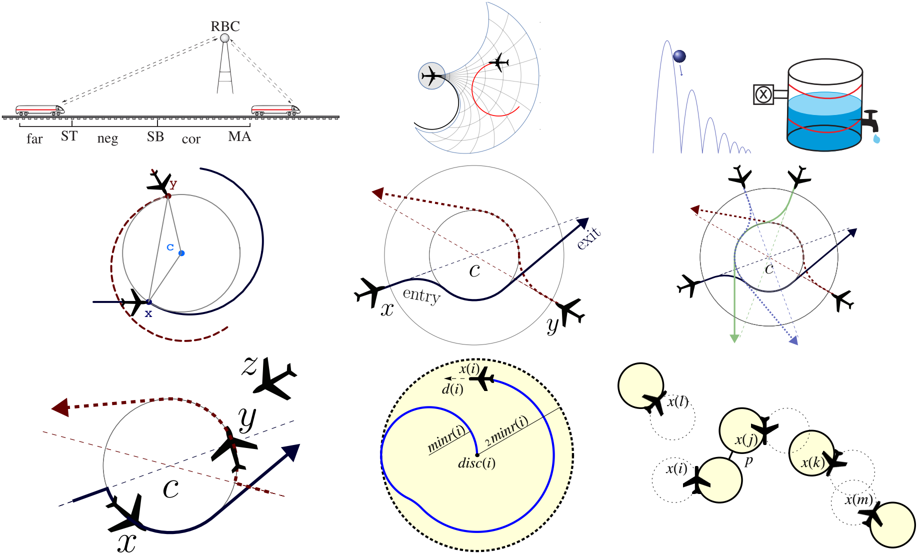
Provability theory

Math

Character-istic PDE

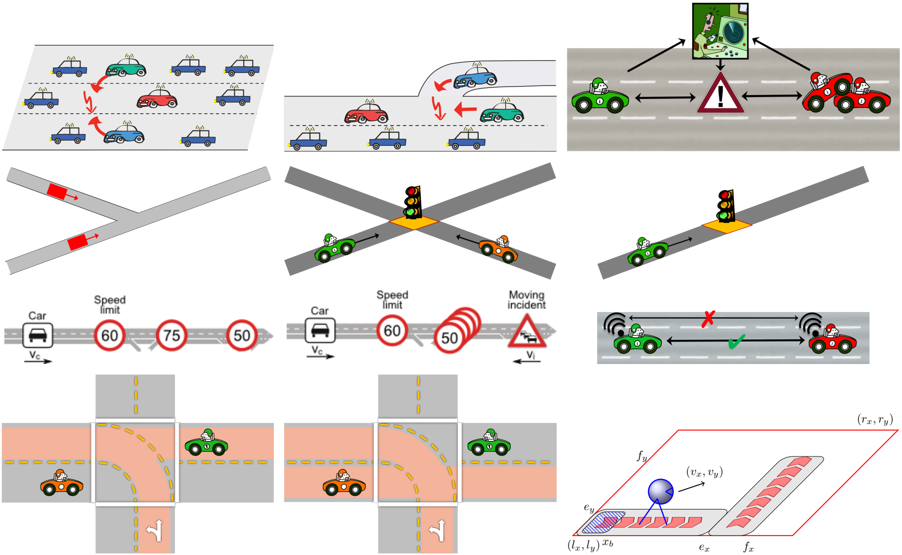
JLogComput'10,CAV'08,FMSD'09,LMCS'12,ITP'12

Successful CPS Proofs



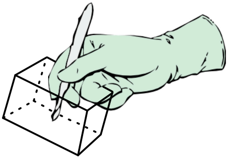
ICFEM'09,JAIS'14,CAV'08,FM'09,HSCC'11,HSCC'13

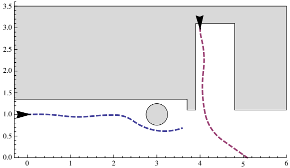
Successful CPS Proofs

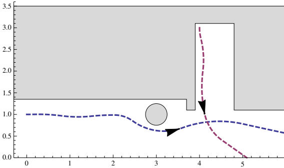


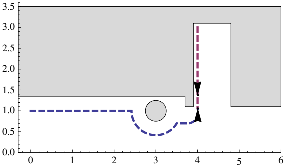
FM'11,LMCS'12,ICCPS'12,ITSC'11,ITSC'13,IJCAR'12

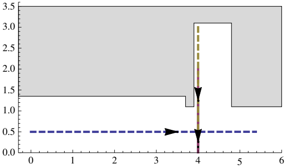
Successful CPS Proofs

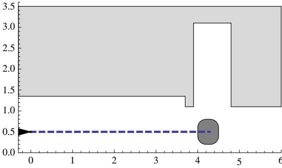


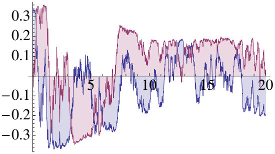


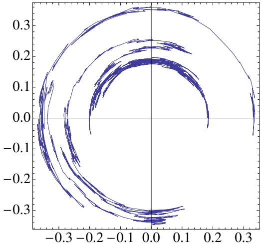


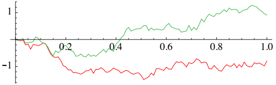




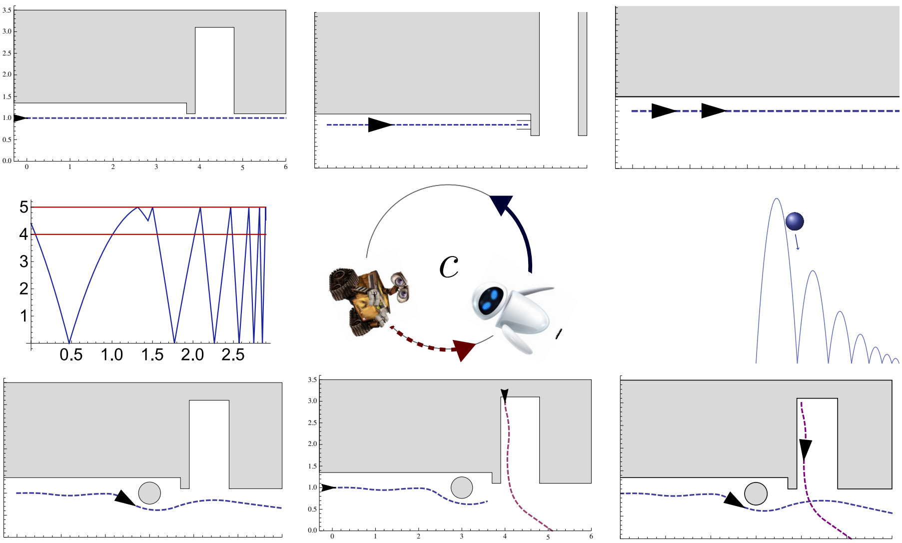








HSCC'13,RSS'13,CADE'12



15-424/624 *Foundations of Cyber-Physical Systems* students

Indicators for Success

Particularly successful applications:

- Parametric systems
- Structured systems
- Linear/nonlinear
- Dimension $\approx 1 \dots 20$ or ∞
- Principled system designs
- Systems understood by parts

More challenging if:

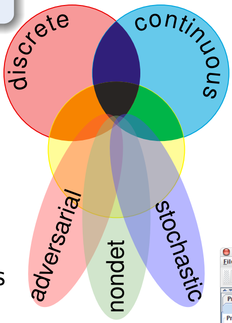
- System ill-structured
- Magic numbers in the models that are ill-understood
- Arithmetic becomes intangible

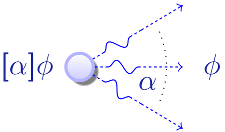
Important V&V Challenges

- Education & professional training
  $\rightsquigarrow$ make a big difference
- Tame curse of dimensionality
  $\rightsquigarrow$ not as big an issue in symbolic methods but ultimately happens
- Combine sound reasoning with aggressive optimizations
- Gradual verification
- Formal proofs for nonlinear real arithmetic
- Augment system structures to simplify V&V
- Leverage designer insights during V&V
  $\rightsquigarrow$ Analysis is part of the design, not a separate afterthought

differential dynamic logic

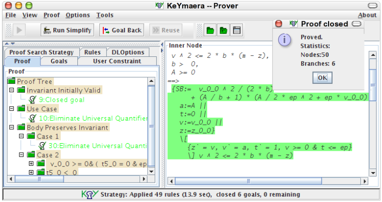
$$d\mathcal{L} = \text{DL} + \text{HP}$$

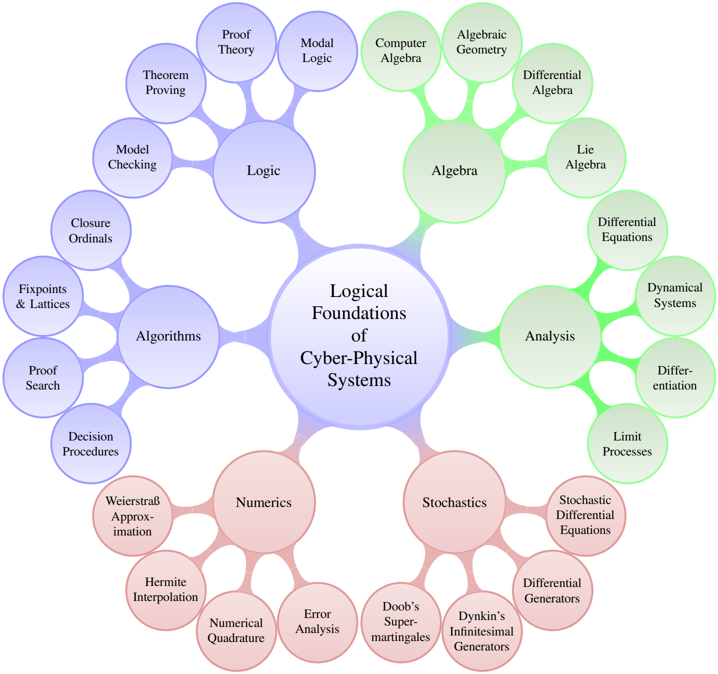


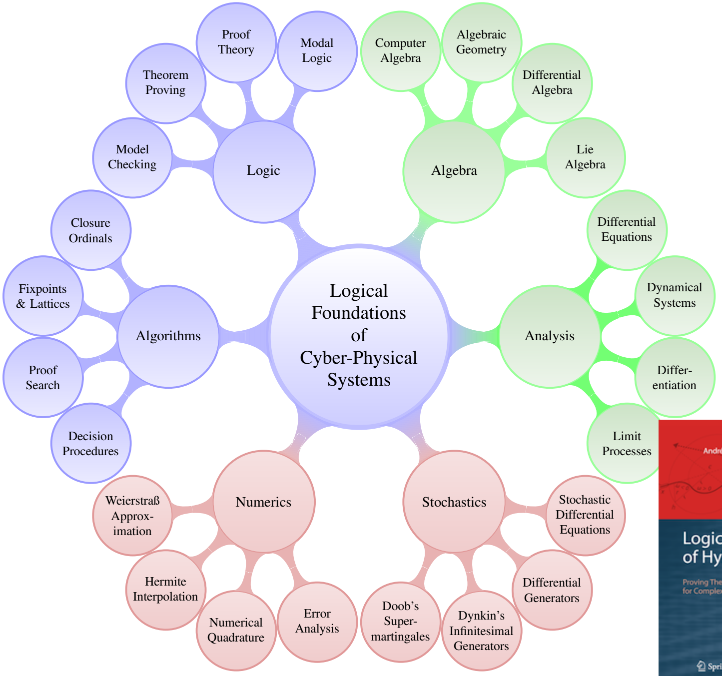


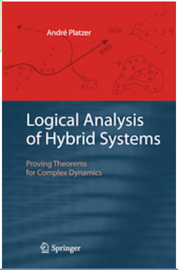
- Multi-dynamical systems
- Combine simple dynamics
- Tame complexity
- Logic & proofs for CPS
- Theory of CPS
- Applications

KeYmaera




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


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


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

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

André Platzer.
Foundations of cyber-physical systems.
Lecture Notes 15-424/624, Carnegie Mellon University, 2013.
URL: http://www.cs.cmu.edu/~aplatzer/course/fcps13/fcps13.pdf.

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.
A complete axiomatization of quantified differential dynamic logic for distributed hybrid systems.

Logical Methods in Computer Science, 8(4):1–44, 2012.
Special issue for selected papers from CSL'10.
doi:10.2168/LMCS-8(4:17)2012.

André Platzer.
Stochastic differential dynamic logic for stochastic hybrid programs.
In Nikolaj Bjørner and Viorica Sofronie-Stokkermans, editors, *CADE*, volume 6803 of *LNCS*, pages 431–445. Springer, 2011.
doi:10.1007/978-3-642-22438-6_34.

André Platzer.
A complete axiomatization of differential game logic for hybrid games.
Technical Report CMU-CS-13-100R, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, January, Revised and extended in July 2013.

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.
The complete proof theory of hybrid systems.
In LICS [13], pages 541–550.
doi:10.1109/LICS.2012.64.

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 and Edmund M. Clarke.
Computing differential invariants of hybrid systems as fixedpoints.
Form. Methods Syst. Des., 35(1):98–120, 2009.
Special issue for selected papers from CAV'08.
doi:10.1007/s10703-009-0079-8.

André Platzer.
The structure of differential invariants and differential cut elimination.
Logical Methods in Computer Science, 8(4):1–38, 2012.
doi:10.2168/LMCS-8(4:16)2012.

André Platzer.
A differential operator approach to equational differential invariants.
In Lennart Beringer and Amy Felty, editors, *ITP*, volume 7406 of *LNCS*, pages 28–48. Springer, 2012.
doi:10.1007/978-3-642-32347-8_3.

Proceedings of the 27th Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2012, Dubrovnik, Croatia, June 25–28, 2012.
IEEE, 2012.