Differential Equation Axiomatization
The Impressive Power of Differential Ghosts

André Platzer    Yong Kiam Tan

Carnegie Mellon University
Computer Science Department
1. Differential Dynamic Logic

2. Proofs for Differential Equations
   - Differential Invariants / Cuts / Ghosts

3. Completeness for Differential Equation Invariants
   - Darboux are Differential Ghosts
   - Derived Semialgebraic Invariants
   - Real Induction
   - Derived Local Progress
   - Completeness for Invariants

4. Summary
Fixed law describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)
Contributions: Differential Equation Axiomatization

- Classical approach: ① Given ODE ② Solve ODE ③ Analyze solution
- Descriptive power of ODEs: ODE much easier than its solution
- Analyzing ODEs via their solutions undoes their descriptive power!

\[
\text{describe ODE } \leftarrow \text{ analyze ODE} \quad \quad \text{Poincaré 1881}
\]

\[
\begin{align*}
\text{describe solution} & \leftarrow \text{ analyze solution} \\
\text{Now: Logical foundations of differential equation invariants} \\
\text{Identify axioms for differential equations} \\
\text{Completeness for differential equation invariants} \\
\text{Uniformly substitutable axioms, not infinite axiom schemata} \\
\text{Decide invariance by proof}
\end{align*}
\]
Outline

1. Differential Dynamic Logic

2. Proofs for Differential Equations
   - Differential Invariants / Cuts / Ghosts

3. Completeness for Differential Equation Invariants
   - Darboux are Differential Ghosts
   - Derived Semialgebraic Invariants
   - Real Induction
   - Derived Local Progress
   - Completeness for Invariants

4. Summary
\[ u^2 \leq \frac{v^2}{2} + \frac{9}{2} \rightarrow [u' = -v + \frac{u}{4}(1-u^2-v^2), v' = u + \frac{v}{4}(1-u^2-v^2)] \]

\[ u^2 + v^2 = 1 \rightarrow [u' = -v + \frac{u}{4}(1-u^2-v^2), v' = u + \frac{v}{4}(1-u^2-v^2)] \]
1. Differential Dynamic Logic

2. Proofs for Differential Equations
   - Differential Invariants / Cuts / Ghosts

3. Completeness for Differential Equation Invariants
   - Darboux are Differential Ghosts
   - Derived Semialgebraic Invariants
   - Real Induction
   - Derived Local Progress
   - Completeness for Invariants

4. Summary
Differential Invariants for Differential Equations

Differential Invariant

Differential Cut

Differential Ghost

\[ \frac{dx}{dt} = f(x) \]

\[ x' = f(x) & Q \]

\[ 0 \]

\[ 0 \]

\[ x = 0 \]

\[ x' = f(x) & Q \]

\[ 0 \]

\[ x = 0 \]

\[ x' = f(x) & Q \]

\[ 0 \]

\[ x = 0 \]

\[ x' = f(x) & Q \]

\[ 0 \]
Differential Invariants for Differential Equations

Differential Invariant

Differential Cut

Differential Ghost

\[ x' = f(x) \& Q \]

André Platzer, Yong Kiam Tan (CMU)
Differential Invariants for Differential Equations

Differential Invariant

Differential Cut

Differential Ghost

\[ x' = f(x) & Q \]

\[ x' = f(x) & Q \]

\[ x' = f(x) & Q \]

\[ x' = f(x) & Q \]

\[ x' = f(x) & Q \]
Differential Invariants for Differential Equations

Differential Invariant

\[ x' = f(x) \& Q \]

Differential Cut

\[ x' = f(x) \& Q \]

Differential Ghost

\[ x' = f(x) \& Q \]

\[ x = \text{function of } t \]

\[ 0 \]

\[ t \]

\[ x \]

\[ u \]

\[ Q \]

\[ w \]

\[ r \]

\[ x' = f(x) \& Q \]

\[ x = \text{function of } t \]

\[ 0 \]

\[ t \]

\[ x \]

\[ u \]

\[ Q \]

\[ w \]

\[ r \]

\[ x' = f(x) \& Q \]

\[ x = \text{function of } t \]

\[ 0 \]

\[ t \]

\[ x \]

\[ u \]

\[ Q \]

\[ w \]

\[ r \]

\[ x' = f(x) \& Q \]

André Platzer, Yong Kiam Tan (CMU)

Differential Equation Axiomatization

LICS’18 5 / 18
Differential Invariants for Differential Equations

Differential Invariant

Differential Cut

Differential Ghost

\[
x' = f(x) \land Q
\]

\[
x = x(0)
\]

\[
x' = f(x) \land Q
\]

André Platzer, Yong Kiam Tan (CMU)
Differential Invariants for Differential Equations

Differential Invariant

\[ x' = f(x) & Q \]

Differential Cut

\[ x' = f(x) & Q \]

Differential Ghost

\[ x' = f(x) & Q \]
Differential Invariants for Differential Equations

**Differential Invariant**

- $x' = f(x) \& Q$
- $x'$ and $r$ are variables.
- $Q$ is a condition.

**Differential Cut**

- $x' = f(x) \& Q$
- $C$ is a cut set.

**Differential Ghost**

- $x' = f(x) \& Q$
- $G$ is a ghost set.

André Platzer, Yong Kiam Tan (CMU)

Differential Equation Axiomatization

LICS'18 5 / 18
Differential Invariants for Differential Equations

Differential Invariant

\[ x' = f(x) \land Q \]

Differential Cut

\[ x' = f(x) \land Q \]

Differential Ghost

\[ y' = g(x,y) \]

\[ x' = f(x) \land Q \]

\[ x' = f(x) \land Q \]

\[ x' = f(x) \land Q \]

André Platzer, Yong Kiam Tan (CMU)
Differential Invariants for Differential Equations

**Differential Invariant**

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

**Differential Cut**

\[
P \vdash [x' = f(x) \& Q]C \quad P \vdash [x' = f(x) \& Q \& C]P \\
\overline{P \vdash [x' = f(x) \& Q]P}
\]

**Differential Ghost**

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

deductive power adds \( \text{DI} \prec \text{DC} \prec \text{DG} \)

---

JLogComput’10, LMCS’12, LICS’12, JAR’17, LICS’18
Differential Invariants for Differential Equations

**Differential Invariant**

\[
Q \vdash [x' := f(x)](P)'
\]

\[
P \vdash [x' = f(x) & Q]P
\]

**Differential Cut**

\[
P \vdash [x' = f(x) & Q]C
\]

\[
P \vdash [x' = f(x) & Q \land C]P
\]

\[
P \vdash [x' = f(x) & Q]P
\]

**Differential Ghost**

\[
P \leftrightarrow \exists y \ G
\]

\[
G \vdash [x' = f(x), y' = g(x, y) & Q]G
\]

\[
P \vdash [x' = f(x) & Q]P
\]

if new \( y' = g(x, y) \) has long enough solution

André Platzer, Yong Kiam Tan (CMU)  
Differential Equation Axiomatization

JLogComput’10, LMCS’12, LICS’12, JAR’17, LICS’18
Outline

1. Differential Dynamic Logic

2. Proofs for Differential Equations
   - Differential Invariants / Cuts / Ghosts

3. Completeness for Differential Equation Invariants
   - Darboux are Differential Ghosts
   - Derived Semialgebraic Invariants
   - Real Induction
   - Derived Local Progress
   - Completeness for Invariants

4. Summary
Theorem (Algebraic Completeness) (LICS’18)

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

Theorem (Semialgebraic Completeness) (LICS’18)

\( dL \) calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations. They are decidable in \( dL \).
ODE Axiomatization: Derived Darboux Rules

Gaston Darboux 1878

Darboux equalities are DG

\[
Q \vdash p' = gp \\
p = 0 \vdash [x' = f(x) \& Q]p = 0
\]

\((g \in \mathbb{R}[x])\)

Definable \(p'\) for Lie-derivative w.r.t. ODE
Darboux equalities are DG

\[
\begin{align*}
Q & \vdash p' = gp \\
p = 0 & \vdash [x' = f(x) \& Q]p = 0 \\
\end{align*}
\]

\[
\begin{align*}
\vdash 2uu' + 2vv' &= 2(u^2 + v^2)(u^2 + v^2 - 1) \\
\vdash [u' &= -v - u + u^3 + uv^2] \\
\vdash [v' &= u - v + u^2v + v^3] u^2 + v^2 - 1 = 0
\end{align*}
\]
Darboux equalities are DG

\[
\begin{align*}
Q & \vdash p' = gp \\
p = 0 & \vdash [x' = f(x) \& Q]p = 0
\end{align*}
\quad (g \in \mathbb{R}[x])
\]

Proof Idea.

1. DG counterweight \( y' = -gy \) to reduce \( p = 0 \) to \( py = 0 \land y \neq 0 \).
2. DG counter-counterweight \( z' = gz \) to reduce \( y \neq 0 \) to \( yz = 1 \).
3. \( py = 0 \) and \( yz = 1 \) are now differential invariants by construction.
Darboux inequalities are DG

\[
\frac{Q \vdash p' \geq gp}{p \succeq 0 \vdash [x' = f(x) \& Q]p \succeq 0}
\]

\[g \in \mathbb{R}[x]\]
ODE Axiomatization: Derived Darboux Rules

Darboux inequalities are DG

\[ Q \vdash p' \geq gp \]
\[ p \geq 0 \vdash [x' = f(x) \& Q]p \geq 0 \]
\( (g \in \mathbb{R}[x]) \)

Proof Idea.

1. DG counterweight \( y' = -gy \) to reduce \( p \geq 0 \) to \( py \geq 0 \land y > 0 \).
2. DG counter-counterweight \( z' = \frac{g}{2}z \) to reduce \( y > 0 \) to \( yz^2 = 1 \).
3. \( yz^2 = 1 \) and (after DC with \( y > 0 \)) \( py \geq 0 \) are differential invariants by construction as \( (py)' = p'y - gyp \geq 0 \) from premise since \( y > 0 \).
Darboux inequalities are DG

\[ Q \vdash p' \geq gp \]

\[ p \succeq 0 \vdash [x' = f(x) \& Q]p \succeq 0 \]

\[ (g \in \mathbb{R}[x]) \]

\[ (1-u^2-v^2)' \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2) \]

\[ \ldots \vdash [u' = -v + \frac{u}{4}(1-u^2-v^2) \]

\[ v' = u + \frac{v}{4}(1-u^2-v^2) \]

\[ 1-u^2-v^2 > 0 \]
ODE Axiomatization: Derived Darboux Rules

Darboux inequalities are DG

\[ Q \vdash p' \geq gp \]
\[ p \succeq 0 \vdash [x' = f(x) \& Q] p \succeq 0 \quad (g \in \mathbb{R}[x]) \]

\[ y' = -gy \]
\[ yp = 1 \]
\[ p' = gp \]

\[ (1 - u^2 - v^2)' \geq -\frac{1}{2}(u^2 + v^2)(1 - u^2 - v^2) \]
\[ \ldots \vdash [u' = -v + \frac{u}{4}(1 - u^2 - v^2) \]
\[ v' = u + \frac{v}{4}(1 - u^2 - v^2) \]
\[ y' = \frac{1}{2}(u^2 + v^2)y \]
\[ 1 - u^2 - v^2 > 0 \]

\[ (1 - u^2 - v^2)y > 0 \]
Darboux inequalities are DG

\[ Q \vdash p' \geq gp \]
\[ p \geq 0 \vdash [x' = f(x) \& Q] p \geq 0 \]

\[ (1-u^2-v^2)' \geq -\frac{1}{2}(u^2+v^2)(1-u^2-v^2) \]
\[ \ldots \vdash \begin{cases} u' = -v + \frac{u}{4}(1-u^2-v^2) \\ v' = u + \frac{v}{4}(1-u^2-v^2) \\ y' = \frac{1}{2}(u^2+v^2)y \\ z' = -\frac{1}{4}(u^2+v^2)z \end{cases} \]

\[ 1-u^2-v^2 > 0 \]

\[ (1-u^2-v^2)y > 0 \]

\[ yz^2 = 1 \]
ODE Axiomatization: Derived Darboux Rules

Vectorial Darboux are VDG

\[ Q \vdash p' = Gp \]
\[ p = 0 \vdash [x' = f(x) \& Q]p = 0 \]

\( G \in \mathbb{R}[x]^{n \times n} \)

Definable \( p' \) for component-wise Lie-derivative w.r.t. ODE
ODE Axiomatization: Derived Darboux Rules

Vectorial Darboux are VDG

\[ Q \vdash p' = Gp \]
\[ p = 0 \vdash [x' = f(x) \& Q]p = 0 \]

(G ∈ ℝ[冪n×n])

Proof Idea.

1. DG counterweight \( y' = -G^Ty \) to change \( p = 0 \) to \( p \cdot y = 0 \).
2. But: \( p \cdot y = 0 \nRightarrow p = 0 \) even if \( y \neq 0 \).
3. Redo: time-varying independent DG matrix \( Y' = -YG \) with \( Yp = 0 \).
4. \( Yp = 0 \Rightarrow p = 0 \) if \( \det Y \neq 0 \).
5. DC \( \det Y \neq 0 \) which proves by dbx using Liouville’s identity:
   \[
   \det(Y)' = -\tr(G)\det(Y)
   \]
6. Continuous change of basis \( Y^{-1} \) balancing out motion of \( p \): constant!
7. Continuous change to new evolving variables is sound by DG.

Andre Platzer, Yong Kiam Tan (CMU)
Time is defined so that motion looks simple \( \approx \) Poincaré
Vectorial Darboux are VDG

\[ Q \vdash p' = Gp \]

\[ p = 0 \vdash [x' = f(x) \& Q]p = 0 \]
ODE Axiomatization: Derived Invariant Rules

**Vectorial Darboux are VDG**

\[ Q \vdash p' = Gp \]

\[ p = 0 \vdash [x' = f(x) \& Q]p = 0 \]

**Differential Radical Invariants are vdbx**

\[ \Gamma, Q \vdash \bigwedge_{i=0}^{N-1} p^{(i)} = 0 \quad Q \vdash p^{(N)} = \sum_{i=0}^{N-1} g_ip^{(i)} \]

\[ \Gamma \vdash [x' = f(x) \& Q]p = 0 \]
ODE Axiomatization: Derived Invariant Rules

Vectorial Darboux are VDG

\[ Q \vdash p' = Gp \]
\[ p = 0 \vdash [x' = f(x) \& Q]p = 0 \]

Differential Radical Invariants are vdbx

\[ \Gamma, Q \vdash \bigwedge_{i=0}^{N-1} p(i) = 0 \]
\[ Q \vdash p^{(N)} = \sum_{i=0}^{N-1} g_i p(i) \]
\[ \Gamma \vdash [x' = f(x) \& Q]p = 0 \]

Proof Idea.

by vdbx with \( G = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ g_0 & g_1 & \cdots & g_{N-2} & g_{N-1} \end{pmatrix} \), \( p = \begin{pmatrix} p \\ p^{(1)} \\ p^{(2)} \\ \vdots \\ p^{(N-1)} \end{pmatrix} \)
Vectorial Darboux are VDG

\[ Q \vdash p' = Gp \]
\[
\frac{p = 0}{x' = f(x) \& Q} p = 0
\]

Differential Radical Invariants are vdbx

\[
\Gamma, Q \vdash \bigwedge_{i=0}^{N-1} p^{(i)} = 0 \quad Q \vdash p^{(N)} = \sum_{i=0}^{N-1} g_i p^{(i)}
\]
\[
\Gamma \vdash [x' = f(x) \& Q] p = 0
\]

\[ p' = 0 \]

\[ N \text{ exists} \]
**ODE Axiomatization: Derived Invariant Rules**

**Vectorial Darboux are VDG**

\[
Q \vdash p' = Gp \\
\vdash [x' = f(x) \& Q]p = 0
\]

\(p'\) = 0

**Differential Radical Invariants are vdbx**

\[
\Gamma, Q \vdash \bigwedge_{i=0}^{N-1} p(i) = 0 \quad Q \vdash p^{(N)} = \sum_{i=0}^{N-1} g_i p^{(i)} \\
\vdash [x' = f(x) \& Q]p = 0
\]

\(N\) exists

**Semialgebraic Invariants are derived**

\[
p = 0 \vdash p' \geq 0 \quad \ldots \quad p = 0 \land \ldots \land p^{(N-2)} = 0 \vdash p^{(N-1)} \geq 0 \\
p \geq 0 \vdash [x' = f(x)]p \geq 0
\]

\(p'\) * \geq 0

---

André Platzer, Yong Kiam Tan (CMU)
ODE Axiomatization from Higher Derivatives and Ghosts

Local coordinates: \( \left( \frac{z}{2}, \frac{q}{4} \right) \)

Local coordinates: \( \left( \frac{z}{5}, \frac{6}{5} \right) \)

Proofs use continuously changing basis to keep invariants at constant local coordinates

Proofs with higher Lie derivatives

- \( p'' \) safe
- \( p'' \) inconcluci
- \( p' \) inconcluci

Sound and complete ODE invariance proofs
Semialgebraic invariants are derived

\[ P \models \bigvee_{i=0}^{M} \left( \bigwedge_{j=0}^{m(i)} p_{ij}^{\prime*} \geq 0 \land \bigwedge_{j=0}^{n(i)} q_{ij}^{\prime*} > 0 \right) \quad \neg P \models \bigvee_{i=0}^{N} \left( \bigwedge_{j=0}^{a(i)} r_{ij}^{\prime*} \geq 0 \land \bigwedge_{j=0}^{b(i)} s_{ij}^{\prime*} > 0 \right) \]

\[ P \models [x' = f(x)]P \]

\[ P \equiv \bigvee_{i=0}^{M} \left( \bigwedge_{j=0}^{m(i)} p_{ij} \geq 0 \land \bigwedge_{j=0}^{n(i)} q_{ij} > 0 \right) \quad \neg P \equiv \bigvee_{i=0}^{N} \left( \bigwedge_{j=0}^{a(i)} r_{ij} \geq 0 \land \bigwedge_{j=0}^{b(i)} s_{ij} > 0 \right) \]

\[ p^{\prime*} = 0 \equiv \bigwedge_{i=0}^{N-1} p^{(i)} = 0 \quad p^{\prime*} \geq 0 \equiv p^{\prime*} > 0 \lor p^{\prime*} = 0 \quad p^{(N)} = \sum_{i=0}^{N-1} g_i p^{(i)} \]

\[ q^{\prime*} > 0 \equiv q \geq 0 \land (q = 0 \rightarrow q' \geq 0) \land (q = 0 \land q' = 0 \rightarrow q^{(2)} \geq 0) \land \ldots \land (q = 0 \land q' = 0 \land \cdots \land q^{(N-2)} = 0 \rightarrow q^{(N-1)} > 0) \]

Definable \( p^{\prime*} \) for all/most significant Lie derivatives w.r.t. backwards ODE
Semialgebraic invariants are derived

\[
P \vdash M \bigvee_{i=0}^{M} \bigwedge_{j=0}^{m(i)} p_{ij}^{*}\]

\[
P \equiv \bigvee_{i=0}^{M} \bigwedge_{j=0}^{m(i)} p_{ij}^{*}
\]

Definition $p^{*}$ for all/most significant Lie derivatives w.r.t. backwards ODE
Extended Axiomatization for Semialgebraics

Real Induction

\[ [x' = f(x)]P \leftrightarrow \forall y [x' = f(x) & P \lor x = y] \]
\[ (x = y \to P \land \langle x' = f(x) & P \rangle \land x \neq y) \]

Continuous Existence

\[ p > 0 \to \langle x' = f(x) & p > 0 \rangle \circ \]

Unique Solutions

\[ \langle x' = f(x) & Q_1 \rangle P_1 \land \langle x' = f(x) & Q_2 \rangle P_2 \]
\[ \to \langle x' = f(x) & Q_1 \land Q_2 \rangle (P_1 \lor P_2) \]
ODE Axiomatization: Derived Local Progress Rules

Local Progress Step

\[ p > 0 \lor p = 0 \land \langle x' = f(x) & p' \geq 0 \rangle \circ \]

\[ \rightarrow \langle x' = f(x) & p \geq 0 \rangle \circ \]

Local Progress ≥

\[ p'^* \geq 0 \rightarrow \langle x' = f(x) & p \geq 0 \rangle \circ \]

Local Progress >

\[ p'^* > 0 \rightarrow \langle x' = f(x) & p > 0 \rangle \bigcirc \]
**Theorem (Algebraic Completeness) (LICS'18)**

\[ \text{dL calculus is a sound & complete axiomatization of algebraic invariants of polynomial differential equations. They are decidable with a derived axiom (on open Q for completeness):} \]

\[
(DRI) \quad [x' = f(x) & Q]p = 0 \iff (Q \rightarrow p'^* = 0)
\]

**Theorem (Semialgebraic Completeness) (LICS'18)**

\[ \text{dL calculus with RI is a sound & complete axiomatization of semialgebraic invariants of differential equations. They are decidable with derived axiom} \]

\[
(SAI) \quad \forall x (P \rightarrow [x' = f(x)]P) \iff \forall x (P \rightarrow P'^*) \land \forall x (\neg P \rightarrow (\neg P)'^*)
\]

Definable \( p'^* \) is short for *all/most significant* Lie derivatives w.r.t. ODE
Definable \( p'^*^- \) is w.r.t. backwards ODE. Also for DNF \( P \).
Outline

1. Differential Dynamic Logic

2. Proofs for Differential Equations
   - Differential Invariants / Cuts / Ghosts

3. Completeness for Differential Equation Invariants
   - Darboux are Differential Ghosts
   - Derived Semialgebraic Invariants
   - Real Induction
   - Derived Local Progress
   - Completeness for Invariants

4. Summary
Logical Foundation for Differential Equation Invariants

**differential dynamic logic**

dL = DL + HP

1. Poincaré: qualitative ODE
2. Complete axiomatization
3. Algebraic ODE invariants
4. Semialgebraic ODE invariants
5. Algebraic hybrid systems
6. Local ODE progress
7. Decide by dL proof/disproof
8. Uniform substitution axioms

**Properties**

1. MVT
2. Prefix
3. Picard-Lind
4. R-complete
5. Existence
6. Uniqueness

1. Differential invariants
2. Differential cuts
3. Differential ghosts
4. Real induction
5. Continuous existence
6. Unique solutions

Impressive power of differential ghosts
Differential Equation Axiomatization vs. Derived Rules
### Part: Elementary Cyber-Physical Systems
1. Differential Equations & Domains
2. Choice & Control
3. Safety & Contracts
4. Dynamical Systems & Dynamic Axioms
5. Truth & Proof
6. Control Loops & Invariants
7. Events & Responses
8. Reactions & Delays

### Part: Differential Equations Analysis
9. Differential Equations & Differential Invariants
10. Differential Equations & Proofs
11. Ghosts & Differential Ghosts
12. Differential Invariants & Proof Theory

### Part: Adversarial Cyber-Physical Systems
13-16. Hybrid Systems & Hybrid Games

### Part: Comprehensive CPS Correctness
André Platzer and Yong Kiam Tan.
Differential equation axiomatization: The impressive power of
differential ghosts.
York, 2018. ACM.

André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.

André Platzer.
The structure of differential invariants and differential cut elimination.

André Platzer.
A complete uniform substitution calculus for differential dynamic logic.
André Platzer.

Logical Foundations of Cyber-Physical Systems.
URL: http://www.springer.com/978-3-319-63587-3,
doi:10.1007/978-3-319-63588-0.