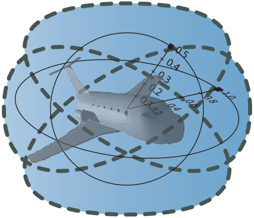
A Uniform Substitution Calculus for Differential Dynamic Logic

André Platzer

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

The Secret for Simpler Sound Hybrid Systems Provers



Outline

Outline

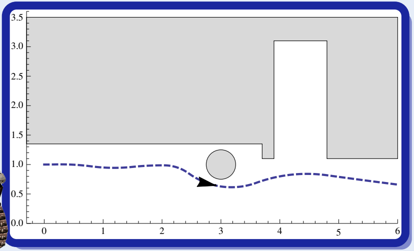
1. Cyber-Physical Systems
2. Uniform Substitution Calculus for Differential Dynamic Logic
   - Uniform Substitution Calculus
   - Axiom vs. Axiom Schemata
   - Uniform Substitutions
   - Differential Axioms
   - Examples
3. Differential-form Differential Dynamic Logic
   - Semantics: Local
   - Differential Substitution Lemmas
   - Static Semantics
4. Summary

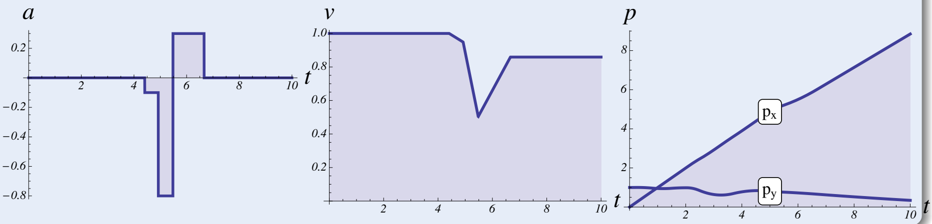
CPS Analysis

Challenge (CPS)

Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



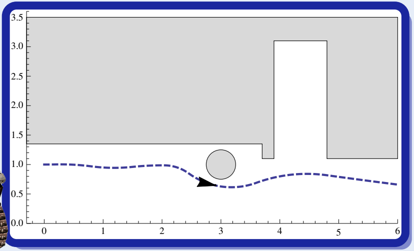


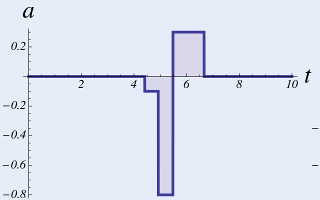
CPS Analysis

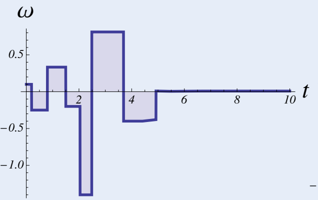
Challenge (CPS)

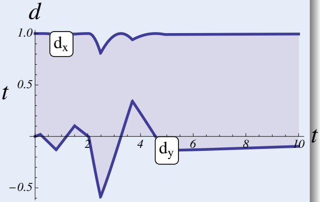
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



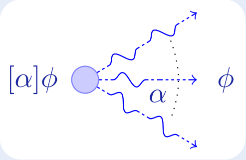






CPS Analysis

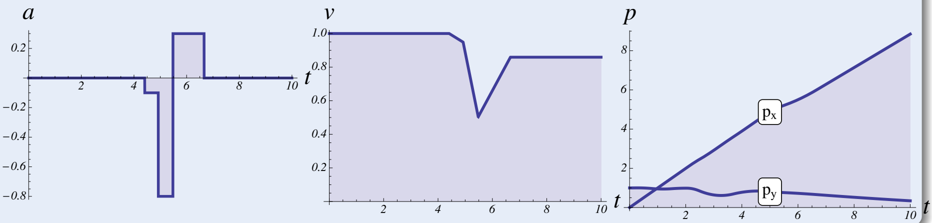
Differential Dynamic Logic



Seq. Compose

Nondet. Repeat

$$\underbrace{x \neq o \wedge b > 0}_{\text{init}} \to \Big[\Big(\underbrace{\texttt{if}(\text{tooClose}(x,o))\ a := -b}_{\text{discrete control}} \;;\; \underbrace{x' = v, v' = a}_{\text{ODE}}\Big)^*\Big]\underbrace{x \neq o}_{\text{post}}$$



Key Contributions

Q: How to build a prover with a small soundness-critical core?
A: Uniform substitution [Church]

Q: How to enable flexible yet sound reasoning?
A: Axioms with local meaning [Philosophy, Algebraic Geometry]

Q: What's the local meaning of a differential equation?
A: Differential forms [Differential Geometry]

Q: How to do hybrid systems proving?
A: Uniform substitution calculus for differential dynamic logic

Q: What's the impact of uniform substitution on a prover core?
A: 65 989 ↘ 1 682 LOC (2.5%) [KeYmaera X]

Outline

1. Cyber-Physical Systems

2. Uniform Substitution Calculus for Differential Dynamic Logic
   - Uniform Substitution Calculus
   - Axiom vs. Axiom Schemata
   - Uniform Substitutions
   - Differential Axioms
   - Examples

3. Differential-form Differential Dynamic Logic
   - Semantics: Local
   - Differential Substitution Lemmas
   - Static Semantics

4. Summary

Differential Dynamic Logic: Comparison

$[x := f]p(x) \leftrightarrow p(f)$	[:=]	$[x := \theta]\phi(x) \leftrightarrow \phi(\theta)$
$[?q]p \leftrightarrow (q \rightarrow p)$	[?]	$[?H]\phi \leftrightarrow (H \rightarrow \phi)$
$[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})$	[∪]	$[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \land [\beta]\phi$
$[a; b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$	[;]	$[\alpha; \beta]\phi \leftrightarrow [\alpha][\beta]\phi$
$[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \land [a][a^*]p(\bar{x})$	[*]	$[\alpha^*]\phi \leftrightarrow \phi \land [\alpha][\alpha^*]\phi$
$[a](p(\bar{x}) \rightarrow q(\bar{x})) \rightarrow ([a]p(\bar{x}) \rightarrow [a]q(\bar{x}))$	K	$[\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$
$[a^*](p(\bar{x}) \rightarrow [a]p(\bar{x})) \rightarrow (p(\bar{x}) \rightarrow [a^*]p(\bar{x}))$	I	$[\alpha^*](\phi \rightarrow [\alpha]\phi) \rightarrow (\phi \rightarrow [\alpha^*]\phi)$
$p \rightarrow [a]p$	V	$\phi \rightarrow [\alpha]\phi$
	[']	$[x' = \theta]\phi \leftrightarrow \forall t \geq 0\, [x := x(t)]\phi$
CADE'15		LICS'12

Differential Dynamic Logic: Comparison

$[x := f]p(x) \leftrightarrow p(f)$	[:=]	$[x := \theta]\phi(x) \leftrightarrow \phi(\theta)$
$[?q]p \leftrightarrow (q \rightarrow p)$ Axiom	[?]	$[?H]\phi \leftrightarrow (H \rightarrow \phi)$ Schema
$[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \wedge [b]p(\bar{x})$	[∪]	$[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$
$[a; b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$	[;]	$[\alpha; \beta]\phi \leftrightarrow [\alpha][\beta]\phi$
$[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \wedge [a][a^*]p(\bar{x})$	[*]	$[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha][\alpha^*]\phi$
$[a](p(\bar{x}) \rightarrow q(\bar{x})) \rightarrow ([a]p(\bar{x}) \rightarrow [a]q(\bar{x}))$	K	$[\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$
$[a^*](p(\bar{x}$ Axiom $p(\bar{x})) \rightarrow (p(\bar{x}) \rightarrow [a^*]p(\bar{x}))$	I	$[\alpha^*](\phi$ Schema $\rightarrow (\phi \rightarrow [\alpha^*]\phi)$
$p \rightarrow [a]p$	V	$\phi \rightarrow [\alpha]\phi$
	[']	$[x' = \theta]\phi \leftrightarrow \forall t \geq 0\, [x := x(t)]\phi$
CADE'15		LICS'12

Axiom vs. Axiom Schemata

Axiom

$[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})$

Schema

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

Axiom

$p \rightarrow [a]p$

Schema

$\phi \rightarrow [\alpha]\phi \ldots$

Axiom vs. Axiom Schemata

Axiom

$[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})$

Schema

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

Pattern match formulas for shape $\alpha \cup \beta$

Placeholder α schema variable matcher

Same instance of ϕ in all places

Axiom

$p \rightarrow [a]p$

Schema

$\phi \rightarrow [\alpha]\phi\ldots$

Axiom vs. Axiom Schemata

Axiom

$[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})$

Schema

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

Pattern match formulas for shape $\alpha \cup \beta$

Placeholder α schema variable matcher

Same instance of ϕ in all places

Axiom

$p \rightarrow [a]p$

Schema

$\phi \rightarrow [\alpha]\phi\dots$

- $x = 0 \rightarrow [y' = 5]x = 0$
- $x = y \rightarrow [y' = 5]x = y$
- $x = z \rightarrow [y' = 5]x = z$

Axiom vs. Axiom Schemata

Axiom

$[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})$

Schema

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

Pattern match formulas for shape $\alpha \cup \beta$

Placeholder α schema variable matcher

Same instance of ϕ in all places

Axiom

$p \rightarrow [a]p$

Schema

$\phi \rightarrow [\alpha]\phi \dots$

special vs. degenerate instances

✓ $x = 0 \rightarrow [y' = 5]x = 0$

× $x = y \rightarrow [y' = 5]x = y$

✓ $x = z \rightarrow [y' = 5]x = z$

rule out by side conditions

Axiom vs. Axiom Schemata: Formula vs. Algorithm

1 Formula

Axiom

$[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})$

Generic formula.
No exceptions.

Algorithm

Schema

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

Pattern match formulas for shape $\alpha \cup \beta$

Placeholder α schema variable matcher

Same instance of ϕ in all places

Axiom

$p \rightarrow [a]p$

Schema

$\phi \rightarrow [\alpha]\phi \ldots$

special vs. degenerate instances

✓ $x = 0 \rightarrow [y' = 5]x = 0$

× $x = y \rightarrow [y' = 5]x = y$

✓ $x = z \rightarrow [y' = 5]x = z$

rule out by side conditions

Generic Formulas in Axioms are like Generic Points

An analogy from algebraic geometry

Axiom schemata with side conditions are like **concrete points**

$\exists x\, ax^2 + bx + c = 0$ iff $b^2 \geq 4ac$ except $a = 0$ except $b = 0$ except $c = 0$

This Way

Axioms The generic formulas in axioms are like **generic points**

$ax^2 + bx + c = 0$ iff $x = -b \pm \sqrt{b^2 - 4ac}/(2a)$

Paying attention during substitutions to avoid degenerates (no $/0$, $\sqrt{-1}$)

Axioms vs. Axiom Schemata: Philosophy Affects Provers

- ✓ Soundness easier: literal formula, not instantiation mechanism
- ✓ An axiom is one formula. Axiom schema is a decision algorithm.
- ✓ Generic formula, not some shape with characterization of exceptions
- ✓ No schema variable or meta variable algorithms
- ✓ No matching mechanisms / unification in prover kernel
- ✓ No side condition subtlety or occurrence pattern checks (per schema)
- × Need other means of instantiating axioms: uniform substitution (US)
- ✓ US + renaming: isolate static semantics
- ✓ US independent from axioms: modular logic vs. prover separation
- ✓ More flexible by syntactic contextual equivalence
- × Extra proofs branches since instantiation is explicit proof step

Axioms vs. Axiom Schemata: Philosophy Affects Provers

- ✓ Soundness easier: literal formula, not instantiation mechanism
- ✓ An axiom is one formula. Axiom schema is a decision algorithm.
- ✓ Generic formula, not some shape with characterization of exceptions
- ✓ No schema variable or meta variable algorithms
- ✓ No matching mechanisms / unification in prover kernel
- ✓ No side condition subtlety or occurrence pattern checks (per schema)
- × Need other means of instantiating axioms: uniform substitution (US)
- ✓ US + renaming: isolate static semantics
- ✓ US independent from axioms: modular logic vs. prover separation
- ✓ More flexible by syntactic contextual equivalence
- × Extra proofs branches since instantiation is explicit proof step

---

$\sum$ Net win for soundness since significantly simpler prover

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

$$US\ \frac{\phi}{\sigma(\phi)}$$

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \mathrm{BV}(\otimes(\cdot))$ of operator $\otimes$
are not free in the substitution on its argument θ (U-admissible)

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[x := x+1 \cup x' = 1]x \geq 0 \leftrightarrow [x := x+1]x \geq 0 \land [x' = 1]x \geq 0}$$

Uniform Substitution: Definition expanded explicitly

$$
\begin{array}{rcll}
\sigma(f(\theta)) & = & (\sigma(f))(\sigma(\theta)) & \text{for function symbol } f \in \sigma \\
 & \overset{\text{def}}{=} & \{\cdot \mapsto \sigma(\theta)\}(\sigma f(\cdot)) & \\
\sigma(\theta + \eta) & = & \sigma(\theta) + \sigma(\eta) & \\
\sigma((\theta)') & = & (\sigma(\theta))' & \text{if } \sigma\ \mathcal{V} \cup \mathcal{V}'\text{-admissible for } \theta \\
\hline
\sigma(p(\theta)) & \equiv & (\sigma(p))(\sigma(\theta)) & \text{for predicate symbol } p \in \sigma \\
\sigma(C(\phi)) & \equiv & \sigma(C)(\sigma(\phi)) & \text{if } \sigma\ \mathcal{V} \cup \mathcal{V}'\text{-admissible for } \phi,\ C \in \sigma \\
\sigma(\phi \land \psi) & \equiv & \sigma(\phi) \land \sigma(\psi) & \\
\sigma(\forall x\, \phi) & = & \forall x\, \sigma(\phi) & \text{if } \sigma\ \{x\}\text{-admissible for } \phi \\
\sigma([\alpha]\phi) & = & [\sigma(\alpha)]\sigma(\phi) & \text{if } \sigma\ \mathrm{BV}(\sigma(\alpha))\text{-admissible for } \phi \\
\hline
\sigma(a) & \equiv & \sigma a & \text{for program constant } a \in \sigma \\
\sigma(x := \theta) & \equiv & x := \sigma(\theta) & \\
\sigma(x' = \theta \,\&\, H) & \equiv & x' = \sigma(\theta) \,\&\, \sigma(H) & \text{if } \sigma\ \{x, x'\}\text{-admissible for } \theta, H \\
\sigma(\alpha \cup \beta) & \equiv & \sigma(\alpha) \cup \sigma(\beta) & \\
\sigma(\alpha; \beta) & \equiv & \sigma(\alpha); \sigma(\beta) & \text{if } \sigma\ \mathrm{BV}(\sigma(\alpha))\text{-admissible for } \beta \\
\sigma(\alpha^*) & \equiv & (\sigma(\alpha))^* & \text{if } \sigma\ \mathrm{BV}(\sigma(\alpha))\text{-admissible for } \alpha
\end{array}
$$

Uniform Substitution: Examples

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \qquad \sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x^2][(z := x{+}z)^*; z := x{+}yz]y{\geq}x \leftrightarrow [(z := x^2{+}z^*); z := x^2{+}yz]y{\geq}x^2}$$

$$\text{with } \sigma = \{f \mapsto x^2, p(\cdot) \mapsto [(z := \cdot + z)^*; z := \cdot + yz]y \geq \cdot\}$$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -1]x \geq 0} \qquad \sigma = \{a \mapsto x' = -1, p \mapsto x \geq 0\}$$

$$\frac{(-x)^2 \geq 0}{[x' = -1](-x)^2 \geq 0} \quad \text{by} \quad \frac{p(\bar{x})}{[a]p(\bar{x})} \quad \sigma = \{a \mapsto x' = -1, p(\cdot) \mapsto (-\cdot)^2 \geq 0\}$$

Uniform Substitution: Examples

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \qquad \sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x^2][(z := x{+}z)^*; z := x{+}yz]y{\geq}x \leftrightarrow [(z := x^2{+}z^*); z := x^2{+}yz]y{\geq}x^2}$$

with $\sigma = \{f \mapsto x^2, p(\cdot) \mapsto [(z := \cdot + z)^*; z := \cdot + yz]y \geq \cdot\}$

$$\frac{p \to [a]p}{x \geq 0 \to [x' = -1]x \geq 0} \qquad \sigma = \{a \mapsto x' = -1, p \mapsto x \geq 0\}$$

$$\frac{(-x)^2 \geq 0}{[x' = -1](-x)^2 \geq 0} \quad \text{by} \quad \frac{p(\bar{x})}{[a]p(\bar{x})} \quad \sigma = \{a \mapsto x' = -1, p(\cdot) \mapsto (-\cdot)^2 \geq 0\}$$

Uniform Substitution: Examples

BV

Clash

FV

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \qquad \sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x^2][(z := x{+}z)^*; z := x{+}yz]y{\geq}x \leftrightarrow [(z := x^2{+}z^*); z := x^2{+}yz]y{\geq}x^2}$$

with $\sigma = \{f \mapsto x^2, p(\cdot) \mapsto [(z := \cdot + z)^*; z := \cdot + yz]y \geq \cdot\}$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -1]x \geq 0} \qquad \sigma = \{a \mapsto x' = -1, p \mapsto x \geq 0\}$$

$$\frac{(-x)^2 \geq 0}{[x' = -1](-x)^2 \geq 0} \quad \text{by} \quad \frac{p(\bar{x})}{[a]p(\bar{x})} \qquad \sigma = \{a \mapsto x' = -1, p(\cdot) \mapsto (-\cdot)^2 \geq 0\}$$

Uniform Substitution: Examples

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \qquad \sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

Clash

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x^2][(z := x+z)^*; z := x+yz]y \geq x \leftrightarrow [(z := x^2+z^*); z := x^2+yz]y \geq x^2}$$

with $\sigma = \{f \mapsto x^2, p(\cdot) \mapsto [(z := \cdot + z)^*; z := \cdot + yz]y \geq \cdot\}$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -1]x \geq 0} \qquad \sigma = \{a \mapsto x' = -1, p \mapsto x \geq 0\}$$

$$\frac{(-x)^2 \geq 0}{[x' = -1](-x)^2 \geq 0} \quad \text{by} \quad \frac{p(\bar{x})}{[a]p(\bar{x})} \quad \sigma = \{a \mapsto x' = -1, p(\cdot) \mapsto (-\cdot)^2 \geq 0\}$$

Uniform Substitution: Examples

$$\frac{[x:=f]p(x)\leftrightarrow p(f)}{[x:=x+1]x\neq x\leftrightarrow x+1\neq x}$$

Clash

$$\sigma=\{f\mapsto x+1,\ p(\cdot)\mapsto(\cdot\neq x)\}$$

$$\frac{[x:=f]p(x)\leftrightarrow p(f)}{[x:=x^2][(z:=x+z)^*;z:=x+yz]y\geq x\leftrightarrow[(z:=x^2+z^*);z:=x^2+yz]y\geq x^2}$$

Correct

with $\sigma=\{f\mapsto x^2,\ p(\cdot)\mapsto[(z:=\cdot+z)^*;z:=\cdot+yz]y\geq\cdot\}$

$$\frac{p\to[a]p}{x\geq 0\to[x'=-1]x\geq 0}$$

$$\sigma=\{a\mapsto x'=-1,\ p\mapsto x\geq 0\}$$

$$\frac{(-x)^2\geq 0}{[x'=-1](-x)^2\geq 0}\quad\text{by}\quad\frac{p(\bar{x})}{[a]p(\bar{x})}\quad\sigma=\{a\mapsto x'=-1,\ p(\cdot)\mapsto(-\cdot)^2\geq 0\}$$

Uniform Substitution: Examples

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x}$$

Clash

$$\sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x^2][(z := x+z)^*; z := x+yz]y \geq x \leftrightarrow [(z := x^2+z^*); z := x^2+yz]y \geq x^2}$$

Correct

with $\sigma = \{f \mapsto x^2, p(\cdot) \mapsto [(z := \cdot + z)^*; z := \cdot + yz]y \geq \cdot\}$

$$\frac{[a]p}{x \geq 0 \rightarrow [x' = -1]x \geq 0}$$

BV

Clash

$$\sigma = \{a \mapsto x' = -1, p \mapsto x \geq 0\}$$

FV

$$\frac{(-x)^2 \geq 0}{[x' = -1](-x)^2 \geq 0} \quad \text{by} \quad \frac{p(\bar{x})}{[a]p(\bar{x})} \quad \sigma = \{a \mapsto x' = -1, p(\cdot) \mapsto (-\cdot)^2 \geq 0\}$$

Uniform Substitution: Examples

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x+1]x \neq x \leftrightarrow x+1 \neq x} \qquad \sigma = \{f \mapsto x+1, p(\cdot) \mapsto (\cdot \neq x)\}$$

Clash

$$\frac{[x := f]p(x) \leftrightarrow p(f)}{[x := x^2][(z := x+z)^*; z := x+yz]y \geq x \leftrightarrow [(z := x^2+z^*); z := x^2+yz]y \geq x^2}$$

Correct

with $\sigma = \{f \mapsto x^2, p(\cdot) \mapsto [(z := \cdot + z)^*; z := \cdot + yz]y \geq \cdot\}$

$$\frac{p \rightarrow [a]p}{x \geq 0 \rightarrow [x' = -1]x \geq 0} \qquad \sigma = \{a \mapsto x' = -1, p \mapsto x \geq 0\}$$

Clash

$$\frac{(-x)^2 \geq 0}{[x' = -1](-x)^2 \geq 0} \text{ by } \frac{p(\bar{x})}{[a]p(\bar{x})} \qquad \sigma = \{a \mapsto x' = -1, p(\cdot) \mapsto (-\cdot)^2 \geq 0\}$$

Correct

Solving Differential Equations? By Axiom Schema?

$[\prime]\ [x' = \theta]\phi \leftrightarrow \forall t{\geq}0\, [x := x(t)]\phi$ $\quad$ (t fresh and $x'(t) = \theta$)

Axiom schema with side conditions:

1. Occurs check: t fresh
2. Solution check: x solves the ODE $x'(t) = \theta$
3. Initial value check: x solves the symbolic IVP $x(0) = x$

Quite nontrivial soundness-critical algorithms . . .

LICS'12

Differential Equation Axioms & Differential Axioms

$$\text{DW}\quad [x' = f(x)\,\&\,q(x)]q(x)$$

$$\text{DC}\quad \begin{array}{l}\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)\\ \leftarrow [x' = f(x)\,\&\,q(x)]r(x)\end{array}$$

$$\text{DE}\quad [x' = f(x)\,\&\,q(x)]p(x,x') \leftrightarrow [x' = f(x)\,\&\,q(x)][x' := f(x)]p(x,x')$$

$$\text{DI}\quad [x' = f(x)\,\&\,q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \land [x' = f(x)\,\&\,q(x)](p(x))'\big)$$

$$\text{DG}\quad [x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)$$

$$\text{DS}\quad [x' = f\,\&\,q(x)]p(x) \leftrightarrow \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\; q(x + fs)) \rightarrow [x := x + ft]p(x)\big)$$

$$[{}':=]\quad [x' := f]p(x') \leftrightarrow p(f)$$

$$+'\quad (f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))'$$

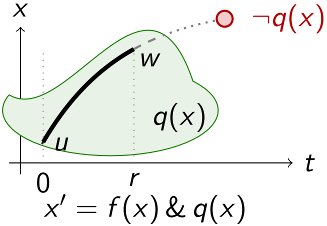
$$\cdot'\quad (f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$$

$$\circ'\quad [y := g(x)][y' := 1]\big((f(g(x)))' = (f(y))' \cdot (g(x))'\big)$$

Differential Equation Axioms

Axiom (Differential Weakening)

$$\mathrm{DW} \quad [x' = f(x) \,\&\, q(x)]q(x)$$



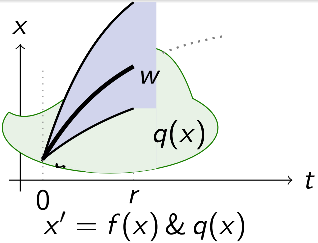
Differential equations cannot leave their evolution domains. Implies:

$$[x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x)]\big(q(x) \to p(x)\big)$$

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC}\quad \begin{array}{l}\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)\\ \leftarrow [x' = f(x)\,\&\,q(x)]r(x)\end{array}$$



DC is a cut for differential equations.

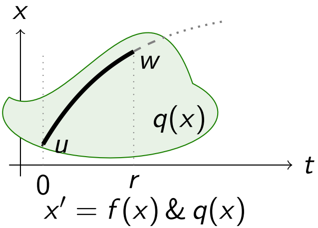
DC is a differential modal modus ponens K.

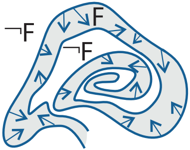
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

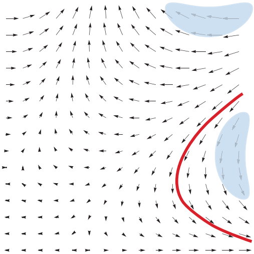
Differential Equation Axioms

Axiom (Differential Invariant)

DI $[x' = f(x) \,\&\, q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \wedge [x' = f(x) \,\&\, q(x)](p(x))'\big)$





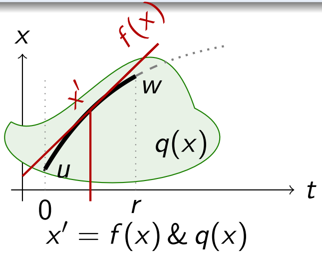


Differential invariant: $p(x)$ true now and its differential $(p(x))'$ true always
What's the differential of a formula???
What's the meaning of a differential term . . . in a state???

Differential Equation Axioms

Axiom (Differential Effect)

$$\text{DE} \quad [x' = f(x) \,\&\, q(x)]p(x, x') \leftrightarrow [x' = f(x) \,\&\, q(x)][x' := f(x)]p(x, x')$$



Effect of differential equation on differential symbol x'

$[x' := f(x)]$ instantly mimics continuous effect $[x' = f(x)]$ on x'

$[x' := f(x)]$ selects vector field $x' = f(x)$ for subsequent differentials

Example: Differential Invariants Don't Solve. Prove!

1. DI proves a property of an ODE inductively by its differentials
2. DE exports vector field, possibly after DW exports evolution domain
3. CE+CQ reason efficiently in Equivalence or eQuational context
4. G isolates postcondition
5. $[':=]$ differential substitution uses vector field
6. $\cdot'$ differential computations are axiomatic (US)

$$
\text{DI}\,\dfrac{\text{DE}\,\dfrac{\text{CE}\,\dfrac{\text{G}\,\dfrac{[':=]\,\dfrac{\mathbb{R}\,\dfrac{*}{x^3\cdot x + x\cdot x^3 \ge 0}}{[x' := x^3]x'\cdot x + x\cdot x' \ge 0}}{[x' = x^3][x' := x^3]x'\cdot x + x\cdot x' \ge 0} \qquad \dfrac{\text{CQ}\,\dfrac{\dfrac{\text{US}\,\dfrac{\cdot'\,\dfrac{*}{(f(\bar{x})\cdot g(\bar{x}))' = (f(\bar{x}))'\cdot g(\bar{x}) + f(\bar{x})\cdot (g(\bar{x}))'}}{(x\cdot x)' = (x)'\cdot x + x\cdot (x)'}}{(x\cdot x)' = x'\cdot x + x\cdot x'}}{(x\cdot x)' \ge 0 \leftrightarrow x'\cdot x + x\cdot x' \ge 0}}{(x\cdot x \ge 1)' \leftrightarrow x'\cdot x + x\cdot x' \ge 0}}{[x' = x^3][x' := x^3](x\cdot x \ge 1)'}}{[x' = x^3](x\cdot x \ge 1)'}}{x\cdot x \ge 1 \rightarrow [x' = x^3]x\cdot x \ge 1}
$$

Example: Soundly Solving Differential Equations

1. DG introduces time t, DC cuts solution in, that DI proves and
2. DW exports to postcondition
3. inverse DC removes evolution domain constraints
4. inverse DG removes original ODE
5. DS solves remaining ODE for time

$$
\begin{array}{ll}
 & \quad * \\
\hline
\mathbb{R} & \phi \rightarrow \forall s{\geq}0\,(x_0 + \frac{a}{2}s^2 + v_0 s \geq 0) \\
\hline
[:=] & \phi \rightarrow \forall s{\geq}0\,[t := 0 + 1s]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0 \\
\hline
\text{DS} & \phi \rightarrow [t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0 \\
\hline
\text{DG} & \phi \rightarrow [v' = a, t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0 \\
\hline
\text{DG} & \phi \rightarrow [x' = v, v' = a, t' = 1]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0 \\
\hline
\text{DC} & \phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0 \\
\hline
\text{DC} & \phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at \land x = x_0 + \frac{a}{2}t^2 + v_0 t]x_0 + \frac{a}{2}t^2 + v_0 t \geq 0 \\
\hline
\text{G,K} & \phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at \land x = x_0 + \frac{a}{2}t^2 + v_0 t](x{=}x_0{+}\frac{a}{2}t^2{+}v_0 t \rightarrow x{\geq}0) \\
\hline
\text{DW} & \phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at \land x = x_0 + \frac{a}{2}t^2 + v_0 t]x \geq 0 \\
\hline
\text{DC} & \phi \rightarrow [x' = v, v' = a, t' = 1\,\&\, v = v_0 + at]x \geq 0 \\
\hline
\text{DC} & \phi \rightarrow [x' = v, v' = a, t' = 1]x \geq 0 \\
\hline
 & \phi \rightarrow \exists t\,[x' = v, v' = a, t' = 1]x \geq 0 \\
\hline
\text{DG} & \phi \rightarrow [x' = v, v' = a]x \geq 0
\end{array}
$$

Outline

1. Cyber-Physical Systems

2. Uniform Substitution Calculus for Differential Dynamic Logic
   - Uniform Substitution Calculus
   - Axiom vs. Axiom Schemata
   - Uniform Substitutions
   - Differential Axioms
   - Examples

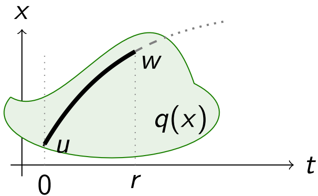
3. Differential-form Differential Dynamic Logic
   - Semantics: Local
   - Differential Substitution Lemmas
   - Static Semantics

4. Summary

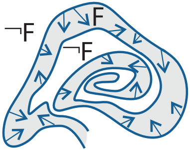
Differential Equation Axioms

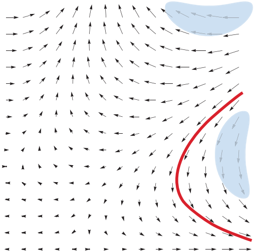
Axiom (Differential Invariant)

DI $[x' = f(x) \,\&\, q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \land [x' = f(x) \,\&\, q(x)](p(x))'\big)$



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





Differential invariant: $p(x)$ true now and its differential $(p(x))'$ true always
What's the differential of a formula???
What's the meaning of a differential term … in a state???

The Meaning of Primes

$$[\![(\theta)']\!]u = \ ???$$

$$[\![(x^2)']\!]u$$

The Meaning of Primes

$$[\![(\theta)']\!]u = \ ???$$

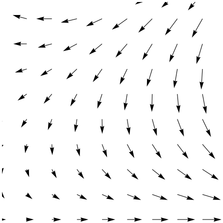
$$[\![(x^2)']\!]u = [\![2x]\!]u \ ?$$

The Meaning of Primes

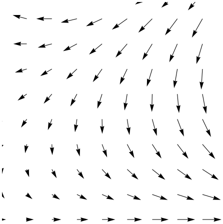
$[\![(\theta)']\!]u =$???

$[\![(x^2)']\!]u = [\![2x]\!]u$?

depends on the differential equation . . .



The Meaning of Primes



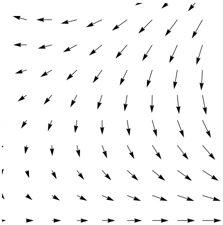
$[\![(\theta)']\!]u = \ ???$

$[\![(x^2)']\!]u = [\![2x]\!]u\ ?$

depends on the differential equation . . .

well-defined locally in an isolated state at all?

The Meaning of Primes



$\to \mathbb{R}$

$[\![(\theta)']\!]u = \ ???$

$[\![(x^2)']\!]u = [\![2x]\!]u\ ?$

depends on the differential equation . . .

well-defined locally in an isolated state at all?

$$[\![(\theta)']\!]u = \sum_x u(x')\frac{\partial [\![\theta]\!]^I}{\partial x}(u) = \sum_x u(x')\frac{\partial [\![\theta]\!] u_x^X}{\partial X}$$

$$[\![(\theta)']\!] = d[\![\theta]\!] = \sum_{i=1}^{n} \frac{\partial [\![\theta]\!]}{\partial x^i} dx^i$$

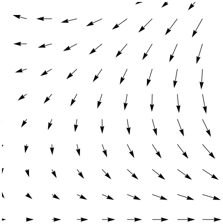
depends on $u(x_i') = dx^i$

depends on state u

tangent space basis

cotangent space basis

The Meaning of Primes



$\to \mathbb{R}$

$$[\![(\theta)']\!]u = \ ???$$

$$[\![(x^2)']\!]u = [\![2x]\!]u \ ?$$

depends on the differential equation . . .

well-defined locally in an isolated state at all?

$$[\![(\theta)']\!]u = \sum_x u(x') \frac{\partial [\![\theta]\!]^I}{\partial x}(u) = \sum_x u(x') \frac{\partial [\![\theta]\!] u_x^X}{\partial X}$$

$$[\![(\theta)']\!] = d[\![\theta]\!] = \sum_{i=1}^{n} \frac{\partial [\![\theta]\!]}{\partial x^i} dx^i$$

$u(x')$ is the local shadow of $\frac{\mathrm{d}x}{\mathrm{d}t}$ if that existed

$(\theta)'$ represents how θ changes locally, depending on x'

Differential Substitution Lemmas

Lemma (Differential lemma)

If $I, \varphi \models x' = \theta \land H$ *for duration* $r > 0$*, then for all* $0 \leq \zeta \leq r$*:*

Syntactic

$$\llbracket(\eta)'\rrbracket^{I}\varphi(\zeta) = \frac{\mathrm{d}\llbracket\eta\rrbracket^{I}\varphi(t)}{\mathrm{d}t}(\zeta)$$

Analytic

Lemma (Differential assignment)

If $I, \varphi \models x' = \theta \land H$ *then* $I, \varphi \models \phi \leftrightarrow [x' := \theta]\phi$

Lemma (Derivations)

$$\begin{aligned}
(\theta + \eta)' &= (\theta)' + (\eta)' \\
(\theta \cdot \eta)' &= (\theta)' \cdot \eta + \theta \cdot (\eta)' \\
[y := \theta][y' := 1]\big((f(\theta))' &= (f(y))' \cdot (\theta)'\big) && \text{for } y, y' \notin \theta \\
(f)' &= 0 && \text{for arity 0 functions/numbers } f
\end{aligned}$$

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

$$\text{US}\ \frac{\phi}{\sigma(\phi)}$$

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \text{BV}(\otimes(\cdot))$ of operator $\otimes$
are not free in the substitution on its argument θ (U-admissible)

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function $f(\theta)$ for any θ by $\eta(\theta)$
quantifier $C(\phi)$ for any ϕ by $\psi(\theta)$
program const. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[x := x+1 \cup x' = 1]x \geq 0 \leftrightarrow [x := x+1]x \geq 0 \land [x' = 1]x \geq 0}$$

Uniform Substitution

Theorem (Soundness) replace all occurrences of $p(\cdot)$

Modular interface:
Prover vs. Logic

$$\text{US}\quad \frac{\phi}{\sigma(\phi)}$$

provided $FV(\sigma|_{\Sigma(\theta)}) \cap BV(\otimes(\cdot)) = \emptyset$ *for each operation* $\otimes(\theta)$ *in* ϕ

i.e. bound variables $U = \mathrm{BV}(\otimes(\cdot))$ of operator $\otimes$
are not free in the substitution on its argument θ (U-admissible)

Uniform substitution σ replaces all occurrences of $p(\theta)$ for any θ by $\psi(\theta)$
function $f(\theta)$ for any θ by $\eta(\theta)$
quantifier $C(\phi)$ for any ϕ by $\psi(\theta)$
program const. a by α

$$\text{US}\ \frac{[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})}{[x := x+1 \cup x' = 1]x \geq 0 \leftrightarrow [x := x+1]x \geq 0 \land [x' = 1]x \geq 0}$$

Correctness of Static Semantics

Lemma (Bound effect lemma) (Only BV(·) change)

If $(u, w) \in [\![\alpha]\!]^I$, *then* $u = w$ *on* $BV(\alpha)^\complement$.

Lemma (Coincidence lemma) (Only FV(·) determine truth)

If $u = \tilde{u}$ *on* $FV(\theta)$ *and* $I = J$ *on* $\Sigma(\theta)$, *then*

$$[\![\theta]\!]^I u = [\![\theta]\!]^J \tilde{u}$$

$$u \in [\![\phi]\!]^I \text{ iff } \tilde{u} \in [\![\phi]\!]^J$$

$$\begin{tikzcd}
u \arrow[r, "\alpha"'] \arrow[r, bend left, equal, "\text{on } BV(\alpha)^\complement"] \arrow[d, equal, "\text{on } V \supseteq FV(\alpha)"'] & w \arrow[d, equal, "\text{on } V \cup MBV(\alpha)"] \\
\tilde{u} \arrow[r, dashed, "\alpha", "\exists"'] \arrow[r, bend right, equal, "\text{on } BV(\alpha)^\complement"'] & \tilde{w}
\end{tikzcd}$$

Differential Dynamic Logic d$\mathcal{L}$: Static Semantics

$$
\begin{aligned}
\mathsf{FV}((\theta)')\\
\mathsf{FV}(p(\theta_1,\dots,\theta_k))\\
\mathsf{FV}(C(\phi))\\
\mathsf{FV}(\phi\land\psi)\\
\mathsf{FV}(\forall x\,\phi) = \mathsf{FV}(\exists x\,\phi)\\
\mathsf{FV}([\alpha]\phi) = \mathsf{FV}(\langle\alpha\rangle\phi)\\
\mathsf{FV}(a)\\
\mathsf{FV}(x:=\theta) = \mathsf{FV}(x':=\theta)\\
\mathsf{FV}(?H)\\
\mathsf{FV}(x'=\theta\,\&\,H)\\
\mathsf{FV}(\alpha\cup\beta)\\
\mathsf{FV}(\alpha;\beta)\\
\mathsf{FV}(\alpha^*)
\end{aligned}
$$

Differential Dynamic Logic d$\mathcal{L}$: Static Semantics

$$
\begin{array}{rll}
\mathsf{FV}((\theta)') & = \mathsf{FV}(\theta) & \\
\hline
\mathsf{FV}(p(\theta_1,\dots,\theta_k)) & = \mathsf{FV}(\theta_1) \cup \dots \cup \mathsf{FV}(\theta_k) & \\
\mathsf{FV}(C(\phi)) & = \mathcal{V} \cup \mathcal{V}' & \\
\mathsf{FV}(\phi \land \psi) & = \mathsf{FV}(\phi) \cup \mathsf{FV}(\psi) & \\
\mathsf{FV}(\forall x\, \phi) = \mathsf{FV}(\exists x\, \phi) & = \mathsf{FV}(\phi) \setminus \{x\} & \\
\mathsf{FV}([\alpha]\phi) = \mathsf{FV}(\langle\alpha\rangle\phi) & = \mathsf{FV}(\alpha) \cup (\mathsf{FV}(\phi) \setminus \mathsf{BV}(\alpha)) & \\
\hline
\mathsf{FV}(a) & = \mathcal{V} \cup \mathcal{V}' & \text{for program const. } a \\
\mathsf{FV}(x := \theta) = \mathsf{FV}(x' := \theta) & = \mathsf{FV}(\theta) & \\
\mathsf{FV}(?H) & = \mathsf{FV}(H) & \\
\mathsf{FV}(x' = \theta \,\&\, H) & = \{x\} \cup \mathsf{FV}(\theta) \cup \mathsf{FV}(H) & \\
\mathsf{FV}(\alpha \cup \beta) & = \mathsf{FV}(\alpha) \cup \mathsf{FV}(\beta) & \\
\mathsf{FV}(\alpha ; \beta) & = \mathsf{FV}(\alpha) \cup (\mathsf{FV}(\beta) \setminus \mathsf{BV}(\alpha)) & \\
\mathsf{FV}(\alpha^*) & = \mathsf{FV}(\alpha) &
\end{array}
$$

Differential Dynamic Logic d$\mathcal{L}$: Static Semantics

$$
\begin{array}{rll}
\mathrm{FV}((\theta)') & = \mathrm{FV}(\theta) \cup \mathrm{FV}(\theta)' & \text{caution} \\
\hline
\mathrm{FV}(p(\theta_1,\dots,\theta_k)) & = \mathrm{FV}(\theta_1) \cup \dots \cup \mathrm{FV}(\theta_k) & \\
\mathrm{FV}(C(\phi)) & = \mathcal{V} \cup \mathcal{V}' & \\
\mathrm{FV}(\phi \land \psi) & = \mathrm{FV}(\phi) \cup \mathrm{FV}(\psi) & \\
\mathrm{FV}(\forall x\, \phi) = \mathrm{FV}(\exists x\, \phi) & = \mathrm{FV}(\phi) \setminus \{x\} & \\
\mathrm{FV}([\alpha]\phi) = \mathrm{FV}(\langle\alpha\rangle\phi) & = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\phi) \setminus \mathrm{MBV}(\alpha)) & \text{caution} \\
\hline
\mathrm{FV}(a) & = \mathcal{V} \cup \mathcal{V}' & \text{for program const. } a \\
\mathrm{FV}(x := \theta) = \mathrm{FV}(x' := \theta) & = \mathrm{FV}(\theta) & \\
\mathrm{FV}(?H) & = \mathrm{FV}(H) & \\
\mathrm{FV}(x' = \theta \,\&\, H) & = \{x\} \cup \mathrm{FV}(\theta) \cup \mathrm{FV}(H) & \\
\mathrm{FV}(\alpha \cup \beta) & = \mathrm{FV}(\alpha) \cup \mathrm{FV}(\beta) & \\
\mathrm{FV}(\alpha ; \beta) & = \mathrm{FV}(\alpha) \cup (\mathrm{FV}(\beta) \setminus \mathrm{MBV}(\alpha)) & \text{caution} \\
\mathrm{FV}(\alpha^*) & = \mathrm{FV}(\alpha) &
\end{array}
$$

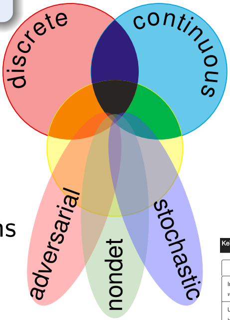
Outline

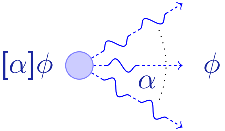
Uniform Substitution for Differential Dynamic Logic

differential dynamic logic

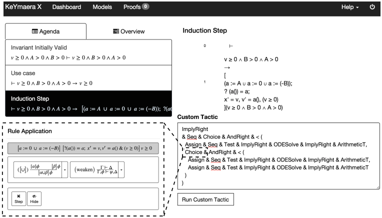
$$\mathrm{d}\mathcal{L} = \mathrm{DL} + \mathrm{HP}$$

- Differential forms
  $\rightsquigarrow$ local axioms of ODEs
- Uniform substitution
  $\rightsquigarrow$ modular generic axioms
  (not schemata)
- Modular: Logic $\|$ Prover
- Straightforward to implement
- Tactics regain efficiency
- Fast contextual equivalence





KeYmaera X



Invariant Initially Valid

$v \geq 0 \land A > 0 \land B > 0 \vdash v \geq 0 \land B > 0 \land A > 0$

Use case

$\vdash v \geq 0 \land B > 0 \land A > 0 \rightarrow v \geq 0$

Induction Step

$\vdash v \geq 0 \land B > 0 \land A > 0 \rightarrow$ $[(a := A \cup a := 0 \cup a := (-B));$ $?(a($

Rule Application

$[a := 0 \cup a := (-B)]\ [?(a()) = a;\ x' = v, v' = a()\ \&\ (v \geq 0)]\ v \geq 0$

$([\cup])\ \dfrac{[\alpha]\phi \qquad [\beta]\phi}{[\alpha\cup\beta]\phi}$ $\quad$ $(\text{weaken})\ \dfrac{\Gamma \vdash \Delta}{\Gamma, \phi \vdash \psi, \Delta}$

Induction Step

```
0        ⊢

         v ≥ 0 ∧ B > 0 ∧ A > 0
         →
         [
1        (a := A ∪ a := 0 ∪ a := (-B));
         ? (a()) = a;
         x' = v, v' = a(), (v ≥ 0)
         ](v ≥ 0 ∧ B > 0 ∧ A > 0)
```

Custom Tactic

```
ImplyRight
& Seq & Choice & AndRight & < (
 Assign & Seq & Test & ImplyRight & ODESolve & ImplyRight & ArithmeticT,
 Choice & AndRight & < (
  Assign & Seq & Test & ImplyRight & ODESolve & ImplyRight & ArithmeticT,
  Assign & Seq & Test & ImplyRight & ODESolve & ImplyRight & ArithmeticT
 )
)
```

Key Contributions

Q: How to build a prover with a small soundness-critical core?

A: Uniform substitution [Church]

Q: How to enable flexible yet sound reasoning?

A: Axioms with local meaning [Philosophy, Algebraic Geometry]

Q: What's the local meaning of a differential equation?

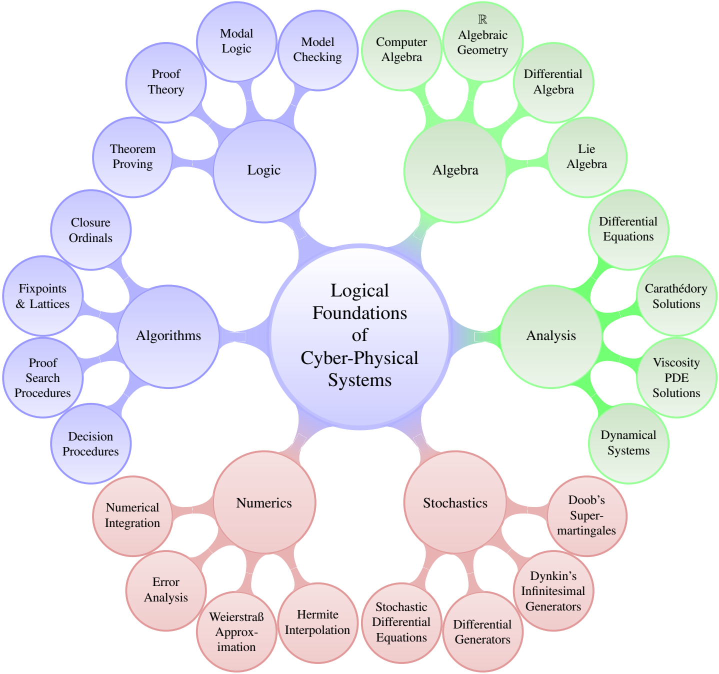
A: Differential forms [Differential Geometry]

Q: How to do hybrid systems proving?

A: Uniform substitution calculus for differential dynamic logic

Q: What's the impact of uniform substitution on a prover core?

A: 65 989 ↘ 1 682 LOC (2.5%) [KeYmaera X]



Logical Foundations of Cyber-Physical Systems

Logic

Theorem Proving

Proof Theory

Modal Logic

Model Checking

Algebra

Computer Algebra

ℝ Algebraic Geometry

Differential Algebra

Lie Algebra

Analysis

Differential Equations

Carathédory Solutions

Viscosity PDE Solutions

Dynamical Systems

Stochastics

Doob's Super-martingales

Dynkin's Infinitesimal Generators

Differential Generators

Stochastic Differential Equations

Numerics

Hermite Interpolation

Weierstraß Approx-imation

Error Analysis

Numerical Integration

Algorithms

Decision Procedures

Proof Search Procedures

Fixpoints & Lattices

Closure Ordinals

KeYmaera X Kernel: Qualifies as a Microkernel

	≈LOC	
KeYmaera X	1 682	
KeYmaera	65 989	
KeY	51 328	
HOL Light	396	
Isabelle/Pure	8 113	
Nuprl	15 000	+ 50 000
Coq	20 000	
HSolver	20 000	
Flow*	25 000	
PHAVer	30 000	
dReal	50 000	+ millions
SpaceEx	100 000	
HyCreate2	6 081	+ user model analysis

Disclaimer: These self-reported estimates of the soundness-critical lines of code + rules are to be taken with a grain of salt. Different languages, capabilities, styles

André Platzer.
A uniform substitution calculus for differential dynamic logic.
In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481. Springer, 2015.
`doi:10.1007/978-3-319-21401-6_32`.

André Platzer.
The complete proof theory of hybrid systems.
In *LICS*, pages 541–550. IEEE, 2012.
`doi:10.1109/LICS.2012.64`.

André Platzer.
Differential game logic.
ACM Trans. Comput. Log.
To appear. Preprint at arXiv 1408.1980.

Differential Dynamic Logic: Axioms

[:=] $[x := f]p(x) \leftrightarrow p(f)$

[?] $[?q]p \leftrightarrow (q \rightarrow p)$

[∪] $[a \cup b]p(\bar{x}) \leftrightarrow [a]p(\bar{x}) \land [b]p(\bar{x})$

[;] $[a; b]p(\bar{x}) \leftrightarrow [a][b]p(\bar{x})$

[*] $[a^*]p(\bar{x}) \leftrightarrow p(\bar{x}) \land [a][a^*]p(\bar{x})$

K $[a](p(\bar{x}) \rightarrow q(\bar{x})) \rightarrow ([a]p(\bar{x}) \rightarrow [a]q(\bar{x}))$

I $[a^*](p(\bar{x}) \rightarrow [a]p(\bar{x})) \rightarrow (p(\bar{x}) \rightarrow [a^*]p(\bar{x}))$

V $p \rightarrow [a]p$

CADE'15

Differential Dynamic Logic: Axioms

$$\text{G}\ \frac{p(\bar{x})}{[a]p(\bar{x})}$$

$$\forall\ \frac{p(x)}{\forall x\, p(x)}$$

$$\text{MP}\ \frac{p \to q \quad p}{q}$$

$$\text{CT}\ \frac{f(\bar{x}) = g(\bar{x})}{c(f(\bar{x})) = c(g(\bar{x}))}$$

$$\text{CQ}\ \frac{f(\bar{x}) = g(\bar{x})}{p(f(\bar{x})) \leftrightarrow p(g(\bar{x}))}$$

$$\text{CE}\ \frac{p(\bar{x}) \leftrightarrow q(\bar{x})}{C(p(\bar{x})) \leftrightarrow C(q(\bar{x}))}$$

Differential Equation Axioms & Differential Axioms

DW $[x' = f(x) \,\&\, q(x)]q(x)$

DC $\big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \wedge r(x)]p(x)\big) \leftarrow [x' = f(x) \,\&\, q(x)]r(x)$

DE $[x' = f(x) \,\&\, q(x)]p(x, x') \leftrightarrow [x' = f(x) \,\&\, q(x)][x' := f(x)]p(x, x')$

DI $[x' = f(x) \,\&\, q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \wedge [x' = f(x) \,\&\, q(x)](p(x))'\big)$

DG $[x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x) \,\&\, q(x)]p(x)$

DS $[x' = f \,\&\, q(x)]p(x) \leftrightarrow \forall t \geq 0\, \big((\forall 0 \leq s \leq t\, q(x + fs)) \rightarrow [x := x + ft]p(x)\big)$

$[':=]$ $[x' := f]p(x') \leftrightarrow p(f)$

$+'$ $(f(\bar{x}) + g(\bar{x}))' \;=\; (f(\bar{x}))' + (g(\bar{x}))'$

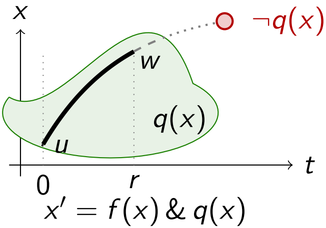
$\cdot'$ $(f(\bar{x}) \cdot g(\bar{x}))' \;=\; (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))'$

$\circ'$ $[y := g(x)][y' := 1]\big((f(g(x)))' = (f(y))' \cdot (g(x))'\big)$

Differential Equation Axioms

Axiom (Differential Weakening)

$$\text{DW} \quad [x' = f(x) \,\&\, q(x)]q(x)$$



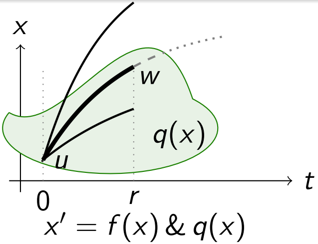
Differential equations cannot leave their evolution domains. Implies:

$$[x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x)]\big(q(x) \to p(x)\big)$$

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC} \quad \begin{array}{l}([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \land r(x)]p(x)) \\ \leftarrow [x' = f(x) \,\&\, q(x)]r(x)\end{array}$$



DC is a cut for differential equations.

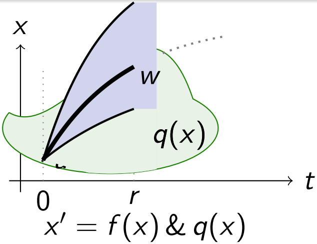
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC} \quad \begin{array}{l}([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)) \\ \leftarrow [x' = f(x)\,\&\,q(x)]r(x)\end{array}$$



DC is a cut for differential equations.

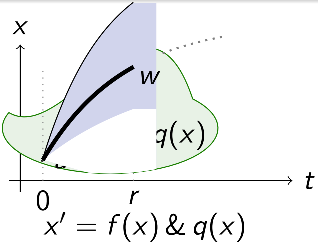
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC}\quad \begin{aligned}&\big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big)\\ &\leftarrow [x' = f(x)\,\&\,q(x)]r(x)\end{aligned}$$



DC is a cut for differential equations.

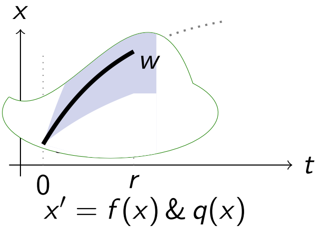
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC} \quad \begin{aligned}&([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x))\\ &\leftarrow [x' = f(x)\,\&\,q(x)]r(x)\end{aligned}$$



DC is a cut for differential equations.

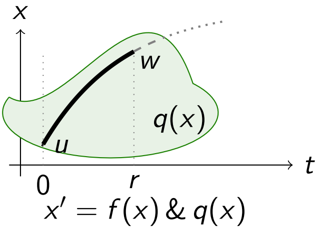
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC} \quad \begin{aligned}&([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \land r(x)]p(x)) \\ &\leftarrow [x' = f(x) \,\&\, q(x)]r(x)\end{aligned}$$



DC is a cut for differential equations.

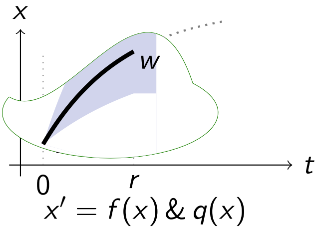
DC is a differential modal modus ponens K.

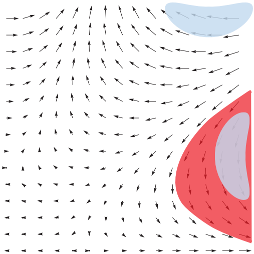
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC}\quad \begin{array}{l}([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)) \\ \leftarrow [x' = f(x)\,\&\,q(x)]r(x)\end{array}$$





DC is a cut for differential equations.

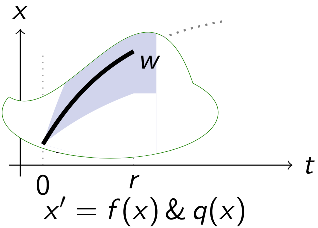
DC is a differential modal modus ponens K.

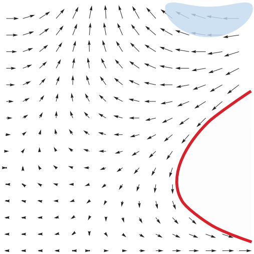
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)\big) \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$





DC is a cut for differential equations.

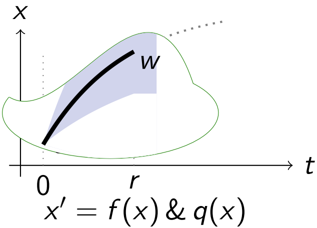
DC is a differential modal modus ponens K.

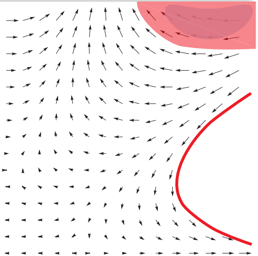
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC}\quad \begin{array}{l}([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x) \land r(x)]p(x)) \\ \leftarrow [x' = f(x)\,\&\,q(x)]r(x)\end{array}$$





DC is a cut for differential equations.

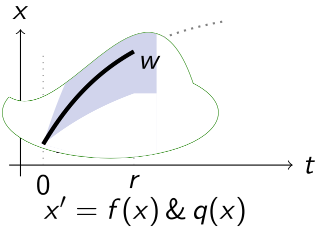
DC is a differential modal modus ponens K.

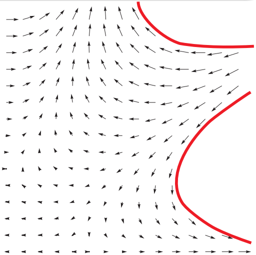
Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

Differential Equation Axioms

Axiom (Differential Cut)

$$\text{DC}\quad \big([x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow [x' = f(x)\,\&\,q(x){\land}r(x)]p(x)\big) \\ \leftarrow [x' = f(x)\,\&\,q(x)]r(x)$$





DC is a cut for differential equations.

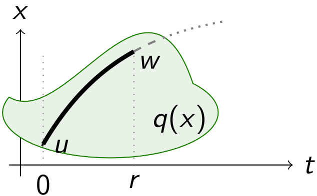
DC is a differential modal modus ponens K.

Can't leave $r(x)$, then might as well restrict state space to $r(x)$.

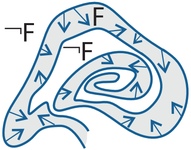
Differential Equation Axioms

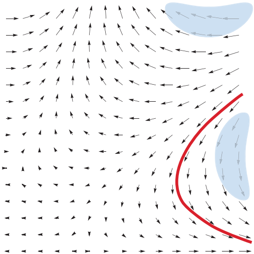
Axiom (Differential Invariant)

$$\text{DI} \quad [x' = f(x) \,\&\, q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \land [x' = f(x) \,\&\, q(x)](p(x))'\big)$$



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





Differential invariant: $p(x)$ true now and its differential $(p(x))'$ true always

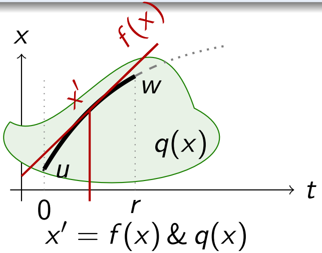
What's the differential of a formula???

What's the meaning of a differential term … in a state???

Differential Equation Axioms

Axiom (Differential Effect)

$$\text{DE} \quad [x' = f(x) \,\&\, q(x)]p(x,x') \leftrightarrow [x' = f(x) \,\&\, q(x)][x' := f(x)]p(x,x')$$



Effect of differential equation on differential symbol x'

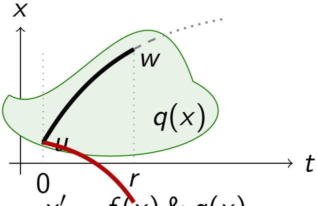
$[x' := f(x)]$ instantly mimics continuous effect $[x' = f(x)]$ on x'

$[x' := f(x)]$ selects vector field $x' = f(x)$ for subsequent differentials

Differential Equation Axioms

Axiom (Differential Ghost)

$$\mathrm{DG}\ [x' = f(x)\,\&\,q(x)]p(x) \leftrightarrow \exists y\,[x' = f(x), y' = a(x)y + b(x)\,\&\,q(x)]p(x)$$



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

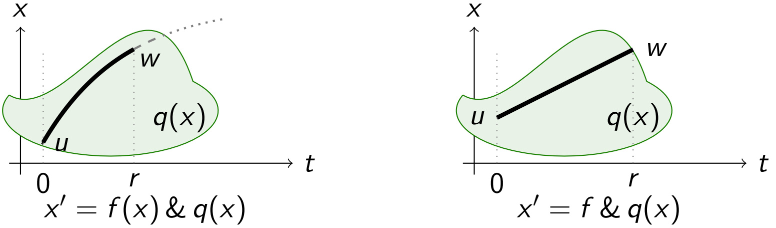
$$y' = a(x)y + b(x)$$

Differential ghost/auxiliaries: extra differential equations that exist
Can cause new invariants
"Dark matter" counterweight to balance conserved quantities

Differential Equation Axioms

Axiom (Differential Solution)

$$\text{DS}\ \ [x' = f \,\&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\; q(x{+}fs)) \rightarrow [x := x + ft]p(x)\big)$$



Differential solutions: solve differential equations
with DG,DC and inverse companions

Differential-form Differential Dynamic Logic: Semantics

Definition (Term semantics) $([\![\cdot]\!] : \mathrm{Trm} \to (\mathcal{S} \to \mathbb{R}))$

$$[\![(\theta)']\!]^I u = \sum_x u(x') \frac{\partial [\![\theta]\!]^I}{\partial x}(u) = \sum_x u(x') \frac{\partial [\![\theta]\!]^I u_x^X}{\partial X}$$

Definition (d$\mathcal{L}$ semantics) $([\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathcal{S}))$

$$\begin{aligned} [\![C(\phi)]\!]^I &= I(C)([\![\phi]\!]^I) \\ [\![\langle\alpha\rangle\phi]\!]^I &= [\![\alpha]\!]^I \circ [\![\phi]\!]^I \\ [\![[\alpha]\phi]\!]^I &= [\![\neg\langle\alpha\rangle\neg\phi]\!]^I \end{aligned}$$

Definition (Program semantics) $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

$$\begin{aligned} [\![x' = \theta \,\&\, H]\!]^I &= \{(\varphi(0)|_{\{x'\}^\complement}, \varphi(r)) \ : \ I, \varphi \models x' = \theta \land H\} \\ [\![\alpha \cup \beta]\!]^I &= [\![\alpha]\!]^I \cup [\![\beta]\!]^I \\ [\![\alpha ; \beta]\!]^I &= [\![\alpha]\!]^I \circ [\![\beta]\!]^I \\ [\![\alpha^*]\!]^I &= ([\![\alpha]\!]^I)^* = \bigcup_{n\in\mathbb{N}} [\![\alpha^n]\!]^I \end{aligned}$$

Differential-form Differential Dynamic Logic: Semantics

Definition (Term semantics) $(\llbracket\cdot\rrbracket : \mathrm{Trm} \to (\mathcal{S} \to \mathbb{R}))$

$$\begin{aligned}
\llbracket x\rrbracket^I u &= u(x) && \text{for variable } x \in \mathcal{V}\\
\llbracket x'\rrbracket^I u &= u(x') && \text{for differential symbol } x' \in \mathcal{V}'\\
\llbracket f(\theta_1,\dots,\theta_k)\rrbracket^I u &= I(f)\big(\llbracket\theta_1\rrbracket^I u,\dots,\llbracket\theta_k\rrbracket^I u\big) && \text{for function symbol } f\\
\llbracket\theta+\eta\rrbracket^I u &= \llbracket\theta\rrbracket^I u + \llbracket\eta\rrbracket^I u\\
\llbracket\theta\cdot\eta\rrbracket^I u &= \llbracket\theta\rrbracket^I u \cdot \llbracket\eta\rrbracket^I u\\
\llbracket(\theta)'\rrbracket^I u &= \sum_x u(x')\frac{\partial\llbracket\theta\rrbracket^I}{\partial x}(u) && = \sum_x u(x')\frac{\partial\llbracket\theta\rrbracket^I u_x^X}{\partial X}
\end{aligned}$$

Definition (d$\mathcal{L}$ semantics) $(\llbracket\cdot\rrbracket : \mathrm{Fml} \to \wp(\mathcal{S}))$

$$\begin{aligned}
\llbracket C(\phi)\rrbracket^I &= I(C)\big(\llbracket\phi\rrbracket^I\big)\\
\llbracket\langle\alpha\rangle\phi\rrbracket^I &= \llbracket\alpha\rrbracket^I \circ \llbracket\phi\rrbracket^I\\
\llbracket[\alpha]\phi\rrbracket^I &= \llbracket\neg\langle\alpha\rangle\neg\phi\rrbracket^I
\end{aligned}$$

Definition (Program semantics) $(\llbracket\cdot\rrbracket : \mathrm{HP} \to \wp(\mathcal{S}\times\mathcal{S}))$

Differential-form Differential Dynamic Logic: Semantics

Definition (Term semantics) $([\![\cdot]\!] : \mathrm{Trm} \to (\mathcal{S} \to \mathbb{R}))$

$$[\![(\theta)']\!]^I u \;=\; \sum_x u(x') \frac{\partial [\![\theta]\!]^I}{\partial x}(u) = \sum_x u(x') \frac{\partial [\![\theta]\!]^I u_x^X}{\partial X}$$

Definition (d$\mathcal{L}$ semantics) $([\![\cdot]\!] : \mathrm{Fml} \to \wp(\mathcal{S}))$

$$\begin{aligned}
[\![\theta \geq \eta]\!]^I &= \{u \;:\; [\![\theta]\!]^I u \geq [\![\eta]\!]^I u\} \\
[\![p(\theta_1, \ldots, \theta_k)]\!]^I &= \{u \;:\; ([\![\theta_1]\!]^I u, \ldots, [\![\theta_k]\!]^I u) \in I(p)\} \\
[\![C(\phi)]\!]^I &= I(C)\big([\![\phi]\!]^I\big) \\
[\![\neg\phi]\!]^I &= ([\![\phi]\!]^I)^{\complement} \\
[\![\phi \wedge \psi]\!]^I &= [\![\phi]\!]^I \cap [\![\psi]\!]^I \\
[\![\exists x\, \phi]\!]^I &= \{u \in \mathcal{S} \;:\; u_x^r \in [\![\phi]\!]^I \text{ for some } r \in \mathbb{R}\} \\
[\![\langle\alpha\rangle\phi]\!]^I &= [\![\alpha]\!]^I \circ [\![\phi]\!]^I = \{u \;:\; w \in [\![\phi]\!]^I \text{ for some } w \;(u, w) \in [\![\alpha]\!]^I\} \\
[\![[\alpha]\phi]\!]^I &= [\![\neg\langle\alpha\rangle\neg\phi]\!]^I = \{u \;:\; w \in [\![\phi]\!]^I \text{ for all } w \;(u, w) \in [\![\alpha]\!]^I\}
\end{aligned}$$

Definition (Program semantics) $([\![\cdot]\!] : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

Differential-form Differential Dynamic Logic: Semantics

Definition (Term semantics) $(\llbracket\cdot\rrbracket : \mathrm{Trm} \to (\mathcal{S} \to \mathbb{R}))$

$$\llbracket(\theta)'\rrbracket^I u = \sum_x u(x') \frac{\partial \llbracket\theta\rrbracket^I}{\partial x}(u) = \sum_x u(x') \frac{\partial \llbracket\theta\rrbracket^I u_x^X}{\partial X}$$

Definition (d$\mathcal{L}$ semantics) $(\llbracket\cdot\rrbracket : \mathrm{Fml} \to \wp(\mathcal{S}))$

$$\begin{aligned}
\llbracket C(\phi)\rrbracket^I &= I(C)(\llbracket\phi\rrbracket^I)\\
\llbracket\langle\alpha\rangle\phi\rrbracket^I &= \llbracket\alpha\rrbracket^I \circ \llbracket\phi\rrbracket^I\\
\llbracket[\alpha]\phi\rrbracket^I &= \llbracket\neg\langle\alpha\rangle\neg\phi\rrbracket^I
\end{aligned}$$

Definition (Program semantics) $(\llbracket\cdot\rrbracket : \mathrm{HP} \to \wp(\mathcal{S} \times \mathcal{S}))$

$$\begin{aligned}
\llbracket a\rrbracket^I &= I(a)\\
\llbracket x := \theta\rrbracket^I &= \{(u, w) \;:\; w = u \text{ except } \llbracket x\rrbracket^I w = \llbracket\theta\rrbracket^I u\}\\
\llbracket x' := \theta\rrbracket^I &= \{(u, w) \;:\; w = u \text{ except } \llbracket x'\rrbracket^I w = \llbracket\theta\rrbracket^I u\}\\
\llbracket ?H\rrbracket^I &= \{(u, u) \;:\; u \in \llbracket H\rrbracket^I\}\\
\llbracket x' = \theta \,\&\, H\rrbracket^I &= \{(\varphi(0)|_{\{x'\}^\complement}, \varphi(r)) \;:\; I, \varphi \models x' = \theta \land H\}
\end{aligned}$$