Non-Standard Semantics for Differential Dynamic Logic

Noah Abou El Wafa

December 18, 2020

Proving Properties of Differential Equations

1. Discretize:

$$[x' = f(x)]F \leftrightarrow \forall t \geq 0 \exists \varepsilon < 0 \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*](t \geq 0 \rightarrow \neg U_\varepsilon(\neg F))$$

Proving Properties of Differential Equations

1. Discretize:

$$[x' = f(x)]F \leftrightarrow \forall t \geq 0 \exists \varepsilon < 0 \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*](t \geq 0 \rightarrow \neg U_\varepsilon(\neg F))$$

2. Average:

$$\vDash x > 0 \rightarrow [x' = f(x)]x > 0 \quad \Leftarrow \quad \vDash x > 0 \rightarrow f(x) > 0$$

The hyperreals

Theorem (A. Robinson)

There is an extension $\mathbb{R}^*$ of $\mathbb{R}$ as ordered fields containing an infinitesimal ε.

Expanding $\mathrm{d}\mathcal{L}$

Plan: Redefine the semantics for $\mathrm{d}\mathcal{L}$ over the hyperreals.

Expanding $\mathrm{d}\mathcal{L}$

Plan: Redefine the semantics for $\mathrm{d}\mathcal{L}$ over the hyperreals.
First extend the syntax to allow to refer to ε and $\widehat{\ }$.

Expanding $\mathrm{d}\mathcal{L}$

Plan: Redefine the semantics for $\mathrm{d}\mathcal{L}$ over the hyperreals.
First extend the syntax to allow to refer to ε and $\widehat{\ }$.
The syntax for $\mathrm{d}\mathcal{L}^*$ is the syntax for $\mathrm{d}\mathcal{L}$ with an additional constant symbol ε and a unary function symbol $\widehat{\ }$:

Terms: $e ::= x \mid x' \mid c \mid e + \tilde{e} \mid e - \tilde{e} \mid e \cdot \tilde{e} \mid e/\tilde{e} \mid q \mid \varepsilon \mid \widehat{e}$

Formulas: $P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid \exists x P \mid [\alpha]P$

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

Semantics for $\mathrm{d}\mathcal{L}^*$

Definition

Let $\mathcal{V}$ be the set of variables. A hyperstate is a map $\omega : \mathcal{V} \to \mathbb{R}^*$. Write $\mathcal{S}^*$ for the set of hyperstates.

The semantics are defined almost entirely like the semantics for $\mathrm{d}\mathcal{L}$.

Semantics for $\mathrm{d}\mathcal{L}^*$

Definition

Let $\mathcal{V}$ be the set of variables. A hyperstate is a map $\omega : \mathcal{V} \to \mathbb{R}^*$. Write $\mathcal{S}^*$ for the set of hyperstates.

The semantics are defined almost entirely like the semantics for $\mathrm{d}\mathcal{L}$.

- $\omega_* [\![\varepsilon]\!] = \varepsilon$
- $\omega_* [\![\widehat{e}]\!] = \widehat{e}$

Write $\vDash_*$ for those semantics.

Definition (Semantics of ODE programs)

For a continuous program $(\omega, \nu) \in [\![x' = f(x) \,\&\, Q]\!]_*$ exactly if there is $r \in \mathbb{R}^*$ finite and a map

$$\varphi : [0, r]^* \to \mathcal{S}^*, \quad t \mapsto \varphi_t$$

such that $\varphi_0 = \omega$ except at x', $\varphi_r = \nu$ and $\varphi \vDash_* x' = f(x) \,\&\, Q$. Here $\varphi \vDash_* x' = f(x) \,\&\, Q$ abbreviates the statement that $\varphi_z(y) = \varphi_0(y)$ for all $y \in \mathcal{V} \setminus \{x, x'\}$ whenever $z \in [0, r]^*$ and for all $n \in \mathbb{N}^*$ with $n \cdot \varepsilon \leq r$:

1. $\varphi_{n\cdot\varepsilon}(x) = W^n(\varphi_0(x))$, where W^n is the hyperreal walk,
2. $z \mapsto \varphi_z(x)$ is constant on $[n \cdot \varepsilon, (n+1) \cdot \varepsilon)^*$ and
3. $\varphi_{n\cdot\varepsilon} \in [\![x' = f(x) \wedge Q]\!]_*$.

Transfer principle

Theorem (ODE Transfer Principle)

For $\mathcal{L}$-formulas $p(x), q(x)$ and a standard state $\omega \in \mathcal{S}$. Equivalent are

- $\omega \vDash [x' = f(x) \;\&\; q(x)]p(x)$
- $\omega \vDash_* [x' = f(x) \;\&\; q(\widehat{x}) \wedge \mathrm{fin}(x)]p(\widehat{x})$

A proof calculus for $\mathrm{d}\mathcal{L}^*$

We consider a proof calculus $\vdash_*$ for $\mathrm{d}\mathcal{L}^*$:

A proof calculus for $\mathrm{d}\mathcal{L}^*$

We consider a proof calculus $\vdash_*$ for $\mathrm{d}\mathcal{L}^*$:

- Base: sequent calculus
- $\vdash_* P$ for all first-order $\mathrm{d}\mathcal{L}^*$ formulas with $\mathbb{R}^* \vDash P$
- $\vdash_*$ contains the axiom $[:=]$ and the proof rules G and $\mathrm{M}[\cdot]$

A proof calculus for $\mathrm{d}\mathcal{L}^*$

We consider a proof calculus $\vdash_*$ for $\mathrm{d}\mathcal{L}^*$:

- Base: sequent calculus
- $\vdash_* P$ for all first-order $\mathrm{d}\mathcal{L}^*$ formulas with $\mathbb{R}^* \vDash P$
- $\vdash_*$ contains the axiom $[:=]$ and the proof rules G and $\mathrm{M}[\cdot]$

This calculus is sound.

A proof calculus for $\mathrm{d}\mathcal{L}^*$

We consider a proof calculus $\vdash_*$ for $\mathrm{d}\mathcal{L}^*$:

- Base: sequent calculus
- $\vdash_* P$ for all first-order $\mathrm{d}\mathcal{L}^*$ formulas with $\mathbb{R}^* \vDash P$
- $\vdash_*$ contains the axiom $[:=]$ and the proof rules G and $\mathrm{M}[\cdot]$

This calculus is sound.
The axioms DG and DC are also sound for $\vDash_*$.

A Differential Invariant Proof Rule

We can add another sound proof rule DI^* to $\vdash_*$ to get:

Theorem

For a modality free $\mathrm{d}\mathcal{L}$-formula $p(x)$ the following are equivalent

1. $\vdash_* p(x) \to [x' = f(x) \,\&\, q(x)]p(x)$
2. $\vdash_* p(x) \wedge q(x) \to [x := x + \varepsilon f(x)](q(x) \to p(x))$

A Differential Invariant Proof Rule

We can add another sound proof rule DI^* to $\vdash_*$ to get:

Theorem

For a modality free $\mathrm{d}\mathcal{L}$-formula $p(x)$ the following are equivalent

1. $\vdash_* p(x) \to [x' = f(x) \,\&\, q(x)]p(x)$
2. $\vdash_* p(x) \wedge q(x) \to [x := x + \varepsilon f(x)](q(x) \to p(x))$

Remark: It is crucial that the formula $p(x)$ does not contain $\widehat{\ }$.

A Differential Invariant Proof Rule

We can add another sound proof rule DI^* to $\vdash_*$ to get:

Theorem

For a modality free $\mathrm{d}\mathcal{L}$-formula $p(x)$ the following are equivalent

1. $\vdash_* p(x) \to [x' = f(x) \,\&\, q(x)]p(x)$
2. $\vdash_* p(x) \wedge q(x) \to [x := x + \varepsilon f(x)](q(x) \to p(x))$

Remark: It is crucial that the formula $p(x)$ does not contain $\widehat{\ }$. But f may contain ε.

A Differential Invariant Proof Rule

We can add another sound proof rule DI^* to $\vdash_*$ to get:

Theorem

For a modality free $\mathrm{d}\mathcal{L}$-formula $p(x)$ the following are equivalent

1. $\vdash_* p(x) \to [x' = f(x) \,\&\, q(x)]p(x)$
2. $\vdash_* p(x) \wedge q(x) \to [x := x + \varepsilon f(x)](q(x) \to p(x))$

Remark: It is crucial that the formula $p(x)$ does not contain $\widehat{\ }$. But f may contain ε.

Example

Proving $x > 0 \to [x' = -x]x > 0$ is equivalent to proving $x > 0 \to x - \varepsilon x > 0$.

Proving more differential invariants

How can we prove differential invariants containing hats?

Proving more differential invariants

How can we prove differential invariants containing hats? Track the error.

Proving more differential invariants

How can we prove differential invariants containing hats? Track the error.

Idea: Introduce a ghost variable $\rho = x - \widehat{x}$.

Proving more differential invariants

How can we prove differential invariants containing hats? Track the error.

Idea: Introduce a ghost variable $\rho = x - \widehat{x}$.

Small errors stay small:

Theorem

For any $m > 1$ and any hat-free term g the axiom

$$\rho \approx 0 \land \mathrm{fin}(g) \to [\rho' = g \cdot \varepsilon^m]\rho \approx 0$$

is sound for $\models_*$.

Question: Can every differential invariant, including those containing hats, be proved in (a modification of) $\vdash_*$.