A Logic of Proofs for Differential Dynamic Logic

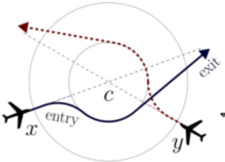
Toward Independently Checkable Proof Certificates for Differential Dynamic Logic

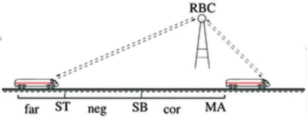
Nathan Fulton   Andrè Platzer
Carnegie Mellon University
CPP'16

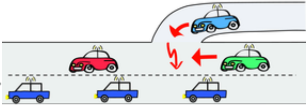
January 19, 2016

Motivation

Strong evidence that Cyber-Physical Systems are safe.

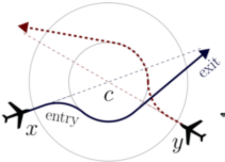


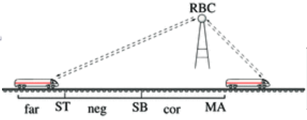


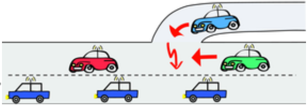


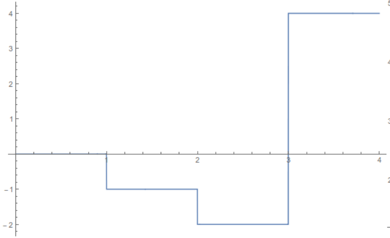
Motivation

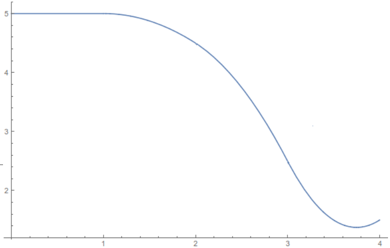
Strong evidence that Cyber-Physical Systems are safe.



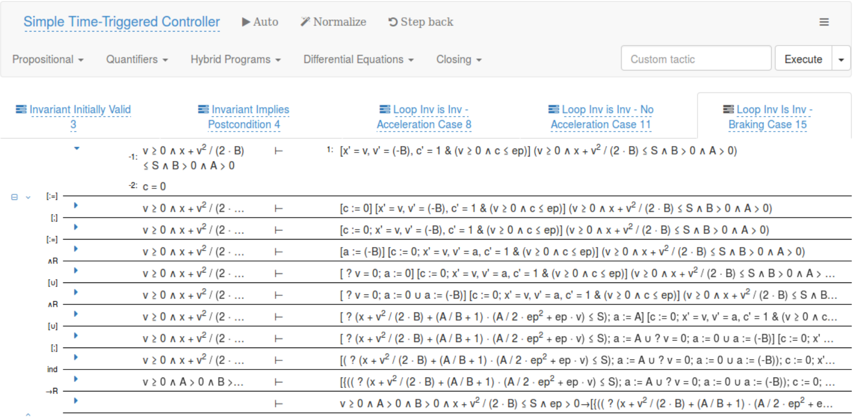








KeYmaera X



Simple Time-Triggered Controller
▶ Auto
Normalize
Step back
Propositional
Quantifiers
Hybrid Programs
Differential Equations
Closing
Custom tactic
Execute
Invariant Initially Valid 3
Invariant Implies Postcondition 4
Loop Inv is Inv - Acceleration Case 8
Loop Inv is Inv - No Acceleration Case 11
Loop Inv Is Inv - Braking Case 15
-1: v ≥ 0 ∧ x + v² / (2 · B) ≤ S ∧ B > 0 ∧ A > 0
-2: c = 0
⊢
1: [x' = v, v' = (-B), c' = 1 & (v ≥ 0 ∧ c ≤ ep)] (v ≥ 0 ∧ x + v² / (2 · B) ≤ S ∧ B > 0 ∧ A > 0)
[:=]
v ≥ 0 ∧ x + v² / (2 · … ⊢ [c := 0] [x' = v, v' = (-B), c' = 1 & (v ≥ 0 ∧ c ≤ ep)] (v ≥ 0 ∧ x + v² / (2 · B) ≤ S ∧ B > 0 ∧ A > 0)
[;]
v ≥ 0 ∧ x + v² / (2 · … ⊢ [c := 0; x' = v, v' = (-B), c' = 1 & (v ≥ 0 ∧ c ≤ ep)] (v ≥ 0 ∧ x + v² / (2 · B) ≤ S ∧ B > 0 ∧ A > 0)
[:=]
v ≥ 0 ∧ x + v² / (2 · … ⊢ [a := (-B)] [c := 0; x' = v, v' = a, c' = 1 & (v ≥ 0 ∧ c ≤ ep)] (v ≥ 0 ∧ x + v² / (2 · B) ≤ S ∧ B > 0 ∧ A > 0)
∧R
v ≥ 0 ∧ x + v² / (2 · … ⊢ [? v = 0; a := 0] [c := 0; x' = v, v' = a, c' = 1 & (v ≥ 0 ∧ c ≤ ep)] (v ≥ 0 ∧ x + v² / (2 · B) ≤ S ∧ B > 0 ∧ A > …
[∪]
v ≥ 0 ∧ x + v² / (2 · … ⊢ [? v = 0; a := 0 ∪ a := (-B)] [c := 0; x' = v, v' = a, c' = 1 & (v ≥ 0 ∧ c ≤ ep)] (v ≥ 0 ∧ x + v² / (2 · B) ≤ S ∧ B…
∧R
v ≥ 0 ∧ x + v² / (2 · … ⊢ [? (x + v² / (2 · B) + (A / B + 1) · (A / 2 · ep² + ep · v) ≤ S); a := A] [c := 0; x' = v, v' = a, c' = 1 & (v ≥ 0 ∧ c…
[∪]
v ≥ 0 ∧ x + v² / (2 · … ⊢ [? (x + v² / (2 · B) + (A / B + 1) · (A / 2 · ep² + ep · v) ≤ S); a := A ∪ ? v = 0; a := 0 ∪ a := (-B)] [c := 0; x' …
[;]
v ≥ 0 ∧ x + v² / (2 · … ⊢ [(? (x + v² / (2 · B) + (A / B + 1) · (A / 2 · ep² + ep · v) ≤ S); a := A ∪ ? v = 0; a := 0 ∪ a := (-B)); c := 0; x'…
ind
v ≥ 0 ∧ A > 0 ∧ B >… ⊢ [{((? (x + v² / (2 · B) + (A / B + 1) · (A / 2 · ep² + ep · v) ≤ S); a := A ∪ ? v = 0; a := 0 ∪ a := (-B)); c := 0; …
→R
⊢ v ≥ 0 ∧ A > 0 ∧ B > 0 ∧ x + v² / (2 · B) ≤ S ∧ ep > 0→[{((? (x + v² / (2 · B) + (A / B + 1) · (A / 2 · ep² + e…

Criteria for Evidence of a Successful Verification Effort

- ☑ Hybrid Systems Proofs (via KeYmaera X)
- ☐ Persistent – truth-preservation is insufficient!
- ☐ Permanent – Tactics are not proofs
- ☐ Portable – Between machines, between logics

Approach

$$e : \phi$$

Approach

$$e : \phi$$

Outline:

- The Language of Differential Dynamic Logic
- Uniform Substitution Calculus of d$\mathcal{L}$
- LPd$\mathcal{L}$

Hybrid Programs Model Cyber-Physical Systems

Definition (Hybrid Programs)

Assign	$x := \theta$
Test	$?\varphi$
Sequence	$\alpha; \beta$
Choice	$\alpha \cup \beta$
Iteration	α^*

Hybrid Programs Model Cyber-Physical Systems

Definition (Hybrid Programs)

Assign	$x := \theta$
Test	$?\varphi$
Sequence	$\alpha; \beta$
Choice	$\alpha \cup \beta$
Iteration	α^*
ODEs	$\{x_1' = \theta_1, \dots, x_n' = \theta_n \& \varphi\}$

Example

$$\Big(\underbrace{(acc := A \cup acc := 0)}_{\textit{Control}}\ ;\ \underbrace{\{pos' = vel,\ vel' = acc\}}_{\textit{Physical System Model}}\Big)^*$$

d$\mathcal{L}$

FOL over Real Closed Fields $+ [\alpha]\varphi + \langle\alpha\rangle\varphi$

Example

$$\underbrace{vel \geq 0 \land A > 0}_{\text{initial condition}} \rightarrow$$

$$[(\underbrace{(acc := A \cup acc := 0)}_{ctrl}\ ;\ \underbrace{\{pos' = vel,\ vel' = acc\}}_{plant})^*]\ \underbrace{vel \geq 0}_{\text{postcondition}}$$

Deduction in Differential Dynamic Logic

$$\dfrac{v \geq 0, z < m \vdash \forall t \geq 0 [z := -\dfrac{b}{2}t^2 + vt + z] z \leq m}{v \geq 0, z < m \vdash [z' = v, v' = -b] z \leq m} \textsc{DiffSolve}$$

Uniform Substitution Isolates Binding Structure

DiffSolve as a single axiom:

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

Sound **uniform substitutions** are used in deductions:

$$\frac{\varphi}{\sigma(\varphi)}\mathrm{US}$$

Significant Features of d$\mathcal{L}$

$$\textsc{BoxChoice}\quad \frac{\Gamma \vdash [\alpha]\varphi \qquad \Gamma \vdash [\beta]\varphi}{\Gamma \vdash [\alpha \cup \beta]\varphi}$$

Significant Features of d$\mathcal{L}$

$$\textsc{BoxChoice}\ \frac{\Gamma \vdash [\alpha]\varphi \qquad \Gamma \vdash [\beta]\varphi}{\Gamma \vdash [\alpha \cup \beta]\varphi}$$

$$\frac{}{\Gamma \vdash \underbrace{[x := 4 \cup x := 5]x > 3}_{\psi}}$$

Significant Features of d$\mathcal{L}$

$$\frac{\Gamma \vdash [\alpha]\varphi \qquad \Gamma \vdash [\beta]\varphi}{\Gamma \vdash [\alpha \cup \beta]\varphi}\ \textsc{BoxChoice}$$

$$\frac{\underline{[a \cup b]p(?) \leftrightarrow [a]p(?) \wedge [b]p(?)}}{\Gamma \vdash \underbrace{[x := 4 \cup x := 5]x > 3}_{\psi}}$$

$\sigma =$

$$a \leadsto x := 4$$

$$b \leadsto x := 5$$

$$p(?) \leadsto x > 3$$

Significant Features of d$\mathcal{L}$

$$\textsc{BoxChoice}\quad \frac{\Gamma \vdash [\alpha]\varphi \qquad \Gamma \vdash [\beta]\varphi}{\Gamma \vdash [\alpha \cup \beta]\varphi}$$

$$\dfrac{\dfrac{[a \cup b]p(?) \leftrightarrow [a]p(?) \land [b]p(?)}{\psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3}}{\Gamma \vdash \underbrace{[x := 4 \cup x := 5]x > 3}_{\psi}}$$

$\sigma =$

$$a \rightsquigarrow x := 4$$

$$b \rightsquigarrow x := 5$$

$$p(?) \rightsquigarrow x > 3$$

Significant Features of d$\mathcal{L}$

$$\frac{\textsc{BoxChoice} \quad \Gamma \vdash [\alpha]\varphi \qquad \Gamma \vdash [\beta]\varphi}{\Gamma \vdash [\alpha \cup \beta]\varphi}$$

$$\dfrac{\dfrac{[a \cup b]p(?) \leftrightarrow [a]p(?) \wedge [b]p(?)}{\psi \leftrightarrow [x := 4]x > 3 \wedge [x := 5]x > 3} \qquad \dfrac{}{\Gamma, \psi \leftrightarrow [x := 4]x > 3 \wedge [x := 5]x > 3 \vdash \psi}}{\Gamma \vdash \underbrace{[x := 4 \cup x := 5]x > 3}_{\psi}}$$

$\sigma =$

$$a \rightsquigarrow x := 4$$

$$b \rightsquigarrow x := 5$$

$$p(?) \rightsquigarrow x > 3$$

Significant Features of d$\mathcal{L}$

$$\textsc{BoxChoice}\quad \frac{\Gamma \vdash [\alpha]\varphi \qquad \Gamma \vdash [\beta]\varphi}{\Gamma \vdash [\alpha \cup \beta]\varphi}$$

$$\frac{\dfrac{[a \cup b]p(?) \leftrightarrow [a]p(?) \wedge [b]p(?)}{\psi \leftrightarrow [x := 4]x > 3 \wedge [x := 5]x > 3} \qquad \dfrac{\dfrac{}{\Gamma, \cdots \vdash [x := 4]x > 3 \wedge [x := 5]x > 3}}{\Gamma, \psi \leftrightarrow [x := 4]x > 3 \wedge [x := 5]x > 3 \vdash \psi}}{\Gamma \vdash \underbrace{[x := 4 \cup x := 5]x > 3}_{\psi}}$$

$\sigma =$

$$a \rightsquigarrow x := 4$$

$$b \rightsquigarrow x := 5$$

$$p(?) \rightsquigarrow x > 3$$

Significant Features of d$\mathcal{L}$

$$\textsc{BoxChoice}\ \frac{\Gamma \vdash [\alpha]\varphi \qquad \Gamma \vdash [\beta]\varphi}{\Gamma \vdash [\alpha \cup \beta]\varphi}$$

$$\dfrac{\dfrac{[a \cup b]p(?) \leftrightarrow [a]p(?) \land [b]p(?)}{\psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3} \qquad \dfrac{\dfrac{\dfrac{}{\Gamma \vdash [x := 4]x > 3 \land [x := 5]x > 3}}{\Gamma, \cdots \vdash [x := 4]x > 3 \land [x := 5]x > 3}}{\Gamma, \psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3 \vdash \psi}}{\Gamma \vdash \underbrace{[x := 4 \cup x := 5]x > 3}_{\psi}}$$

$\sigma =$

$$a \rightsquigarrow x := 4$$

$$b \rightsquigarrow x := 5$$

$$p(?) \rightsquigarrow x > 3$$

Significant Features of d$\mathcal{L}$

$$\textsc{BoxChoice}\ \frac{\Gamma \vdash [\alpha]\varphi \qquad \Gamma \vdash [\beta]\varphi}{\Gamma \vdash [\alpha \cup \beta]\varphi}$$

$$\dfrac{\dfrac{[a \cup b]p(?) \leftrightarrow [a]p(?) \wedge [b]p(?)}{\psi \leftrightarrow [x := 4]x > 3 \wedge [x := 5]x > 3} \qquad \dfrac{\dfrac{\dfrac{\Gamma \vdash [x := 4]x > 3 \qquad \Gamma \vdash [x := 5]x > 3}{\Gamma \vdash [x := 4]x > 3 \wedge [x := 5]x > 3}}{\Gamma, \cdots \vdash [x := 4]x > 3 \wedge [x := 5]x > 3}}{\Gamma, \psi \leftrightarrow [x := 4]x > 3 \wedge [x := 5]x > 3 \vdash \psi}}{\Gamma \vdash \underbrace{[x := 4 \cup x := 5]x > 3}_{\psi}}$$

$\sigma =$

$$a \rightsquigarrow x := 4$$

$$b \rightsquigarrow x := 5$$

$$p(?) \rightsquigarrow x > 3$$

Contribution: A Logic of Proofs for d$\mathcal{L}$

LPd$\mathcal{L}$ extends the grammar of d$\mathcal{L}$ with formulas of the form

$$\underbrace{e}_{\textbf{LPd}\mathcal{L}\textbf{ proof term}} : \underbrace{\varphi}_{\mathrm{d}\mathcal{L}\textit{formula}}$$

Contribution: A Logic of Proofs for d$\mathcal{L}$

LPd$\mathcal{L}$ extends the grammar of d$\mathcal{L}$ with formulas of the form

$$\underbrace{e}_{\textbf{LPd}\mathcal{L}\textbf{ proof term}} \quad : \quad \underbrace{\varphi}_{\text{d}\mathcal{L}\textit{formula}}$$

$\langle e, d \ \rangle ::= \ c_\phi$

Example (Proof Constants)

$$(i_{[:=]}) : ([x := t]p(x) \leftrightarrow p(t))$$
$$(j_{x>y \wedge y>z \rightarrow x>z}) : (x > y \wedge y > z \rightarrow x > z)$$

Contribution: A Logic of Proofs for d$\mathcal{L}$

LPd$\mathcal{L}$ extends the grammar of d$\mathcal{L}$ with formulas of the form

$$\underbrace{e}_{\textbf{LPd}\mathcal{L}\textbf{ proof term}} : \underbrace{\varphi}_{\text{d}\mathcal{L}\textit{formula}}$$

$$\begin{aligned} \langle e, d \rangle ::= \;& c_\phi \\ \mid \;& e \wedge d \end{aligned}$$

Example (Conjunctions)

$$(i_{:=} \wedge j_{x>0}) : (([x := t]p(x) \leftrightarrow p(t)) \wedge x > 0)$$

Contribution: A Logic of Proofs for d$\mathcal{L}$

LPd$\mathcal{L}$ extends the grammar of d$\mathcal{L}$ with formulas of the form

$$\underbrace{e}_{\textbf{LPd}\mathcal{L}\textbf{ proof term}} : \underbrace{\varphi}_{\text{d}\mathcal{L}\textit{formula}}$$

$$\begin{aligned}\langle e, d\ \rangle ::= &\ c_\phi \\ |&\quad e \wedge d \\ |&\quad e \bullet d \mid e \bullet_{\leftarrow} d \mid e \bullet_{\rightarrow} d\end{aligned}$$

Example ($\bullet$)

If

$$e : \varphi \rightarrow \psi \tag{1}$$
$$d : \varphi \tag{2}$$

Then $e \bullet d : \psi$.

Directional application performs a similar operation on equivalences.

Contribution: A Logic of Proofs for d$\mathcal{L}$

LPd$\mathcal{L}$ extends the grammar of d$\mathcal{L}$ with formulas of the form

$$\underbrace{e}_{\textbf{LPd}\mathcal{L}\textbf{ proof term}} \quad : \quad \underbrace{\varphi}_{\mathrm{d}\mathcal{L}\textit{formula}}$$

$$\begin{aligned}\langle e, d\ \rangle \ ::= \ & c_\phi \\ | \quad & e \wedge d \\ | \quad & e \bullet d \mid e \bullet_{\leftarrow} d \mid e \bullet_{\rightarrow} d \\ | \quad & \sigma e \mid \mathscr{B} e\end{aligned}$$

Example (Uniform Substitution of Axiom $[x := t]p(x) \leftrightarrow p(t)$)

$$\sigma_{\{t \mapsto 0\ ,\ p(\cdot) \mapsto \cdot \geq 0\}}(i_{[:=]}) : [x := 0]x \geq 0 \leftrightarrow 0 \geq 0$$

Contribution: A Logic of Proofs for d$\mathcal{L}$

LPd$\mathcal{L}$ extends the grammar of d$\mathcal{L}$ with formulas of the form

$$\underbrace{e}_{\textbf{LPd}\mathcal{L}\textbf{ proof term}} \quad : \quad \underbrace{\varphi}_{\mathrm{d}\mathcal{L}\textit{formula}}$$

$$\begin{aligned}
\langle e, d\,\rangle \;::=\;& c_\phi \\
\mid\;& e \wedge d \\
\mid\;& e \bullet d \mid e \bullet_\leftarrow d \mid e \bullet_\rightarrow d \\
\mid\;& \sigma e \mid \mathscr{B} e \\
\mid\;& \mathrm{CT}_\sigma e \mid \mathrm{CQ}_\sigma e \mid \mathrm{CE}_\sigma e
\end{aligned}$$

Example (US Instances of Proof Rules)

$CE_{\{t \rightsquigarrow 0\ ,\ p(\cdot) \rightsquigarrow \cdot \geq 0\}}\, i_{[x:=t]p(t) \leftrightarrow p(x)}$:

$$([\{z' = a\}][x := 0]x \geq 0) \leftrightarrow ([\{z' = a\}]0 \geq 0)$$

Sampling of Axioms and Proof Rules

$$\phi \qquad \text{(d}\mathcal{L}\text{ Axiom)}$$

$$i_A : A \qquad \text{(d}\mathcal{L}\text{ Constants)}$$

$$\frac{e : \phi \qquad d : \psi}{(e \wedge d) : (\phi \wedge \psi)} \qquad \text{(And)}$$

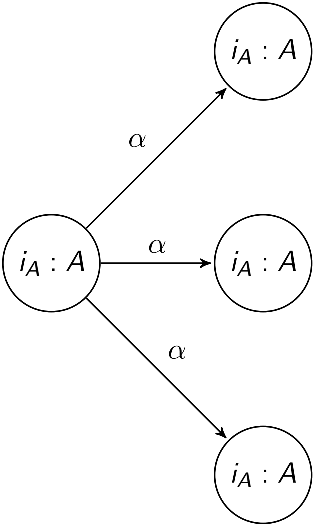
$$\frac{e : (\phi \rightarrow \psi) \qquad d : \phi}{e \bullet d : \psi} \qquad \text{(Application)}$$

$$\frac{e : \phi}{\sigma e : \sigma(\phi)} \qquad \text{(US Proof Term)}$$

$$\frac{\sigma e : \sigma(p(\bar{x}) \leftrightarrow q(\bar{x}))}{\mathrm{CE}_\sigma e : \sigma(C(p(\bar{x}) \leftrightarrow C(q(\bar{x})))} \qquad (\mathrm{CE}_\sigma)$$

Only side-condition: admissibility of σs.

Semantics of LPd$\mathcal{L}$



- $[\![\phi]\!]^I = [\![\phi]\!]^I_{\mathsf{d}\mathcal{L}}$
- $[\![i_A : A]\!]^I = S$ for d$\mathcal{L}$ axioms A
- $[\![j_T : T]\!] = S$ for $\mathsf{FOL}_{\mathbb{R}}$ tautologies T
- $[\![e \wedge d : \phi \wedge \psi]\!]^I =$ $[\![e : \phi]\!]^I \cap [\![d : \psi]\!]^I$
- $[\![e \bullet d : \phi]\!]^I =$ $\bigcup_\psi [\![e : (\psi \to \phi)]\!]^I \cap [\![d : \psi]\!]^I$
- ...

Correctness Properties

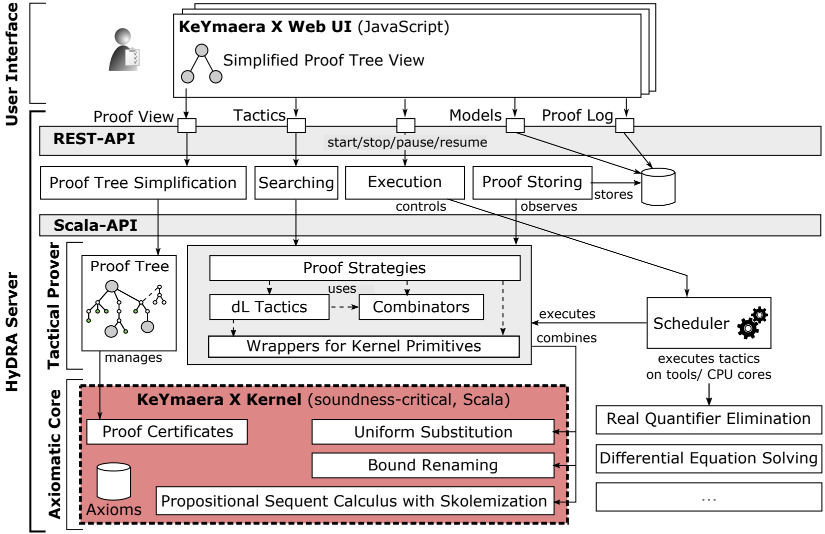
Theorem (Proof terms justify theorems)

Let e be a proof term and ϕ a d$\mathcal{L}$ *formula. If* $\vdash_{\mathsf{LPd}\mathcal{L}} e : \phi$ *then* $\vdash \phi$.

Correctness Properties

Theorem (Proof terms justify theorems)

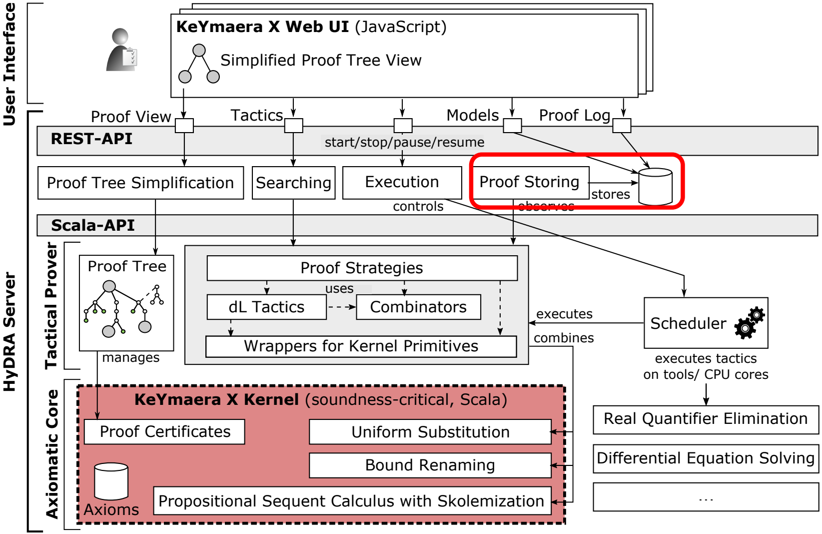
Let e be a proof term and ϕ a $\mathsf{d}\mathcal{L}$ formula. If $\vdash_{\mathsf{LPd}\mathcal{L}} e : \phi$ then $\vdash \phi$.



Correctness Properties

Theorem (Proof terms justify theorems)

Let e be a proof term and ϕ a d$\mathcal{L}$ formula. If $\vdash_{\mathrm{LPd}\mathcal{L}} e : \phi$ then $\vdash \phi$.



Adding Proof Terms Without Adding Soundness-Critical Code

Proof.

Case σe**.** Suppose that $\vdash_{\mathsf{LPd}\mathcal{L}} \sigma e : \phi$. By [a lemma], $\phi = \sigma(\phi')$ and $\vdash_{\mathsf{LPd}\mathcal{L}} e : \phi'$ for some ϕ'. The induction hypothesis for the smaller proof term e gives $\vdash_{\mathsf{d}\mathcal{L}} \phi'$. Therefore, $\vdash_{\mathsf{d}\mathcal{L}} \sigma(\phi')$ (i.e., ϕ) is provable by US. $\square$

```
def ProofChecker(e : ProofTerm, phi: Formula) = ...
  case UsubstTerm(e, phiPrime, usubst) => {
    val phiPrimeCert = ProofChecker(e, phiPrime)
    Provable.startProof(phi)
      .(UniformSubstitutionRule(
          usubst,
          phiPrime), 0)
      .(phiPrimeCert, 0)
  }
```

Ongoing Work

- Controller Synthesis from Non-deterministic Models
- A proof term construction semantics for the Bellerophon tactics language of KeYmaera X

Conclusion

LPd$\mathcal{L}$ provides **persistent permanent portable proofs**

Conclusion

LPd$\mathcal{L}$ provides **persistent permanent portable proofs**

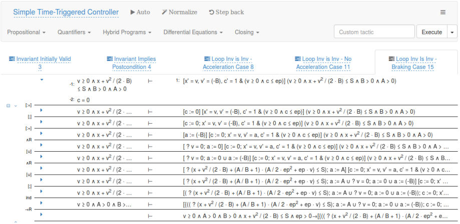
and furthermore **reifies** the structure of proofs

Conclusion

LPd$\mathcal{L}$ provides **persistent permanent portable proofs**

and furthermore **reifies** the structure of proofs
by **parsimoniously extending** existing theory and implementation.

$$
\begin{array}{rl}
\text{DW} & [x' = f(x) \,\&\, q(x)]q(x) \\
\text{DC} & \big([x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow [x' = f(x) \,\&\, q(x) \wedge r(x)]p(x)\big) \leftarrow [x' = f(x) \,\&\, q(x)]r(x) \\
\text{DE} & [x' = f(x) \,\&\, q(x)]p(x, x') \leftrightarrow [x' = f(x) \,\&\, q(x)][x' := f(x)]p(x, x') \\
\text{DI} & [x' = f(x) \,\&\, q(x)]p(x) \leftarrow \big(q(x) \rightarrow p(x) \wedge [x' = f(x) \,\&\, q(x)](p(x))'\big) \\
\text{DG} & [x' = f(x) \,\&\, q(x)]p(x) \leftrightarrow \exists y\, [x' = f(x), y' = a(x)y + b(x) \,\&\, q(x)]p(x) \\
\text{DS} & [x' = f \,\&\, q(x)]p(x) \leftrightarrow \forall t{\geq}0\, \big((\forall 0{\leq}s{\leq}t\, q(x + fs)) \rightarrow [x := x + ft]p(x)\big) \\
[' :=] & [x' := f]p(x') \leftrightarrow p(f) \\
+' & (f(\bar{x}) + g(\bar{x}))' = (f(\bar{x}))' + (g(\bar{x}))' \\
\cdot' & (f(\bar{x}) \cdot g(\bar{x}))' = (f(\bar{x}))' \cdot g(\bar{x}) + f(\bar{x}) \cdot (g(\bar{x}))' \\
\circ' & [y := g(x)][y' := 1]\big((f(g(x)))' = (f(y))' \cdot (g(x))'\big)
\end{array}
$$



keymaeraX.org · github.com/LS-Lab/KeYmaeraX-release
nfulton@nfulton.org