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.
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

Outline:

- The Language of Differential Dynamic Logic
- Uniform Substitution Calculus of $d\mathcal{L}$
- $LPd\mathcal{L}$
Definition (Hybrid Programs)

Assign $x := \theta$

Test $\mathcal{P}$

Sequence $\alpha; \beta$

Choice $\alpha \cup \beta$

Iteration $\alpha^*$
Definition (Hybrid Programs)

Assign \( x := \theta \)

Test \(?\varphi\)

Sequence \( \alpha; \beta \)

Choice \( \alpha \cup \beta \)

Iteration \( \alpha^* \)

ODEs \( \{x'_1 = \theta_1, \ldots, x'_n = \theta_n & \varphi\} \)
Example

\[
\left(\begin{array}{l}
\text{Control} \\
\quad \text{(acc := } A \cup \text{acc := } 0) ; \{\text{pos' = vel, vel' = acc}\}
\end{array}\right) \ast
\]

\[
\text{Physical System Model}
\]
FOL over Real Closed Fields + $[\alpha] \varphi + \langle \alpha \rangle \varphi$

Example

\[
vel \geq 0 \land A > 0 \rightarrow
\]
initial condition

\[
\left[ (\text{acc} := A \cup \text{acc} := 0) ; \{pos' = vel, \ vel' = acc\} )^* \right] \text{vel} \geq 0
\]
postcondition
\[
\forall t \geq 0[z := -\frac{b}{2}t^2 + vt + z]z \leq m
\]
\[
\nu \geq 0, z < m \vdash [z' = \nu, v' = -b]z \leq m
\]

\text{DiffSolve}
Uniform Substitution Isolates Binding Structure

DiffSolve as a single axiom:

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

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

$$ \frac{\varphi}{\sigma(\varphi)} \quad \text{US} $$
Significant Features of $d\mathcal{L}$

\[\text{BoxChoice} \quad \frac{\Gamma \vdash [\alpha] \varphi \quad \Gamma \vdash [\beta] \varphi}{\Gamma \vdash [\alpha \cup \beta] \varphi}\]
Significant Features of $d\mathcal{L}$

**BoxChoice**

\[
\begin{align*}
\Gamma &\vdash [\alpha] \varphi & \Gamma &\vdash [\beta] \varphi \\
\hline
\Gamma &\vdash [\alpha \cup \beta] \varphi
\end{align*}
\]

\[
\Gamma \vdash [x := 4 \cup x := 5] x > 3
\]

\[
\psi
\]
Significant Features of $\text{dL}$

**BoxChoice**

\[
\frac{\Gamma \vdash [\alpha] \varphi \quad \Gamma \vdash [\beta] \varphi}{\Gamma \vdash [\alpha \cup \beta] \varphi}
\]

\[ [a \cup b] p(?) \leftrightarrow [a] p(?) \land [b] p(?) \]

\[
\Gamma \vdash \left[ x := 4 \cup x := 5 \right] x > 3
\]

$\sigma =$

\[
\begin{align*}
a &\leadsto x := 4 \\
b &\leadsto x := 5 \\
p(?) &\leadsto x > 3
\end{align*}
\]
Significant Features of $d\mathcal{L}$

**BoxChoice**

\[
\Gamma \vdash [\alpha] \varphi \quad \Gamma \vdash [\beta] \varphi
\]

\[
\Gamma \vdash [\alpha \cup \beta] \varphi
\]

\[
[a \cup b]p(?) \leftrightarrow [a]p(?) \land [b]p(?)
\]

\[
\psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3
\]

\[
\Gamma \vdash [x := 4 \cup x := 5]x > 3
\]

\[
\psi
\]

\[
\sigma =
\]

\[
a \leadsto x := 4
\]

\[
b \leadsto x := 5
\]

\[
p(?) \leadsto x > 3
\]
**Significant Features of dL**

\[ \text{BoxChoice} \]

\[
\Gamma \vdash [\alpha] \varphi \quad \Gamma \vdash [\beta] \varphi
\]

\[
\Gamma \vdash [\alpha \cup \beta] \varphi
\]

\[
[a \cup b]p(?) \leftrightarrow [a]p(?) \land [b]p(?)
\]

\[
\psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3
\]

\[
\Gamma, \psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3 \vdash \psi
\]

\[
\Gamma \vdash [x := 4 \cup x := 5]x > 3
\]

\[
\psi
\]

\[
\sigma =
\]

\[
a \leadsto x := 4
\]

\[
b \leadsto x := 5
\]

\[
p(?) \leadsto x > 3
\]
Significant Features of $d\mathcal{L}$

**BoxChoice**

\[
\Gamma \vdash [\alpha] \varphi \quad \Gamma \vdash [\beta] \varphi \\
\hline
\Gamma \vdash [\alpha \cup \beta] \varphi
\]

\[
[a \cup b]p(?) \leftrightarrow [a]p(?) \land [b]p(?)
\]

\[
\psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3
\]

\[
\Gamma, \cdots \vdash [x := 4]x > 3 \land [x := 5]x > 3
\]

\[
\Gamma, \psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3 \vdash \psi
\]

\[
\Gamma \vdash [x := 4 \cup x := 5]x > 3
\]

\[
\psi
\]

\[
\sigma =
\]

\[
a \rightsquigarrow x := 4
\]

\[
b \rightsquigarrow x := 5
\]

\[
p(?) \rightsquigarrow x > 3
\]
Significant Features of dŁ

**BoxChoice**

\[
\Gamma \vdash [\alpha] \varphi \quad \Gamma \vdash [\beta] \varphi \\
\hline
\Gamma \vdash [\alpha \cup \beta] \varphi
\]

\[
[a \cup b] p(?) \leftrightarrow [a] p(?) \land [b] p(?)
\]

\[
\psi \leftrightarrow [x := 4] x > 3 \land [x := 5] x > 3
\]

\[
\Gamma \vdash [x := 4] x > 3 \land [x := 5] x > 3
\]

\[
\Gamma, \psi \leftrightarrow [x := 4] x > 3 \land [x := 5] x > 3 \vdash \psi
\]

\[
\Gamma \vdash [x := 4 \cup x := 5] x > 3 \quad \psi
\]

\[
\sigma =
\]

\[
a \leadsto x := 4
\]

\[
b \leadsto x := 5
\]

\[
p(?) \leadsto x > 3
\]
Significant Features of dℒ

**BoxChoice**

\[ \Gamma \vdash [\alpha] \varphi \quad \Gamma \vdash [\beta] \varphi \]

\[ \Gamma \vdash [\alpha \cup \beta] \varphi \]

\[ [a \cup b]p(?) \leftrightarrow [a]p(?) \land [b]p(?) \]

\[ \psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3 \]

\[ \Gamma \vdash [x := 4]x > 3 \quad \Gamma \vdash [x := 5]x > 3 \]

\[ \Gamma \vdash [x := 4]x > 3 \land [x := 5]x > 3 \]

\[ \Gamma, \cdot \cdot \cdot \vdash [x := 4]x > 3 \land [x := 5]x > 3 \]

\[ \Gamma, \psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3 \vdash \psi \]

\[ \Gamma \vdash [x := 4 \cup x := 5]x > 3 \]

\[ \psi \]

\[ \sigma = \]

\[ a \rightsquigarrow x := 4 \]

\[ b \rightsquigarrow x := 5 \]

\[ p(?) \rightsquigarrow x > 3 \]
LPdL extends the grammar of dL with formulas of the form

\[ \langle e, \phi \rangle ::= c \]
Contribution: A Logic of Proofs for d$L$

LP$dL$ extends the grammar of $dL$ with formulas of the form

\[
\langle e, d \rangle ::= c_\phi
\]

**Example (Proof Constants)**

\[
(i_{[:=]}): ([x := t]p(x) \leftrightarrow p(t))
\]

\[
(j_{x>y \land y>z \rightarrow x>z}): (x > y \land y > z \rightarrow x > z)
\]
Contribution: A Logic of Proofs for $d\mathcal{L}$

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

\[
\langle e, d \rangle ::= \ c_\phi \\
| \ e \land d
\]

Example (Conjunctions)

\[(i := \land j \geq 0) : \ ((\ [x := t] p(x) \leftrightarrow p(t)) \land x > 0)\]
Contribution: A Logic of Proofs for \( d\mathcal{L} \)

\( \text{LPd}\mathcal{L} \) extends the grammar of \( d\mathcal{L} \) with formulas of the form

\[
\langle e, d \rangle ::= c_\phi \\
\mid e \land d \\
\mid e \cdot d \mid e \cdot\leftarrow d \mid e \cdot\rightarrow d
\]

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.
LPdL extends the grammar of dL with formulas of the form

\[ \langle e, d \rangle :: = \begin{array}{l}
  c \phi \\
  e \land d \\
  e \cdot d \\
  e \cdot \leftarrow d \\
  e \cdot \rightarrow d \\
  \sigma e \\
  B e
\end{array} \]

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

\[ \sigma\{t \mapsto 0, p(\cdot) \mapsto \geq 0\}(i_{[\cdot := \ ]}) : \left[ x := 0 \right] x \geq 0 \leftrightarrow 0 \geq 0 \]
Contribution: A Logic of Proofs for dL

LPdL extends the grammar of dL with formulas of the form

\[
\langle e, d \rangle ::= c_\phi \\
| e \land d \\
| e \bullet d | e \bullet \leftarrow d | e \bullet \rightarrow d \\
| \sigma e | \mathcal{B} e \\
| \text{CT}_\sigma e | \text{CQ}_\sigma e | \text{CE}_\sigma e
\]

Example (US Instances of Proof Rules)

\[
\text{CE}_{\{t \sim 0, \, p(\cdot) \sim \cdot \geq 0\}} \ i_{[x := t]} p(t) \leftrightarrow p(x) :
\]

\[
([\{z' = a\}] [x := 0] x \geq 0) \leftrightarrow ([\{z' = a\}] 0 \geq 0)
\]
Sampling of Axioms and Proof Rules

\[ \phi \]
\[ i_A : A \]
\[ e : \phi \quad d : \psi \]
\[ (e \land d) : (\phi \land \psi) \]
\[ e : (\phi \rightarrow \psi) \quad d : \phi \]
\[ e \cdot d : \psi \]
\[ e : \phi \]
\[ \sigma e : \sigma(\phi) \]
\[ \sigma e : \sigma(p(\bar{x}) \leftrightarrow q(\bar{x})) \]
\[ \text{CE}_\sigma e : \sigma(C(p(\bar{x}) \leftrightarrow C(q(\bar{x})))) \]

(\text{dL Axiom})

(\text{dL Constants})

(And)

(Application)

(US Proof Term)

(CE_\sigma)

Only side-condition: admissibility of \(\sigma\)s.
Semantics of LPd\(\mathcal{L}\)

- \([\phi]^I = [\phi]_{d\mathcal{L}}^I\)
- \([i_A : A]^I = S\) for d\(\mathcal{L}\) axioms \(A\)
- \([j_T : T]^I = S\) for FOL\(^R\) tautologies \(T\)
- \([e \land d : \phi \land \psi]^I = [e : \phi]^I \cap [d : \psi]^I\)
- \([e \bullet d : \phi]^I = \bigcup_{\psi} [e : (\psi \rightarrow \phi)]^I \cap [d : \psi]^I\)
- \(\ldots\)
Correctness Properties

Theorem (Proof terms justify theorems)

Let $\alpha$ be a proof term and $\phi$ a $d\mathcal{L}$ formula. If $\vdash_{LPd\mathcal{L}} e : \phi$ then $\vdash \phi$. 
Theorem (Proof terms justify theorems)

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

KeYmaera X Web UI (JavaScript)
Simplified Proof Tree View

KeYmaera X Kernel (soundness-critical, Scala)
Real Quantifier Elimination
Bound Renaming
Propositional Sequent Calculus with Skolemization
Differential Equation Solving
Uniform Substitution
Bound Renaming
Propositional Sequent Calculus with Skolemization

REST-API
Proof View
Tactics
Models
Proof Log
start/stop/pause/resume

Scala-API
Proof Tree Simplification
Searching
Execution
Proof Storing
stores
controls

HYDRA Server
Tactical Prover
Proof Tree
 Proof Strategies
$dL$ Tactics
Combinators
Wrappers for Kernel Primitives

Axiomatic Core
KeYmaera X Kernel (soundness-critical, Scala)
Proof Certificates
Uniform Substitution
Bound Renaming
Propositional Sequent Calculus with Skolemization

Scheduler
executes tactics on tools/ CPU cores
manages
Proof Tree
uses
executes
combines

Scheduler
Real Quantifier Elimination
Differential Equation Solving
…
Correctness Properties

**Theorem (Proof terms justify theorems)**

*Let* \( e \) *be a proof term and* \( \phi \) *a d\( \mathcal{L} \) formula. If* \( \vdash_{LPd\mathcal{L}} e : \phi \) *then* \( \vdash \phi \).
Adding Proof Terms Without Adding Soundness-Critical Code

Proof.

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

```
1  def ProofChecker(e : ProofTerm, phi : Formula) = ...
2   case UsubstTerm(e, phiPrime, usubst) => {
3       val phiPrimeCert = ProofChecker(e, phiPrime)
4       Provable.startProof(phi)
5          .(UniformSubstitutionRule(
6            usubst,
7            phiPrime), 0)
8          .(phiPrimeCert, 0)
9     }
```
Ongoing Work

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

LPdL provides **persistent permanent portable proofs**
Conclusion

LPdŁ provides persistent permanent portable proofs

and furthermore reifies the structure of proofs
Conclusion

LPdŁ provides **persistent permanent portable proofs** and furthermore **reifies** the structure of proofs by **parsimoniously extending** existing theory and implementation.

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

nfulton@nfulton.org