A Logic of Proofs for Differential Dynamic Logic

Toward Independently Checkable Proof Certificates for Differential Dynamic Logic

Nathan Fulton    André Platzer
Carnegie Mellon University
CPP’16

February 10, 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 $d\mathcal{L}$
- $LPd\mathcal{L}$
Hybrid Programs Model Cyber-Physical Systems

Definition (Hybrid Programs)

- **Assign** $x := \theta$
- **Test** $?\varphi$
- **Sequence** $\alpha; \beta$
- **Choice** $\alpha \cup \beta$
- **Iteration** $\alpha^*$
Hybrid Programs Model Cyber-Physical Systems

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

\[
\begin{align*}
\left( \text{acc} &:= A \cup \text{acc} := 0 \right) ; \\
\{ \text{pos}' = \text{vel}, \ \text{vel}' = \text{acc} \}^* \\
\end{align*}
\]

Control \hspace{2cm} \text{Physical System Model}
FOL over Real Closed Fields + $[\alpha] \varphi + \langle \alpha \rangle \varphi$

Example

$\left( vel \geq 0 \land A > 0 \rightarrow \right.$

\begin{align*}
&\text{initial condition} \\
&[[ (acc := A \cup acc := 0) ; \{pos' = vel, \ vel' = acc\} ]^* ] \\
&\text{ctrl} \hspace{5cm} \text{plant} \\
&\text{vel} \geq 0 \\
&\text{postcondition}
\end{align*}
\(v \geq 0, z < m \vdash \forall t \geq 0[z := -\frac{b}{2}t^2 + vt + z]z \leq m\)

\(\frac{}{v \geq 0, z < m \vdash [z' = v, v' = -b]z \leq m}\)

\(\text{DiffSolve}\)
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 dL

BoxChoice

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

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

**BoxChoice**

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

$$
\Gamma \vdash \left\{ x := 4 \cup x := 5 \right\} x > 3
$$

$$
\psi
$$
Significant Features of d\(\mathcal{L}\)

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

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

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

\(\psi\)

\[
\sigma = \begin{cases} 
\text{a \mapsto x := 4} \\
\text{b \mapsto x := 5} \\
p(?) \mapsto x > 3
\end{cases}
\]
Significant Features of $\mathcal{dL}$

**BoxChoice**

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

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

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

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

\[
\sigma =
\]

\[
a \leadsto x := 4
\]

\[
b \leadsto x := 5
\]

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

**BoxChoice**

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

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

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

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

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

\[
\psi
\]

\[
\sigma =
\]

\[
a \rightsquigarrow x := 4
\]

\[
b \rightsquigarrow x := 5
\]

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

**BoxChoice**

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

\[
[a \cup b]p(?) \leftrightarrow [a]p(?) \land [b]p(?) \\
\psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3 \\
\Gamma, \cdots \vdash [x := 4]x > 3 \land [x := 5]x > 3 \\
\Gamma, \psi \leftrightarrow [x := 4]x > 3 \land [x := 5]x > 3 \vdash \psi
\]

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

\[
\psi
\]

\[
\sigma =
\]

\[
a \sim x := 4
\]

\[
b \sim x := 5
\]

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

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

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

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

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

\[
\sigma =
\]

\[
a \leadsto x := 4
\]

\[
b \leadsto x := 5
\]

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

BoxChoice

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

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

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

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

\[ \sigma = \]

\[ a \leadsto x := 4 \]

\[ b \leadsto x := 5 \]

\[ p(?) \leadsto x > 3 \]
LPdŁ extends the grammar of dŁ with formulas of the form

\[
\begin{align*}
\langle e, \varphi \rangle \quad &
\begin{cases}
\text{LPdŁ proof term} & \text{dŁ formula}
\end{cases}
\end{align*}
\]
Contribution: A Logic of Proofs for $d\mathcal{L}$

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

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

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 dL

LPdL extends the grammar of dL with formulas of the form

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

Example (Conjunctions)

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

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

$$\langle e, d \rangle : \varphi$$

$LPd\mathcal{L}$ proof term $d\mathcal{L}$ formula

\[
\langle e, d \rangle ::= c_\varphi \\
| e \land d \\
| e \bullet d \mid e \bullet\leftarrow d \mid e \bullet\rightarrow d
\]

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.
Contribution: A Logic of Proofs for dL

LPdL extends the grammar of dL with formulas of the form

\[
\begin{align*}
\langle e, d \rangle & ::= \ c_\phi \\
& \mid e \land d \\
& \mid e \bullet d \mid e \bullet \leftarrow d \mid e \bullet \rightarrow d \\
& \mid \sigma e \mid \mathcal{B} e
\end{align*}
\]

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

\[
\sigma\{t \mapsto 0, \ p(\cdot) \mapsto \geq 0\} (i[\cdot :=]) : \ [x := 0]x \geq 0 \leftrightarrow 0 \geq 0
\]
Contribution: A Logic of Proofs for $d\mathcal{L}$

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

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

$$| e \land d$$

$$| e \bullet d | e \bullet \leftarrow d | e \bullet \rightarrow d$$

$$| \sigma e | \mathcal{B} e$$

$$| \mathcal{C}T_\sigma e | \mathcal{C}Q_\sigma e | \mathcal{C}E_\sigma e$$

Example (US Instances of Proof Rules)

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

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

\[ \begin{align*}
\phi \\
\text{(dL Axiom)}
\end{align*} \]

\[ \begin{align*}
i_A : A \\
\text{(dL Constants)}
\end{align*} \]

\[ \begin{align*}
e : \phi \\
\text{(And)}
\end{align*} \]

\[ \begin{align*}
d : \psi \\
\text{(Application)}
\end{align*} \]

\[ \begin{align*}
(e \land d) : (\phi \land \psi) \\
\text{(US Proof Term)}
\end{align*} \]

\[ \begin{align*}
e : (\phi \rightarrow \psi) \\
\text{(CE}_\sigma\text{)}
\end{align*} \]

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

\begin{itemize}
  \item \([\phi]^l = [\phi]_{d\mathcal{L}}\)
  \item \([i_A : A]^l = S\) for \(d\mathcal{L}\) axioms \(A\)
  \item \([j_T : T] = S\) for \(\text{FOL}_R\) tautologies \(T\)
  \item \([e \land d : \phi \land \psi]^l = [e : \phi]^l \cap [d : \psi]^l\)
  \item \([e \bullet d : \phi]^l = \bigcup_\psi [e : (\psi \rightarrow \phi)]^l \cap [d : \psi]^l\)
  \item \(\ldots\)
\end{itemize}
Correctness Properties

Theorem (Proof terms justify theorems)

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


Correctness Properties

Theorem (Proof terms justify theorems)

Let $e$ be a proof term and $\phi$ a dL formula. If $\vdash_{L^PdL} e : \phi$ then $\vdash \phi$. 
Correctness Properties

Theorem (Proof terms justify theorems)

Let $e$ be a proof term and $\phi$ a dŁ formula. If $\vdash_{LPdŁ} e : \phi$ then $\vdash \phi$. 

KeYmaera X Web UI (JavaScript)

Simplified Proof Tree View

REST-API

Proof View  Tactics  Models  Proof Log

start/stop/pause/resume

Proof View Simplification  Searching  Execution

Scala-API

Proof Tree Simplification  Proof Strategies

Proof Tree

Scheduler

manages

executes tactics on tools/ CPU cores

HyDRA Server

Tactical Prover

executes

combines

Proof Tree

Proof Certificates  Uniform Substitution

KeYmaera X Kernel (soundness-critical, Scala)

Axiomatic Core

Axioms

Propositional Sequent Calculus with Skolemization

Real Quantifier Elimination

Differential Equation Solving

…
Adding Proof Terms Without Adding Soundness-Critical Code

Proof.

Case $\sigma \text{e}$. Suppose that $\vdash_{\text{LPdL}} \sigma \text{e} : \phi$. By [a lemma], $\phi = \sigma(\phi')$ and $\vdash_{\text{LPdL}} \text{e} : \phi'$ for some $\phi'$. The induction hypothesis for the smaller proof term $\text{e}$ gives $\vdash_{dL} \phi'$. Therefore, $\vdash_{dL} \sigma(\phi')$ (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