Towards an Implementation of Differential Dynamic Logic in PVS

J. Tanner Slagel,[1] César Muñoz*,[1] Swee Balachandran†,[2]
Mariano Moscato,[2], Aaron Dutle,[1] Paolo Masci,[2]
Lauren White[1]

[1] NASA Langley Research Center
Hampton, VA, USA
j.tanner.slagel@nasa.gov

[2] National Institute of Aerospace
Hampton, VA, USA

* Currently at Amazon Web Services
† Currently at Xwing

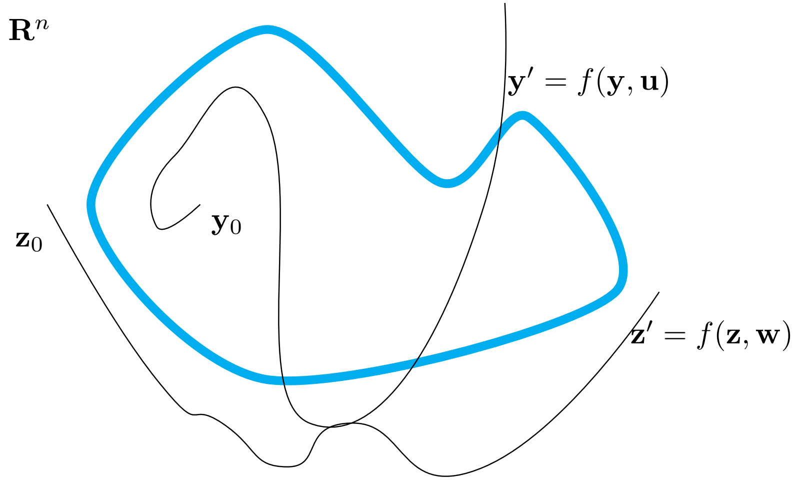
June 2022 @ SOAP 2022: 11th ACM SIGPLAN International Workshop on the State Of the Art in Program Analysis

Overview

- **dL:** Differential Dynamic Logic for hybrid programs [1]
- **PVS:** Interactive theorem prover [2]

Result: Embedding of dL in PVS

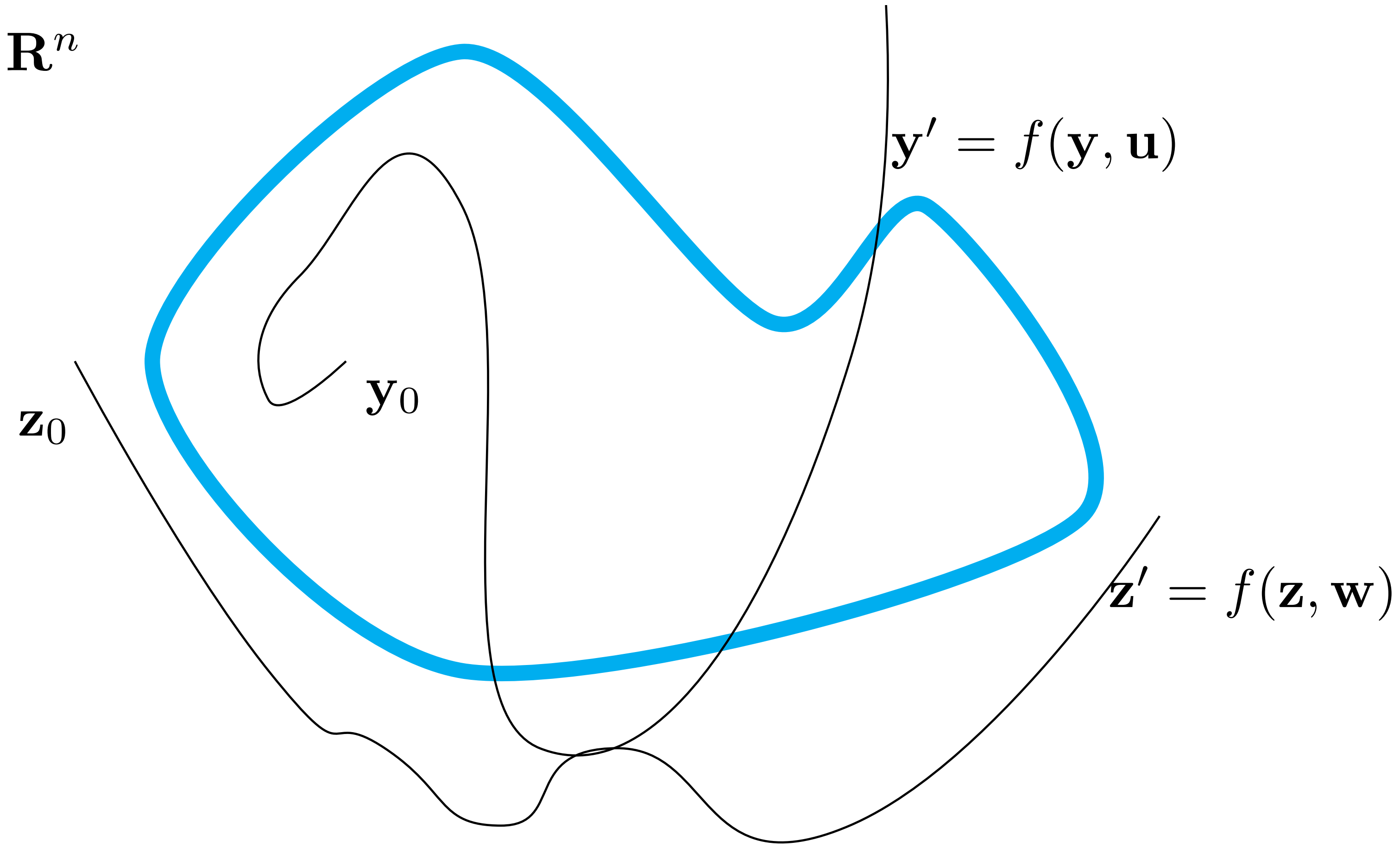
- Formally verified soundness of **dL**
- Fully operational in **PVS**
- Leveraging features of **PVS** to extend **dL**



[1] Differential Dynamic Logic website, André Platzer: https://symbolaris.com/logic/dL.html

[2] PVS website, SRI International: https://pvs.csl.sri.com

Hybrid Systems



- **Hybrid system:** dynamical system that exhibits
  - Continuous behavior
  - Discrete behavior

Want

- **Formal specification** of hybrid systems
- **Formal reasoning** of hybrid systems

Hybrid Programs

Hybrid programs allow **formal specification** of hybrid systems:

- Discrete jump set:

$$(x_1 \coloneqq \theta_1, \dots, x_n \coloneqq \theta_n)$$

- Differential equations:

$$\{x_1' \coloneqq \theta_1, \dots, x_n' \coloneqq \theta_n \;\&\; \chi\}$$

  - $\{x_i\}_{i=1}^{n}$ variables
  - $\{\theta_i\}_{i=1}^{n}$ assignments (ex. – functions of past variable assignments)
  - χ first order formula that describes domain

Hybrid Programs (continued)

For hybrid programs Hp_1, Hp_2, first-order formula χ:

- Union

$$(Hp_1 \cup Hp_2)$$

- Sequence

$$(Hp_1; Hp_2)$$

- Repeat

$$(Hp_1)^*$$

- Test

$$(?\,\chi)$$

Example:

$$\big((a \coloneqq a + 1); \{x' = v, v' = a\}\big)^*$$

dL: Differential Dynamic Logic

dL allows **formal reasoning** of hybrid programs:

- For hybrid program Hp and predicate P
  - All runs

$$[Hp]\mathrm{P}$$

  - Some runs

$$\langle Hp\rangle\mathrm{P}$$

Example: Let

$$Hp \equiv \big((a \coloneqq a + 1); \{x' = v, v' = a\}\big)^*$$

$$\mathrm{P} = (x = 10),$$

then

$$\vdash \langle Hp\rangle\mathrm{P} \qquad\qquad \nvdash [Hp]\mathrm{P}$$

dL: Differential Dynamic Logic

dL allows **formal reasoning** of hybrid programs:

- For hybrid program Hp and predicate P
  - All runs

$$[Hp]\mathrm{P}$$

  - Some runs

$$\langle Hp\rangle \mathrm{P}$$

Another example:

$$x \geq 1 \land v \geq 0 \land a \geq 0 \ \vdash$$

$$\left[\left((a \coloneqq a+1);\{x' = v, v' = a\}\right)^{*}\right](x \geq 1)$$

dL: Differential Dynamic Logic – Rule Schema [3]

Union axiom:

$$\frac{[Hp_1]P \wedge [Hp_2]P}{[Hp_1 \cup Hp_2]P}$$

Loop rule:

$$\frac{\Gamma \vdash J \qquad J \vdash [\alpha]J \qquad J \vdash P}{\Gamma \vdash [\alpha^*]P}$$

Differential invariant rule:

$$\frac{\Gamma, q(x) \vdash p(x) \qquad q(x) \vdash [x' := f(x)](p(x))'}{\Gamma \vdash [x' = f(x) \,\&\, q(x)]p(x)}$$

….and many more! [4]

[3] André Platzer. 2018. Logical Foundations of Cyber-Physical Systems. Springer, Cham. https://doi.org/10.1007/978-3-319-63588-0
[4] **dL** "Cheat Sheet," André Platzer, https://symbolaris.com/logic/dL-sheet.pdf

KeYmeara X

- KeYmeara X: formal verification tool for hybrid systems implementing $\mathbf{dL}$
- Verification of:
  - Railway systems [5]
  - Automotive systems [6]
  - Aviation transportation systems [7]
  - Autonomous robotics [8]
  - Etc.

[5] André Platzer and Jan-David Quesel. European Train Control System: A case study in formal verification. *11th International Conference on Formal Engineering Methods, ICFEM, Rio de Janeiro, Brazil*, 2009

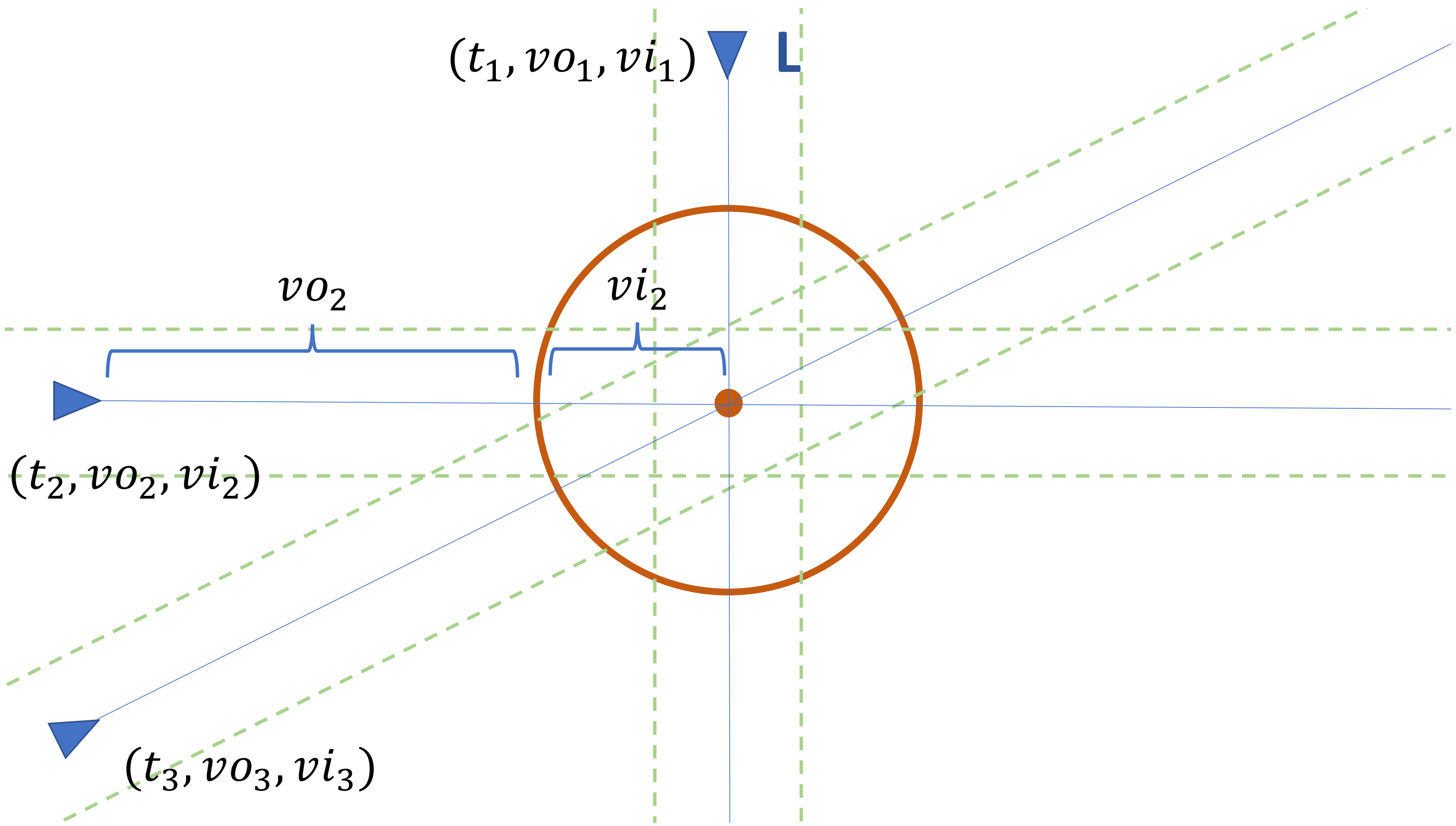
[6] Sarah M. Loos, André Platzer, and Ligia Nistor. Adaptive cruise control: Hybrid, distributed, and now formally verified. *17th International Symposium on Formal Methods, FM, Limerick, Ireland,* 2011

[7] André Platzer and Edmund M. Clarke. Formal verification of curved flight collision avoidance maneuvers: A case study *16th International Symposium on Formal Methods, FM, Eindhoven, Netherlands* 2009

[8] Stefan Mitsch, Khalil Ghorbal and André Platzer. On provably safe obstacle avoidance for autonomous robotic ground vehicles *Robotics: Science and Systems, RSS, 20139*, 2013

Outline

- Introduction
  - Hybrid programs
  - **dL**
- **dL** in PVS
  - PVS
  - Extensions of **dL** in PVS
  - Examples
- Concluding remarks



PVS

- “Prototype Verification System” developed by SRI International
- Interactive theorem prover
  - Higher order logic
  - Completely typed, dependent types
- Automation
  - Customizable tactics and strategies
- PVSio animation and rapid prototyping
- NASA PVS library [9]
  - 58 libraries
- Visual studio code extension [10]

```
deriv_test :

{-1}   b >= 0
{-2}   b > 0
{-3}   c /= 0
  |-------
[1]    deriv(LAMBDA (x: real): cos(x ^ 10 + b) + exp(x ^ 2) / c) =
        LAMBDA (x: real):
          -sin(x ^ 10 + b) * 10 * x ^ 9 + exp(x ^ 2) * 2 * x / c

>> (deriv)

Q.E.D.
```

[9] NASAlib, maintained by NASA Langley Formal Methods Group: https://github.com/nasa/pvslib
[10] VSCode-PVS, Paolo Masci: https://github.com/nasa/vscode-pvs

PVS – Prototype Verification System

Specification (.pvs)

```
% Define half
half(a:real,b:real | b>a):
  {r:real | abs(a-r) = abs(b-r)} =
    (a+b)/2

% Theorem about half
prove | show-prooflite
half_sq: THEOREM
 FORALL(a:real,b:real | b>a):
  EXISTS(n:posnat):
   a>n AND b>n
   IMPLIES half(a,b) < half(a^n,b^n)
```

Interactive theorem prover

```
half_sq.1.1 :

{-1}   b < b ^ 2
[-2]   a < a ^ 2
[-3]   a > 2
[-4]   b > 2
  |-------
[1]   half(a, b) < half(a ^ 2, b ^ 2)

>> (expand "half")

- Ctrl+SPACE shows the full list of commands.
- TAB autocompletes commands. Double click expands definitions.
```

PVS – Prototype Verification System

Proof (.prf)

```
half_sq : PROOF
(then (skeep)(inst 1 "2")(flatten)
  (spread (case "a<a^2")
   ((spread (case "b<b^2")
     ((then (expand "half")(mult-by 1 "2")(assert))
      (then (div-by 1 "b")(grind))))
    (then (div-by 1 "a")(grind)))))
QED half_sq
```

Interactive theorem prover

```
half_sq.1.1 :

{-1}   b < b ^ 2
[-2]   a < a ^ 2
[-3]   a > 2
[-4]   b > 2
  |-------
[1]   half(a, b) < half(a ^ 2, b ^ 2)

>> (expand "half")

- Ctrl+SPACE shows the full list of commands.
- TAB autocompletes commands. Double click expands definitions.
```

Hybrid Programs in PVS

Values of variables

```
Environment : TYPE = [nat->real]
%For example:
x: nat = 0
y: nat = 1
env: Environment = (LAMBDA(i:nat): 0)
  WITH [(x) := 10, (y) := -sqrt(5)]
```

Assignments

```
Assigns      : TYPE = MapExprInj
ODEs         : TYPE = MapExprInj
%For example
exp_ex: ODEs
= (: (x, val(x)), (y, val(y)+cnst(1)) :)
```

Functions on environments

```
%Predicates
BoolExpr    : TYPE = [Environment->bool]
%Quantified boolean expressions
QBoolExpr   : TYPE = [real->BoolExpr]
%Real-valued functions
RealExpr    : TYPE = [Environment->real]
%For example
val(i:nat): RealExpr
  = LAMBDA(env:Environment): env(i)
```

Hybrid Programs in PVS

Syntax of hybrid programs

```
HP : DATATYPE
BEGIN
  IMPORTING hp_def
  ASSIGN(assigns:Assigns) : assign?
  DIFF(odes:ODEs,be:BoolExpr) : diff?
  TEST(be:BoolExpr) : test?
  SEQ(stm1,stm2:HP) : seq?
  UNION(stm1,stm2:HP) : union?
  STAR(stm:HP) : star?
END HP
```

Semantics of hybrid programs

```
semantic_rel(hp:HP)(envi:Environment)
  (envo:Environment):
  INDUCTIVE bool = ...
```

Semantics of `ASSIGN(l:MapExprInj)`

```
(FORALL (i:below(length(l))) :
LET (k,re) = nth(l,i) IN
envo(k) = re(envi)) AND
FORALL (i:(not_in_map(l))) :envo(i) = envi(i)
```

Hybrid Programs in PVS

Recall:

$$x \geq 1 \wedge v \geq 0 \wedge a \geq 0 \;\vdash$$

$$\left[\left((a \coloneqq a + 1); \{x' = v, v' = a\}\right)^{*}\right](x \geq 1)$$

In PVS:

```
hp_ex: LEMMA
LET alpha = STAR(SEQ(ASSIGN( (: a, val(a) + cnst(1) :)),
DIFF( (: (x, val(v)), (v,val(a)) :) ))) IN
    (: :) |- (: DLIMPLIES( (: val(x) >= cnst(1),
   val(v) >= cnst(0), val(a) >= cnst(0) :),
    ALLRUNS(alpha, val(x) >= cnst(1))):)
```

$\mathbf{dL}$ in PVS- Results

- **Formal verification** of soundness of $\mathbf{dL}$[11]

- **Fully operational** embedding $\mathbf{dL}$

- **Extensions of $\mathbf{dL}$ in PVS**

[11] Previous Formal Verification of soundness of $\mathbf{dL}$ in Coq and Isabelle/Hol:
Brandon Bohrer, Vincent Rahli, Ivana Vukotic, Marcus Völp, and André Platzer. 2017. Formally verified differential dynamic logic.
In Proceedings of the 6th ACM SIGPLAN Conference on Certified Programs and Proofs.208–221. https://doi.org/10.1145/3018610.3018616

Formal Verification of Soundness of $\boldsymbol{dL}$

Loop rule:

```
dl_loop : LEMMA
  FORALL (Gamma,Delta)(J,P)(A):
    (Gamma |- cons(J,Delta)) AND
    (J |- P) AND
    (J |- ALLRUNS(A,J)) IMPLIES
    (Gamma |- cons(ALLRUNS(STAR(A),P),Delta))
```

Differential invariant rule:

```
dl_dI: LEMMA
  FORALL  (P:(ddl_dom?))(Gamma,Delta)(nnP,Q)(ode:ODEs):
    derivable_up_nqbool?(max_var(ode),P)(nnP) AND
    ( cons(Q,Gamma) |- cons(nqb_to_be(nnP),Delta) ) AND
    ( Q |- SUB_DIFT(P,ode)(nnP) ) IMPLIES
    ( Gamma |-
     cons(ALLRUNS(DIFF(ode,DLAND(P,Q)),nqb_to_be(nnP)),Delta) )
```

81 proven rules/axioms of **dl** in PVS

Fully Operational Embedding of **dL**

- Proof rules implemented as strategies in PVS
  - Fully operational **dL** within interactive prover console of PVS

```
discrete_loop_ex :

  |-------
{1}   (: val(x) >= cnst(1), val(v) >= cnst(0), val(a) >= cnst(0) :) |-
       (: ALLRUNS(STAR(SEQ(ASSIGN((: (a, val(a) + cnst(1)) :)),
                           DIFF((: (x, val(v)), (v, val(a)) :),
                                DLBOOL(TRUE))))),
                  val(x) >= cnst(1)) :)

>> (dl-loop "val(x) >= cnst(1) AND val(v) >= cnst(0) AND val(a) >=cnst(0)")
```

Fully Operational Embedding of $\mathbf{dL}$

- Proof rules implemented as strategies in PVS
  - Fully operational $\mathbf{dL}$ within interactive prover console of PVS

```
discrete_loop_ex.1 :

  |-------
{1}   ((: val(x) >= cnst(1), val(v) >= cnst(0), val(a) >= cnst(0) :) |-
        (: DLAND(val(x) >= cnst(1),
                 DLAND(val(v) >= cnst(0), val(a) >= cnst(0))) :))

>> (dl-assert)
```

Fully Operational Embedding of **dL**

- Proof rules implemented as strategies in PVS
  - Fully operational **dL** within interactive prover console of PVS

```
discrete_loop_ex.2 :

  |-------
{1}   ((: DLAND(val(x) >= cnst(1),
              DLAND(val(v) >= cnst(0), val(a) >= cnst(0))) :)
         |- (: val(x) >= cnst(1) :))

>> (dl-assert)
```

Fully Operational Embedding of **dL**

- Proof rules implemented as strategies in PVS
  - Fully operational **dL** within interactive prover console of PVS

```
discrete_loop_ex.3 :

  ├──────
{1}   ((: DLAND(val(x) >= cnst(1),
            DLAND(val(v) >= cnst(0), val(a) >= cnst(0))) :)
       |-
       (: ALLRUNS(SEQ(ASSIGN((: (a, val(a) + cnst(1)) :)),
                   DIFF((: (x, val(v)), (v, val(a)) :), DLBOOL(TRUE))),
                DLAND(val(x) >= cnst(1),
                   DLAND(val(v) >= cnst(0), val(a) >= cnst(0)))) :))

>>
```

Fully Operational Embedding of **dL**

- Proof rules implemented as strategies in PVS
  - Fully operational **dL** within interactive prover console of PVS

```
diff_inv_ex :

  |-------
{1}   ((: val(x) >= cnst(1), val(a) >= cnst(0) :) |-
        (: ALLRUNS(DIFF((: (x, val(v)), (v, val(a)) :), val(v) >= cnst(0)),
                   val(x) >= cnst(1)) :))

>> (dl-diffinv)
```

Fully Operational Embedding of **dL**

- Proof rules implemented as strategies in PVS
  - Fully operational **dL** within interactive prover console of PVS

```
diff_inv_ex.1 :

  |-------
{1}   ((: val(v) >= cnst(0), (val(x) >= cnst(1)), val(a) >= cnst(0) :) |-
        (: (val(x) >= cnst(1)) :))

>> (dl-assert)
```

Fully Operational Embedding of **dL**

- Proof rules implemented as strategies in PVS
  - Fully operational **dL** within interactive prover console of PVS

```
diff_inv_ex.2 :

  |-------
{1}   ((: val(v) >= cnst(0) :) |- (: val(v) >= cnst(0) :))

>> (dl-assert)

Q.E.D.
```

dL in PVS – Generalized Reasoning of Hybrid Programs

- **Fully typed** specification of hybrid programs
    - Reasoning at the type level (properties of groups of hybrid programs)
    - Reasoning for arbitrary hybrid programs (e.g., arbitrarily many variables)

```
behind: TYPE
 = {hp: (diff?) |
     (: behind?(odes(hp)) :) |- (: ALLRUNS(hp,behind?(odes(hp))) :)}

slow: TYPE
 = {hp: (diff?) |
   (: :) |- (: slower?(odes(hp)) :)}
```

- **A hybrid program of type** `slow` **is always of type** `behind`

```
slow_is_behind: JUDGEMENT
  slow SUBTYPE_OF behind
```

Summary

- **dL:** Differential Dynamic Logic for hybrid programs
- **PVS:** Interactive theorem prover

Result: Embedding of dL in PVS

- Formal verification **dL** (done)
- Fully operational in **PVS** (close)
- Leveraging features of **PVS** to extend **dL** (ongoing)