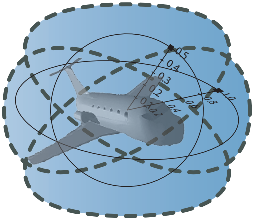
How to Explain Cyber-Physical Systems to Your Verifier

André Platzer

aplatzer@cs.cmu.edu
Computer Science Department
Carnegie Mellon University, Pittsburgh, PA

http://symbolaris.com/



Outline

Outline

1. Motivation
2. Differential Dynamic Logic $d\mathcal{L}$
3. Axiomatization
4. Differential Cuts, Differential Ghosts & Differential Invariants
   - Differential Invariants
   - Differential Cuts
   - Differential Ghosts
5. Survey
6. Applications
   - Ground Robots
7. Summary

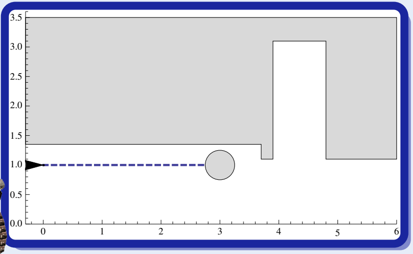
Can you trust a computer to control physics?

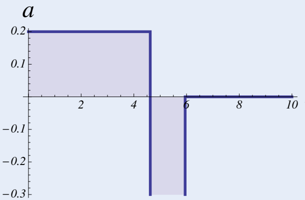
Hybrid Systems Analysis

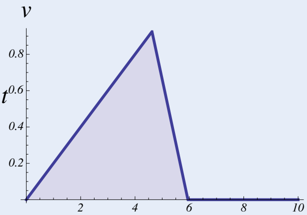
Challenge (Hybrid Systems)

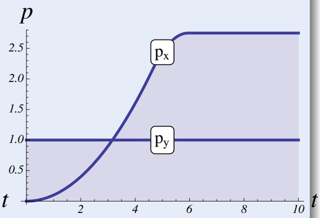
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)





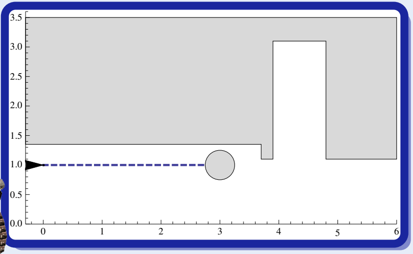


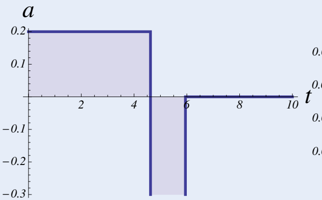


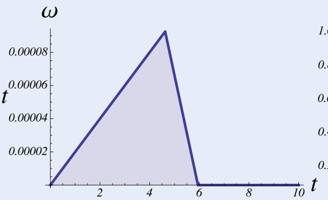
Challenge (Hybrid Systems)

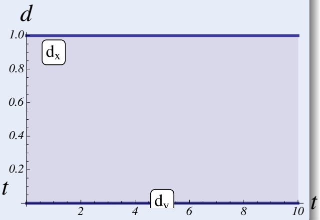
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)







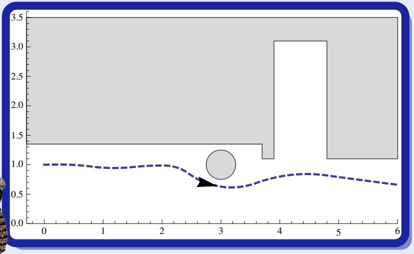


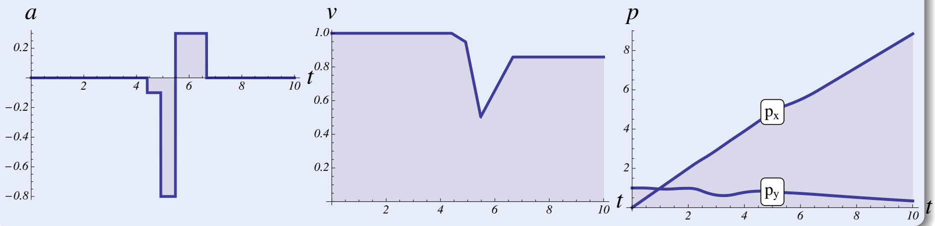
Hybrid Systems Analysis

Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



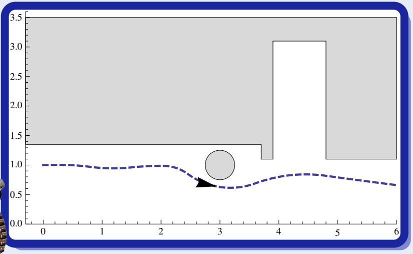


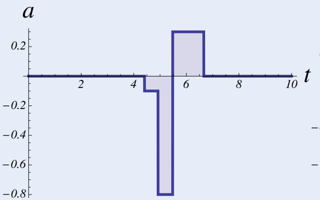
Hybrid Systems Analysis

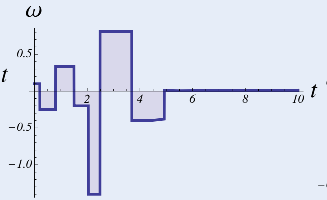
Challenge (Hybrid Systems)

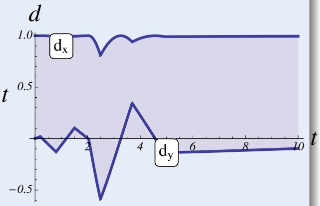
Fixed rule describing state evolution with both

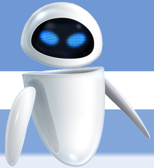
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)







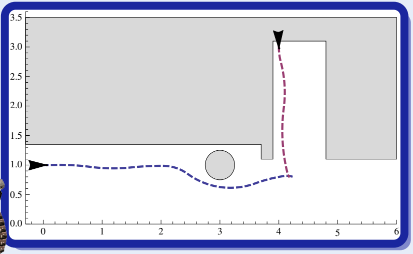


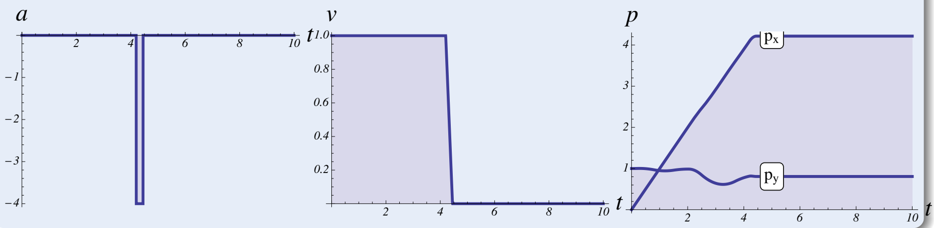


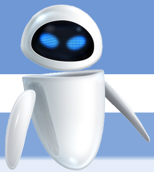
Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



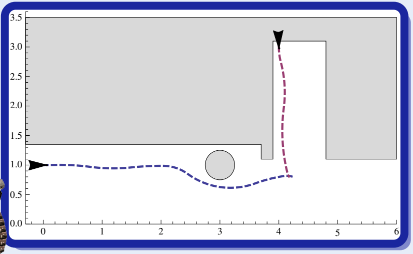


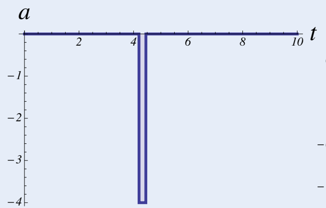


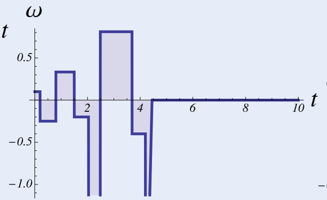
Challenge (Hybrid Systems)

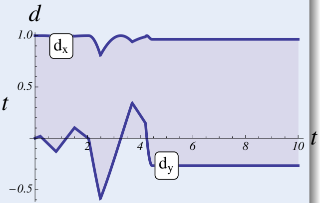
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)

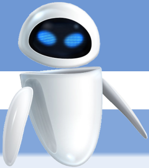








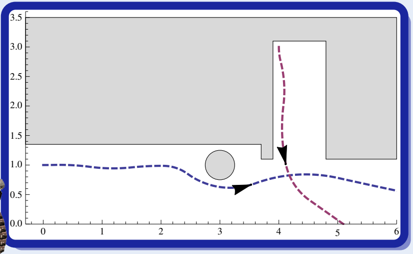
Hybrid Systems Analysis

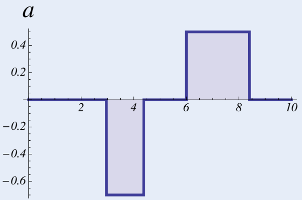


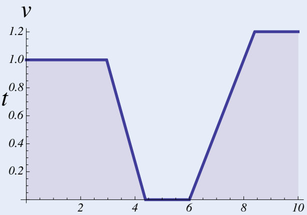
Challenge (Hybrid Systems)

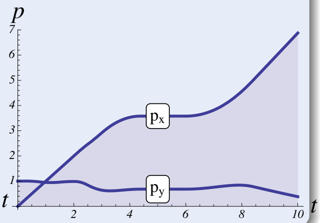
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)

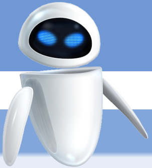








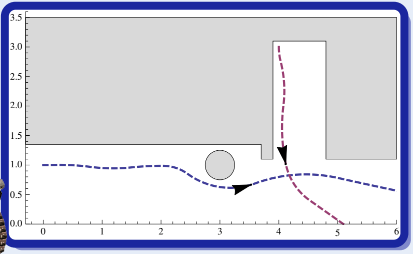
Hybrid Systems Analysis

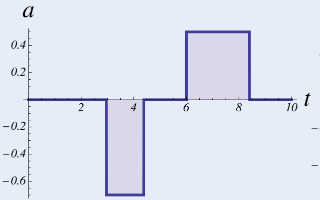


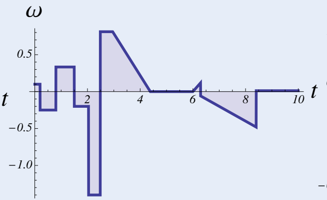
Challenge (Hybrid Systems)

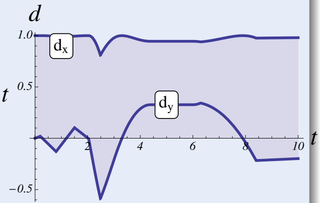
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)









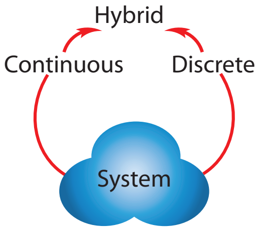
Outline

Outline

Complete Proof Theory of Hybrid Systems

Theorem (Complete Alignment) (JAR 2008, LICS'12)

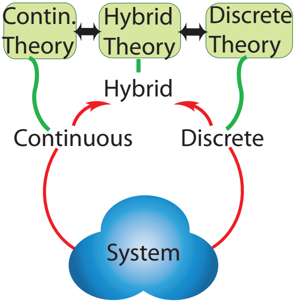
hybrid = continuous = discrete (proof-theoretically)



Complete Proof Theory of Hybrid Systems

Theorem (Complete Alignment) (JAR 2008, LICS'12)

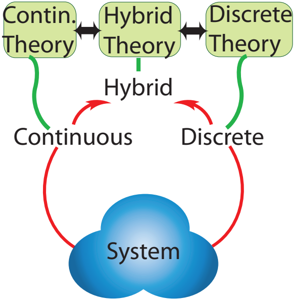
hybrid = continuous = discrete (proof-theoretically)



Complete Proof Theory of Hybrid Systems

Theorem (Complete Alignment) (JAR 2008, LICS'12)

hybrid $=$ *continuous* $=$ *discrete (proof-theoretically)*

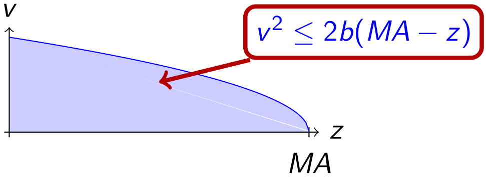


Corollary (Hybridization recipe)

Every verification technique can be hybridized. *(add enough logic)*

differential dynamic logic

$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$

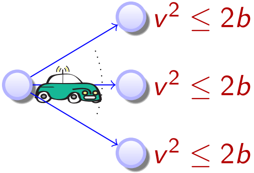


Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$

$$\mathcal{C} \rightarrow [\underbrace{\texttt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \le 2b$$



Logic for Hybrid Systems

differential dynamic logic

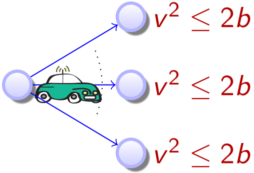
$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{DL} + \text{HP}$

$$\mathcal{C} \rightarrow [\underbrace{\texttt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \leq 2b$$

Initial condition

System dynamics

Post condition



Differential Dynamic Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

$$x := \theta \mid ?H \mid x' = f(x) \,\&\, H \mid \alpha \cup \beta \mid \alpha; \beta \mid \alpha^*$$

Definition (d$\mathcal{L}$ Formula ϕ)

$$\theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

Differential Dynamic Logic d$\mathcal{L}$: Syntax

Discrete Assign | Test Condition | Differential Equation | Nondet. Choice | Seq. Compose | Nondet. Repeat

Definition (Hybrid program α)

$$x := \theta \mid ?H \mid x' = f(x) \,\&\, H \mid \alpha \cup \beta \mid \alpha;\beta \mid \alpha^*$$

Definition (d$\mathcal{L}$ Formula ϕ)

$$\theta_1 \geq \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x\, \phi \mid \exists x\, \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

All Reals | Some Reals | All Runs | Some Runs

CPS Design & CPS Contracts in Programs

HP Reveal in layers

Contracts Reason about CPS

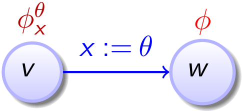
```
@requires(v^2 ≤ 2*b*(m−x))
@requires(v ≥ 0 ∧ A ≥ 0 ∧ b>0)
@ensures(x ≤ m)
  {
     if (v^2 ≤ 2*b*(m−x) − (A+b)*(A+2*v)) {
         a := A;
     } else {
         a := −b;
     }
     t := 0;
     {x'=v, v'=a, t'=1, v ≥ 0 ∧ t ≤ 1}
  }*@invariant(v^2 ≤ 2*b*(m−x))
```

CPS Simulate for intuition

CT Design-by-invariant

Outline

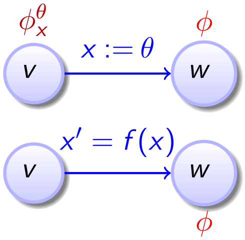
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$



Proofs for Hybrid Systems

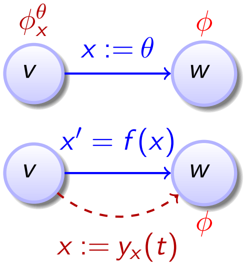
$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

$$\frac{\forall t{\geq}0\, [x := y_x(t)]\phi}{[x' = f(x)]\phi}$$



$$\frac{\phi_x^\theta}{[x := \theta]\phi}$$

$$\frac{\forall t{\geq}0\, [x := y_x(t)]\phi}{[x' = f(x)]\phi}$$

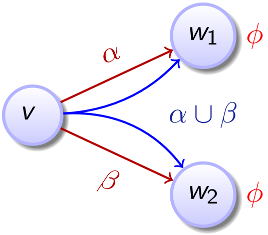


Proofs for Hybrid Systems

compositional semantics $\Rightarrow$ compositional rules!

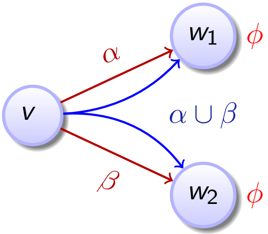
Proofs for Hybrid Systems

$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$

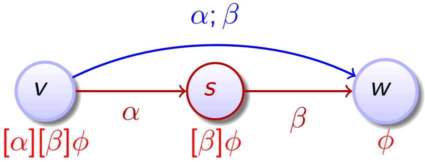


Proofs for Hybrid Systems

$$\frac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$$

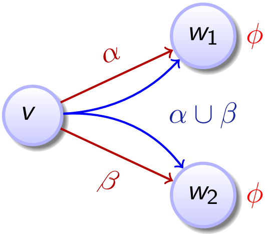


$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$

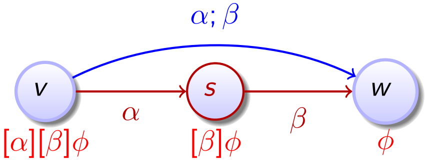


Proofs for Hybrid Systems

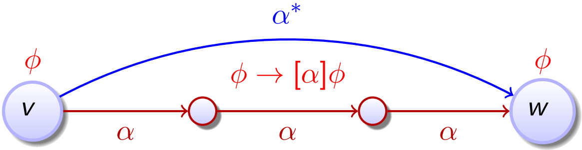
$$\frac{[\alpha]\phi \land [\beta]\phi}{[\alpha \cup \beta]\phi}$$



$$\frac{[\alpha][\beta]\phi}{[\alpha;\beta]\phi}$$



$$\frac{\phi \quad (\phi \to [\alpha]\phi)}{[\alpha^*]\phi}$$

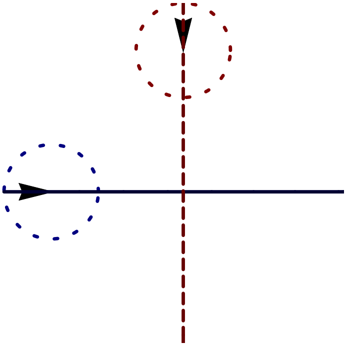


Outline

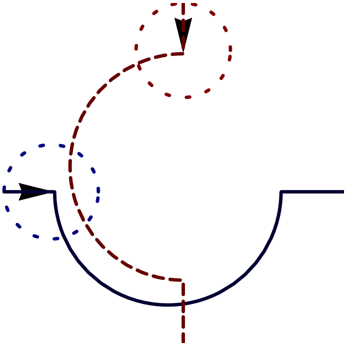
1. Motivation
2. Differential Dynamic Logic $d\mathcal{L}$
3. Axiomatization
4. Differential Cuts, Differential Ghosts & Differential Invariants
   - Differential Invariants
   - Differential Cuts
   - Differential Ghosts
5. Survey
6. Applications
   - Ground Robots
7. Summary

Differential Cuts, Differential Ghosts & Differential Invariants

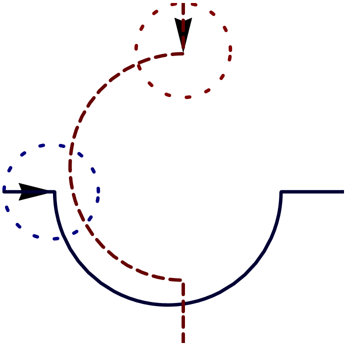

Air Traffic Control



Air Traffic Control



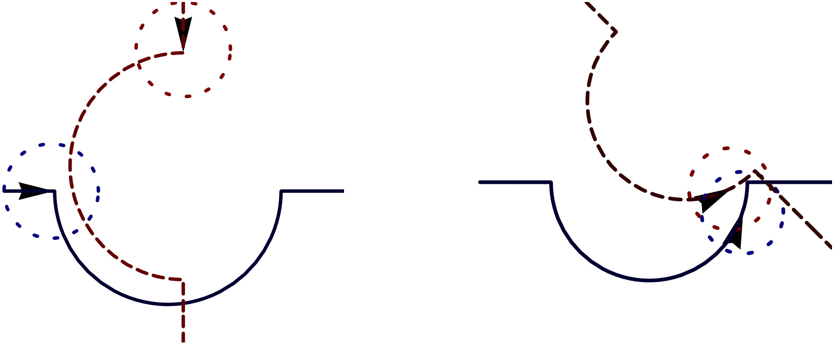
Air Traffic Control



Verification?

looks correct

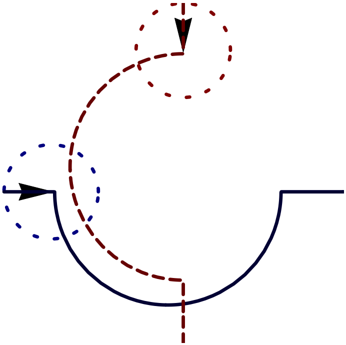
Air Traffic Control

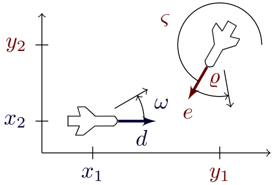


Verification?

looks correct NO!

Air Traffic Control



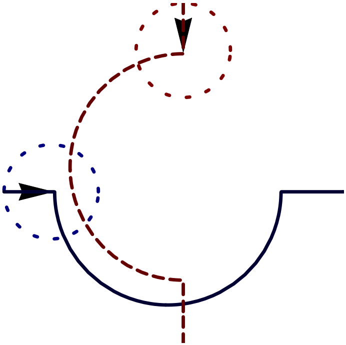


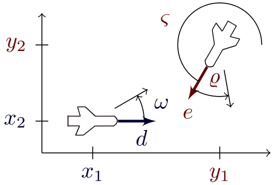
$$\begin{bmatrix} x_1' = & -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = & v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = & \varpi - \omega \end{bmatrix}$$

Verification?

looks correct NO!

Air Traffic Control





$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

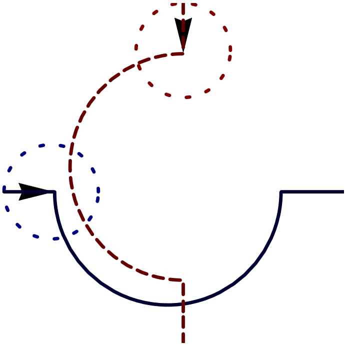
Example ("Solving" differential equations)

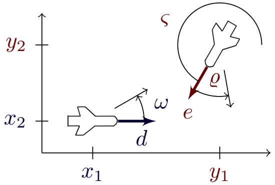
$$x_1(t) = \frac{1}{\omega\varpi}\big(x_1\omega\varpi \cos t\omega - v_2\omega \cos t\omega \sin\vartheta + v_2\omega \cos t\omega \cos t\varpi \sin\vartheta - v_1\varpi \sin t\omega$$

$$+ x_2\omega\varpi \sin t\omega - v_2\omega \cos\vartheta \cos t\varpi \sin t\omega - v_2\omega\sqrt{1 - \sin\vartheta^2} \sin t\omega$$

$$+ v_2\omega \cos\vartheta \cos t\omega \sin t\varpi + v_2\omega \sin\vartheta \sin t\omega \sin t\varpi\big) \ldots$$

Air Traffic Control





$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example ("Solving" differential equations)

$$\forall t \geq 0 \quad \frac{1}{\omega\varpi}\Big(x_1\omega\varpi \cos t\omega - v_2\omega \cos t\omega \sin\vartheta + v_2\omega \cos t\omega \cos t\varpi \sin\vartheta - v_1\varpi \sin t\omega$$

$$+ x_2\omega\varpi \sin t\omega - v_2\omega \cos\vartheta \cos t\varpi \sin t\omega - v_2\omega\sqrt{1 - \sin\vartheta^2} \sin t\omega$$

$$+ v_2\omega \cos\vartheta \cos t\omega \sin t\varpi + v_2\omega \sin\vartheta \sin t\omega \sin t\varpi\Big) \ldots$$

```
\forall R ts2.
  (   0 <= ts2 & ts2 <= t2_0
   ->       (  (om_1)^-1
             * (omb_1)^-1
             * (  om_1 * omb_1 * x1 * Cos(om_1 * ts2)
                + om_1 * v2 * Cos(om_1 * ts2) * (1 + -1 * (Cos(u))^2)^(1 / 2)
                + -1 * omb_1 * v1 * Sin(om_1 * ts2)
                + om_1 * omb_1 * x2 * Sin(om_1 * ts2)
                + om_1 * v2 * Cos(u) * Sin(om_1 * ts2)
                + -1 * om_1 * v2 * Cos(omb_1 * ts2) * Cos(u) * Sin(om_1 * ts2)
                + om_1 * v2 * Cos(om_1 * ts2) * Cos(u) * Sin(omb_1 * ts2)
                + om_1 * v2 * Cos(om_1 * ts2) * Cos(omb_1 * ts2) * Sin(u)
                + om_1 * v2 * Sin(om_1 * ts2) * Sin(omb_1 * ts2) * Sin(u)))
        ^2
       +    (  (om_1)^-1
             * (omb_1)^-1
             * (  -1 * omb_1 * v1 * Cos(om_1 * ts2)
                + om_1 * omb_1 * x2 * Cos(om_1 * ts2)
                + omb_1 * v1 * (Cos(om_1 * ts2))^2
                + om_1 * v2 * Cos(om_1 * ts2) * Cos(u)
                + -1 * om_1 * v2 * Cos(om_1 * ts2) * Cos(omb_1 * ts2) * Cos(u)
                + -1 * om_1 * omb_1 * x1 * Sin(om_1 * ts2)
                +   -1
                  * om_1
                  * v2
                  * (1 + -1 * (Cos(u))^2)^(1 / 2)
                  * Sin(om_1 * ts2)
                + omb_1 * v1 * (Sin(om_1 * ts2))^2
                + -1 * om_1 * v2 * Cos(u) * Sin(om_1 * ts2) * Sin(omb_1 * ts2)
                + -1 * om_1 * v2 * Cos(omb_1 * ts2) * Sin(om_1 * ts2) * Sin(u)
                + om_1 * v2 * Cos(om_1 * ts2) * Sin(omb_1 * ts2) * Sin(u)))
        ^2
      >= (p)^2),
 t2_0 >= 0,
 x1^2 + x2^2 >= (p)^2
==>
```

```
\forall R t7.
  (   t7 >= 0
   ->       (  (om_3)^-1
             * (    om_3
                  * (  (om_1)^-1
                     * (omb_1)^-1
                     * (  om_1 * omb_1 * x1 * Cos(om_1 * t2_0)
                        +   om_1
                          * v2
                          * Cos(om_1 * t2_0)
                          * (1 + -1 * (Cos(u))^2)^(1 / 2)
                        + -1 * omb_1 * v1 * Sin(om_1 * t2_0)
                        + om_1 * omb_1 * x2 * Sin(om_1 * t2_0)
                        + om_1 * v2 * Cos(u) * Sin(om_1 * t2_0)
                        +   -1
                          * om_1
                          * v2
                          * Cos(omb_1 * t2_0)
                          * Cos(u)
                          * Sin(om_1 * t2_0)
                        +   om_1
                          * v2
                          * Cos(om_1 * t2_0)
                          * Cos(u)
                          * Sin(omb_1 * t2_0)
                        +   om_1
                          * v2
                          * Cos(om_1 * t2_0)
                          * Cos(omb_1 * t2_0)
                          * Sin(u)
                        +   om_1
                          * v2
                          * Sin(om_1 * t2_0)
                          * Sin(omb_1 * t2_0)
                          * Sin(u)))
```

```
    * Cos(om_3 * t5)
  +   v2
    * Cos(om_3 * t5)
    *   (  1
         +   -1
           * (Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4))^2)
     ^(1 / 2)
  + -1 * v1 * Sin(om_3 * t5)
  +   om_3
    * (  (om_1)^-1
       * (omb_1)^-1
       * (  -1 * omb_1 * v1 * Cos(om_1 * t2_0)
          + om_1 * omb_1 * x2 * Cos(om_1 * t2_0)
          + omb_1 * v1 * (Cos(om_1 * t2_0))^2
          + om_1 * v2 * Cos(om_1 * t2_0) * Cos(u)
          +   -1
            * om_1
            * v2
            * Cos(om_1 * t2_0)
            * Cos(omb_1 * t2_0)
            * Cos(u)
          + -1 * om_1 * omb_1 * x1 * Sin(om_1 * t2_0)
          +   -1
            * om_1
            * v2
            * (1 + -1 * (Cos(u))^2)^(1 / 2)
            * Sin(om_1 * t2_0)
          + omb_1 * v1 * (Sin(om_1 * t2_0))^2
          +   -1
            * om_1
            * v2
            * Cos(u)
            * Sin(om_1 * t2_0)
            * Sin(omb_1 * t2_0)
```

```
                 +   -1
                   * om_1
                   * v2
                   * Cos(omb_1 * t2_0)
                   * Sin(om_1 * t2_0)
                   * Sin(u)
                 +   om_1
                   * v2
                   * Cos(om_1 * t2_0)
                   * Sin(omb_1 * t2_0)
                   * Sin(u)))
           * Sin(om_3 * t5)
         +   v2
           * Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
           * Sin(om_3 * t5)
         +   v2
           * (Cos(om_3 * t5))^2
           * Sin(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
         +   v2
           * (Sin(om_3 * t5))^2
           * Sin(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)))
 ^2
+   (  (om_3)^-1
     * (  -1 * v1 * Cos(om_3 * t5)
         +   om_3
           * (  (om_1)^-1
              * (omb_1)^-1
              * (  -1 * omb_1 * v1 * Cos(om_1 * t2_0)
                 + om_1 * omb_1 * x2 * Cos(om_1 * t2_0)
                 + omb_1 * v1 * (Cos(om_1 * t2_0))^2
                 + om_1 * v2 * Cos(om_1 * t2_0) * Cos(u)
                 +   -1
                   * om_1
                   * v2
                   * Cos(om_1 * t2_0)
                   * Cos(omb_1 * t2_0)
```

```
          + -1 * om_1 * omb_1 * x1 * Sin(om_1 * t2_0)
          +   -1
            * om_1
            * v2
            * (1 + -1 * (Cos(u))^2)^(1 / 2)
            * Sin(om_1 * t2_0)
          + omb_1 * v1 * (Sin(om_1 * t2_0))^2
          +   -1
            * om_1
            * v2
            * Cos(u)
            * Sin(om_1 * t2_0)
            * Sin(omb_1 * t2_0)
          +   -1
            * om_1
            * v2
            * Cos(omb_1 * t2_0)
            * Sin(om_1 * t2_0)
            * Sin(u)
          +   om_1
            * v2
            * Cos(om_1 * t2_0)
            * Sin(omb_1 * t2_0)
            * Sin(u)))
    * Cos(om_3 * t5)
  + v1 * (Cos(om_3 * t5))^2
  +   v2
    * Cos(om_3 * t5)
    * Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
  +   -1
    * v2
    * (Cos(om_3 * t5))^2
    * Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
```

```
+   -1
  * om_3
  * (  (om_1)^-1
     * (omb_1)^-1
     * (  om_1 * omb_1 * x1 * Cos(om_1 * t2_0)
        +   om_1
          * v2
          * Cos(om_1 * t2_0)
          * (1 + -1 * (Cos(u))^2)^(1 / 2)
        + -1 * omb_1 * v1 * Sin(om_1 * t2_0)
        + om_1 * omb_1 * x2 * Sin(om_1 * t2_0)
        + om_1 * v2 * Cos(u) * Sin(om_1 * t2_0)
        +   -1
          * om_1
          * v2
          * Cos(omb_1 * t2_0)
          * Cos(u)
          * Sin(om_1 * t2_0)
        +   om_1
          * v2
          * Cos(om_1 * t2_0)
          * Cos(u)
          * Sin(omb_1 * t2_0)
        +   om_1
          * v2
          * Cos(om_1 * t2_0)
          * Cos(omb_1 * t2_0)
          * Sin(u)
        +   om_1
          * v2
          * Sin(om_1 * t2_0)
          * Sin(omb_1 * t2_0)
          * Sin(u)))
  * Sin(om_3 * t5)
```

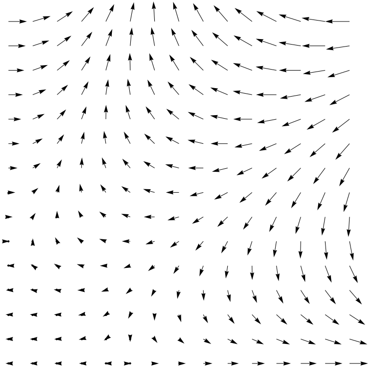
```
        +   -1
          * v2
          *   (  1
                +   -1
                  * (Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4))^2)
           ^(1 / 2)
          * Sin(om_3 * t5)
        + v1 * (Sin(om_3 * t5))^2
        +   -1
          * v2
          * Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
          * (Sin(om_3 * t5))^2))
  ^2
>= (p)^2)
```

This is just one branch to prove for aircraft . . .

Differential Invariants for Differential Equations

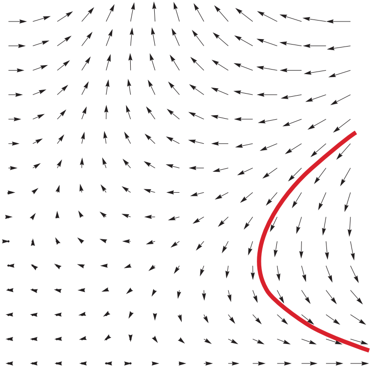
"Definition" (Differential Invariant)

"Formula that remains true in the direction of the dynamics"



"Definition" (Differential Invariant)

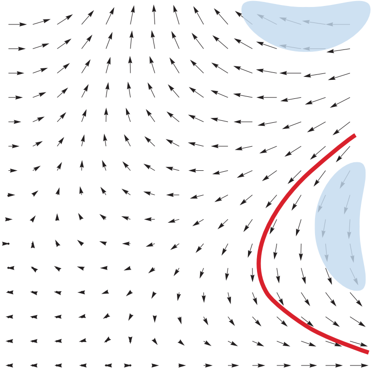
"Formula that remains true in the direction of the dynamics"



Differential Invariants for Differential Equations

"Definition" (Differential Invariant)

"Formula that remains true in the direction of the dynamics"



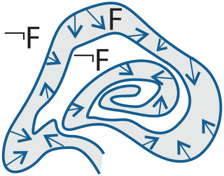
Differential Invariants: Local Dynamics w/o Solutions

Definition (Differential Invariant) (J.Log.Comput. 2010)

F closed under total differentiation with respect to differential constraints

Definition (Differential Invariant) (J.Log.Comput. 2010)

F closed under total differentiation with respect to differential constraints

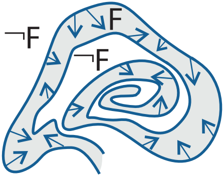


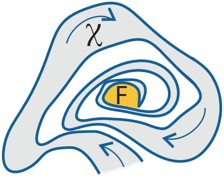
$$\frac{(\chi \rightarrow F')}{\chi \rightarrow F \rightarrow [x' = \theta \,\&\, \chi]F}$$

$$\frac{F \rightarrow [\alpha]F}{F \rightarrow [\alpha^*]F}$$

Definition (Differential Invariant) (J.Log.Comput. 2010)

F closed under total differentiation with respect to differential constraints

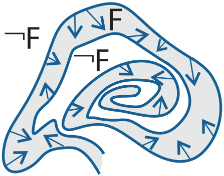


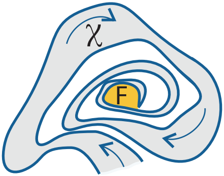


$$\frac{(\chi \rightarrow F')}{\chi \rightarrow F \rightarrow [x' = \theta \,\&\, \chi]F}$$

Definition (Differential Invariant) (J.Log.Comput. 2010)

F closed under total differentiation with respect to differential constraints





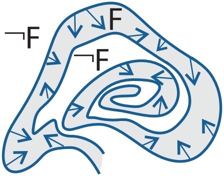
$$\frac{(\chi \to F')}{\chi \to F \to [x' = \theta \,\&\, \chi]F}$$

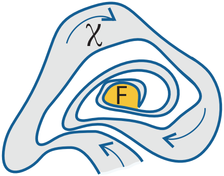
$$\frac{(\neg F \land \chi \to F'_{\gg})}{[x' = \theta \,\&\, \neg F]\chi \to \langle x' = \theta \,\&\, \chi\rangle F}$$

Differential Invariants: Local Dynamics w/o Solutions

Definition (Differential Invariant) (J.Log.Comput. 2010)

F closed under total differentiation with respect to differential constraints





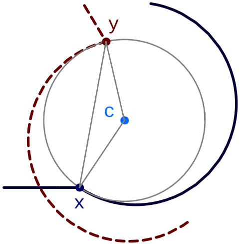
$$\frac{(\chi \to F')}{\chi \to F \to [x' = \theta \,\&\, \chi] F}$$

$$\frac{(\neg F \land \chi \to F'_{\gg})}{[x' = \theta \,\&\, \neg F]\chi \to \langle x' = \theta \,\&\, \chi\rangle F}$$

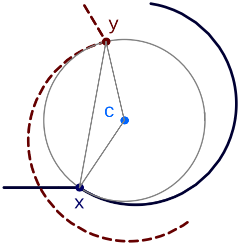
Total differential F' of *formulas*?

Differential Invariants for Aircraft Roundabouts

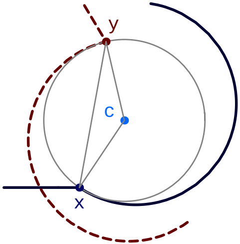
$$\overline{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



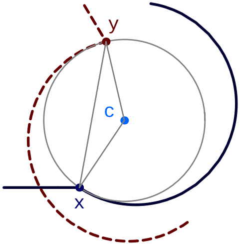
$$\frac{\dfrac{\partial\|x-y\|^2}{\partial x_1}x_1' + \dfrac{\partial\|x-y\|^2}{\partial y_1}y_1' + \dfrac{\partial\|x-y\|^2}{\partial x_2}x_2' + \dfrac{\partial\|x-y\|^2}{\partial y_2}y_2' \geq \dfrac{\partial p^2}{\partial x_1}x_1' \ldots}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



$$\dfrac{\dfrac{\partial\|x-y\|^2}{\partial x_1}x_1' + \dfrac{\partial\|x-y\|^2}{\partial y_1}y_1' + \dfrac{\partial\|x-y\|^2}{\partial x_2}x_2' + \dfrac{\partial\|x-y\|^2}{\partial y_2}y_2' \geq \dfrac{\partial p^2}{\partial x_1}x_1' \dots}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1-y_1)^2 + (x_2-y_2)^2 \geq p^2}$$

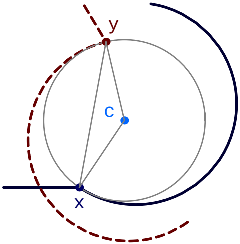


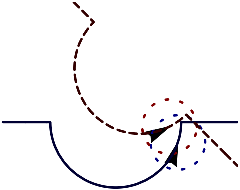
$$\frac{\dfrac{\partial\|x-y\|^2}{\partial x_1}d_1 + \dfrac{\partial\|x-y\|^2}{\partial y_1}e_1 + \dfrac{\partial\|x-y\|^2}{\partial x_2}d_2 + \dfrac{\partial\|x-y\|^2}{\partial y_2}e_2 \geq \dfrac{\partial p^2}{\partial x_1}d_1 \ldots}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



Differential Invariants for Aircraft Roundabouts

$$\frac{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}{\frac{\dfrac{\partial \|x-y\|^2}{\partial x_1} d_1 + \dfrac{\partial \|x-y\|^2}{\partial y_1} e_1 + \dfrac{\partial \|x-y\|^2}{\partial x_2} d_2 + \dfrac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \dfrac{\partial p^2}{\partial x_1} d_1 \ldots}{2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}}$$

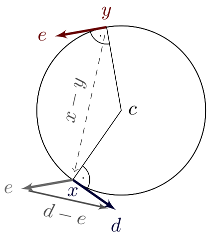


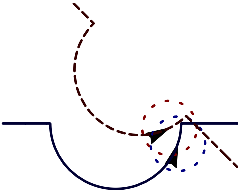


$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots$$

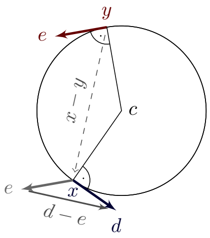
$$[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

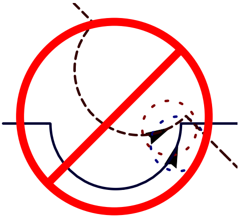




Differential Invariants for Aircraft Roundabouts

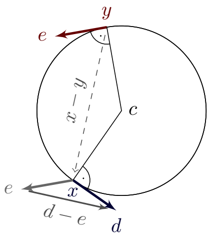
$$\frac{\dfrac{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}{\dfrac{\partial\|x-y\|^2}{\partial x_1} d_1 + \dfrac{\partial\|x-y\|^2}{\partial y_1} e_1 + \dfrac{\partial\|x-y\|^2}{\partial x_2} d_2 + \dfrac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \dfrac{\partial p^2}{\partial x_1} d_1 \ldots}}{2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}$$





$$\overline{.. \rightarrow [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)}$$

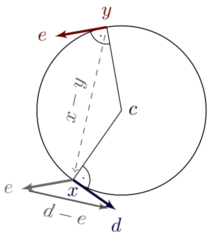
$$\cfrac{\cfrac{\cfrac{2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\dots}}{[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}$$



$$\overline{..\rightarrow[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)}$$

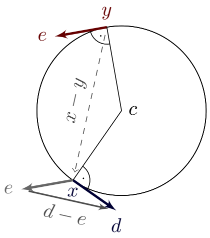
Differential Invariants for Aircraft Roundabouts

$$\frac{\dfrac{\dfrac{\dfrac{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}{}}{\frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}}{2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}}{2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0}$$



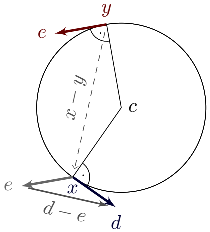
$$\frac{\dfrac{}{\frac{\partial(d_1-e_1)}{\partial d_1} d_1' + \frac{\partial(d_1-e_1)}{\partial e_1} e_1' = -\frac{\partial\omega(x_2-y_2)}{\partial x_2} x_2' - \frac{\partial\omega(x_2-y_2)}{\partial y_2} y_2'}}{.. \rightarrow [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..]\, d_1 - e_1 = -\omega(x_2 - y_2)}$$

$$\frac{\frac{\frac{2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial y_2}e_2\geq\frac{\partial p^2}{\partial x_1}d_1\dots}}{[x_1'=d_1,d_1'=-\omega d_2,x_2'=d_2,d_2'=\omega d_1,..](x_1-y_1)^2+(x_2-y_2)^2\geq p^2}$$



$$\frac{\overline{\frac{\partial(d_1-e_1)}{\partial d_1}d_1'+\frac{\partial(d_1-e_1)}{\partial e_1}e_1'=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}x_2'-\frac{\partial\omega(x_2-y_2)}{\partial y_2}y_2'}}{..\to[d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)}$$

$$\frac{\dfrac{\dfrac{2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0}{2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}}{\frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}}{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



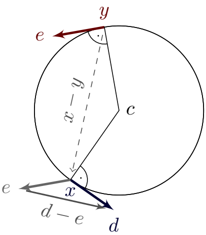
$$\frac{\frac{\partial(d_1 - e_1)}{\partial d_1}(-\omega d_2) + \frac{\partial(d_1 - e_1)}{\partial e_1}(-\omega e_2) = -\frac{\partial\omega(x_2 - y_2)}{\partial x_2} d_2 - \frac{\partial\omega(x_2 - y_2)}{\partial y_2} e_2}{.. \rightarrow [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)}$$

$$2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0$$

$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \dots$$

$$[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



$$-\omega d_2 + \omega e_2 = -\omega(d_2 - e_2)$$

$$\frac{\partial(d_1 - e_1)}{\partial d_1}(-\omega d_2) + \frac{\partial(d_1 - e_1)}{\partial e_1}(-\omega e_2) = -\frac{\partial \omega(x_2 - y_2)}{\partial x_2} d_2 - \frac{\partial \omega(x_2 - y_2)}{\partial y_2} e_2$$

$$.. \rightarrow [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)$$

Differential Invariants & Differential Cuts

$$2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0$$

$$2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

$$\frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots$$

$$[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

Proposition (Differential cut saturation)

C differential invariant of $[x' = \theta \,\&\, H]\phi$, then

$$[x' = \theta \,\&\, H]\phi \quad \text{iff} \quad [x' = \theta \,\&\, H \wedge C]\phi$$

$$-\omega d_2 + \omega e_2 = -\omega(d_2 - e_2)$$

$$\frac{\partial(d_1 - e_1)}{\partial d_1}(-\omega d_2) + \frac{\partial(d_1 - e_1)}{\partial e_1}(-\omega e_2) = -\frac{\partial \omega(x_2 - y_2)}{\partial x_2} d_2 - \frac{\partial \omega(x_2 - y_2)}{\partial y_2} e_2$$

$$.. \rightarrow [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..]\, d_1 - e_1 = -\omega(x_2 - y_2)$$

Differential Invariants & Differential Cuts

$$\dfrac{\dfrac{\dfrac{[x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}{\frac{\partial \|x-y\|^2}{\partial x_1} d_1 + \frac{\partial \|x-y\|^2}{\partial y_1} e_1 + \frac{\partial \|x-y\|^2}{\partial x_2} d_2 + \frac{\partial \|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}}{2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}}{2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0}$$

refine dynamics

by differential cut

$$-\omega d_2 + \omega e_2 = -\omega(d_2 - e_2)$$

$$\frac{\partial(d_1 - e_1)}{\partial d_1}(-\omega d_2) + \frac{\partial(d_1 - e_1)}{\partial e_1}(-\omega e_2) = -\frac{\partial \omega(x_2 - y_2)}{\partial x_2} d_2 - \frac{\partial \omega(x_2 - y_2)}{\partial y_2} e_2$$

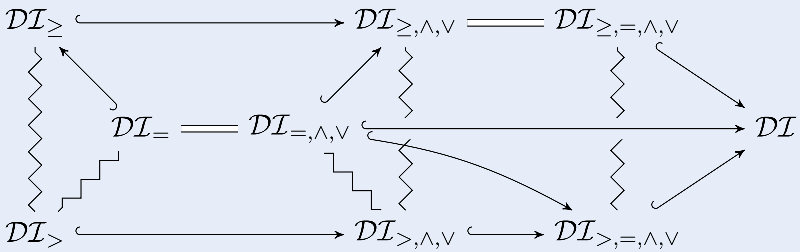
$$.. \to [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)$$

The Structure of Differential Invariants

Theorem (Closure properties of differential invariants) (LMCS 2012)

Closed under conjunction, differentiation, and propositional equivalences.

Theorem (Differential Invariance Chart) (LMCS 2012)

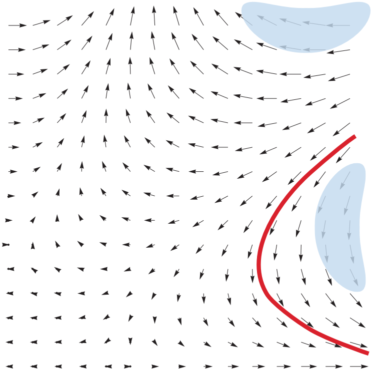


Theorem (Structure of invariant equations / differential cuts)(ITP'12)

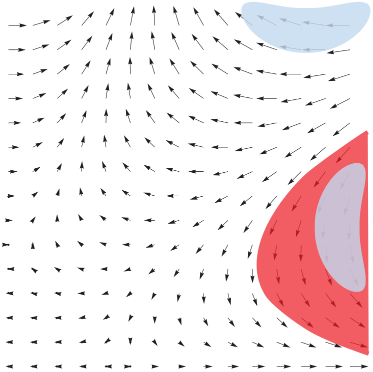
Differential invariants and invariants form chain of differential ideals.

Differential Cuts: Change Dynamics, Not System

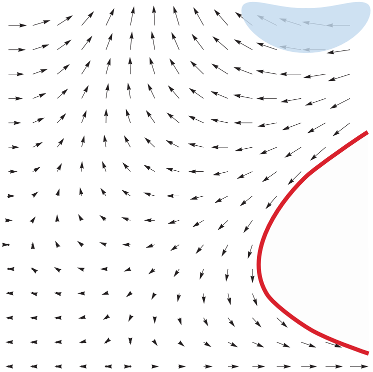
$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \land C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$



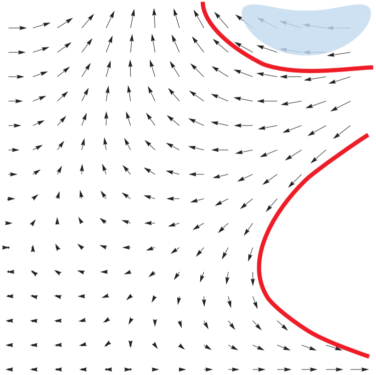
$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \land C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$



$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \wedge C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$

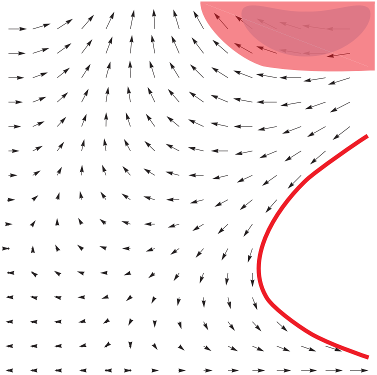


$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \wedge C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$



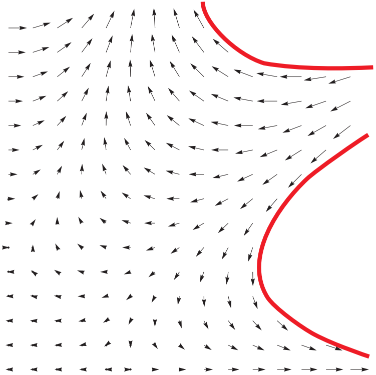
Differential Cuts: Change Dynamics, Not System

$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \land C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$



Differential Cuts: Change Dynamics, Not System

$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \land C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$



Differential Cuts: Change Dynamics, Not System

$$\frac{F\rightarrow[x' = \theta \,\&\, H]C \qquad F\rightarrow[x' = \theta \,\&\, (H \land C)]F}{F\rightarrow[x' = \theta \,\&\, H]F}$$

Theorem (Gentzen's Cut Elimination) (1935)

$$\frac{A\rightarrow B \lor C \quad A \land C\rightarrow B}{A\rightarrow B}$$ *cut can be eliminated*

Differential Cuts: Change Dynamics, Not System

$$\frac{F \rightarrow [x' = \theta \,\&\, H]C \qquad F \rightarrow [x' = \theta \,\&\, (H \land C)]F}{F \rightarrow [x' = \theta \,\&\, H]F}$$

Theorem (Gentzen's Cut Elimination) (1935)

$$\frac{A \rightarrow B \lor C \qquad A \land C \rightarrow B}{A \rightarrow B}$$

cut can be eliminated

Theorem (No Differential Cut Elimination) (LMCS 2012)

Deductive power with differential cut exceeds deductive power without.

$$\mathcal{DCI} > \mathcal{DI}$$

Differential Auxiliaries: Prove in Extra Dimensions

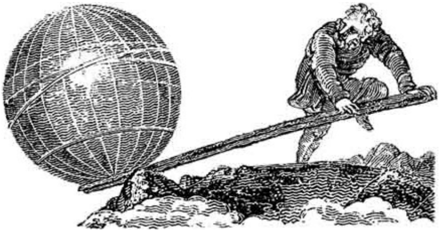
$$\frac{\phi \leftrightarrow \exists y\, \psi \quad \psi \rightarrow [x' = \theta, y' = \vartheta \,\&\, H]\psi}{\phi \rightarrow [x' = \theta \,\&\, H]\phi}$$

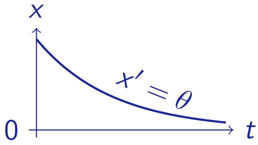
if $y' = \vartheta$ has solution $y : [0, \infty) \rightarrow \mathbb{R}^n$

Theorem (Auxiliary Differential Variables) (LMCS 2012)

Deductive power with differential auxiliaries exceeds power without.

$$\mathcal{DCI} + DA > \mathcal{DCI}$$





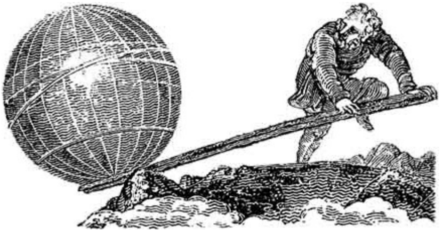
$$\frac{\phi \leftrightarrow \exists y\, \psi \quad \psi \rightarrow [x' = \theta, y' = \vartheta \,\&\, H]\psi}{\phi \rightarrow [x' = \theta \,\&\, H]\phi}$$

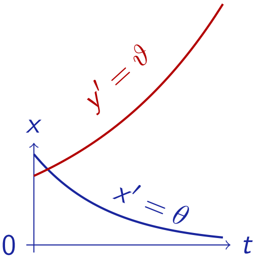
if $y' = \vartheta$ has solution $y : [0, \infty) \rightarrow \mathbb{R}^n$

Theorem (Auxiliary Differential Variables) (LMCS 2012)

Deductive power with differential auxiliaries exceeds power without.

$$\mathcal{DCI} + DA > \mathcal{DCI}$$





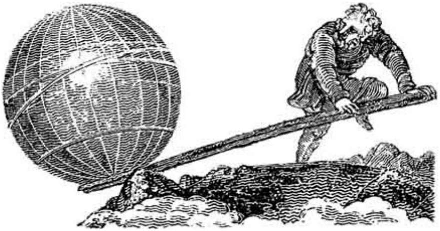
$$\frac{\phi \leftrightarrow \exists y\, \psi \quad \psi \rightarrow [x' = \theta, y' = \vartheta \,\&\, H]\psi}{\phi \rightarrow [x' = \theta \,\&\, H]\phi}$$

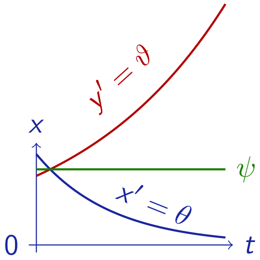
if $y' = \vartheta$ has solution $y : [0, \infty) \to \mathbb{R}^n$

Theorem (Auxiliary Differential Variables) (LMCS 2012)

Deductive power with differential auxiliaries exceeds power without.

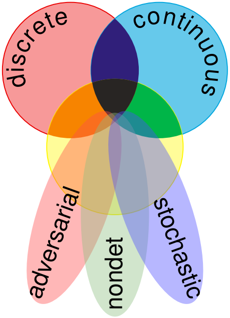
$$\mathcal{DCI} + DA > \mathcal{DCI}$$





Outline

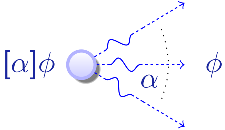
Family of Differential Dynamic Logics

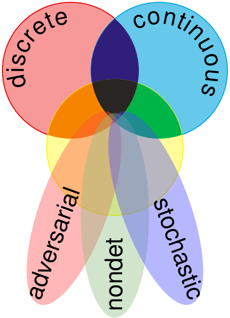


Family of Differential Dynamic Logics

differential dynamic logic

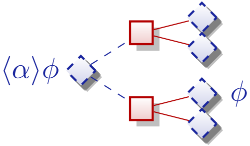
$\text{d}\mathcal{L} = \text{DL} + \text{HP}$





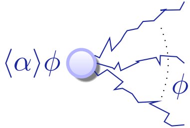
differential game logic

$\text{dG}\mathcal{L} = \text{GL} + \text{HG}$



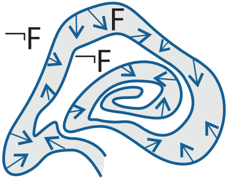
stochastic differential DL

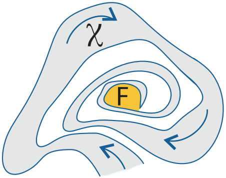
$\text{Sd}\mathcal{L} = \text{DL} + \text{SHP}$

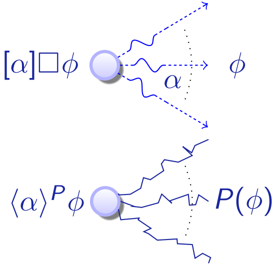


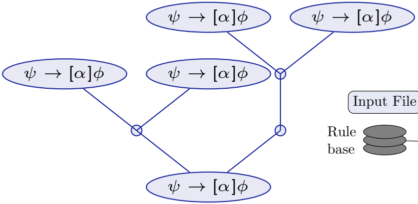
quantified differential DL

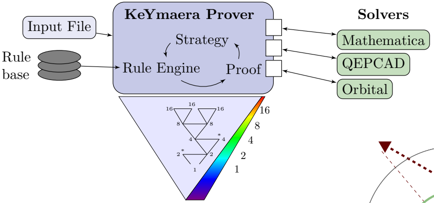
$\text{Qd}\mathcal{L} = \text{FOL} + \text{DL} + \text{QHP}$

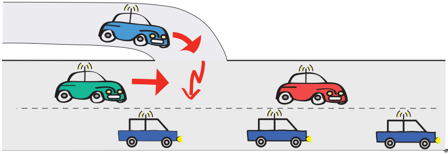

¬F
F
¬F

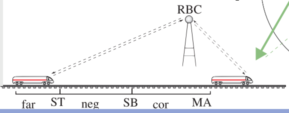

χ
F

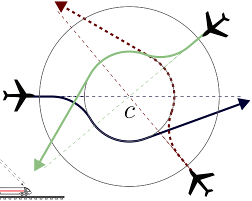

$[\alpha]\Box\phi$
α
ϕ
$\langle\alpha\rangle^P\phi$
$P(\phi)$

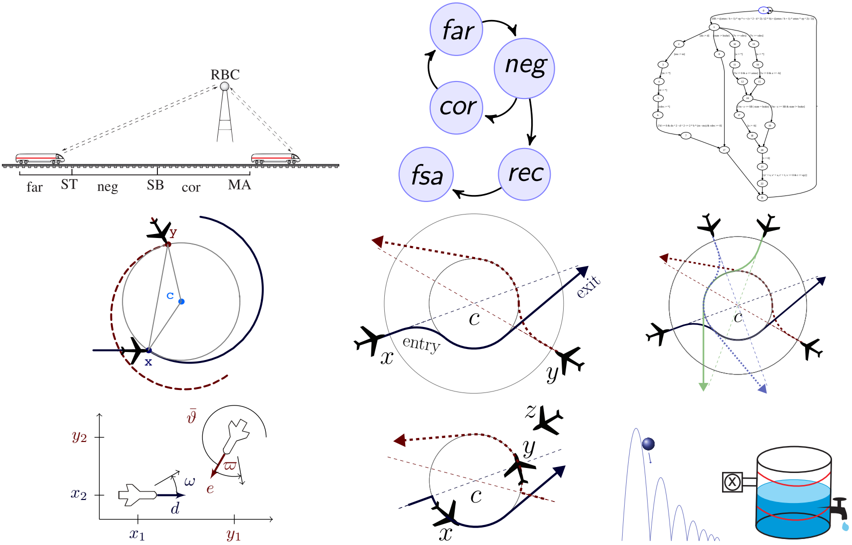

$\psi \to [\alpha]\phi$
$\psi \to [\alpha]\phi$
$\psi \to [\alpha]\phi$
$\psi \to [\alpha]\phi$
$\psi \to [\alpha]\phi$


KeYmaera Prover
Input File
Rule
base
Strategy
Rule Engine
Proof
Solvers
Mathematica
QEPCAD
Orbital
16
8
4
2
1

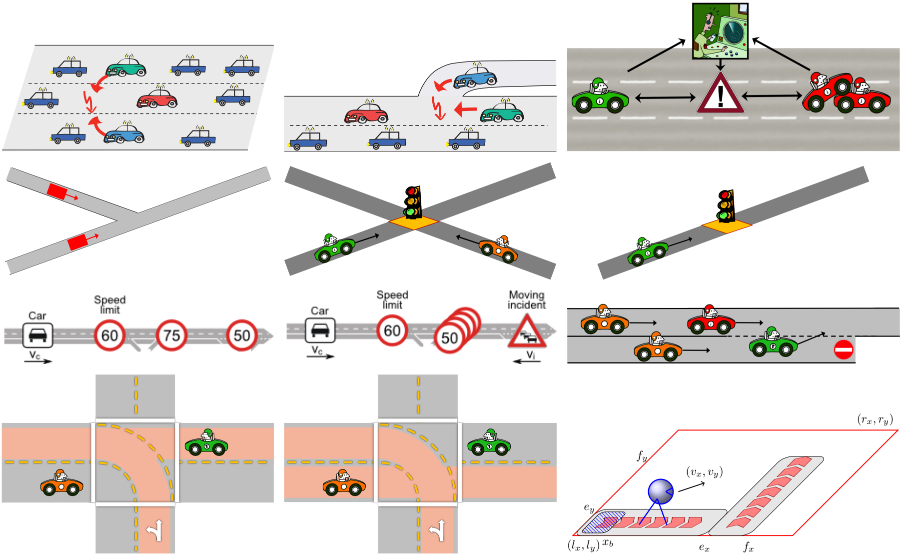



RBC
far
ST
neg
SB
cor
MA

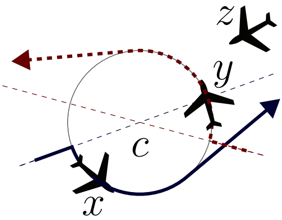

c

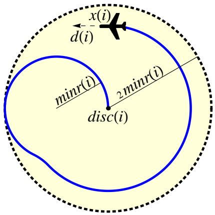

RBC
far
ST
neg
SB
cor
MA
far
neg
cor
fsa
rec
y
c
x
c
entry
exit
x
y
c
$\bar{\vartheta}$
y_2
x_2
ω
ϖ
e
d
x_1
y_1
z
y
c
x

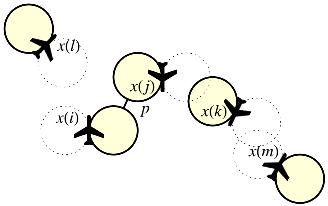
Successful Hybrid Systems Proofs

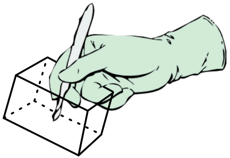


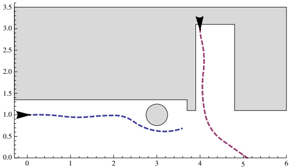
Successful Hybrid Systems Proofs

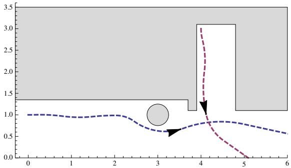


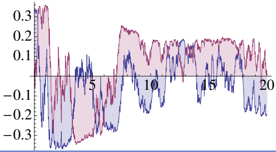


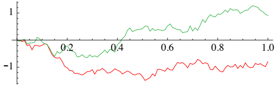


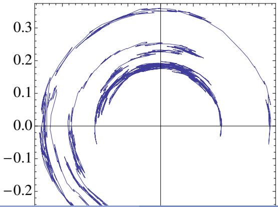










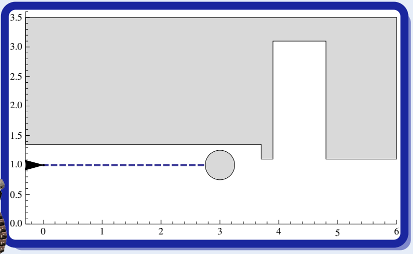


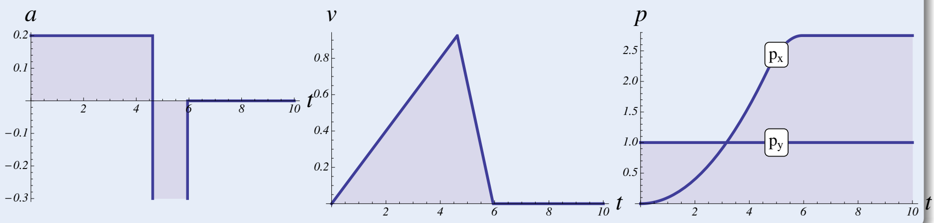
Outline

Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)

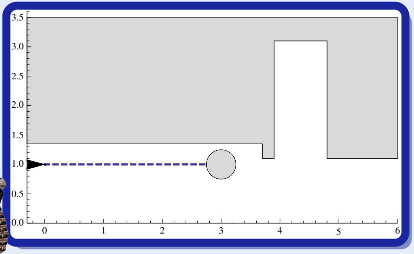


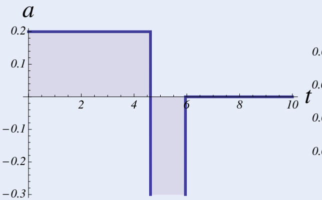


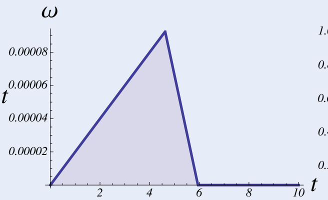
Challenge (Hybrid Systems)

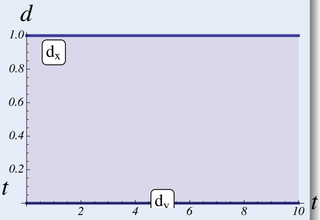
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)





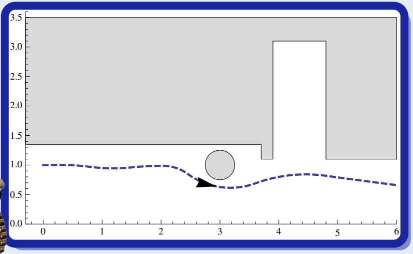


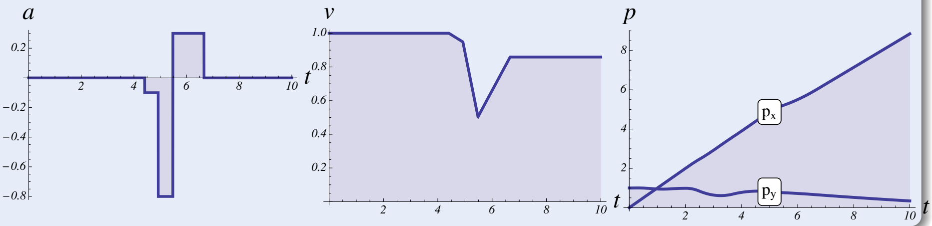


Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)

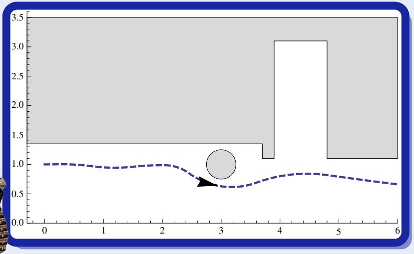


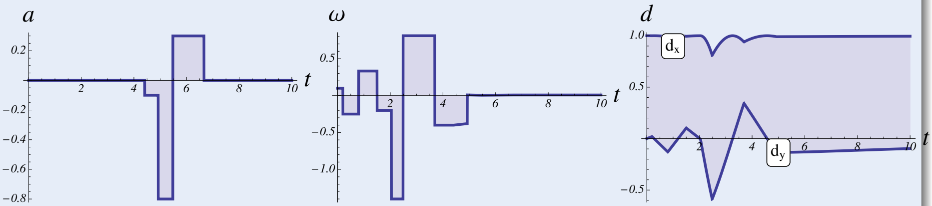


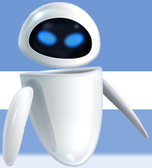
Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



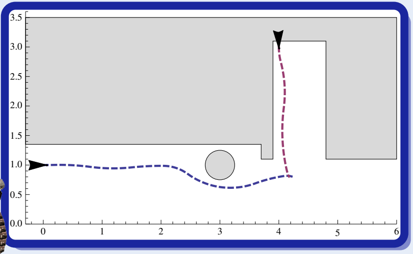


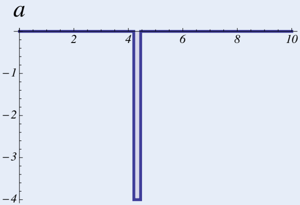


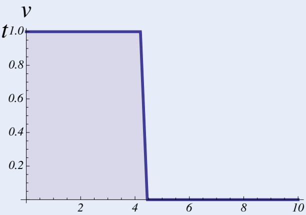
Challenge (Hybrid Systems)

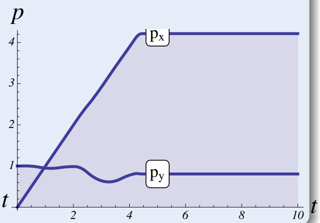
Fixed rule describing state evolution with both

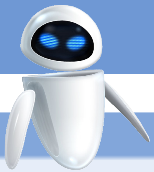
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)







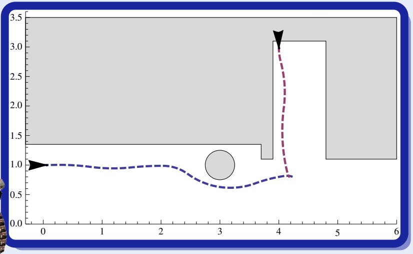


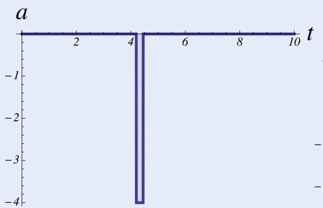


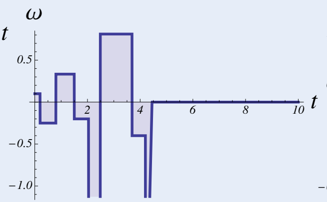
Challenge (Hybrid Systems)

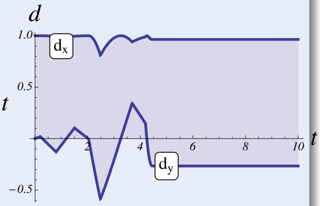
Fixed rule describing state evolution with both

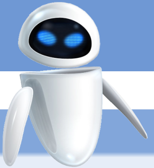
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)







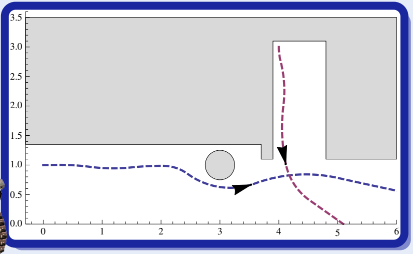


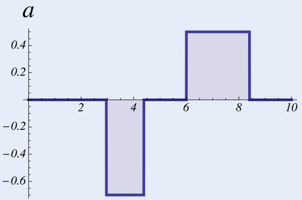


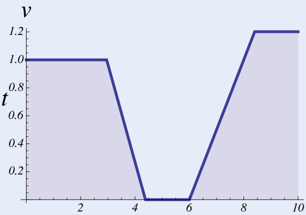
Challenge (Hybrid Systems)

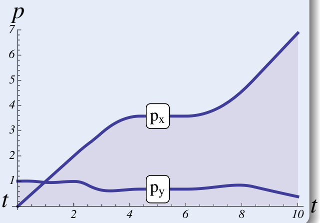
Fixed rule describing state evolution with both

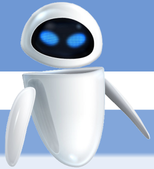
- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)







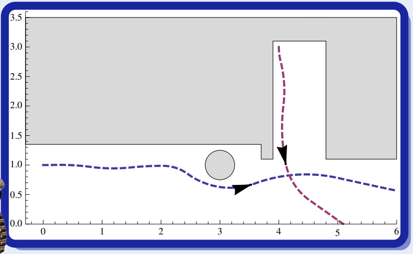


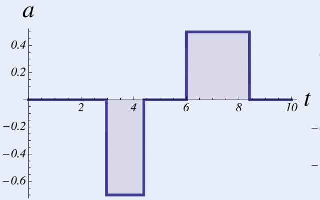


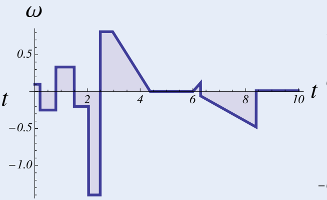
Challenge (Hybrid Systems)

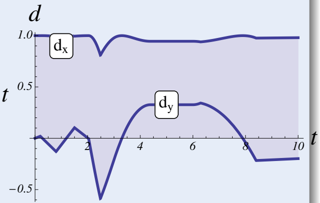
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)





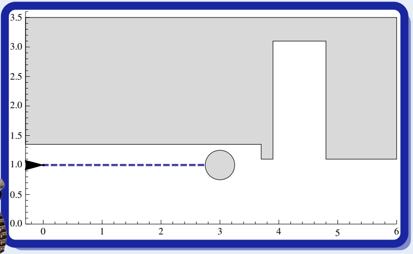


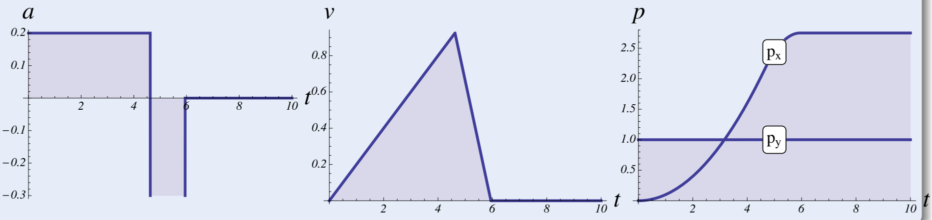


Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)

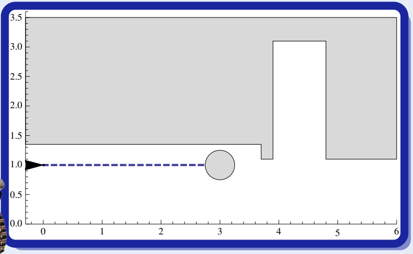


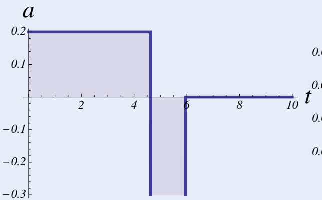


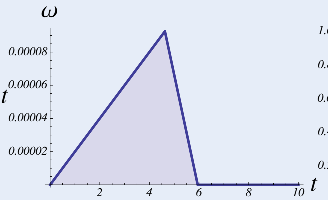
Challenge (Hybrid Systems)

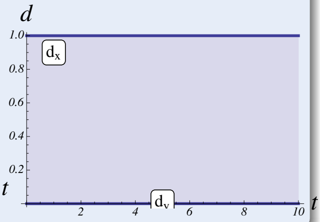
Fixed rule describing state evolution with both

- Discrete dynamics (control decisions)
- Continuous dynamics (differential equations)



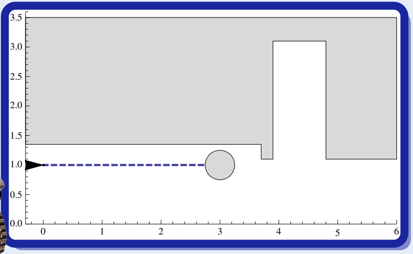


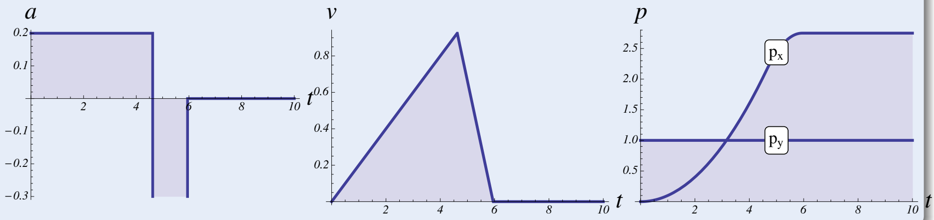




Challenge (Hybrid Systems)

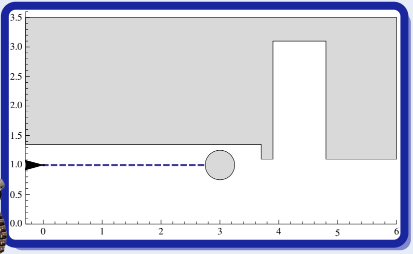
$$a_r := -b$$
$$\cup\ (a_r := *; ?-b \le a_r \le A)$$

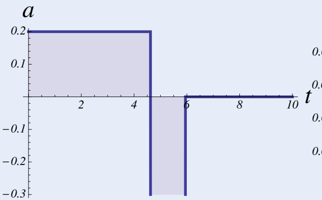


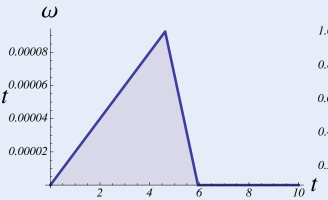


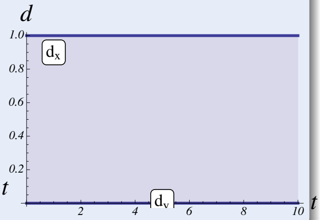
Challenge (Hybrid Systems)

$$a_r := -b$$
$$\cup \ (a_r := *; ?-b \le a_r \le A)$$



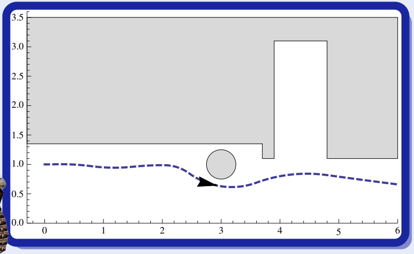


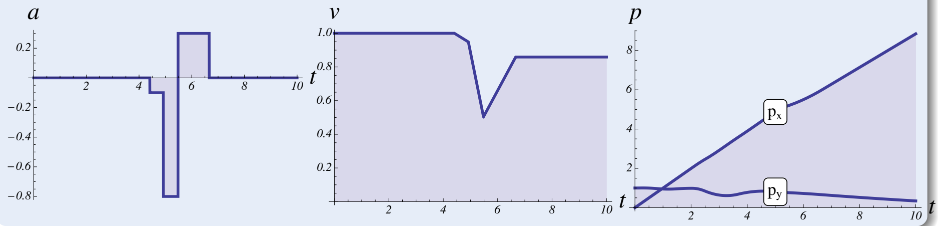




Challenge (Hybrid Systems)

$$
\begin{aligned}
& a_r := -b \\
\cup\ & (a_r := *; ?-b \leq a_r \leq A; \\
& \quad \omega_r := *; ?-\Omega \leq \omega_r \leq \Omega; \\
& \quad ?\mathrm{SafeCtrl}) \\
\cup\ & (?v_r = 0; a_r := 0; \omega_r := 0)
\end{aligned}
$$





Hybrid Systems Analysis

Challenge (Hybrid Systems)

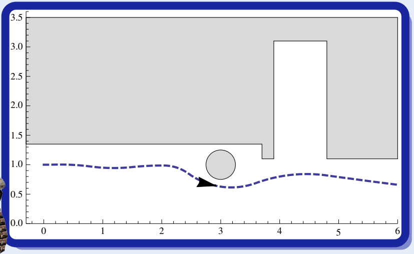
$a_r := -b$

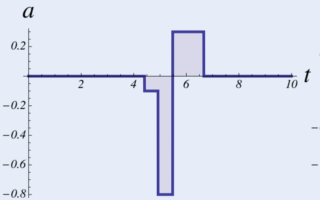
$\cup\ (a_r := *; ?-b \le a_r \le A;$

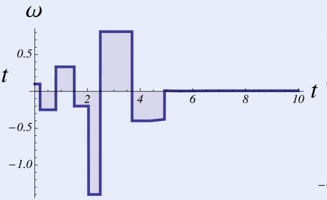
$\quad \omega_r := *; ?-\Omega \le \omega_r \le \Omega;$

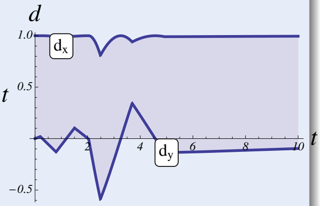
$\quad ?\text{SafeCtrl})$

$\cup\ (?v_r = 0; a_r := 0; \omega_r := 0)$

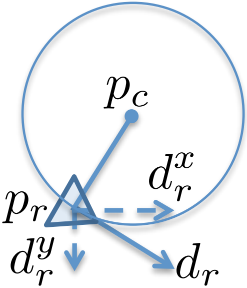


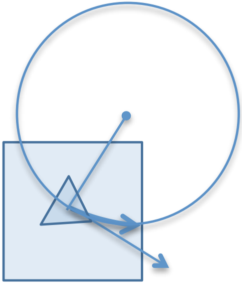






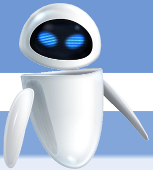
translational ODE	$p_r' = v_r d_r$	$v_r' = a_r$	
rotational DAE	$\omega_r' \|p_r - p_c\| = a_r$		
	$d_r^{x\prime} = -\omega_r d_r^y$	$d_r^{y\prime} = \omega_r d_r^x$	





Example (Differential invariants)

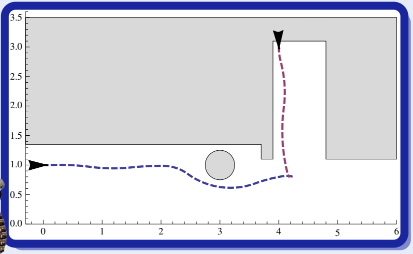
1. Move on circle: $p_r - p_c = \omega d_r^{\perp}$
2. Stay in the box: $\|p_r - p_0\|_\infty \leq v_r t + \frac{a_r}{2} t^2$

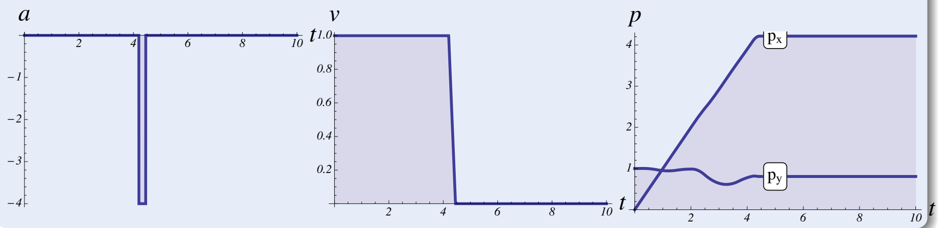


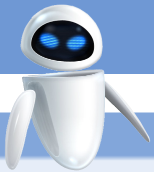
Challenge (Hybrid Systems)

Moving obstacles: distance on current curve not enough

- Dynamic obstacles (other agents)
- Avoid collisions (define safety)



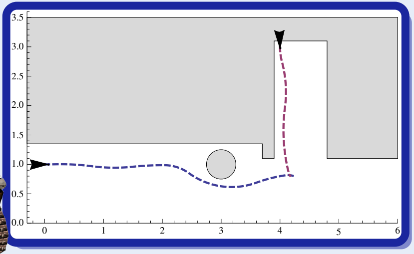


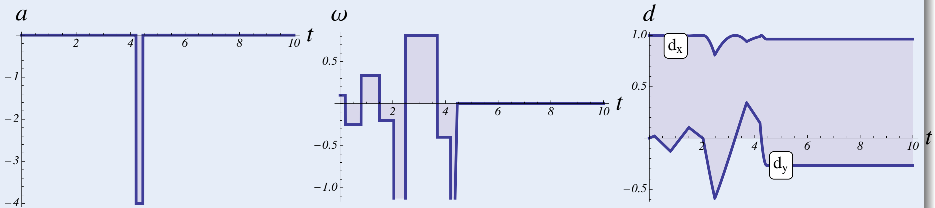


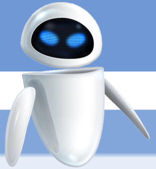
Challenge (Hybrid Systems)

Moving obstacles: distance on current curve not enough

- Dynamic obstacles (other agents)
- Avoid collisions (define safety)



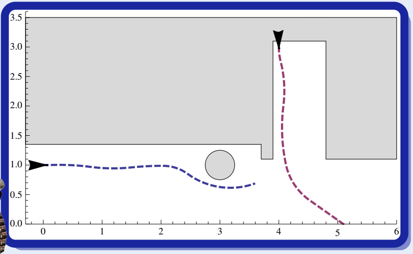


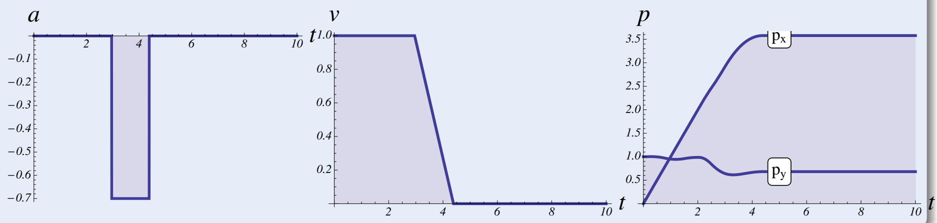


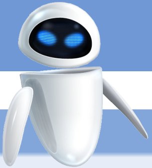
Challenge (Hybrid Systems)

Passive safety: no active collision while moving

- Dynamic obstacles (other agents)
- Avoid collisions (passive safety)



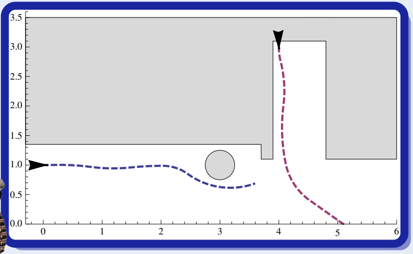


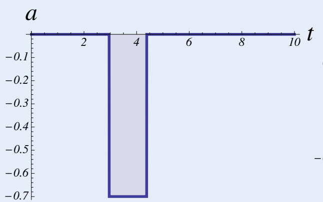


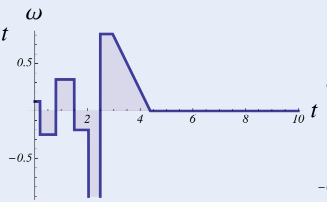
Challenge (Hybrid Systems)

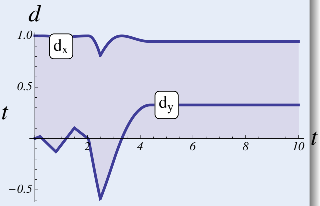
Passive safety: no active collision while moving

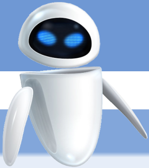
- Dynamic obstacles (other agents)
- Avoid collisions (passive safety)







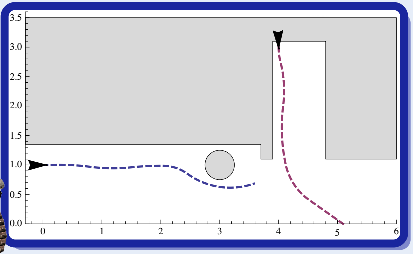


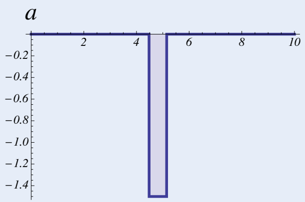


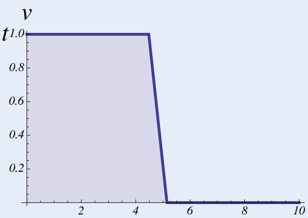
Challenge (Hybrid Systems)

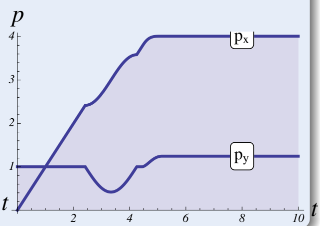
Passive friendly safety: don't cause unavoidable collision

- Dynamic obstacles (other agents)
- Avoid collisions (friendly safety)

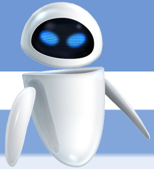








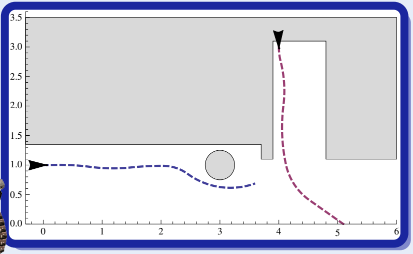
Hybrid Systems Analysis

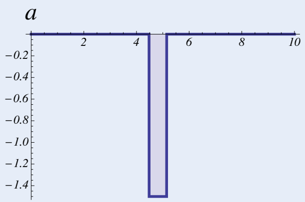


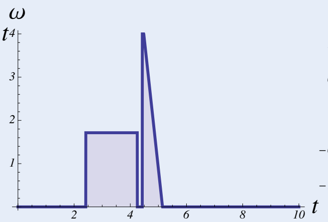
Challenge (Hybrid Systems)

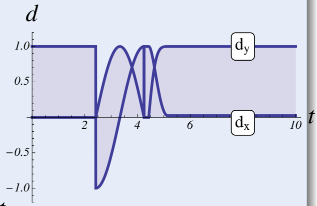
Passive friendly safety: don't cause unavoidable collision

- Dynamic obstacles (other agents)
- Avoid collisions (friendly safety)

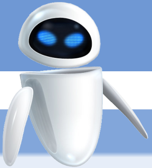






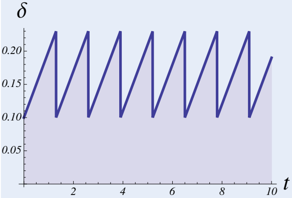


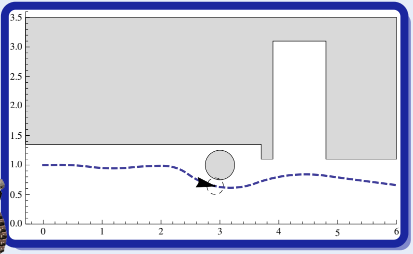
Hybrid Systems Analysis

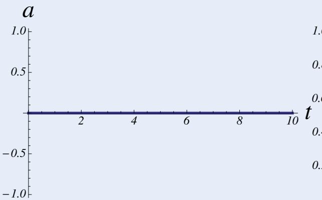


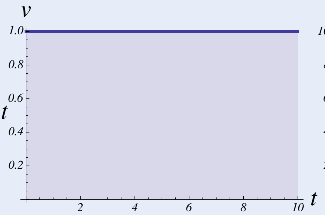
Challenge (Hybrid Systems)

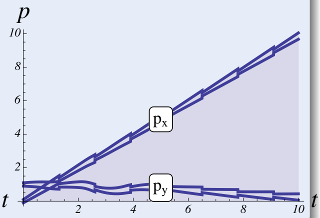
Sensor failure: Uncertainty of fallback to dead reckoning

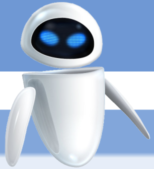






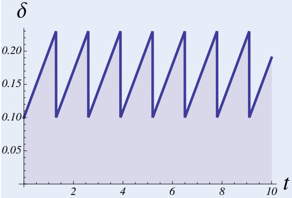


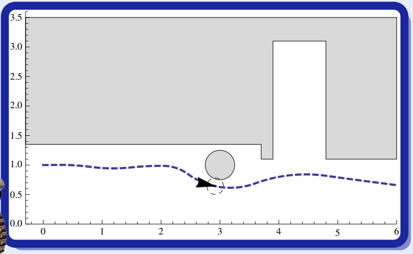


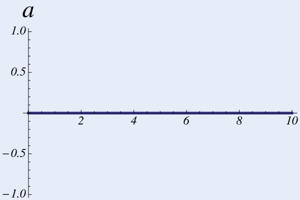


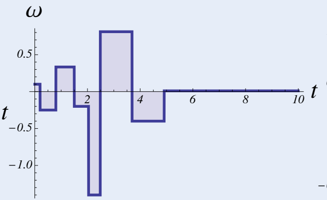
Challenge (Hybrid Systems)

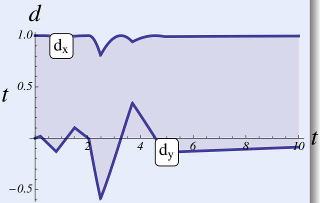
Sensor failure: Uncertainty of fallback to dead reckoning







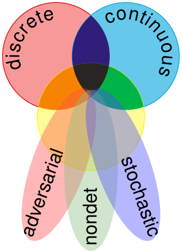




Robot Invariants and Constraints

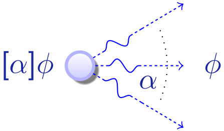
Safety	Invariant	+ Safe Control	(RSS'13)
static	$\|p_r - p_o\|_\infty > \frac{v_r^2}{2b}$	$+\left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon v_r\right)$	
passive	$v_r = 0 \lor \|p_r - p_o\|_\infty > \frac{v_r^2}{2b}$	$+V\frac{v_r}{b} + \left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$	
+ sensor	$\|\hat{p}_r - p_o\|_\infty > \frac{v_r^2}{2b} + V\frac{v_r}{b}$	$+\left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right) + U_p$	
+ disturb	$\|p_r - p_o\|_\infty > \frac{v_r^2}{2bU_m} + V\frac{v_r}{bU_m}$	$+\left(\frac{A}{bU_m}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$	
+ failure	$\|\hat{p}_r - p_o\|_\infty > \frac{v_r^2}{2b} + V\frac{v_r}{b}$	$+\left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v + V)\right) + U_p + g\Delta$	
friendly	$\|p_r - p_o\|_\infty > \frac{v_r^2}{2b} + \frac{V^2}{2b_o} + V\left(\frac{v_r}{b} + \tau\right)$	$+\left(\frac{A}{b}+1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon(v_r + V)\right)$	

Outline



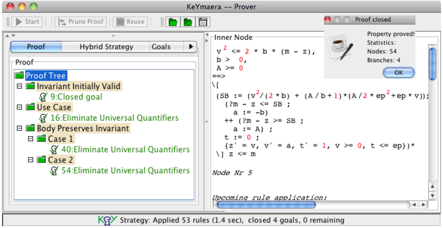
differential dynamic logic

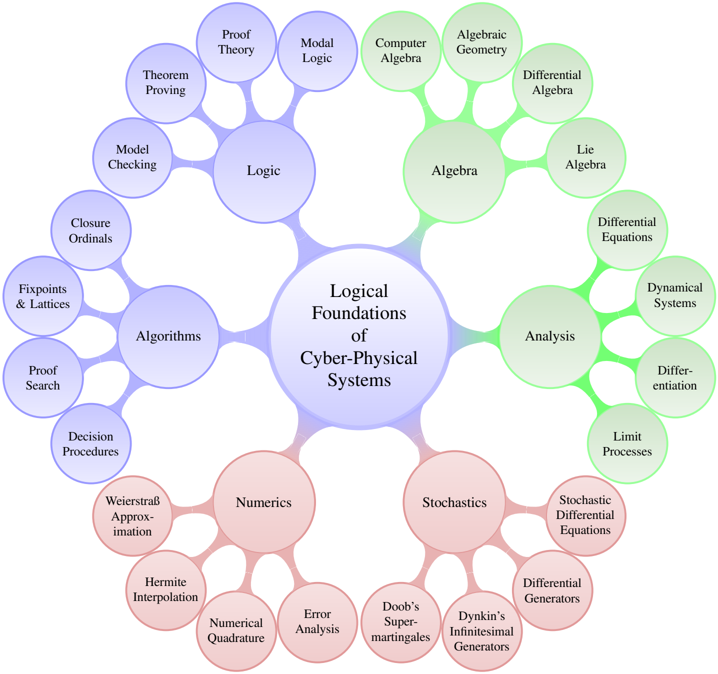
$$d\mathcal{L} = \text{DL} + \text{HP}$$

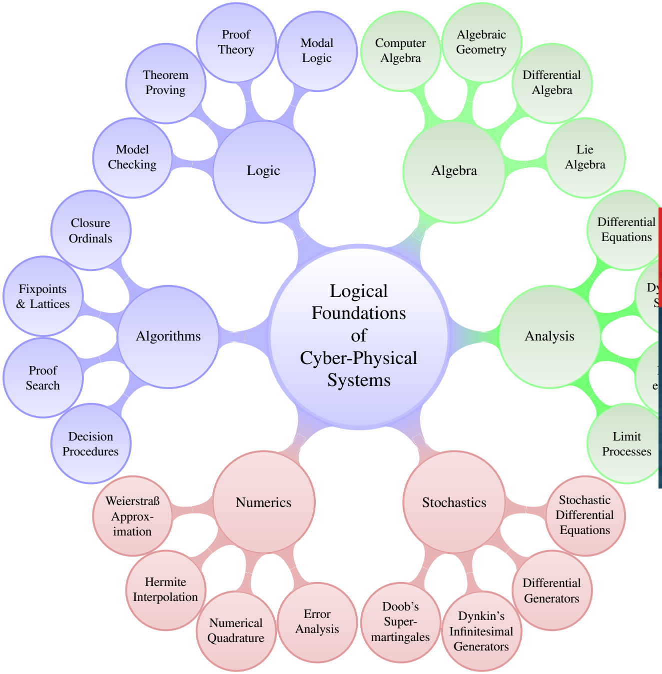


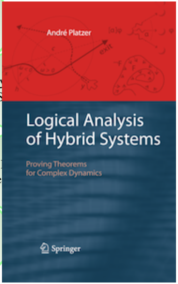
- Logic for hybrid systems
- Logic + distributed hybrid systems
- Logic + stochastic hybrid systems
- Compositional proofs
- Sound & complete / ODE
- Differential invariants

KeYmaera




Logical Foundations of Cyber-Physical Systems
Logic
Proof Theory
Modal Logic
Theorem Proving
Model Checking
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Lie Algebra
Analysis
Differential Equations
Dynamical Systems
Differ- entiation
Limit Processes
Algorithms
Closure Ordinals
Fixpoints & Lattices
Proof Search
Decision Procedures
Numerics
Weierstraß Approx- imation
Hermite Interpolation
Numerical Quadrature
Error Analysis
Stochastics
Stochastic Differential Equations
Differential Generators
Dynkin's Infinitesimal Generators
Doob's Super- martingales


Logical Foundations of Cyber-Physical Systems
Logic
Proof Theory
Modal Logic
Theorem Proving
Model Checking
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Lie Algebra
Algorithms
Closure Ordinals
Fixpoints & Lattices
Proof Search
Decision Procedures
Analysis
Differential Equations
Limit Processes
Numerics
Weierstraß Approx-imation
Hermite Interpolation
Numerical Quadrature
Error Analysis
Stochastics
Stochastic Differential Equations
Differential Generators
Doob's Super-martingales
Dynkin's Infinitesimal Generators


André Platzer
Logical Analysis of Hybrid Systems
Proving Theorems for Complex Dynamics
Springer

Outline

Differential Dynamic Logic: Axiomatization

$$[:=] \quad [x := \theta][(x)]\phi x \leftrightarrow [(x)]\phi\theta$$

$$[?] \quad [?H]\phi \leftrightarrow (H \rightarrow \phi)$$

$$['] \quad [x' = f(x)]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi \qquad (y'(t) = f(y))$$

$$[\cup] \quad [\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \land [\beta]\phi$$

$$[;] \quad [\alpha; \beta]\phi \leftrightarrow [\alpha][\beta]\phi$$

$$[^*] \quad [\alpha^*]\phi \leftrightarrow \phi \land [\alpha][\alpha^*]\phi$$

$$\text{K} \quad [\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$$

$$\text{I} \quad [\alpha^*](\phi \rightarrow [\alpha]\phi) \rightarrow (\phi \rightarrow [\alpha^*]\phi)$$

$$\text{C} \quad [\alpha^*]\forall v{>}0\, (\varphi(v) \rightarrow \langle\alpha\rangle\varphi(v-1)) \rightarrow \forall v\, (\varphi(v) \rightarrow \langle\alpha^*\rangle\exists v{\leq}0\, \varphi(v))$$