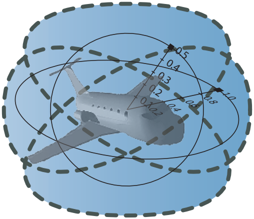
Theorem Proving for Dynamic Systems

André Platzer

aplatzer@cs.cmu.edu
Logical Systems Lab
Carnegie Mellon University, Pittsburgh, PA

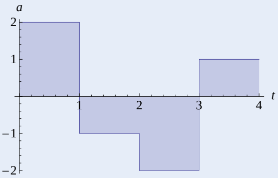


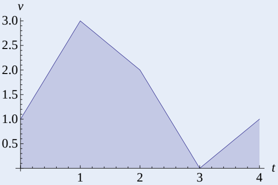
How can we design computers that are guaranteed to interact correctly with the physical world?

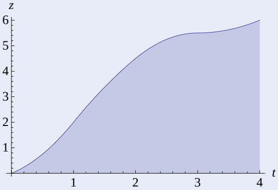
Challenge

Hybrid Systems

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







Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

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

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe

Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

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

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe
2. More than physics: braking control $v^2 \leq 2b(M - z)$ $\not\Rightarrow$ safe

Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

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

1. More than computers: no `NullPointerException` $\not\Rightarrow$ safe
2. More than physics: braking control $v^2 \leq 2b(M - z) \not\Rightarrow$ safe
3. Joint dynamics requires: $SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v \ldots$

Challenge

Hybrid Systems

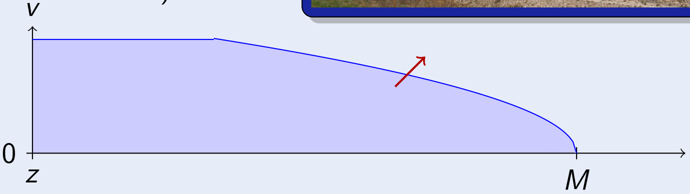
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

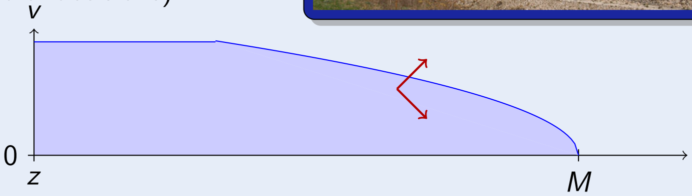
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid Systems

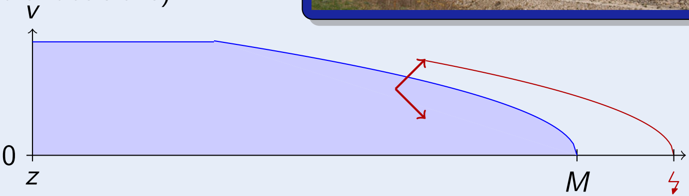
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



Challenge

Hybrid Systems

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

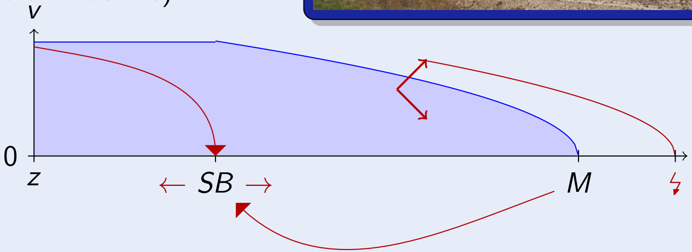


Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

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

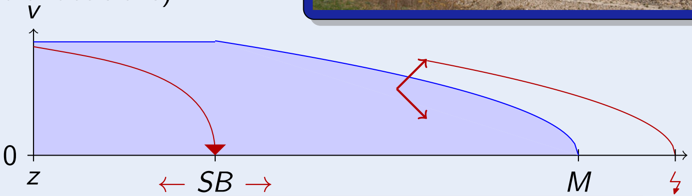


Hybrid Systems Analysis: Train Control

Challenge

Hybrid Systems

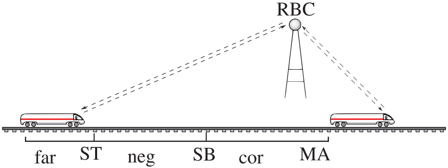
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)



$$\boxed{SB \geq \frac{v^2}{2b} + \frac{a^2\varepsilon^2}{2b} + \frac{a}{b}\varepsilon v + \frac{a}{2}\varepsilon^2 + \varepsilon v}$$

differential dynamic logic

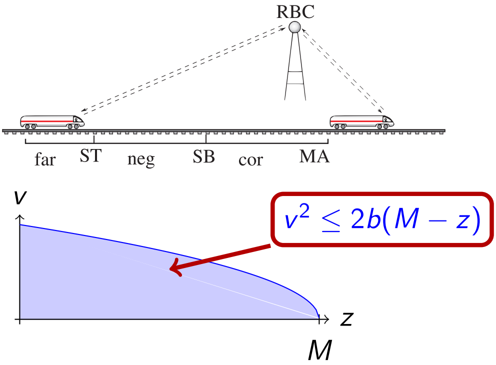
$d\mathcal{L} = \quad DL + HP$



André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

differential dynamic logic

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

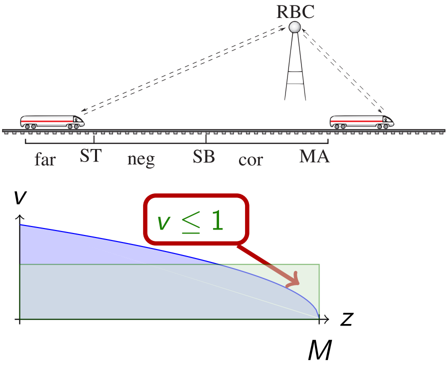


André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

Logic for Hybrid Systems

differential dynamic logic

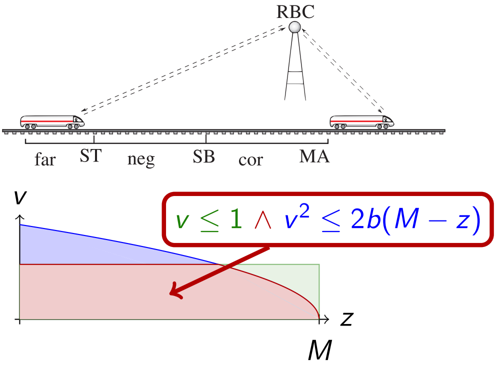
$\mathsf{d}\mathcal{L} = \mathsf{FOL}_{\mathbb{R}}$



André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

differential dynamic logic

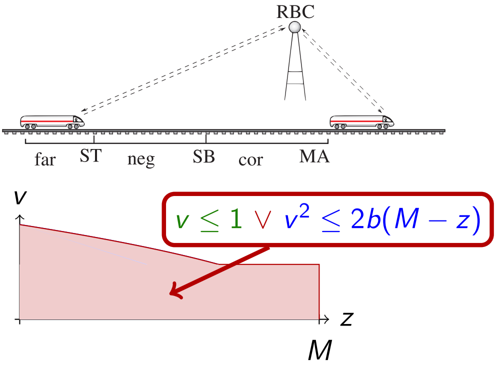
$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$



André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

differential dynamic logic

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



André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

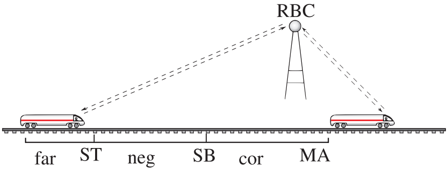
Logic for Hybrid Systems

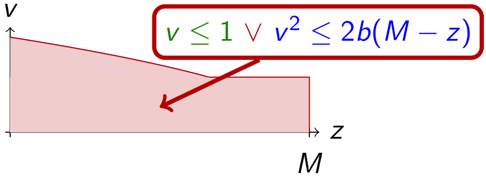
differential dynamic logic

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

$\forall MA\, \exists SB \;\ldots$

$\forall t \geq 0 \;\ldots$



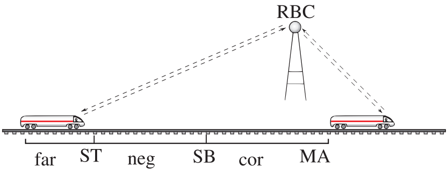


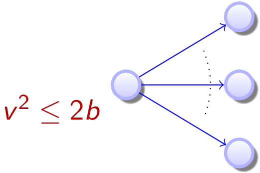
André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

Logic for Hybrid Systems

differential dynamic logic

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



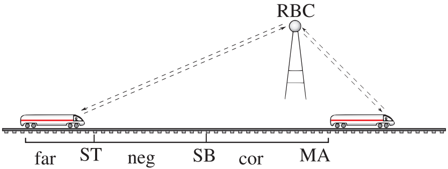


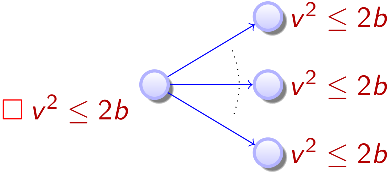
André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

Logic for Hybrid Systems

differential dynamic logic

$d\mathcal{L} = FOL_{\mathbb{R}} + ML$



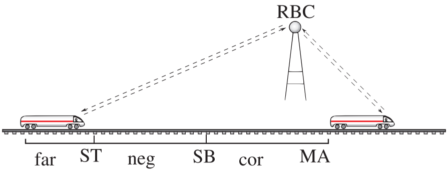


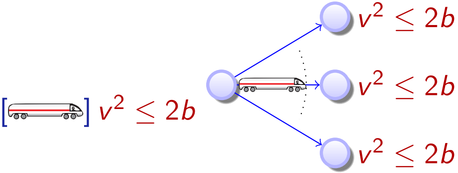
André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

Logic for Hybrid Systems

differential dynamic logic

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



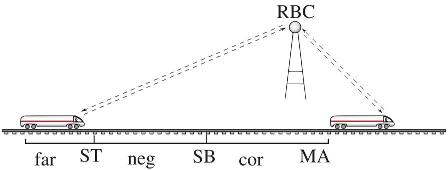


André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

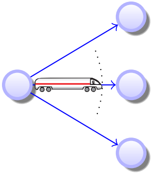
Logic for Hybrid Systems

differential dynamic logic

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



$$[z'' = a]\, v^2 \le 2b$$



$v^2 \le 2b$

$v^2 \le 2b$

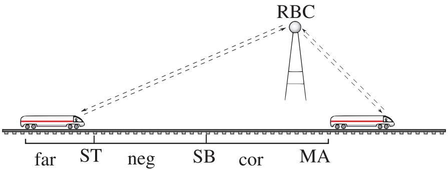
$v^2 \le 2b$

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

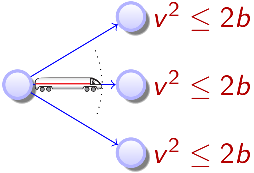
Logic for Hybrid Systems

differential dynamic logic

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



$[\mathtt{if}(z > SB)\, a := -b;\ z'' = a]\, v^2 \leq 2b$

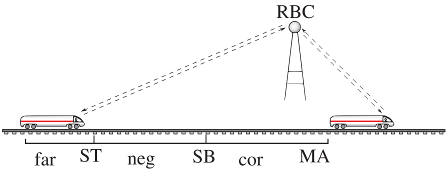


André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

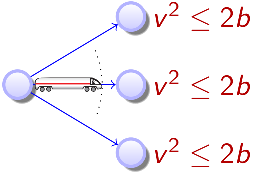
Logic for Hybrid Systems

differential dynamic logic

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



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

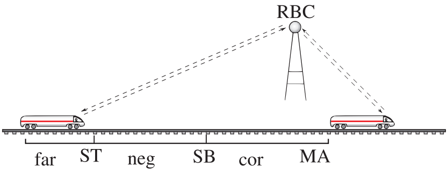


André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

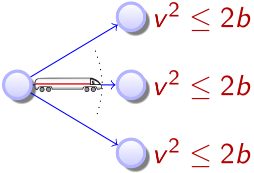
Logic for Hybrid Systems

differential dynamic logic

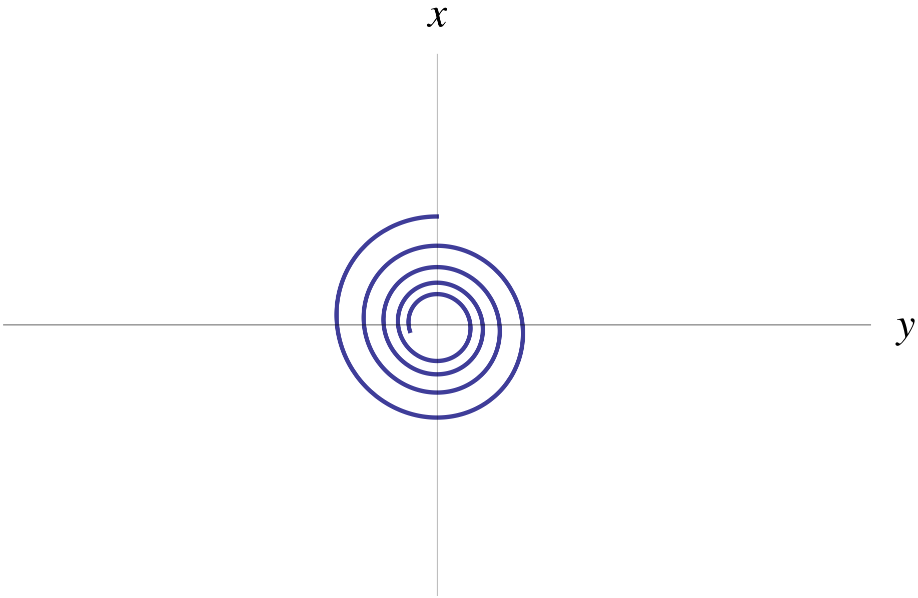
$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}} + \mathrm{DL} + \mathrm{HP}$



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

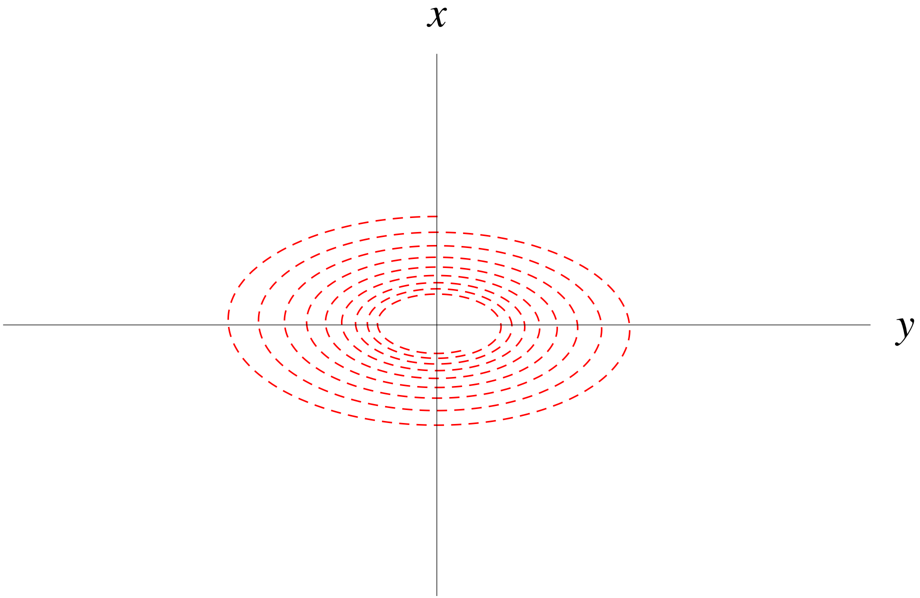


André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

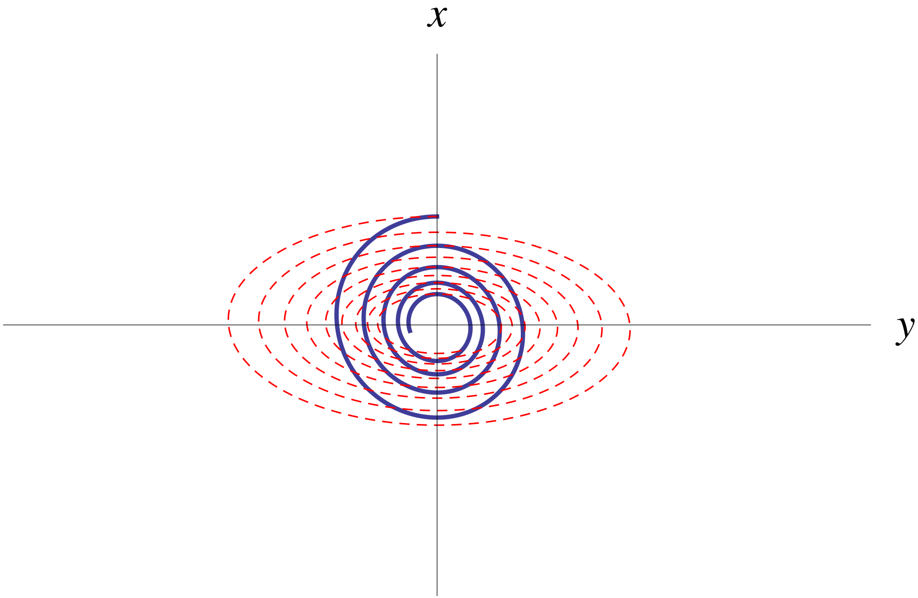


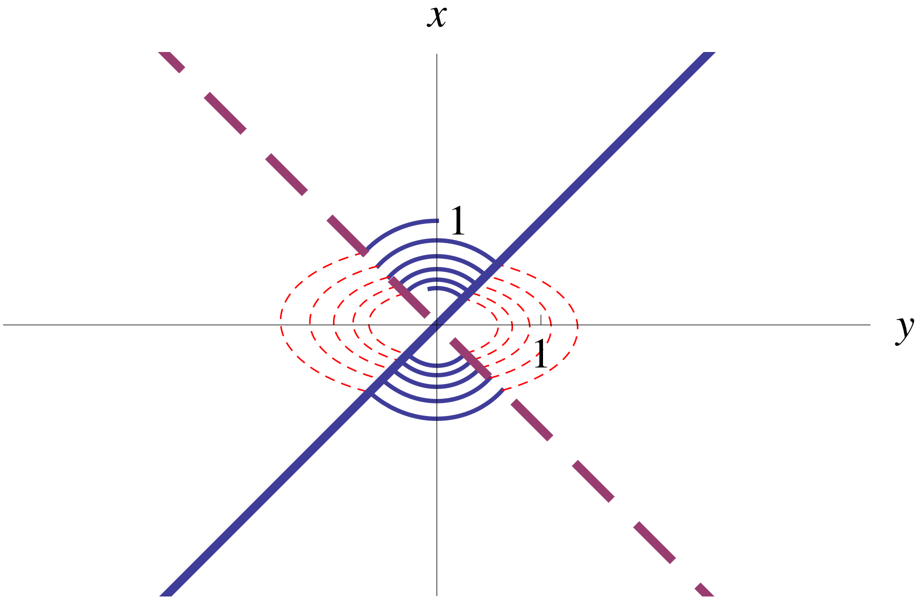
x
y

Safe Switching in Hybrid Systems

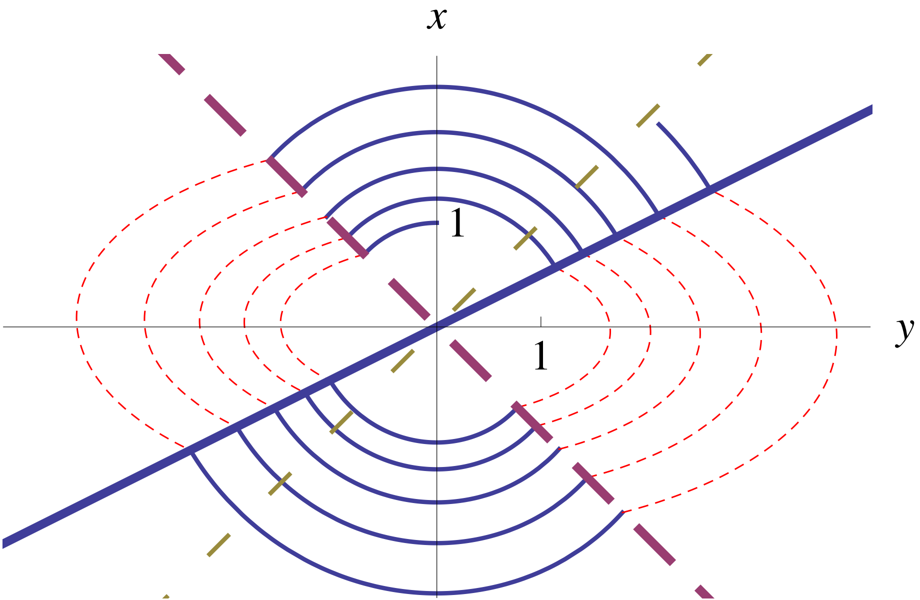


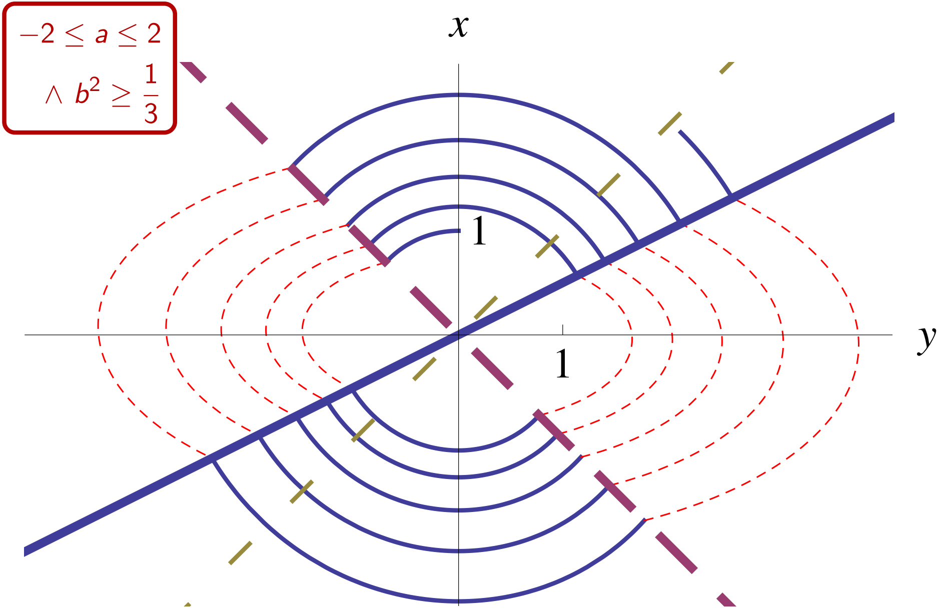
Safe Switching in Hybrid Systems



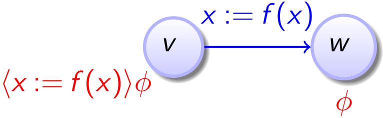

x
y
1
1

Safe Switching in Hybrid Systems

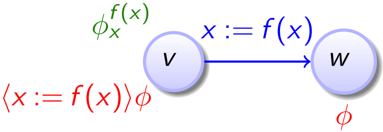



$-2 \leq a \leq 2$
$\land\ b^2 \geq \frac{1}{3}$
x
y
1
1

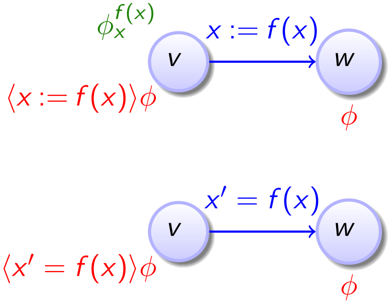
Proof by Symbolic Decomposition

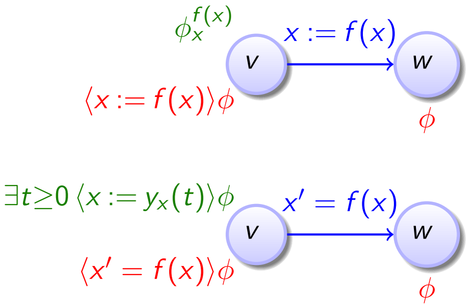


Proof by Symbolic Decomposition

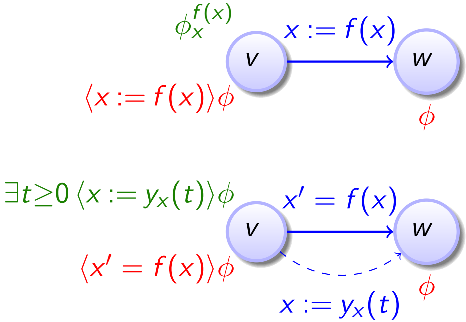


Proof by Symbolic Decomposition

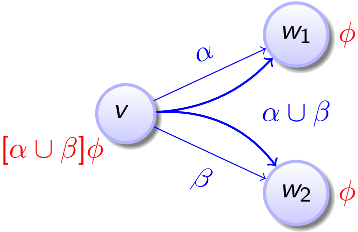


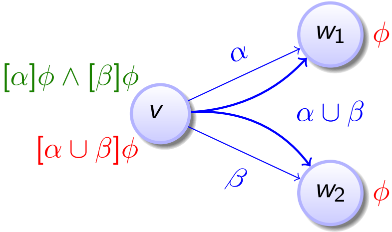

$\phi_x^{f(x)}$
$x := f(x)$
v
w
$\langle x := f(x) \rangle \phi$
ϕ
$\exists t \geq 0 \, \langle x := y_x(t) \rangle \phi$
$x' = f(x)$
v
w
$\langle x' = f(x) \rangle \phi$
ϕ

Proof by Symbolic Decomposition

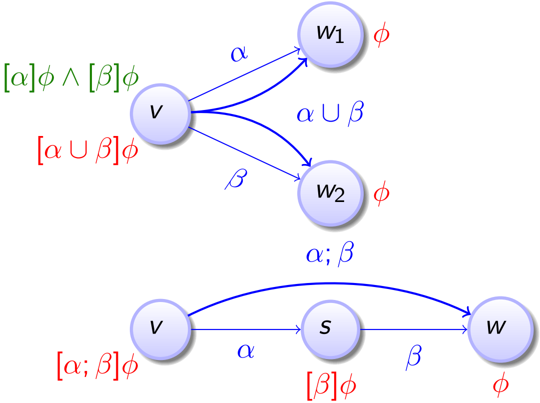


Proof by Symbolic Decomposition

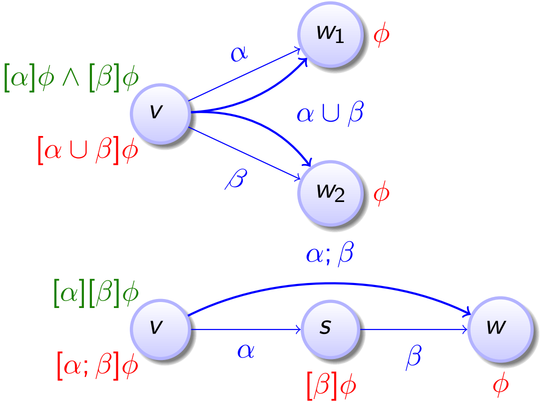



$[\alpha]\phi \land [\beta]\phi$
$[\alpha \cup \beta]\phi$
v
α
$\alpha \cup \beta$
β
w_1
ϕ
w_2
ϕ

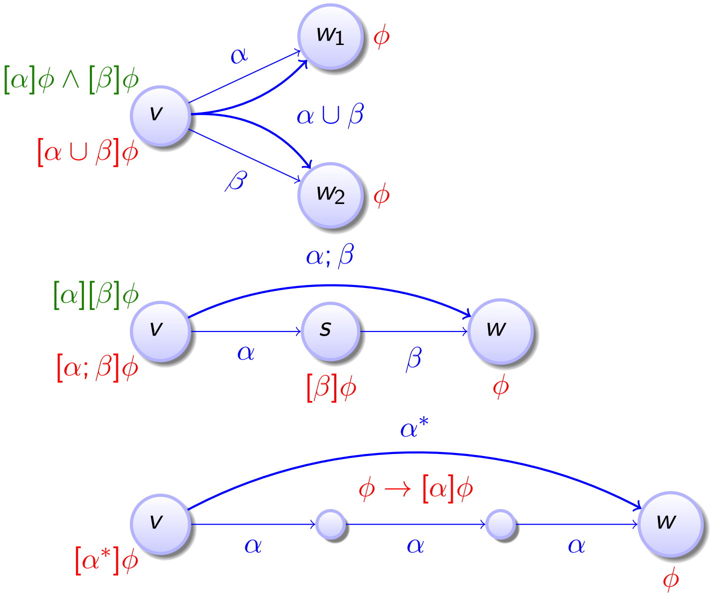
Proof by Symbolic Decomposition

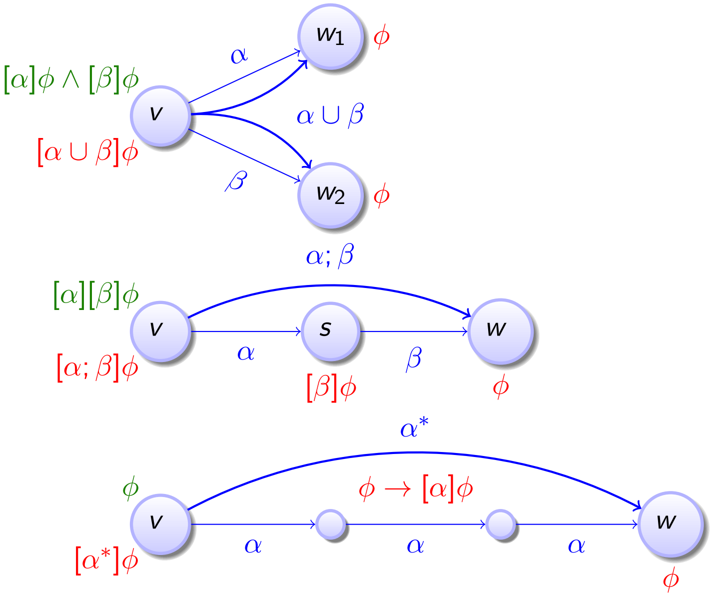


Proof by Symbolic Decomposition

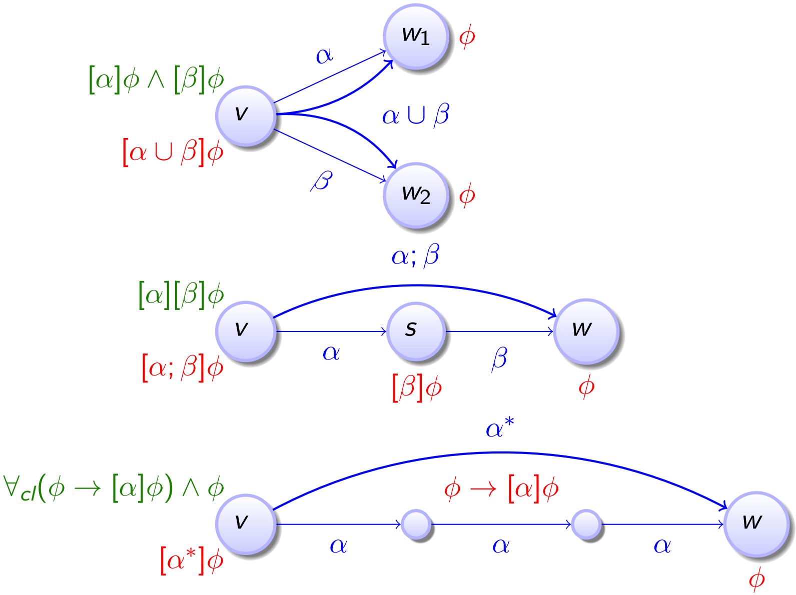


Proof by Symbolic Decomposition




w_1
ϕ
α
$[\alpha]\phi \wedge [\beta]\phi$
v
$\alpha \cup \beta$
$[\alpha \cup \beta]\phi$
β
w_2
ϕ
$\alpha; \beta$
$[\alpha][\beta]\phi$
v
s
w
$[\alpha; \beta]\phi$
α
β
$[\beta]\phi$
ϕ
α^*
ϕ
$\phi \to [\alpha]\phi$
v
w
$[\alpha^*]\phi$
α
α
α
ϕ

Proof by Symbolic Decomposition



Soundness and Completeness

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations.*

Proof Outline 15p

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

Soundness and Completeness

Theorem (Relative Completeness)

d$\mathcal{L}$ *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations.* Proof Outline 15p

Corollary (Proof-theoretical Alignment)

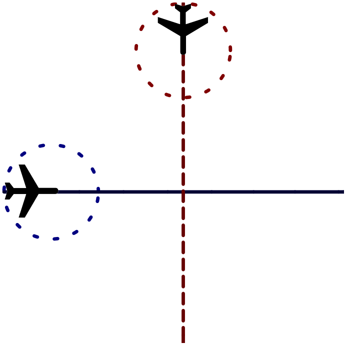
verification of hybrid systems = verification of dynamical systems!

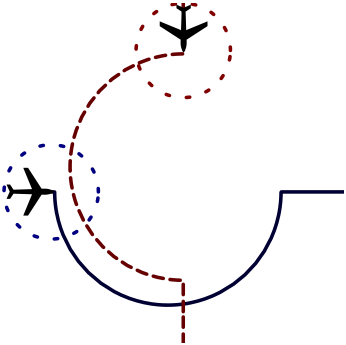
Corollary (Compositionality)

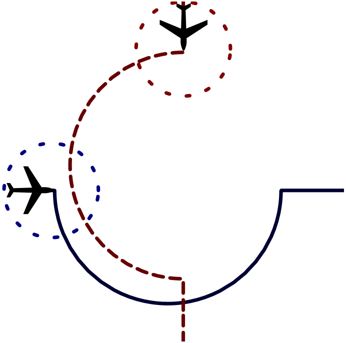
hybrid systems can be verified by recursive decomposition

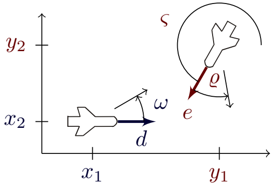
André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

Hybrid Systems Analysis: Air Traffic Control

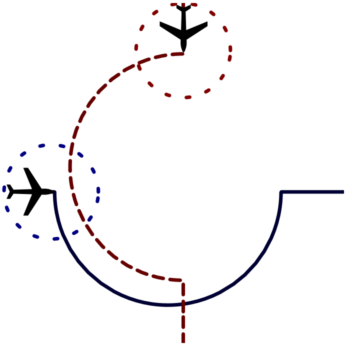


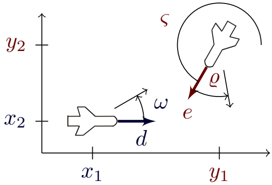






$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varrho - \omega \end{bmatrix}$$



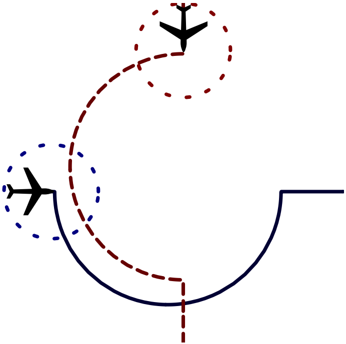


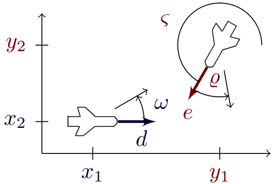
$$\begin{bmatrix} x_1' = -v_1 + v_2 \cos\vartheta + \omega x_2 \\ x_2' = v_2 \sin\vartheta - \omega x_1 \\ \vartheta' = \varrho - \omega \end{bmatrix}$$

Example ("Solving" differential equations)

$$x_1(t) = \frac{1}{\omega\varrho}\Big(x_1\omega\varrho\cos t\omega - v_2\omega\cos t\omega\sin\vartheta + v_2\omega\cos t\omega\cos t\varrho\sin\vartheta - v_1\varrho\sin t\omega$$
$$+ x_2\omega\varrho\sin t\omega - v_2\omega\cos\vartheta\cos t\varrho\sin t\omega - v_2\omega\sqrt{1-\sin\vartheta^2}\sin t\omega$$
$$+ v_2\omega\cos\vartheta\cos t\omega\sin t\varrho + v_2\omega\sin\vartheta\sin t\omega\sin t\varrho\Big)\ldots$$

Hybrid Systems Analysis: Air Traffic Control





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

Example ("Solving" differential equations)

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

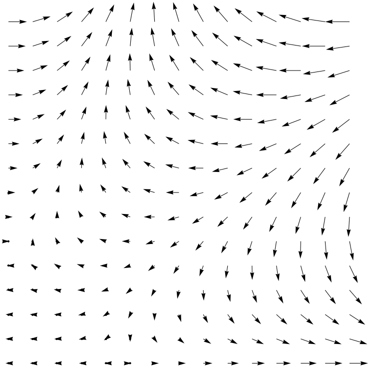
$$+ x_2\omega\varrho\sin t\omega - v_2\omega\cos\vartheta\cos t\varrho\sin t\omega - v_2\omega\sqrt{1 - \sin\vartheta^2}\sin t\omega$$

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

Idea: Exploit Vector Field of Differential Equations

"Definition" (Differential Invariant)

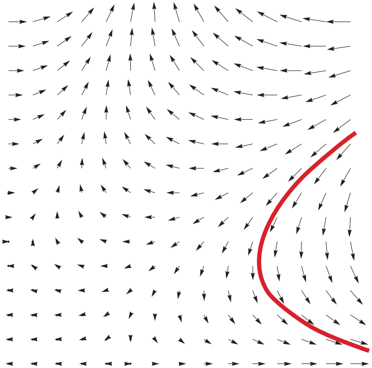
"Logical formula that remains true in the direction of the dynamics"



Idea: Exploit Vector Field of Differential Equations

"Definition" (Differential Invariant)

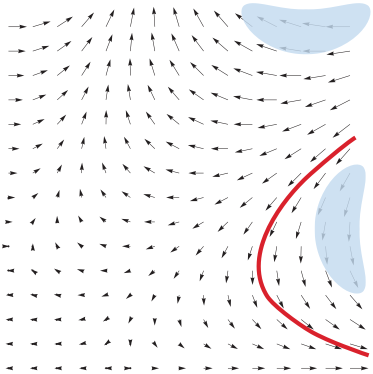
"Logical formula that remains true in the direction of the dynamics"



Idea: Exploit Vector Field of Differential Equations

"Definition" (Differential Invariant)

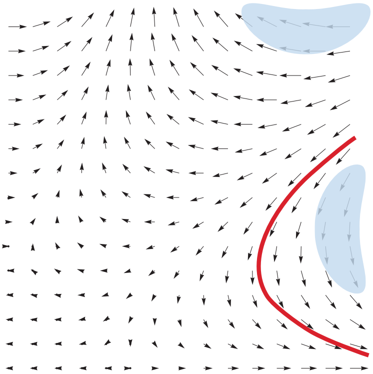
"Logical formula that remains true in the direction of the dynamics"

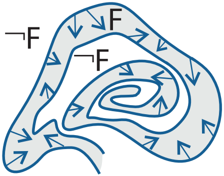


Idea: Exploit Vector Field of Differential Equations

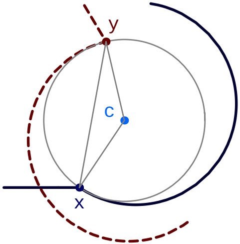
"Definition" (Differential Invariant)

"Logical formula that remains true in the direction of the dynamics"



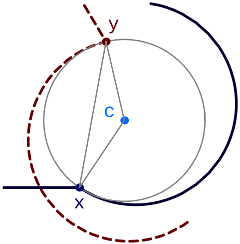


$$\overline{\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



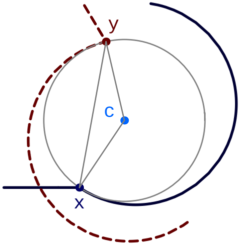
Differential Induction for Aircraft Roundabouts

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



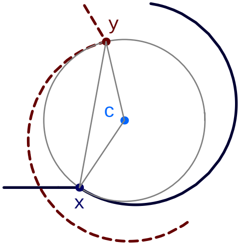
Differential Induction for Aircraft Roundabouts

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



Differential Induction for Aircraft Roundabouts

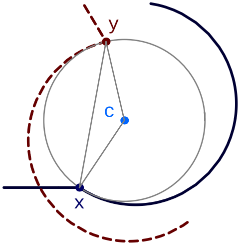
$$\frac{\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1} d_1 \ldots}{\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2'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

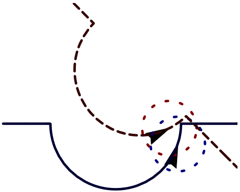


$$\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0$$

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

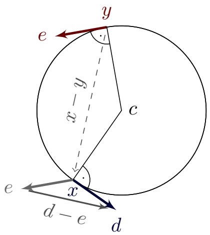
$$\vdash [x_1' = d_1, d_1' = -\omega d_2, x_2' = d_2, d_2' = \omega d_1, ..](x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

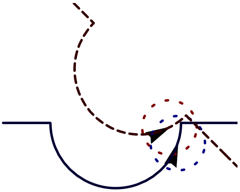




Differential Induction for Aircraft Roundabouts

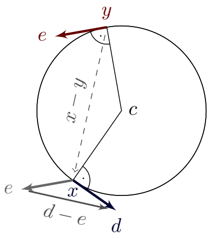
$$\dfrac{\dfrac{\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}{\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2} d_2 + \frac{\partial\|x-y\|^2}{\partial y_2} e_2 \geq \frac{\partial p^2}{\partial x_1}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

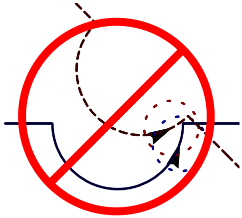




Differential Induction for Aircraft Roundabouts

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

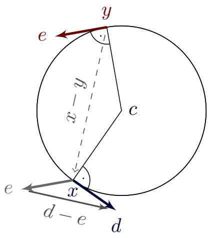




$$\dfrac{}{.. \vdash [d_1' = -\omega d_2, e_1' = -\omega e_2, x_2' = d_2, d_2' = \omega d_1, ..] d_1 - e_1 = -\omega(x_2 - y_2)}$$

Differential Induction for Aircraft Roundabouts

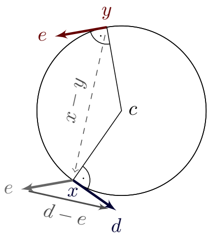
$$\frac{\frac{\frac{\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0}{\vdash 2(x_1 - y_1)(d_1 - e_1) + 2(x_2 - y_2)(d_2 - e_2) \geq 0}}{\vdash \frac{\partial\|x-y\|^2}{\partial x_1} d_1 + \frac{\partial\|x-y\|^2}{\partial y_1} e_1 + \frac{\partial\|x-y\|^2}{\partial x_2}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



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

Differential Induction for Aircraft Roundabouts

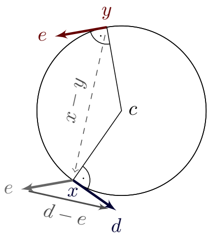
$$\dfrac{\dfrac{\dfrac{\vdash 2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{\vdash 2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\vdash \frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial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



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

Differential Induction for Aircraft Roundabouts

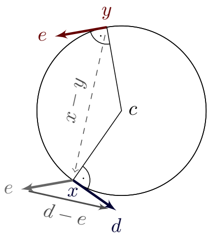
$$\dfrac{\dfrac{\dfrac{\vdash 2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{\vdash 2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\vdash \frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial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



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

Differential Induction for Aircraft Roundabouts

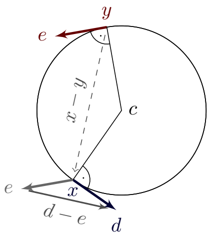
$$\dfrac{\dfrac{\dfrac{\dfrac{\vdash 2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{\vdash 2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\vdash \frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial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



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

Differential Induction for Aircraft Roundabouts

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



$$
\begin{array}{l}
\quad\vdash -\omega d_2+\omega e_2=-\omega(d_2-e_2)\\
\hline
\quad\vdash \frac{\partial(d_1-e_1)}{\partial d_1}(-\omega d_2)+\frac{\partial(d_1-e_1)}{\partial e_1}(-\omega e_2)=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}d_2-\frac{\partial\omega(x_2-y_2)}{\partial y_2}e_2\\
\hline
..\vdash [d_1'=-\omega d_2,e_1'=-\omega e_2,x_2'=d_2,d_2'=\omega d_1,..]d_1-e_1=-\omega(x_2-y_2)
\end{array}
$$

Differential Induction & Differential Cuts

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

Proposition (Differential cut saturation)

F differential invariant of $[x'=\theta\wedge H]\phi$, then

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

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

Differential Induction & Differential Cuts

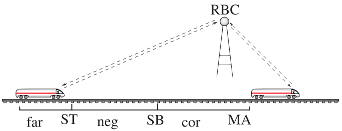
$$\dfrac{\dfrac{\dfrac{\vdash 2(x_1-y_1)(-\omega(x_2-y_2))+2(x_2-y_2)\omega(x_1-y_1)\geq 0}{\vdash 2(x_1-y_1)(d_1-e_1)+2(x_2-y_2)(d_2-e_2)\geq 0}}{\vdash \frac{\partial\|x-y\|^2}{\partial x_1}d_1+\frac{\partial\|x-y\|^2}{\partial y_1}e_1+\frac{\partial\|x-y\|^2}{\partial x_2}d_2+\frac{\partial\|x-y\|^2}{\partial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

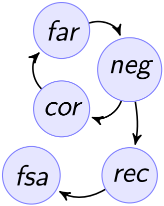
refine dynamics

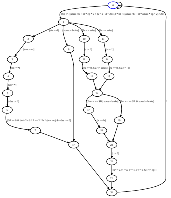
by differential cut

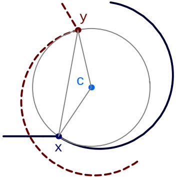
$$\dfrac{\dfrac{\vdash -\omega d_2+\omega e_2=-\omega(d_2-e_2)}{\vdash \frac{\partial(d_1-e_1)}{\partial d_1}(-\omega d_2)+\frac{\partial(d_1-e_1)}{\partial e_1}(-\omega e_2)=-\frac{\partial\omega(x_2-y_2)}{\partial x_2}d_2-\frac{\partial\omega(x_2-y_2)}{\partial y_2}e_2}}{..\vdash [d_1'=-\omega d_2,e_1'=-\omega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

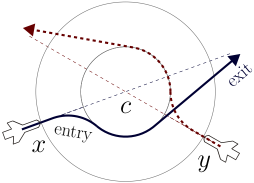
Successful Hybrid Systems Analysis

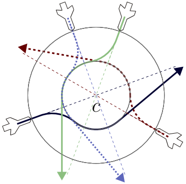


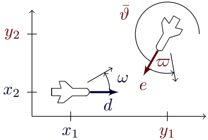


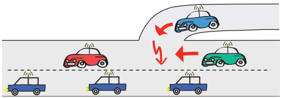


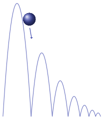


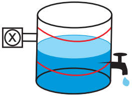


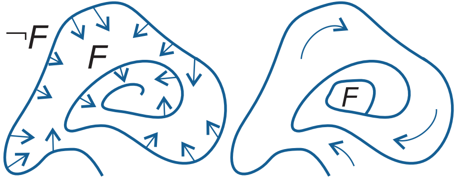


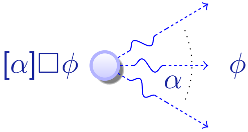


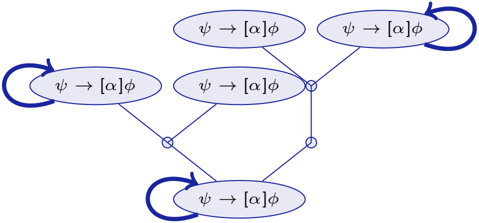


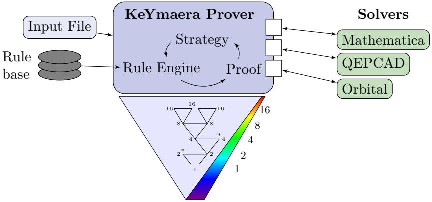


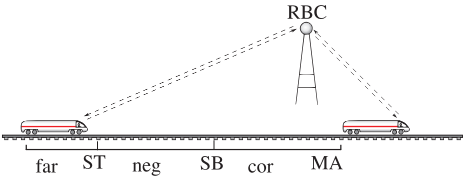


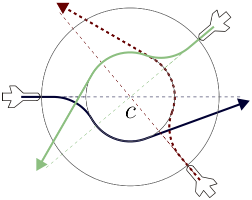

¬F
F
F


$[\alpha]\Box\phi$
α
ϕ


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


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

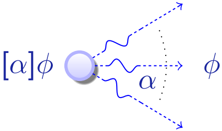

RBC
far
ST
neg
SB
cor
MA


c

Theorem Proving for Dynamic Systems

differential dynamic logic

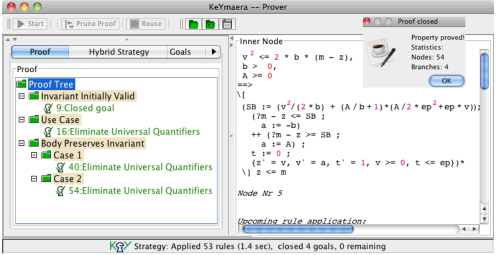
$\mathrm{d}\mathcal{L} = \mathrm{DL} + \mathrm{HP}$



Verifying hybrid systems:

- Logic for hybrid systems++
- Compositional calculi
- Algorithms
- Challenging applications

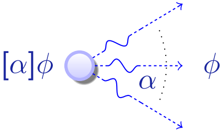
KeYmaera



Theorem Proving for Dynamic Systems

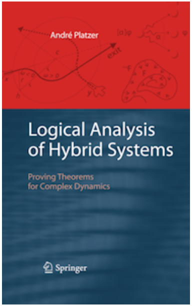
differential dynamic logic

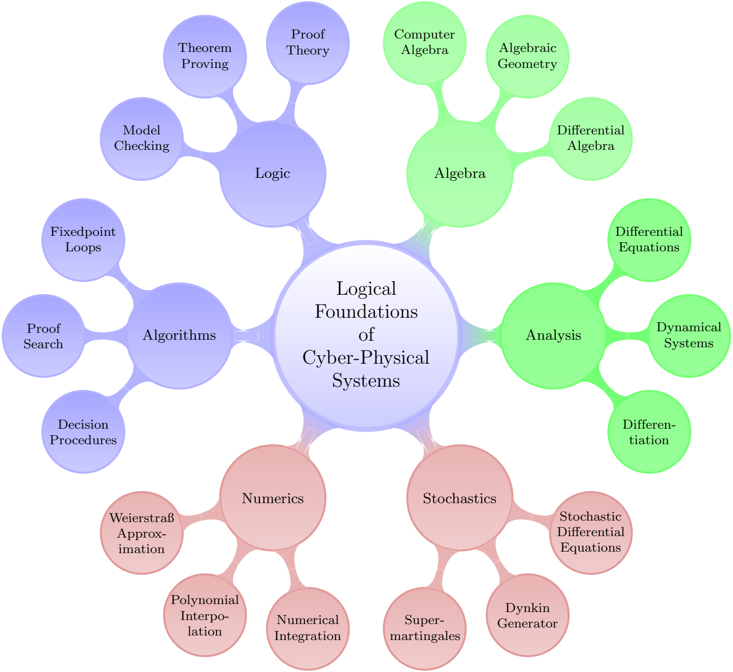
$$d\mathcal{L} = \mathrm{DL} + \mathrm{HP}$$

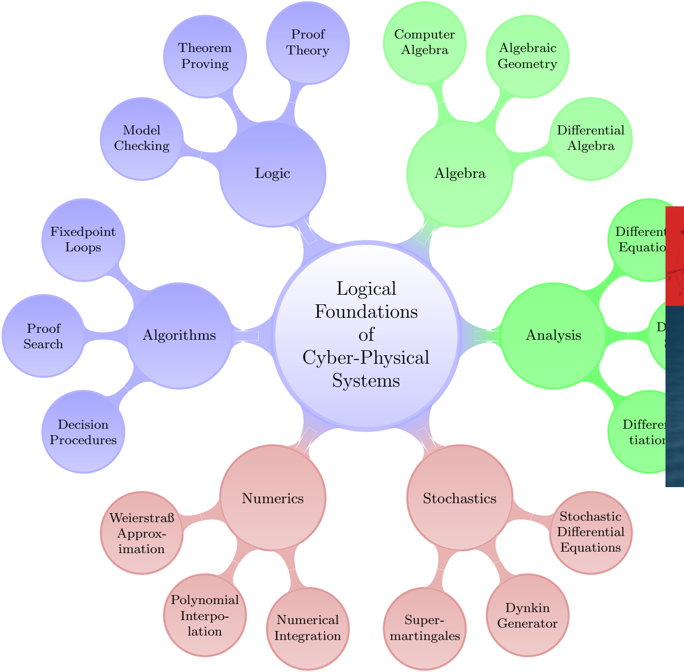


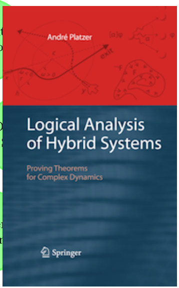
Verifying hybrid systems:

- Logic for hybrid systems++
- Compositional calculi
- Algorithms
- Challenging applications




Logical Foundations of Cyber-Physical Systems
Logic
Model Checking
Theorem Proving
Proof Theory
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Algorithms
Fixedpoint Loops
Proof Search
Decision Procedures
Analysis
Differential Equations
Dynamical Systems
Differen- tiation
Numerics
Weierstraß Approx- imation
Polynomial Interpo- lation
Numerical Integration
Stochastics
Super- martingales
Dynkin Generator
Stochastic Differential Equations


Logical Foundations of Cyber-Physical Systems
Logic
Theorem Proving
Proof Theory
Model Checking
Algebra
Computer Algebra
Algebraic Geometry
Differential Algebra
Algorithms
Fixedpoint Loops
Proof Search
Decision Procedures
Analysis
Numerics
Weierstraß Approximation
Polynomial Interpolation
Numerical Integration
Stochastics
Stochastic Differential Equations
Super-martingales
Dynkin Generator


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

André Platzer.
Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.
Springer, 2010.

André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput., 35(1): 309–352, 2010.

André Platzer and Edmund M. Clarke.
Computing differential invariants of hybrid systems as fixedpoints.
Form. Methods Syst. Des., 35(1):98–120, 2009. Special CAV'08 issue.

André Platzer and Jan-David Quesel.
KeYmaera: A hybrid theorem prover for hybrid systems.
In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *IJCAR*, volume 5195 of *LNCS*, pages 171–178. Springer, 2008.