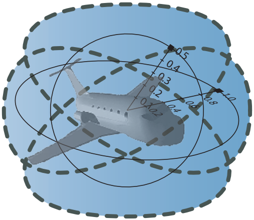
The Complete Proof Theory of Hybrid Systems

André Platzer

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

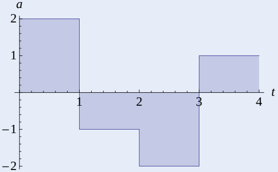


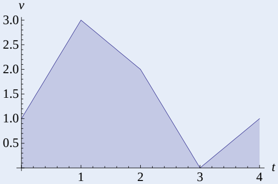
Hybrid Systems: e.g., Car Control

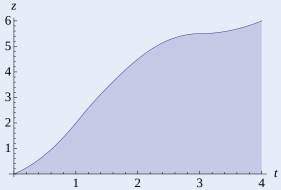
Challenge (Hybrid Systems)

Fixed rule describing state evolution

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







Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution

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

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

Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution

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

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

Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution

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

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

Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution

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

Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution

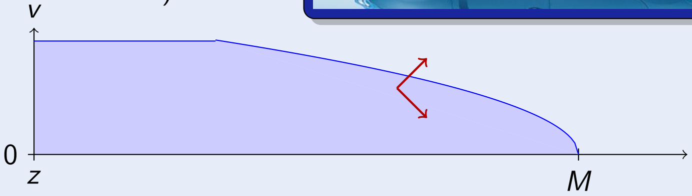
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution

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

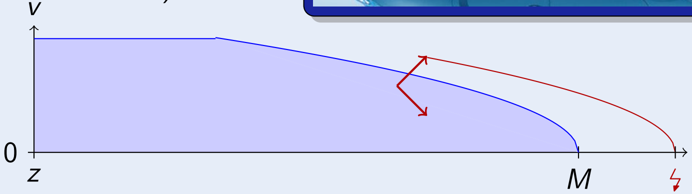


Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution

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

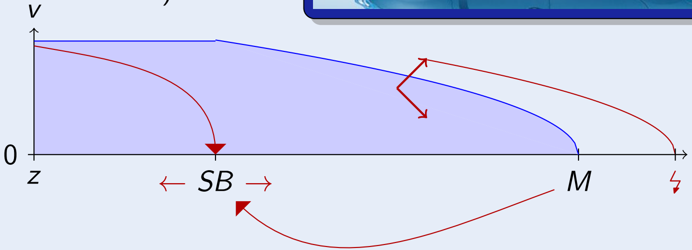


Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

Fixed rule describing state evolution

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



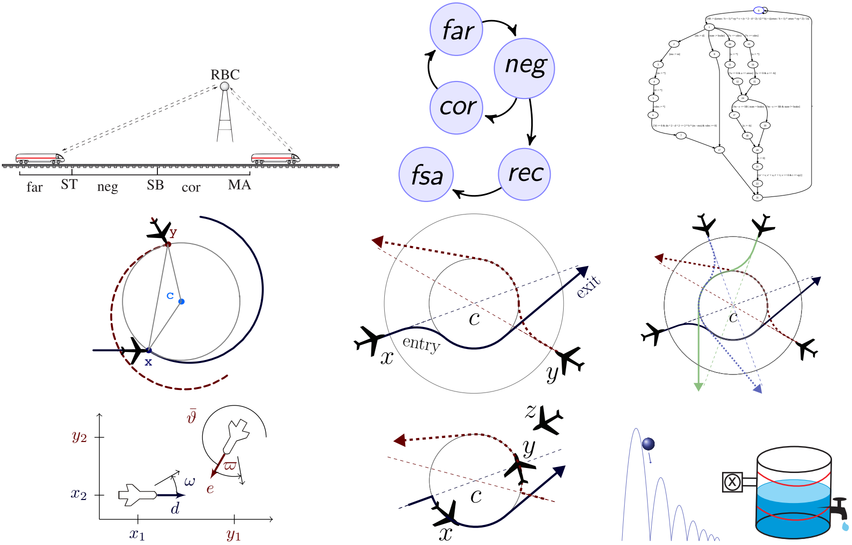
Hybrid Systems: e.g., Car Control

Challenge (Hybrid Systems)

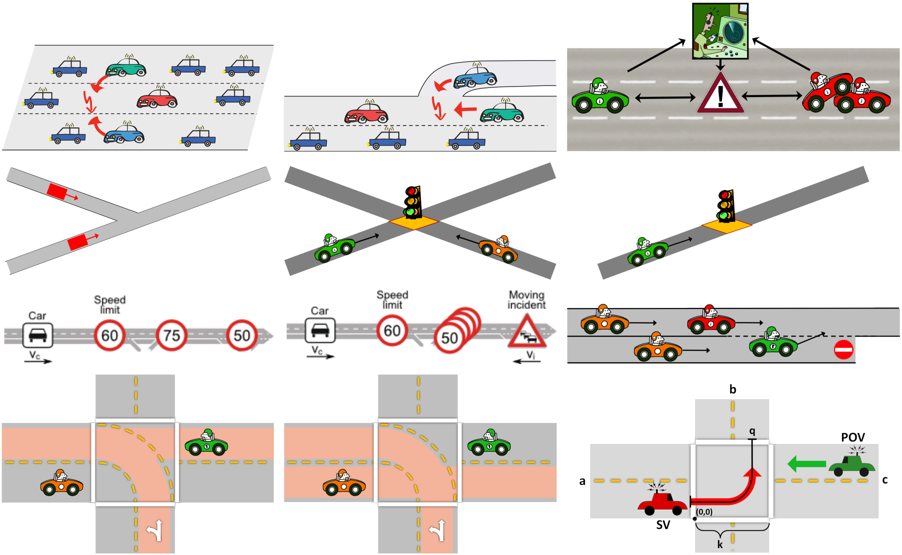
Fixed rule describing state evolution

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

Successful Hybrid Systems Proofs



Successful Hybrid Systems Proofs



hybrid = continuous = discrete

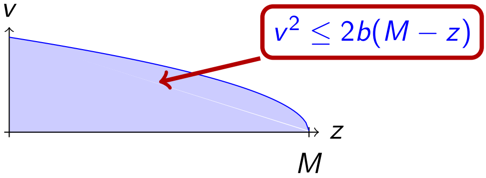
Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

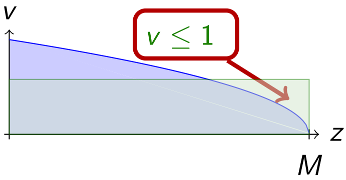
differential dynamic logic

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



differential dynamic logic

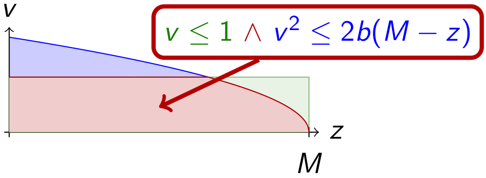
$\mathrm{d}\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$



Differential Dynamic Logic for Hybrid Systems

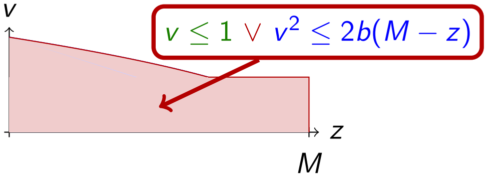
differential dynamic logic

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



differential dynamic logic

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



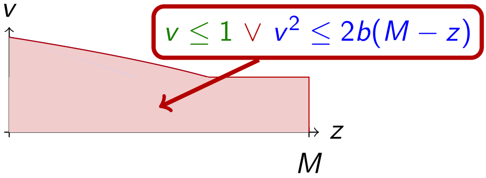
Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

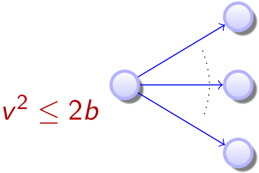
$\forall M A\, \exists S B \ \ldots$

$\forall t{\geq}0 \ \ldots$



differential dynamic logic

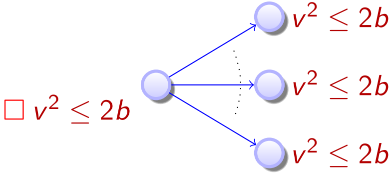
$d\mathcal{L} = \text{FOL}_{\mathbb{R}} +$



Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

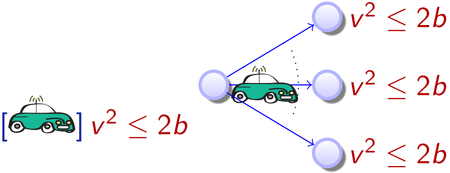
$d\mathcal{L} = \text{FOL}_{\mathbb{R}} + \text{ML}$



Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

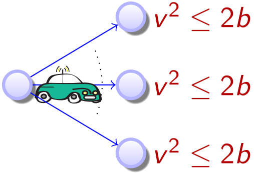


Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

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

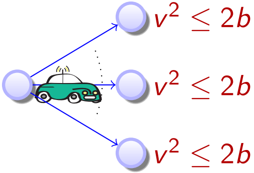


Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

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

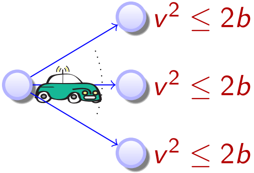


Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

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

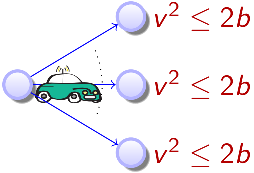


Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

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

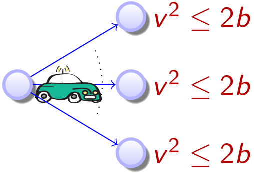


Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

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



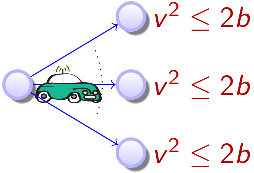
Initial condition

Differential Dynamic Logic for Hybrid Systems

differential dynamic logic

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

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



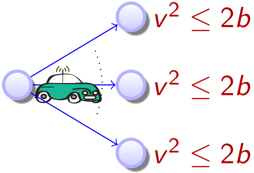
Initial condition

System dynamics

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

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

Definition (Hybrid program α)

$$
\begin{aligned}
\rho(x := \theta) &= \{(v,w) \;:\; w = v \text{ except } [\![x]\!]_w = [\![\theta]\!]_v\} \\
\rho(?H) &= \{(v,v) \;:\; v \models H\} \\
\rho(x' = f(x)) &= \{(\varphi(0),\varphi(r)) \;:\; \varphi \models x' = f(x) \text{ for some duration } r\} \\
\rho(\alpha \cup \beta) &= \rho(\alpha) \cup \rho(\beta) \\
\rho(\alpha;\beta) &= \rho(\beta) \circ \rho(\alpha) \\
\rho(\alpha^*) &= \bigcup_{n\in\mathbb{N}} \rho(\alpha^n)
\end{aligned}
$$

Definition (d$\mathcal{L}$ Formula ϕ)

$$
\begin{aligned}
& v \models \theta_1 \geq \theta_2 && \text{iff} \quad [\![\theta_1]\!]_v \geq [\![\theta_2]\!]_v \\
& v \models [\alpha]\phi && \text{iff} \quad w \models \phi \text{ for all } w \text{ with } (v,w) \in \rho(\alpha) \\
& v \models \langle\alpha\rangle\phi && \text{iff} \quad w \models \phi \text{ for some } w \text{ with } (v,w) \in \rho(\alpha) \\
& v \models \forall x\, \phi && \text{iff} \quad w \models \phi \text{ for all } w \text{ that agree with } v \text{ except for } x \\
& v \models \exists x\, \phi && \text{iff} \quad w \models \phi \text{ for some } w \text{ that agrees with } v \text{ except for } x
\end{aligned}
$$

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

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

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

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

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

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

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

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

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

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

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

G $\dfrac{\phi}{[\alpha]\phi}$

MP $\dfrac{\phi \to \psi \quad \phi}{\psi}$

$\forall$ $\dfrac{\phi}{\forall x\, \phi}$

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

G $\quad \dfrac{\phi}{[\alpha]\phi}$

MP $\quad \dfrac{\phi \to \psi \quad \phi}{\psi}$

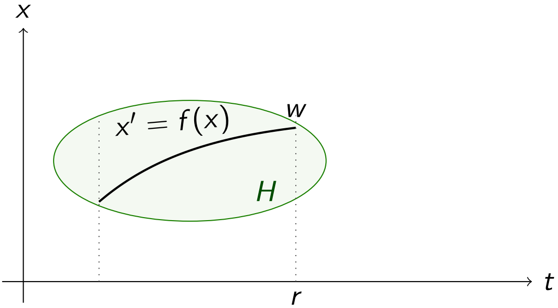
∀ $\quad \dfrac{\phi}{\forall x\, \phi}$

B $\quad \forall x\, [\alpha]\phi \to [\alpha]\forall x\, \phi \qquad (x \notin \alpha)$

V $\quad \phi \to [\alpha]\phi \qquad (FV(\phi) \cap BV(\alpha) = \emptyset)$

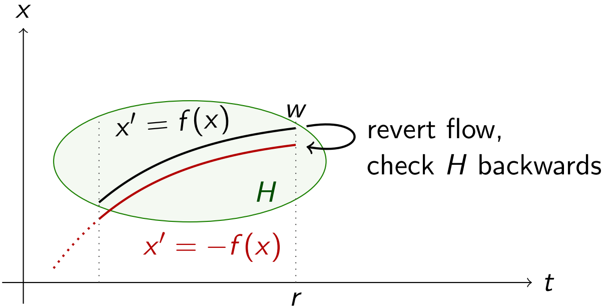
Differential Dynamic Logic d$\mathcal{L}$: Axiomatization

[&] $[x' = f(x) \,\&\, H]\phi \leftrightarrow [x' = f(x)](\phi)$

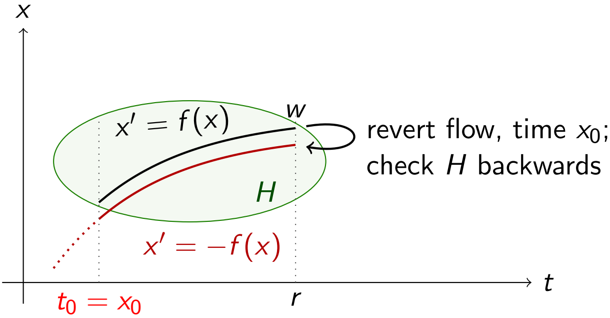


Differential Dynamic Logic d$\mathcal{L}$: Axiomatization

[&] $[x' = f(x) \,\&\, H]\phi$
$\leftrightarrow \quad [x' = f(x)]\big([x' = -f(x)](H) \to \phi\big)$

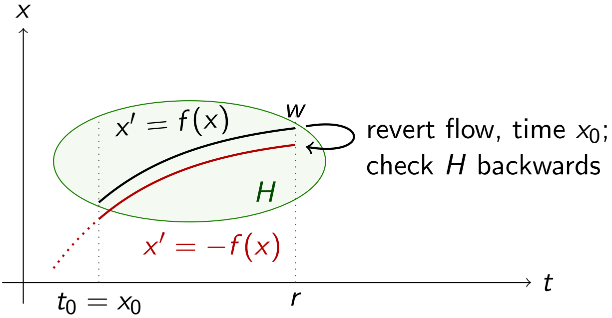


[&] $[x' = f(x)\,\&\,H]\phi$
$\leftrightarrow \forall t_0{=}x_0 [x' = f(x)]\big([x' = -f(x)](x_0 \geq t_0 \rightarrow H) \rightarrow \phi\big)$



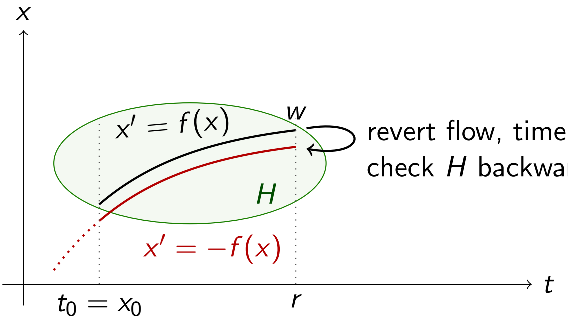
“There and Back Again” Axiom of d$\mathcal{L}$

$$[\&] \quad [x' = f(x) \,\&\, H]\phi \leftrightarrow \forall t_0{=}x_0 [x' = f(x)]\big([x' = -f(x)](x_0 \geq t_0 \rightarrow H) \rightarrow \phi\big)$$



“There and Back Again” Axiom of d$\mathcal{L}$

$$[\&] \quad [x' = f(x) \,\&\, H]\phi \leftrightarrow \forall t_0{=}x_0 [x' = f(x)]\big([x' = -f(x)](x_0 \geq t_0 \rightarrow H) \rightarrow \phi\big)$$



revert flow, time x_0;
check H backwards

Lemma

Evolution domain axiomatizable

Soundness

Theorem (Soundness)

dℒ *calculus is sound, i.e., all provable* dℒ *formulas are valid:*

$$\vdash \phi \text{ implies } \vDash \phi$$

What about the converse?

Continuous Completeness

Theorem (Relative Completeness / Continuous)

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

Proof Outline 6p

$$\vDash \phi \textit{ implies } Taut_{FOD} \vdash \phi$$

Continuous Completeness

Theorem (Relative Completeness / Continuous)

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

▸ Proof Outline 6p

$$\vDash \phi \text{ implies } Taut_{FOD} \vdash \phi$$

Corollary (Proof-theoretical Alignment)

proving hybrid systems = proving continuous dynamical systems!

Corollary (Compositionality)

hybrid systems can be verified by recursive decomposition

Discrete Completeness

Theorem (Relative Completeness / Continuous)

dℒ *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations.*

Proof Outline 6p

$$\vDash \phi \text{ implies } Taut_{FOD} \vdash \phi$$

Theorem (Relative Completeness / Discrete)

dℒ *calculus is a sound & complete axiomatization of hybrid systems relative to discrete dynamics.*

Proof Outline +5p

$$\vDash \phi \text{ implies } Taut_{DL} \vdash \phi$$

Discrete Completeness

Theorem (Relative Completeness / Continuous)

d$\mathcal{L}$ *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations.* ▸ Proof Outline 6p

$$\vDash \phi \text{ implies } Taut_{FOD} \vdash \phi$$

Theorem (Relative Completeness / Discrete)

d$\mathcal{L}$ *calculus is a sound & complete axiomatization of hybrid systems relative to discrete dynamics.* ▸ Proof Outline +5p

$$\vDash \phi \text{ implies } Taut_{DL} \vdash \phi$$

Corollary (Complete Proof-theoretical Alignment)

hybrid = continuous = discrete

Discrete Completeness

Theorem (Relative Completeness / Continuous)

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

Proof Outline 6p

$$\vDash \phi \text{ implies } Taut_{FOD} \vdash \phi$$

Theorem (Relative Completeness / Discrete)

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

Proof Outline +5p

$$\vDash \phi \text{ implies } Taut_{DL} \vdash \phi$$

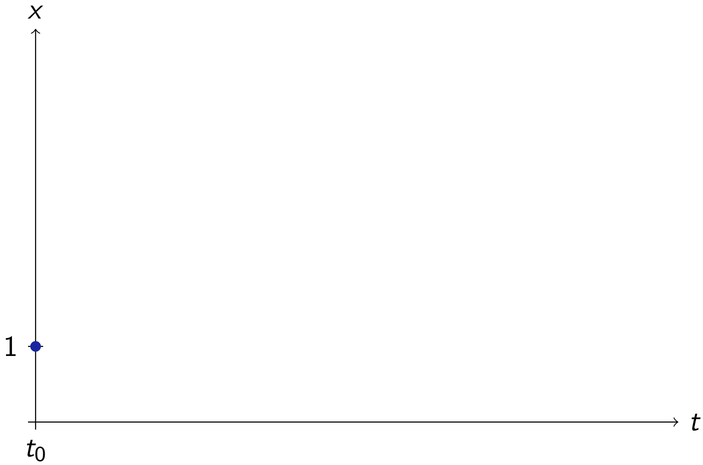
Corollary (Complete Proof-theoretical Alignment)

hybrid = continuous = discrete

Corollary (Interdisciplinary Integrability)

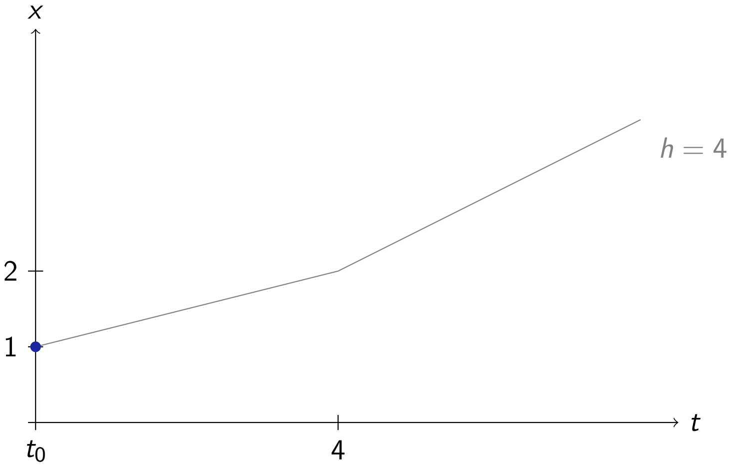
"Discrete computer science + continuous control are integrable"

$$[x' = \frac{x}{4}]F$$



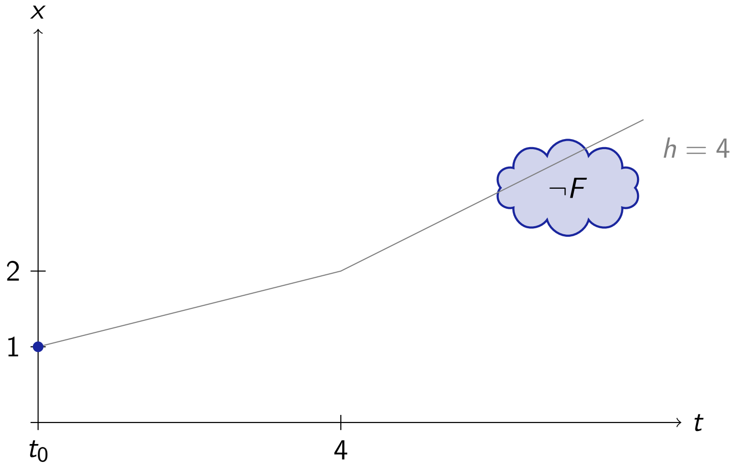
Continuous Dynamics vs. Discrete Dynamics

$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



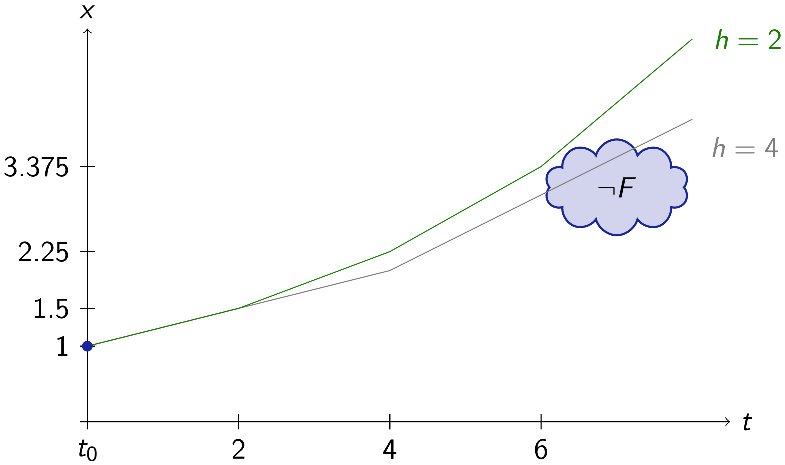
Continuous Dynamics vs. Discrete Dynamics

$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



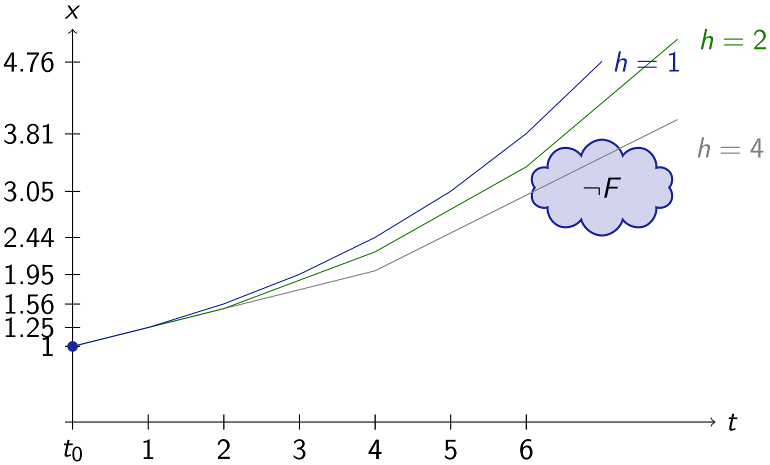
Continuous Dynamics vs. Discrete Dynamics

$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



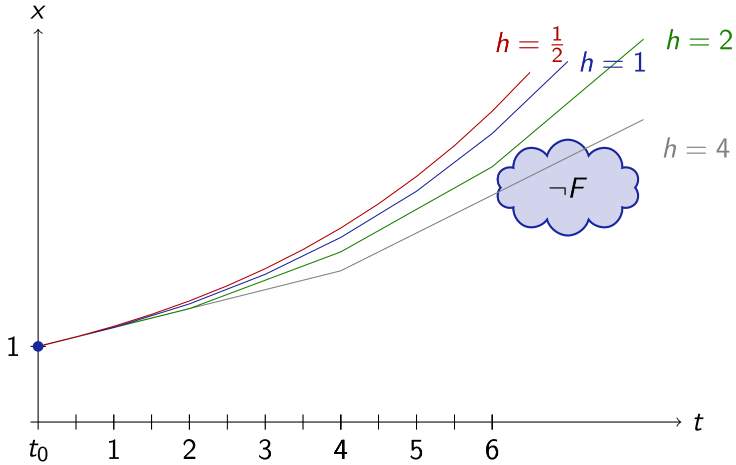
Continuous Dynamics vs. Discrete Dynamics

$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



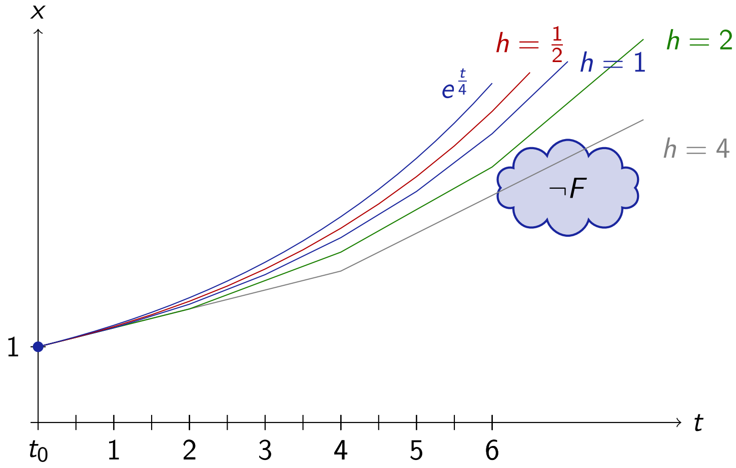
Continuous Dynamics vs. Discrete Dynamics

$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



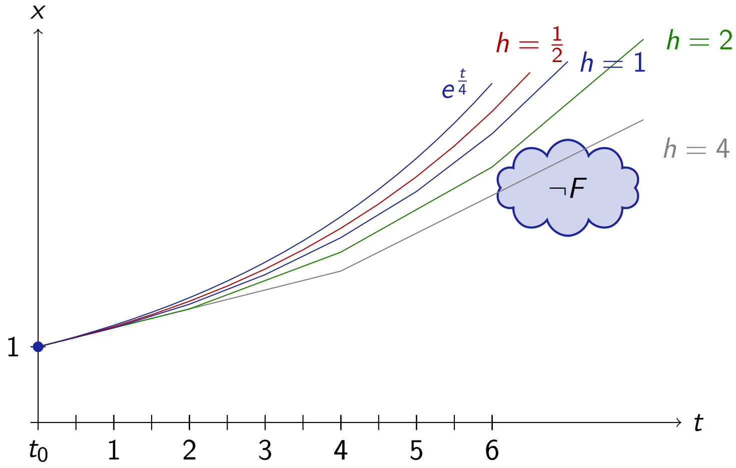
Continuous Dynamics vs. Discrete Dynamics

$$[x' = \frac{x}{4}]F \quad \text{vs.} \quad [(x := x + h\frac{x}{4})^*]F$$



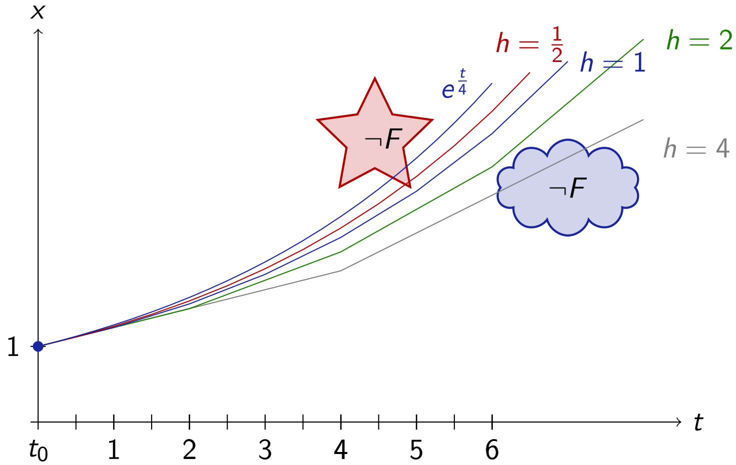
Continuous Dynamics vs. Discrete Dynamics

$$[x' = \frac{x}{4}]F \quad \not\Rightarrow \quad [(x := x + h\frac{x}{4})^*]F$$



Continuous Dynamics vs. Discrete Dynamics

$$[x' = \frac{x}{4}]F \quad \not\leftarrow \quad [(x := x + h\frac{x}{4})^*]F$$



Discrete Euler Approximation Axiom $\overleftarrow{\Delta}$

$$\overleftarrow{\Delta} \quad [x' = f(x)]F \leftarrow \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*]F$$

Discrete Euler Approximation Axiom $\overleftarrow{\Delta}$

$$\overleftarrow{\Delta} \quad [x' = f(x)]F \leftarrow \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*]F$$

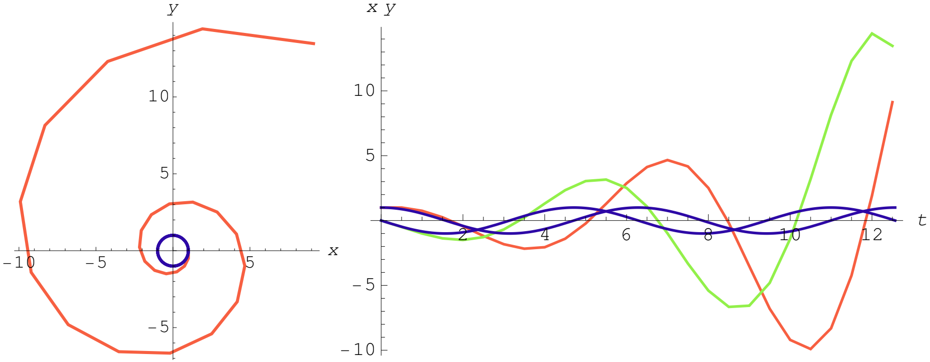
Example ()

$$\vDash x^2 + y^2 \leq 1.1 \rightarrow [x' = y, y' = -x]x^2 + y^2 \leq 1.1$$

$\overleftarrow{\Delta}$ $\quad [x' = f(x)]F$
$\leftarrow \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*]F$

Example (Insufficient, not global)

$$\vDash x^2 + y^2 \leq 1.1 \rightarrow [x' = y, y' = -x]x^2 + y^2 \leq 1.1$$

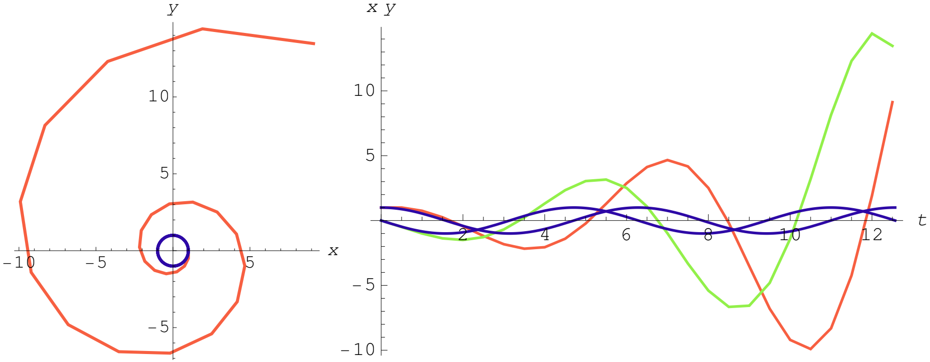


$$\overleftarrow{\Delta} \quad [x' = f(x)]F \leftarrow \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*]F$$

(closed)

Example (Unsound for open F, only in closure)

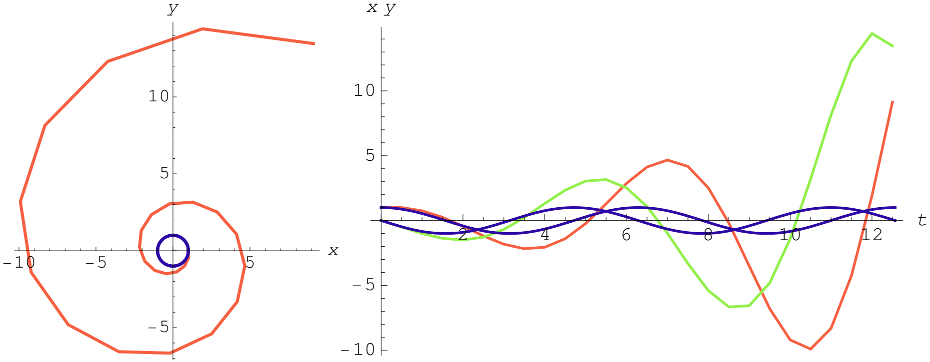
$$\nvDash x = 1 \land y = 0 \to [x' = y, y' = -x](x \leq 0 \to x^2 + y^2 > 1)$$



$$\overleftarrow{\Delta} \quad [x' = f(x)]F \leftarrow \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*]F \qquad \text{(closed)}$$

Example (Insufficient, not global)

$$\vDash x^2 + y^2 \leq 1.1 \rightarrow [x' = y, y' = -x]x^2 + y^2 \leq 1.1$$



Discrete Euler Approximation Axiom $\overrightarrow{\Delta}$ $t' = -1$

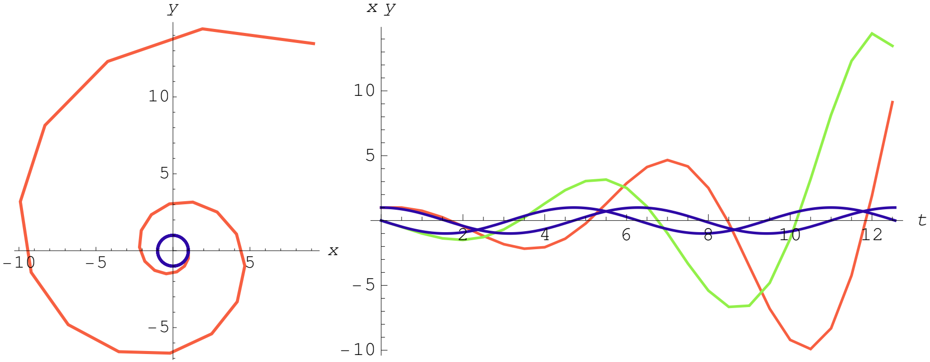
$$\overrightarrow{\Delta} \quad [x' = f(x)]F \\ \rightarrow \forall t{\geq}0\, \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*](t \geq 0 \rightarrow F)$$

Discrete Euler Approximation Axiom $\overrightarrow{\Delta}$

$$\overrightarrow{\Delta} \quad [x' = f(x)]F \rightarrow \forall t{\geq}0\, \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*](t \geq 0 \rightarrow F)$$

Example (Converse unsound for open F)

$$\not\models x = 1 \land y = 0 \rightarrow [x' = y, y' = -x](x \leq 0 \rightarrow x^2 + y^2 > 1)$$

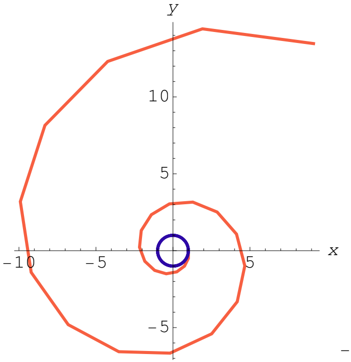


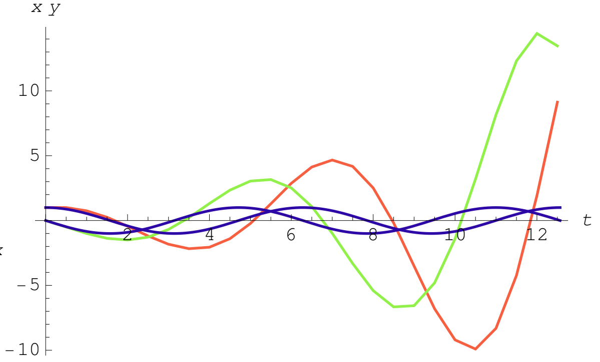
Discrete Euler Approximation Axiom $\overrightarrow{\Delta}$

$\overrightarrow{\Delta}$ $$[x' = f(x)]F \rightarrow \forall t{\geq}0\, \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*](t \geq 0 \rightarrow F)$$ (open)

Example (Unsound for closed F, only holds in the limit)

$$\vDash x^2 + y^2 = 1 \rightarrow [x' = y, y' = -x]x^2 + y^2 = 1$$





Discrete Euler Approximation Axiom $\overleftrightarrow{\Delta}$ $t' = -1$

$$[x' = f(x)]F$$
$$\leftrightarrow \forall t{\geq}0 \exists \varepsilon_0{>}0 \forall 0{<}\varepsilon{<}\varepsilon_0 \exists h_0{>}0 \forall 0{<}h{<}h_0 [(x := x{+}hf(x))^*]\big(t{\geq}0 \to \neg\mathcal{U}_\varepsilon(\neg F)\big)$$

$[x' = f(x)]F$
$\leftrightarrow \forall t{\geq}0 \exists \varepsilon_0{>}0 \forall 0{<}\varepsilon{<}\varepsilon_0 \exists h_0{>}0 \forall 0{<}h{<}h_0 [(x := x{+}hf(x))^*]\big(t{\geq}0 \to \neg\mathcal{U}_\varepsilon(\neg F)\big)$

Example ()

$$\vDash x^2 + y^2 < 1.1 \to [x' = y, y' = -x]x^2 + y^2 < 1.1$$

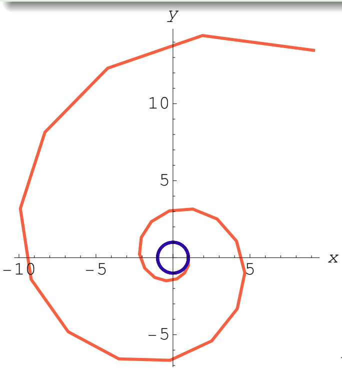
$\mathcal{R}$ Discrete Euler Approximation Axiom $\overleftrightarrow{\Delta}$ $\quad t' = -1$

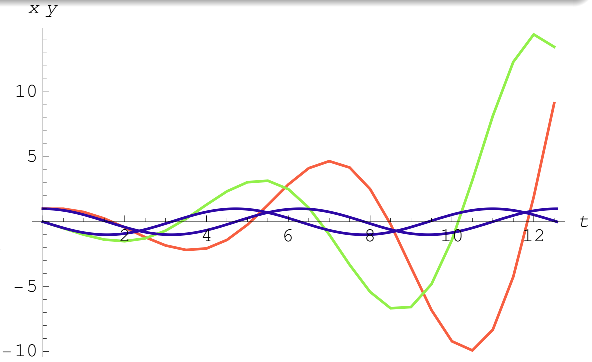
$[x' = f(x)]F$

$\leftrightarrow \forall t{\geq}0\,\exists\varepsilon_0{>}0\,\forall 0{<}\varepsilon{<}\varepsilon_0\,\exists h_0{>}0\,\forall 0{<}h{<}h_0\,[(x := x{+}hf(x))^*]\big(t{\geq}0 \to \neg\mathcal{U}_\varepsilon(\neg F)\big)$

Example (Insufficient for closed F)

$$\vDash x^2 + y^2 \leq 1 \to [x' = y, y' = -x]x^2 + y^2 \leq 1$$



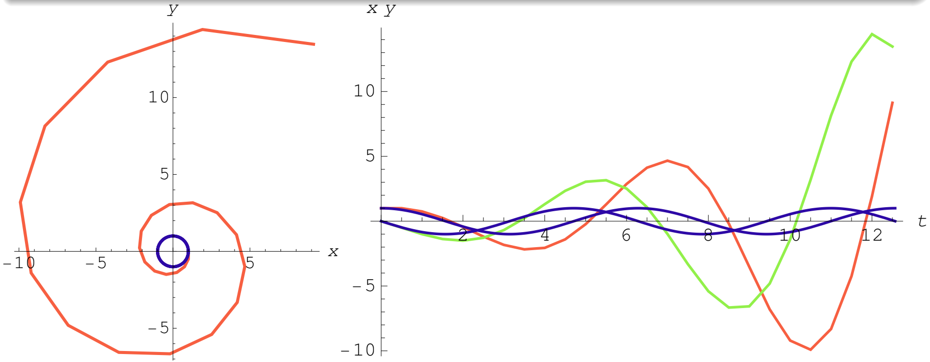


$[x' = f(x)]F$ *(open)*

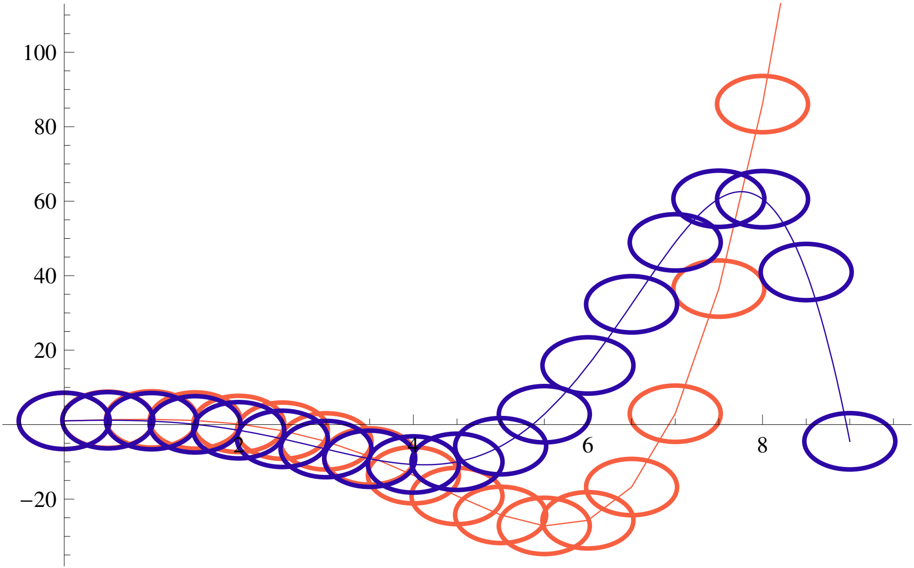
$\leftrightarrow \forall t{\geq}0 \exists \varepsilon_0{>}0 \forall 0{<}\varepsilon{<}\varepsilon_0 \exists h_0{>}0 \forall 0{<}h{<}h_0 [(x := x{+}hf(x))^*] \big(t{\geq}0 \rightarrow \neg \mathcal{U}_\varepsilon(\neg F)\big)$

Example (Insufficient for closed F)

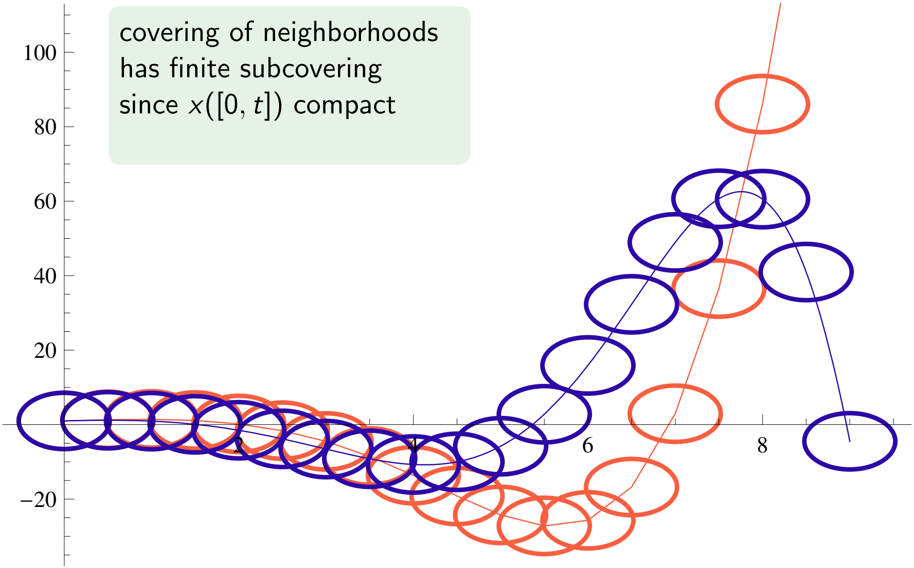
$$\vDash x^2 + y^2 \leq 1 \rightarrow [x' = y, y' = -x] x^2 + y^2 \leq 1$$



Partial Covering for Solution and Approximation



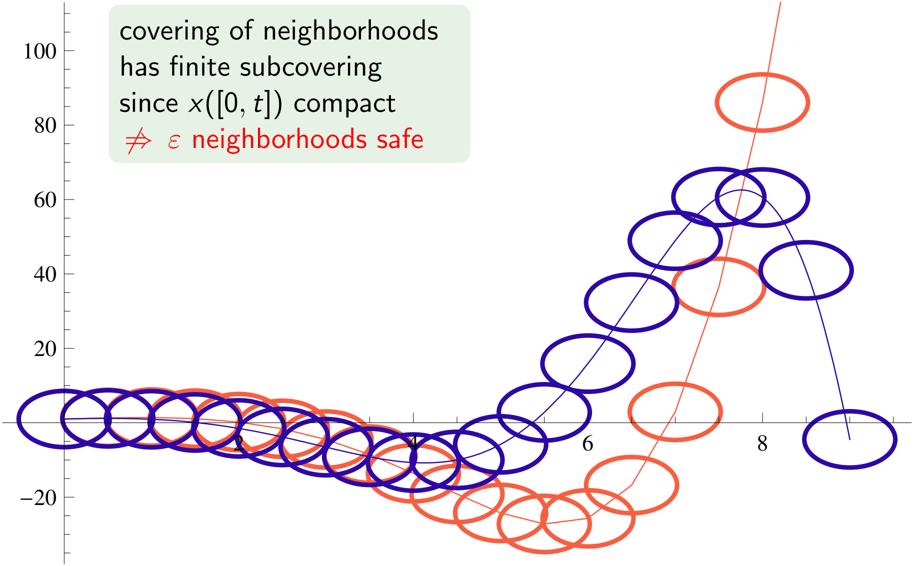
Partial Covering for Solution and Approximation



covering of neighborhoods has finite subcovering since $x([0,t])$ compact

Partial Covering for Solution and Approximation

covering of neighborhoods
has finite subcovering
since $x([0,t])$ compact
$\not\Rightarrow$ ε neighborhoods safe

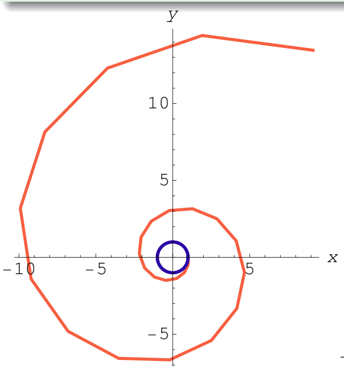


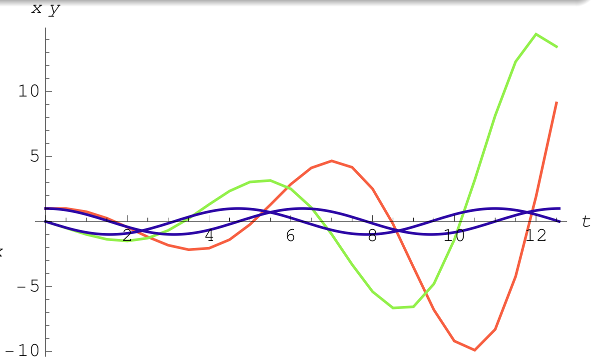
$$[x' = f(x)]F \qquad (open)$$

$$\leftrightarrow \forall t{\geq}0 \exists \varepsilon_0{>}0 \forall 0{<}\varepsilon{<}\varepsilon_0 \exists h_0{>}0 \forall 0{<}h{<}h_0 [(x := x{+}hf(x))^*] \big(t{\geq}0 \to \neg\mathcal{U}_\varepsilon(\neg F)\big)$$

Example (Insufficient for closed F)

$$\vDash x^2 + y^2 \leq 1 \to [x' = y, y' = -x] x^2 + y^2 \leq 1$$





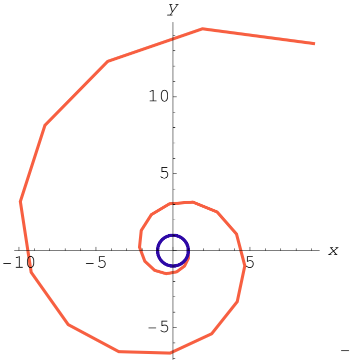
Closed Discrete Completeness (derivable)

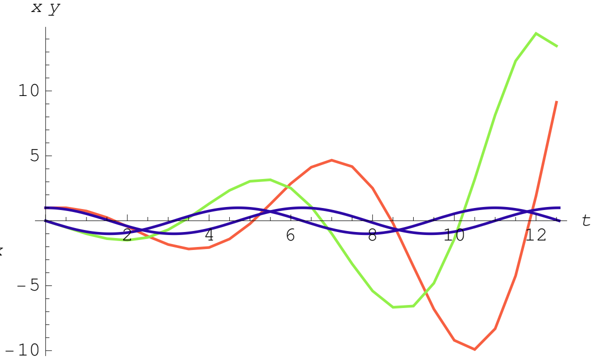
$\mathring{U}$ $[x' = f(x)]F \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)]\mathcal{U}_{\check{\varepsilon}}(F)$ $(\Leftarrow \text{B,V,G,K})$

$\mathring{U}$ $[x' = f(x)]F \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)]\mathcal{U}_{\check{\varepsilon}}(F)$ $(\Leftarrow$ B,V,G,K$)$

Example (Closed ⇝ Quantified Open)

$$\vDash x^2 + y^2 \leq 1 \rightarrow [x' = y, y' = -x]x^2 + y^2 \leq 1$$

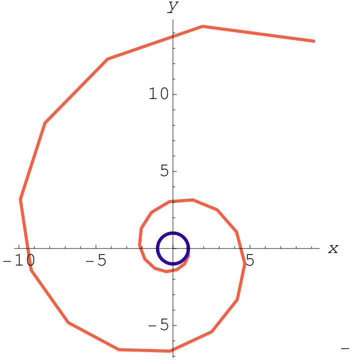


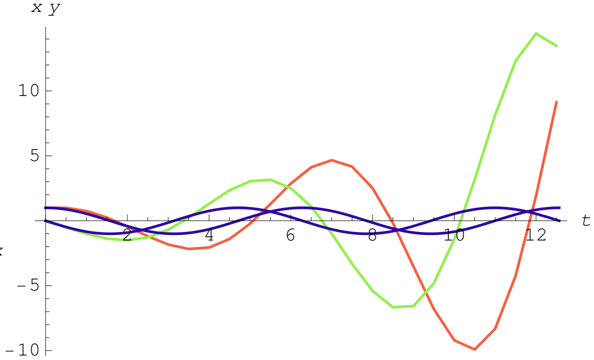


$\mathring{U}$ $[x' = f(x)]F \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)]\mathcal{U}_{\check{\varepsilon}}(F)$ $(\Leftarrow$ B,V,G,K$)$

Example (Closed $\leadsto$ Quantified Open)

$$\vDash x^2 + y^2 \le 1 \rightarrow [x' = y, y' = -x]\forall \check{\varepsilon}{>}0\, x^2 + y^2 < 1 + \check{\varepsilon}$$



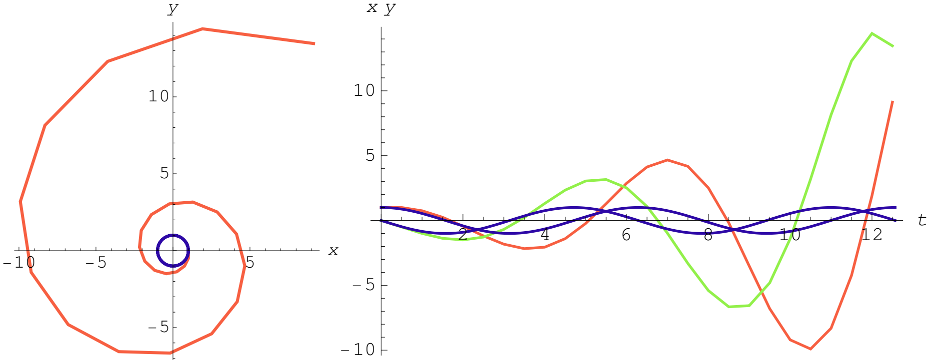


Closed Discrete Completeness (derivable)

$\mathring{U}$ $\quad [x' = f(x)]F \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)]\mathcal{U}_{\check{\varepsilon}}(F)$ $\qquad (\Leftarrow$ B,V,G,K$)$

Example (Closed $\leadsto$ Quantified Open)

$$\vDash x^2 + y^2 \leq 1 \rightarrow \forall \check{\varepsilon}{>}0\, [x' = y, y' = -x]x^2 + y^2 < 1 + \check{\varepsilon}$$



Locally Closed Discrete Completeness: $O \land C$ (derivable)

Example (Locally Closed $\rightsquigarrow$ Open, Closed)

$$\vDash O \land C \to [x' = y, y' = -x](O \land C)$$

Locally Closed Discrete Completeness: $O \land C$ (derivable)

$[]\land \quad [\alpha](O \land C) \leftrightarrow [\alpha]O \land [\alpha]C \qquad (\Leftarrow \text{K})$

Example (Locally Closed $\leadsto$ Open, Closed)

$$\vDash O \land C \rightarrow [x' = y, y' = -x](O \land C)$$

Locally Closed Discrete Completeness: $O \wedge C$ (derivable)

$[]\wedge \quad [\alpha](O \wedge C) \leftrightarrow [\alpha]O \wedge [\alpha]C \qquad (\Leftarrow \text{K})$

Example (Locally Closed $\rightsquigarrow$ Open, Closed)

$$\vDash O \wedge C \rightarrow [x' = y, y' = -x]O \wedge [x' = y, y' = -x]C$$

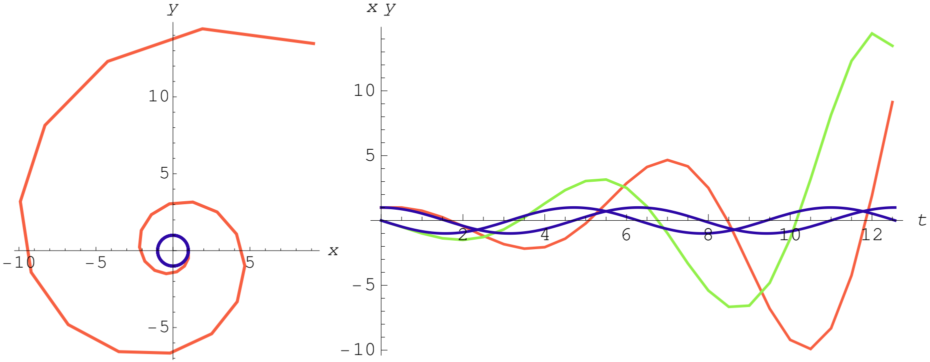
0-Order Discrete Completeness (derivable)

$$\check{U} \quad [x' = f(x)](O \lor C) \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \lor \mathcal{U}_{\check{\varepsilon}}(C)) \qquad (\Leftarrow \text{ B,V,G,K})$$

$\check{U}$ $[x' = f(x)](O \lor C) \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \lor \mathcal{U}_{\check{\varepsilon}}(C))$ $(\Leftarrow$ B,V,G,K)

Example ((Open ∨ Closed) ⇝ Quantified Open)

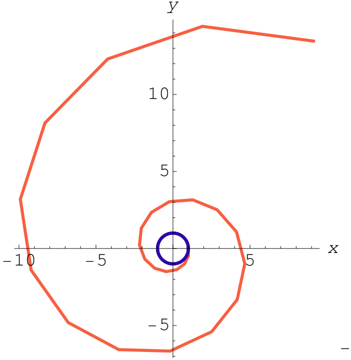
$$\vDash O \lor C \to [x' = y, y' = -x](O \lor C)$$

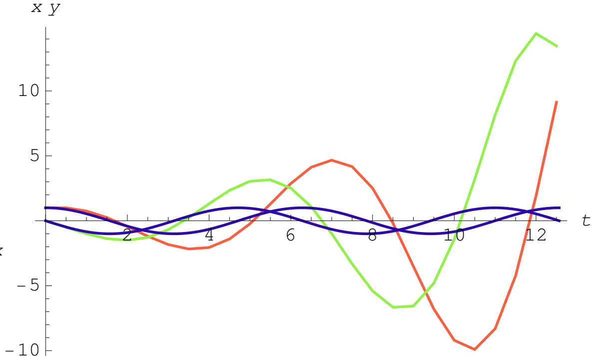


$\check{U}$ $[x' = f(x)](O \vee C) \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \vee \mathcal{U}_{\check{\varepsilon}}(C))$ $(\Leftarrow$ B,V,G,K$)$

Example ((Open ∨ Closed) ⇝ Quantified Open)

$$\vDash O \vee C \rightarrow [x' = y, y' = -x](O \vee \forall \check{\varepsilon}{>}0\, \mathcal{U}_{\check{\varepsilon}}(C))$$

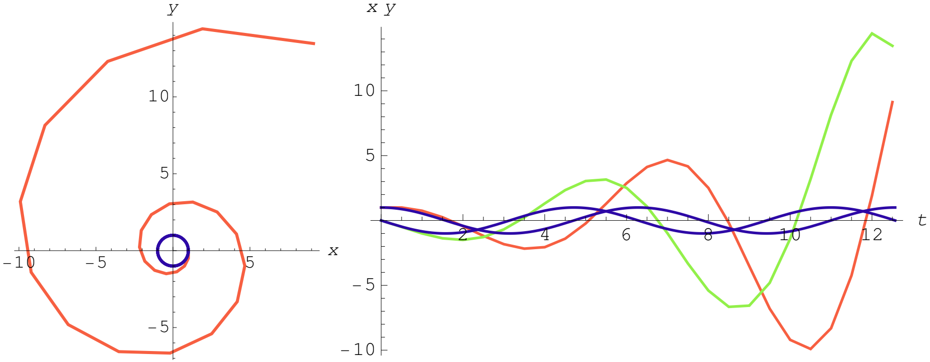




$\check{U}$ $[x' = f(x)](O \vee C) \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \vee \mathcal{U}_{\check{\varepsilon}}(C))$ $(\Leftarrow$ B,V,G,K)

Example ((Open $\vee$ Closed) $\rightsquigarrow$ Quantified Open)

$$\vDash O \vee C \to \forall \check{\varepsilon}{>}0\, [x' = y, y' = -x](O \vee \mathcal{U}_{\check{\varepsilon}}(C))$$



Discrete Completeness

Theorem (Relative Completeness / Continuous)

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

Proof Outline 6p

$$\vDash \phi \text{ implies } Taut_{FOD} \vdash \phi$$

Theorem (Relative Completeness / Discrete)

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

Proof Outline +5p

$$\vDash \phi \text{ implies } Taut_{DL} \vdash \phi$$

Proof Sketch.

Talked about 0-Order

Paper proves $\forall, \exists$ ...

Paper proves $[\alpha], \langle\alpha\rangle$ with hybrid system α ...

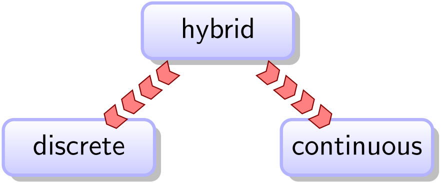
Paper proves nesting ... □

Equi-expressibility

Theorem (Equi-expressibility)

d$\mathcal{L}$ (constructively) expressible in FOD and in DL:

$$\forall\phi\ \exists\phi^\flat \in FOD \quad \vDash \phi \leftrightarrow \phi^\flat$$
$$\forall\phi\ \exists\phi^\# \in DL \quad \vDash \phi \leftrightarrow \phi^\#$$

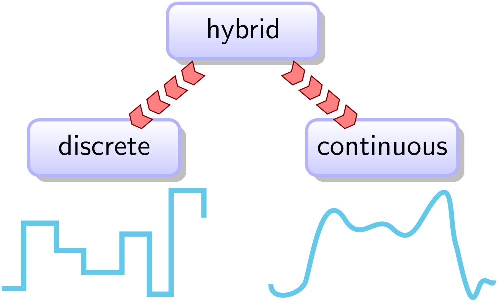


Equi-expressibility

Theorem (Equi-expressibility)

d$\mathcal{L}$ *(constructively) expressible in FOD and in DL:*

$$\forall \phi \ \exists \phi^\flat \in \mathit{FOD} \ \vDash \phi \leftrightarrow \phi^\flat$$
$$\forall \phi \ \exists \phi^\# \in \mathit{DL} \ \vDash \phi \leftrightarrow \phi^\#$$

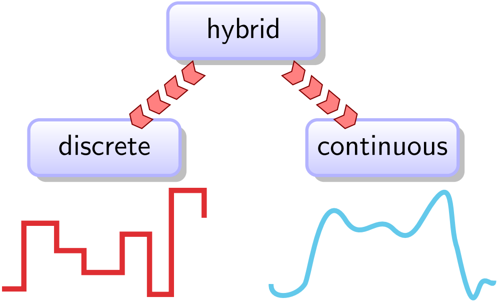


Equi-expressibility

Theorem (Equi-expressibility)

d$\mathcal{L}$ *(constructively) expressible in FOD and in DL:*

$$\forall \phi \;\; \exists \phi^\flat \in FOD \;\; \vDash \phi \leftrightarrow \phi^\flat$$
$$\forall \phi \;\; \exists \phi^\# \in DL \;\; \vDash \phi \leftrightarrow \phi^\#$$

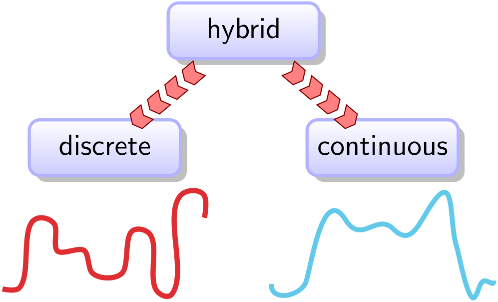


Equi-expressibility

Theorem (Equi-expressibility)

d$\mathcal{L}$ (constructively) expressible in FOD and in DL:

$$\forall \phi\ \exists \phi^\flat \in FOD \quad \vDash \phi \leftrightarrow \phi^\flat$$
$$\forall \phi\ \exists \phi^\# \in DL \quad \vDash \phi \leftrightarrow \phi^\#$$

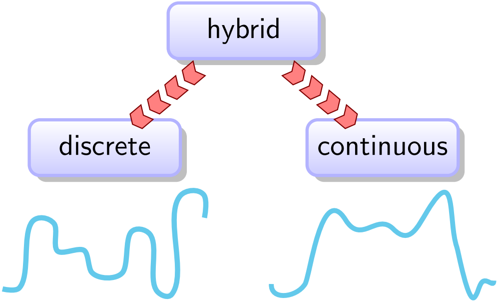


Equi-expressibility

Theorem (Equi-expressibility)

d$\mathcal{L}$ *(constructively) expressible in FOD and in DL:*

$$\forall\phi\ \exists\phi^\flat \in FOD \quad \vDash \phi \leftrightarrow \phi^\flat$$
$$\forall\phi\ \exists\phi^\# \in DL \quad \vDash \phi \leftrightarrow \phi^\#$$

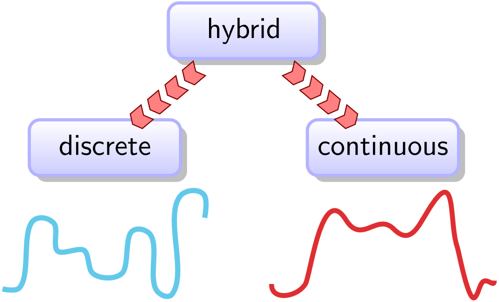


Equi-expressibility

Theorem (Equi-expressibility)

d$\mathcal{L}$ (constructively) expressible in FOD and in DL:

$$\forall\phi\ \exists\phi^\flat \in FOD \ \vDash \phi \leftrightarrow \phi^\flat$$
$$\forall\phi\ \exists\phi^\# \in DL \ \vDash \phi \leftrightarrow \phi^\#$$

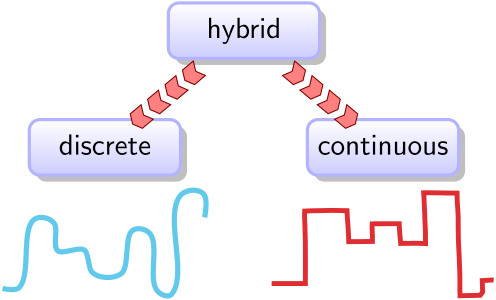


Equi-expressibility

Theorem (Equi-expressibility)

d$\mathcal{L}$ *(constructively) expressible in FOD and in DL:*

$$\forall\phi\ \exists\phi^\flat \in FOD \quad \vDash \phi \leftrightarrow \phi^\flat$$
$$\forall\phi\ \exists\phi^\# \in DL \quad \vDash \phi \leftrightarrow \phi^\#$$

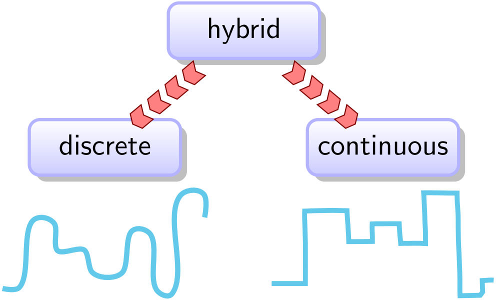


Equi-expressibility

Theorem (Equi-expressibility)

d$\mathcal{L}$ (constructively) expressible in FOD and in DL:

$$\forall \phi \;\; \exists \phi^\flat \in FOD \;\; \vDash \phi \leftrightarrow \phi^\flat$$
$$\forall \phi \;\; \exists \phi^\# \in DL \;\; \vDash \phi \leftrightarrow \phi^\#$$



Relative Decidability

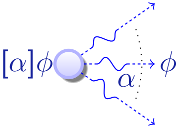
Theorem (Relative Decidability)

Validity of $d\mathcal{L}$ *sentences is decidable relative to FOD or DL.*

The Complete Proof Theory of Hybrid Systems

differential dynamic logic

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



proof-theoretical alignment

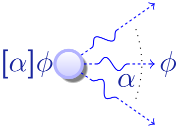
hybrid $=$ continuous $=$ discrete

- Differential dynamic logic
- Hybrid systems
- Axiomatization
- Complete / continuous
- Complete / discrete
- Constructive
- Euler $\overleftrightarrow{\Delta}$
- Perfect proof lifting
- Computer $+$ Control Science

The Complete Proof Theory of Hybrid Systems

differential dynamic logic

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



proof-theoretical alignment

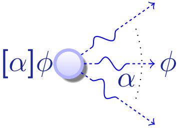
hybrid $=$ continuous $=$ discrete

- Differential dynamic logic
- Hybrid systems
- Axiomatization
- Complete / continuous
- Complete / discrete
- Constructive
- Euler $\overleftrightarrow{\Delta}$
- Perfect proof lifting
- Computer + Control Science
- Discrete invariant

The Complete Proof Theory of Hybrid Systems

differential dynamic logic

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



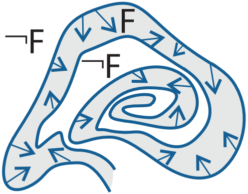
proof-theoretical alignment

hybrid = continuous = discrete

- Differential dynamic logic
- Hybrid systems
- Axiomatization
- Complete / continuous
- Complete / discrete
- Constructive
- Euler $\overleftrightarrow{\Delta}$

- Perfect proof lifting
- Computer + Control Science
- Discrete invariant

$\rightsquigarrow$ differential invariant



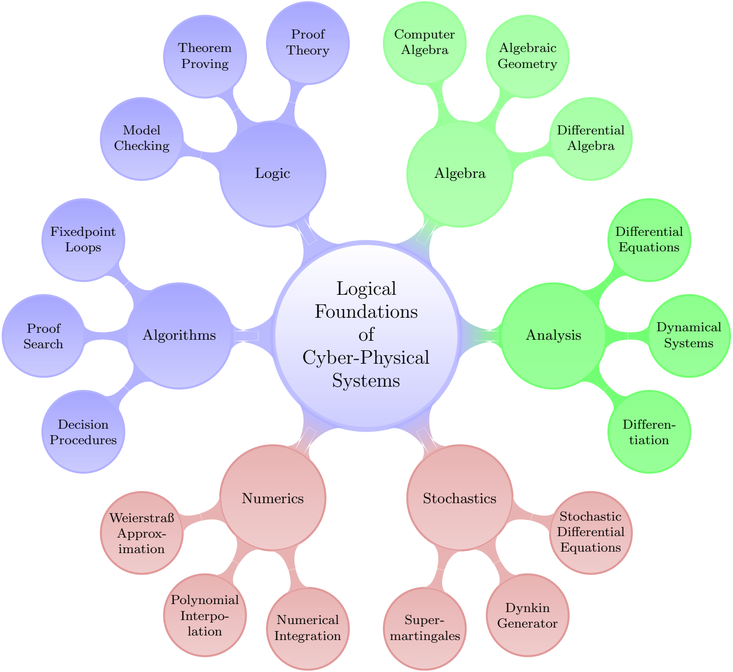
André Platzer.
The complete proof theory of hybrid systems.
LICS, 2012.

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

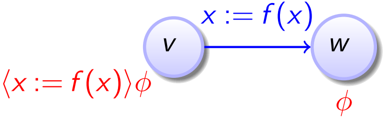
André Platzer.
Differential dynamic logic for hybrid systems.
J. Autom. Reas., 41(2):143–189, 2008.

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

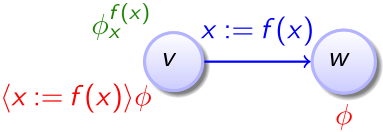
André Platzer and Edmund M. Clarke.
The image computation problem in hybrid systems model checking.
In A. Bemporad, A. Bicchi, and G. Buttazzo, editors, *HSCC*, volume 4416 of *LNCS*, pages 473–486. Springer, 2007.


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

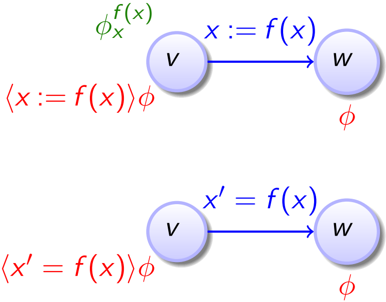
Proof by Symbolic Decomposition



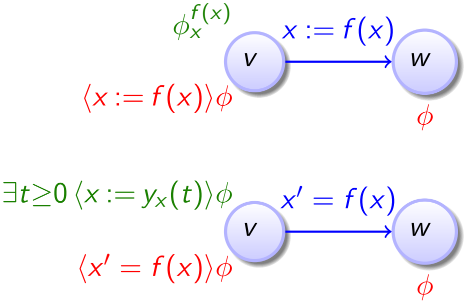
Proof by Symbolic Decomposition



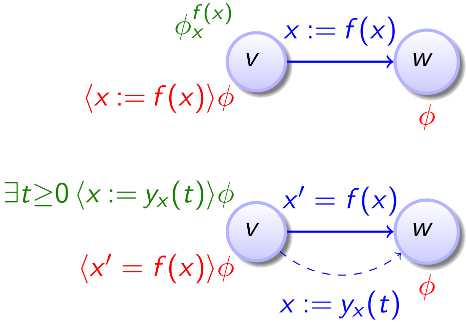
Proof by Symbolic Decomposition



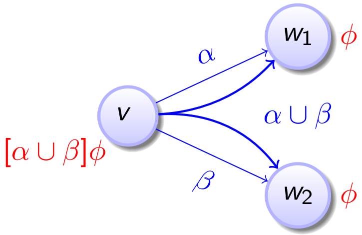
Proof by Symbolic Decomposition



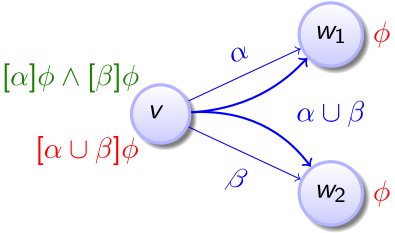
Proof by Symbolic Decomposition



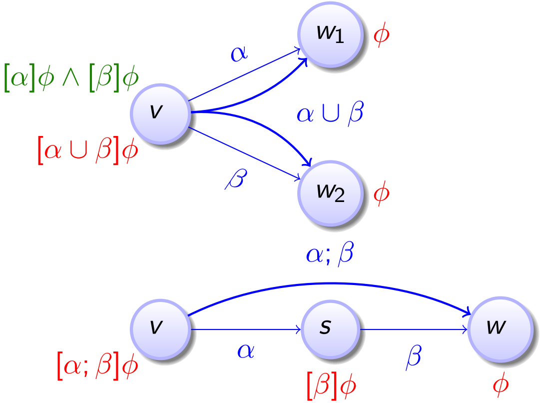
Proof by Symbolic Decomposition



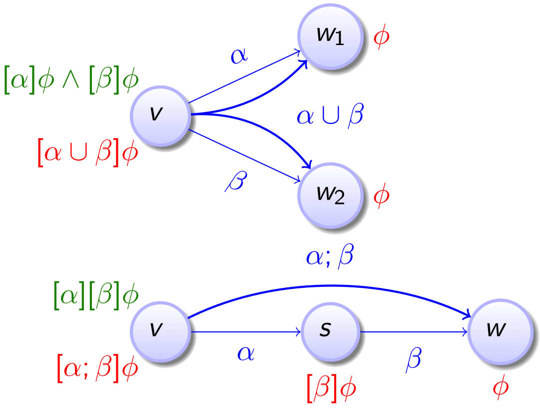
Proof by Symbolic Decomposition



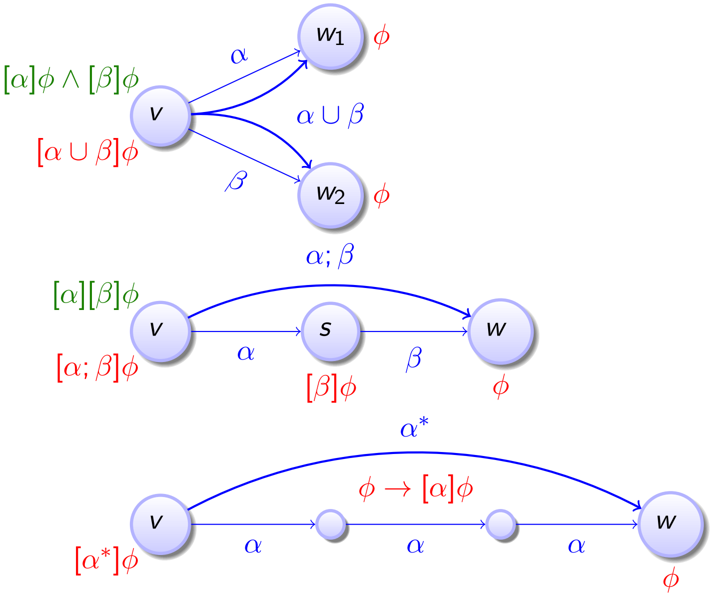
Proof by Symbolic Decomposition



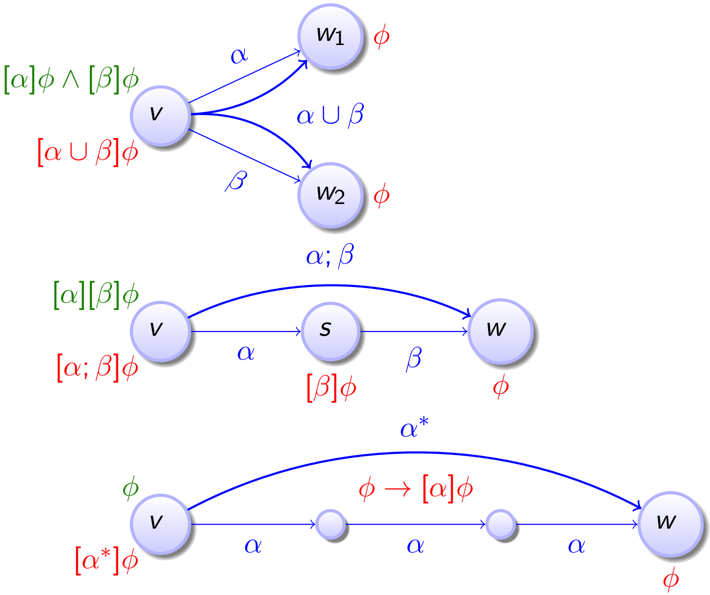
Proof by Symbolic Decomposition



Proof by Symbolic Decomposition



Proof by Symbolic Decomposition



Proof by Symbolic Decomposition