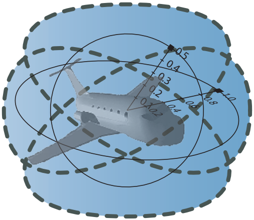
The Complete Proof Theory of Hybrid Systems

André Platzer

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

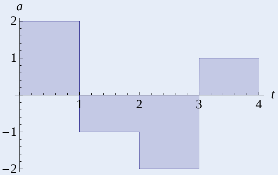


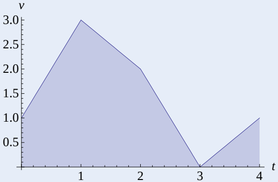
Hybrid Systems: e.g., Car Control

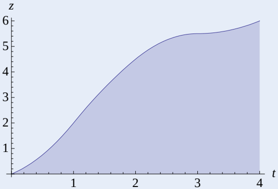
Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

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







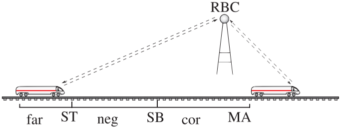
Hybrid Systems: e.g., Car Control

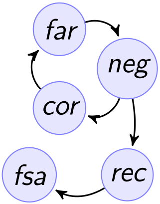
Challenge (Hybrid Systems)

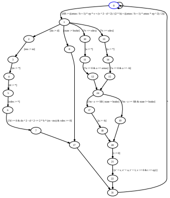
Fixed rule describing state evolution with both

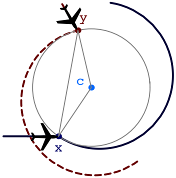
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

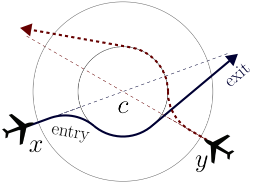
Successful Hybrid Systems Proofs

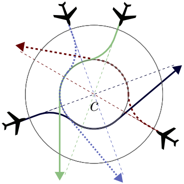


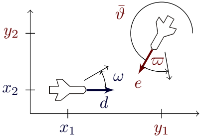


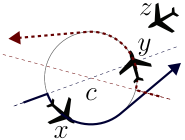


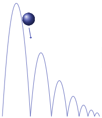


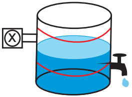




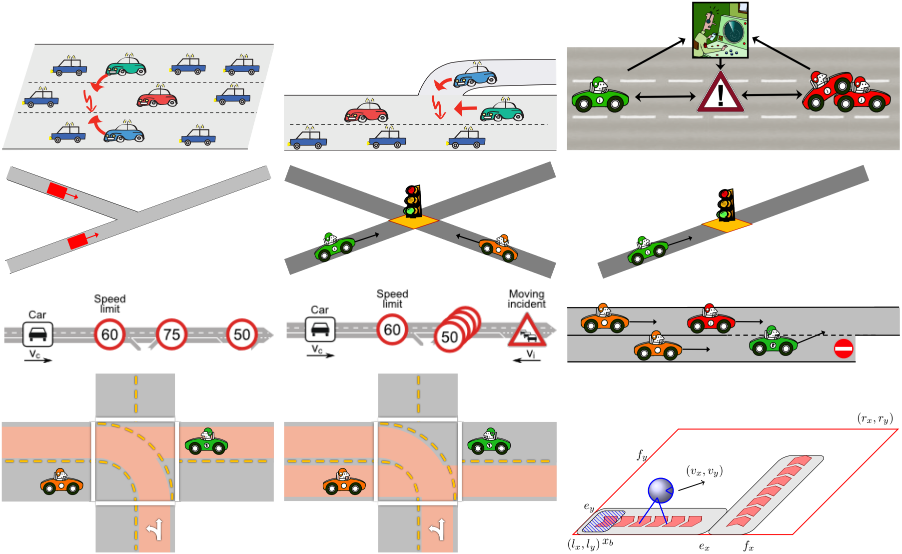








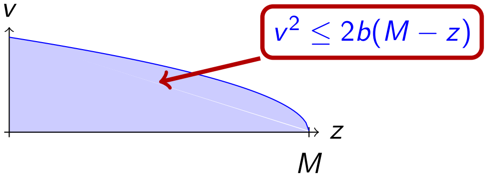
Successful Hybrid Systems Proofs



Proof theory: hybrid = continuous = discrete

differential dynamic logic

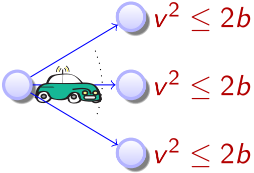
$d\mathcal{L} = \mathrm{FOL}_{\mathbb{R}}$



differential dynamic logic

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

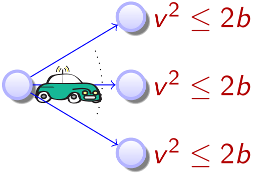
$$\mathcal{C} \rightarrow [\underbrace{\texttt{if}(z > SB)\, a := -b;\ z'' = a}_{\text{hybrid program}}]\, v^2 \leq 2b$$



differential dynamic logic

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

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



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)

$v \models \theta_1 \geq \theta_2$	iff	$[\![\theta_1]\!]_v \geq [\![\theta_2]\!]_v$
$v \models [\alpha]\phi$	iff	$w \models \phi$ for all w with $(v,w) \in \rho(\alpha)$
$v \models \langle\alpha\rangle\phi$	iff	$w \models \phi$ for some w with $(v,w) \in \rho(\alpha)$
$v \models \forall x\, \phi$	iff	$w \models \phi$ for all w that agree with v except for x
$v \models \exists x\, \phi$	iff	$w \models \phi$ for some w that agrees with v except for x
$v \models \phi \wedge \psi$	iff	$v \models \phi$ and $v \models \psi$

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

[:=]	$[x := \theta]\phi(x) \leftrightarrow \phi(\theta)$
[?]	$[?H]\phi \leftrightarrow (H \rightarrow \phi)$
[']	$[x' = f(x)]\phi \leftrightarrow \forall t{\geq}0\, [x := y(t)]\phi \qquad (y'(t) = f(y))$
[∪]	$[\alpha \cup \beta]\phi \leftrightarrow [\alpha]\phi \wedge [\beta]\phi$
[;]	$[\alpha; \beta]\phi \leftrightarrow [\alpha][\beta]\phi$
[*]	$[\alpha^*]\phi \leftrightarrow \phi \wedge [\alpha][\alpha^*]\phi$
K	$[\alpha](\phi \rightarrow \psi) \rightarrow ([\alpha]\phi \rightarrow [\alpha]\psi)$
I	$[\alpha^*](\phi \rightarrow [\alpha]\phi) \rightarrow (\phi \rightarrow [\alpha^*]\phi)$
C	$[\alpha^*]\forall v{>}0\, (\varphi(v) \rightarrow \langle\alpha\rangle\varphi(v-1)) \rightarrow \forall v\, (\varphi(v) \rightarrow \langle\alpha^*\rangle\exists v{\leq}0\, \varphi(v))$

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

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

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

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

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

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

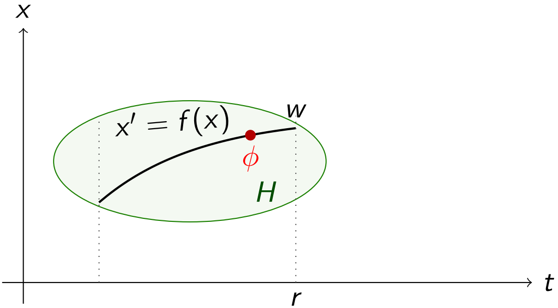
MP $\quad \dfrac{\phi \to \psi \quad \phi}{\psi}$

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

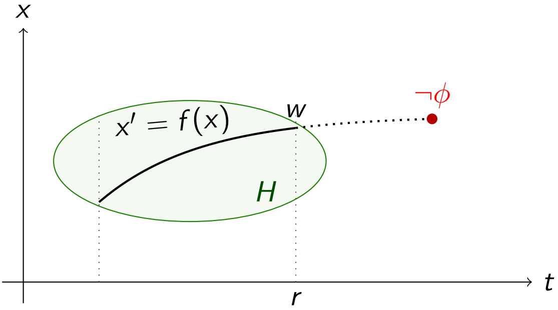
B $\quad \forall x\, [\alpha]\phi \to [\alpha]\forall x\, \phi \qquad (x \notin \alpha)$

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

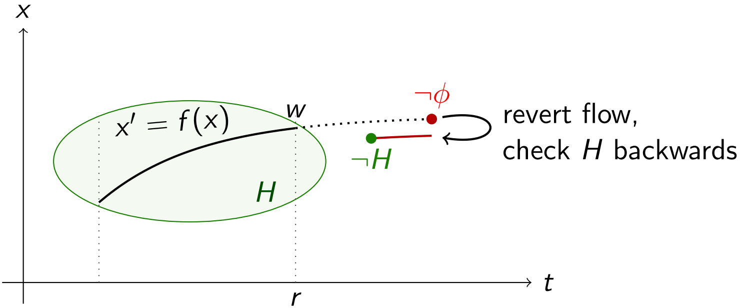
[&] $[x' = f(x)\,\&\,H]\phi \leftrightarrow [x' = f(x)](\phi)$



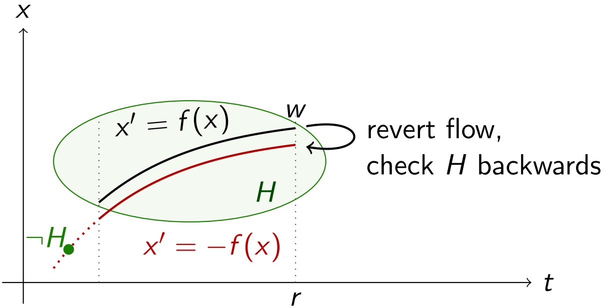
[&] $[x' = f(x) \,\&\, H]\phi \leftrightarrow [x' = f(x)](\phi)$



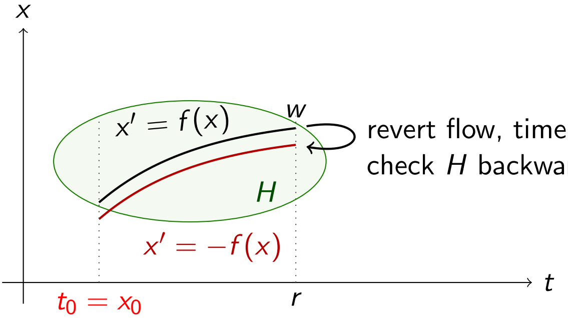
$$[\&] \quad [x' = f(x) \,\&\, H]\phi \leftrightarrow [x' = f(x)]\big([x' = -f(x)](H) \rightarrow \phi\big)$$



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



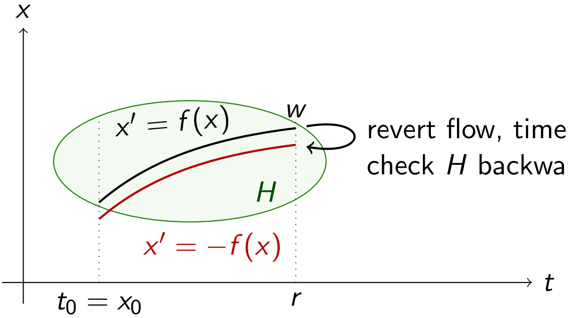
[&] $[x' = f(x) \,\&\, H]\phi$
$\leftrightarrow \forall t_0{=}x_0[x' = f(x)]\big([x' = -f(x)](x_0 \geq t_0 \rightarrow H) \rightarrow \phi\big)$



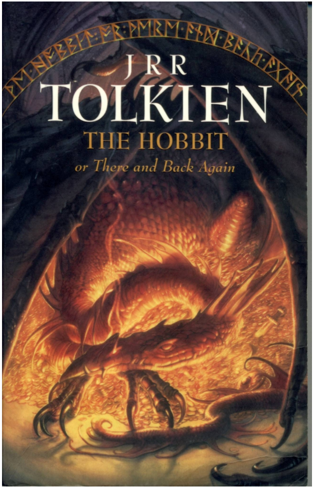
revert flow, time x_0;
check H backwards

"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)

d$\mathcal{L}$ *calculus is sound, i.e., all provable* d$\mathcal{L}$ *formulas are valid:*

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

What about the converse?

Soundness

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e., all provable* d$\mathcal{L}$ *formulas are valid:*

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

What about the converse?

$$(s := s + 2n + 1; n := n + 1)^* \quad \rightsquigarrow \quad s = n^2$$

Soundness

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e., all provable* d$\mathcal{L}$ *formulas are valid:*

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

What about the converse?

$$\begin{array}{lcl} (s := s + 2n + 1; n := n + 1)^* & \leadsto & s = n^2 \\ x' = 5 & \leadsto & x(t) = 5t + x_0 \end{array}$$

Soundness

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e., all provable* d$\mathcal{L}$ *formulas are valid:*

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

What about the converse?

$$(s := s + 2n + 1; n := n + 1)^* \quad \rightsquigarrow \quad s = n^2$$
$$x' = 5 \quad \rightsquigarrow \quad x(t) = 5t + x_0$$
$$x' = x \quad \rightsquigarrow \quad x(t) = x_0 e^t$$

Soundness

Theorem (Soundness)

d$\mathcal{L}$ *calculus is sound, i.e., all provable* d$\mathcal{L}$ *formulas are valid:*

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

What about the converse?

$$\begin{array}{lcl}
(s := s + 2n + 1; n := n + 1)^* & \leadsto & s = n^2 \\
x' = 5 & \leadsto & x(t) = 5t + x_0 \\
x' = x & \leadsto & x(t) = x_0 e^t \\
x'' = -x & \leadsto & x(t) = x_0 \cos t + x_0' \sin t
\end{array}$$

Continuous Completeness

Theorem (Relative Completeness / Continuous)

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

▸ Proof Outline

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

Continuous Completeness

Theorem (Relative Completeness / Continuous)

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

Proof Outline

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

$$\text{FOD} \quad = \quad \text{FOL} + [x' = f(x)]F$$

Continuous Completeness

Theorem (Relative Completeness / Continuous)

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

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

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

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

Theorem (Relative Completeness / Discrete)

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

Proof Outline

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

Discrete Completeness

Theorem (Relative Completeness / Continuous)

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

▸ Proof Outline

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

Theorem (Relative Completeness / Discrete)

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

▸ Proof Outline

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

Corollary (Complete Proof-theoretical Alignment)

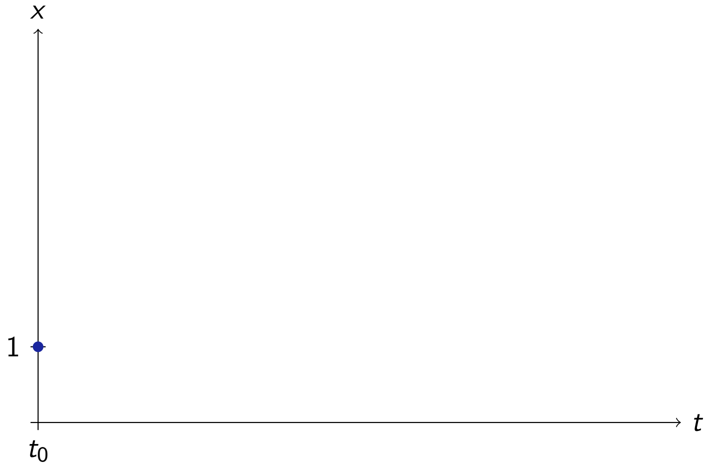
hybrid = continuous = discrete

Corollary (Interdisciplinary Integrability)

"Discrete computer science + continuous control are integrable"

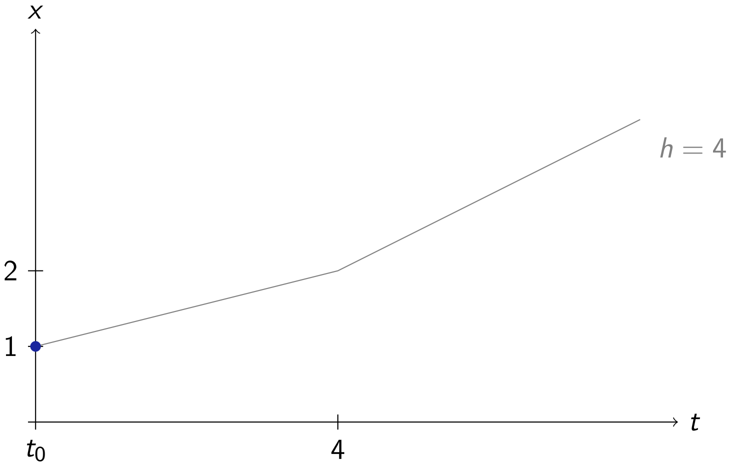
Proof of "hybrid = continuous = discrete"

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



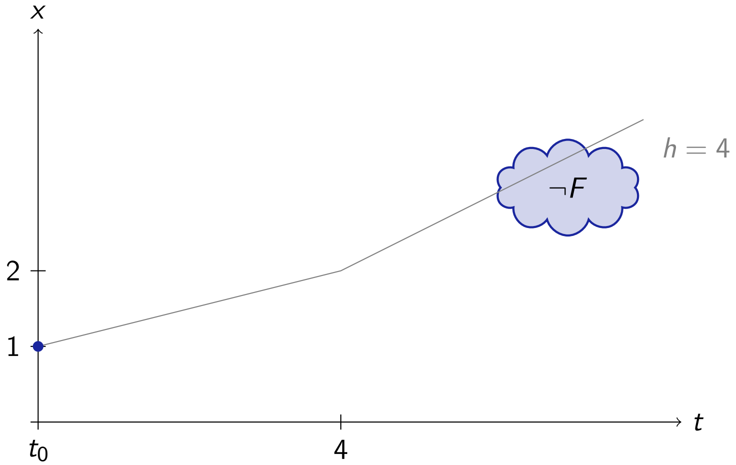
Continuous Dynamics $\neq$ Discrete Dynamics

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

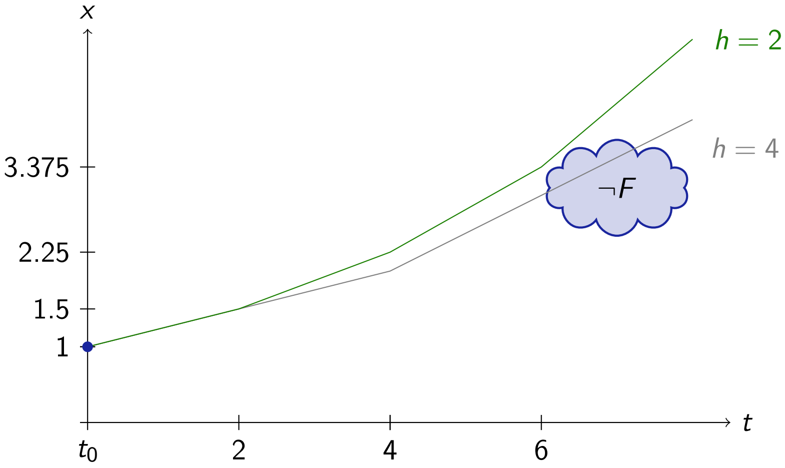


Continuous Dynamics $\neq$ Discrete Dynamics

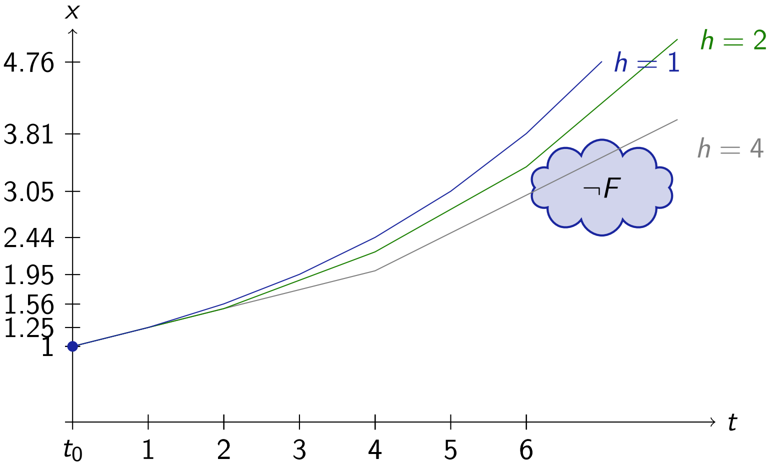
$$[x' = \frac{x}{4}]F \quad \not\Rightarrow \quad [(x := x + h\frac{x}{4})^*]F$$



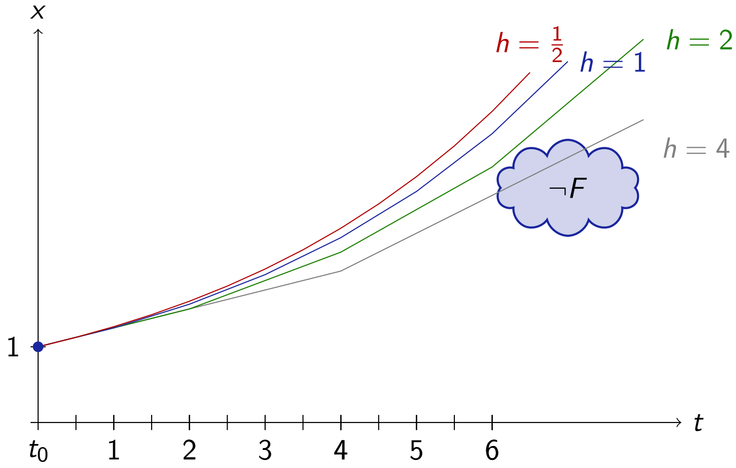
$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



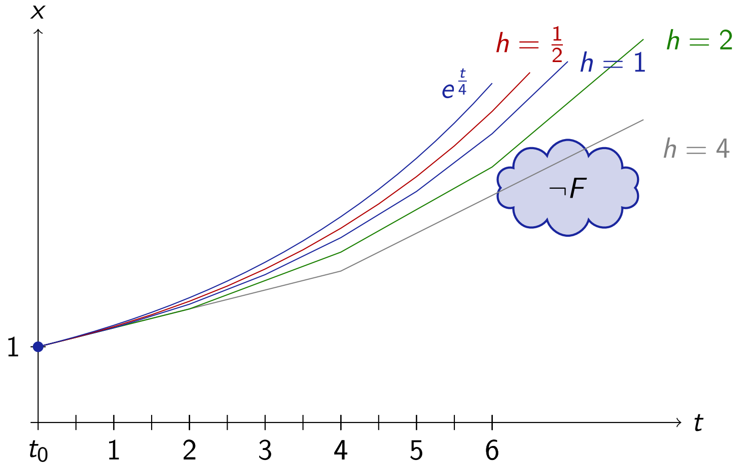
$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



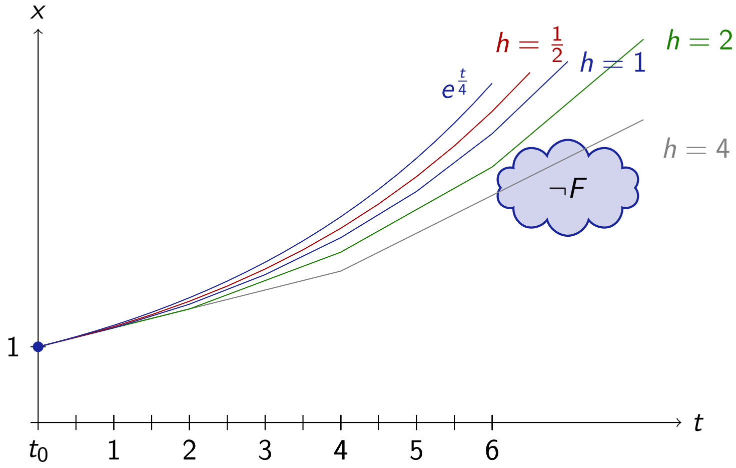
$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



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

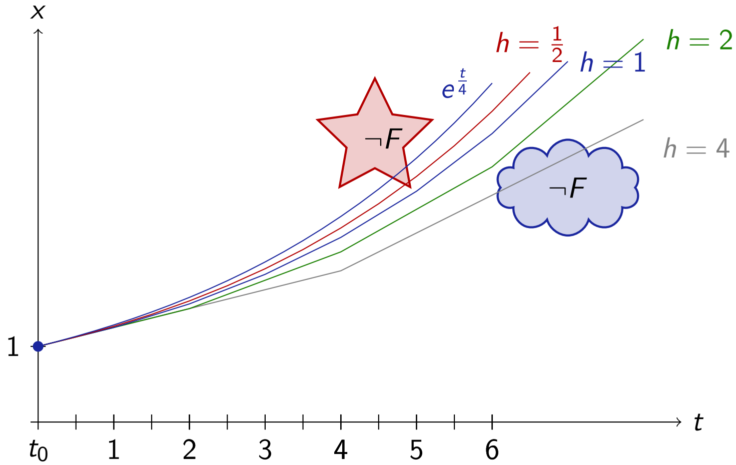


$$[x' = \frac{x}{4}]F \quad \not\Rightarrow \quad [(x := x + h\frac{x}{4})^*]F$$



Continuous Dynamics $\neq$ Discrete Dynamics

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



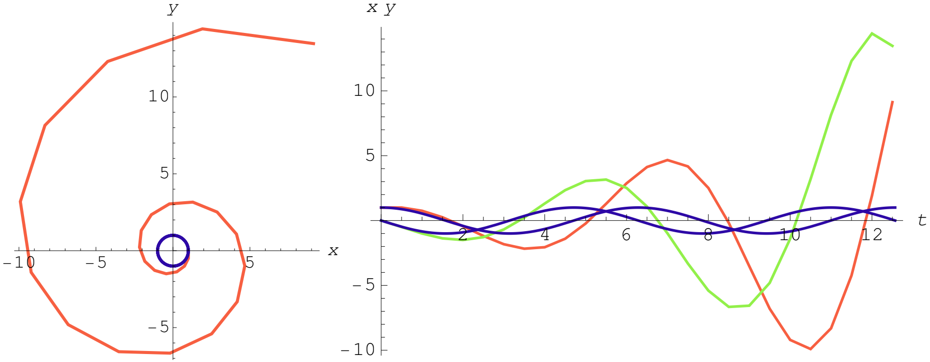
Discrete Euler Approximation Axiom $\overleftarrow{\Delta}$

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

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

Example (Insufficient, not global)

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

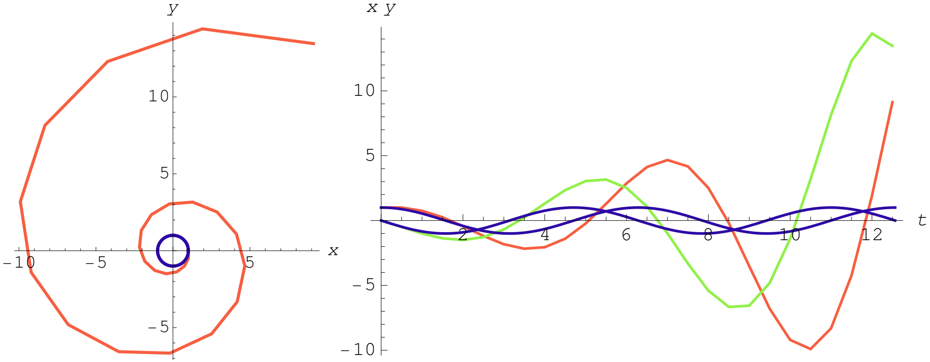


Discrete Euler Approximation Axiom $\overleftarrow{\Delta}$

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

Example (Unsound for open F, only in closure)

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

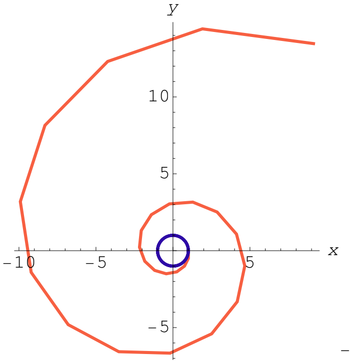


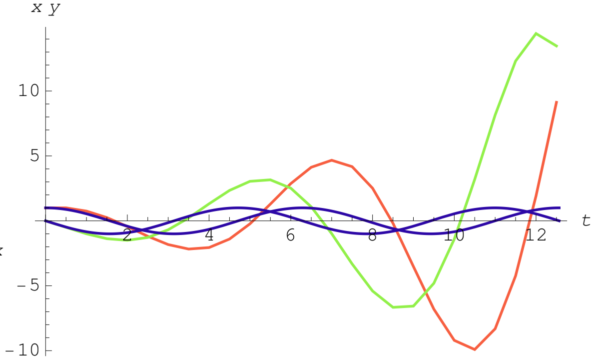
Discrete Euler Approximation Axiom $\overleftarrow{\Delta}$

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

Example (Insufficient, not global)

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



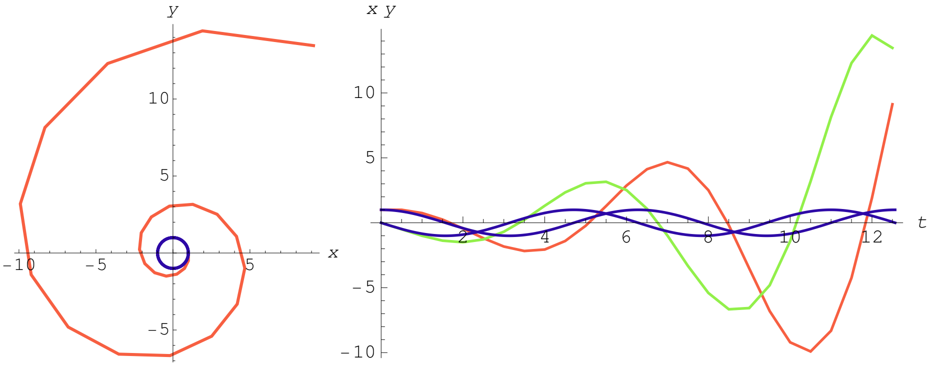


$\overrightarrow{\Delta}$ $[x' = f(x)]F$
$\rightarrow \forall t{\geq}0\, \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*](t \geq 0 \rightarrow F)$

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

Example (Converse unsound for open F — $\overleftarrow{\Delta}$ for closed F)

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



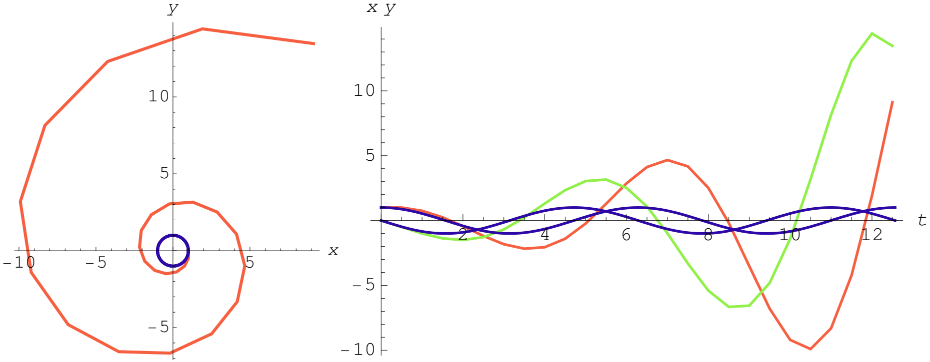
$\mathcal{R}$ Discrete Euler Approximation Axiom $\overrightarrow{\Delta}$ $t' = -1$

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

(open)

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

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



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

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

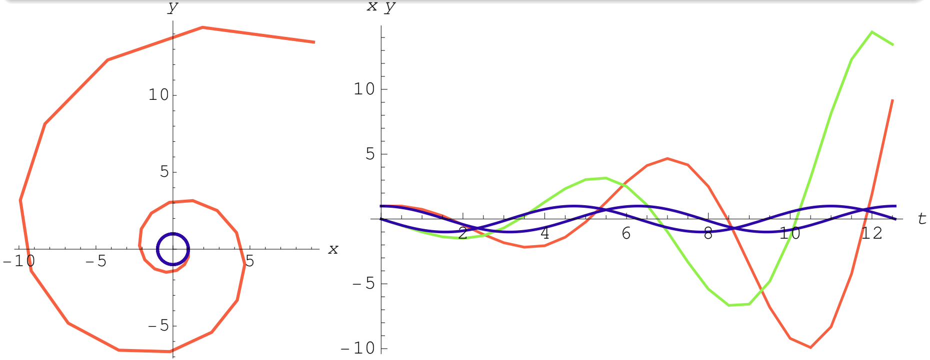
Example ()

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

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

Example (Insufficient for closed F)

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

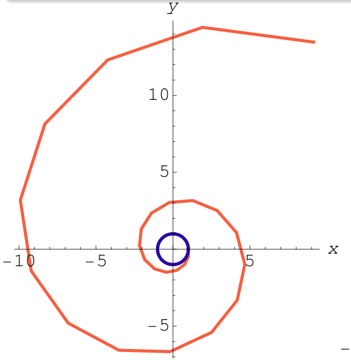


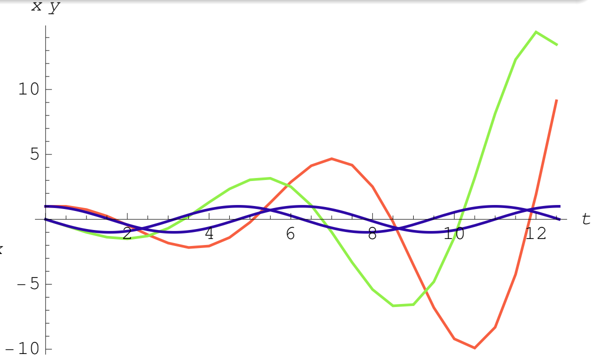
$\overleftrightarrow{\Delta}$ $[x' = f(x)]F$ *(open)*

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

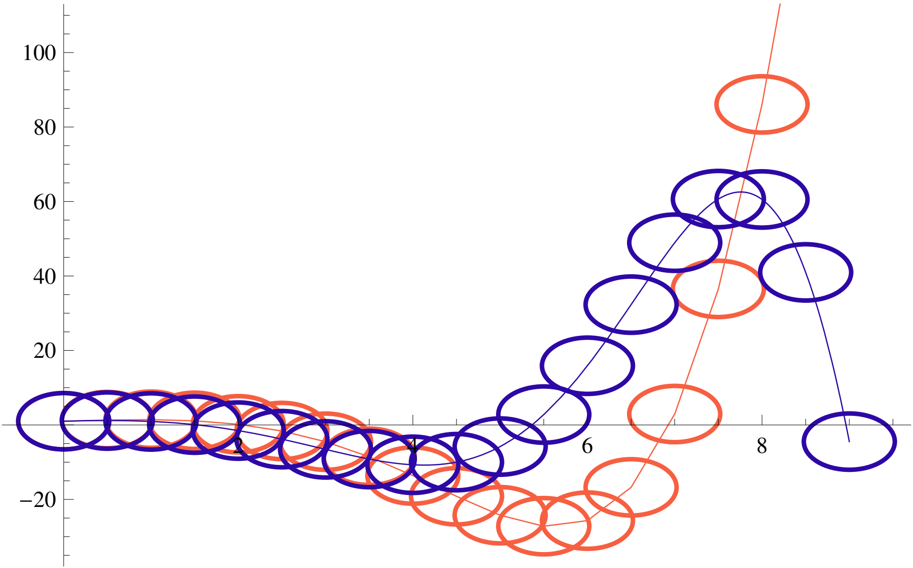
Example (Insufficient for closed F)

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





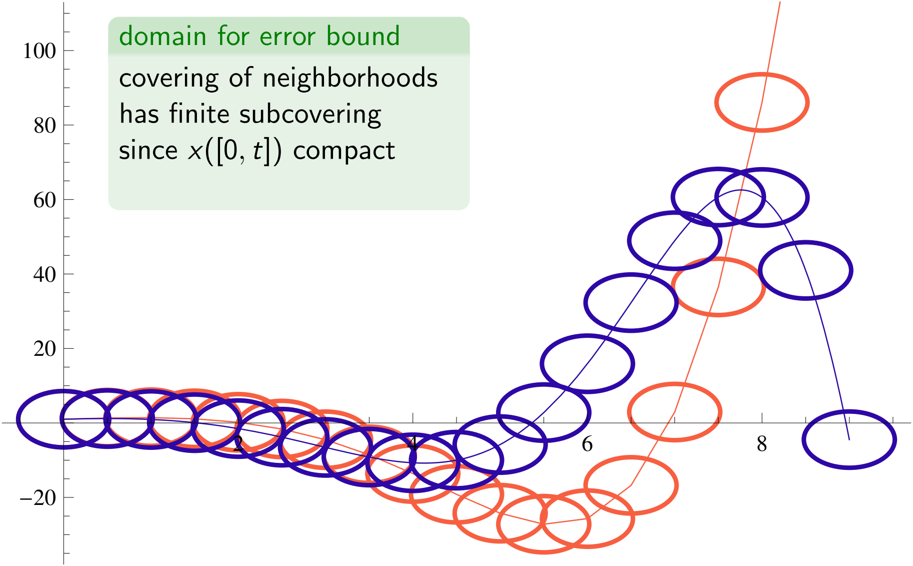
$\mathcal{A}$ $\overleftrightarrow{\Delta}$ Proof: Partial Covering for Solution, Approximation



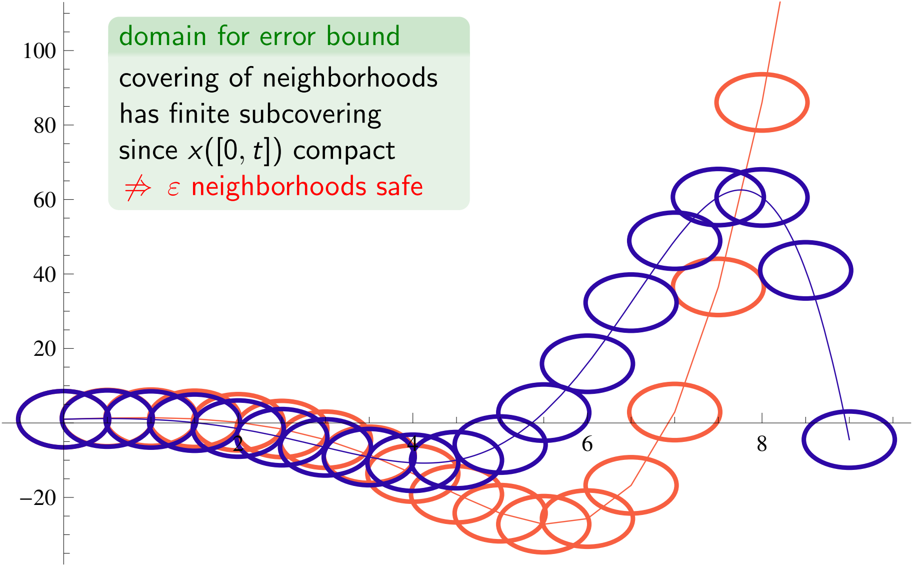
Proof: Partial Covering for Solution, Approximation

domain for error bound

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



$\overleftrightarrow{\Delta}$ Proof: Partial Covering for Solution, Approximation



domain for error bound

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

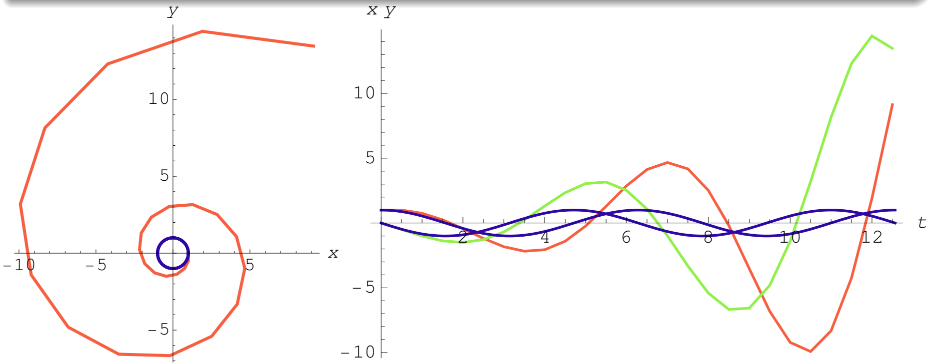
$\overleftrightarrow{\Delta}$ axiom for open F, but F may be closed

$\overleftrightarrow{\Delta}$ $[x' = f(x)]F$ (*open*)

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

Example (Insufficient for closed F)

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



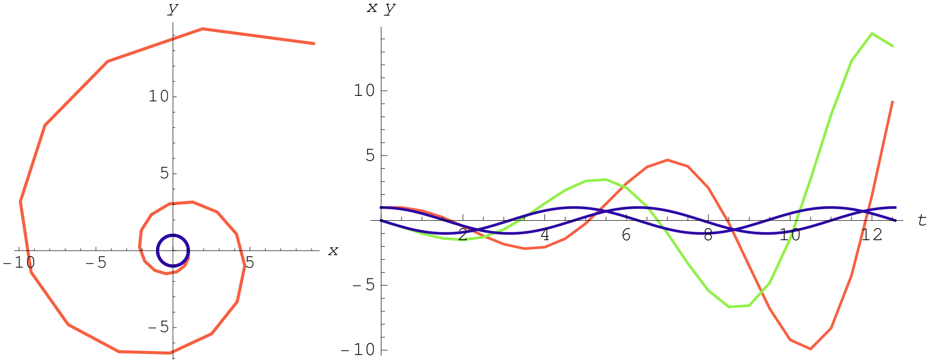
Closed Discrete Completeness (derivable)

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

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

Example (Closed $\leadsto$ Quantified Open)

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

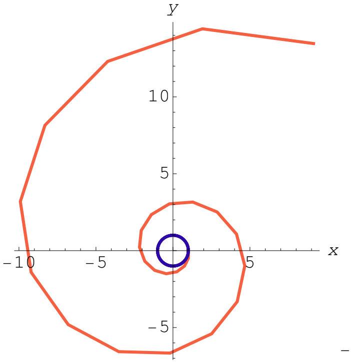


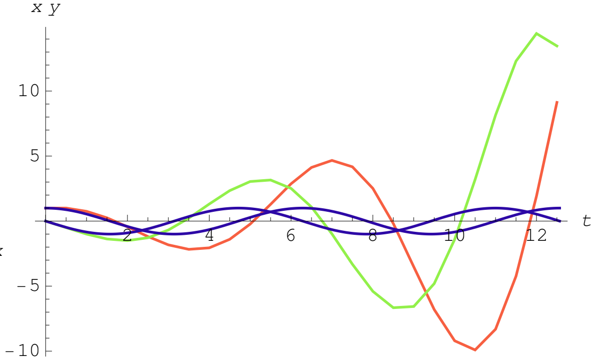
Closed Discrete Completeness (derivable)

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

Example (Closed $\rightsquigarrow$ Quantified Open)

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

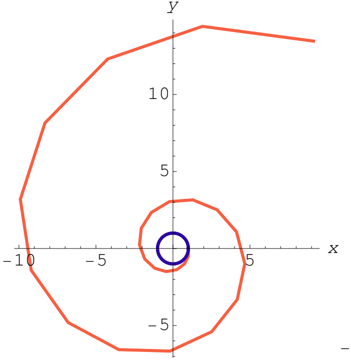


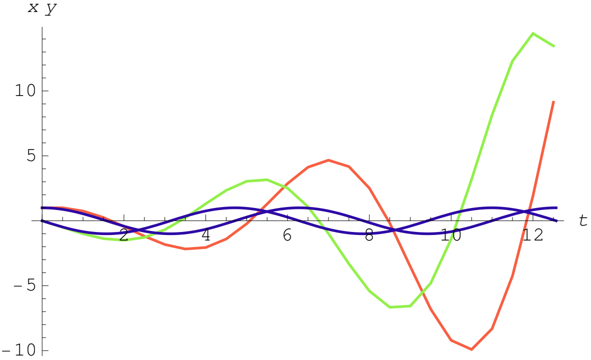


$\mathring{U}$ $[x' = f(x)]F \leftrightarrow \forall \check{\varepsilon}{>}0\,[x' = f(x)]\mathcal{U}_{\check{\varepsilon}}(F)$ $(\Leftarrow \text{B,V,G,K})$

Example (Closed $\rightsquigarrow$ Quantified Open)

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





$\overleftrightarrow{\Delta}$ axiom for open/closed F, but otherwise?

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

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

Locally Closed Discrete Completeness (derivable)

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

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

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

Locally Closed Discrete Completeness (derivable)

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

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

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

Semialgebraic Discrete Completeness (derivable)

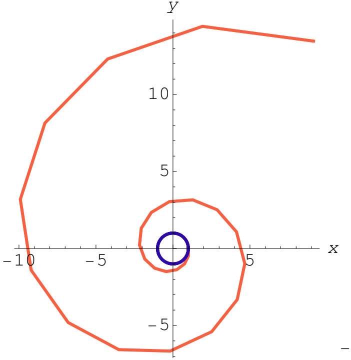
$\check{U}$ $[x' = f(x)](O \lor C) \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \lor \mathcal{U}_{\check{\varepsilon}}(C))$ $(\Leftarrow$ B,V,G,K)

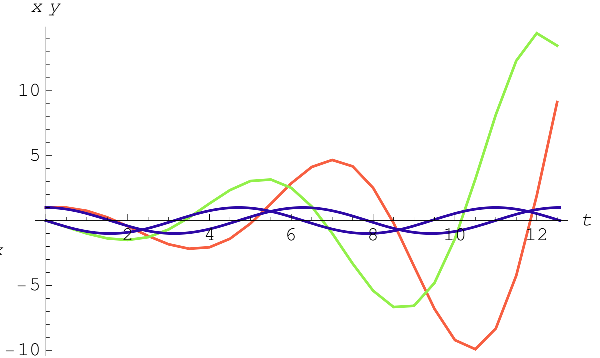
Semialgebraic Discrete Completeness (derivable)

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

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

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

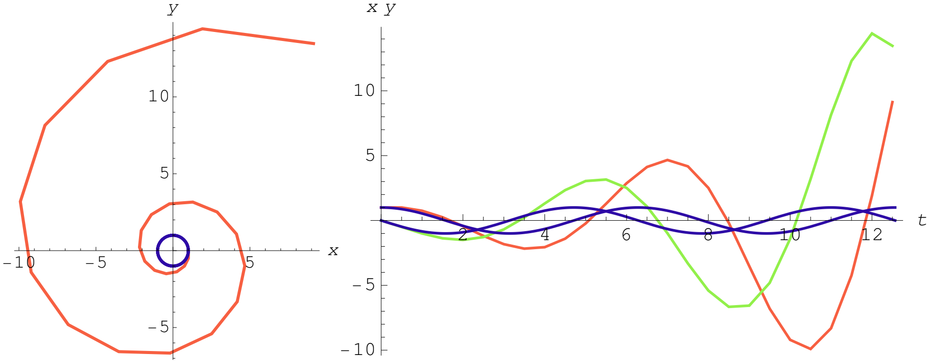




$\check{U}$ $[x' = f(x)](O \vee C) \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \vee \mathcal{U}_{\check{\varepsilon}}(C))$ $(\Leftarrow$ B,V,G,K$)$

Example ((Open ∨ Closed) ⇝ Quantified Open)

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

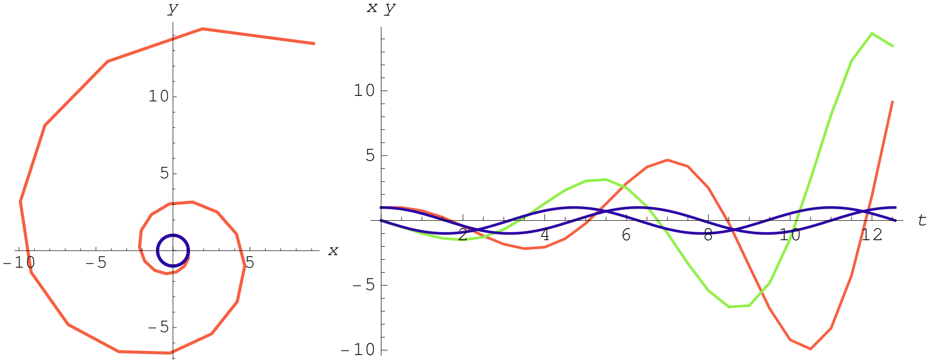


Semialgebraic Discrete Completeness (derivable)

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

Example ((Open ∨ Closed) ⇝ Quantified Open)

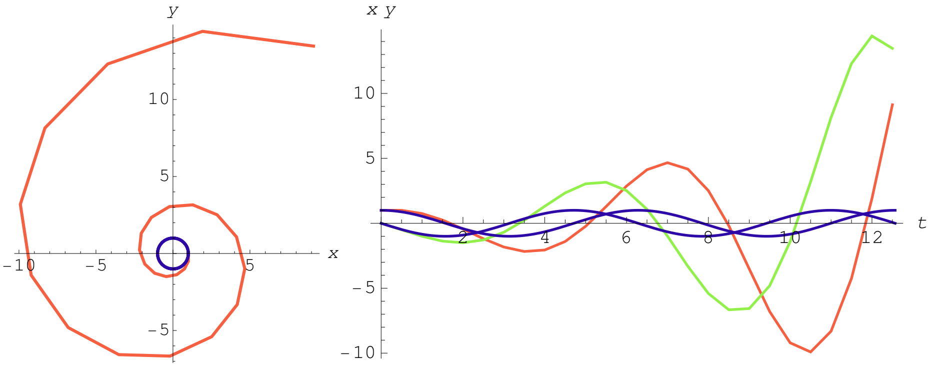
$$\vDash O \vee C \rightarrow [x' = y, y' = -x]\forall \check{\varepsilon}{>}0\,(O \vee \mathcal{U}_{\check{\varepsilon}}(C))$$



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

Example ((Open ∨ Closed) ⇝ Quantified Open)

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



$\overleftrightarrow{\Delta}$ axiom for semialgebraic F, but otherwise?

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* $+\overleftrightarrow{\Delta}$ *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 semialgebraic

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

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

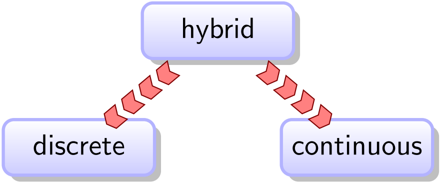
Paper proves nesting ... □

Equi-expressibility

Theorem (Equi-expressibility)

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

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

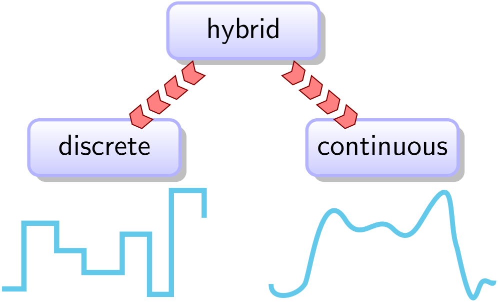


Equi-expressibility

Theorem (Equi-expressibility)

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

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

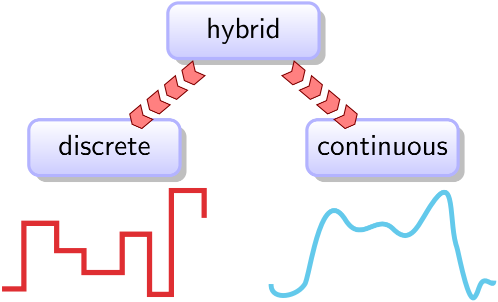


Equi-expressibility

Theorem (Equi-expressibility)

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

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

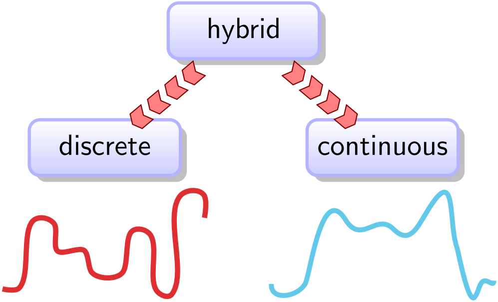


Equi-expressibility

Theorem (Equi-expressibility)

dℒ *(constructively) expressible in FOD and in DL:*

$$\begin{array}{lll} \forall\phi\ \exists\phi^\flat \in FOD & \vDash \phi \leftrightarrow \phi^\flat \\ \forall\phi\ \exists\phi^\# \in DL & \vDash \phi \leftrightarrow \phi^\# \end{array}$$

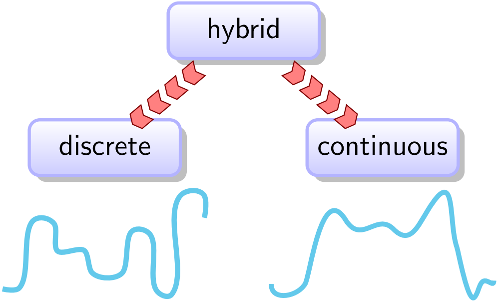


Equi-expressibility

Theorem (Equi-expressibility)

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

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

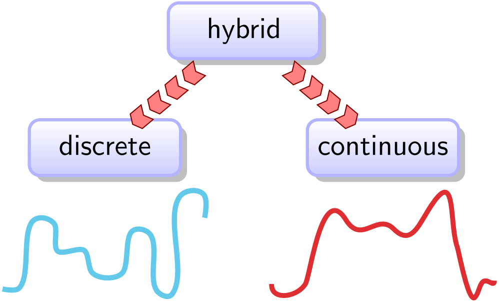


Equi-expressibility

Theorem (Equi-expressibility)

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

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

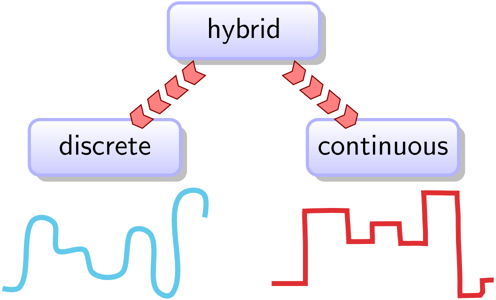


Equi-expressibility

Theorem (Equi-expressibility)

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

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

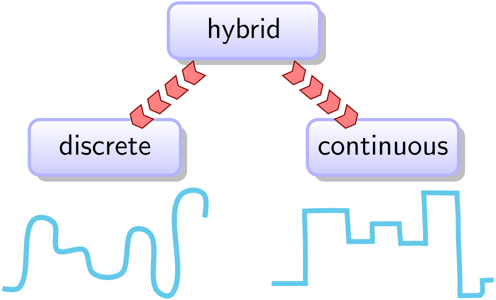


Equi-expressibility

Theorem (Equi-expressibility)

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

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



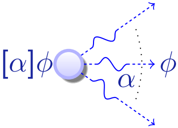
Relative Decidability

Theorem (Relative Decidability)

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

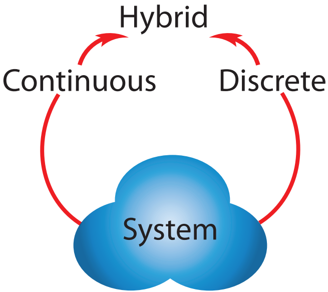
differential dynamic logic

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



proof-theoretical alignment

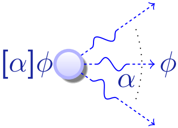
hybrid = continuous = discrete



The Complete Proof Theory of Hybrid Systems

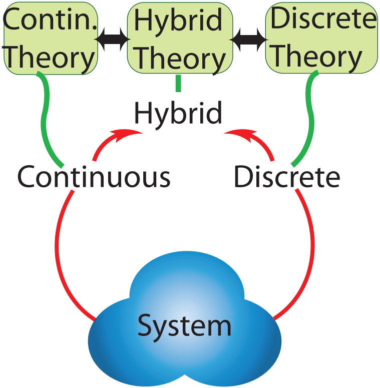
differential dynamic logic

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



proof-theoretical alignment

hybrid = continuous = discrete



André Platzer.
The complete proof theory of hybrid systems.
LICS, pages 541–550. IEEE 2012.

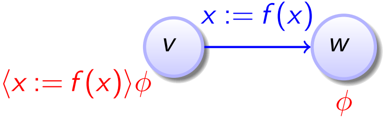
André Platzer.
Logical Analysis of Hybrid Systems:
Proving Theorems for Complex Dynamics.
Springer, 2010.

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

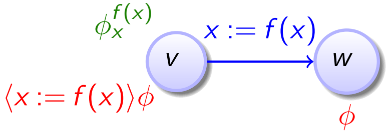
André Platzer.
Differential-algebraic dynamic logic for differential-algebraic programs.
J. Log. Comput., 35(1): 309–352, 2010.

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.

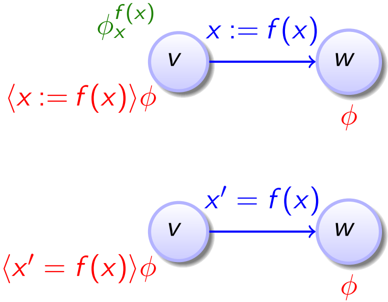
Proof by Symbolic Decomposition



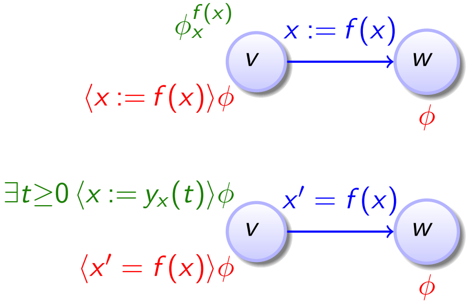
Proof by Symbolic Decomposition



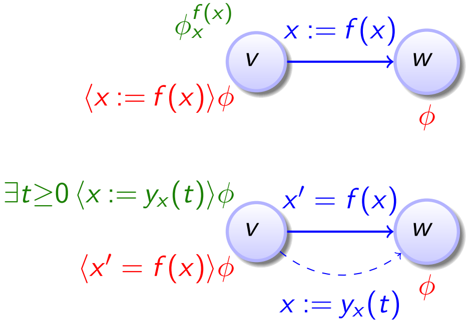
Proof by Symbolic Decomposition



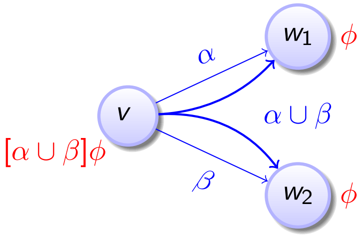
Proof by Symbolic Decomposition



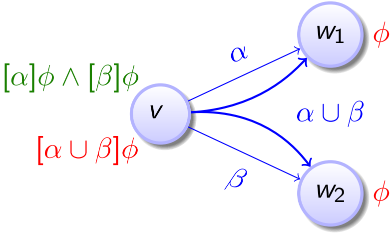
Proof by Symbolic Decomposition



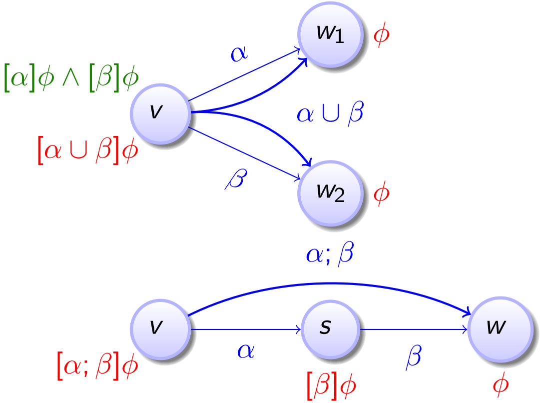
Proof by Symbolic Decomposition



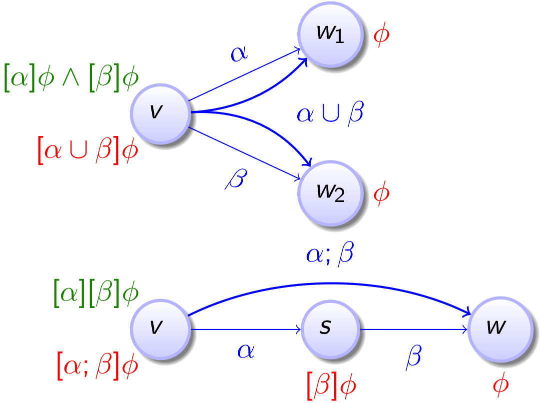
Proof by Symbolic Decomposition



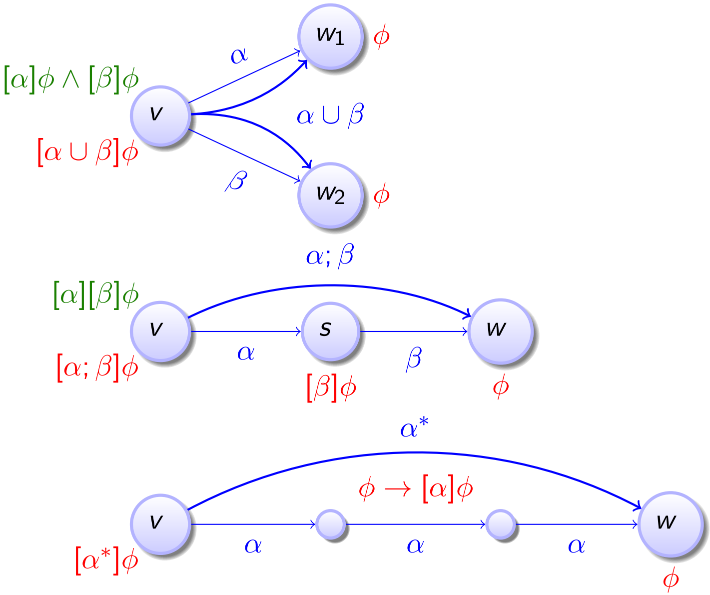
Proof by Symbolic Decomposition



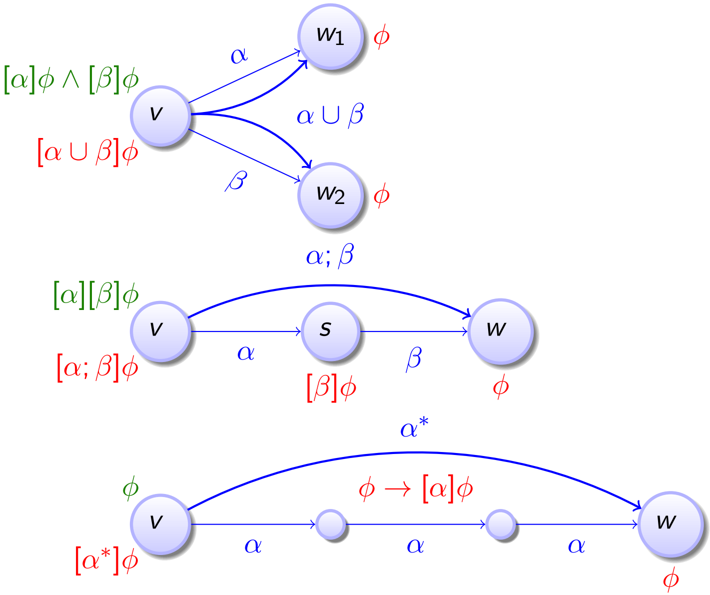
Proof by Symbolic Decomposition



Proof by Symbolic Decomposition



Proof by Symbolic Decomposition



Proof by Symbolic Decomposition