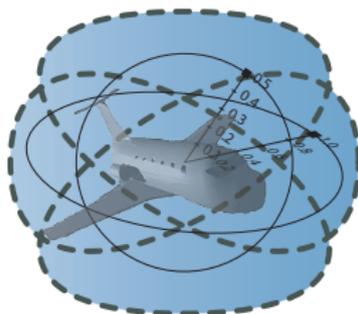


# The Complete Proof Theory of Hybrid Systems

André Platzer

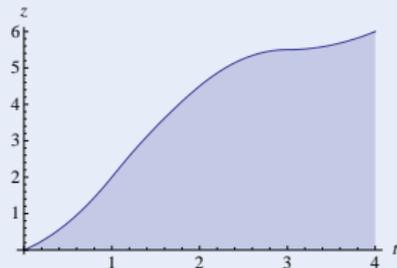
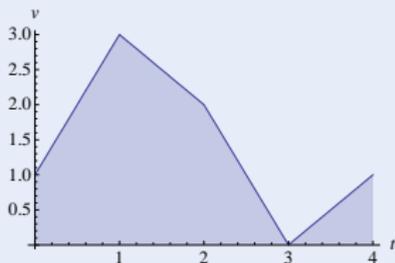
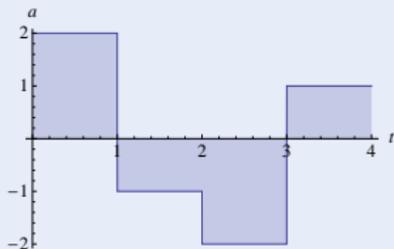
aplatzer@cs.cmu.edu  
Computer Science Department  
Carnegie Mellon University, Pittsburgh, PA



## Challenge (Hybrid Systems)

Fixed rule describing state evolution with both

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



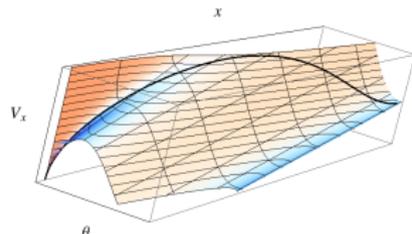
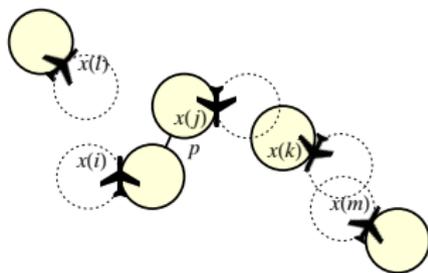
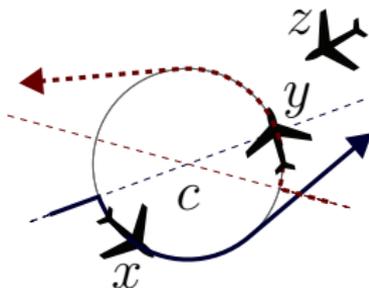
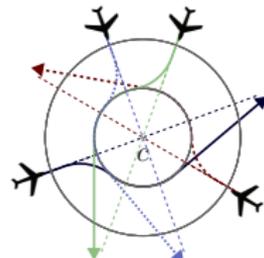
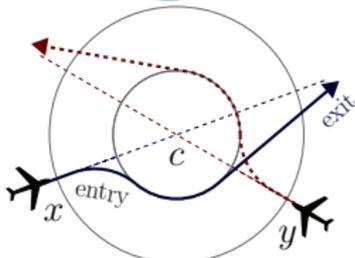
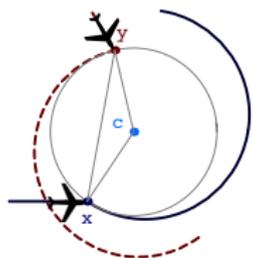
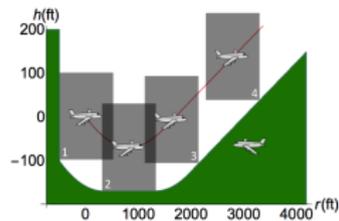
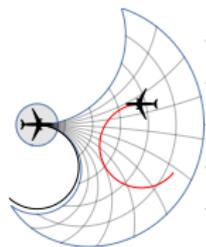
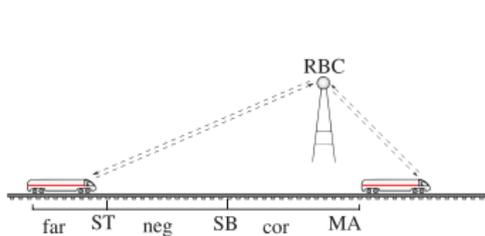
## Challenge (Hybrid Systems)

**Fixed rule** describing state evolution with both

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

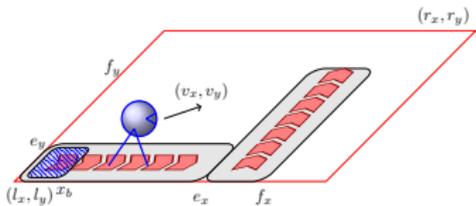
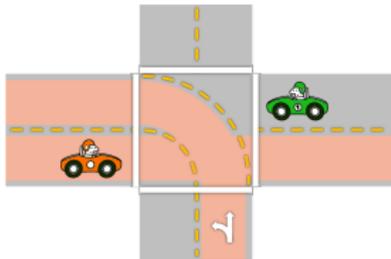
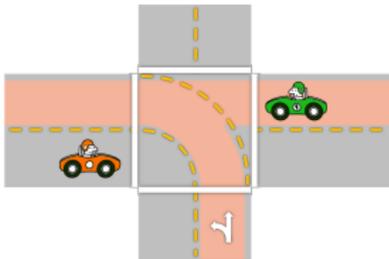
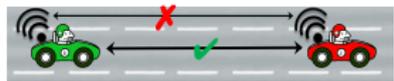
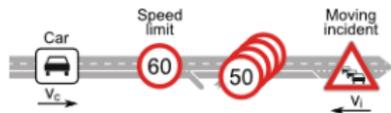
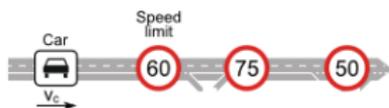
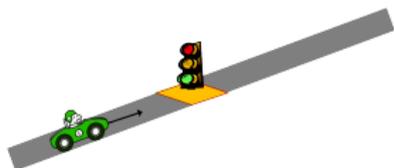
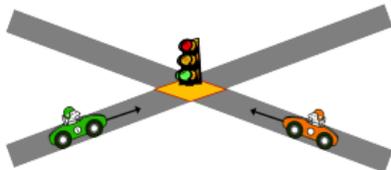
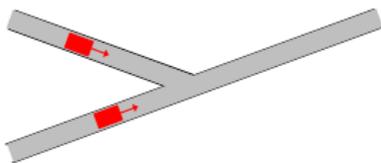
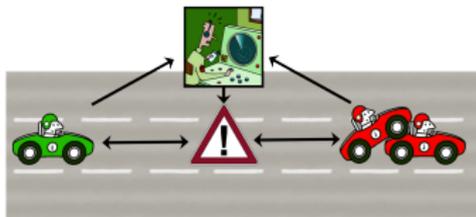
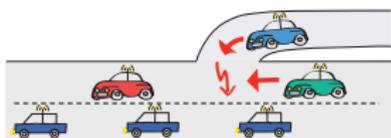
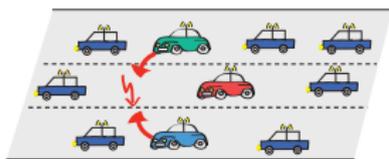


# Verified Hybrid Systems Applications



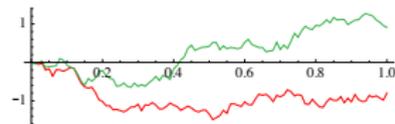
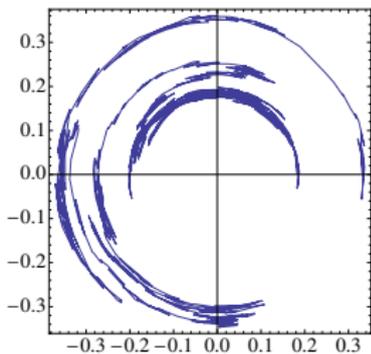
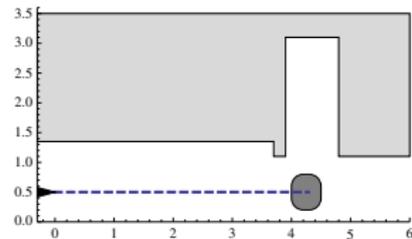
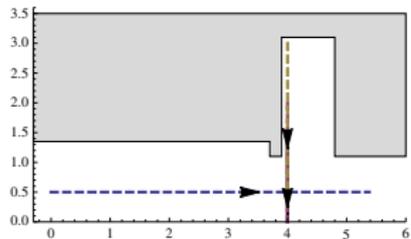
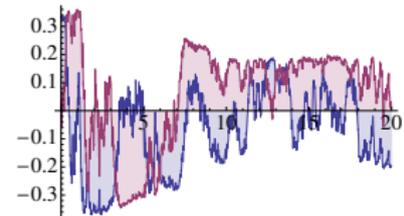
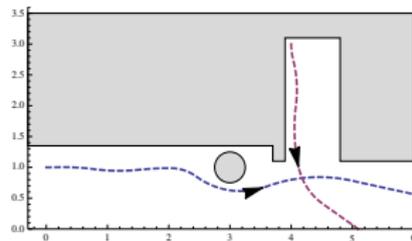
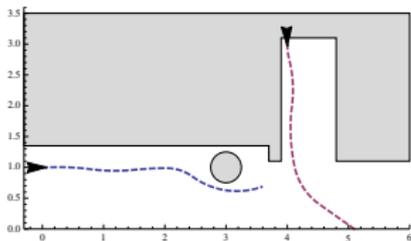
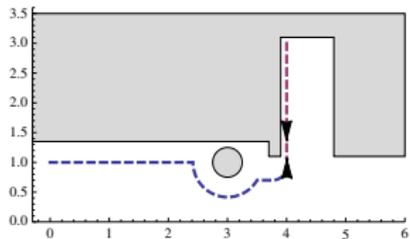
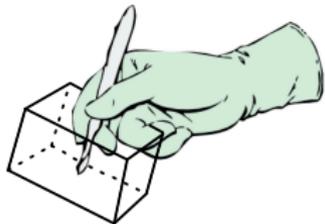
FEM'09, JAIS'14, TACAS'15, EMSOFT'15, CAV'08, FM'09, HSCC'11, HSCC'13, TACAS'14

# Verified Hybrid Systems Applications



FM'11, LMCS'12, ICCPS'12, ITSC'11, ITSC'13, IJCAR'12

# Verified Hybrid Systems Applications



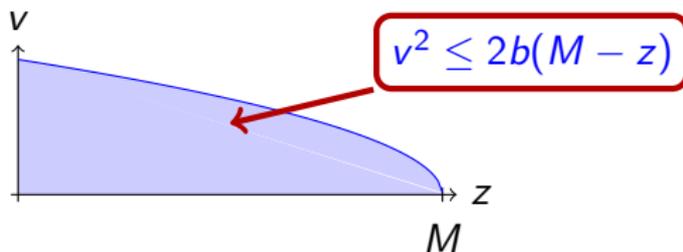
HSCC'13, RSS'13, CADE'12



Proof theory: hybrid = continuous = discrete

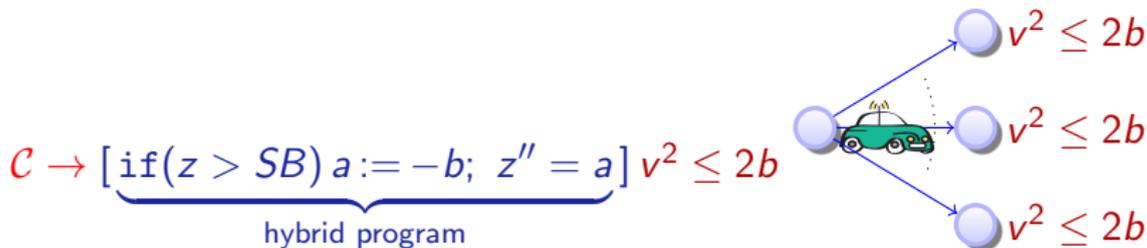
differential dynamic logic

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



differential dynamic logic

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



differential dynamic logic

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

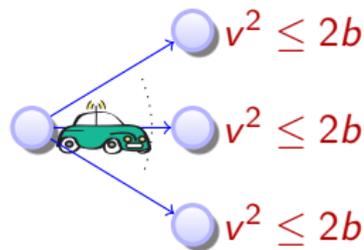


$$C \rightarrow \underbrace{[\text{if}(z > SB) a := -b; z'' = a]}_{\text{hybrid program}} v^2 \leq 2b$$

Initial  
condition

System  
dynamics

Post  
condition





Definition (Hybrid program  $\alpha$ )

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

Definition (d $\mathcal{L}$  Formula  $\phi$ )

$$\theta \geq \eta \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi \mid \exists x \phi \mid [\alpha]\phi \mid \langle \alpha \rangle \phi$$



# Differential Dynamic Logic dL: Syntax

Discrete Assign

Test Condition

Differential Equation

Nondet. Choice

Seq. Compose

Nondet. Repeat

Definition (Hybrid program  $\alpha$ )

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

Definition (dL Formula  $\phi$ )

$\theta \geq \eta \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi \mid \exists x \phi \mid [\alpha]\phi \mid \langle \alpha \rangle \phi$

All Reals

Some Reals

All Runs

Some Runs

Definition (Hybrid program semantics)

 $([\![\cdot]\!] : \text{HP} \rightarrow \wp(\mathcal{S} \times \mathcal{S}))$ 

$$\rho(x := f(x)) = \{(v, w) : w = v \text{ except } \llbracket x \rrbracket_w = \llbracket f(x) \rrbracket_v\}$$

$$\rho(?H) = \{(v, v) : v \models H\}$$

$$\rho(x' = f(x)) = \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \text{ for some duration } r\}$$

$$\rho(\alpha \cup \beta) = \rho(\alpha) \cup \rho(\beta)$$

$$\rho(\alpha; \beta) = \rho(\alpha) \circ \rho(\beta)$$

$$\rho(\alpha^*) = \bigcup_{n \in \mathbb{N}} \rho(\alpha^n)$$

Definition (dL semantics)

 $([\![\cdot]\!] : \text{Fml} \rightarrow \wp(\mathcal{S}))$ 

$$[\![\theta \geq \eta]\!] = \{v : \llbracket \theta \rrbracket_v \geq \llbracket \eta \rrbracket_v\}$$

$$[\![\neg\phi]\!] = [\![\phi]\!]^c$$

$$[\![\phi \wedge \psi]\!] = [\![\phi]\!] \cap [\![\psi]\!]$$

$$[\![\langle \alpha \rangle \phi]\!] = \rho(\alpha) \circ [\![\phi]\!] = \{v : w \models \phi \text{ for some } w : (v, w) \in \rho(\alpha)\}$$

$$[\![[\alpha]\phi]\!] = [\![\neg\langle \alpha \rangle \neg\phi]\!] = \{v : w \models \phi \text{ for all } w : (v, w) \in \rho(\alpha)\}$$

$$[\![\exists x \phi]\!] = \{v : v'_x \in [\![\phi]\!] \text{ for some } r \in \mathbb{R}\}$$

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

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

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

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

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

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

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

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

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

$$\text{G} \quad \frac{\phi}{[\alpha]\phi}$$

$$\text{MP} \quad \frac{\phi \rightarrow \psi \quad \phi}{\psi}$$

$$\forall \quad \frac{\phi}{\forall x \phi}$$



$$\text{G} \quad \frac{\phi}{[\alpha]\phi}$$

$$\text{MP} \quad \frac{\phi \rightarrow \psi \quad \phi}{\psi}$$

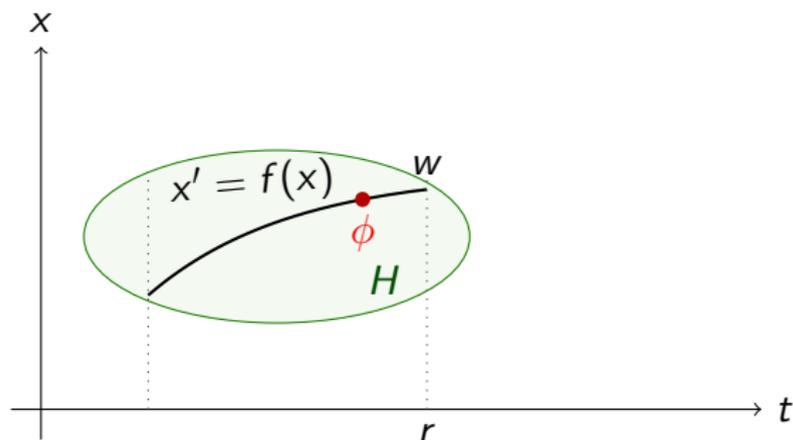
$$\forall \quad \frac{\phi}{\forall x \phi}$$

$$\text{B} \quad \forall x [\alpha]\phi \rightarrow [\alpha]\forall x \phi \quad (x \notin \alpha)$$

$$\text{V} \quad \phi \rightarrow [\alpha]\phi \quad (FV(\phi) \cap BV(\alpha) = \emptyset)$$

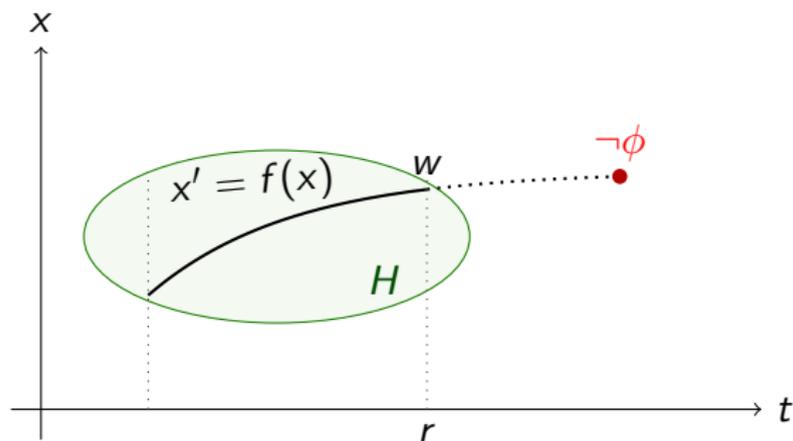
$$[\&] \quad [x' = f(x) \& H]\phi$$

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



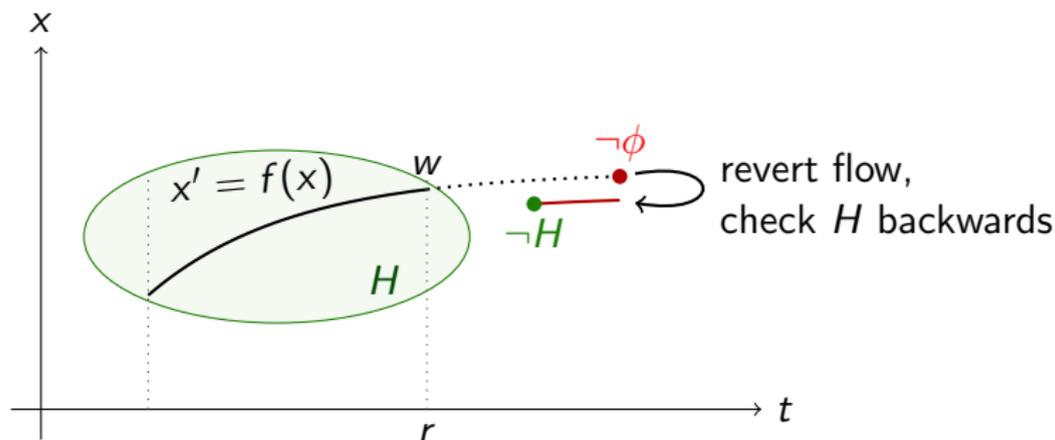
$$[\&] \quad [x' = f(x) \& H]\phi$$

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



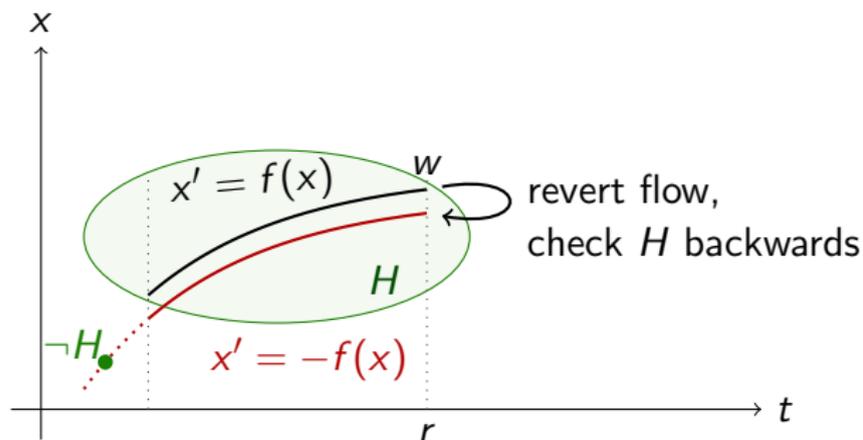
$$[\&] \quad [x' = f(x) \& H]\phi$$

$$\leftrightarrow [x' = f(x)]([x' = -f(x)](H) \rightarrow \phi)$$



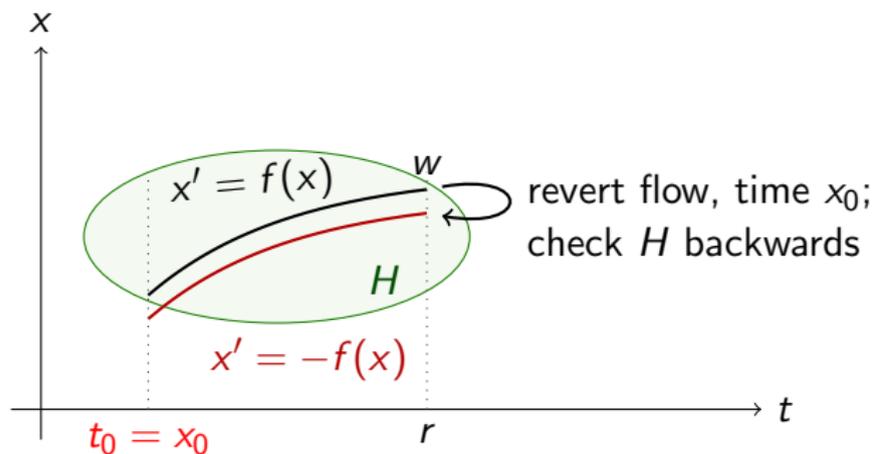
$$[\&] \quad [x' = f(x) \& H]\phi$$

$$\leftrightarrow [x' = f(x)]([x' = -f(x)](H) \rightarrow \phi)$$



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

$$\leftrightarrow \forall t_0 = x_0 [x' = f(x)] ([x' = -f(x)] (x_0 \geq t_0 \rightarrow H) \rightarrow \phi)$$

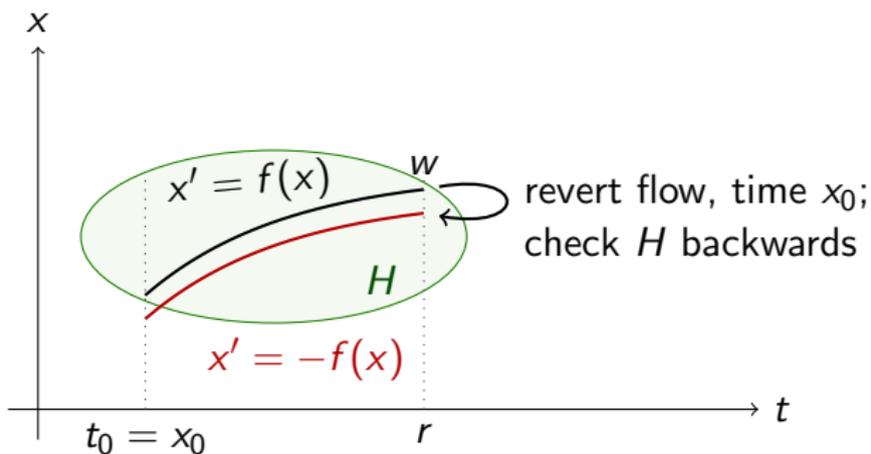




# “There and Back Again” Axiom of $d\mathcal{L}$

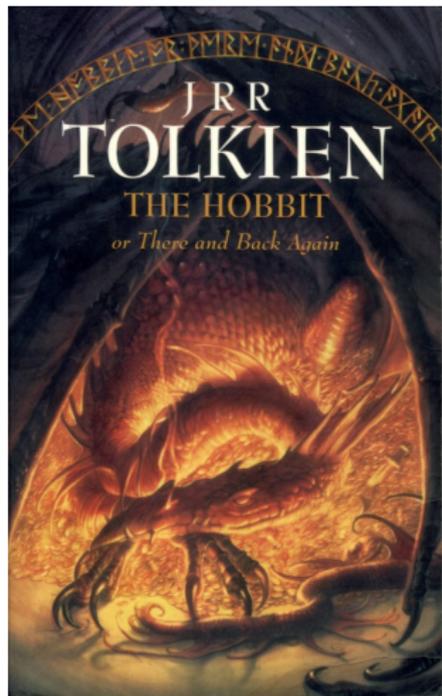
$$[\&] \quad [x' = f(x) \& H] \phi$$

$$\leftrightarrow \forall t_0 = x_0 [x' = f(x)] ([x' = -f(x)] (x_0 \geq t_0 \rightarrow H) \rightarrow \phi)$$



Lemma

*Evolution domain axiomatizable*



## Theorem (Soundness)

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

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

What about the converse?

## Theorem (Soundness)

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

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

What about the converse?

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

## Theorem (Soundness)

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

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

What about the converse?

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

## Theorem (Soundness)

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

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

What about the converse?

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

## Theorem (Soundness)

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

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

What about the converse?

$(s := s + 2n + 1; n := n + 1)^*$	$\rightsquigarrow$	$s = n^2$
$x' = 5$	$\rightsquigarrow$	$x(t) = 5t + x_0$
$x' = x$	$\rightsquigarrow$	$x(t) = x_0 e^t$
$x'' = -x$	$\rightsquigarrow$	$x(t) = x_0 \cos t + x'_0 \sin t$

## Theorem (Relative Completeness / Continuous)

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

[▶ Proof Outline](#)

$$\models \phi \text{ iff } \text{Taut}_{\text{FOD}} \vdash \phi$$

## Theorem (Relative Completeness / Continuous)

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

[▶ Proof Outline](#)

$$\models \phi \text{ iff } \text{Taut}_{\text{FOD}} \vdash \phi$$

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

## Theorem (Relative Completeness / Continuous)

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

[▶ Proof Outline](#)

$$\models \phi \text{ iff } \text{Taut}_{\text{FOD}} \vdash \phi$$

## Corollary (Proof-theoretical Alignment)

proving hybrid systems = proving continuous dynamical systems!

## Corollary (Compositionality)

hybrid systems can be verified by recursive decomposition

## Theorem (Relative Completeness / Continuous)

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

[▶ Proof Outline](#)

$$\models \phi \text{ iff } \text{Taut}_{FOD} \vdash \phi$$

## Theorem (Relative Completeness / Discrete)

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

[▶ Proof Outline](#)

$$\models \phi \text{ iff } \text{Taut}_{DL} \vdash \phi$$

## Theorem (Relative Completeness / Continuous)

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

[▶ Proof Outline](#)

$$\models \phi \text{ iff } \text{Taut}_{FOD} \vdash \phi$$

## Theorem (Relative Completeness / Discrete)

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

[▶ Proof Outline](#)

$$\models \phi \text{ iff } \text{Taut}_{DL} \vdash \phi$$

## Corollary (Complete Proof-theoretical Alignment)

**hybrid = continuous = discrete**

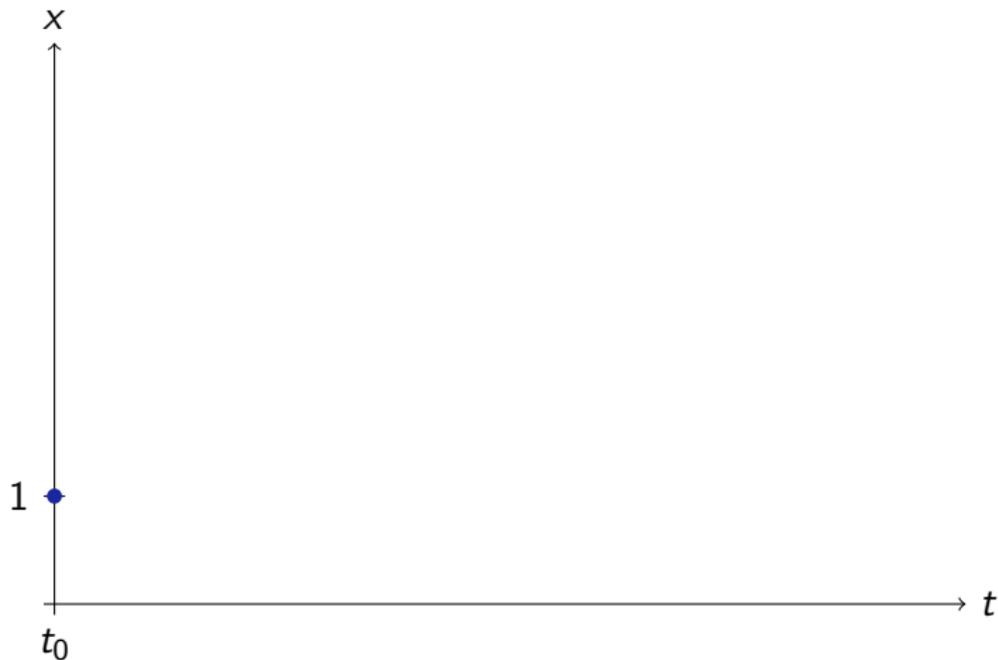
## Corollary (Interdisciplinary Integrability)

“Discrete computer science + continuous control are integrable”

# Proof of “hybrid = continuous = discrete”



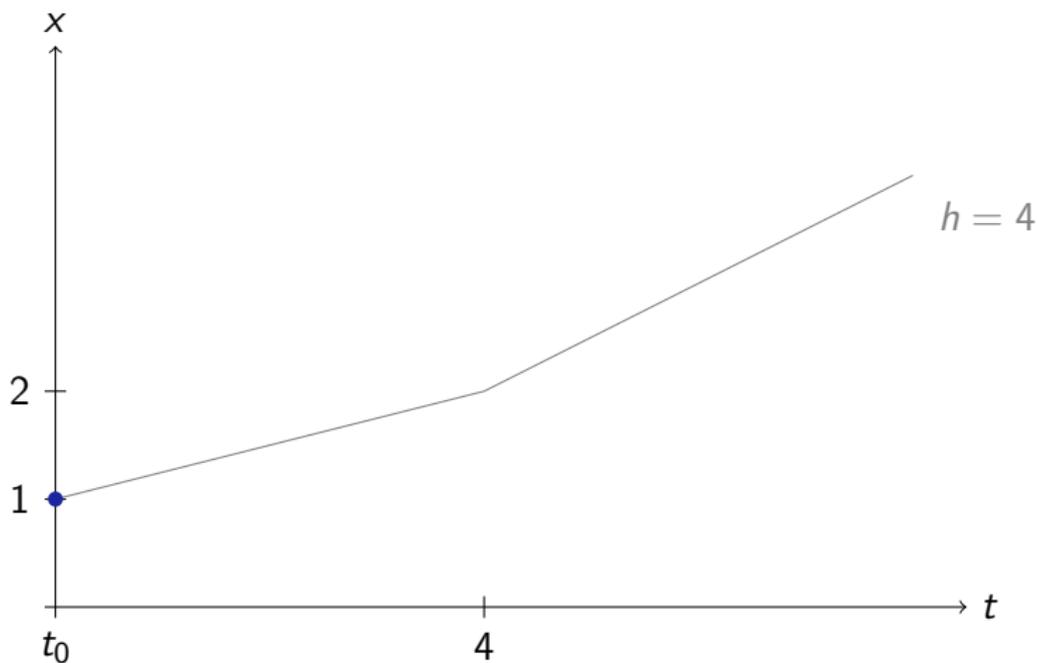
$$[x' = \frac{x}{4}]F$$



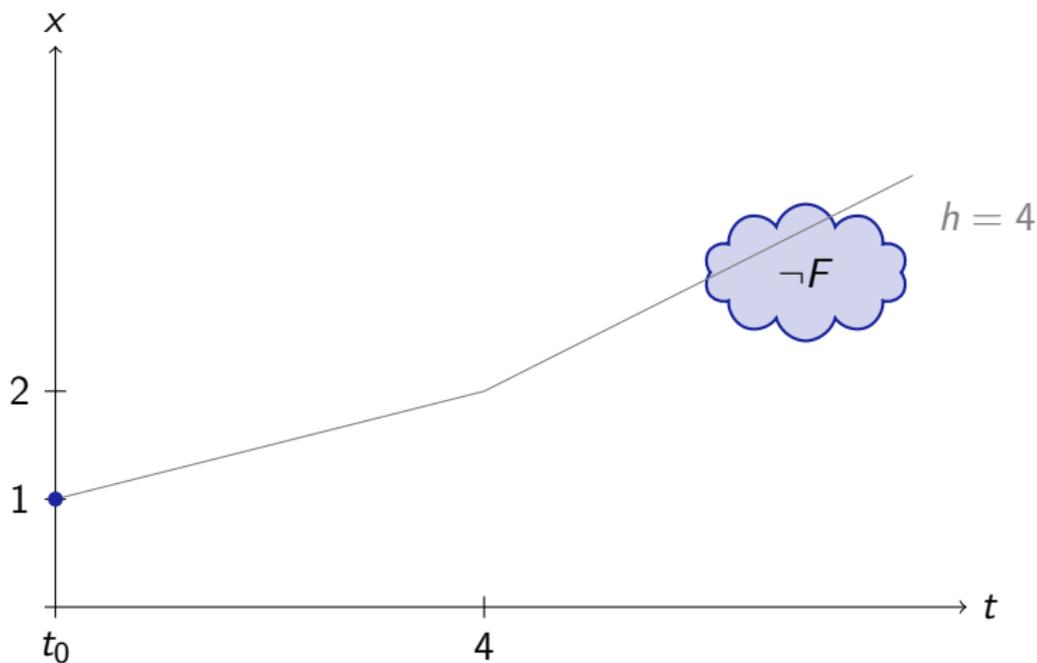


$$[x' = \frac{x}{4}]F$$

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



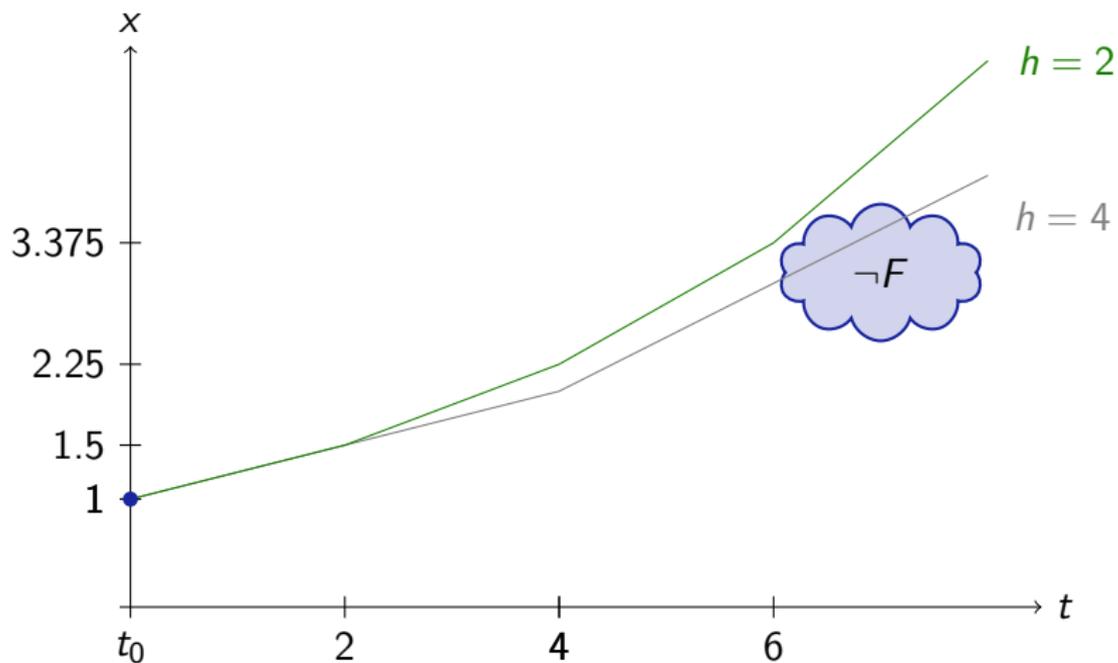
$$[x' = \frac{x}{4}]F \not\Rightarrow [(x := x + h\frac{x}{4})^*]F$$





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

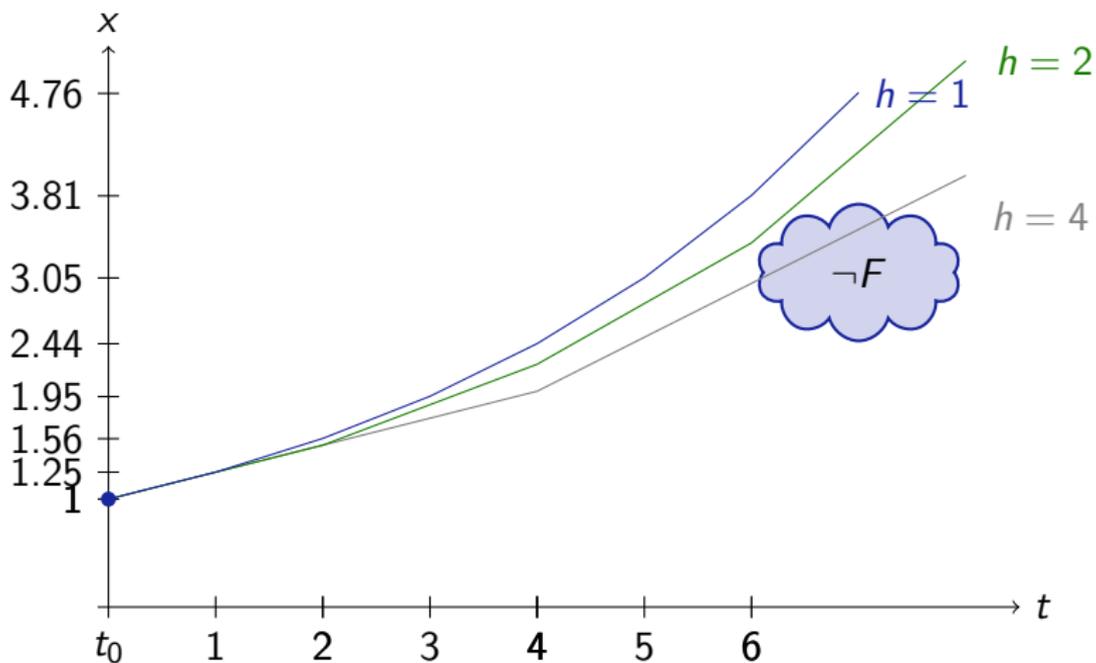
$$[(x := x + h\frac{x}{4})^*]F$$





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

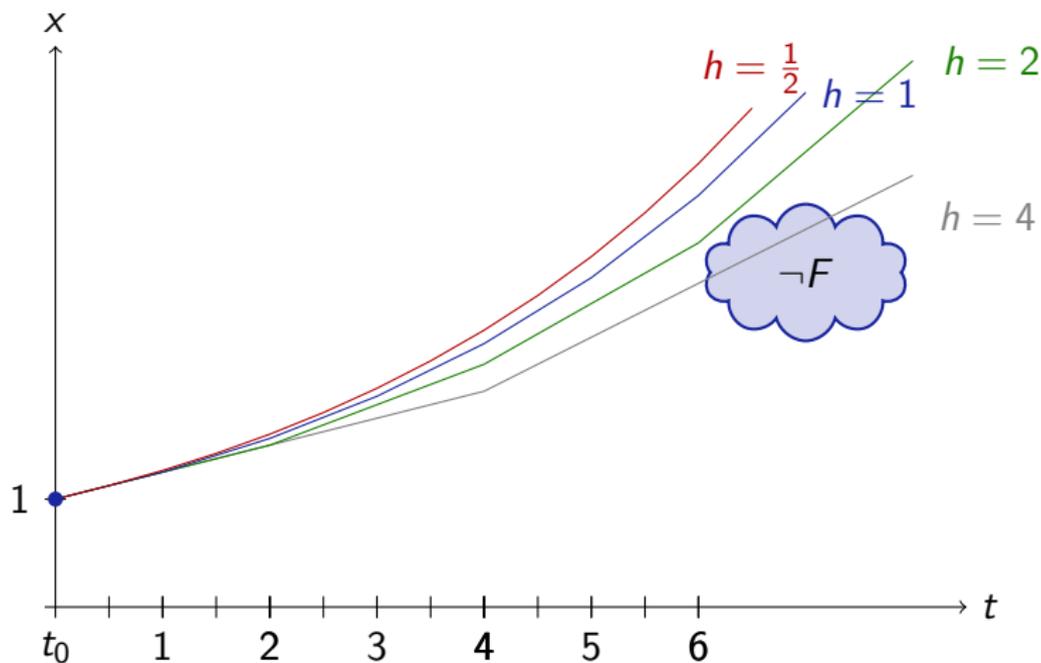
$$[(x := x + h\frac{x}{4})^*]F$$





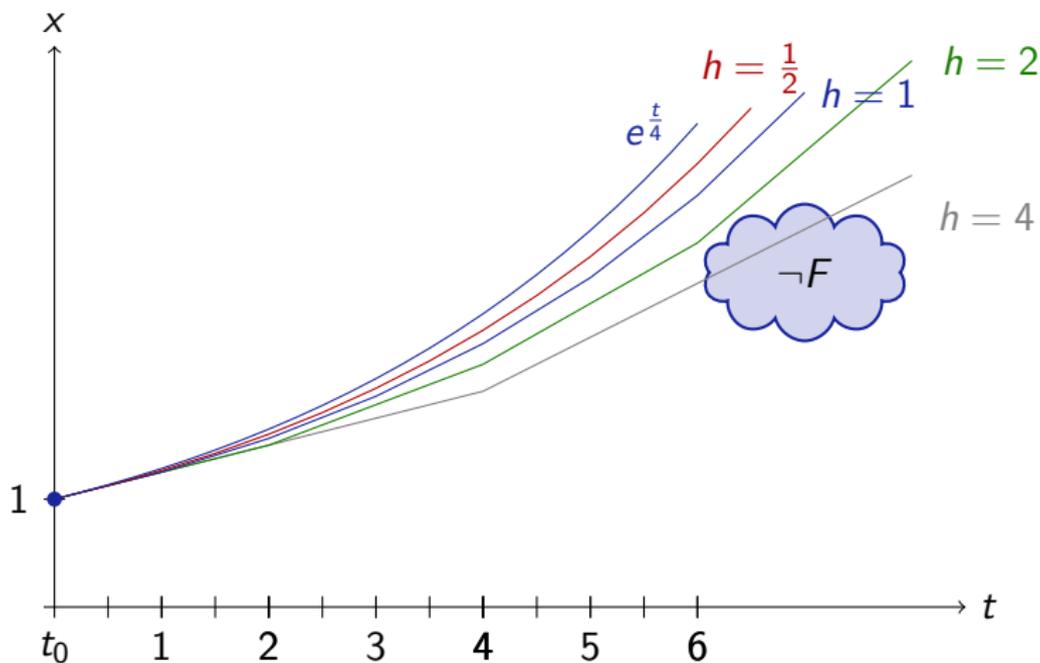
$$[x' = \frac{x}{4}]F$$

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



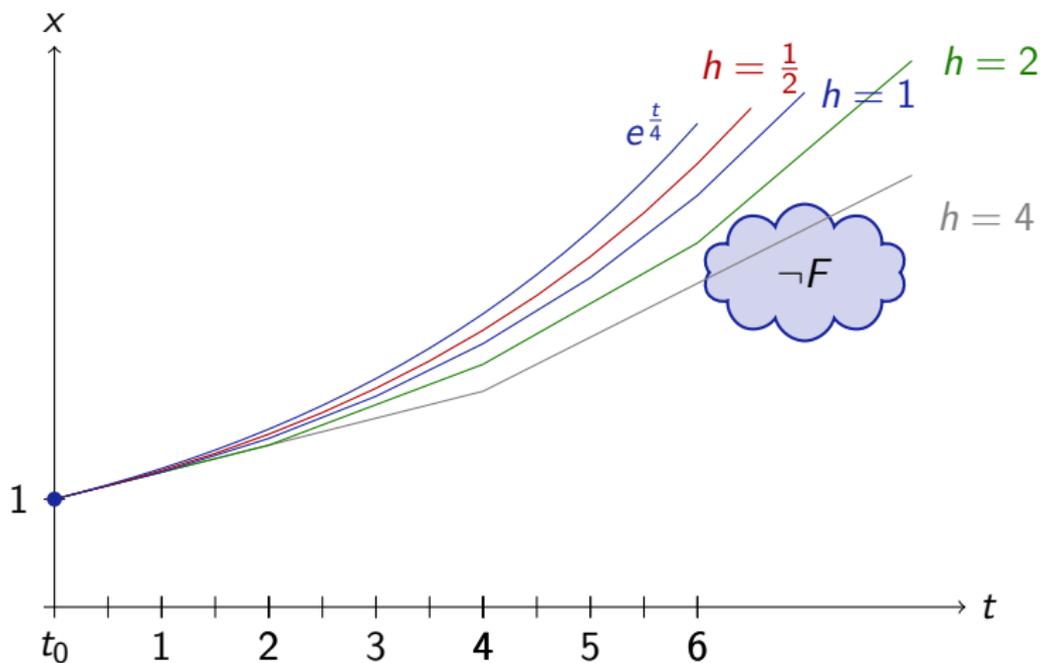


$$[x' = \frac{x}{4}]F \quad \text{vs.} \quad [(x := x + h\frac{x}{4})^*]F$$

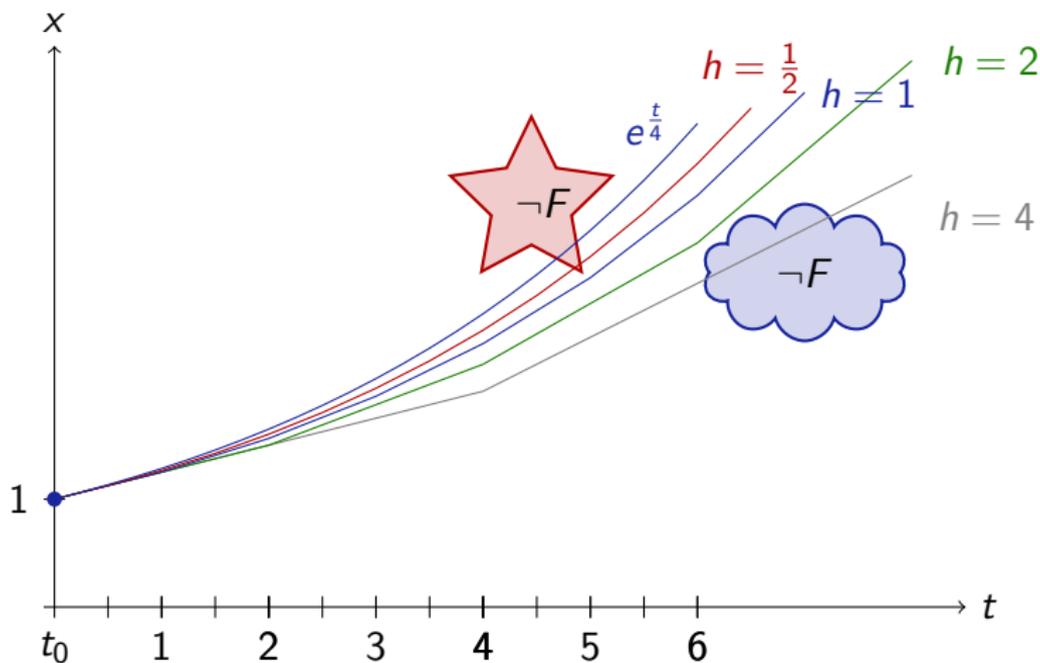




$$[x' = \frac{x}{4}]F \not\Rightarrow [(x := x + h\frac{x}{4})^*]F$$



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



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

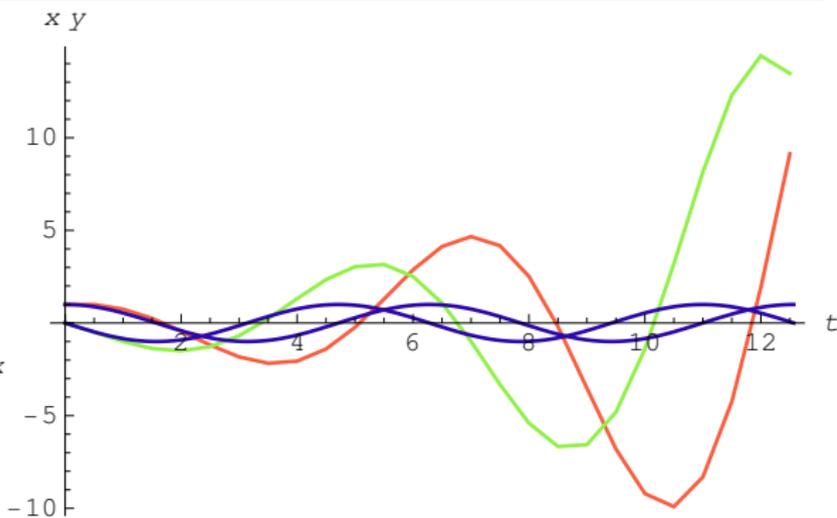
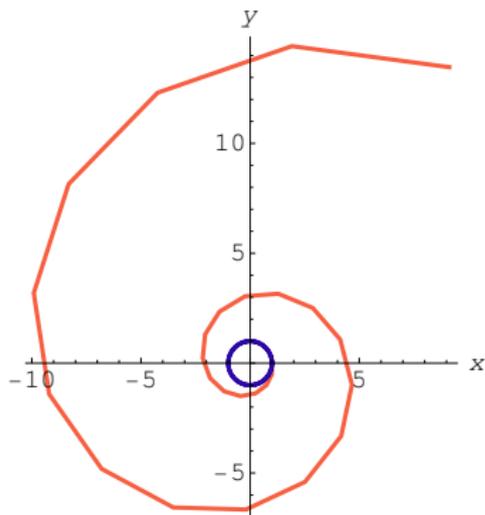


$$\triangleleft [x' = f(x)]F$$

$$\triangleleft \leftarrow \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*]F$$

Example (Insufficient, not global)

$$\models x^2 + y^2 \leq 1 \rightarrow [x' = y, y' = -x]x^2 + y^2 \leq 1.1$$





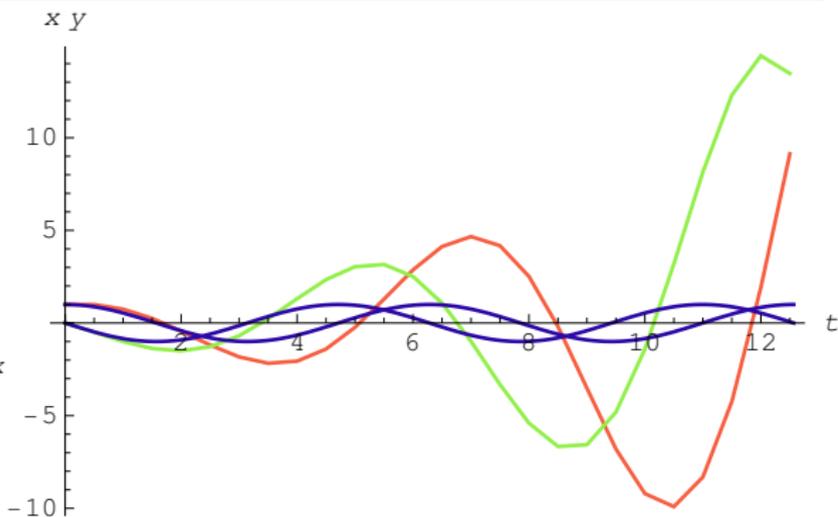
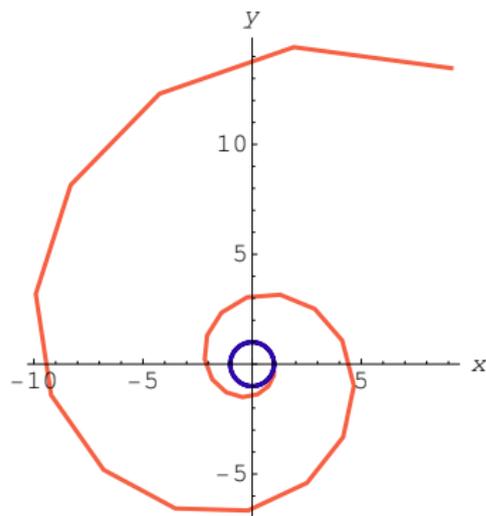
$$\overleftarrow{\Delta} \quad [x' = f(x)]F$$

$$\leftarrow \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*]F$$

(closed)

Example (Unsound for open  $F$ , only in closure)

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



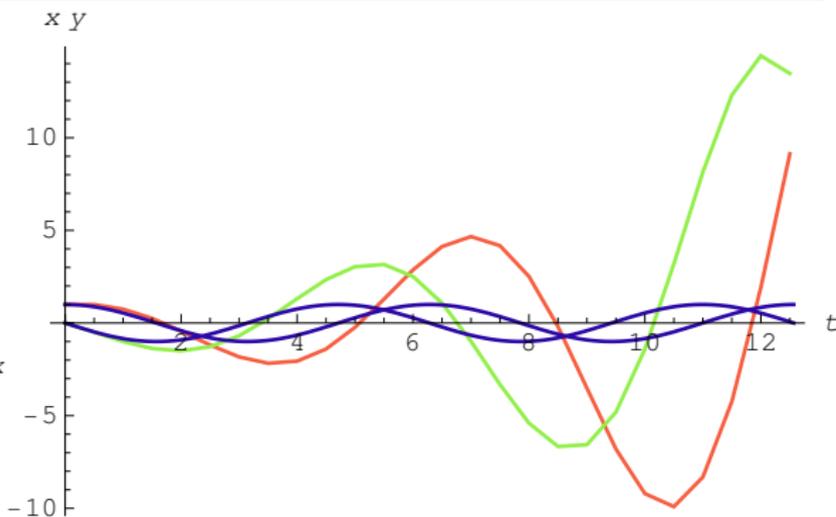
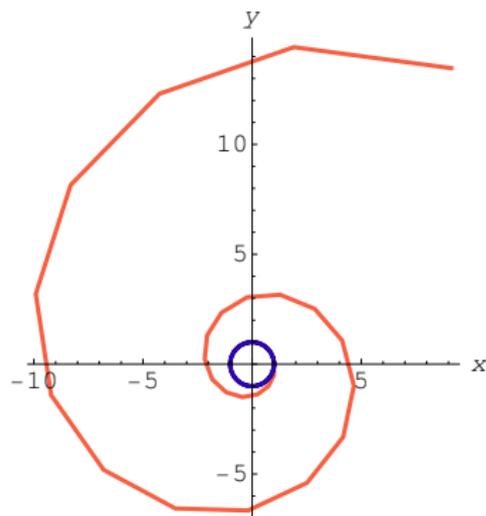


$$\overleftarrow{\Delta} \quad [x' = f(x)]F \quad \text{(closed)}$$

$$\leftarrow \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*]F$$

Example (Insufficient, not global)

$$\models x^2 + y^2 \leq 1 \rightarrow [x' = y, y' = -x]x^2 + y^2 \leq 1.1$$



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

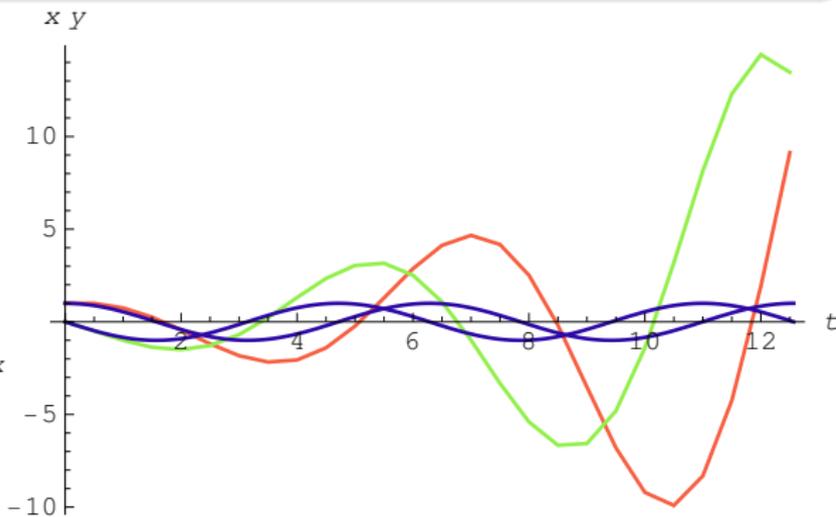
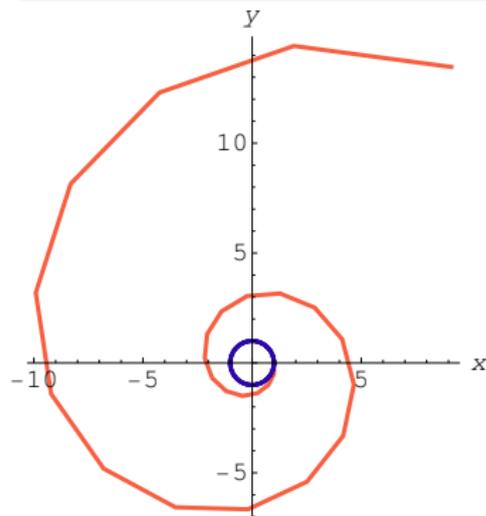


$$\vec{\Delta} [x' = f(x)]F$$

$$\rightarrow \forall t \geq 0 \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*](t \geq 0 \rightarrow F)$$

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

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

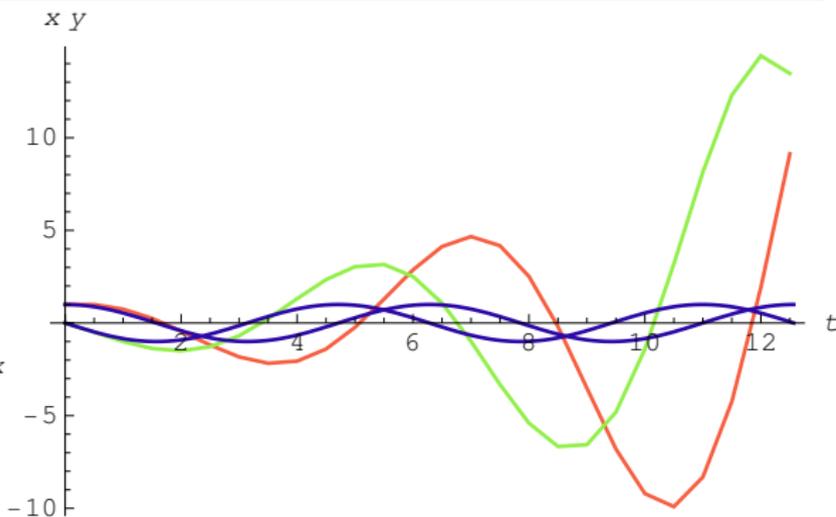
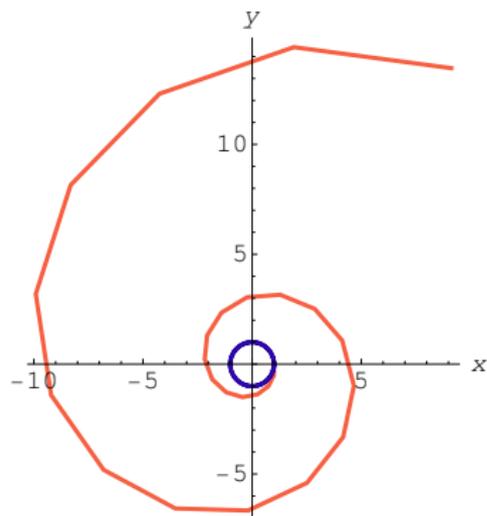




$$\vec{\Delta} [x' = f(x)]F \rightarrow \forall t \geq 0 \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*(t \geq 0 \rightarrow F)] \quad (\text{open})$$

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

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





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

$$\begin{aligned} \Delta \quad [x' = f(x)]F \\ \Leftrightarrow \forall t \geq 0 \exists \epsilon > 0 \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*](t \geq 0 \rightarrow \neg \mathcal{U}_\epsilon(\neg F)) \end{aligned}$$

Example ()

$$\models x^2 + y^2 < 1 \rightarrow [x' = y, y' = -x]x^2 + y^2 < 1.1$$

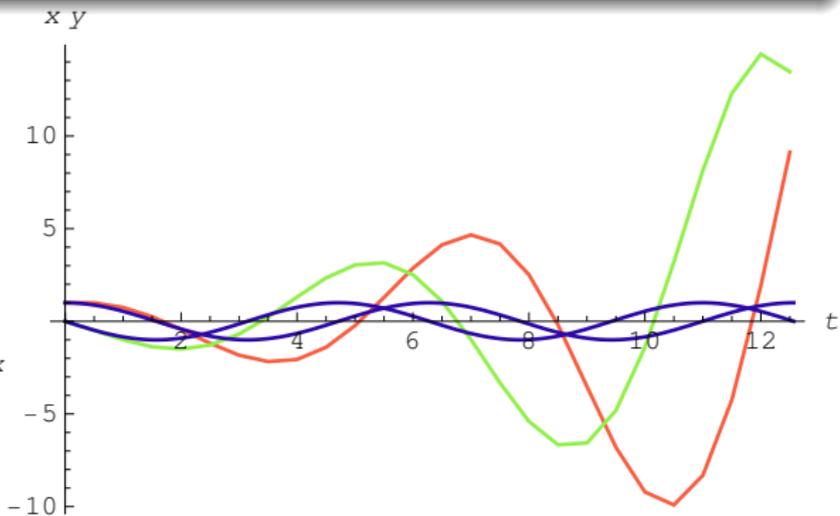
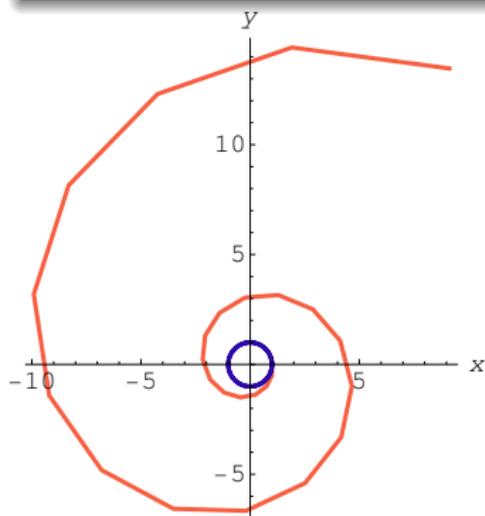


$$\overleftrightarrow{\Delta} [x' = f(x)]F$$

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

Example (Insufficient for closed  $F$ )

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



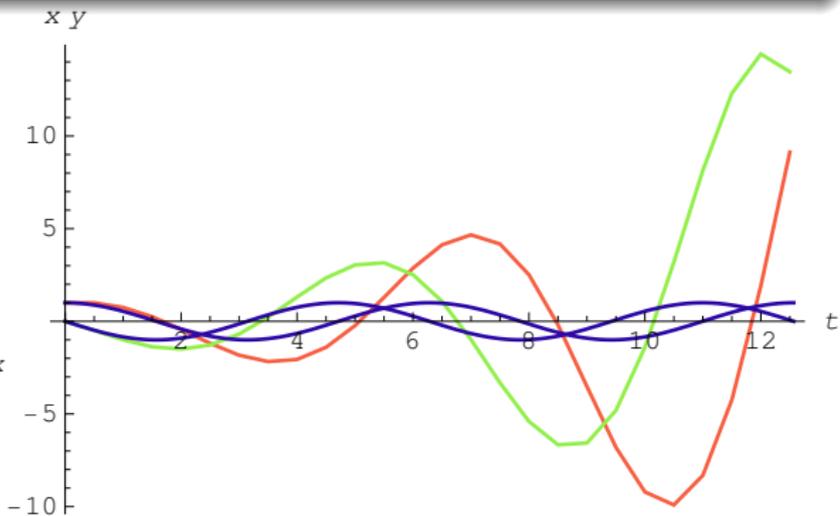
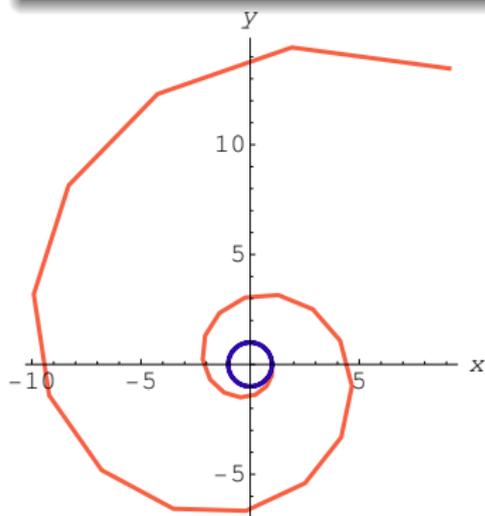


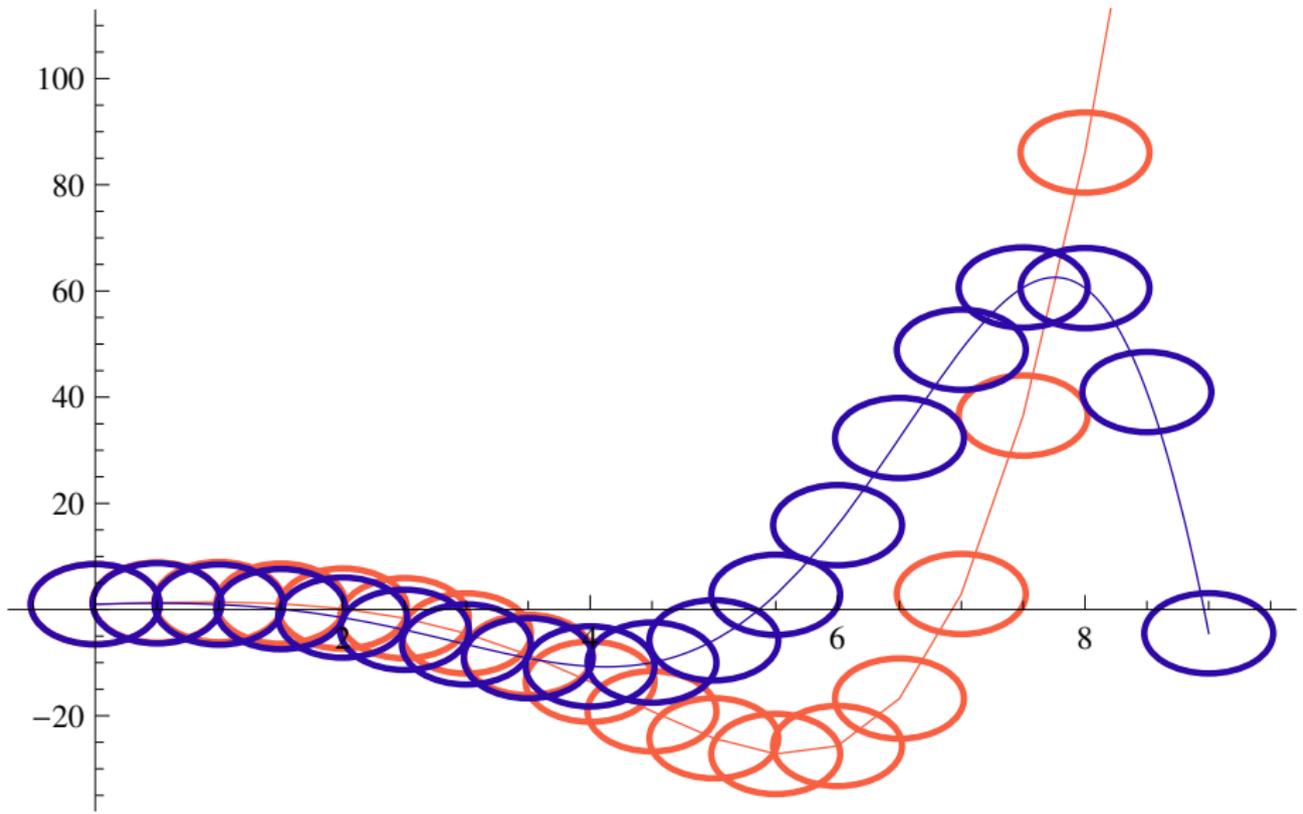
$$\overleftrightarrow{\Delta} [x' = f(x)]F \quad (\text{open})$$

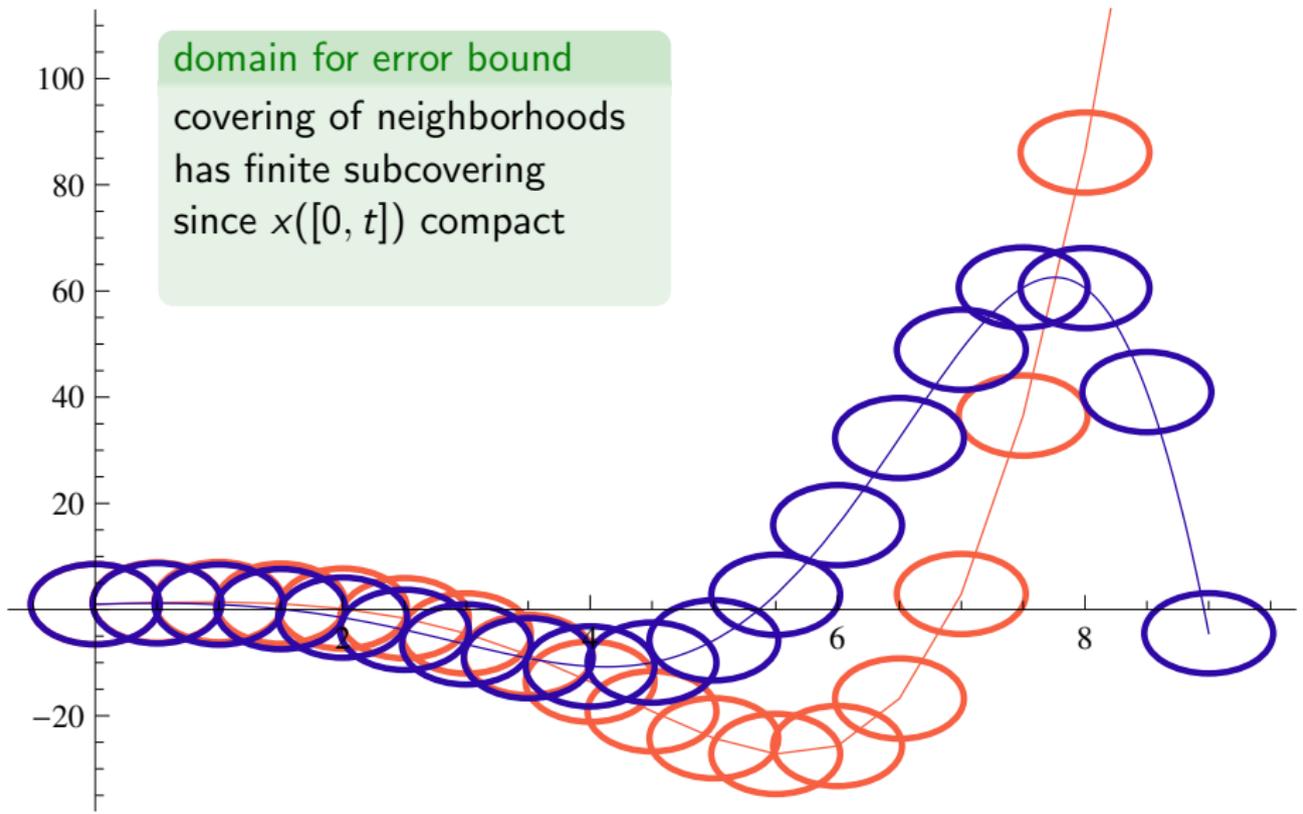
$$\leftrightarrow \forall t \geq 0 \exists \epsilon > 0 \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*](t \geq 0 \rightarrow \neg \mathcal{U}_\epsilon(\neg F))$$

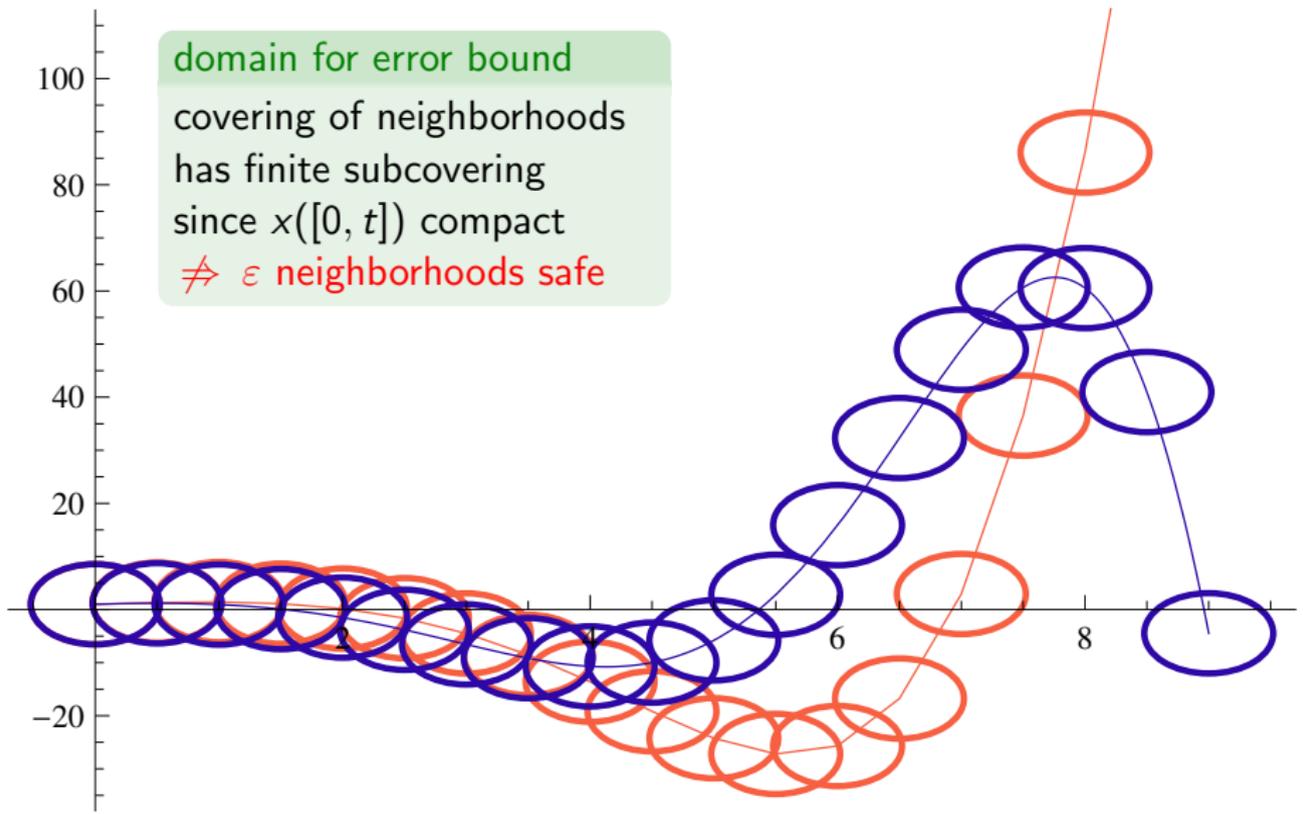
Example (Insufficient for closed  $F$ )

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









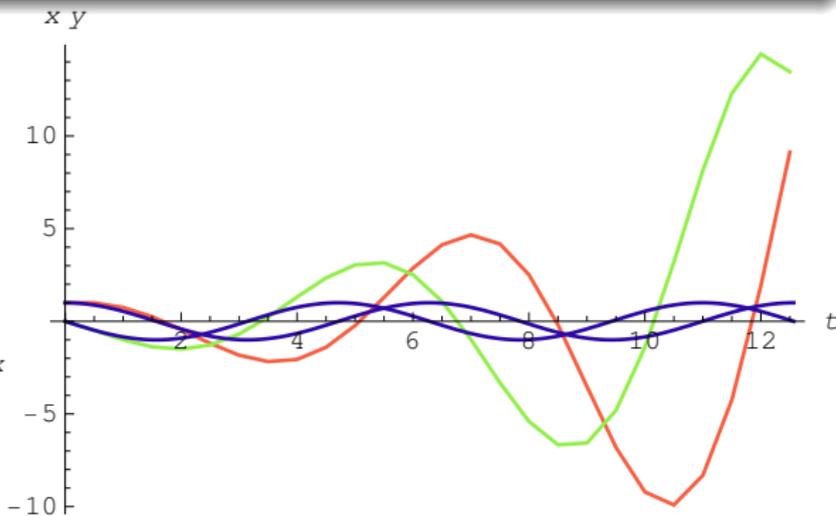
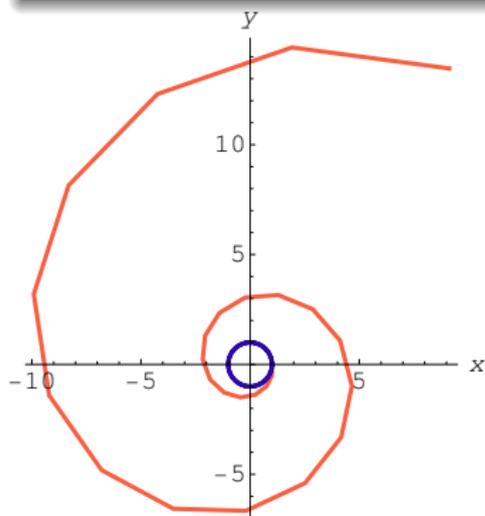
$\Leftrightarrow \Delta$  axiom for open  $F$ , but  $F$  may be closed



$$\begin{aligned} \Delta & [x' = f(x)]F && \text{(open)} \\ \Leftrightarrow & \forall t \geq 0 \exists \epsilon > 0 \exists h_0 > 0 \forall 0 < h < h_0 [(x := x + hf(x))^*](t \geq 0 \rightarrow \neg \mathcal{U}_\epsilon(\neg F)) \end{aligned}$$

Example (Insufficient for closed  $F$ )

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



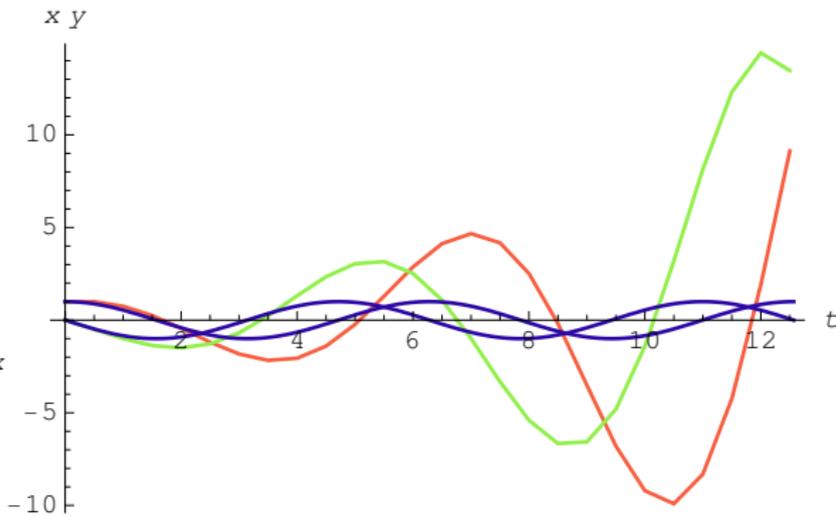
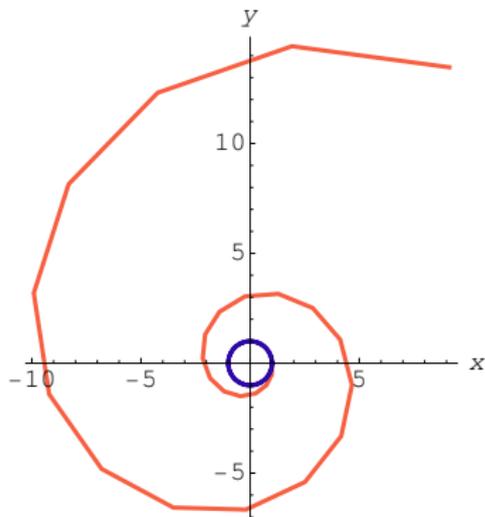
$$\dot{U} \quad [x' = f(x)]F \leftrightarrow \forall \epsilon > 0 [x' = f(x)]\mathcal{U}_\epsilon(F)$$

( $\Leftarrow$  B,V,G,K)

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

Example (Closed  $\leadsto$  Quantified Open)

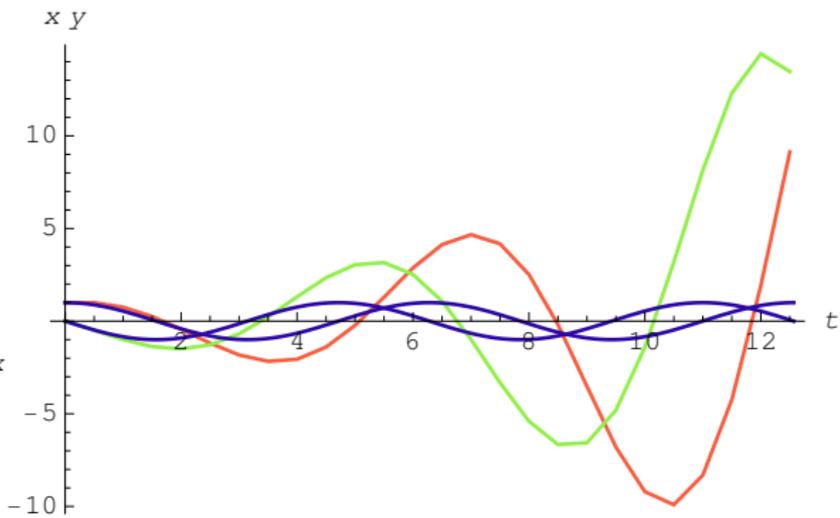
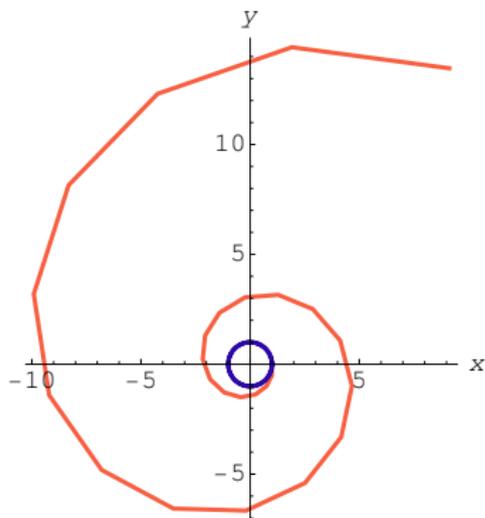
$$\models x^2 + y^2 \leq 1 \rightarrow [x' = y, y' = -x]x^2 + y^2 \leq 1$$



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

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

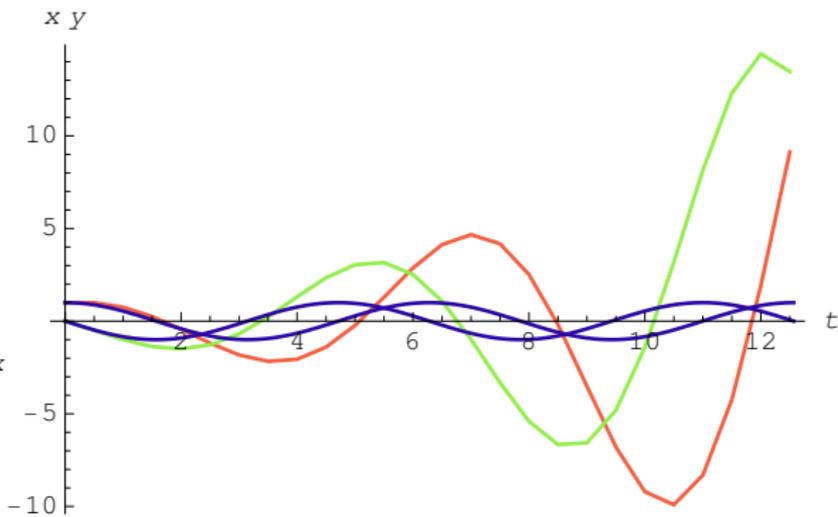
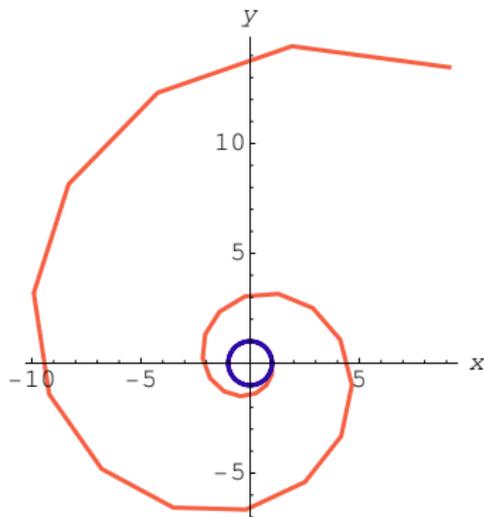
$$\models x^2 + y^2 \leq 1 \rightarrow [x' = y, y' = -x] \forall \epsilon > 0 x^2 + y^2 < 1 + \epsilon$$



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

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

$$\models x^2 + y^2 \leq 1 \rightarrow \forall \epsilon > 0 [x' = y, y' = -x]x^2 + y^2 < 1 + \epsilon$$



$\leftrightarrow$   
 $\Delta$  axiom for open/closed  $F$ , but otherwise?

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

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



$$\Box \wedge [\alpha](O \wedge C) \leftrightarrow [\alpha]O \wedge [\alpha]C \quad (\Leftarrow K)$$

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

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



$$\Box \wedge [\alpha](O \wedge C) \leftrightarrow [\alpha]O \wedge [\alpha]C \quad (\Leftarrow K)$$

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

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

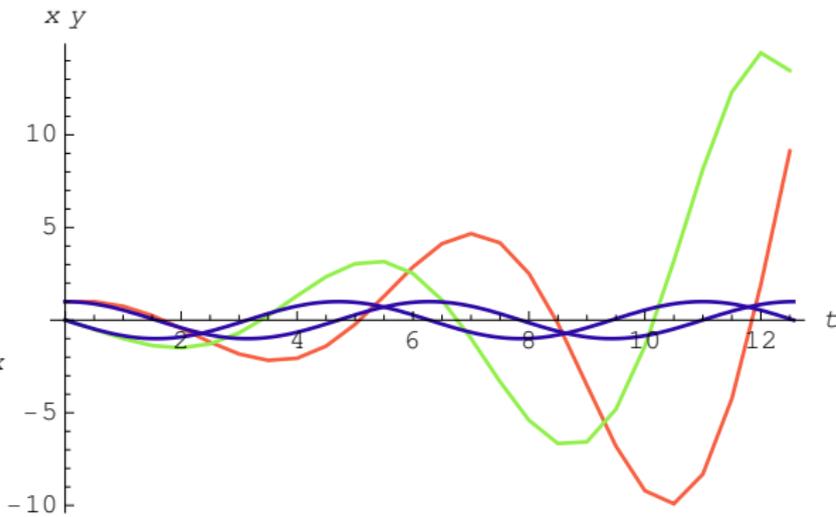
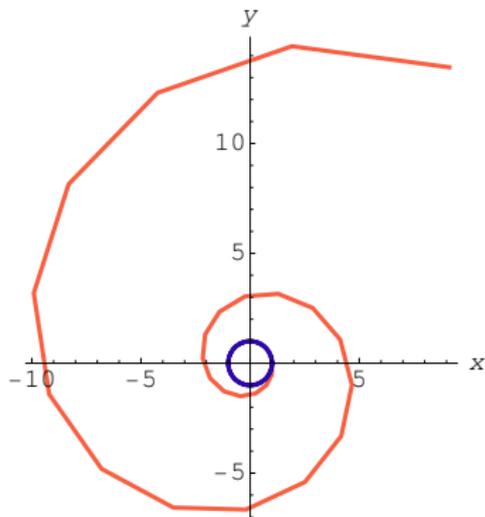
$$\checkmark \quad [x' = f(x)](O \vee C) \leftrightarrow \forall \epsilon > 0 [x' = f(x)](O \vee \mathcal{U}_\epsilon(C)) \quad (\Leftarrow \text{B,V,G,K})$$



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

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

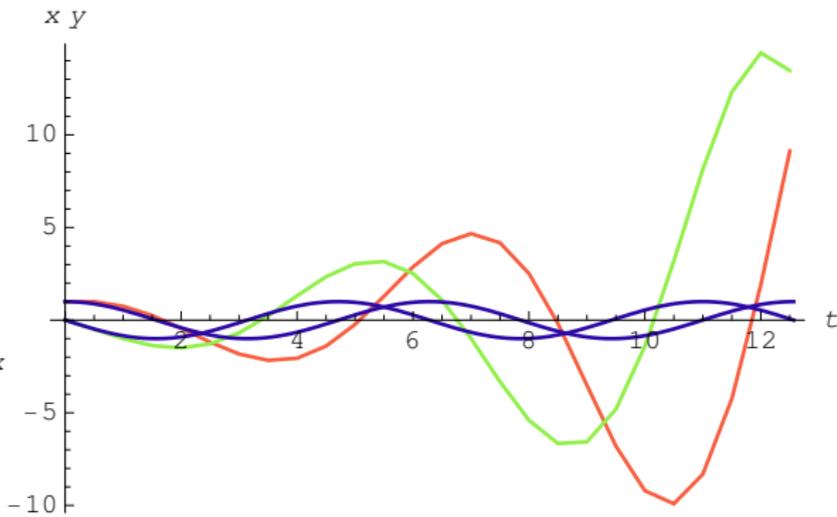
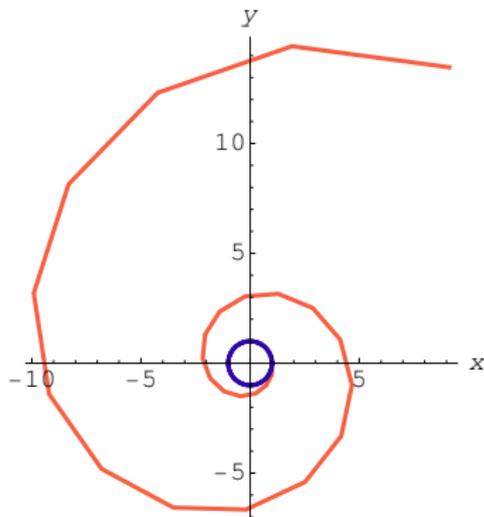
$$\models O \vee C \rightarrow [x' = y, y' = -x](O \vee C)$$



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

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

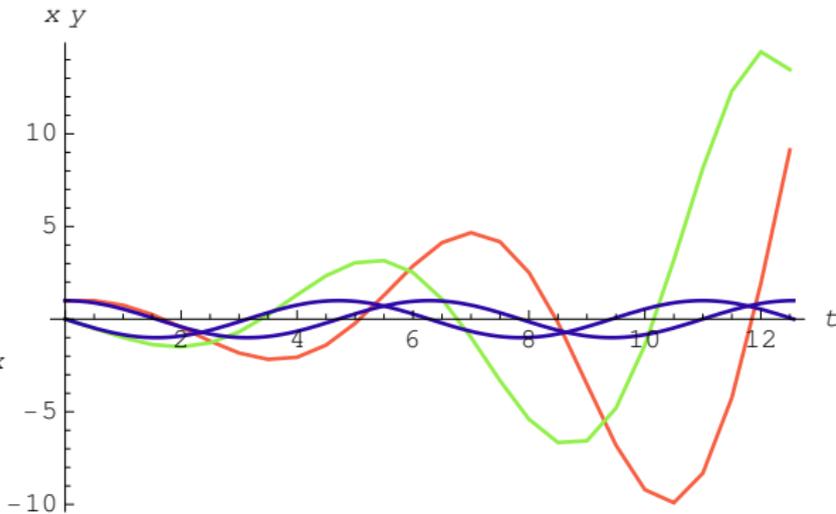
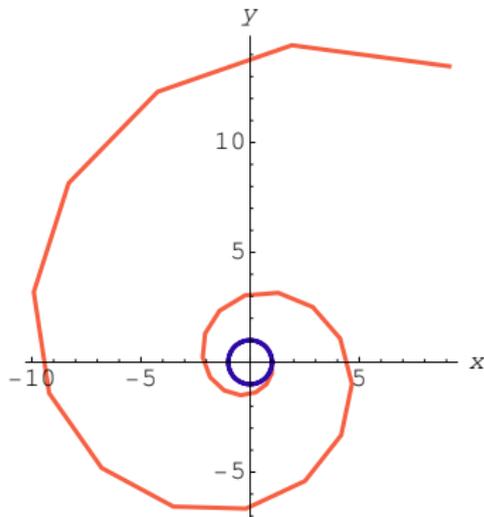
$$\models O \vee C \rightarrow [x' = y, y' = -x](O \vee \forall \epsilon > 0 \mathcal{U}_\epsilon(C))$$



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

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

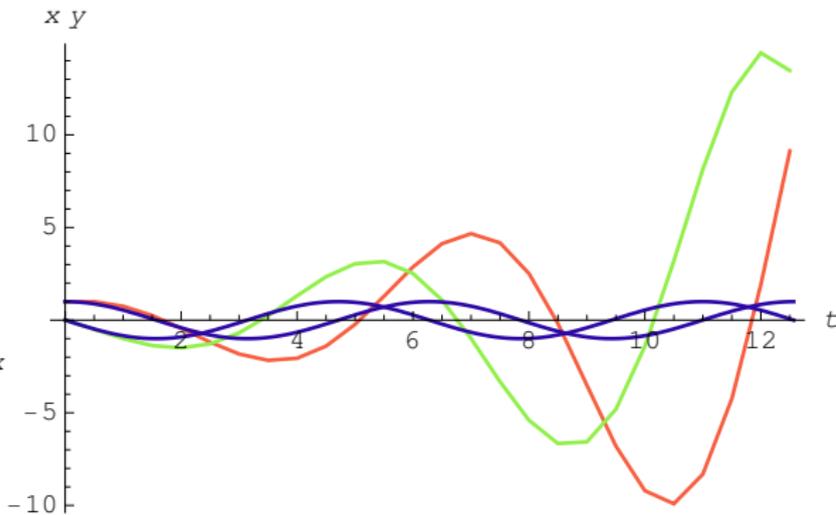
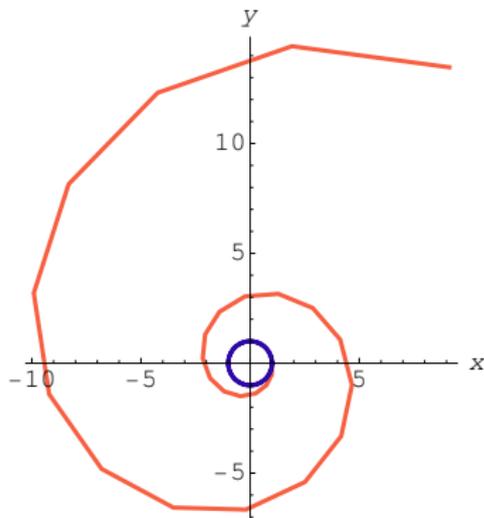
$$\models O \vee C \rightarrow [x' = y, y' = -x] \forall \epsilon > 0 (O \vee \mathcal{U}_\epsilon(C))$$



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

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

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



$\Delta$  axiom for semialgebraic  $F$ , but otherwise?

## Theorem (Relative Completeness / Continuous)

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

[▶ Proof Outline 6p](#)

$\models \phi$  implies  $\text{Taut}_{FOD} \vdash \phi$

## 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](#)

$\models \phi$  implies  $\text{Taut}_{DL} \vdash \phi$

## Proof Sketch.

Talked about 0-order semialgebraic

LICS'12 proves  $\forall, \exists \dots$

LICS'12 proves  $[\alpha], \langle \alpha \rangle$  with hybrid system  $\alpha \dots$

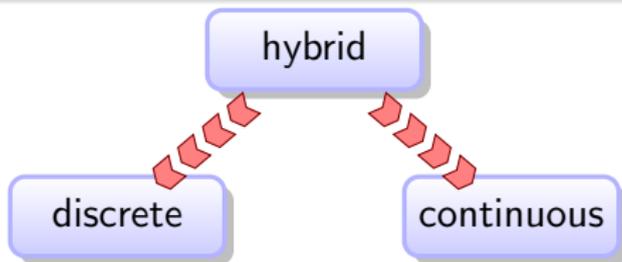
LICS'12 proves nesting  $\dots$



## Theorem (Equi-expressibility)

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

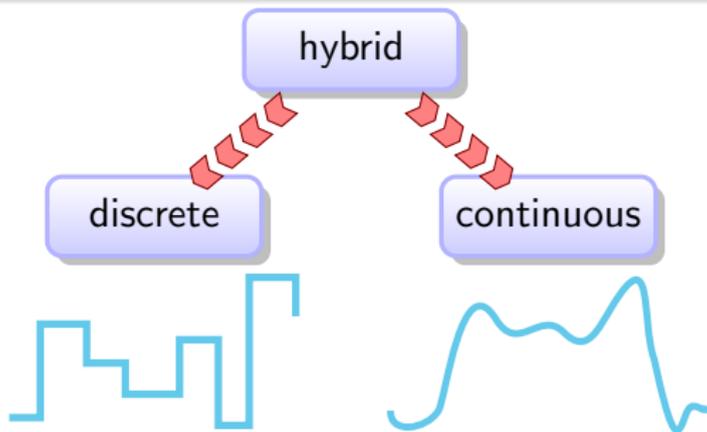
$$\begin{aligned}\forall\phi \exists\phi^b \in FOD &\models \phi \leftrightarrow \phi^b \\ \forall\phi \exists\phi^\# \in DL &\models \phi \leftrightarrow \phi^\#\end{aligned}$$



## Theorem (Equi-expressibility)

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

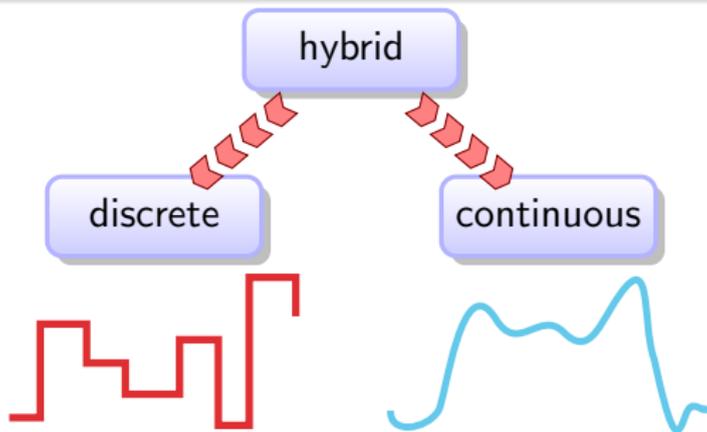
$$\begin{aligned}\forall\phi \exists\phi^b \in FOD &\models \phi \leftrightarrow \phi^b \\ \forall\phi \exists\phi^\# \in DL &\models \phi \leftrightarrow \phi^\#\end{aligned}$$



## Theorem (Equi-expressibility)

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

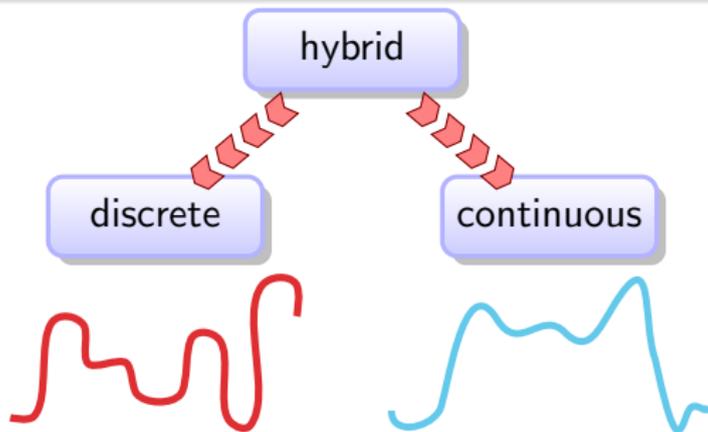
$$\begin{aligned}\forall\phi \exists\phi^b \in FOD &\models \phi \leftrightarrow \phi^b \\ \forall\phi \exists\phi^\# \in DL &\models \phi \leftrightarrow \phi^\#\end{aligned}$$



## Theorem (Equi-expressibility)

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

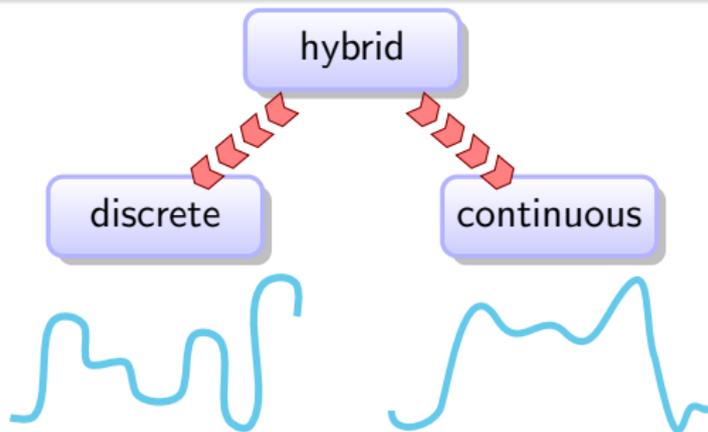
$$\begin{aligned}\forall\phi \exists\phi^b \in FOD &\models \phi \leftrightarrow \phi^b \\ \forall\phi \exists\phi^\# \in DL &\models \phi \leftrightarrow \phi^\#\end{aligned}$$



## Theorem (Equi-expressibility)

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

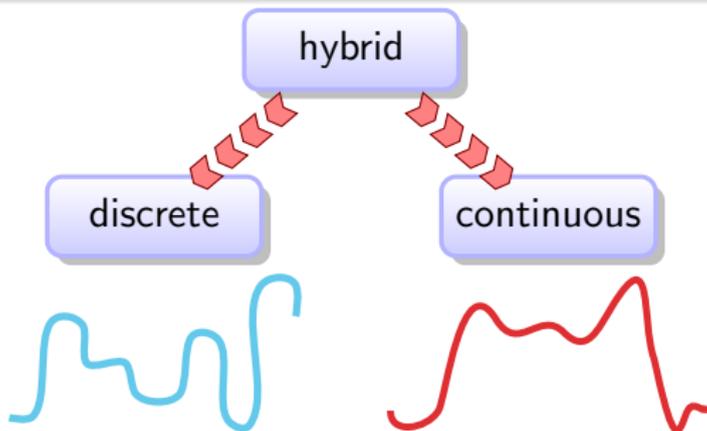
$$\begin{aligned}\forall\phi \exists\phi^b \in FOD &\models \phi \leftrightarrow \phi^b \\ \forall\phi \exists\phi^\# \in DL &\models \phi \leftrightarrow \phi^\#\end{aligned}$$



## Theorem (Equi-expressibility)

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

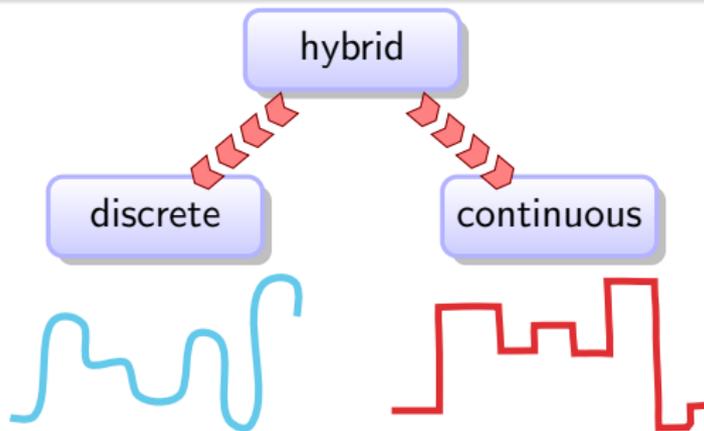
$$\begin{aligned}\forall\phi \exists\phi^b \in FOD &\models \phi \leftrightarrow \phi^b \\ \forall\phi \exists\phi^\# \in DL &\models \phi \leftrightarrow \phi^\#\end{aligned}$$



## Theorem (Equi-expressibility)

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

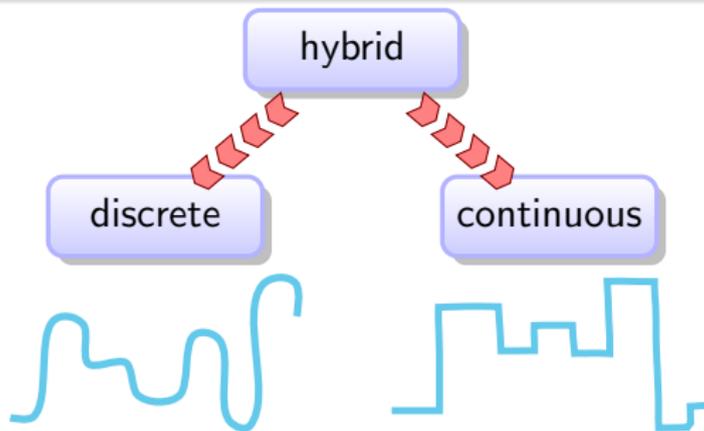
$$\begin{aligned}\forall\phi \exists\phi^b \in FOD &\models \phi \leftrightarrow \phi^b \\ \forall\phi \exists\phi^\# \in DL &\models \phi \leftrightarrow \phi^\#\end{aligned}$$



## Theorem (Equi-expressibility)

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

$$\begin{aligned}\forall\phi \exists\phi^b \in FOD &\models \phi \leftrightarrow \phi^b \\ \forall\phi \exists\phi^\# \in DL &\models \phi \leftrightarrow \phi^\#\end{aligned}$$



## Theorem (Relative Decidability)

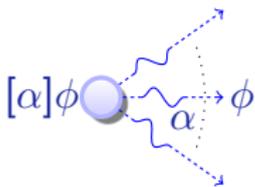
*Validity of  $d\mathcal{L}$  sentences is decidable relative to FOD or DL.*



# The Complete Proof Theory of Hybrid Systems

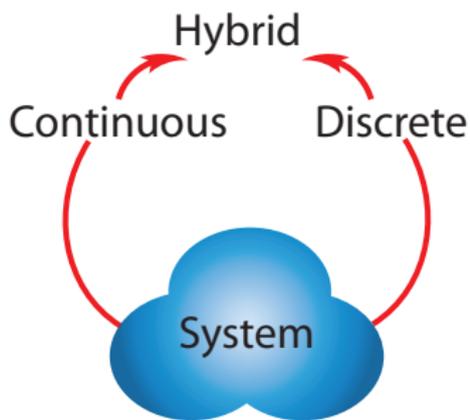
differential dynamic logic

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



proof-theoretical alignment

hybrid = continuous = discrete

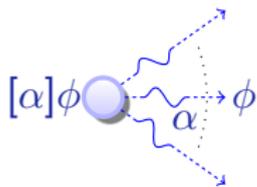




# The Complete Proof Theory of Hybrid Systems

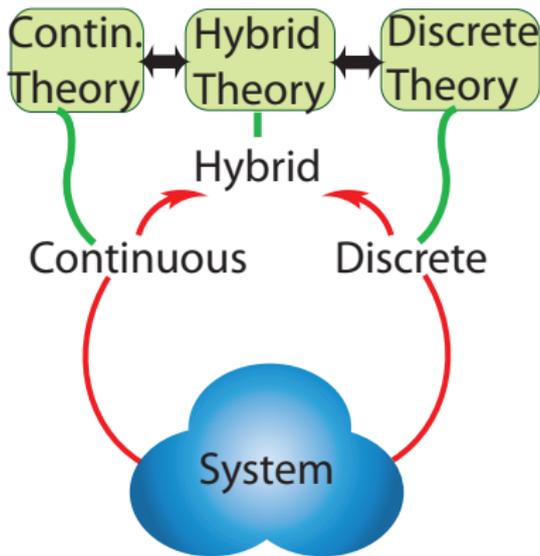
differential dynamic logic

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



proof-theoretical alignment

hybrid = continuous = discrete



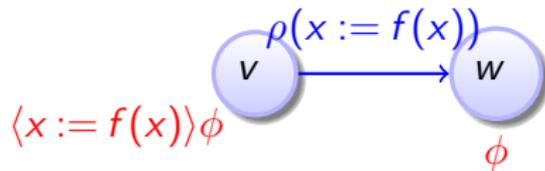
 André Platzer.  
The complete proof theory of hybrid systems.  
*LICS*, pages 541–550. IEEE 2012.

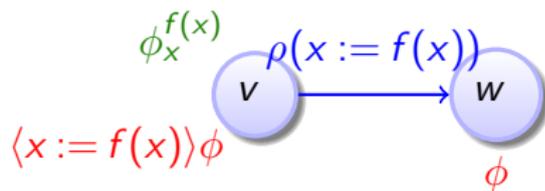
 André Platzer.  
*Logical Analysis of Hybrid Systems:  
Proving Theorems for Complex Dynamics.*  
Springer, 2010.

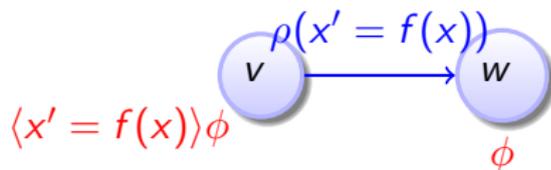
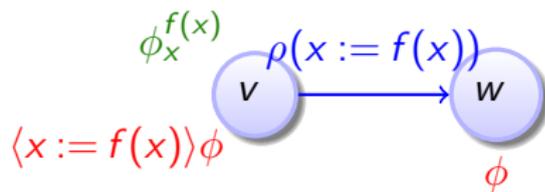
 André Platzer.  
Differential dynamic logic for hybrid systems.  
*J. Autom. Reas.*, 41(2):143–189, 2008.

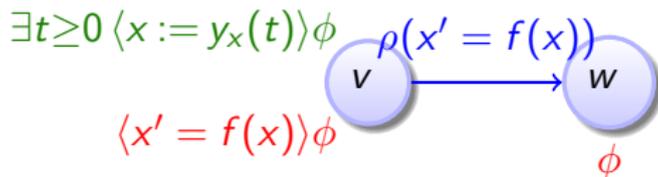
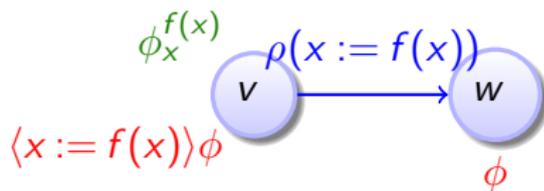
 André Platzer.  
Differential-algebraic dynamic logic for differential-algebraic programs.  
*J. Log. Comput.*, 35(1): 309–352, 2010.

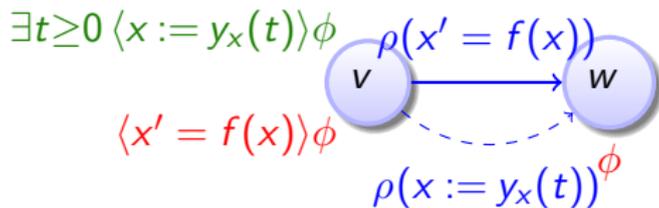
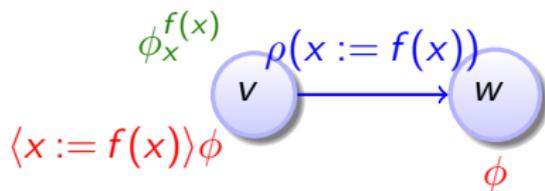
 André Platzer and Edmund M. Clarke.  
The image computation problem in hybrid systems model checking.  
In A. Bemporad, A. Bicchi, and G. Buttazzo, editors, *HSCC*, volume  
4416 of *LNCS*, pages 473–486. Springer, 2007.

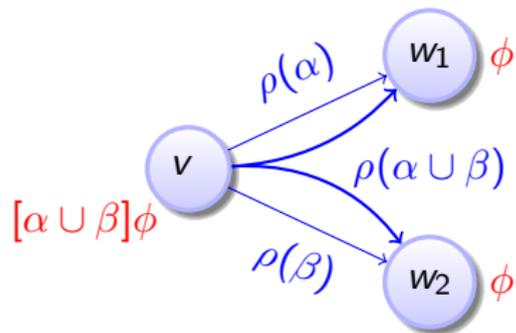


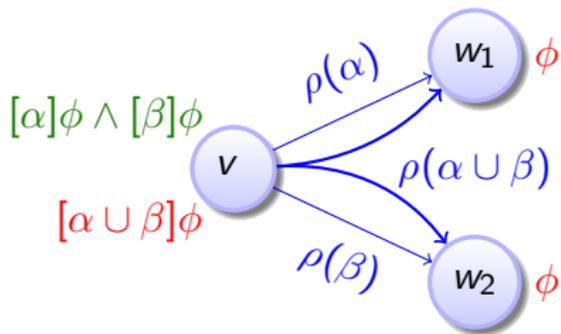




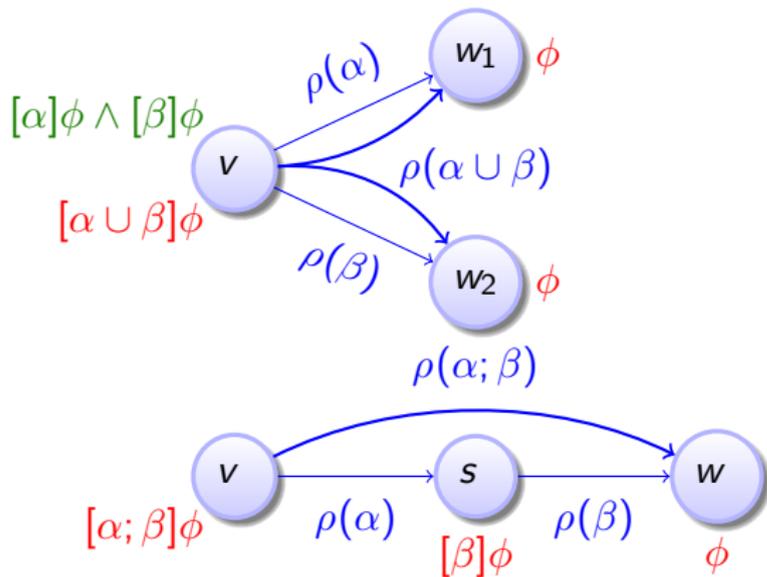






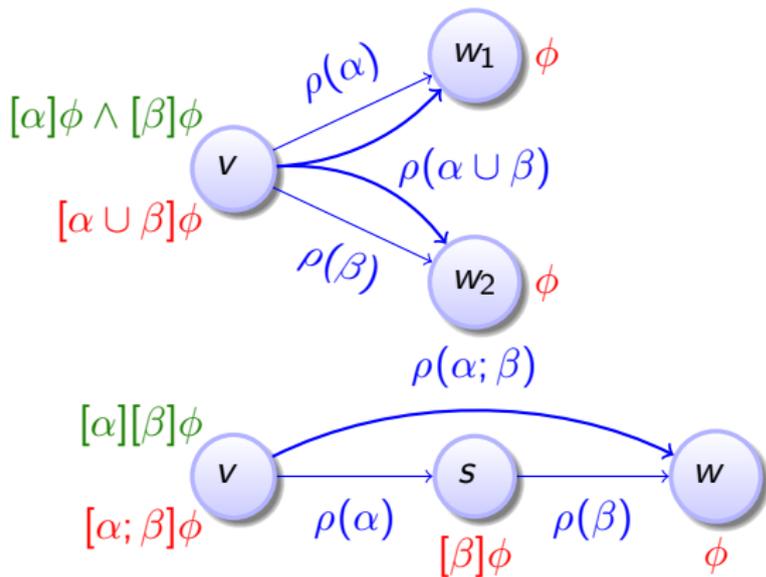


# $\mathcal{A}$ Proof by Symbolic Decomposition



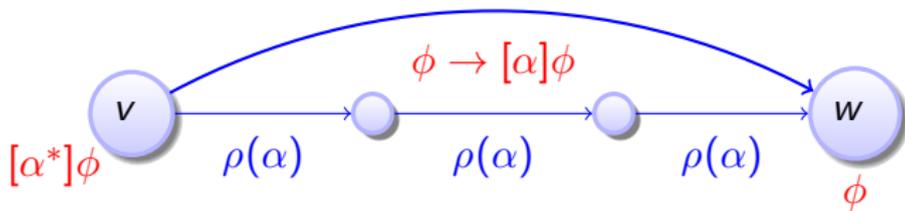
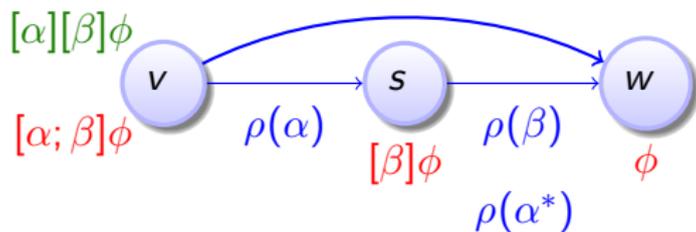
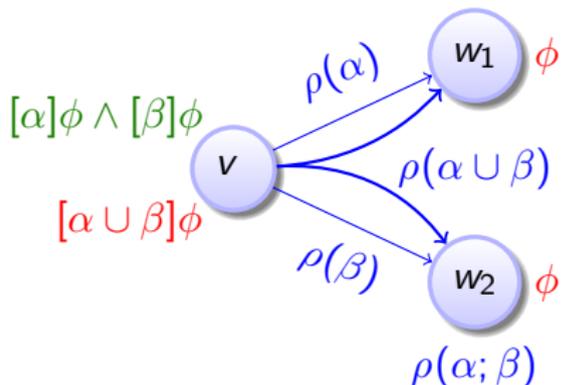


# Proof by Symbolic Decomposition

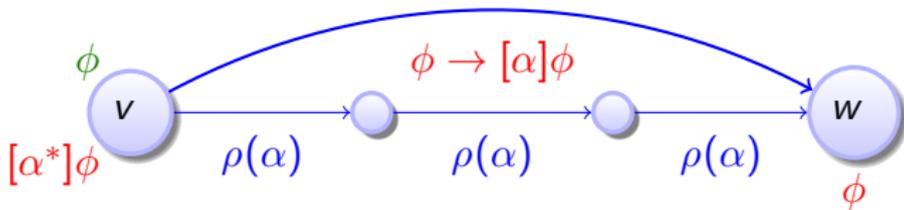
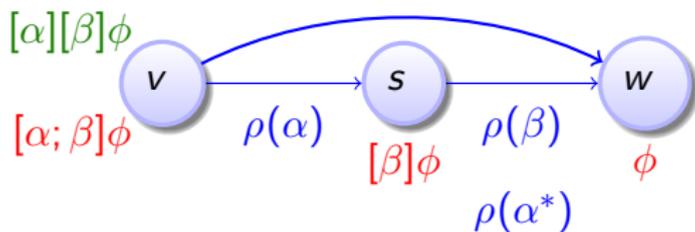
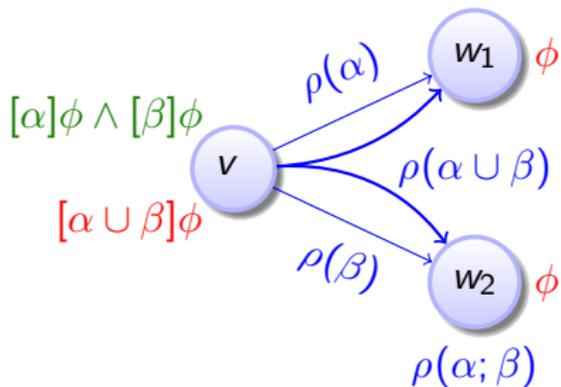




# Proof by Symbolic Decomposition



# Proof by Symbolic Decomposition



# Proof by Symbolic Decomposition

