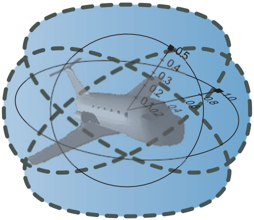
Hybrid Systems & Complete Proofs

André Platzer

Karlsruhe Institute of Technology
Department of Informatics

Computer Science Department
Carnegie Mellon University



Outline

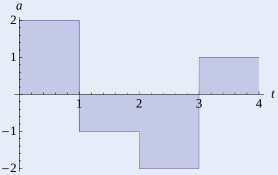
Outline

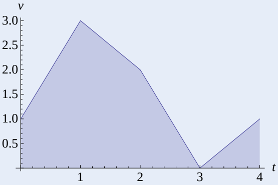
Hybrid Systems: e.g., Car Control

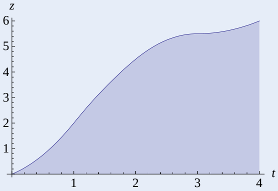
Challenge (Hybrid Systems)

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

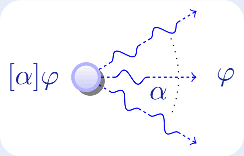
- Continuous dynamics (differential equations)
- Discrete dynamics (control decisions)

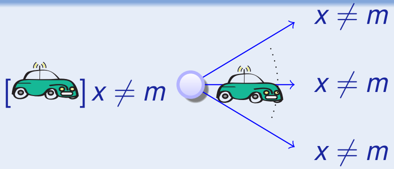
Proof theory: continuous = hybrid = discrete

Outline

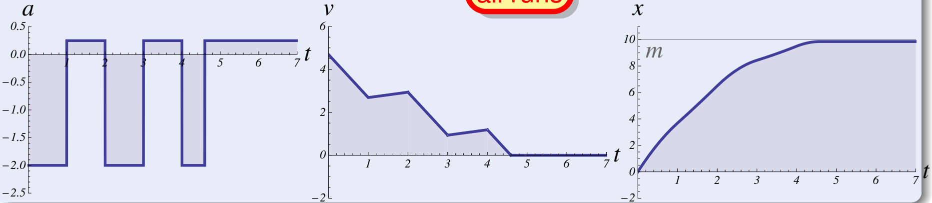
1. Hybrid Systems
2. Differential Dynamic Logic
   - Syntax
   - Semantics
   - Axiomatization
3. Continuous Completeness
   - Schematic Completeness
   - Expressibility and Rendition of Hybrid Programs
4. Discrete Completeness
   - Open Discrete Completeness
   - Closed Discrete Completeness
   - Semialgebraic Discrete Completeness of dL $+\Delta$
   - Discrete Completeness of dL $+\Delta$
   - Equi-expressible
   - Relative Decidable
5. Summary

Concept (Differential Dynamic Logic) (JAR'08,LICS'12)



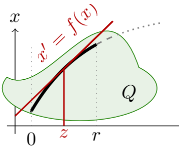


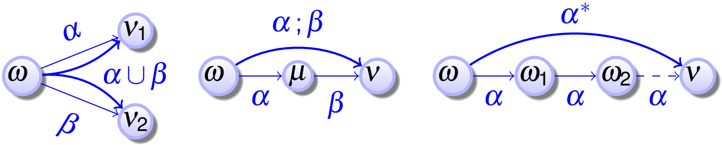
$$\underbrace{x \neq m \wedge b > 0}_{\text{init}} \rightarrow \underbrace{[((\mathtt{if}(SB(x,m))\ a := -b)\ ;\ x' = v, v' = a)^*]}_{\text{all runs}} \underbrace{x \neq m}_{\text{post}}$$



Definition (Hybrid program)

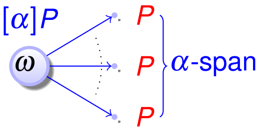
$$\alpha, \beta \ ::= \ x := e \mid ?Q \mid x' = f(x) \,\&\, Q \mid \alpha \cup \beta \mid \alpha ; \beta \mid \alpha^*$$





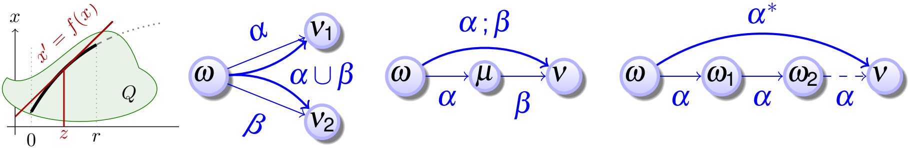
Definition (Differential dynamic logic)

$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid P \vee Q \mid P \rightarrow Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle \alpha \rangle P$$



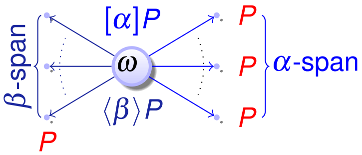
Definition (Hybrid program)

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



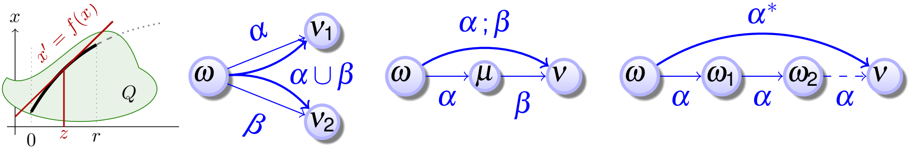
Definition (Differential dynamic logic)

$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid P \vee Q \mid P \rightarrow Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle \alpha \rangle P$$



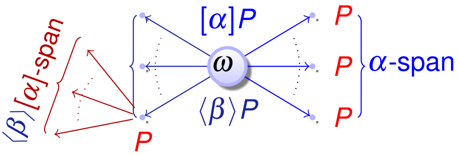
Definition (Hybrid program)

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



Definition (Differential dynamic logic)

$$P, Q ::= e \geq \tilde{e} \mid \neg P \mid P \wedge Q \mid P \vee Q \mid P \rightarrow Q \mid \forall x\, P \mid \exists x\, P \mid [\alpha]P \mid \langle \alpha \rangle P$$



Differential Dynamic Logic dL: Semantics

Definition (Hybrid program semantics) $(\llbracket\cdot\rrbracket : \mathrm{HP} \to \wp(\mathscr{S} \times \mathscr{S}))$

$$\begin{aligned}
\llbracket x := e \rrbracket &= \{(\omega, \nu) : \nu = \omega \text{ except } \nu\llbracket x \rrbracket = \omega\llbracket e \rrbracket\} \\
\llbracket ?Q \rrbracket &= \{(\omega, \omega) : \omega \models Q\} \\
\llbracket x' = f(x) \rrbracket &= \{(\varphi(0), \varphi(r)) : \varphi \models x' = f(x) \text{ for some duration } r\} \\
\llbracket \alpha \cup \beta \rrbracket &= \llbracket \alpha \rrbracket \cup \llbracket \beta \rrbracket \\
\llbracket \alpha ; \beta \rrbracket &= \llbracket \alpha \rrbracket \circ \llbracket \beta \rrbracket \\
\llbracket \alpha^* \rrbracket &= \llbracket \alpha \rrbracket^* = \bigcup_{n \in \mathbb{N}} \llbracket \alpha^n \rrbracket
\end{aligned}$$

compositional semantics

Definition (dL semantics) $(\llbracket\cdot\rrbracket : \mathrm{Fml} \to \wp(\mathscr{S}))$

$$\begin{aligned}
\llbracket e \geq \tilde{e} \rrbracket &= \{\omega : \omega\llbracket e \rrbracket \geq \omega\llbracket \tilde{e} \rrbracket\} \\
\llbracket \neg P \rrbracket &= \llbracket P \rrbracket^{\complement} \\
\llbracket P \wedge Q \rrbracket &= \llbracket P \rrbracket \cap \llbracket Q \rrbracket \\
\llbracket \langle \alpha \rangle P \rrbracket &= \llbracket \alpha \rrbracket \circ \llbracket P \rrbracket = \{\omega : \nu \models P \text{ for some } \nu : (\omega, \nu) \in \llbracket \alpha \rrbracket\} \\
\llbracket [\alpha] P \rrbracket &= \llbracket \neg\langle \alpha \rangle \neg P \rrbracket = \{\omega : \nu \models P \text{ for all } \nu : (\omega, \nu) \in \llbracket \alpha \rrbracket\} \\
\llbracket \exists x\, P \rrbracket &= \{\omega : \omega_x^r \in \llbracket P \rrbracket \text{ for some } r \in \mathbb{R}\}
\end{aligned}$$

equations of truth

$[:=]\quad [x := e]P(x) \leftrightarrow P(e)$

$[?]\quad [?Q]P \leftrightarrow (Q \rightarrow P)$

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

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

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

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

$\mathrm{K}\quad [\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$

$\mathrm{I}\quad [\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$

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

laws of logic of
laws of physics

LICS'12,JAR'17

equations of truth

[:=] $[x := e]P(x) \leftrightarrow P(e)$

[?] $[?Q]P \leftrightarrow (Q \rightarrow P)$

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

[∪] $[\alpha \cup \beta]P \leftrightarrow [\alpha]P \wedge [\beta]P$

[;] $[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$

[*] $[\alpha^*]P \leftrightarrow P \wedge [\alpha][\alpha^*]P$

K $[\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$

I $[\alpha^*]P \leftrightarrow P \wedge [\alpha^*](P \rightarrow [\alpha]P)$

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

laws of logic of
laws of physics

LICS'12,JAR'17

equations of truth

[:=]	$[x := e]P(x) \leftrightarrow P(e)$
[?]	$[?Q]P \leftrightarrow (Q \rightarrow P)$
[′]	$[x' = f(x)]P \leftrightarrow \forall t{\geq}0\, [x := y(t)]P$ $\quad (y'(t) = f(y))$
[∪]	$[\alpha \cup \beta]P \leftrightarrow [\alpha]P \land [\beta]P$
[;]	$[\alpha;\beta]P \leftrightarrow [\alpha][\beta]P$
[*]	$[\alpha^*]P \leftrightarrow P \land [\alpha][\alpha^*]P$
K	$[\alpha](P \rightarrow Q) \rightarrow ([\alpha]P \rightarrow [\alpha]Q)$
I	$[\alpha^*]P \leftrightarrow P \land [\alpha^*](P \rightarrow [\alpha]P)$
C	$[\alpha^*]\forall v{>}0\,(P(v) \rightarrow \langle\alpha\rangle P(v-1)) \rightarrow \forall v\,(P(v) \rightarrow \langle\alpha^*\rangle \exists v{\leq}0\, P(v))$

laws of logic of laws of physics

LICS'12,JAR'17

Differential Dynamic Logic dL: Axiomatization

G $$\frac{P}{[\alpha]P}$$

∀ $$\frac{P}{\forall x\, P}$$

MP $$\frac{P \to Q \quad P}{Q}$$

rules of truth

laws of logic of
laws of physics

LICS'12,JAR'17

rules of truth

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

∀ $\dfrac{P}{\forall x\, P}$

MP $\dfrac{P \to Q \quad P}{Q}$

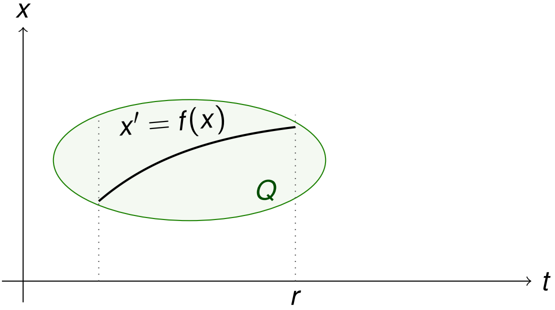
B $\forall x\,[\alpha]P \to [\alpha]\forall x\, P \qquad (x \notin \alpha)$

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

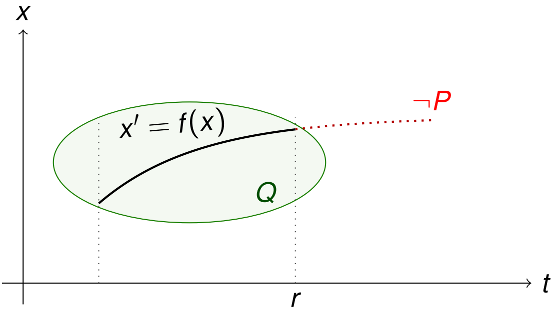
laws of logic of
laws of physics

LICS'12,JAR'17

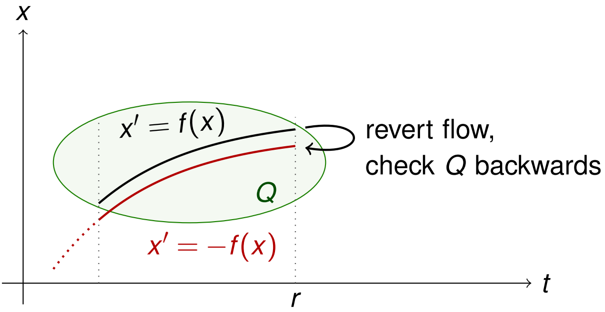
$$[\&] \quad [x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x)](P)$$



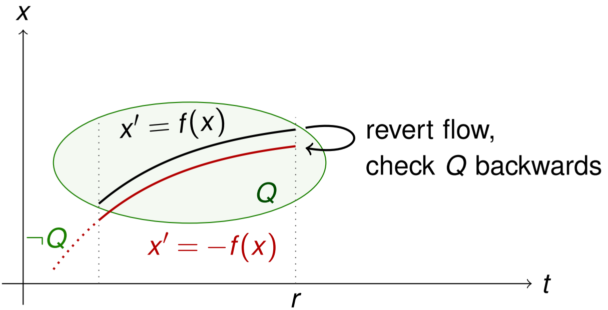
$$[\&] \quad [x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x)](P)$$



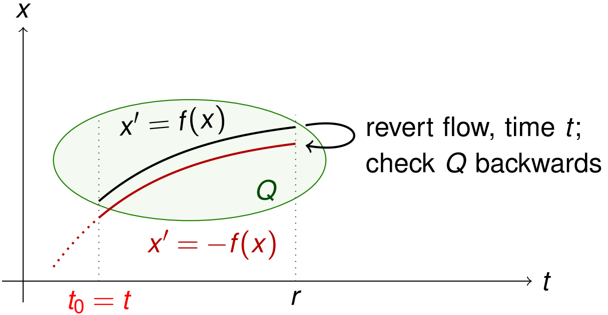
[&] $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x)]\big([x' = -f(x)](Q) \to P\big)$



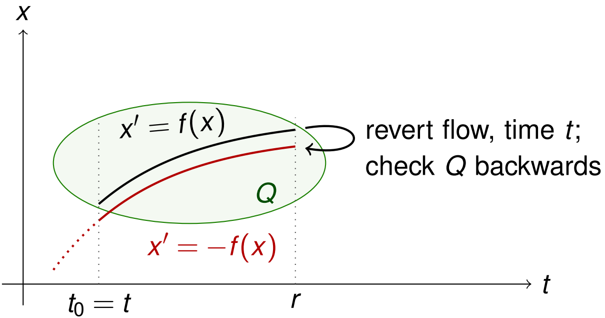
[&] $[x' = f(x) \,\&\, Q]P \leftrightarrow [x' = f(x)]\big([x' = -f(x)](Q) \rightarrow P\big)$



[&] $[x' = f(x) \,\&\, Q]P$
$\leftrightarrow \forall t_0{=}t[x' = f(x)]\big([x' = -f(x)](t \geq t_0 \rightarrow Q) \rightarrow P\big)$



$$[\&] \quad [x' = f(x) \,\&\, Q]P \leftrightarrow \forall t_0{=}t[x' = f(x)]\big([x' = -f(x)](t \geq t_0 \rightarrow Q) \rightarrow P\big)$$



Lemma

Evolution domain axiomatizable

Outline

Continuous Completeness

Theorem (Relative Completeness / Continuous) (JAR'08,LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations:* $\vDash \varphi$ *iff* $\mathrm{Taut}_{\mathrm{FOD}} \vdash \varphi$

Corollary (Complete Proof-theoretical Alignment)

proving: continuous = hybrid

Corollary (Compositionality)

hybrid systems can be verified by recursive decomposition

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

Discrete Completeness

Theorem (Relative Completeness / Continuous) (JAR'08,LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations:* $\vDash \varphi$ *iff* $\mathrm{Taut}_{\mathrm{FOD}} \vdash \varphi$

Theorem (Relative Completeness / Discrete) (LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to discrete dynamics:* $\vDash \varphi$ *iff* $\mathrm{Taut}_{\mathrm{DL}} \vdash \varphi$

Corollary (Complete Proof-theoretical Alignment)

proving: continuous = hybrid = discrete

Corollary (Interdisciplinary Integrability)

"Discrete mathematics + continuous mathematics are integrable"

Schematic Completeness

Theorem (Relative Completeness / Continuous) (JAR'08,LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations:* $\vDash \varphi$ *iff* $\text{Taut}_{\text{FOD}} \vdash \varphi$

Theorem (Relative Completeness / Discrete) (LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to discrete dynamics:* $\vDash \varphi$ *iff* $\text{Taut}_{\text{DL}} \vdash \varphi$

Theorem (Schematic Completeness) (JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to any (differentially) expressive logic L:* $\vDash \varphi$ *iff* $\text{Taut}_{L} \vdash \varphi$

Differentially expressive

$\forall \varphi \in \text{dL}\ \exists \varphi^\flat \in L \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall \varphi \in L \vdash_L \langle x' = f(x)\rangle \varphi \leftrightarrow (\langle x' = f(x)\rangle \varphi)^\flat$

Proof of “continuous = hybrid = discrete”

Schematic Completeness Proof

Proof Sketch (ϕ in NNF, induction on well-founded $\prec$) (JAR'17).

0. ϕ first-order formula $\Rightarrow \phi \in L$ so $\vdash_L \phi$ if $\vDash \phi$ (Also for $\neg\phi_1$ by NNF)
1. $\phi \equiv \phi_1 \wedge \phi_2 \Rightarrow \vDash \phi_1$ and $\vDash \phi_2 \overset{\text{IH}}{\Rightarrow} \vdash_L \phi_1$ and $\vdash_L \phi_2 \Rightarrow \vdash_L \phi_1 \wedge \phi_2$.
2. $\phi \equiv \exists x\, \phi_2, \forall x\, \phi_2, \langle\alpha\rangle\phi_2$ or $[\alpha]\phi_2$ covered in next case with $\phi_1 \equiv$ *false*.
3. $\phi \equiv \phi_1 \vee \langle\!\![\alpha]\!\!\rangle\phi_2$ is (by associativity and commutativity to reorder):

$$\begin{array}{ll} \phi_1 \vee \langle\alpha\rangle\phi_2 & \phi_1 \vee \exists x\, \phi_2 \\ \phi_1 \vee [\alpha]\phi_2 & \phi_1 \vee \forall x\, \phi_2 \end{array}$$

Then, $\phi_2 \prec \phi$ and $\phi_1 \prec \phi$ as less HP/quantifier. Let $F \equiv \neg\phi_1$ and $G \equiv \phi_2$ then $\vDash F \rightarrow \langle\!\![\alpha]\!\!\rangle G$. Show $\vdash_L F \rightarrow \langle\!\![\alpha]\!\!\rangle G$, which derives $\vdash_L \phi_1 \vee \langle\!\![\alpha]\!\!\rangle\phi_2$.

$\vdash_L \phi$ iff $\text{Taut}_L \vdash \phi$

$\prec$ is lexicographic order of HP, formula, with L at the bottom

□

Proof Sketch (ϕ in NNF, induction on well-founded $\prec$) (JAR'17).

4. $[\![\alpha]\!] \equiv \forall x$ with $\vDash F \to \forall x\, G$, wlog $x \notin F$ by bound variable renaming. Hence, $\vDash F \to G \overset{\text{IH}}{\Rightarrow} \vdash_L F \to G$ as $(F \to G) \prec (F \to \forall x\, G)$ less $\forall$.

$$\dfrac{\dfrac{\dfrac{F \to G}{\forall x\,(F \to G)}\,\forall}{\forall x\, F \to \forall x\, G}\,\forall\!\to}{F \to \forall x\, G}\,V_\forall$$

5. $[\![\alpha]\!] \equiv \exists x$ with $\vDash F \to \exists x\, G$. Have $\vDash G^\flat \leftrightarrow G \Rightarrow \vDash F \to \exists x\,(G^\flat) \overset{\text{IH}}{\Rightarrow}$ $\vdash_L F \to \exists x\,(G^\flat)$ as $(F \to \exists x\,(G^\flat)) \prec (F \to \exists x\, G)$ as $G^\flat \in L$. Also $\vDash G^\flat \leftrightarrow G \Rightarrow \vDash G^\flat \to G \overset{\text{IH}}{\Rightarrow} \vdash_L G^\flat \to G$ since $(G^\flat \to G) \prec \phi$ as $G^\flat \in L$.

$$\dfrac{F \to \exists x\,(G^\flat) \qquad \dfrac{\dfrac{G^\flat \to G}{\forall x\,(G^\flat \to G)}\,\forall}{\exists x\,(G^\flat) \to \exists x\, G}\,\forall\!\to}{F \to \exists x\, G}\,\text{MP}$$

□

Schematic Completeness Proof

Proof Sketch (ϕ in NNF, induction on well-founded $\prec$) (JAR'17).

6. $\vDash F \to \langle x' = f(x)\rangle G$ implies $\vDash F \to (\langle x' = f(x)\rangle G^\flat)^\flat \overset{\text{IH}}{\Rightarrow}$ $\vdash_L F \to (\langle x' = f(x)\rangle G^\flat)^\flat$ as $(\langle x' = f(x)\rangle G^\flat)^\flat \in L$ is smaller.
   $\vdash_L \langle x' = f(x)\rangle G^\flat \leftrightarrow (\langle x' = f(x)\rangle G^\flat)^\flat$ as L differentially expressive.
   By IH $\vdash_L G^\flat \to G$ as $G^\flat \in L$. So $\vdash_L \langle x' = f(x)\rangle G^\flat \to \langle x' = f(x)\rangle G$ by M.
   Thus $\vdash_L F \to \langle x' = f(x)\rangle G$ propositionally.
7. $\vDash F \to [?Q]G$ implies $\vDash F \to (Q \to G) \overset{\text{IH}}{\Rightarrow} \vdash_L F \to (Q \to G)$ since $(Q \to G) \prec [?Q]G$. Thus $\vdash_L F \to [?Q]G$ as $[?Q]G \leftrightarrow (Q \to G)$ by [?].
8. $\vDash F \to [\beta \cup \gamma]G$ implies $\vDash F \to [\beta]G \wedge [\gamma]G \overset{\text{IH}}{\Rightarrow} \vdash_L F \to [\beta]G \wedge [\gamma]G$ as $[\beta]G \wedge [\gamma]G \prec [\beta \cup \gamma]G$ has smaller HP. Thus $\vdash_L F \to [\beta \cup \gamma]G$ by [$\cup$].
9. $\vDash F \to [\beta;\gamma]G$ implies $\vDash F \to [\beta][\gamma]G \overset{\text{IH}}{\Rightarrow} \vdash_L F \to [\beta][\gamma]G$ as $[\beta][\gamma]G \prec [\beta;\gamma]G$ has smaller HP. Thus $\vdash_L F \to [\beta;\gamma]G$ by [;].

□

Schematic Completeness Proof

Proof Sketch (ϕ in NNF, induction on well-founded $\prec$) (JAR'17).

10. $\vDash F \rightarrow [y := \theta]G$. Rename bound variable to fresh variable x where G_y^x is the result of uniformly renaming y to x in G:

$$\cfrac{\cfrac{F \rightarrow \forall x\, (x = \theta \rightarrow G_y^x)}{F \rightarrow [x := \theta]G_y^x}\;[:=]_=}{F \rightarrow [y := \theta]G}\;\text{BR}$$

using the derivable equational form of the assignment axiom $[:=]$

$$[:=]_= \quad [x := f]P \leftrightarrow \forall x\, (x = f \rightarrow P)$$

Only used equivalences, so premise valid iff conclusion valid.
$\vDash F \rightarrow \forall x\, (x = \theta \rightarrow G_y^x) \overset{\text{IH}}{\Rightarrow} \vdash_L F \rightarrow \forall x\, (x = \theta \rightarrow G_y^x)$ as $(F \rightarrow \forall x\, (x = \theta \rightarrow G_y^x)) \prec (F \rightarrow [y := \theta]G)$ has less modalities.

□

Schematic Completeness Proof

Proof Sketch (ϕ in NNF, induction on well-founded $\prec$) (JAR'17).

11. $\vDash F \to [\beta^*]G$. Formula $[\beta^*]G$ is loop invariant as $\vDash [\beta^*]G \to [\beta][\beta^*]G$.

$$J \equiv ([\beta^*]G)^\flat \text{ equivalent loop invariant in simpler } L$$

Then $\vDash F \to J$ and $\vDash J \to G \overset{\text{IH}}{\Rightarrow} \vdash_L F \to J$ and $\vdash_L J \to G$ since $(F \to J) \prec \phi$ and $(J \to G) \prec \phi$ as $J \in L$ is smaller.

Moreover $\vDash J \to [\beta]J \overset{\text{IH}}{\Rightarrow} \vdash_L J \to [\beta]J$ since β has less loops than β^*.

$$\text{MP}\dfrac{F \to J \qquad \text{MP}\dfrac{\text{ind}\dfrac{J \to [\beta]J}{J \to [\beta^*]J} \qquad \text{M}[\cdot]\dfrac{J \to G}{[\beta^*]J \to [\beta^*]G}}{J \to [\beta^*]G}}{F \to [\beta^*]G}$$

□

Schematic Completeness Proof

Proof Sketch (ϕ in NNF, induction on well-founded $\prec$) (JAR'17).

12 $\vDash F \rightarrow \langle\beta^*\rangle G$. Let $x = FV(\langle\beta^*\rangle G)$. Since $\langle\beta^*\rangle G$ is a least pre-fixpoint:

$$\vDash \forall x\,(G \vee \langle\beta\rangle p(x) \rightarrow p(x)) \rightarrow (\langle\beta^*\rangle G \rightarrow p(x))$$

As $\vDash F \rightarrow \langle\beta^*\rangle G$ also $\vDash \forall x\,(G \vee \langle\beta\rangle p(x) \rightarrow p(x)) \rightarrow (F \rightarrow p(x)) \overset{IH}{\Rightarrow}$
$\vdash_L \forall x\,(G \vee \langle\beta\rangle p(x) \rightarrow p(x)) \rightarrow (F \rightarrow p(x))$ as
$(\forall x\,(G \vee \langle\beta\rangle p(x) \rightarrow p(x)) \rightarrow (F \rightarrow p(x))) \prec \phi$. $\sigma = \{p(x) \mapsto \langle\beta^*\rangle G\}$
admissible since $FV(\sigma) = \emptyset$ as $x = FV(\langle\beta^*\rangle G)$ and since p is fresh:

$$\dfrac{\text{US}\dfrac{\forall x\,(G \vee \langle\beta\rangle p(x) \rightarrow p(x)) \rightarrow (F \rightarrow p(x))}{\forall x\,(G \vee \langle\beta\rangle\langle\beta^*\rangle G \rightarrow \langle\beta^*\rangle G) \rightarrow (F \rightarrow \langle\beta^*\rangle G)} \qquad \forall\dfrac{[^*],\langle\cdot\rangle\dfrac{*}{G \vee \langle\beta\rangle\langle\beta^*\rangle G \rightarrow \langle\beta^*\rangle G}}{\forall x\,(G \vee \langle\beta\rangle\langle\beta^*\rangle G \rightarrow \langle\beta^*\rangle G)}}{F \rightarrow \langle\beta^*\rangle G}\text{MP}$$

Note: could also use modified $(\langle\beta^*\rangle G)^\flat$ with convergence rule con.

□

Theorem (Relative Completeness / Continuous) (JAR'08,LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations:* $\vDash \varphi$ *iff* $\mathrm{Taut}_{\mathrm{FOD}} \vdash \varphi$

Theorem (Relative Completeness / Continuous) (JAR'08,LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations:* $\vDash \varphi$ *iff* $\text{Taut}_{\text{FOD}} \vdash \varphi$

Theorem (Schematic Completeness) (JAR'17)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to any (differentially) expressive logic L:* $\vDash \varphi$ *iff* $\text{Taut}_L \vdash \varphi$

Differentially expressive

$\forall \varphi \in \text{dL}\ \exists \varphi^\flat \in L \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall \varphi \in L \vdash_L \langle x' = f(x)\rangle \varphi \leftrightarrow (\langle x' = f(x)\rangle \varphi)^\flat$

Lemma (dL Expressibility in FOD)

$\forall \varphi \in \mathrm{dL}\ \exists \varphi^\flat \in \mathrm{FOD} \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall \varphi \in \mathrm{FOD} \vdash_L \langle x' = f(x) \rangle \varphi \leftrightarrow (\langle x' = f(x) \rangle \varphi)^\flat$

Proof Sketch.

1. Strong enough invariants and variants expressible in dL!
2. dL expressible in FOD?
3. Finite FOD formula characterizing unbounded hybrid repetition.
4. FOD characterizes $\mathbb{R}$-Gödel encoding (pairing/unpairing on $\mathbb{R}$).
5. FOD characterizes HP transitions.
6. FOD expresses dL formulas. □

$$\mathrm{FOD} = \mathrm{FOL}_{\mathbb{R}} + [x' = f(x)]F$$

Continuous Completeness Proof

Lemma (dL Expressibility in FOD)

$\forall \varphi \in \text{dL}\ \exists \varphi^\flat \in \text{FOD} \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall \varphi \in \text{FOD} \vdash_L \langle x' = f(x)\rangle \varphi \leftrightarrow (\langle x' = f(x)\rangle \varphi)^\flat$

Proof Sketch.

1. Strong enough invariants and variants expressible in dL!
2. dL expressible in FOD?
3. Finite FOD formula characterizing unbounded hybrid repetition.
4. FOD characterizes $\mathbb{R}$-Gödel encoding (pairing/unpairing on $\mathbb{R}$).
5. FOD characterizes HP transitions.
6. FOD expresses dL formulas. □

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

Lemma (dL Expressibility in FOD)

$\forall \varphi \in \text{dL } \exists \varphi^\flat \in \text{FOD} \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall \varphi \in \text{FOD} \vdash_L \langle x' = f(x) \rangle \varphi \leftrightarrow (\langle x' = f(x) \rangle \varphi)^\flat$

Proof Sketch.

1. Strong enough invariants and variants expressible in dL!
2. dL expressible in FOD?
3. Finite FOD formula characterizing unbounded hybrid repetition.
4. FOD characterizes $\mathbb{R}$-Gödel encoding (pairing/unpairing on $\mathbb{R}$).
5. FOD characterizes HP transitions.
6. FOD expresses dL formulas. □

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

Continuous Completeness Proof

Lemma (dL Expressibility in FOD)

$\forall \varphi \in \text{dL}\ \exists \varphi^\flat \in \text{FOD} \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall \varphi \in \text{FOD} \vdash_L \langle x' = f(x) \rangle \varphi \leftrightarrow (\langle x' = f(x) \rangle \varphi)^\flat$

Proof Sketch.

1. Strong enough invariants and variants expressible in dL!
2. dL expressible in FOD?
3. Finite FOD formula characterizing unbounded hybrid repetition.
4. FOD characterizes $\mathbb{R}$-Gödel encoding (pairing/unpairing on $\mathbb{R}$).
5. FOD characterizes HP transitions.
6. FOD expresses dL formulas. □

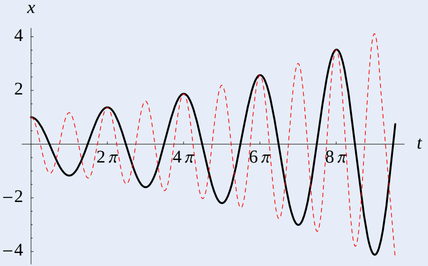
$$\text{FOD} = \text{FOL}_{\mathbb{R}} + [x' = f(x)]F$$

Continuous Completeness Proof

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

Proof Sketch ($\mathbb{R}$-Gödel encoding).

FOD characterizes constructive bijection $\mathbb{R} \to \mathbb{R}^2$



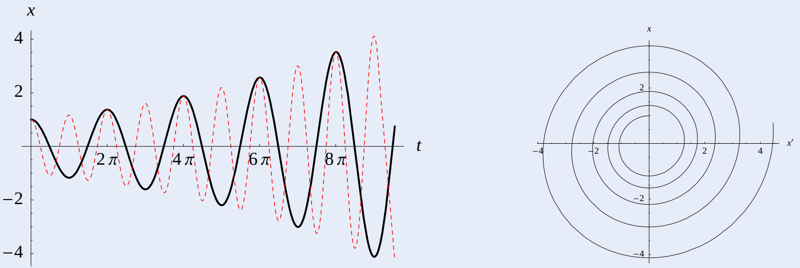
□

Continuous Completeness Proof

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

Proof Sketch ($\mathbb{R}$-Gödel encoding).

FOD characterizes constructive bijection $\mathbb{R} \to \mathbb{R}^2$



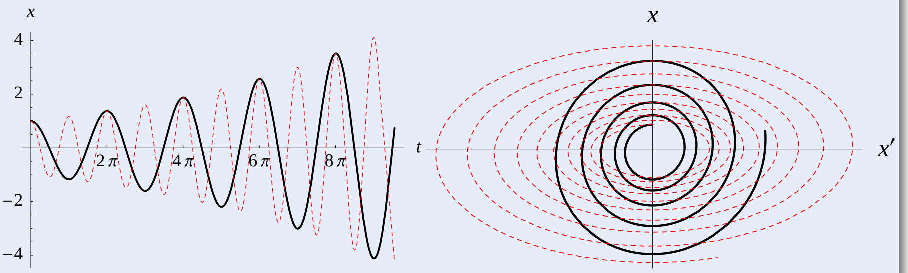
□

Continuous Completeness Proof

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

Proof Sketch ($\mathbb{R}$-Gödel encoding).

FOD characterizes constructive bijection $\mathbb{R} \to \mathbb{R}^2$



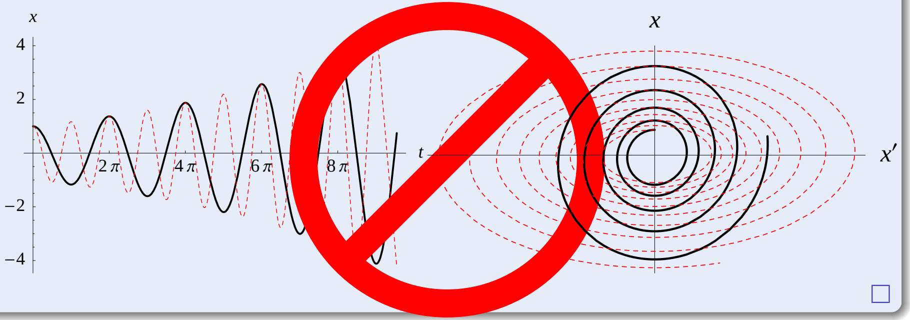
□

Continuous Completeness Proof

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

Proof Sketch ($\mathbb{R}$-Gödel encoding).

FOD characterizes constructive bijection $\mathbb{R} \to \mathbb{R}^2$ not differentiable, Morayne!



□

Continuous Completeness Proof

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

Proof Sketch ($\mathbb{R}$-Gödel encoding).

FOD characterizes constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=0}^{\infty} \frac{a_i}{2^i} = a_0.a_1a_2\ldots$$

$$\sum_{i=0}^{\infty} \frac{b_i}{2^i} = b_0.b_1b_2\ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i-1}} + \frac{b_i}{2^{2i}} \right) = a_0b_0.a_1b_1a_2b_2\ldots$$

□

Continuous Completeness Proof

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

Proof Sketch ($\mathbb{R}$-Gödel encoding).

FOD characterizes constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=0}^{\infty} \frac{a_i}{2^i} = a_0.a_1a_2\ldots$$

$$\sum_{i=0}^{\infty} \frac{b_i}{2^i} = b_0.b_1b_2\ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i-1}} + \frac{b_i}{2^{2i}} \right) = a_0b_0.a_1b_1a_2b_2\ldots$$

$Z_j^{(n)} = z$ is jth $\mathbb{R}$ of n reals Z

$$\text{at}(Z,n,j,z) \leftrightarrow \forall i{:}\mathbb{Z}\ \text{digit}(z,i) = \text{digit}(Z,n(i-1)+j) \land n > 0 \land n,j \in \mathbb{N}$$

$$\text{digit}(a,i) = \text{intpart}(2\,\text{frac}(2^{i-1}a))$$

$$\text{intpart}(a) = a - \text{frac}(a)$$

$$\text{frac}(a) = z \leftrightarrow \exists i{:}\mathbb{Z}\ z = a - i \land -1 < z \land z < 1 \land az \geq 0 \quad \text{“keep sign”}$$

□

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

Proof Sketch ($\mathbb{R}$-Gödel encoding).

FOD characterizes constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=0}^{\infty} \frac{a_i}{2^i} = a_0.a_1 a_2 \ldots$$

$$\sum_{i=0}^{\infty} \frac{b_i}{2^i} = b_0.b_1 b_2 \ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i-1}} + \frac{b_i}{2^{2i}} \right) = a_0 b_0.a_1 b_1 a_2 b_2 \ldots$$

$$\text{at}(Z,n,j,z) \leftrightarrow \forall i{:}\mathbb{Z}\ \text{digit}(z,i) = \text{digit}(Z, n(i-1)+j) \land n > 0 \land n,j \in \mathbb{N}$$

$$\text{digit}(a,i) = \text{intpart}(2\,\text{frac}(2^{i-1}a))$$

$$\text{intpart}(a) = a - \text{frac}(a)$$

$$\text{frac}(a) = z \leftrightarrow \exists i{:}\mathbb{Z}\ z = a - i \land -1 < z \land z < 1 \land az \geq 0 \quad \text{“keep sign”}$$

□

Continuous Completeness Proof

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

Proof Sketch ($\mathbb{R}$-Gödel encoding).

FOD characterizes constructive bijection $\mathbb{R} \to \mathbb{R}^2$

$$\sum_{i=0}^{\infty} \frac{a_i}{2^i} = a_0.a_1 a_2 \ldots$$

$$\sum_{i=0}^{\infty} \frac{b_i}{2^i} = b_0.b_1 b_2 \ldots$$

$$\sum_{i=0}^{\infty} \left(\frac{a_i}{2^{2i-1}} + \frac{b_i}{2^{2i}} \right) = a_0 b_0.a_1 b_1 a_2 b_2 \ldots$$

$$\begin{aligned} 2^i = z \leftrightarrow\ & i \geq 0 \land \langle x := 1; t := 0; x' = x \ln 2, t' = 1 \rangle (t = i \land x = z) \\ \lor\ & i < 0 \land \langle x := 1; t := 0; x' = -x \ln 2, t' = -1 \rangle (t = i \land x = z) \end{aligned}$$

$$\ln 2 = z \leftrightarrow \langle x := 1; t := 0; x' = x, t' = 1 \rangle (x = 2 \land t = z)$$

syntactic abbreviation without recursion □

Continuous Completeness Proof

Lemma (dL Expressibility in FOD)

$\forall \varphi \in \text{dL}\ \exists \varphi^\flat \in \text{FOD} \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall \varphi \in \text{FOD} \vdash_L \langle x' = f(x) \rangle \varphi \leftrightarrow (\langle x' = f(x) \rangle \varphi)^\flat$

Proof Sketch.

1. Strong enough invariants and variants expressible in dL!
2. dL expressible in FOD?
3. Finite FOD formula characterizing unbounded hybrid repetition.
4. FOD characterizes $\mathbb{R}$-Gödel encoding (pairing/unpairing on $\mathbb{R}$).
5. FOD characterizes HP transitions.
6. FOD expresses dL formulas. □

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

Continuous Completeness Proof

Lemma (dL Expressibility in FOD)

$\forall\varphi\in\text{dL}\ \exists\varphi^\flat\in\text{FOD} \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall\varphi\in\text{FOD} \vdash_L \langle x' = f(x)\rangle\varphi \leftrightarrow (\langle x' = f(x)\rangle\varphi)^\flat$

Proof Sketch.

1. Strong enough invariants and variants expressible in dL!
2. dL expressible in FOD?
3. Finite FOD formula characterizing unbounded hybrid repetition.
4. FOD characterizes $\mathbb{R}$-Gödel encoding (pairing/unpairing on $\mathbb{R}$).
5. FOD characterizes HP transitions.
6. FOD expresses dL formulas. □

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

Continuous Completeness Proof

Lemma (dL Expressibility in FOD)

$\forall \varphi \in \text{dL}\ \exists \varphi^\flat \in \text{FOD} \vDash \varphi \leftrightarrow \varphi^\flat$ and $\forall \varphi \in \text{FOD} \vdash_L \langle x' = f(x) \rangle \varphi \leftrightarrow (\langle x' = f(x) \rangle \varphi)^\flat$

Proof Sketch.

1. Strong enough invariants and variants expressible in dL!
2. dL expressible in FOD?
3. Finite FOD formula characterizing unbounded hybrid repetition.
4. FOD characterizes $\mathbb{R}$-Gödel encoding (pairing/unpairing on $\mathbb{R}$).
5. FOD characterizes HP transitions.
6. FOD expresses dL formulas. □

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

Program Rendition in FOD

Lemma (Program rendition)

$\forall \alpha \in$ HP with variables among $x = x_1, \dots, x_k$ $\exists \mathscr{S}_\alpha(x, v) \in$ FOD with variables among distinct $x = x_1, \dots, x_k$ and $v = v_1, \dots, v_k$: $\quad \vDash \mathscr{S}_\alpha(x, v) \leftrightarrow \langle \alpha \rangle x = v$

Proof Sketch (by induction on α).

$$\mathscr{S}_{x_i:=\theta}(x, v) \equiv v_i = \theta \land \bigwedge_{j \neq i} (v_j = x_j)$$

$$\mathscr{S}_{x'=\theta}(x, v) \equiv \langle x' = \theta \rangle \, v = x$$

$$\mathscr{S}_{x'=\theta \,\&\, Q}(x, v) \equiv \exists t \, (t=0 \land \langle x'=\theta, t'=1 \rangle (v=x \land [x'=-\theta, t'=-1](t \geq 0 \to Q)))$$

$$\mathscr{S}_{?Q}(x, v) \equiv v = x \land Q$$

$$\mathscr{S}_{\beta \cup \gamma}(x, v) \equiv \mathscr{S}_\beta(x, v) \lor \mathscr{S}_\gamma(x, v)$$

$$\mathscr{S}_{\beta ; \gamma}(x, v) \equiv \exists z \, (\mathscr{S}_\beta(x, z) \land \mathscr{S}_\gamma(z, v))$$

$$\mathscr{S}_{\beta^*}(x, v) \equiv \exists Z \, \exists n{:}\mathbb{N} \big(Z_1^{(n)} = x \land Z_n^{(n)} = v \land \forall i{:}\mathbb{N} (1 \leq i < n \to \mathscr{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)}))\big)$$

□

Program Rendition in FOD

Lemma (Program rendition)

$\forall \alpha \in \mathrm{HP}$ *with variables among* $x = x_1, \ldots, x_k$ $\exists \mathscr{S}_\alpha(x,v) \in \mathrm{FOD}$ *with variables among distinct* $x = x_1, \ldots, x_k$ *and* $v = v_1, \ldots, v_k$*:* $\vDash \mathscr{S}_\alpha(x,v) \leftrightarrow \langle \alpha \rangle x = v$

Proof Sketch (by induction on α).

$$\mathscr{S}_{x_i:=\theta}(x,v) \equiv v_i = \theta \land \bigwedge_{j \neq i}(v_j = x_j)$$

$$\mathscr{S}_{x'=\theta}(x,v) \equiv \langle x' = \theta \rangle\, v = x$$

$$\mathscr{S}_{x'=\theta\,\&\,Q}(x,v) \equiv \exists t\, (t{=}0 \land \langle x'{=}\theta, t'{=}1 \rangle (v{=}x \land [x'{=}{-}\theta, t'{=}{-}1](t{\geq}0 {\to} Q)))$$

$$\mathscr{S}_{?Q}(x,v) \equiv v = x \land Q$$

$$\mathscr{S}_{\beta\cup\gamma}(x,v) \equiv \mathscr{S}_\beta(x,v) \lor \mathscr{S}_\gamma(x,v)$$

$$\mathscr{S}_{\beta;\gamma}(x,v) \equiv \exists z\, (\mathscr{S}_\beta(x,z) \land \mathscr{S}_\gamma(z,v))$$

$$\mathscr{S}_{\beta^*}(x,v) \equiv \exists Z\, \exists n{:}\mathbb{N} (Z_1^{(n)}{=}x \land Z_n^{(n)}{=}v \land \forall i{:}\mathbb{N}(1{\leq}i{<}n {\to} \mathscr{S}_\beta(Z_i^{(n)}, Z_{i+1}^{(n)})))$$

□

Program Rendition in FOD

Lemma (Program rendition)

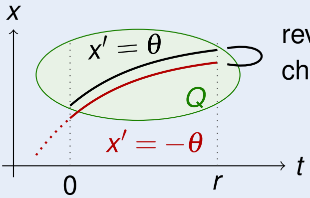
$\forall \alpha \in \mathrm{HP}$ *with variables among* $x = x_1, \ldots, x_k$ $\exists \mathscr{S}_\alpha(x,v) \in \mathrm{FOD}$ *with variables among distinct* $x = x_1, \ldots, x_k$ *and* $v = v_1, \ldots, v_k$*:* $\quad \vDash \mathscr{S}_\alpha(x,v) \leftrightarrow \langle\alpha\rangle x = v$

Proof Sketch (by induction on α).

$$\mathscr{S}_{x'=\theta\,\&\,Q}(x,v) \equiv \exists t\,(t{=}0 \land \langle x'{=}\theta, t'{=}1\rangle(v{=}x \land [x'{=}{-}\theta, t'{=}{-}1](t{\geq}0 {\rightarrow} Q)))$$

$$\equiv \exists t\,\exists r\,(t{=}0 \land \langle x'{=}\theta, t'{=}1\rangle(v{=}x \land r = t) \land$$

$$\forall x\,\forall t\,(x = v \land t = r \rightarrow [x'{=}{-}\theta, t'{=}{-}1](t{\geq}0 {\rightarrow} Q)))$$



revert flow and time
check Q backwards

□

Expressibility

Lemma (dL Expressibility in FOD)

$\forall \varphi \in \text{dL}\ \exists \varphi^\flat \in \text{FOD} \vDash \varphi \leftrightarrow \varphi^\flat$

Proof (by induction on φ).

1. φ first-order, then $\varphi^\flat := \varphi$ already is a FOD-formula.
2. $\varphi \equiv \phi \vee \psi \overset{\text{IH}}{\Rightarrow}$ have $\phi^\flat, \psi^\flat$ such that $\vDash \phi \leftrightarrow \phi^\flat$ and $\vDash \psi \leftrightarrow \psi^\flat$. By congruence $\vDash (\phi \vee \psi) \leftrightarrow (\phi^\flat \vee \psi^\flat)$ giving $\vDash \varphi \leftrightarrow \varphi^\flat$ for $\varphi^\flat \equiv \phi^\flat \vee \psi^\flat$.
3. Likewise for propositional connectives or quantifiers.
4. $\varphi \equiv \langle\alpha\rangle\psi$ uses $\vDash \langle\alpha\rangle\psi \leftrightarrow \exists v\, (\mathscr{S}_\alpha(x,v) \wedge \psi^\flat \frac{v}{x})$
5. $\varphi \equiv [\alpha]\psi$ uses $\vDash [\alpha]\psi \leftrightarrow \forall v\, (\mathscr{S}_\alpha(x,v) \rightarrow \psi^\flat \frac{v}{x})$ □

Outline

Discrete Completeness

Theorem (Relative Completeness / Continuous) (JAR'08,LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations:* $\vDash \varphi$ *iff* $\mathrm{Taut}_{\mathrm{FOD}} \vdash \varphi$

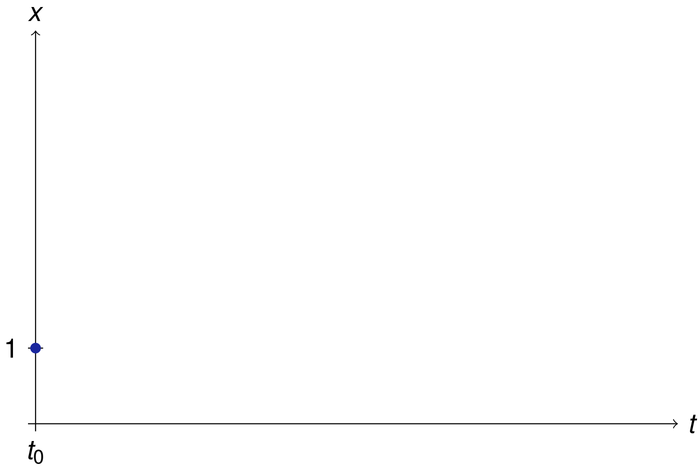
Theorem (Relative Completeness / Discrete) (LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to discrete dynamics:* $\vDash \varphi$ *iff* $\mathrm{Taut}_{\mathrm{DL}} \vdash \varphi$

Corollary (Complete Proof-theoretical Alignment)

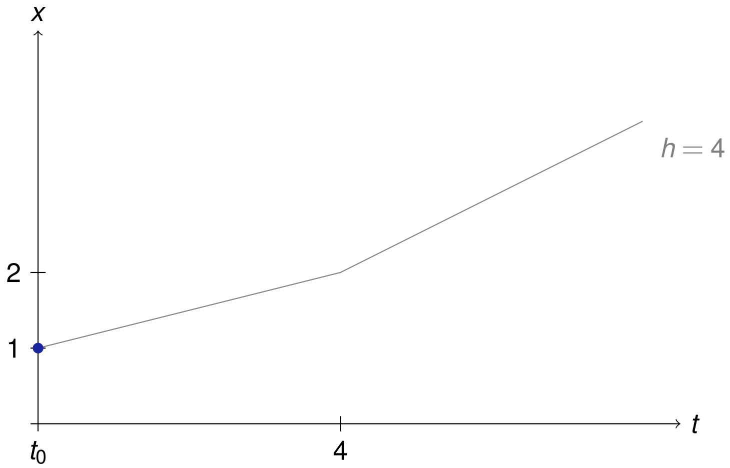
proving: continuous = hybrid = discrete

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



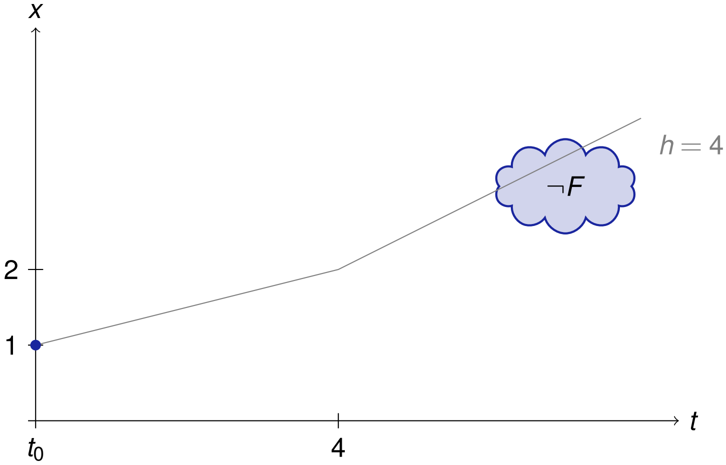
Continuous Dynamics $\neq$ Discrete Dynamics

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



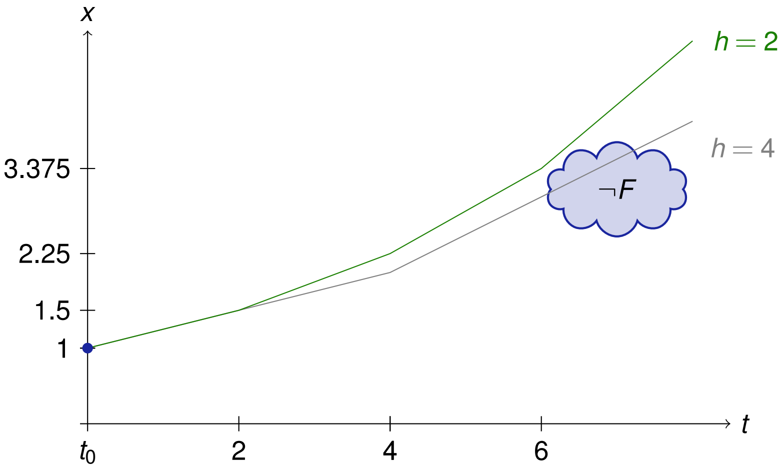
Continuous Dynamics $\neq$ Discrete Dynamics

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



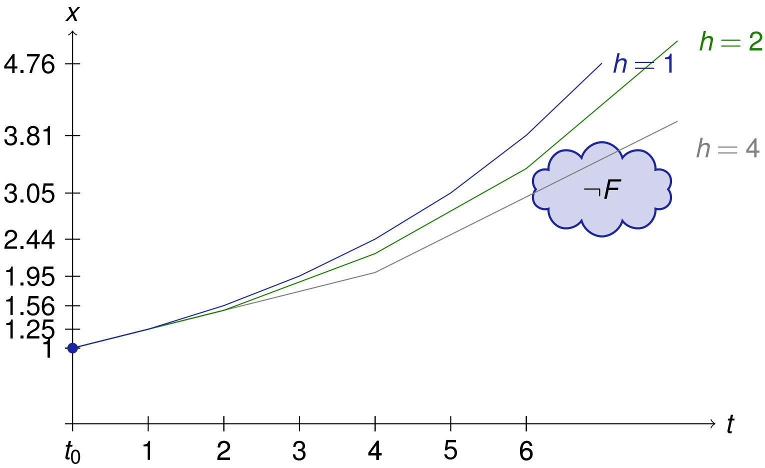
Continuous Dynamics $\neq$ Discrete Dynamics

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

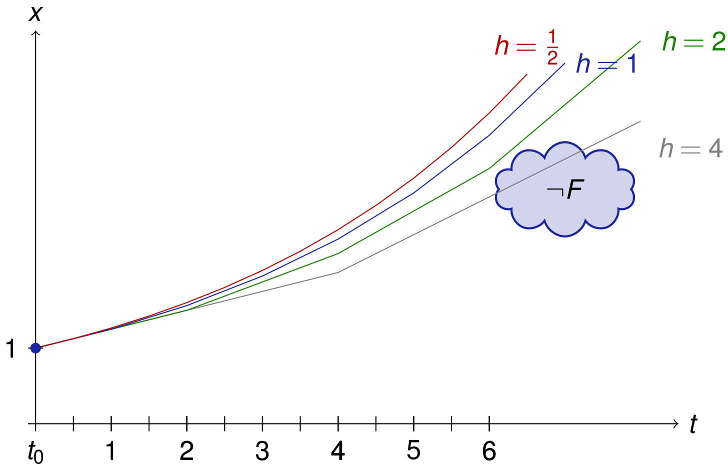


Continuous Dynamics $\neq$ Discrete Dynamics

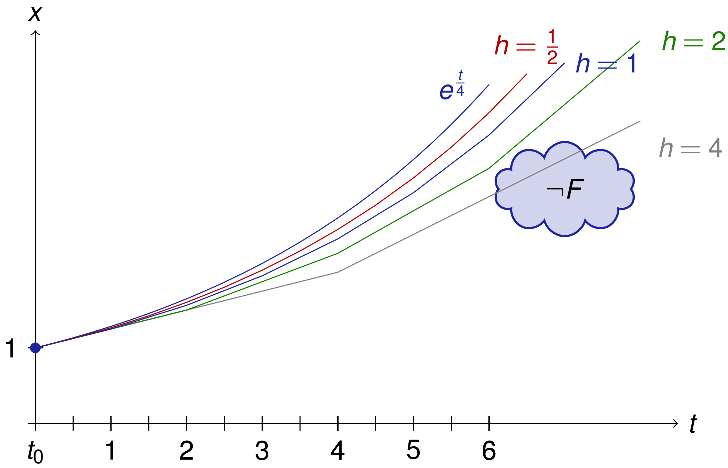
$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



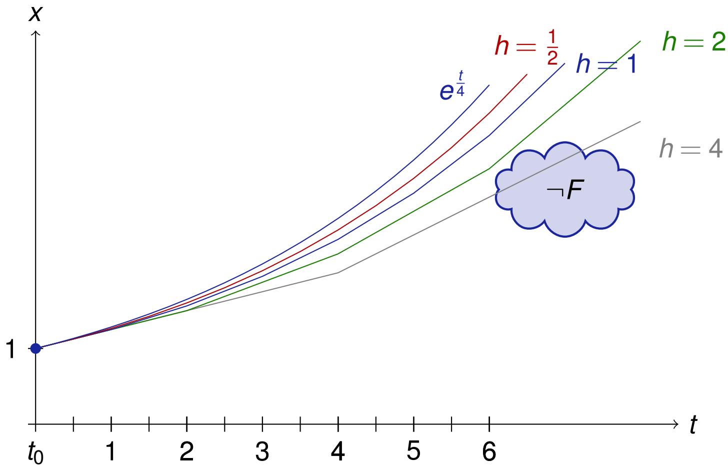
$$[x' = \frac{x}{4}]F \qquad [(x := x + h\frac{x}{4})^*]F$$



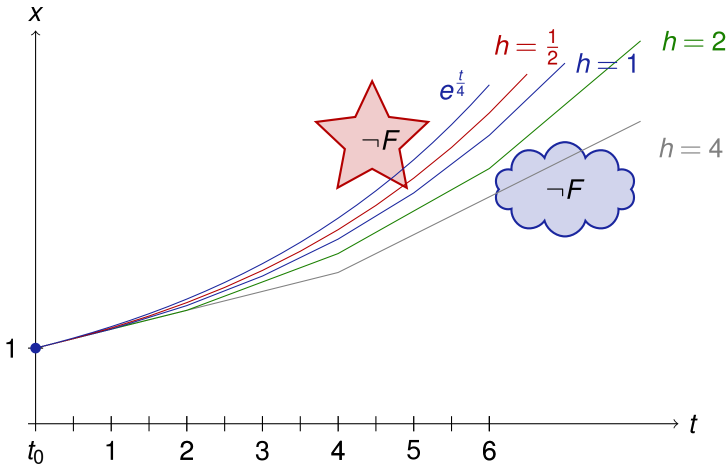
$$[x' = \frac{x}{4}]F \quad \text{vs.} \quad [(x := x + h\frac{x}{4})^*]F$$



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



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



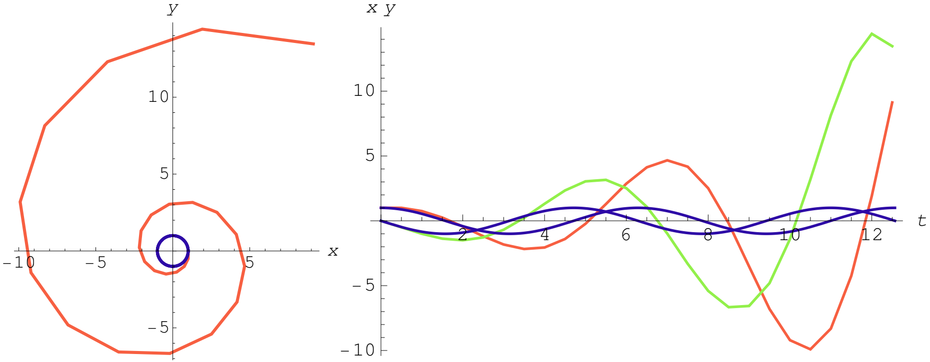
Discrete Euler Approximation Axiom $\overleftarrow{\Delta}$

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

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

Example (Incomplete, not global)

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



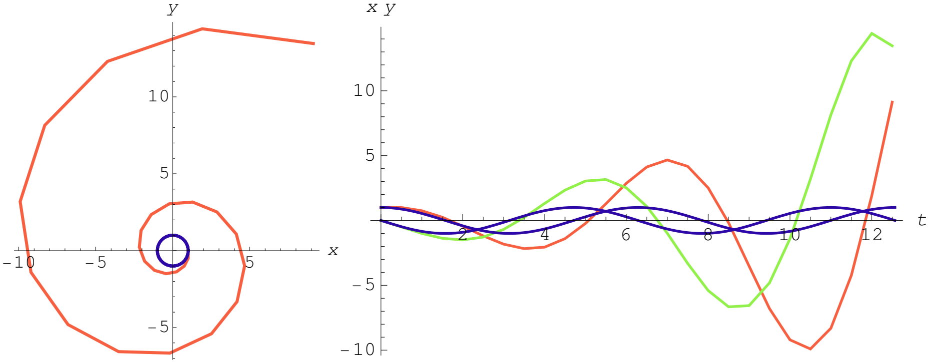
Discrete Euler Approximation Axiom $\overleftarrow{\Delta}$

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

(closed)

Example (Unsound for open F, only in closure)

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

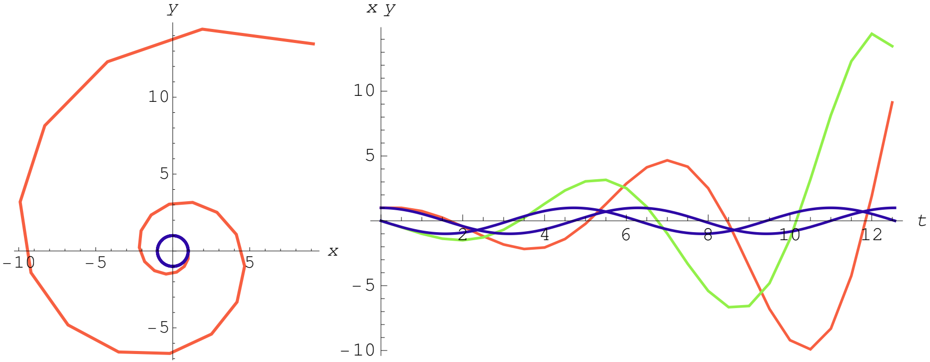


Discrete Euler Approximation Axiom $\overleftarrow{\Delta}$

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

Example (Incomplete, not global)

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

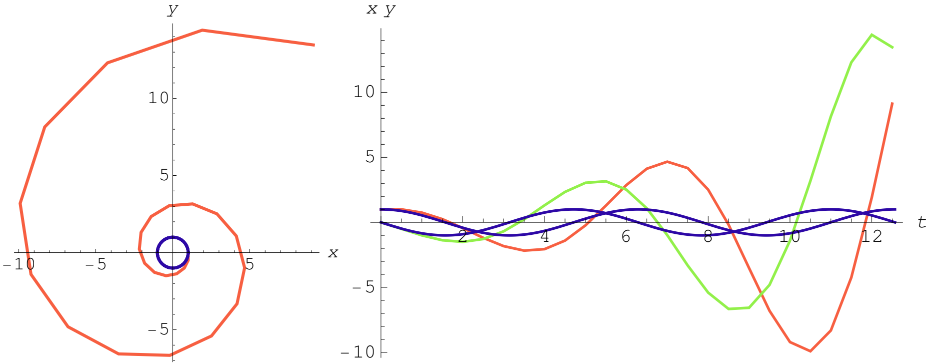


$$\overrightarrow{\Delta} \quad [x' = f(x)]F \\ \rightarrow \forall t \geq 0\, \exists h_0 > 0\, \forall 0 < h < h_0\, [(x := x + hf(x))^*](t \geq 0 \rightarrow F)$$

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

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

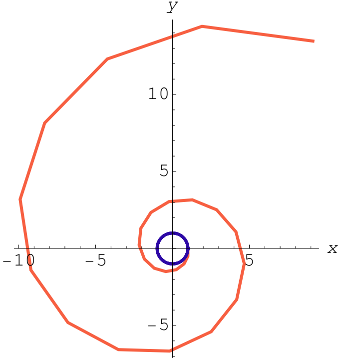
$$\nvDash x = 1 \wedge y = 0 \rightarrow [x' = y, y' = -x](x \leq 0 \rightarrow x^2 + y^2 > 1)$$

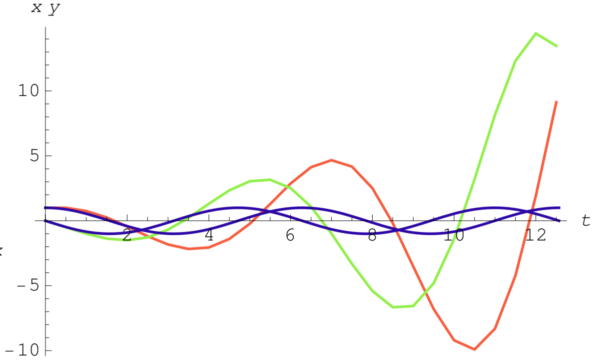


$\overrightarrow{\Delta}$ $[x' = f(x)]F$
$\rightarrow \forall t{\geq}0\, \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*](t \geq 0 \rightarrow F)$ (open)

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

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





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

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

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

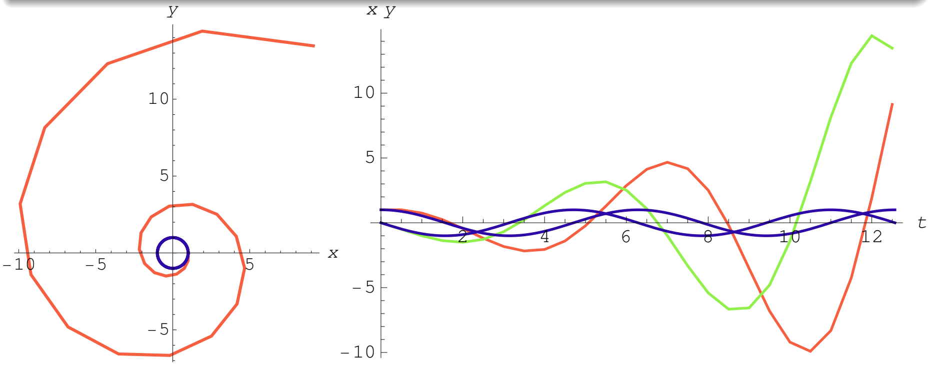
Example ()

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

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

Example (Incomplete for closed F)

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

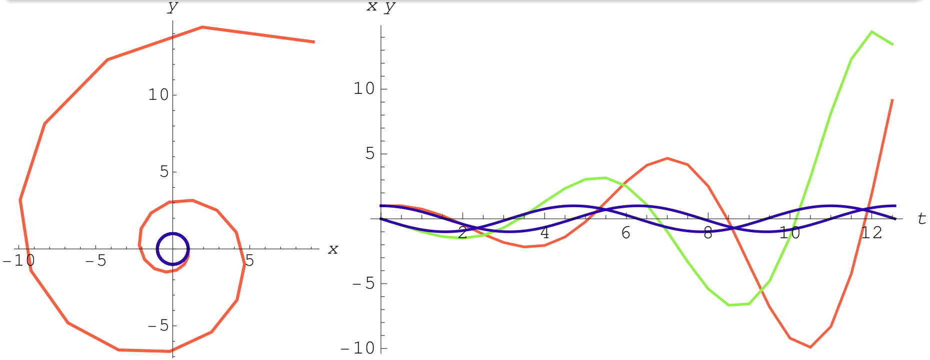


$\overleftrightarrow{\Delta}$ $[x' = f(x)]F$ *(open)*

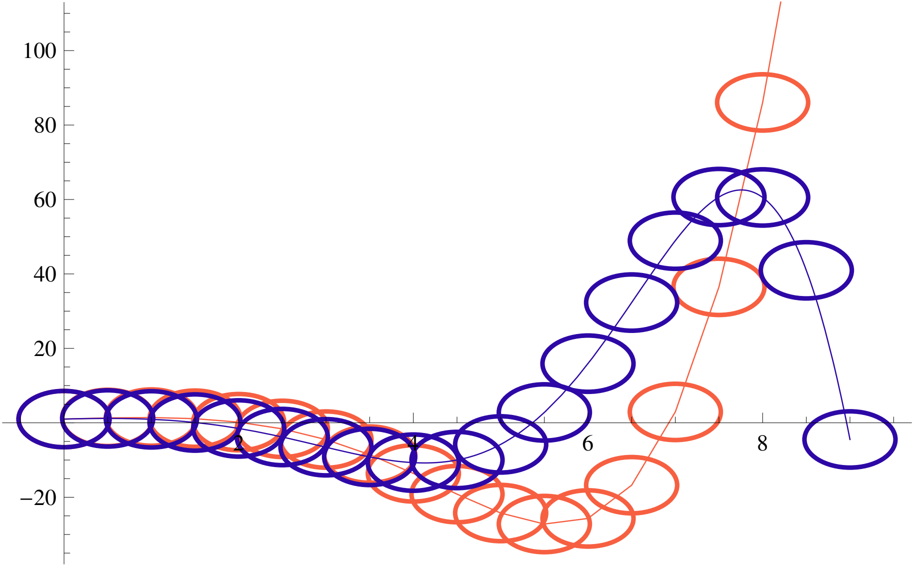
$$\leftrightarrow \forall t{\geq}0 \exists \varepsilon{>}0 \exists h_0{>}0 \forall 0{<}h{<}h_0 [(x := x + hf(x))^*] \big(t{\geq}0 \rightarrow \neg \mathscr{U}_\varepsilon(\neg F)\big)$$

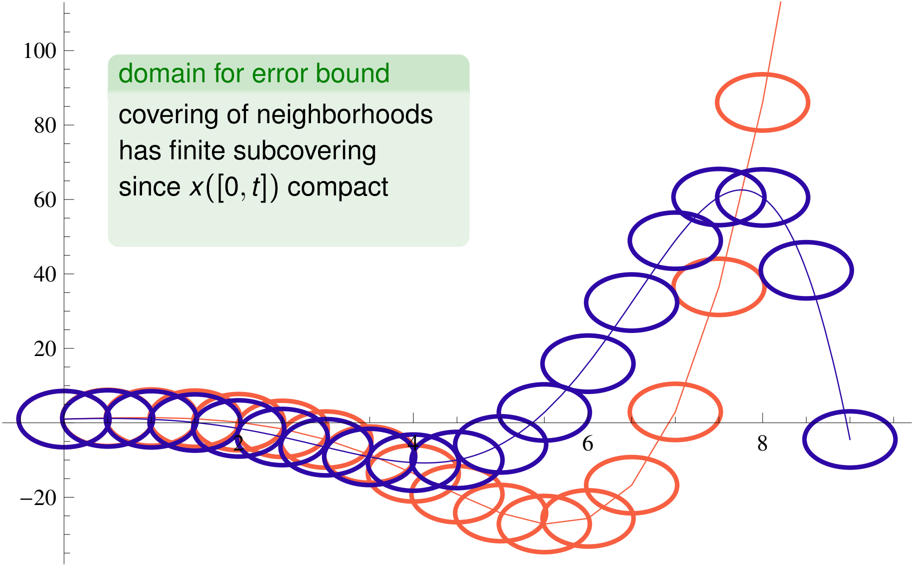
Example (Incomplete for closed F)

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



Proof: Partial Covering for Solution, Approximation





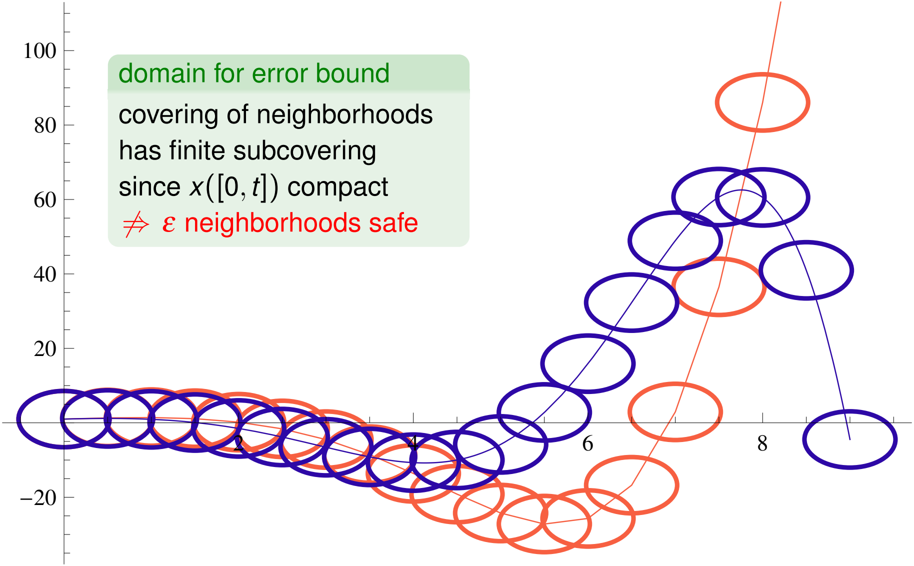
domain for error bound

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

domain for error bound

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

$\not\Rightarrow$ ε neighborhoods safe



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

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

Proof Sketch.

1. $\omega \models \exists h_0{>}0\,\forall 0{<}h{<}h_0\,[(x := x{+}hf(x))^*]F$ $\qquad \hat{x}^n = x$ at iteration n
2. $x \in C^2([0,t])$ solves $x' = f(x)$ and $x(0) = \omega$. NTS $x(t) \models F$
3. $f \in C^1$ locally Lipschitz iff Lipschitz on compact subsets $\Leftarrow$ loc. compact
4. Fix $E > 0$. Let L Lipschitz constant of $f \in C^1$ on compact image $U \stackrel{\text{def}}{=} \overline{\mathscr{U}}_E(x([0,t])) = \bigcup_{q\in x([0,t])} \overline{\mathscr{U}}_E(q)$ of $x([0,t]) \times \overline{\mathscr{U}}_E(0)$ under $+$.

   $$\|x(nh) - \hat{x}^n\| \le h \max_{\zeta\in[0,t]} \|x''(\zeta)\| \frac{e^{Lt}-1}{2L} < \varepsilon < E \qquad \text{for small } (h{\ll}1)$$

   $$\|x(t) - x(nh)\| \stackrel{\text{MVT}}{=} \|x'(\xi)\|(t{-}nh) \le \max_{\xi\in[0,t]} \|f(x(\xi))\|(t{-}nh) < \varepsilon \ (h{\ll}1)$$

   $$\|x(t) - \hat{x}^n\| \le \|x(t) - x(nh)\| + \|x(nh) - \hat{x}^n\| < 2\varepsilon \qquad (h{\ll}1)$$
5. Sequence $\hat{x}^n \to x(t)$ as $h \to 0$ and $\hat{x}^n \models F$ closed so $x(t) \models F$. $\square$

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

Proof Sketch.

1. $\omega \models [x' = f(x)]F$ $\quad\quad \hat{x}^n = x$ at iteration n
2. $x \in C^2([0,t])$ solves $x' = f(x)$ and $x(0) = \omega$. Compact $x([0,t]) \subseteq F$ open
3. $0 < E < \inf_{q \in x([0,t])} d(q, [\![F]\!]^\complement)$ has compact $U \overset{\text{def}}{=} \overline{\mathscr{U}_E}(x([0,t]))$ in F.
4. Let L Lipschitz constant of $f \in C^1$ on compact U.

$$\|x(nh) - \hat{x}^n\| \leq h \max_{\zeta \in [0,t]} \|x''(\zeta)\| \frac{e^{Lt} - 1}{2L} < \varepsilon < E \qquad \text{for small } (h \ll 1)$$

$$\|x(t) - x(nh)\| \overset{\text{MVT}}{=} \|x'(\xi)\|(t - nh) \leq \max_{\xi \in [0,t]} \|f(x(\xi))\|(t - nh) < \varepsilon \ (h \ll 1)$$

$$\|x(t) - \hat{x}^n\| \leq \|x(t) - x(nh)\| + \|x(nh) - \hat{x}^n\| < 2\varepsilon \qquad (h \ll 1)$$

5. $\omega \models \exists h_0{>}0\, \forall 0{<}h{<}h_0\, [(x := x + hf(x))^*](t{\geq}0 \to F)$ for $h \ll 1, nh \leq t$ as $\hat{x}^n \models F$ for $h \ll 1, nh \leq t$ by 4a since $t \geq 0$ after loop iff $nh \leq t$ before □

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

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

Proof Sketch. (open).

1. "$\to$" $\omega \models [x' = f(x)]F$ ("$\leftarrow$" derives from $\overleftarrow{\Delta}$ as $\neg\mathscr{U}_\varepsilon(\neg F)$ closed)
2. $x \in C^2([0,t])$ solves $x' = f(x)$ and $x(0) = \omega$. Compact $x([0,t]) \subseteq F$ open
3. $0 < E < \inf_{q \in x([0,t])} d(q, [\![F]\!]^\complement)$ has compact $U \stackrel{\text{def}}{=} \overline{\mathscr{U}}_E(x([0,t]))$ in F.
4. $\omega \models [x' = f(x)]\big(t \ge 0 \to \forall z\,(\|z - x\| < E \to F(z))\big)$ by (3)

$$\|x(nh) - \hat{x}^n\| \le h \max_{\zeta \in [0,t]} \|x''(\zeta)\| \frac{e^{Lt} - 1}{2L} < \varepsilon < E \qquad \text{for small } (h \ll 1)$$

$$\|x(t) - x(nh)\| \stackrel{\text{MVT}}{=} \|x'(\xi)\|(t - nh) \le \max_{\xi \in [0,t]} \|f(x(\xi))\|(t - nh) < \varepsilon \ (h \ll 1)$$

$$\|x(t) - \hat{x}^n\| \le \|x(t) - x(nh)\| + \|x(nh) - \hat{x}^n\| < 2\varepsilon \qquad (h \ll 1)$$

5. $\|x(nh) - z\| \le \|x(nh) - \hat{x}^n\| + \|\hat{x}^n - z\| < 2\varepsilon \le E$ for $h \ll 1$, $\|\hat{x}^n - z\| < \varepsilon$.
6. $F(z)$ true at these z by ④.
7. nth iterate $\omega_n \models t{\ge}0 \to \underbrace{\forall z\,(\|z - x\| < \varepsilon \to F(z))}_{\neg\mathscr{U}_\varepsilon(\neg F)}$ as $\omega_n \models t{\ge}0$ iff $\omega \models nh{\le}t$

□

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

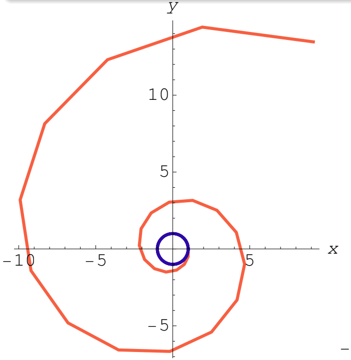
Discrete Euler Approximation Axiom $\overleftrightarrow{\Delta}$ $\quad t' = -1$

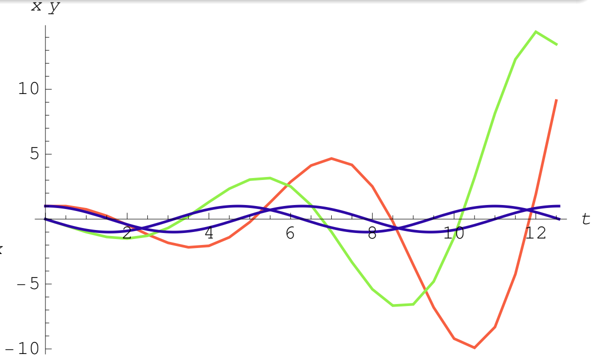
$\overleftrightarrow{\Delta}$ $\quad [x' = f(x)]F$ $\quad$ (*open*)

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

Example (Incomplete for closed F)

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



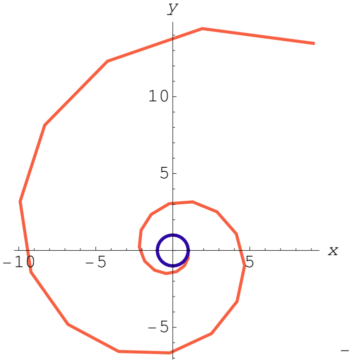


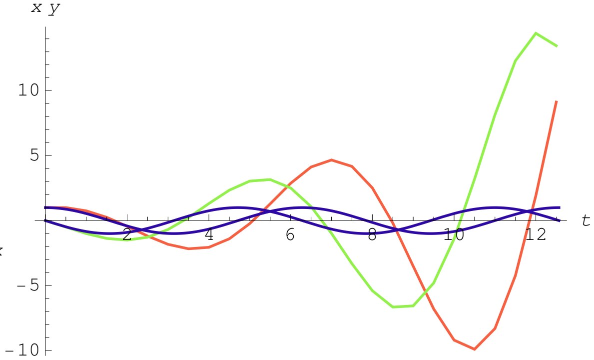
$\mathring{U}$ $[x' = f(x)]F \leftrightarrow \forall \check{\varepsilon}>0\,[x' = f(x)]\mathscr{U}_{\check{\varepsilon}}(F)$ $(\Leftarrow$ B,V,G,K)

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

Example (Closed $\rightsquigarrow$ Quantified Open)

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



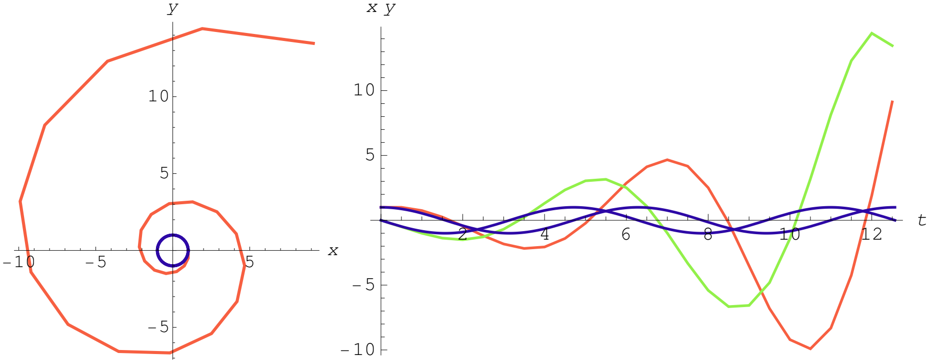


Closed Discrete Completeness (derivable)

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

Example (Closed $\rightsquigarrow$ Quantified Open)

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

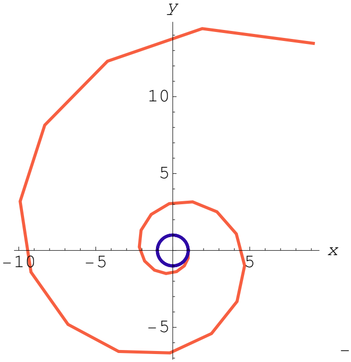


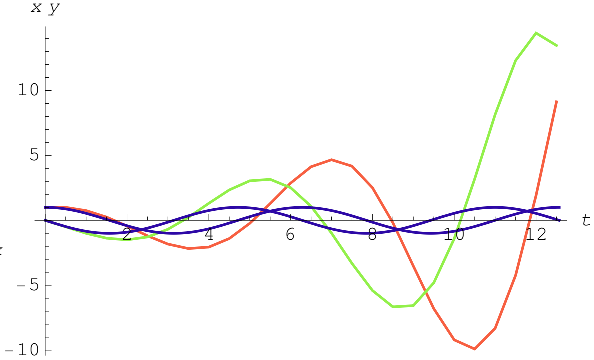
Closed Discrete Completeness (derivable)

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

Example (Closed $\rightsquigarrow$ Quantified Open)

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





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

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

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

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

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

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

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)

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

Semialgebraic Discrete Completeness (derivable)

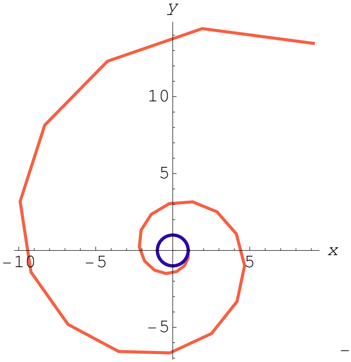
$\check{U}$ $[x' = f(x)](O \vee C) \leftrightarrow \forall \check{\varepsilon}{>}0\,[x' = f(x)](O \vee \mathscr{U}_{\check{\varepsilon}}(C))$ $(\Leftarrow$ B,V,G,K)

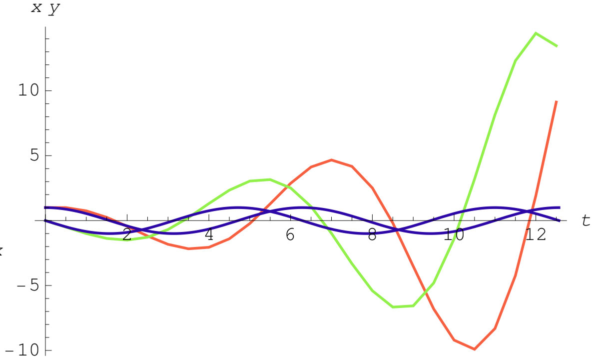
Semialgebraic Discrete Completeness (derivable)

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

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

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

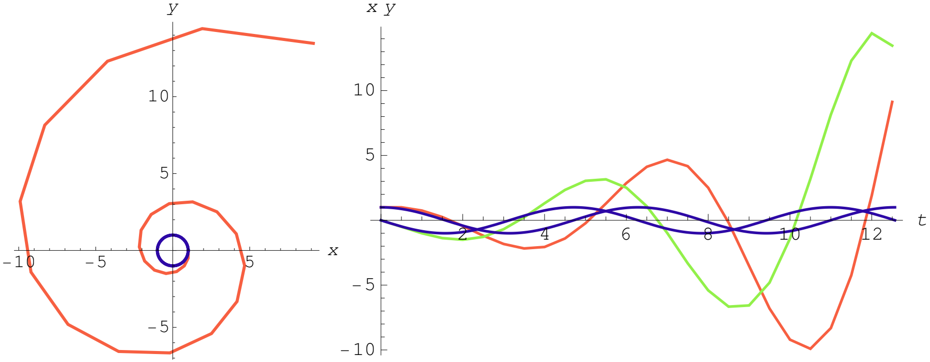




$\check{U}$ $[x' = f(x)](O \vee C) \leftrightarrow \forall \check{\varepsilon}{>}0\, [x' = f(x)](O \vee \mathscr{U}_{\check{\varepsilon}}(C))$ $(\Leftarrow$ B,V,G,K)

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

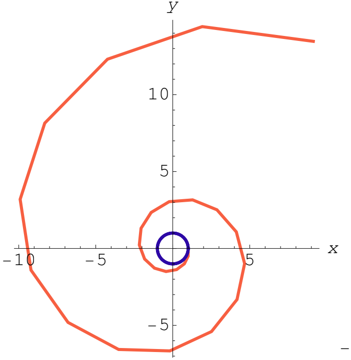
$$\vDash O \vee C \rightarrow [x' = y, y' = -x](O \vee \forall \check{\varepsilon}{>}0\, \mathscr{U}_{\check{\varepsilon}}(C))$$

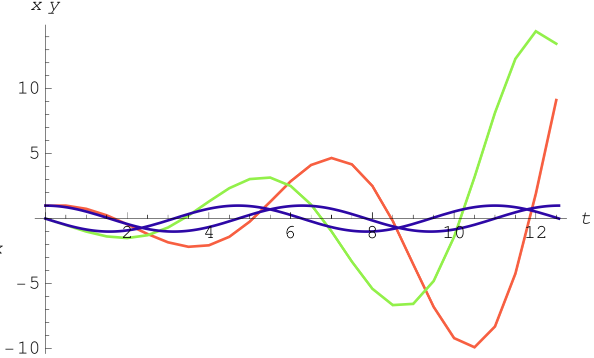


$\check{U} \quad [x' = f(x)](O \vee C) \leftrightarrow \forall \check{\varepsilon}{>}0\,[x' = f(x)](O \vee \mathscr{U}_{\check{\varepsilon}}(C)) \qquad (\Leftarrow$ B,V,G,K)

Example ((Open ∨ Closed) ⇝ Quantified Open)

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

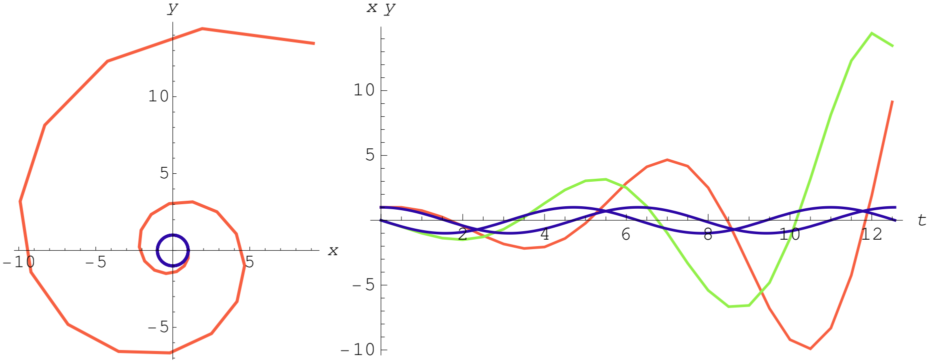




$\check{U}$ $[x' = f(x)](O \vee C) \leftrightarrow \forall \check{\varepsilon} > 0\, [x' = f(x)](O \vee \mathscr{U}_{\check{\varepsilon}}(C))$ $(\Leftarrow$ B,V,G,K)

Example ((Open ∨ Closed) ⇝ Quantified Open)

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



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

Discrete Completeness

Theorem (Relative Completeness / Continuous) (JAR'08,LICS'12)

dL *calculus is a sound & complete axiomatization of hybrid systems relative to differential equations.* $\vDash \varphi$ *implies* $\text{Taut}_{\text{FOD}} \vdash \varphi$

Theorem (Relative Completeness / Discrete) (LICS'12)

dL *calculus* $+ \overleftrightarrow{\Delta}$ *is a sound & complete axiomatization of hybrid systems relative to discrete dynamics.* $\vDash \varphi$ *implies* $\text{Taut}_{\text{DL}} \vdash \varphi$

Proof.

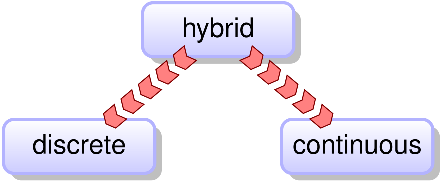
1. dL/ODE complete $\Rightarrow$ suffices $\vDash \varphi$ implies $\text{Taut}_{\text{DL}} \vdash \varphi$ for $\varphi \in \text{FOD}$
2. $[x' = f(x)]F$ for first-order F see previous slides.
3. propositional connectives and quantifiers see schematic completeness.
4. $\vdash_{\text{DL}} \langle x' = f(x)\rangle F \leftrightarrow (\langle x' = f(x)\rangle F)^\flat$ see previous slides. □

Equi-expressibility

Theorem (Equi-expressibility) (LICS'12)

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

$$\forall \varphi \; \exists \varphi^\flat \in \mathrm{FOD} \;\; \vDash \varphi \leftrightarrow \varphi^\flat$$
$$\forall \varphi \; \exists \varphi^\# \in \mathrm{DL} \;\; \vDash \varphi \leftrightarrow \varphi^\#$$

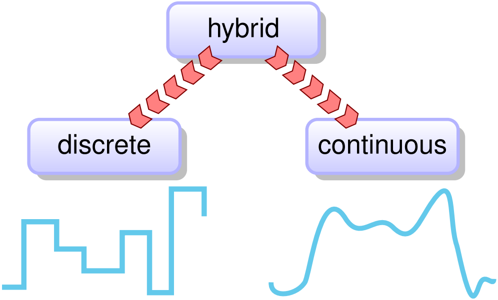


Equi-expressibility

Theorem (Equi-expressibility) (LICS'12)

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

$$\forall \varphi\ \exists \varphi^\flat \in \mathrm{FOD}\ \vDash \varphi \leftrightarrow \varphi^\flat$$
$$\forall \varphi\ \exists \varphi^\# \in \mathrm{DL}\ \vDash \varphi \leftrightarrow \varphi^\#$$

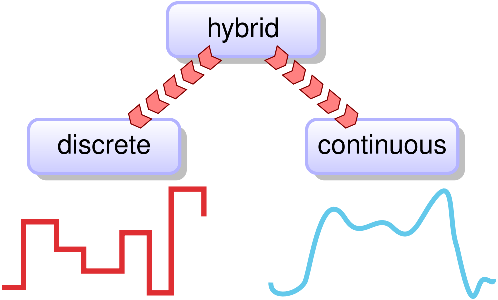


Equi-expressibility

Theorem (Equi-expressibility) (LICS'12)

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

$$\forall \varphi\ \exists \varphi^\flat \in \mathrm{FOD} \ \vDash \varphi \leftrightarrow \varphi^\flat$$
$$\forall \varphi\ \exists \varphi^\# \in \mathrm{DL} \ \vDash \varphi \leftrightarrow \varphi^\#$$

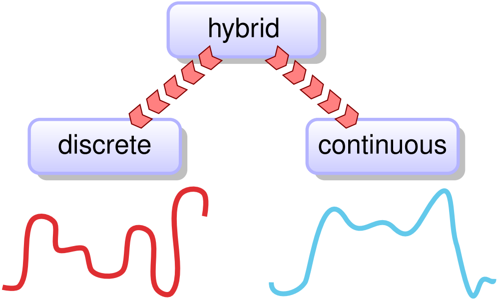


Equi-expressibility

Theorem (Equi-expressibility) (LICS'12)

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

$$\forall\varphi\ \exists\varphi^\flat \in \text{FOD}\ \vDash \varphi \leftrightarrow \varphi^\flat$$
$$\forall\varphi\ \exists\varphi^\# \in \text{DL}\ \vDash \varphi \leftrightarrow \varphi^\#$$

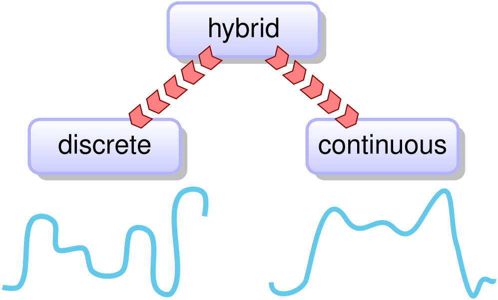


Equi-expressibility

Theorem (Equi-expressibility) (LICS'12)

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

$$\forall \varphi\ \exists \varphi^\flat \in \text{FOD} \ \vDash \varphi \leftrightarrow \varphi^\flat$$
$$\forall \varphi\ \exists \varphi^\# \in \text{DL} \ \vDash \varphi \leftrightarrow \varphi^\#$$

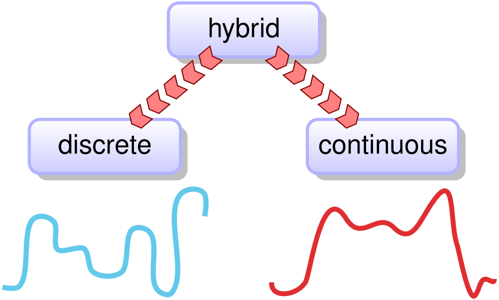


Equi-expressibility

Theorem (Equi-expressibility) (LICS'12)

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

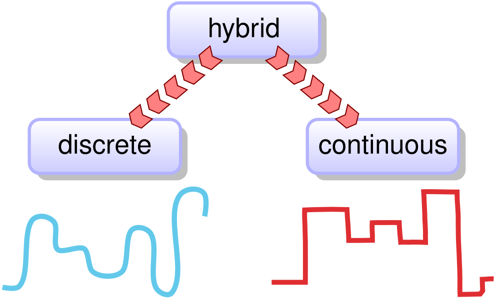
$$\forall \varphi\ \exists \varphi^\flat \in \text{FOD}\ \vDash \varphi \leftrightarrow \varphi^\flat$$
$$\forall \varphi\ \exists \varphi^\# \in \text{DL}\ \ \vDash \varphi \leftrightarrow \varphi^\#$$



Theorem (Equi-expressibility) (LICS'12)

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

$$\forall\varphi\ \exists\varphi^\flat \in \text{FOD} \ \vDash \varphi \leftrightarrow \varphi^\flat$$
$$\forall\varphi\ \exists\varphi^\# \in \text{DL} \ \vDash \varphi \leftrightarrow \varphi^\#$$

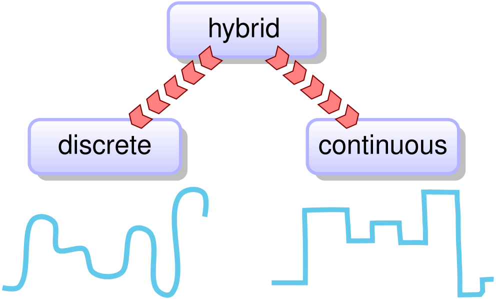


Equi-expressibility

Theorem (Equi-expressibility) (LICS'12)

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

$$\forall\varphi\ \exists\varphi^\flat \in \mathrm{FOD}\ \vDash \varphi \leftrightarrow \varphi^\flat$$
$$\forall\varphi\ \exists\varphi^\# \in \mathrm{DL}\ \vDash \varphi \leftrightarrow \varphi^\#$$



Theorem (Relative Decidability) (LICS'12)

Validity of dL *sentences is decidable relative to FOD or relative to DL.*

Proof.

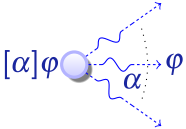
1. Let φ a sentence in dL ($\mathrm{FV}(\varphi) = \emptyset$) and ω a state.
2. Either $\omega \models \varphi$ or $\omega \not\models \varphi$. So either $\omega \models \varphi$ or $\omega \models \neg\varphi$.
3. By coincidence, $\omega \models \varphi$ iff $\nu \models \varphi$ for arbitrary ν, as $\mathrm{FV}(\varphi)$, no symbols.
4. Either $\vDash \varphi$ or $\vDash \neg\varphi$.
5. Either $\vdash_L \varphi$ or $\vdash_L \neg\varphi$ by completeness relative to $L = \mathrm{FOD}$, $L = \mathrm{DL}$. □

Outline

Complete Proof Theory of Hybrid Systems

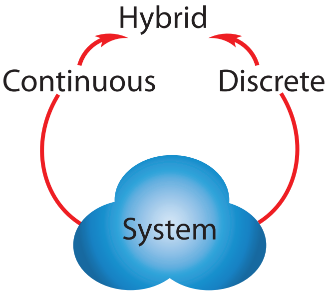
differential dynamic logic

$\mathsf{dL} = \mathsf{DL} + \mathsf{HP}$



proof-theoretical alignment

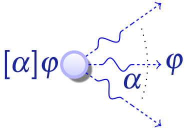
continuous = hybrid = discrete



Complete Proof Theory of Hybrid Systems

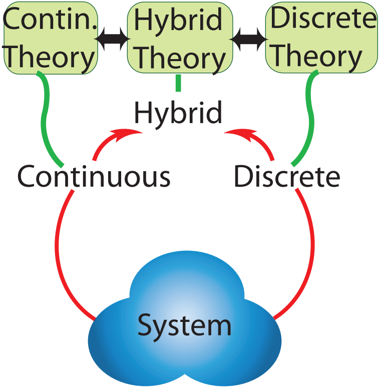
differential dynamic logic

$\mathsf{dL} = \mathsf{DL} + \mathsf{HP}$



proof-theoretical alignment

continuous = hybrid = discrete



André Platzer.
The complete proof theory of hybrid systems.
In LICS [6], pages 541–550.

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

André Platzer.
A complete uniform substitution calculus for differential dynamic logic.
J. Autom. Reas., 59(2):219–265, 2017.

André Platzer.
Differential game logic.
ACM Trans. Comput. Log., 17(1):1:1–1:51, 2015.

André Platzer.
Logics of dynamical systems.
In LICS [6], pages 13–24.

Logic in Computer Science (LICS), 2012 27th Annual IEEE Symposium on, Los Alamitos, 2012. IEEE.