TECHNISCHE UNIVERSITÄT DRESDEN

Constructing and Verifying Cyber Physical Systems

Differential Invariants

Marcus Völp

Overview

Introduction	Math
Mathematical Foundations (Differential Equations and Laplace Transformation)	
Control and Feedback	Physics
Transfer Functions and State Space Models	
Poles, Zeros / PID Control	Feedback Control
Stability, Root Locust Method, Digital Control	
Mixed-Criticality Scheduling and Real-Time Operating Systems (RTOS)	RTOS
Coordinating Networked Cyber-Physical Systems	CPS
Program Verification	Verification
Differential Dynamic Logic and KeYmaera X	
Differential Invariants	

Overview

Differential Algebraic Logic

↓

symbolaris.com

Local Reasoning about Differential Equations

↓

Andre Platzer: Logical Analysis of Hybrid-Systems

Differential Cut / Weakening

↓

Differential Induction and Differential Invariants

↓

Proving While Termination

↓

Differential Variants

↓

How to improve this Course?

Differential Dynamic Logic

$$(\text{i}\forall \text{ quantifier elimination})\ \frac{\Gamma \vdash \mathrm{QE}(\forall X\,(\Phi(X) \vdash \Psi(X))), \Delta}{\Gamma, \Phi(s(X_1,..,X_n)) \vdash \Psi(s(X_1,..,X_n)), \Delta}\ 3 \qquad (\text{i}\exists \text{ eliminate existential})\ \frac{\Gamma \vdash \mathrm{QE}(\exists X\ \bigwedge_i(\Phi_i \vdash \Psi_i)), \Delta}{\Gamma, \Phi_1 \vdash \Psi_1, \Delta \quad \ldots \quad \Gamma, \Phi_n \vdash \Psi_n, \Delta}\ 4$$

$$([]\text{ generalization})\ \frac{\Gamma \vdash [\alpha]\phi, \Delta \qquad \Gamma \vdash \forall^\alpha(\phi \to \psi), \Delta}{\Gamma \vdash [\alpha]\psi, \Delta} \qquad (\langle\rangle\text{ generalization})\ \frac{\Gamma \vdash \langle\alpha\rangle\phi, \Delta \qquad \Gamma \vdash \forall^\alpha(\phi \to \psi), \Delta}{\Gamma \vdash \langle\alpha\rangle\psi, \Delta}$$

$$(\textit{ind}\text{ loop invariant})\ \frac{\Gamma \vdash \phi, \Delta \qquad \Gamma \vdash \forall^\alpha(\phi \to [\alpha]\phi), \Delta \qquad \Gamma \vdash \forall^\alpha(\phi \to \psi), \Delta}{\Gamma \vdash [\alpha^*]\psi, \Delta}$$

$$(\textit{con}\text{ loop convergence})\ \frac{\Gamma \vdash \exists v\,\varphi(v), \Delta \qquad \Gamma \vdash \forall^\alpha \forall v{>}0\,(\varphi(v) \to \langle\alpha\rangle\varphi(v-1)), \Delta \qquad \Gamma \vdash \forall^\alpha(\exists v{\leq}0\,\varphi(v) \to \psi), \Delta}{\Gamma \vdash \langle\alpha^*\rangle\psi, \Delta}$$

$$(DI\text{ differential invariant})\ \frac{\Gamma, H \vdash F, \Delta \qquad \Gamma \vdash \forall^\alpha(H \to F'^{\theta_1 \ldots \theta_n}_{x_1' \ldots x_n'}), \Delta}{\Gamma \vdash [x_1' = \theta_1, .., x_n' = \theta_n \,\&\, H]F, \Delta}$$

$$(DV\text{ differential variant})\ \frac{\Gamma \vdash [x_1' = \theta_1, .., x_n' = \theta_n \,\&\, {\sim}F]H, \Delta \qquad \Gamma \vdash \exists\varepsilon{>}0\,\forall^\alpha(\neg F \wedge H \to (F' \geq \varepsilon)^{\theta_1 \ldots \theta_n}_{x_1' \ldots x_n'}), \Delta}{\Gamma \vdash \langle x_1' = \theta_1, .., x_n' = \theta_n \,\&\, H\rangle F, \Delta}\ 5$$

$$(DW\text{ differential weaken})\ \frac{\Gamma \vdash \forall^\alpha(H \to \phi), \Delta}{\Gamma \vdash [x' = \theta \,\&\, H]\phi, \Delta}$$

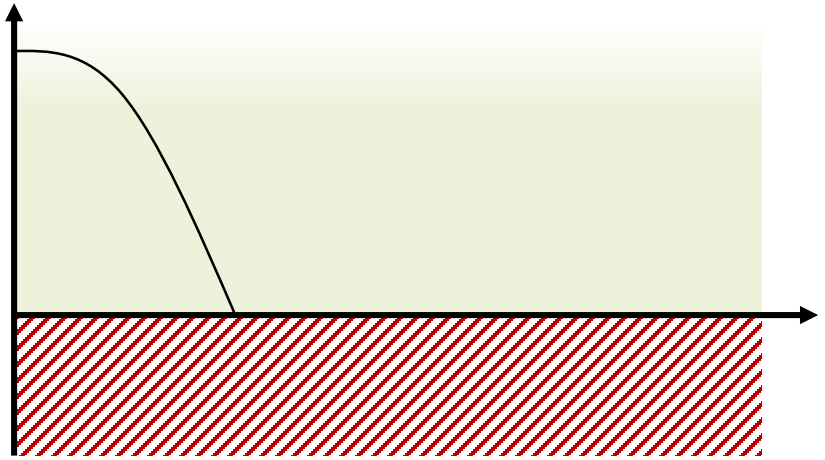
$$(DC\text{ differential cut})\ \frac{\Gamma \vdash [x' = \theta \,\&\, H]C, \Delta \qquad \Gamma \vdash [x' = \theta \,\&\, (H \wedge C)]\phi, \Delta}{\Gamma \vdash [x' = \theta \,\&\, H]\phi, \Delta}$$

$$(DA\text{ differential auxiliaries})\ \frac{\phi \leftrightarrow \exists y\,\psi \qquad \Gamma \vdash [x' = \theta, y' = \vartheta \,\&\, H]\psi, \Delta}{\Gamma \vdash [x' = \theta \,\&\, H]\phi, \Delta}\ 6$$

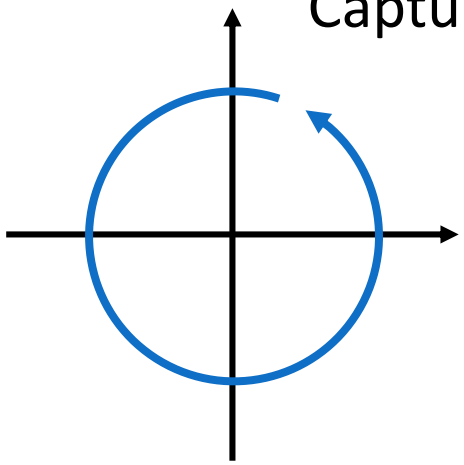
$$(IA\text{ auxiliary variable})\ \frac{\Gamma \vdash [y := \theta]\phi, \Delta}{\Gamma \vdash \phi, \Delta}\ 7 \qquad (\langle :* \rangle\text{ random})\ \frac{\exists X\,\langle x := X\rangle\phi}{\langle x := *\rangle\phi}\ 8 \qquad ([:*]\text{ random})\ \frac{\forall X\,[x := X]\phi}{[x := *]\phi}\ 8$$

Differential Algebraic Logic

$$\{h' = v, v' = -g \,\&\, h \geq 0\}$$



Capture short term evolution of complicated dynamics

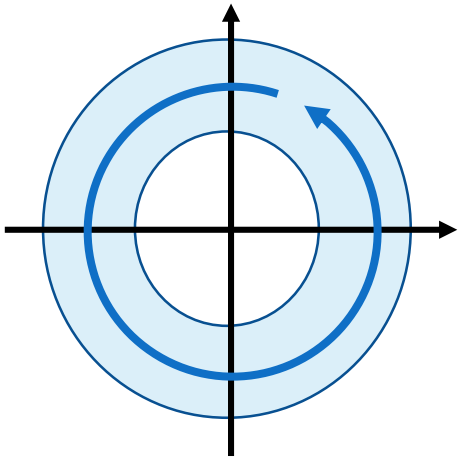


$$\{x' = r\,cos(\varphi), y' = r\,sin(\varphi), \varphi' = \omega\}$$

$$\{x' = d_1, y' = d_2 \,\&\, d_1' = -\omega d_2 \wedge d_2' = \omega d_1 \wedge d_1^2 + d_2^2 = r^2\}$$

Differential Algebraic Logic

$$\{h' = v, v' = -g \,\&\, h \geq 0\}$$



Capture parametric systems with reasonable bounds for all parameters

=> we need a symbolic solution

$$\{x' = d_1, y' = d_2 \,\&\, \exists\omega.\, -1 < \omega \wedge w < 1 \wedge d_1' = -\omega d_2 \wedge d_2' = \omega d_1 \wedge d_1^2 + d_2^2 = r^2\}$$

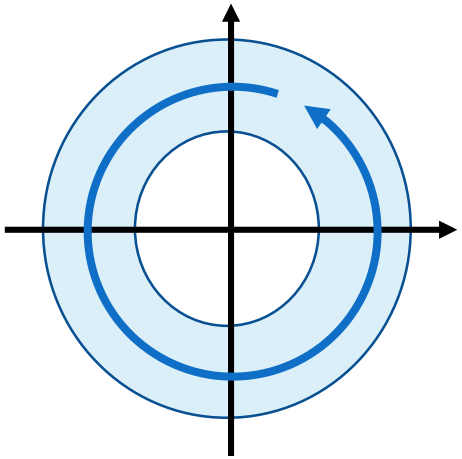
$$\{x' = d_1, y' = d_2 \,\&\, \exists r.\, 3 < r \wedge r < 4 \wedge d_1' = -\omega d_2 \wedge d_2' = \omega d_1 \wedge d_1^2 + d_2^2 = r^2\}$$

Differential Algebraic Constraints

E.g. "Whatever parametrized obstacles do, the car has a chance to avoid collision!" $\exists p.\, [\alpha]\langle\beta\rangle\varphi$

Differential Jump Constraints: $\exists a.\, (w := a^2 \wedge a < 5)$

Differential Algebraic Logic



Semantic:

Differential Jump Constraints:

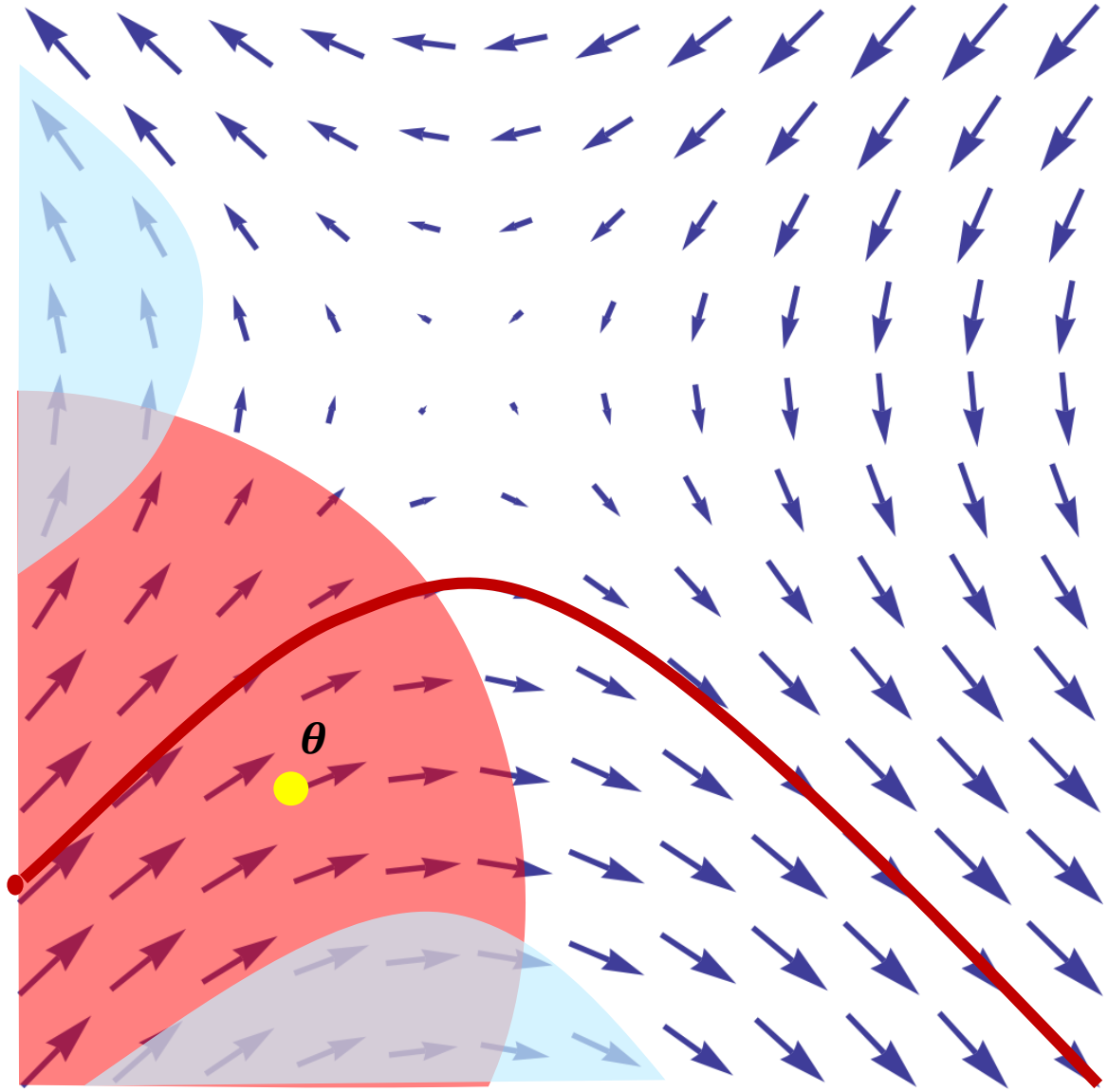
$(v, w) \vDash \forall x.\, \Phi \iff (v_x, w) \vDash \Phi$

for all states v_x that agree with v but have an arbitrary value r at x

$(v, w) \vDash \exists x.\, \Phi \iff (v_x, w) \vDash \Phi$

for some v_x with some value r at x

Local Reasoning about Diff. Eq.



$$\{x' = \theta \,\&H\}$$

At every point, the right hand side of the differential equation describes the dynamics where this point moves to.

$(DI$ differential invariant$)$

$(DV$ differential variant$)$

$(DW$ differential weaken$)$

$(DC$ differential cut$)$

$(DA$ differential auxiliaries$)$

Symbolic Differentiation

Idea: compute the derivative of the differential equation and the property to show
=> $\boldsymbol{\theta}$ in $\{\boldsymbol{x}' = \boldsymbol{\theta}\}$ immediately reveals how the property evolves at each point

$$D(r) = 0$$

$$D\left(x^{(n)}\right) = x^{(n+1)} \quad (e.g., D(x') = x'')$$

$$D(a + b) = D(a) + D(b)$$

$$D(a - b) = D(a) - D(b)$$

$$D(a \cdot b) = D(a) \cdot b + a \cdot D(b)$$

$$D\left(\frac{a}{b}\right) = D(a) \cdot b - a \cdot D(b)/b^2$$

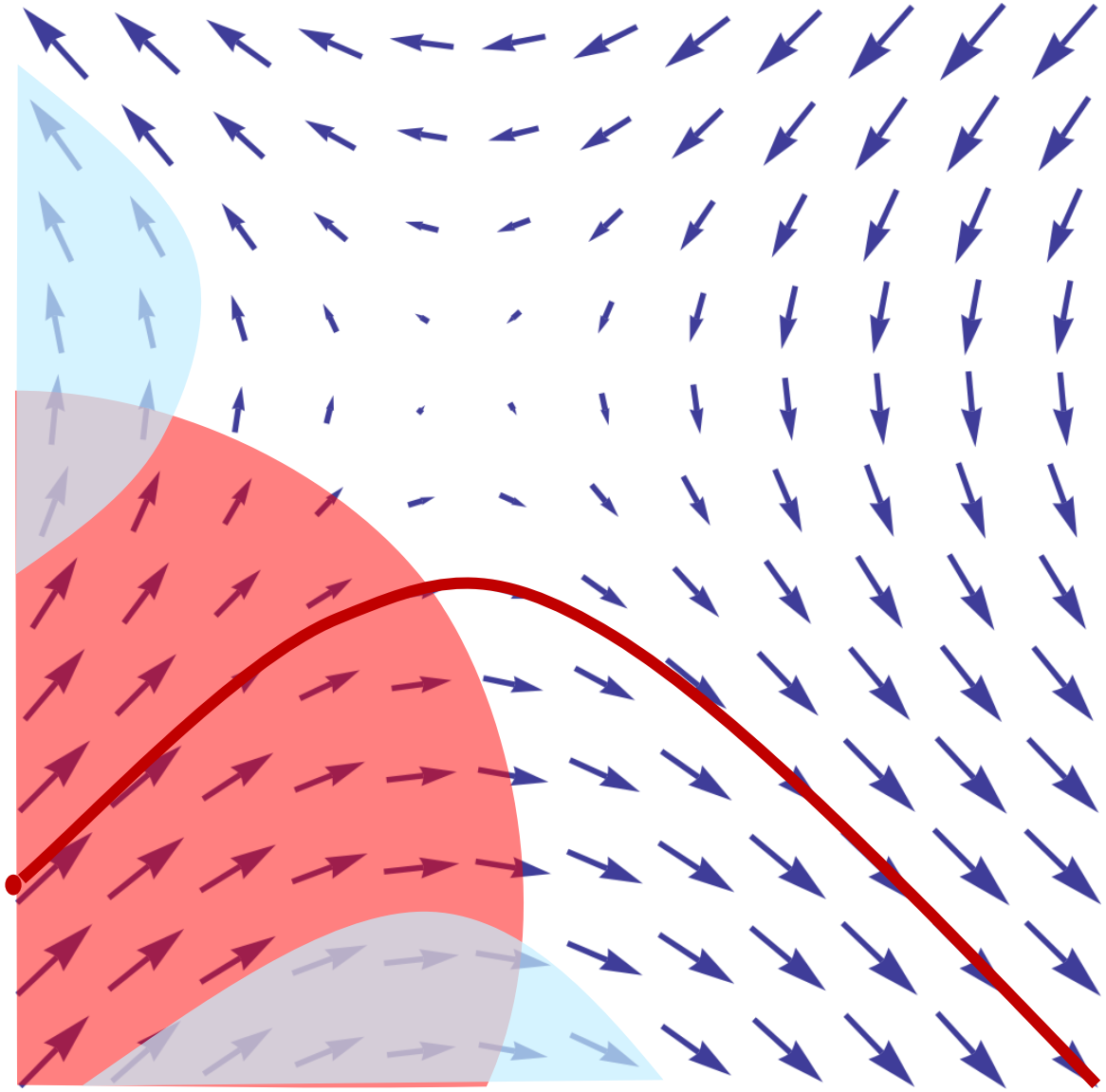
$$D(F) = \bigwedge_{i=1}^{m} D(F_i) \; where \; \{F_1, \ldots, F_m\} \; is \; the \; set \; of \; literals \; in \; F$$

$$D(a * b) = D(a) * D(b) \; where \; * \; \epsilon \{\leq, \geq, <, >, =\}$$

$$D(\neg a) = \neg D(a)$$

in particular: $D(a \vee b) = D(a) \wedge D(b)$

Local Reasoning about Diff. Eq.



(DI differential invariant)

(DV differential variant)

(DW differential weaken)

(DC differential cut)

(DA differential auxiliaries)

differentially augmented state

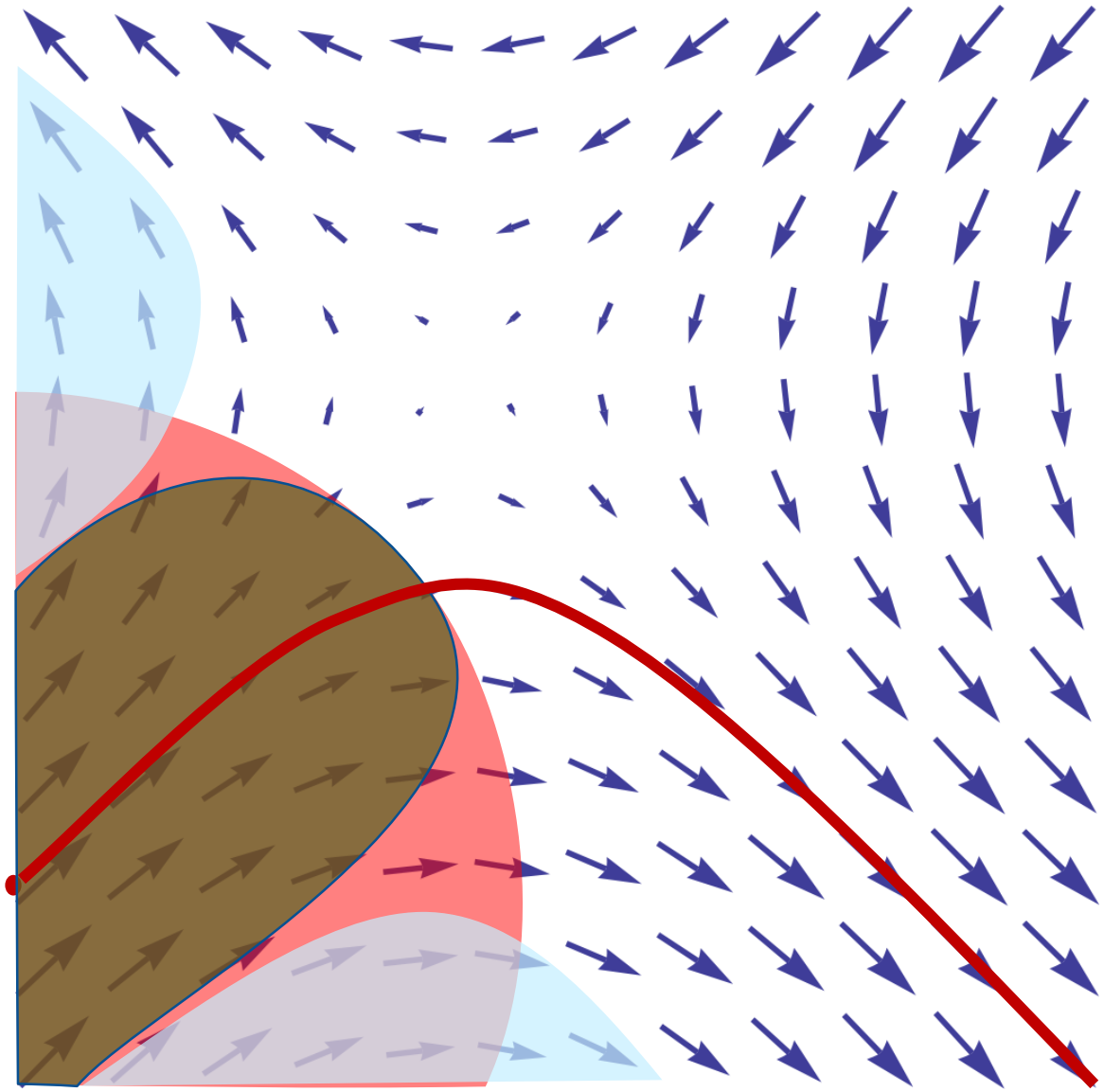
like $\varphi(\zeta)$ except $x^{(n)} = \frac{d^n \varphi(t)(x)}{dt^n}(\zeta)$

Lemma 3.1: (Derivation Lemma).

$$\frac{\boldsymbol{d\, val(\varphi(t), \theta)}}{\boldsymbol{dt}}(\boldsymbol{\zeta}) = \boldsymbol{val}\big(\overline{\boldsymbol{\varphi}}(\boldsymbol{\zeta}), \boldsymbol{D(\theta)}\big)$$

along the flow, analytic derivatives of valuations co-incide with valuations of syntactic derivations.

Differential Weaken



(DI differential invariant)

(DV differential variant)

(DW differential weaken)

(DC differential cut)

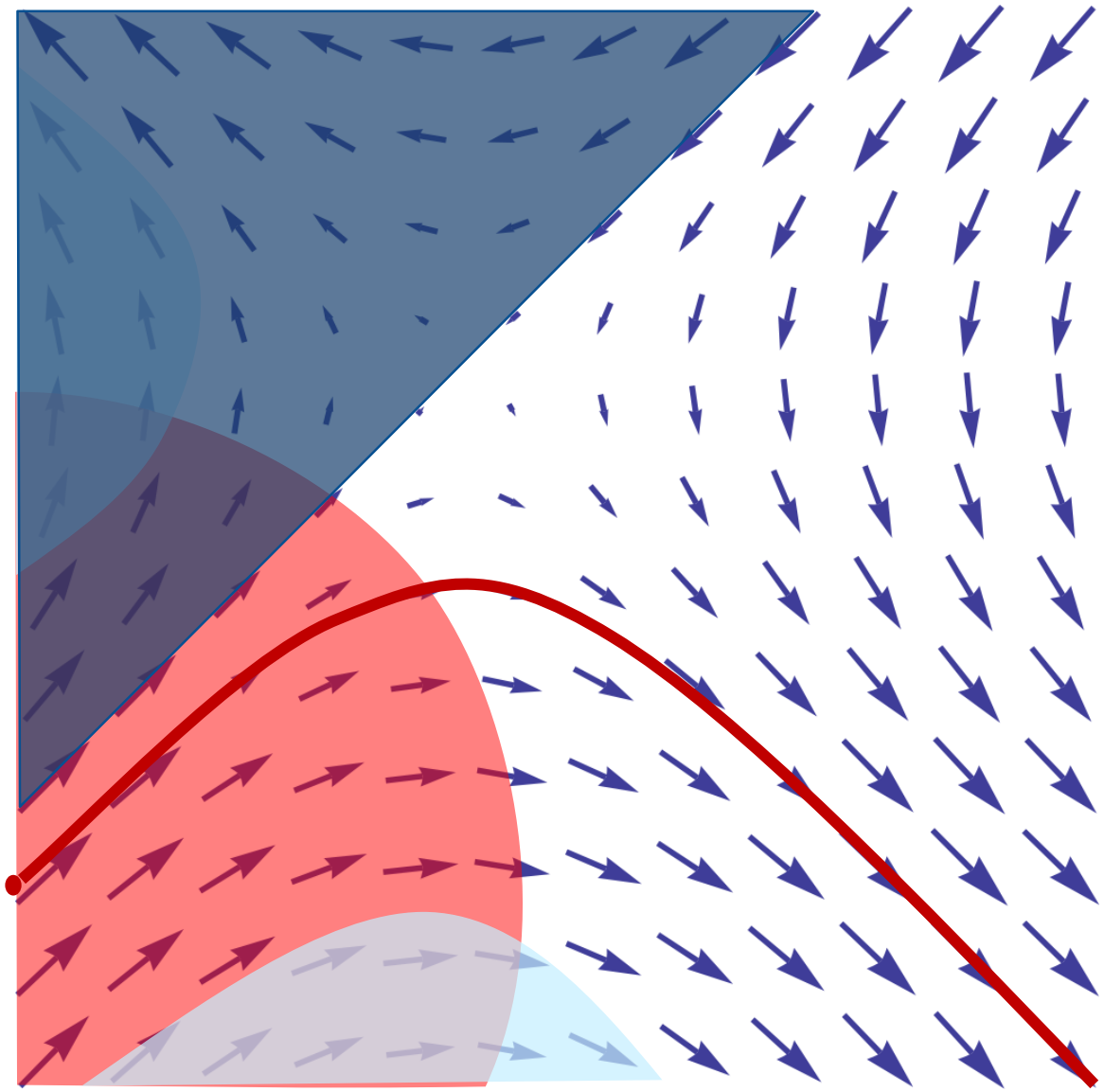
(DA differential auxiliaries)

DW: differential weaken

$$\frac{\Gamma \vdash \forall^{\alpha}(H \rightarrow \phi), \Delta}{\Gamma \vdash [x' = \theta \& H]\phi, \Delta}$$

Ignore differential equation if evolution domain constraint H already implies ϕ.

Differential Cut



(DI differential invariant)

(DV differential variant)

(DW differential weaken)

(DC differential cut)

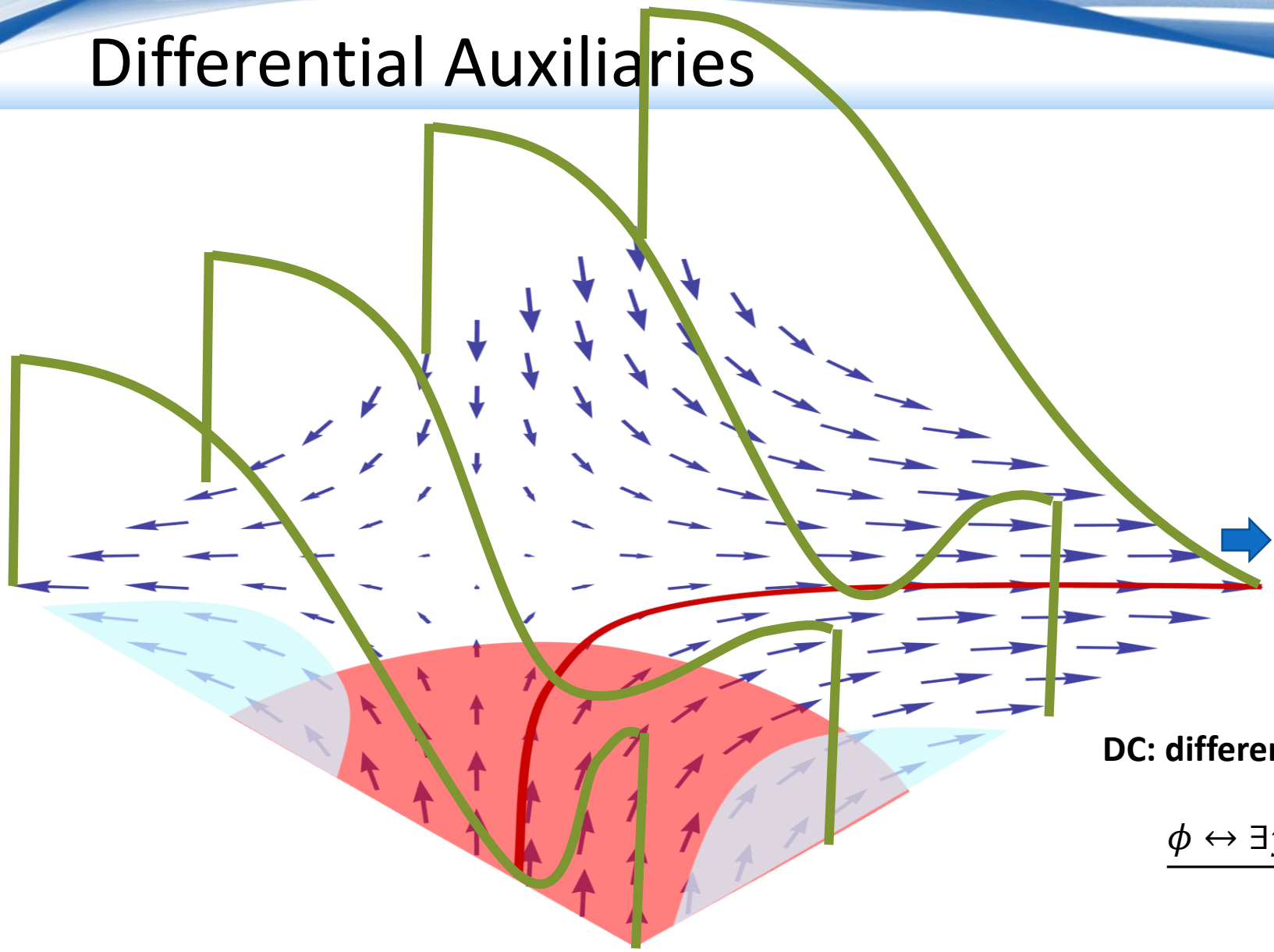
(DA differential auxiliaries)

DC: differential cut

$$\frac{\Gamma \vdash [x' = \theta \& H]C, \Delta \qquad \Gamma \vdash [x' = \theta \& H \wedge C]\phi, \Delta}{\Gamma \vdash [x' = \theta \& H]\phi, \Delta}$$

Ignore differential equation if evolution domain constraint H already implies ϕ.

Differential Auxiliaries



(DI differential invariant)

(DV differential variant)

(DW differential weaken)

(DC differential cut)

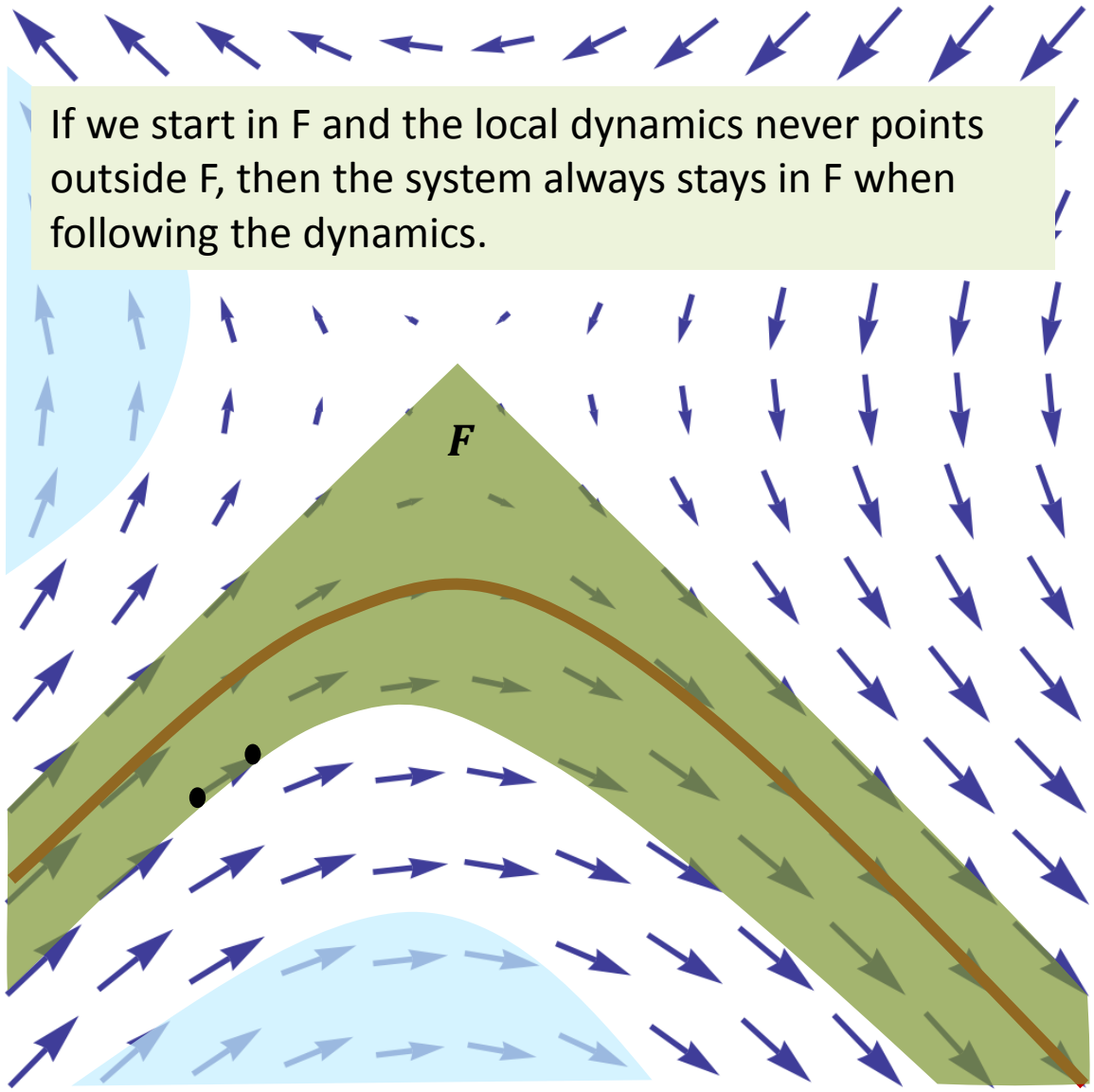
(DA differential auxiliaries)

DC: differential cut

$$\frac{\phi \leftrightarrow \exists y \Psi \qquad \Gamma \vdash [x' = \theta, y' = \nu \& H]\Psi, \Delta}{\Gamma \vdash [x' = \theta \& H]\phi, \Delta}$$

Ignore differential equation if evolution domain constraint H already implies ϕ.

Differential Induction



Induction (over iterations)

$$\frac{\vdash \forall^{\alpha} \phi \rightarrow [\alpha]\phi}{\phi \vdash [\alpha^*]\phi}$$

DI: Differential Induction

- Continuous form of induction
- Derivative points to the direction how the solution of a differential equation will evolve

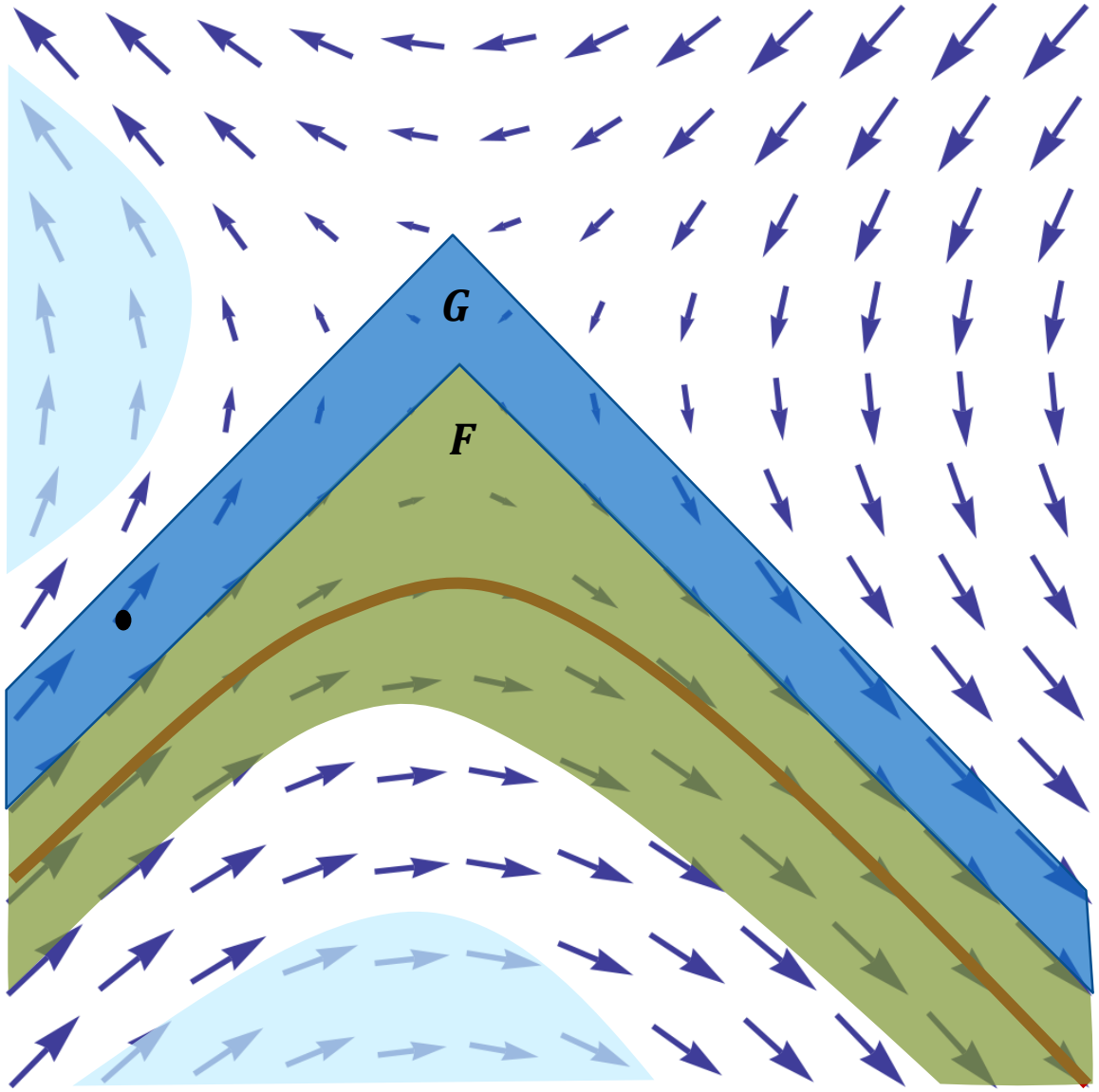
$$\frac{\Gamma, H \vdash F, \Delta \qquad \Gamma \vdash \forall^{\alpha}(H \rightarrow {F'}^{\theta_1,\ldots,\theta_n}_{x'_1,\ldots,x'_n}), \Delta}{\Gamma \vdash [x'_1 = \theta_1, \ldots, x'_n = \theta_n \& H]F, \Delta}$$

where ${F'}^{\theta_1,\ldots,\theta_n}_{x'_1,\ldots,x'_n}$ abbreviates $D(F)$ with $z' = 0$ for variables that do not change.

Differential Invariant:

- Region where the derivative always points into the region

Differential Induction



DI: Differential Induction

$$\frac{\Gamma, H \vdash F, \Delta \qquad \Gamma \vdash \forall^{\alpha}(H \rightarrow F'^{\theta_1,\ldots,\theta_n}_{x'_1,\ldots,x'_n}), \Delta}{\Gamma \vdash [x'_1 = \theta_1, \ldots, x'_n = \theta_n \& H]F, \Delta}$$

Notice: it is crucial that

$$D(F \vee G) = D(F) \wedge D(G)$$

or alternatively:

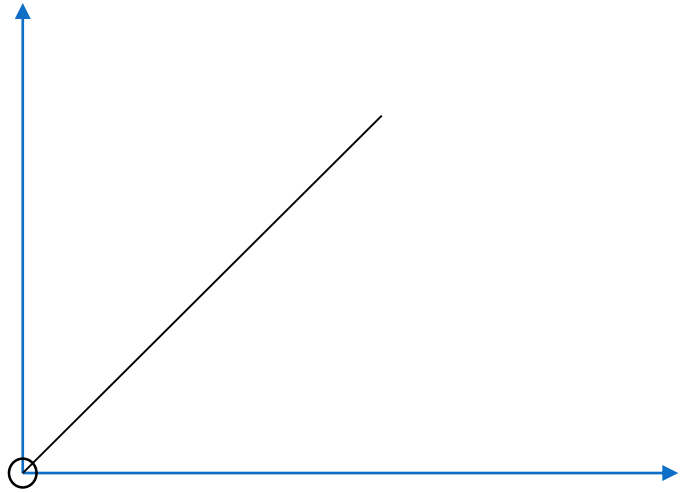
$$D(F \vee G) = (F \wedge D(F)) \vee (G \wedge D(G))$$

Differential Induction

UNSOUND!!! Differential Induction

$$\frac{\vdash \forall^{\alpha}(F \wedge H \to F'^{\theta_1,\ldots,\theta_n}_{x'_1,\ldots,x'_n})}{[H]F \vdash [x'_1 = \theta_1, \ldots, x'_n = \theta_n \& H]F}$$

$$\frac{\frac{*\,(unsound)}{\vdash \forall x.\,(x^2 \leq 0 \to 2x \leq 0)}}{x^2 \leq 0 \vdash [x' = 1]x^2 \leq 0}$$



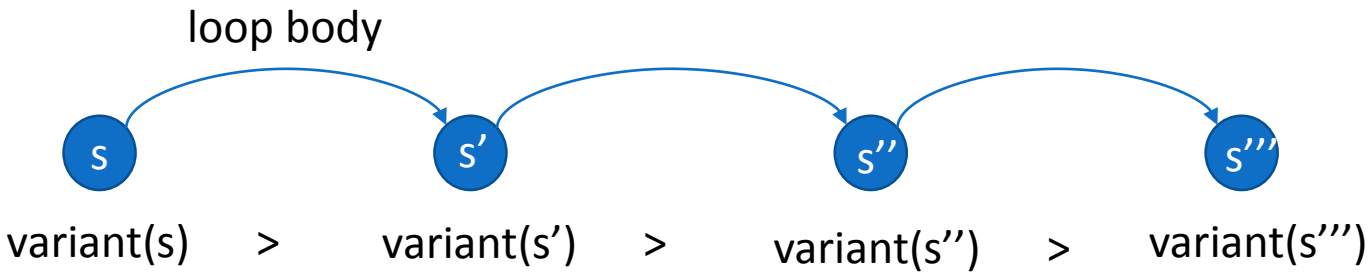
It is unsound to restrict the "induction step" to F only.

While Termination

Loop variant:
mathematical function on program state space whose value is monotonically decreasing wrt. a well-founded relation.

Well-founded relation:
Every nonempty subset $S \subseteq X$ of a class X has a minimal element:

$$\forall S \subseteq X. S \neq \emptyset \rightarrow \exists m \in S. \forall\, s \in S\ (s, m) \notin R$$



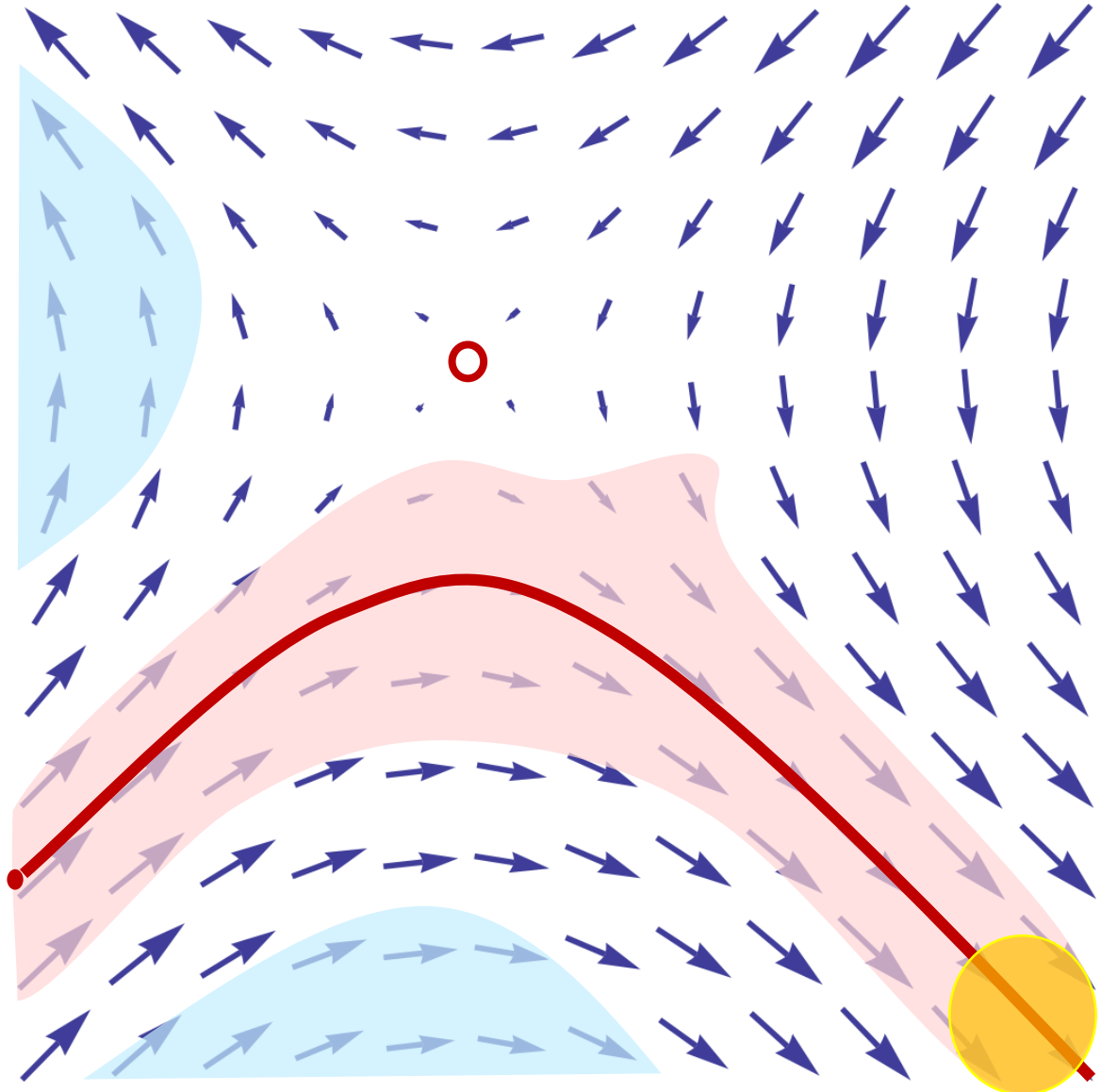
partial correctness:

$$\frac{\{I \wedge C\} S \{I\}}{\{I\}\ \textbf{while}\ C\ \textbf{do}\ S\ \{I\ \wedge \neg C\}}$$

total correctness:

$$\frac{< well\text{–}founded\ \ \{I \wedge C \wedge V = z\} S \{I \wedge V < z\}}{\{I\}\ \textbf{while}\ C\ \textbf{do}\ S\ \{I\ \wedge \neg C\}}$$

Differential Variant



DV: Differential Variant

$$\frac{\Gamma \vdash \exists \varepsilon > 0.\, \forall^{\alpha} (\neg F \wedge H \rightarrow (F' \geq \varepsilon)^{\theta_1,\ldots,\theta_n}_{x'_1,\ldots,x'_n}), \Delta}{\Gamma \vdash \langle x'_1 = \theta_1, \ldots, x'_n = \theta_n \& H \rangle F, \Delta}$$

where ~ is the weak negation, i.e., like ¬ except that $\sim(a \geq b) \equiv b \geq a$ and $\sim(\mathrm{a} > \mathrm{b}) \equiv a \leq b$

Overview

Differential Algebraic Logic

↓

symbolaris.com

Local Reasoning about Differential Equations

↓

Andre Platzer: Logical Analysis of Hybrid-Systems

Differential Cut / Weakening

↓

Differential Induction and Differential Invariants

↓

Proving While Termination

↓

Differential Variants

↓

How to improve this Course?

Overview

Introduction	Math
Mathematical Foundations (Differential Equations and Laplace Transformation)	
Control and Feedback	Physics
Transfer Functions and State Space Models	
Poles, Zeros / PID Control	Feedback Control
Stability, Root Locust Method, Digital Control	
Mixed-Criticality Scheduling and Real-Time Operating Systems (RTOS)	RTOS
Coordinating Networked Cyber-Physical Systems	CPS
Program Verification	Verification
Differential Dynamic Logic and KeYmaera X	
Differential Invariants	