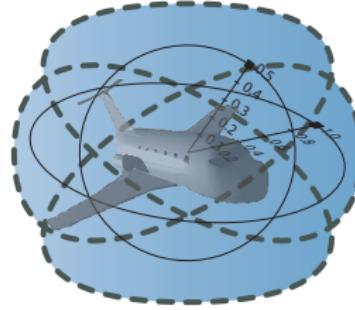


12: Ghosts & Differential Ghosts

15-424: Foundations of Cyber-Physical Systems

André Platzer

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



Outline

- 1 Learning Objectives
- 2 Recap: Proofs for Differential Equations
- 3 The Ghosts of CPS
 - Arithmetic Ghosts
 - Ghosts of Choice
 - Differential-algebraic Ghosts
 - Discrete Ghosts
 - Differential Ghosts
 - Substitute Ghosts
 - Solvable Ghosts
 - Axiomatic Ghosts
- 4 Summary

Outline

1 Learning Objectives

2 Recap: Proofs for Differential Equations

3 The Ghosts of CPS

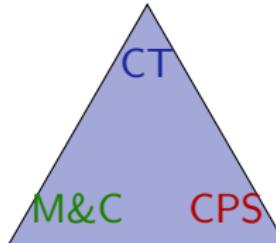
- Arithmetic Ghosts
- Ghosts of Choice
- Differential-algebraic Ghosts
- Discrete Ghosts
- Differential Ghosts
- Substitute Ghosts
- Solvable Ghosts
- Axiomatic Ghosts

4 Summary

Learning Objectives

Ghosts & Differential Ghosts

- rigorous reasoning about ODEs
- extra dimensions for extra invariants
- higher-dimensional retreat
- extra state enables reasoning
- invent dark energy
- intuition for differential invariants
- states and proofs



- none: ghosts are for proofs
- mark ghosts in models
- syntax of models
- solutions of ODEs

- relations of state
- extra ghost state
- CPS semantics

Outline

1 Learning Objectives

2 Recap: Proofs for Differential Equations

3 The Ghosts of CPS

- Arithmetic Ghosts
- Ghosts of Choice
- Differential-algebraic Ghosts
- Discrete Ghosts
- Differential Ghosts
- Substitute Ghosts
- Solvable Ghosts
- Axiomatic Ghosts

4 Summary

Differential Invariants for Differential Equations

Differential Weakening

$$\frac{Q \vdash F}{P \vdash [x' = f(x) \& Q]F}$$

Differential Invariant

$$\frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \& Q]F}$$

Differential Cut

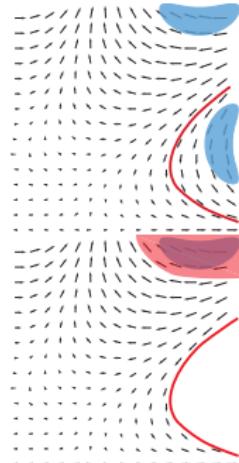
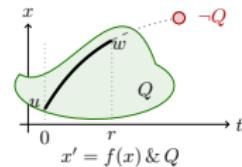
$$\frac{F \vdash [x' = f(x) \& Q]C \quad F \vdash [x' = f(x) \& Q \wedge C]F}{F \vdash [x' = f(x) \& Q]F}$$

$$\text{DW } [x' = f(x) \& Q]F \leftrightarrow [x' = f(x) \& Q](Q \rightarrow F)$$

$$\text{DI } [x' = f(x) \& Q]F \leftarrow (Q \rightarrow F \wedge [x' = f(x) \& Q](F)')$$

$$\text{DC } ([x' = f(x) \& Q]F \leftrightarrow [x' = f(x) \& Q \wedge C]F) \leftarrow [x' = f(x) \& Q]C$$

$$\text{DE } [x' = f(x) \& Q]F \leftrightarrow [x' = f(x) \& Q][x' := f(x)]F$$



Outline

1 Learning Objectives

2 Recap: Proofs for Differential Equations

3 The Ghosts of CPS

- Arithmetic Ghosts
- Ghosts of Choice
- Differential-algebraic Ghosts
- Discrete Ghosts
- Differential Ghosts
- Substitute Ghosts
- Solvable Ghosts
- Axiomatic Ghosts

4 Summary

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

Wait, what about ...

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

$$\textcircled{1} \quad e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$$

$$\textcircled{2} \quad -e \stackrel{\text{def}}{=} 0 - e$$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

$$① \quad e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$$

$$② \quad -e \stackrel{\text{def}}{=} 0 - e$$

$$③ \quad e^n$$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

$$① \quad e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$$

$$② \quad -e \stackrel{\text{def}}{=} 0 - e$$

$$③ \quad e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e$$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

$$① \quad e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$$

$$② \quad -e \stackrel{\text{def}}{=} 0 - e$$

$$③ \quad e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \text{ } n \in \mathbb{N} \text{ times, not } e^\pi$$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

$$\textcircled{1} \quad e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$$

$$\textcircled{2} \quad -e \stackrel{\text{def}}{=} 0 - e$$

$$\textcircled{3} \quad e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$$

$$\textcircled{4} \quad e/k$$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends}$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

$$\textcircled{1} \quad e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$$

$$\textcircled{2} \quad -e \stackrel{\text{def}}{=} 0 - e$$

$$\textcircled{3} \quad e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \quad n \in \mathbb{N} \text{ times, not } e^\pi$$

$$\textcircled{4} \quad e/k \stackrel{\text{def}}{=} \text{depends} \quad q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b$$

Arithmetic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

$$\textcircled{1} \quad e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$$

$$\textcircled{2} \quad -e \stackrel{\text{def}}{=} 0 - e$$

$$\textcircled{3} \quad e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \quad n \in \mathbb{N} \text{ times, not } e^\pi$$

$$\textcircled{4} \quad e/k \stackrel{\text{def}}{=} \begin{array}{l} \text{depends} \\ q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \\ q := \frac{b}{c} \end{array}$$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b$
 $q := \frac{b}{c} \quad \rightsquigarrow \quad q := *; ?qc = b$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$
 $q := \frac{b}{c} \quad \rightsquigarrow \quad q := *; ?qc = b \wedge c \neq 0$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$
 $q := \frac{b}{c} \rightsquigarrow q := *; ?qc = b \wedge c \neq 0$

$$x := 2 + \frac{b}{c} + e$$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$q := \frac{b}{c} \quad \rightsquigarrow \quad q := *; ?qc = b \wedge c \neq 0$$

$$x := 2 + \frac{b}{c} + e \quad \rightsquigarrow \quad q := *; ?qc = b \quad ; \quad x := 2 + q + e$$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$q := \frac{b}{c} \quad \rightsquigarrow \quad q := *; \ ?qc = b \wedge c \neq 0$$

$$x := 2 + \frac{b}{c} + e \quad \rightsquigarrow \quad q := *; \ ?qc = b \wedge c \neq 0; \ x := 2 + q + e$$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$q := \frac{b}{c} \quad \rightsquigarrow \quad q := *; ?qc = b \wedge c \neq 0$$

$$x := 2 + \frac{b}{c} + e \quad \rightsquigarrow \quad q := *; ?qc = b \wedge c \neq 0; x := 2 + q + e$$

$$x := a + \sqrt{4y}$$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$q := \frac{b}{c} \quad \rightsquigarrow \quad q := *; \ ?qc = b \wedge c \neq 0$$

$$x := 2 + \frac{b}{c} + e \quad \rightsquigarrow \quad q := *; \ ?qc = b \wedge c \neq 0; \ x := 2 + q + e$$

$$x := a + \sqrt{4y} \quad \rightsquigarrow \quad q := *; \ ?q^2 = 4y; \ x := a + q$$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$q := \frac{b}{c} \quad \rightsquigarrow \quad q := *; \ ?qc = b \wedge c \neq 0$$

$$x := 2 + \frac{b}{c} + e \quad \rightsquigarrow \quad q := *; \ ?qc = b \wedge c \neq 0; \ x := 2 + q + e$$

$$x := a + \sqrt{4y} \quad \rightsquigarrow \quad q := *; \ ?q^2 = 4y \wedge 4y \geq 0; \ x := a + q$$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

④ arithmetic ghost: auxiliary for the model where $c \neq 0$

$$q := \frac{b}{c} \rightsquigarrow q := *; ?qc = b \wedge c \neq 0$$

$$x := 2 + \frac{b}{c} + e \rightsquigarrow q := *; ?qc = b \wedge c \neq 0; x := 2 + q + e$$

$$x := a + \sqrt{4y} \rightsquigarrow q := *; ?q^2 = 4y \wedge 4y \geq 0; x := a + q$$

Arithmetic Ghosts / Ghosts of Division

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

① $e - k \stackrel{\text{def}}{=} e + (-1) \cdot k$

② $-e \stackrel{\text{def}}{=} 0 - e$

③ $e^n \stackrel{\text{def}}{=} e \cdot \dots \cdot e \ n \in \mathbb{N} \text{ times, not } e^\pi$

nondeterministic assignment $q := *$ not in syntax

$$q := * \quad \text{not in syntax}$$

$$q := \frac{b}{c} \quad \rightsquigarrow \quad q := *; \ ?qc = b \wedge c \neq 0$$

$$x := 2 + \frac{b}{c} + e \quad \rightsquigarrow \quad q := *; \ ?qc = b \wedge c \neq 0; \ x := 2 + q + e$$

$$x := a + \sqrt{4y} \quad \rightsquigarrow \quad q := *; \ ?q^2 = 4y \wedge 4y \geq 0; \ x := a + q$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax.

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax. ① Modular add

Syntax

$\alpha ::= \dots \mid x := *$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax. ① Modular add

Syntax

$\alpha ::= \dots \mid x := *$

Semantics

$\llbracket x := * \rrbracket = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax. ① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow$$
$$[:*] [x := *] P \leftrightarrow$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax. ① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$
$$[:*] [x := *] P \leftrightarrow \forall x P$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax.

① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$
$$[:*] [x := *] P \leftrightarrow \forall x P$$

② Or derived definition

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax.

① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$

$$[:*] [x := *] P \leftrightarrow \forall x P$$

② Or derived definition

Derived

$$x := * \stackrel{\text{def}}{\equiv}$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax.

① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$

$$[:*] [x := *] P \leftrightarrow \forall x P$$

② Or derived definition

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1 \cup x' = -1$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax.

① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$

$$[:*] [x := *] P \leftrightarrow \forall x P$$

② Or derived definition

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1 \cup x' = -1$$

Derived

$$x := * \stackrel{\text{def}}{\equiv}$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax.

① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$
$$[:*] [x := *] P \leftrightarrow \forall x P$$

② Or derived definition

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1 \cup x' = -1$$

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1; x' = -1$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax. ① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$
$$[\dots] [\![x := *]\!] P \leftrightarrow \forall x P$$

discrete time?

continuous time?

② Or derived definition

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1 \cup x' = -1$$

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1; x' = -1$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax.

① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$

$$[:*] [x := *] P \leftrightarrow \forall x P$$

invisible time! time is relative.

② Or derived definition

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1 \cup x' = -1$$

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1; x' = -1$$

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax.

① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$

$$[:*] [x := *] P \leftrightarrow \forall x P$$

invisible time! time is relative.

② Or derived definition

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1 \cup x' = -1$$

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1; x' = -1$$

$x := * \not\equiv x' = 1, t' = 1 \cup x' = -1, t' = 1$ visible time

Ghosts of Choice: Nondeterministic Assignment

Nondeterministic assignment $x := *$ not in HP syntax. ① Modular add

Syntax

$$\alpha ::= \dots \mid x := *$$

Semantics

$$[\![x := *]\!] = \{(\omega, \nu) : \nu = \omega \text{ except for value of } x \text{ (any } \mathbb{R})\}$$

Axioms

$$\langle :* \rangle \langle x := * \rangle P \leftrightarrow \exists x P$$

$$[:*] [x := *] P \leftrightarrow \forall x P$$

② Or derived definition

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1 \cup x' = -1$$

Derived

$$x := * \stackrel{\text{def}}{\equiv} x' = 1; x' = -1$$

I'm just a ghost of your imagination. I'm definable.

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0$$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow \textcolor{red}{q := *; ?qc=1; } x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \& 2x \neq 0 \wedge \frac{c}{2x} > 0$$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \& 2x \neq 0 \wedge \frac{c}{2x} > 0 \rightsquigarrow q := *; ?q2x=1; x' = cq \& 2x \neq 0 \wedge cq > 0$$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \& 2x \neq 0 \wedge \frac{c}{2x} > 0 \rightsquigarrow \cancel{q := *; ?q2x=1; x' = cq} \& 2x \neq 0 \wedge cq > 0$$

inverse only of initial x

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \& 2x \neq 0 \wedge \frac{c}{2x} > 0 \rightsquigarrow q := *; ?q2x=1; x' = cq \& 2x \neq 0 \wedge cq > 0$$

change rate of q :

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \& 2x \neq 0 \wedge \frac{c}{2x} > 0 \rightsquigarrow q := *; ?q2x=1; x' = cq \& 2x \neq 0 \wedge cq > 0$$

change rate of q : $q' = \left(\frac{1}{2x} \right)' = \frac{-2x'}{4x^2} = \frac{-2\frac{c}{2x}}{4x^2} = -\frac{c}{4x^3}$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \& 2x \neq 0 \wedge \frac{c}{2x} > 0 \rightsquigarrow q := *; ?q2x=1; x' = cq \& c \neq 0 \wedge cq > 0$$

still $1/x$

change rate of q : $q' = \left(\frac{1}{2x} \right)' = \frac{-2x'}{4x^2} = \frac{-2\frac{c}{2x}}{4x^2} = -\frac{c}{4x^3}$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \& 2x \neq 0 \wedge \frac{c}{2x} > 0 \rightsquigarrow q := *; ?q2x=1; x' = cq \& 2x \neq 0 \wedge cq > 0$$

change rate of q : $q' = \left(\frac{1}{2x} \right)' = \frac{-2x'}{4x^2} = \frac{-2\frac{c}{2x}}{4x^2} = -\frac{c}{4x^3}$

$$\rightsquigarrow x' = cq, \color{red} q' = * \& \color{red} q2x=1 \wedge 2x \neq 0 \wedge cq > 0$$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends} \quad q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \& c \neq 0 \wedge c \neq 0 \rightsquigarrow \begin{array}{ccccccccc} 2 & 0 & 1 & 0 & 1 & 0 & 2 & 0 & 3 \\ x' = \frac{c}{2x} & & & & & & & & x \neq 0 \wedge cq > 0 \end{array}$$

continuously changing nondeterministic value

change rate of q : $q' = \left(\frac{1}{2x} \right)' = \frac{-2x'}{4x^2} = \frac{-2\frac{c}{2x}}{4x^2} = -\frac{c}{4x^3}$

$$\rightsquigarrow x' = cq, q' = * \& q2x=1 \wedge 2x \neq 0 \wedge cq > 0$$

Differential-algebraic Ghosts

Syntax

$$e ::= x \mid x' \mid f(e) \mid e + k \mid e \cdot k \mid (e)'$$

Syntax

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

Syntax

$$P ::= e \geq k \mid p(e) \mid \neg P \mid P \wedge Q \mid \forall x P \mid \exists x Q \mid [\alpha]P \mid \langle \alpha \rangle P$$

④ $e/k \stackrel{\text{def}}{=} \text{depends } q = \frac{b}{c} \stackrel{\text{def}}{\equiv} qc = b \text{ where } c \neq 0$

$$x' = \frac{2x}{c} \& c \neq 0 \wedge \frac{x+1}{c} > 0 \rightsquigarrow q := *; ?qc=1; x' = 2xq \& c \neq 0 \wedge (x+1)q > 0$$

$$x' = \frac{c}{2x} \stackrel{?}{=} 0 \wedge cq > 0$$

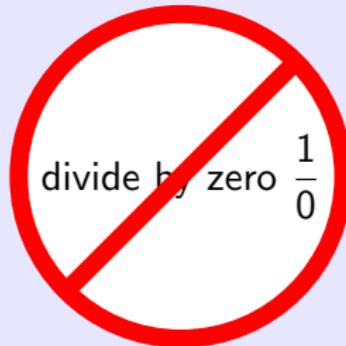
differential-algebraic ghost: auxiliary for the model

change rate of q : $q' = \left(\frac{1}{2x} \right)' = \frac{-2x'}{4x^2} = \frac{-2\frac{c}{2x}}{4x^2} = -\frac{c}{4x^3}$

$$\rightsquigarrow x' = cq, q' = * \& q2x=1 \wedge 2x \neq 0 \wedge cq > 0$$

Divisions by Zero

Divisions

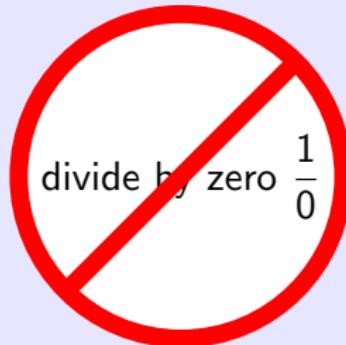


- ➊ Scrutinize every division or possible singularity.
- ➋ Missing requirements in the system.
- ➌ Stopping distance $\frac{v^2}{2b}$ from initial velocity v

Don't divide by zero. It's not worth it.
~~Divide & Conquer~~ Divide & Regret

Divisions by Zero

Divisions



- ➊ Scrutinize every division or possible singularity.
- ➋ Missing requirements in the system.
- ➌ Stopping distance $\frac{v^2}{2b}$ from initial velocity v
- ➍ ... needs brakes to work $b \neq 0$ though ...

Don't divide by zero. It's not worth it.
~~Divide & Conquer~~ Divide & Regret

Discrete Ghosts

$$\text{IA} \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \quad (y \text{ new})$$

$$\xrightarrow{\rightarrow R} \frac{}{\vdash xy - 1 = 0 \rightarrow [x' = x, y' = -y]xy = 1}$$

Clou: Ask a ghost to remember some auxiliary state for the proof.

Discrete Ghosts

$$\text{IA} \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \quad (y \text{ new})$$

$p \leftrightarrow [y := e]p$ by $[:=]$

$$\begin{array}{c} \text{IA} \\ \hline \text{→R} \frac{xy - 1 = 0 \vdash [x' = x, y' = -y]xy = 1}{\vdash xy - 1 = 0 \rightarrow [x' = x, y' = -y]xy = 1} \end{array}$$

Clou: Ask a ghost to remember some auxiliary state for the proof.

Discrete Ghosts

$$\text{IA } \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \quad (y \text{ new})$$

$p \leftrightarrow [y := e]p$ by $[:=]$

discrete ghost remembers function of old state

$$\begin{array}{c} [:=]= \\ \hline \text{IA } \frac{\begin{array}{c} xy - 1 = 0 \vdash [c := xy][x' = x, y' = -y]xy = 1 \\ xy - 1 = 0 \vdash [x' = x, y' = -y]xy = 1 \end{array}}{\rightarrow R \quad \vdash xy - 1 = 0 \rightarrow [x' = x, y' = -y]xy = 1} \end{array}$$

Clou: Ask a ghost to remember some auxiliary state for the proof.

Discrete Ghosts

$$\text{IA} \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \quad (y \text{ new})$$

$p \leftrightarrow [y := e]p$ by $[:=]$

$$[:=]_=\frac{\Gamma, y = e \vdash p(y), \Delta}{\Gamma \vdash [x := e]p(x), \Delta}$$

$$\begin{array}{c} \text{MR} \\ \hline xy - 1 = 0, \color{red}{c = xy} \vdash [x' = x, y' = -y]xy = 1 \\ [:=]_= \frac{}{xy - 1 = 0 \vdash [\color{red}{c := xy}] [x' = x, y' = -y]xy = 1} \\ \text{IA} \frac{}{xy - 1 = 0 \vdash [x' = x, y' = -y]xy = 1} \\ \hline \rightarrow R \quad \vdash xy - 1 = 0 \rightarrow [x' = x, y' = -y]xy = 1 \end{array}$$

Clou: Ask a ghost to remember some auxiliary state for the proof.

Discrete Ghosts

$$\text{IA} \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \quad (y \text{ new})$$

$p \leftrightarrow [y := e]p$ by $[:=]$

$$[:=] = \frac{\Gamma, y = e \vdash p(y), \Delta}{\Gamma \vdash [x := e]p(x), \Delta} \quad (y \text{ new})$$

$$\begin{array}{c} \text{dl} \\ \hline \text{MR} \frac{xy - 1 = 0, c = xy \vdash [x' = x, y' = -y]c = xy}{xy - 1 = 0, c = xy \vdash [x' = x, y' = -y]xy = 1} \\ \hline [:=] = \frac{xy - 1 = 0 \vdash [c := xy][x' = x, y' = -y]xy = 1}{\text{IA} \frac{xy - 1 = 0 \vdash [x' = x, y' = -y]xy = 1}{\rightarrow R \quad \vdash xy - 1 = 0 \rightarrow [x' = x, y' = -y]xy = 1}} \end{array}$$

Clou: Ask a ghost to remember some auxiliary state for the proof.

Discrete Ghosts

$$\text{IA} \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \quad (y \text{ new})$$

$p \leftrightarrow [y := e]p$ by $[:=]$

$$[:=] = \frac{\Gamma, y = e \vdash p(y), \Delta}{\Gamma \vdash [x := e]p(x), \Delta} \quad (y \text{ new})$$

$$\begin{array}{c} [':=] \\ \hline \text{dl} \quad \frac{}{\vdash [x' := x][y' := -y]0 = x'y + xy'} \\ \text{MR} \quad \frac{}{\vdash [x' = x, y' = -y]c = xy} \quad \triangleright \\ \hline [:=] = \frac{\text{dl} \quad \frac{}{\vdash [x' = x, y' = -y]xy = 1}}{\text{IA} \quad \frac{}{\vdash [c := xy][x' = x, y' = -y]xy = 1}} \\ \hline \rightarrow R \quad \frac{}{\vdash xy - 1 = 0 \rightarrow [x' = x, y' = -y]xy = 1} \end{array}$$

Clou: Ask a ghost to remember some auxiliary state for the proof.

Discrete Ghosts

$$\text{IA} \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \quad (y \text{ new})$$

$p \leftrightarrow [y := e]p$ by $[:=]$

$$[:=] = \frac{\Gamma, y = e \vdash p(y), \Delta}{\Gamma \vdash [x := e]p(x), \Delta} \quad (y \text{ new})$$

\mathbb{R}	$\vdash 0 = xy + x(-y)$	
$[':=]$	$\vdash [x' := x][y' := -y]0 = x'y + xy'$	
dl	$xy - 1 = 0, c = xy \vdash [x' = x, y' = -y]c = xy$	\triangleright
MR	$xy - 1 = 0, c = xy \vdash [x' = x, y' = -y]xy = 1$	
$[:=] =$	$xy - 1 = 0 \vdash [c := xy][x' = x, y' = -y]xy = 1$	
IA	$xy - 1 = 0 \vdash [x' = x, y' = -y]xy = 1$	
$\rightarrow R$	$\vdash xy - 1 = 0 \rightarrow [x' = x, y' = -y]xy = 1$	

Clou: Ask a ghost to remember some auxiliary state for the proof.

Discrete Ghosts

$$\text{IA} \frac{\Gamma \vdash [y := e]p, \Delta}{\Gamma \vdash p, \Delta} \quad (y \text{ new})$$

$p \leftrightarrow [y := e]p$ by $[:=]$

$$[:=] = \frac{\Gamma, y = e \vdash p(y), \Delta}{\Gamma \vdash [x := e]p(x), \Delta} \quad (y \text{ new})$$

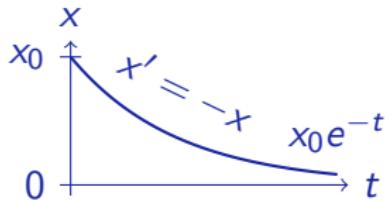
$$\begin{array}{c} * \\ \hline \mathbb{R} \quad \vdash 0 = xy + x(-y) \\ \hline [':=] \quad \vdash [x' := x][y' := -y]0 = x'y + xy' \\ \hline \text{dl} \quad xy - 1 = 0, c = xy \vdash [x' = x, y' = -y]c = xy \quad \triangleright \\ \hline \text{MR} \quad xy - 1 = 0, c = xy \vdash [x' = x, y' = -y]xy = 1 \\ \hline [:=] = \quad xy - 1 = 0 \vdash [c := xy][x' = x, y' = -y]xy = 1 \\ \hline \text{IA} \quad xy - 1 = 0 \vdash [x' = x, y' = -y]xy = 1 \\ \hline \rightarrow R \quad \vdash xy - 1 = 0 \rightarrow [x' = x, y' = -y]xy = 1 \end{array}$$

Clou: Ask a ghost to remember some auxiliary state for the proof.

Ex: Exponentials

Counterexample ()

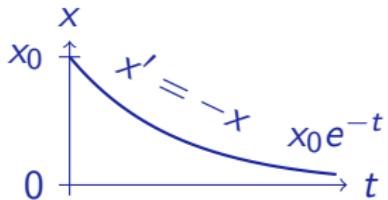
$$\text{dl } \overline{x > 0 \vdash [x' = -x]x > 0}$$



Ex: Exponentials

Counterexample ()

$$\frac{[':=] \quad \vdash [x' := -x] \textcolor{red}{x'} > 0}{\text{dl } x > 0 \vdash [x' = -x] x > 0}$$

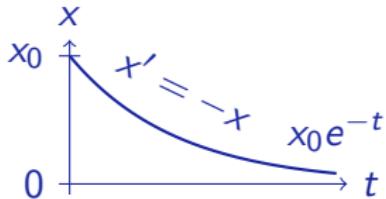


Ex: Exponentials

Counterexample ()

$$\frac{\mathbb{R} \quad \frac{}{\vdash -x > 0}}{[':=] \quad \frac{}{\vdash [x' := -x]x' > 0}}$$

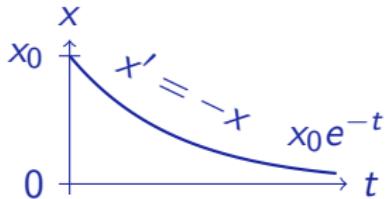
dI $\frac{x > 0 \vdash [x' = -x]x > 0}{}$



Ex: Exponentials

Counterexample (Cannot prove like this)

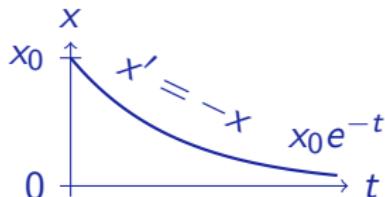
$$\frac{\text{not valid}}{\mathbb{R} \frac{}{\vdash -x > 0}} \\ [':=] \frac{}{\vdash [x' := -x]x' > 0} \\ \text{dl } \frac{}{x > 0 \vdash [x' = -x]x > 0}$$



Ex: Exponentials

Counterexample (Cannot prove like this)

$$\frac{\text{not valid}}{\mathbb{R} \vdash \neg x > 0}$$
$$[\doteq] \frac{}{\vdash [x' := -x]x' > 0}$$
$$\text{dl } \frac{}{x > 0 \vdash [x' = -x]x > 0}$$



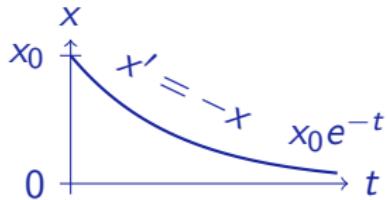
Matters get worse over time

Differential Ghosts: Proofs in Extra Dimensions

Example (▶ Sneaky proof)

DA

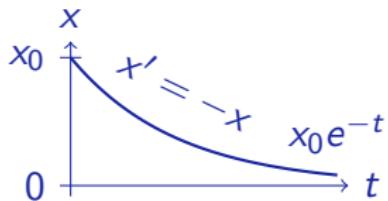
$$x > 0 \vdash [x' = -x]x > 0$$



Differential Ghosts: Proofs in Extra Dimensions

Example (▶ Sneaky proof)

$$\frac{\text{DA} \quad \frac{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y xy^2 = 1 \quad \text{dl} \quad \overline{xy^2 = 1 \vdash [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \vdash [x' = -x]x > 0}}$$

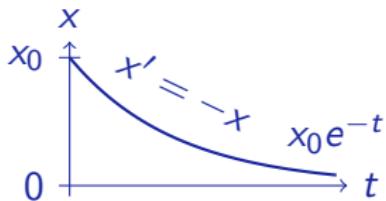


Differential Ghosts: Proofs in Extra Dimensions

Example (▶ Sneaky proof)

$$\frac{\text{DA} \quad \frac{*}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y \ xy^2 = 1} \text{ dl } \frac{}{xy^2 = 1 \vdash [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{x > 0 \vdash [x' = -x]x > 0}$$

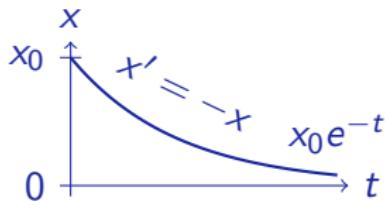
differential ghost: dream me up



Differential Ghosts: Proofs in Extra Dimensions

Example (▶ Sneaky proof)

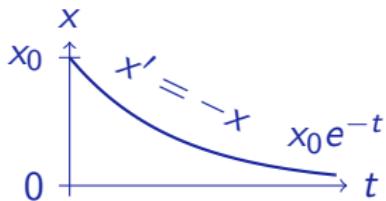
$$\frac{\text{DA} \quad \frac{\mathbb{R} \frac{*}{\vdash x > 0 \leftrightarrow \exists y xy^2 = 1} \quad \frac{[':=] \frac{}{\vdash [x' := -x][y' := \frac{y}{2}]x'y^2 + x2yy' = 0}}{\text{dl} \quad \frac{xy^2 = 1 \vdash [x' = -x, y' = \frac{y}{2}]xy^2 = 1}{\vdash [x' = -x]x > 0}}}{}}{}}$$



Differential Ghosts: Proofs in Extra Dimensions

Example (▶ Sneaky proof)

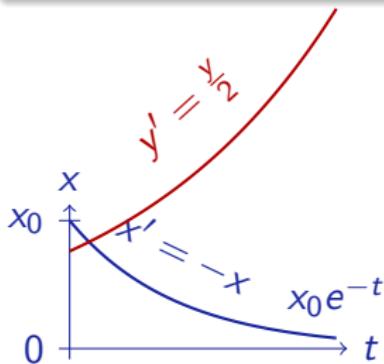
$$\frac{\text{DA} \quad x > 0 \vdash [x' = -x]x > 0}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y xy^2 = 1}$$



Differential Ghosts: Proofs in Extra Dimensions

Example (▶ Sneaky proof)

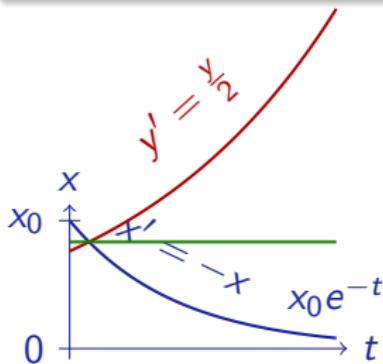
$$\frac{\text{DA} \quad \frac{\frac{*}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y \ xy^2 = 1} \quad \frac{*}{\mathbb{R} \vdash -xy^2 + 2xy\frac{y}{2} = 0}}{\vdash [x' := -x][y' := \frac{y}{2}]x'y^2 + x2yy' = 0} \quad \text{dl} \quad \frac{xy^2 = 1 \vdash [x' = -x, y' = \frac{y}{2}]xy^2 = 1}{x > 0 \vdash [x' = -x]x > 0}}{\frac{}{}}$$



Differential Ghosts: Proofs in Extra Dimensions

Example (▶ Sneaky proof)

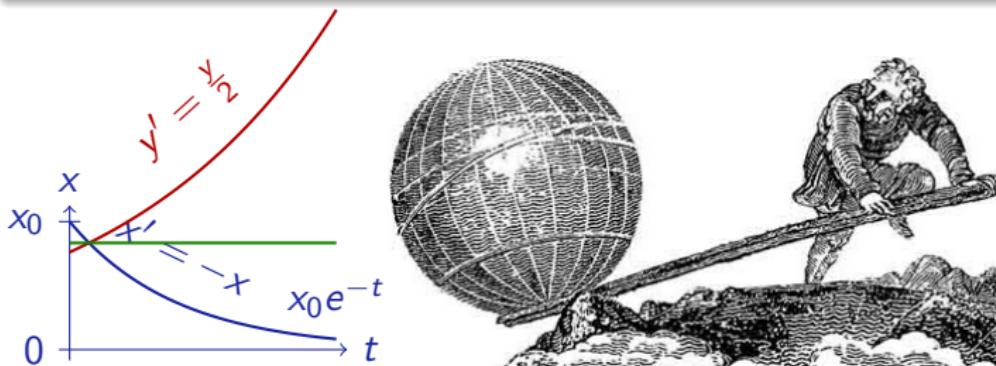
$$\frac{\text{DA} \quad \frac{\frac{*}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y \ xy^2 = 1} \quad \frac{*}{\mathbb{R} \vdash -xy^2 + 2xy\frac{y}{2} = 0} \quad \frac{\frac{\frac{*}{\vdash [x' := -x][y' := \frac{y}{2}]x'y^2 + x2yy' = 0}}{\vdash [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{\vdash x > 0 \vdash [x' = -x]x > 0}}{\text{dl}}$$



Differential Ghosts: Proofs in Extra Dimensions

Example (▶ Sneaky proof)

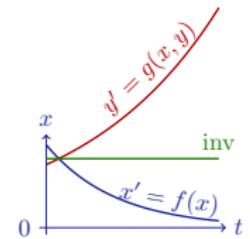
$$\frac{\text{DA} \quad \frac{\frac{*}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y \ xy^2 = 1} \quad \frac{*}{\mathbb{R} \vdash x > 0} \quad \frac{\frac{[':=]}{\mathbb{R} \vdash [x' := -x][y' := \frac{y}{2}]x'y^2 + x2yy' = 0} \quad \frac{\text{dl}}{xy^2 = 1 \vdash [x' = -x, y' = \frac{y}{2}]xy^2 = 1}}{\vdash [x' = -x]x > 0}}{\vdash [x' = -x]x > 0}$$



Differential Ghosts

Differential Ghost

$$\text{DA} \quad \frac{F \leftrightarrow \exists y \ G \quad G \vdash [x' = f(x), y' = g(x, y) \ \& \ Q]G}{F \vdash [x' = f(x) \ \& \ Q]F}$$

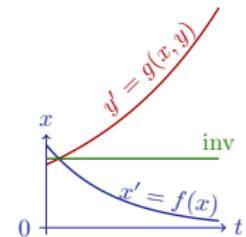


Differential Ghosts

Differential Ghost

$$\text{DA} \quad \frac{F \leftrightarrow \exists y \ G \quad G \vdash [x' = f(x), y' = g(x, y) \ \& \ Q]G}{F \vdash [x' = f(x) \ \& \ Q]F}$$

if new $y' = g(x, y)$ has a global solution

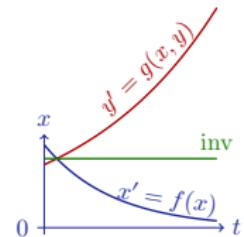


Differential Ghosts

Differential Ghost

$$\text{DA} \quad \frac{F \leftrightarrow \exists y \ G \quad G \vdash [x' = f(x), y' = g(x, y) \ \& \ Q]G}{F \vdash [x' = f(x) \ \& \ Q]F}$$

if new $y' = g(x, y)$ has a global solution
such as linear $g(x, y) \stackrel{\text{def}}{=} a(x)y + b(x)$



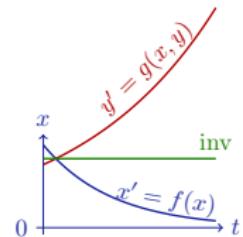
I can invent time $y' = 1$ for you

Differential Ghosts

Differential Ghost

$$\text{DA} \quad \frac{F \leftrightarrow \exists y \ G \quad G \vdash [x' = f(x), y' = g(x, y) \ \& \ Q]G}{F \vdash [x' = f(x) \ \& \ Q]F}$$

if new $y' = g(x, y)$ has a global solution
such as linear $g(x, y) \stackrel{\text{def}}{=} a(x)y + b(x)$



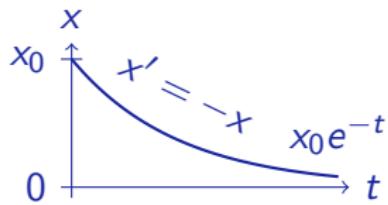
Differential Ghost

$$\text{DG} \quad [x' = f(x) \ \& \ Q]P \leftrightarrow \exists y \ [x' = f(x), y' = a(x)y + b(x) \ \& \ Q]P$$

Substitute Ghosts

DA

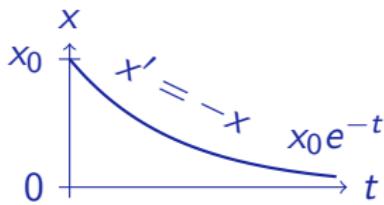
$$x > 0 \vdash [x' = -x]x > 0$$



Matters get worse over time

Substitute Ghosts

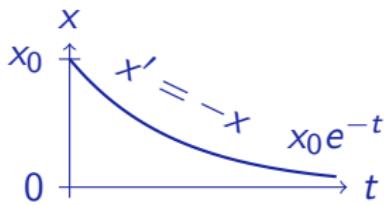
$$\frac{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y \ xy^2 = 1 \quad \text{dl} \quad \mathbb{R} \vdash xy^2 = 1 \vdash [x' = -x, y' = \text{cloud}]xy^2 = 1}{\text{DA} \quad x > 0 \vdash [x' = -x]x > 0}$$



Matters get worse over time

Substitute Ghosts

$$\frac{\begin{array}{c} * \\ \hline \mathbb{R} \vdash x > 0 \leftrightarrow \exists y \ xy^2 = 1 \end{array}}{\text{DA} \quad x > 0 \vdash [x' = -x]x > 0} \text{ dl } \frac{}{xy^2 = 1 \vdash [x' = -x, y' = \text{cloud}]xy^2 = 1}$$

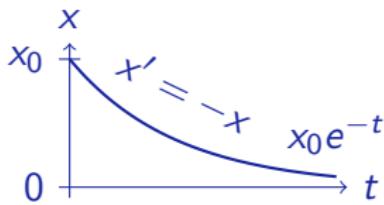


Matters get worse over time

Substitute Ghosts

$$\frac{\begin{array}{c} * \\ \mathbb{R} \vdash x > 0 \leftrightarrow \exists y \ xy^2 = 1 \end{array}}{\text{DA}}$$
$$\frac{[':=] \quad \vdash [x' := -x][y' := \text{cloud}] x'y^2 + x2yy' = 0}{\text{dI} \quad xy^2 = 1 \vdash [x' = -x, y' = \text{cloud}] xy^2 = 1}$$

$$x > 0 \vdash [x' = -x] x > 0$$

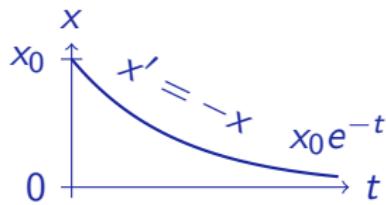


Matters get worse over time

Substitute Ghosts

DA

$$x > 0 \vdash [x' = -x] x > 0$$



Matters get worse over time

Substitute Ghosts

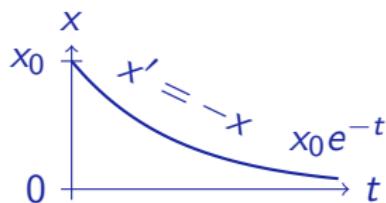
could prove if $\text{ghost} = \frac{y}{2}$

$$\vdash -xy^2 + 2xy\text{ghost} = 0$$

$$\frac{* \quad \quad \quad [':=] \quad \quad \quad \vdash [x' := -x][y' := \text{ghost}]x'y^2 + x2yy' = 0}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y xy^2 = 1 \quad \text{dl} \quad xy^2 = 1 \vdash [x' = -x, y' = \text{ghost}]xy^2 = 1}$$

DA

$$x > 0 \vdash [x' = -x]x > 0$$



Matters get worse over time

Substitute Ghosts

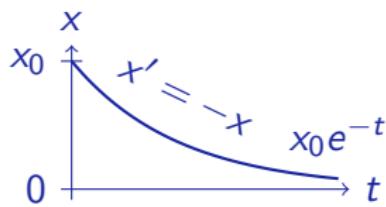
could prove if $\text{ghost} = \frac{y}{2}$

$$\vdash -xy^2 + 2xy\text{ghost} = 0$$

$$\frac{* \quad \quad \quad [':=] \quad \quad \quad \vdash [x' := -x][y' := \text{ghost}]x'y^2 + x2yy' = 0}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y xy^2 = 1 \quad \text{dl} \quad xy^2 = 1 \vdash [x' = -x, y' = \text{ghost}]xy^2 = 1}$$

DA

$$x > 0 \vdash [x' = -x]x > 0$$



Matters get worse over time

Substitute Ghosts

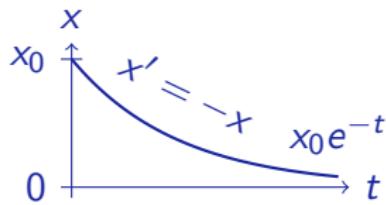
could prove if $\frac{y}{2} = \frac{y}{2}$ proved!

$$\vdash -xy^2 + 2xy\frac{y}{2} = 0$$

$$\frac{* \quad \quad \quad \vdash [x':=-x][y':=\frac{y}{2}]x'y^2+x2yy'=0}{\mathbb{R} \vdash x>0 \leftrightarrow \exists y xy^2=1 \quad \text{dl} \quad xy^2=1 \vdash [x' = -x, y' = \frac{y}{2}]xy^2 = 1}$$

DA

$$x > 0 \vdash [x' = -x]x > 0$$



Matters get worse over time

Substitute Ghosts

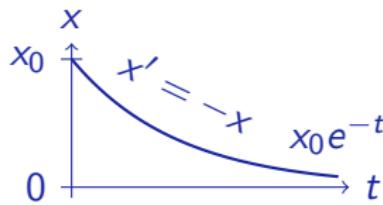
could prove if $j(y) = \frac{y}{2}$

$$\vdash -xy^2 + 2xyj(y) = 0$$

$$\frac{* \quad \quad \quad [':=] \quad \quad \quad \vdash [x' := -x][y' := j(y)]x'y^2 + x2yy' = 0}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y xy^2 = 1 \quad \text{dl} \quad xy^2 = 1 \vdash [x' = -x, y' = j(y)]xy^2 = 1}$$

DA

$$x > 0 \vdash [x' = -x]x > 0$$



Matters get worse over time

Function symbol $j(y)$ can play the role of a ghost

Substitute Ghosts

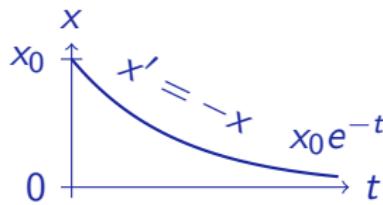
could prove if $\frac{y}{2} = \frac{y}{2}$ proved!

$$\vdash -xy^2 + 2xy\frac{y}{2} = 0$$

$$\frac{* \quad \quad \quad \vdash [x' := -x][y' := \frac{y}{2}]x'y^2 + x2yy' = 0}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y xy^2 = 1 \quad \text{dl} \quad xy^2 = 1 \vdash [x' = -x, y' = \frac{y}{2}]xy^2 = 1}$$

DA

$$x > 0 \vdash [x' = -x]x > 0$$



Matters get worse over time

Function symbol $j(y)$ can be substituted uniformly

Substitute Ghosts

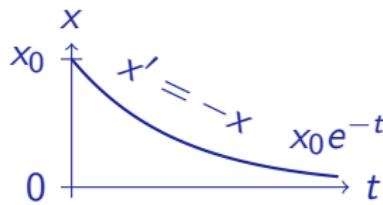
could prove if $j(y) = \frac{y}{2}$

$$\vdash -xy^2 + 2xyj(y) = 0$$

$$\frac{* \quad \vdash [x' := -x][y' := j(y)]x'y^2 + x2yy' = 0}{\mathbb{R} \vdash x > 0 \leftrightarrow \exists y xy^2 = 1 \quad \text{dl} \quad xy^2 = 1 \vdash [x' = -x, y' = j(y)]xy^2 = 1}$$

DA

$$x > 0 \vdash [x' = -x]x > 0$$



Matters get worse over time

Function symbol $j(y)$ needs to be instantiated linearly in y

Solvable Ghosts: Axiomatic Differential Equation Solver

- ① DG introduces time t , DC cuts solution in, that DI proves and
- ② DW exports to postcondition
- ③ inverse DC removes evolution domain constraints
- ④ inverse DG removes original ODE
- ⑤ DS solves remaining ODE for time $[x' = c()]P \leftrightarrow \forall t \geq 0 [x := x + c()t]P$

*

$$\mathbb{R} \frac{}{\phi \vdash \forall s \geq 0 (x_0 + \frac{a}{2}s^2 + v_0s \geq 0)}$$

$$[:=] \frac{}{\phi \vdash \forall s \geq 0 [t := 0 + 1s]x_0 + \frac{a}{2}t^2 + v_0t \geq 0}$$

$$DS \frac{}{\phi \vdash [t' = 1]x_0 + \frac{a}{2}t^2 + v_0t \geq 0}$$

$$DG \frac{}{\phi \vdash [v' = a, t' = 1]x_0 + \frac{a}{2}t^2 + v_0t \geq 0}$$

$$DG \frac{}{\phi \vdash [x' = v, v' = a, t' = 1]x_0 + \frac{a}{2}t^2 + v_0t \geq 0} \triangleright$$

$$DC \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x_0 + \frac{a}{2}t^2 + v_0t \geq 0} \triangleright$$

$$DC \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at \wedge x = x_0 + \frac{a}{2}t^2 + v_0t]x_0 + \frac{a}{2}t^2 + v_0t \geq 0} \triangleright$$

$$MR \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at \wedge x = x_0 + \frac{a}{2}t^2 + v_0t](x = x_0 + \frac{a}{2}t^2 + v_0t \rightarrow x \geq 0)}$$

$$DW \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at \wedge x = x_0 + \frac{a}{2}t^2 + v_0t]x \geq 0} \triangleright$$

$$DC \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x \geq 0} \triangleright$$

$$DC \frac{}{\phi \vdash [x' = v, v' = a, t' = 1]x \geq 0} t := 0$$

$$DG \frac{}{\phi \vdash \exists t [x' = v, v' = a, t' = 1]x \geq 0}$$

$$DG \frac{}{\phi \vdash [x' = v, v' = a]x \geq 0}$$

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

$$\text{dl } \overline{\phi \vdash [x' = v, v' = a, t' = 1] v = v_0 + at}$$

$$\text{dl } \overline{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at] x = x_0 + \frac{a}{2}t^2 + v_0 t}$$

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

$$\text{dl} \frac{[':=] \vdash [v' := a][t' := 1]v' = at'}{\phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at}$$

$$\text{dl} \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t}$$

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

$$\frac{\mathbb{R} \vdash a = a \cdot 1}{\frac{[':=] \vdash [v' := a][t' := 1]v' = at'}{\text{dl } \phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at}}$$

$$\text{dl } \phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t$$

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

$$\frac{\begin{array}{c} * \\ \mathbb{R} \quad \frac{}{\vdash a = a \cdot 1} \\ [':=] \quad \frac{}{\vdash [v' := a][t' := 1]v' = at'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at} \end{array}}{\phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at}$$

$$\text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t}$$

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

$$\begin{array}{c} * \\ \hline \mathbb{R} \frac{}{\vdash a = a \cdot 1} \\ \hline [':=] \frac{}{\vdash [v' := a][t' := 1]v' = at'} \\ \text{dl } \frac{}{\phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at} \end{array}$$

$$\begin{array}{c} [':=] \frac{}{\vdash v = v_0 + at \rightarrow [x' := v][t' := 1]x' = att' + v_0 t'} \\ \text{dl } \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t} \end{array}$$

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

$$\frac{\begin{array}{c} * \\ \mathbb{R} \quad \frac{}{\vdash a = a \cdot 1} \\ [':=] \quad \frac{}{\vdash [v' := a][t' := 1]v' = at'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at} \end{array}}{}$$

$$\frac{\begin{array}{c} \mathbb{R} \quad \frac{}{\vdash v = v_0 + at \rightarrow v = at \cdot 1 + v_0 \cdot 1} \\ [':=] \quad \frac{}{\vdash v = v_0 + at \rightarrow [x' := v][t' := 1]x' = att' + v_0 t'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t} \end{array}}{}$$

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

$$\frac{\begin{array}{c} * \\ \mathbb{R} \quad \frac{}{\vdash a = a \cdot 1} \end{array}}{\begin{array}{c} [=] \quad \frac{}{\vdash [v' := a][t' := 1]v' = at'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at} \end{array}}$$

$$\frac{\begin{array}{c} * \\ \mathbb{R} \quad \frac{}{\vdash v = v_0 + at \rightarrow v = at \cdot 1 + v_0 \cdot 1} \end{array}}{\begin{array}{c} [=] \quad \frac{}{\vdash v = v_0 + at \rightarrow [x' := v][t' := 1]x' = att' + v_0 t'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t} \end{array}}$$

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

$$\frac{\begin{array}{c} * \\ \mathbb{R} \quad \frac{}{\vdash a = a \cdot 1} \end{array}}{\begin{array}{c} [=] \quad \frac{}{\vdash [v' := a][t' := 1]v' = at'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at} \end{array}}$$

$$\frac{\begin{array}{c} * \\ \mathbb{R} \quad \frac{}{\vdash v = v_0 + at \rightarrow v = at \cdot 1 + v_0 \cdot 1} \end{array}}{\begin{array}{c} [=] \quad \frac{}{\vdash v = v_0 + at \rightarrow [x' := v][t' := 1]x' = att' + v_0 t'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t} \end{array}}$$

But ϕ needs $v = v_0 \wedge x = x_0$ initially

▷ Proving Solutions of Differential Equations

These are the side branches elided above by ▷

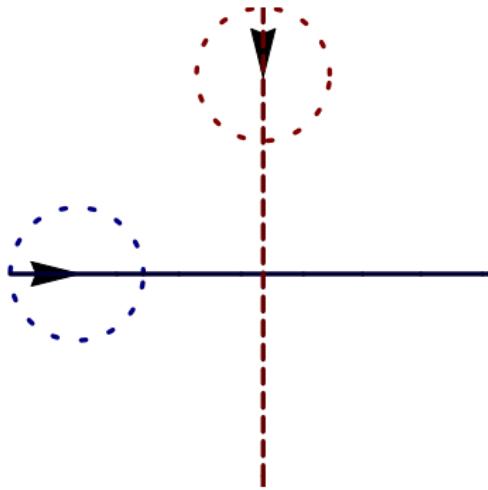
$$\frac{\begin{array}{c} * \\ \mathbb{R} \quad \frac{}{\vdash a = a \cdot 1} \end{array}}{\begin{array}{c} [=] \quad \frac{}{\vdash [v' := a][t' := 1]v' = at'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1]v = v_0 + at} \end{array}}$$

$$\frac{\begin{array}{c} * \\ \mathbb{R} \quad \frac{}{\vdash v = v_0 + at \rightarrow v = at \cdot 1 + v_0 \cdot 1} \end{array}}{\begin{array}{c} [=] \quad \frac{}{\vdash v = v_0 + at \rightarrow [x' := v][t' := 1]x' = att' + v_0 t'} \\ \text{dl} \quad \frac{}{\phi \vdash [x' = v, v' = a, t' = 1 \& v = v_0 + at]x = x_0 + \frac{a}{2}t^2 + v_0 t} \end{array}}$$

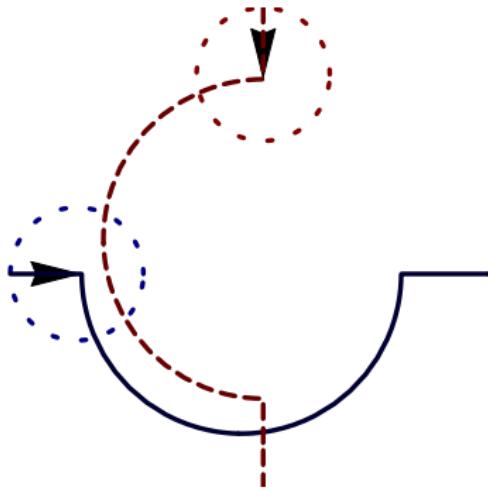
But ϕ needs $v = v_0 \wedge x = x_0$ initially

Discrete ghosts to the rescue: $[x_0 := x][v_0 := v] \dots$
who can remember initial value on demand.

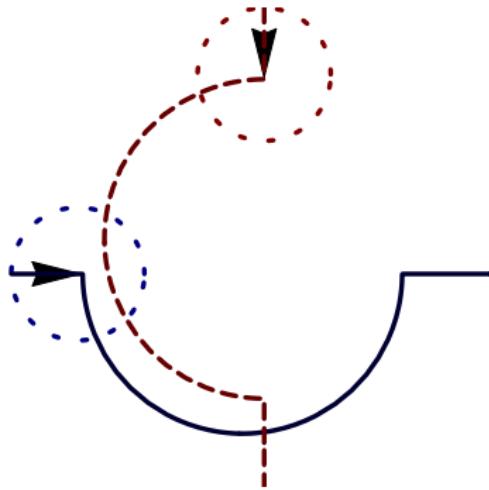
Air Traffic Control



Air Traffic Control



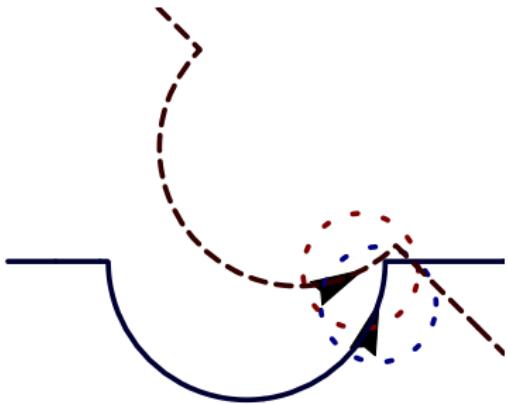
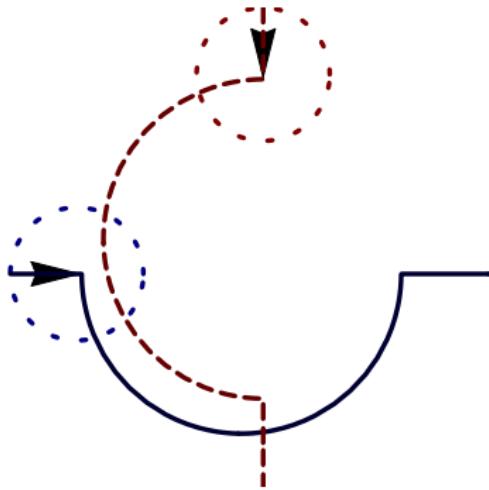
Air Traffic Control



Verification?

looks correct

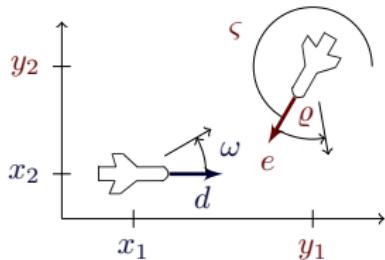
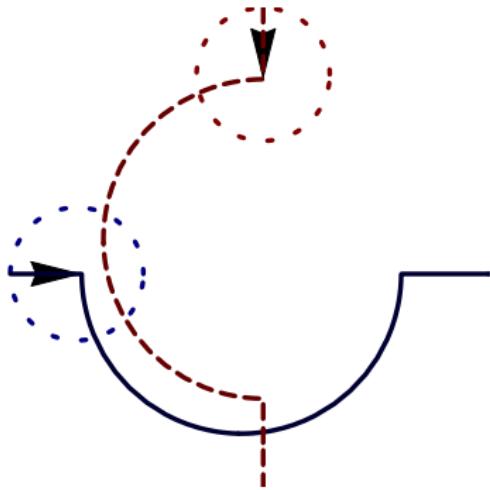
Air Traffic Control



Verification?

looks correct **NO!**

Air Traffic Control

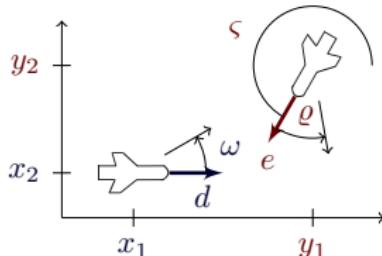
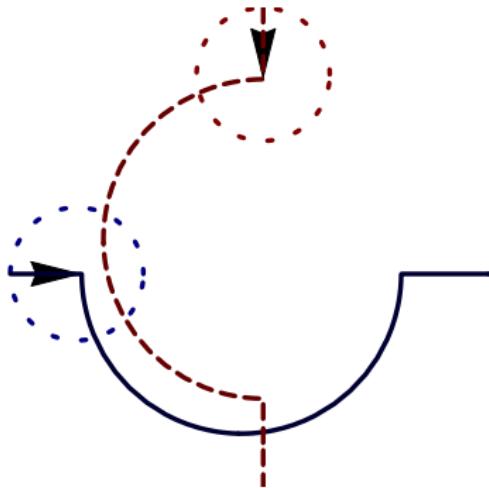


$$\begin{bmatrix} x'_1 = -v_1 + v_2 \cos \vartheta + \omega x_2 \\ x'_2 = v_2 \sin \vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Verification?

looks correct NO!

Air Traffic Control

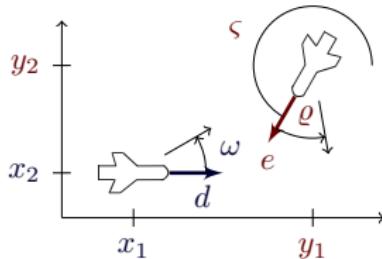
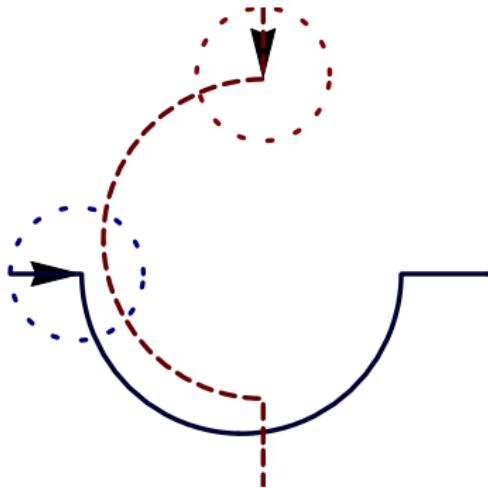


$$\begin{bmatrix} x'_1 = -v_1 + v_2 \cos \vartheta + \omega x_2 \\ x'_2 = v_2 \sin \vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example (“Solving” differential equations)

$$x_1(t) = \frac{1}{\omega\varpi} (x_1\omega\varpi \cos t\omega - v_2\omega \cos t\omega \sin \vartheta + v_2\omega \cos t\omega \cos t\varpi \sin \vartheta - v_1\varpi \sin t\omega + x_2\omega\varpi \sin t\omega - v_2\omega \cos \vartheta \cos t\varpi \sin t\omega - v_2\omega \sqrt{1 - \sin^2 \vartheta} \sin t\omega + v_2\omega \cos \vartheta \cos t\omega \sin t\varpi + v_2\omega \sin \vartheta \sin t\omega \sin t\varpi) \dots$$

Air Traffic Control



$$\begin{bmatrix} x'_1 = -v_1 + v_2 \cos \vartheta + \omega x_2 \\ x'_2 = v_2 \sin \vartheta - \omega x_1 \\ \vartheta' = \varpi - \omega \end{bmatrix}$$

Example (“Solving” differential equations)

$$\begin{aligned} \forall t \geq 0 \quad & \frac{1}{\omega \varpi} (x_1 \omega \varpi \cos t \omega - v_2 \omega \cos t \omega \sin \vartheta + v_2 \omega \cos t \omega \cos t \varpi \sin \vartheta - v_1 \omega \sin t \omega \\ & + x_2 \omega \varpi \sin t \omega - v_2 \omega \cos \vartheta \cos t \varpi \sin t \omega - v_2 \omega \sqrt{1 - \sin \vartheta^2} \sin t \omega \\ & + v_2 \omega \cos \vartheta \cos t \omega \sin t \varpi + v_2 \omega \sin \vartheta \sin t \omega \sin t \varpi) \dots \end{aligned}$$

```

\forall R ts2.
( 0 <= ts2 & ts2 <= t2_0
-> ( (om_1)^{-1}
  * (omb_1)^{-1}
  * ( om_1 * omb_1 * x1 * Cos(om_1 * ts2)
    + om_1 * v2 * Cos(om_1 * ts2) * (1 + -1 * (Cos(u))^2)^(1 / 2)
    + -1 * omb_1 * v1 * Sin(om_1 * ts2)
    + om_1 * omb_1 * x2 * Sin(om_1 * ts2)
    + om_1 * v2 * Cos(u) * Sin(om_1 * ts2)
    + -1 * om_1 * v2 * Cos(omb_1 * ts2) * Cos(u) * Sin(om_1 * ts2)
    + om_1 * v2 * Cos(om_1 * ts2) * Cos(u) * Sin(omb_1 * ts2)
    + om_1 * v2 * Cos(om_1 * ts2) * Cos(omb_1 * ts2) * Sin(u)
    + om_1 * v2 * Sin(om_1 * ts2) * Sin(omb_1 * ts2) * Sin(u)))
^2
+ ( (om_1)^{-1}
  * (omb_1)^{-1}
  * ( -1 * omb_1 * v1 * Cos(om_1 * ts2)
    + om_1 * omb_1 * x2 * Cos(om_1 * ts2)
    + omb_1 * v1 * (Cos(om_1 * ts2))^2
    + om_1 * v2 * Cos(om_1 * ts2) * Cos(u)
    + -1 * om_1 * v2 * Cos(om_1 * ts2) * Cos(omb_1 * ts2) * Cos(u)
    + -1 * om_1 * omb_1 * x1 * Sin(om_1 * ts2)
    + -1
    * om_1
    * v2
    * (1 + -1 * (Cos(u))^2)^(1 / 2)
    * Sin(om_1 * ts2)
    + omb_1 * v1 * (Sin(om_1 * ts2))^2
    + -1 * om_1 * v2 * Cos(u) * Sin(om_1 * ts2) * Sin(omb_1 * ts2)
    + -1 * om_1 * v2 * Cos(omb_1 * ts2) * Sin(om_1 * ts2) * Sin(u)
    + om_1 * v2 * Cos(om_1 * ts2) * Sin(omb_1 * ts2) * Sin(u)))
^2
>= (p)^2,
t2_0 >= 0,
x1^2 + x2^2 >= (p)^2
==>

```

```

\forall R t7.
  ( t7 >= 0
  ->   ( (om_3)^{-1}
        * ( om_3
            * ( (om_1)^{-1}
                * (omb_1)^{-1}
                * ( om_1 * omb_1 * x1 * Cos(om_1 * t2_0)
                    + om_1
                    * v2
                    * Cos(om_1 * t2_0)
                    * (1 + -1 * (Cos(u))^2)^(1 / 2)
                    + -1 * omb_1 * v1 * Sin(om_1 * t2_0)
                    + om_1 * omb_1 * x2 * Sin(om_1 * t2_0)
                    + om_1 * v2 * Cos(u) * Sin(om_1 * t2_0)
                    + -1
                    * om_1
                    * v2
                    * Cos(omb_1 * t2_0)
                    * Cos(u)
                    * Sin(om_1 * t2_0)
                    + om_1
                    * v2
                    * Cos(om_1 * t2_0)
                    * Cos(u)
                    * Sin(omb_1 * t2_0)
                    + om_1
                    * v2
                    * Cos(om_1 * t2_0)
                    * Cos(omb_1 * t2_0)
                    * Sin(u)
                    + om_1
                    * v2
                    * Sin(om_1 * t2_0)
                    * Sin(omb_1 * t2_0)
                    * Sin(u)))

```

```

* Cos(om_3 * t5)
+
v2
* Cos(om_3 * t5)
*
( 1
+ -1
* (Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4))^2)
^(1 / 2)
+
-1 * v1 * Sin(om_3 * t5)
+
om_3
*
( (om_1)^-1
* (omb_1)^-1
* (-1 * omb_1 * v1 * Cos(om_1 * t2_0)
+ om_1 * omb_1 * x2 * Cos(om_1 * t2_0)
+ omb_1 * v1 * (Cos(om_1 * t2_0))^2
+ om_1 * v2 * Cos(om_1 * t2_0) * Cos(u)
+ -1
* om_1
* v2
* Cos(om_1 * t2_0)
* Cos(omb_1 * t2_0)
* Cos(u)
+ -1 * om_1 * omb_1 * x1 * Sin(om_1 * t2_0)
+ -1
* om_1
* v2
* (1 + -1 * (Cos(u))^2)^(1 / 2)
* Sin(om_1 * t2_0)
+ omb_1 * v1 * (Sin(om_1 * t2_0))^2
+ -1
* om_1
* v2
* Cos(u)
* Sin(om_1 * t2_0)
* Sin(omb_1 * t2_0)

```

```

+    -1
* om_1
* v2
* Cos(omb_1 * t2_0)
* Sin(om_1 * t2_0)
* Sin(u)
+   om_1
* v2
* Cos(om_1 * t2_0)
* Sin(omb_1 * t2_0)
* Sin(u)))
* Sin(om_3 * t5)
+
v2
* Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
* Sin(om_3 * t5)
+
v2
* (Cos(om_3 * t5))^2
* Sin(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
+
v2
* (Sin(om_3 * t5))^2
* Sin(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)))
^2
+
( (om_3)^-1
* (-1 * v1 * Cos(om_3 * t5)
+   om_3
* ( (om_1)^-1
* (omb_1)^-1
* ( -1 * omb_1 * v1 * Cos(om_1 * t2_0)
+   om_1 * omb_1 * x2 * Cos(om_1 * t2_0)
+   omb_1 * v1 * (Cos(om_1 * t2_0))^2
+   om_1 * v2 * Cos(om_1 * t2_0) * Cos(u)
+   -1
* om_1
* v2
* Cos(om_1 * t2_0)
* Cos(omb_1 * t2_0)

```

```

+ -1 * om_1 * omb_1 * x1 * Sin(om_1 * t2_0)
+
+   -1
+     * om_1
+     * v2
+     * (1 + -1 * (Cos(u))^2)^(1 / 2)
+     * Sin(om_1 * t2_0)
+   omb_1 * v1 * (Sin(om_1 * t2_0))^2
+
+   -1
+     * om_1
+     * v2
+     * Cos(u)
+     * Sin(om_1 * t2_0)
+     * Sin(omb_1 * t2_0)
+
+   -1
+     * om_1
+     * v2
+     * Cos(omb_1 * t2_0)
+     * Sin(om_1 * t2_0)
+     * Sin(u)
+
+   om_1
+     * v2
+     * Cos(om_1 * t2_0)
+     * Sin(omb_1 * t2_0)
+     * Sin(u)))
* Cos(om_3 * t5)
+
+ v1 * (Cos(om_3 * t5))^2
+
+ v2
* Cos(om_3 * t5)
* Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
+
+   -1
+     * v2
+     * (Cos(om_3 * t5))^2
+     * Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)

```

```

+      -1
* om_3
* ( (om_1)^-1
* (omb_1)^-1
* ( om_1 * omb_1 * x1 * Cos(om_1 * t2_0)
+   om_1
* v2
* Cos(om_1 * t2_0)
* (1 + -1 * (Cos(u))^2)^(1 / 2)
+ -1 * omb_1 * v1 * Sin(om_1 * t2_0)
+ om_1 * omb_1 * x2 * Sin(om_1 * t2_0)
+ om_1 * v2 * Cos(u) * Sin(om_1 * t2_0)
+   -1
* om_1
* v2
* Cos(omb_1 * t2_0)
* Cos(u)
* Sin(om_1 * t2_0)
+   om_1
* v2
* Cos(om_1 * t2_0)
* Cos(u)
* Sin(omb_1 * t2_0)
+   om_1
* v2
* Cos(om_1 * t2_0)
* Cos(omb_1 * t2_0)
* Sin(u)
+   om_1
* v2
* Sin(om_1 * t2_0)
* Sin(omb_1 * t2_0)
* Sin(u)))
* Sin(om_3 * t5)

```

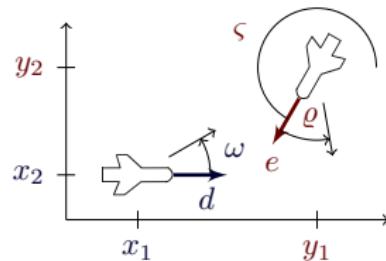
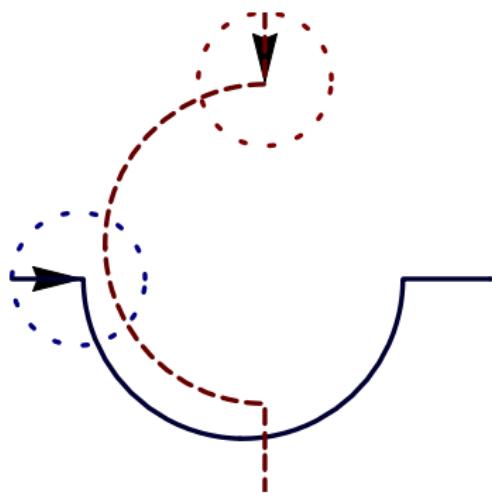
```

+   -1
* v2
*   ( 1
+   -1
* (Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4))^2)
^(1 / 2)
* Sin(om_3 * t5)
+ v1 * (Sin(om_3 * t5))^2
+   -1
* v2
* Cos(-1 * om_1 * t2_0 + omb_1 * t2_0 + u + Pi / 4)
* (Sin(om_3 * t5))^2))
^2
>= (p)^2

```

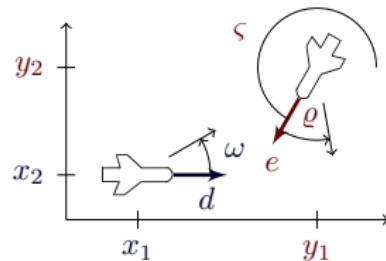
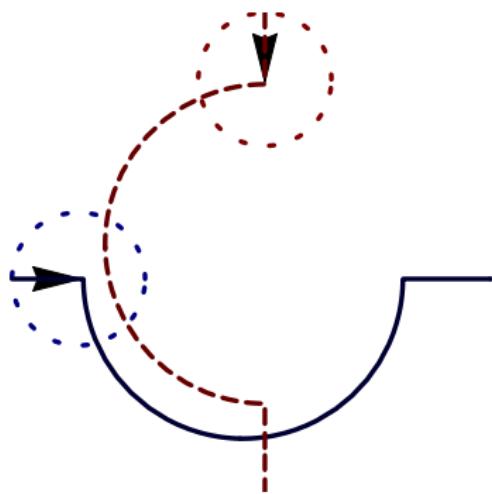
This is just one branch to prove for aircraft ...

Air Traffic Control



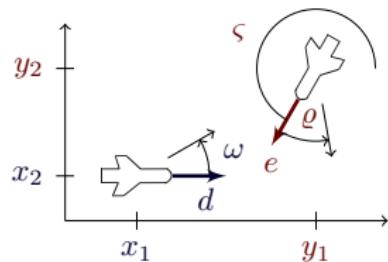
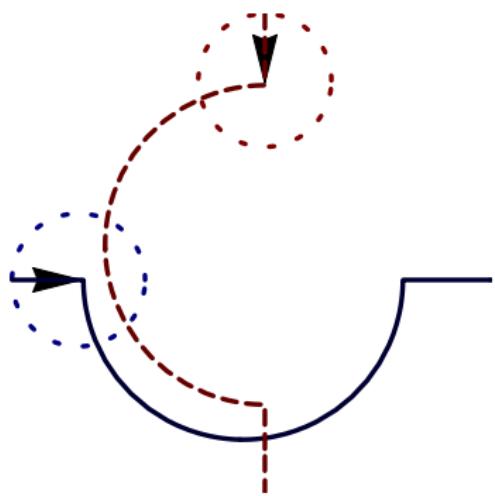
$$\begin{bmatrix} x'_1 = v \cos \vartheta & y'_1 = u \cos \varsigma \\ x'_2 = v \sin \vartheta & y'_2 = u \sin \varsigma \\ \vartheta' = \omega & \varsigma' = \varrho \end{bmatrix}$$

Air Traffic Control

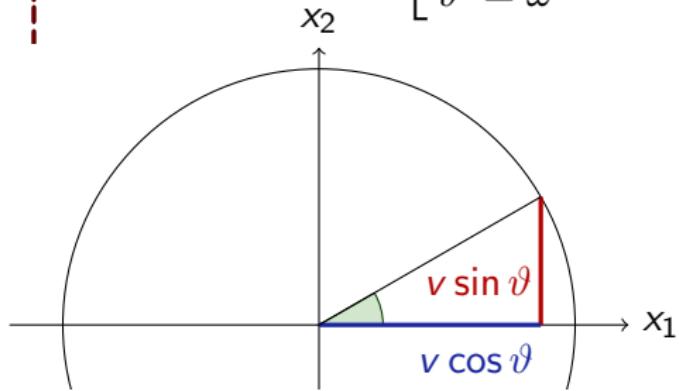


$$\begin{bmatrix} x'_1 = v \cos \vartheta \\ x'_2 = v \sin \vartheta \\ \vartheta' = \omega \end{bmatrix} \quad \begin{bmatrix} y'_1 = u \cos \varsigma \\ y'_2 = u \sin \varsigma \\ \varsigma' = \varrho \end{bmatrix}$$

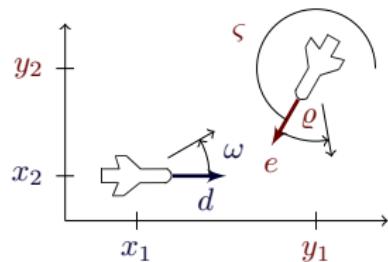
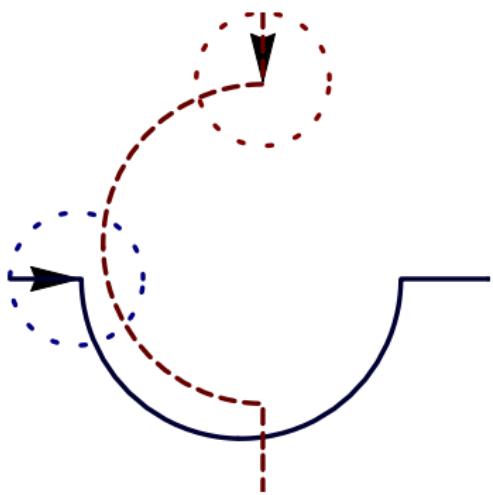
Air Traffic Control



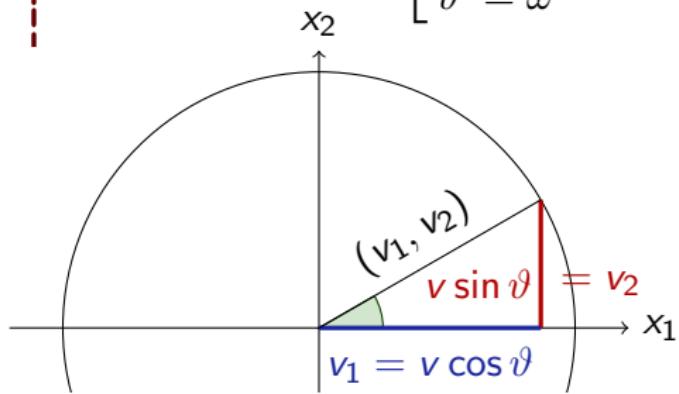
$$\begin{bmatrix} x'_1 = v \cos \vartheta & y'_1 = u \cos \varsigma \\ x'_2 = v \sin \vartheta & y'_2 = u \sin \varsigma \\ \vartheta' = \omega & \varsigma' = \varrho \end{bmatrix}$$



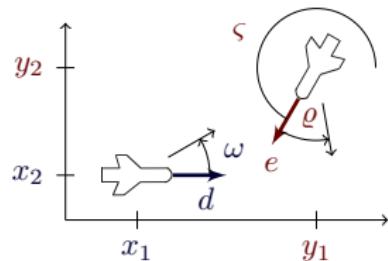
Air Traffic Control



$$\begin{bmatrix} x'_1 = v \cos \vartheta = v_1 & y'_1 = u \cos \varsigma \\ x'_2 = v \sin \vartheta = v_2 & y'_2 = u \sin \varsigma \\ \vartheta' = \omega & \varsigma' = \varrho \end{bmatrix}$$



Differential Axiomatization of Flight Dynamics

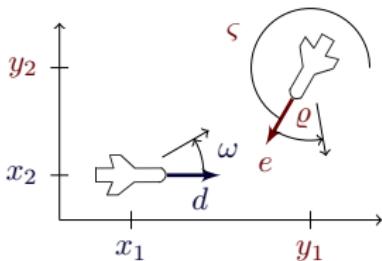


$$\begin{bmatrix} x'_1 = v \cos \vartheta = v_1 & y'_1 = u \cos \zeta = u_1 \\ x'_2 = v \sin \vartheta = v_2 & y'_2 = u \sin \zeta = u_2 \\ v'_1 = & u'_1 = \\ v'_2 = & u'_2 = \\ \vartheta' = \omega & \zeta' = \varrho \end{bmatrix}$$

$$v'_1 =$$

$$v'_2 =$$

Differential Axiomatization of Flight Dynamics

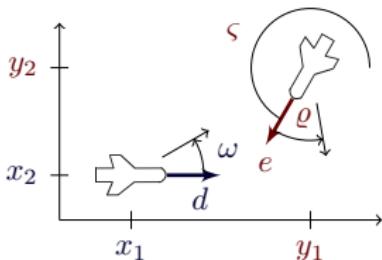


$$\begin{bmatrix} x'_1 = v \cos \vartheta = v_1 & y'_1 = u \cos \varsigma = u_1 \\ x'_2 = v \sin \vartheta = v_2 & y'_2 = u \sin \varsigma = u_2 \\ v'_1 = & u'_1 = \\ v'_2 = & u'_2 = \\ \vartheta' = \omega & \varsigma' = \varrho \end{bmatrix}$$

$$v'_1 = (v \cos \vartheta)'$$

$$v'_2 = (v \sin \vartheta)'$$

Differential Axiomatization of Flight Dynamics

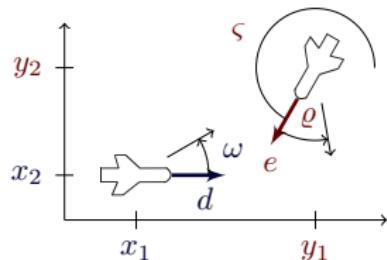


$$\begin{bmatrix} x'_1 = v \cos \vartheta = v_1 & y'_1 = u \cos \varsigma = u_1 \\ x'_2 = v \sin \vartheta = v_2 & y'_2 = u \sin \varsigma = u_2 \\ v'_1 = & u'_1 = \\ v'_2 = & u'_2 = \\ \vartheta' = \omega & \varsigma' = \varrho \end{bmatrix}$$

$$v'_1 = (v \cos \vartheta)' = v' \cos \vartheta + v(-\sin \vartheta)\vartheta'$$

$$v'_2 = (v \sin \vartheta)' = v' \sin \vartheta + v(\cos \vartheta)\vartheta'$$

Differential Axiomatization of Flight Dynamics

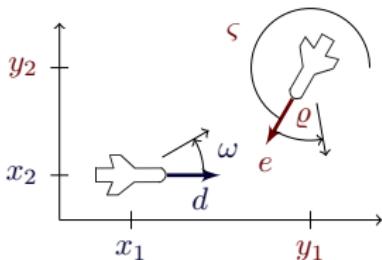


$$\begin{bmatrix} x'_1 = v \cos \vartheta = v_1 & y'_1 = u \cos \varsigma = u_1 \\ x'_2 = v \sin \vartheta = v_2 & y'_2 = u \sin \varsigma = u_2 \\ v'_1 = & u'_1 = \\ v'_2 = & u'_2 = \\ \vartheta' = \omega & \varsigma' = \varrho \end{bmatrix}$$

$$v'_1 = (v \cos \vartheta)' = v' \cos \vartheta + v(-\sin \vartheta)\vartheta' = -(v \sin \vartheta)\omega$$

$$v'_2 = (v \sin \vartheta)' = v' \sin \vartheta + v(\cos \vartheta)\vartheta' = (v \cos \vartheta)\omega$$

Differential Axiomatization of Flight Dynamics

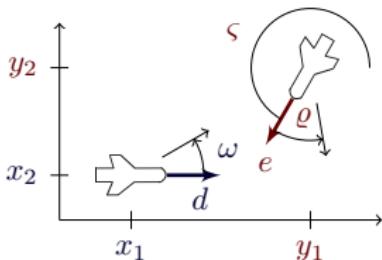


$$\begin{bmatrix} x'_1 = v \cos \vartheta = v_1 & y'_1 = u \cos \varsigma = u_1 \\ x'_2 = v \sin \vartheta = v_2 & y'_2 = u \sin \varsigma = u_2 \\ v'_1 = -\omega v_2 & u'_1 = \\ v'_2 = \omega v_1 & u'_2 = \\ \vartheta' = \omega & \varsigma' = \varrho \end{bmatrix}$$

$$v'_1 = (v \cos \vartheta)' = v' \cos \vartheta + v(-\sin \vartheta)\vartheta' = -(v \sin \vartheta)\omega = -\omega v_2$$

$$v'_2 = (v \sin \vartheta)' = v' \sin \vartheta + v(\cos \vartheta)\vartheta' = (v \cos \vartheta)\omega = \omega v_1$$

Differential Axiomatization of Flight Dynamics

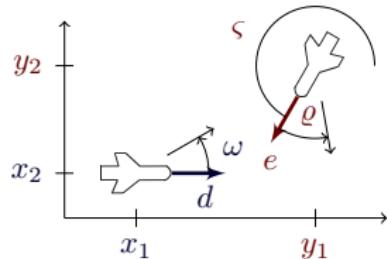


$$\begin{bmatrix} x'_1 = v \cos \vartheta = v_1 & y'_1 = u \cos \varsigma = u_1 \\ x'_2 = v \sin \vartheta = v_2 & y'_2 = u \sin \varsigma = u_2 \\ v'_1 = -\omega v_2 & u'_1 = -\varrho u_2 \\ v'_2 = \omega v_1 & u'_2 = \varrho u_1 \\ \vartheta' = \omega & \varsigma' = \varrho \end{bmatrix}$$

$$v'_1 = (v \cos \vartheta)' = v' \cos \vartheta + v(-\sin \vartheta)\vartheta' = -(v \sin \vartheta)\omega = -\omega v_2$$

$$v'_2 = (v \sin \vartheta)' = v' \sin \vartheta + v(\cos \vartheta)\vartheta' = (v \cos \vartheta)\omega = \omega v_1$$

Differential Axiomatization of Flight Dynamics



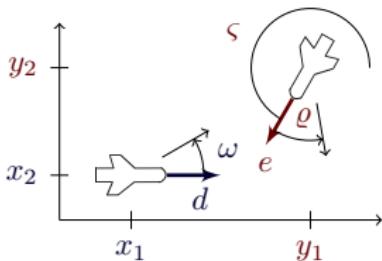
$$\begin{bmatrix} x'_1 = v \cos \vartheta = v_1 & y'_1 = u \cos \varsigma = u_1 \\ x'_2 = v \sin \vartheta = v_2 & y'_2 = u \sin \varsigma = u_2 \\ v'_1 = -\omega v_2 & u'_1 = -\varrho u_2 \\ v'_2 = \omega v_1 & u'_2 = \varrho u_1 \end{bmatrix}$$

$$v'_1 = (v \cos \vartheta)' = v' \cos \vartheta + v(-\sin \vartheta)\vartheta' = -(v \sin \vartheta)\omega = -\omega v_2$$

$$v'_2 = (v \sin \vartheta)' = v' \sin \vartheta + v(\cos \vartheta)\vartheta' = (v \cos \vartheta)\omega = \omega v_1$$

$$v = \|(v_1, v_2)\| = \sqrt{v_1^2 + v_2^2}$$

Differential Axiomatization of Flight Dynamics



$$\begin{bmatrix} x'_1 = v_1 & y'_1 = u_1 \\ x'_2 = v_2 & y'_2 = u_2 \\ v'_1 = -\omega v_2 & u'_1 = -\varrho u_2 \\ v'_2 = \omega v_1 & u'_2 = \varrho u_1 \end{bmatrix}$$

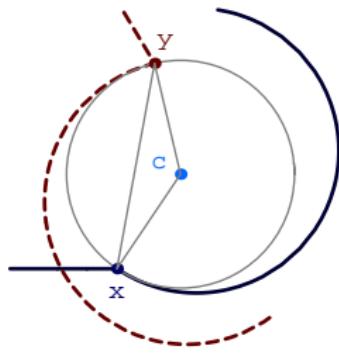
$$v'_1 = (v \cos \vartheta)' = v' \cos \vartheta + v(-\sin \vartheta)\vartheta' = -(v \sin \vartheta)\omega = -\omega v_2$$

$$v'_2 = (v \sin \vartheta)' = v' \sin \vartheta + v(\cos \vartheta)\vartheta' = (v \cos \vartheta)\omega = \omega v_1$$

$$v = \|(v_1, v_2)\| = \sqrt{v_1^2 + v_2^2}$$

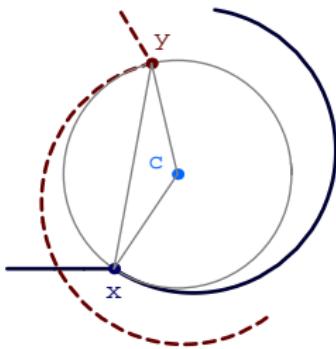
► Differential Invariants for Aircraft Roundabouts

$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



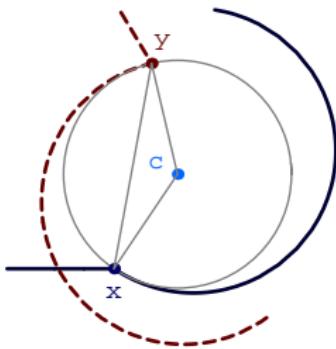
► Differential Invariants for Aircraft Roundabouts

$$\frac{\partial \|x-y\|^2}{\partial x_1} x'_1 + \frac{\partial \|x-y\|^2}{\partial y_1} y'_1 + \frac{\partial \|x-y\|^2}{\partial x_2} x'_2 + \frac{\partial \|x-y\|^2}{\partial y_2} y'_2 \geq \frac{\partial p^2}{\partial x_1} x'_1 \dots$$
$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



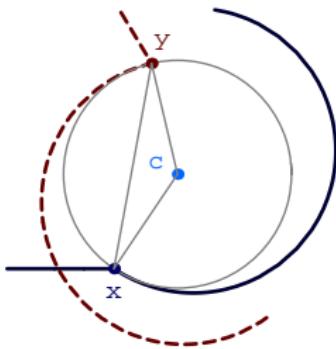
► Differential Invariants for Aircraft Roundabouts

$$\frac{\partial \|x-y\|^2}{\partial x_1} x'_1 + \frac{\partial \|x-y\|^2}{\partial y_1} y'_1 + \frac{\partial \|x-y\|^2}{\partial x_2} x'_2 + \frac{\partial \|x-y\|^2}{\partial y_2} y'_2 \geq \frac{\partial p^2}{\partial x_1} x'_1 \dots$$
$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



► Differential Invariants for Aircraft Roundabouts

$$\frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots$$
$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

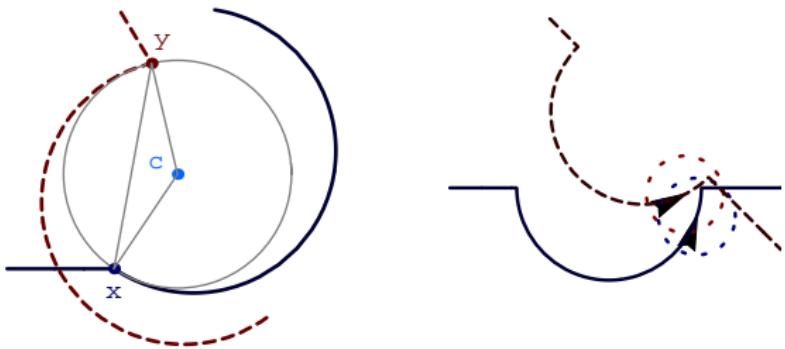


► Differential Invariants for Aircraft Roundabouts

$$\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0$$

$$\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots$$

$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

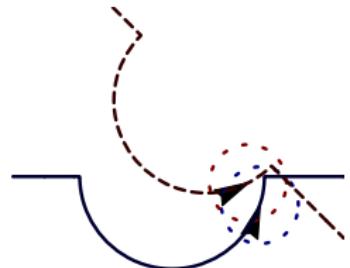
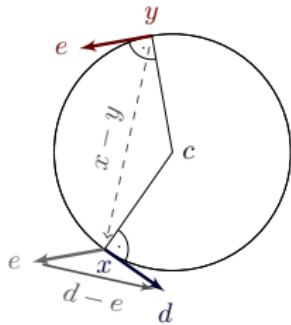


► Differential Invariants for Aircraft Roundabouts

$$\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0$$

$$\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots$$

$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

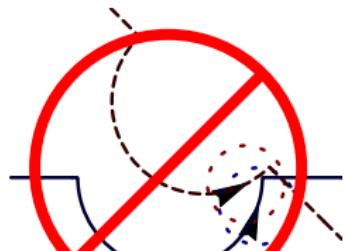
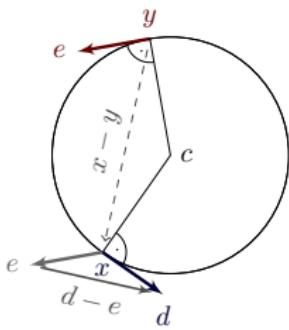


Differential Invariants for Aircraft Roundabouts

$$\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0$$

$$\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots$$

$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



$$\dots \vdash [v'_1 = -\omega v_2, u'_1 = -\omega u_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] v_1 - u_1 = -\omega(x_2 - y_2)$$

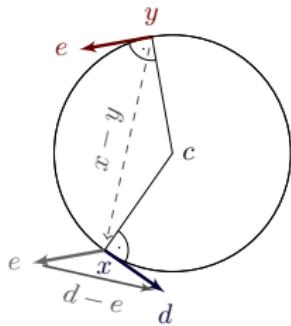
► Differential Invariants for Aircraft Roundabouts

$$\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0$$

$$\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0$$

$$\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots$$

$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



$$\dots \vdash [v'_1 = -\omega v_2, u'_1 = -\omega u_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] v_1 - u_1 = -\omega(x_2 - y_2)$$

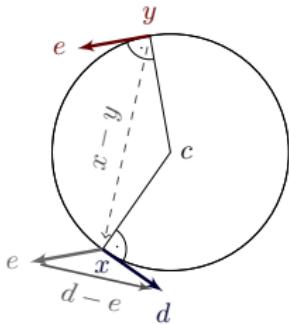
Differential Invariants for Aircraft Roundabouts

$$\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0$$

$$\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0$$

$$\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots$$

$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$

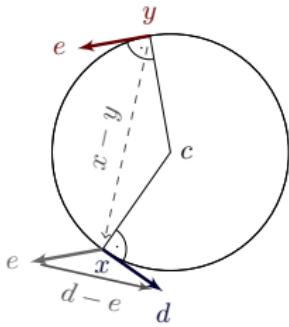


$$\vdash \frac{\partial(v_1 - u_1)}{\partial v_1} v'_1 + \frac{\partial(v_1 - u_1)}{\partial u_1} u'_1 = -\frac{\partial\omega(x_2 - y_2)}{\partial x_2} x'_2 - \frac{\partial\omega(x_2 - y_2)}{\partial y_2} y'_2$$

$$\dots \vdash [v'_1 = -\omega v_2, u'_1 = -\omega u_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] \mathbf{v}_1 - \mathbf{u}_1 = -\omega(\mathbf{x}_2 - \mathbf{y}_2)$$

Differential Invariants for Aircraft Roundabouts

$$\begin{array}{c}
 \vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0 \\
 \hline
 \vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0 \\
 \hline
 \vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots \\
 \hline
 \vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2
 \end{array}$$

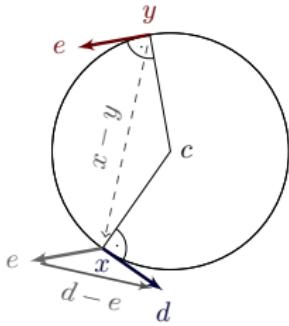


$$\begin{array}{c}
 \vdash \frac{\partial(v_1 - u_1)}{\partial v_1} v'_1 + \frac{\partial(v_1 - u_1)}{\partial u_1} u'_1 = -\frac{\partial\omega(x_2 - y_2)}{\partial x_2} x'_2 - \frac{\partial\omega(x_2 - y_2)}{\partial y_2} y'_2 \\
 \dots \vdash [v'_1 = -\omega v_2, u'_1 = -\omega u_2, x'_2 = v_2, y'_2 = \omega v_1, \dots] v_1 - u_1 = -\omega(x_2 - y_2)
 \end{array}$$

Differential Invariants for Aircraft Roundabouts

$$\frac{\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0}{\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0}$$

$$\frac{\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots}{\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$



$$\frac{\vdash \frac{\partial(v_1-u_1)}{\partial v_1}(-\omega v_2) + \frac{\partial(v_1-u_1)}{\partial u_1}(-\omega u_2) = -\frac{\partial\omega(x_2-y_2)}{\partial x_2} v_2 - \frac{\partial\omega(x_2-y_2)}{\partial y_2} u_2}{.. \vdash [v'_1 = -\omega v_2, u'_1 = -\omega u_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] v_1 - u_1 = -\omega(x_2 - y_2)}$$

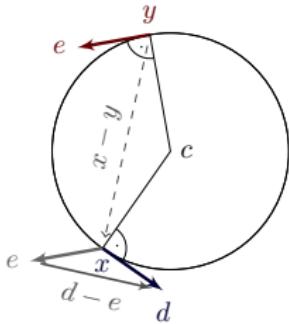
Differential Invariants for Aircraft Roundabouts

$$\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0$$

$$\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0$$

$$\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots$$

$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



$$\vdash -\omega v_2 + \omega u_2 = -\omega(v_2 - u_2)$$

$$\vdash \frac{\partial(v_1 - u_1)}{\partial v_1}(-\omega v_2) + \frac{\partial(v_1 - u_1)}{\partial u_1}(-\omega u_2) = -\frac{\partial\omega(x_2 - y_2)}{\partial x_2} v_2 - \frac{\partial\omega(x_2 - y_2)}{\partial y_2} u_2$$

$$\dots \vdash [v'_1 = -\omega v_2, u'_1 = -\omega u_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] v_1 - u_1 = -\omega(x_2 - y_2)$$

► Differential Invariants & Differential Cuts

$$\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0$$

$$\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0$$

$$\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots$$

$$\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2$$



Proposition (Differential cut saturation)

C differential invariant of $[x' = f(x) \& H]P$, then
 $[x' = f(x) \& H]P$ iff $[x' = f(x) \& H \wedge C]P$

$$\vdash -\omega v_2 + \omega u_2 = -\omega(v_2 - u_2)$$

$$\vdash \frac{\partial(v_1 - u_1)}{\partial v_1}(-\omega v_2) + \frac{\partial(v_1 - u_1)}{\partial u_1}(-\omega u_2) = -\frac{\partial\omega(x_2 - y_2)}{\partial x_2} v_2 - \frac{\partial\omega(x_2 - y_2)}{\partial y_2} u_2$$

$$\dots \vdash [v'_1 = -\omega v_2, u'_1 = -\omega u_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] v_1 - u_1 = -\omega(x_2 - y_2)$$

Differential Invariants & Differential Cuts

$$\frac{\vdash 2(x_1 - y_1)(-\omega(x_2 - y_2)) + 2(x_2 - y_2)\omega(x_1 - y_1) \geq 0}{\vdash 2(x_1 - y_1)(v_1 - u_1) + 2(x_2 - y_2)(v_2 - u_2) \geq 0}$$
$$\frac{\vdash \frac{\partial \|x-y\|^2}{\partial x_1} v_1 + \frac{\partial \|x-y\|^2}{\partial y_1} u_1 + \frac{\partial \|x-y\|^2}{\partial x_2} v_2 + \frac{\partial \|x-y\|^2}{\partial y_2} u_2 \geq \frac{\partial p^2}{\partial x_1} v_1 \dots}{\vdash [x'_1 = v_1, v'_1 = -\omega v_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] (x_1 - y_1)^2 + (x_2 - y_2)^2 \geq p^2}$$

refine dynamics

by differential cut

$$\frac{\vdash -\omega v_2 + \omega u_2 = -\omega(v_2 - u_2)}{\vdash \frac{\partial(v_1 - u_1)}{\partial v_1}(-\omega v_2) + \frac{\partial(v_1 - u_1)}{\partial u_1}(-\omega u_2) = -\frac{\partial \omega(x_2 - y_2)}{\partial x_2} v_2 - \frac{\partial \omega(x_2 - y_2)}{\partial y_2} u_2}$$
$$\dots \vdash [v'_1 = -\omega v_2, u'_1 = -\omega u_2, x'_2 = v_2, v'_2 = \omega v_1, \dots] v_1 - u_1 = -\omega(x_2 - y_2)$$

Outline

1 Learning Objectives

2 Recap: Proofs for Differential Equations

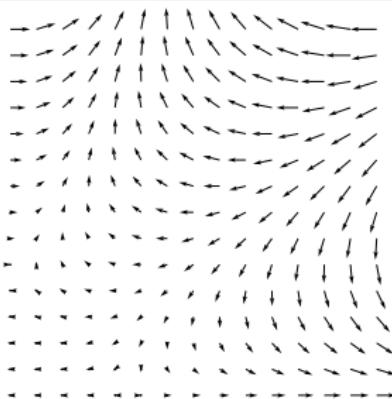
3 The Ghosts of CPS

- Arithmetic Ghosts
- Ghosts of Choice
- Differential-algebraic Ghosts
- Discrete Ghosts
- Differential Ghosts
- Substitute Ghosts
- Solvable Ghosts
- Axiomatic Ghosts

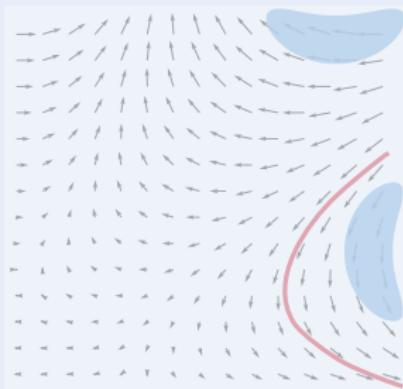
4 Summary

Differential Invariants for Differential Equations

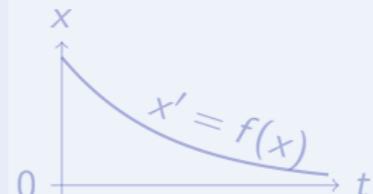
Differential Invariant



Differential Cut



Differential Ghost



Logic

Probability
theory

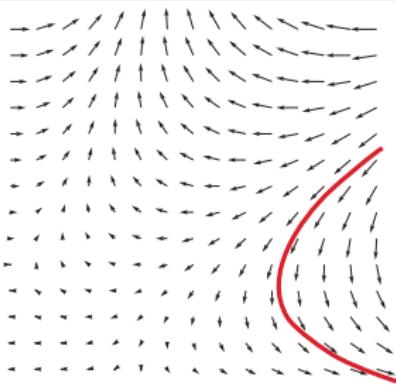
Math

Characteristic PDE

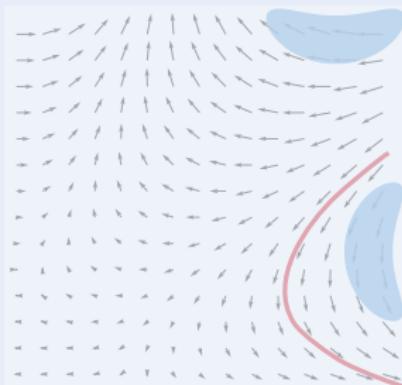
JLogComput'10, CAV'08, FMSD'09, LMCS'12, ITP'12

Differential Invariants for Differential Equations

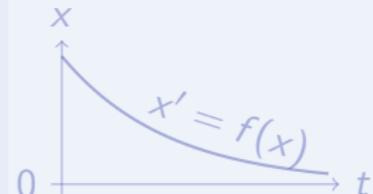
Differential Invariant



Differential Cut



Differential Ghost



Logic

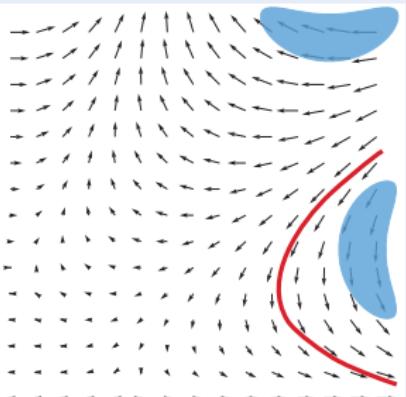
Probability
theory

Math

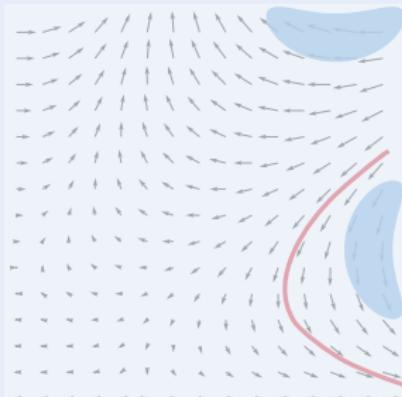
Characteristic PDE

Differential Invariants for Differential Equations

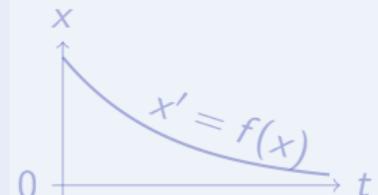
Differential Invariant



Differential Cut



Differential Ghost



Logic

Probability theory

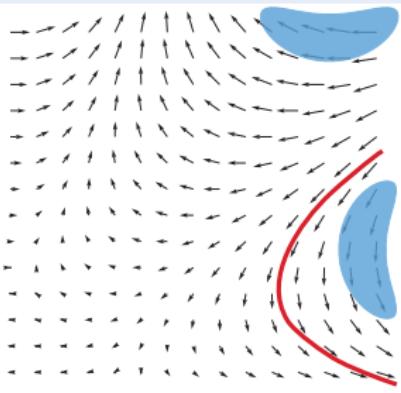
Math

Characteristic PDE

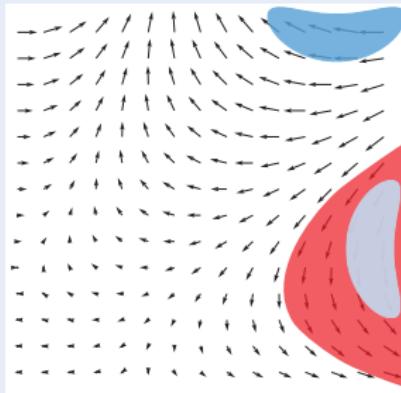
JLogComput'10, CAV'08, FMSD'09, LMCS'12, ITP'12

Differential Invariants for Differential Equations

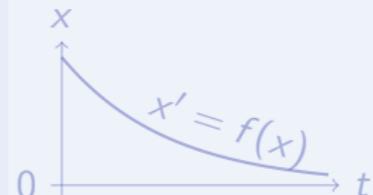
Differential Invariant



Differential Cut



Differential Ghost



Logic

Probability
theory

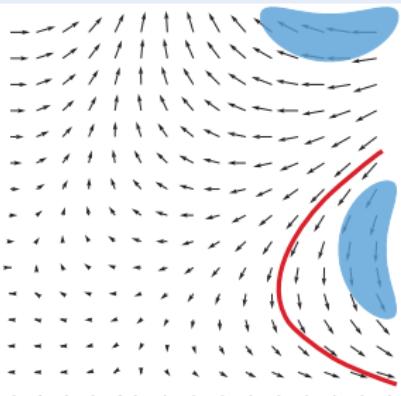
Math

Characteristic PDE

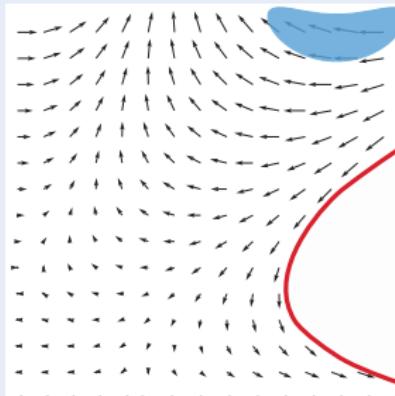
JLogComput'10, CAV'08, FMSD'09, LMCS'12, ITP'12

Differential Invariants for Differential Equations

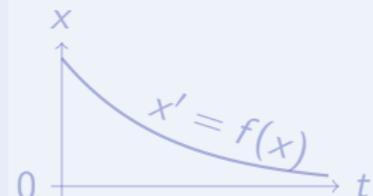
Differential Invariant



Differential Cut



Differential Ghost



Logic

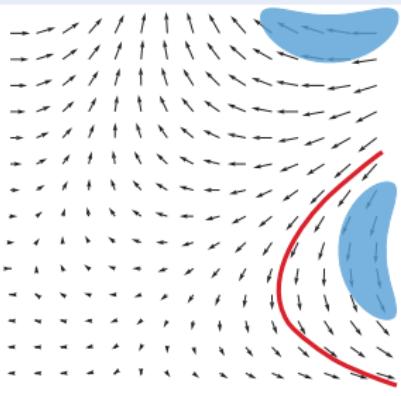
Probability
theory

Math

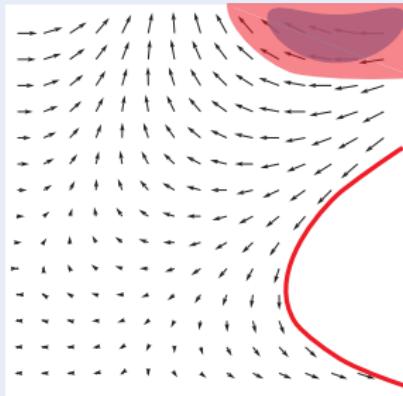
Characteristic PDE

Differential Invariants for Differential Equations

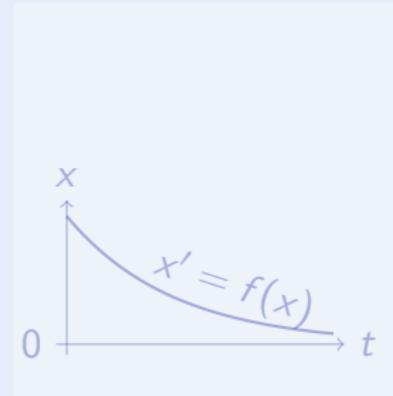
Differential Invariant



Differential Cut



Differential Ghost



Logic

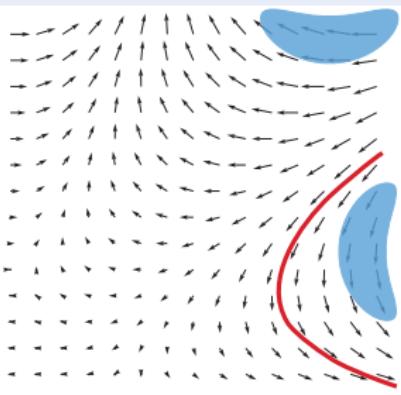
Probability
theory

Math

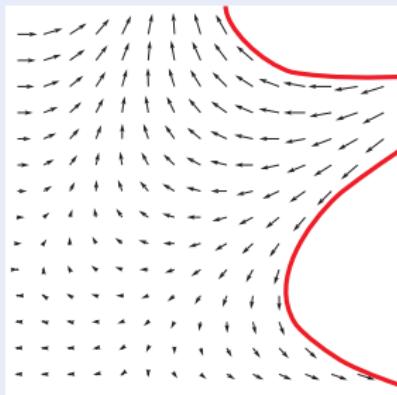
Characteristic PDE

Differential Invariants for Differential Equations

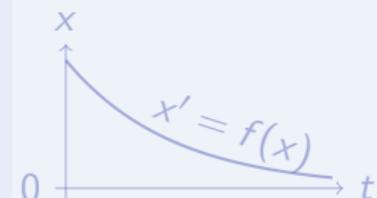
Differential Invariant



Differential Cut



Differential Ghost



Logic

Probability
theory

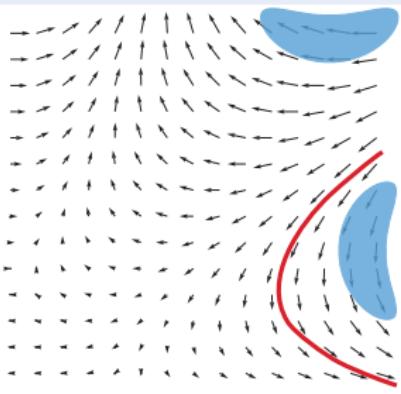
Math

Characteristic PDE

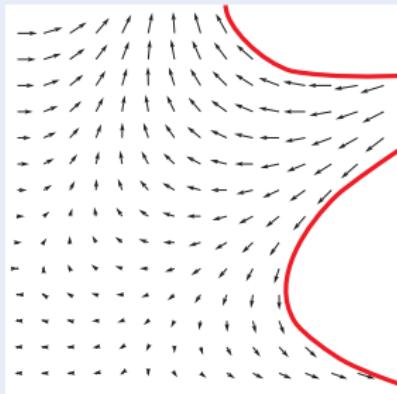
JLogComput'10, CAV'08, FMSD'09, LMCS'12, ITP'12

Differential Invariants for Differential Equations

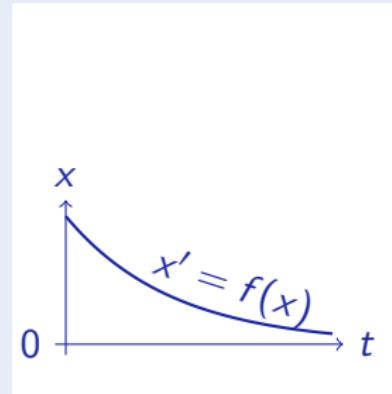
Differential Invariant



Differential Cut



Differential Ghost



Logic

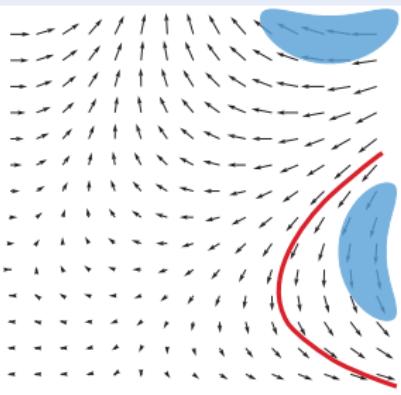
Probability theory

Math

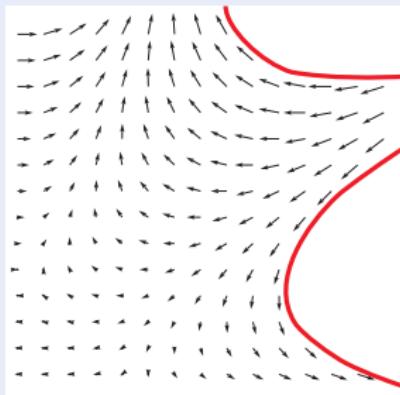
Characteristic PDE

Differential Invariants for Differential Equations

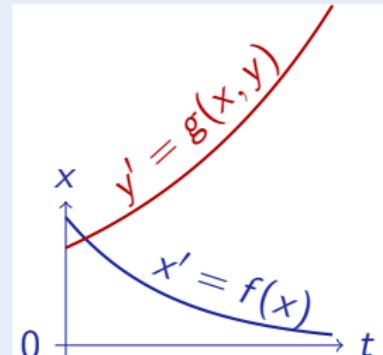
Differential Invariant



Differential Cut



Differential Ghost



Logic

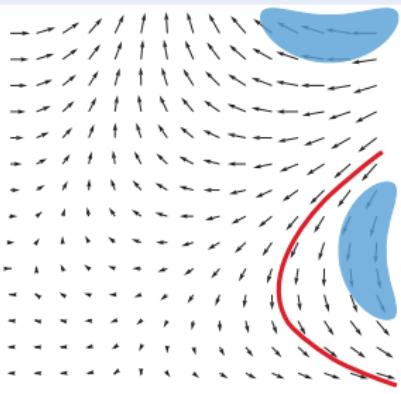
Probability theory

Math

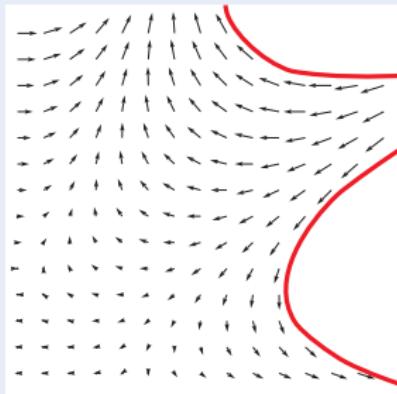
Characteristic PDE

Differential Invariants for Differential Equations

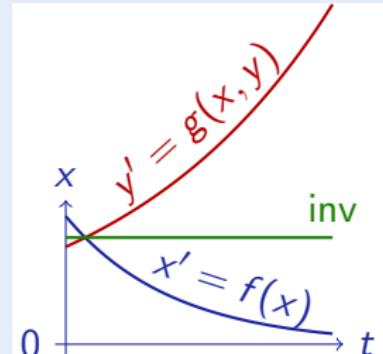
Differential Invariant



Differential Cut



Differential Ghost



Logic

Probability theory

Math

Characteristic PDE

Differential Invariants for Differential Equations

Differential Invariant

$$\frac{Q \vdash [x' := f(x)](F)'}{F \vdash [x' = f(x) \& Q]F}$$

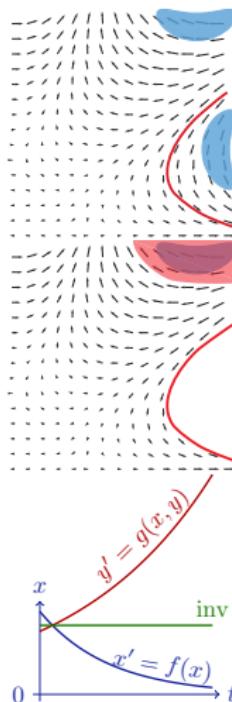
Differential Cut

$$\frac{F \vdash [x' = f(x) \& Q]C \quad F \vdash [x' = f(x) \& Q \wedge C]F}{F \vdash [x' = f(x) \& Q]F}$$

Differential Ghost

$$\frac{F \leftrightarrow \exists y \ G \quad G \vdash [x' = f(x), y' = g(x, y) \& Q]G}{F \vdash [x' = f(x) \& Q]F}$$

if new $y' = g(x, y)$ has a global solution





André Platzer.

Foundations of cyber-physical systems.

Lecture Notes 15-424/624, Carnegie Mellon University, 2016.

URL: <http://www.cs.cmu.edu/~aplatzer/course/fcps16.html>.



André Platzer.

A uniform substitution calculus for differential dynamic logic.

In Amy Felty and Aart Middeldorp, editors, *CADE*, volume 9195 of *LNCS*, pages 467–481. Springer, 2015.

doi:10.1007/978-3-319-21401-6_32.



André Platzer.

The structure of differential invariants and differential cut elimination.

Log. Meth. Comput. Sci., 8(4):1–38, 2012.

doi:10.2168/LMCS-8(4:16)2012.



André Platzer.

A differential operator approach to equational differential invariants.

In Lennart Beringer and Amy Felty, editors, *ITP*, volume 7406 of *LNCS*, pages 28–48. Springer, 2012.

[doi:10.1007/978-3-642-32347-8_3](https://doi.org/10.1007/978-3-642-32347-8_3).



André Platzer.

Differential-algebraic dynamic logic for differential-algebraic programs.

J. Log. Comput., 20(1):309–352, 2010.

[doi:10.1093/logcom/exn070](https://doi.org/10.1093/logcom/exn070).



André Platzer and Edmund M. Clarke.

Computing differential invariants of hybrid systems as fixedpoints.

In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008.

[doi:10.1007/978-3-540-70545-1_17](https://doi.org/10.1007/978-3-540-70545-1_17).



André Platzer and Edmund M. Clarke.

Computing differential invariants of hybrid systems as fixedpoints.

Form. Methods Syst. Des., 35(1):98–120, 2009.

Special issue for selected papers from CAV'08.

[doi:10.1007/s10703-009-0079-8](https://doi.org/10.1007/s10703-009-0079-8).