A Deductive Refinement Calculus for Differential-Algebraic Equations

IJCAR 2026

Jonathan Hellwig[1], Long Qian[2], André Platzer[1]

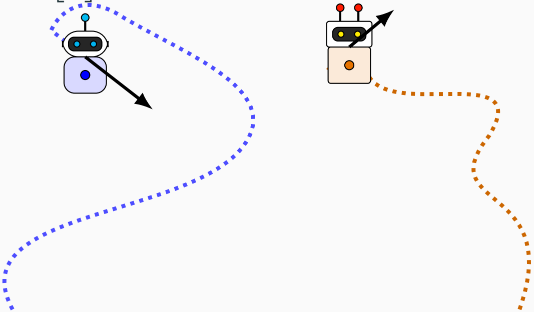
July 28, 2026

[1]Karlsruhe Institute of Technology

[2]Carnegie Mellon University

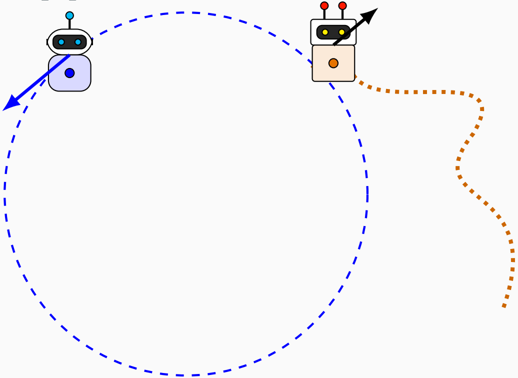
Modeling Physical Systems with DAEs

$$m_1 \begin{bmatrix} \ddot{x}_1 \\ \ddot{y}_1 \end{bmatrix} = \mathbf{F}_1 \qquad m_2 \begin{bmatrix} \ddot{x}_2 \\ \ddot{y}_2 \end{bmatrix} = \mathbf{F}_2$$



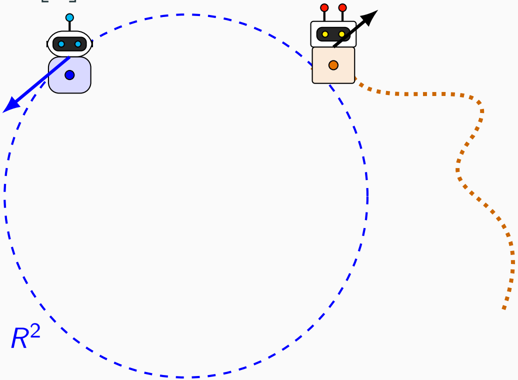
Modeling Physical Systems with DAEs

$$m_1 \begin{bmatrix} \ddot{x}_1 \\ \ddot{y}_1 \end{bmatrix} = \mathbf{F}_1 \qquad m_2 \begin{bmatrix} \ddot{x}_2 \\ \ddot{y}_2 \end{bmatrix} = \mathbf{F}_2$$



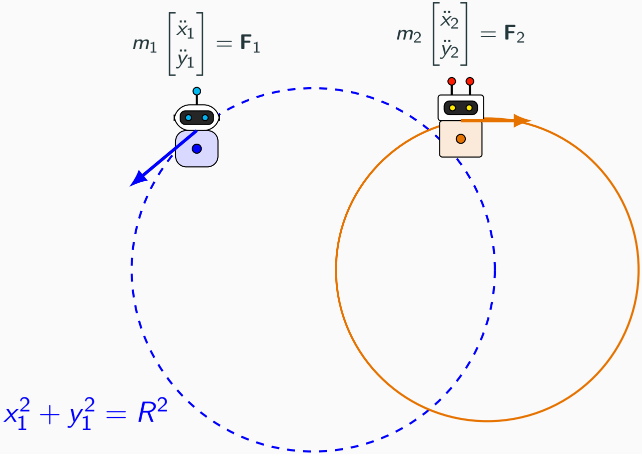
Modeling Physical Systems with DAEs

$$m_1 \begin{bmatrix} \ddot{x}_1 \\ \ddot{y}_1 \end{bmatrix} = \mathbf{F}_1 \qquad m_2 \begin{bmatrix} \ddot{x}_2 \\ \ddot{y}_2 \end{bmatrix} = \mathbf{F}_2$$

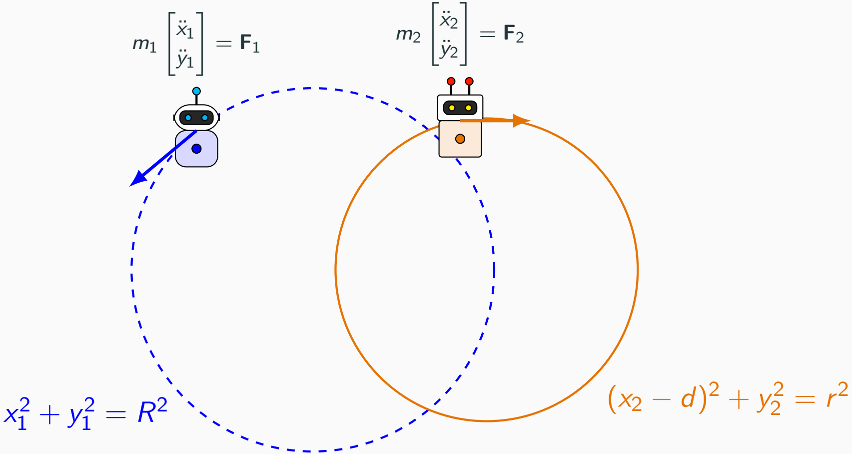


$$x_1^2 + y_1^2 = R^2$$

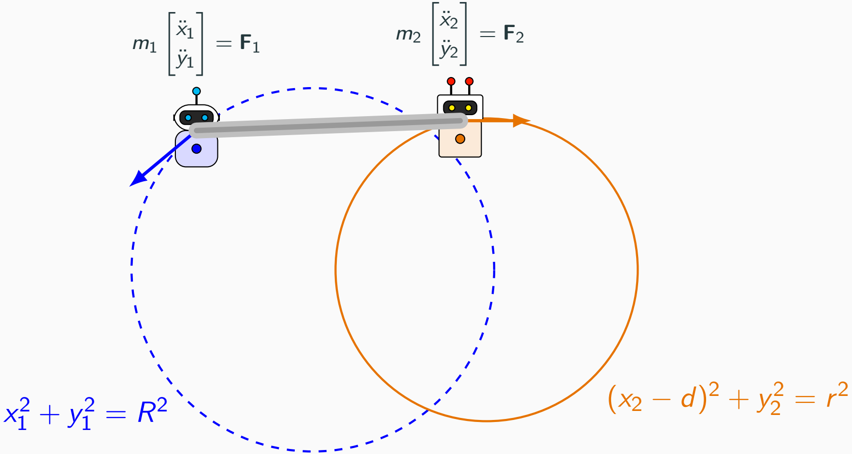
Modeling Physical Systems with DAEs



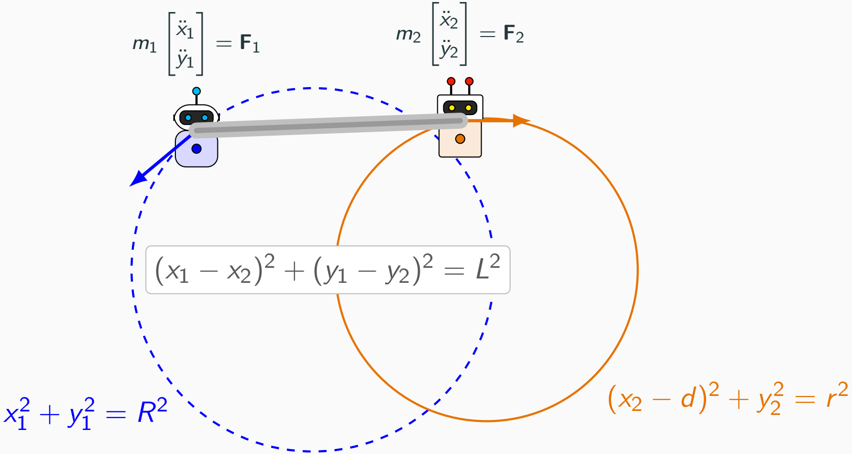
Modeling Physical Systems with DAEs



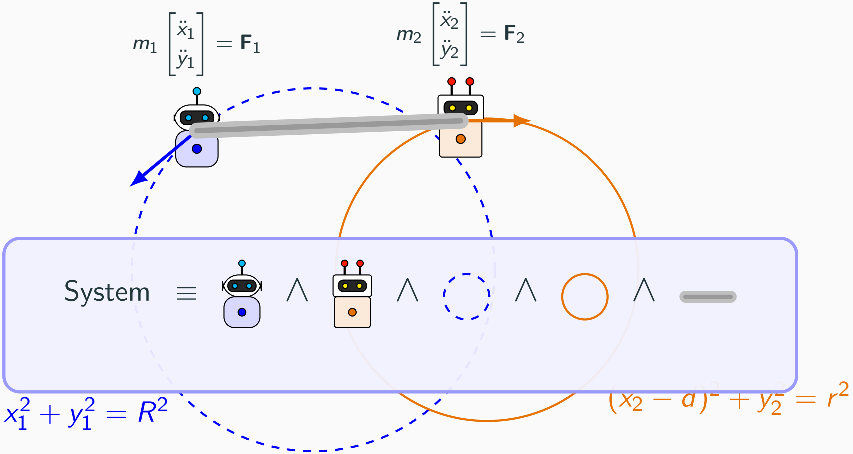
Modeling Physical Systems with DAEs



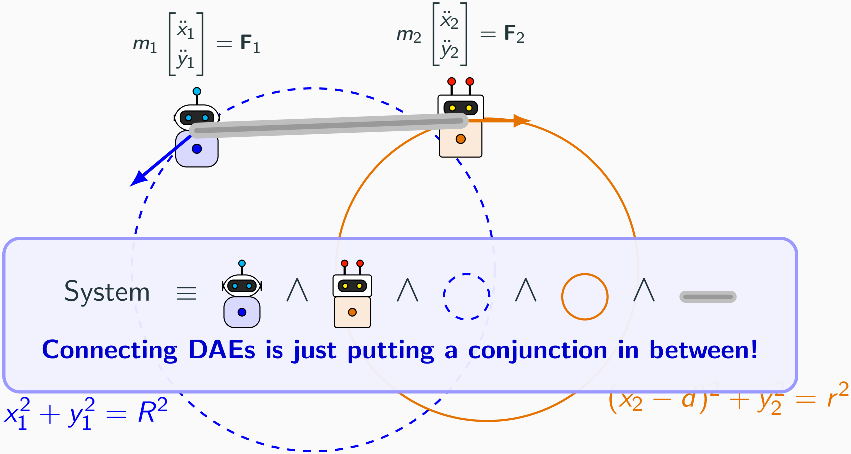
Modeling Physical Systems with DAEs



Modeling Physical Systems with DAEs

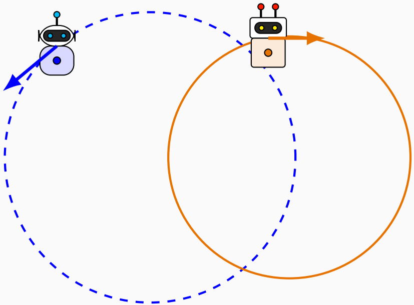


Modeling Physical Systems with DAEs

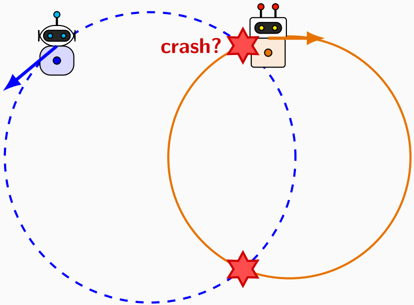


Connecting DAEs is just putting a conjunction in between!

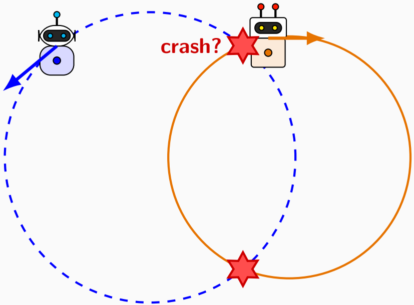
The DAE Verification Problem



The DAE Verification Problem



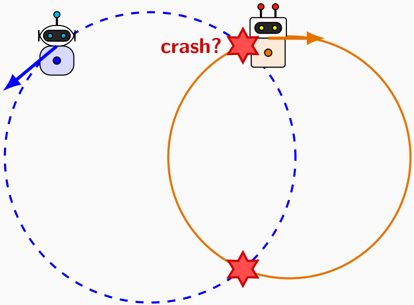
The DAE Verification Problem



DAEs are a powerful modeling paradigm, but

-  solutions are *not unique* and *non-smooth*,
- $\boxed{x^{100} + xy = 0}$ contain *non-linear algebraic equations*,
- $\boxed{x' = ?}$ leave dynamics *hidden*.

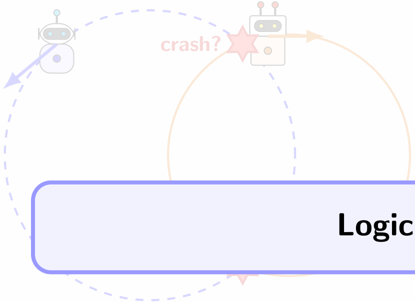
The DAE Verification Problem



DAEs are a powerful modeling paradigm, but

- solutions are *not unique* and *non-smooth*,
- $\boxed{x^{100} + xy = 0}$ contain *non-linear algebraic equations*,
- $\boxed{x' = ?}$ leave dynamics *hidden*.

How can we possibly verify such DAE systems?



DAEs are a powerful modeling paradigm, but

- solutions are *not unique* and *non-smooth*,
- $x' = ?$ leave dynamics *hidden*.

Logic to the Rescue!

How can we possibly verify such DAE systems?

Contributions: The dARL Proof Calculus

We introduce **dARL** $= \mathrm{d}\mathcal{L} + \mathrm{DAPs} + \mathrm{Refinement}$:

- C^1 **Trace Semantics** (Generalizes real-analytic DAPs)
  Rigorously defines DAE behavior, handling *non-unique and non-smooth* solutions $(\min, |\cdot|)$.

- $\boxed{x^{100} + xy = 0}$ **Modular Refinement calculus** $(\alpha \leq_{\mathbf{x}} \beta)$ (First for DAEs)
  Avoids solving *non-linear algebraic equations* by reasoning about them deductively.

- $\boxed{x' = ?}$ **Soundly uncovering hidden dynamics**
  Systematically reveals *hidden dynamics* and enables relational reasoning between DAPs.

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P} \mid \overbrace{[\alpha]P} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q} \mid \underbrace{\{\mathbf{x} : F\}} \mid \underbrace{\alpha \cup \beta \mid \alpha; \beta \mid (\alpha)^*}$$

Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P} \mid \overbrace{\color{blue}{\alpha \leq_{\mathbf{x}} \beta}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q} \mid \underbrace{\color{blue}{\{\mathbf{x} : F\}}} \mid \underbrace{\alpha \cup \beta \mid \alpha; \beta \mid (\alpha)^*}$$

Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q} \mid \underbrace{\{\mathbf{x} : F\}} \mid \underbrace{\alpha \cup \beta \mid \alpha;\, \beta \mid (\alpha)^*}$$

Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}^{\text{Refinement}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q} \mid \underbrace{\{\mathbf{x} : F\}} \mid \underbrace{\alpha \cup \beta \mid \alpha ; \beta \mid (\alpha)^*}$$

Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}^{\text{Refinement}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q}_{\text{Discrete}} \mid \underbrace{\{\mathbf{x} : F\}} \mid \underbrace{\alpha \cup \beta \mid \alpha; \beta \mid (\alpha)^*}$$

Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}^{\text{Refinement}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q}_{\text{Discrete}} \mid \underbrace{\{\mathbf{x} : F\}}_{\text{DAP}} \mid \underbrace{\alpha \cup \beta \mid \alpha; \beta \mid (\alpha)^*}$$

Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}^{\text{Refinement}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q}_{\text{Discrete}} \mid \underbrace{\{\mathbf{x} : F\}}_{\text{DAP}} \mid \underbrace{\alpha \cup \beta \mid \alpha;\, \beta \mid (\alpha)^*}_{\text{Combinators}}$$

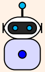
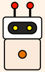
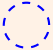
Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}^{\text{Refinement}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q}_{\text{Discrete}} \mid \underbrace{\{\mathbf{x} : F\}}_{\text{DAP}} \mid \underbrace{\alpha \cup \beta \mid \alpha;\, \beta \mid (\alpha)^*}_{\text{Combinators}}$$

Example: Safety Formula in dARL

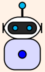
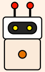
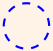
$\mathbf{x} \neq \mathbf{y} \rightarrow [\{\mathbf{x}, \mathbf{y} :$  $\wedge$  $\wedge$  $\wedge$  $\wedge$  $\}]\, \mathbf{x} \neq \mathbf{y}$

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}^{\text{Refinement}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q}_{\text{Discrete}} \mid \underbrace{\{\mathbf{x} : F\}}_{\text{DAP}} \mid \underbrace{\alpha \cup \beta \mid \alpha;\, \beta \mid (\alpha)^*}_{\text{Combinators}}$$

Example: Safety Formula in dARL

$\underbrace{\mathbf{x} \neq \mathbf{y}}_{\text{Initial Condition}} \rightarrow [\{\mathbf{x}, \mathbf{y} :$  $\wedge$  $\wedge$  $\wedge$  $\wedge$  $\}]\, \underbrace{\mathbf{x} \neq \mathbf{y}}$

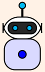
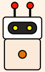
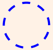
Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}^{\text{Refinement}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q}_{\text{Discrete}} \mid \underbrace{\{\mathbf{x} : F\}}_{\text{DAP}} \mid \underbrace{\alpha \cup \beta \mid \alpha;\, \beta \mid (\alpha)^*}_{\text{Combinators}}$$

Example: Safety Formula in dARL

$\underbrace{\mathbf{x} \neq \mathbf{y}}_{\text{Initial Condition}} \rightarrow [\{\mathbf{x}, \mathbf{y} :$  $\wedge$  $\wedge$  $\wedge$  $\wedge$  $\}]\, \underbrace{\mathbf{x} \neq \mathbf{y}}$

DAE

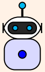
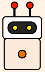
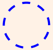
Syntax

dARL syntax

$$P, Q ::= \overbrace{e \leq g \mid \neg P \mid P \wedge Q \mid \forall x\, P}^{\text{FOL}} \mid \overbrace{[\alpha]P}^{\text{Box}} \mid \overbrace{\alpha \leq_{\mathbf{x}} \beta}^{\text{Refinement}}$$

$$\alpha, \beta ::= \underbrace{x := e \mid ?Q}_{\text{Discrete}} \mid \underbrace{\{\mathbf{x} : F\}}_{\text{DAP}} \mid \underbrace{\alpha \cup \beta \mid \alpha;\, \beta \mid (\alpha)^*}_{\text{Combinators}}$$

Example: Safety Formula in dARL

$\underbrace{\mathbf{x} \neq \mathbf{y}}_{\text{Initial Condition}} \rightarrow [\{\mathbf{x}, \mathbf{y} :$  $\wedge$  $\wedge$  $\wedge$  $\wedge$  $\}]\, \underbrace{\mathbf{x} \neq \mathbf{y}}_{\text{Postcondition}}$

DAE

Proof Architecture: Safety via Refinement

Complex DAE Program

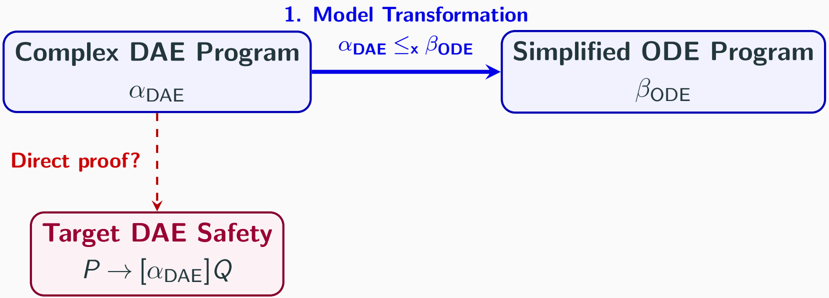
α_{DAE}

$$
\begin{tikzcd}
\text{Complex DAE Program } \alpha_{\mathsf{DAE}} \arrow[d, dashed, "\text{Direct proof?}"'] \\
\text{Target DAE Safety } P \to [\alpha_{\mathsf{DAE}}]Q
\end{tikzcd}
$$

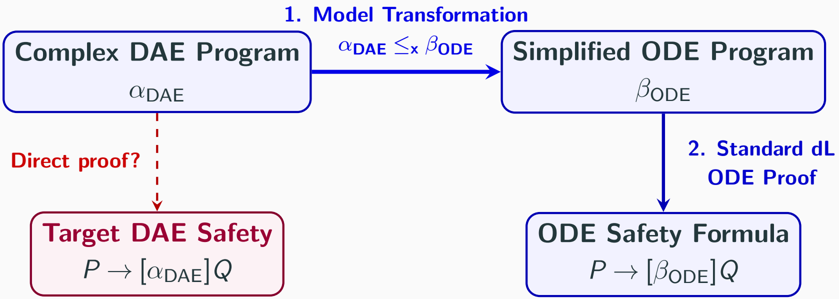
Target DAE Safety

$P \to [\alpha_{\mathsf{DAE}}]Q$

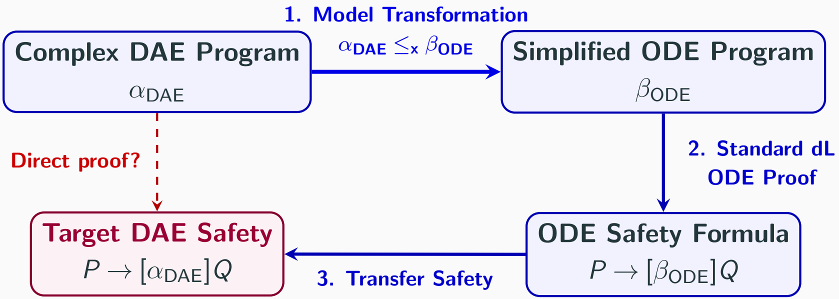
Proof Architecture: Safety via Refinement



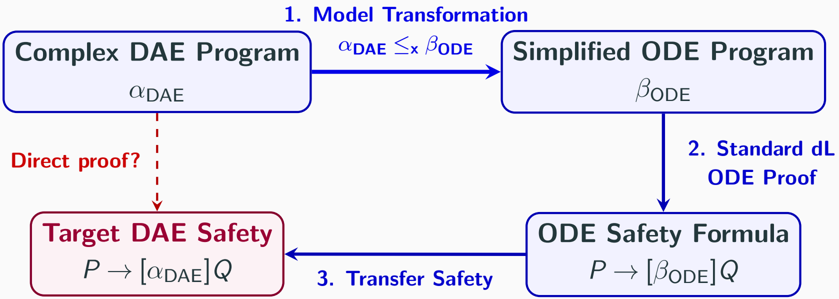
Proof Architecture: Safety via Refinement



Proof Architecture: Safety via Refinement

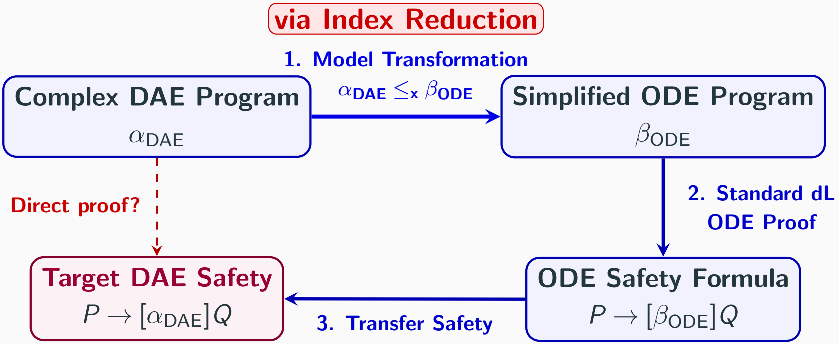


Proof Architecture: Safety via Refinement



Refinement transfers safety from simplified models to complex DAEs!

Proof Architecture: Safety via Refinement



Refinement transfers safety from simplified models to complex DAEs!

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \;\wedge\; y' = y + z \;\wedge\; x = y \qquad\qquad\qquad\qquad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \;\wedge\; y' = y + z \;\wedge\; x = y \qquad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \;\wedge\; y' = y + z \;\wedge\; x = y \wedge x' = y' \qquad\qquad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \; \wedge \; y' = y + z \; \wedge \; \cancel{x = y} \wedge x' = y' \qquad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \;\wedge\; y' = y + z \;\wedge\; x = y \wedge x' = y' \qquad\qquad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \; \wedge \; y' = y + z \; \wedge \; x = y \wedge x' = y' \qquad\qquad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \;\land\; y' = y + z \;\land\; x = y \land x - z = y + z \quad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \ x' = x - z \ \wedge \ y' = y + z \ \wedge \ x = y \wedge z = 0 \qquad\qquad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \;\wedge\; y' = y + z \;\wedge\; x = y \wedge z = 0 \qquad\qquad \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \; \wedge \; y' = y + z \; \wedge \; x = y \wedge z = 0 \; \wedge \; z' = 0 \; \}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \;\land\; y' = y + z \land x = y \land z = 0 \;\land\; z' = 0 \;\}$$

Informal Index Reduction

Index reduction reveals hidden constraints by repeated differentiation.

$$D \equiv \{x, y, z : \; x' = x - z \;\wedge\; y' = y + z \;\wedge\; x = y \wedge z = 0 \;\wedge\; z' = 0 \;\}$$

1. Pick $e = 0$ → **2. Differentiate** $(e)' = 0$ → **3. Algebraic Reduction** → **4. Augment** DAP

Repeat until explicit ODE

Index Reduction in dARL

Derivable Proof Rule: Index Reduction (IR)

Let $\mathbf{r}_0, \ldots, \mathbf{r}_m$ be a sequence of term vectors. Then IR is derivable in dARL:

$$\mathrm{IR}\ \frac{\Gamma \vdash \bigwedge_{k=0}^{m} (\mathbf{r}_k)' = \mathbf{0} \quad \vdash \bigwedge_{k=0}^{m} (\mathbf{f}_k = \mathbf{0} \land Q \rightarrow \mathbf{r}_k = \mathbf{0})}{\Gamma \vdash \{\mathbf{x} : \mathbf{f}_{m+1} = \mathbf{0} \land Q\} =_{\mathbf{x}^\bullet} \{\mathbf{x} : \mathbf{f}_0 = \mathbf{0} \land Q\}}\ \mathrm{FV}(\mathbf{r}_1, \ldots, \mathbf{r}_m) \subseteq \mathbf{x}$$

Why Informal Index Reduction is Unsound

Naive index reduction produces systems incomparable to the original:

1. **Ignoring initial consistency conditions** (introduces drift / spurious behavior)
2. **Unsound algebraic simplifications**
3. **Violating regularity conditions** (may exclude valid C^1 solutions)

Index Reduction in dARL

Derivable Proof Rule: Index Reduction (IR)

Let $\mathbf{r}_0, \ldots, \mathbf{r}_m$ be a sequence of term vectors. Then IR is derivable in dARL:

$$\mathrm{IR}\ \frac{\Gamma \vdash \bigwedge_{k=0}^{m} (\mathbf{r}_k)' = \mathbf{0} \qquad \vdash \bigwedge_{k=0}^{m} (\mathbf{f}_k = \mathbf{0} \land Q \rightarrow \mathbf{r}_k = \mathbf{0})}{\Gamma \vdash \{\mathbf{x} : \mathbf{f}_{m+1} = \mathbf{0} \land Q\} =_{\mathbf{x}^\bullet} \{\mathbf{x} : \mathbf{f}_0 = \mathbf{0} \land Q\}}\ \mathrm{FV}(\mathbf{r}_1, \ldots, \mathbf{r}_m) \subseteq \mathbf{x}$$

Why Informal Index Reduction is Unsound

Naive index reduction produces systems incomparable to the original:

1. **Ignoring initial consistency conditions** (introduces drift / spurious behavior)
2. **Unsound algebraic simplifications**
3. **Violating regularity conditions** (may exclude valid C^1 solutions)

Index Reduction in dARL

Derivable Proof Rule: Index Reduction (IR)

Let $\mathbf{r}_0, \ldots, \mathbf{r}_m$ be a sequence of term vectors. Then IR is derivable in dARL:

$$\mathrm{IR}\ \frac{\Gamma \vdash \bigwedge_{k=0}^{m} (\mathbf{r}_k)' = \mathbf{0} \qquad \vdash \bigwedge_{k=0}^{m} (\mathbf{f}_k = \mathbf{0} \land Q \to \mathbf{r}_k = \mathbf{0})}{\Gamma \vdash \{\mathbf{x} : \mathbf{f}_{m+1} = \mathbf{0} \land Q\} =_{\mathbf{x}^\bullet} \{\mathbf{x} : \mathbf{f}_0 = \mathbf{0} \land Q\}}\ \mathrm{FV}(\mathbf{r}_1, \ldots, \mathbf{r}_m) \subseteq \mathbf{x}$$

Why Informal Index Reduction is Unsound

Naive index reduction produces systems incomparable to the original:

1. **Ignoring initial consistency conditions** (introduces drift / spurious behavior)
2. **Unsound algebraic simplifications**
3. **Violating regularity conditions** (may exclude valid C^1 solutions)

Index Reduction in dARL

Derivable Proof Rule: Index Reduction (IR)

Let $\mathbf{r}_0, \ldots, \mathbf{r}_m$ be a sequence of term vectors. Then IR is derivable in dARL:

$$\mathrm{IR}\ \frac{\Gamma \vdash \bigwedge_{k=0}^{m} (\mathbf{r}_k)' = \mathbf{0} \quad \vdash \bigwedge_{k=0}^{m} (\mathbf{f}_k = \mathbf{0} \land Q \to \mathbf{r}_k = \mathbf{0})}{\Gamma \vdash \{\mathbf{x} : \mathbf{f}_{m+1} = \mathbf{0} \land Q\} =_{\mathbf{x}^\bullet} \{\mathbf{x} : \mathbf{f}_0 = \mathbf{0} \land Q\}}\ \mathrm{FV}(\mathbf{r}_1, \ldots, \mathbf{r}_m) \subseteq \mathbf{x}$$

Why Informal Index Reduction is Unsound

Naive index reduction produces systems incomparable to the original:

1. **Ignoring initial consistency conditions** (introduces drift / spurious behavior)
2. **Unsound algebraic simplifications**
3. **Violating regularity conditions** (may exclude valid C^1 solutions)

Index Reduction in dARL

Derivable Proof Rule: Index Reduction (IR)

Let $\mathbf{r}_0, \dots, \mathbf{r}_m$ be a sequence of term vectors. Then IR is derivable in dARL:

$$\mathrm{IR}\ \frac{\Gamma \vdash \bigwedge_{k=0}^{m} (\mathbf{r}_k)' = \mathbf{0} \quad \vdash \bigwedge_{k=0}^{m} (\mathbf{f}_k = \mathbf{0} \wedge Q \to \mathbf{r}_k = \mathbf{0})}{\Gamma \vdash \{\mathbf{x} : \mathbf{f}_{m+1} = \mathbf{0} \wedge Q\} =_{\mathbf{x}^\bullet} \{\mathbf{x} : \mathbf{f}_0 = \mathbf{0} \wedge Q\}}\ \mathrm{FV}(\mathbf{r}_1, \dots, \mathbf{r}_m) \subseteq \mathbf{x}$$

Why Informal Index Reduction is Unsound

Naive index reduction produces systems incomparable to the original:

1. **Ignoring initial consistency conditions** (introduces drift / spurious behavior)
2. **Unsound algebraic simplifications**
3. **Violating regularity conditions** (may exclude valid C^1 solutions)

Index Reduction in dARL

Derivable Proof Rule: Index Reduction (IR)

Let $\mathbf{r}_0, \ldots, \mathbf{r}_m$ be a sequence of term vectors. Then IR is derivable in dARL:

$$\mathrm{IR}\ \frac{\Gamma \vdash \bigwedge_{k=0}^{m} (\mathbf{r}_k)' = \mathbf{0} \qquad \vdash \bigwedge_{k=0}^{m} (\mathbf{f}_k = \mathbf{0} \land Q \to \mathbf{r}_k = \mathbf{0})}{\Gamma \vdash \{\mathbf{x} : \mathbf{f}_{m+1} = \mathbf{0} \land Q\} =_{\mathbf{x}^\bullet} \{\mathbf{x} : \mathbf{f}_0 = \mathbf{0} \land Q\}}\ \mathrm{FV}(\mathbf{r}_1, \ldots, \mathbf{r}_m) \subseteq \mathbf{x}$$

Why Informal Index Reduction is Unsound

Naive index reduction produces systems incomparable to the original:

1. **Ignoring initial consistency conditions** (introduces drift / spurious behavior)
2. **Unsound algebraic simplifications**
3. **Violating regularity conditions** (may exclude valid C^1 solutions)

The dARL Proof Calculus (excerpt)

Refinement & Cut Axiom

$[\leq_{\mathsf{x}}]$ $\quad \alpha \leq_{\mathsf{x}} \beta \rightarrow ([\beta]P \rightarrow [\alpha]P)$ [1]

$\leq^t_{\mathsf{x}}$ $\quad \alpha \leq_{\mathsf{x}} \beta \wedge \beta \leq_{\mathsf{x}} \gamma \rightarrow \alpha \leq_{\mathsf{x}} \gamma$

DC $\quad [\{\mathsf{x} : F\}]R \rightarrow \{\mathsf{x} : F\} \leq_{\mathsf{x}^\bullet} \{\mathsf{x} : R\}$

[1] $\mathrm{FV}(P) \cap \mathrm{BV}(\alpha, \beta) \subseteq \mathsf{x}$

Box Axioms

DW $\quad [\{\mathsf{x} : F\}]F$

DHC $\quad (e)' = 0 \rightarrow [\{\mathsf{x} : e = 0\}](e)' = 0 \quad \mathrm{FV}(e) \subseteq \mathsf{x}$

$\mathrm{DI}_{\preceq}$ $\quad e \preceq 0 \rightarrow [\{\mathsf{x} : (e)' \leq 0\}]e \preceq 0 \quad \mathrm{FV}(e) \subseteq \mathsf{x}$

Subsystem Axioms (DAE Monotonicity & Reduction)

DM $\quad \{\mathsf{x} : F\} \leq_{\mathsf{x}^\bullet} \{\mathsf{x} : G\} \rightarrow \{\mathsf{x} : F \wedge R\} \leq_{\mathsf{x}^\bullet} \{\mathsf{x} : G \wedge R\}$

DR $\quad \forall \mathsf{z} \forall \mathsf{z}'(\{\mathsf{x}, \mathsf{z} : R \wedge F\} \leq_{\mathsf{x}^\bullet} \{\mathsf{x} : F\})$

Soundness Theorem: The dARL proof calculus is sound w.r.t. C^1 DAE flow semantics.

Core Engine for Modular Transfer: DC, DHC, DM

DC Differential Cut

$$[\{\mathbf{x} : F\}]R \rightarrow \{\mathbf{x} : F\} \leq_{\mathbf{x}^\bullet} \{\mathbf{x} : R\}$$

Cuts proved continuous invariants R directly into the DAE system.

DHC Differential Hidden Constraint

$$(e)' = 0 \rightarrow [\{\mathbf{x} : e = 0\}](e)' = 0 \qquad \mathrm{FV}(e) \subseteq \mathbf{x}$$

Differentiates algebraic constraints ($e = 0 \implies (e)' = 0$) during index reduction.

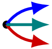
DM Differential Monotonicity

$$\{\mathbf{x} : F\} \leq_{\mathbf{x}^\bullet} \{\mathbf{x} : G\} \rightarrow \{\mathbf{x} : F \wedge R\} \leq_{\mathbf{x}^\bullet} \{\mathbf{x} : G \wedge R\}$$

Preserves refinement $\alpha \leq_{\mathbf{x}} \beta$ under shared context constraints R.

Takeaway: Together, DC + DHC + DM enable modular verification of complex systems.

Summary & Future Work



C^1 **Trace Semantics**

$\boxed{x^{100} + xy = 0}$

Modular Refinement Calculus

$\boxed{x' = ?}$

Sound Index Reduction

Summary & Future Work

C^1 **Trace Semantics**

$\boxed{x^{100} + xy = 0}$

Modular Refinement Calculus

$\boxed{x' = ?}$

Sound Index Reduction

Hidden constraints causing soundness chaos? Logic to the rescue!

Thank You

Questions? Contact: `jonathan.hellwig@kit.edu`

Refinement

Refinement Semantics

$$[\![\alpha \leq_{\mathsf{x}} \beta]\!] = \{\omega \in \mathbb{S} \mid \forall \varphi \in [\![\alpha]\!](\omega)\ \exists \psi \in [\![\beta]\!](\omega) : \psi \sim_{\mathsf{x}} \varphi\}$$

Refinement $(\alpha \leq_{x,y} \beta)$