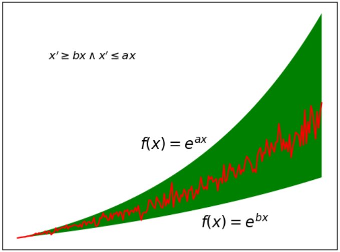
Differential-Algebraic Dynamic Logic for KeYmaera X

CPS Grand Prix

Benjamin Lim   Yao Chong Lim

School of Computer Science, Carnegie Mellon University

December 11, 2018



Motivation

Imprecision is everywhere in actual Cyber-Physical systems...

Motivation

Imprecision is everywhere in actual Cyber-Physical systems...
but how do we precisely model its semantics and prove guarantees?

Differential-Algebraic Dynamic Logic (d$\mathcal{AL}$)

$$x \le m \;\rightarrow\; \big[\{x' = v, v' = a \,\&\, v \ge 0\}\big]\, x \le m$$

Differential-Algebraic Dynamic Logic (dA$\mathcal{L}$)

$$x \leq m \ \rightarrow\ \left[\{x' = v, v' = a \,\&\, v \geq 0\}\right] x \leq m$$

Differential-Algebraic Dynamic Logic (dA$\mathcal{L}$)

$$x \le m \rightarrow \left[\{\exists\, \delta.\, (x' = v, v' = a + \delta \,\&\, v \ge 0 \wedge \delta^2 \le \frac{|v|}{100})\} \right] x \le m$$

Differential-Algebraic Dynamic Logic (dA$\mathcal{L}$)

dA$\mathcal{L}$ = d$\mathcal{L}$ + existentially quantified ODEs

$$\{\exists\, \bar{y}.\, (x_1' = \theta_1, x_2' = \theta_2, \cdots, x_n' = \theta_n \,\&\, Q)\}$$

dA$\mathcal{L}$ Example (Perturbed Circular Motion)

$$x^2 + y^2 = 1 \rightarrow \left[\{x' = -y, y' = x\}\right] x^2 + y^2 \leq 1$$

dA$\mathcal{L}$ Example (Perturbed Circular Motion)

$$x^2 + y^2 = 1 \rightarrow \left[\{\exists e.(x' = -y + e, y' = x \,\&\, x \cdot e \leq 0)\}\right] x^2 + y^2 \leq 1$$

Uniform Substitution (Abridged)

- $[x := e]P(x) \rightarrow P(e)$ Axiom Schema

Uniform Substitution (Abridged)

- $[x := e]P(x) \rightarrow P(e)$ Axiom Schema
- $[x := x + x][y := 3]x > 0 \rightarrow [y := 3]x + x > 0$

Uniform Substitution (Abridged)

- $[x := e]P(x) \rightarrow P(e)$ Axiom Schema
- $[x := x + x][y := 3]x > 0 \rightarrow [y := 3]x + x > 0$ Valid instance!

Uniform Substitution (Abridged)

- $[x := e]P(x) \rightarrow P(e)$ Axiom Schema
- $[x := x + x][y := 3]x > 0 \rightarrow [y := 3]x + x > 0$ Valid instance!
- $[x := x + y][y := 3]x > 0 \rightarrow [y := 3]x + y > 0$

Uniform Substitution (Abridged)

- $[x := e]P(x) \rightarrow P(e)$ Axiom Schema
- $[x := x + x][y := 3]x > 0 \rightarrow [y := 3]x + x > 0$ Valid instance!
- $[x := x + y][y := 3]x > 0 \rightarrow [y := 3]x + y > 0$ Invalid instance!

Uniform Substitution (Abridged)

- $[x := e]P(x) \rightarrow P(e)$ Axiom Schema
- $[x := x + x][y := 3]x > 0 \rightarrow [y := 3]x + x > 0$ Valid instance!
- $[x := x + y][y := 3]x > 0 \rightarrow [y := 3]x + y > 0$ Invalid instance!

Uniform Substitution (Abridged)

- $[x := e]P(x) \rightarrow P(e)$ Axiom Schema
- $[x := x + x][y := 3]x > 0 \rightarrow [y := 3]x + x > 0$ Valid instance!
- $[x := x + y][y := 3]x > 0 \rightarrow [y := 3]x + y > 0$ Invalid instance!
- Side conditions necessary...

Uniform Substitution (Abridged)

- $[x := e]P(x) \to P(e)$ Axiom Schema
- $[x := x + x][y := 3]x > 0 \to [y := 3]x + x > 0$ Valid instance!
- $[x := x + y][y := 3]x > 0 \to [y := 3]x + y > 0$ Invalid instance!
- Side conditions necessary...but which ones?

Uniform Substitution (Abridged)

- $[x := e]P(x) \rightarrow P(e)$ Axiom Schema
- $[x := x + x][y := 3]x > 0 \rightarrow [y := 3]x + x > 0$ Valid instance!
- $[x := x + y][y := 3]x > 0 \rightarrow [y := 3]x + y > 0$ Invalid instance!
- Side conditions necessary...but which ones?
- Key observation: Never bind a free variable that was free!

Uniform Substitution (Abridged)

Instead of schema each with their own unique side conditions...

$$[x := e]P(x) \to P(e) \quad (\text{+some set of side conditions})$$

Uniform Substitution (Abridged)

Instead of schema each with their own unique side conditions...

$$[x := e]P(x) \rightarrow P(e) \quad (+\text{some set of side conditions})$$

You have substitution axioms (without side conditions)...

$$[x := c()]p(x) \rightarrow p(c())$$

Uniform Substitution (Abridged)

Instead of schema each with their own unique side conditions...

$$[x := e]P(x) \rightarrow P(e) \quad (+\text{some set of side conditions})$$

You have substitution axioms (without side conditions)...

$$[x := c()]p(x) \rightarrow p(c())$$

and generic *admissibility rules* for each logical construct (checked recursively) preventing capture of free variables.

Uniform Substitution (Abridged)

Upshot: A significantly reduced soundness-critical core that is easier to maintain and understand

Plan of Attack

- Modernize d$\mathcal{AL}$, providing a uniform substitution calculus for it similar to that for d$\mathcal{L}$.

Plan of Attack

- Modernize d$\mathcal{AL}$, providing a uniform substitution calculus for it similar to that for d$\mathcal{L}$.
- Implement uniform substitution axioms into KeYmaeraX.

Plan of Attack

- Modernize d$\mathcal{AL}$, providing a uniform substitution calculus for it similar to that for d$\mathcal{L}$.
- Implement uniform substitution axioms into KeYmaeraX.
- Implement derived axioms and tactics into KeYmaeraX.

Plan of Attack

- Modernize d$\mathsf{A}\mathcal{L}$, providing a uniform substitution calculus for it similar to that for d$\mathcal{L}$.
- Implement uniform substitution axioms into KeYmaeraX.
- Implement derived axioms and tactics into KeYmaeraX.
- Prove stuff!

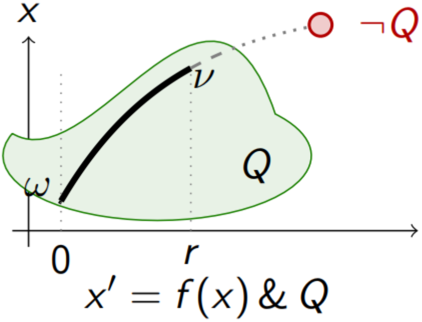
d$\mathcal{L}$ Recap

DW $[c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x})](q(\bar{x}) \rightarrow p(\bar{x}))$

DC $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x}) \wedge r(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})]r(\bar{x})$

DE $[x' = f(\bar{x}), c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [x' = f(\bar{x}), c \,\&\, q(\bar{x})][x' := f(\bar{x})]p(\bar{x})$

DI $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [?q(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})](p(\bar{x}))'$



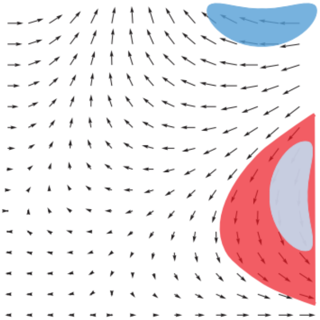
d$\mathcal{L}$ Recap

DW $[c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x})](q(\bar{x}) \rightarrow p(\bar{x}))$

DC $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x}) \wedge r(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})]r(\bar{x})$

DE $[x' = f(\bar{x}), c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [x' = f(\bar{x}), c \,\&\, q(\bar{x})][x' := f(\bar{x})]p(\bar{x})$

DI $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [?q(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})](p(\bar{x}))'$



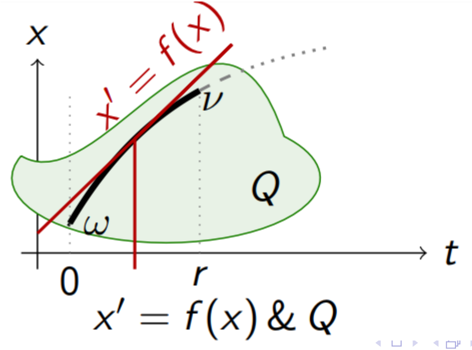
d$\mathcal{L}$ Recap

DW $[c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x})](q(\bar{x}) \rightarrow p(\bar{x}))$

DC $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x}) \wedge r(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})]r(\bar{x})$

DE $[x' = f(\bar{x}), c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [x' = f(\bar{x}), c \,\&\, q(\bar{x})][x' := f(\bar{x})]p(\bar{x})$

DI $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [?q(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})](p(\bar{x}))'$



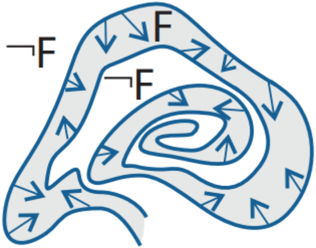
d$\mathcal{L}$ Recap

DW $[c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x})](q(\bar{x}) \rightarrow p(\bar{x}))$

DC $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x}) \wedge r(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})]r(\bar{x})$

DE $[x' = f(\bar{x}), c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [x' = f(\bar{x}), c \,\&\, q(\bar{x})][x' := f(\bar{x})]p(\bar{x})$

DI $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [?q(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})](p(\bar{x}))'$



Attempts at Uniformity

$$
\begin{array}{rl}
\text{DW} & [c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x})](q(\bar{x}) \rightarrow p(\bar{x})) \\
\text{DC} & ([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x}) \wedge r(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})]r(\bar{x}) \\
\text{DE} & [x' = f(\bar{x}), c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [x' = f(\bar{x}), c \,\&\, q(\bar{x})][x' := f(\bar{x})]p(\bar{x}) \\
\text{DI} & ([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [?q(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})](p(\bar{x}))'
\end{array}
$$

Attempts at Uniformity

DW $[c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x})](q(\bar{x}) \rightarrow p(\bar{x}))$

DC $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x}) \wedge r(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})]r(\bar{x})$

DE $[x' = f(\bar{x}), c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [x' = f(\bar{x}), c \,\&\, q(\bar{x})][x' := f(\bar{x})]p(\bar{x})$

DI $([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [?q(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})](p(\bar{x}))'$

Attempts at Uniformity

$$
\begin{array}{rl}
\text{DW} & [c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x})](q(\bar{x}) \rightarrow p(\bar{x})) \\
\text{DC} & ([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x}) \wedge r(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})]r(\bar{x}) \\
\text{DE} & [x' = f(\bar{x}), c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [x' = f(\bar{x}), c \,\&\, q(\bar{x})][x' := f(\bar{x})]p(\bar{x}) \\
\text{DI} & ([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [?q(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})](p(\bar{x}))'
\end{array}
$$

$$([\exists \bar{y}.(c \,\&\, q(\bar{x}, \bar{y}))]p(\bar{x}) \leftrightarrow \forall \bar{y}.[?q(\bar{x}, \bar{y})]p(\bar{x})) \leftarrow \forall \bar{y}.[c \,\&\, q(\bar{x}, \bar{y})](p(\bar{x}))'$$

Attempts at Uniformity

$$\begin{array}{rl}
\text{DW} & [c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x})](q(\bar{x}) \rightarrow p(\bar{x})) \\
\text{DC} & ([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [c \,\&\, q(\bar{x}) \wedge r(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})]r(\bar{x}) \\
\text{DE} & [x' = f(\bar{x}), c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [x' = f(\bar{x}), c \,\&\, q(\bar{x})][x' := f(\bar{x})]p(\bar{x}) \\
\text{DI} & ([c \,\&\, q(\bar{x})]p(\bar{x}) \leftrightarrow [?q(\bar{x})]p(\bar{x})) \leftarrow [c \,\&\, q(\bar{x})](p(\bar{x}))'
\end{array}$$

$$([\exists \bar{y}.(c \,\&\, q(\bar{x}, \bar{y}))]p(\bar{x}) \leftrightarrow \forall \bar{y}.[?q(\bar{x}, \bar{y})]p(\bar{x})) \leftarrow \forall \bar{y}.[c \,\&\, q(\bar{x}, \bar{y})](p(\bar{x}))'$$

Wrong!

Attempts at Uniformity

$$([\exists \bar{y}.(c \,\&\, q(\bar{x}, \bar{y}))]p(\bar{x}) \leftrightarrow \forall \bar{y}.[?q(\bar{x}, \bar{y})]p(\bar{x})) \leftarrow \forall \bar{y}.[c \,\&\, q(\bar{x}, \bar{y})](p(\bar{x}))'$$

Attempts at Uniformity

$$([\exists \bar{y}.(c \,\&\, q(\bar{x},\bar{y}))]p(\bar{x}) \leftrightarrow \forall \bar{y}.[?q(\bar{x},\bar{y})]p(\bar{x})) \leftarrow \forall \bar{y}.[c \,\&\, q(\bar{x},\bar{y})](p(\bar{x}))'$$

Counterexample:

$$\begin{aligned}(\left[\{\exists y.(x' = y, z' = -1 \,\&\, y \geq z)\}\right] x \geq 0 \leftrightarrow \forall y.\,[?y \geq z]\, x \geq 0) \\ \leftarrow \forall y.\left[\{x' = y, z' = -1 \,\&\, y \geq z\}\right](x \geq 0)'\end{aligned}$$

Attempts at Uniformity

$$([\exists\bar{y}.(c\,\&\,q(\bar{x},\bar{y}))]p(\bar{x}) \leftrightarrow \forall\bar{y}.[?q(\bar{x},\bar{y})]p(\bar{x})) \leftarrow \forall\bar{y}.[c\,\&\,q(\bar{x},\bar{y})](p(\bar{x}))'$$

Counterexample:

$$\begin{aligned}(\left[\{\exists y.(x' = y, z' = -1\,\&\, y \geq z)\}\right] x \geq 0 \leftrightarrow \forall y. [?y \geq z]\, x \geq 0)\\ \leftarrow \forall y. \left[\{x' = y, z' = -1\,\&\, y \geq z\}\right] (x \geq 0)'\end{aligned}$$

Pick a state with $x \geq 0 \wedge z \geq 0$:

Attempts at Uniformity

$$([\exists\bar{y}.(c\,\&\,q(\bar{x},\bar{y}))]p(\bar{x}) \leftrightarrow \forall\bar{y}.[?q(\bar{x},\bar{y})]p(\bar{x})) \leftarrow \forall\bar{y}.[c\,\&\,q(\bar{x},\bar{y})](p(\bar{x}))'$$

Counterexample:

$$\begin{aligned}(\,\big[\{\exists y.(x' = y, z' = -1\,\&\,y \geq z)\}\big]\,x \geq 0 \leftrightarrow \forall y.\,[?y \geq z]\,x \geq 0)\\ \leftarrow \forall y.\,\big[\{x' = y, z' = -1\,\&\,y \geq z\}\big]\,(x \geq 0)'\end{aligned}$$

Pick a state with $x \geq 0 \wedge z \geq 0$:

- Premise 1: $\forall y.\,[\{x' = y, z' = -1\,\&\,y \geq z\}]\,(x \geq 0)'$ True!

Attempts at Uniformity

$$([\exists\bar{y}.(c\,\&\,q(\bar{x},\bar{y}))]p(\bar{x}) \leftrightarrow \forall\bar{y}.[?q(\bar{x},\bar{y})]p(\bar{x})) \leftarrow \forall\bar{y}.[c\,\&\,q(\bar{x},\bar{y})](p(\bar{x}))'$$

Counterexample:

$$\begin{aligned}(\,\big[\{\exists y.(x' = y, z' = -1\,\&\,y \geq z)\}\big]\,x \geq 0 \leftrightarrow \forall y.\,[?y \geq z]\,x \geq 0) \\ \leftarrow \forall y.\,\big[\{x' = y, z' = -1\,\&\,y \geq z\}\big]\,(x \geq 0)'\end{aligned}$$

Pick a state with $x \geq 0 \wedge z \geq 0$:

- Premise 1: $\forall y.\,[\{x' = y, z' = -1\,\&\,y \geq z\}]\,(x \geq 0)'$ True!
- Premise 2: $\forall y.\,[?y \geq z]\,x \geq 0$ True!

Attempts at Uniformity

$$([\exists \bar{y}.(c \,\&\, q(\bar{x},\bar{y}))]p(\bar{x}) \leftrightarrow \forall \bar{y}.[?q(\bar{x},\bar{y})]p(\bar{x})) \leftarrow \forall \bar{y}.[c \,\&\, q(\bar{x},\bar{y})](p(\bar{x}))'$$

Counterexample:

$$\begin{aligned}(\left[\{\exists y.(x' = y, z' = -1 \,\&\, y \geq z)\}\right] x \geq 0 \leftrightarrow \forall y.\, [?y \geq z]\, x \geq 0) \\ \leftarrow \forall y.\, \left[\{x' = y, z' = -1 \,\&\, y \geq z\}\right] (x \geq 0)'\end{aligned}$$

Pick a state with $x \geq 0 \wedge z \geq 0$:

- Premise 1: $\forall y.\, [\{x' = y, z' = -1 \,\&\, y \geq z\}]\, (x \geq 0)'$ True!
- Premise 2: $\forall y.\, [?y \geq z]\, x \geq 0$ True!
- Conclusion: $[\{\exists y.(x' = y, z' = -1 \,\&\, y \geq z)\}]\, x \geq 0$ False??

Uniform Substitution for dA$\mathcal{L}$

$$\text{DC} \quad ([c \,\&\, q]p \leftrightarrow [c \,\&\, q \wedge r]p) \leftarrow [c \,\&\, q]r$$

$$\text{DI} \quad ([c \,\&\, q]p \leftrightarrow [?q]p) \leftarrow [c \,\&\, q](p)'$$

$$\text{DW} \quad [c \,\&\, q]p \leftrightarrow [c \,\&\, q](q \rightarrow p)$$

$$\text{DE} \quad [x' = f, c \,\&\, q]p \leftrightarrow [x' = f, c \,\&\, q][x' := f]p$$

$$\text{DAC} \quad ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q \wedge r)\}]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, r$$

$$\text{DAI} \quad ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [?q]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (p)'$$

$$\text{DAW} \quad [\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (q \rightarrow p)$$

$$\text{DAE} \quad \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] p \leftrightarrow \forall \bar{y}.\, \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] \left[x' := f\right] p$$

Uniform Substitution for dA$\mathcal{L}$

$$\begin{array}{rl}
\text{DC} & ([c\,\&\,q]p \leftrightarrow [c\,\&\,q \land r]p) \leftarrow [c\,\&\,q]r \\
\text{DI} & ([c\,\&\,q]p \leftrightarrow [?q]p) \leftarrow [c\,\&\,q](p)' \\
\text{DW} & [c\,\&\,q]p \leftrightarrow [c\,\&\,q](q \rightarrow p) \\
\text{DE} & [x' = f, c\,\&\,q]p \leftrightarrow [x' = f, c\,\&\,q][x' := f]p
\end{array}$$

$$\begin{array}{rl}
\text{DAC} & ([\{\exists \bar{y}.(c\,\&\,q)\}]\,p \leftrightarrow [\{\exists \bar{y}.(c\,\&\,q \land r)\}]\,p) \leftarrow [\{\exists \bar{y}.(c\,\&\,q)\}]\,r \\
\text{DAI} & ([\{\exists \bar{y}.(c\,\&\,q)\}]\,p \leftrightarrow \forall \bar{y}.\,[?q]\,p) \leftarrow [\{\exists \bar{y}.(c\,\&\,q)\}]\,(p)' \\
\text{DAW} & [\{\exists \bar{y}.(c\,\&\,q)\}]\,p \leftrightarrow [\{\exists \bar{y}.(c\,\&\,q)\}]\,(q \rightarrow p) \\
\text{DAE} & \left[\{\exists \bar{y}.(x' = f, c\,\&\,q)\}\right] p \leftrightarrow \forall \bar{y}.\,\left[\{\exists \bar{y}.(x' = f, c\,\&\,q)\}\right] \left[x' := f\right] p
\end{array}$$

Uniform Substitution for dA$\mathcal{L}$

$$
\begin{array}{rl}
\text{DC} & ([c\,\&\,q]p \leftrightarrow [c\,\&\,q \wedge r]p) \leftarrow [c\,\&\,q]r \\
\text{DI} & ([c\,\&\,q]p \leftrightarrow [?q]p) \leftarrow [c\,\&\,q](p)' \\
\text{DW} & [c\,\&\,q]p \leftrightarrow [c\,\&\,q](q \rightarrow p) \\
\text{DE} & [x' = f, c\,\&\,q]p \leftrightarrow [x' = f, c\,\&\,q][x' := f]p
\end{array}
$$

$$
\begin{array}{rl}
\text{DAC} & ([\{\exists \bar{y}.(c\,\&\,q)\}]\,p \leftrightarrow [\{\exists \bar{y}.(c\,\&\,q \wedge r)\}]\,p) \leftarrow [\{\exists \bar{y}.(c\,\&\,q)\}]\,r \\
\text{DAI} & ([\{\exists \bar{y}.(c\,\&\,q)\}]\,p \leftrightarrow \forall \bar{y}.\,[?q]\,p) \leftarrow [\{\exists \bar{y}.(c\,\&\,q)\}]\,(p)' \\
\text{DAW} & [\{\exists \bar{y}.(c\,\&\,q)\}]\,p \leftrightarrow [\{\exists \bar{y}.(c\,\&\,q)\}]\,(q \rightarrow p) \\
\text{DAE} & \left[\{\exists \bar{y}.(x' = f, c\,\&\,q)\}\right]p \leftrightarrow \forall \bar{y}.\,\left[\{\exists \bar{y}.(x' = f, c\,\&\,q)\}\right]\left[x' := f\right]p
\end{array}
$$

Uniform Substitution for dA$\mathcal{L}$

$$
\begin{array}{rl}
\text{DC} & ([c \,\&\, q]p \leftrightarrow [c \,\&\, q \wedge r]p) \leftarrow [c \,\&\, q]r \\
\text{DI} & ([c \,\&\, q]p \leftrightarrow [?q]p) \leftarrow [c \,\&\, q](p)' \\
\text{DW} & [c \,\&\, q]p \leftrightarrow [c \,\&\, q](q \rightarrow p) \\
\text{DE} & [x' = f, c \,\&\, q]p \leftrightarrow [x' = f, c \,\&\, q][x' := f]p
\end{array}
$$

$$
\begin{array}{rl}
\text{DAC} & ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q \wedge r)\}]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, r \\
\text{DAI} & ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [?q]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (p)' \\
\text{DAW} & [\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (q \rightarrow p) \\
\text{DAE} & \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] p \leftrightarrow \forall \bar{y}.\, \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] \left[x' := f\right] p
\end{array}
$$

Uniform Substitution for dA$\mathcal{L}$

$$
\begin{array}{rl}
\text{DAC} & ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q \wedge r)\}]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, r \\
\text{DAI} & ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [?q]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (p)' \\
\text{DAW} & [\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (q \rightarrow p) \\
\text{DAE} & \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] p \leftrightarrow \forall \bar{y}.\, \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] \left[x' := f\right] p
\end{array}
$$

Uniform Substitution for dA$\mathcal{L}$

$$\begin{aligned}
&\text{DAC} && ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q \land r)\}]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, r \\
&\text{DAI} && ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [?q]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (p)' \\
&\text{DAW} && [\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (q \rightarrow p) \\
&\text{DAE} && \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] p \leftrightarrow \forall \bar{y}.\, \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] \left[x' := f\right] p
\end{aligned}$$

Uniform Substitution for dA$\mathcal{L}$

$$
\begin{aligned}
&\text{DAC} && ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q \wedge r)\}]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, r \\
&\text{DAI} && ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [?q]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (p)' \\
&\text{DAW} && [\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (q \rightarrow p) \\
&\text{DAE} && \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] p \leftrightarrow \forall \bar{y}.\, \left[\{\exists \bar{y}.(x' = f, c \,\&\, q)\}\right] \left[x' := f\right] p
\end{aligned}
$$

DAE too weak for technical reasons, DAW actually unnecessary!

Uniform Substitution for dA$\mathcal{L}$

$$\text{DAC} \quad ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q \land r)\}]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, r$$

$$\text{DAI} \quad ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [?q]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (p)'$$

$$\text{DAS} \quad [\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [\{\exists \bar{y}.(c \,\&\, q)\}]\, [\{c \,\&\, q\}]\, p$$

What we actually need is a 'differential algebraic stutter' axiom (DAS)!

Uniform Substitution for dA$\mathcal{L}$

$$
\begin{array}{rl}
\text{DAC} & ([\{\exists\bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists\bar{y}.(c \,\&\, q \wedge r)\}]\, p) \leftarrow [\{\exists\bar{y}.(c \,\&\, q)\}]\, r \\
\text{DAI} & ([\{\exists\bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall\bar{y}.\, [?q]\, p) \leftarrow [\{\exists\bar{y}.(c \,\&\, q)\}]\, (p)' \\
\text{DAS} & [\{\exists\bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall\bar{y}.\, [\{\exists\bar{y}.(c \,\&\, q)\}]\, [\{c \,\&\, q\}]\, p
\end{array}
$$

Theorem (Soundness of Uniform Substitution Calculus for dA$\mathcal{L}$)

The above substitution axioms for dA$\mathcal{L}$ are sound.

Uniform Substitution for dA$\mathcal{L}$

$$\text{DAC}\quad ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow [\{\exists \bar{y}.(c \,\&\, q \wedge r)\}]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, r$$
$$\text{DAI}\quad ([\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [?q]\, p) \leftarrow [\{\exists \bar{y}.(c \,\&\, q)\}]\, (p)'$$
$$\text{DAS}\quad [\{\exists \bar{y}.(c \,\&\, q)\}]\, p \leftrightarrow \forall \bar{y}.\, [\{\exists \bar{y}.(c \,\&\, q)\}]\, [\{c \,\&\, q\}]\, p$$

Theorem (Soundness of Uniform Substitution Calculus for dA$\mathcal{L}$)

The above substitution axioms for dA$\mathcal{L}$ are sound.

We have created a sound and 'minimal' uniform substitution calculus for dA$\mathcal{L}$ that we can implement into KeYmaeraX!

Implementation Details

- Modified the parser and core data structures in KeYmaeraX to support dA$\mathcal{L}$
- We support singly-quantified differential systems (due to lack of vectorial support and significant compatibility changes required)
- Modified to unification, uniform substitution and other necessary algorithms supported by KeYmaeraX
- Uniform Substitution axioms added to trusted axiom base
- Derived axioms and derived tactics proven from trusted axioms
- Tested proving examples using derived axioms and tactics

Implementation Details

- Modified the parser and core data structures in KeYmaeraX to support dA$\mathcal{L}$
- We support singly-quantified differential systems (due to lack of vectorial support and significant compatibility changes required)
- Modified to unification, uniform substitution and other necessary algorithms supported by KeYmaeraX
- Uniform Substitution axioms added to trusted axiom base
- Derived axioms and derived tactics proven from trusted axioms
- Tested proving examples using derived axioms and tactics

A successful extension that minimally extends the trusted core!

Derived Tactics

$$\frac{Q(x,\bar{y}) \vdash P(x)}{\Gamma \vdash \left[\{\exists \bar{y}.(x' = f(x,\bar{y}) \,\&\, Q(x,\bar{y}))\}\right] P(x), \Delta}\,\mathtt{dAW}$$

$$\frac{Q(x,\bar{y}) \vdash \left[x' := f(x,\bar{y})\right] (P(x))'}{P(x) \vdash \left[\{\exists \bar{y}.(x' = f(x,\bar{y}) \,\&\, Q(x,\bar{y}))\}\right] P(x)}\,\mathtt{dAI}$$

$$\frac{\Gamma \vdash [\{\exists \bar{y}.(c \,\&\, Q \wedge R)\}]\, P, \Delta \qquad \Gamma \vdash [\{\exists \bar{y}.(c \,\&\, Q)\}]\, R, \Delta}{\Gamma \vdash [\{\exists \bar{y}.(c \,\&\, Q)\}]\, P, \Delta}\,\mathtt{dAC}$$

Example (Perturbed Circular Motion)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{*}{x \cdot e \leq 0 \vdash 2x(-y+e) + 2yx \leq 0}\ \mathbb{R}}{x \cdot e \leq 0 \vdash \left[x' := -y + e\right] \left[y' := x\right] 2xx' + 2yy' \leq 0}\ [':=]}{x \cdot e \leq 0 \vdash \left[x' := -y + e; y' := x\right] (x^2 + y^2 \leq 1)'}\ ['],[;]}{x^2 + y^2 = 1 \vdash \left[\{\exists e.(x' = -y + e, y' = x \,\&\, x \cdot e \leq 0)\}\right] x^2 + y^2 \leq 1}\ \mathtt{dAI}}{\vdash x^2 + y^2 = 1 \rightarrow \left[\{\exists e.(x' = -y + e, y' = x \,\&\, x \cdot e \leq 0)\}\right] x^2 + y^2 \leq 1}\ {\rightarrow}\mathrm{R}$$

$$\dfrac{Q(x,\bar{y}) \vdash \left[x' := f(x,\bar{y})\right] (P(x))'}{P(x) \vdash \left[\{\exists \bar{y}.(x' = f(x,\bar{y}) \,\&\, Q(x,\bar{y}))\}\right] P(x)}\ \mathtt{dAI}$$

Conclusion and Future Work

- Constructed a uniform substitution calculus for d$A\mathcal{L}$
- Implemented it in KeYmaeraX for a single existentially quantified variable
- Constructed derived axioms and rules for actual use
- Future extensions:
  - Support for multiple quantifiers
  - WebUI support
  - 'Desugared' syntax
  - Support for more derived rules
  - Support for hybrid games with differential-algebraic components

Conclusion and Future Work

- Constructed a uniform substitution calculus for dA$\mathcal{L}$
- Implemented it in KeYmaeraX for a single existentially quantified variable
- Constructed derived axioms and rules for actual use
- Future extensions:
  - Support for multiple quantifiers
  - WebUI support
  - 'Desugared' syntax
  - Support for more derived rules
  - Support for hybrid games with differential-algebraic components

Conclusion and Future Work

- Constructed a uniform substitution calculus for d$A\mathcal{L}$
- Implemented it in KeYmaeraX for a single existentially quantified variable
- Constructed derived axioms and rules for actual use
- Future extensions:
  - Support for multiple quantifiers
  - WebUI support
  - 'Desugared' syntax
  - Support for more derived rules
  - Support for hybrid games with differential-algebraic components

Conclusion and Future Work

- Constructed a uniform substitution calculus for d$\mathcal{AL}$
- Implemented it in KeYmaeraX for a single existentially quantified variable
- Constructed derived axioms and rules for actual use
- Future extensions:
  - Support for multiple quantifiers
  - WebUI support
  - 'Desugared' syntax
  - Support for more derived rules
  - Support for hybrid games with differential-algebraic components

Conclusion and Future Work

- Constructed a uniform substitution calculus for dA$\mathcal{L}$
- Implemented it in KeYmaeraX for a single existentially quantified variable
- Constructed derived axioms and rules for actual use
- Future extensions:
  - Support for multiple quantifiers
  - WebUI support
  - 'Desugared' syntax
  - Support for more derived rules
  - Support for hybrid games with differential-algebraic components

Questions?