Relational Differential Dynamic Logic

Methods and Tools for Distributed Hybrid Systems
Amsterdam, 26/08/19

Jérémy Dubut
National Institute of Informatics
Japanese-French Laboratory of Informatics

Collaborations

Joint work with:

- from Tokyo: Ichiro Hasuo, Akihisa Yamada, David Sprunger, and Shin-ya Katsumata
- from France: Juraj Kolčák

Initiated by discussions with Kenji Kamijo, Yoshiyuki Shinya, and Takamasa Suetomi from Mazda Motor Corporation

Sources:

- J. Kolčák, I. Hasuo, J. Dubut, S. Katsumata, D. Sprunger, A. Yamada, Relational Differential Dynamic Logic. Preprint arXiv:1903.00153.
- some implementation on GitHub

Basic example: simplified ISO26262

$\dot{v} = 0$

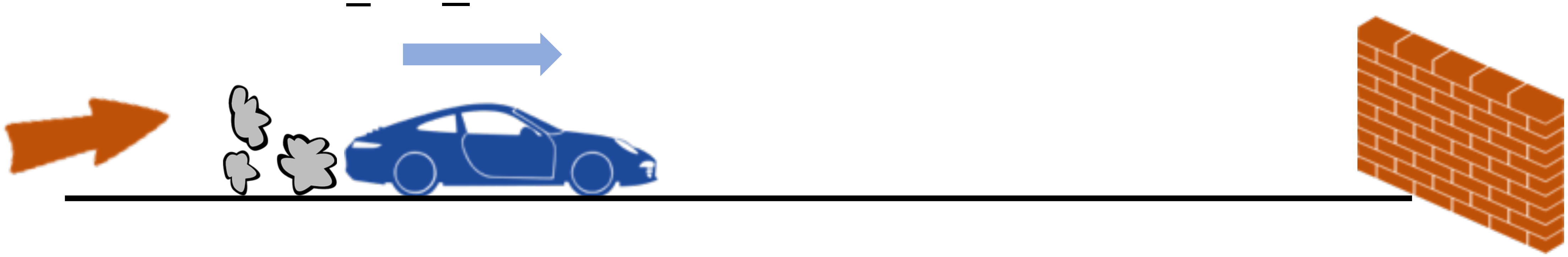
$\dot{v} = a > 0$

In which cases will the vehicle crash hard?

Monotonicity property?

$$\dot{\overline{v}} = \overline{a} > 0$$

$$\underline{\dot{v}} = \underline{a} > 0$$



When $\overline{a} < \underline{a}$ which vehicle crash harder?

Elementary proof

Consider the following easy dynamics:

$$\dot{\underline{x}} = \underline{v}$$
$$\dot{\underline{v}} = \underline{a}$$

$$\dot{\overline{x}} = \overline{v}$$
$$\dot{\overline{v}} = \overline{a}$$

Elementary proof

Consider the following easy dynamics:

$$\dot{\underline{x}} = \underline{v}$$
$$\dot{\underline{v}} = \underline{a}$$

$$\dot{\overline{x}} = \overline{v}$$
$$\dot{\overline{v}} = \overline{a}$$

Solving the equations:

$$\underline{v} = \underline{a} \,.\, \underline{t} + \underline{v}_0$$

$$\underline{x} = \frac{\underline{a}}{2} \,.\, \underline{t}^2 + \underline{v}_0 \,.\, \underline{t}$$

$$\overline{v} = \overline{a} \,.\, \overline{t} + \overline{v}_0$$

$$\overline{x} = \frac{\overline{a}}{2} \,.\, \overline{t}^2 + \overline{v}_0 \,.\, \overline{t}$$

Elementary proof

Consider the following easy dynamics:

$$\dot{\underline{x}} = \underline{v}$$
$$\dot{\underline{v}} = \underline{a}$$

$$\dot{\overline{x}} = \overline{v}$$
$$\dot{\overline{v}} = \overline{a}$$

Solving the equations:

$$\underline{v} = \underline{a}\,.\,\underline{t} + \underline{v}_0$$

$$\underline{x} = \frac{\underline{a}}{2}\,.\,\underline{t}^2 + \underline{v}_0\,.\,\underline{t}$$

$$\overline{v} = \overline{a}\,.\,\overline{t} + \overline{v}_0$$

$$\overline{x} = \frac{\overline{a}}{2}\,.\,\overline{t}^2 + \overline{v}_0\,.\,\overline{t}$$

The time at which the vehicles reach the position x is:

$$\underline{t}(x) = \frac{\sqrt{\underline{v}_0^2 + 2\underline{a}x} - \underline{v}_0}{\underline{a}}$$

$$\overline{t}(x) = \frac{\sqrt{\overline{v}_0^2 + 2\overline{a}x} - \overline{v}_0}{\overline{a}}$$

Elementary proof

Consider the following easy dynamics:

$$\dot{\underline{x}} = \underline{v}$$
$$\dot{\underline{v}} = \underline{a}$$

$$\dot{\bar{x}} = \bar{v}$$
$$\dot{\bar{v}} = \bar{a}$$

Solving the equations:

$$\underline{v} = \underline{a}\,.\,\underline{t} + \underline{v}_0 \qquad \bar{v} = \bar{a}\,.\,\bar{t} + \bar{v}_0$$

$$\underline{x} = \frac{\underline{a}}{2}\,.\,\underline{t}^2 + \underline{v}_0\,.\,\underline{t} \qquad \bar{x} = \frac{\bar{a}}{2}\,.\,\bar{t}^2 + \bar{v}_0\,.\,\bar{t}$$

The time at which the vehicles reach the position x is:

$$\underline{t}(x) = \frac{\sqrt{\underline{v}_0^2 + 2\underline{a}x} - \underline{v}_0}{\underline{a}} \qquad \bar{t}(x) = \frac{\sqrt{\bar{v}_0^2 + 2\bar{a}x} - \bar{v}_0}{\bar{a}}$$

The speed at position x is:

$$\underline{v}(x) = \sqrt{\underline{v}_0^2 + 2\underline{a}x} \qquad \bar{v}(x) = \sqrt{\bar{v}_0^2 + 2\bar{a}x}$$

Elementary proof

Consider the following easy dynamics:

$$\dot{\underline{x}} = \underline{v} \qquad \dot{\underline{v}} = \underline{a}$$

$$\dot{\overline{x}} = \overline{v} \qquad \dot{\overline{v}} = \overline{a}$$

Solving the equations:

$$\underline{v} = \underline{a}\,.\,\underline{t} + \underline{v}_0 \qquad \overline{v} = \overline{a}\,.\,\overline{t} + \overline{v}_0$$

$$\underline{x} = \frac{\underline{a}}{2}\,.\,\underline{t}^2 + \underline{v}_0\,.\,\underline{t} \qquad \overline{x} = \frac{\overline{a}}{2}\,.\,\overline{t}^2 + \overline{v}_0\,.\,\overline{t}$$

The time at which the vehicles reach the position x is:

$$\underline{t}(x) = \frac{\sqrt{\underline{v}_0^2 + 2\underline{a}x} - \underline{v}_0}{\underline{a}} \qquad \overline{t}(x) = \frac{\sqrt{\overline{v}_0^2 + 2\overline{a}x} - \overline{v}_0}{\overline{a}}$$

The speed at position x is:

$$\underline{v}(x) = \sqrt{\underline{v}_0^2 + 2\underline{a}x} \qquad \overline{v}(x) = \sqrt{\overline{v}_0^2 + 2\overline{a}x}$$

If $\underline{a} \leq \overline{a}$ and $\underline{v}_0 \leq \overline{v}_0$ then $\underline{v}(x) \leq \overline{v}(x)$ and the blue car crashes harder!

Elementary proof

Consider the following easy dynamics:

$$\dot{\underline{x}} = \underline{v} \qquad \dot{\underline{v}} = \underline{a}$$

$$\dot{\bar{x}} = \bar{v} \qquad \dot{\bar{v}} = \bar{a}$$

Solving the equations:

$$\underline{v} = \underline{a}\,.\,\underline{t} + \underline{v}_0 \qquad \bar{v} = \bar{a}\,.\,\bar{t} + \bar{v}_0$$

$$\underline{x} = \frac{\underline{a}}{2}\,.\,\underline{t}^2 + \underline{v}_0\,.\,\underline{t} \qquad \bar{x} = \frac{\bar{a}}{2}\,.\,\bar{t}^2 + \bar{v}_0\,.\,\bar{t}$$

The time at which the vehicles reach the position x is:

$$\underline{t}(x) = \frac{\sqrt{\underline{v}_0^2 + 2\underline{a}x} - \underline{v}_0}{\underline{a}} \qquad \bar{t}(x) = \frac{\sqrt{\bar{v}_0^2 + 2\bar{a}x} - \bar{v}_0}{\bar{a}}$$

The speed at position x is:

$$\underline{v}(x) = \sqrt{\underline{v}_0^2 + 2\underline{a}x} \qquad \bar{v}(x) = \sqrt{\bar{v}_0^2 + 2\bar{a}x}$$

If $\underline{a} \leq \bar{a}$ and $\underline{v}_0 \leq \bar{v}_0$ then $\underline{v}(x) \leq \bar{v}(x)$ and the blue car crashes harder!

Differential dynamic logic in a nutshell

- A Hoare-triples-style syntax to formalise properties of hybrid system
- A sequent calculus to implement proofs of those properties
- A tool: KeYmaeraX

Ref: A. Platzer's group http://symbolaris.com

$$\Gamma \vdash [\alpha]\, P$$

Γ, P: sets of first order formulae of real arithmetic

α: hybrid program

$$\alpha ::= ?P \mid \alpha;\alpha \mid \dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})\ \&\ Q \mid \alpha^\star \mid x := e \mid \ldots$$

Invariants

$$\frac{\Gamma \vdash \textsf{\textbf{Inv}} \quad \textsf{\textbf{Inv}} \vdash [\alpha]\,\textsf{\textbf{Inv}} \quad \textsf{\textbf{Inv}} \vdash P}{\Gamma \vdash [\alpha]\,P}(\textsf{\textbf{Inv}})$$

Invariants

$$\frac{\Gamma \vdash \textbf{Inv} \qquad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \qquad \textbf{Inv} \vdash P}{\Gamma \vdash [\alpha]\,P}(\textbf{Inv})$$

To prove the statement $\Gamma \vdash [\alpha]\,P$

Invariants

It is enough to find an invariant such that:

$$\frac{\Gamma \vdash \textbf{Inv} \qquad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \qquad \textbf{Inv} \vdash P}{\Gamma \vdash [\alpha]\,P}(\textbf{Inv})$$

To prove the statement $\Gamma \vdash [\alpha]\,P$

Invariants

It is enough to find an invariant such that:

- holds initially

$$\frac{\boxed{\Gamma \vdash \textbf{Inv}} \quad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \quad \textbf{Inv} \vdash P}{\Gamma \vdash [\alpha]\,P}(\textbf{Inv})$$

To prove the statement $\Gamma \vdash [\alpha]\,P$

Invariants

It is enough to find an invariant which:

- **holds initially**
- **implies the post-condition**

$$\frac{\boxed{\Gamma \vdash \textbf{Inv}} \quad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \quad \boxed{\textbf{Inv} \vdash P}}{\Gamma \vdash [\alpha]\,P}(\textbf{Inv})$$

To prove the statement $\Gamma \vdash [\alpha]\,P$

Invariants

It is enough to find an invariant which:

- **holds initially**
- **implies the post-condition**
- **is an invariant**

$$\frac{\Gamma \vdash \textbf{Inv} \qquad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \qquad \textbf{Inv} \vdash P}{\Gamma \vdash [\alpha]\,P}\,(\textbf{Inv})$$

To prove the statement $\Gamma \vdash [\alpha]\,P$

Loop invariants

$$\frac{\Gamma \vdash \textbf{Inv} \qquad \textbf{Inv} \vdash [\alpha]\,\textbf{Inv} \qquad \textbf{Inv} \vdash P}{\Gamma \vdash [\alpha^\star]\,P}\,(\textbf{LI})$$

Differential invariants?

$$\dot{\mathbf{x}} = \mathbf{e} \ \& \ Q \quad \simeq \quad \left(?Q; \mathbf{x} := \mathbf{x} + dt \,.\, \mathbf{e}\right)^{\star}; ?Q$$

$$\frac{\Gamma, Q \vdash \mathbf{Inv} \qquad \mathbf{Inv}, Q \vdash \mathbf{Inv}(\mathbf{x} \leftarrow \mathbf{x} + dt \,.\, \mathbf{e}) \qquad \mathbf{Inv} \vdash P}{\Gamma \vdash [\dot{\mathbf{x}} = \mathbf{e} \ \& \ Q]P} \ \textbf{(dtI)}$$

Assume that $P = \mathbf{Inv} \equiv f = 0$. We want something to ensure:

$$f(\omega) = 0 \Rightarrow f(\omega + dt \,.\, \mathbf{e}(\omega)) = 0$$

It is enough to require that f is constant along the dynamics, that is, if ψ is a solution of $\dot{\mathbf{x}} = \mathbf{e}$, then $K : t \mapsto f(\psi(t))$ is constant, that is, its derivative is zero.

$$\dot{K}(t) = \sum_{x \in \mathbf{X}} \frac{\partial f}{\partial x}(\psi(t)) \,.\, \dot{\psi}(t) = \sum_{x \in \mathbf{X}} \frac{\partial f}{\partial x}(\psi(t)) \,.\, \mathbf{e}_x(\psi(t))$$

So it is enough that the function $\mathscr{L}_{\mathbf{e}} f = \sum_{x \in \mathbf{X}} \frac{\partial f}{\partial x} \,.\, \mathbf{e}_x$ to be zero along the dynamics.

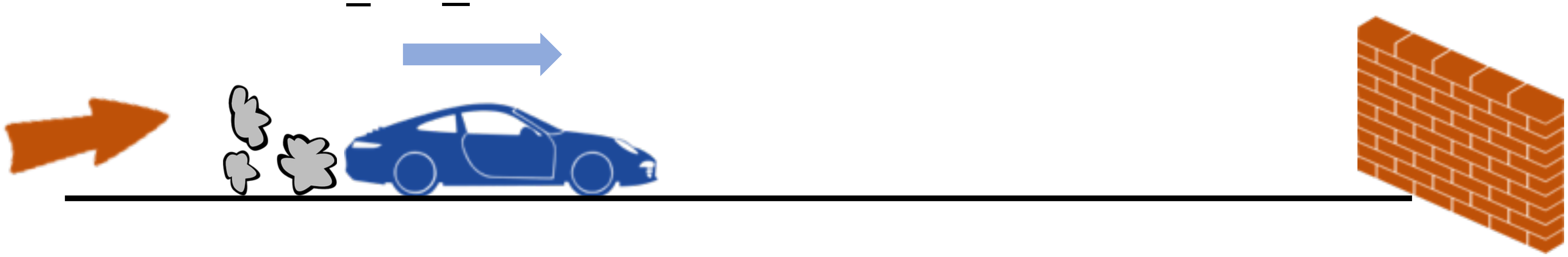
Differential invariants

$$\frac{\Gamma, Q \vdash f = 0 \quad \Gamma \vdash [\dot{\mathbf{x}} = \mathbf{e} \,\&\, Q]\, \mathscr{L}_{\mathbf{e}} f = 0}{\Gamma \vdash [\dot{\mathbf{x}} = \mathbf{e} \,\&\, Q]\, f = 0}(\mathbf{DI})$$

Monotonicity property?

$$\dot{\bar{v}} = \bar{a} > 0$$

$$\dot{\underline{v}} = \underline{a} > 0$$



When $\bar{a} < \underline{a}$ which vehicle crash harder?

Relational formulae

$$[\{\dot{\underline{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}})\ \&\ \underline{Q}\};\{\dot{\overline{\mathbf{x}}} = \overline{f}(\overline{\mathbf{x}})\ \&\ \overline{Q}\};?\underline{g}(\underline{\mathbf{x}}) = \overline{g}(\overline{\mathbf{x}})]\,B$$

Relational formulae

$$[\{\dot{\underline{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}}) \;\&\; \underline{Q}\}; \{\dot{\overline{\mathbf{x}}} = \overline{f}(\overline{\mathbf{x}}) \;\&\; \overline{Q}\}; ?\underline{g}(\underline{\mathbf{x}}) = \overline{g}(\overline{\mathbf{x}})]\, B$$

System 1

Relational formulae

$$[\{\underline{\dot{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}}) \;\&\; \underline{Q}\};\, \{\dot{\bar{\mathbf{x}}} = \bar{f}(\bar{\mathbf{x}}) \;\&\; \overline{Q}\};\, ?\underline{g}(\underline{\mathbf{x}}) = \overline{g}(\bar{\mathbf{x}})]\, B$$

System 1

$$\underline{\dot{x}} = \underline{v}$$
$$\underline{\dot{v}} = \underline{a}$$

Relational formulae

$$[\{\dot{\underline{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}}) \,\&\, \underline{Q}\}; \{\dot{\overline{\mathbf{x}}} = \overline{f}(\overline{\mathbf{x}}) \,\&\, \overline{Q}\}; ?\underline{g}(\underline{\mathbf{x}}) = \overline{g}(\overline{\mathbf{x}})]\, B$$

System 1

System 2

$$\dot{\underline{x}} = \underline{v}$$
$$\dot{\underline{v}} = \underline{a}$$

Relational formulae

$$[\{\underline{\dot{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}}) \;\&\; \underline{Q}\};\{\dot{\bar{\mathbf{x}}} = \bar{f}(\bar{\mathbf{x}}) \;\&\; \overline{Q}\};?\underline{g}(\underline{\mathbf{x}}) = \bar{g}(\bar{\mathbf{x}})]\,B$$

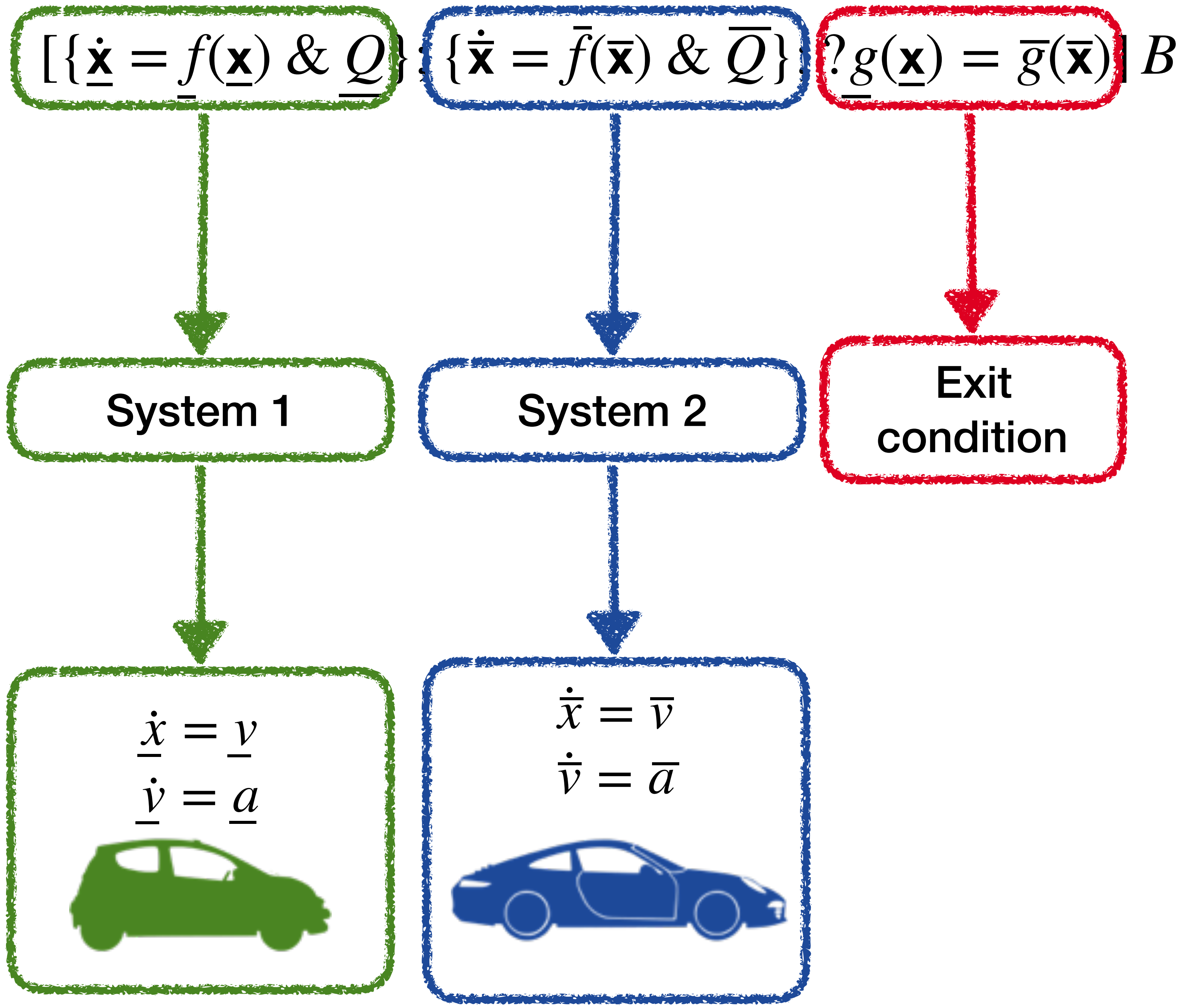
System 1

System 2

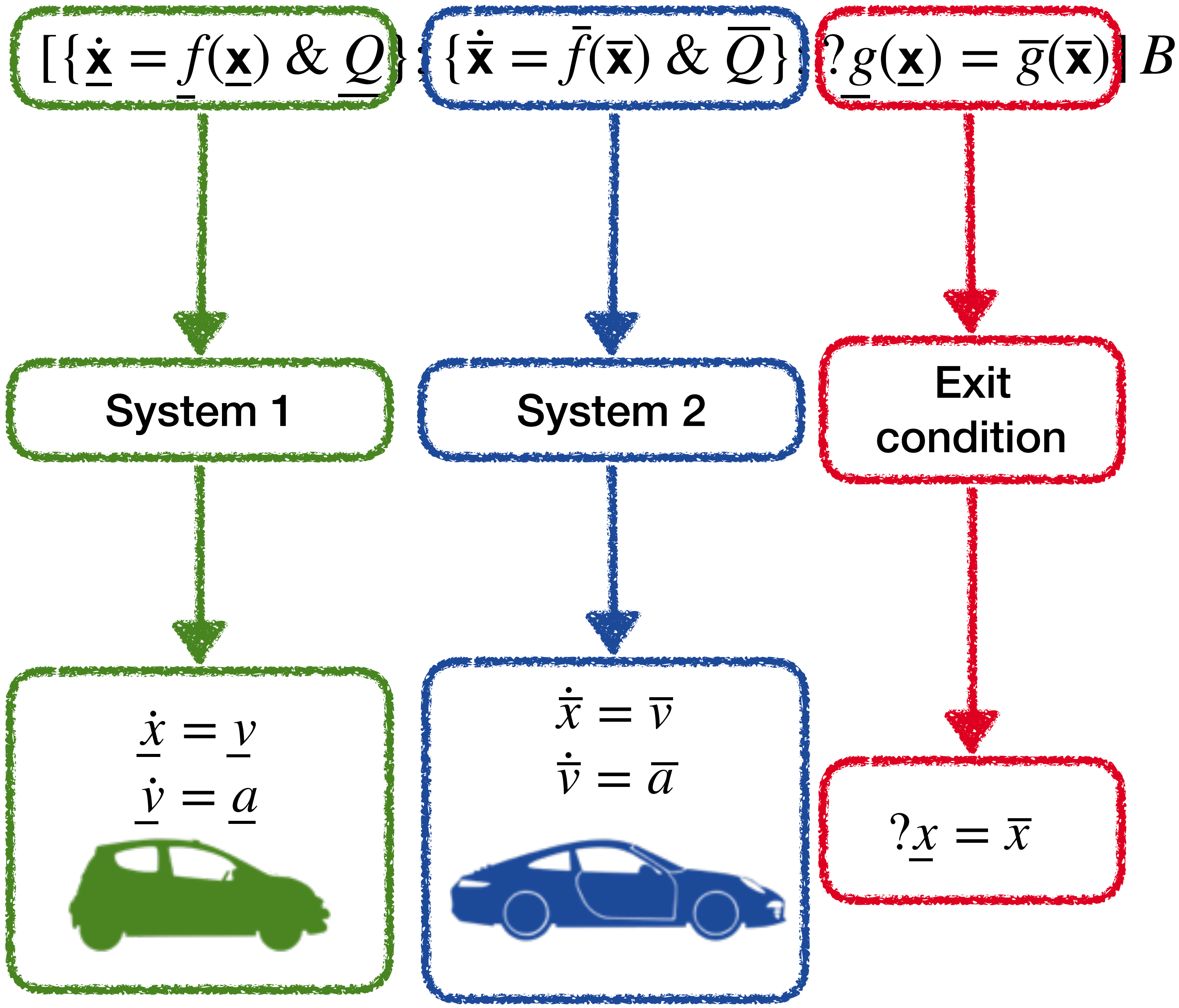
$$\underline{\dot{x}} = \underline{v}$$
$$\underline{\dot{v}} = \underline{a}$$

$$\dot{\bar{x}} = \bar{v}$$
$$\dot{\bar{v}} = \bar{a}$$

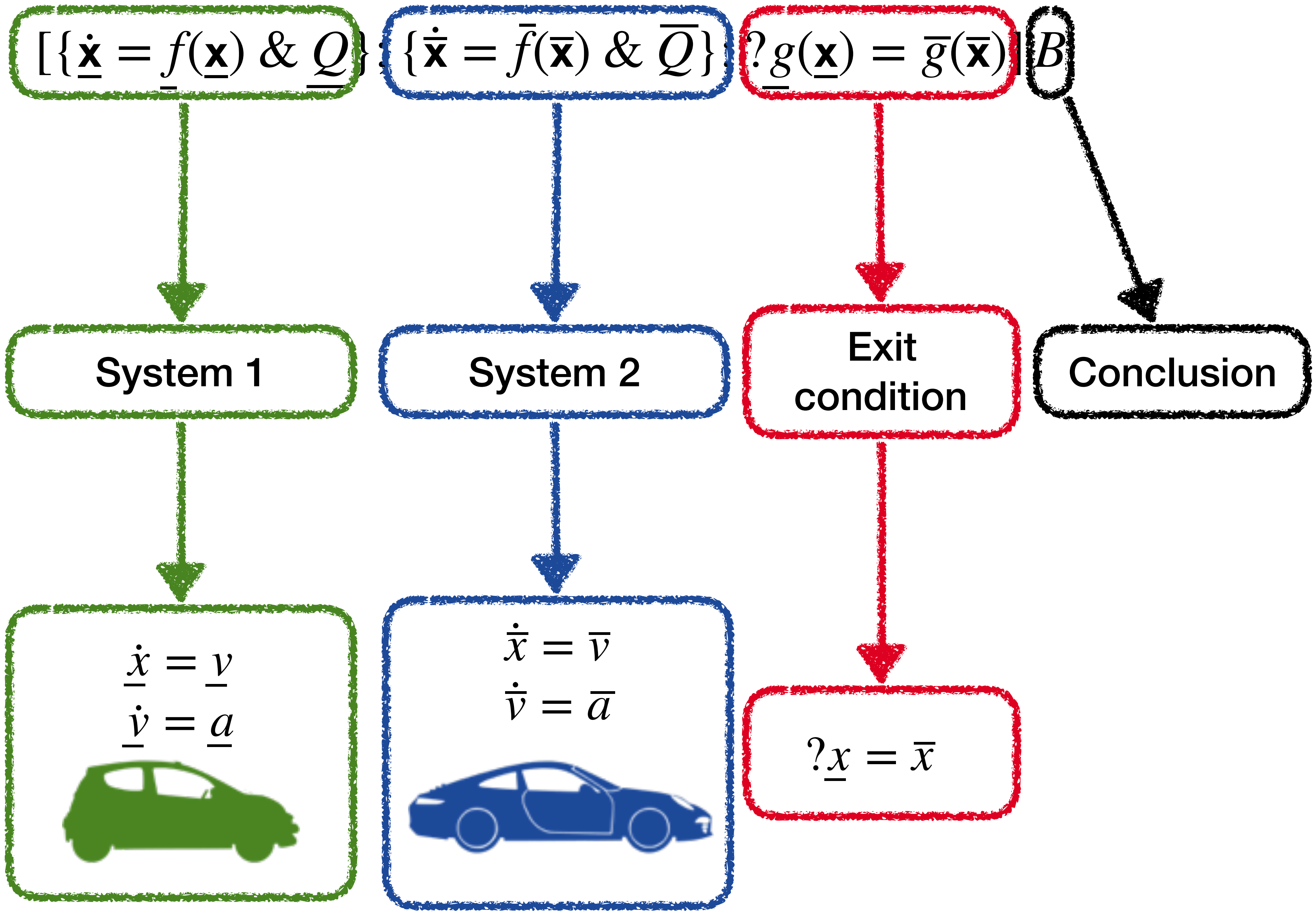
Relational formulae



Relational formulae



Relational formulae



Relational formulae

$$[\{\underline{\dot{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}})\ \&\ \underline{Q}\};\{\dot{\overline{\mathbf{x}}} = \overline{f}(\overline{\mathbf{x}})\ \&\ \overline{Q}\};?\underline{g}(\underline{\mathbf{x}}) = \overline{g}(\overline{\mathbf{x}})]B$$

System 1

$$\dot{\underline{x}} = \underline{v}$$
$$\dot{\underline{v}} = \underline{a}$$

System 2

$$\dot{\overline{x}} = \overline{v}$$
$$\dot{\overline{v}} = \overline{a}$$

Exit condition

$$?\underline{x} = \overline{x}$$

Conclusion

$$\underline{v} \leq \overline{v}$$

Relational invariant

$$\frac{\Gamma, \underline{Q}, \overline{Q} \vdash \textsf{Inv} \quad \textsf{Inv} \vdash [\underline{\delta}; \overline{\delta}; ?E]\, \textsf{Inv} \quad \textsf{Inv}, E \vdash B}{\Gamma \vdash [\underline{\delta}; \overline{\delta}; ?E]\, B}(\textsf{RI})$$

$$\underline{\delta} \equiv \dot{\underline{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}}) \;\&\; \underline{Q}$$

$$\overline{\delta} \equiv \dot{\overline{\mathbf{x}}} = \overline{f}(\overline{\mathbf{x}}) \;\&\; \overline{Q}$$

$$E \equiv \underline{g}(\underline{\mathbf{x}}) = \overline{g}(\overline{\mathbf{x}})$$

Relational invariant, for ISO26262

We know that:

$$\underline{v}(x) = \sqrt{\underline{v}_0^2 + 2\underline{a}x} \qquad \overline{v}(x) = \sqrt{\overline{v}_0^2 + 2\overline{a}x}$$

So:

$$\frac{\underline{v}(x)^2 - \underline{v}_0^2}{2\underline{a}} = x = \frac{\overline{v}(x)^2 - \overline{v}_0^2}{2\overline{a}}$$

And then:

$$R \equiv \overline{a}(\underline{v}^2 - \underline{v}_0^2) = \underline{a}(\overline{v}^2 - \overline{v}_0^2)$$

is a relational invariant.

Relational invariant, for ISO26262

We know that:

$$\underline{v}(x) = \sqrt{\underline{v}_0^2 + 2\underline{a}x} \qquad \overline{v}(x) = \sqrt{\overline{v}_0^2 + 2\overline{a}x}$$

So:

$$\frac{\underline{v}(x)^2 - \underline{v}_0^2}{2\underline{a}} = x = \frac{\overline{v}(x)^2 - \overline{v}_0^2}{2\overline{a}}$$

And then:

$$R \;\equiv\; \overline{a}(\underline{v}^2 - \underline{v}_0^2) = \underline{a}(\overline{v}^2 - \overline{v}_0^2)$$

is a relational invariant.

That is, one has to prove the following statements:

- $\underline{a} \leq \overline{a}, \underline{v} \geq \underline{v}_0, \overline{v} \geq \overline{v}_0, R \vdash \overline{v} \geq \underline{v}$
- $\underline{v} = \underline{v}_0, \overline{v} = \overline{v}_0 \vdash R$
- $R \vdash [\{\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}\}; \{\dot{\overline{x}} = \overline{v}, \dot{\overline{v}} = \overline{a}\}; ?\underline{x} = \overline{x}]\, R$

The invariant implies the property (easy proof)

Relational invariant, for ISO26262

We know that:

$$\underline{v}(x) = \sqrt{\underline{v}_0^2 + 2\underline{a}x} \qquad \overline{v}(x) = \sqrt{\overline{v}_0^2 + 2\overline{a}x}$$

So:

$$\frac{\underline{v}(x)^2 - \underline{v}_0^2}{2\underline{a}} = x = \frac{\overline{v}(x)^2 - \overline{v}_0^2}{2\overline{a}}$$

And then:

$$R \;\equiv\; \overline{a}(\underline{v}^2 - \underline{v}_0^2) = \underline{a}(\overline{v}^2 - \overline{v}_0^2)$$

is a relational invariant.

That is, one has to prove the following statements:

- $\underline{a} \leq \overline{a}, \underline{v} \geq \underline{v}_0, \overline{v} \geq \overline{v}_0, R \vdash \overline{v} \geq \underline{v}$
- $\underline{v} = \underline{v}_0, \overline{v} = \overline{v}_0 \vdash R$
- $R \vdash [\{\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}\}; \{\dot{\overline{x}} = \overline{v}, \dot{\overline{v}} = \overline{a}\}; ?\underline{x} = \overline{x}]\, R$

The invariant holds initially
(easy proof)

Relational invariant, for ISO26262

We know that:

$$\underline{v}(x) = \sqrt{\underline{v}_0^2 + 2\underline{a}x} \qquad \overline{v}(x) = \sqrt{\overline{v}_0^2 + 2\overline{a}x}$$

So:

$$\frac{\underline{v}(x)^2 - \underline{v}_0^2}{2\underline{a}} = x = \frac{\overline{v}(x)^2 - \overline{v}_0^2}{2\overline{a}}$$

And then:

$$R \equiv \overline{a}(\underline{v}^2 - \underline{v}_0^2) = \underline{a}(\overline{v}^2 - \overline{v}_0^2)$$

is a relational invariant.

That is, one has to prove the following statements:

- $\underline{a} \leq \overline{a}, \underline{v} \geq \underline{v}_0, \overline{v} \geq \overline{v}_0, R \vdash \overline{v} \geq \underline{v}$
- $\underline{v} = \underline{v}_0, \overline{v} = \overline{v}_0 \vdash R$
- $R \vdash [\{\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}\}; \{\dot{\overline{x}} = \overline{v}, \dot{\overline{v}} = \overline{a}\}; ?\underline{x} = \overline{x}]\, R$

The invariant is preserved by the dynamics (easy proof?)

Problems to tackle

We want a method that:

- does not require the solutions of the differential equations in any way
- transforms the two dynamics into one unique, so that we can use known methods from differential invariants.

Two systems into one?

What we have now:

- one system on $\underline{x}, \underline{v}$
- one system on $\overline{x}, \overline{v}$

that take different times to arrive at a particular position.

What we want:

- one system on $\underline{x}, \underline{v}, \overline{x}, \overline{v}$

such that the positions are synchronized, that is, at all time t:

$$\underline{x}(t) = \overline{x}(t)$$

Reparametrisation of dynamics

Crucial idea: reparametrise the time of $\bar{x}, \bar{v}$

Time stretch function: derivable function $k : \mathbb{R} \longrightarrow \mathbb{R}$ with

$$\dot{k} > 0$$

Reparamatrised dynamics: let $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ be a differential equation.
It reparametrisation by k is $\dot{\mathbf{x}} = \dot{k}(t) \,.\, \mathbf{f}(\mathbf{x})$.

x is a solution of $\dot{\mathrm{x}} = \mathrm{f}(\mathrm{x})$ iff
$\mathrm{x} \circ k$ is a solution of $\dot{\mathrm{x}} = \dot{k}(t) \,.\, \mathrm{f}(\mathrm{x})$.

Is it OK?

Fix some initial condition x_0. Then
$\{x(t) \mid x \text{ sol. of } \dot{x} = f(x) \text{ at } x_0\} = \{x(t) \mid x \text{ sol. of } \dot{x} = \dot{k}(t) \,.\, f(x) \text{ at } x_0\}$.

Why is it OK then?

→ we do not care about « at time t, the vehicle is at position x with speed v »

→ we care about « at position x, the vehicle has speed v »

Which reparametrisation to choose?

Fix $\underline{v}_0, \overline{v}_0$ and note $(\underline{\psi}_x, \underline{\psi}_v)$ the solution of $\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}$ at $\underline{x} = 0, \underline{v} = \underline{v}_0$, $(\overline{\psi}_x, \overline{\psi}_v)$ the solution of $\dot{\overline{x}} = \overline{v}, \dot{\overline{v}} = \overline{a}$ at $\overline{x} = 0, \overline{v} = \overline{v}_0$.

We have a time stretch function $k : \mathbb{R} \longrightarrow \mathbb{R}$ such that for every x

$$k(\underline{t}(x)) = \overline{t}(x)$$

given by:

$$k(t) = \frac{\sqrt{at^2 + 2\underline{v}_0\overline{a}t + \overline{v}_0^2} - \overline{v}_0}{\overline{a}}$$

Which reparametrisation to choose?

Fix $\underline{v}_0, \overline{v}_0$ and note $(\underline{\psi}_x, \underline{\psi}_v)$ the solution of $\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}$ at $\underline{x} = 0, \underline{v} = \underline{v}_0$, $(\overline{\psi}_x, \overline{\psi}_v)$ the solution of $\dot{\overline{x}} = \overline{v}, \dot{\overline{v}} = \overline{a}$ at $\overline{x} = 0, \overline{v} = \overline{v}_0$.

We have a time stretch function $k : \mathbb{R} \longrightarrow \mathbb{R}$ such that for every x

$$k(\underline{t}(x)) = \overline{t}(x)$$

So we want to look at:

$$\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}, \dot{\overline{x}} = \dot{k}(t)\,.\,\overline{v}, \dot{\overline{v}} = \dot{k}(t)\,.\,\overline{a}$$

But we have:

$$\overline{\psi}_x(k(t)) = \underline{\psi}_x(t)$$

Then:

$$\dot{k}(t)\,.\,\overline{\psi}_v(k(t)) = \underline{\psi}_v(t)$$

So we want to look at:

$$\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}, \dot{\overline{x}} = \frac{\underline{v}}{\overline{v}}\,.\,\overline{v}, \dot{\overline{v}} = \frac{\underline{v}}{\overline{v}}\,.\,\overline{a}$$

How to generalize to relational formulae?

In general, from

$$\dot{\underline{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}})$$

and

$$\dot{\overline{\mathbf{x}}} = \bar{f}(\overline{\mathbf{x}})$$

under the exit condition

$$\underline{g}(\underline{\mathbf{x}}) = \overline{g}(\overline{\mathbf{x}})$$

we consider:

$$\dot{\underline{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}}), \dot{\overline{\mathbf{x}}} = \frac{\mathcal{L}_{\underline{f}}\ \underline{g}}{\mathcal{L}_{\bar{f}}\ \overline{g}} . \bar{f}(\overline{\mathbf{x}})$$

Synchronisation rule

$$\frac{\Gamma, \underline{Q}, \overline{Q} \vdash E \quad \Gamma \vdash [\underline{\delta}]\, \mathscr{L}_{\underline{f}}\, \underline{g} > 0 \quad \Gamma \vdash [\overline{\delta}]\, \mathscr{L}_{\bar{f}}\, \overline{g} > 0 \quad \Gamma \vdash [\delta]\, B}{\Gamma \vdash [\underline{\delta}; \overline{\delta}; ?E]\, B}(\textbf{Syn})$$

$$\underline{\delta} \equiv \underline{\dot{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}})\ \&\ \underline{Q}$$

$$\overline{\delta} \equiv \dot{\overline{\mathbf{x}}} = \bar{f}(\overline{\mathbf{x}})\ \&\ \overline{Q}$$

$$E \equiv \underline{g}(\underline{\mathbf{x}}) = \overline{g}(\overline{\mathbf{x}})$$

$$\overline{\delta} \equiv \underline{\dot{\mathbf{x}}} = \underline{f}(\underline{\mathbf{x}}), \dot{\overline{\mathbf{x}}} = \frac{\mathscr{L}_{\underline{f}}\, \underline{g}}{\mathscr{L}_{\bar{f}}\, \overline{g}} . \bar{f}(\overline{\mathbf{x}})\ \&\ \underline{Q} \wedge \overline{Q}$$

Relational invariant, for ISO26262

We know that:

$$\underline{v}(x) = \sqrt{\underline{v}_0^2 + 2\underline{a}x} \qquad \overline{v}(x) = \sqrt{\overline{v}_0^2 + 2\overline{a}x}$$

So:

$$\frac{\underline{v}(x)^2 - \underline{v}_0^2}{2\underline{a}} = x = \frac{\overline{v}(x)^2 - \overline{v}_0^2}{2\overline{a}}$$

And then:

$$R \equiv \overline{a}(\underline{v}^2 - \underline{v}_0^2) = \underline{a}(\overline{v}^2 - \overline{v}_0^2)$$

is a relational invariant.

That is, one has to prove the following statements:

- $\underline{a} \leq \overline{a}, \underline{v} \geq \underline{v}_0, \overline{v} \geq \overline{v}_0, R \vdash \overline{v} \geq \underline{v}$
- $\underline{v} = \underline{v}_0, \overline{v} = \overline{v}_0 \vdash R$
- $R \vdash [\{\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}\}; \{\dot{\overline{x}} = \overline{v}, \dot{\overline{v}} = \overline{a}\}; ?\underline{x} = \overline{x}]\, R$

The invariant is preserved by the dynamics (easy proof?)

Relational invariant, for ISO26262

Let's prove the following statement with the (**Syn**) rule:

$$R \vdash [\{\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}\}; \{\dot{\overline{x}} = \overline{v}, \dot{\overline{v}} = \overline{a}\}; ?\underline{x} = \overline{x}]\, R$$

with $R \equiv \overline{a}(\underline{v}^2 - \underline{v}_0^2) = \underline{a}(\overline{v}^2 - \overline{v}_0^2)$, that is:

- $\underline{v} > 0, \underline{a} \geq 0 \vdash [\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}]\, \underline{v} > 0$ (easy with differential invariant)
- $\overline{v} > 0, \overline{a} \geq 0 \vdash [\dot{\overline{x}} = \overline{v}, \dot{\overline{v}} = \overline{a}]\, \overline{v} > 0$ (easy with differential invariant)
- $R \vdash [\{\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}, \dot{\overline{x}} = \frac{\underline{v}}{\overline{v}} . \overline{v}, \dot{\overline{v}} = \frac{\underline{v}}{\overline{v}} . \overline{a}\}]\, R$

using differential invariant rule:

$$R \vdash [\{\dot{\underline{x}} = \underline{v}, \dot{\underline{v}} = \underline{a}, \dot{\overline{x}} = \frac{\underline{v}}{\overline{v}} . \overline{v}, \dot{\overline{v}} = \frac{\underline{v}}{\overline{v}} . \overline{a}\}]\, 2\overline{a}\underline{v}\underline{a} = 2\underline{a}\overline{v}\frac{\underline{v}}{\overline{v}}\overline{a}$$

Summary

Guideline:

- start with two independent systems and compare them under some conditions
- synchronize them by reparametrising one of them using the (**Syn**) rule
- use usual invariant techniques from dL

Case studies:

- monotonicity properties
- abstraction