Relational Differential Dynamic Logic

Juraj Kolčák[1,2], Ichiro Hasuo[1,3], Jérémy Dubut[1,4], Shin-ya Katsumata[1], David Sprunger[1], Akihisa Yamada[1]

[1]National Institute of Informatics, Japan; [2]LSV, CNRS & ENS Paris-Saclay, Université Paris-Saclay, France;
[3]The Graduate University for Advanced Studies (SOKENDAI), Japan; [4]Japanese-French Laboratory for Informatics, Japan

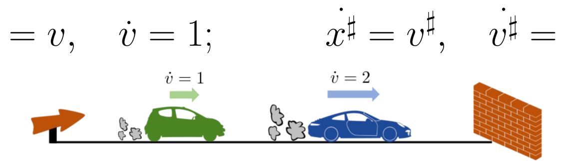
Introduction

Cyber-physical systems (CPS) are becoming exceedingly common in industry, including numerous safety-critical applications (e.g. **automated driving**), making **quality assurance** of CPS an important issue.
CPS are generally characterised by a union of continuous (physical) dynamics and discrete (digital) control, referred to as a **hybrid system**.
Verification of hybrid systems is an intriguing challenge bringing together two research communities of **control theory** and **formal methods** focused on continuous and discrete dynamics respectively.
To handle infinite state space seamlessly, we turn to deductive verification. In particular, we make use of **differential dynamic logic** dL [2], a well established and powerful tool for reasoning about continuous dynamics.

Motivating Example

Our industry collaboration revealed an interesting application summarised in the following example.
Imagine two cars with the following dynamics, where $x, x^\sharp$ and $v, v^\sharp$ denote their positions and velocities, respectively, and an equally distant obstacle.

$$\dot{x} = v, \quad \dot{v} = 1; \qquad \dot{x^\sharp} = v^\sharp, \quad \dot{v^\sharp} = 2.$$



Our aim is then to ascertain the following natural claim:

> Starting from the initial state $x_0 = x_0^\sharp = v_0 = v_0^\sharp = 0$ and following the two dynamics above, we obtain $v \leq v^\sharp$ when $x = x^\sharp = 1$.

Figure 1 displays an ad-hoc proof of the claim using closed-form solutions of the dynamics. (The hatched areas represent $x, x^\sharp$.) Instead of global properties (e.g. solutions) of the dynamics, we want to rely on **local reasoning**. Local reasoning is well established in differential dynamic logic dL, in particular via differential invariant (DI). Intuitively, one can view (DI) as a continuous version of **loop invariant**.
It turns out, however, that local **relational reasoning**, e.g. with two different dynamics, is not easy in dL.

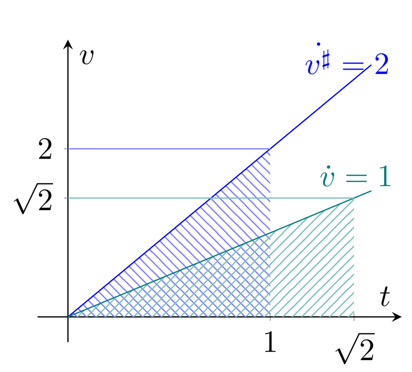


Figure 1: An ad-hoc proof.

Our Contribution

We introduce **time stretch functions** as means of reasoning about relational invariant properties. We built time stretch functions into a proof rule which allows us to **synchronise** the two dynamics on an essential property (e.g. the distance travelled). Left with single differential dynamics, we unlock the full potential of invariant reasoning in dL.
Along with the time stretch (TS) rule, we propose several other rules for relational reasoning. Although the rules appear new to us, they might be derivable in the comprehensive calculus in [1].
We showcase our proof rules in several case studies. Our methods are especially well suited for monotonicity properties (e.g. for test case reduction), or formally relating concrete models and their abstractions.

Differential Dynamic Logic

In a nutshell, dL is a modal logic with the modal operators realised as hybrid programs. Hybrid programs allow mixing discrete operators such as assignment, $x := \theta$, or test, $?\phi$, with differential dynamics:

$$[\dot{x} := f(x) \,\&\, Q(x)]$$

The modality above translates to any state reachable by $\dot{x} := f(x)$ provided $Q(x)$ holds at all times. Refer to literature [1] for full exposure to dL.

Relational Formulas

We expect the relational property to be captured by **relational differential dynamics formulas** (RDD formulas):

$$\left[\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, Q(\boldsymbol{x});\ \dot{\boldsymbol{x}^\sharp} = \boldsymbol{f}^\sharp(\boldsymbol{x}^\sharp) \,\&\, Q^\sharp(\boldsymbol{x}^\sharp);\ ?E\right] B$$

Or a shorthand with $\delta \equiv \dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \& Q(\boldsymbol{x})$ and $\delta^\sharp \equiv \dot{\boldsymbol{x}^\sharp} = \boldsymbol{f}^\sharp(\boldsymbol{x}^\sharp) \& Q^\sharp(\boldsymbol{x}^\sharp)$:

$$\left[\langle\!\langle \delta \mid \delta^\sharp \rangle\!\rangle\, E\right] B$$

where $\boldsymbol{x}$ and $\boldsymbol{x}^\sharp$ are disjoint and E, B are formulas on both $\boldsymbol{x}$ and $\boldsymbol{x}^\sharp$.
An RDD formula is interpreted as,"after any execution of $\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \& Q(\boldsymbol{x})$ and $\dot{\boldsymbol{x}^\sharp} = \boldsymbol{f}^\sharp(\boldsymbol{x}^\sharp) \,\&\, Q^\sharp(\boldsymbol{x}^\sharp)$ concurrently, e.g. allowing different amount of time for the two dynamics, and synchronisation on E, B must hold" We assume the following equality form of the test $E \equiv (g(\boldsymbol{x}) = g^\sharp(\boldsymbol{x}^\sharp))$.

Time Stretch Function

In a sense, B in RDD formulas is an relational invariant – or, liberally speaking, a (bi)simulation. An RDD formula is in fact true, if the test E, which relates elapsed times of the two dynamics, aligns with the simulation. Moreover, if g and $g^\sharp$ in E are monotonic in time, we get a unique solution:

$$\frac{dt^\sharp}{dt} = \frac{\mathcal{L}_{\boldsymbol{f}} g(\psi(\boldsymbol{x}_0, t))}{\mathcal{L}_{\boldsymbol{f}^\sharp} g^\sharp(\psi^\sharp(\boldsymbol{x}_0^\sharp, k(t)))}$$

Here $\mathcal{L}_{\boldsymbol{f}} g$ is the Lie derivate of g and $\psi(\boldsymbol{x}_0, t)$ the solution at time t.
The above relationship allows us to "stretch" the time of the second "sharp" dynamics to match the first dynamics:

$$\delta_s \equiv \left(\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}), \dot{x^\sharp} = f^\sharp(x^\sharp) \cdot \frac{dt^\sharp}{dt} \,\&\, Q(\boldsymbol{x}) \wedge Q^\sharp(\boldsymbol{x}^\sharp)\right)$$

The time stretching can be followed by any established dL rules using single dynamics. We list the dL rules used in the case studies in the table below.

Selected dL Proof Rules

$$\frac{\Gamma, Q \vdash g(\boldsymbol{x}) \sim 0 \quad \Gamma \vdash [\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, Q]\, \mathcal{L}_{\boldsymbol{f}} g(\boldsymbol{x}) \simeq 0}{\Gamma \vdash [\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, Q]\, g(\boldsymbol{x}) \sim 0}\ \text{DI [1]} \quad (\sim \in \{<, \leq, \geq, >\})$$

$$\frac{\Gamma \vdash [\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, Q]\, C \quad \Gamma \vdash [\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, (Q \wedge C)]\, \varphi}{\Gamma \vdash [\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, Q]\, \varphi}\ \text{DC [1]}$$

$$\frac{Q \vdash \varphi}{\Gamma \vdash [\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, Q]\, \varphi}\ \text{DW [1]} \qquad \frac{Q \vdash \mathcal{L}_{\boldsymbol{f}} h \geq gh}{h > 0 \vdash [\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, Q]\, h > 0}\ \text{dbx}_> \text{ [3]}\ (g \text{ is polynomial})$$

$$\frac{\Gamma \vdash [?Q \wedge Q^\sharp]\, g(\boldsymbol{x}) = g^\sharp(\boldsymbol{x}^\sharp) \quad \Gamma \vdash [\delta; \delta^\sharp]\, \frac{\mathcal{L}_{\boldsymbol{f}} g(\boldsymbol{x})}{\mathcal{L}_{\boldsymbol{f}^\sharp} g^\sharp(\boldsymbol{x}^\sharp)} > 0}{\Gamma \vdash [\langle\!\langle \delta \mid \delta^\sharp \rangle\!\rangle g(\boldsymbol{x}) = g^\sharp(\boldsymbol{x}^\sharp)]\, B \iff [\delta_A]\, B}\ \text{TS}$$

$$\frac{\Gamma, Q \vdash g(\boldsymbol{x}) \geq 0 \quad \Gamma \vdash [\delta]\, D_n g(\boldsymbol{x})}{\Gamma \vdash [\dot{\boldsymbol{x}} = \boldsymbol{f}(\boldsymbol{x}) \,\&\, Q]\, g(\boldsymbol{x}) \geq 0}\ \text{DII}_n \quad \left(\begin{array}{l} D_n g(\boldsymbol{x}) \equiv \bigvee_{p=0}^{n-1} \Big(\bigwedge_{k=1}^{p} \mathcal{L}_{\boldsymbol{f}}^{(k)} g(\boldsymbol{x}) \geq 0 \Big) \\ \wedge\, \mathcal{L}_{\boldsymbol{f}}^{(p+1)} g(\boldsymbol{x}) > 0 \end{array}\right)$$

Case Study: Cars with Constant Acceleration

For the first case study we consider a generalisation of the motivating example, where the accelerations are parameters, however, considered constant. We thus consider the following dynamics δ, $\delta^\sharp$ and initial condition Γ for the cars. We also use δ_s to denote the synchronised dynamics:

$$\delta \equiv \dot{x} = v, \dot{v} = a; \qquad \delta^\sharp \equiv \dot{x^\sharp} = v^\sharp, \dot{v^\sharp} = a^\sharp; \qquad \Gamma \equiv 0 = x = x^\sharp, 0 < v = v^\sharp, 0 < a < a^\sharp; \qquad \delta_s \equiv \dot{x} = v, \dot{v} = a, \dot{x^\sharp} = \frac{v^\sharp \cdot v}{v^\sharp}, \dot{v^\sharp} = \frac{a^\sharp \cdot v}{v^\sharp}.$$

$$\dfrac{\dfrac{\cdots}{\Gamma \vdash [\delta]\, v > 0}\,\text{DI} \qquad \dfrac{\dfrac{\cdots}{\Gamma \vdash x = x^\sharp} \quad \dfrac{\dfrac{\dfrac{\cdots}{\Gamma^\sharp \vdash [\delta^\sharp]\, v^\sharp > 0}\,\text{DI} \quad \cdots}{\Gamma^\sharp \wedge v > 0 \vdash [\delta^\sharp]\, \frac{v}{v^\sharp} > 0}\,\text{DC}\{v^\sharp > 0\}}{\Gamma \vdash [\langle\!\langle \delta \,\&\, v > 0 \mid \delta^\sharp \rangle\!\rangle]\, \frac{v}{v^\sharp} > 0}\,\text{DW} \quad \dfrac{\dfrac{\cdots}{\Gamma \vdash v \leq v^\sharp} \quad \dfrac{\dfrac{\cdots \quad \dfrac{\cdots}{\Gamma \vdash [\delta_s \,\&\, v > 0 \wedge v \leq v^\sharp]\, \frac{a \cdot a^\sharp \cdot v}{v^\sharp} \leq a^\sharp \cdot a}\,\text{DW}}{\Gamma \vdash [\delta_s \,\&\, v > 0 \wedge v \leq v^\sharp]\, a \cdot v^\sharp < a^\sharp \cdot v}\,\text{DI} \quad \cdots}{\Gamma \vdash [\delta_s \,\&\, v > 0 \wedge v \leq v^\sharp]\, a < \frac{a^\sharp \cdot v}{v^\sharp}}\,\text{DC}\{a \cdot v^\sharp < a^\sharp \cdot v\}}{\Gamma \vdash [\delta_s \,\&\, v > 0]\, v \leq v^\sharp}\,\text{DII}_1}{\Gamma \vdash [\langle\!\langle \delta \,\&\, v > 0 \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v \leq v^\sharp}\,\text{TS}}{\Gamma \vdash [\langle\!\langle \delta \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v \leq v^\sharp}\,\text{DC}\{v > 0\}$$

Case Study: Collision Speed under Drag

We once again compare velocities at collision, however, this time we use different models of drag. The first dynamics δ uses linear drag, while the second dynamics $\delta^\sharp$ uses the standard (quadratic) drag equation. We prove that the "sharp" model with stronger (quadratic) drag has lower impact velocity. To avoid the edge case with velocity lower than 1, where the quadratic effect reverses, we assume the obstacle is hit at velocity higher than 1.

$$\delta \equiv \dot{x} = v, \dot{v} = -v; \qquad \delta^\sharp \equiv \dot{x^\sharp} = v^\sharp, \dot{v^\sharp} = -(v^\sharp)^2 \,\&\, v^\sharp \geq 1; \qquad \Gamma \equiv x = x^\sharp = 0, v = v^\sharp > 1; \qquad \delta_s \equiv \dot{x} = v, \dot{v} = -v, \dot{x^\sharp} = \frac{v^\sharp \cdot v}{v^\sharp}, \dot{v^\sharp} = \frac{-(v^\sharp)^2 \cdot v}{v^\sharp} \,\&\, v^\sharp \geq 1.$$

$$\dfrac{\dfrac{\cdots}{\Gamma \vdash [\delta]\, v > 0}\,\text{dbx}_> \qquad \dfrac{\dfrac{\cdots}{\Gamma \vdash x = x^\sharp} \quad \dfrac{\cdots}{\Gamma \vdash [\langle\!\langle \delta \,\&\, v > 0 \mid \delta^\sharp \rangle\!\rangle]\, \frac{v}{v^\sharp} > 0}\,\text{DW} \quad \dfrac{\cdots \quad \dfrac{\cdots}{\Gamma \vdash [\delta_s \,\&\, v > 0]\, \frac{-(v^\sharp)^2 \cdot v}{v^\sharp} \leq -v}\,\text{DW}}{\Gamma \vdash [\delta_s \,\&\, v > 0]\, v^\sharp \leq v}\,\text{DI}}{\Gamma \vdash [\langle\!\langle \delta \,\&\, v > 0 \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v^\sharp \leq v}\,\text{TS}}{\Gamma \vdash [\langle\!\langle \delta \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v^\sharp \leq v}\,\text{DC}\{v > 0\}$$

Case Study: Dynamics Abstraction

In this case study, we consider the acceleration to be constant only up to speed V (dynamics δ). Beyond V the acceleration decays (dynamics δ_2). Instead of considering two cars, we consider the "sharp" dynamics to be an abstraction of the first dynamics, with no acceleration decay.

$$\delta \equiv \dot{x} = v, \dot{v} = a \ \&\ v \leq V; \qquad \delta_2 \equiv \dot{x} = v, \dot{v} = \frac{a \cdot V}{v}; \qquad \delta^\sharp \equiv \dot{x^\sharp} = v^\sharp, \dot{v^\sharp} = a; \qquad \Gamma \equiv 0 < a, 0 < V, 0 = x = x^\sharp, 0 < v = v^\sharp;$$

$$\delta_s \equiv \dot{x} = v, \dot{v} = a, \dot{x^\sharp} = \frac{v^\sharp \cdot a}{a}, \dot{v^\sharp} = \frac{a^2}{a} \,\&\, v \leq V; \qquad \delta_{s2} \equiv \dot{x} = v, \dot{v} = \frac{a \cdot V}{v}, \dot{x^\sharp} = \frac{v^\sharp \cdot a \cdot V}{a \cdot v}, \dot{v^\sharp} = \frac{a^2 \cdot V}{a \cdot v} \,\&\, v \leq V; \qquad \Gamma' \equiv 0 < a, 0 < V, x = x^\sharp, V = v = v^\sharp.$$

We prove that the abstract model has higher impact velocity. Limits shown for the velocity of the abstract model thus carry over to the concrete one.

$$\dfrac{\cdots \qquad \dfrac{\dfrac{\cdots \qquad \dfrac{\dfrac{\cdots}{\Gamma \vdash [\delta_s]\, x = x^\sharp}\,\text{DI} \quad \dfrac{\dfrac{\dfrac{\cdots \quad \dfrac{\cdots}{\Gamma' \vdash [\delta_{s2}]\, x \geq x^\sharp}\,\text{DC}\{V \leq v = v^\sharp\}}{\Gamma' \vdash [\langle\!\langle \delta_2 \mid \delta^\sharp \rangle\!\rangle\, v = v^\sharp]\, x \geq x^\sharp}\,\text{TS} \quad \cdots}{\Gamma' \vdash [\langle\!\langle \delta_2 \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v \leq v^\sharp}\,\text{MCS}}{\Gamma \vdash [\delta_s \,\&\, x = x^\sharp; ?v = v^\sharp = V]\, [\langle\!\langle \delta_2 \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v \leq v^\sharp}\,\text{DW}}{\Gamma \vdash [\delta_s; ?v = v^\sharp = V]\, [\langle\!\langle \delta_2 \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v \leq v^\sharp}\,\text{DC}\{x = x^\sharp\}}{\Gamma \vdash [\langle\!\langle \delta \mid \delta^\sharp \,\&\, v^\sharp \leq V \rangle\!\rangle\, v = v^\sharp]\, [?v = V \wedge v^\sharp = V]\, [\langle\!\langle \delta_2 \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v \leq v^\sharp}\,\text{TS} \quad \cdots}{\Gamma \vdash [\langle\!\langle \delta \mid \delta^\sharp \,\&\, v^\sharp \leq V \rangle\!\rangle\, v = V \wedge v^\sharp = V]\, [\langle\!\langle \delta_2 \mid \delta^\sharp \rangle\!\rangle\, x = x^\sharp]\, v \leq v^\sharp}\,\text{RDC}}{\Gamma \vdash [\langle\!\langle \delta \mid \delta^\sharp \rangle\!\rangle\, v = V]\, [\delta_2; ?x = x^\sharp]\, v \leq v^\sharp}\,\text{DDS}$$

$$\frac{\begin{array}{c} \Gamma \vdash [\langle\!\langle \delta \mid \delta^\sharp \rangle\!\rangle\, h(\boldsymbol{x}) = h^\sharp(\boldsymbol{x}^\sharp)]\, g(\boldsymbol{x}) \geq g^\sharp(\boldsymbol{x}^\sharp) \\ \Gamma \vdash [?Q \wedge Q^\sharp]\, h(\boldsymbol{x}) \leq h^\sharp(\boldsymbol{x}^\sharp) \quad \Gamma \vdash [\delta]\, \mathcal{L}_{\boldsymbol{f}} g(\boldsymbol{x}) > 0 \\ \Gamma \vdash [\delta]\, \mathcal{L}_{\boldsymbol{f}} h(\boldsymbol{x}) \geq 0 \qquad \Gamma \vdash [\delta^\sharp]\, \mathcal{L}_{\boldsymbol{f}^\sharp} h^\sharp(\boldsymbol{x}^\sharp) \geq 0 \end{array}}{\Gamma \vdash [\langle\!\langle \delta \mid \delta^\sharp \rangle\!\rangle\, g(\boldsymbol{x}) = g^\sharp(\boldsymbol{x}^\sharp)]\, h(\boldsymbol{x}) \leq h^\sharp(\boldsymbol{x}^\sharp)}\ \text{MCS}$$

$$\frac{\begin{array}{c} \Gamma \vdash [\delta; \delta^\sharp; ?g(\boldsymbol{x}) = g^\sharp(\boldsymbol{x}^\sharp); ?P]\, \varphi \\ \Gamma \vdash [\delta; \delta^\sharp; ?P]\, g(\boldsymbol{x}) = g^\sharp(\boldsymbol{x}^\sharp) \end{array}}{\Gamma \vdash [\delta; \delta^\sharp; ?P]\, \varphi}\ \text{RDC}$$

$$\frac{\begin{array}{c} \Gamma \vdash [\delta \,\&\, Q]\, \mathcal{L}_{\boldsymbol{f}} g(\boldsymbol{x}) > 0 \qquad g(\boldsymbol{x}) \leq p \vdash Q \\ \Gamma \vdash [\delta \,\&\, Q \wedge g(\boldsymbol{x}) \leq p; ?g(\boldsymbol{x}) = p; \delta \,\&\, Q]\, P \end{array}}{\Gamma \vdash [\delta \,\&\, Q]\, P}\ \text{DDS}$$

References

[1] A. Platzer. A complete uniform substitution calculus for differential dynamic logic. *J. Autom. Reas.*, 59(2):219–265, 2017.

[2] A. Platzer. *Logical Foundations of Cyber-Physical Systems*. Springer, 2018.

[3] A. Platzer and Y. K. Tan. Differential equation axiomatization: The impressive power of differential ghosts. In A. Dawar and E. Grädel, editors, *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, July 09-12, 2018*, pages 819–828. ACM, 2018.

Acknowledgements

Thanks are due to Kenji Kamijo, Yoshiyuki Shinya and Takamasa Suetomi from Mazda Motor Corporation for helpful discussions. The authors are supported by ERATO HASUO Metamathematics for Systems Design Project (No. JPMJER1603), JST. J.K. is supported by ANR-FNR project "AlgoReCell" ANR-16-CE12-0034. I.H. is supported by Grants-in-Aid No. 15KT0012, JSPS.

Ideas presented here are developed on arXiv: `https://arxiv.org/abs/1903.00153`