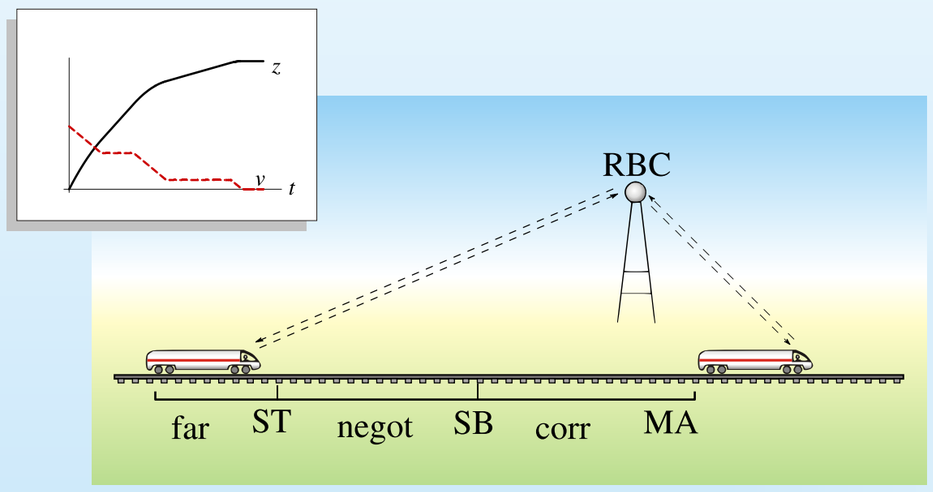
Differential Logic for Reasoning about Hybrid Systems

HSCC07 Hybrid Systems Computation and Control

André Platzer

University of Oldenburg, Germany
E-mail: andre.platzer@informatik.uni-oldenburg.de

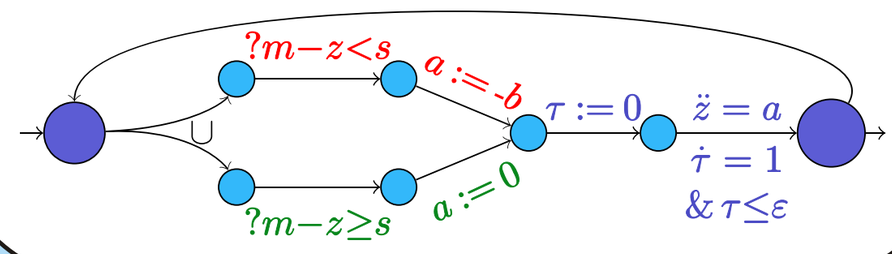
Abstract
We propose a first-order dynamic logic for reasoning about hybrid systems. As a uniform model for discrete and continuous evolutions in hybrid systems, we introduce hybrid programs with differential actions. Our logic can be used to specify and verify correctness statements about hybrid programs, which are suitable for symbolic processing by calculus rules. Using first-order variables, our logic supports systems with symbolic parameters. With dynamic modalities, it is prepared to handle multiple system components.



Dynamic Logic

$$\begin{aligned} \psi &\rightarrow [control^*]\, z \leq m \\ \psi &\equiv b > 0 \wedge \varepsilon > 0 \\ control &\equiv corr; drive \\ corr &\equiv (?m - z < s; a := -b) \cup (?m - z \geq s; a := 0) \\ drive &\equiv \tau := 0; (\ddot{z} = a, \dot{\tau} = 1 \,\&\, \dot{z} \geq 0 \wedge \tau \leq \varepsilon) \end{aligned}$$

Hybrid Program



spec **model**

Deductive Proof

$$\dfrac{\dfrac{\dfrac{\dfrac{\dots \;\vdash\; v^2 \leq 2b(m-z)}{\dots \;\vdash\; \dots}}{\psi \;\vdash\; [a := -b][drive]\psi} \qquad \dfrac{\dfrac{\dots \;\vdash\; s \geq \varepsilon v + \frac{v^2}{2b}}{\dots \;\vdash\; \dots}}{\psi, m-z \geq s \;\vdash\; [a := 0][drive]\psi}}{\psi \;\vdash\; [corr][drive]\psi}}{\psi \;\vdash\; [control]\psi}$$

$$\vdash \psi \rightarrow [(control)^*]z \leq m$$

$$v^2 \leq 2b(m-z)$$
$$s \geq \varepsilon v + \frac{v^2}{2b}$$

check

yes **no**

References
[1] Damm, W., Hungar, H., Olderog, E.R.: Verification of cooperating travel agents. International Journal of Control 79(5) (2006) 395–421
[2] Platzer, A.: Towards a hybrid dynamic logic for hybrid dynamic systems. In Blackburn, P., Bolander, T., Braüner, T., de Paiva, V., Villadsen, J., eds.: Proc., LICS International Workshop on Hybrid Logic, Seattle, USA. ENTCS (2006)
[3] Davoren, J.M., Nerode, A.: Logics for hybrid systems. Proc. IEEE 88(7) (2000) 985–1010

DAAD Deutscher Akademischer Austausch Dienst German Academic Exchange Service
Deutsche Forschungsgemeinschaft DFG
Universität Oldenburg
Albert-Ludwigs-Universität Freiburg
Universität des Saarlandes