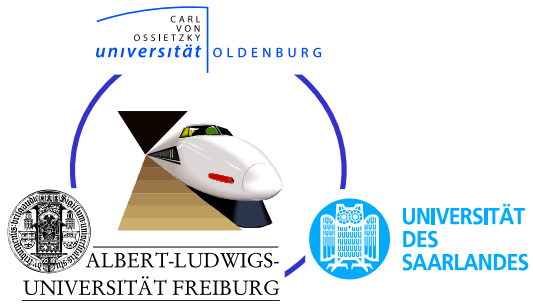
KeYmaera: A Hybrid Theorem Prover for Hybrid Systems

André Platzer **Jan-David Quesel**

University of Oldenburg, Department of Computing Science, Germany

International Joint Conference on Automated Reasoning, Sydney 2008

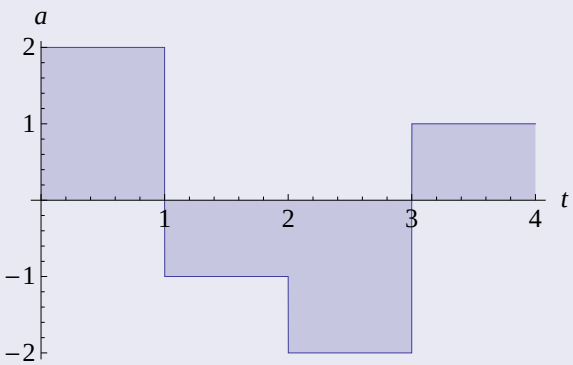


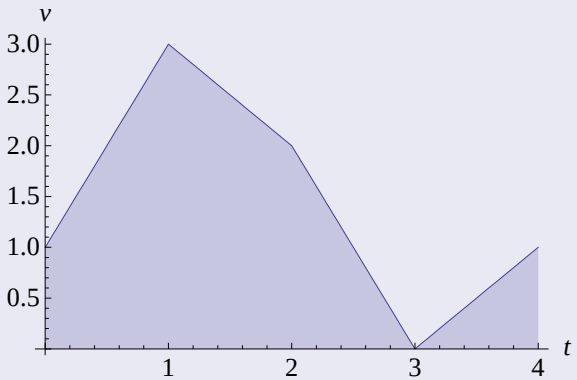
Motivation

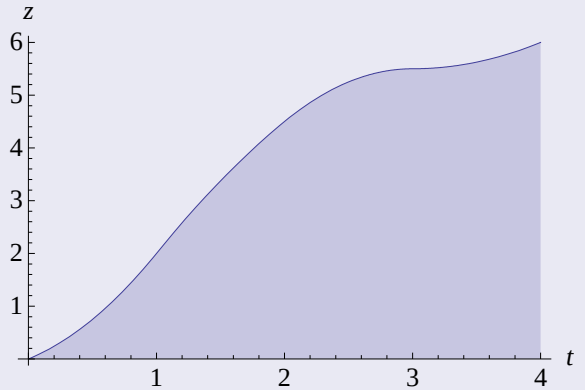
KeYmaera: Verification tool for hybrid systems

Hybrid System

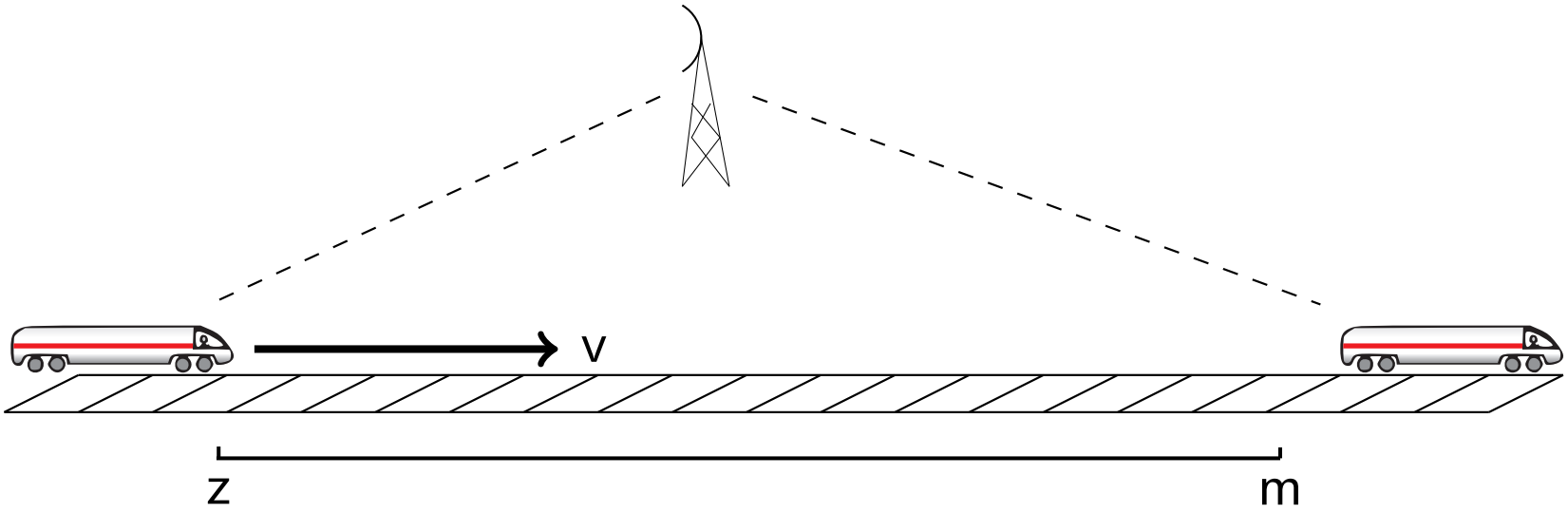
- Continuous evolutions (differential equations)
- Discrete jumps (control decisions)







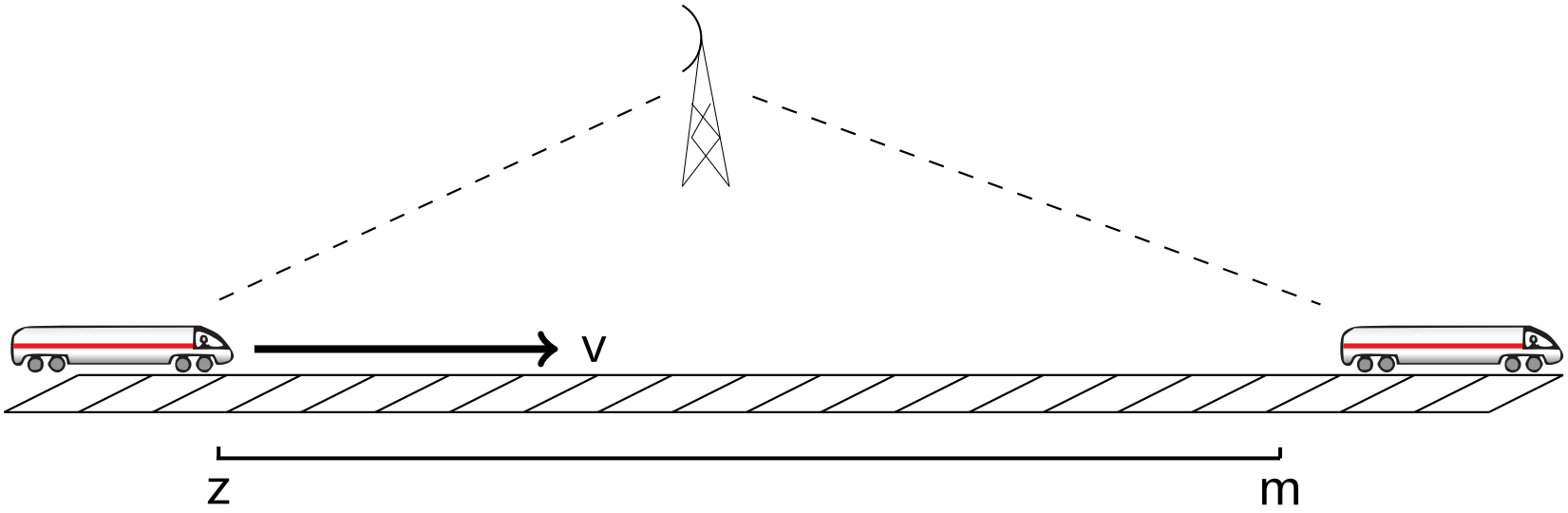
Differential Dynamic Logic (d$\mathcal{L}$)



Example

$$\underbrace{\qquad}_{\text{Precondition}} \longrightarrow [\underbrace{\qquad\qquad\qquad\qquad}_{\text{Operational model}}](\underbrace{\quad}_{\text{Property}})$$

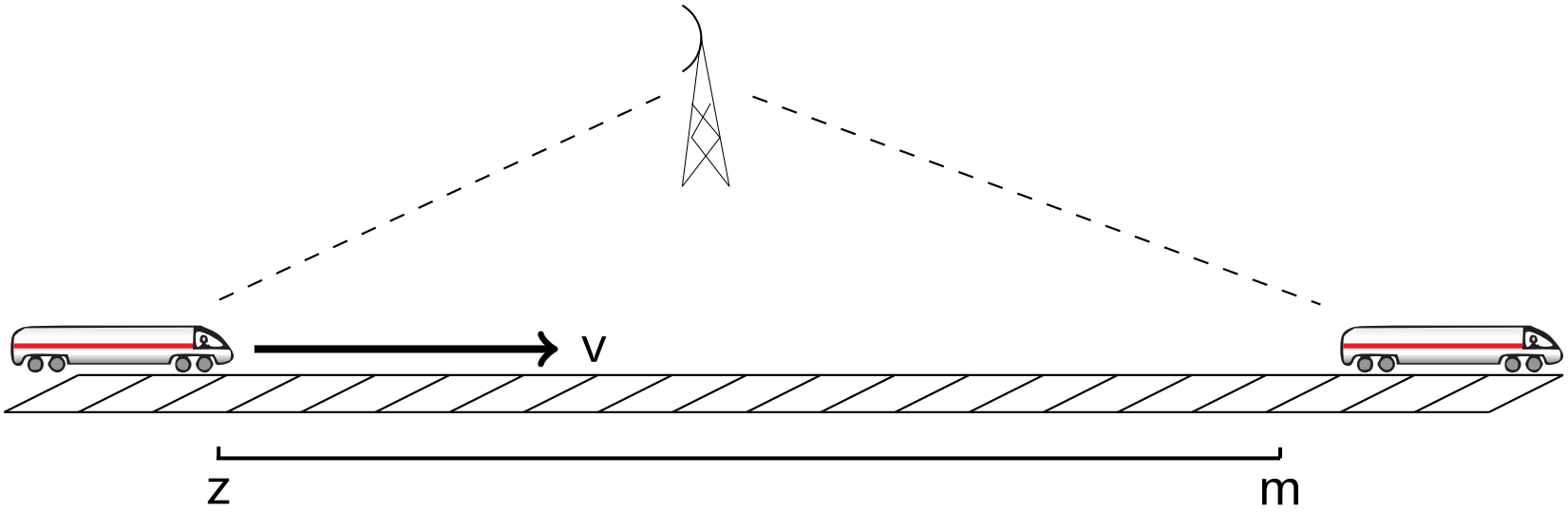
Differential Dynamic Logic (d$\mathcal{L}$)



Example

$$\underbrace{v^2 \leq 2b(m-z)}_{\text{Precondition}} \longrightarrow [\underbrace{\qquad\qquad}_{\text{Operational model}}](\underbrace{z \leq m}_{\text{Property}})$$

Differential Dynamic Logic (dℒ)

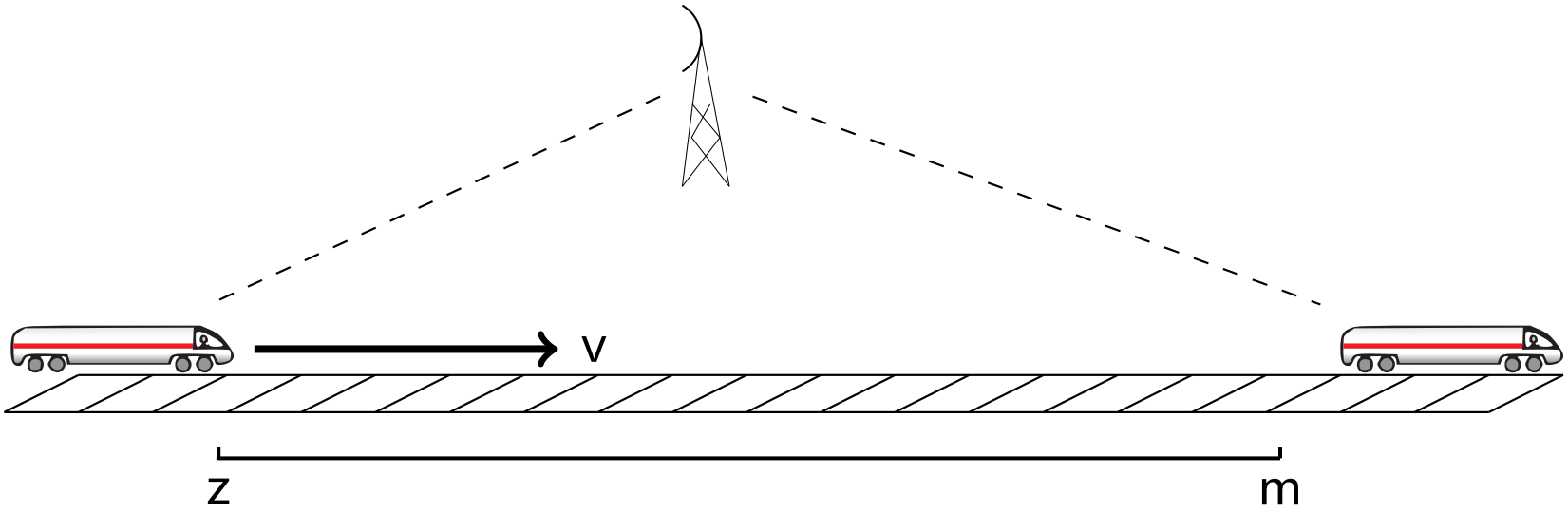


Example

$$\underbrace{v^2 \leq 2b(m-z)}_{\text{Precondition}} \longrightarrow \underbrace{[\underbrace{z' = v, v' = a}_{\text{Operational model}}]\underbrace{(z \leq m)}_{\text{Property}}}$$

Continuous evolution: differential equation

Differential Dynamic Logic (d$\mathcal{L}$)

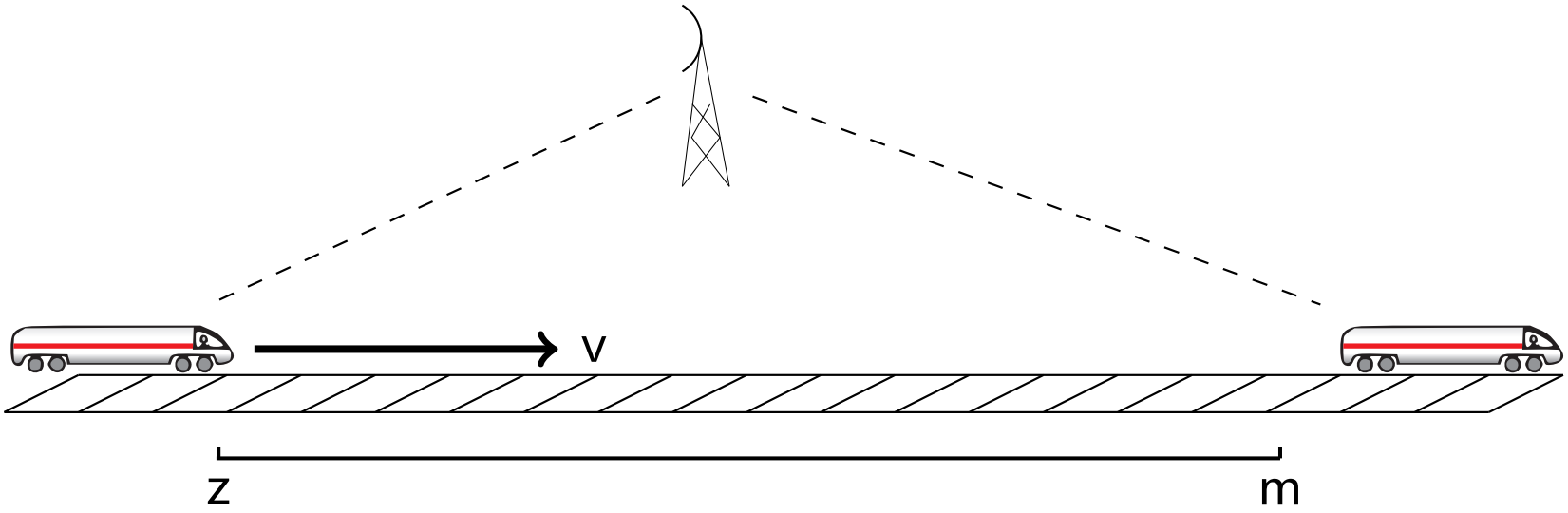


Example

$$\underbrace{v^2 \leq 2b(m-z)}_{\text{Precondition}} \longrightarrow \underbrace{[a := *; \quad z' = v, v' = a]}_{\text{Operational model}}\underbrace{(z \leq m)}_{\text{Property}}$$

Random assignment

Differential Dynamic Logic (dℒ)



Example

$$\underbrace{v^2 \leq 2b(m-z)}_{\text{Precondition}} \longrightarrow \underbrace{[a := *;\ ?a \leq -b;\ z' = v, v' = a]}_{\text{Operational model}}\underbrace{(z \leq m)}_{\text{Property}}$$

Test

Syntax of Differential Dynamic Logic

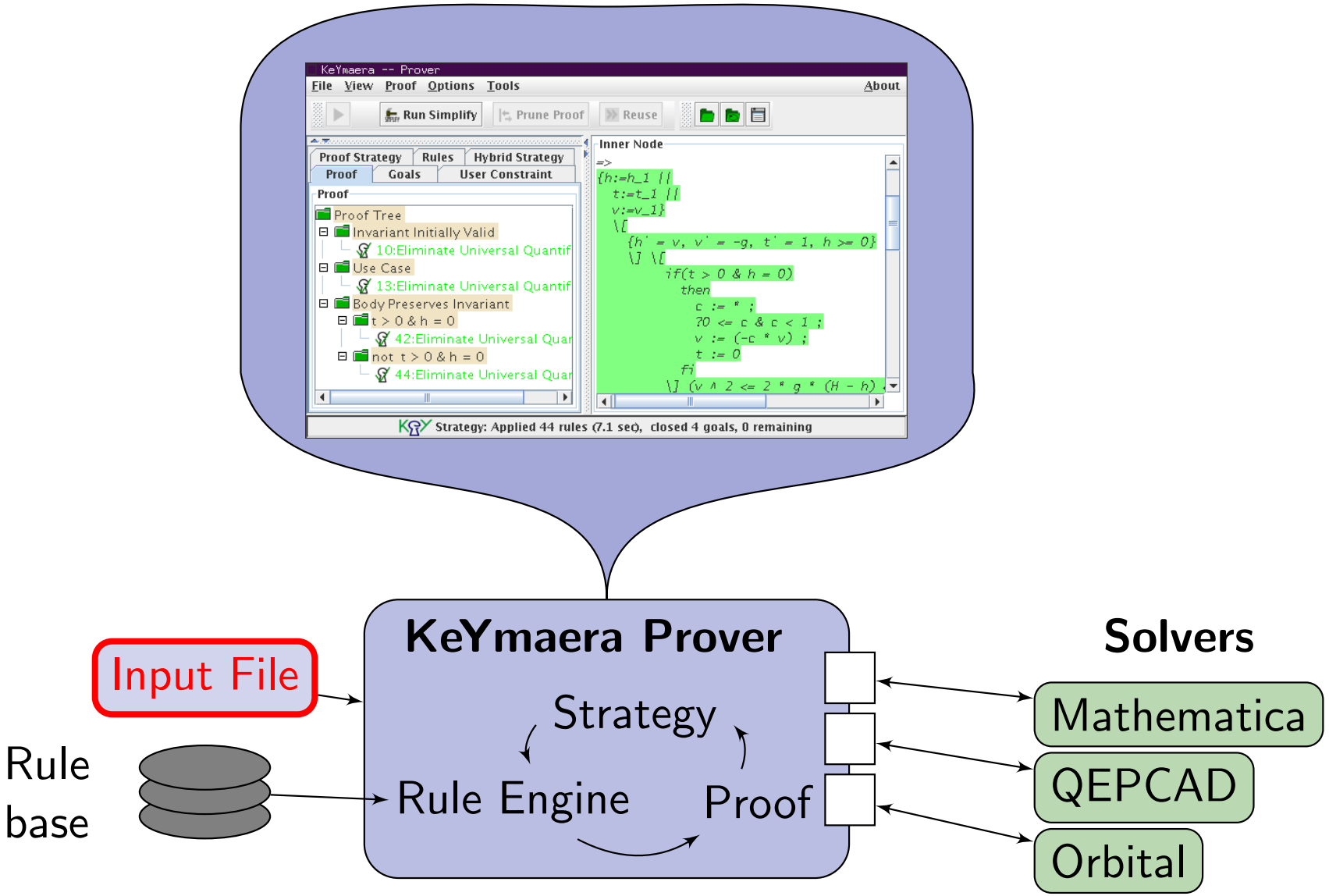
dℒ Formulas

$$\phi ::= \theta_1 \sim \theta_2 \mid \neg\phi \mid \phi \wedge \psi \mid \forall x \phi \mid \exists x \phi \mid [\alpha]\phi \mid \langle\alpha\rangle\phi$$

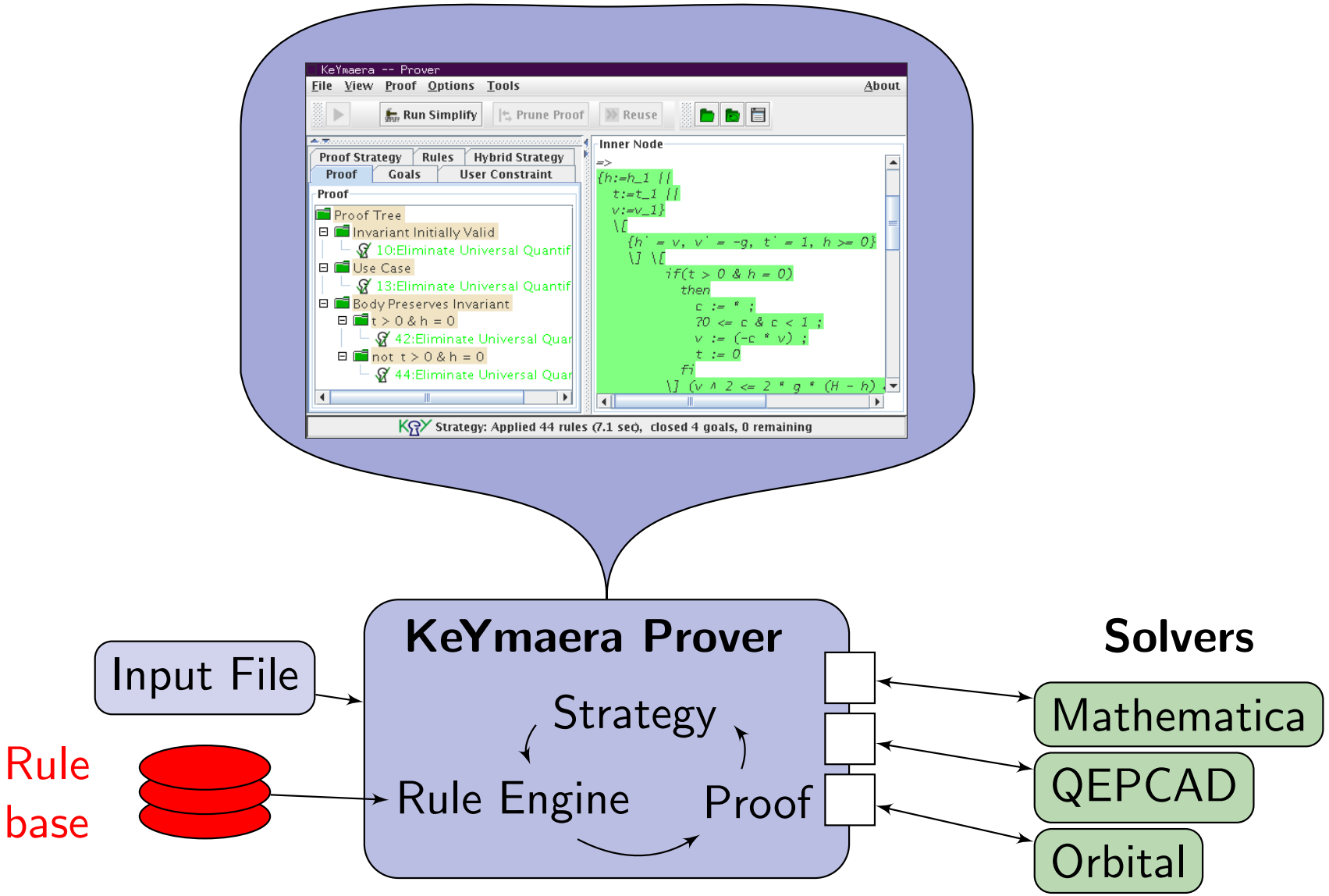
Hybrid Program	Effect
$\alpha;\ \beta$	sequential composition
$\alpha\ \cup\ \beta$	nondeterministic choice
α^*	nondeterministic repetition
$x := \theta$	discrete assignment (jump)
$x := *$	nondeterministic assignment
$(x_1' = \theta_1, \ldots, x_n' = \theta_n, F)$	continuous evolution of x_i
$?F$	check if formula F holds

A. Platzer.
Differential Dynamic Logic for Hybrid Systems.
Journal of Automated Reasoning, 41(2), 2008, to appear.

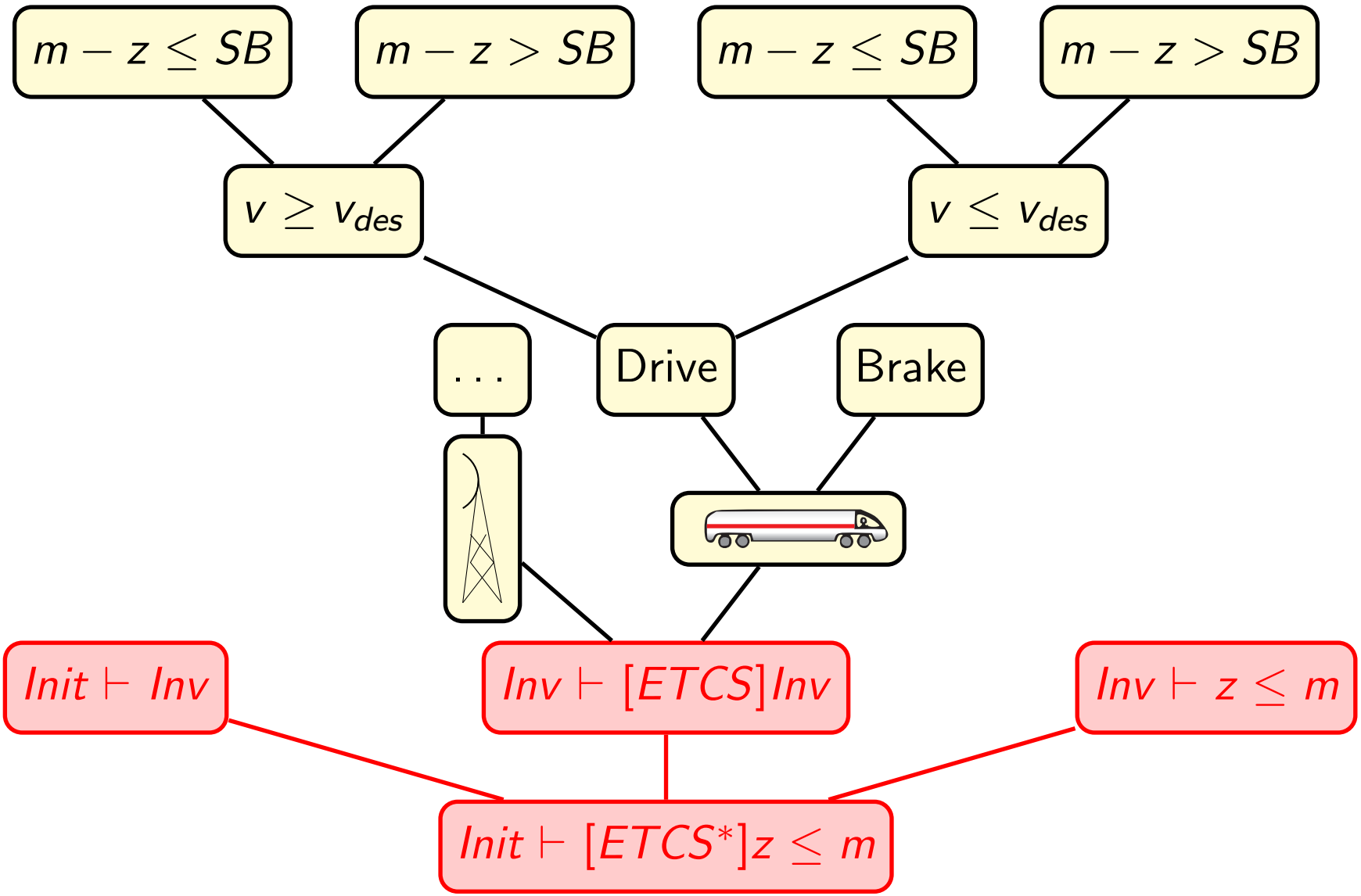
KeYmaera Architecture



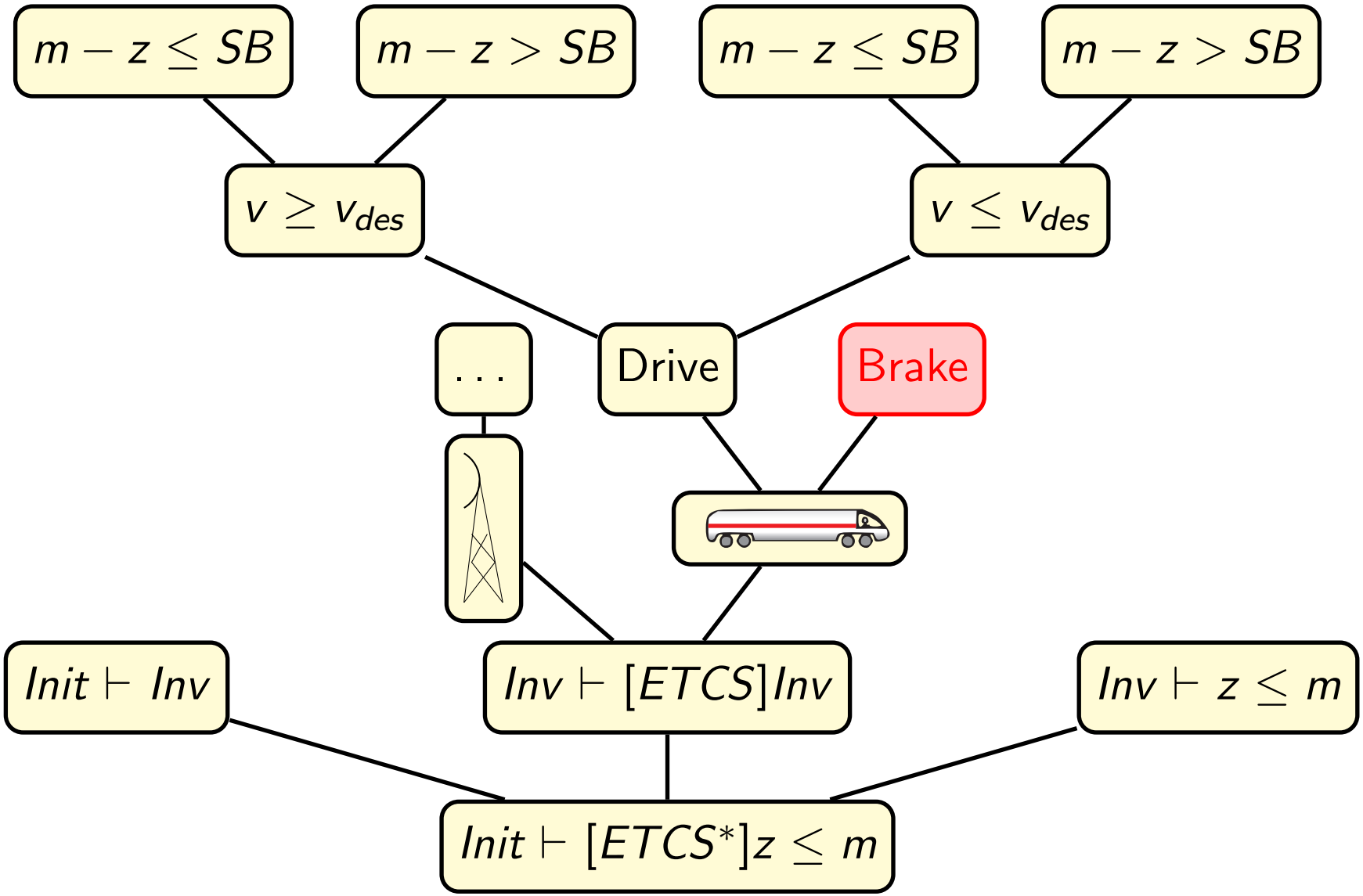
KeYmaera Architecture



Proof Sketch



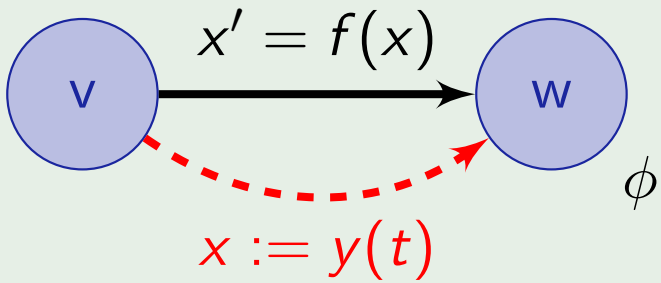
Proof Sketch



Handling Differential Equations

Example

$$\frac{\forall t \geq 0\ [x := y(t)]\,\phi}{[x' = f(x)]\,\phi}$$

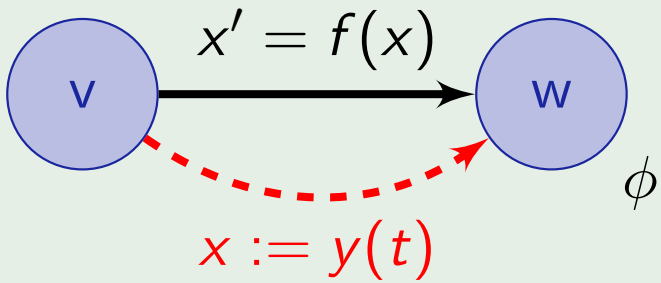


$$\ldots \vdash [z' = v, v' = -b]z \leq m$$

Handling Differential Equations

Example

$$\frac{\forall t \geq 0\ [x := y(t)]\,\phi}{[x' = f(x)]\,\phi}$$

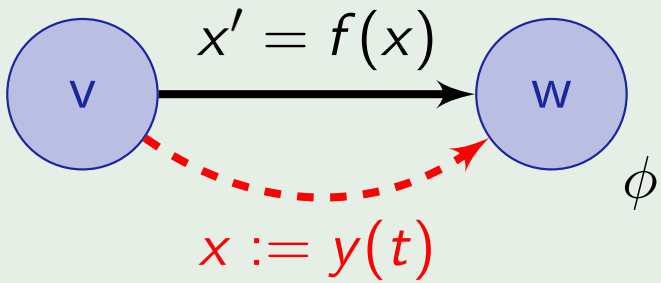


$$\frac{}{\ldots \vdash \forall t \geq 0\,[z := -\tfrac{1}{2}bt^2 + tv + z]z \leq m}$$
$$\ldots \vdash [z' = v, v' = -b]z \leq m$$

Handling Differential Equations

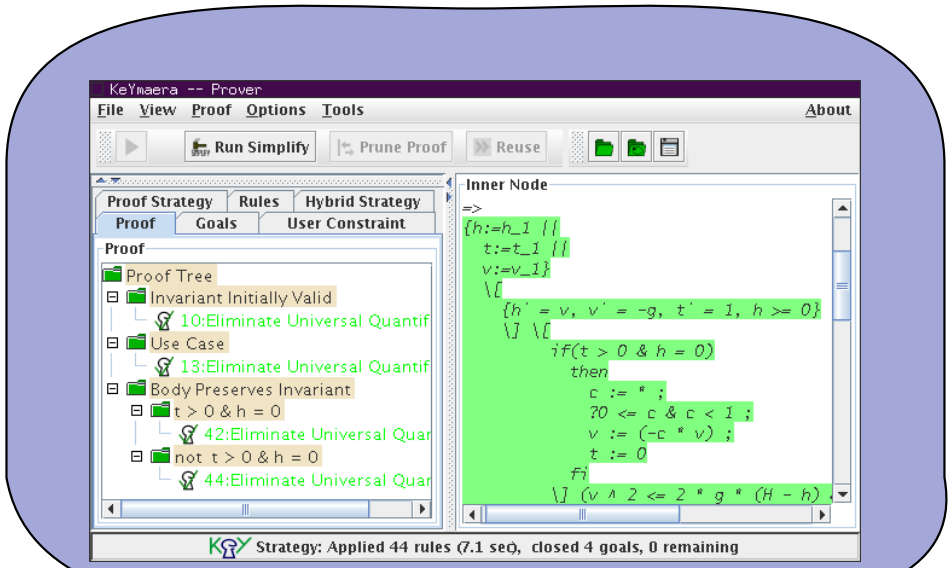
Example

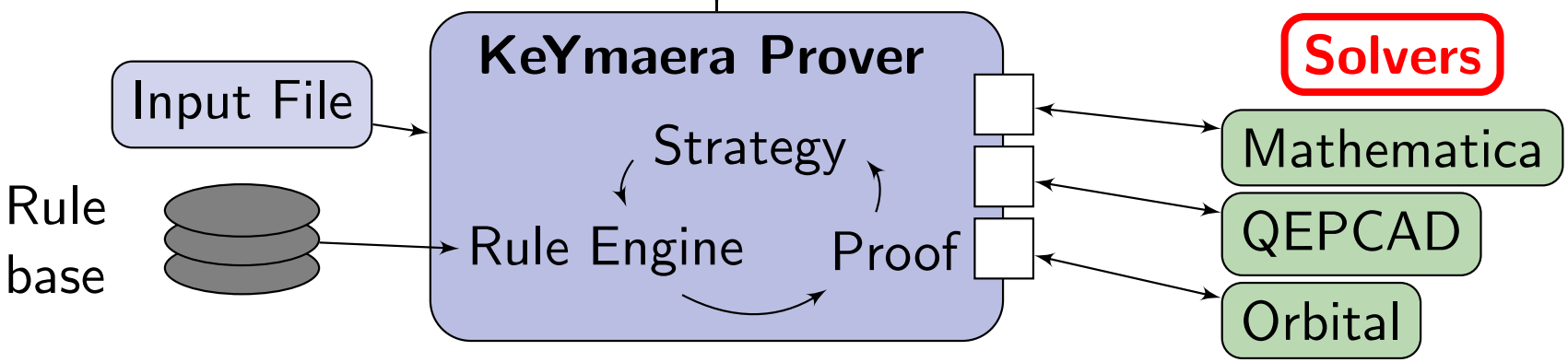
$$\frac{\forall t \geq 0\ [x := y(t)]\,\phi}{[x' = f(x)]\,\phi}$$



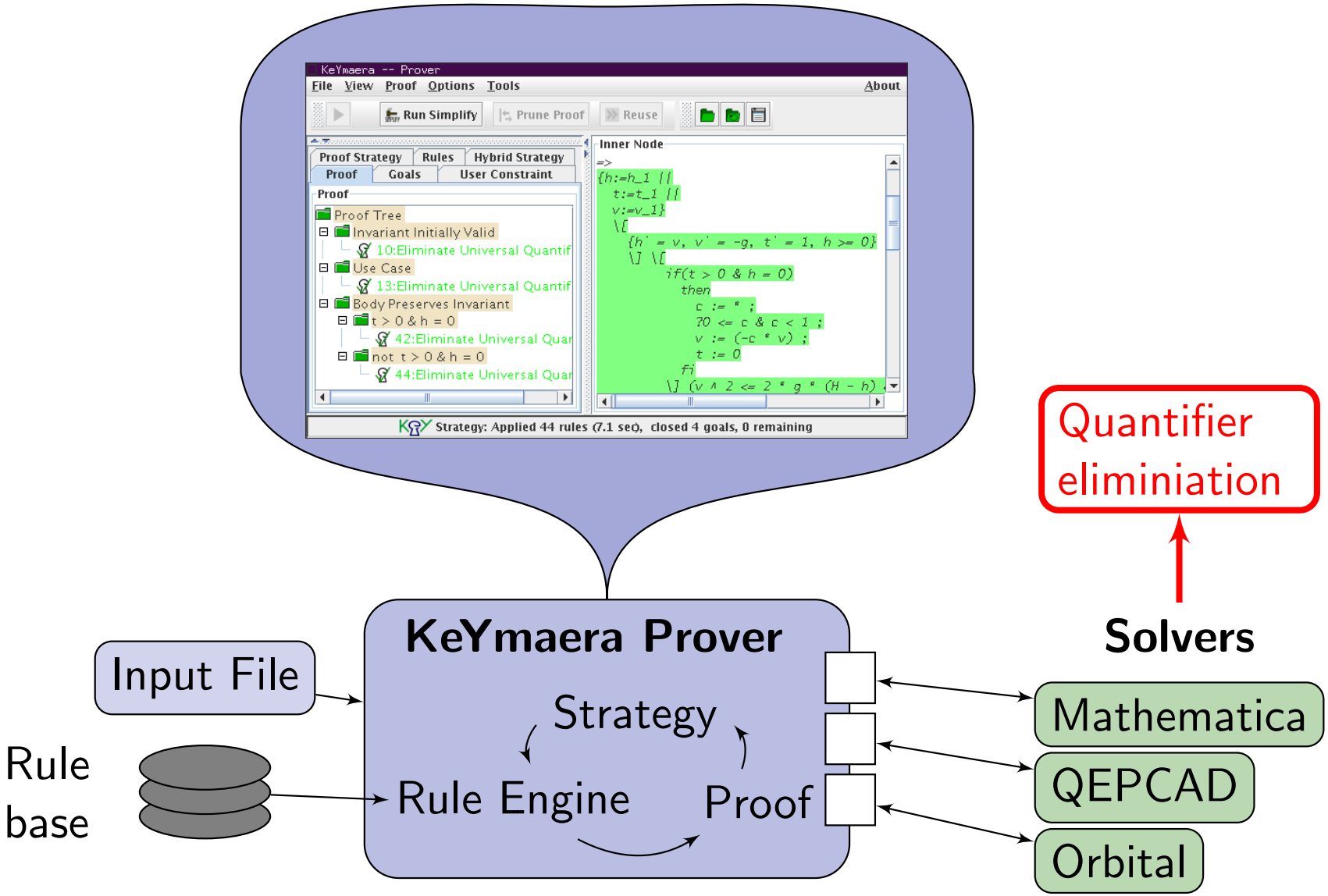
$$\frac{\dots \quad \vdash \forall t \geq 0\,(-\frac{1}{2}bt^2 + tv + z \leq m)}{\dots \quad \vdash \forall t \geq 0\,[z := -\frac{1}{2}bt^2 + tv + z]z \leq m}$$
$$\frac{}{\dots \quad \vdash [z' = v, v' = -b]z \leq m}$$

KeYmaera Architecture

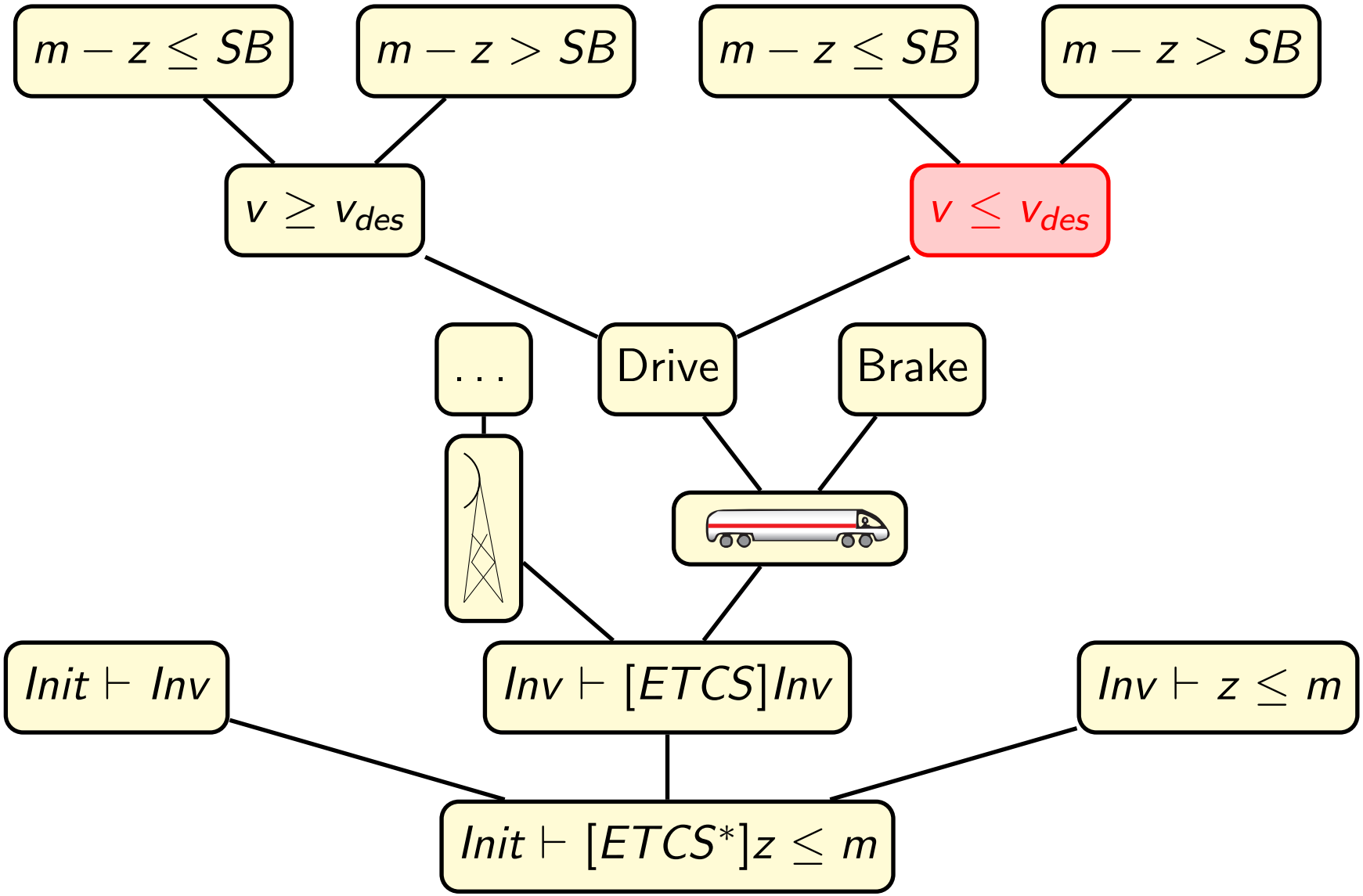




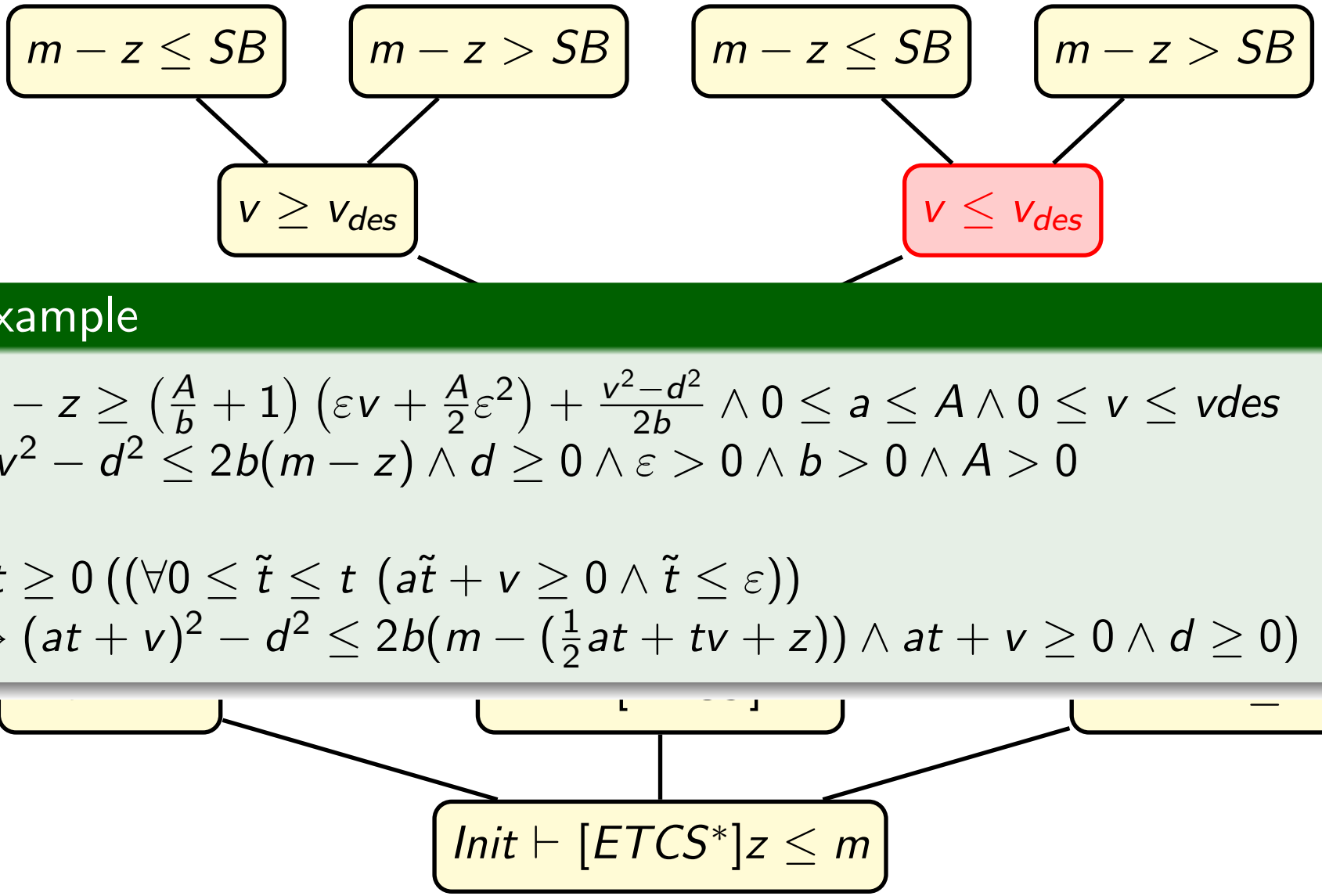
KeYmaera Architecture



Proof Sketch



Proof Sketch



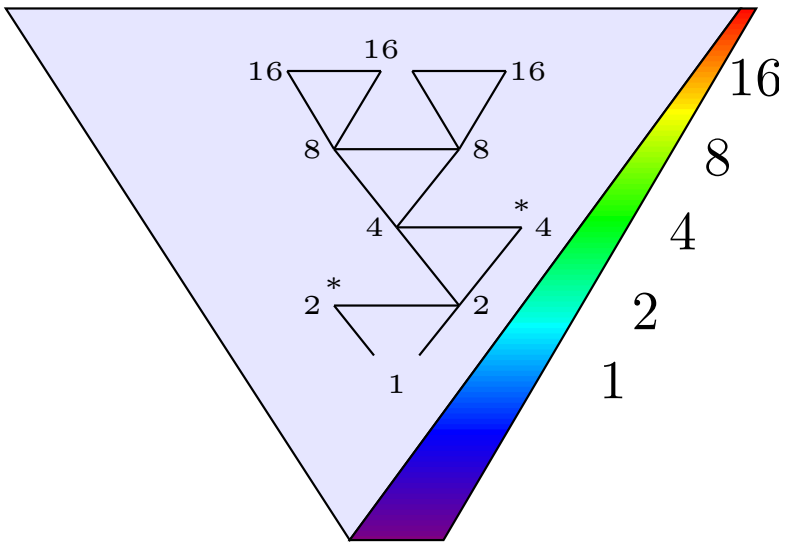
Example

$$m - z \geq \left(\frac{A}{b} + 1\right)\left(\varepsilon v + \frac{A}{2}\varepsilon^2\right) + \frac{v^2 - d^2}{2b} \wedge 0 \leq a \leq A \wedge 0 \leq v \leq vdes$$
$$\wedge v^2 - d^2 \leq 2b(m - z) \wedge d \geq 0 \wedge \varepsilon > 0 \wedge b > 0 \wedge A > 0$$
$$\vdash$$
$$\forall t \geq 0 \left((\forall 0 \leq \tilde{t} \leq t \ (a\tilde{t} + v \geq 0 \wedge \tilde{t} \leq \varepsilon)\right)$$
$$\rightarrow (at + v)^2 - d^2 \leq 2b(m - (\tfrac{1}{2}at + tv + z)) \wedge at + v \geq 0 \wedge d \geq 0)$$

Iterative Background Closure

- Quantifier elimination is doubly exponential
- Choice conflict:
  1. Apply quantifier elimination
  2. Split using

$$\frac{\vdash F \qquad \vdash G}{\vdash F \wedge G}$$



Experimental Results

Case Study	Interact	Steps	IBC(s)	Eager QE(s)
ETCS essentials	0	46	47.8	∞
	1	46	6.6	8.8
ETCS complete	0	163	2045.2	∞
	1	168	23.3	∞
ETCS reactivity	0	49	76.2	∞
ETCS liveness	3	112	17.6	16.0
Aircraft TRM	0	94	10.9	∞
	1	94	1.2	1.2
TRM 3 Planes	0	187	171.8	∞
	1	187	21.2	∞
TRM 4 Planes	0	255	704.3	∞
	1	255	170	∞
Water tank	0	-	∞	∞
	1	375	2.0	2.0

$\infty \mathrel{\hat{=}}$ more than five hours

Experimental Results

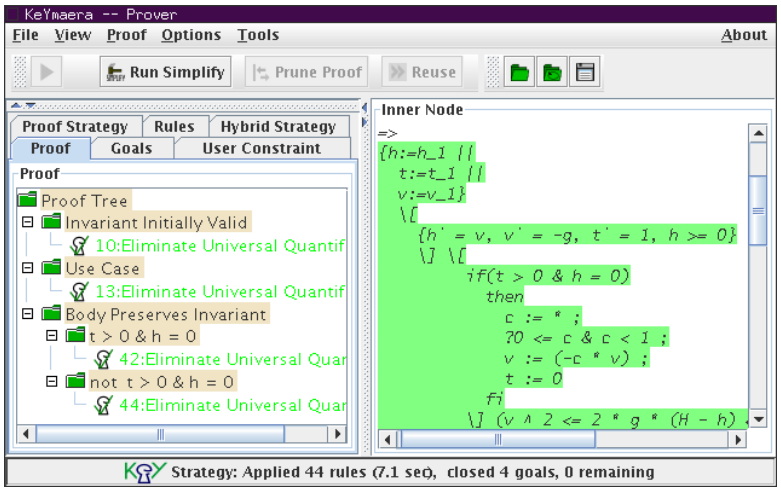
Case Study	Interact	Steps	IBC(s)	Eager QE(s)
ETCS essentials	0	46	47.8	∞
	1	46	6.6	8.8
ETCS complete	0	163	2045.2	∞
	1	168	23.3	∞
ETCS reactivity	0	49	76.2	∞
ETCS liveness	3	112	17.6	16.0
Aircraft TRM	0	94	10.9	∞
	1	94	1.2	1.2
TRM 3 Planes	0	187	171.8	∞
	1	187	21.2	∞
TRM 4 Planes	0	255	704.3	∞
	1	255	170	∞
Water tank	0	-	∞	∞
	1	375	2.0	2.0

$\infty \mathrel{\hat{=}}$ more than five hours

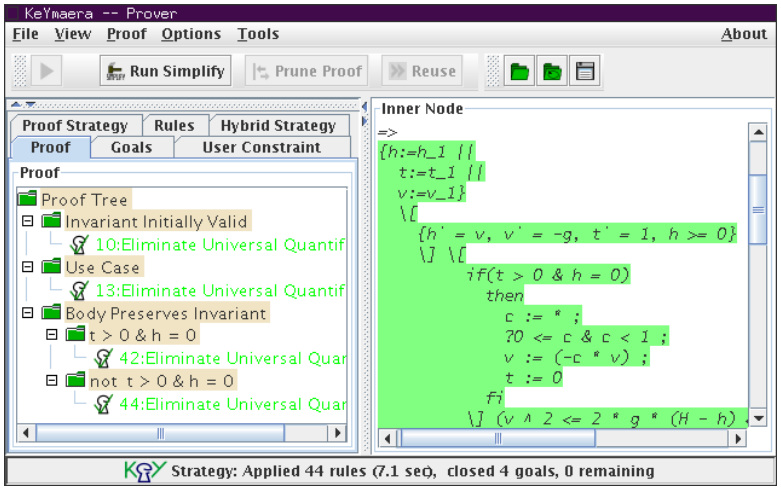
Conclusions

KeYmaera Summary

- Hybrid theorem prover for verifying hybrid systems
  - Differential Dynamic Logic (d$\mathcal{L}$) and Hybrid Programs
  - Sequent calculus
  - Quantifier elimination, computer algebra
- Automatic proof strategies (95 – 100%)
- Plugin-architecture for backends



Conclusions



Features

- Verify controllability, reactivity, safety and liveness properties
- Counterexample generation
- Automatic invariant discovery
- Handling differential inequalities ($z'' \leq a$)
- Support for proof annotations
- Equational Gröbner basis verification support


A. Platzer.
Differential Dynamic Logic for Verifying Parametric Hybrid Systems.
In N. Olivetti, editor, *TABLEAUX*, volume 4548 of *LNCS*, pages 216–232. Springer, 2007.


A. Platzer.
Differential Dynamic Logic for Hybrid Systems.
Journal of Automated Reasoning, 41(2), 2008, to appear.


A. Platzer and E. M. Clarke.
Computing Differential Invariants of Hybrid Systems as Fixedpoints.
In A. Gupta and S. Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189, 2008.


A. Platzer and J.-D. Quesel.
Logical Verification and Systematic Parametric Analysis in Train Control.
In M. Egerstedt and B. Mishra, editors, *HSCC*, volume 4981 of *LNCS*, pages 646-649. Springer, 2008.