KeYmaera X

A Tutorial on Interactive Verification for Hybrid Systems

Nathan Fulton

Marktoberdorf 2017

August 11, 2017

Examples: https://nfulton.org/marktoberdorf.zip
Slides: https://nfulton.org/slides/marktoberdorf.pdf

Motivation

KeYmaera X provides strong evidence that Cyber-Physical Systems are safe. But you need to provide the model and sometimes help the proof.

Motivation

KeYmaera X provides strong evidence that Cyber-Physical Systems are safe. But you need to provide the model and sometimes help the proof.

André's Lectures:

- Differential Dynamic Logics
  – Syntax and Semantics
- Sound and relatively complete axiomatizations
- Some examples

Motivation

KeYmaera X provides strong evidence that Cyber-Physical Systems are safe. But you need to provide the model and sometimes help the proof.

André's Lectures:

- Differential Dynamic Logics – Syntax and Semantics
- Sound and relatively complete axiomatizations
- Some examples

This Lecture:

- Practical advice for modeling systems
- Hands-on Exercise proving theorems
- Example-driven

Outline

The Stop Sign Model

Take-Aways from the Stop Sign Model

- Focus on interesting questions by `unfolding`.

Take-Aways from the Stop Sign Model

- Focus on interesting questions by `unfolding`.
- Use contextual reasoning to avoid repetition of expensive or difficult proof steps.

Take-Aways from the Stop Sign Model

- Focus on interesting questions by `unfolding`.
- Use contextual reasoning to avoid repetition of expensive or difficult proof steps.
- KeYmaera X's **edit tool** checks your arithmetic (common and annoying source of errors, both in proofs and implementations!)

Take-Aways from the Stop Sign Model

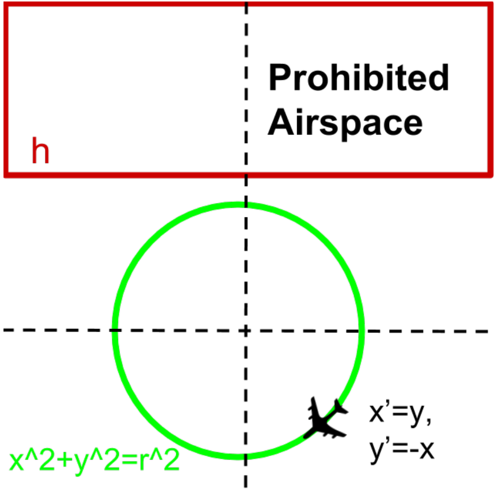
- Focus on interesting questions by `unfolding`.
- Use contextual reasoning to avoid repetition of expensive or difficult proof steps.
- KeYmaera X's **edit tool** checks your arithmetic (common and annoying source of errors, both in proofs and implementations!)
- Quantifier Elimination is a **powerful tool** useful for more than just decision procedures:
  - **Find assumptions and loop invariants** by reducing the system to arithmetic and eliminating quantifiers.
  - **ModelPlex**: $\forall x_0, x_1, \ldots, x_n . \exists y_0, \ldots, x_n . \varphi$ is kinda hard to check at runtime...

Outline

Loitering Outside Prohibited Airspace

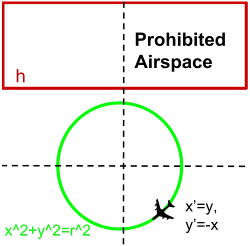
Loitering Outside Prohibited Airspace

$$y \leq h \rightarrow [\underbrace{r := *; ?r \leq h \wedge x^2 + y^2 = r^2}_{\text{Choose circle below h}}; \underbrace{x' = y, y' = -x}_{\text{Circular dynamics}}] y \leq h$$



Lie Derivative Computations

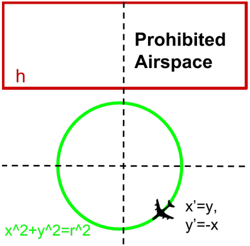
$$(y \le h)' \equiv (y)' \le (h)' \equiv -x \le 0 \quad \textbf{FALSE}$$



Lie Derivative Computations

$$(y \leq h)' \equiv (y)' \leq (h)' \equiv -x \leq 0 \quad \textbf{FALSE}$$

$$(x^2+y^2 = r^2)' \equiv (x^2+y^2)' = (r^2)' \equiv 2xx'+2yy' = 0 \equiv 2xy-2xy = 0$$

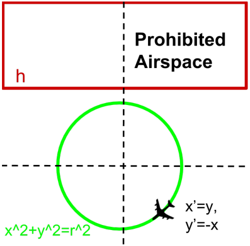


Lie Derivative Computations

$$(y \leq h)' \equiv (y)' \leq (h)' \equiv -x \leq 0 \quad \textbf{FALSE}$$

$$(x^2+y^2 = r^2)' \equiv (x^2+y^2)' = (r^2)' \equiv 2xx'+2yy' = 0 \equiv 2xy-2xy = 0$$

$$r \leq h \wedge x^2 + y^2 = r^2 \rightarrow^{?} y \leq h$$



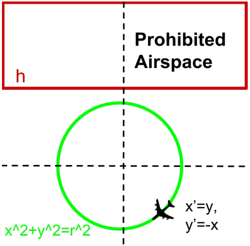
Lie Derivative Computations

$$(y \leq h)' \equiv (y)' \leq (h)' \equiv -x \leq 0 \quad \textbf{FALSE}$$

$$(x^2+y^2 = r^2)' \equiv (x^2+y^2)' = (r^2)' \equiv 2xx'+2yy' = 0 \equiv 2xy-2xy = 0$$

$$r \leq h \wedge x^2 + y^2 = r^2 \to^? y \leq h \quad \textbf{FALSE}$$

COUNTER-EXAMPLE: $-2 \leq -2 \wedge 3 + 1 = 4 \not\to -1 \leq -2$



On Annoying Assumptions

HOME › EXTREME › THE ESA HAS FIGURED OUT WHAT KILLED THE SCHIAPARELLI MARS LANDER

The ESA has figured out what killed the Schiaparelli Mars lander

By Jessica Hall on November 30, 2016 at 2:00 pm | 38 Comments

The Schiaparelli lander model

When the navigation system got wind of the IMU's wacky output, it decided that meant the spacecraft had "an estimated altitude that was negative" — that is, below ground level. In its scramble, the system released the backshell too early, fired the braking thrusters, and finally flicked on the on-ground systems as if Schiaparelli had already

Take-aways from Loitering Example

- Like loop invariants, differential invariants sometimes need **strengthening**.

Take-aways from Loitering Example

- Like loop invariants, differential invariants sometimes need **strengthening**.
- In these cases, try using differential cuts to **describe geometric constraints** on the system.

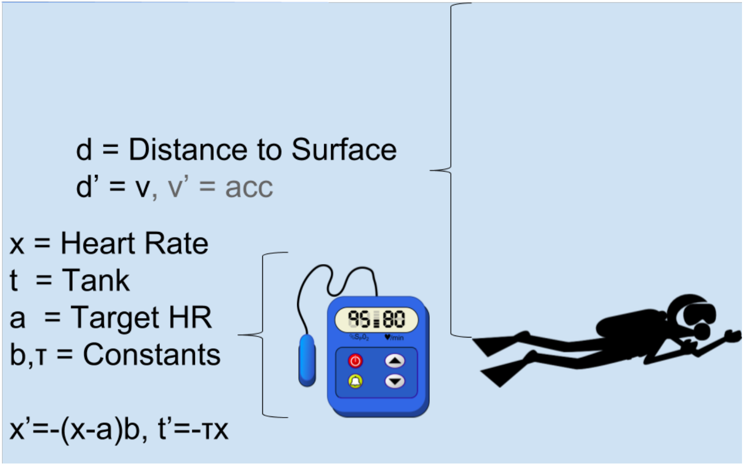
Take-aways from Loitering Example

- Like loop invariants, differential invariants sometimes need **strengthening**.
- In these cases, try using differential cuts to **describe geometric constraints** on the system.
- Most early proof attempts fail due to missing *obvious* assumptions:
  - Upper/lower-bounds (esp. positivity).
  - Missing $t' = 1$ in time-triggered systems.
  - Missing control epsilon $t \leq T$ in evolution domain.
  - Interesting dynamics (e.g., missing $v \geq 0$).

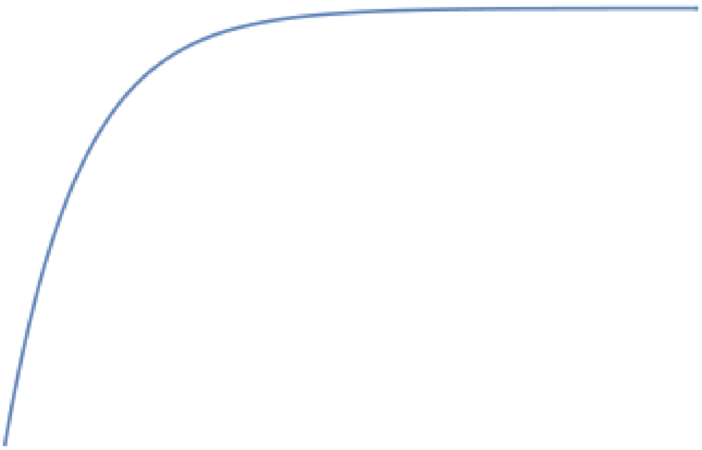
  Use counter-examples to find these errors.

Outline

Safe SCUBA diving



Heart Rate Function

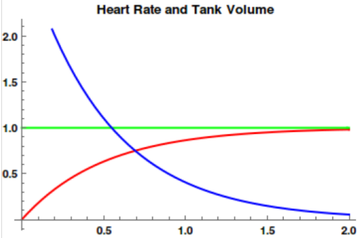


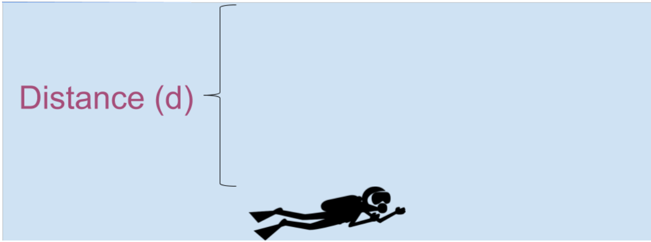
$$x' = -(x - HR_{max})b$$

SCUBA Ascent Case

Differential Program:

$$x' = -(x-a)b,$$
$$t' = -\tau x,$$
$$d' = v,$$
$$c' = 1$$
$$\& \; d \geq 0 \; \& \; c \leq C$$





Control Goal: Find a condition that ensures the diver reaches the surface before running out of oxygen.

SCUBA Proof Idea

$$x' = -(x - a)b, t' = -\tau x, d' = v, c' = C \;\;\&\;\; c \leq C \wedge d \geq 0$$

Idea: Bound time and all non-linear terms, then prove linear inequalities on these bounds by integrating.

SCUBA Proof Idea

$$x' = -(x-a)b, t' = -\tau x, d' = v, c' = C \;\;\&\;\; c \leq C \wedge d \geq 0$$

Idea: Bound time and all non-linear terms, then prove linear inequalities on these bounds by integrating.

- Non-linear term: $x \leq HR_{max}$

SCUBA Proof Idea

$$x' = -(x - a)b, t' = -\tau x, d' = v, c' = C \;\;\&\;\; c \leq C \wedge d \geq 0$$

Idea: Bound time and all non-linear terms, then prove linear inequalities on these bounds by integrating.

- Non-linear term: $x \leq HR_{max}$
- Bound time: $d_0 + vc \geq 0 \Rightarrow$ bound on time (denote as $z = \frac{-d}{v_0}$).

SCUBA Proof Idea

$$x' = -(x-a)b, t' = -\tau x, d' = v, c' = C \;\;\&\;\; c \leq C \wedge d \geq 0$$

Idea: Bound time and all non-linear terms, then prove linear inequalities on these bounds by integrating.

- Non-linear term: $x \leq HR_{max}$
- Bound time: $d_0 + vc \geq 0 \Rightarrow$ bound on time (denote as $z = \frac{-d}{v_0}$).

$$t = t_0 - \tau xc \geq t_0 - \tau HR_{max} c \geq \underbrace{t_0 - \tau HR_{max} z \geq 0}_{\text{Initial safe states!}}$$

SCUBA Proof Idea

$$x' = -(x-a)b, t' = -\tau x, d' = v, c' = C \;\;\&\;\; c \leq C \wedge d \geq 0$$

Idea: Bound time and all non-linear terms, then prove linear inequalities on these bounds by integrating.

- Non-linear term: $x \leq HR_{max}$
- Bound time: $d_0 + vc \geq 0 \Rightarrow$ bound on time (denote as $z = \frac{-d}{v_0}$).

$$t = t_0 - \tau xc \geq t_0 - \tau HR_{max} c \geq \underbrace{t_0 - \tau HR_{max} z \geq 0}_{\text{Initial safe states!}}$$

The first step requires $x \leq HR_{max}$. This is the only interesting lemma.

Computing the Differential Ghost

Let's prove $x < HR_{max}$ instead to avoid extra case splitting due to the $x = HR_{max}$ bifurcation point.

Computing the Differential Ghost

Let's prove $x < HR_{max}$ instead to avoid extra case splitting due to the $x = HR_{max}$ bifurcation point.

- Step 1: Find an existential condition equivalent to our goal:

$$\models_{\mathbb{R}C\mathcal{F}} x < HR_{max} \leftrightarrow \exists y.?$$

Computing the Differential Ghost

Let's prove $x < HR_{max}$ instead to avoid extra case splitting due to the $x = HR_{max}$ bifurcation point.

- Step 1: Find an existential condition equivalent to our goal:

$$\vDash_{\mathbb{R}\mathcal{CF}} x < HR_{max} \leftrightarrow \exists y.\ y^2(x - HRmax) = -1$$

Computing the Differential Ghost

Let's prove $x < HR_{max}$ instead to avoid extra case splitting due to the $x = HR_{max}$ bifurcation point.

- Step 1: Find an existential condition equivalent to our goal:

$$\models_{\mathbb{R}\mathcal{CF}} x < HR_{max} \leftrightarrow \exists y.\ y^2(x - HRmax) = -1$$

- Step 2: Find y' s.t. $(y^2(x - HR_{max}) = -1)'$ is true:

Computing the Differential Ghost

Let's prove $x < HR_{max}$ instead to avoid extra case splitting due to the $x = HR_{max}$ bifurcation point.

- Step 1: Find an existential condition equivalent to our goal:

$$\models_{\mathbb{R}C\mathcal{F}} x < HR_{max} \leftrightarrow \exists y.\ y^2(x - HRmax) = -1$$

- Step 2: Find y' s.t. $(y^2(x - HR_{max}) = -1)'$ is true:

$$\begin{aligned}
(y^2(x - HRmax) = -1)' &\equiv (y^2(x - HR_{max}))' = 0 \\
&\equiv 2yy'(x - HR_{max}) + y^2x' = 0 \\
&\equiv 2yy'(x - HR_{max} + y^2(-(x - a)b) = 0 \\
&\equiv \ldots \\
&\equiv y' = \frac{b}{2}y
\end{aligned}$$

(All equivalences are with respect to the ODE.)

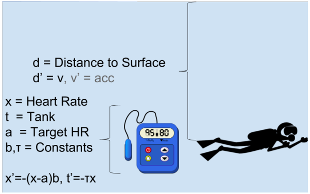
Take-aways from SCUBA Example

- As systems become harder to model, **parametric models** save the day.
- Identifying and using **differential ghosts** is (sometimes) systematic.
- **Partial solutions** to fragments of an ODE's dynamics are useful whenever you can upper-bound terms.
- Tactics $\Rightarrow$ proof reuse

Summary


STOP


Prohibited
Airspace
Google


d = Distance to Surface
d' = v, v' = acc
x = Heart Rate
t = Tank
a = Target HR
b,τ = Constants
x'=-(x-a)b, t'=-τx
95 80

Resources

Notes, slides, and examples from this talk:

`https://nfulton.org/marktoberdorf`

KeYmaera X website:

`https://keymaeraX.org`

Online Instance (**With Mathematica!**):

`https://web.keymaeraX.org`

Source Code (Scala):

`https://github.com/LS-Lab/KeYmaeraX-release`

KeYmaera X Credits: Stefan Mitsch, Jan-David Quesel, Marcus Völp, Brandon Bohrer, Yong Kiam Tan, André Platzer, . . .
SCUBA Credits: Karim Elmaaroufi and Viren Bajaj

Outline

The ODE Solver

To solve $x' = v, v' = a$:

- Add a time variable:

$$[x' = v, v' = a, t' = 1]P(x, v)$$

The ODE Solver

To solve $x' = v, v' = a$:

- Add a time variable:

$$[x' = v, v' = a, t' = 1]P(x, v)$$

- Use differential cuts to add solutions in linear order:

$$[x' = v, v' = a, t' = 1 \& v = at + v_0 \land x = \frac{at^2}{2} + v_0 t + x_0]P(x, v)$$

The ODE Solver

To solve $x' = v, v' = a$:

- Add a time variable:

$$[x' = v, v' = a, t' = 1]P(x, v)$$

- Use differential cuts to add solutions in linear order:

$$[x' = v, v' = a, t' = 1 \& v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0]P(x, v)$$

- Rewrite the post-condition in terms of t:

$$[x' = v, v' = a, t' = 1 \& v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0]P(t)$$

The ODE Solver

To solve $x' = v, v' = a$:

- Add a time variable:

$$[x' = v, v' = a, t' = 1]P(x, v)$$

- Use differential cuts to add solutions in linear order:

$$[x' = v, v' = a, t' = 1 \& v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0]P(x, v)$$

- Rewrite the post-condition in terms of t:

$$[x' = v, v' = a, t' = 1 \& v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0]P(t)$$

- Inverse differential ghosts to remove all equations except time:

$$[t' = 1 \& v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0]P(t)$$

The ODE Solver

To solve $x' = v, v' = a$:

- Add a time variable:

$$[x' = v, v' = a, t' = 1]P(x, v)$$

- Use differential cuts to add solutions in linear order:

$$[x' = v, v' = a, t' = 1 \& v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0]P(x, v)$$

- Rewrite the post-condition in terms of t:

$$[x' = v, v' = a, t' = 1 \& v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0]P(t)$$

- Inverse differential ghosts to remove all equations except time:

$$[t' = 1 \& v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0]P(t)$$

- Use univariate solve:

$$\forall s \forall 0 \leq t \leq s. v = at + v_0 \wedge x = \frac{at^2}{2} + v_0 t + x_0 \rightarrow P(t)$$

Taylor Approximations in KeYmaera X

$$s' = c, c' = -s$$

$$\begin{aligned} s = \mathit{sin}\ x &= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots \\ c = \mathit{cos}\ x &= 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots \end{aligned}$$

Taylor Approximations in KeYmaera X

$$s' = c, c' = -s, x' = 1$$

$$s = sin\ x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots$$
$$c = cos\ x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots$$