« Cyber-Physical Systems (CPS) Seminar »

Albert Rizaldi

January 30, 2017

Two classes of formal verification techniques in CPS

1. Automated — for example reachability analysis
   - push button technology
   - no need of specific knowledge
   - no need of guidance
   - state space explosion problem
2. Manual — for example theorem proving in KeYmaera
   - interactive with proof system
   - require specific knowledge
   - require guidance
   - limited only to your knowledge

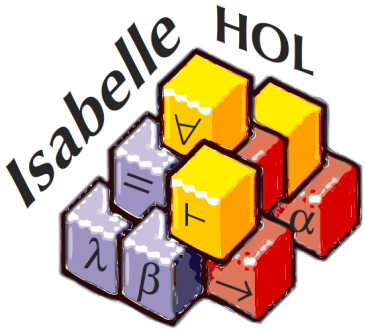
Formal verification underlying the proposed topics

We combine both techniques: formalising automated verification technique in a generic theorem prover.

General requirements for these topics

Familiarity with

- Interactive theorem prover
- Functional programming
- Mathematics: linear algebræ, topology, analysis, etc.

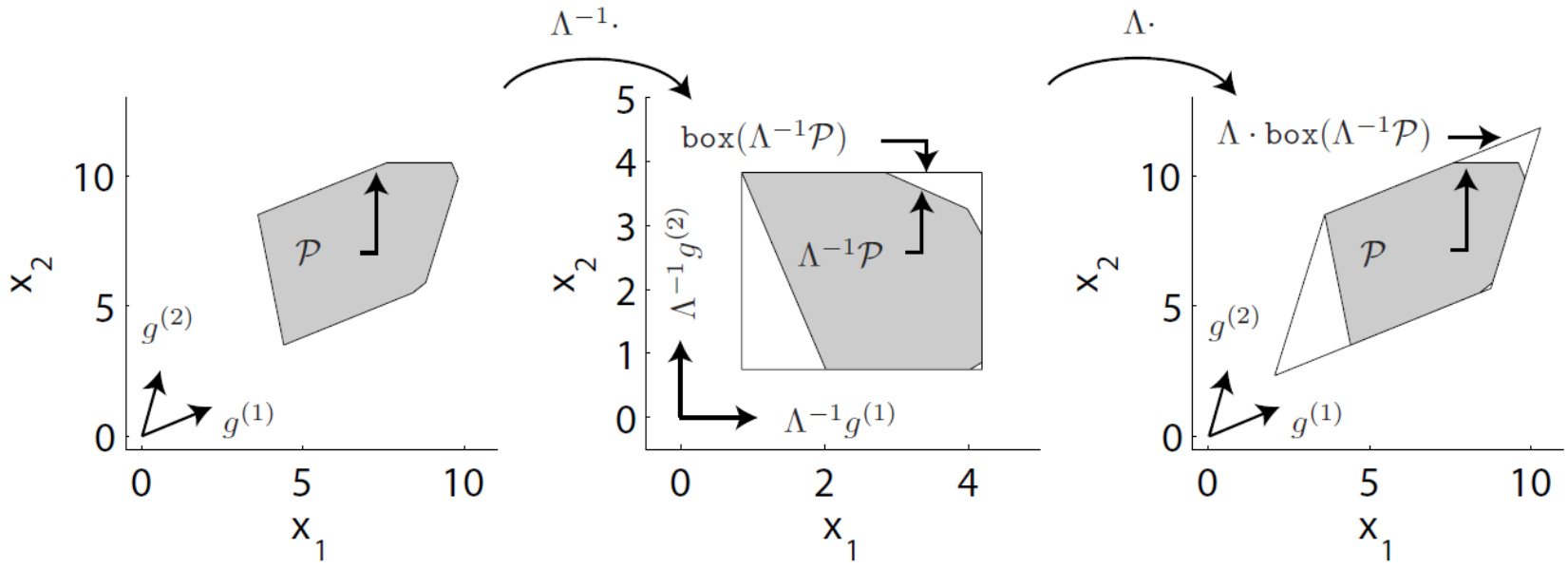




Not allergic to

- Logics
- Formal proofs

1st topic — Isabelle's proof of polytope enclosure



Theorem

An over-approximating parallelotope Ψ *of a polytope* $\mathcal{P}$ *is obtained as :* $\Psi = \Lambda \cdot box(\Lambda^{-1}\mathcal{P})$.

Theorem (In Isabelle)

lemma $\mathcal{P} \subseteq \Lambda \times box(\mathsf{inv}\,\Lambda \times \mathcal{P})$ *when* Λ *is of full rank.*

2^{nd} topic — Affine arithmetic of matrix inverse

Motivating example:

```
B = [117                 , 822.2940998481383;
     822.2940998481383, 5783.81879511911];

B * B^-1

ans =
     1.000000000000026  -0.000000000000008
    -0.000000000000242   0.999999999999994
```

Floating-point numbers has finite precision while real numbers infinite!

2nd topic — Affine arithmetic of matrix inverse

- Meet affine arithmetic

  Each variable X is interpreted as a set of values instead of a single value.

$$X = X_0 + \sum_{i=1}^{n} w_i \cdot \epsilon_i \qquad \text{with } w_i \in [-1; 1]$$

- Proposed solution

  To use affine arithmetic library in Isabelle/HOL for finding inverse of a matrix.

- Your tasks

  Find the matrix inverse of 4×4 matrix and prove its correctness!

3rd topic — Refactoring the correctness proofs of finding extreme points

Given a parallelotope

$$X = X_0 + \sum_{i=1}^{n} w_i \cdot \epsilon_i \qquad \text{with } w_i \in [-1; 1]$$

the extreme points can be found by enumerating all 1 and -1 combinations for each w_i.

Mathematically speaking,

$$x_0 \in \mathit{set}\ (\text{point-of-aform } X) \Longrightarrow x_1 \in \text{ Affine } X \Longrightarrow \ldots$$
$$x_2 \in \text{ Affine } X \Longrightarrow \forall l \in [0; 1].\quad l \cdot x1 + (1 - l) \cdot x2 \neq x0$$

3rd topic — Refactoring the correctness proofs of finding extreme points

- Current status

  I have proved the correctness proof of this theorem;

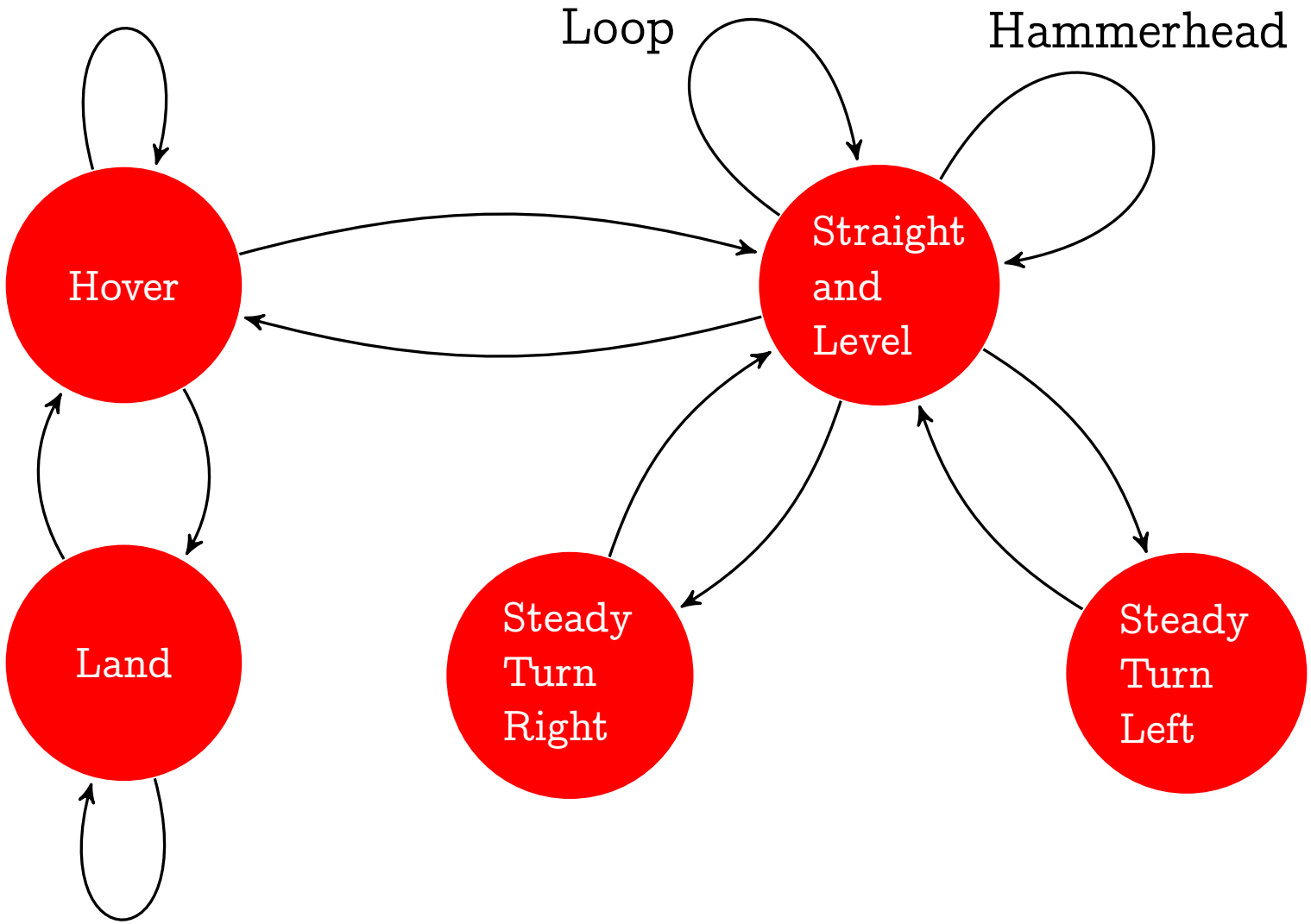
- Problem definition

  Unfortunately, I have done this before the new release of Isabelle 2016-1. In the new release, there are many formalisation regarding extreme points of polytope, parallelotope, etc;

- Your task

  Refactor the proof using as many definitions and theorems in Isabelle 2016-1 as possible.

4^{th} topic — Refactoring proofs about Manœuvre Automata and its LTL interpretation



4^{th} topic — Refactoring proofs about Manœuvre Automata and its LTL interpretation

- Current status

  I have formalised Manœuvre Automata in Isabelle/HOL;

- Problem definition

  Fabian Immler — the main person behind the formalisation of reachability analysis in Isabelle/HOL — has updated his formalisation in the new Archive of Formal Proofs (AFP) 2016;

- Your task
  - Refactor the proof using as many definitions and theorems in AFP 2016 as possible.
  - Formalise the LTL interpretation over MA — Hannes last CPS seminar's work.

Timeline for the seminar

The time for doing this seminar is roughly two-and-half months:

1. First month

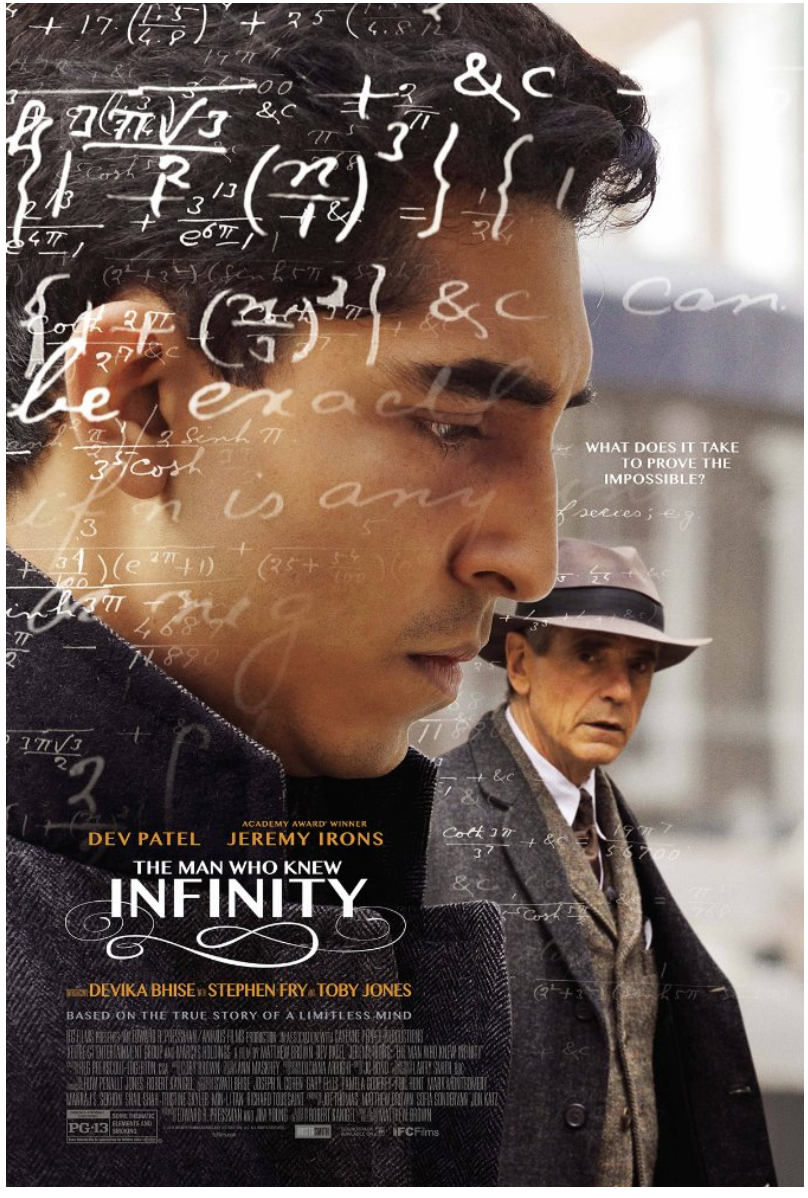
   familiarising yourself with Isabelle/HOL theorem prover — trying and experiment under my guidance

2. Second month

   formalise the theorems specific to your topic

3. Rest of the weeks

   preparing presentation, presenting your work, and writing your report

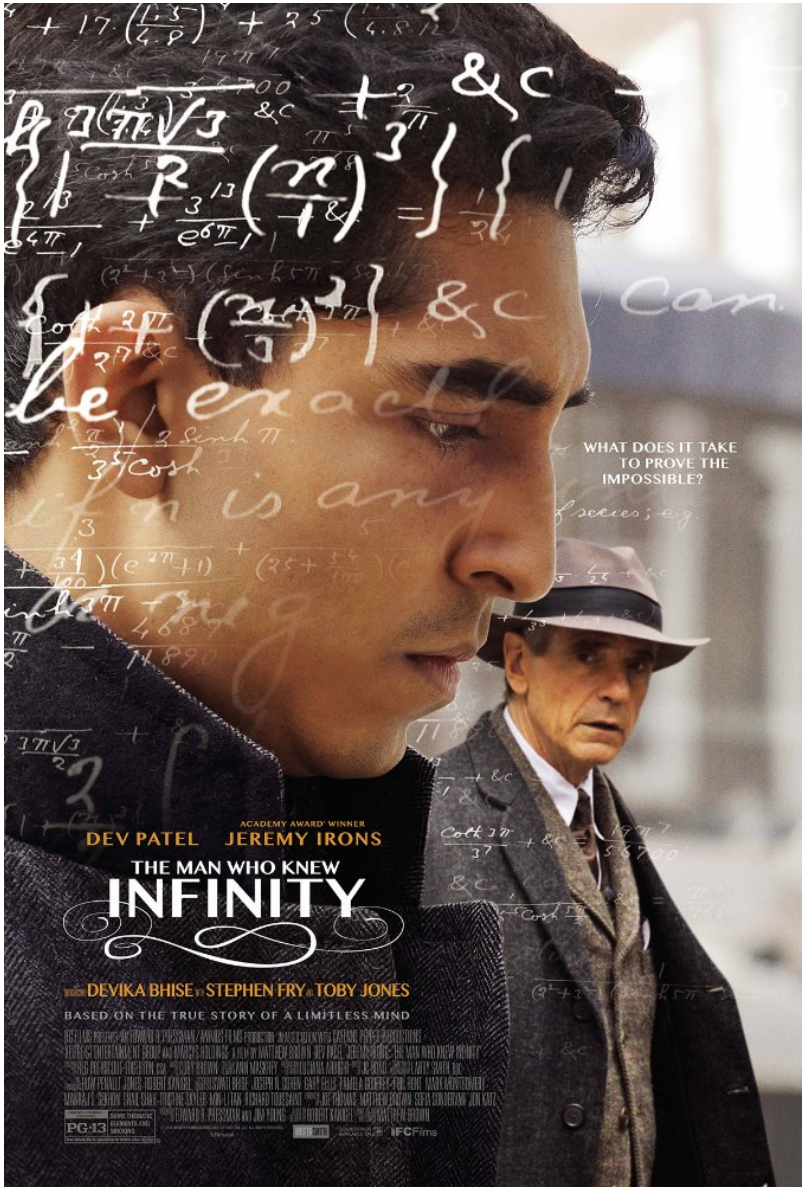


RAMANUJAN

Mr. Hardy, I don't understand why we waste our time doing all these proofs. I have the formulas.

HARDY

It's not that I can't see what you've claimed. It's that I'm not sure that you know how you got there or, indeed, that your claims are correct. There are subtleties which...



RAMANUJAN
But they are right, sir.
I have more important new ideas.

HARDY
Yes, but intuition is not enough. It has to be held accountable.