Candidature pour allocation doctorale

Quentin Garchery

Mardi 12 juin 2018

Cursus universitaire: 2009-2016

- 2009-2011 : MPSI à Jeanne d'Albret et MP* à Louis-le-Grand
- 2011-2016 : ÉNS Cachan, antenne de Bretagne
  Stage de juin à juillet 2012 à l'IMJ :
  Théorie additive des nombres, Eric Balandraud
  Stage de mai à juin 2014 à l'IMJ :
  Représentation de groupes, Olivier Brunat
- 2014-2015 : Préparation à l'agrégation de mathématiques
  rang 66^{e} sur 274 admis
- 2015-2016 : M2 mathématiques fondamentales à Paris Diderot
  Stage de mai à août 2016 chez Eonos :
  Algèbres de Clifford et application en informatique, Thomas Dionysopoulos
  Programmation en Bash et en R

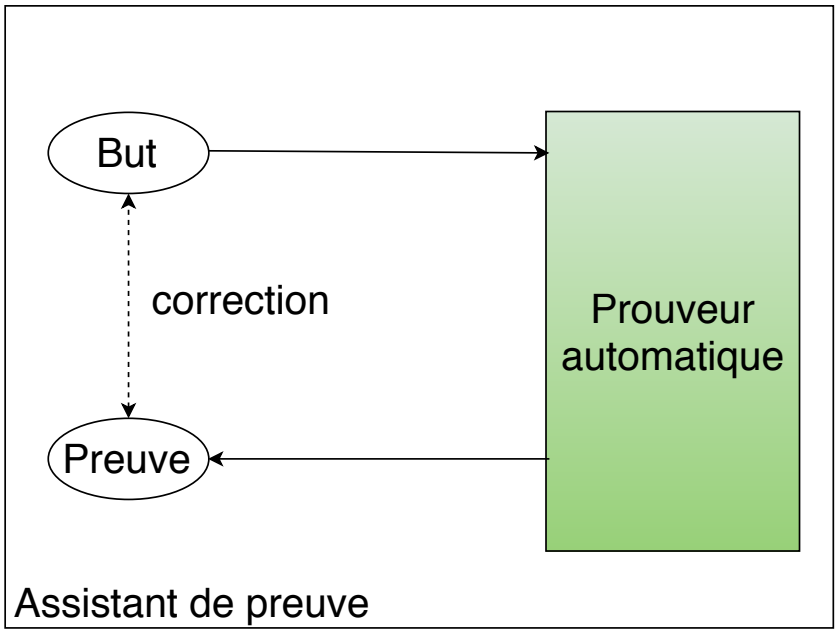
Cursus universitaire: 2016-2018

- 2016-2017 : M1 Informatique parcours recherche à Paris Diderot
  Travail de Recherche Encadré de mars à juin 2017 :
  Les systèmes distribués, Gustavo Petri et Constantin Enea
  Vérification grâce à Alloy

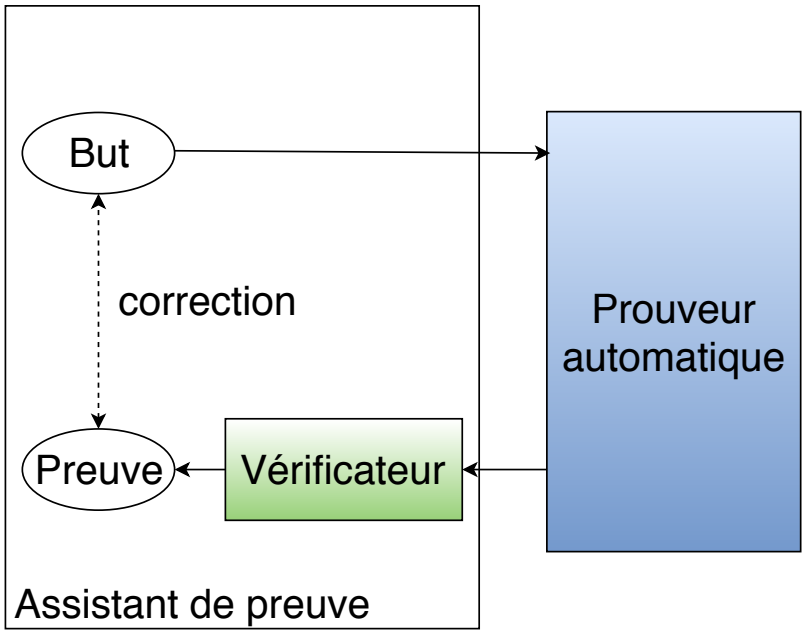
- 2017-2018 : M2 MPRI à Paris Diderot
  Stage de mars à août 2018 au LRI :
  Démonstration automatique en Coq, Chantal Keller et Valentin Blot
  Programmation en OCaml et en Coq

Automatisation des assistants de preuve

Les prouveurs automatiques : une source d'automatisation pour les assistants de preuve.



Approche autarcique : vérifier le code du prouveur automatique.



Approche sceptique : vérifier la réponse du prouveur automatique à chaque appel de celui-ci.

Présentation de SMTCoq

SMTCoq : une interface sceptique aux différents prouveurs automatiques initialement développée par Chantal Keller puis en collaboration avec l'université d'Iowa.

But : amélioration de l'automatisation de Coq et de la confiance dans les prouveurs automatiques.

Sait prouver automatiquement le théorème suivant :

$$\forall x \forall y.(x < 7) \vee (y < 4) \vee (x + y \geq 11)$$

Amélioration de l'expressivité

SMTCoq ne sait pas montrer que :

$$\forall h.homme(h) \Rightarrow mortel(h)$$

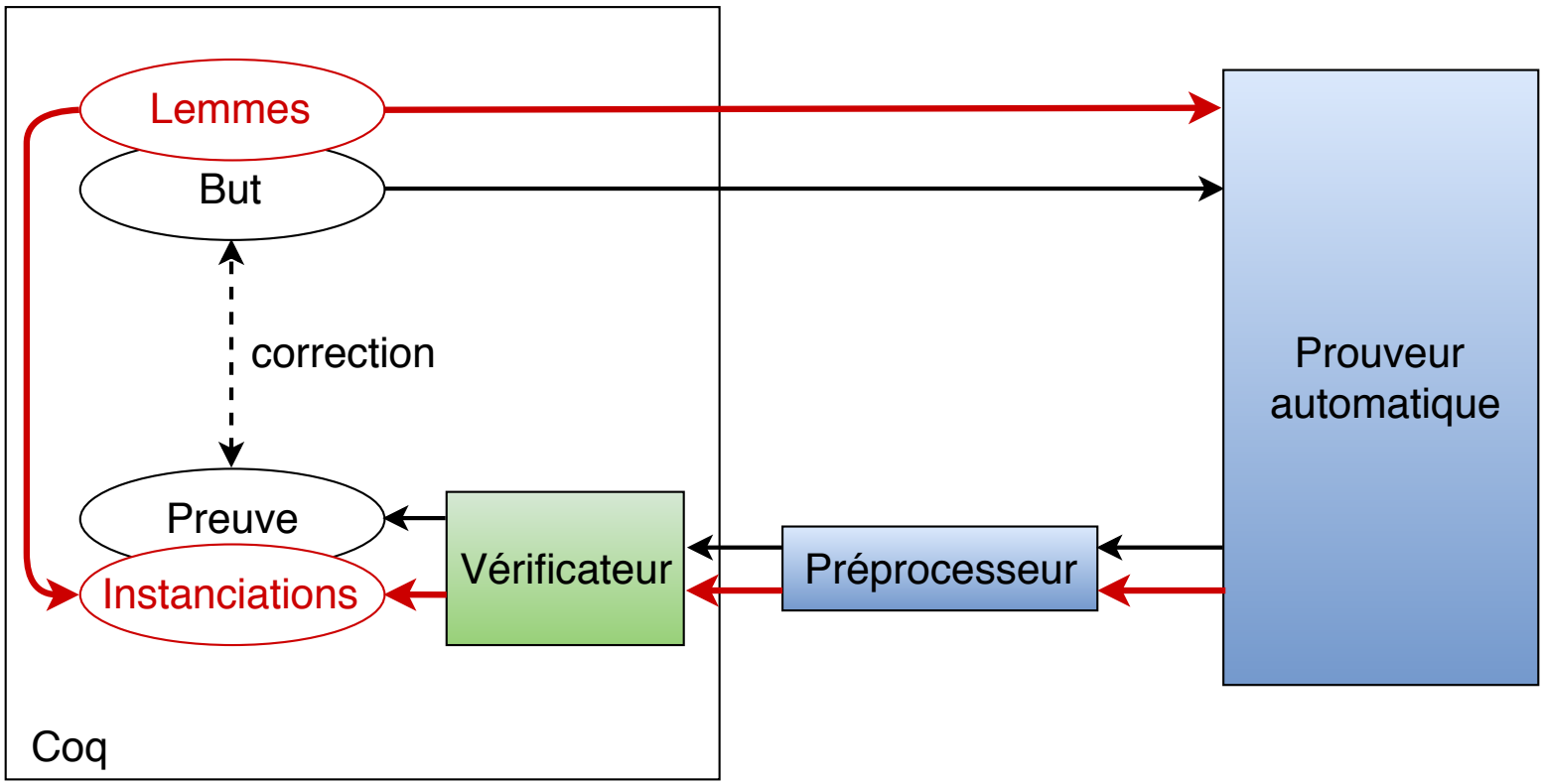
$$homme(Socrate)$$

implique :

$$mortel(Socrate)$$

Objectifs du stage : permettre l'ajout de lemmes quantifiés au contexte et tenir compte de leurs instanciations dans le certificat.

Ajout de lemmes au contexte



Résultats du stage

Vérificateur : s'appuie sur une preuve calculatoire en Coq.

Théorème de correction

$\forall c.\quad \mathit{checker}\ l\ c = \mathit{true} \quad \Rightarrow \quad \mathit{interp}\ l$

Un exemple en Coq :

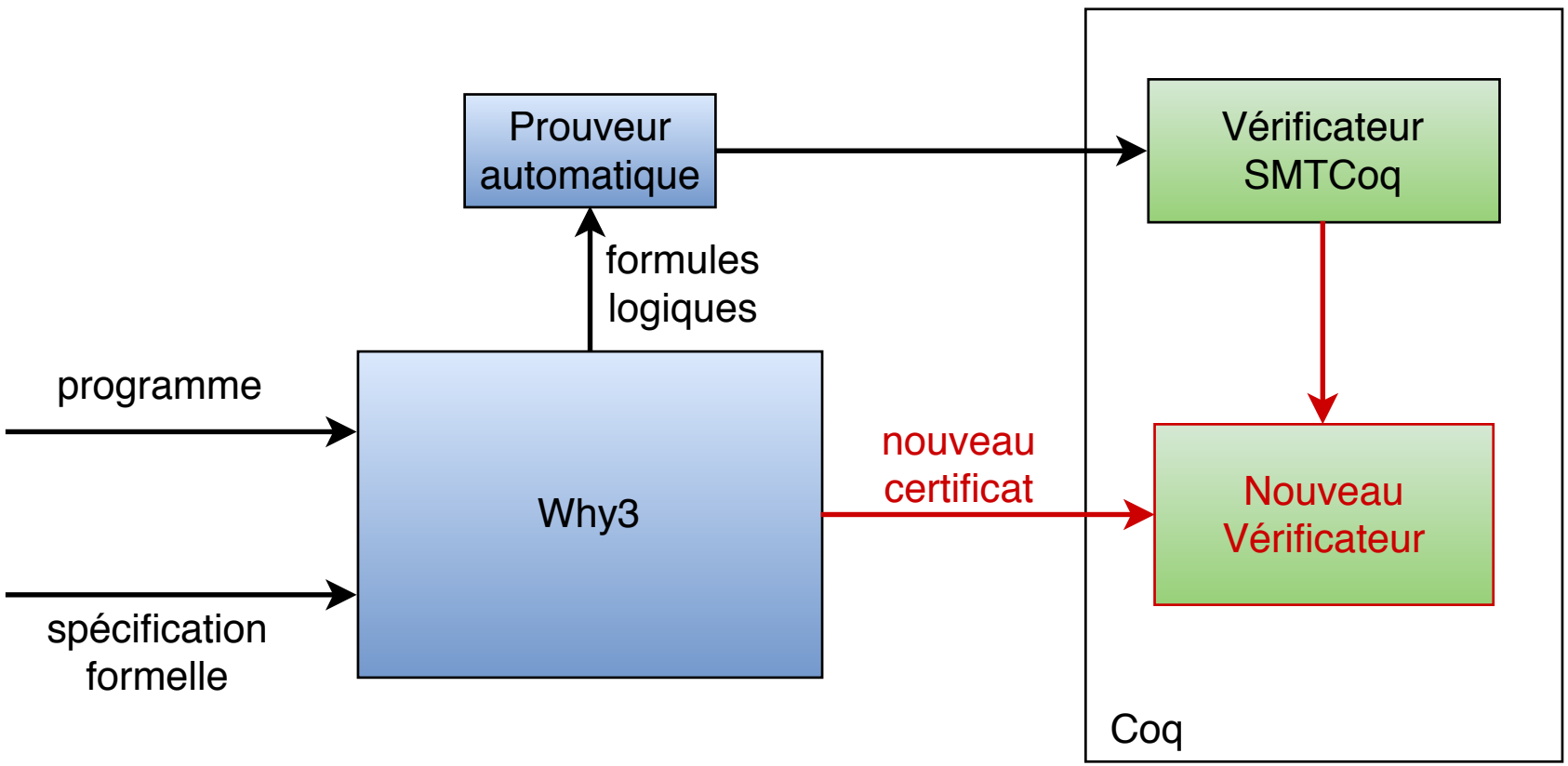
```
Axiom hommes_mortels : forall h, homme h --> mortel h.
Axiom homme_Socrate : homme Socrate.

Lemma mortel_Socrate :
  mortel Socrate.

Proof.
  verit hommes_mortels homme_Socrate.
Qed.
```

$\longrightarrow$ github.com/QGarchery/smtcoq-1

Objectifs de la thèse

- Améliorer la confiance dans les outils de vérification déductive
- Vérification de programmes par l'approche sceptique
- Développement d'outils de preuve de programmes comme Why3

Génération et vérification de certificats



Motivations personnelles

- Certification : dans la continuité du sujet de stage.
- EJCP 2018 à Lyon.
- Sujet informatique en lien fort avec les mathématiques.

Cadre de la thèse

Certification de la génération et la transformation d'obligations de preuve

Claude Marché, Chantal Keller et Andrei Paskevich

S'inscrit dans une collaboration entre le LRI et le CEA LIST sur la certification d'outils d'analyse de code C critique.