Le projet BWare

Une plate-forme pour la vérification automatique d'obligations de preuve B

David Delahaye[1] Claude Marché[2]

David Mentré[3]

[1]Cnam / Cedric / Inria, Paris

[2]Inria Saclay - Île-de-France & LRI, CNRS, Univ. Paris-Sud, Orsay

[3]Mitsubishi Electric R&D Centre Europe, Rennes

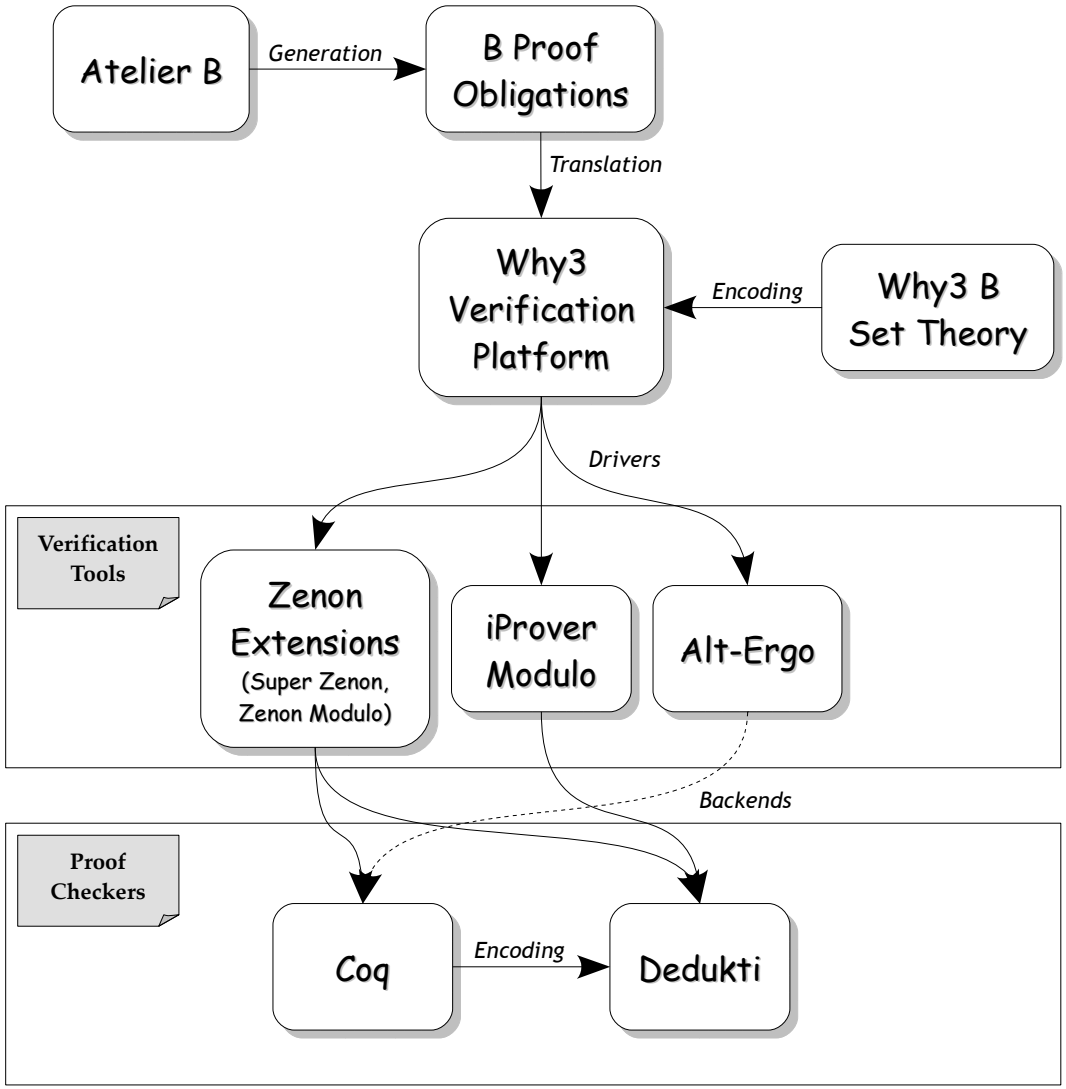
Le projet BWare

- Programme « Ingénierie Numérique & Sécurité » de l'ANR ;
- Partenaires académiques : Cnam, LRI, Inria ;
- Partenaires industriels : Mitsubishi Electric R&D Centre Europe, ClearSy, OCamlPro.

Objectifs

- Environnement pour la vérification automatique d'OP B ;
- Plate-forme générique (basée sur Why3) ;
- Outils au premier ordre (Zenon, iProver Modulo) ;
- Solveurs SMT (Alt-Ergo) ;
- « Backends » (Coq, Dedukti).

Le projet BWare



Résultats préliminaires

BWare

Résumé compact

- Environ 10,500 OP (fournies par ClearSy et Mitsubishi).

mp	Alt-Ergo	iProver Modulo	Zenon
84%	58%	19%	< 1%

Observations

- Bons résultats pour Alt-Ergo, mais à améliorer (mp) ;
- Difficultés pour le premier ordre (iProver Modulo et Zenon).

Axes de travail

BWare

Travail sur Alt-Ergo

- Versions améliorées d'Alt-Ergo ;
- 98% des OP prouvées (mp supplanté) ;
- Référence :

  S. Conchon, M. Iguernelala. *Tuning the Alt-Ergo SMT Solver for B Proof Obligations.* ABZ (2014).

Extension à la déduction modulo

- Extension de Zenon à la déduction modulo ;
- Intégration de théories au moyen de règles de réécriture ;
- Théorie des ensembles de B comme une théorie modulo.

Extension de Zenon à la déduction modulo

BWare

Objectifs

- Améliorer la recherche de preuve dans les théories ;
- Réduire la taille des preuves ;
- Nouvel outil : Zenon + déduction modulo = Zenon Modulo !
  `https://www.rocq.inria.fr/deducteam/ZenonModulo/`

Benchmarks (TPTP)

- Amélioration des résultats de Zenon ;
- Environ 50% dans la catégorie SET ;
- Preuve d'environ 30 problèmes difficiles ;
- Référence :

  D. Delahaye, D. Doligez, F. Gilbert, P. Halmagrand, O. Hermant. *Zenon Modulo : When Achilles Outruns the Tortoise using Deduction Modulo.* LPAR (2013).

Théorie des ensembles de B modulo

BWare

Règles

Axiomes de la théorie des ensembles

$$x \in s \times t \longrightarrow \pi_1 x \in s \wedge \pi_2 x \in t$$
$$s \in \mathbb{P}(t) \longrightarrow \forall x\ (x \in s \Rightarrow x \in t)$$
$$s = t \longrightarrow \forall x\ (x \in s \Leftrightarrow x \in t)$$
$$\text{choice}(s) \in s \longrightarrow \exists x\ (x \in s)$$

Inclusion ensembliste

$$s \subseteq t \longrightarrow s \in \mathbb{P}(t) \qquad s \subset t \longrightarrow s \subseteq t \wedge s \neq t$$

Constructions dérivées

$$x \in s \cup t \longrightarrow x \in s \vee x \in t \qquad x \in s \cap t \longrightarrow x \in s \wedge x \in t$$
$$x \in s - t \longrightarrow x \in s \wedge x \notin t \qquad x \in \emptyset \longrightarrow \bot$$
$$x \in \{a\} \longrightarrow x = a \qquad \mathbb{P}_1(s) \longrightarrow \mathbb{P}(s) - \{\emptyset\}$$

Benchmarks

BWare

Résultats récents

- Propriétés du B-Book (chap. 2) : 319 propriétés.

Zenon	Zenon Modulo	iProver	iProver Modulo	Vampire	E
6	245	68	248	76	48
1.9%	76.8%	21.3%	77.7%	23.8%	15%

- Vérification des preuves par Dedukti :
  - 245 preuves vérifiées pour Zenon Modulo (100%) ;
  - 233 preuves vérifiées pour iProver Modulo (94%).

Autres axes de travail

BWare

Outils basés sur la déduction modulo

- Application à la collection d'OP ;
- Extension à l'arithmétique (en cours pour Zenon) ;
- Outils alternatifs : Zipperposition avec ensembles.

Encodage Why3 de la théorie de B

- Considérer toutes les OP fournies ;
- Ajouter des constructions B à l'axiomatisation ;
- Modifier le traducteur d'OP de l'Atelier B vers Why3.

Autres axes de travail

Benchmarks complets

- Intégration de plus de projets de développement ;
- Taux de couverture de preuve de la plate-forme.

Intégration à l'Atelier B

- Dissémination and exploitation des résultats ;
- Sortie multi-outils de vérification pour l'Atelier B.

Une architecture basée sur OCaml

- Outils pour le « profiling » mémoire ;
- OCaml multi-runtime.