The BWare Project

Building a Proof Platform for the Automated Verification of B Proof Obligations

David Delahaye[1] Catherine Dubois[2]

Claude Marché[3] David Mentré[4]

[1] Cnam / Cedric / Inria, Paris, France

[2] ENSIIE / Cedric / Inria, Évry, France

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

[4] Mitsubishi Electric R&D Centre Europe, Rennes, France

Presentation

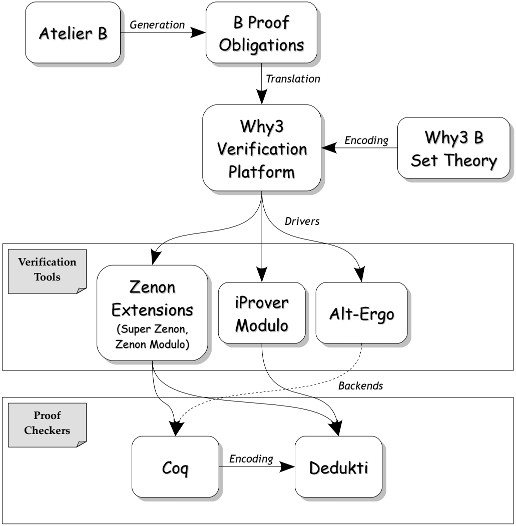
The BWare Project

- INS prog. of the French National Research Agency (ANR);
- Academic entities: Cnam, LRI, Inria;
- Industrial partners: Mitsubishi Electric R&D Centre Europe, ClearSy, OCamlPro.

Goals

- Mechanized framework for automated verification of B PO;
- Generic platform (based on Why3);
- First order ATP (Zenon, iProver Modulo);
- SMT solvers (Alt-Ergo);
- Backends (Coq, Dedukti).

The BWare Project



Preliminary Results

Compact Summary

- About 10,500 PO (provided by ClearSy and Mitsubishi).

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

Observations

- Good results for Alt-Ergo, but to be improved (mp);
- Difficulties for first order tools (iProver Modulo and Zenon).

Lines of Work

Work over Alt-Ergo

- Improved versions of Alt-Ergo;
- 98% of the PO proved (mp superseded);
- Reference:

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

  See the talk on Friday!

Extension to Deduction Modulo

- Extension of Zenon to deduction modulo;
- Integration of theories by means of rewrite systems;
- Formulation of the B set theory as a theory modulo.

Extension of Zenon to Deduction Modulo

Goals

- Improve the proof search in theories;
- Reduce the proof size;
- New tool: Zenon + deduction modulo = Zenon Modulo!
  `https://www.rocq.inria.fr/deducteam/ZenonModulo/`

Benchmarks (TPTP)

- Improvement of the results of Zenon;
- About 50% in the SET category;
- Proof of about 30 difficult problems;
- Reference:

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

  See P. Halmagrand's talk yesterday (SETS 2014)!

B Set Theory Modulo

Rules

Axioms of Set Theory

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

Set Inclusion

$$\begin{array}{rlrl}
s \subseteq t & \longrightarrow s \in \mathbb{P}(t) & s \subset t & \longrightarrow s \subseteq t \wedge s \neq t
\end{array}$$

Derived Constructs

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

Benchmarks

Recent Results

- Properties of the B-Book (Chap. 2): 319 properties.

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%

- Verification of the proofs by Dedukti:
  - 245 proofs verified for Zenon Modulo (100%);
  - 233 proofs verified for iProver Modulo (94%).
- Reference:

  G. Burel, D. Delahaye, D. Doligez, P. Halmagrand, O. Hermant. *Automated Deduction in the B Set Theory using Deduction Modulo.* Submitted (2014).

Other Lines of Work

Deduction Modulo Based Tools

- Application to the collection of PO;
- Extension to arithmetic (current work for Zenon);
- Alternative tools: Zipperposition with sets.

Why3 Encoding

- Consider all the provided PO;
- Add B constructs to the axiomatization;
- Modify the translator of PO from Atelier B to Why3.

Other Lines of Work

Extensive Benchmarking

- Integration of more development projects;
- Proof coverage ratio of the platform.

Integration to Atelier B

- Dissemination and exploitation of the results;
- Multi-prover output of Atelier B.

A Full OCaml-Based Architecture

- Memory usage profiling;
- Multi-runtime OCaml.