The BWare Project

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

David Delahaye\textsuperscript{1} \quad Catherine Dubois\textsuperscript{2}

Claude Marché\textsuperscript{3} \quad David Mentré\textsuperscript{4}

\textsuperscript{1}Cnam / Cedric / Inria, Paris, France

\textsuperscript{2}ENSIIE / Cedric / Inria, Évry, France

\textsuperscript{3}Inria Saclay - Île-de-France & LRI, CNRS, Univ. Paris-Sud, Orsay, France

\textsuperscript{4}Mitsubishi Electric R&D Centre Europe, Rennes, France
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

- **Atelier B**
  - **Generation**
  - **B Proof Obligations**
  - **Translation**
  - **Why3 Verification Platform**
  - **Drivers**
  - **Verification Tools**
  - **Zenon Extensions** (Super Zenon, Zenon Modulo)
  - **iProver Modulo**
  - **Alt-Ergo**
  - **Backends**
  - **Proof Checkers**
  - **Coq**
  - **Dedukti**

- **Why3 B Set Theory**
  - **Encoding**

- **Presentation**
  - Preliminary Results
  - Lines of Work
  - Deduction Modulo
  - Other Lines of Work

ABZ’14
June 4, 2014
Toulouse, France
Preliminary Results

Compact Summary

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

<table>
<thead>
<tr>
<th></th>
<th>mp</th>
<th>Alt-Ergo</th>
<th>iProver Modulo</th>
<th>Zenon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Results</td>
<td>84%</td>
<td>58%</td>
<td>19%</td>
<td>&lt; 1%</td>
</tr>
</tbody>
</table>

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- 98% of the PO proved (mp superseded);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:

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:
  See P. Halmagrand’s talk yesterday (SETS 2014)!
B Set Theory Modulo

Rules

Axioms of Set Theory

\[ x \in s \times t \quad \rightarrow \quad \pi_1 x \in s \land \pi_2 x \in t \]
\[ s \in \mathcal{P}(t) \quad \rightarrow \quad \forall x \ (x \in s \Rightarrow x \in t) \]
\[ s = t \quad \rightarrow \quad \forall x \ (x \in s \iff x \in t) \]
\[ \text{choice}(s) \in s \quad \rightarrow \quad \exists x \ (x \in s) \]

Set Inclusion

\[ s \subseteq t \quad \rightarrow \quad s \in \mathcal{P}(t) \]
\[ s \subset t \quad \rightarrow \quad s \subseteq t \land s \neq t \]

Derived Constructs

\[ x \in s \cup t \quad \rightarrow \quad x \in s \lor x \in t \]
\[ x \in s \setminus t \quad \rightarrow \quad x \in s \land x \notin t \]
\[ x \in \{a\} \quad \rightarrow \quad x = a \]
\[ x \in \emptyset \quad \rightarrow \quad \bot \]
\[ \mathcal{P}_1(s) \quad \rightarrow \quad \mathcal{P}(s) - \{\emptyset\} \]
Benchmarks

Recent Results

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

<table>
<thead>
<tr>
<th></th>
<th>Zenon</th>
<th>Zenon Modulo</th>
<th>iProver</th>
<th>iProver Modulo</th>
<th>Vampire</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zenon</td>
<td>6</td>
<td>245</td>
<td>68</td>
<td>248</td>
<td>76</td>
<td>48</td>
</tr>
<tr>
<td>Zenon Modulo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iProver</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iProver Modulo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vampire</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.9%</td>
<td>76.8%</td>
<td>21.3%</td>
<td>77.7%</td>
<td>23.8%</td>
<td>15%</td>
<td></td>
</tr>
</tbody>
</table>

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

- Reference:
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.