Tableaux Modulo Theories using Superdeduction

An Application to the Verification of B Proof Rules with the Zenon Automated Theorem Prover

David Delahaye

David.Delahaye@cnam.fr

CPR Team / Deducteam
(CEDRIC / Inria)

CPR / Deducteam Seminar

Inria, Paris
June 8, 2012

Introduction

Collaboration with Siemens (IC-MOL)

- M. Jacquel's PhD thesis, superv. by K. Berkani, D. Delahaye, C. Dubois ;
- VAL, automatic metro systems, optical guidance for buses/trolleybuses ;
- Meteor line (line 14) at Paris, opened 13 years ago.

Use of the B Method

The B Method

- Defined in the B-Book (1996) by J.-R. Abrial ;
- Based on a (typed) set theory ;
- Generation of executable code which conforms to formal specifications ;
- Notion of machines, which are refined until implementations ;
- Generation of proof obligations (consistency, refinement) ;
- Supporting tool : Atelier B (ClearSy).

Proof Activity with Atelier B

- Automated proofs (pp) ;
- Interactive proofs :
  - Apply some tactics ;
  - Add some rules (axioms).
- If the added rule is wrong then :
  - The proof of the proof obligation may be unsound ;
  - The generated code may contain some bugs.

Use of the B Method

The B Method

- Defined in the B-Book (1996) by J.-R. Abrial ;
- Based on a (typed) set theory ;
- Generation of executable code which conforms to formal specifications ;
- Notion of machines, which are refined until implementations ;
- Generation of proof obligations (consistency, refinement) ;
- Supporting tool : Atelier B (ClearSy).

Figures

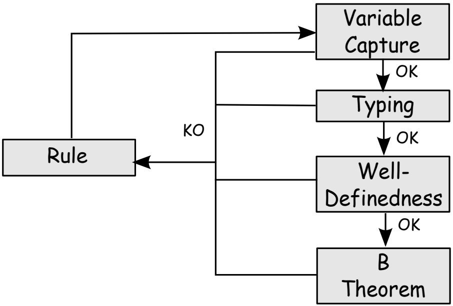
- Meteor : 27,800 proof obligations, 1,400 added rules ;
- Currently about 5,300 rules in the rule database of Siemens.

Rule Verification

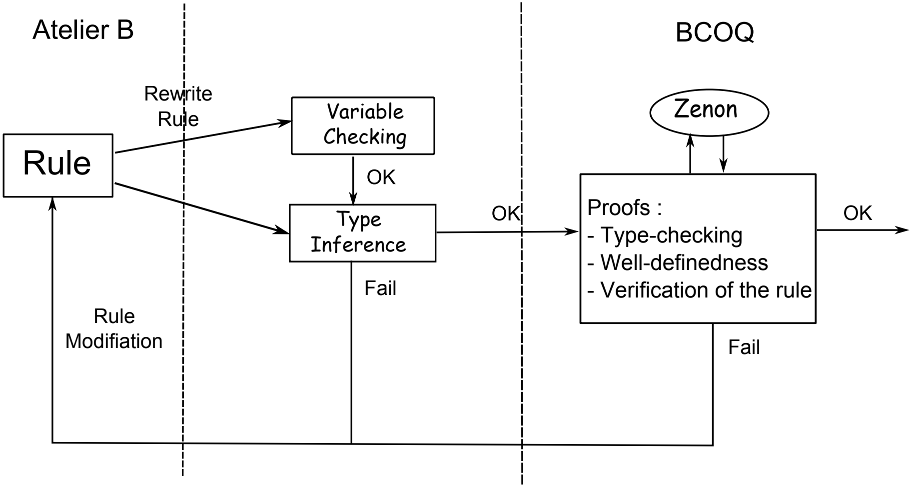
Rules

- Set formulas with metavariables and guards ;
- Deduction rule :
  InSetXY : binhyp($f \in A \mathrel{+\!\!\!\rightarrow} B$) $\wedge$ $(a \in \mathrm{dom}(f)) \wedge (f(a) \in u) \Rightarrow (a \in f^{-1}[u])$
- Rewrite rule :
  Associativity : $a \cup (b \cup c) == a \cup b \cup c$

Verification Process



The BCARe Environment



Automated Verification of Rules

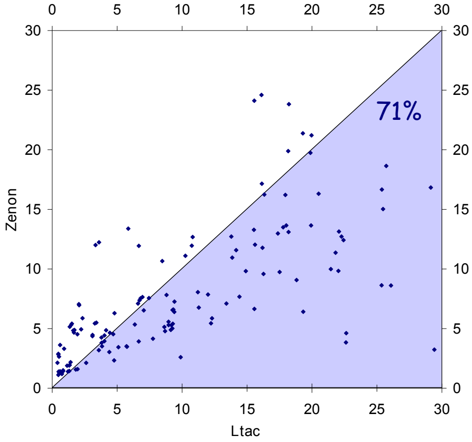
$\mathcal{L}_{tac}$ Approach

- Proof algorithm written in Coq using $\mathcal{L}_{tac}$;
- Preliminary normalization to get rid of set constructs ;
- Naive and incomplete heuristic ;
- No unification, no contraction.

Zenon Approach

- Use of a complete and efficient ATP ;
- Preliminary normalization (as previously) ;
- Unreification of formulas required ;
- Rereification of the generated Coq proofs.

Derived Rules



Proof Times using Zenon and $\mathcal{L}_{tac}$ (in s)

Benchmarks

Figures

- Derived rules of the B-Book :
  - For 71% of the rules of the graph, Zenon is faster than $\mathcal{L}_{tac}$;
  - Over 200 tested derived rules, 15 of them cannot be proved using $\mathcal{L}_{tac}$.
- Added rules of the rule database of Siemens :
  - 1735 tested rules (only rules with set operators) ;
  - 1269 rules (73%) proved by the Zenon approach ;
  - 804 rules (46%) proved by the $\mathcal{L}_{tac}$ approach.
- See the SEFM'11 paper for more details.

Problems

- Incomplete approaches (preliminary normalization) ;
- Weak performances in terms of time (preliminary normalization).

Deduction Modulo and Superdeduction

Inclusion

$$\forall a \forall b\,((a \subseteq b) \Leftrightarrow (\forall x\,(x \in a \Rightarrow x \in b)))$$

Proof in Sequent Calculus

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{\ldots, x \in A \vdash A \subseteq A, x \in A}\,\mathrm{Ax}}{\ldots \vdash A \subseteq A, x \in A \Rightarrow x \in A}\,{\Rightarrow}\mathrm{R}}{\ldots \vdash A \subseteq A, \forall x\,(x \in A \Rightarrow x \in A)}\,\forall\mathrm{R} \qquad \cfrac{}{\ldots, A \subseteq A \vdash A \subseteq A}\,\mathrm{Ax}}{\ldots, (\forall x\,(x \in A \Rightarrow x \in A)) \Rightarrow A \subseteq A \vdash A \subseteq A}\,{\Rightarrow}\mathrm{L}}{A \subseteq A \Leftrightarrow (\forall x\,(x \in A \Rightarrow x \in A)) \vdash A \subseteq A}\,\wedge\mathrm{L}}{\forall a \forall b\,((a \subseteq b) \Leftrightarrow (\forall x\,(x \in a \Rightarrow x \in b))) \vdash A \subseteq A}\,\forall\mathrm{L} \times 2$$

Deduction Modulo and Superdeduction

Inclusion

$$\forall a \forall b\, ((a \subseteq b) \rightarrow (\forall x\, (x \in a \Rightarrow x \in b)))$$

Rewrite Rule

$$(a \subseteq b) \rightarrow (\forall x\, (x \in a \Rightarrow x \in b))$$

Proof in Deduction Modulo

$$\dfrac{\dfrac{\dfrac{}{x \in A \vdash x \in A}\,\mathrm{Ax}}{\vdash x \in A \Rightarrow x \in A}\,\Rightarrow\mathrm{R}}{\vdash A \subseteq A}\,\forall\mathrm{R},\ A \subseteq A \rightarrow \forall x\, (x \in A \Rightarrow x \in A)$$

Inclusion

$$\forall a \forall b\, ((a \subseteq b) \rightarrow (\forall x\, (x \in a \Rightarrow x \in b)))$$

Computation of the Superdeduction Rule

$$\frac{\Gamma \vdash \forall x\, (x \in a \Rightarrow x \in b), \Delta}{\Gamma \vdash a \subseteq b, \Delta}$$

Deduction Modulo and Superdeduction

Inclusion

$$\forall a \forall b\, ((a \subseteq b) \to (\forall x\, (x \in a \Rightarrow x \in b)))$$

Computation of the Superdeduction Rule

$$\dfrac{\dfrac{\dfrac{\Gamma, x \in a \vdash x \in b, \Delta}{\Gamma \vdash x \in a \Rightarrow x \in b, \Delta}\Rightarrow\mathrm{R}}{\Gamma \vdash \forall x\, (x \in a \Rightarrow x \in b), \Delta}\forall\mathrm{R},\ x \notin \Gamma, \Delta}{\Gamma \vdash a \subseteq b, \Delta}$$

Deduction Modulo and Superdeduction

Inclusion

$$\forall a \forall b\, ((a \subseteq b) \rightarrow (\forall x\, (x \in a \Rightarrow x \in b)))$$

Computation of the Superdeduction Rule

$$\frac{\Gamma, x \in a \vdash x \in b, \Delta}{\Gamma \vdash a \subseteq b, \Delta}\ \mathrm{IncR},\ x \notin \Gamma, \Delta$$

Proof in Superdeduction

$$\dfrac{\dfrac{}{x \in A \vdash x \in A}\ \mathrm{Ax}}{\vdash A \subseteq A}\ \mathrm{IncR}$$

The Tableau Method

- We start from the negation of the goal (no clausal form) ;
- We apply the rules in a top-down fashion ;
- We build a tree whose each branch must be closed ;
- When the tree is closed, we have a proof of the goal.

Closure and Cut Rules

$$\frac{\bot}{\odot}\ \odot_\bot \qquad \frac{\neg\top}{\odot}\ \odot_{\neg\top} \qquad \frac{}{P \mid \neg P}\ \text{cut}$$

$$\frac{\neg R_r(t,t)}{\odot}\ \odot_r \qquad \frac{P \quad \neg P}{\odot}\ \odot \qquad \frac{R_s(a,b) \quad \neg R_s(b,a)}{\odot}\ \odot_s$$

Integrating Superdeduction to Zenon

Analytic Rules

$$\frac{\neg\neg P}{P}\ \alpha_{\neg\neg} \qquad \frac{P \Leftrightarrow Q}{\neg P, \neg Q \mid P, Q}\ \beta_{\Leftrightarrow} \qquad \frac{\neg(P \Leftrightarrow Q)}{\neg P, Q \mid P, \neg Q}\ \beta_{\neg\Leftrightarrow}$$

$$\frac{P \wedge Q}{P, Q}\ \alpha_{\wedge} \qquad \frac{\neg(P \vee Q)}{\neg P, \neg Q}\ \alpha_{\neg\vee} \qquad \frac{\neg(P \Rightarrow Q)}{P, \neg Q}\ \alpha_{\neg\Rightarrow}$$

$$\frac{P \vee Q}{P \mid Q}\ \beta_{\vee} \qquad \frac{\neg(P \wedge Q)}{\neg P \mid \neg Q}\ \beta_{\neg\wedge} \qquad \frac{P \Rightarrow Q}{\neg P \mid Q}\ \beta_{\Rightarrow}$$

$$\frac{\exists x\ P(x)}{P(\epsilon(x).P(x))}\ \delta_{\exists} \qquad \frac{\neg\forall x\ P(x)}{\neg P(\epsilon(x).\neg P(x))}\ \delta_{\neg\forall}$$

Integrating Superdeduction to Zenon

γ-Rules

$$\frac{\forall x\ P(x)}{P(X)}\ \gamma_{\forall M} \qquad \frac{\neg\exists x\ P(x)}{\neg P(X)}\ \gamma_{\neg\exists M}$$

$$\frac{\forall x\ P(x)}{P(t)}\ \gamma_{\forall \mathrm{inst}} \qquad \frac{\neg\exists x\ P(x)}{\neg P(t)}\ \gamma_{\neg\exists \mathrm{inst}}$$

Relational Rules

- Equality, reflexive, symmetric, transitive rules ;
- Are not involved in the computation of superdeduction rules.

Computation of Superdeduction Rules

- $\mathcal{S} \equiv$ closure rules, analytic rules, $\gamma_{\forall M}$ and $\gamma_{\neg\exists M}$ rules ;
- Axiom : $R : P \rightarrow \varphi$;
- A positive superdeduction rule R (and a negative one $\neg R$) :
  - We initialize the procedure with the formula φ ;
  - We apply the rules of $\mathcal{S}$ until there is no applicable rule anymore ;
  - We collect the premises and the conclusion, and replace φ by P.
- If metavariables, we add an instantiation rule R_{inst} (or $\neg R_{\text{inst}}$).

Example (inclusion)

$$\dfrac{\dfrac{\forall x\,(x \in a \Rightarrow x \in b)}{X \in a \Rightarrow X \in b}\,\gamma_{\forall M}}{X \notin a \mid X \in b}\,\beta_{\Rightarrow}$$

$$\dfrac{\dfrac{\neg\forall x\,(x \in a \Rightarrow x \in b)}{\neg(\epsilon_x \in a \Rightarrow \epsilon_x \in b)}\,\delta_{\neg\forall}}{\epsilon_x \in a, \epsilon_x \notin b}\,\alpha_{\neg\Rightarrow}$$

with $\epsilon_x = \epsilon(x).\neg(x \in a \Rightarrow x \in b)$

Integrating Superdeduction to Zenon

Computation of Superdeduction Rules

- $\mathcal{S} \equiv$ closure rules, analytic rules, $\gamma_{\forall M}$ and $\gamma_{\neg\exists M}$ rules ;
- Axiom : $R : P \rightarrow \varphi$;
- A positive superdeduction rule R (and a negative one $\neg R$) :
  - We initialize the procedure with the formula φ ;
  - We apply the rules of $\mathcal{S}$ until there is no applicable rule anymore ;
  - We collect the premises and the conclusion, and replace φ by P.
- If metavariables, we add an instantiation rule R_{inst} (or $\neg R_{\text{inst}}$).

Example (inclusion)

$$\frac{a \subseteq b}{X \notin a \mid X \in b}\ \text{Inc} \qquad \frac{a \nsubseteq b}{\epsilon_X \in a, \epsilon_X \notin b}\ \neg\text{Inc}$$

with $\epsilon_X = \epsilon(x).\neg(x \in a \Rightarrow x \in b)$

Integrating Superdeduction to Zenon

Computation of Superdeduction Rules

- $\mathcal{S} \equiv$ closure rules, analytic rules, $\gamma_{\forall M}$ and $\gamma_{\neg\exists M}$ rules ;
- Axiom : $R : P \rightarrow \varphi$;
- A positive superdeduction rule R (and a negative one $\neg R$) :
  - We initialize the procedure with the formula φ ;
  - We apply the rules of $\mathcal{S}$ until there is no applicable rule anymore ;
  - We collect the premises and the conclusion, and replace φ by P.
- If metavariables, we add an instantiation rule R_{inst} (or $\neg R_{\mathrm{inst}}$).

Example (inclusion)

$$\frac{a \subseteq b}{X \notin a \mid X \in b}\ \mathrm{Inc} \qquad \frac{a \subseteq b}{t \notin a \mid t \in b}\ \mathrm{Inc_{inst}} \qquad \frac{a \not\subseteq b}{\epsilon_x \in a, \epsilon_x \notin b}\ \neg\mathrm{Inc}$$

with $\epsilon_x = \epsilon(x).\neg(x \in a \Rightarrow x \in b)$

Superdeduction Rules for the B Set Theory

Axioms (4 over 6)

$$(x, y) \in a \times b \Leftrightarrow x \in a \wedge y \in b$$
$$a \in \mathbb{P}(b) \Leftrightarrow \forall x \ (x \in a \Rightarrow x \in b)$$
$$x \in \{ \ y \mid P(y) \ \} \Leftrightarrow P(x)$$
$$a = b \Leftrightarrow \forall x \ (x \in a \Leftrightarrow x \in b)$$

Superdeduction Rules (Comprehension and Equality)

$$\frac{x \in \{ \ y \mid P(y) \ \}}{P(x)} \ \{|\} \qquad \frac{x \notin \{ \ y \mid P(y) \ \}}{\neg P(x)} \ \neg\{|\}$$

$$\frac{a = b}{X \notin a, X \notin b \mid X \in a, X \in b} \ = \qquad \frac{a \neq b}{\epsilon_x \notin a, \epsilon_x \in b \mid \epsilon_x \in a, \epsilon_x \notin b} \ \neq$$

with $\epsilon_x = \epsilon(x).\neg(x \in a \Leftrightarrow x \in b)$

Superdeduction Rules for the B Set Theory

Axioms (4 over 6)

$$(x, y) \in a \times b \rightarrow x \in a \wedge y \in b$$
$$a \in \mathbb{P}(b) \rightarrow \forall x\, (x \in a \Rightarrow x \in b)$$
$$x \in \{\, y \mid P(y) \,\} \rightarrow P(x)$$
$$a = b \rightarrow \forall x\, (x \in a \Leftrightarrow x \in b)$$

Superdeduction Rules (Comprehension and Equality)

$$\frac{x \in \{\, y \mid P(y) \,\}}{P(x)}\ \{|\} \qquad \frac{x \notin \{\, y \mid P(y) \,\}}{\neg P(x)}\ \neg\{|\}$$

$$\frac{a = b}{X \notin a, X \notin b \mid X \in a, X \in b}\ = \qquad \frac{a \neq b}{\epsilon_x \notin a, \epsilon_x \in b \mid \epsilon_x \in a, \epsilon_x \notin b}\ \neq$$

with $\epsilon_x = \epsilon(x).\neg(x \in a \Leftrightarrow x \in b)$

Superdeduction Rules for the B Set Theory

Definitions

$E \triangleq F$
$R : x \in E \to x \in F$
$a \cup b \triangleq \{ x \mid x \in a \vee x \in b \}$
$a \cap b \triangleq \{ x \mid x \in a \wedge x \in b \}$
$\cup : x \in a \cup b \to x \in \{ x \mid x \in a \vee x \in b \}$
$\cap : x \in a \cap b \to x \in \{ x \mid x \in a \wedge x \in b \}$

Superdeduction Rules (Union and Intersection)

$$\frac{x \in a \cup b}{x \in a \mid x \in b}\ \cup \qquad \frac{x \in a \cap b}{x \in a, x \in b}\ \cap$$

$$\frac{x \notin a \cup b}{x \notin a, x \notin b}\ \neg\cup \qquad \frac{x \notin a \cap b}{x \notin a \mid x \notin b}\ \neg\cap$$

Superdeduction Rules for the B Set Theory

Relations

$$E \triangleq F$$
$$R : (x, y) \in E \rightarrow (x, y) \in F$$
$$R : x \in E \rightarrow \exists y \exists z \ (x = (y, z) \wedge (y, z) \in F)$$

Superdeduction Rules (Inverse)

$$\frac{(x, y) \in a^{-1}}{(y, x) \in a} \ a^{-1} \qquad \frac{(x, y) \notin a^{-1}}{(y, x) \notin a} \ \neg a^{-1}$$

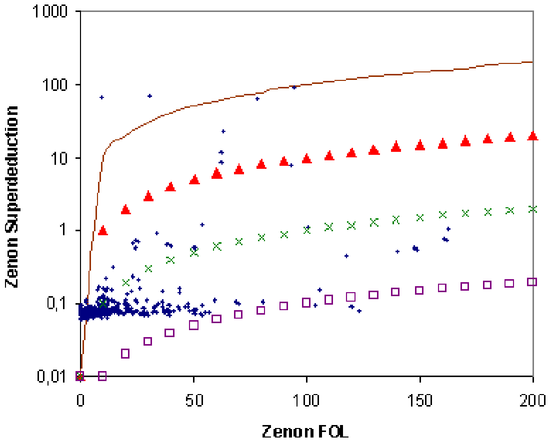
$$\frac{x \in a^{-1}}{x = (\epsilon_y, \epsilon_z), (\epsilon_z, \epsilon_y) \in a} \ a^{-1*}$$

with $\epsilon_y = \epsilon(y).(\exists z \ (x = (y, z) \wedge (y, z) \in a^{-1}))$

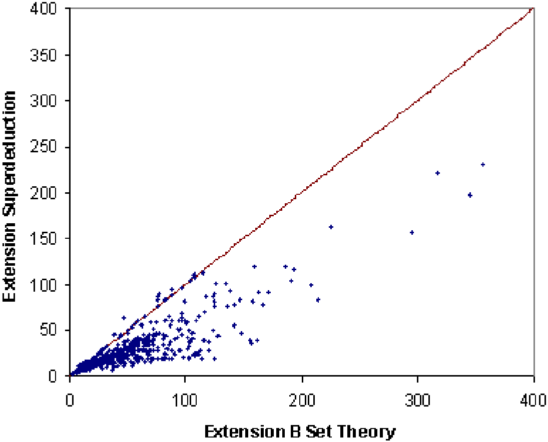
and $\epsilon_z = \epsilon(z).(x = (\epsilon_y, z) \wedge (\epsilon_y, z) \in a^{-1})$

$$\frac{x \notin a^{-1}}{x \neq (Y, Z) \mid (Z, Y) \notin a} \ \neg a^{-1*}$$

Superdeduction vs Pre-Normalization (Time)



Superdeduction vs Prawitz's Approach (Number of Nodes)



Benchmarks

Figures

- Number of rules that can be handled : 1397 rules ;
- Initial approach (with Zenon) : 1145 proved rules (82%) ;
- With Zenon extended to superdeduction :
  - 1340 proved rules (96%) ;
  - On average, proved 67 times faster (best ratio : 1,540).
- With Zenon à la Prawitz :
  - 1340 proved rules (96%) ;
  - On average, 1.6 times more nodes (best ratio : 6.25).
- See the IJCAR'12 paper for more details.

Remarks

- Initial approach with Zenon : problems of the preliminary normalization.
- No example due to incompleteness yet identified.

Generalization of the Approach

For any Theory

- Automated orientation of the theories ;
- Not oriented axioms left as axioms ;
- Superdeduction rules computed using other superdeduction rules ;
- New tool : Superdeduction + Zenon = Super Zenon !

Figures

- Over 6644 FOF problems of the TPTP library ;
- Zenon : 1612 proved problems ;
- Super Zenon :

Super Zenon

- Next CASC competition (IJCAR'12), FOFT and FOF divisions ;
- Download : `http://cedric.cnam.fr/~delahaye/super-zenon/`.

Generalization of the Approach

For any Theory

- Automated orientation of the theories ;
- Not oriented axioms left as axioms ;
- Superdeduction rules computed using other superdeduction rules ;
- New tool : Superdeduction + Zenon = Super Zenon !

Figures

- Over 6644 FOF problems of the TPTP library ;
- Zenon : 1612 proved problems ;
- Super Zenon : 2435 proved problems (increase of 12%).

Super Zenon

- Next CASC competition (IJCAR'12), FOFT and FOF divisions ;
- Download : http://cedric.cnam.fr/~delahaye/super-zenon/.

Demo