Polarized Rewriting and Tableaux in B Set Theory

SETS 2018

Olivier Hermant
CRI, MINES ParisTech, PSL Research University

June 5, 2018

PSL RESEARCH UNIVERSITY PARIS

MINES ParisTech

Institut Mines-Télécom

Introduction

- Assumes familiarity with FOL
- Tableaux method
- Extension with rewriting : Tableaux Modulo Theory
- Implementation and benchmark : Zenon Modulo and B Set theory
- Proposed extension : polarized rewriting
- Discussions

Tableaux Method

$$\frac{\bot}{\odot}\ \odot_{\bot} \qquad \frac{F, \neg F}{\odot}\ \odot \qquad \frac{\neg\top}{\odot}\ \odot_{\neg\top}$$

$$\frac{\neg\neg F}{F}\ \alpha_{\neg\neg} \qquad \frac{F \wedge G}{F, G}\ \alpha_{\wedge} \qquad \frac{\neg(F \vee G)}{\neg F, \neg G}\ \alpha_{\neg\vee} \qquad \frac{\neg(F \Rightarrow G)}{F, \neg G}\ \alpha_{\neg\Rightarrow}$$

$$\frac{F \vee G}{F \mid G}\ \beta_{\vee} \qquad \frac{\neg(F \wedge G)}{\neg F \mid \neg G}\ \beta_{\neg\wedge} \qquad \frac{F \Rightarrow G}{\neg F \mid G}\ \beta_{\Rightarrow}$$

$$\frac{\exists x\ F(x)}{F(c)}\ \delta_{\exists} \qquad \frac{\neg\forall x\ F(x)}{\neg F(c)}\ \delta_{\neg\forall}$$

$$\frac{\forall x\ F(x)}{F(t)}\ \gamma_{\forall} \qquad \frac{\neg\exists x\ F(x)}{\neg F(t)}\ \gamma_{\neg\exists}$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y \; X \subseteq Y \Leftrightarrow (\forall z \; z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y \; X \subseteq Y \Leftrightarrow (\forall z \; z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\forall X \forall Y \; X \subseteq Y \Leftrightarrow (\forall z \; z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\gamma_{\forall}\ \frac{\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)}{\forall y\ A \subseteq Y \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in Y)}$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\gamma_\forall \dfrac{\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)}{\gamma_\forall \dfrac{\forall y\ A \subseteq Y \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in Y)}{A \subseteq A \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in A)}}$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\alpha_\wedge \dfrac{\gamma_\forall \dfrac{\gamma_\forall \dfrac{{\color{red}\forall X} \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)}{{\color{red}\forall y}\ A \subseteq Y \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in Y)}}{A \subseteq A {\color{red}\Leftrightarrow} (\forall z\ z \in A \Rightarrow z \in A)}}{(\forall z\ z \in A \Rightarrow z \in A) {\color{red}\Rightarrow} A \subseteq A, A \subseteq A \Rightarrow (\forall z\ z \in A \Rightarrow z \in A)}$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\beta_{\Rightarrow}\ \alpha_{\wedge}\ \dfrac{\gamma_{\forall}\ \dfrac{\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)}{\gamma_{\forall}\ \dfrac{\forall y\ A \subseteq Y \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in Y)}{A \subseteq A \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in A)}}}{\dfrac{(\forall z\ z \in A \Rightarrow z \in A) \Rightarrow A \subseteq A, A \subseteq A \Rightarrow (\forall z\ z \in A \Rightarrow z \in A)}{A \subseteq A \quad | \quad \neg\forall z\ (z \in A \Rightarrow z \in A)}}$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\gamma_\forall \dfrac{\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)}{\gamma_\forall \dfrac{\forall y\ A \subseteq Y \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in Y)}{\alpha_\wedge \dfrac{A \subseteq A \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in A)}{\beta_\Rightarrow \dfrac{(\forall z\ z \in A \Rightarrow z \in A) \Rightarrow A \subseteq A, A \subseteq A \Rightarrow (\forall z\ z \in A \Rightarrow z \in A)}{\odot \dfrac{A \subseteq A}{\odot} \quad \mid \quad \neg \forall z\ (z \in A \Rightarrow z \in A)}}}}$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y \; X \subseteq Y \Leftrightarrow (\forall z \; z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y \; X \subseteq Y \Leftrightarrow (\forall z \; z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\beta_{\Rightarrow}\;\alpha_{\wedge}\;\cfrac{\gamma_{\forall}\;\cfrac{\forall X \forall Y \; X \subseteq Y \Leftrightarrow (\forall z \; z \in X \Rightarrow z \in Y), \neg(A \subseteq A)}{\gamma_{\forall}\;\cfrac{\forall y \; A \subseteq Y \Leftrightarrow (\forall z \; z \in A \Rightarrow z \in Y)}{A \subseteq A \Leftrightarrow (\forall z \; z \in A \Rightarrow z \in A)}}}{\cfrac{(\forall z \; z \in A \Rightarrow z \in A) \Rightarrow A \subseteq A, A \subseteq A \Rightarrow (\forall z \; z \in A \Rightarrow z \in A)}{\odot\;\cfrac{A \subseteq A}{\odot} \quad \Big| \quad \cfrac{\neg \forall z \; (z \in A \Rightarrow z \in A)}{\neg(c \in A \Rightarrow c \in A)}\;\delta_{\neg\forall}}}$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\gamma_\forall\ \frac{\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)}{\forall y\ A \subseteq Y \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in Y)}$$

$$\gamma_\forall\ \frac{\forall y\ A \subseteq Y \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in Y)}{A \subseteq A \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in A)}$$

$$\alpha_\wedge\ \frac{A \subseteq A \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in A)}{(\forall z\ z \in A \Rightarrow z \in A) \Rightarrow A \subseteq A, A \subseteq A \Rightarrow (\forall z\ z \in A \Rightarrow z \in A)}$$

$$\beta_\Rightarrow\ \frac{(\forall z\ z \in A \Rightarrow z \in A) \Rightarrow A \subseteq A, A \subseteq A \Rightarrow (\forall z\ z \in A \Rightarrow z \in A)}{A \subseteq A \quad | \quad \neg\forall z\ (z \in A \Rightarrow z \in A)}$$

$$\odot\ \frac{A \subseteq A}{\odot}$$

$$\frac{\neg\forall z\ (z \in A \Rightarrow z \in A)}{\neg(c \in A \Rightarrow c \in A)}\ \delta_{\neg\forall}$$

$$\frac{\neg(c \in A \Rightarrow c \in A)}{c \in A, \neg(c \in A)}\ \alpha_{\neg\Rightarrow}$$

Example : Inclusion

- we want to show $A \subseteq A$, for a given set A
- axiomatization of inclusion is

$$\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y)$$

- we shall refute $\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)$
- the proof :

$$\gamma_\forall\ \dfrac{\forall X \forall Y\ X \subseteq Y \Leftrightarrow (\forall z\ z \in X \Rightarrow z \in Y), \neg(A \subseteq A)}{\gamma_\forall\ \dfrac{\forall y\ A \subseteq Y \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in Y)}{\alpha_\wedge\ \dfrac{A \subseteq A \Leftrightarrow (\forall z\ z \in A \Rightarrow z \in A)}{\beta_\Rightarrow\ \dfrac{(\forall z\ z \in A \Rightarrow z \in A) \Rightarrow A \subseteq A, A \subseteq A \Rightarrow (\forall z\ z \in A \Rightarrow z \in A)}{\odot\ \dfrac{A \subseteq A}{\odot} \quad \Big| \quad \dfrac{\neg \forall z\ (z \in A \Rightarrow z \in A)}{\dfrac{\neg(c \in A \Rightarrow c \in A)}{\dfrac{c \in A, \neg(c \in A)}{\odot}\ \odot}\ \alpha_{\neg\Rightarrow}}\ \delta_{\neg\forall}}}}}$$

Deduction Modulo Theory

Rewrite Rule

A term (resp. proposition) rewrite rule is a pair of terms (resp. formulæ) $l \to r$, where $\mathcal{FV}(l) \subseteq \mathcal{FV}(r)$ and, in the propositiona case, l is atomic.

Examples :

- term rewrite rule :

$$a \cup \emptyset \to a$$

- proposition rewrite rule :

$$a \subseteq b \to \forall x \; x \in a \Rightarrow x \in b$$

Conversion modulo a Rewrite System

We consider the congruence $\equiv$ generated by a set of proposition rewrite rules $\mathcal{R}$ and a set of term rewrite rules $\mathcal{E}$ (often implicit). Forward-only rewriting is denoted $\twoheadrightarrow$.

Example :

$$A \cup \emptyset \subseteq A \quad \equiv \quad \forall x \; x \in A \Rightarrow x \in A$$

Tableaux Modulo Theory

- two flavors, essentially equivalent
- add a conversion rule :

$$\frac{F}{G}\,(Conv),\ \text{if } F \equiv G$$

- or integrate conversion inside each rule :

$$\frac{H}{F, G}\,\alpha_{\wedge},\ \text{if } H \equiv F \wedge G$$

Example : Inclusion

- delete the axiom $\forall X \forall Y\ (X \subseteq Y \Leftrightarrow \forall z\ z \in X \Rightarrow z \in Y)$
- replace with the rewrite rule $X \subseteq Y \rightarrow \forall z\ z \in X \Rightarrow z \in Y$
- we now refute only $\neg(A \subseteq A)$

Example : Inclusion

- delete the axiom $\forall X \forall Y \; (X \subseteq Y \Leftrightarrow \forall z \; z \in X \Rightarrow z \in Y)$
- replace with the rewrite rule $X \subseteq Y \rightarrow \forall z \; z \in X \Rightarrow z \in Y$
- we now refute only $\neg(A \subseteq A)$
- yields

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg(A \subseteq A)}{\neg(\forall z \; z \in A \Rightarrow z \in A)}\,(Conv)}{\neg(c \in A \Rightarrow c \in A)}\,\alpha_{\neg\forall}}{\neg(c \in A), c \in A}\,\alpha_{\neg\Rightarrow}}{\odot}\,\odot$$

Expressing B Set Theory with Rewriting

- for power set and comprehension

$$s \in \mathbb{P}(t) \longrightarrow \forall x \cdot (x \in s \Rightarrow x \in t)$$
$$x \in \{z \mid P(z)\} \longrightarrow P(x)$$

- derived constructs
- with typing, too

$$s \in_{\textbf{set}(\alpha)} \mathbb{P}_\alpha(t) \longrightarrow \forall x : \alpha \cdot (x \in_\alpha s \Rightarrow x \in_\alpha t)$$

Zenon

- Zenon : classical first-order tableaux-based ATP
- Extended to **ML polymorphism**
- Extended to **Deduction Modulo Theory**
- Extended to **linear arithmetic**
- Reads TPTP input format
- Dedukti certificates
- work of P. Halmagrand, G. Bury

Zenon

- Zenon : classical first-order tableaux-based ATP
- Extended to **ML polymorphism**
- Extended to **Deduction Modulo Theory**
- Extended to **linear arithmetic**
- Reads TPTP input format
- Dedukti certificates
- work of P. Halmagrand, G. Bury
- We propose to extend it to **Polarized** Deduction Modulo Theory

Benchmarks

A set of Proof Obligations

- Provided by Industrial Partners
- 12.876 PO
- Provable : proved in Atelier B (automatically or interactively)
- Wide spectrum
- Mild difficulty, large files

Zenon results

	All Tools (98,9%)					
12.876	mp	Zenon	Zenon Types	Zenon Arith	Zenon Modulo	Zenon Mod+Ari
%	85%	2%	48%	57%	80%	95%
Time (s)	-	6,9	2,3	2,5	3,0	2,6
Unique	329	0	0	0	34	946

Protocol

- Processor Intel Xeon E5-2660 v2
- Timeout 120 s
- Memory 1 GiB

Polarized Rewriting

- **asymetry**
  - rewrite positive formulas a certain way
  - rewrite negative formulas another way
  - interchangeable : $F \twoheadrightarrow_{-} G$ iff $\neg F \twoheadrightarrow_{+} \neg G$
- let $\mathcal{R}_{+}$ and $\mathcal{R}_{-}$ be two sets of rewrite rules

Polarized Rewriting

$F \rightarrow_{+} G$ is there exists a positive (resp. negative) occurrence H in F, a substitution σ, and a rule $l \rightarrow r \in \mathcal{R}^{+}$ (resp. $\mathcal{R}^{-}$), such that $H = l\sigma$ and G is F where H has been replaced with $r\sigma$.

Tableaux Modulo Polarized Theory

- tableaux is one-sided, we need only positive rewriting
- add to first-order tableau, the conversion rule

$$\frac{F}{G} \twoheadrightarrow_+ \text{, if } F \twoheadrightarrow_+ G$$

- notice forward rewriting only

Example : Inclusion

- delete the axiom $\forall X \forall Y \ (X \subseteq Y \Leftrightarrow \forall z \ z \in X \Rightarrow z \in Y)$
- replace it with two rewrite rules
  - $X \subseteq Y \rightarrow_+ (\forall z \ z \in X \Rightarrow z \in Y)$,
  - $X \subseteq Y \rightarrow_- (f(X, Y) \in X \Rightarrow f(X, Y) \in Y)$
- f is a fresh symbol (Skolem symbol)
  - negative $\forall$ quantifiers can be Skolemized !
  - impossible in Deduction Modulo Theory : unpolarized rewriting
  - here positive rewriting applied in positive contexts, negative in negative contexts
  - “pre-apply” $\delta_{\neg\forall}$ and $\delta_{\exists}$: Skolemize

Example : Inclusion

- delete the axiom $\forall X \forall Y\ (X \subseteq Y \Leftrightarrow \forall z\ z \in X \Rightarrow z \in Y)$
- replace it with two rewrite rules
  - $X \subseteq Y \rightarrow_{+} (\forall z\ z \in X \Rightarrow z \in Y)$,
  - $X \subseteq Y \rightarrow_{-} (f(X, Y) \in X \Rightarrow f(X, Y) \in Y)$
- f is a fresh symbol (Skolem symbol)
  - negative $\forall$ quantifiers can be Skolemized !
  - impossible in Deduction Modulo Theory : unpolarized rewriting
  - here positive rewriting applied in positive contexts, negative in negative contexts
  - "pre-apply" $\delta_{\neg\forall}$ and $\delta_{\exists}$: Skolemize
- the proof becomes

$$\dfrac{\dfrac{\dfrac{\neg(A \subseteq A)}{\neg(f(A,A) \in A \Rightarrow f(A,A) \in A)}\ \twoheadrightarrow}{\neg(f(A,A) \in A), f(A,A) \in A}\ \alpha_{\neg\Rightarrow}}{\odot}\ \odot$$

Advantages

- Skolemization of the rules = a single Skolem symbol
  - instead of a fresh one for each δ-rule, even if the formula is the same
  - fixable with ϵ-Hilbert operator ?
- Skolemization at **pre-processing**, once and for all
- more axioms become rewrite rules
  - Deduction Modulo Theory, sole shape

$$\forall \overline{x}(P \Leftrightarrow F)$$

  - Polarization allows two more shapes
    - $\forall \overline{x}(P \Rightarrow F)$ turned into $P \rightarrow_{+} F$
    - $\forall \overline{x}(F \Rightarrow P)$ turned into $P \rightarrow_{-} F$
    - $\forall \overline{x}(P \Leftrightarrow F)$ subsumed

Issues

- Deciding rewriting in Deduction Modulo Theory :
  - strongly needs **non confusion**

    if $F \equiv G$, then they have the same main connective

  - needs **confluence**

    if $F \equiv G$, then there is H such that $F \twoheadrightarrow H \twoheadleftarrow G$

  - allows to have a simpler additional tableaux rule

$$\frac{F}{G}\ (Conv), \text{ if } F \equiv G$$

  - **termination** of rewriting helps, too
- the more rules, the more potential troubles
  - needs proper study (and definitions !)
- Completeness
  - not implied by confluence and termination
  - e.g. requires narrowing
  - we do not care much, except for nice theoretical results
  - performance is more important

Issues

- Deciding rewriting in Deduction Modulo Theory :
  - strongly needs **non confusion**

if $F \equiv G$, then they have the same main connective

  - needs **confluence**

if $F \equiv G$, then there is H such that $F \twoheadrightarrow H \twoheadleftarrow G$

  - allows to have a simpler additional tableaux rule

$$\frac{F}{G}\ (Conv),\ \text{if } F \twoheadrightarrow G$$

  - **termination** of rewriting helps, too
- the more rules, the more potential troubles
  - needs proper study (and definitions !)
- Completeness
  - not implied by confluence and termination
  - e.g. requires narrowing
  - we do not care much, except for nice theoretical results
  - performance is more important

Conclusion

- implement and test
- theory can come later
  - except soundness
  - develop proper notions of confluence, cut elimination, models, etc.
- which Skolemization ?