Nancy-Université – LORIA – mpii

Automating Theories in Intuitionistic Logic

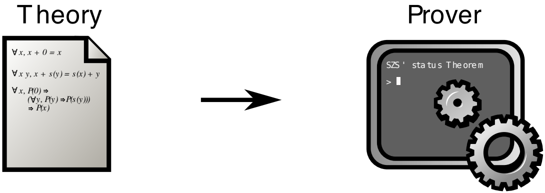
FroCoS'09

Guillaume Burel

Wednesday September 16th, 2009

Challenges

- Automating proof search in proof assistants
  ($\rightsquigarrow$ intuitionistic logic)
- Automating proof search in a given theory
  (e.g. arithmetic, set theory, . . .)



First approach

Use an axiomatization of the theory

- for instance Peano's axiomatization of first-order arithmetic

in a general theorem prover

Problem: Not adapted for proof search

1+1=2

In Γ:

$$\forall x,\ x + \mathsf{O} = x$$

$$\forall x\ y,\ x + s(y) = s(x + y)$$

$$\forall x\ y,\ x = y \Rightarrow X(x) \Rightarrow X(y)$$

$$\dfrac{\dfrac{\dfrac{}{\Gamma, \underline{1} + \mathsf{O} = \underline{1} \vdash \underline{1} + \mathsf{O} = \underline{1}, \underline{1} + \underline{1} = \underline{2}}\,\widehat{\vdash}}{\Gamma \vdash \underline{1} + \mathsf{O} = \underline{1}, \underline{1} + \underline{1} = \underline{2}}\,\forall\vdash \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}) \vdash \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}), \underline{1} + \underline{1} = \underline{2}}\,\widehat{\vdash}}{\Gamma \vdash \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}), \underline{1} + \underline{1} = \underline{2}}\,\forall\vdash \qquad \dfrac{}{\Gamma, \underline{1} + \underline{1} = \underline{2} \vdash \underline{1} + \underline{1} = \underline{2}}\,\widehat{\vdash}}{\Gamma, \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}) \Rightarrow \underline{1} + \underline{1} = \underline{2} \vdash \underline{1} + \underline{1} = \underline{2}}\,\Rightarrow\vdash}{\vdots}}{\dfrac{\Gamma, \underline{1} + \mathsf{O} = \underline{1} \Rightarrow \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}) \Rightarrow \underline{1} + \underline{1} = \underline{2} \vdash \underline{1} + \underline{1} = \underline{2}}{\Gamma \vdash \underline{1} + \underline{1} = \underline{2}}\,\forall\vdash}\,\Rightarrow\vdash$$

1+1=2

In Γ:

$$\forall x,\ x + \mathsf{O} = x$$

$$\forall x\ y,\ x + s(y) = s(x+y)$$

$$\forall x\ y,\ x = y \Rightarrow X(x) \Rightarrow X(y)$$

$$\frac{}{\Gamma, \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}) \vdash \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}), \underline{1} + \underline{1} = \underline{2}}\ \widehat{\vdash}$$

$$\frac{\Gamma, \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}) \vdash \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}), \underline{1} + \underline{1} = \underline{2}}{\Gamma \vdash \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}), \underline{1} + \underline{1} = \underline{2}}\ \forall\vdash$$

$$\frac{}{\Gamma, \underline{1} + \underline{1} = \underline{2} \vdash \underline{1} + \underline{1} = \underline{2}}\ \widehat{\vdash}$$

$$\frac{\Gamma \vdash \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}), \underline{1} + \underline{1} = \underline{2} \qquad \Gamma, \underline{1} + \underline{1} = \underline{2} \vdash \underline{1} + \underline{1} = \underline{2}}{\Gamma, \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}) \Rightarrow \underline{1} + \underline{1} = \underline{2} \vdash \underline{1} + \underline{1} = \underline{2}}\ \Rightarrow\vdash$$

$$\frac{}{\Gamma, \underline{1} + \mathsf{O} = \underline{1} \vdash \underline{1} + \mathsf{O} = \underline{1}, \underline{1} + \underline{1} = \underline{2}}\ \widehat{\vdash}$$

$$\frac{\Gamma, \underline{1} + \mathsf{O} = \underline{1} \vdash \underline{1} + \mathsf{O} = \underline{1}, \underline{1} + \underline{1} = \underline{2}}{\Gamma \vdash \underline{1} + \mathsf{O} = \underline{1}, \underline{1} + \underline{1} = \underline{2}}\ \forall\vdash$$

$$\frac{\Gamma \vdash \underline{1} + \mathsf{O} = \underline{1}, \underline{1} + \underline{1} = \underline{2} \qquad \vdots}{\Gamma, \underline{1} + \mathsf{O} = \underline{1} \Rightarrow \color{red}{\underline{1} + \underline{1} = s(}\underline{1} + \mathsf{O}\color{red}{)} \Rightarrow \underline{1} + \underline{1} = \underline{2} \vdash \underline{1} + \underline{1} = \underline{2}}\ \Rightarrow\vdash$$

$$\frac{\Gamma, \underline{1} + \mathsf{O} = \underline{1} \Rightarrow \underline{1} + \underline{1} = s(\underline{1} + \mathsf{O}) \Rightarrow \underline{1} + \underline{1} = \underline{2} \vdash \underline{1} + \underline{1} = \underline{2}}{\Gamma \vdash \underline{1} + \underline{1} = \underline{2}}\ \forall\vdash$$

Other approach

Use decision procedures specific to a theory

- for instance linear arithmetic and simplex

Combine them with a propositional prover $\rightsquigarrow$ SMT

Problem: Not generic

Poincaré's principle

In a proof, distinguish deduction from computation to better combine them

Deduction modulo: inference rules (deduction) are applied modulo a congruence (computation)

Universal model for computation: rewriting $\rightsquigarrow$ congruence based on a rewrite system over terms and formulæ

Example

$$x + \mathsf{0} \rightarrow x$$
$$x + s(y) \rightarrow s(x + y)$$

$$\mathsf{0} = \mathsf{0} \rightarrow \top$$
$$s(x) = s(y) \rightarrow x = y$$

$$\underline{1} + \underline{1} = \underline{2} \longrightarrow s(\underline{1} + \mathsf{0}) = \underline{2} \longrightarrow s(\underline{1}) = \underline{2} \stackrel{+}{\longrightarrow} \mathsf{0} = \mathsf{0} \longrightarrow \top$$

$$\vdash\!\top \; \frac{}{\vdash \underline{1} + \underline{1} = \underline{2}}$$

Theorem proving methods

Proof search procedures based on deduction modulo:

- ENAR: resolution with narrowing and E-unification
- TaMed: tableau method with narrowing

More efficient to search modulo the congruence

Note: To be complete, need cut admissibility (may not be the case in deduction modulo)

Encoding theories

Express a theory as a rewrite system

$\leadsto$ proof systems / proof-search procedures } adapted to that theory (provided cut admissibility holds)

Done by hand for:

- HOL [Dowek et al., 2003]
- Peano's arithmetic [Dowek and Werner, 2005]
- Zermelo's set theory [Dowek and Miquel, 2006]
- type theory [Burel, 2008]

Can this be automated?

Classical logic

Theorem 1 ([Burel and Kirchner, 2008]).
For every classical FO presentation of a theory Θ *there exists a rewrite system* $\mathcal{R}$ *such that* $\Theta \vdash P$ *iff* $\vdash^{cf}_{\mathcal{R}} P$

Use the fact that any axiom is classically equivalent to a formula $A \Leftrightarrow P$ with A atomic that can be oriented as $A \rightarrow P$

Not always possible in intuitionistic logic

Outline

- Introduction
- Negative results
- Transformation procedure
- Conclusion

Non-automatable theory

Proposition 2 (Disjunction property).
In intuitionistic logic, if the sequent calculus modulo $\mathcal{R}$ admits cuts, then $\vdash_{\mathcal{R}} A \vee B$ implies $\vdash_{\mathcal{R}} A$ or $\vdash_{\mathcal{R}} B$

Hence the theory presented by $A \vee B$ cannot be transformed into a rewrite system with a sequent calculus modulo admitting cuts

Undecidability of the automation

Theorem 3.
The set of presentations that can be transformed into a compatible rewrite system with a sequent calculus modulo admitting cuts is not co-recursively enumerable.

Sketch of proof: P is valid iff $(A \Rightarrow P) \vee A$ can be transformed into a compatible rewrite system with a sequent calculus modulo admitting cuts.

Outline

- Introduction
- Negative results
- Transformation procedure
  - Transition rules
  - Correctness
- Conclusion

Encoding procedure

No algorithm transforming an intuitionistic theory into a rewrite system with cut admissibility

However, a (possibly non-terminating) procedure using oracles

Transition rules $S, \mathcal{R} \rightsquigarrow S', \mathcal{R}'$
S, S': sets of sequents
$\mathcal{R}, \mathcal{R}'$: sets of rewrite rules

Starts with $\{\vdash P : P \text{ axiom of the theory}\}, \emptyset$

Example

Theory: $A \vee (B \Rightarrow A)$

S	$\mathcal{R}$
$\vdash A \vee (B \Rightarrow A)$	

Example

Theory: $A \vee (B \Rightarrow A)$

	S	$\mathcal{R}$
	$\vdash A \vee (B \Rightarrow A)$	
$\rightsquigarrow$	$\vdash A, B \Rightarrow A$	

$$\vdash\vee \frac{\vdash A, B \Rightarrow A}{\vdash A \vee (B \Rightarrow A)}$$ is invertible

Example

Theory: $A \vee (B \Rightarrow A)$

	S	$\mathcal{R}$
	$\vdash A \vee (B \Rightarrow A)$	
$\leadsto$	$\vdash A, B \Rightarrow A$	
$\leadsto$	$\vdash B \Rightarrow A$	

$A \vdash B \Rightarrow A$

Example

Theory: $A \vee (B \Rightarrow A)$

	S	$\mathcal{R}$
	$\vdash A \vee (B \Rightarrow A)$	
$\rightsquigarrow$	$\vdash A, B \Rightarrow A$	
$\rightsquigarrow$	$\vdash B \Rightarrow A$	
$\rightsquigarrow$	$B \vdash A$	

$$\vdash\Rightarrow \frac{B \vdash A}{\vdash B \Rightarrow A}$$ is invertible

Example

Theory: $A \vee (B \Rightarrow A)$

	S	$\mathcal{R}$
	$\vdash A \vee (B \Rightarrow A)$	
$\rightsquigarrow$	$\vdash A, B \Rightarrow A$	
$\rightsquigarrow$	$\vdash B \Rightarrow A$	
$\rightsquigarrow$	$B \vdash A$	
$\rightsquigarrow$		$B \longrightarrow^{-} A$

Orient

- $\Gamma, A \vdash \Delta \rightsquigarrow A \longrightarrow^{-} \forall x_1, \ldots, x_n, \bigwedge \Gamma \Rightarrow \bigvee \Delta$
- $\Gamma \vdash A \rightsquigarrow A \longrightarrow^{+} \exists x_1, \ldots, x_n, \bigwedge \Gamma$

A atomic, $x_1, \ldots, x_n$ variables free in Γ, Δ but not in A

Polarized rewrite rules: $\longrightarrow^{+}$ can only be applied at positive positions

Decompose

- $\Gamma \vdash \Delta \rightsquigarrow \bigcup_{1 \leq i \leq n} \{\Gamma_i \vdash \Delta_i\}$

if r $\dfrac{\Gamma_1 \vdash \Delta_1 \quad \cdots \quad \Gamma_n \vdash \Delta_n}{\Gamma \vdash \Delta}$ is invertible

To maximize the number of invertible rules: LBi

Only $\vdash\Rightarrow$ and $\vdash\forall$ with multiple conclusions are not invertible

Discard

- $S \cup \{\Gamma \vdash P, \Delta\}, \mathcal{R} \rightsquigarrow S \cup \{\Gamma \vdash \Delta\}, \mathcal{R}$

if $\Gamma, P \vdash^{S}_{\mathcal{R}} \Delta$

Drop conclusions that imply others

Delete

- $S \cup \{\Gamma \vdash \Delta\}, \mathcal{R} \rightsquigarrow S, \mathcal{R}$

if $\Gamma \vdash^{S}_{\mathcal{R}} \Delta$ without cut

Drop redundant axioms

Deduce

- $S, \mathcal{R} \rightsquigarrow S \cup \{\Gamma \vdash \Delta\}, \mathcal{R}$

if there is a critical proof of $\Gamma \vdash \Delta$ in $\mathcal{R}$:

$$\circlearrowleft\!\vdash \frac{\overset{\pi}{\Gamma, P \vdash \Delta} \qquad \overset{\pi'}{\Gamma \vdash Q, \Delta}}{\Gamma \vdash \Delta}$$

- $P \underset{\mathcal{R}}{\longleftarrow} A \underset{\mathcal{R}}{\longrightarrow} Q$;
- π and π' are cut-free;
- P (resp. Q) is the principal formula of the last inference rule of π (resp. π');
- all formulæ in Γ, Δ are principal in one of the inference rules of π or π';
- $\Gamma \not\vdash^{cf}_{\mathcal{R}} \Delta$

Ensures cut admissibility

Soundness

Proposition 4.

If $S, \mathcal{R} \rightsquigarrow S', \mathcal{R}'$ *then for all sequents* $\Gamma \vdash \Delta$*, we have* $\Gamma \vdash^{S}_{\mathcal{R}} \Delta$ *iff* $\Gamma \vdash^{S'}_{\mathcal{R}'} \Delta$

Moreover, $\Gamma \vdash^{S,cf}_{\mathcal{R}} \Delta$ *iff* $\Gamma \vdash^{S',cf}_{\mathcal{R}'} \Delta$

Corollary 5.

Given a presentation Θ*, if* $\{\vdash P : P \in \Theta\}, \emptyset \rightsquigarrow^* \emptyset, \mathcal{R}$*, then* $\Theta \vdash P$ *iff* $\vdash_{\mathcal{R}} P$

Fairness condition

At any moment with $S, \mathcal{R}$,
if $\Gamma \vdash \Delta \notin S$ is the conclusion of a critical proof in $\mathcal{R}$
then **Deduce** will eventually add $\Gamma \vdash \Delta$ in the set of sequents.

Proposition 6.

Under this fairness condition,
if the procedure terminates and produces $\emptyset, \mathcal{R}$
then cut admissibility holds modulo $\mathcal{R}$

Outline

- Introduction
- Negative results
- Transformation procedure
- Conclusion

Conclusion

From theories to automated theorem proving tools:

- transform axiomatic presentations into rewrite systems
- use these systems in provers based on deduction modulo

In the paper:

- equational sub-theories (using Knuth-Bendix)
- axiom schemata
- Skolemization

Further work

- Reduction of the non-determinism
  (confluence of the rewrite system)

- Towards an implementation
  (oracles for $\vdash_{\mathcal{R}}$ and the set of critical proofs?)

- Combination of theories

Baaz, M. and Iemhoff, R. (2008).
On Skolemization in constructive theories.
The Journal of Symbolic Logic, 73(3):969–998.

Burel, G. (2008).
A first-order representation of pure type systems using superdeduction.
In Pfenning, F., editor, *LICS*, pages 253–263. IEEE Computer Society.

Burel, G. and Kirchner, C. (2007).
Cut elimination in deduction modulo by abstract completion.
In Artemov, S. N. and Nerode, A., editors, *LFCS*, volume 4514 of *LNCS*, pages 115–131. Springer.

Burel, G. and Kirchner, C. (2008).

Regaining cut admissibility in deduction modulo using abstract completion.
Submitted.

Dowek, G. (2002).
What is a theory?
In Alt, H. and Ferreira, A., editors, *STACS*, volume 2285 of *LNCS*, pages 50–64. Springer.

Dowek, G. (2003).
Confluence as a cut elimination property.
In Nieuwenhuis, R., editor, *RTA*, volume 2706 of *LNCS*, pages 2–13. Springer.

Dowek, G., Hardin, T., and Kirchner, C. (2003).
Theorem proving modulo.
Journal of Automated Reasoning, 31(1):33–72.

Dowek, G. and Miquel, A. (2006).
Cut elimination for Zermelo's set theory.
Available on authors' web page.

Dowek, G. and Werner, B. (2005).
Arithmetic as a theory modulo.
In Giesl, J., editor, *RTA*, volume 3467 of *LNCS*, pages 423–437. Springer.

Kleene, S. C. (1967).
Mathematical Logic.
John Wiley, New York, USA.