Reasoning methods in Automated Theorem Proving

Presentation at BOREAL team's seminar

Julie Cailler

February 7, 2023

PhD student in the MaREL team
LIRMM, Université de Montpellier, CNRS

Formal methods and proofs

Formal methods

« Formal method are mathematically rigorous techniques for the specification, development, and verification of software and hardware systems. »

More precisely

- Critical system (life, money)
- Safety by proving ($\neq$ tests)
- But expensive and hard to understand

How to make a proof?

Data

- A language
- Some hypotheses (or not)
- A goal

Inference rules

$$\frac{H1 \qquad H2}{C}$$

How to make a proof?

Data

- A language
- Some hypotheses (or not)
- A goal

Inference rules

$$\frac{A \qquad A \Rightarrow B}{B}$$

Valid and satisifable

Validity

- Always true
- Proof by refutation ($\neg F$ is unsatisfiable)
- Theorem proving

Satisfiability

- True in at least one interpretation
- Building an interpretation
- Constraints solving, find bugs or counter-example

Many possibilites!

Different ways to make a proof

- Hand
- Proof assistant
- Automated theorem prover

Depending of the context

- Valid or satisfiable
- Logic (classical, modal, ...)
- Reasoning inside theories

Logic, expressivity and automation

Decidable Semi-decidable Undecidable

Propositional logic	Fragments of Theories	First-order logic	Higher-order logic	Intuitionist type theory

SAT provers	Decision procedure	SMT provers	First-order provers	Higher-order provers	Interactive proof assistants

Automation Expressiveness

Logic, expressivity and automation

Decidable	Semi-decidable	Undecidable

Propositional logic	Fragments of Theories	First-order logic	Higher-order logic	Intuitionist type theory

SAT provers	Decision procedure	SMT provers	First-order provers	Higher-order provers	Interactive proof assistants

Automation	Expressiveness

Many ways to prove, depending of what you get and what you want!

Automated reasoning

Automated reasoning

Automated theorem proving

Given a set of hypotheses and a goal, automatically find a proof!

Reasoning methods in first-order logic

- Saturation based methods
- Tableaux based methods
- Inverse method

Resolution

Context and use

- 1960 by Davis and Putnam
- Saturation based
- Split the original formula into clauses
- Resolve clauses and try to find the empty one

Pros

- Gives the best practical results
- Easy to implement

Cons

- Breaks the initial formula into clauses
- No proof

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

CNF :

$$\{\neg A\}, \{A \vee A\}, \{\neg B \vee A\}$$

$$\{\neg A\}$$

$$\{A \vee A\}$$

$$\{\neg B \vee A\}$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

CNF : $$\{\neg A\}, \{A \vee A\}, \{\neg B \vee A\}$$

$$\begin{tikzcd}
\{\neg A\} \arrow[dr, dash] & \\
\{A \vee A\} \arrow[r, dash] & \{A\} \\
\{\neg B \vee A\} &
\end{tikzcd}$$

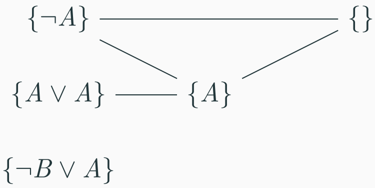
Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

CNF :

$$\{\neg A\}, \{A \vee A\}, \{\neg B \vee A\}$$



Method of analytics tableaux

Context and use

- 1955 by Beth and Hintikka
- Sequent based
- Tree structure
- Reduce goal to subgoals and try to solve them

Pros

- Gives a proof of the initial formula
- Useful in non-classical logic
- Good match with interactive theorem provers

Cons

- Slower than resolution
- Harder to implement

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

$$\dfrac{\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)}{(A \Rightarrow B) \Rightarrow A, \neg A}\ \alpha_{\neg\Rightarrow}$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

$$\cfrac{\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)}{\cfrac{(A \Rightarrow B) \Rightarrow A, \neg A}{\neg(A \Rightarrow B) \qquad A}\ \beta_{\Rightarrow}}\ \alpha_{\neg\Rightarrow}$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

$$\dfrac{\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)}{\dfrac{(A \Rightarrow B) \Rightarrow A, \neg A}{\dfrac{\neg(A \Rightarrow B)}{A, \neg B}\,\alpha_{\neg\Rightarrow} \qquad \dfrac{A}{\odot}\,\odot}\,\beta_{\Rightarrow}}\,\alpha_{\neg\Rightarrow}$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

$$\dfrac{\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)}{\dfrac{(A \Rightarrow B) \Rightarrow A, \neg A}{\dfrac{\neg(A \Rightarrow B)}{\dfrac{A, \neg B}{\odot}\ \odot}\ \alpha_{\neg\Rightarrow} \qquad \dfrac{A}{\odot}\ \odot}\ \beta_{\Rightarrow}}\ \alpha_{\neg\Rightarrow}$$

Inverse method

Context and use

- 1964 by S.Ju. Maslov
- Construct goals from previously proved subgoals
- Use a saturation algorithm
- Forward-chaining proof-search
- Subformula property

Pros

- Gives a proof of the initial formula
- Isomorphic to skolem chase

Cons

- Few implementations
- Slower than resolution and tableaux
- Harder to implement

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

Rules needed : $\dfrac{\neg P \qquad Q}{P \Rightarrow Q} \Rightarrow$ $\qquad \dfrac{P, \neg Q}{\neg(P \Rightarrow Q)} \neg\Rightarrow$

Available axioms : $\dfrac{}{\Gamma, A, \neg A}\, ax$ $\qquad \dfrac{}{\Gamma, B, \neg B}\, ax$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

Rules needed : $\dfrac{\neg P \qquad Q}{P \Rightarrow Q} \Rightarrow \qquad \dfrac{P, \neg Q}{\neg(P \Rightarrow Q)} \neg\Rightarrow$

Available axioms : $\dfrac{}{\Gamma, A, \neg A}\ ax \qquad \dfrac{}{\Gamma, B, \neg B}\ ax$

$$\dfrac{}{A, \neg A}\ ax$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

Rules needed :
$$\frac{\neg P \qquad Q}{P \Rightarrow Q} \Rightarrow \qquad \frac{P, \neg Q}{\neg(P \Rightarrow Q)} \neg\Rightarrow$$

Available axioms :
$$\frac{}{\Gamma, A, \neg A}\ ax \qquad \frac{}{\Gamma, B, \neg B}\ ax$$

$$\frac{}{A, \neg A, \neg B}\ ax$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

Rules needed :

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

Available axioms :

$$\frac{}{\Gamma, A, \neg A}\ ax \qquad \frac{}{\Gamma, B, \neg B}\ ax$$

$$\dfrac{\dfrac{}{A, \neg A, \neg B}\ ax}{\neg(A \Rightarrow B)} \neg \Rightarrow$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

Rules needed :
$$\frac{\neg P \qquad Q}{P \Rightarrow Q} \Rightarrow \qquad \frac{P, \neg Q}{\neg(P \Rightarrow Q)} \neg\Rightarrow$$

Available axioms :
$$\frac{}{\Gamma, A, \neg A}\, ax \qquad \frac{}{\Gamma, B, \neg B}\, ax$$

$$\frac{\dfrac{}{A, \neg A, \neg B}\, ax}{\neg(A \Rightarrow B)} \neg\Rightarrow \qquad \frac{}{A, \neg A}\, ax$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

Rules needed : $\dfrac{\neg P \qquad Q}{P \Rightarrow Q} \Rightarrow \qquad \dfrac{P, \neg Q}{\neg(P \Rightarrow Q)} \neg\Rightarrow$

Available axioms : $\dfrac{}{\Gamma, A, \neg A}\, ax \qquad \dfrac{}{\Gamma, B, \neg B}\, ax$

$$\dfrac{\dfrac{\dfrac{}{A, \neg A, \neg B}\, ax}{\neg(A \Rightarrow B)} \neg\Rightarrow \qquad \dfrac{}{A, \neg A}\, ax}{(A \Rightarrow B) \Rightarrow A} \Rightarrow$$

Example

Formula to prove

$$\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)$$

Rules needed : $\dfrac{\neg P \qquad\qquad Q}{P \Rightarrow Q} \Rightarrow \qquad \dfrac{P, \neg Q}{\neg(P \Rightarrow Q)} \neg \Rightarrow$

Available axioms : $\dfrac{}{\Gamma, A, \neg A}\, ax \qquad \dfrac{}{\Gamma, B, \neg B}\, ax$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A, \neg A, \neg B}\, ax}{\neg(A \Rightarrow B)} \neg \Rightarrow \qquad \dfrac{}{A, \neg A}\, ax}{(A \Rightarrow B) \Rightarrow A} \Rightarrow}{\neg(((A \Rightarrow B) \Rightarrow A) \Rightarrow A)} \neg \Rightarrow$$

To go further

Reasoning with theory

Core provers

- SAT solver
- First-order theorem prover
- ...

Specific provers

- Decision procedure
- Background reasoner
- Equality reasoning

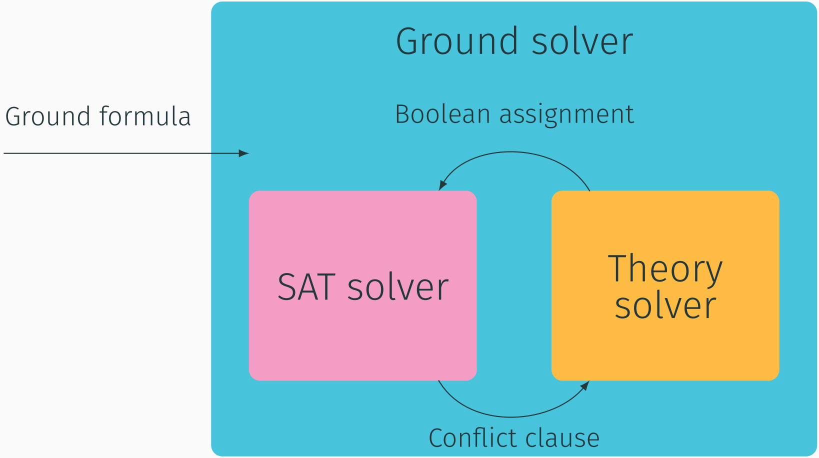
Nesting dolls principle

Expressive logic,
semi-automated tools
(ex : Proof assistants)

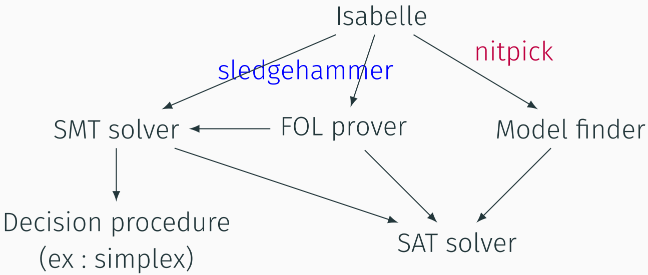
Limited logic,
efficient provers
(ex : SAT)

Intermediate tools
(ex : first-order prover,
background reasoners)

SMT = SAT + Theory solver



Isabelle


Isabelle
sledgehammer
nitpick
SMT solver
FOL prover
Model finder
Decision procedure
(ex : simplex)
SAT solver

Conclusion

Combinations of techniques

- Automated reasoning makes formal method more accessible
- Various methods for various situations
- Cooperation is the key

To go further

- Portfolio approach
- Unification
- Graph algorithms

Thank you for you attention!