Herbrand constructivization for automated intuitionistic theorem proving

Gabriel Ebner

TABLEAUX 2019
2019-09-03

TU Wien

Automated intuitionistic theorem proving

- Many proof assistants use intuitionistic logic
  - Coq, Agda, ...
  - some foundations even prove $\neg\forall p\, (p \vee \neg p)$
    - e.g. homotopy type theory
- Program synthesis via Curry-Howard

Automated intuitionistic theorem provers

- Connection calculus
  - ileanCoP, ...
- Inverse method
  - imogen, ...

- Intuitionistic Logic Theorem Proving library (ILTP; Raths, Otten, Kreitz 2006)
  - 2670 first-order problems
  - In total 1154 problems solved by existing provers
    - Vampire (classical prover) solves 2420

Proof constructivization

- Transform a classical proof into an intuitionistic proof

$\rightarrow$ Use a really good classical prover,
and then constructivize its proofs

Proof constructivization

Possible on multiple levels:

- Sequent calculus proofs
  - Glivenko classes (Orevkov 1968)
  - Recently for LK proofs generated by Zenon (Cauderlier 2016, Gilbert 2017)

- Lists of formulas (subsequents of the end-sequent)
  - Use classical prover to filter out assumptions
  - Often used in “hammers” for proof assistants
  - Requires another first-order prover

Proof constructivization

Possible on multiple levels:

- Sequent calculus proofs
  - Glivenko classes (Orevkov 1968)
  - Recently for LK proofs generated by Zenon (Cauderlier 2016, Gilbert 2017)

- **Expansion proofs ($\simeq$ quantifier inferences; our approach)**

- Lists of formulas (subsequents of the end-sequent)
  - Use classical prover to filter out assumptions
  - Often used in “hammers” for proof assistants
  - Requires another first-order prover

Theorem (special case of Herbrand 1930)

Let $\varphi(x)$ be a quantifier-free first-order formula.

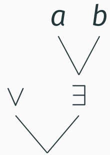
Then $\exists x\, \varphi(x)$ is valid in classical *logic iff there exist terms $t_1, \ldots, t_n$ such that $\varphi(t_1) \vee \cdots \vee \varphi(t_n)$ is a quasi-tautology.*

Quasi-tautology = tautology modulo equality.

Expansion proofs generalize to HOL (Miller 1987)

Expansion trees/proofs

- Natural data structure for non-prenex formulas



$$p(f(a)) \vee p(f(b)) \rightarrow \exists x\, p(f(x))$$

- c.f. global substitution in tableaux provers, quantifier instances in SMT solvers

Why expansion proofs?

- Abstracts away from propositional reasoning
  - and also equational reasoning!
- Deskolemization is straightforward
  - Skolemization unsound as preprocessing:
    $(\neg\forall x\, P(x)) \rightarrow \exists x\, \neg P(x)$
    $(\neg P(c)) \rightarrow \exists x\, \neg P(x)$

Problem statement

Given an expansion proof E of a sequent S,
find a cut-free proof in mLJ using only quantifier inferences from E

(without repeating an eigenvariable inference on any thread of the proof)

mLJ = multi-succedent calculus for intuitionistic logic (Maehara 1954)

Maehara's multi-succedent calculus (mLJ)

$$\frac{}{\varphi \vdash \varphi}\,\text{ax} \quad \frac{\Gamma \vdash \Delta}{\varphi, \Gamma \vdash \Delta}\,w_l \quad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, \varphi}\,w_r \quad \frac{\Gamma \vdash \Delta, \varphi \qquad \varphi, \Pi \vdash \Lambda}{\Gamma, \Pi \vdash \Delta, \Lambda}\,\text{cut}$$

$$\frac{}{\vdash t = t}\,\text{rfl} \quad \frac{\Gamma \vdash \Delta, \varphi(t)}{\Gamma, t = s \vdash \Delta, \varphi(s)}\,\text{eq}_r^{\rightarrow} \quad \frac{\Gamma \vdash \Delta, \varphi(s)}{\Gamma, t = s \vdash \Delta, \varphi(t)}\,\text{eq}_r^{\leftarrow}$$

$$\frac{\varphi(t), \Gamma \vdash \Delta}{\varphi(s), \Gamma, t = s \vdash \Delta}\,\text{eq}_l^{\rightarrow} \quad \frac{\varphi(s), \Gamma \vdash \Delta}{\varphi(t), \Gamma, t = s \vdash \Delta}\,\text{eq}_l^{\leftarrow}$$

$$\frac{}{\vdash \top}\,\top_r \quad \frac{}{\bot \vdash}\,\bot_l \quad \frac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, \varphi \vee \psi}\,\vee_r \quad \frac{\varphi, \Gamma \vdash \Delta \qquad \psi, \Gamma \vdash \Delta}{\varphi \vee \psi, \Gamma \vdash \Delta}\,\vee_l$$

$$\frac{\varphi, \psi, \Gamma \vdash \Delta}{\varphi \wedge \psi, \Gamma \vdash \Delta}\,\wedge_l \quad \frac{\Gamma \vdash \Delta, \varphi \qquad \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \wedge \psi}\,\wedge_r$$

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\,\to_r \quad \frac{\Gamma \vdash \Delta, \varphi \qquad \psi, \Gamma \vdash \Delta}{\varphi \to \psi, \Gamma \vdash \Delta}\,\to_l$$

$$\frac{\Gamma \vdash \Delta, \varphi(t)}{\Gamma \vdash \Delta, \exists x\, \varphi(x)}\,\exists_r \quad \frac{\varphi(\alpha), \Gamma \vdash \Delta}{\exists x\, \varphi(x), \Gamma \vdash \Delta}\,\exists_l \quad \frac{\varphi(t), \Gamma \vdash \Delta}{\forall x\, \varphi(x), \Gamma \vdash \Delta}\,\forall_l \quad \frac{\Gamma \vdash \varphi(\alpha)}{\Gamma \vdash \forall x\, \varphi(x)}\,\forall_r$$

Maehara's multi-succedent calculus (mLJ)

- Only three restrictions on the succedent:

$$\frac{\varphi, \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \to \psi} \to_r$$

$$\frac{\varphi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi} \neg_r$$

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \forall x\, \varphi} \forall_r$$

Maehara's multi-succedent calculus (mLJ)

- Only three restrictions on the succedent:

$$\frac{\varphi, \Gamma \vdash \Delta, \psi}{\Gamma \vdash \Delta, \varphi \to \psi} \to_r \qquad \frac{\varphi, \Gamma \vdash \psi}{\Gamma \vdash \varphi \to \psi} \to_r$$

$$\frac{\varphi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi} \neg_r \qquad \frac{\varphi, \Gamma \vdash}{\Gamma \vdash \neg\varphi} \neg_r$$

$$\frac{\Gamma \vdash \Delta, \varphi}{\Gamma \vdash \Delta, \forall x\, \varphi} \forall_r \qquad \frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall x\, \varphi} \forall_r$$

SAT solvers

- Solve validity problem in classical propositional logic
- Equivalently: derivability via cut (and structural rules):
  Given a set of sequents $\mathcal{S}$ and a sequent T,
  can T be derived from $\mathcal{S}$ via cut?
- Already successfully used for propositional intuitionistic logic
  (Intuit prover; Claessen, Rosén 2015—however no proof output)

SAT encoding

- Can directly encode $\wedge, \vee, \rightarrow^-, \neg^-, \forall^-, \exists^+$:

$$\varphi \wedge \psi \vdash \varphi \qquad \varphi \wedge \psi \vdash \psi \qquad \varphi, \psi \vdash \varphi \wedge \psi$$

$$\varphi \vee \psi \vdash \varphi \qquad \varphi \vdash \varphi \vee \psi \qquad \psi \vdash \varphi \vee \psi$$

$$\varphi, \varphi \rightarrow \psi \vdash \psi \qquad \varphi, \neg\varphi \vdash$$

$$\forall x\, \varphi(x) \vdash \varphi(t) \qquad \varphi(t) \vdash \exists x\, \varphi(x)$$

  (where $\varphi \wedge \psi, \ldots$ are subformulas of the expansion proof, and $\varphi(t)$ is a quantifier instance in the expansion proof)

- Complete if no positive occurrences of $\rightarrow, \forall, \neg$ and no negative occurrences of $\exists$

Backtracking for $\exists_l, \forall_r, \rightarrow_r, \neg_r$

1. Is $\Gamma \vdash \Delta$ derivable?

2. If not, we get a countermodel. This corresponds to the conclusion of a bottom-most $\exists_l/\forall_r/\rightarrow_r/\neg_r$ inference in a cut-free proof of $\Gamma \vdash \Delta$, e.g.:

$$\frac{\Gamma' \vdash \Delta', \forall x\, \varphi(x)}{\Gamma \vdash \Delta}$$

(note that $\vee_{l,r}, \wedge_{l,r}, \rightarrow_l, \neg_l$ have been exhaustively applied)

3. Go back to 1: is $\Gamma' \vdash \varphi(\alpha)$ derivable?

Introduction

Constructivization procedure

Empirical evaluation

Conclusion

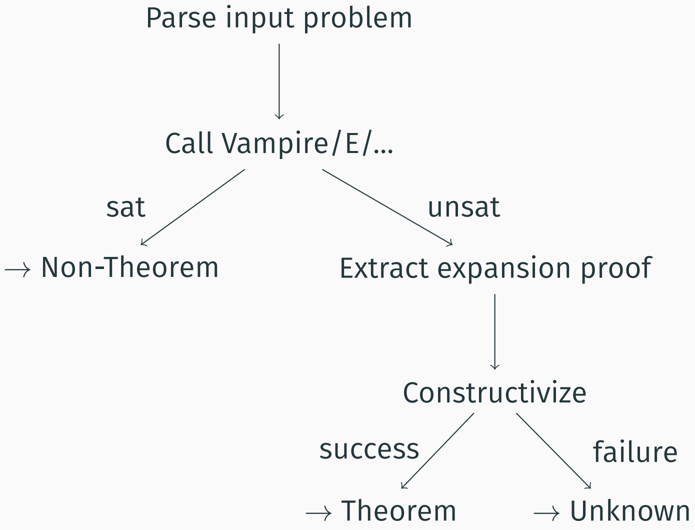
GAPT: General Architecture for Proof Theory

- open source, written in Scala
- `https://github.com/gapt/gapt`

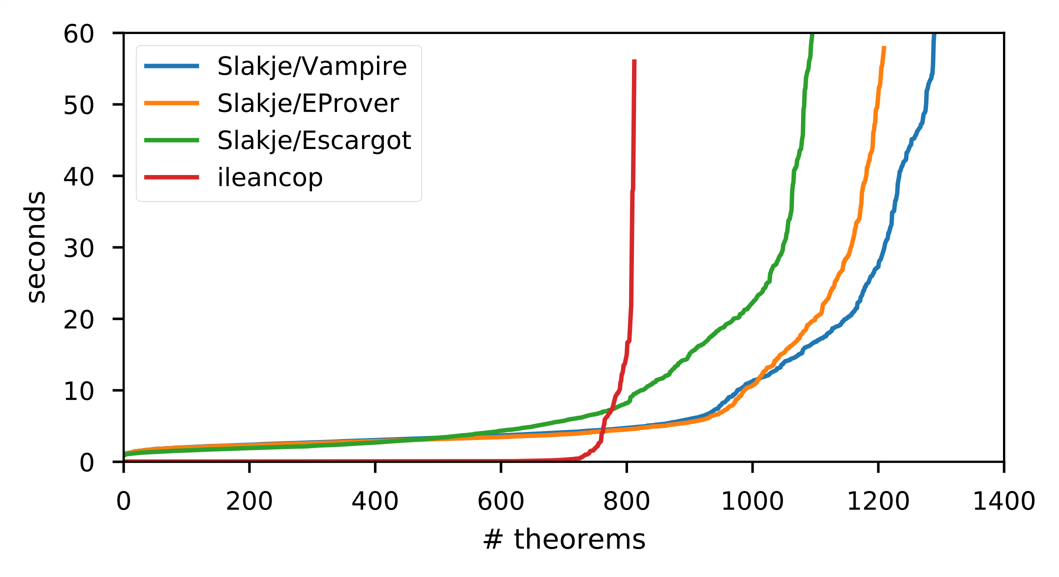
- Centered around Herbrand's theorem and expansion proofs

- Proof transformations: LK $\leftrightarrow$ ET $\leftrightarrow$ Res, cut-elimination, cut-introduction, Skolemization, deskolemization, ...
- Automated reasoning: proof import for 11 provers
- Proof visualization

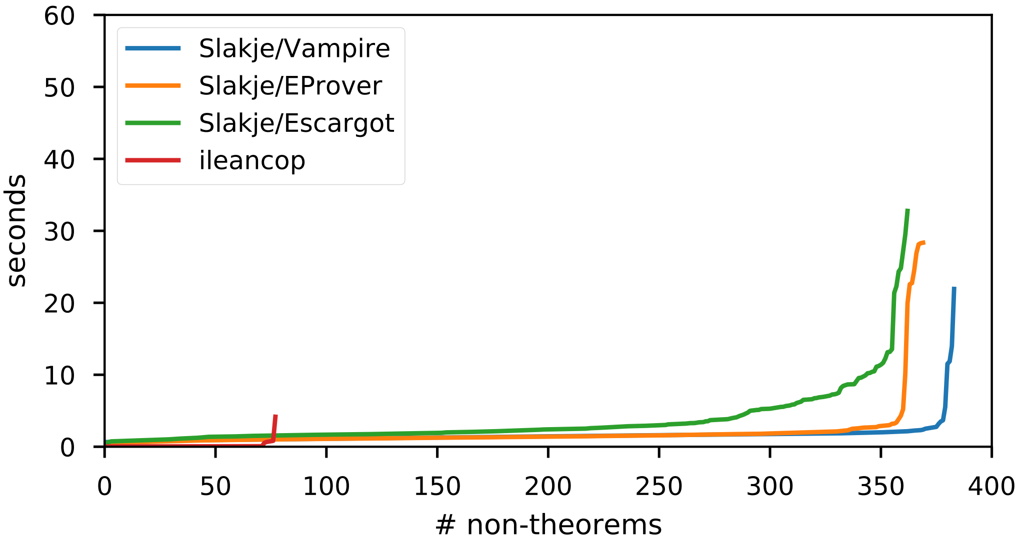
Prover architecture and implementation in Slakje (GAPT)



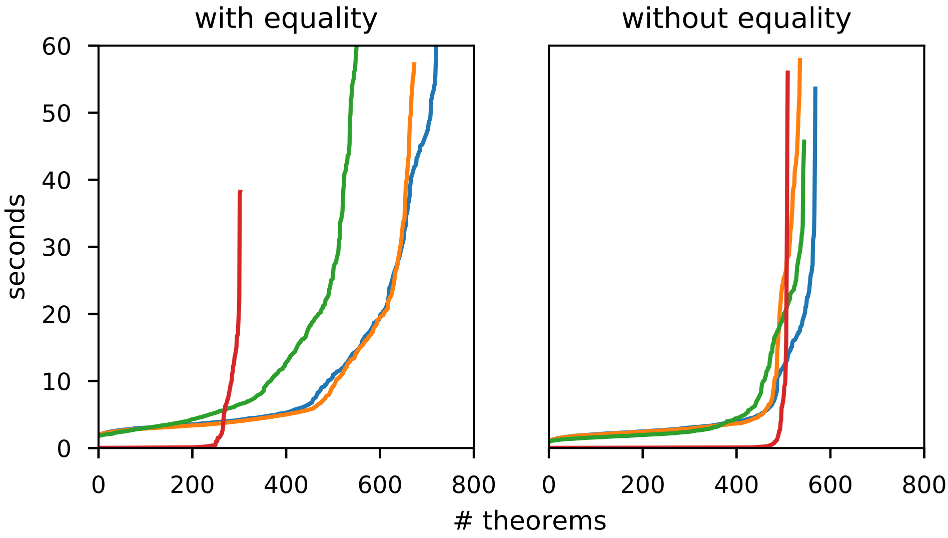
Empirical evaluation on the ILTP (theorems)



Empirical evaluation on the ILTP (non-theorems)



Empirical evaluation on the ILTP (equality)



Introduction

Constructivization procedure

Empirical evaluation

Conclusion

Conclusion

- Classical theorem proving seems to be fundamentally easier
- Dedicated equational reasoning is crucial
- Proof constructivization is a practical approach for automated intuitionistic theorem proving
- What to do about incompleteness?

Backup slides

Definition

A set of sequents $\mathcal{S}$ is a Glivenko class if:
$\forall S \in \mathcal{S}$: S intuitionistically provable $\Leftrightarrow$ S classically provable

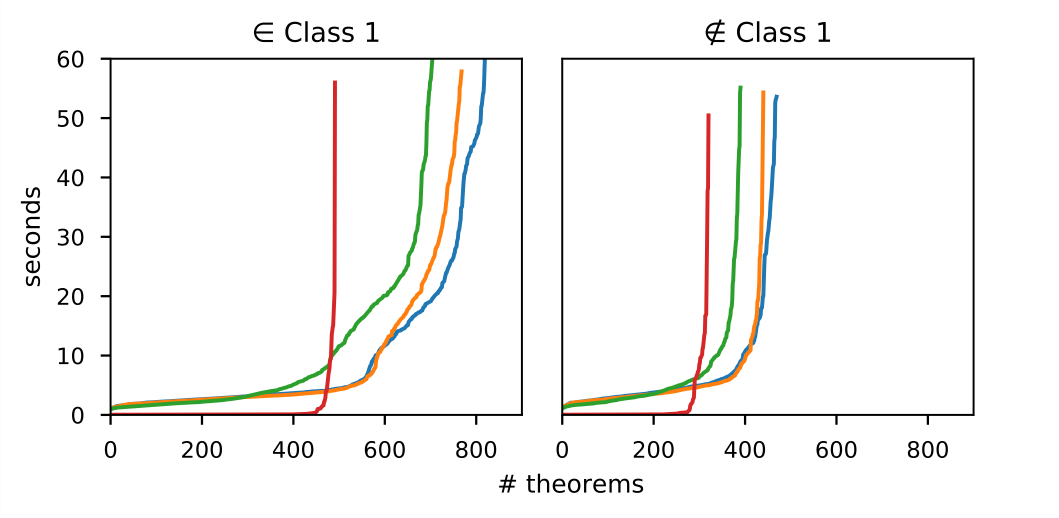
For example Class 1 (Orevkov 1968):
sequents without positive occurrences of $\to, \neg, \forall$

$$(\varphi \to \psi) \to \theta, \dots \vdash \dots \quad \neg\varphi \to \psi, \dots \vdash \dots \quad (\forall x\, \varphi) \to \psi, \dots \vdash \dots$$

Proof.
Every cut-free proof in LK of $S \in$ Class 1 is a proof in mLJ. □

(Slakje is complete for Class 1.)

Empirical evaluation on the ILTP (Class 1)



Empirical evaluation on the ILTP (all provers)