Herbrand constructivization for automated intuitionistic theorem proving

Gabriel Ebner

3rd FISP workshop
2018-12-08

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, jprover, ...
- Inverse method
    - imogen, ...

- Intuitionistic Logic Theorem Proving library (ILTP; Raths, Otten, Kreitz 2006)
    - 2670 first-order problems
    - In total 957 problems solved by known 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

Expansion trees/proofs

- Concise proof format
- Sound and complete in classical logic
- Captures just eigenvariables and weak quantifier terms

$$a \quad b$$

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

Why expansion proofs?

- Abstracts away from propositional reasoning
    - and also equational reasoning!
- Deskolemization is straightforward

Maehara's multi-succedent calculus (mG3i)

- LK with three restrictions:

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

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

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

Maehara’s multi-succedent calculus (mG3i)

- LK with three restrictions:

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

$$\cancel{\dfrac{\varphi, \Gamma \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi} \neg_r}$$

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

$$\dfrac{\varphi, \Gamma \vdash \psi}{\Gamma \vdash \varphi \to \psi} \to_r$$

$$\dfrac{\varphi, \Gamma \vdash}{\Gamma \vdash \neg\varphi} \neg_r$$

$$\dfrac{\Gamma \vdash \varphi}{\Gamma \vdash \forall x\, \varphi} \forall_r$$

Problem statement

Given an expansion proof E of a sequent S,
find a cut-free proof in mG3i using only quantifier inferences from E

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

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?

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 $\varphi \wedge \psi, \dots$ 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 $\exists_l, \forall_r, \to_r, \neg_r$

1. Is $\Gamma \vdash \Delta$ derivable?
2. If not, we get a countermodel. This corresponds to the conclusion of a bottom-most $\exists_l/\forall_r/\to_r/\neg_r$ 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 $\vee_{l,r}, \wedge_{l,r}, \to_l, \neg_l$ have been exhaustively applied)
3. Go back to 1: is $\Gamma' \vdash \varphi(\alpha)$ derivable?

- Already successfully used for propositional formulas (Claessen, Rosén 2015—however not proof-producing)

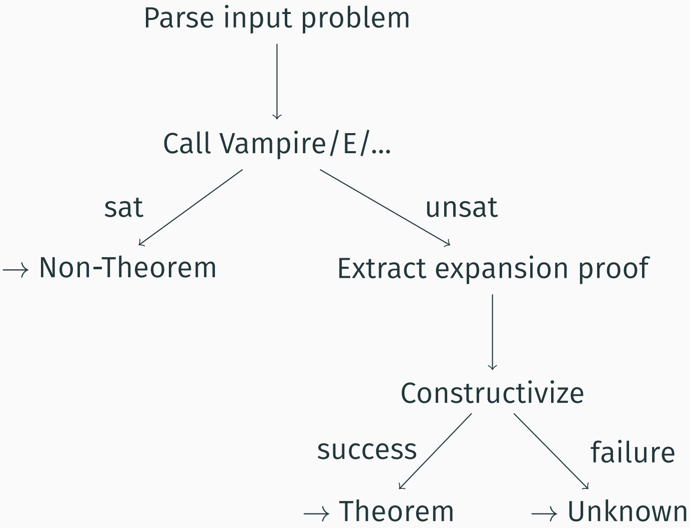
GAPT: General Architecture for Proof Theory

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

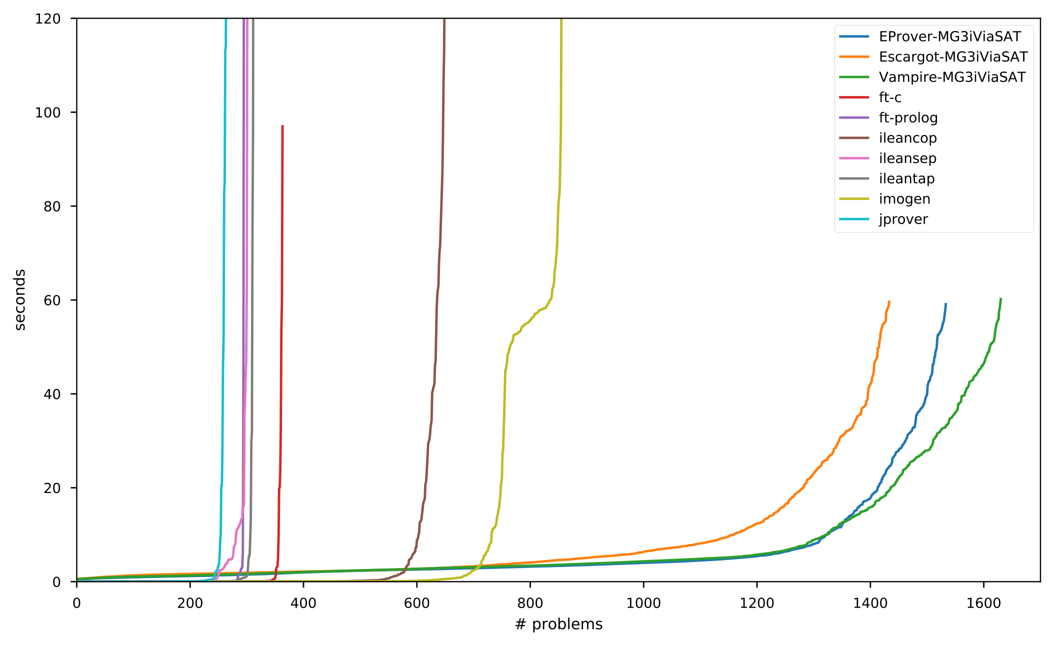
- Centered around Herbrand's theorem and expansion proofs

- 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

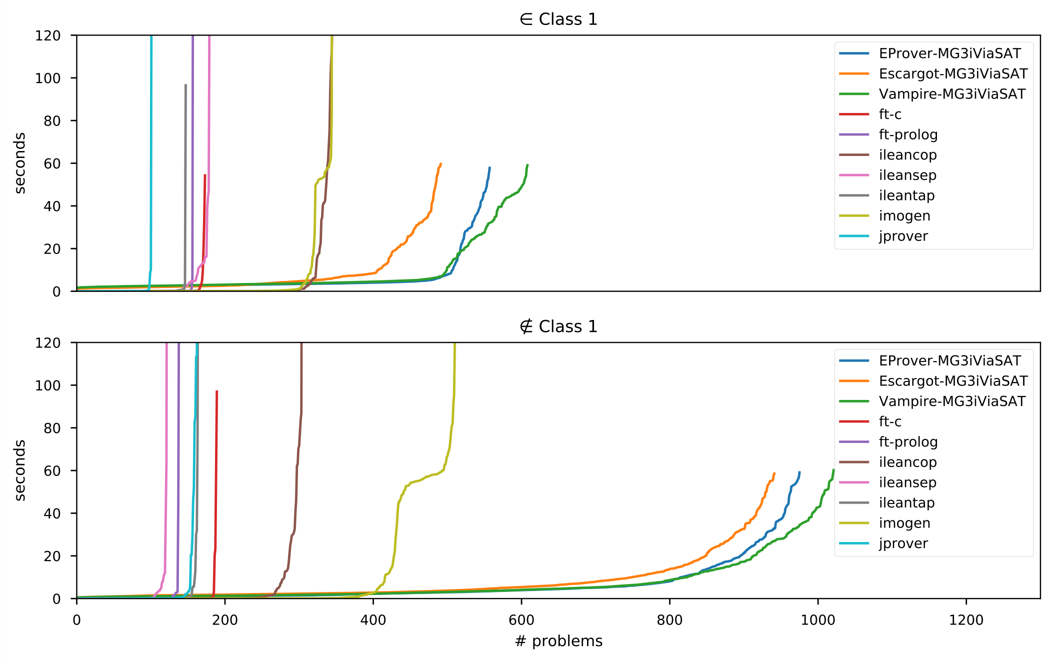


Conclusion

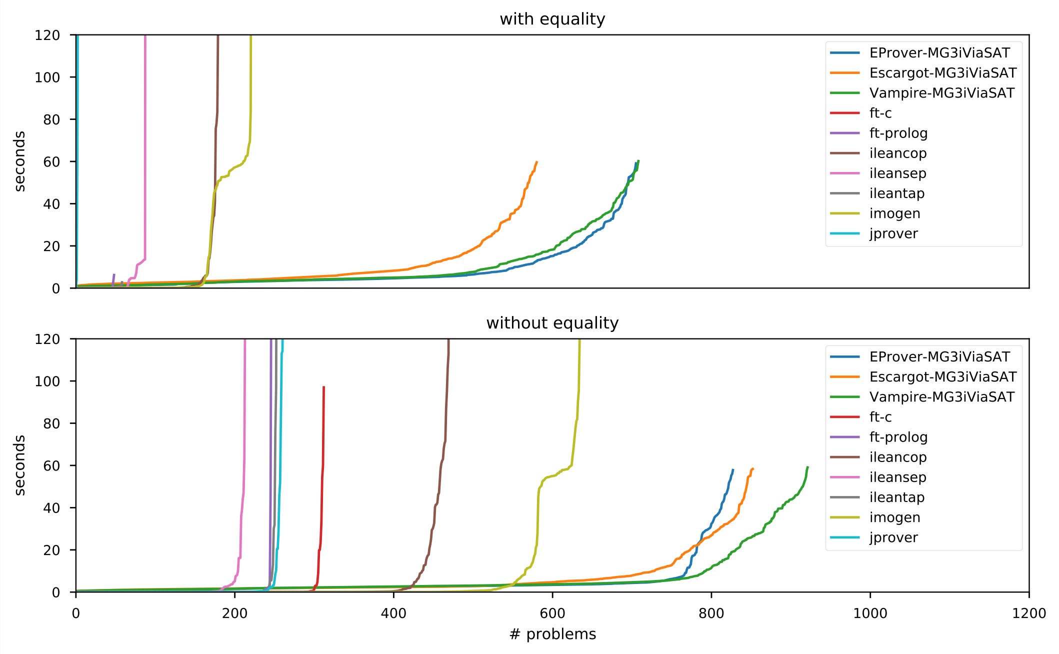
- Classical theorem proving seems to be fundamentally easier
- Proof constructivization is a practical approach for automated intuitionistic theorem proving
- What to do about incompleteness?
  - mine classical proofs of complete translations?
  - heuristic instantiation?

Backup slides

Empirical evaluation on the ILTP (Class 1)



Empirical evaluation on the ILTP (equality)



Glivenko classes

Definition

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

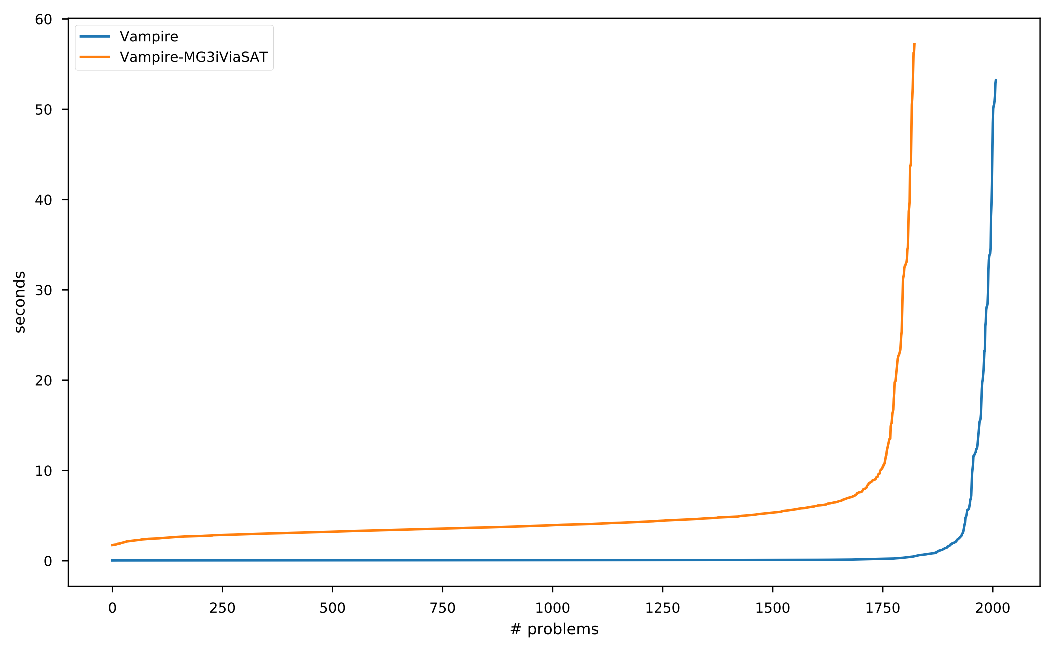
For example Class 1 (Orevkov 1968):
sequents without positive occurrences of $\rightarrow, \neg, \forall$

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

Proof.
Every cut-free proof in LK of $S \in$ Class 1 is a proof in mG3i. $\square$

(Slakje is complete for Class 1.)

Constructivization success on CoqHammer benchmarks



Empirical evaluation on the ILTP (all variants)